



Manual

Version 1.00

DWL-8200AP

Managed Dualband Access Point

Table of Contents

| | |
|------------------------------------|-----|
| Table of Contents | 2 |
| Package Contents | 3 |
| Introduction | 4 |
| Features and Benefits | 6 |
| Wireless Basics | 7 |
| Three Operational Modes | 10 |
| Getting Started | 11 |
| Using the Configuration Menu | 14 |
| Using the AP Manager | 59 |
| Networking Basics | 99 |
| Troubleshooting | 115 |
| Technical Specifications | 121 |
| Contacting Technical Support | 124 |
| Warranty | 125 |
| Registration | 129 |

Package Contents



- **D-Link Air Premier® DWL-8200AP**
Managed Dualband Access Point
- Power over Ethernet base unit
- Power Adapter-DC 48V, 0.4A
- Power Cord
- Manual and Warranty on CD
- Quick Installation Guide
- Ethernet Cable
- Mounting Plate

Note: Using a power supply with a different voltage than the one included with the **DWL-8200AP** will cause damage and void the warranty for this product.

If any of the above items are missing, please contact your reseller.

Minimum System Requirements

- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above
- At least 128MB of memory and a 500MHz processor

Introduction

At up to fifteen times the speed of previous wireless devices (maximum wireless signal rate of up to 108Mbps* in Super A and Super G mode), you can work faster and more efficiently, increasing productivity. With the **DWL-8200AP**, bandwidth-intensive applications like graphics or multimedia will benefit significantly because large files are able to move across the network quickly.

Inclusion of all three standards (802.11a; 802.11b; 802.11g) means that the **DWL-8200AP** is versatile enough to allow connection to almost any 802.11 network or device.

The **DWL-8200AP** is capable of operating in one of 3 different modes to meet your wireless networking needs. The **DWL-8200AP** can operate as an access point, or in WDS (Wireless Distribution System) with AP, or in WDS mode.

Use less wiring, enjoy increased flexibility, save time and money with PoE (Power over Ethernet). With PoE, the **DWL-8200AP** shares power and data over the CAT5 cable, making the setup of your network less expensive and more convenient.

An ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, trade shows and special events, the **DWL-8200AP** provides data transfers at up to 108Mbps in Super A and Super G mode when used with other D-Link **Air Premier**[®] or **Air Premier AG**[®] products (The 802.11g standard is backwards compatible with 802.11b devices).

WPA is offered in two flavors: **Enterprise** (used for corporations), and **Personal** (used for home users).

WPA-Personal and **WPA2-Personal** is directed at home users who do not have the server based equipment required for user authentication. The method of authentication is similar to WEP because you define a "Pre-Shared Key" on the wireless router/AP. Once the pre-shared key is confirmed and satisfied on both the client and access point, then access is granted. The encryption method used is referred to as the Temporal Key Integrity Protocol (TKIP), which offers per-packet dynamic hashing. It also includes an integrity checking feature which ensures that the packets were not tampered with during wireless transmission. **WPA2-Personal** is far superior to **WPA-Personal**, because the encryption of data is upgraded with the Advanced Encryption Standard (AES).

*Maximum wireless signal rate derived from IEEE Standard 802.11a and 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 actual data throughput rate.



WPA-Enterprise and **WPA2-Enterprise** is ideal for businesses that have existing security infrastructures in place. Management and security implementation can now be centralized on a server participating on the network. Utilizing 802.1x with a RADIUS (Remote Authentication Dial-in User Service) server, a network administrator can define a list of authorized users who can access the wireless LAN. When attempting to access a wireless LAN with either **WPA-Enterprise** or **WPA2-Enterprise** configured, the new client will be challenged with a username and password. If the new client is authorized by the administration, and enters the correct username and password, then access is granted. In a scenario where an employee leaves the company, the network administrator can remove the employee from the authorized list and not have to worry about the network being compromised by a former employee. **WPA2-Enterprise** is far superior to **WPA-Enterprise**, because the encryption of data is upgraded with the Advanced Encryption Standard (AES).

802.1x: Authentication which is a first line of defense against intrusion. In the authentication process, the Authentication Server verifies the identity of the client attempting to connect to the network. Unfamiliar clients would be denied access.

Features & Benefits

- **3 Different Operation modes** - Capable of operating in one of three different operation modes to meet your wireless networking requirements: Access Point; WDS with AP; or WDS.
- **Easy Installation with PoE (Power over Ethernet).**
- **Faster wireless networking** speeds up to 108Mbps* in Super A and Super G mode.
- **Compatible with 802.11a, 802.11b and 802.11g Devices** that is fully compatible with the IEEE 802.11a, 802.11b and 802.11g standards, the **DWL-8200AP** can connect with existing 802.11b-, 802.11g- or 802.11a-compliant wireless network adapter cards.
- **Compatible with the 802.11b standard** to provide a wireless data rate of up to 11Mbps - that means you can migrate your system to the 802.11g standard on your own schedule without sacrificing connectivity.
- **Better security with WPA** - The **DWL-8200AP** can securely connect wireless clients on the network using WPA (Wi-Fi Protected Access) providing a much higher level of security for your data and communications than has previously been available.
- **AP Manager Setup Wizard** - The new Setup Wizard makes network configuration quick and simple.
- **SNMP for Management** - The **DWL-8200AP** is not just fast but it also supports SNMP v.3 for a better network management. Superior wireless AP manager software is bundled with the **DWL-8200AP** for network configuration and firmware upgrade. Systems administrators can also setup the **DWL-8200AP** easily with the Web-based configuration. A D-Link D-View module will be downloadable for network administration and real-time network traffic monitoring with D-Link D-View software.
- Utilizes **OFDM** technology (**O**rtogonal **F**requency **D**ivision **M**ultiplexing).
- Operates in the 2.437GHz frequency range for an 802.11a network, and in the 5.26GHz frequency range for an 802.11b and 802.11g network.
- **Web-based interface** for managing and configuring.

*Maximum wireless signal rate derived from IEEE Standard 802.11a and 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 actual data throughput rate.

Wireless Basics

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

A Wireless Local Area Network (WLAN) is a computer network that transmits and receives data with radio signals instead of wires. WLANs 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.

People use WLAN technology for many different purposes:

Mobility - Productivity increases when people have access to data in any location within the operating range of the WLAN. Management decisions based on real-time information can significantly improve worker efficiency.

Low Implementation Costs - WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLANs ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.

Installation and Network Expansion - Installing a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Wireless technology allows the network to go where wires cannot go - even outside the home or office.

Inexpensive Solution - Wireless network devices are as competitively priced as conventional Ethernet network devices. The **DWL-8200AP** saves money by providing multi-functionality, configurable in one of three different modes.

Scalability - WLANs can be configured in a variety of ways to meet the needs of specific applications and installations. Configurations are easily changed and range from Peer-to-Peer networks suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Standards-based Technology

The **DWL-8200AP** Wireless Access Point utilizes the **802.11a**, **802.11b** and the **802.11g** standards.

The IEEE **802.11g** standard is an extension of the **802.11b** standard. It increases the maximum wireless signal rate of up to 54Mbps* (maximum wireless signal rate of up to 108Mbps* in Super G mode) within the 2.4GHz band, utilizing **OFDM technology**.

This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing **OFDM (Orthogonal Frequency Division Multiplexing)** technology. **OFDM** works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. **OFDM** reduces the amount of **crosstalk** (interference) in signal transmissions.

The D-Link **DWL-8200AP** will automatically sense the best possible connection speed to ensure the greatest speed and range possible.

The **DWL-8200AP** offers the most advanced network security features available today, including WPA and WPA2.

In addition to its compatibility with 802.11g and 802.11a devices, the **DWL-8200AP** is compatible with 802.11b devices. This means that if you have an existing 802.11b network, or a network with a mixture of 802.11g, 802.11a and 802.11b, the devices in that network will be compatible with the **DWL-8200AP**.

*Maximum wireless signal rate derived from IEEE Standard 802.11a and 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 actual data throughput rate.

Installation Considerations

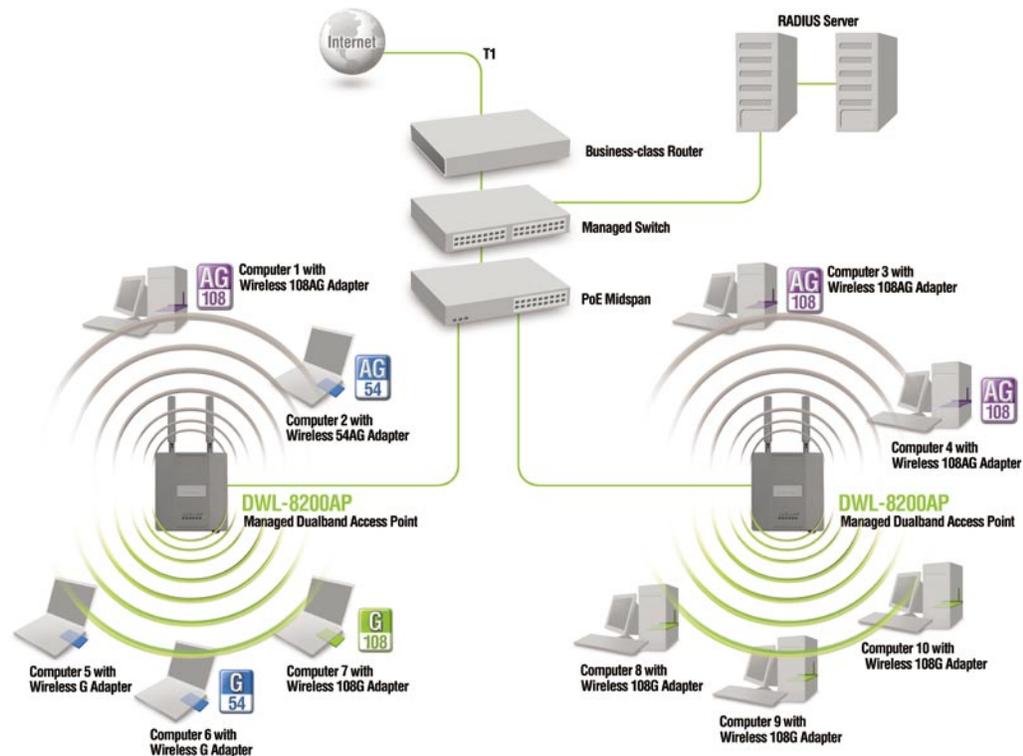
The D-Link *Air Premier*® **DWL-8200AP** lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- 1** Keep the number of walls and ceilings between the **DWL-8200AP** and other network devices to a minimum - each wall or ceiling can reduce your **DWL-8200AP**'s range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- 2** Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- 3** Building materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.
- 4** Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

Three Operational Modes

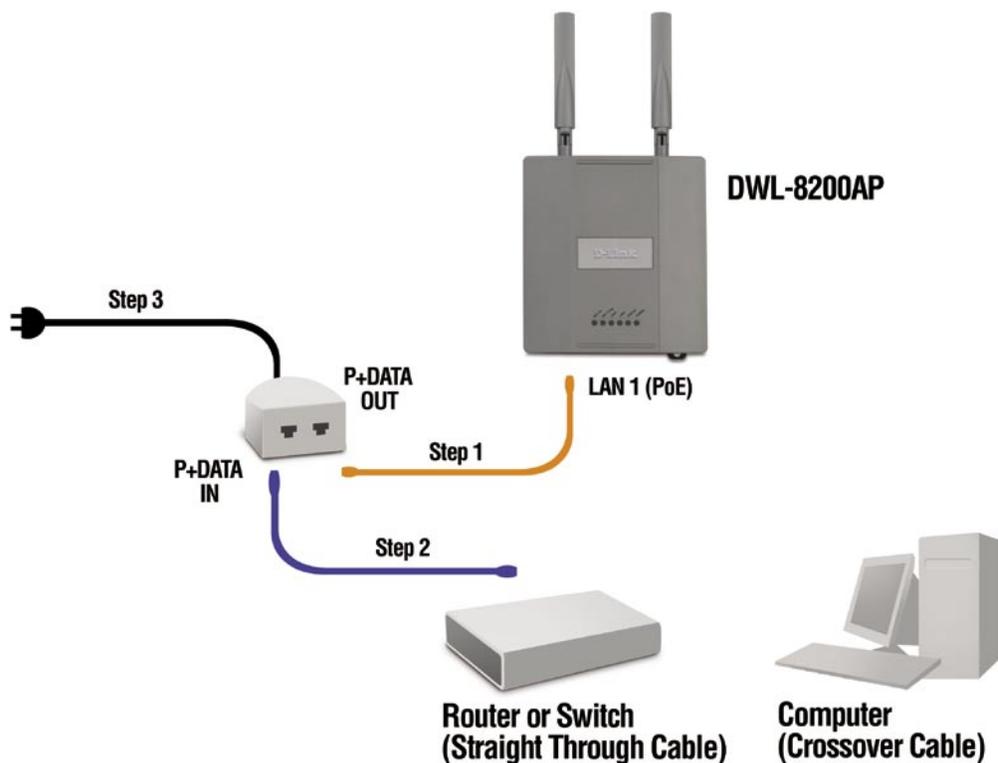
| Operation Mode (Only supports 1 mode at a time) | Function |
|---|--|
| Access Point (AP) | Create a Wireless LAN |
| WDS with AP | Wirelessly Connect Multi Networks While Still Functioning as a Wireless AP |
| WDS | Wirelessly Connect Multi Networks |

Getting Started



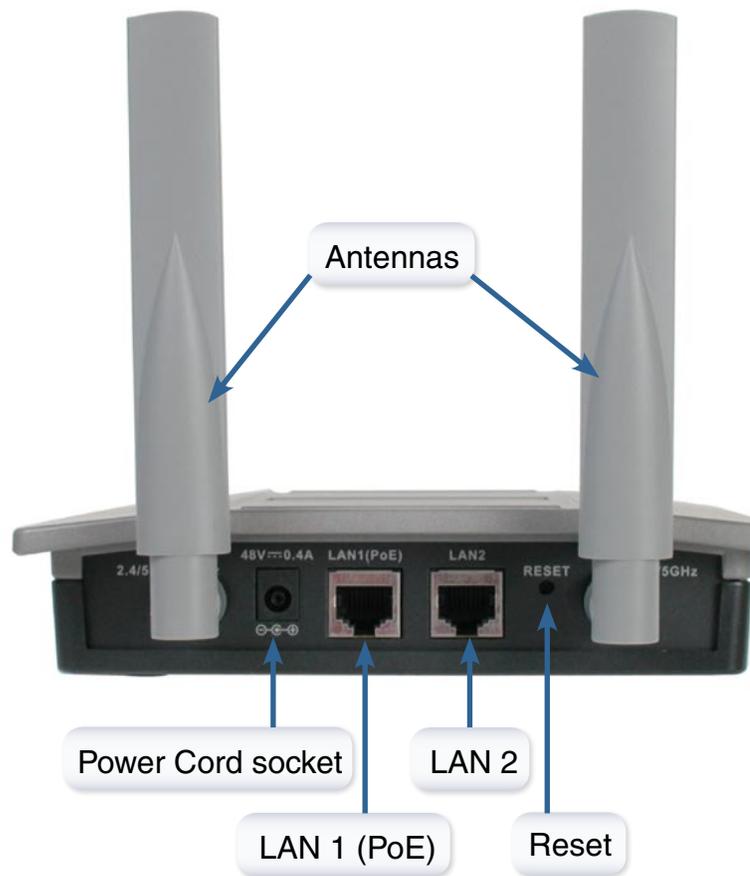
- 1 You will need broadband Internet access.
- 2 Consult with your Cable or DSL provider for proper installation of the modem.
- 3 Connect the Cable or DSL modem to a Router.
(See the printed *Quick Installation Guide* included with your router.)
- 4 Connect the Ethernet Broadband Router to the PoE base unit.
(See the printed *Quick Installation Guide* included with the **DWL-8200AP**.)
- 5 Connect the **DWL-8200AP** to the PoE base unit.
(See the printed *Quick Installation Guide* included with the **DWL-8200AP**.)
- 6 If you are connecting a desktop computer to your network, install the D-Link DWL-AG530 wireless PCI adapter into an available PCI slot on your desktop computer.
(See the printed *Quick Installation Guide* included with the *DWL-AG530*.)
- 7 Install the drivers for the D-Link DWL-AG660 wireless Cardbus adapter into a laptop computer.
(See the printed *Quick Installation Guide* included with the *DWL-AG660*.)

Connecting PoE (Power over Ethernet)



- Step 1** Connect one end of an Ethernet cable (included with your package) to the **LAN port** on the **DWL-8200AP** and the other end of the Ethernet cable to the port labeled **P+DATA OUT** on the PoE base unit.
- Step 2** Connect another Ethernet cable from the **P+DATA IN** port on the PoE base unit to your router/switch or to a PC.
- Step 3** Attach the power adapter to the connector on the PoE base unit. Attach the power cord to the power adapter and into an electrical outlet.

Connecting PoE (Power over Ethernet) *(continued)*



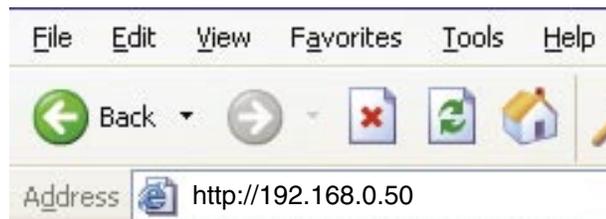
Using the Configuration Menu

To configure the **DWL-8200AP**, use a computer which is connected to the **DWL-8200AP** with an Ethernet cable (see the *Network Layout* diagram).

First, disable the **Access the Internet using a proxy server** function. To disable this function, go to **Control Panel > Internet Options > Connections > LAN Settings** and uncheck the enable box.

Start your web browser program (Internet Explorer, Netscape Navigator) .

Type the IP address of the **DWL-8200AP** in the address field (<http://192.168.0.50>) and press **Enter**. Make sure that the IP addresses of the **DWL-8200AP** and your computer are in the same subnet. **DWL-8200AP** also supports HTTPS Browsing by using the Secure Socket Layer (SSL) Protocol. Just change your Browser's address line from "http://..." to "https://..." and log into the AP again.



After the connection is established, you will see the user identification window as shown.

*Note: If you have changed the default IP address assigned to the **DWL-8200AP**, make sure to enter the correct IP address.*

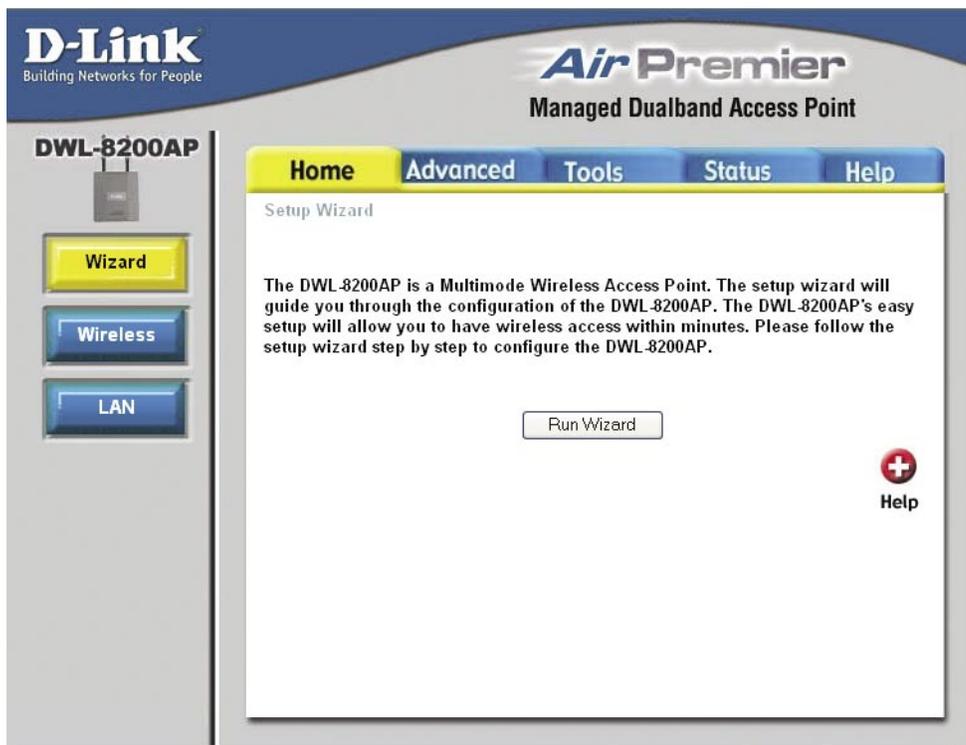
- Type **admin** in the **User Name** field
- Leave the **Password** field blank
- Click **OK**



Note: If you have changed the password, make sure to enter the correct password.

Home > Wizard

The Home>Wizard screen will appear. Please refer to the *Quick Installation Guide* for more information regarding the Setup Wizard.



These buttons appear on most of the configuration screens in this section. Please click on the appropriate button at the bottom of each screen after you have made a configuration change.



Apply

Clicking **Apply** will save changes made to the page



Cancel

Clicking **Cancel** will clear changes made to the page



Help

Clicking **Help** will bring up helpful information regarding the page



Restart

Clicking **Restart** will restart the router. (Necessary for some changes.)

Home > Wireless > Access Point



- Wireless Band:** Select either IEEE 802.11a or IEEE 802.11g
- Mode:** **Access Point** is selected from the pull-down menu.
- SSID:** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **default**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.
- SSID Broadcast:** Enable or Disable SSID broadcast. Enabling this feature broadcasts the SSID across the network.
- Channel:** **52** is the default channel for IEEE 802.11a, and **6** is the default channel for IEEE 802.11g. All devices on the network must share the same channel. (Note: The wireless adapters will automatically scan and match the wireless setting.)



Home > Wireless > Access Point *(continued)*

Auto Channel Scan:

Select **Enable** or **Disable**. (Enable this feature to auto-select the channel for best wireless performance.)

Authentication:

Select **Open System** to communicate the key across the network.

Select **Shared Key** to limit communication to only those devices that share the same WEP settings.

Select **Open System/Shared Key** to allow either form of data encryption.

Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.

Select **WPA-Personal** to secure your network using a password and dynamic key changes. (No RADIUS server required.)

Select **WPA2-Enterprise** to secure your network with the inclusion of a RADIUS server and upgrade the encryption of data with the Advanced Encryption Standard (AES).

Select **WPA2-Personal** to secure your network using a password and dynamic key changes. No RADIUS server required and encryption of data is upgraded with the Advanced Encryption Standard (AES).

Select **WPA-Auto-Enterprise** to allow the client to either use **WPA-Enterprise** or **WPA2-Enterprise**.

Select **WPA-Auto-Enterprise** to allow the client to either use **WPA-Personal** or **WPA2-Personal**.

Home > Wireless > Access Point > Open System and/or Shared Key



Encryption: Select **Disabled** or **Enabled**. (**Disabled** is selected here).

Key Type: Select **HEX** or **ASCII**.

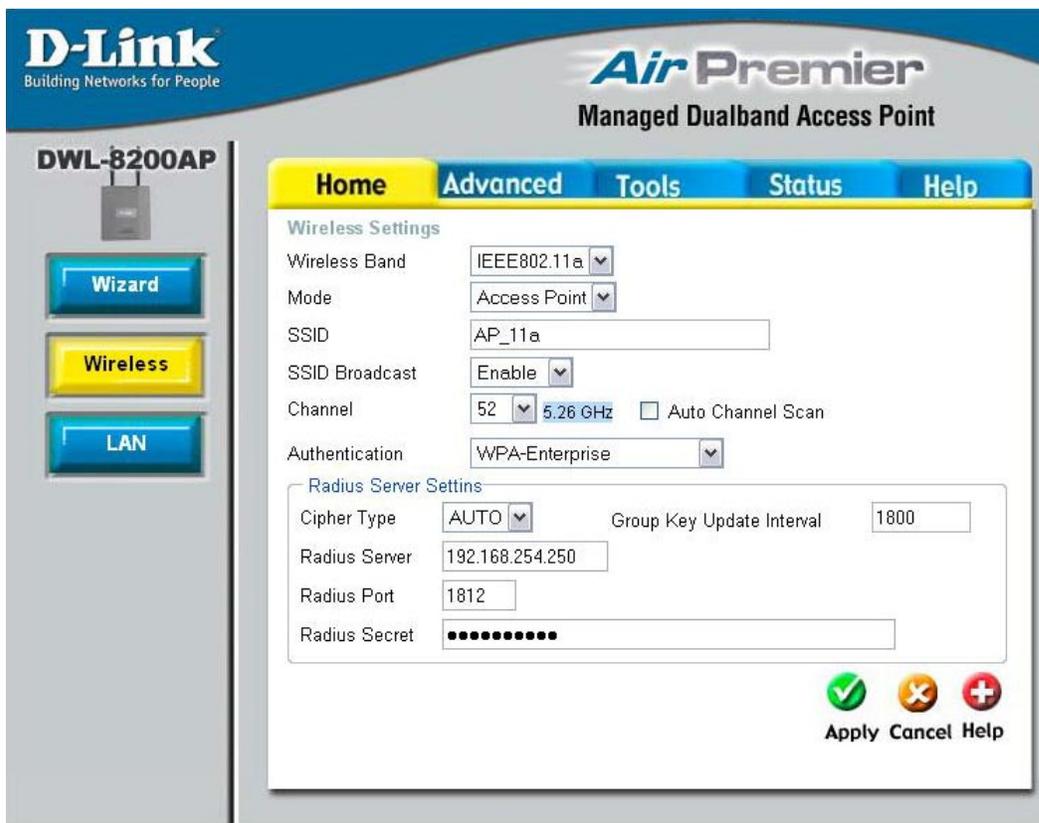
Key Size: Select **64-bit**, **128-bit**, or **152 bits**.

Valid Key: Select the **1st** through the **4th** key to be the active key.

First through Fourth keys: Input up to four keys for encryption. You will select one of these keys in the valid key field.

* **Hexadecimal** digits consist of the numbers 0-9 and the letters A-F.
ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Home > Wireless > Access Point > WPA-Enterprise, WPA2-Enterprise, & WPA-Auto-Enterprise



Cipher Type: When you select **WPA-Enterprise**, **WPA2-Enterprise** or **WPA-Auto-Enterprise**, you must select **AES**, **AUTO**, or **TKIP** from the pull-down menu.

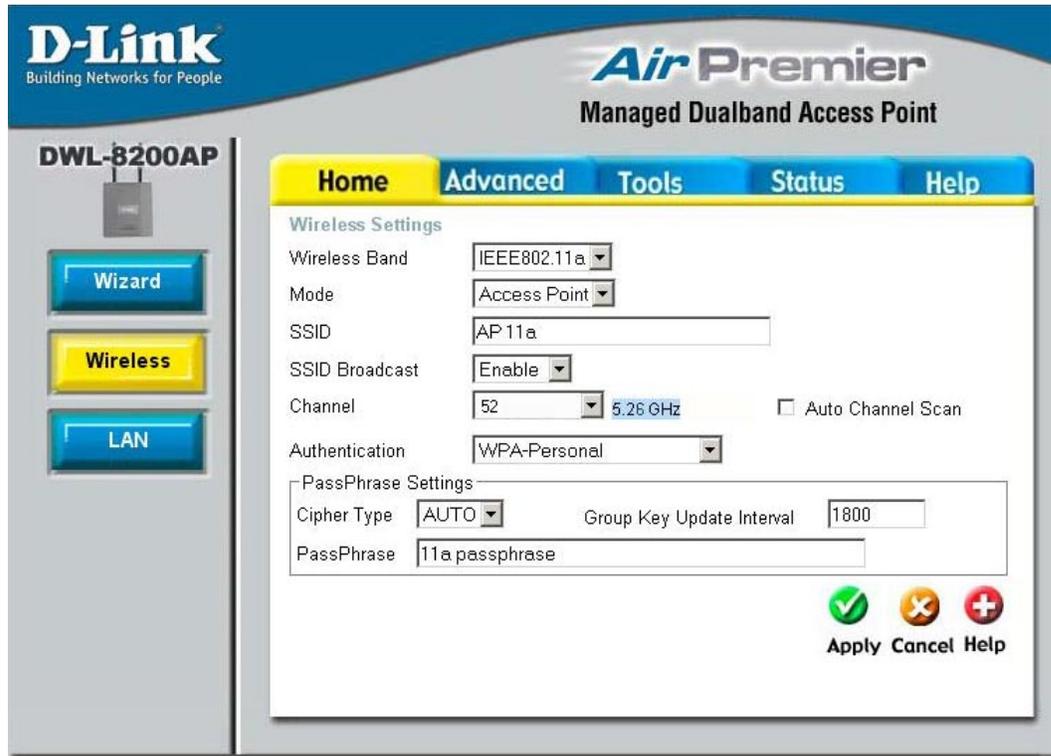
Group Key Update Interval: Select the interval during which the group key will be valid. 1800 is the recommended value. A lower interval may reduce transfer data rate.

Radius Server: Enter the IP address of the Radius server.

Radius Port: Enter the Radius port.

Radius Secret: Enter the Radius secret.

Home > Wireless > Access Point > WPA-Personal, WPA2-Personal, & WPA-Auto-Personal

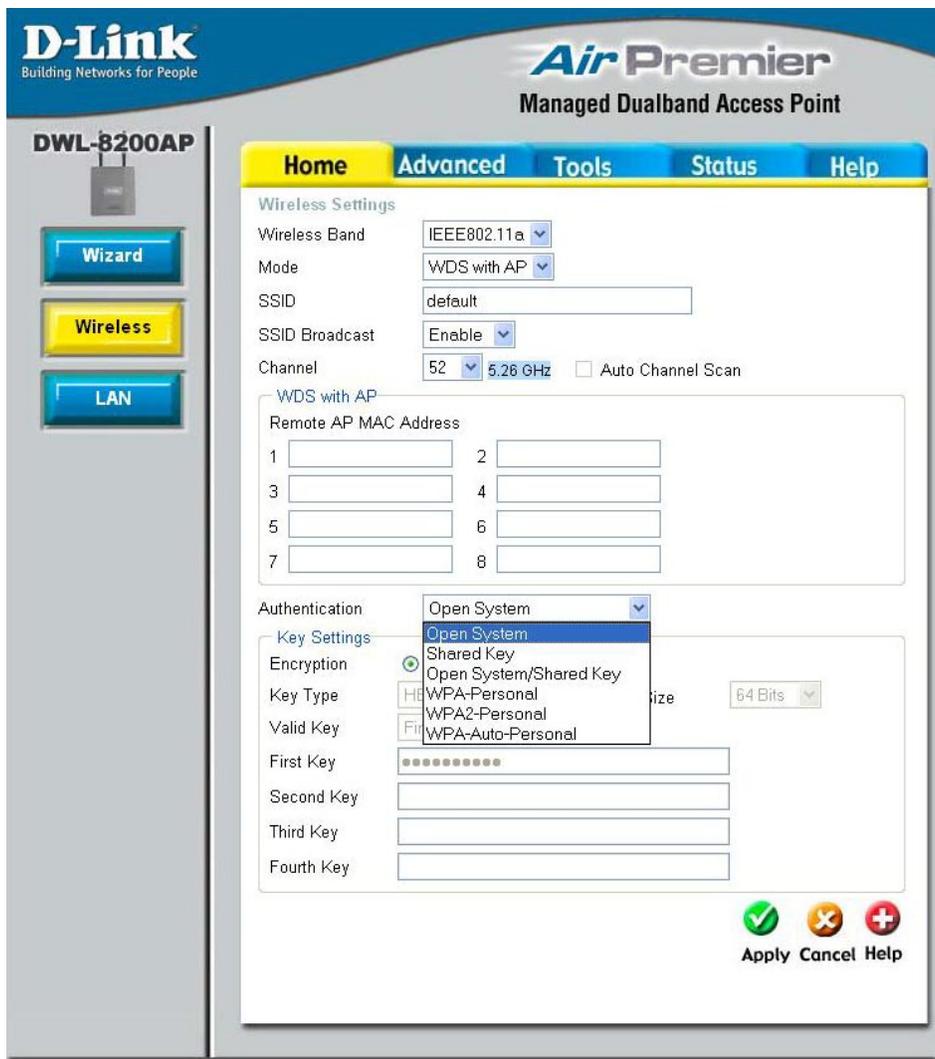


Cipher Type: When you select **WPA-Personal**, **WPA2-Personal**, or **WPA-Auto-Personal**, you must select **AES**, **AUTO**, or **TKIP** from the pull-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. The default value of 1800 is recommended.

PassPhrase: When you select **WPA-Personal**, **WPA2-Personal**, or **WPA-Auto-Personal**, please enter a **PassPhrase** in the corresponding field.

Home > Wireless > WDS with AP



In WDS with AP mode, the **DWL-8200AP** wirelessly connects multiple networks, while still functioning as a wireless AP.

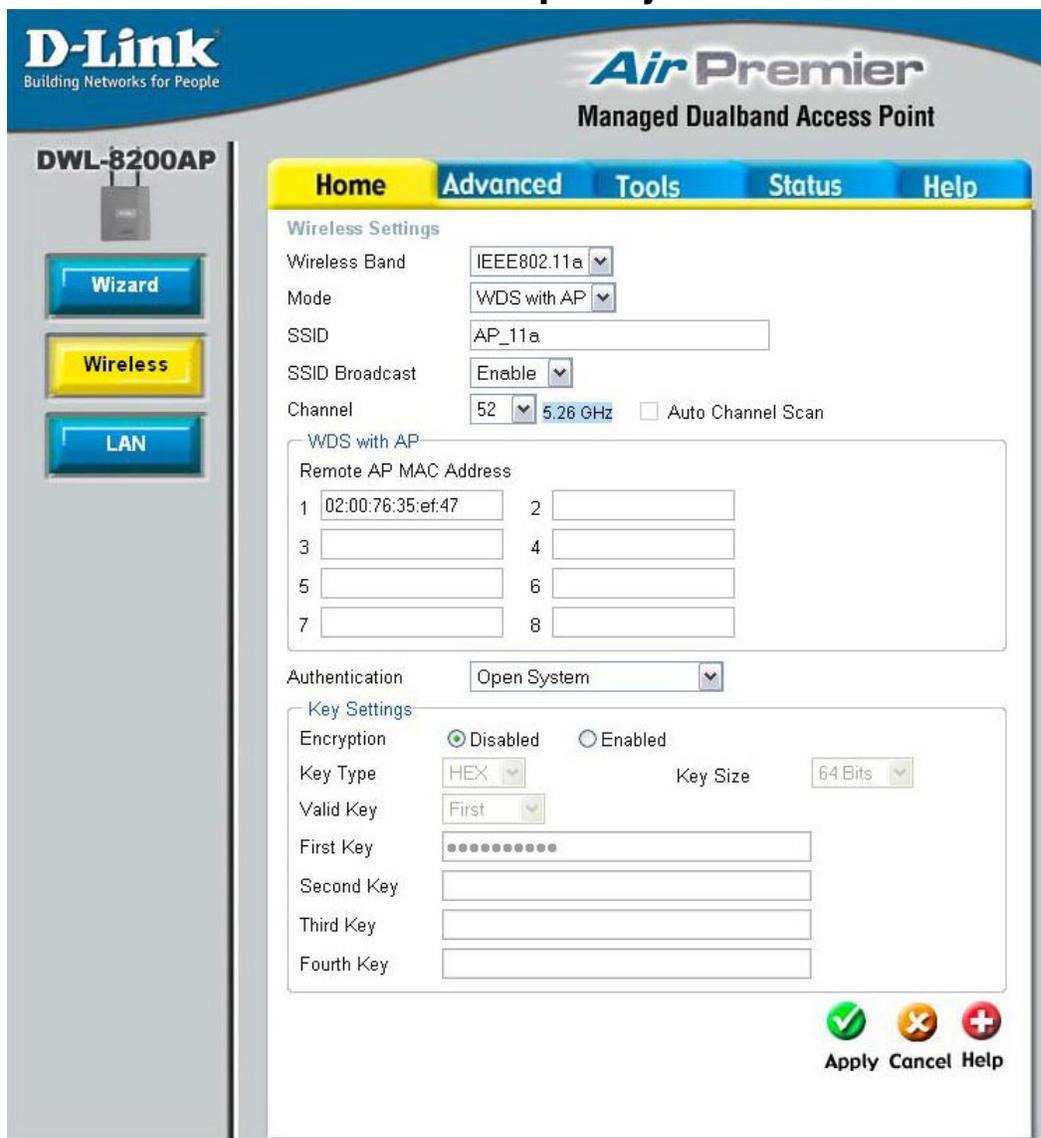
- Wireless Band:** Select either IEEE 802.11a or IEEE 802.11g
- Mode:** **WDS with AP** is selected from the pull-down menu.
- SSID:** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **default**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.



Home > Wireless > WDS with AP *(continued)*

| | |
|-------------------------------|---|
| SSID Broadcast: | Enable or Disable SSID broadcast. Enabling this feature broadcasts the SSID across the network. |
| Channel: | 52 is the default channel for IEEE 802.11a, and 6 is the default channel for IEEE 802.11g. All devices on the network must share the same channel. (Note: The wireless adapters will automatically scan and match the wireless setting.) |
| Auto Channel Scan: | This option is unavailable in WDS with AP mode. |
| Remote AP MAC Address: | Enter the MAC addresses of the APs in your network that will serve as bridges to wirelessly connect multiple networks. |
| Authentication | <p>Select Open System to communicate the key across the network.</p> <p>Select Shared Key to limit communication to only those devices that share the same WEP settings.</p> <p>Select Open System/Shared Key to allow either form of data encryption.</p> <p>Select WPA-Personal to secure your network using a password and dynamic key changes. (No RADIUS server required.)</p> <p>Select WPA2-Personal to secure your network using a password and dynamic key changes. No RADIUS server required and encryption of data is upgraded with the Advanced Encryption Standard (AES).</p> <p>Select WPA-Auto-Personal to allow the client to either use WPA-Personal or WPA2-Personal.</p> |

Home > Wireless > WDS with AP > Open System and/or Shared Key



Encryption: Select **Disabled** or **Enabled**. (**Disabled** is selected here).

Key Type: Select **HEX** or **ASCII**.

Key Size: Select **64-bit**, **128-bit**, or **152 bits**.

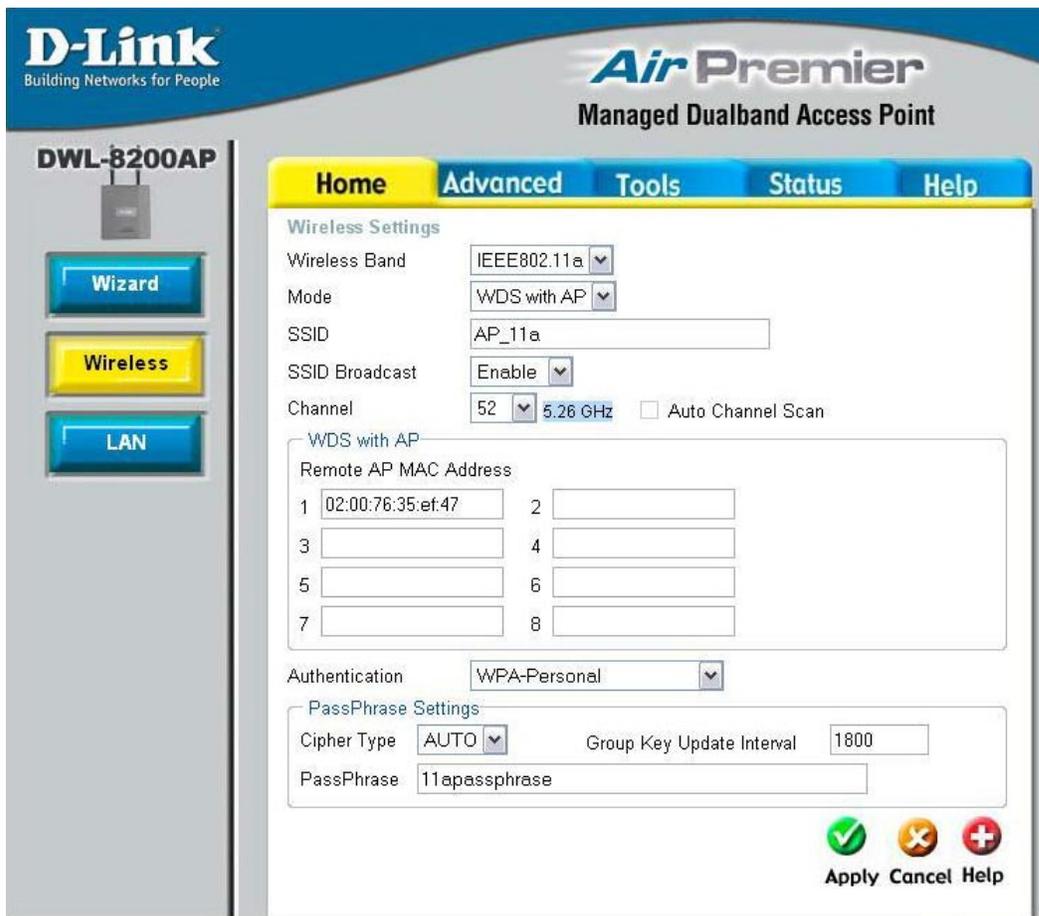
Valid Key: Select the **1st** through the **4th** key to be the active key.

First through Fourth keys: Input up to four keys for encryption. You will select one of these keys in the valid key field.

* **Hexadecimal** digits consist of the numbers 0-9 and the letters A-F.

ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Home > Wireless > WDS with AP > WPA-Personal, WPA2-Personal, & WPA-Auto-Personal

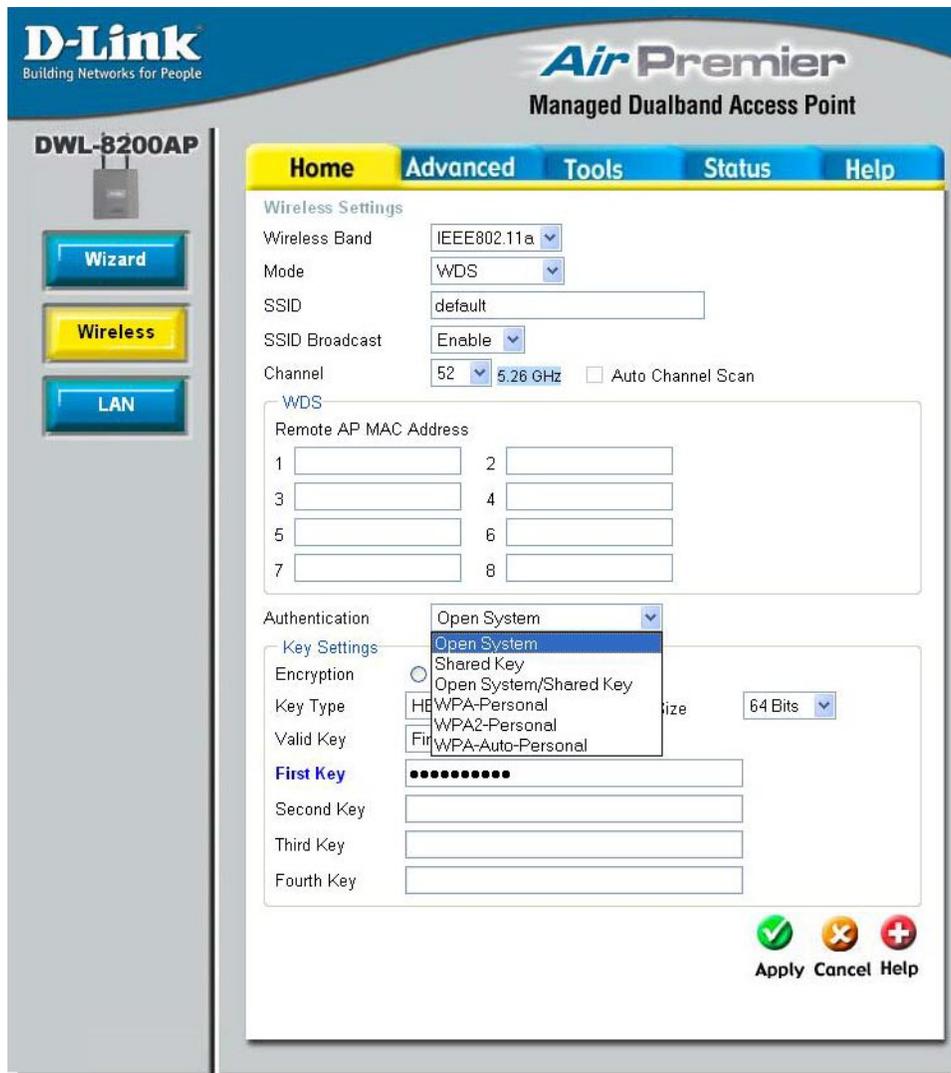


Cipher Type: When you select **WPA-Personal**, **WPA2-Personal**, or **WPA-Auto-Personal** you must select **AES**, **AUTO**, or **TKIP** from the pull-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. The default value of 1800 is recommended.

PassPhrase: When you select **WPA-Personal**, **WPA2-Personal**, or **WPA-Auto-Personal** please enter a **PassPhrase** in the corresponding field.

Home > Wireless > WDS



In WDS, the **DWL-8200AP** wirelessly connects multiple networks, without functioning as a wireless AP.

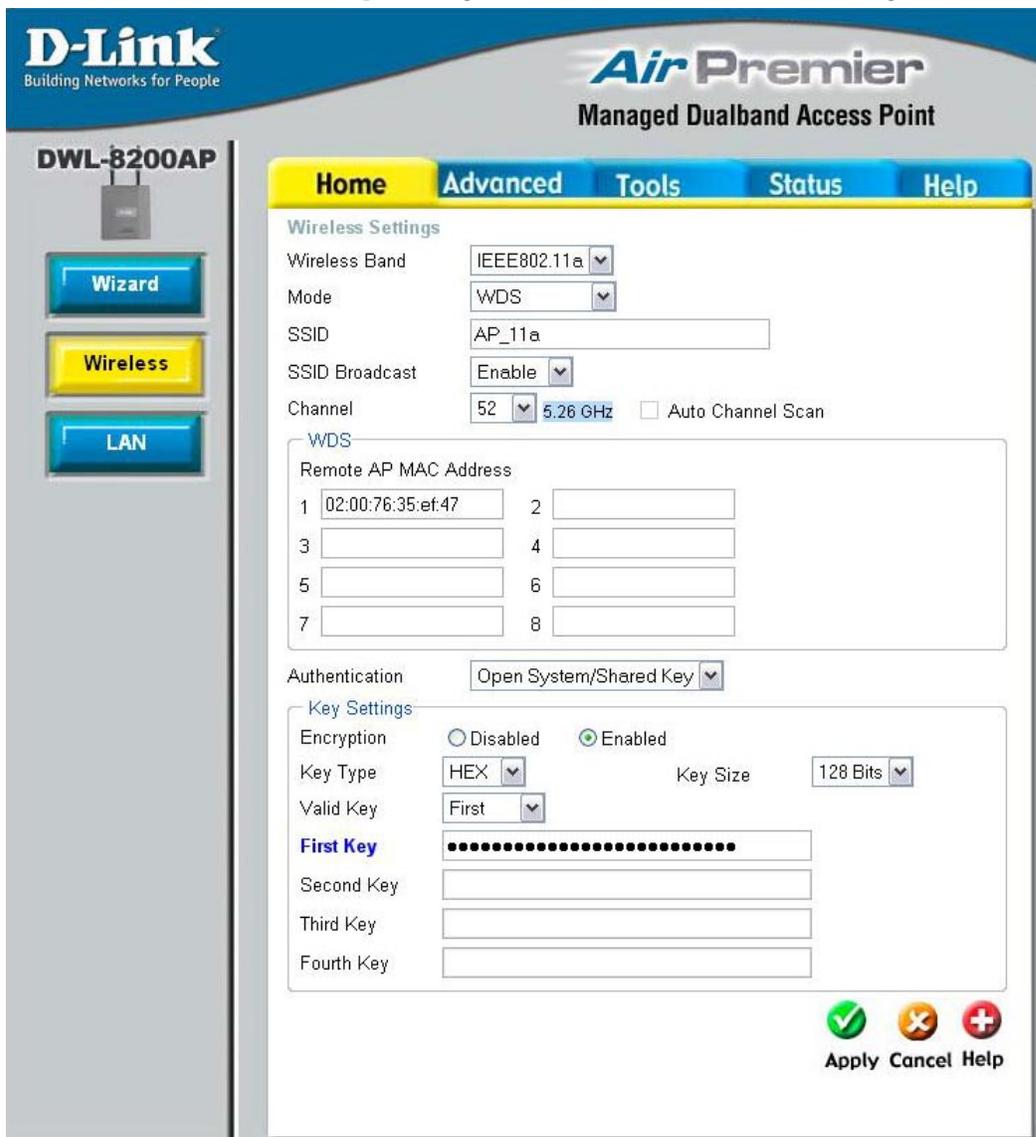
- Wireless Band:** Select either IEEE 802.11a or IEEE 802.11g
- Mode:** **WDS** is selected from the pull-down menu.
- SSID:** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **default**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.



Home > Wireless > WDS (*continued*)

| | |
|-------------------------------|---|
| SSID Broadcast: | Enable or Disable SSID broadcast. Enabling this feature broadcasts the SSID across the network. |
| Channel: | 52 is the default channel for IEEE 802.11a, and 6 is the default channel for IEEE 802.11g. All devices on the network must share the same channel. |
| Auto Channel Scan: | This option is unavailable in WDS mode. |
| Remote AP MAC Address: | Enter the MAC addresses of the APs in your network that will serve as bridges to wirelessly connect multiple networks. |
| Authentication: | <p>Select Open System to communicate the key across the network.</p> <p>Select Shared Key to limit communication to only those devices that share the same WEP settings.</p> <p>Select Open System/Shared Key to allow either form of data encryption.</p> <p>Select WPA-Personal to secure your network using a password and dynamic key changes. (No RADIUS server required.)</p> <p>Select WPA2-Personal to secure your network using a password and dynamic key changes. No RADIUS server required and encryption of data is upgraded with the Advanced Encryption Standard (AES).</p> <p>Select WPA-Auto-Personal to allow the client to either use WPA-Personal or WPA2-Personal.</p> |

Home > Wireless > WDS > Open System and/or Shared Key



Encryption: Select **Disabled** or **Enabled**. (**Disabled** is selected here).

Key Type: Select **HEX** or **ASCII**.

Key Size: Select **64-bit**, **128-bit**, or **152 bits**.

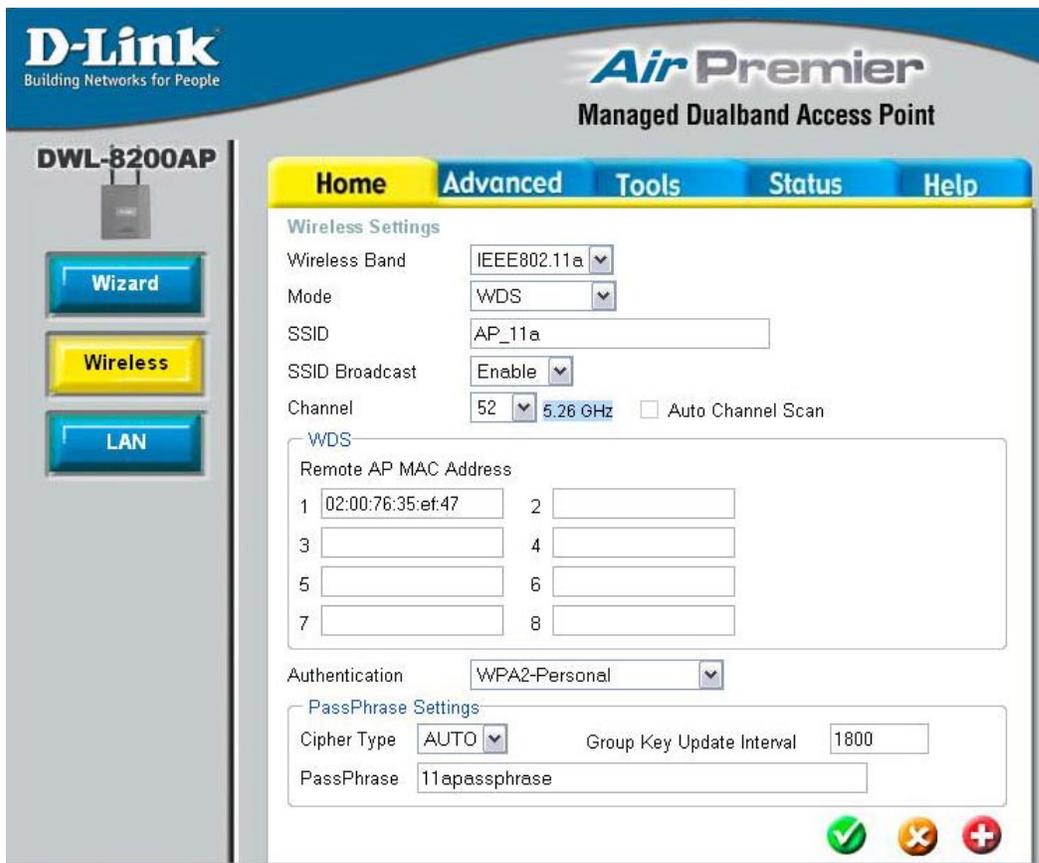
Valid Key: Select the **1st** through the **4th** key to be the active key.

First through Fourth keys: Input up to four keys for encryption. You will select one of these keys in the valid key field.

* **Hexadecimal** digits consist of the numbers 0-9 and the letters A-F.

ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers 0-127.

Home > Wireless > WDS > WPA-Personal, WPA2-Personal, & WPA-Auto-Personal



Cipher Type: When you select **WPA-Personal**, **WPA2-Personal**, or **WPA-Auto-Personal**, you must select **AES**, **AUTO**, or **TKIP** from the pull-down menu.

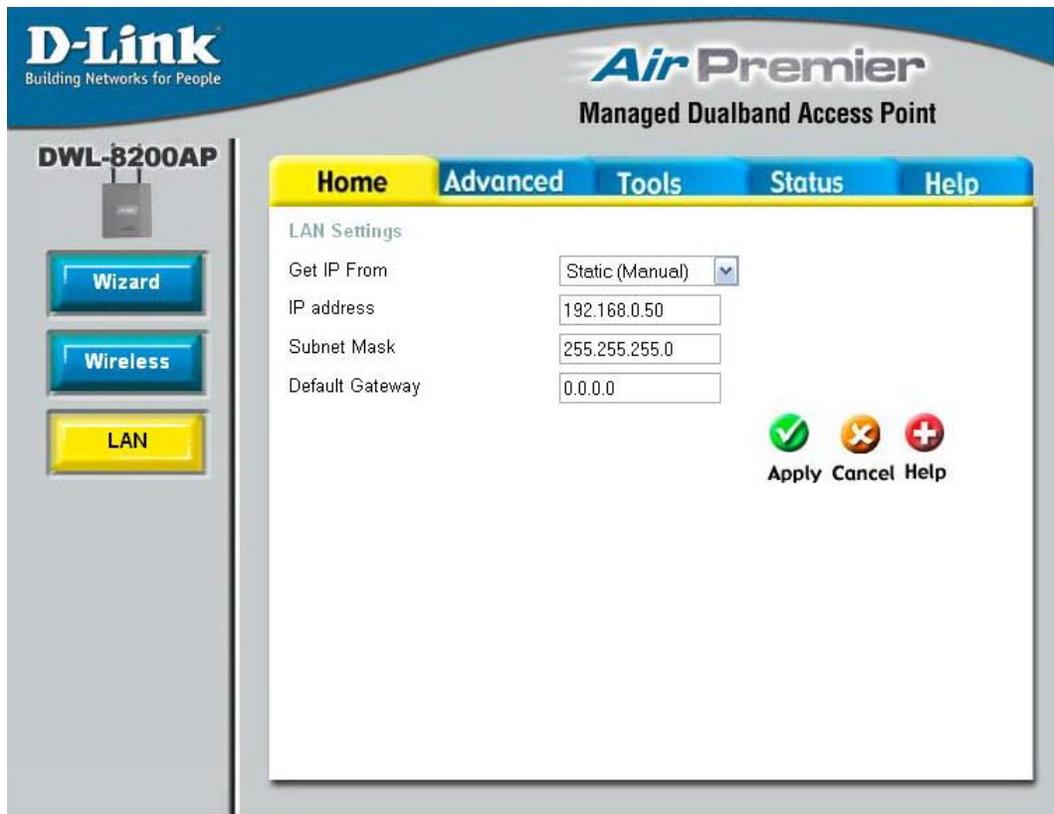
Group Key Update Interval: Select the interval during which the group key will be valid. The default value of 1800 is recommended.

PassPhrase: When you select **WPA-Personal**, **WPA2-Personal**, or **WPA-Auto-Personal**, please enter a **PassPhrase** in the corresponding field.

Note:

| AP Mode | Authentication Available |
|---------------------|---|
| Access Point | Open Shared Both WPA-Enterprise WPA-Personal WPA2-Enterprise WPA2-Personal WPA-Auto-Enterprise WPA-Auto-Personal |
| WDS with AP | Open Shared Both WPA-Personal WPA2-Personal WPA-Auto-Personal |
| WDS | Open Shared Both WPA-Personal WPA2-Personal WPA-Auto-Personal |

Home > LAN



LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the **DWL-8200AP**. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

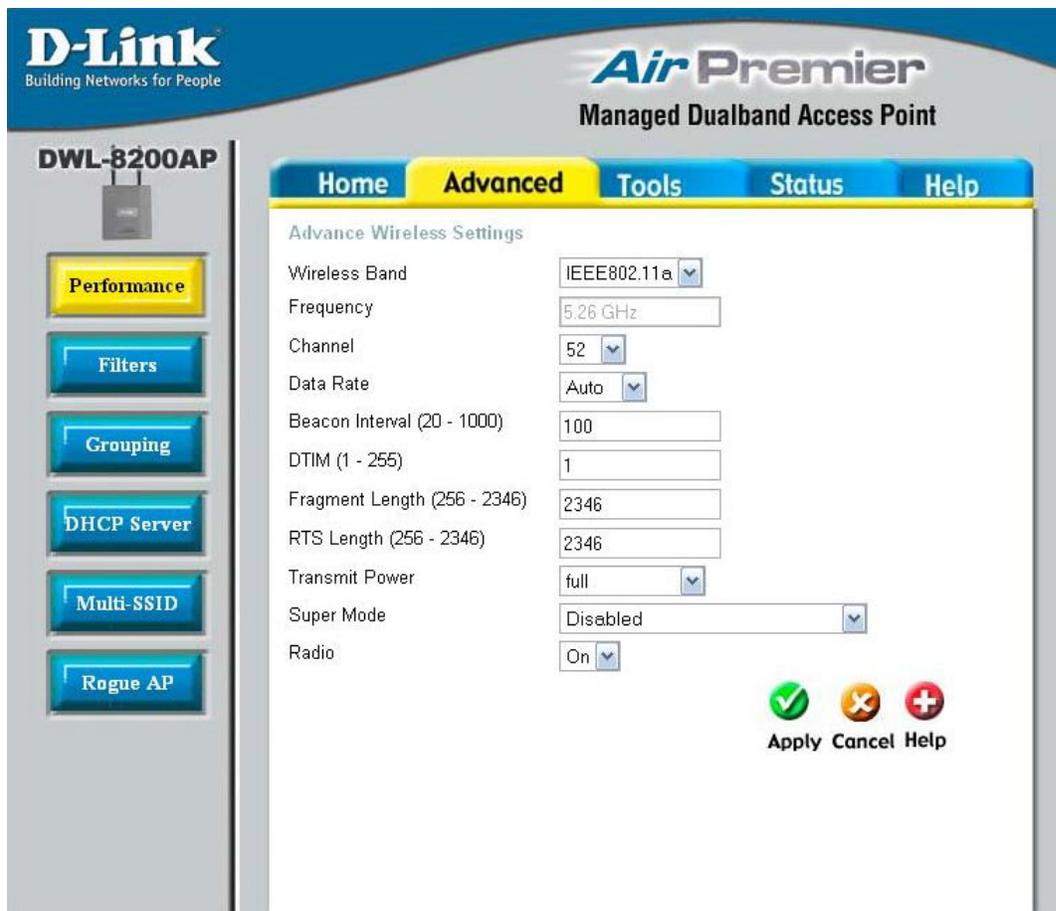
Get IP From: **Static (Manual)** is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the **DWL-8200AP**. When **Dynamic (DHCP)** is selected the other fields here will be greyed out.

IP Address: The default IP address is 192.168.0.50. Assign a static IP address that is within the IP address range of your network.

Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.

Default Gateway: Enter the IP address of the gateway in your network. If there isn't a gateway in your network, please enter an IP address within the range of your network.

Advanced > Performance



By changing radio parameters in the performance section, you can customize the radio network to fit your needs. Performance functions are designed for more advanced users who are familiar with 802.11 wireless networks and radio configuration.

- Wireless Band:** Select IEEE 802.11a or IEEE 802.11g from this pull-down menu.
- Frequency:** The frequency is 2.437GHz for Channel **6**, and 5.26GHz for Channel **52**.
- Channel:** Indicates the channel setting for the **DWL-8200AP**. By default the channel for IEEE 802.11g is set to **6**, and the default channel for IEEE 802.11a is set to **52**. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Advanced > Performance *(continued)*

| | | | |
|---|---|------------------|---|
| Data Rate*: | The default value is set to “ Auto ”, which adjusts the base transfer rate depending on the base rate of the connecting device. The Data Rates are Auto, 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps. | | |
| Beacon Interval (20-1000): | Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a Beacon interval value between 20 and 1000. The default value is set to 100 milliseconds. | | |
| DTIM (1-255): | <i>(Delivery Traffic Indication Message)</i> - Select a setting between 1 and 255. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. | | |
| Fragmentation Length (256-2346): | The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting. | | |
| RTS Length (256-2346): | This value should remain at its default setting of 2346. If you encounter inconsistent data flow, only minor modifications to the value range between 256 and 2346 are recommended. | | |
| Transmit Power: | Choose full, half (-3dB), quarter (-6dB), eighth (-9dB), minimum power. | | |
| Super Mode: | Super Mode is a group of performance enhancement features that increase end user application throughput in an 802.11a and 802.11g network. Super Mode is backwards compatible to standard 802.11g devices. For top performance, all wireless devices on the network should be Super Mode capable. Select either Disabled, Super Mode without Turbo, Super Mode with Static Turbo, or Super Mode with Dynamic Turbo. | | |
| | <table border="1" style="margin-left: 40px;"> <tr> <td style="vertical-align: top;">Disabled:</td> <td>Standard 802.11a and 802.11g support, no enhanced capabilities.</td> </tr> </table> | Disabled: | Standard 802.11a and 802.11g support, no enhanced capabilities. |
| Disabled: | Standard 802.11a and 802.11g support, no enhanced capabilities. | | |

*Maximum wireless signal rate derived from IEEE Standard 802.11a and 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 actual data throughput rate.

Advanced > Performance *(continued)*

Super Mode without Turbo:

Capable of Packet Bursting, FastFrames, Compression, and no Turbo mode.

Super Mode with Static Turbo:

Capable of Packet Bursting, FastFrames, Compression, and Static Turbo. This setting is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all the devices on the wireless network are configured with Super Mode with Static Turbo enabled.

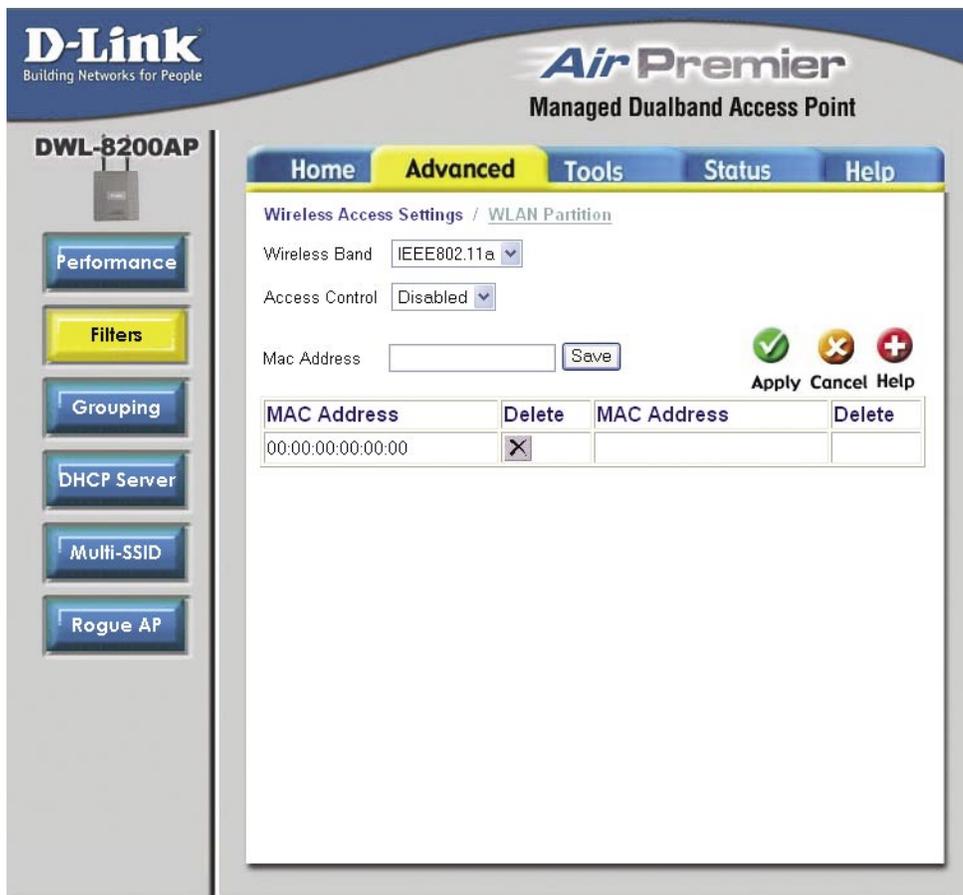
Super Mode with Dynamic Turbo:

Capable of Packet Bursting, FastFrames, Compression, and Dynamic Turbo. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo Mode is only enabled when all devices on the wireless network are configured with Super Mode with Dynamic Turbo enabled.

Radio: Select **ON** or **OFF**.

Note: Super Mode with Static Turbo is only available for 802.11a.

Advanced > Filters > Wireless Access Settings



Wireless Band: Select IEEE 802.a or IEEE 802.11g from this pull-down menu.

Access Control: Select **Disabled** to disable the filters function.
 Select **Accept** to accept only those devices with MAC addresses in the Access Control List.
 Select **Reject** to reject the devices with MAC addresses in the Access Control List.

MAC Address: Enter the MAC addresses that you wish to include in your filters list, and click **Save**.

MAC Address List: When you enter a MAC address, it appears in this list. Click **Delete** to remove it from the list.

Advanced > Filters > WLAN Partition



Wireless Band: Select IEEE 802.a or IEEE 802.11g from this pull-down menu.

Internal Station Connection: Enabling this feature allows wireless clients to communicate with each other. If this is disabled, wireless stations of the selected band are not allowed to exchange data through the access point.

Ethernet to WLAN Access: Enabling this feature allows Ethernet devices to communicate with wireless clients. If this is disabled, all data from the Ethernet to associated wireless devices is blocked. Wireless devices can still send data to the Ethernet.

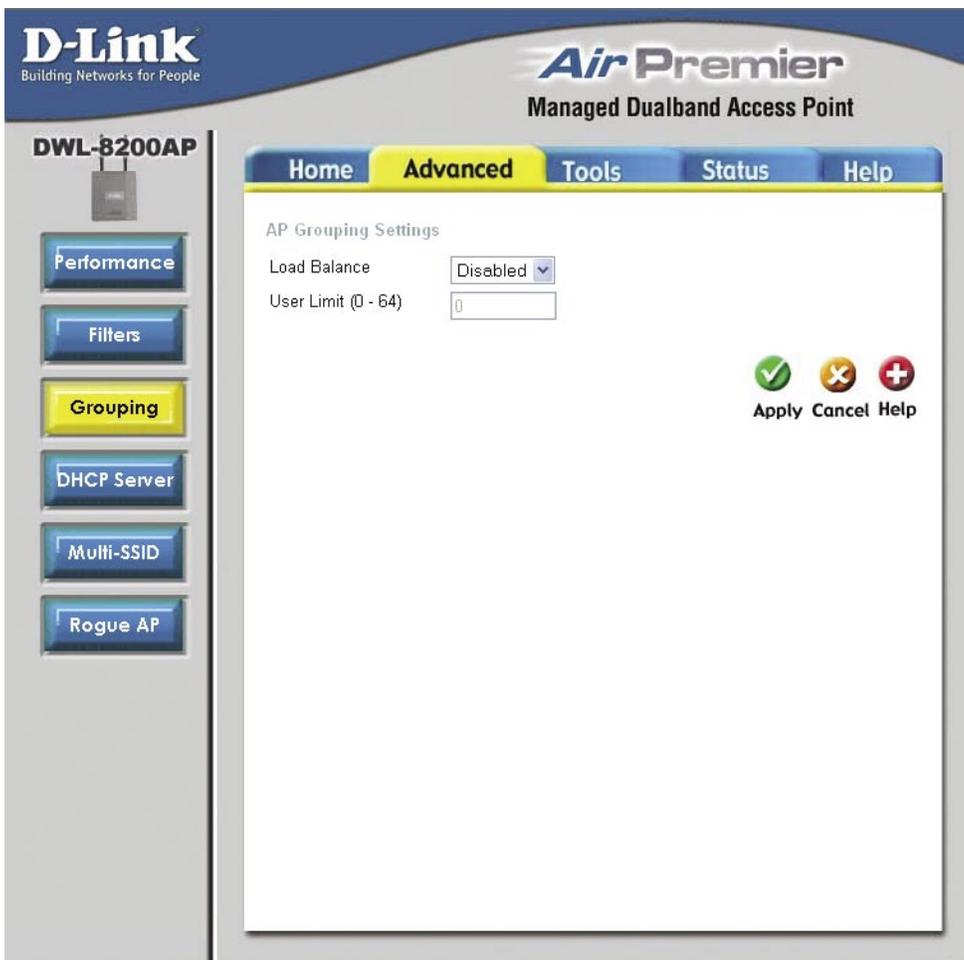


Advanced > Filters > WLAN Partition *(continued)*

| | |
|---|---|
| Internal Station Connection between 802.11a & 802.11g: | Enabling this feature allows devices on the 802.11a network, to exchange data with devices on the 802.11g network through Access Point. If disabled, a partition is created between the networks within the Access Point. |
|---|---|

Note: Only when both 11a and 11g band are in Access Point mode, you will be able to see this feature.

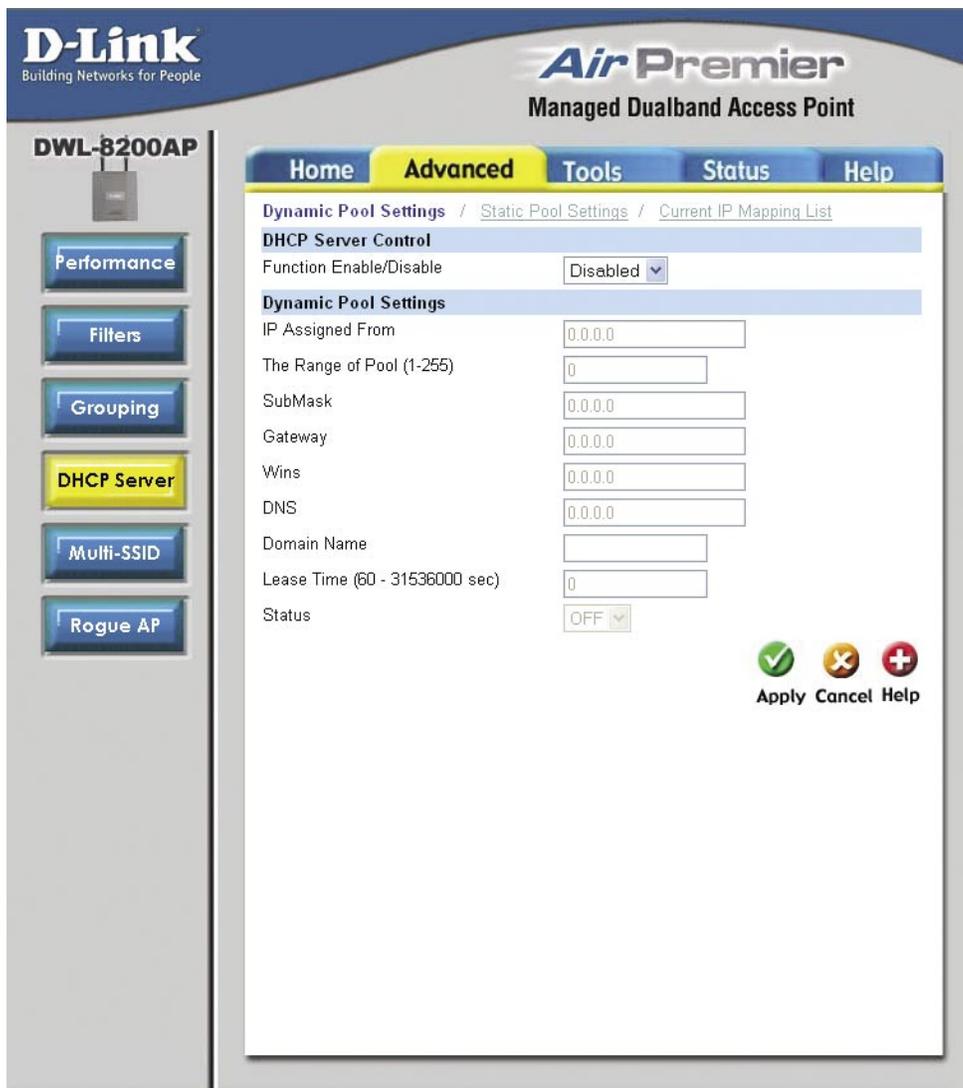
Advanced > Grouping



Load Balance: When **Enabled**, you allow several **DWL-8200APs** to balance wireless network traffic and wireless clients among **DWL-8200APs** in the network. Assign each access point a different **non-overlapping channel** (e.g., 1, 6, 11).

User Limit (0-64): Set the **User Limit** in this field (0-64).

Advanced > DHCP Server > Dynamic Pool Settings



DHCP Server Control: **Dynamic Host Configuration Protocol** assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

Select **Enable** to allow the **DWL-8200AP** to function as a DHCP server.

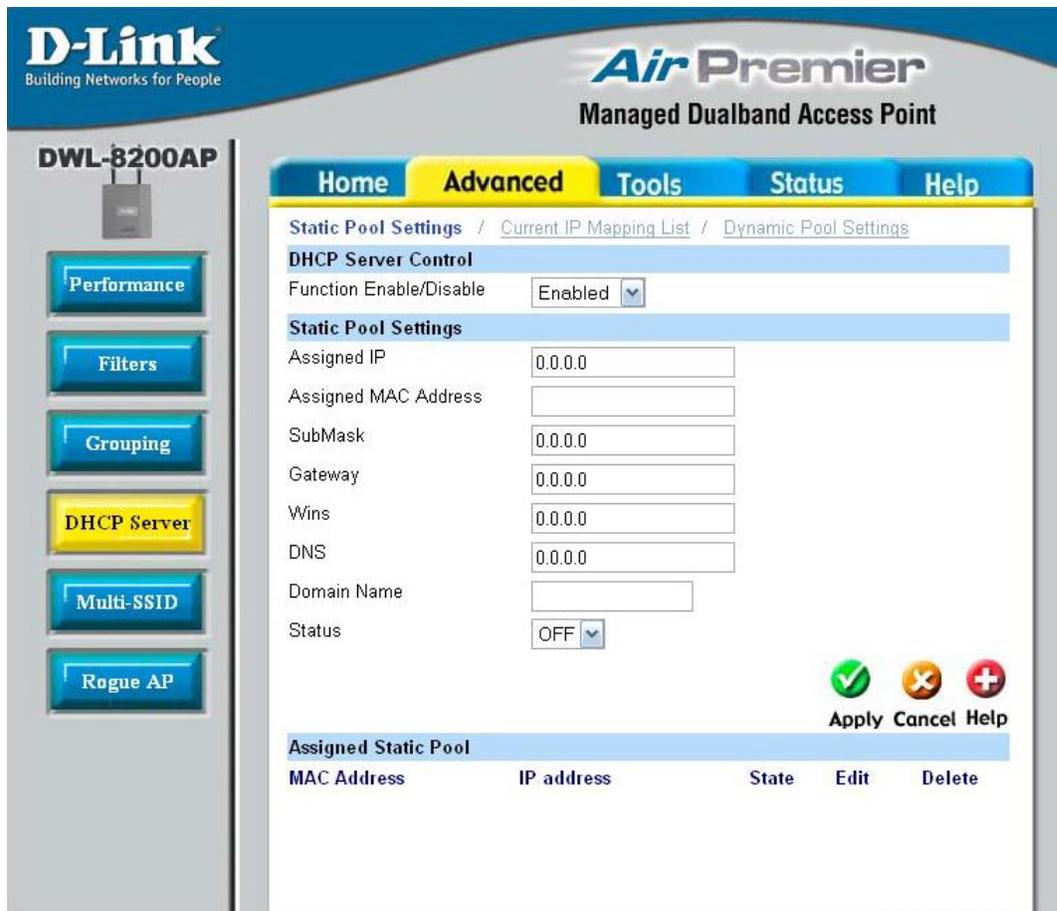
IP Assigned From: Input the first IP address available for assignment in your network.

The Range of Pool (1-255): Enter the number of IP addresses available for assignment.

Advanced > DHCP Server > Dynamic Pool Settings (continued)

- SubMask:** All devices in the network must have the same subnet mask to communicate. Enter the submask for the network here.
- Gateway:** Enter the IP address of the gateway on the network.
- Wins:** **Windows Internet Naming Service** is a system that determines the IP address of a network computer that has a dynamically assigned IP address.
- DNS:** Enter the IP address of the DNS server. The DNS (Domain Name Server) translates domain names such as www.dlink.com into IP addresses.
- Domain Name:** Enter the domain name of the **DWL-8200AP**, if applicable. (An example of a domain name is: www.dlink.com.)
- Lease Time (60-31536000 sec.):** The Lease Time is the period of time before the DHCP server will assign new IP addresses.
- Status:** Turn the **Dynamic Pool Settings ON** or **OFF** here.

Advanced > DHCP Server > Static Pool Settings



DHCP Server Control: **Dynamic Host Configuration Protocol** assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses.

Select **Enable** to allow the **DWL-8200AP** to function as a DHCP server.

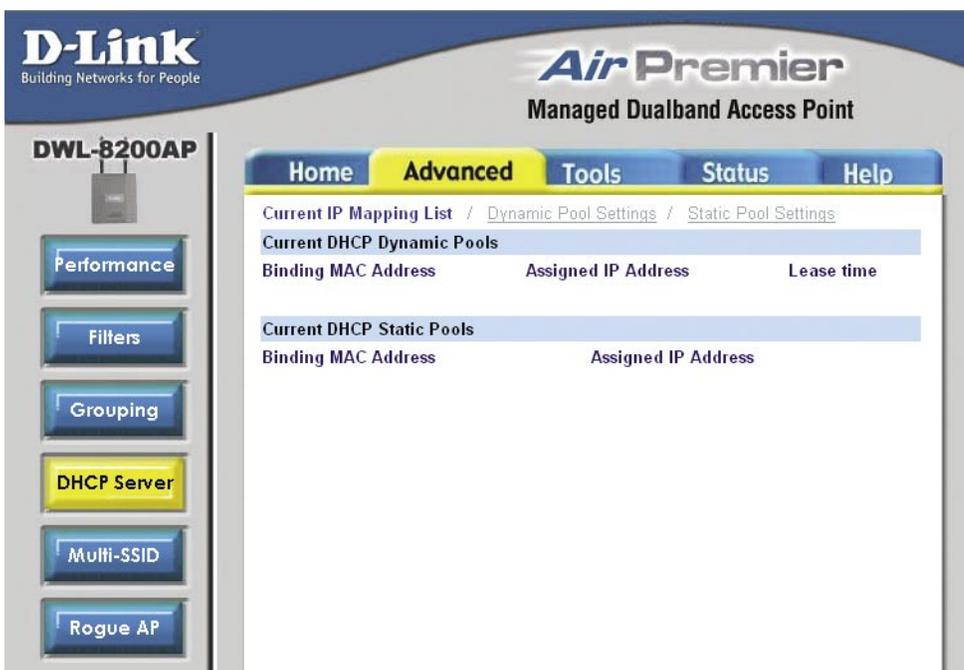
Assigned IP: Use the **Static Pool Settings** to assign the same IP address to a device at every restart. The IP addresses assigned in the Static Pool list must NOT be in the same IP range as the Dynamic Pool. After you have assigned a static IP address to a device via its MAC address, click **Apply**; the device will appear in the **Assigned Static Pool** at the bottom of the screen. Edit or delete the device in this list.

Assigned MAC Address: Enter the MAC address of the device here.

Advanced > DHCP Server > Static Pool Settings *(continued)*

- SubMask:** Enter the subnet mask here.
- Gateway:** Enter the IP address of the gateway on the network.
- Wins:** **Windows Internet Naming Service** is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.
- DNS:** Enter the IP address of the Domain Name Server, if applicable. The DNS translates domain names such as www.dlink.com into IP addresses.
- Domain Name:** Enter the domain name of the **DWL-8200AP**, if applicable.
- Status:** This option turns the Static Pool settings ON or OFF.

Advanced > DHCP Server > Current IP Mapping List



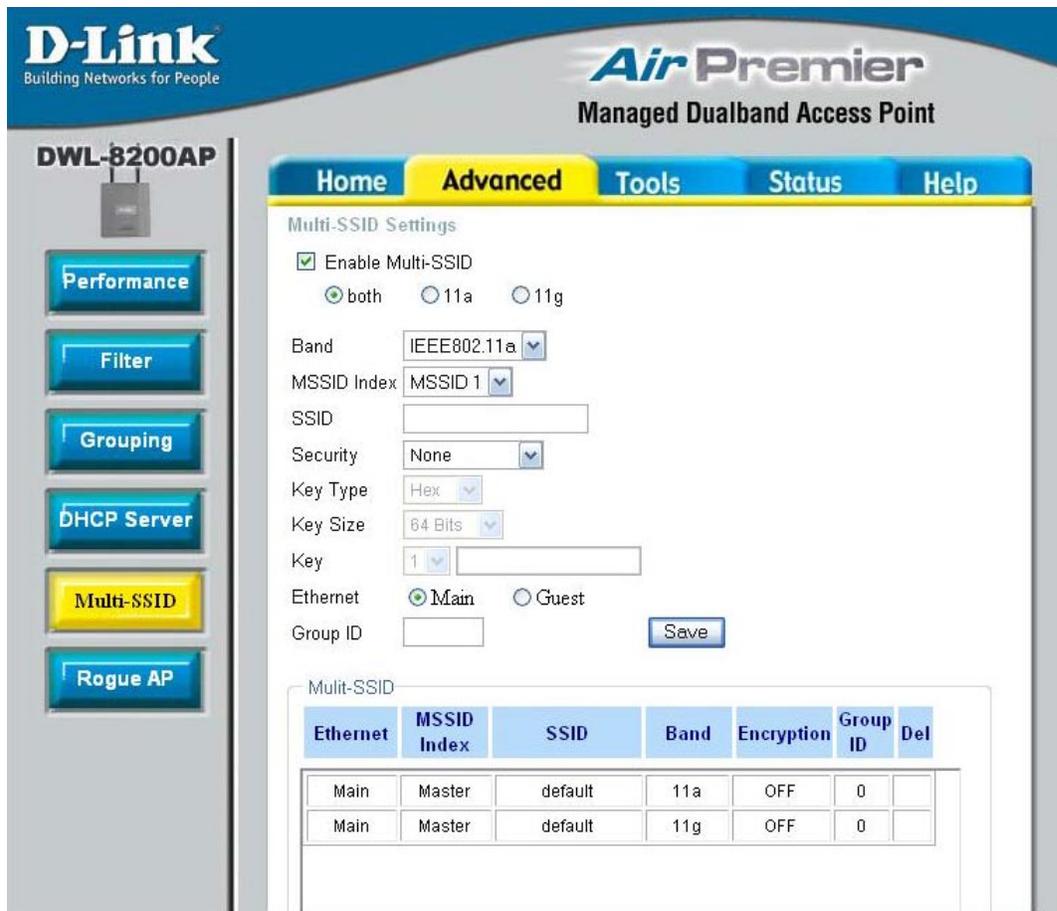
This screen displays information about the current DHCP dynamic and static IP address pools. This information is available when you enable the DHCP function of the **DWL-8200AP** and assign dynamic and static IP address pools.

- Current DHCP Dynamic Pools:** These are IP address pools to which the DHCP server function has assigned dynamic IP addresses.

Advanced > DHCP Server > Current IP Mapping List *(continued)*

| | |
|-----------------------------------|--|
| Binding MAC address: | The MAC address of a device on the network that is within the DHCP dynamic IP address pool. |
| Assigned IP address: | The current corresponding DHCP-assigned dynamic IP address of the device. |
| Lease Time: | The length of time that the dynamic IP address will be valid. |
| Current DHCP Static Pools: | These are IP address pools to which the DHCP server function has assigned static IP addresses. |
| Binding MAC address: | The MAC address of a device on the network that is within the DHCP static IP address pool. |
| Assigned IP address: | The current corresponding DHCP-assigned static IP address of the device. |

Advanced > Multi-SSID



Enable Multi-SSID: When Multi-SSID is enabled, you can configure your SSIDs for either **both**, **11a** only, or **11g** only networks.

Band: Select the wireless band (**IEEE802.11a** or **IEEE802.11g**).

MSSID Index: You can select up to 7 MSSIDs per band, the default MSSID is the primary, which puts the total to 8 MSSIDs per band.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **default**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Security: Select either **None**, **Open System**, or **Shared Key**.

Advanced > Multi-SSID *(continued)*

- Key Type:** Select **HEX** or **ASCII**.
- Key Size:** Select **64-bit**, **128-bit**, or **152-bit**.
- Key:** Select the 1st key all the way through the 4th key, to be set as the active key. Enter key here.
- Ethernet:** Select "**Main**" if you wish to configure the network on LAN 1 (PoE). Select "**Guest**" to set up the network on LAN 2.
- Group ID:** You can assign a value to group all of the SSIDs to each other. The Group ID is 0 by default, which is also considered Primary SSID. Use Group ID 0-15 for "**Main**", or use Group ID 16-30 for "**Guest**".

*Note: Everytime you configure one Multi-SSID, you are required to click on "**Save**" and then "**Apply**".*

Note: If the Master sets security to key 1, then key 1 can not be used. This leaves three Multi-SSIDs that can use security per band. The final result will mean that for each band, four Multi-SSIDs will be without security.

*Note: If Main Master SSID supports **WPA** or **WPA2**, then the guest is not allowed to set security.*

Advanced > Rogue AP

The screenshot shows the configuration page for Rogue AP detection on a D-Link DWL-8200AP. The interface includes a navigation sidebar on the left with buttons for Performance, Filter, Grouping, DHCP Server, Multi-SSID, and Rogue AP. The main content area has tabs for Home, Advanced (selected), Tools, Status, and Help. Under the 'Rogue AP Detection' section, there are three settings: BSS Type (radio buttons for AP BSS, Ad Hoc, Both), Band (checkboxes for 11a, 11b, 11g), and Security (checkboxes for OFF, WEP, WPA-Enterprise, WPA-Personal). Below these is a 'Rogue AP List' table with a 'Detect' button. The 'AP List' table at the bottom shows a list of detected APs with columns for Type, CH, BSSID, Security, MODE, SSID, and Del.

| Type | CH | BSSID | Security | MODE | SSID | Del |
|--------|----|-------------------|----------------|---------|---------|-----|
| ad_hoc | 1 | 00:01:02:03:04:05 | WPA-Enterprise | 802.11b | Leo | |
| AP BSS | 2 | 00:01:02:03:04:06 | WPA-Enterprise | 802.11b | Macleod | |
| AP BSS | 3 | 00:01:02:03:04:07 | WPA-Enterprise | 802.11b | PaPa | |
| AP BSS | 4 | 00:01:02:03:04:08 | WPA-Enterprise | 802.11b | Kathy | |

BSS Type: The Basic Service Set Type allows you to select from **AP BSS**, **Ad Hoc**, or **Both**.

Band: Select the type of network (bands **11a**, **11b**, and **11g**) that you would like the AP detection to search on.



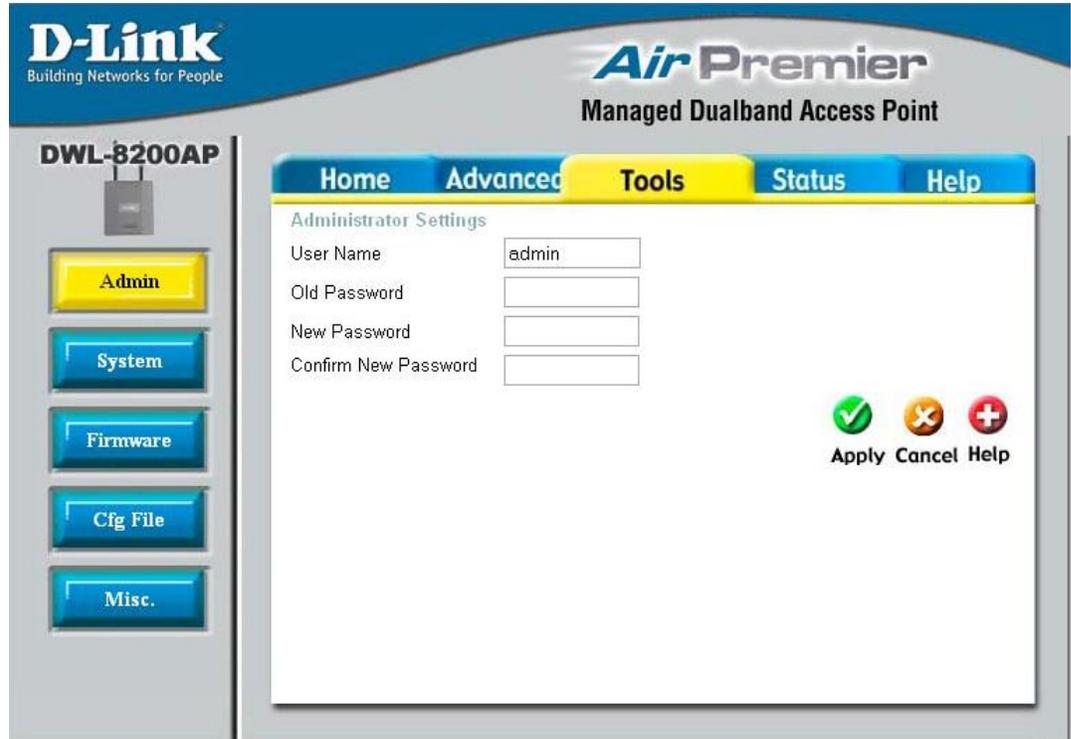
Advanced > Rogue AP *(continued)*

Security: Select the Security type **Off**, **WEP**, **WPA-Enterprise**, and **WPA-Personal** that you would like to be consider during AP detection.

Rogue AP List: This window shows all of the neighbor APs detected, which is based on your criteria from above (BSS Type, Band, and Security). If the AP is in the same network, or if you know the AP, just click on "**Add**" to save it to the AP list.

AP List: This window shows all of the APs that are allowed access on the network.

Tools > Admin



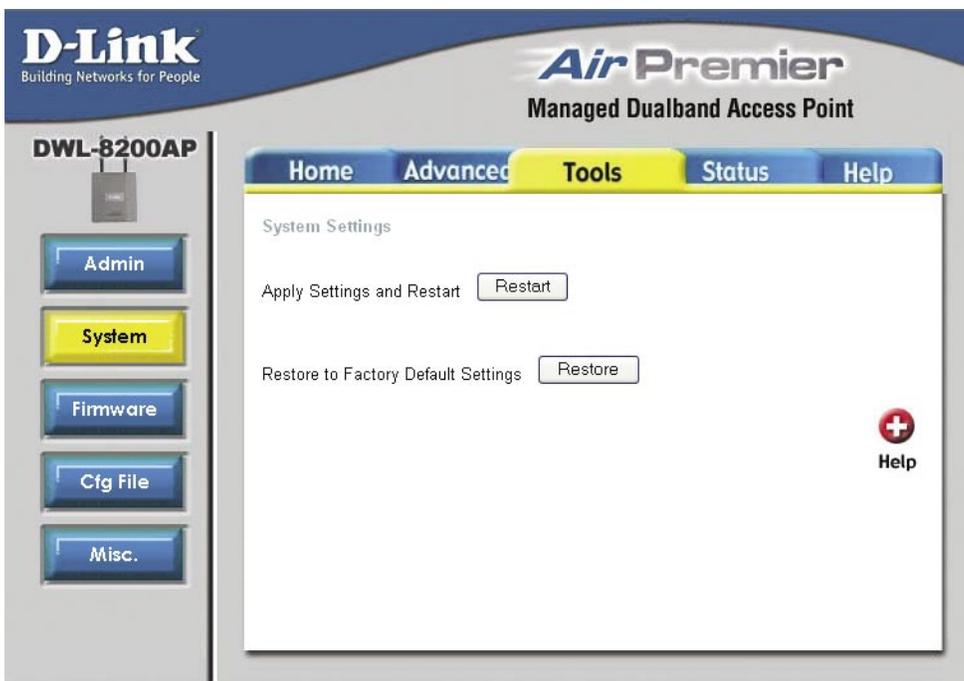
User Name: Enter a user name. The default setting is **admin**.

Old Password: To change your password, enter the old password here.

New Password: Enter your new password here.

Confirm New Password: Enter your new password again.

Tools > System

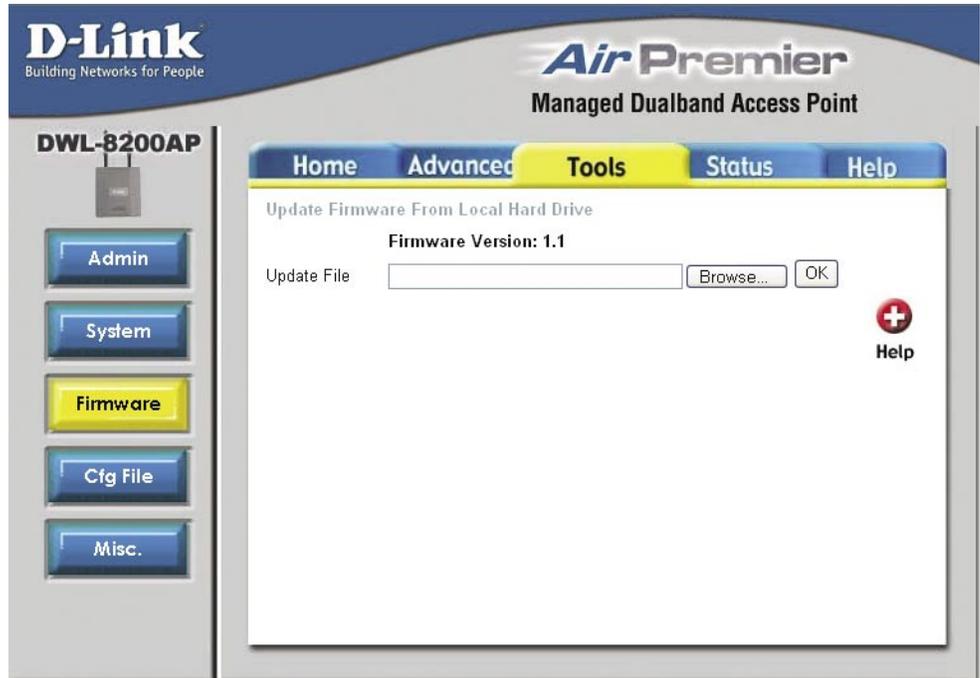


You may restart the **DWL-8200AP** with the changed settings or reset the **DWL-8200AP** back to factory settings.

Apply Settings and Restart: Click **Restart** to apply the system settings and restart the **DWL-8200AP**.

Restore to Factory Default Settings: Click **Restore** to return the **DWL-8200AP** to its factory default settings.

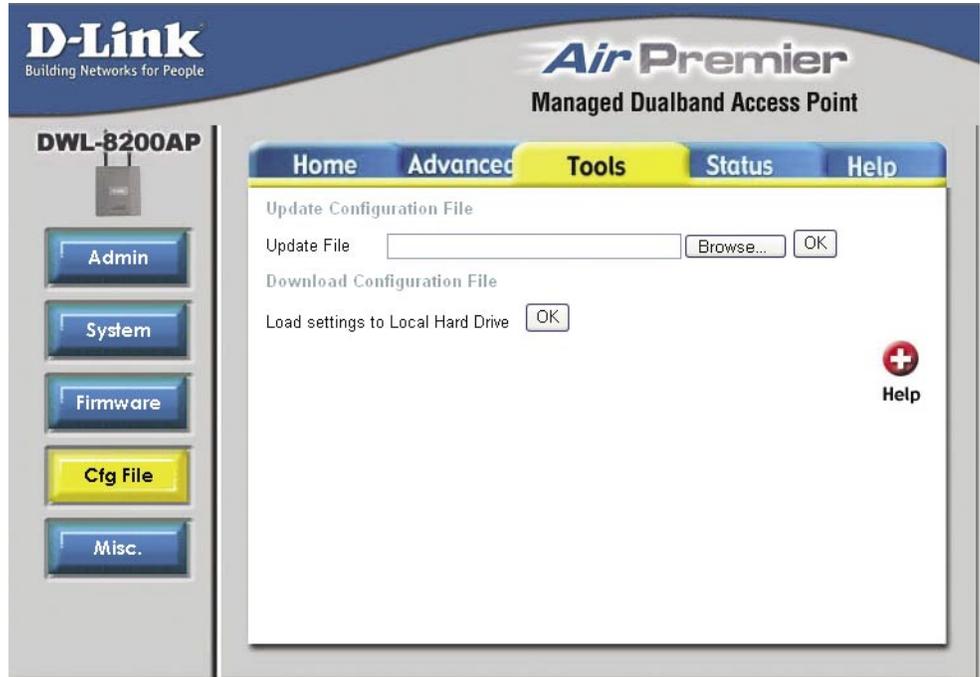
Tools > Firmware



The firmware of the **DWL-8200AP** can be upgraded to resolve any compatibility or system conflicts. Please visit <http://support.dlink.com> for the latest firmware for this device.

Update File: After you have downloaded the most recent version of the firmware from <http://support.dlink.com> to your hard drive, you can **Browse** your hard drive to locate the downloaded file. Select the file and click **OK** to update the firmware. The AP will automatically restart after the firmware upgrade.

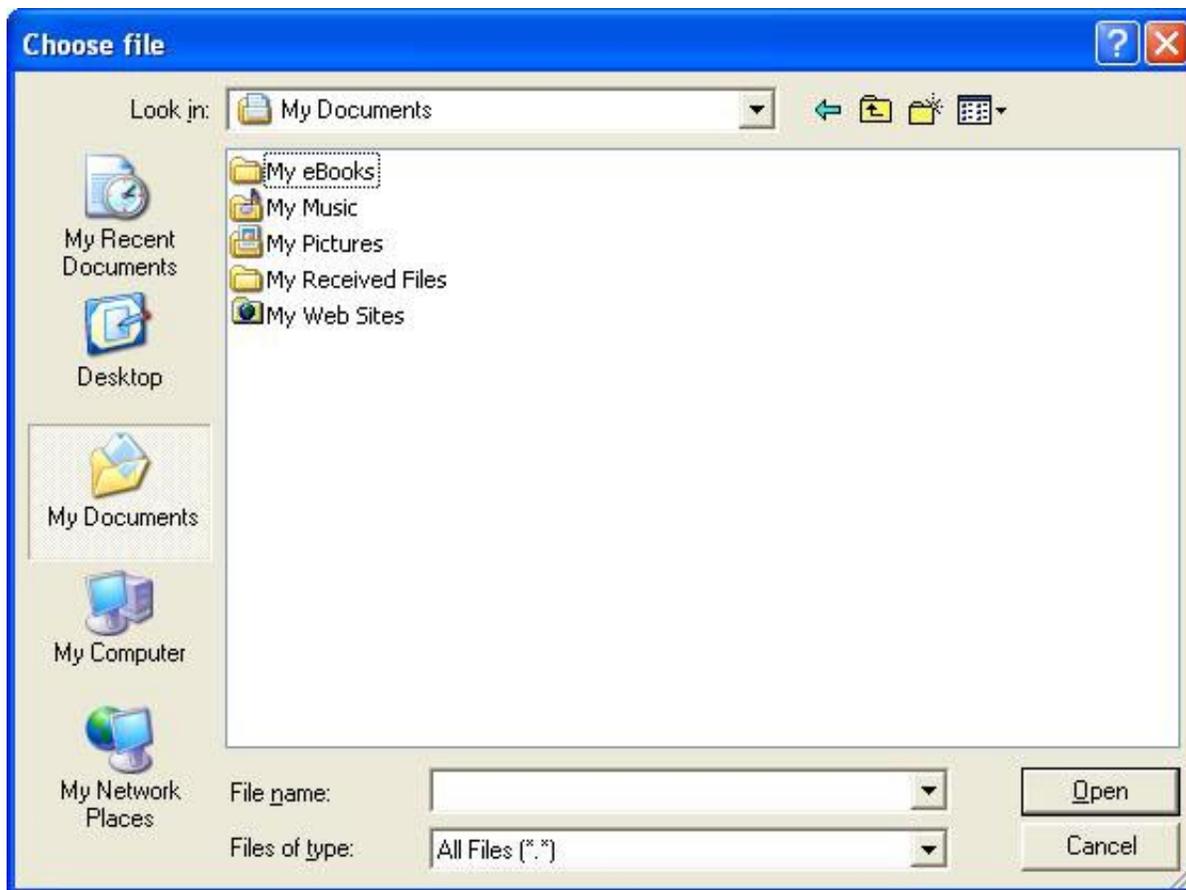
Tools > Cfg File



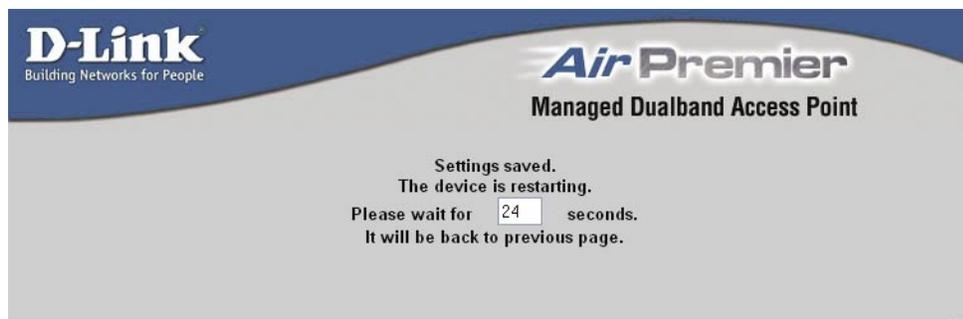
Update File: Browse for the configuration settings that you have saved to your hard drive. Click **OK** after you have selected the settings file.

Load Settings to the Local Hard Drive: Click **OK** to save the selected settings to your hard drive.

Tools > Cfg File > Choose file

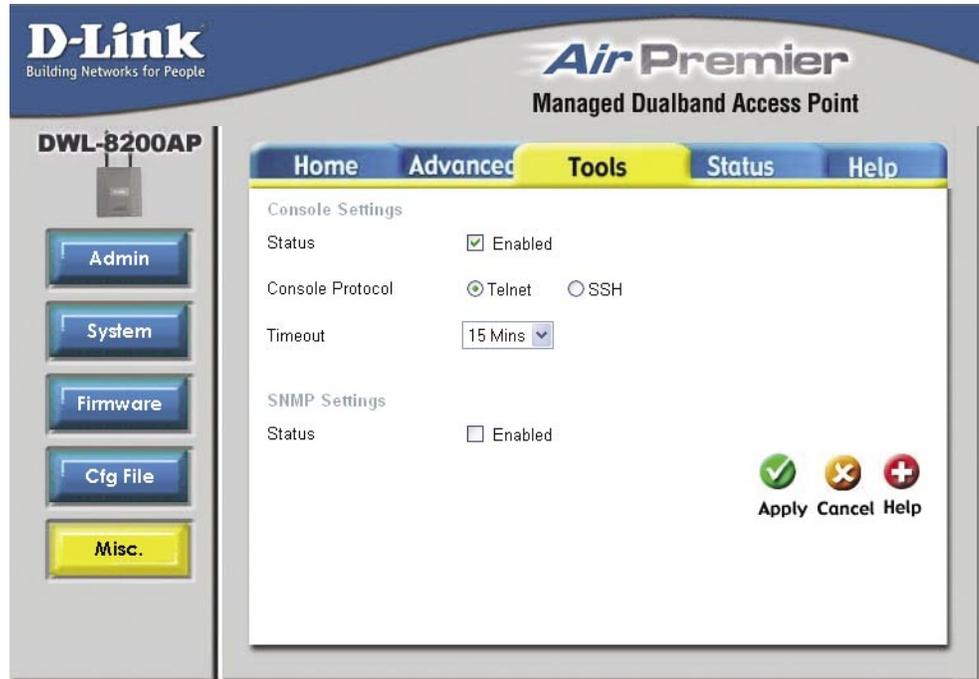


When you click **Browse** in the previous screen, the dialog box shown above appears. Select the file you wish to download and click **Open**.



The dialog box above will appear as the device restarts. Please wait for a few seconds.

Tools > Misc > Telnet Settings



Telnet is a program that allows you to control your device from a single PC.

Status: Check **Enabled** to support Telnet or SSH.

Console Protocol: Select either **Telnet** or **SSH**. **Telnet** is enabled by default.

Timeout: Select a time period after which a session timeout will occur. Your choices are **1 minute**, **3 minutes**, **5 minutes**, **10 minutes**, **15 minutes**, or **Never**.

Status: Check **Enabled** to support SNMP.

Note: SNMP is disabled by default.

Status > Device Info

D-Link
Building Networks for People

Air Premier
Managed Dualband Access Point

DWL-8200AP

Device Info
Stats
Client Info
Log

Home Advanced Tools **Status** Help

Device Information

Firmware Version: v1.00

Ethernet MAC Address: 00:0f:3d:fa:6d:c0
WLAN0 MAC Address: 00:0f:3d:fa:6d:c0 ~ 00:0f:3d:fa:6d:c7
WLAN1 MAC Address: 00:0f:3d:fa:6d:c8 ~ 00:0f:3d:fa:6d:cf

Ethernet

Get IP From: Manual
IP address: 192.168.0.50
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0

Wireless (802.11a)

SSID: default
Channel: 52
Super Mode: Disabled
Rate: Auto
Security Level: Open System / Encryption Disabled

Wireless (802.11g)

SSID: default
Channel: 6
Super Mode: Disabled
Rate: Auto
Security Level: Open System / Encryption Disabled

Help

Device Information: This window displays the settings of the **DWL-8200AP**, the firmware version and the MAC address.

Status > Stats > WLAN 802.11A Traffic Statistics

The screenshot shows the configuration interface for a D-Link Air Premier Managed Dualband Access Point. The page title is "WLAN 802.11A Traffic Statistics" with a link to "WLAN 802.11G Traffic Statistics". The interface includes a navigation menu with "Home", "Advanced", "Tools", "Status", and "Help". The "Status" tab is active. On the left, there are buttons for "Device Info", "Stats", "Client Info", and "Log". The main content area displays traffic statistics for the IEEE 802.11a network.

| ThroughPut | |
|------------------------|-------|
| Transmit Success Rate | 100 % |
| Transmit Retry Rate | 1 % |
| Receive Success Rate | 0 % |
| Receive Duplicate Rate | 0 % |
| RTS Success Count | 20 |
| RTS Failure Count | 58 |

| Transmitted Frame Count | |
|-----------------------------------|----|
| Transmitted Frame Count | 0 |
| Multicast Transmitted Frame Count | 56 |
| Transmitted Error Count | 19 |
| Transmitted Total Retry Count | 81 |
| Transmitted Multiple Retry Count | 58 |

| Received Frame Count | |
|--------------------------------|----|
| Received Frame Count | 48 |
| Multicast Received Frame Count | 35 |
| Received Frame FCS Error Count | 89 |
| Received Frame Duplicate Count | 82 |
| Ack Rcv failure Count | 74 |

| Wep Frame Error Count | |
|--------------------------|----|
| WEP Excluded Frame Count | 17 |
| WEP ICV Error Count | 86 |

Refresh Help

WLAN 802.11A Traffic Statistics: This window displays the statistics data of throughput, transmitted frame, received frame, and WEP frame error for the IEEE 802.11a network.

Status > Stats > WLAN 802.11G Traffic Statistics

The screenshot shows the configuration interface for a D-Link Air Premier Managed Dualband Access Point (DWL-8200AP). The interface includes a navigation menu on the left with buttons for Device Info, Stats, Client Info, and Log. The main content area displays traffic statistics for WLAN 802.11G, with tabs for Home, Advanced, Tools, Status, and Help. The Status tab is active, showing a table of statistics.

| ThroughPut | |
|------------------------|-------|
| Transmit Success Rate | 100 % |
| Transmit Retry Rate | 1 % |
| Receive Success Rate | 0 % |
| Receive Duplicate Rate | 0 % |
| RTS Success Count | 20 |
| RTS Failure Count | 58 |

| Transmitted Frame Count | |
|-----------------------------------|----|
| Transmitted Frame Count | 71 |
| Multicast Transmitted Frame Count | 51 |
| Transmitted Error Count | 30 |
| Transmitted Total Retry Count | 1 |
| Transmitted Multiple Retry Count | 9 |

| Received Frame Count | |
|--------------------------------|----|
| Received Frame Count | 36 |
| Multicast Received Frame Count | 14 |
| Received Frame FCS Error Count | 16 |
| Received Frame Duplicate Count | 99 |
| Ack Rcv failure Count | 44 |

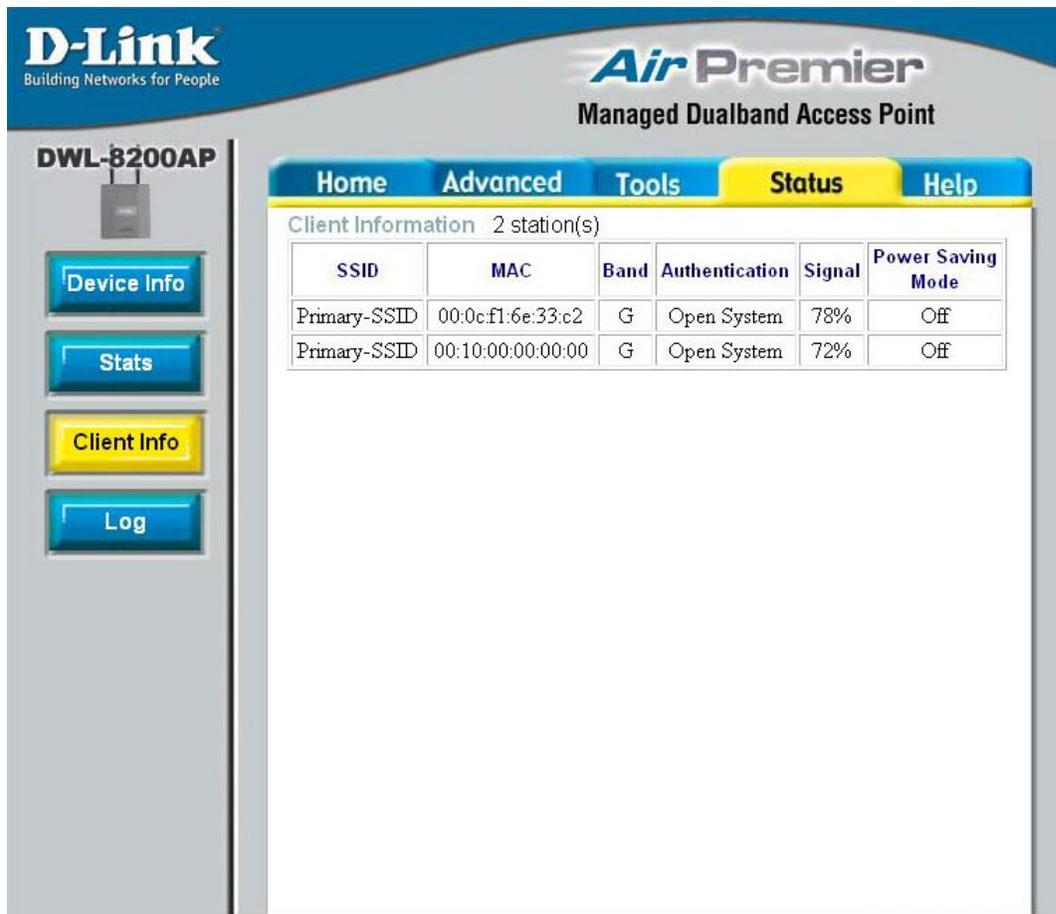
| Wep Frame Error Count | |
|--------------------------|----|
| WEP Excluded Frame Count | 11 |
| WEP ICV Error Count | 0 |

Refresh Help

WLAN 802.11G Traffic Statistics:

This window displays the statistics data of throughput, transmitted frame, received frame, and WEP frame error for the IEEE 802.11g network.

Status > Client Info



Client Information: Select this option to obtain information on wireless clients. (A client is a device on the network that is communicating with the **DWL-8200AP**.)

The following information is available for each client that is communicating with the **DWL-8200AP**.

MAC: Displays the MAC address of the client.

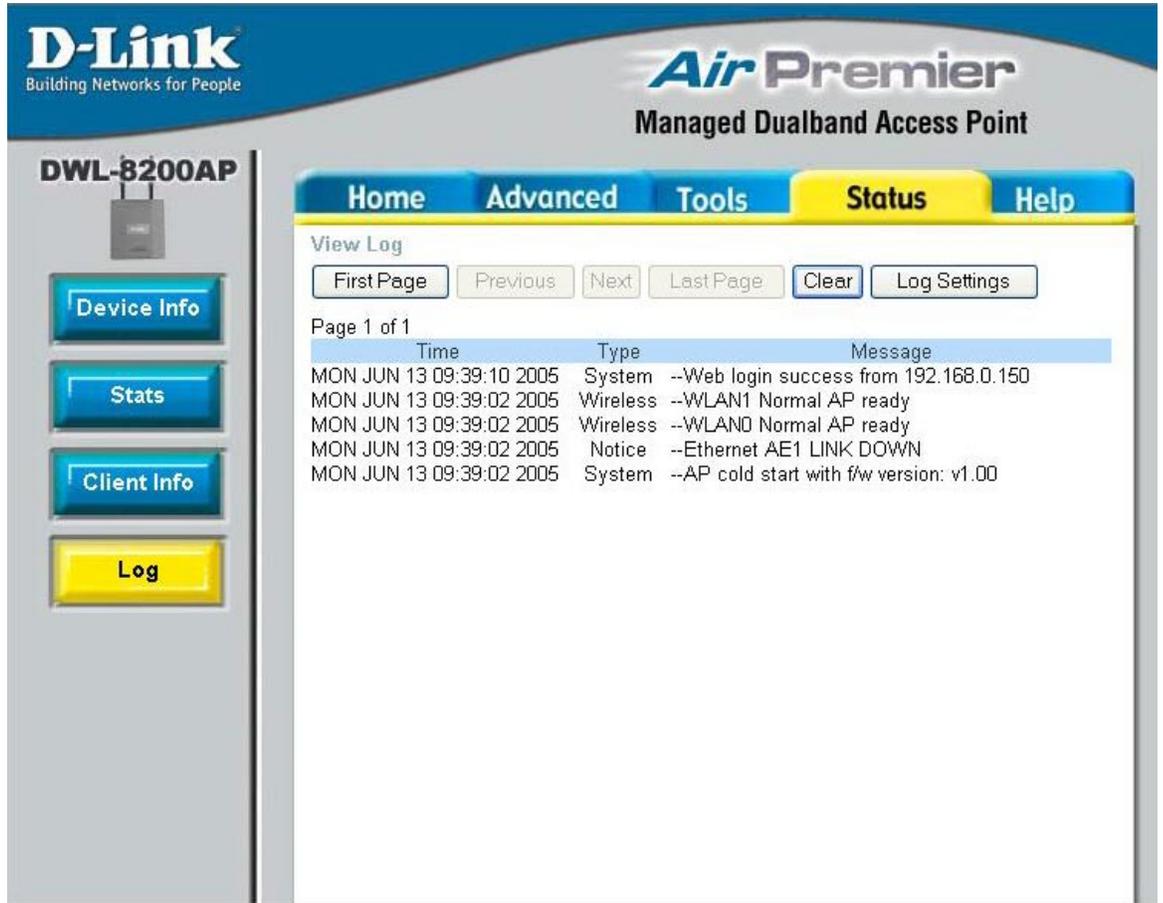
Band: Displays the wireless band.

Authentication: Displays the type of authentication that is enabled.

Signal: Indicates the strength of the signal

Power Saving Mode: Displays the status of the power saving feature.

Status > Log

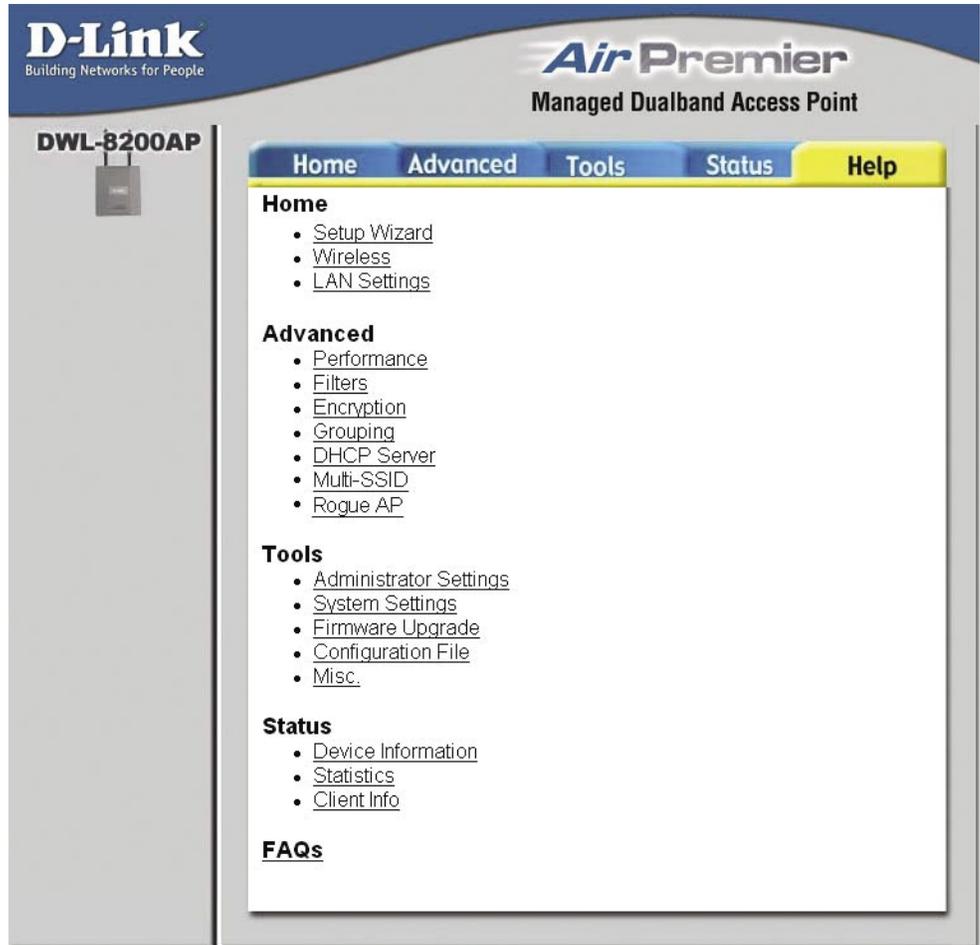


The log information will include, but not limited to, the following items:

- Upgrade Firmware
- Client Associate and Disassociate with AP
- Web login

The embedded memory can hold up to 500 logs.

Help



Help: Click on any item in the Help screen for more information.

Using the AP Manager

The AP Manager is a convenient tool to manage the configuration of your network from a central computer. With AP Manager there is no need to configure devices individually.

To launch the **AP Manager**:

- Go to the **Start Menu**
- Select **Programs**
- Select **D-Link TriMode Dualband AP Manager**
- Select **DWL-8200AP**



Discovering Devices



Click on this button to **discover the devices** available on the network.

| Exist | Model Name | Mac Address | IP Address | Netmask | F/W Version | Device Name | Action | Status |
|-------|------------|--------------|--------------|---------------|-------------|----------------|--------|--------|
| ✓ | DWL-8200AP | 000F3DFA6DC0 | 192.168.0.50 | 255.255.25... | v1.00 Beta | D-Link Acce... | Set IP | |

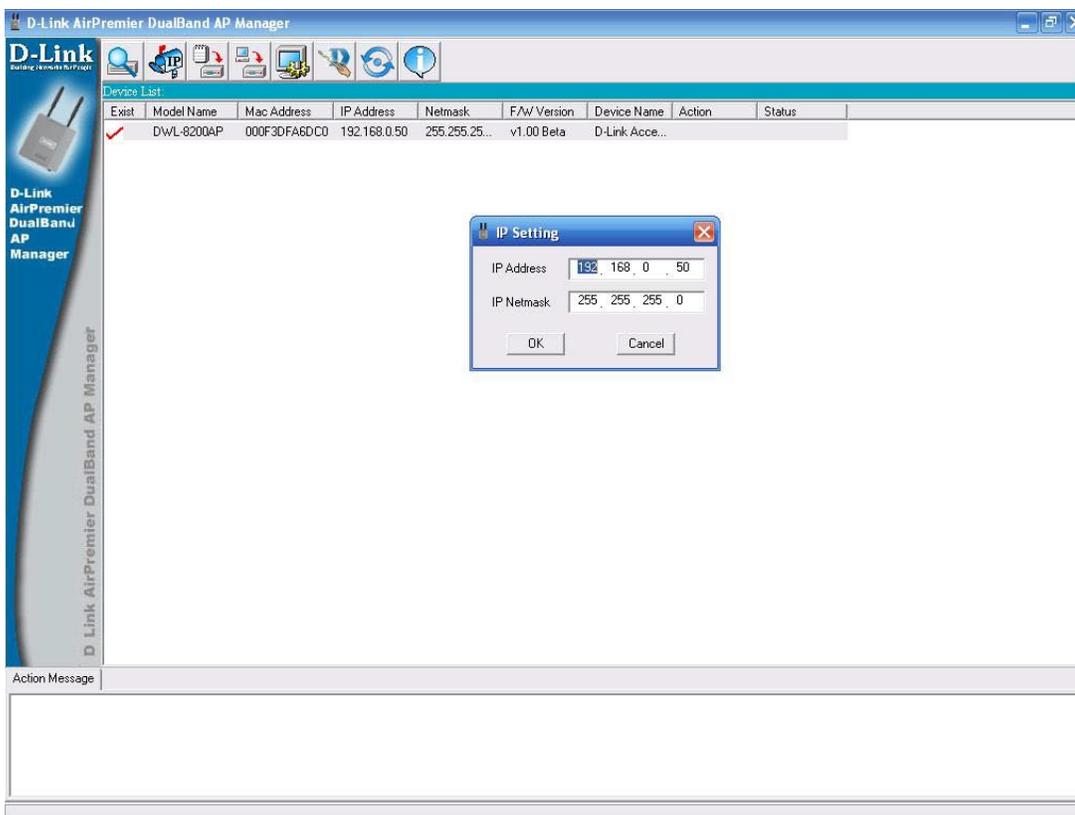
Selecting Devices

The AP Manager allows you to configure multiple devices all at once. To select a single device, simply click on the device you want to select. To select multiple devices, hold down the **Ctrl** key while clicking on each additional device. To select an entire list, hold the **Shift** key, click on the first AP on the list and then click on the last AP on the list.

IP Configuration

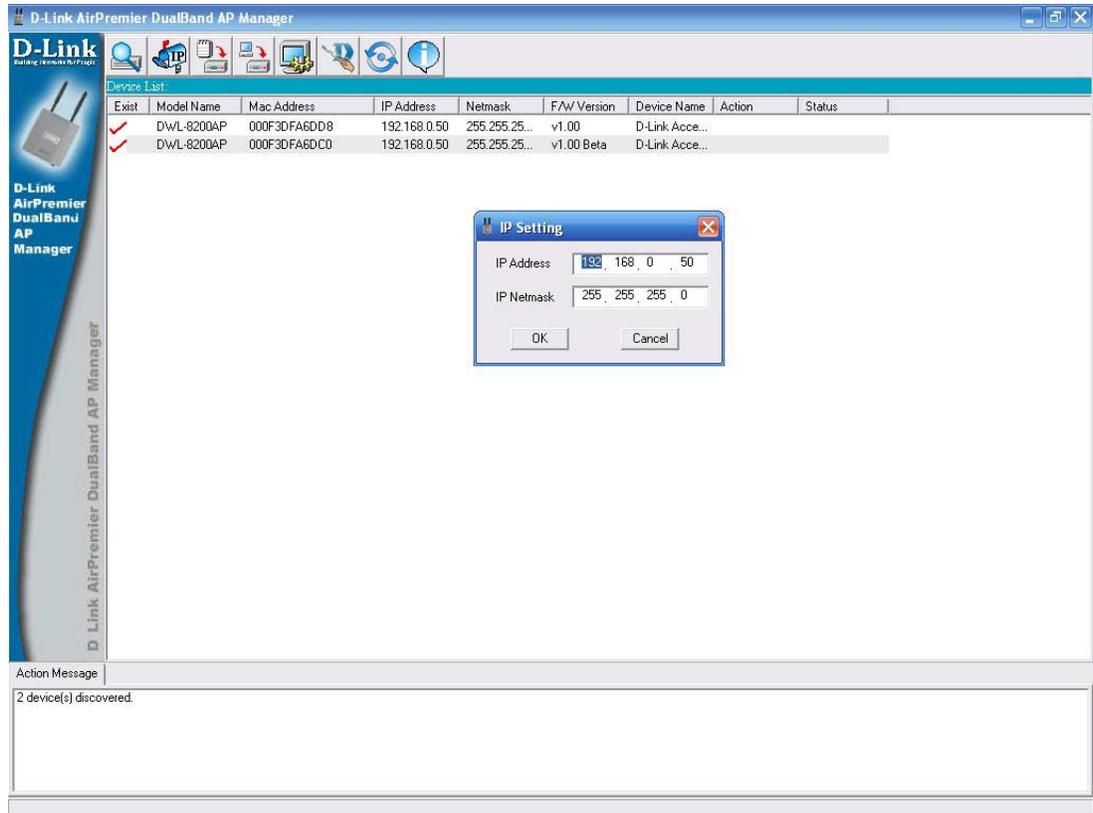


You can assign an IP address to an AP or assign IP addresses to multiple AP's by clicking on this button after selecting the device(s).



Select the AP that you want to assign an IP address to and click the IP button. Enter the IP address and IP netmask for the selected device and click OK.

IP Configuration (continued)



You can configure multiple AP's with IP addresses all at once. Click on the IP button after you've selected all of the AP's you want to assign an IP address. Enter the IP address you want to assign the first unit and the AP manager will automatically assign sequential IP addresses.

Device Configuration



Click on this button to access the configuration properties of the selected device(s).

The device configuration window allows you to configure settings but does not actually apply the settings to the device unless you click the **Apply** button. You can also save and load configuration files from this window. When you load a configuration file, you must click **Apply** if you want the settings to be applied to the selected device(s).

You can configure a single device by highlighting one device in the list, or you can configure multiple devices by highlighting multiple devices before clicking on the Device Configuration icon pictured above. The examples in this section show single device configuration. When you select multiple devices for configuration the procedure will be similar.

Check All

The Check All button will select all configurable options. Any setting that has a checkmark next to it is applied to the device or saved to the configuration file.

Clear Checks

The Clear Checks button deselects all configurable options. This feature is useful if you only want to change a few settings. Deselect all items and only check the items that you want to modify.

Refresh

Refresh will revert to the actual device settings of the selected device(s).

Apply

To save settings to the device, you must click the Apply button. Only settings that have a checkmark next to them will be applied.

Open

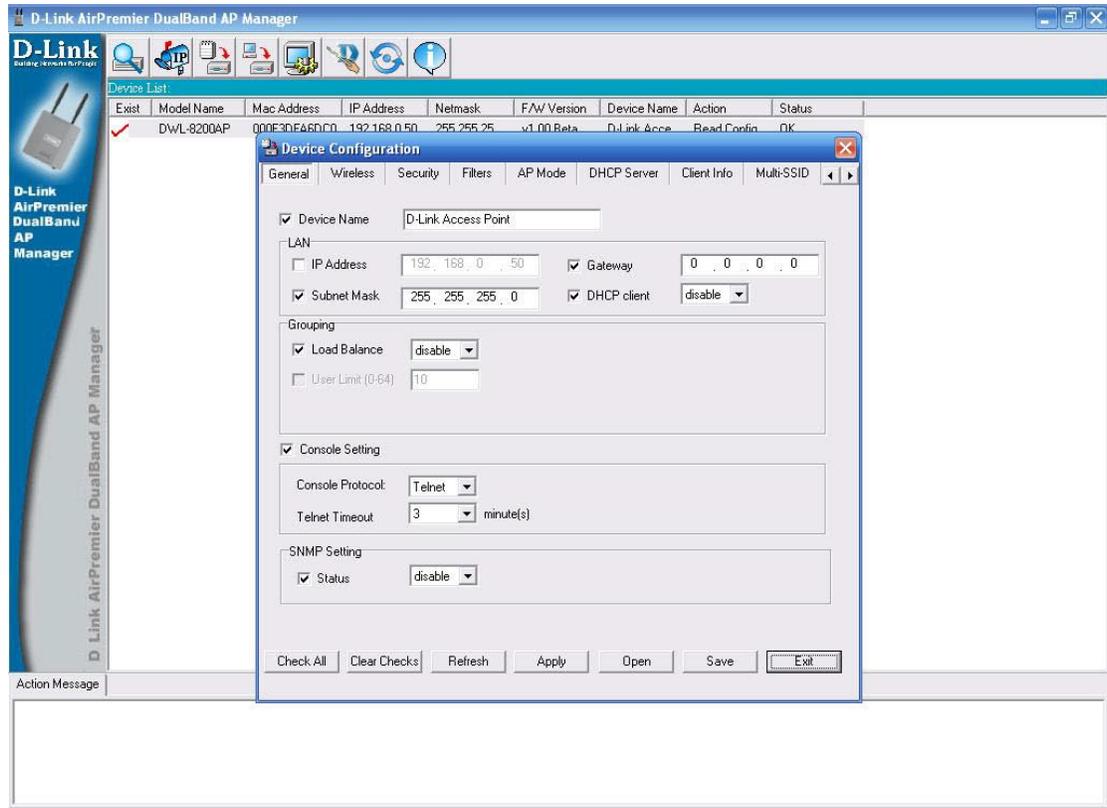
The open button is used to load a previously saved configuration file. After opening a configuration file, you must click the Apply button to save the settings to the selected device(s).

Save

The save button allows you to save a configuration file of the selected device settings. Only settings that have a checkmark next to them are saved. You cannot save a configuration file if you selected more than one device in the device list.

Exit

The Exit button will close the device configuration window. Any settings that haven't been applied will be lost.



Device Configuration > General

When selecting multiple devices for configuration, some options are unavailable for configuration by default as noted(*) below:

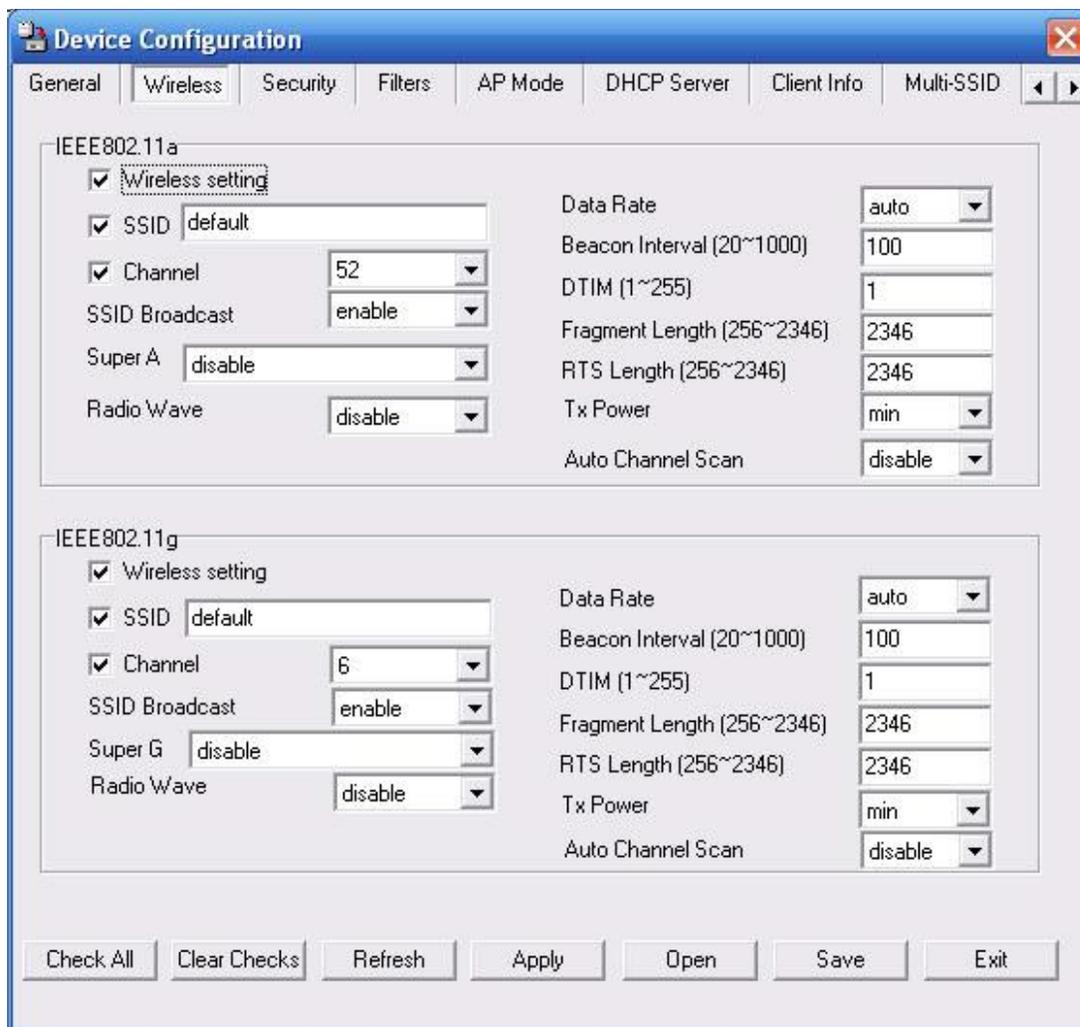
- Device Name(*):** This allows you to change the device name for the selected access point. You must place a checkmark in the Device Name box to change the name. This option should only be configured when one access point is selected for configuration.
- IP address and Subnet Mask(*):** If you've selected one device for configuration and you want to change the IP address of the device, check the IP Address box. You can then enter an IP address and Subnet Mask for the selected access point. This option should only be configurable when one access point is selected for configuration. To configure multiple devices with an IP address at one time, please reference the previous page.
- Gateway:** Enter the IP address of your gateway, typically your router address.



Device Configuration > General (continued)

- DHCP client:** There is a pull-down menu to select enabled or disabled. When enabled, the selected device(s) will function as a DHCP client(s). This allows them to receive IP configuration information from a DHCP server. When disabled, the access point(s) must have a static IP address assigned to them.
- Load Balance:** This pull-down selection enables or disables load balancing. When you enable load balance you allow several access points to balance wireless network traffic and wireless clients among the access points with the same SSID. All the APs that share Load Balancing must have the same SSID. Assign each access point a different non-overlapping channel (e.g., 1, 6, 11).
- User Limit:** Enter the number of the limit of load balancing users, from 0-64.
- Console Protocol:** From the pull-down selection, choose either **Telnet** or **SSH** for Console protocol.
- Telnet Timeout:** This pull-down selection defines the timeout period during a Telnet session with the selected device(s).
- Status:** Select **Enable** to set the SNMP setting.

Device Configuration > Wireless



IEEE 802.11a:

Wireless: Check to enable wireless mode.

SSID: The Service Set (network) Identifier of your wireless network.

Channel: Allows you to select a channel. **52** is the default setting for 802.11a.

SSID Broadcast: Allows you to **enable** or **disable** the broadcasting of the SSID to network clients.

Super A: Select this option to enable a wireless signal rate of up to 108Mbps. **Super A** is a group of performance enhancement features that increase end user application throughput in an 802.11a network. **Super A** is backwards compatible with standard 802.11a devices. For ideal performance, all wireless devices on the network should be **Super A** capable.

Device Configuration > Wireless (*continued*)

| Super A Mode | Function |
|----------------------------|---|
| Disabled | Standard 802.11a support. No enhanced capabilities. |
| Super A without Turbo | Capable of Packet Bursting, FastFrames, Compression. No Turbo mode. |
| Super A with Dynamic Turbo | Capable of Packet Bursting, FastFrames, Compression, and Dynamic Turbo mode. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are configured with Super A and Dynamic Turbo enabled. |
| Super A with Static Turbo | Capable of Packet Bursting, FastFrames, Compression, and Static Turbo mode. This setting is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all devices on the wireless network are configured with Super A and Static Turbo enabled. |

Radio Wave: Select **Enable** or **Disable**.

Data Rate*: A pull-down menu to select the maximum wireless signal rate for the selected device(s).

Beacon Interval (20~1000): Beacons are packets sent by an access point to synchronize a network. Specify the beacon value for the selected device(s) here. The default value of **100** is recommended.

DTIM (1~255): DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next listening window for broadcast and multicast messages.

Fragment Length (256~2346): This sets the fragmentation threshold (specified in bytes). Packets exceeding the value set here will be fragmented. The default is **2346**.

RTS Length (256~2346): The RTS value should not be changed unless you encounter inconsistent data flow. The default value is **2346**.

Tx Power: Choose **full**, **half (-3dB)**, **quarter (-6dB)**, **eighth (-9dB)**, **minimum power**. This tool can be helpful for security purposes if you wish to limit the transmission range.

Auto Channel: **Enable** this option to automatically select the most optimal channel available for wireless networking and to scan for the least populated channel.

*Maximum wireless signal rate derived from IEEE Standard 802.11a and 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 actual data throughput rate.

Device Configuration > Wireless (*continued*)

IEEE 802.11g:

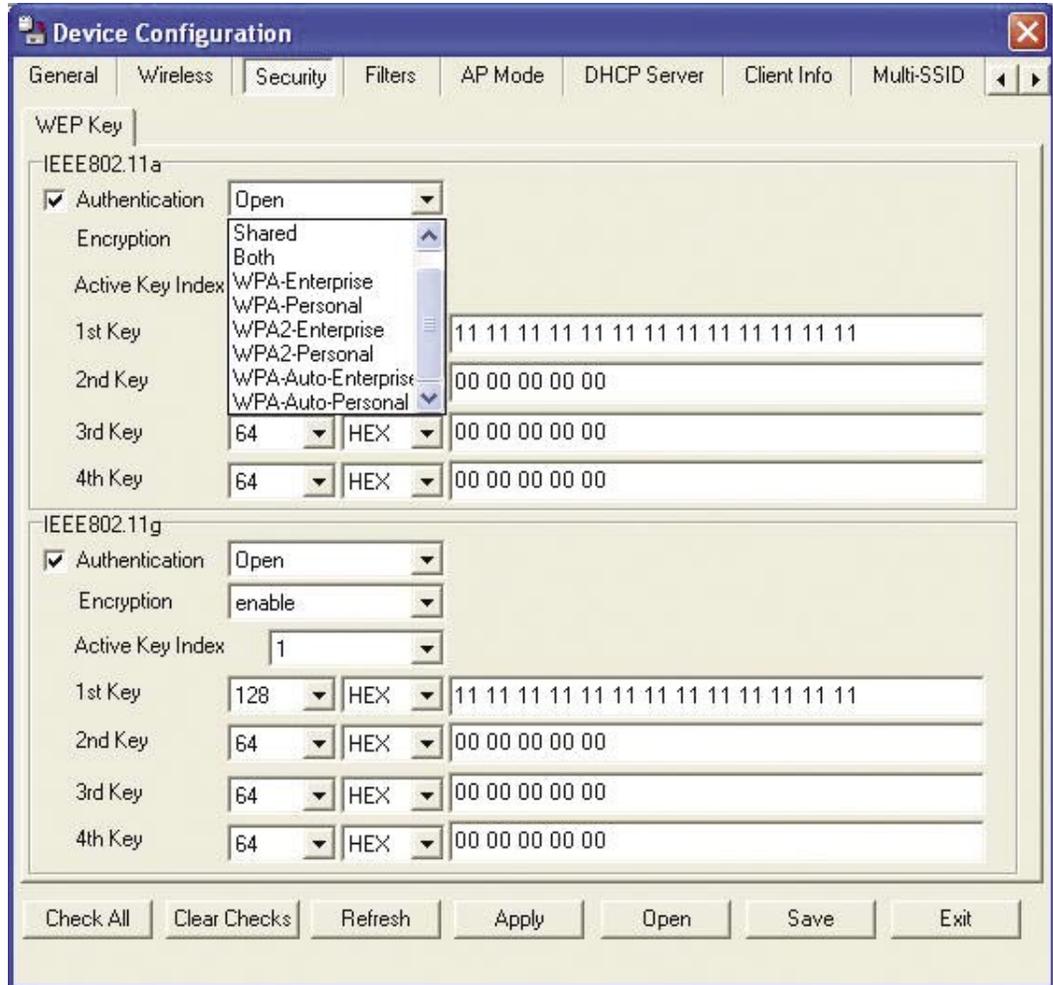
| | |
|------------------------------------|---|
| Wireless: | Check to enable wireless mode. |
| SSID: | The Service Set (network) Identifier of your wireless network. |
| Channel: | Allows you to select a channel. 6 is the default setting. |
| SSID Broadcast: | Allows you to enable or disable the broadcasting of the SSID to network clients. |
| Super G: | Select this option to enable a wireless signal rate of up to 108Mbps. |
| Radio Wave: | Select Enable or Disable . |
| Data Rate*: | A pull-down menu to select the maximum wireless signal rate for the selected device(s). |
| Beacon Interval (20~1000): | Beacons are packets sent by an access point to synchronize a network. Specify the beacon value for the selected device(s) here. The default value of 100 is recommended. |
| DTIM (1~255): | DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next listening window for broadcast and multicast messages. |
| Fragment Length (256~2346): | This sets the fragmentation threshold (specified in bytes). Packets exceeding the value set here will be fragmented. The default is 2346 . |
| RTS Length (256~2346): | The RTS value should not be changed unless you encounter inconsistent data flow. The default value is 2346 . |
| Tx Power: | Choose full , half (-3dB) , quarter (-6dB) , eighth (-9dB) , minimum power . This tool can be helpful for security purposes if you wish to limit the transmission range. |
| Auto Channel: | Select this option to automatically select the most optimal channel available for wireless networking. |

*Maximum wireless signal rate derived from IEEE Standard 802.11a and 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 actual data throughput rate.

Device Configuration > Security > Authentication

| AP Mode | Authentication Available |
|---------------------|---|
| Access Point | Open Shared Both WPA-Enterprise WPA-Personal WPA2-Enterprise WPA2-Personal WPA-Auto-Enterprise WPA-Auto-Personal |
| WDS with AP | Open Shared Both WPA-Personal WPA2-Personal WPA-Auto-Personal |
| WDS | Open Shared Both WPA-Personal WPA2-Personal WPA-Auto-Personal |

Device Configuration > Security > Authentication *(continued)*



Open: The key is communicated across the network.

Shared: Limited to communication with devices that share the same WEP settings.

Both: The key is communicated and identical WEP settings are required.

Authentication: Select **Open System/Shared Key** to allow either form of data encryption.

Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.

Device Configuration > Security > Authentication (*continued*)

Authentication (*continued*):

Select **WPA-Personal** to secure your network using a password and dynamic key changes. (No RADIUS server required.)

Select **WPA2-Enterprise** to secure your network with the inclusion of a RADIUS server and upgrade the encryption of data with the Advanced Encryption Standard (AES).

Select **WPA2-Personal** to secure your network using a password and dynamic key changes. No RADIUS server required and encryption of data is upgraded with the Advanced Encryption Standard (AES).

Select **WPA-Auto-Enterprise** to allow the client to either use **WPA-Enterprise** or **WPA2-Enterprise**.

Select **WPA-Auto-Enterprise** to allow the client to either use **WPA-Personal** or **WPA2-Personal**.

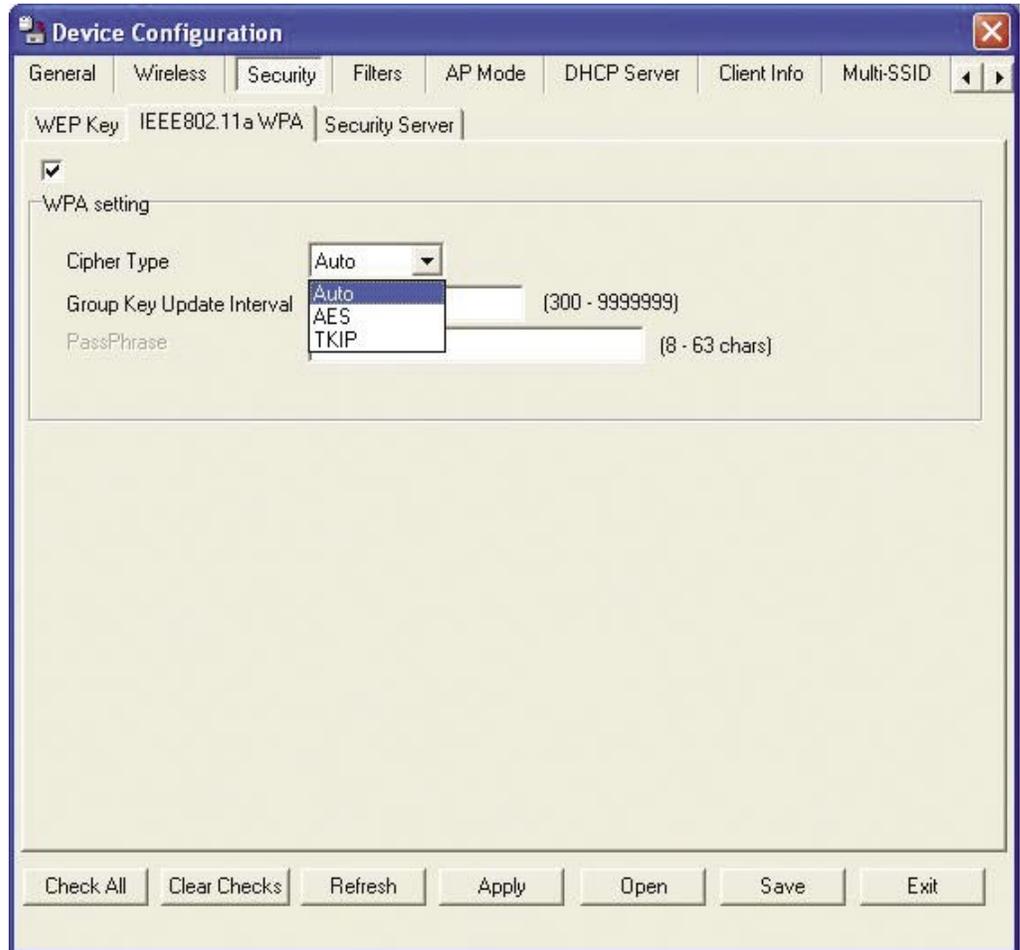
Device Configuration > Security > Open/Shared/Both

The screenshot shows the 'Device Configuration' window with the 'Security' tab selected. The 'WEP Key' section is active. It is divided into two parts: IEEE802.11a and IEEE802.11g. For both, the 'Authentication' is set to 'Open', 'Encryption' is 'disable', and 'Active Key Index' is '1'. There are four key entries for each standard, each with a '64' bit size, 'HEX' type, and a value of '00 00 00 00 00'. At the bottom, there are buttons for 'Check All', 'Clear Checks', 'Refresh', 'Apply', 'Open', 'Save', and 'Exit'.

The Security tab contains the WEP configuration settings on the initial page. If you select WPA as the authentication type, an additional tab will appear with the WPA configuration options based on your selection.

- Authentication Type:** Select from the pull-down menu the type of authentication to be used on the selected device(s). In this example you may select **Open**, **Shared**, or **Both**.
- Encryption:** **Enable** or **Disable** encryption on the selected device(s). This option will only be available when security is set to **Open** or **Both**.
- Active Key Index:** Select which defined key is active on the selected device(s). This option will only be available when security is set to **Open**, **Shared**, or **Both**.
- Key Values:** Select the key size (**64-bit**, **128-bit**, or **152-bit**) and key type (**HEX** or **ASCII**) and then enter a string to use as the key. The key length is automatically adjusted based on the settings you choose. This option will only be available when security is set to **Open**, **Shared**, or **Both**.

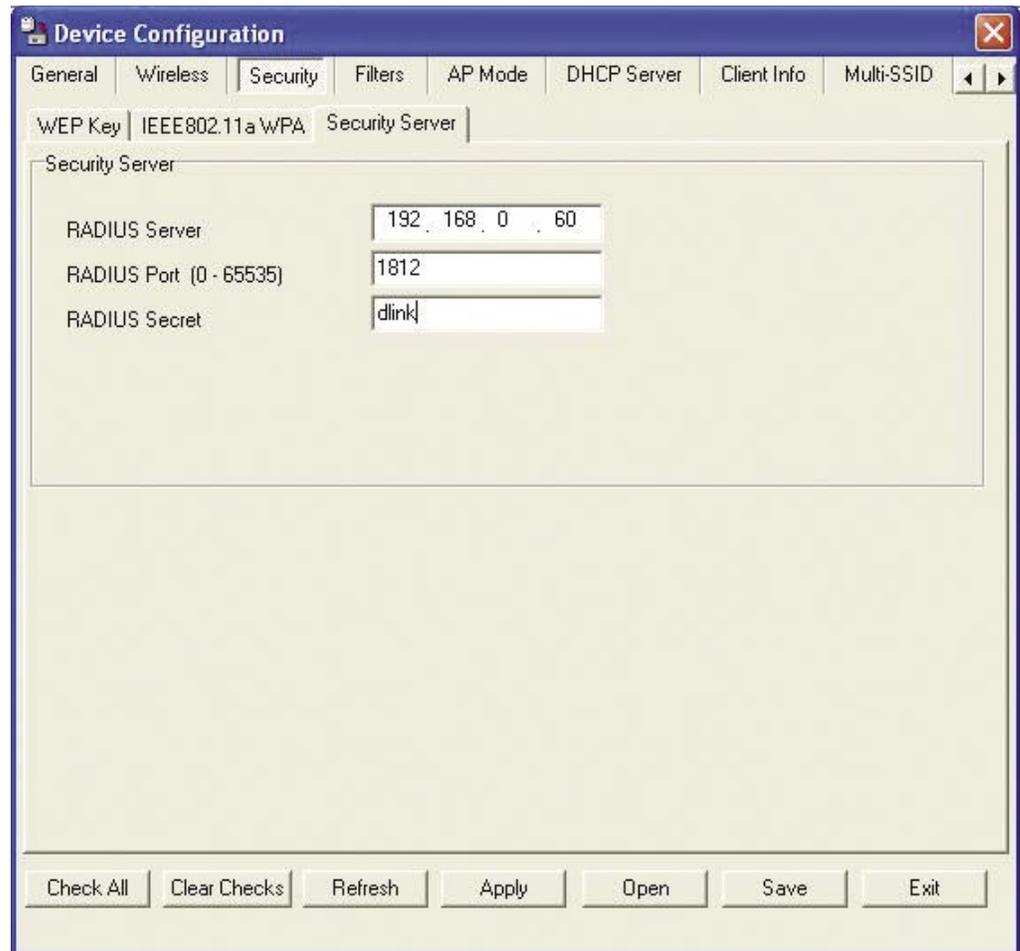
Device Configuration > Security > WPA-Enterprise, WPA2-Enterprise, & WPA-Auto-Enterprise



Cipher Type: Select **Auto**, **TKIP**, or **AES** from the pull-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. **1800** is the recommended setting. A lower interval may reduce transfer rates.

Device Configuration > Security > WPA-Enterprise, WPA2-Enterprise, & WPA-Auto-Enterprise > Security Server



The screenshot shows the 'Device Configuration' window with the 'Security' tab selected. Under the 'Security Server' sub-tab, the following fields are visible:

| Field | Value |
|-------------------------|--------------|
| RADIUS Server | 192.168.0.60 |
| RADIUS Port (0 - 65535) | 1812 |
| RADIUS Secret | dlink |

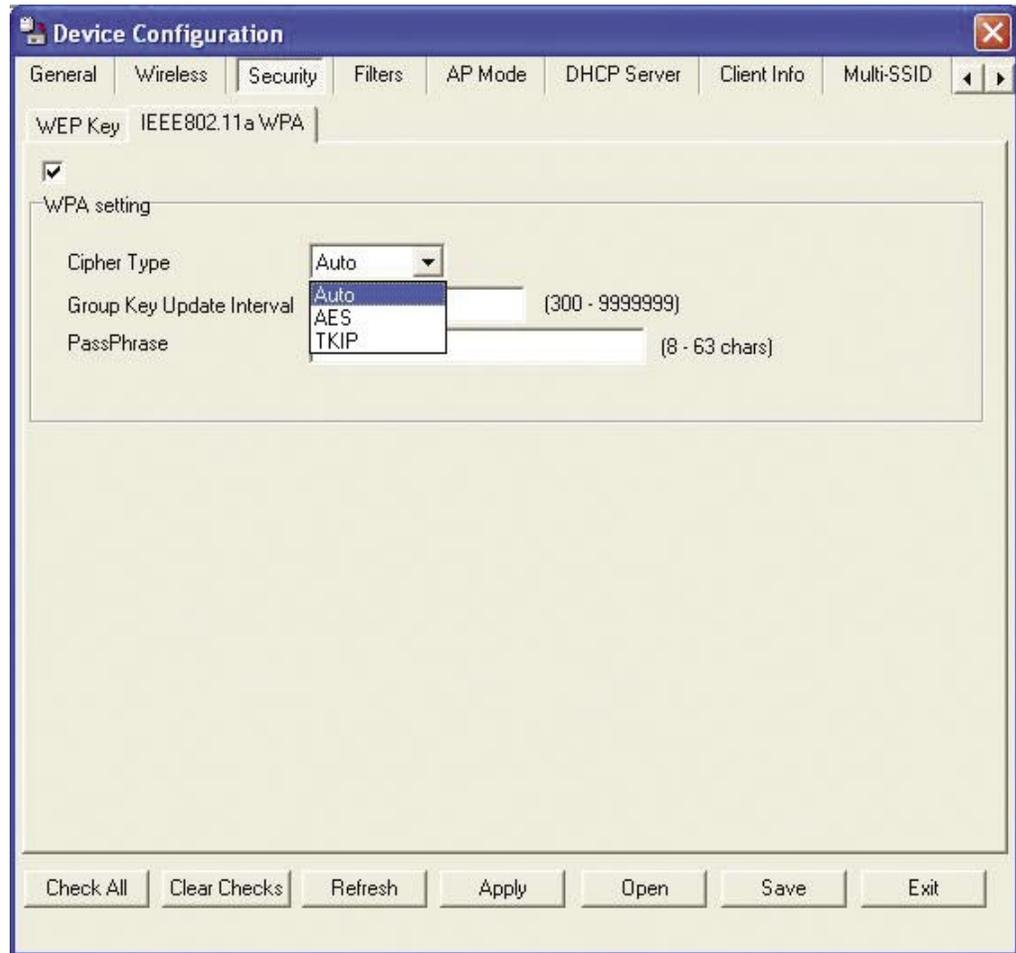
At the bottom of the window, there are buttons for 'Check All', 'Clear Checks', 'Refresh', 'Apply', 'Open', 'Save', and 'Exit'.

RADIUS Server: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the port used on the RADIUS server.

RADIUS Secret: Enter the RADIUS secret.

Device Configuration > Security > WPA-Personal, WPA2-Personal, & WPA-Auto-Personal

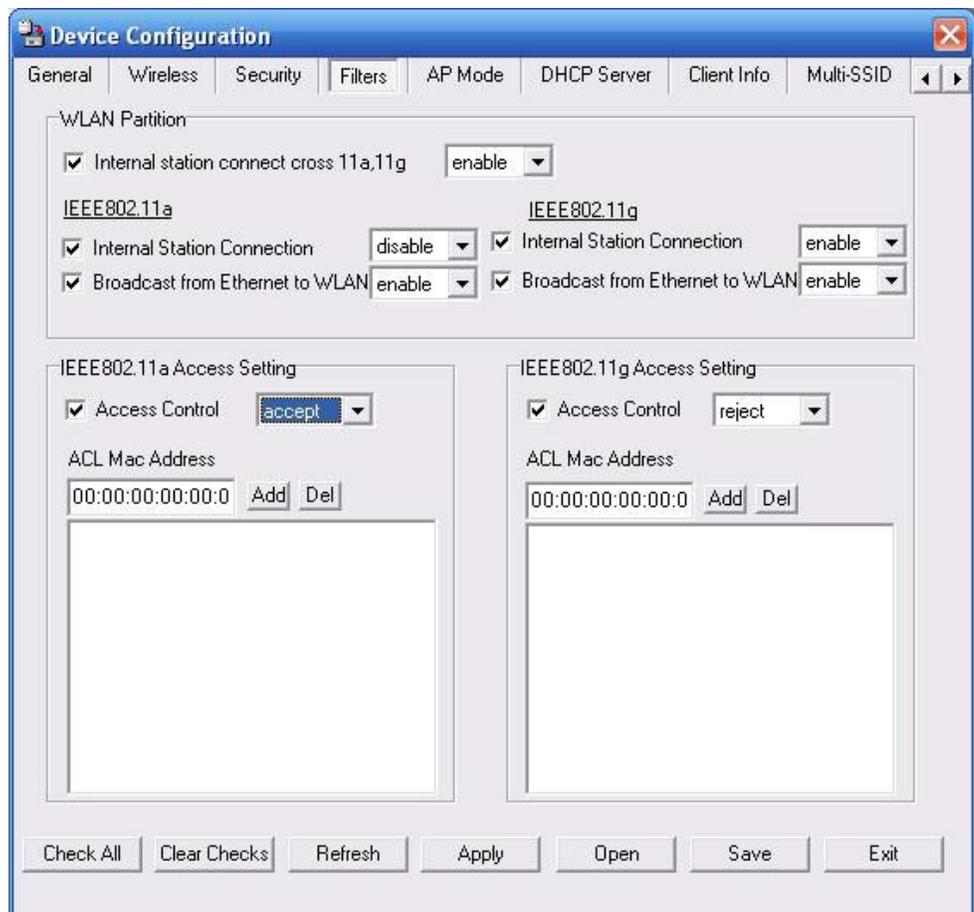


Cipher Type: Select **Auto**, **TKIP**, or **AES** from the pull-down menu.

Group Key Update Interval: Select the interval during which the group key will be valid. **1800** is the recommended setting. A lower interval may reduce transfer rates.

PassPhrase: Enter a **PassPhrase** between 8-63 characters in length.

Device Configuration > Filters



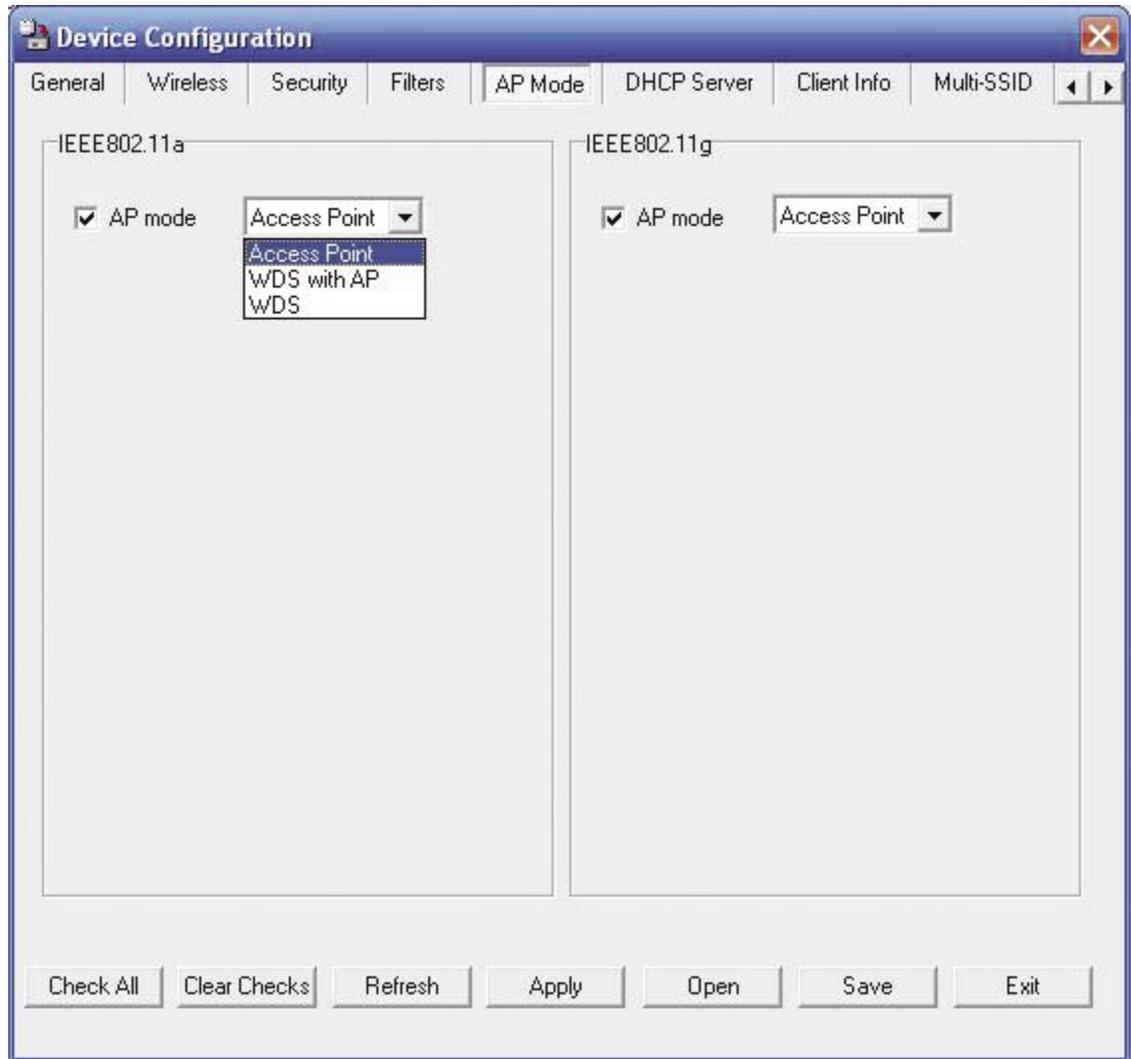
Internal Station Connection: Enabling this allows wireless clients to communicate with each other. When this option is disabled, wireless stations are not allowed to exchange data through the access point.

Ethernet to WLAN Access: Enabling this option allows Ethernet devices to communicate with wireless clients. When this option is disabled, all data from Ethernet to wireless clients is blocked. Wireless devices can still send data to the Ethernet devices when this is disabled.

Access Control: When disabled access control is not filtered based on the MAC address. If Accept or Reject is selected, then a box appears for entering MAC addresses. When **Accept** is selected, only devices with a MAC address in the list are granted access. When **Reject** is selected, devices in the list of MAC addresses are not granted access.

Access Control List: Add or Delete MAC addresses in the Access Control List.

Device Configuration > AP Mode

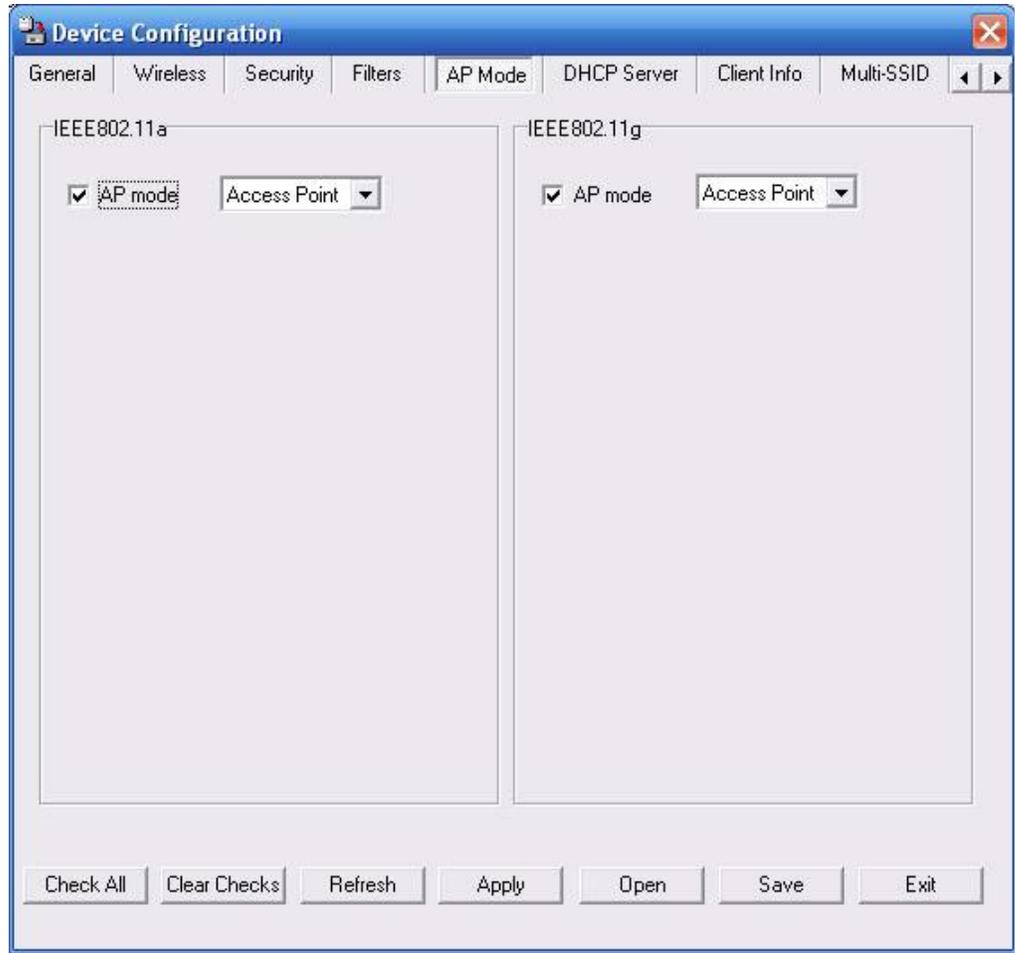


AP Mode: There are 3 AP modes:

- Access Point**
- WDS with AP**
- WDS**

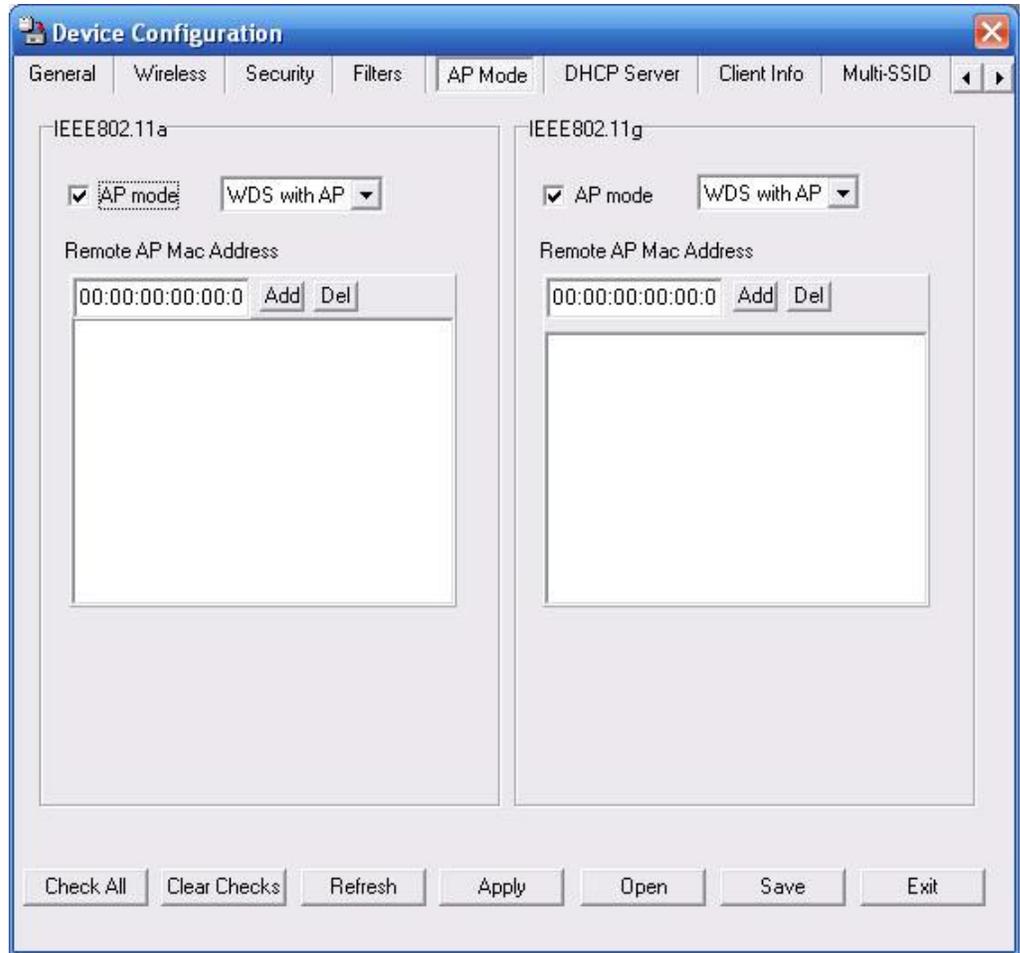
Please see the following pages for an explanation of all the AP modes.

Device Configuration > AP Mode > Access Point



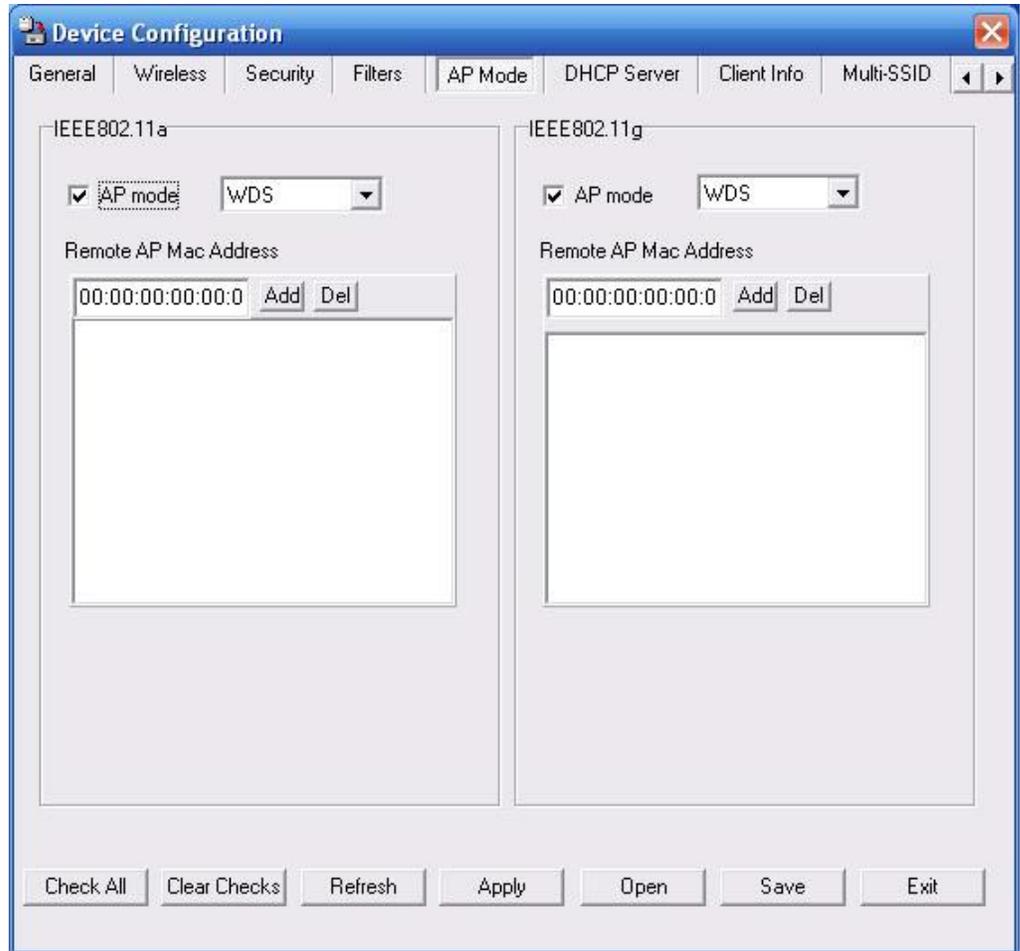
Access Point: Creates a Wireless LAN.

Device Configuration > AP Mode > WDS with AP



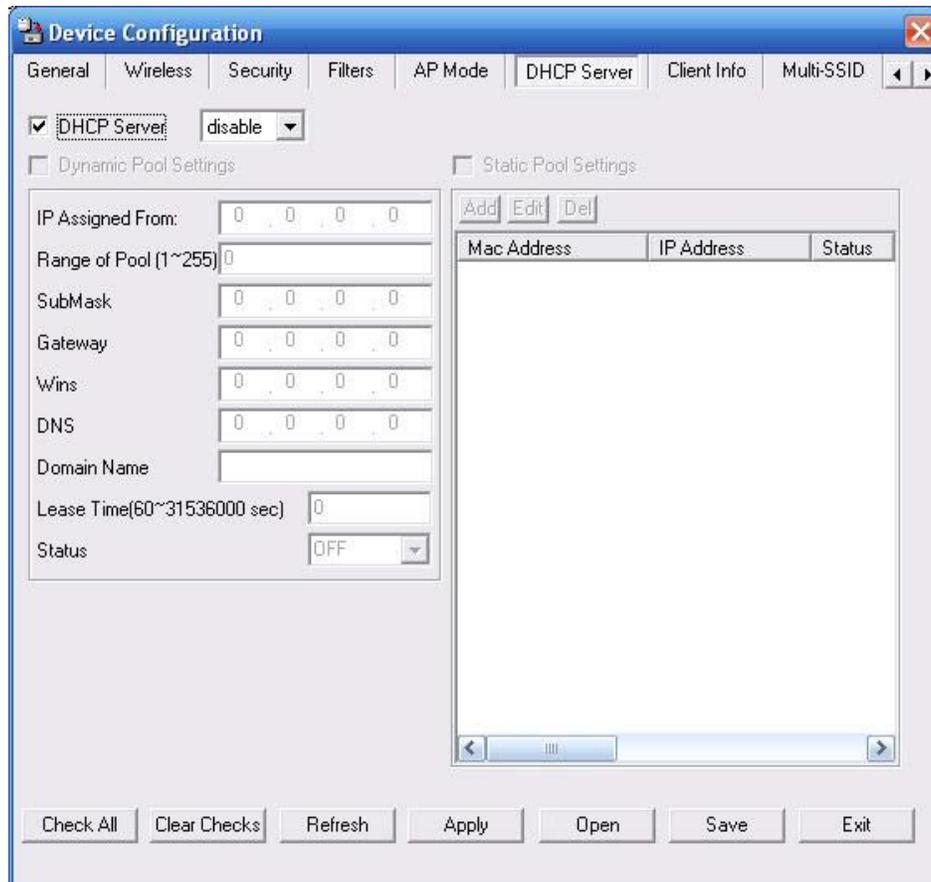
WDS with AP: Wireless Distribution System with Access Points. APs in a network are wirelessly wired together and connected via a Distribution System. The **DWL-8200AP** wirelessly connects multiple networks, while still functioning as a wireless AP.

Device Configuration > AP Mode > WDS



WDS: A Wireless Distribution System that interconnects so called Basic Service Sets (BSS). It bridges two or more wired networks together over wireless. The **DWL-8200AP** wirelessly connects multiple networks without functioning as a wireless AP.

Device Configuration > DHCP Server



DHCP Server: Enable or disable the DHCP server function.

Dynamic Pool Settings: Click to enable Dynamic Pool Settings. Configure the IP address pool in the fields below.

Static Pool Settings: Click to enable Static Pool Settings. Use this function to assign the same IP address to a device at every restart. The IP addresses assigned in the Static Pool list must NOT be in the same IP range as the Dynamic Pool.

IP Assigned From: Enter the initial IP address to be assigned by the DHCP server.

Range of Pool (1~255): Enter the number of allocated IP addresses.

SubMask: Enter the subnet mask.

Gateway: Enter the gateway IP address, typically a router.



Device Configuration > DHCP Server (*continued*)

Wins: Wins (Windows Internet Naming Service) is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

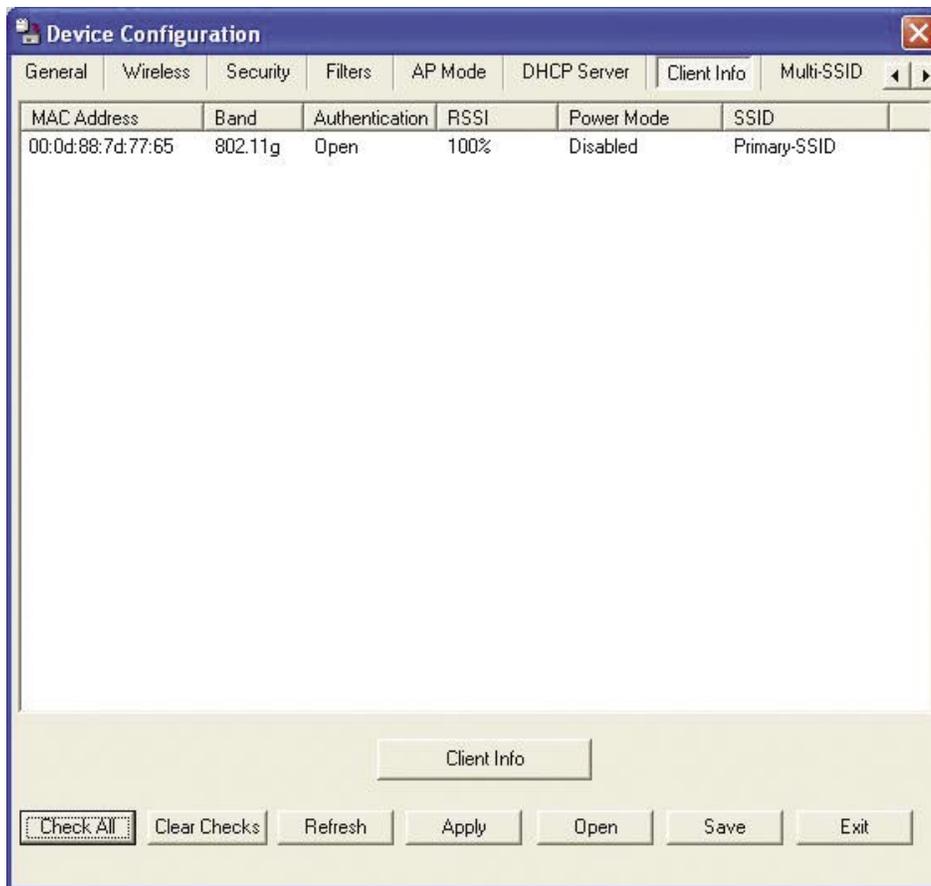
DNS: The IP address of the DNS server, if applicable.

Domain Name: Enter the domain name of the **DWL-8200AP**, if applicable.

Lease Time: The period of time that the client will retain the assigned IP address.

Status: This option turns the dynamic pool settings on or off.

Device Configuration > Client Info



MAC Address: Displays the MAC address of the client.

Band: Displays the wireless band.

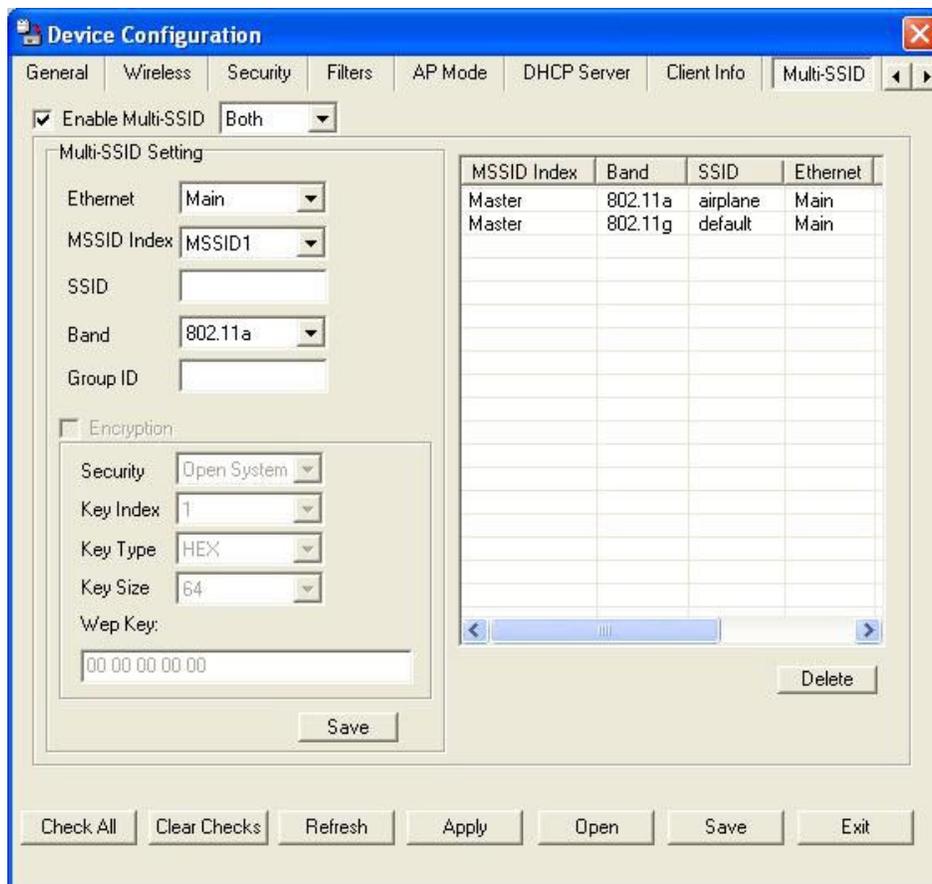
Authentication: Displays the type of authentication that is enabled.

RSSI: Indicates the strength of the signal

Power Mode: Displays the status of the power saving feature.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **default**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Device Configuration > Multi-SSID



Enable Multi-SSID: When Multi-SSID is enabled, you can configure your SSIDs for either **both**, **11a** only, or **11g** only networks.

Ethernet: Select “**Main**” if you wish to configure the network on LAN 1 (PoE). Select “**Guest**” to set up the network on LAN 2.

MSSID Index: You can select up to 7 MSSIDs per band, the default MSSID is the primary, which puts the total to 8 MSSIDs per band.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID’s factory default setting is **default**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Band: Select the wireless band (**IEEE802.11a** or **IEEE802.11g**).

Device Configuration > Multi-SSID (*continued*)

Group ID: You can assign a value to group all of the SSIDs to each other. The Group ID is 0 by default, which is also considered Primary SSID. Use Group ID 0-15 for **“Main”**, or use Group ID 16-30 for **“Guest”**.

Encryption: **Enable** or **Disable** encryption on the selected device(s).

Security: Select either **None**, **Open System**, or **Shared Key**.

Key Index: Select which defined key is active on the selected device(s).

Key Type: Select **HEX** or **ASCII**.

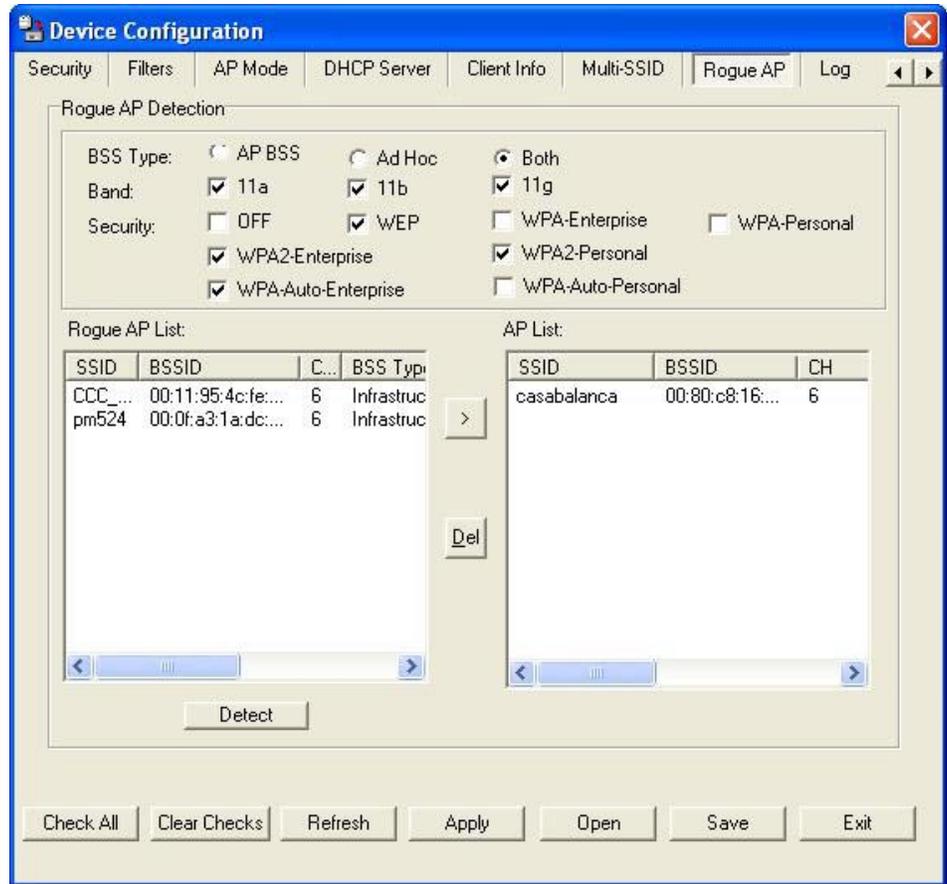
Key Size: Select **64-bit**, **128-bit**, or **152-bit**.

WEP key: Enter a string to use as the key.

Note: If the Master sets security to key 1, then key 1 can not be used. This leaves three Multi-SSIDs that can use security per band. The final result will mean that for each band, four Multi-SSIDs will be without security.

*Note: If Main Master SSID supports **WPA** or **WPA2**, then the guest is not allowed to set security.*

Device Configuration > Rogue AP



BSS Type: The Basic Service Set Type allows you to select from **AP BSS**, **Ad Hoc**, or **Both**.

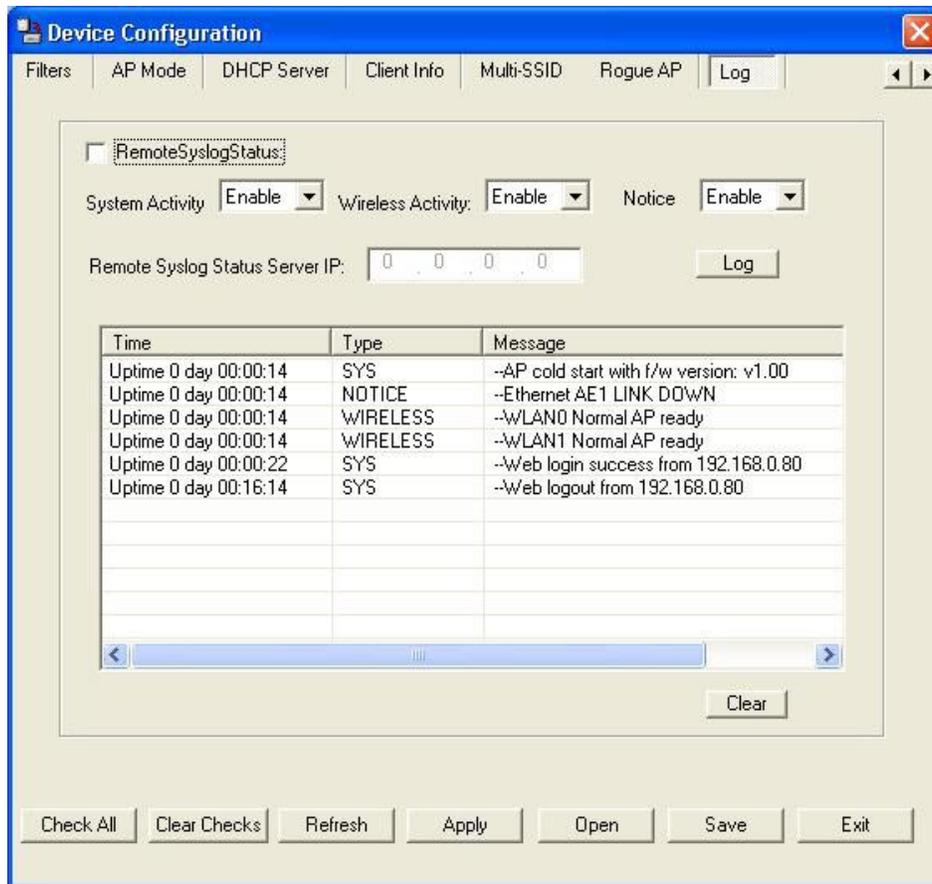
Band: Select the type of network (bands **11a**, **11b**, and **11g**) that you would like the AP detection to search on.

Security: Select the Security type **Off**, **WEP**, **WPA-Enterprise**, and **WPA-Personal** that you would like to be consider during AP detection.

Rogue AP List: This window shows all of the neighbor APs detected, which is based on your criteria from above (BSS Type, Band, and Security). If the AP is in the same network, or if you know the AP, just click on “**Add**” to save it to the AP list.

AP List: This window shows all of the APs that are allowed access on the network.

Device Configuration > Log



RemoteSyslogStatus: Check this option to enable the log and the Remote Syslog Status Server IP.

System Activity: Select **Enable** to allow the logging of system actions, such as logging a firmware upgrade.

Wireless Activity: Select **Enable** to allow the logging of any wireless clients that connect to the AP.

Notice: Select **Enable** to allow all other information to be logged.

Remote Syslog Status Server IP: If you require more space to hold your logs, please provide the IP address of the Server that will store your logs. The embedded memory can only have up to 500 logs.

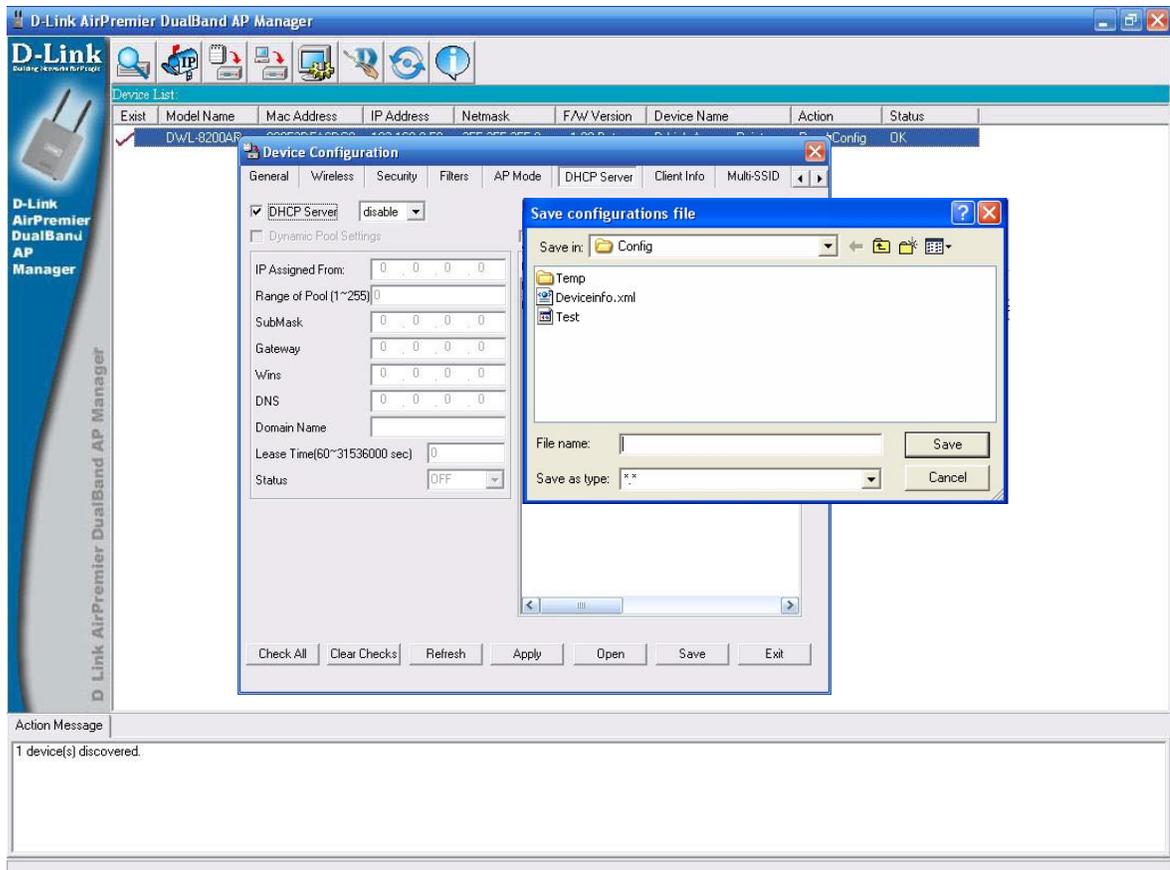
Configuration Files

The **DWL-8200AP** allows you to save the device settings to a configuration file. To save a configuration file follow these steps:

- Select a device from the Device List on the main screen of the AP Manager.
- Click the device configuration button.
- Click the Save button after you have all the settings as you want them.
- A popup window will appear prompting you for a file name and location. Enter the file name, choose a file destination, and click Save.



Device Configuration button.

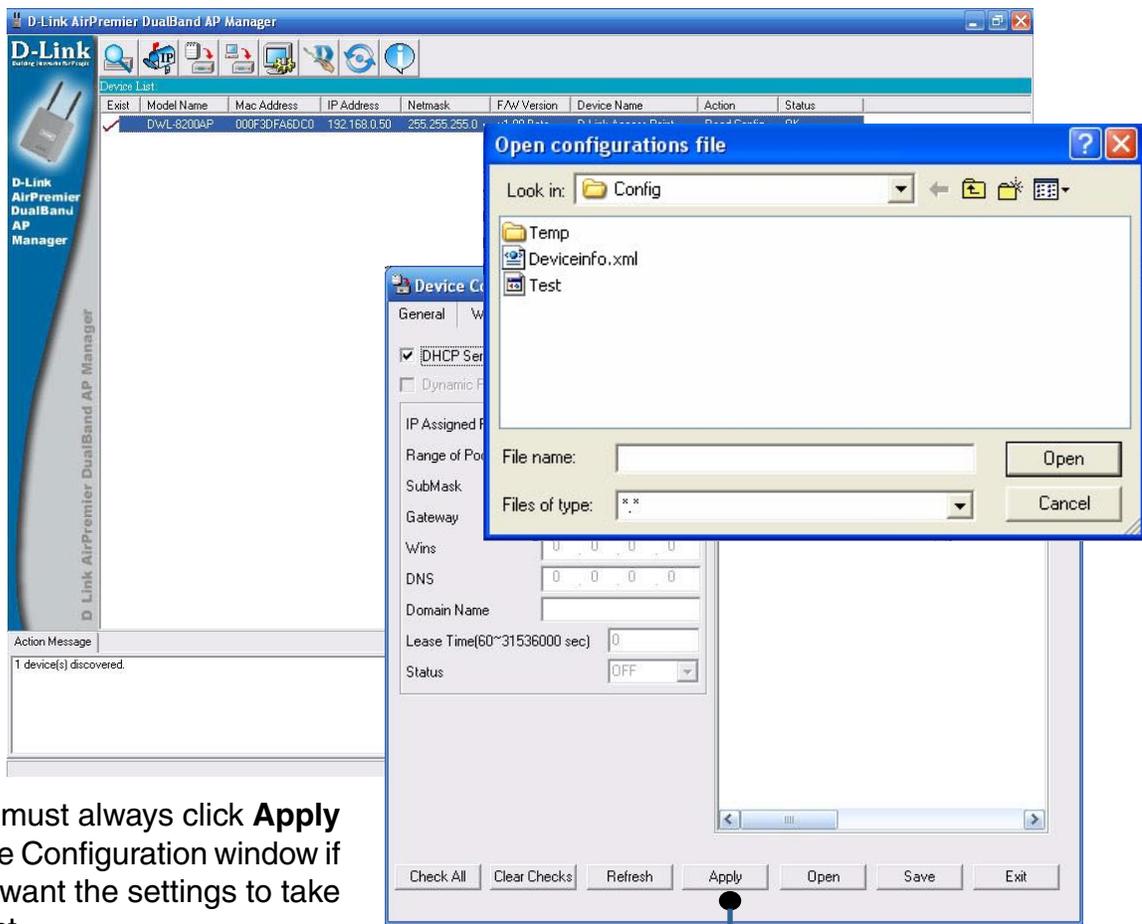


To load a previously saved configuration file, follow these steps:

- Select a device from the Device List on the main screen of the AP Manager.
- Click the device configuration button.
- Click the **Open** button.
- A popup window will appear prompting you to locate the configuration file. Locate the file and click **Open**.
- The configuration file is loaded into the AP Manager but has not actually been written to the device(s). If you want to use the newly loaded configuration for the selected device(s), click **Apply** and the configuration settings will be written to the device(s).



↓
Device Configuration button.



You must always click **Apply** in the Configuration window if you want the settings to take effect.

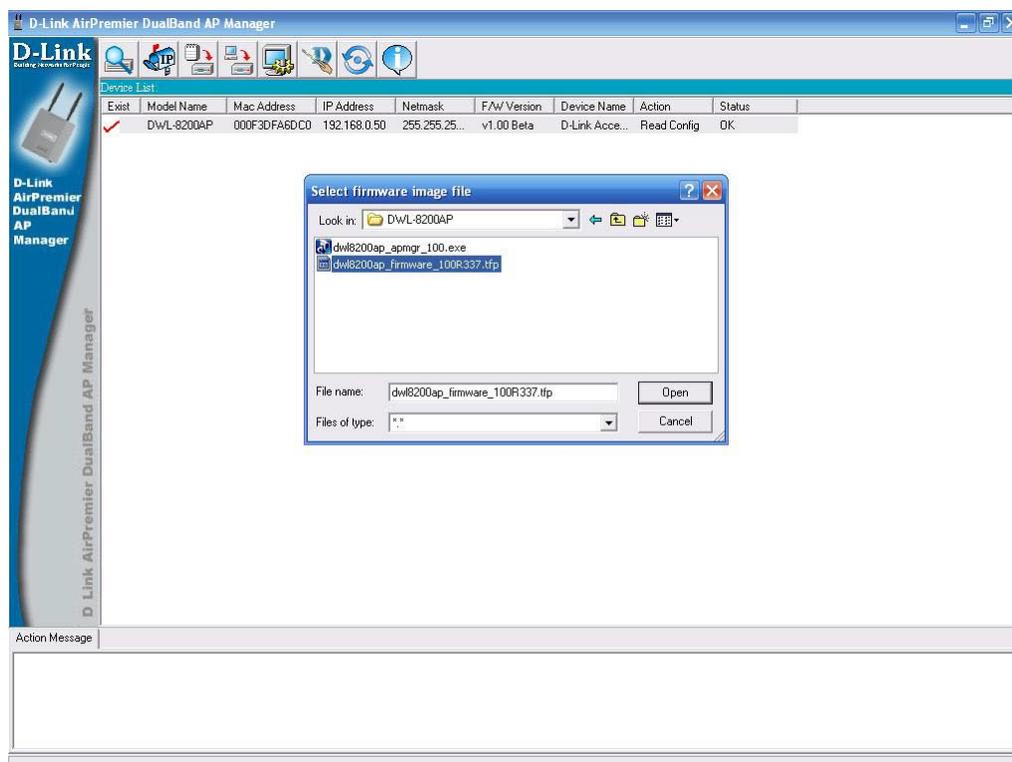
Firmware



You can upgrade the firmware by clicking on this button after selecting the device(s).

To upgrade the firmware:

- Download the latest firmware upgrade from <http://support.dlink.com> to an easy to find location on your hard drive.
- Click on the firmware button as shown above.
- A popup window will appear. Locate the firmware upgrade file and click **Open**.

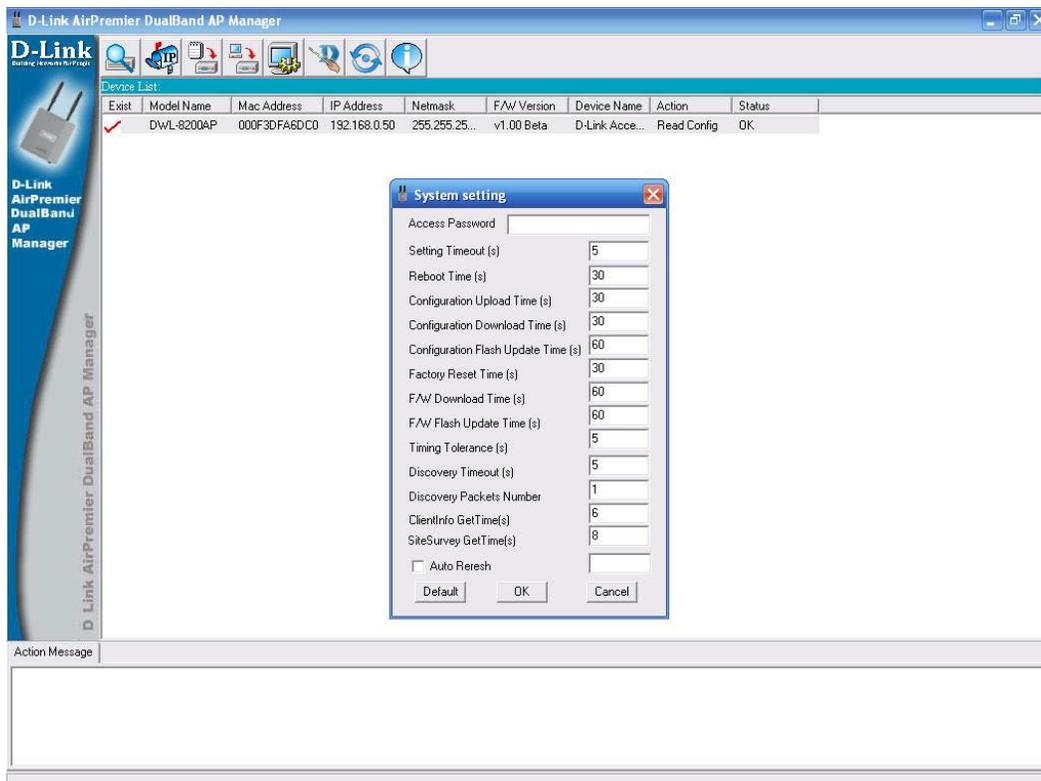


IMPORTANT! DO NOT DISCONNECT POWER FROM THE UNIT WHILE THE FIRMWARE IS BEING UPGRADED.

System Settings



You can customize the basic System Settings for the **DWL-8200AP** by clicking on this button.



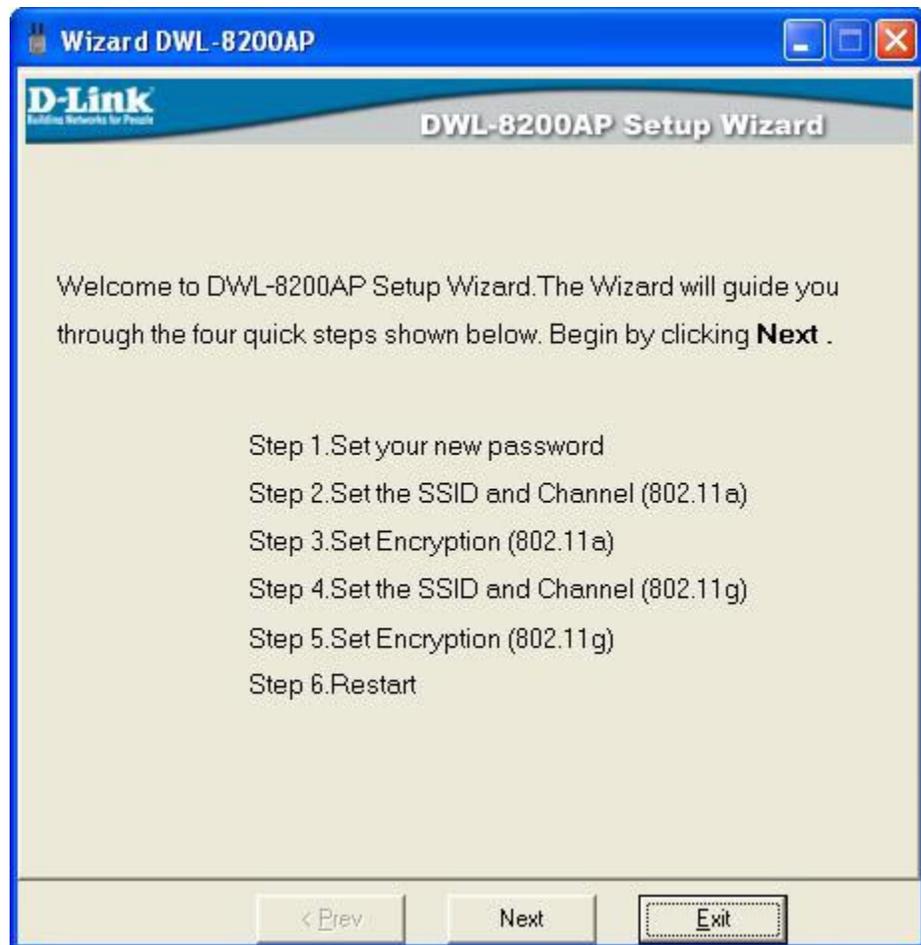
- **Access Password:** This sets the admin password for the selected device(s).
- **Auto Refresh:** This setting allows you to enable auto refreshing of the network device list. By default this option is disabled. If you choose to enable it, you must enter the refresh interval in seconds.

All other settings on this screen should be left at the default setting.

Setup Wizard



This button will launch the Setup Wizard that will guide you through device configuration.



Click **Next**.

Setup Wizard (continued)



Enter a **Password** and retype it in the **Verify Password** field.



Click **Next**.

Setup Wizard (continued)



Enter the **SSID** and the **Channel** for the IEEE 802.11a network.



Click **Next**.

Select **No Security**, if you do not require a method of encryption.



Click **Next**.

Setup Wizard (continued)



Select **WEP**, as your method of encryption. A **Key Size** and **First Key** value are required.



Click **Next**.

Select **WPA-Personal**, as your method of encryption. A **Pass Phrase**, and **Group Key Update Interval** are required.



Click **Next**.

Setup Wizard (continued)



Enter the **SSID** and the **Channel** for the IEEE 802.11g network.



Click **Next**.

Select **No Security**, if you do not require a method of encryption.



Click **Next**.

Setup Wizard (continued)



Select **WEP**, as your method of encryption. A **Key Size** and **First Key** value are required.



Click **Next**.

Select **WPA-Personal**, as your method of encryption. A **Pass Phrase**, and **Group Key Update Interval** are required.



Click **Next**.

Setup Wizard (continued)



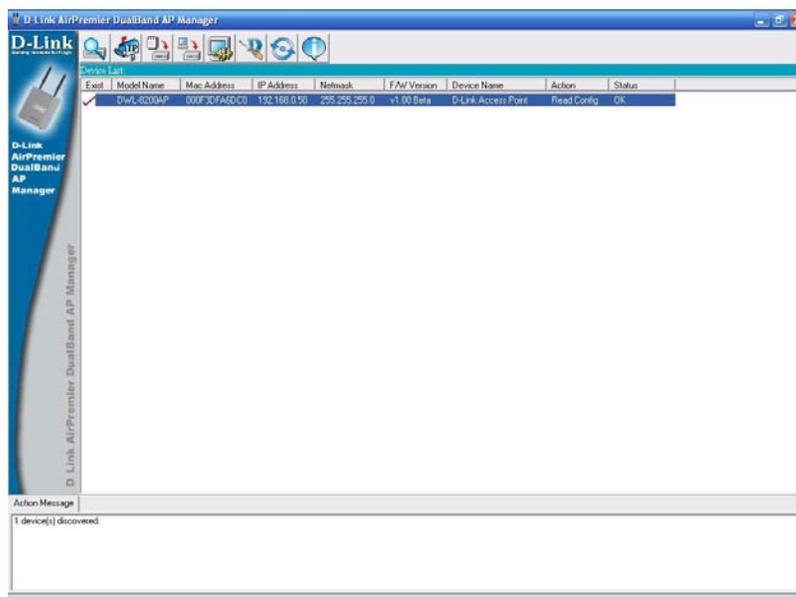
The **DWL-8200AP** setup is complete!

Refresh



Click on this button to **refresh the list of devices** available on the network.

Devices with a checkmark next to them are still available on the network. Devices with an X are no longer available on the network.



About



Click on this button to view the version of AP Manager.



Networking Basics

Using the Network Setup Wizard in Windows XP

In this section you will learn how to establish a network at home or work, using **Microsoft Windows XP**.

Note: Please refer to websites such as <http://www.homenethelp.com> and <http://www.microsoft.com/windows2000> for information about networking computers using Windows 2000.

Go to **Start>Control Panel>Network Connections**
Select **Set up a home or small office network**



When this screen appears, click **Next**.

Please follow all the instructions in this window:



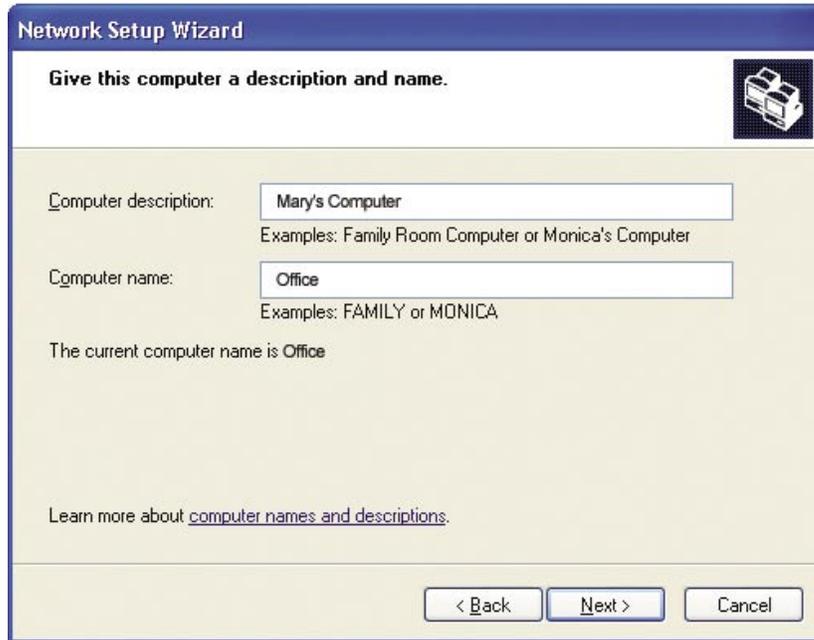
Click **Next**.

In the following window, select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.



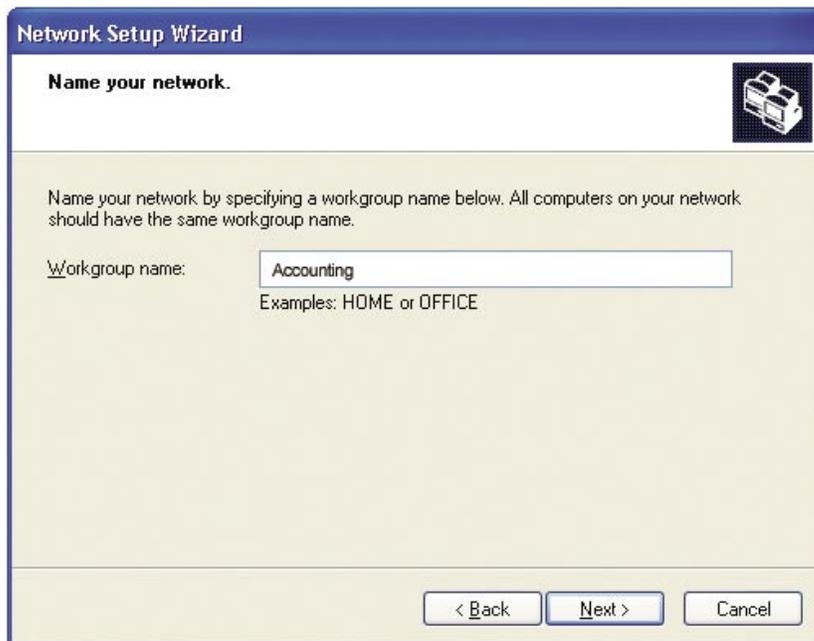
Click **Next**.

Enter a **Computer description** and a **Computer name** (optional).



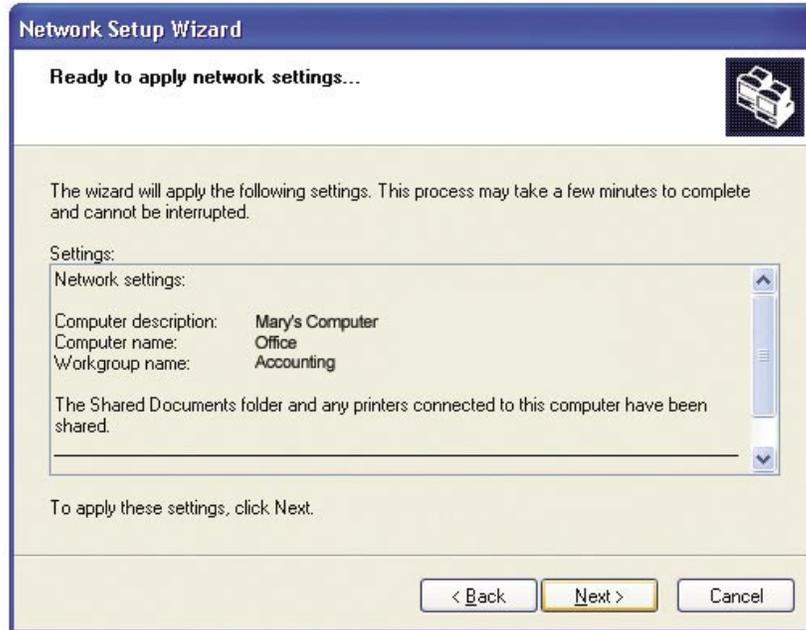
Click **Next**.

Enter a **Workgroup** name. All computers on your network should have the same **Workgroup name**.



Click **Next**.

Please wait while the **Network Setup Wizard** applies the changes.



When the changes are complete, click **Next**.

Please wait while the **Network Setup Wizard** configures the computer. This may take a few minutes.



In the window below, select the option that fits your needs. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click **Next**.



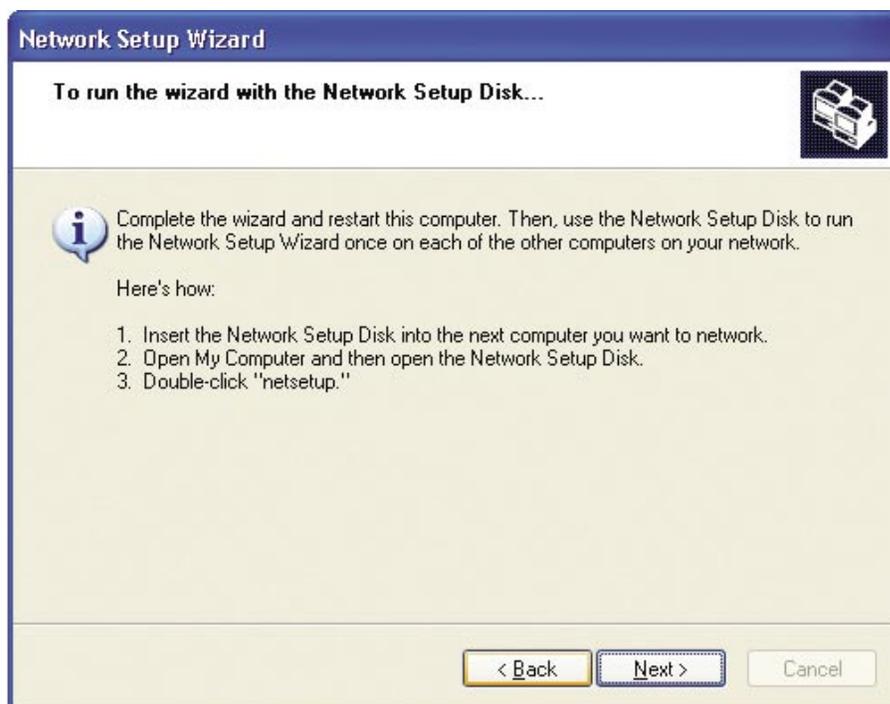
Insert a disk into the Floppy Disk Drive, in this case drive **A**.



Click **Next**.



Please read the information under **Here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. To continue click **Next**.



Please read the information on this screen, then click **Finish** to complete the **Network Setup Wizard**.



The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.



You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new wireless network will be ready to use.

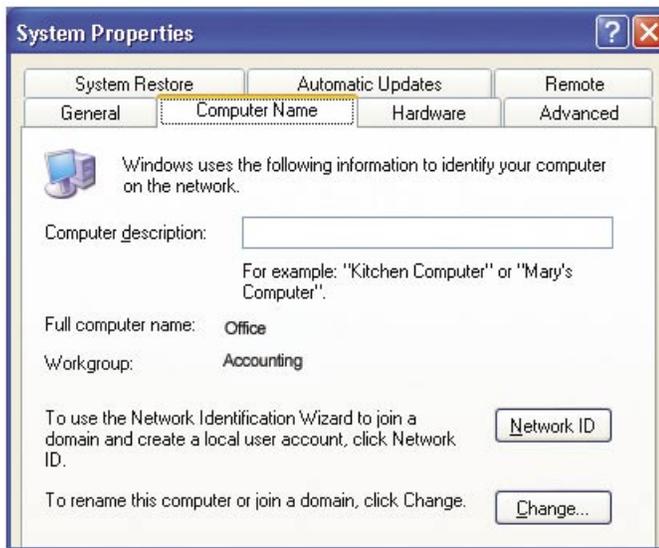
Naming Your Computer

To name your computer in **Windows XP**, please follow these directions.

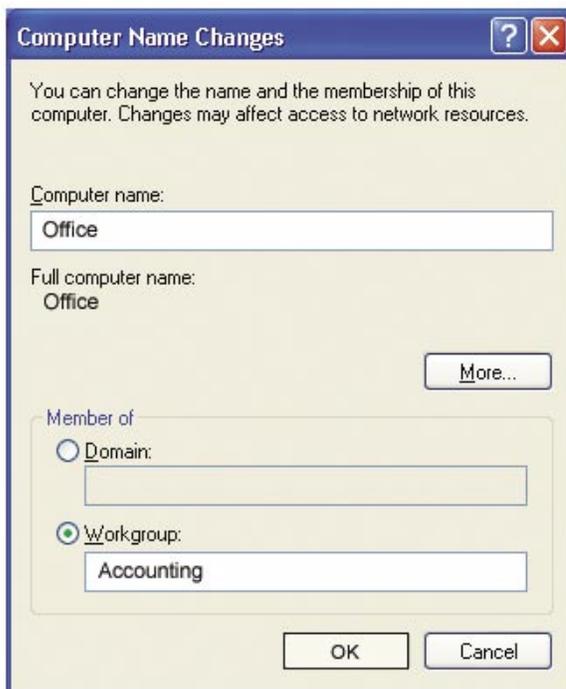
- Click **Start** (in the lower left corner of the screen).
- **Right-click** on **My Computer**.
- Select **Properties** and click.



- Select the **Computer Name Tab** in the System Properties window.
- You may enter a **Computer Description** if you wish; this field is optional.
- To rename the computer and join a domain, Click **Change**.



- In this window, enter the **Computer name**.
- Select **Workgroup** and enter the name of the **Workgroup**.
- All computers on your network must have the same **Workgroup** name.
- Click **OK**.



Checking the IP Address in Windows XP

The wireless adapter-equipped computers in your network must be in the same IP Address range (see Getting Started in this manual for a definition of IP Address Range.) To check on the IP Address of the adapter, please do the following:

- Right-click on the **Local Area Connection icon** in the task bar.
- Click on **Status**.



This window will appear:

- Click the **Support** tab.
- Click **Close**.



Assigning a Static IP Address in Windows XP/2000

Note: DHCP-enabled routers will automatically assign IP addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable router you will not need to assign static IP addresses.

If you are not using a DHCP capable router, or you need to assign a static IP address, please follow these instructions:

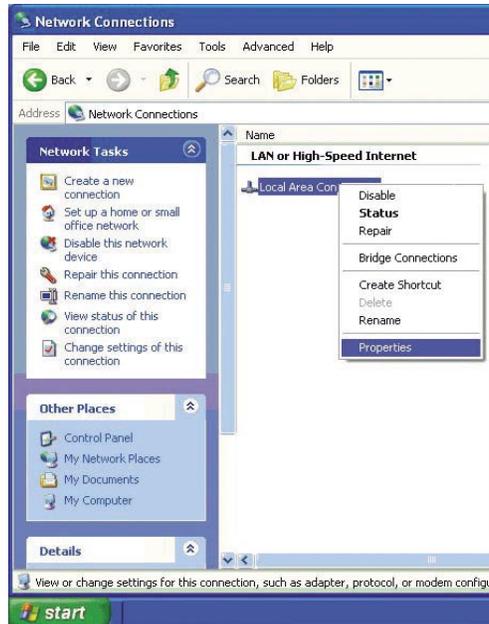
- Go to **Start**.
- Double-click on **Control Panel**.



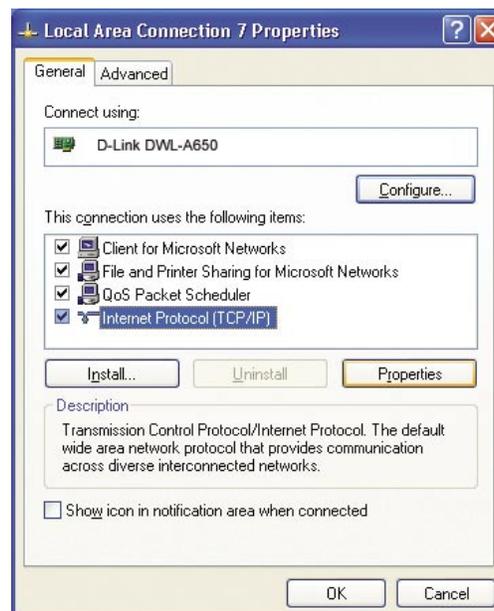
- Double-click on **Network Connections**.



- Right-click on **Local Area Connections**.
- Double-click on **Properties**.



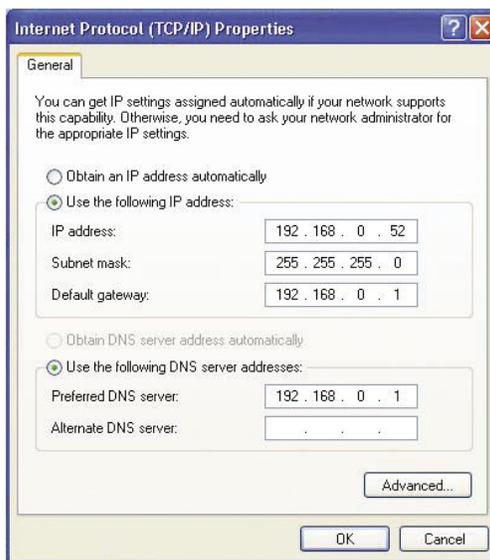
- Click on **Internet Protocol (TCP/IP)**.
- Click **Properties**.
- Input your **IP address and subnet mask**. (The IP addresses on your network must be within the same range. For example, if one computer has an IP address of 192.168.0.2, the other computers should have IP addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)



- Input your **DNS server addresses**. (Note: If you are entering a DNS server, you must enter the IP address of the default gateway.)

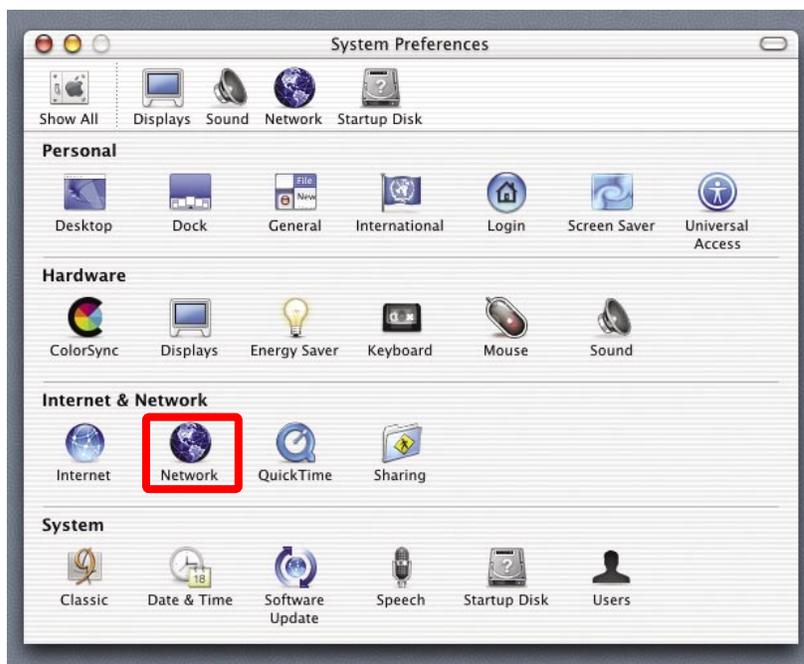
The DNS server information will be supplied by your ISP (Internet Service Provider.)

- Click **OK**.

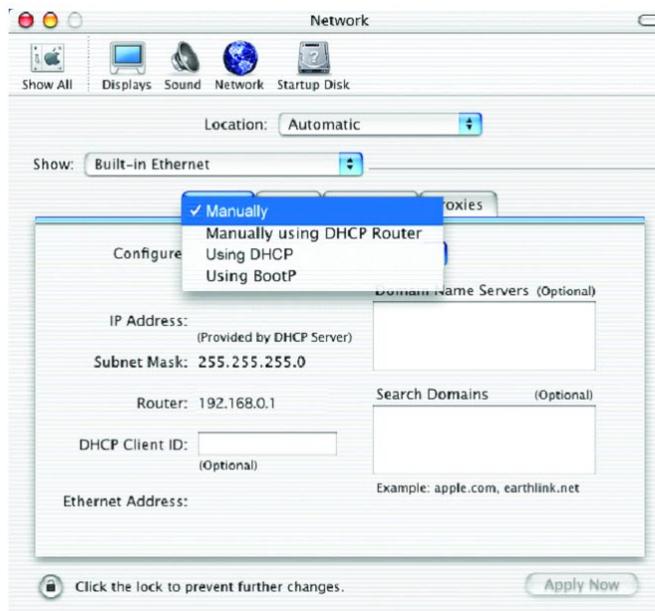


Assigning a Static IP Address in Macintosh OSX

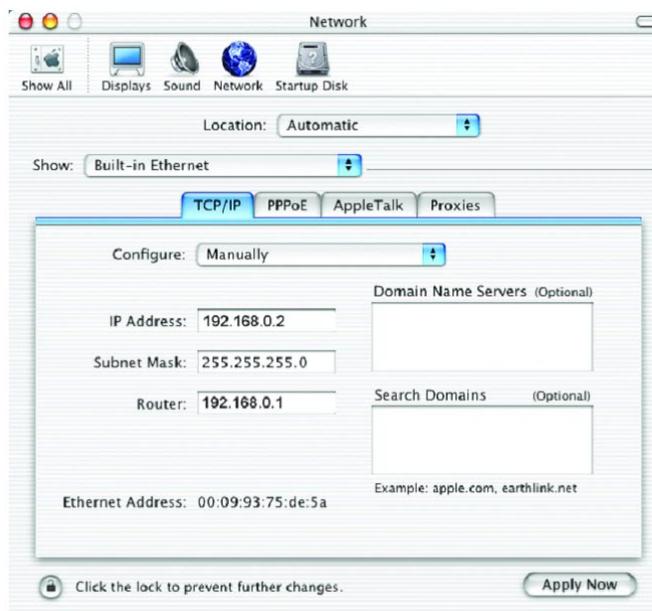
- Go to the **Apple Menu** and select **System Preferences**.
- Click on **Network**.



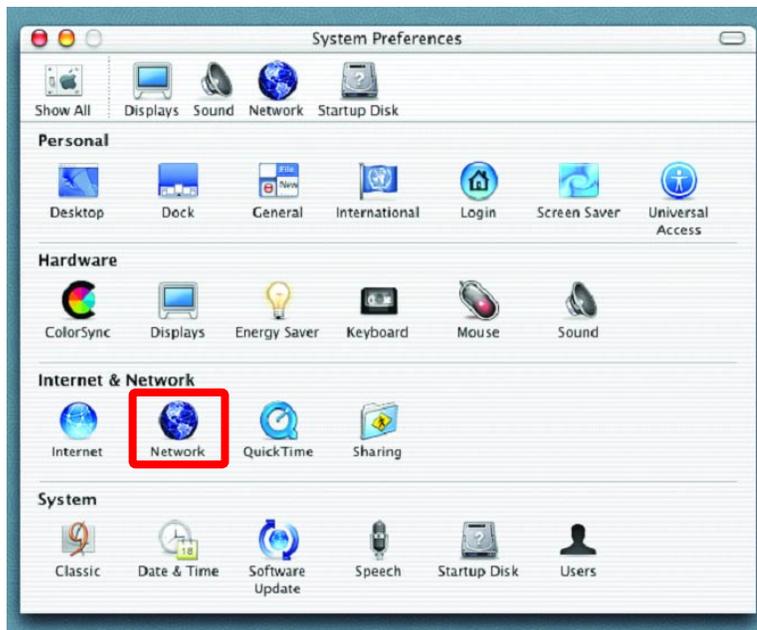
- Select **Built-in Ethernet** in the **Show** pull-down menu.
- Select **Manually** in the **Configure** pull-down menu.



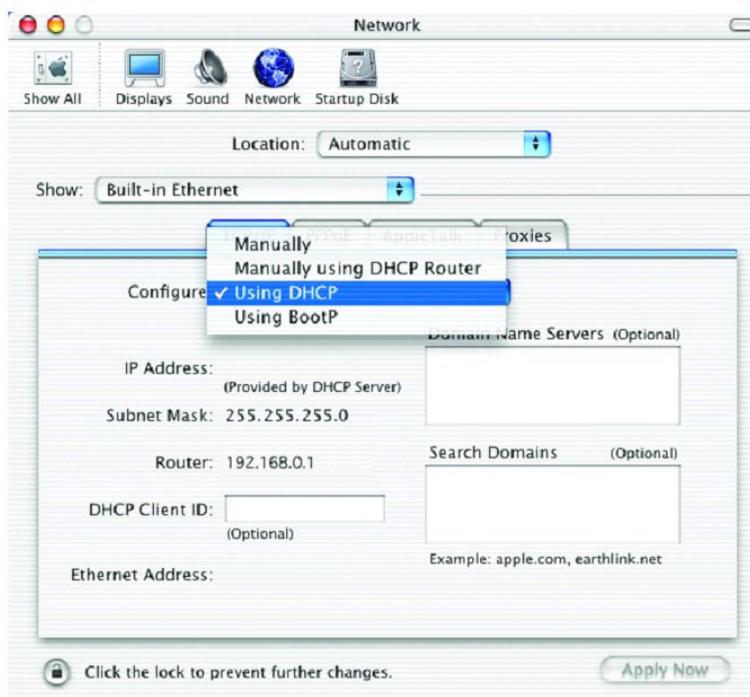
- Input the **Static IP Address**, the **Subnet Mask** and the **Router IP Address** in the appropriate fields.
- Click **Apply Now**.



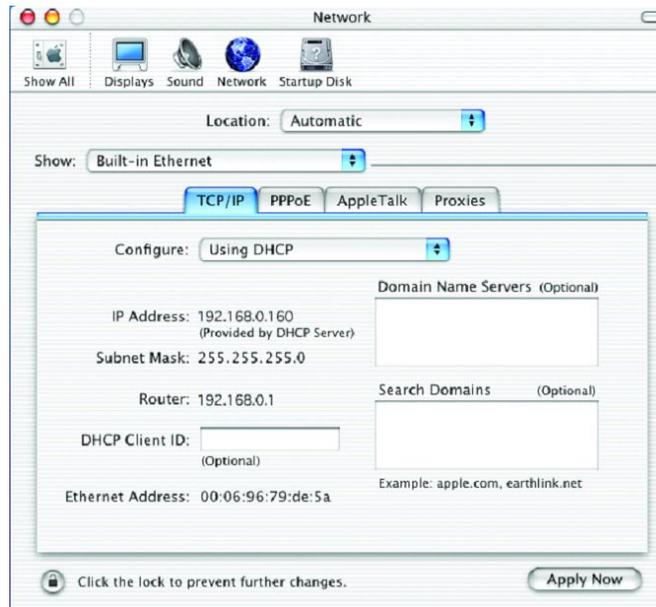
- Go to the **Apple Menu** and select **System Preferences**.
- Click on **Network**.



- Select **Built-in Ethernet** in the **Show** pull-down menu.
- Select **Using DHCP** in the **Configure** pull-down menu.



- Click **Apply Now**.
- The **IP Address**, **Subnet mask**, and the **Router's IP Address** will appear in a few seconds.



Checking the Wireless Connection by Pinging in Windows XP & 2000

Go to **Start > Run > type cmd**. A window similar to this one will appear. Type **ping xxx.xxx.xxx.xxx**, where **xxx** is the **IP address** of the wireless router or access point. A good wireless connection will show four replies from the wireless router or access point, as shown.

```

F:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lab4>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Reply from 192.168.0.50: bytes=32 time=5ms TTL=30
Reply from 192.168.0.50: bytes=32 time=64ms TTL=30
Reply from 192.168.0.50: bytes=32 time=3ms TTL=30
Reply from 192.168.0.50: bytes=32 time=17ms TTL=30

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 64ms, Average = 22ms

F:\Documents and Settings\lab4>_

```

Troubleshooting

This Chapter provides solutions to problems that can occur during the installation and operation of the **DWL-8200AP** Wireless Access Point. We cover various aspects of the network setup, including the network adapters. Please read the following if you are having problems.

Note: It is recommended that you use an Ethernet connection to **configure the DWL-8200AP**.

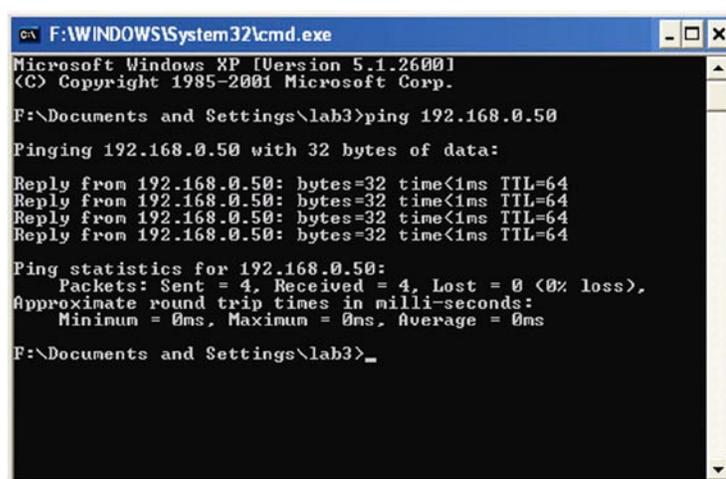
1. The computer used to configure the DWL-8200AP cannot access the Configuration menu.

- Check that the **Ethernet LED** on the **DWL-8200AP** is **ON**. If the **LED** is not **ON**, check that the cable for the Ethernet connection is securely inserted.
- Check that the Ethernet Adapter is working properly. Please see item 3 (**Check that the drivers for the network adapters are installed properly**) in this **Troubleshooting** section to check that the drivers are loaded properly.
- Check that the **IP address** is in the same range and subnet as the **DWL-8200AP**. Please see **Checking the IP Address in Windows XP** in the **Networking Basics** section of this manual.

Note: The IP address of the **DWL-8200AP** is 192.168.0.50. All the computers on the network must have a unique IP address in the same range, e.g., 192.168.0.x. Any computers that have identical IP addresses will not be visible on the network. They must all have the same subnet mask, e.g., 255.255.255.0.

- Do a **Ping test** to make sure that the **DWL-8200AP** is responding. Go to **Start>Run>Type Command>Type ping 192.168.0.50**. A successful ping will show four replies.

Note: If you have changed the default IP address, make sure to ping the correct IP address assigned to the **DWL-8200AP**.



```
GA F:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lab3>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Reply from 192.168.0.50: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

F:\Documents and Settings\lab3>_
```

2. The wireless client cannot access the Internet in the Infrastructure mode.

Make sure the wireless client is associated and joined with the correct access point. To check this connection: **Right-click** on the **Local Area Connection icon** in the taskbar and select **View Available Wireless Networks**. The **Connect to Wireless Network** screen will appear. Please make sure you have selected the correct available network, as shown in the illustrations below.



- Check that the **IP address** assigned to the wireless adapter is within the same **IP address range** as the access point and gateway. *Since the **DWL-8200AP** has an IP address of 192.168.0.50, wireless adapters must have an IP address in the same range, e.g., 192.168.0.x. Each device must have a unique IP address; no two devices may have the same IP address. The subnet mask must be the same for all the computers on the network.)* To check the **IP address** assigned to the wireless adapter: **double-click** on the **Local Area Connection icon** in the taskbar > select the **Support tab** and the **IP address** will be displayed. *Please refer to **Checking the IP Address in the Networking Basics** section of this manual.)*
- If it is necessary to assign a **Static IP Address** to the wireless adapter, please refer to the appropriate section in **Networking Basics**. If you are entering a **DNS Server address** you must also enter the **Default Gateway Address**. *(Remember that if you have a DHCP-capable router, you will not need to assign a static IP address. See **Networking Basics: Assigning a Static IP Address**.)*

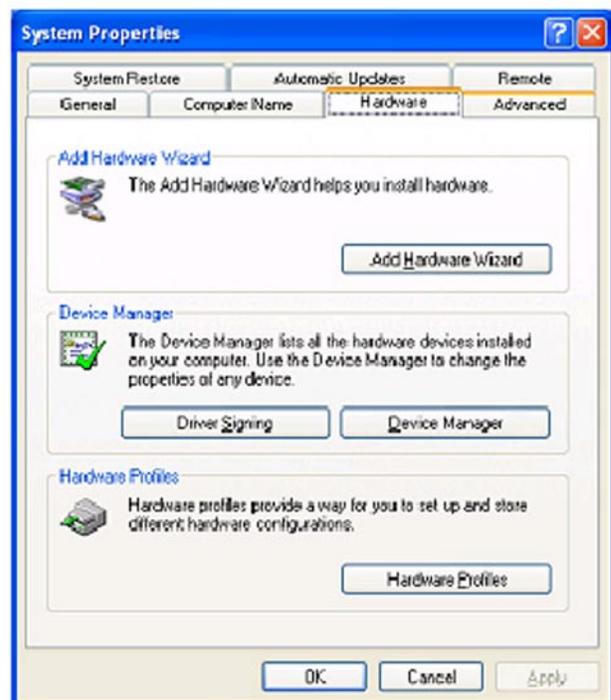
3. Check that the drivers for the network adapters are installed properly.

You may be using different network adapters than those illustrated here, but this procedure will remain the same, regardless of the type of network adapters you are using.

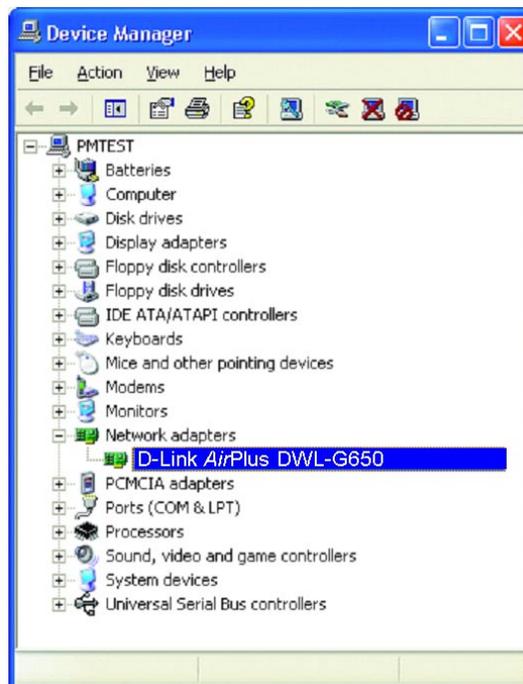
- Go to **Start > My Computer > Properties.**



- **Select the Hardware Tab.**
- **Click Device Manager.**



- Double-click on **Network Adapters**.
- Right-click on **D-Link AirPlus DWL-G650 Wireless Cardbus Adapter**. (In this example we use the DWL-G650; you may be using other network adapters, but the procedure will remain the same.)
- Select **Properties** to check that the drivers are installed properly.



- Look under **Device Status** to check that the device is working properly.
- Click **OK**.



4. What variables may cause my wireless products to lose reception?

D-Link products let you access your network from virtually anywhere you want. However, the positioning of the products within your environment will affect the wireless range. Please refer to **Installation Considerations** in the **Wireless Basics** section of this manual for further information about the most advantageous placement of your D-Link wireless products.

5. Why does my wireless connection keep dropping?

- Antenna Orientation- Try different antenna orientations for the **DWL-8200AP**. Try to keep the antenna at least 6 inches away from the wall or other objects.
- If you are using 2.4GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, and lights, your wireless connection will degrade dramatically or drop altogether. Try changing the channel on your router, access point and wireless adapter to a different channel to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

6. Why can't I get a wireless connection?

If you have enabled encryption on the **DWL-8200AP**, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- Make sure that the SSID on the router and the wireless client are exactly the same. If they are not, wireless connection will not be established.
- Move the **DWL-8200AP** and the wireless client into the same room and then test the wireless connection.
- Disable all security settings.
- Turn off your **DWL-8200AP** and the client. Turn the **DWL-8200AP** back on again, and then turn on the client.
- Make sure that all devices are set to **Infrastructure** mode.
- Check that the LED indicators are indicating normal activity. If not, check that the AC power and Ethernet cables are firmly connected.
- Check that the IP address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, and lights, your wireless connection will degrade dramatically or drop altogether. Try changing the channel on your **DWL-8200AP**, and on all the devices in your network to avoid interference.

- 
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

7. I forgot my encryption key.

- Reset the **DWL-8200AP** to its factory default settings and restore the other devices on your network to their default settings. You may do this by pressing the Reset button on the back of the unit. You will lose the current configuration settings.

Technical Specifications

Standards

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3af
- IEEE 802.3u
- IEEE 802.3x

Device Management

- Web-Based – Internet Explorer v6 or later; Netscape Navigator v7 or later; or other Java-enabled browsers.
- Telnet
- AP Manager
- SNMP v.3

Data Rate

For 802.11a/g:

- 108, 54, 48, 36, 24, 18, 12, 9 and 6Mbps

For 802.11b:

- 11, 5.5, 2, and 1Mbps

Security

- WPA – Enterprise
- WPA – Personal
- WPA2 – Enterprise
- WPA2 – Personal
- 64-bit, 128-bit, and 152-bit WEP
- MAC Address Access Control List

Wireless Frequency Range

- 2.4GHz to 2.4835GHz
- 5.15GHz to 5.35GHz and 5.725GHz to 5.825GHz

Wireless Operating Range*

802.11g (Full Power with 5dBi gain diversity dipole antenna)

Indoors:

- 98ft (30m) @ 54Mbps
- 105ft (32m) @ 48Mbps
- 121ft (37m) @ 36Mbps
- 148ft (45m) @ 24Mbps
- 203ft (62m) @ 18Mbps
- 223ft (68m) @ 12Mbps
- 253ft (77m) @ 9Mbps
- 302ft (92m) @ 6Mbps

Outdoors:

- 328ft (100m) @ 54Mbps
- 968ft (295m) @ 11Mbps
- 1378ft (420m) @ 6Mbps

Operating Voltage

- 48VDC +/- 10% for PoE



Radio and Modulation Type

For 802.11b:

DSSS :

- DBPSK @ 1Mbps
- DQPSK @ 2Mbps
- CCK @ 5.5 and 11Mbps

For 802.11a/g:

OFDM:

- BPSK @ 6 and 9Mbps
- QPSK @ 12 and 18Mbps
- 16QAM @ 24 and 36Mbps
- 64QAM @ 48, 54 and 108Mbps

DSSS:

- DBPSK @ 1Mbps
- DQPSK @ 2Mbps
- CCK @ 5.5 and 11Mbps

Transmit Output Power

For 802.11a:

- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 6mW (7dBm)
- 1mW (0dBm)

For 802.11b:

- 100mW (20dBm)
- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 23mW (13dBm)
- 10mW (10dBm)
- 6mW (7dBm)
- 1mW (0dBm)

For 802.11g:

- 100mW (20dBm)
- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 6mW (7dBm)
- 1mW (0dBm)

Receiver Sensitivity

For 802.11a:

- 6Mbps: -87dBm
- 9Mbps: -86dBm
- 11Mbps: -88dBm
- 12Mbps: -85dBm
- 18Mbps: -83dBm
- 24Mbps: -80dBm
- 36Mbps: -76dBm
- 48Mbps: -71dBm
- 54Mbps: -71dBm

For 802.11b:

- 1Mbps: -92dBm
- 2Mbps: -89dBm
- 5.5Mbps: -88dBm
- 11Mbps: -83dBm

For 802.11g:

- 1Mbps: -95dBm
- 2Mbps: -91dBm
- 5.5Mbps: -89dBm
- 6Mbps: -87dBm
- 9Mbps: -85dBm
- 11Mbps: -88dBm
- 12Mbps: -80dBm
- 18Mbps: -80dBm
- 24Mbps: -77dBm
- 36Mbps: -73dBm
- 48Mbps: -72dBm
- 54Mbps: -72dBm

LEDs

- Power
- Status
- LAN 1
- LAN 2
- 802.11b/g
- 802.11a

Temperature

- Operating: 32 °F to 104°F (0°C to 40°C)
- Storing: -4°F to 149°F (-20°C to 65°C)

Humidity

- Operating: 10%~90% (non-condensing)
- Storing: 5%~95% (non-condensing)

Certifications

- FCC
- Wi-Fi

Dimensions

- L = 10.93 inches (277.7mm)
- W = 6.10 inches (155mm)
- H = 1.77 inches (45mm)

- H = 1.77 inches (45mm)

Warranty

- 1 Year

* Maximum wireless signal rate derived from IEEE Standard 802.11a and 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 actual data throughput rate.

** Environmental conditions may adversely affect wireless signal range.

Contacting Technical Support

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link Technical Support through our website, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 453-5465

Monday to Friday 6:00am - 6:00pm.

D-Link Technical Support over the Internet:

<http://support.dlink.com>

email: support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

(800) 361-5265

Monday to Friday 7:30am to 12:00am EST

D-Link Technical Support over the Internet:

<http://support.dlink.ca>

email: support@dlink.ca

Warranty

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

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

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

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

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

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

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

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

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

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

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

Copyright Statement: No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice. Copyright 2005 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

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

to correct the interference by one or more of the following measures:

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

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

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 caused undesired operation.

IC Statement: The Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation

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.

For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment, and the antenna of this device must be integral.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

Registration



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

06/21/05