DWL-8200AP manual

new cover pending

Table of Contents

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 (802.11g; 802.11a; 802.11b) 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 AG mode when used with other D-Link *Air* **Premier**® 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 adminstrator 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 AG 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**rthogonal **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** (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) 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
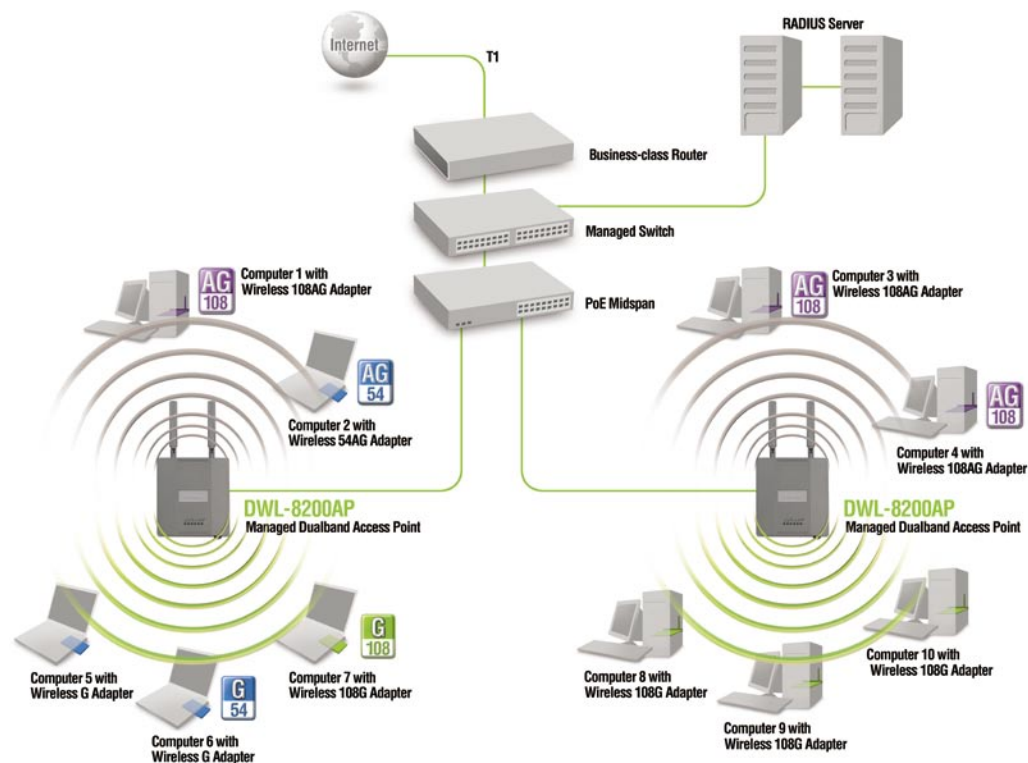
1   You will need broadband Internet access.

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 network adapter.*)

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-AG650.*)

Connecting PoE (Power over Ethernet)
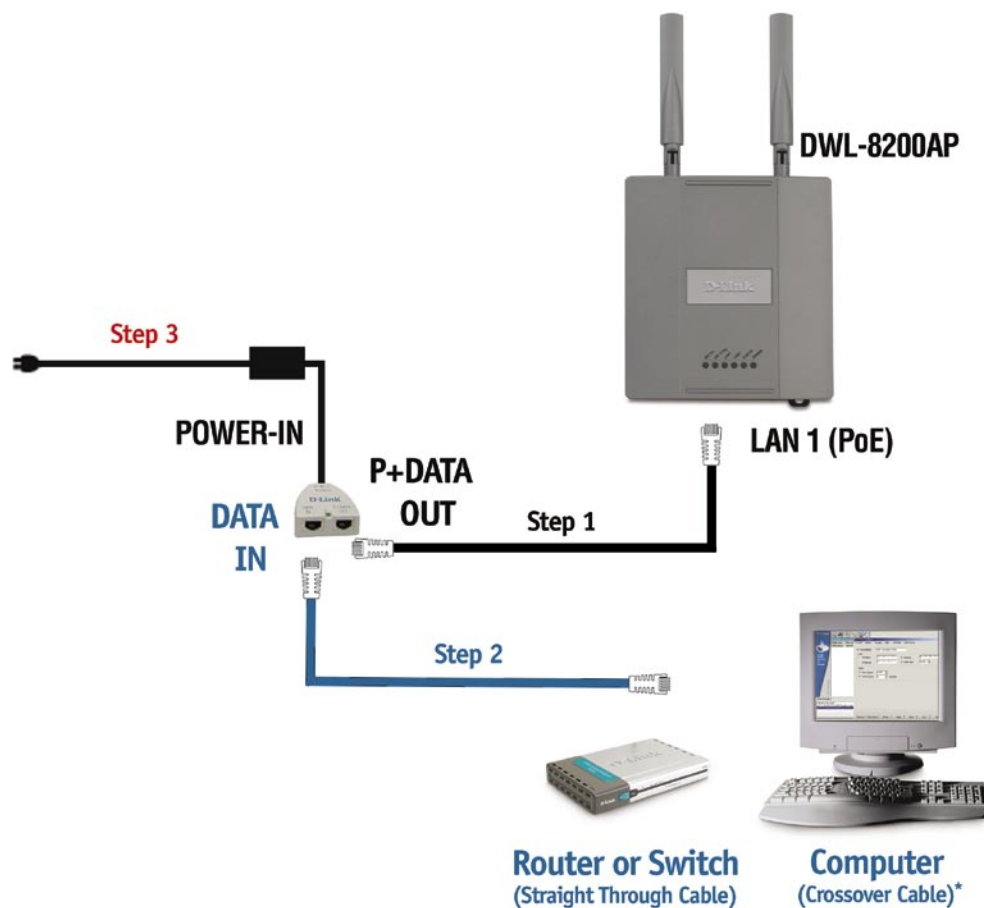
Step 1 Connect one end of an Ethernet cable (included with your package) to the **LAN port** on the **DWL-8200AP** and the other end of the Ethernet cable to the port labeled **P+DATA OUT** on the PoE base unit.

Step 2 Connect another Ethernet cable from the **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 labeled **POWER IN** on the PoE base unit. Attach the power cord to the power adapter and into an electrical outlet.

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

Antennas

Power Cord socket

LAN 2

LAN 1 (PoE)

Reset
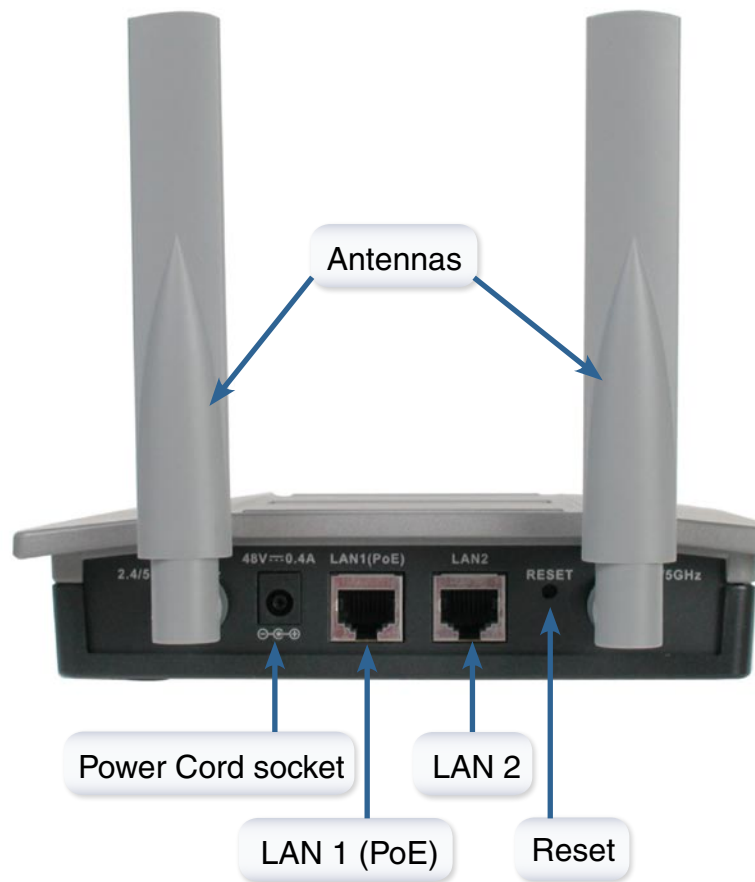
Using the Configuration Menu

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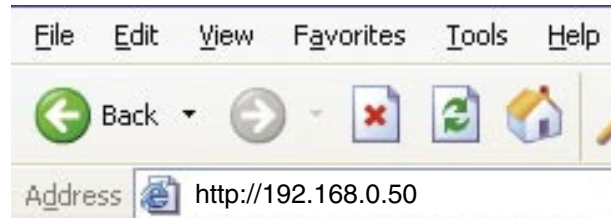
After the connection is established, you will see the user identification window as shown.

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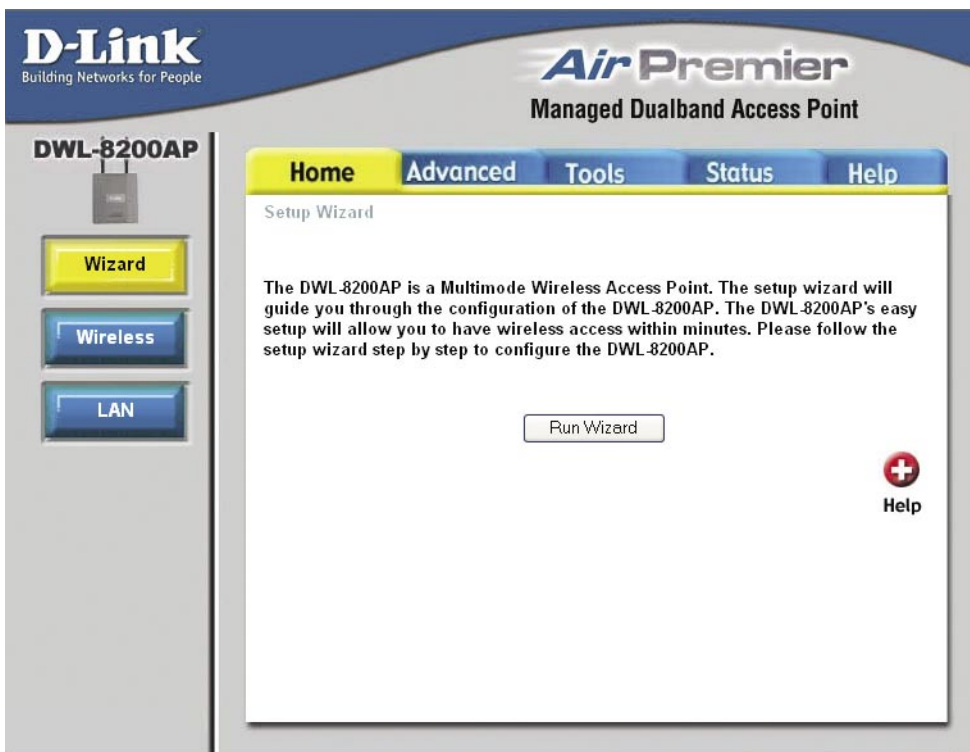
These buttons appear on most of the configuration screens in this section. Please click on the appropriate button at the bottom of each screen after you have made a configuration change.

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

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

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

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

Home > Wireless > Access Point > Authentication
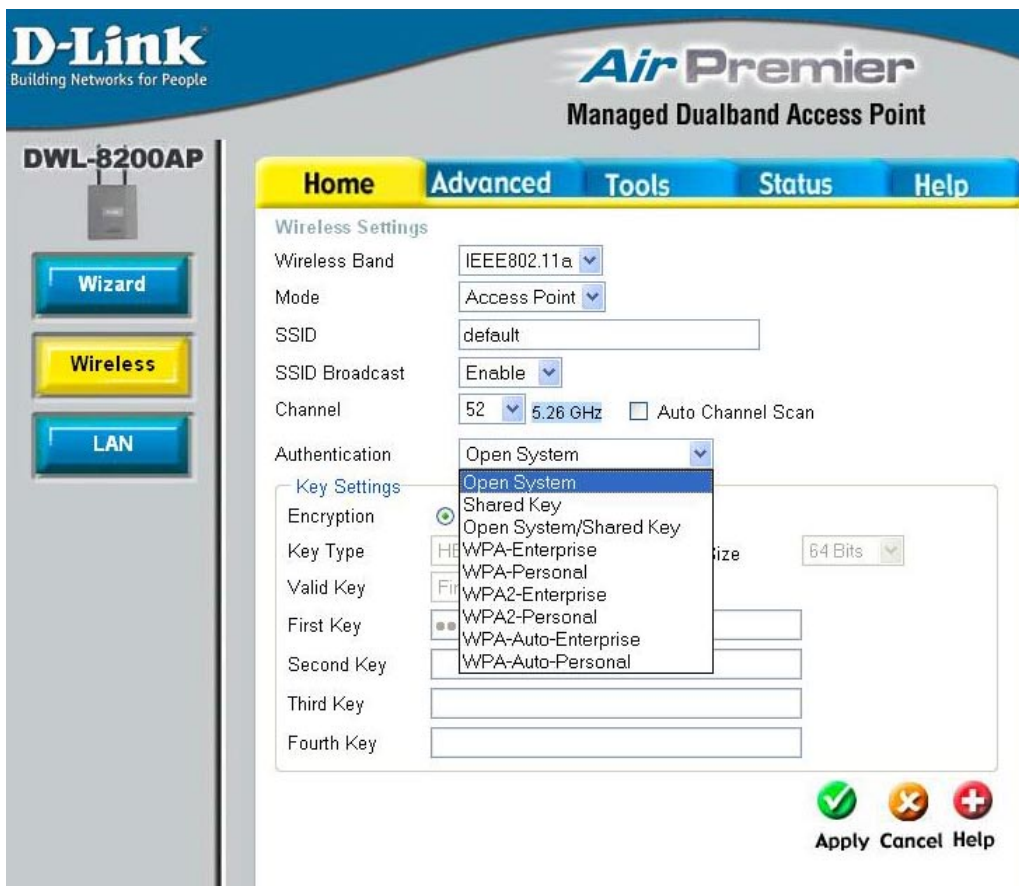
Authentication:	Open System
	Shared Key
	Open System/Shared Key
	WPA-Enterprise
	WPA-Personal
	WPA2-Enterprise
	WPA2-Personal
	WPA-Auto-Enterprise
	WPA-Auto-Personal

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.

Home > Wireless > Access Point > Authentication *(continued)*

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
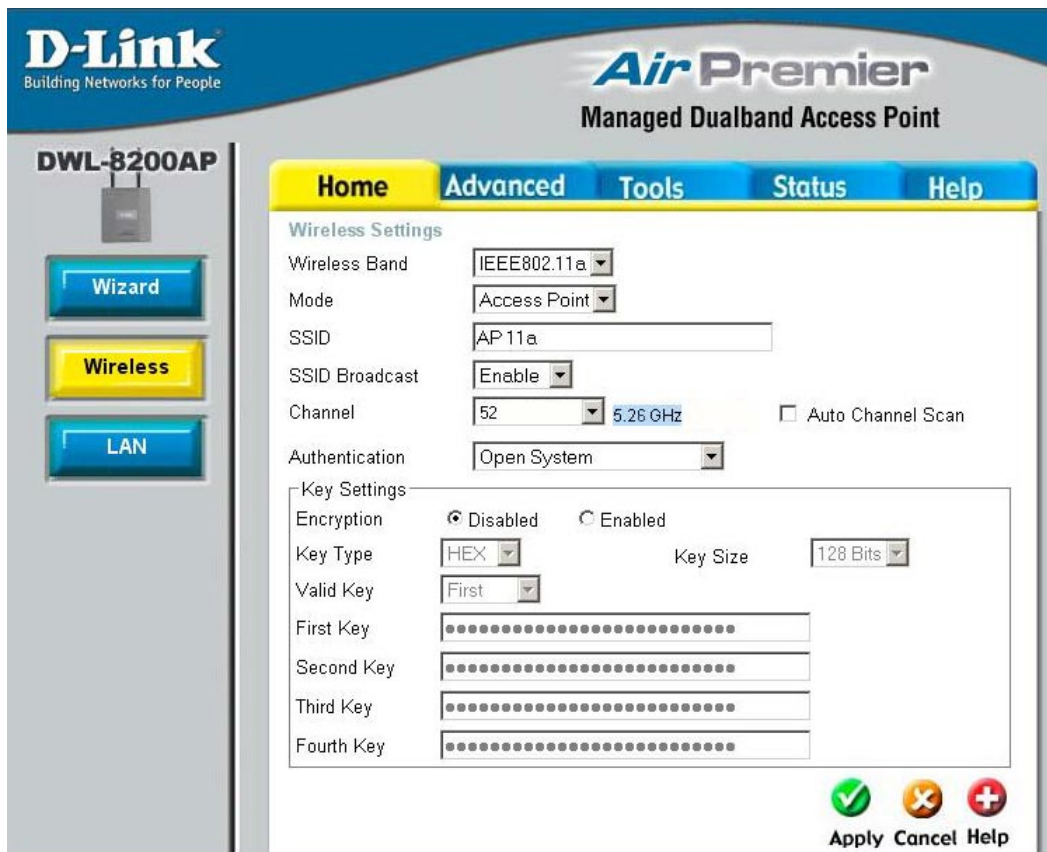
Wireless Band:	Select either IEEE 802.11a or IEEE 802.11g
Mode:	**Access Point** is selected from the pull-down menu.
SSID:	Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **default**. The SSID can be easily 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 > Open System and/or Shared Key *(continued)*

Auto Channel Scan:	Select **Enable** or **Disable**. (Enable this feature to auto-select the channel for best wireless performance.)
Authentication:	See **Home > Wireless > Access Point > Authentication** on pages 16-17.
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
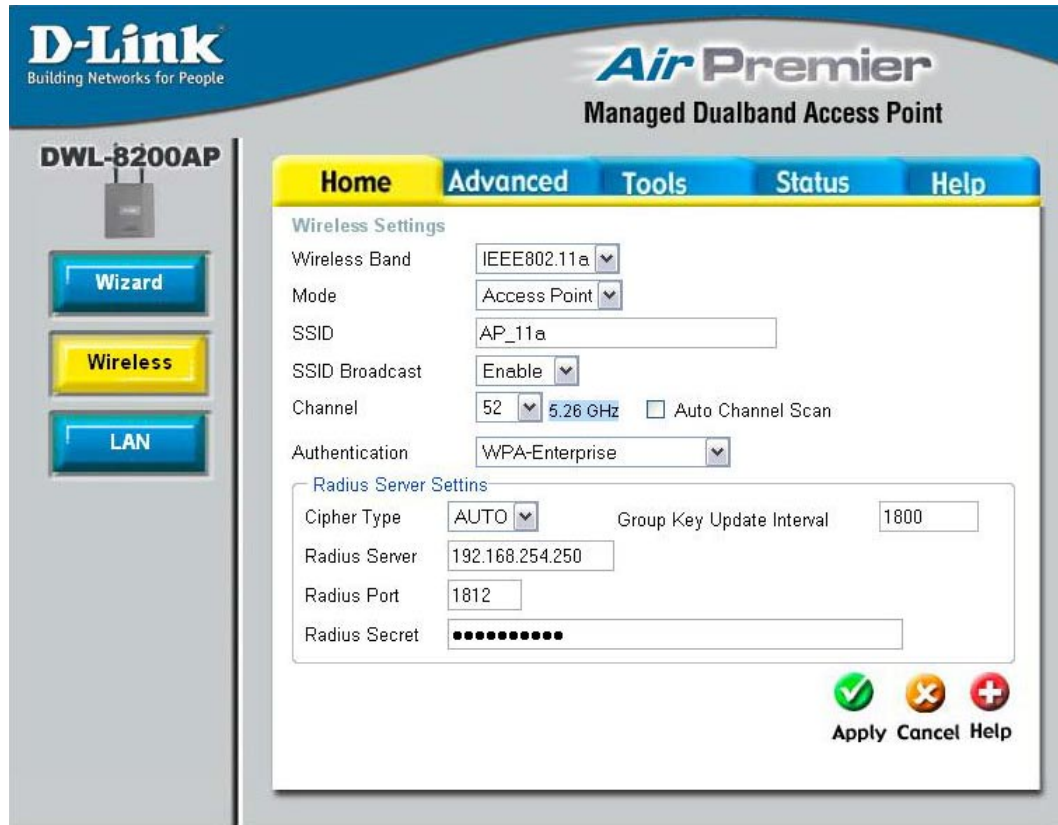
Cipher Type: When you select **WPA-Enterprise**, **WPA2-Enterprise** or **WPA-Auto-Enterprise**, you must select **AES**, **AUTO**, or **TKIP** from the pull-down menu.

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   Select the interval during which the group key will be valid. The
Interval: default value of 1800 is reommended.

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 > Authentication

Authentication:

Open System

Shared Key

Open System/Shared Key

WPA-Personal

WPA2-Personal

WPA-Auto-Personal

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

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

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

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

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 > Open System and/or Shared Key *(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 See **Home > Wireless > WDS with AP > Authentication** on pages 22-23.

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

Home > Wireless > WDS > Authentication

Authentication: **Open System**

Shared Key

Open System/Shared Key

WPA-Personal

WPA2-Personal

WPA-Auto-Personal

Home > Wireless > WDS > Authentication *(continued)*

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

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

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

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 > Open System and/or Shared Key *(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: See **Home > Wireless > WDS > Authentication** on pages 27-28.

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
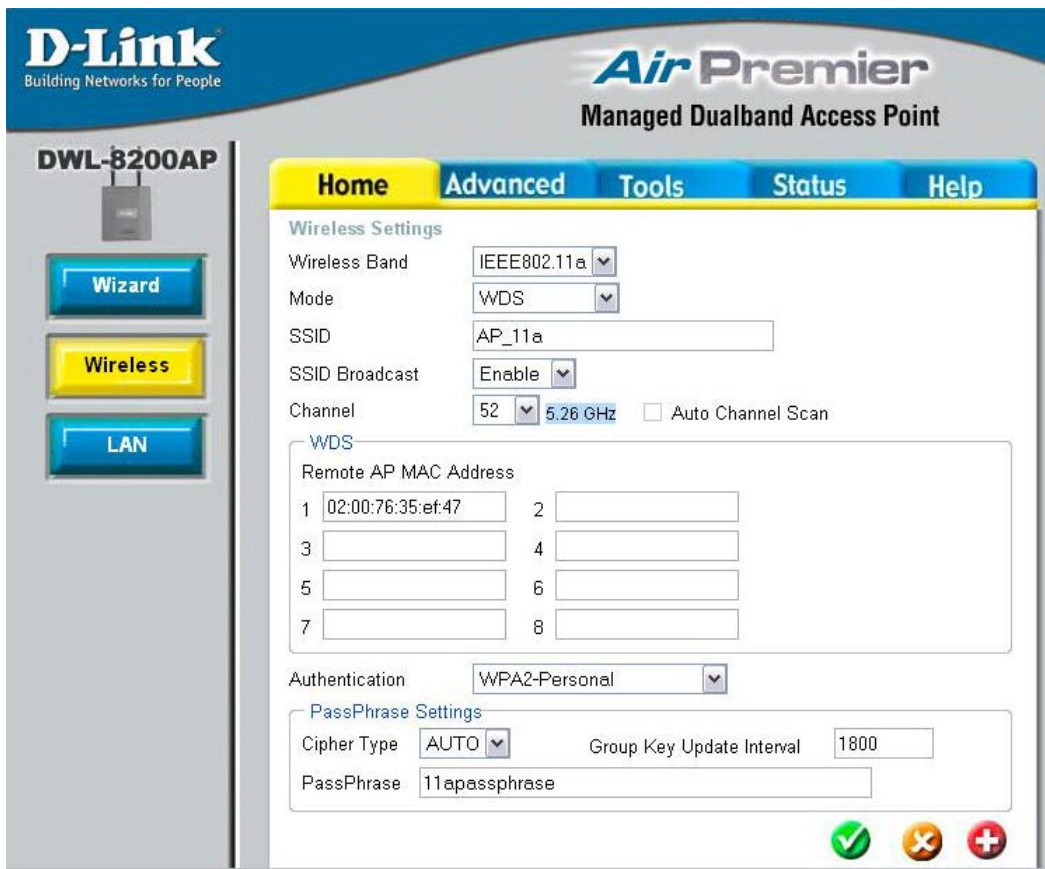
Cipher Type:	When you select **WPA-Personal**, **WPA2-Personal,** or **WPA-Auto-Personal**, you must select **AES**, **AUTO**, or **TKIP** from the pull-down menu.
Group Key Update Interval:	Select the interval during which the group key will be valid. The default value of 1800 is reommended.
PassPhrase:	When you select **WPA-Personal**, **WPA2-Personal,** or **WPA-Auto-Personal**, please enter a **PassPhrase** in the corresponding field.

Home > LAN
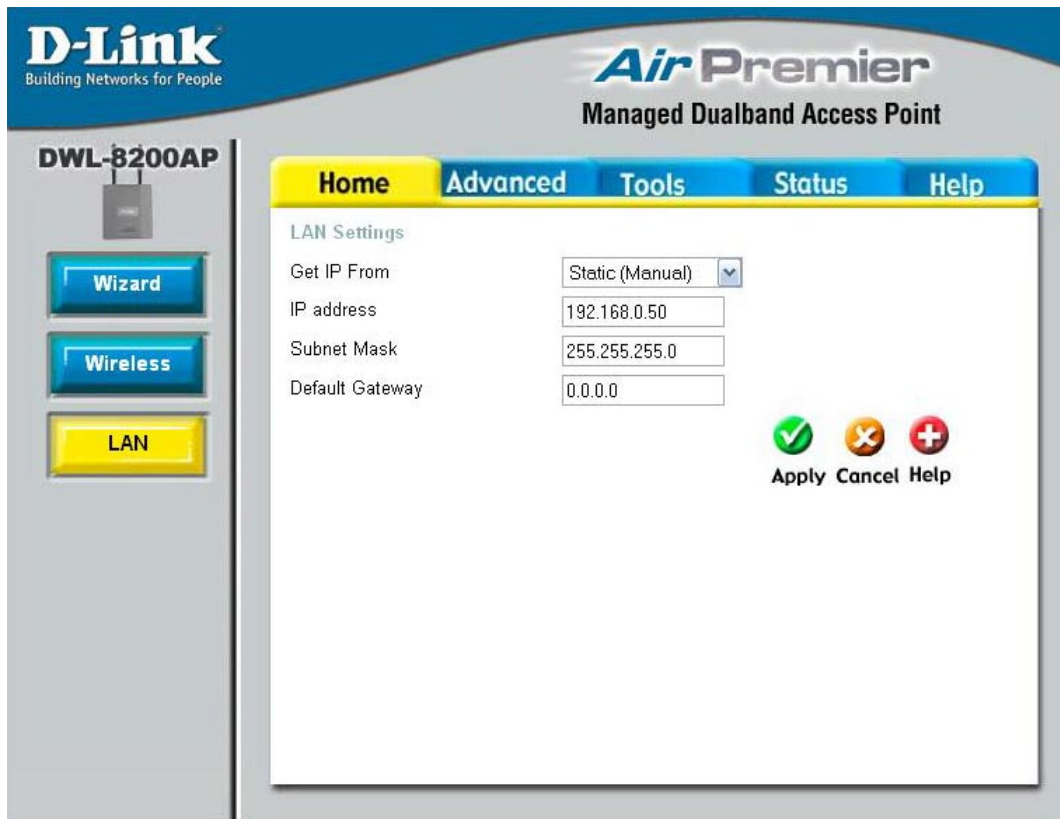
LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the **DWL-8200AP**. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network 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
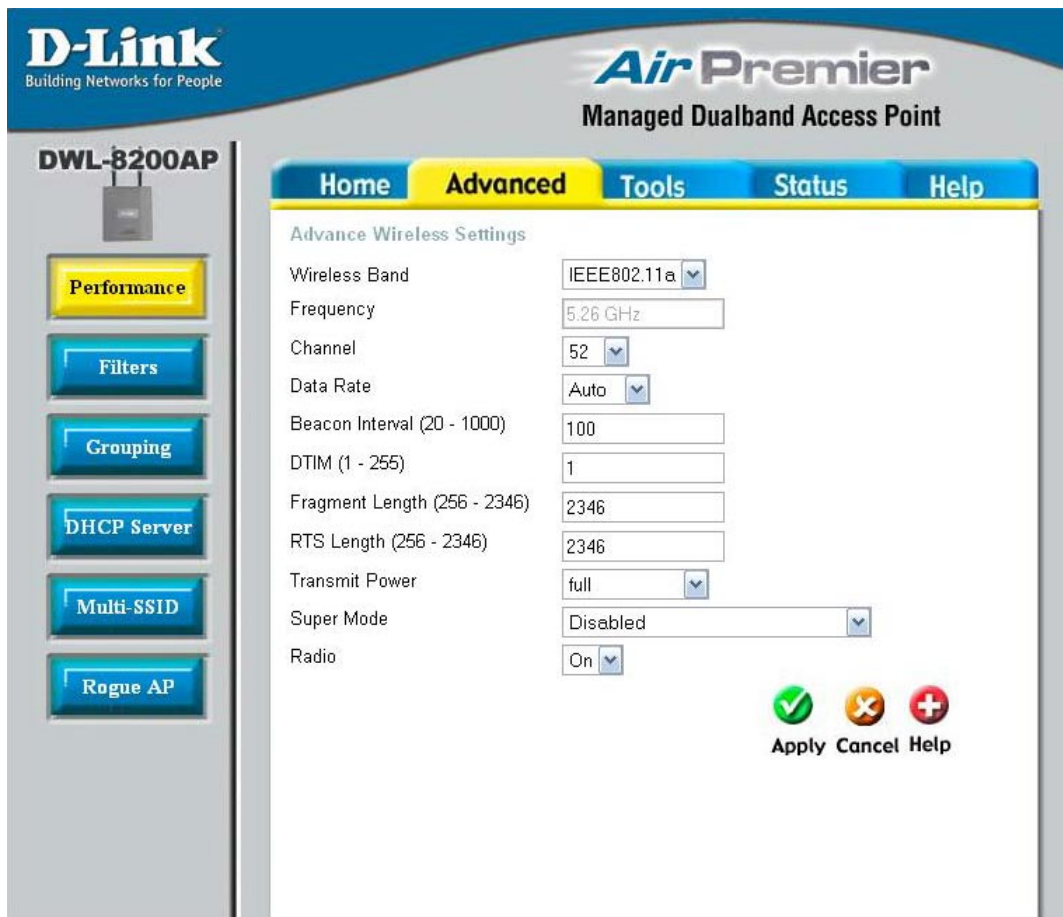
By changing radio parameters in the performance section, you can customize the radio network to fit your needs. Performance functions are designed for more advanced users who are familiar with 802.11 wireless networks and radio configuration.

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): *(Delivery Traffic Indication Message)* - 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.

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 Wave:	Select **ON** or **OFF**.

Advanced > Filters > Wireless Access Settings
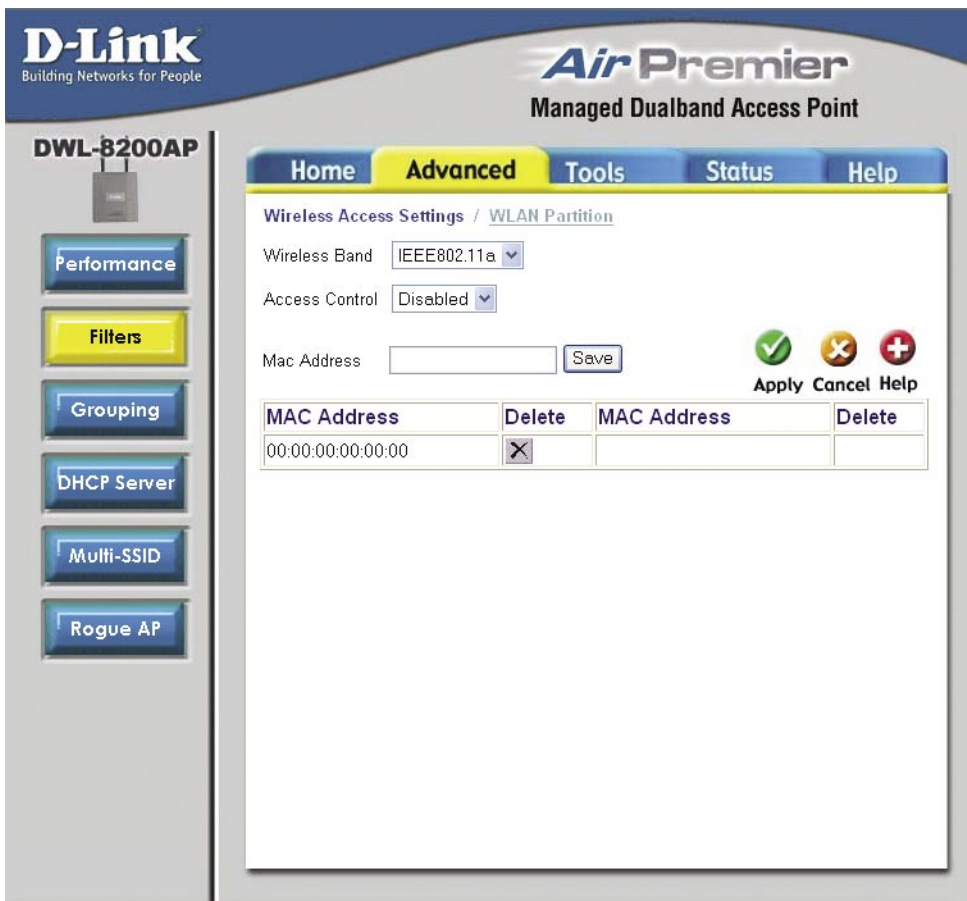
Wireless Band:	Select IEEE 802.a or IEEE 802.11g from this pull-down menu.
Access Control:	Select **Disabled** to disable the filters function. Select **Accept** to accept only those devices with MAC addresses in the Access Control List. Select **Reject** to reject the devices with MAC addresses in the 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
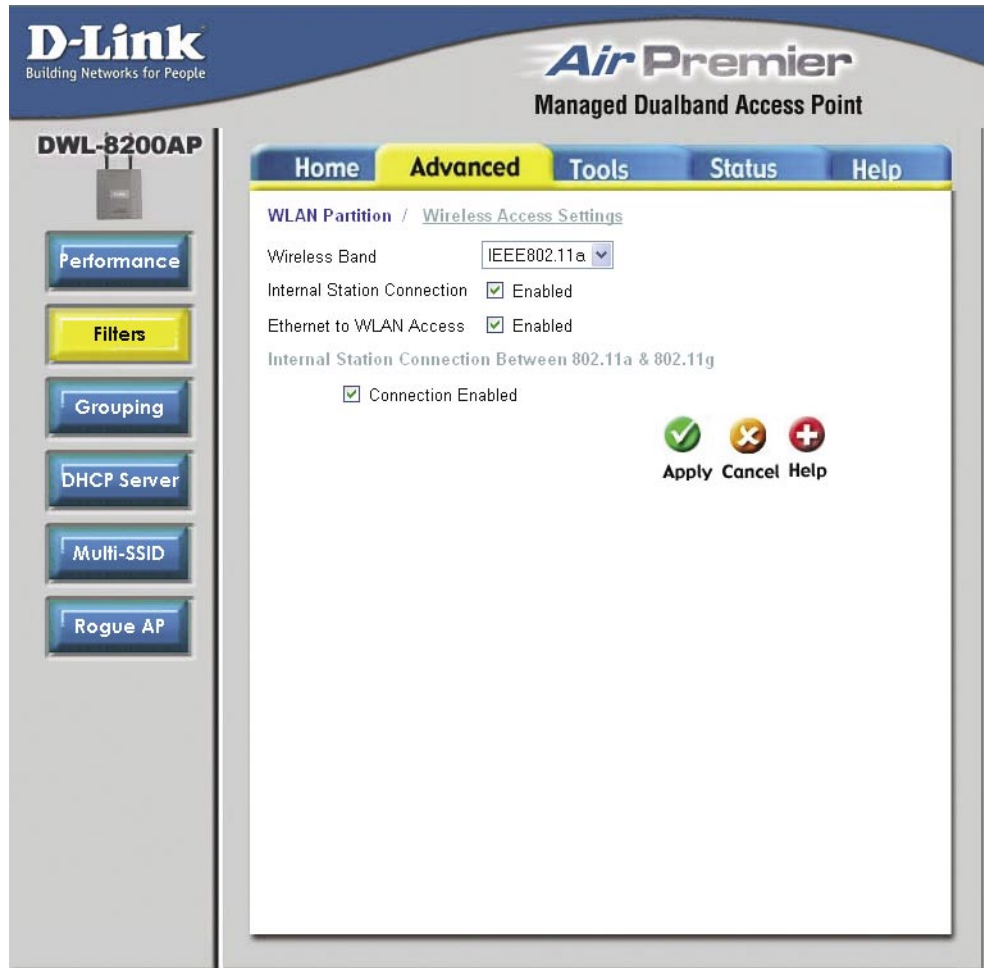
Wireless Band: Select IEEE 802.a or IEEE 802.11g from this pull-down menu.

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.

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.

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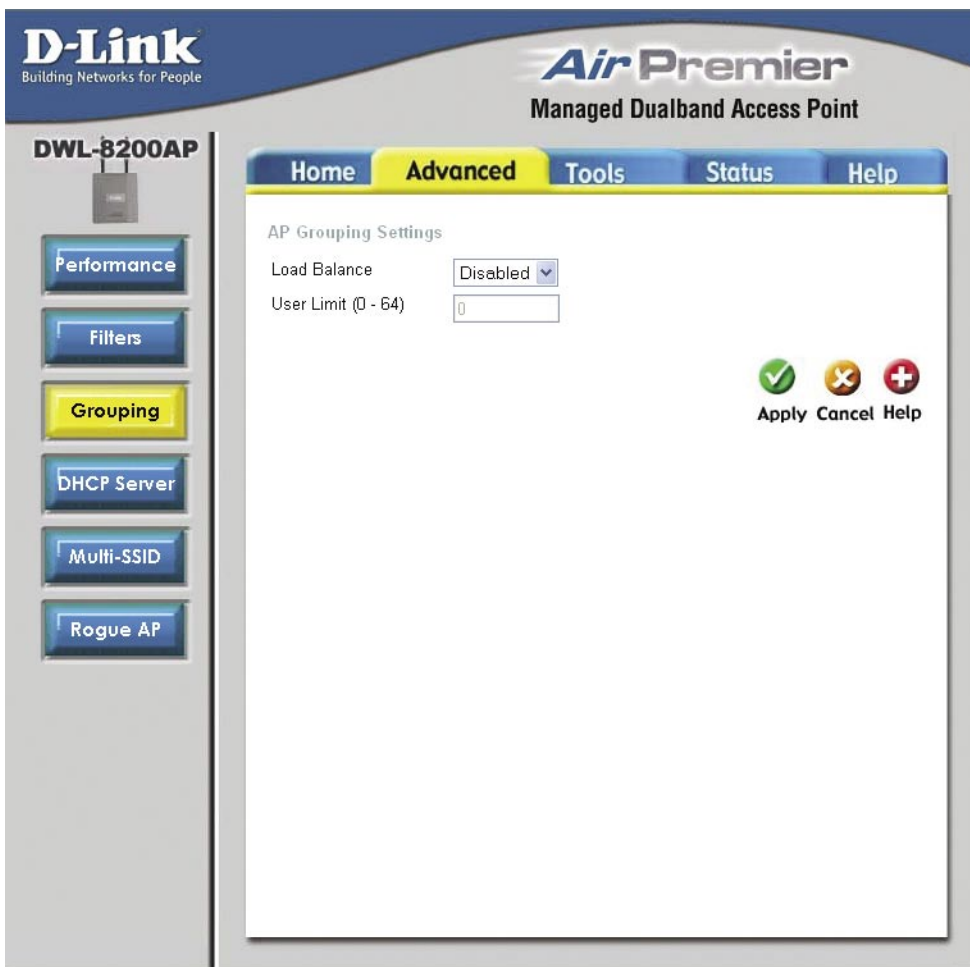
Load Balance: | When **Enabled**, you allow several **DWL-8200AP**s to balance wireless network traffic and wireless clients among **DWL-8200AP**s in the network. Assign each access point a different **non-overlapping channel** (e.g., 1, 6, 11).

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

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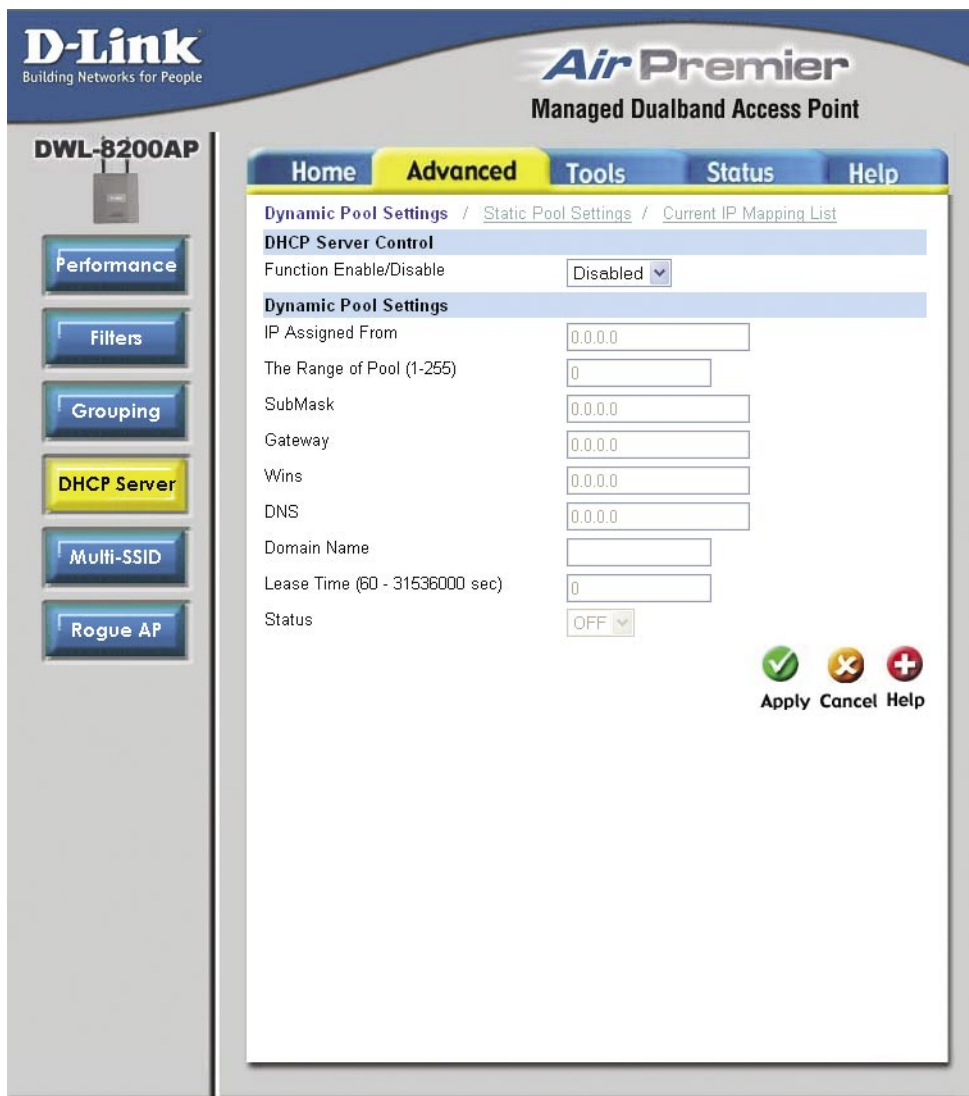
DHCP Server Control:	**Dynamic Host Configuration Protocol** assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.
	Select **Enable**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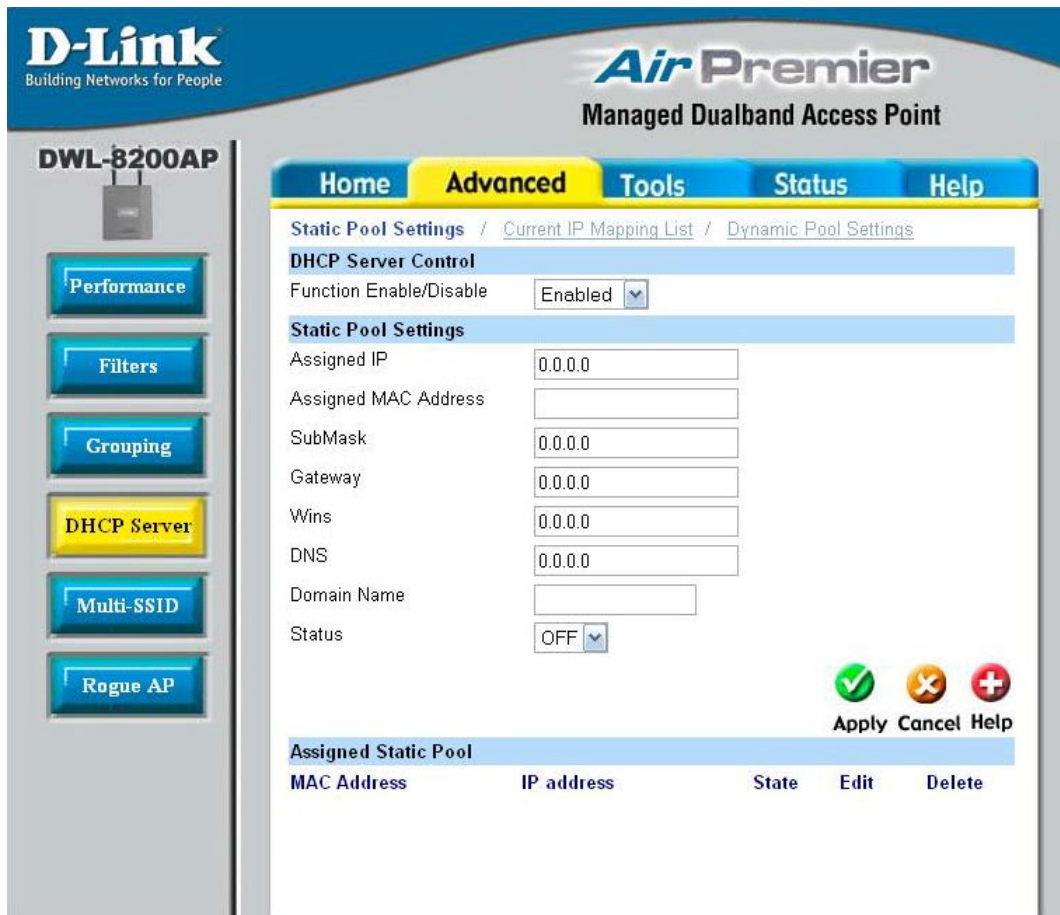
DHCP Server Control: **Dynamic Host Configuration Protocol** assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses.

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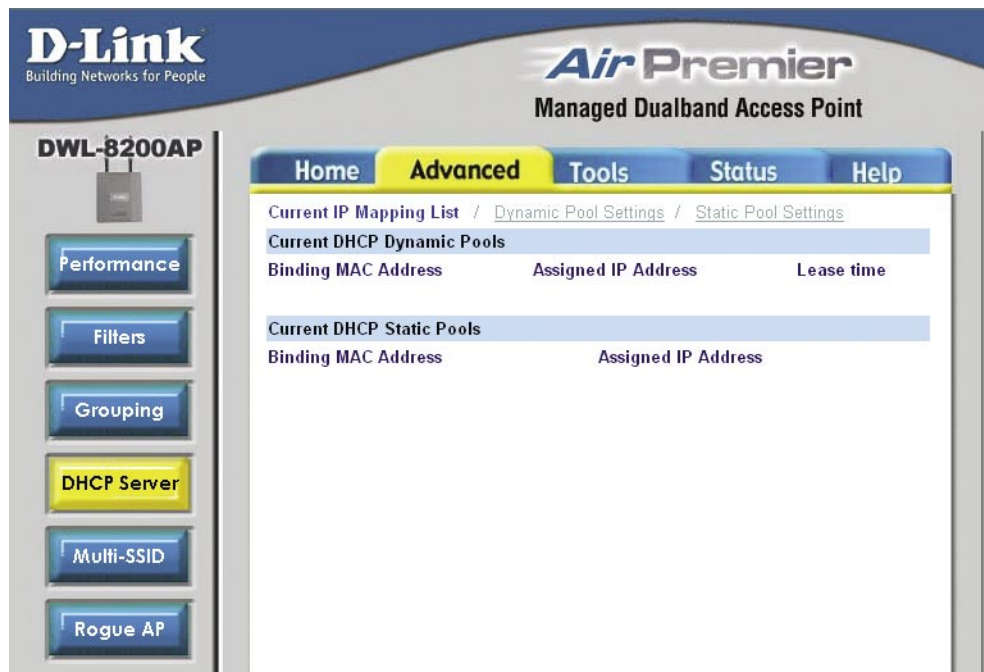
This screen displays information about the current DHCP dynamic and static IP address pools. This information is available when you enable the DHCP function of the **DWL-8200AP** and assign dynamic and static IP address pools.

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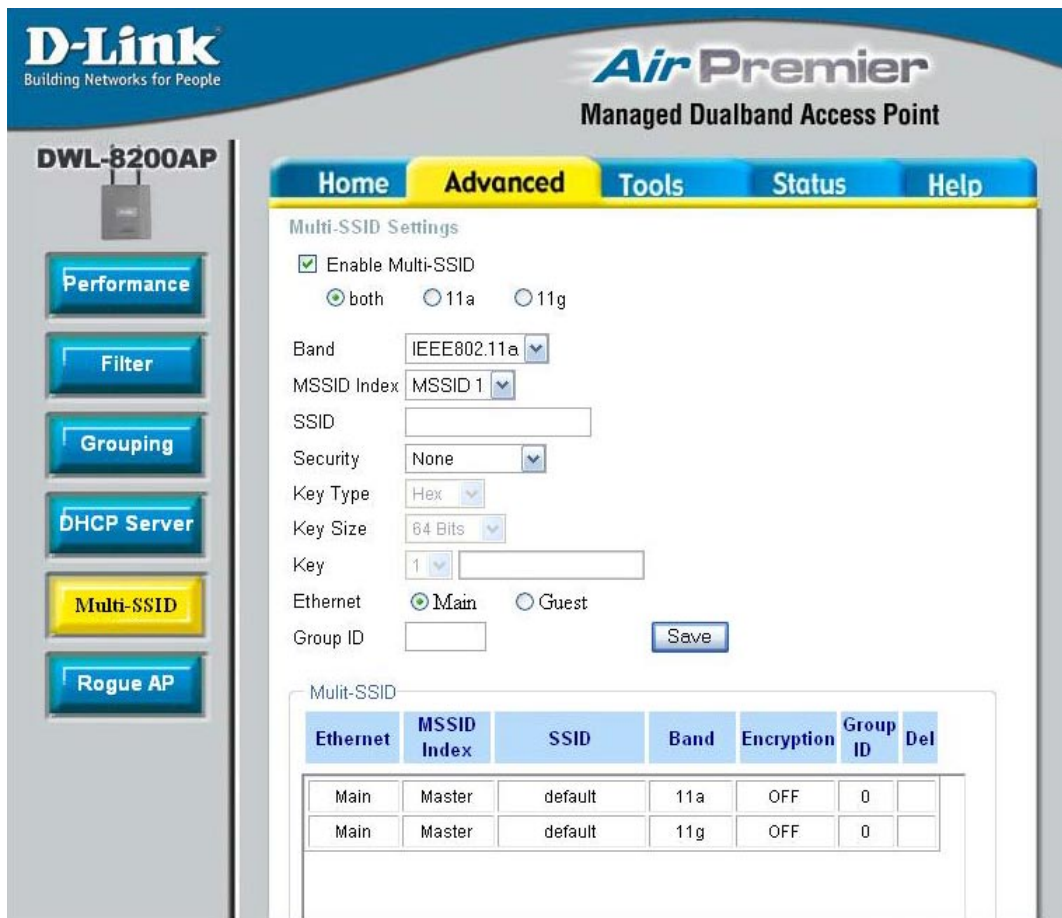
Enable Multi-SSID: When Multi-SSID is enabled, you can configure your SSIDs for either **both**, **11a** only, or **11g** only networks.

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

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
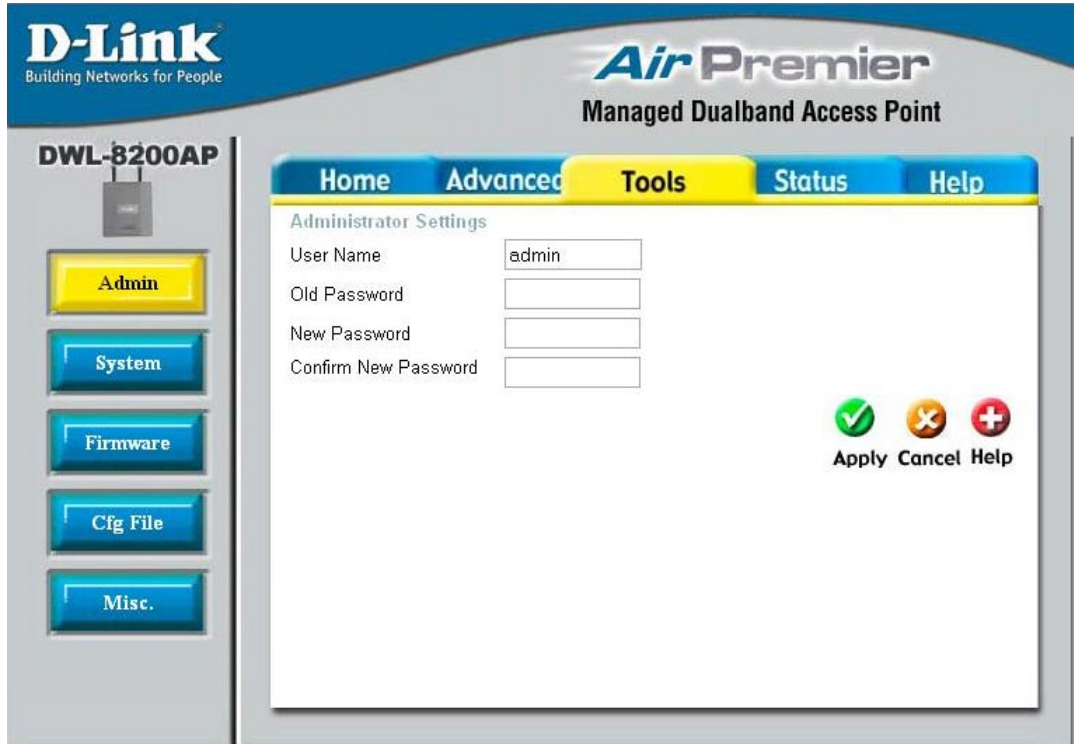
User Name:	Enter a user name. The default setting is **admin**.
Old Password:	To change your password, enter the old password here.
New Password:	Enter your new password here.
Confirm New Password:	Enter your new password again.

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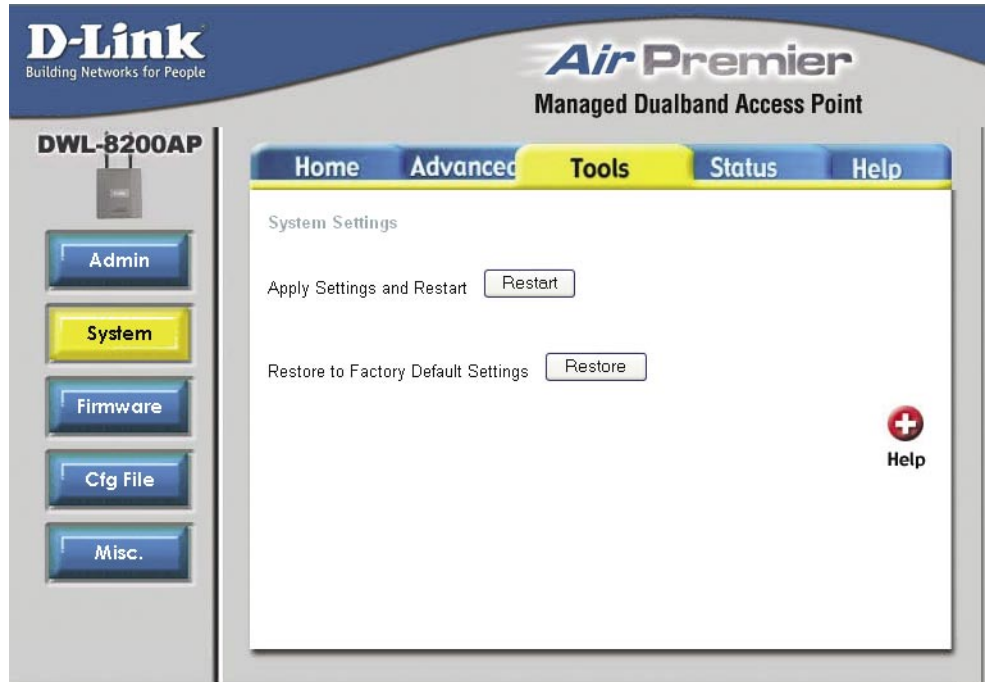
You may restart the **DWL-8200AP** with the changed settings or reset the **DWL-8200AP** back to factory settings.

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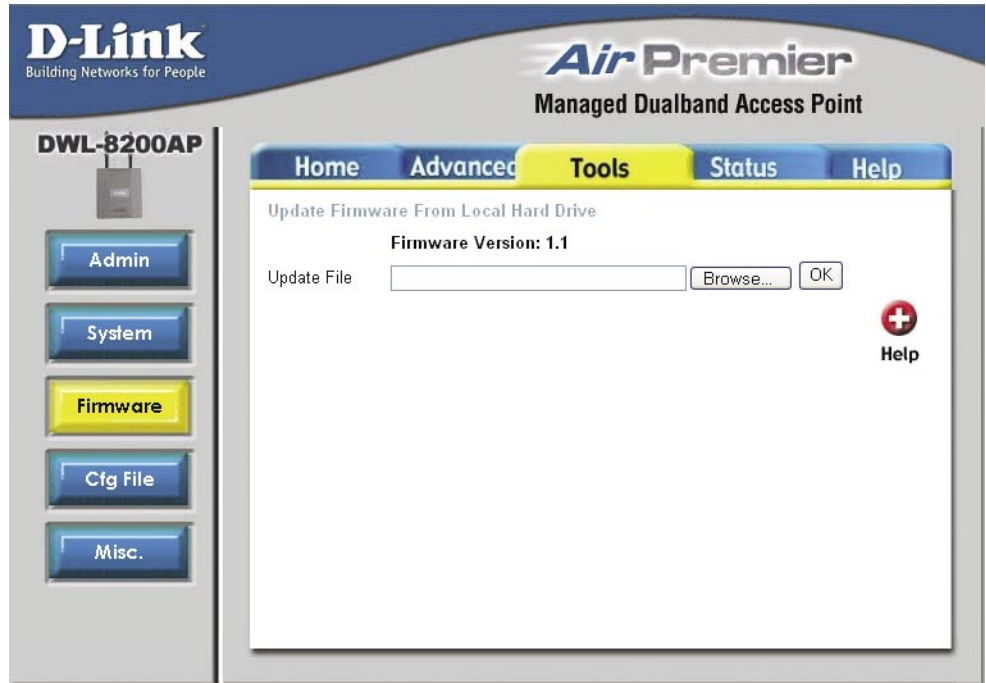
The firmware of the **DWL-8200AP** can be upgraded to resolve any compatibility or system conflicts. Please visit http://support.dlink.com for the latest firmware for this device.

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
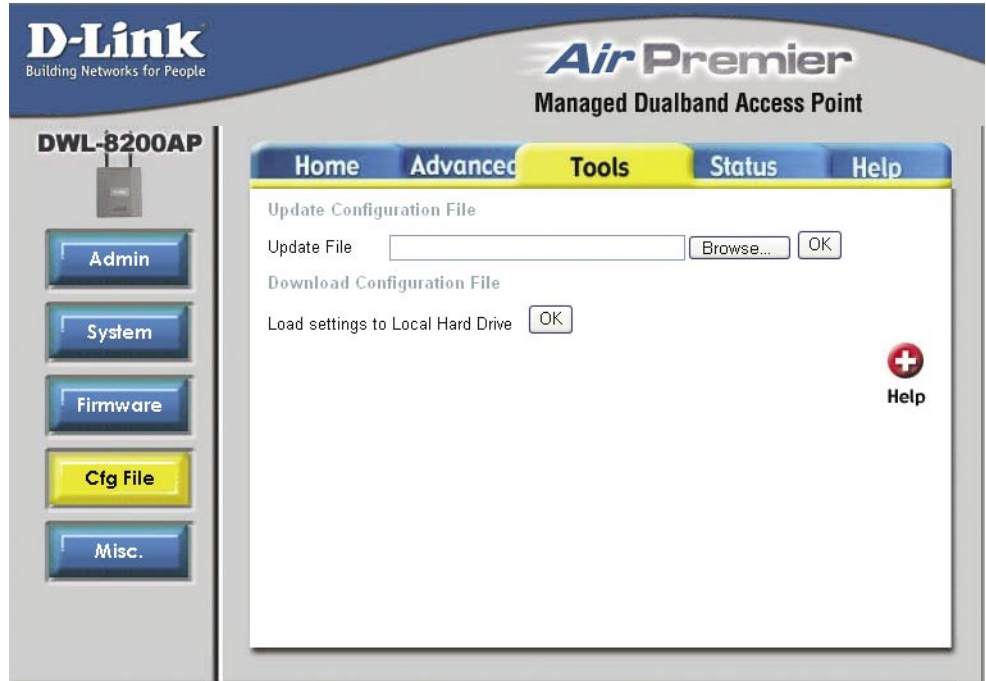
Update File:	Browse for the configuration settings that you have saved to your hard drive. Click **OK** after you have selected the settings file.
Load Settings to the Local Hard Drive:	Click **OK** to save the selected settings to your hard drive.

Tools > Cfg File > Choose file
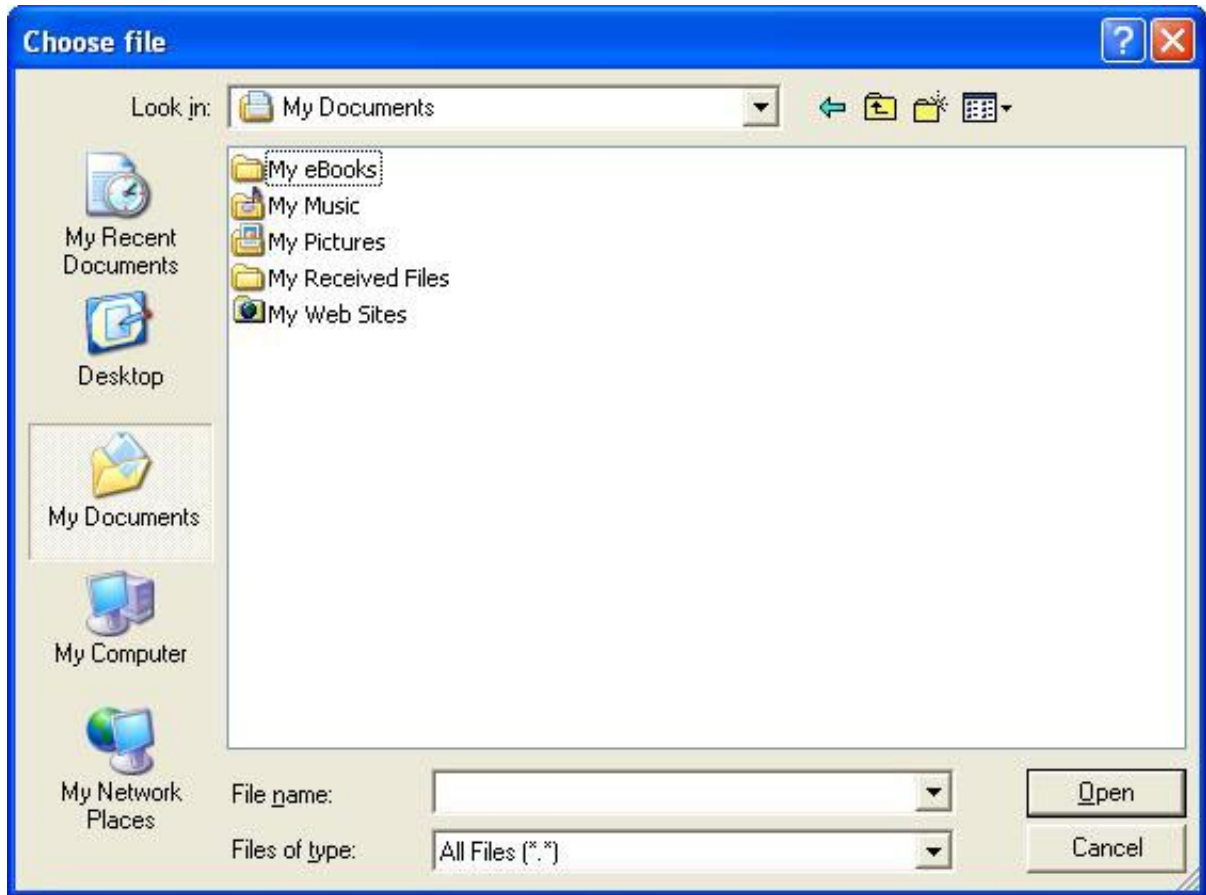
When you click **Browse** in the previous screen, the dialog box shown above appears. Select the file you wish to download and click **Open**.
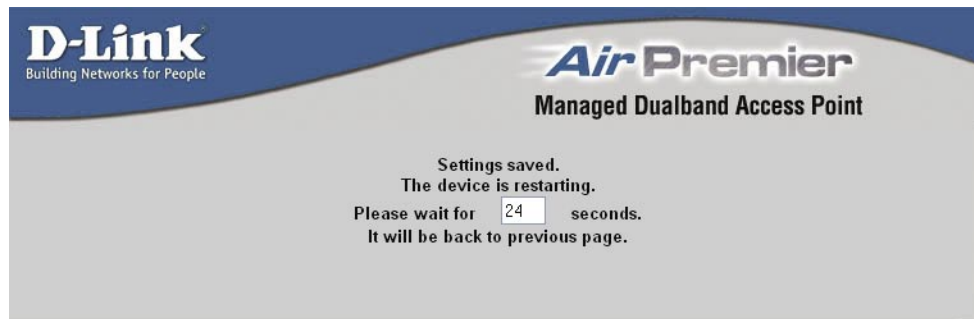
The dialog box above will appear as the device restarts. Please wait for a few seconds.

Tools > Misc > Telnet Settings
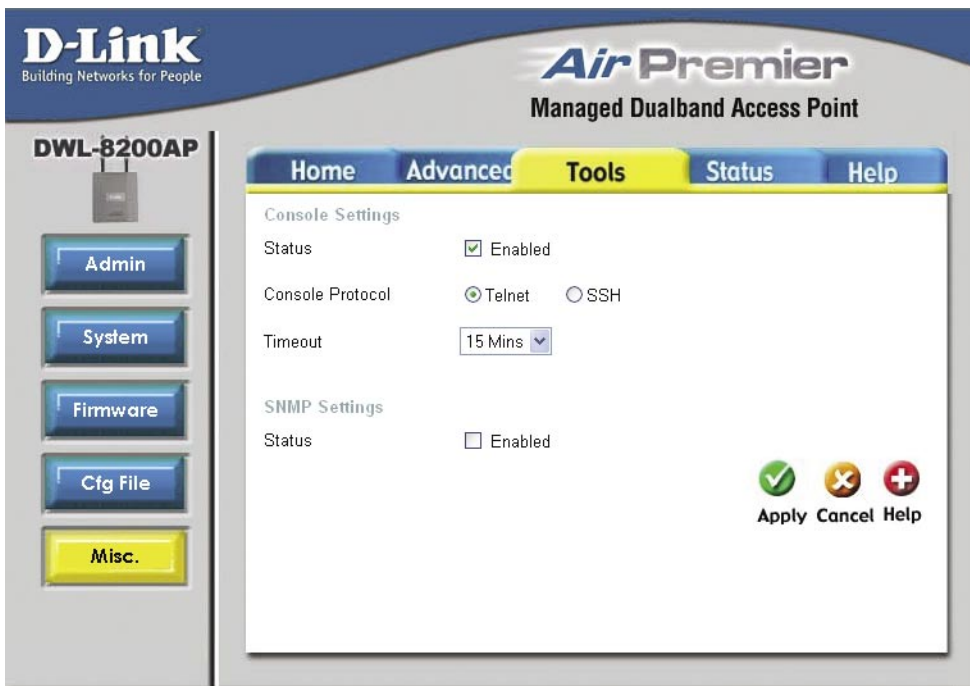
Telnet is a program that allows you to control your device from a single PC.

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

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

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.
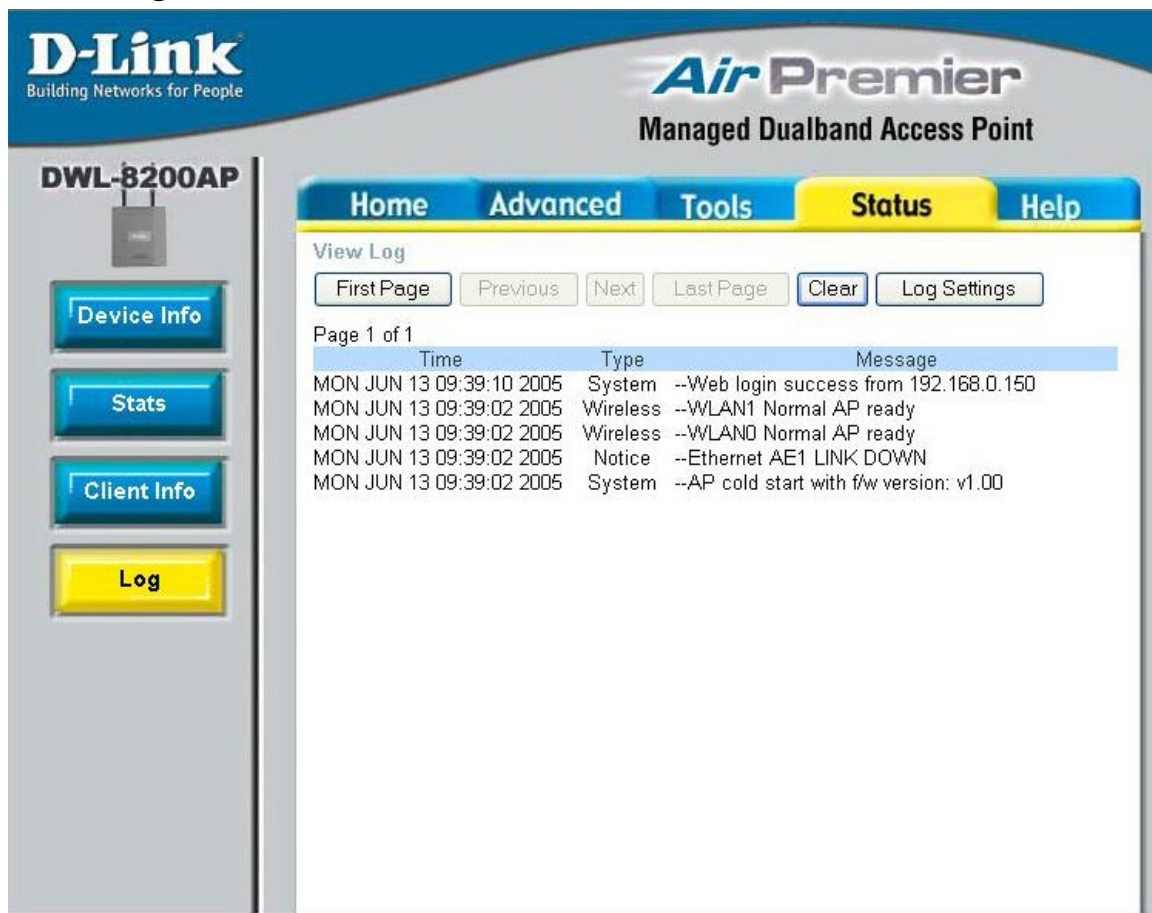
Status > Stats > WLAN 802.11G Traffic Statistics

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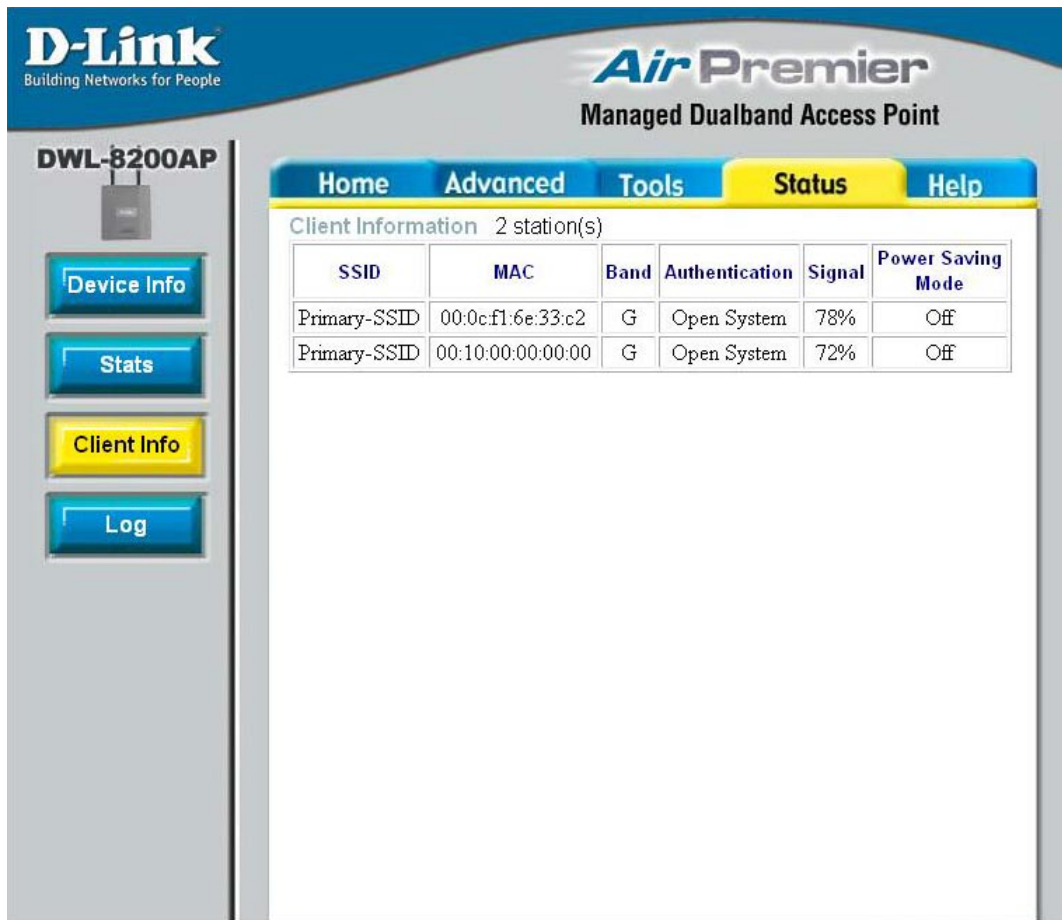
Client Information: Select this option to obtain information on wireless clients.
(A client is a device on the network that is communicating with the **DWL-8200AP**.)

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

Help

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