

DAP-3220  
Release 1.00

**Wireless 108G Exterior Access Point**

 **User Manual**

**Business Class Networking**

---

# Table of Contents

---

Table of Contents .....	2
Package Contents .....	3
Introduction .....	4
Features and Benefits .....	6
Wireless Basics .....	7
Four Operational Modes .....	10
Getting Started .....	11
Using the Configuration Menu .....	13
Troubleshooting .....	61
Technical Specifications .....	64
Warranty .....	66

# Package Contents

---



- **D-Link *DAP-3220* Wireless 108G Exterior Access Point**
- Power over Ethernet base unit
- DC 48V, 0.4A Power Adapter
- Power Cord
- Manual on CD
- Quick Installation Guide
- Ethernet Cable
- Mounting Plate

Warning: Using a power adapter or power cord with different specifications than the one included with the **DAP-3220** 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 or Firefox version 1.5 or above.

# Introduction

---

With up to fifteen times the speed of previous wireless devices (maximum wireless signal rate of up to 108Mbps\* in Super G mode), the DAP-3220 increases productivity by allowing you to work faster and more efficiently. With the DAP-3220, bandwidth-intensive applications like graphics or multimedia will benefit significantly because large files are now able to move across the network quickly.

The DAP-3220 is capable of operating in one of 4 different wireless networking modes; access point, WDS (Wireless Distribution System) with AP, WDS or Wireless Client mode.

Use less wiring, enjoy increased flexibility, save time and money with PoE (Power over Ethernet). With PoE, the DAP-3220 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, and special events for providing data transfers at rates of up the DAP-3220 provides data transfers at up to 108Mbps in Super G mode when used with other D-Link Wireless 108G 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** are directed towards 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 at both the client and access point, access is then 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. The abilities of **WPA2-Personal** exceed **WPA-Personal** because the encryption of data is upgraded with the Advanced Encryption Standard (AES).

\*Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput may vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead can lower actual data throughput rate.

**WPA-Enterprise** and **WPA2-Enterprise** are ideal for businesses that already have existing security infrastructures established. 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 WPA-Enterprise or WPA2-Enterprise configured, the new client will be requested to enter a username with a password.. If the new client is authorized by the administration, and enters the correct username and password, then access is then granted. In the case where an employee leaves the company, the network administrator is able to remove the previous employee from the authorized list to avoid compromising the network. **WPA2-Enterprise** is far superior to **WPA-Enterprise** because the encryption of data is upgraded with the Advanced Encryption Standard (AES).

**EAP (Extensible Authentication Protocol)** is available through the Windows® XP operating system. You will need to use the same type of EAP protocol on all devices in your network when using the 802.1x feature.

# Features and Benefits

---

- **4 Different operation modes** - capable of operating in one of four different operation modes to meet your wireless networking needs: access point; WDS with AP, WDS or wireless client.
- **Easy installation with Power over Ethernet (PoE).**
- **Faster wireless networking** with the 802.11g standard to provide a maximum wireless signal rate of up to 54Mbps\*, and 108Mbps\* in Super G mode.
- **Compatible with the 802.11b standard** to provide a wireless data rate of up to 11Mbps, allowing you to migrate your system to the 802.11g standard on your own schedule without sacrificing connectivity.
- **Better security with WPA** - the DAP-3220 can securely connect wireless clients on the network using WPA (Wi-Fi Protected Access) to provide a much higher level of security for your data and communications than its previous versions.
- **AP Manager II management software** - the real-time display of the network's topology and AP's information makes network configuration and management quick and simple.
- **SNMP for management** - the DAP-3220 is not just fast, but also supports SNMP v.3 for better network management. Superior wireless AP manager software is bundled with the DAP-3220 for network configuration and firmware upgrade. Systems administrators can also setup the DAP-3220 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 2.4GHz frequency range.
- **Web-based interface** for managing and configuring.

\*Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput may vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead can lower actual data throughput rate.

# Wireless Basics

---

D-Link wireless products are based on industry standards to provide high-speed wireless connectivity that is easy to use within your home, business or public access wireless networks. D-Link wireless products provides you with access to the data you want, whenever and wherever you want it. Enjoy the freedom that wireless networking can bring to you.

WLAN use is not only increasing in both home and office environments, but in public areas as well, such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are allowing people to work and communicate more efficiently. Increased mobility and the absence of cabling and other types of fixed infrastructure have proven to be beneficial to many users.

Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards, allowing wireless users to use the same applications as those used on a wired network.

*People use WLAN technology for many different purposes:*

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

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

**Installation and network expansion** - by avoiding the complications of troublesome cables, a WLAN system can be fast and easy during installation, especially since it can eliminate the need to pull cable through walls and ceilings. Wireless technology provides more versatility by extending the network beyond the home or office.

**Inexpensive solution** - wireless network devices are as competitively priced as conventional Ethernet network devices. The DAP-3220 saves money by providing users with multi-functionality configurable in four different modes.

**Scalability** - Configurations can be 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 DAP-3220 Exterior Access Point utilizes the **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 up to 54Mbps\*, and 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 simultaneously transmitted at different frequencies to the receiver. OFDM reduces the amount of **crosstalk** (interference) in signal transmissions.

The D-Link DAP-3220 will automatically sense the best possible connection speed to ensure the greatest possible speed and range.

802.11g offers the most advanced network security features available today, including WPA and WPA2.

## Important Information

This product should **ONLY** be installed by an experienced installer who is familiar with local building and safety codes and where ever applicable, is licensed by the appropriate authorities. Failure to do so may void the D-Link product warranty and may expose the end user

or the service provider to legal and financial liabilities. D-Link and its resellers or distributors are not liable for injury, damage, or violation of regulations associated with the installation of outdoor units or antennas.

A safety grounding system is necessary to protect your outdoor installation from lightning strikes and the build-up of static electricity. The grounding system must comply with the National Electrical Code and safety standards that apply in your country. Always check with a qualified electrician if you are in doubt as to whether your outdoor installation is properly grounded.

\*Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput may vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead can lower actual data throughput rate.

## Installation Considerations

The D-Link DAP-3220 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:

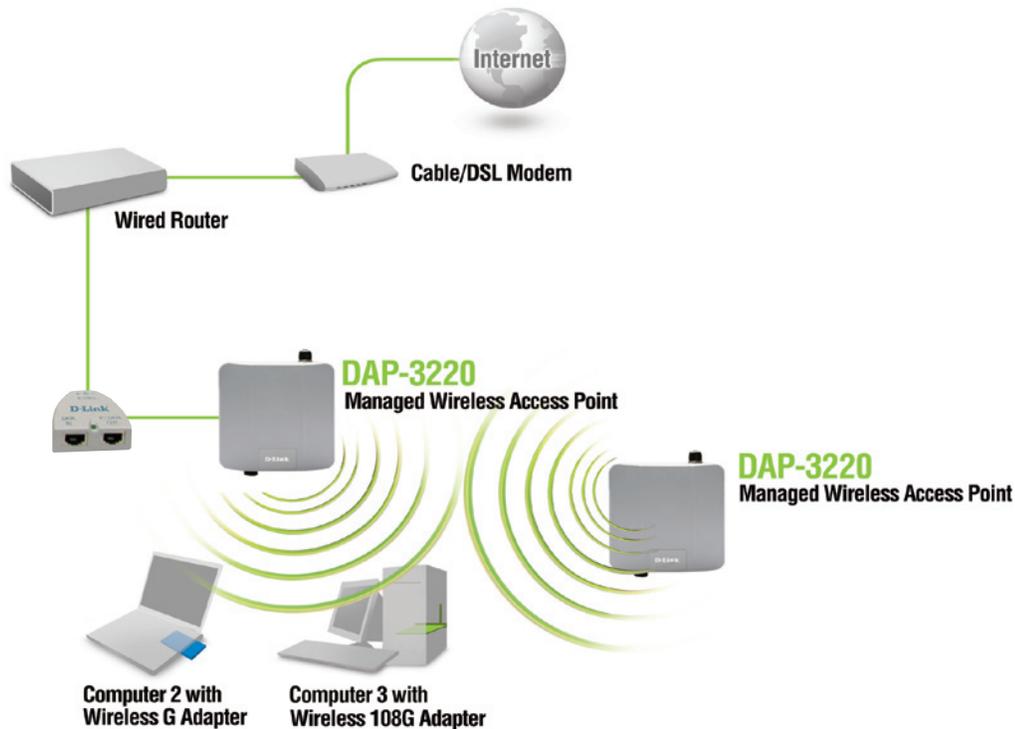
- 1** Keep the number of walls and ceilings between the DAP-3220 and other network devices to a minimum - each wall or ceiling can reduce your DAP-3220's range by 3-90 feet (1-30 meters). Position your devices so that the number of walls or ceilings is minimized.
- 2** Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle, the wall appears to be over 42 feet (14 meters) thick! Position your 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 can 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 through 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.
- 5** If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even when the phone is not in use.

# Four Operational Modes

---

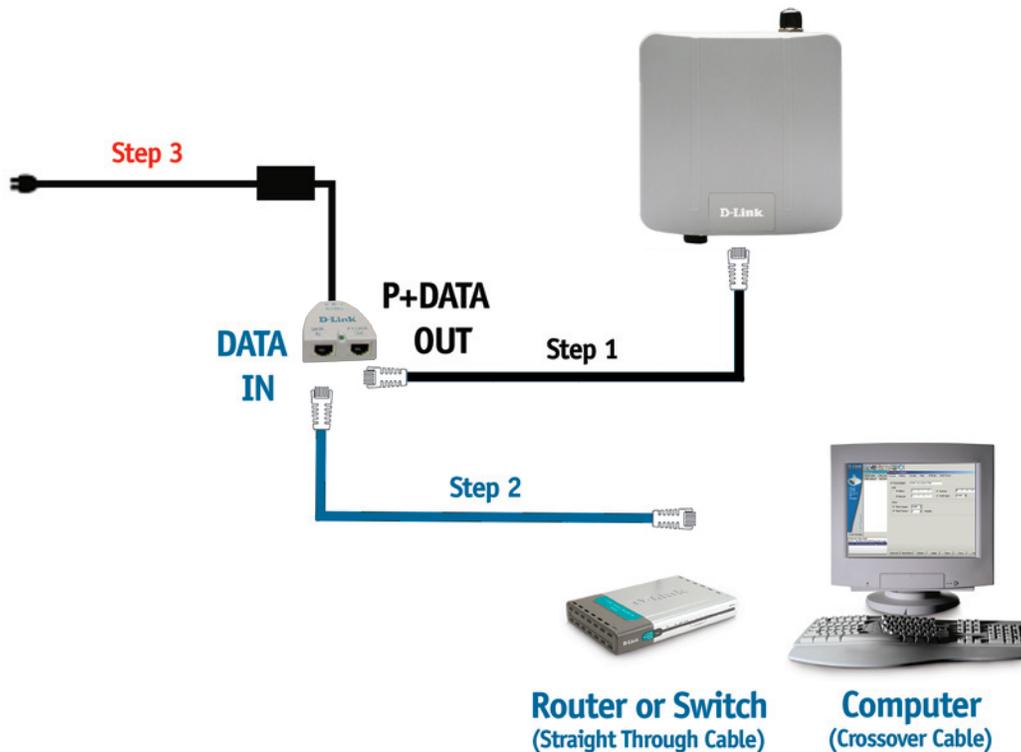
<b>Operation Mode</b> (Only supports 1 mode at a time)	<b>Function</b>
Access Point(AP)	Create a wireless LAN
WDS with AP	Wirelessly connect multiple networks while still functioning as a wireless AP
WDS	Wirelessly connect multiple networks
Wireless Client	AP acts as a wireless network adapter for your Ethernet-enabled device

# 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 DAP-3220.*
- 5 *See the printed Quick Installation Guide included with the DAP-3220.*
- 6 If you are connecting a desktop computer to your network, install a wireless PCI adapter into an available PCI slot on your desktop computer.
- 7 Install the drivers for your wireless CardBus adapter into a laptop computer.

## Connecting PoE (Power over Ethernet)



- Step 1** Connect one end of an Ethernet cable (included with your package) to the **LAN port** on the DAP-3220 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 using a straight through cable, or to a PC with a crossover cable.
- 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.

# Using the Configuration Menu

To configure the DAP-3220, use a computer that is connected to the DAP-3220 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, Mozilla Firefox).

\*Netscape Navigator is rarely used anymore.

Type the IP address and http port of the DAP-3220 in the address field (http://192.168.0.50) and press **Enter**. Make sure that the IP addresses of the DAP-3220 and your computer are in the same subnet.



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

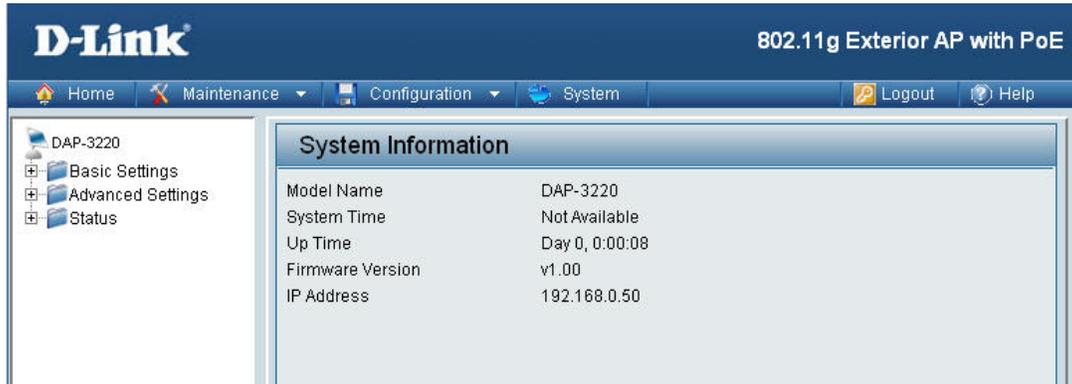
*Note: If you have changed the default IP address assigned to the DAP-3220, make sure to enter the correct IP address.*

- 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.*

After successfully logging into the DAP-3220 the following screen will appear:



When making changes on most of the configuration screens in this section, use the Apply button at the bottom of each screen to save your configuration changes.



Click the Apply button to configure changes.

## Home > Basic Settings > Wireless

The screenshot displays the D-Link configuration web interface for a DAP-3220 device. The main navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with Basic Settings (Wireless, LAN), Advanced Settings, and Status. The main content area is titled 'Wireless Settings' and contains the following fields:

- Wireless Band:** IEEE802.11g
- Mode:** Access Point
- SSID:** dlink
- SSID Broadcast:** Enable
- Channel:** 1, 2.412 GHz,  Auto Channel Scan
- Authentication:** Open System
- Key Settings:**
  - Encryption:**  Disable,  Enable
  - Key Type:** HEX, **Key Size:** 64 Bits
  - Valid Key:** First
  - First Key:** [Redacted]
  - Second Key:** [Empty]
  - Third Key:** [Empty]
  - Fourth Key:** [Empty]

An 'Apply' button is located at the bottom right of the configuration area.

**Wireless Band:** 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 **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

**SSID Broadcast:** Enable or Disable SSID broadcast. Enabling this feature broadcasts the SSID across the network.

**Channel:** **Auto Channel Scan** is set by default. All devices on the network must share the same channel. To change the channel, uncheck Auto Channel Scan. (Note: the wireless adapters will automatically scan and match the wireless settings.)

## Home > Basic Settings > Wireless (continued)

**Auto Channel Scan:** Select **Enable** or **Disable**, enabling this feature automatically selects the channel that provides the best wireless performance.

**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.

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

Select **WPA-Enterprise**, **WPA2-Enterprise**, or **WPA-Auto-Enterprise** to secure your network with the inclusion of a RADIUS server.

Select **WPA-Personal**, **WPA2-Personal**, or **WPA-Auto-Personal** to secure your network using a password and dynamic key changes (No RADIUS server required)

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

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

**Key Size:** Select **64-**, **128-**, **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 (HEX)** digits consist of the numbers 0-9 and the letters A-F.

**\*ASCII (American Standard Code for Information Interchange)** is a code that represents English letters using numbers ranging from 0-127/

## Home > Basic Settings > Wireless > WPA-Enterprise, WPA2-Enterprise, & WPA-Auto-Enterprise

The screenshot shows the D-Link configuration web interface for a DAP-3220 802.11g Exterior AP with PoE. The 'Wireless Settings' page is displayed, showing the following configuration options:

- Wireless Band:** IEEE802.11g
- Mode:** Access Point
- SSID:** dlink
- SSID Broadcast:** Enable
- Channel:** 6, 2.437 GHz,  Auto Channel Scan
- Authentication:** WPA-Enterprise
- RADIUS Server Settings:**
  - Cipher Type:** AUTO
  - Group Key Update Interval:** 1800 Sec
  - Primary radius server setting:**
    - RADIUS Server:** [Empty]
    - RADIUS Port:** 1812
    - RADIUS Secret:** [Empty]
  - Secondary radius server setting:**
    - Secondary RADIUS Mode:** Disable
    - RADIUS Server:** [Empty]
    - RADIUS Port:** 1812
    - RADIUS Secret:** [Empty]
  - Primary accounting server setting:**
    - Accounting Mode:** Disable
    - Accounting Server:** [Empty]
    - Accounting Port:** 1813
  - Secondary accounting server setting:**
    - Secondary Accounting Mode:** Disable
    - Accounting Server:** [Empty]
    - Accounting Port:** 1813

An 'Apply' button is located at the bottom right of the configuration area.

**Cipher Type:** When WPA-Enterprise is selected, you must also select the AUTO, AES, or TKIP option 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 as a lower interval may reduce data transfer rates.

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

**RADIUS Port:** Enter the RADIUS port.

**RADIUS Secret:** Enter the RADIUS secret.

**Accounting Mode:** Select if you want to use a different server for accounting.

**Accounting Server:** Enter the IP address of the Accounting server.

**Accounting Port:** Enter the Accounting port (1813 is the default).

Note: you can input the secondary RADIUS server and accounting server settings if you have the backup RADIUS and accounting server.

## Home > Basic Settings > Wireless > WPA-Personal, WPA2-Personal, & WPA-Auto-Personal

**D-Link** 802.11g Exterior AP with PoE

Home Maintenance Configuration System Logout Help

DAP-3220

- Basic Settings
  - Wireless
  - LAN
- Advanced Settings
- Status

### Wireless Settings

Wireless Band: IEEE802.11g

Mode: Access Point

SSID: dlink

SSID Broadcast: Enable

Channel: 6 2.437 GHz  Auto Channel Scan

Authentication: WPA-Personal

PassPhrase Settings

Cipher Type: AUTO Group Key Update Interval: 1800 Sec

PassPhrase:

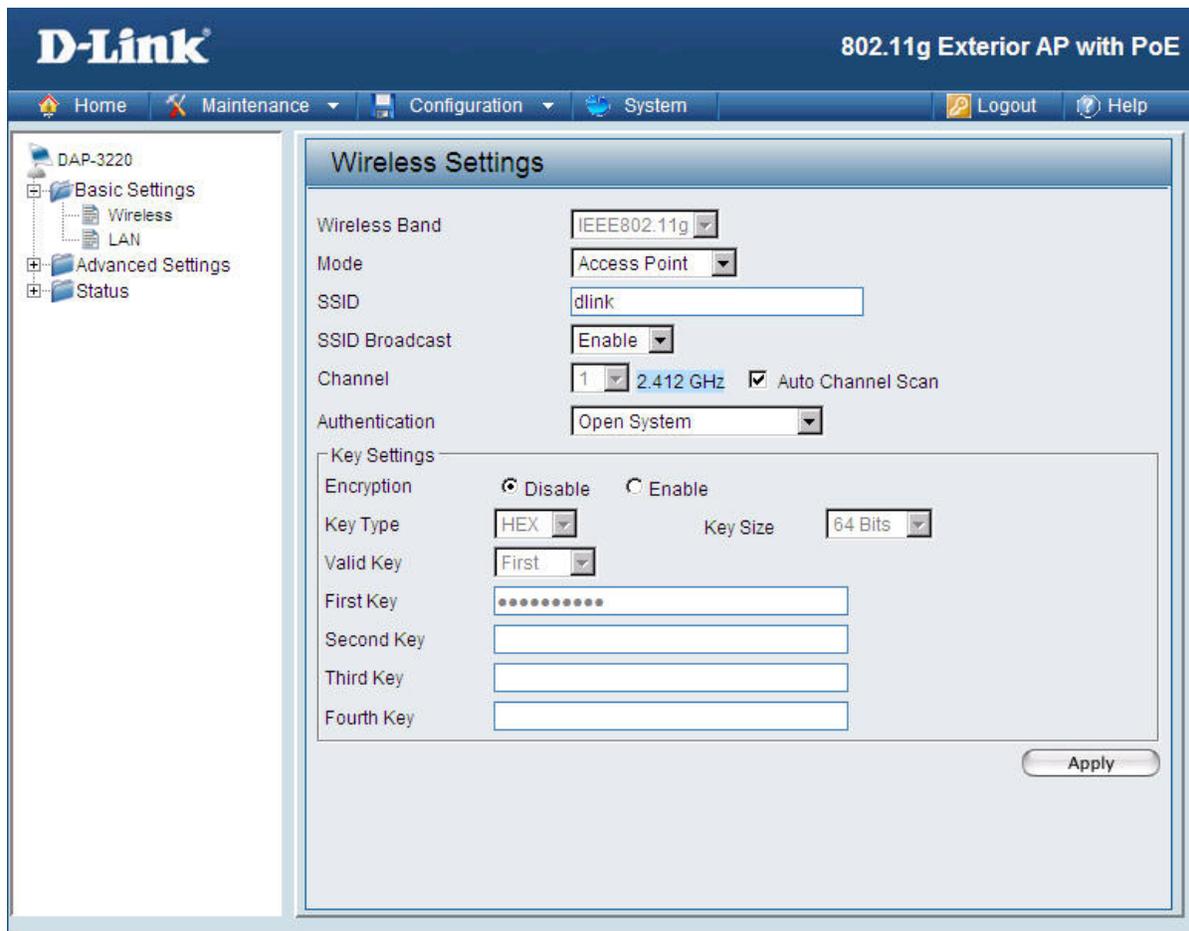
Apply

**Cipher Type:** When you select **WPA-Personal**, you must also select **AUTO**, **AES**, 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**, please enter a **PassPhrase** in the corresponding field.

## Home > Basic Settings > Wireless > Access Point mode



**Wireless Band:** IEEE 802.11g.

**Mode:** Access Point is selected from the drop-down menu.

**SSID:** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID factory default setting is dlink. 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:** **Auto Channel Scan** is selected by default. All devices on the network must share the same channel.

**Radio Frequency:** The radio frequency will vary depending on the wireless channel that is chosen. The frequency in channel 6 is 2.437GHz.

<b>Auto channel scan:</b>	Select Enable or Disable. Enabling this feature automatically selects the channel that provides the best wireless performance..
<b>Authentication:</b>	<p>Select <b>Open System</b> to communicate the key across the network.</p> <p>Select <b>Shared Key</b> to limit communication to only those devices that share the same WEP settings.</p> <p>Select <b>Open System/Shared Key</b> to allow either form of data encryption.</p> <p>Select <b>WPA-Enterprise</b> to secure your network with the inclusion of a RADIUS server.</p> <p>Select <b>WPA-Personal</b> to secure your network using a password and dynamic key changes (No RADIUS server required).</p> <p>Select <b>WPA2-Enterprise</b> to secure your network with the inclusion of a RADIUS server, and upgrade the encryption of data with the Advanced Encryption Standard (AES).</p> <p>Select <b>WPA2-Personal</b> to secure your network using a password and dynamic key changes. No RADIUS server is required and encryption of data is upgraded with the Advanced Encryption Standard (AES).</p> <p>Select <b>WPA-Auto-Enterprise</b> to allow the client to either use <b>WPA-Enterprise</b> or <b>WPA2-Enterprise</b>.</p> <p>Select <b>WPA-Auto-Personal</b> to allow the client to either use <b>WPA-Personal</b> or <b>WPA2-Personal</b>.</p>

## Home > Basic Settings > Wireless > WDS with AP mode

In WDS with AP mode, the DAP-3220 wirelessly connects multiple networks while still functioning as a wireless AP.

**Wireless Band:** IEEE 802.11g

**Mode:** WDS with AP mode is selected from the pull-down menu.

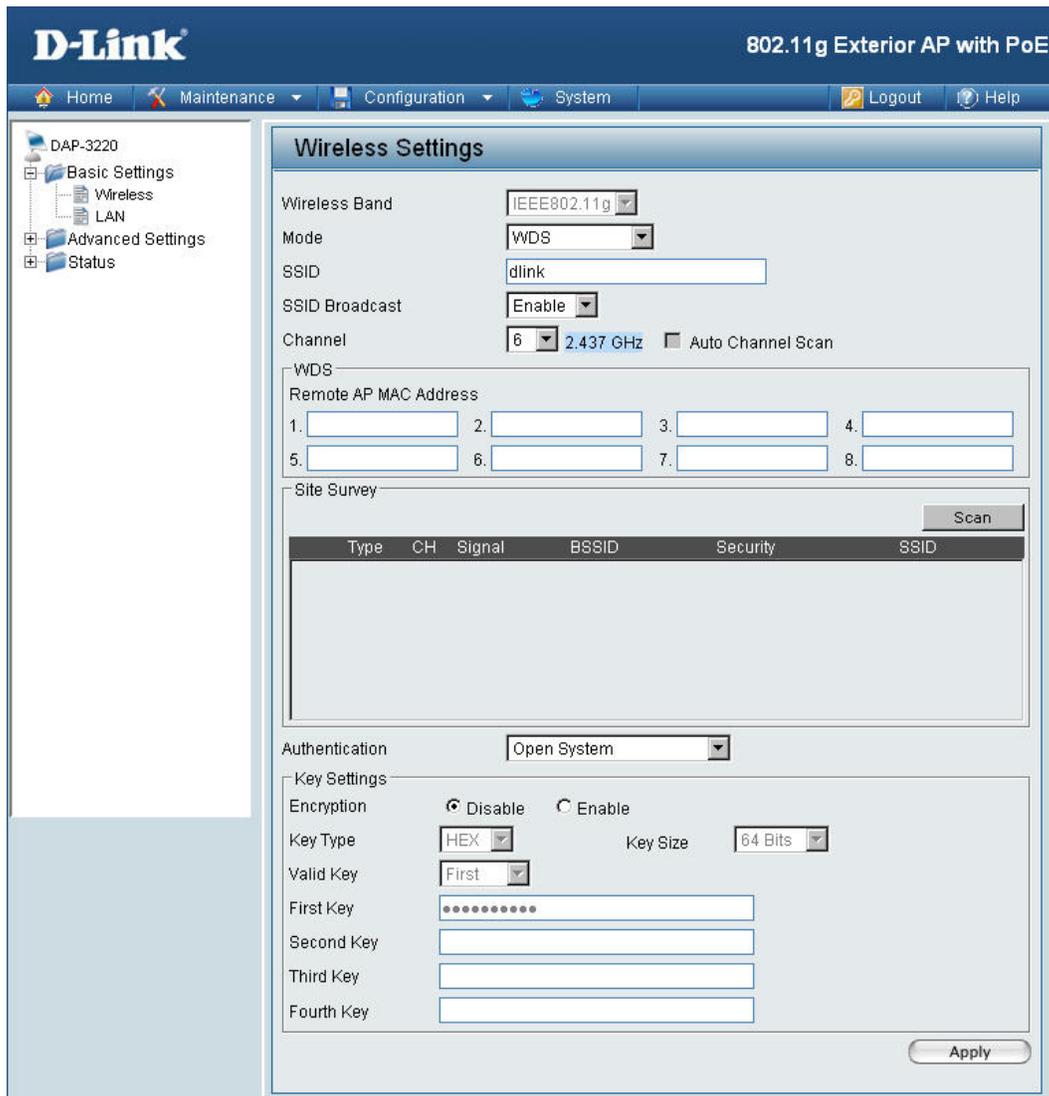
**SSID:** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

**SSID Broadcast:** Enable or Disable SSID broadcast. Enabling this feature broadcasts the SSID across the network.

## Home > Basic Settings > Wireless > WDS with AP (continued)

<b>Channel:</b>	<b>6</b> is the default channel. All devices on the network must share the same channel. (Note: the wireless adapters will automatically scan and match the wireless settings.)
<b>Auto Channel Scan:</b>	Click on the <b>Scan</b> button to search for available wireless networks, then click on the available network that you want to connect to.
<b>Remote AP MAC Address:</b>	Select Enable or Disable. Enabling this feature automatically selects the channel that will provide the best wireless performance.
<b>WDS Site Survey:</b>	Enter the MAC addresses of the APs in your network that will serve as bridges to wirelessly connect multiple networks.
<b>Authentication:</b>	<b>Open System</b> <b>Shared Key</b> <b>Open System/Shared Key</b> <b>WPA-Personal</b> <b>WPA2-Personal</b> <b>WPA-Auto-Personal</b>  Select <b>Open System</b> to communicate the key across the network. Select <b>Shared Key</b> to limit communication to only those devices that share the same WEP settings. Select <b>Open System/Shared Key</b> to allow either form of data encryption. Select <b>WPA-Personal</b> , <b>WPA2-Personal</b> , or <b>WPA-Auto-Personal</b> to secure your network using a password and dynamic key changes (no RADIUS server required).

## Home > Basic Settings > Wireless > WDS mode



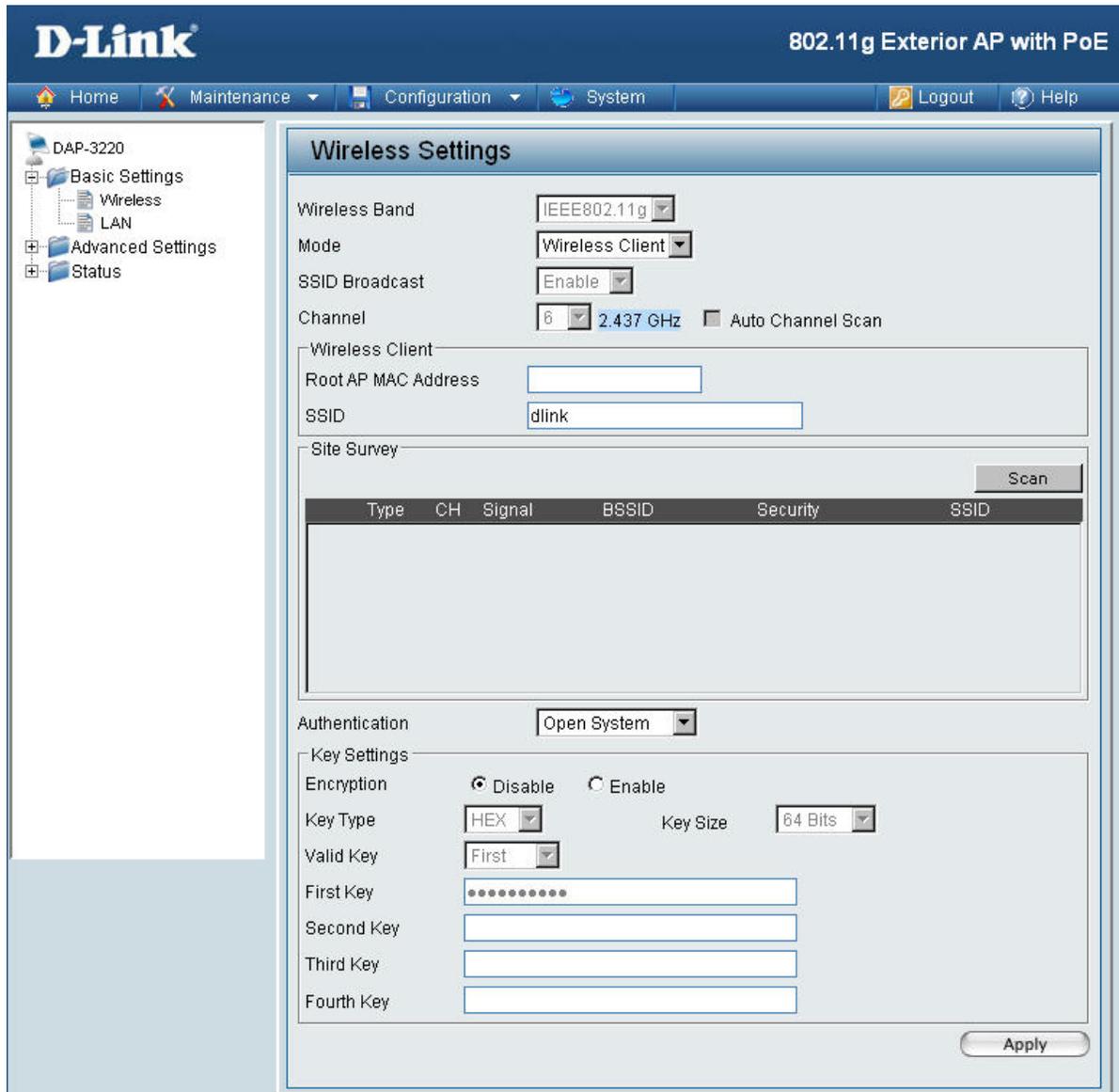
In WDS mode, the DAP-3220 wirelessly connects multiple networks, without functioning as a wireless AP.

- Wireless Band:** 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.
- SSID Broadcast:** Enable or Disable SSID broadcast. Enabling this feature broadcasts the SSID across the network.

---

<b>Channel:</b>	<b>6</b> is the default channel. All devices on the network must share the same channel.
<b>Auto Channel Scan:</b>	Select <b>Enable</b> or <b>Disable</b> . Enabling this feature automatically selects the channel that will provide the best wireless performance.
<b>Remote AP MAC Address:</b>	Enter the MAC addresses of the APs in your network that will serve as bridges to wirelessly connect multiple networks.
<b>WDS Site Survey:</b>	Click on the <b>Scan</b> button to search for available wireless networks, then click on the available network that you want to connect with.
<b>Authentication:</b>	<b>Open System</b> <b>Shared Key</b> <b>Open System/Shared Key</b> <b>WPA-Personal</b> <b>WPA2-Personal</b> <b>WPA-Auto-Personal</b>  Select <b>Open System</b> to communicate the key across the network. Select <b>Shared Key</b> to limit communication to only those devices that share the same WEP settings. Select <b>Open System/Shared Key</b> to allow either form of data encryption. Select <b>WPA-Personal</b> , <b>WPA2-Personal</b> , or <b>WPA-Auto-Personal</b> to secure your network using a password and dynamic key changes. dynamic key changes (no RADIUS server required).

# Home > Basic Settings > Wireless > Wireless Client mode



**Wireless Band:** IEEE 802.11g

**Mode:** Wireless client is selected from the pull-down menu.

**SSID Broadcast:** This option is unavailable in wireless client mode.

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

**Auto Channel Scan:** Select Enable or Disable. Enabling this feature automatically selects the channel that provides the best wireless performance.

**Root AP MAC Address:** Enter the MAC address of the AP in your network that will serve as the root AP.

**Root AP SSID:** that will serve as the root AP.

**Authentication:** **Open System**  
**Shared Key**  
**WPA-Personal**  
**WPA2-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.

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

Select **WPA-Personal, WPA2-Personal, or WPA-Auto-Personal** to secure your network using a password and dynamic key changes.

(No RADIUS Server required).

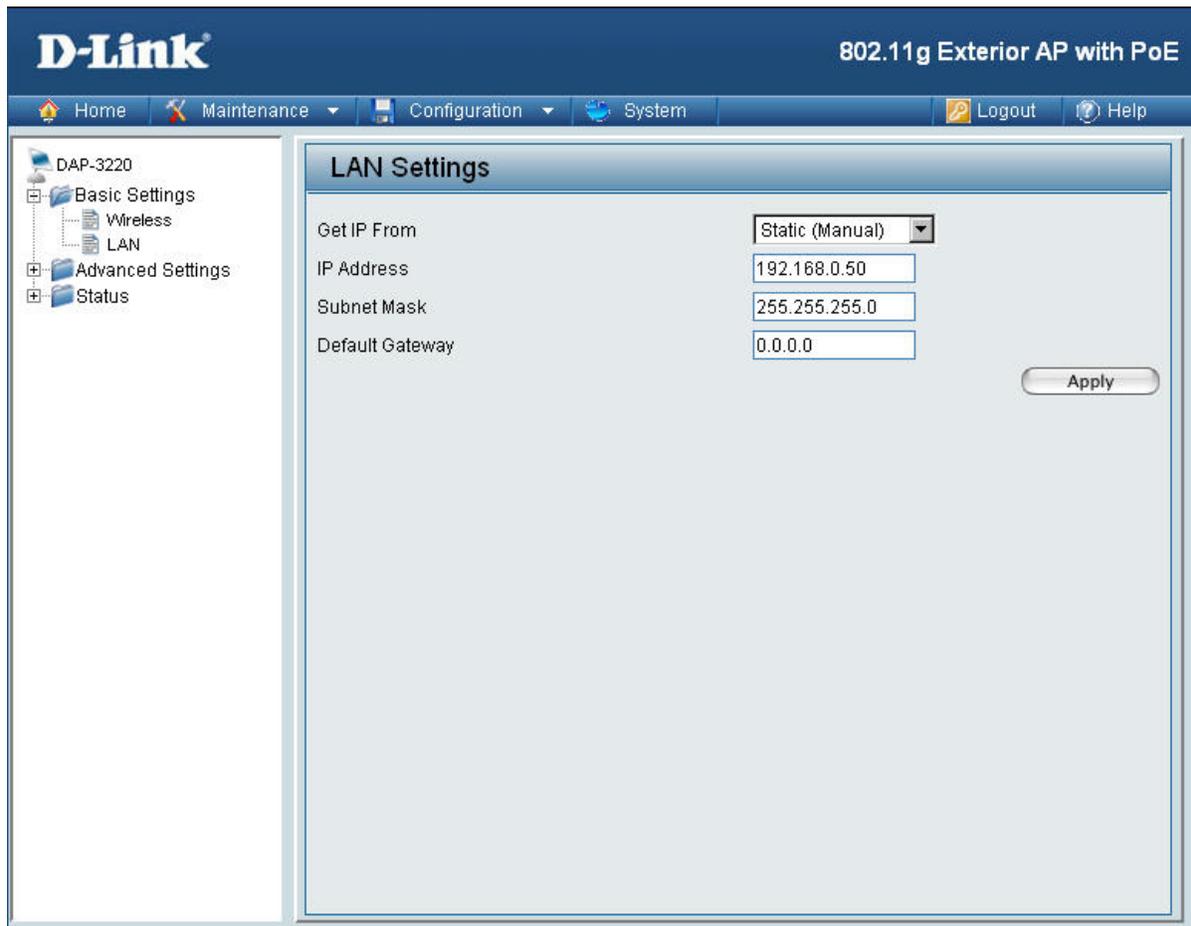
The **Data Rates** are Auto, 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 9Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps.

Beacons are packets sent by an access point to synchronize a network. Specify a beacon interval value. The default (100) is recommended.

## Home > Wireless Modes

AP Mode	Authentication Available
Access Point	Open System Shared Key Open System/Shared Key WPA-Enterprise WPA-Personal WPA2-Enterprise WPA2-Personal WPA-Auto-Enterprise WPA-Auto-Personal
WDS with AP	Open System Shared Key Open System/Shared Key WPA-Personal WPA2-Personal WPA-Auto-Personal
WDS	Open System Shared Key Open System/Shared Key WPA-Personal WPA2-Personal WPA-Auto-Personal
Wireless Client	Open System Shared key WPA-Personal WPA2-Personal

## Home > Basic Settings > 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 DAP-3220. 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.

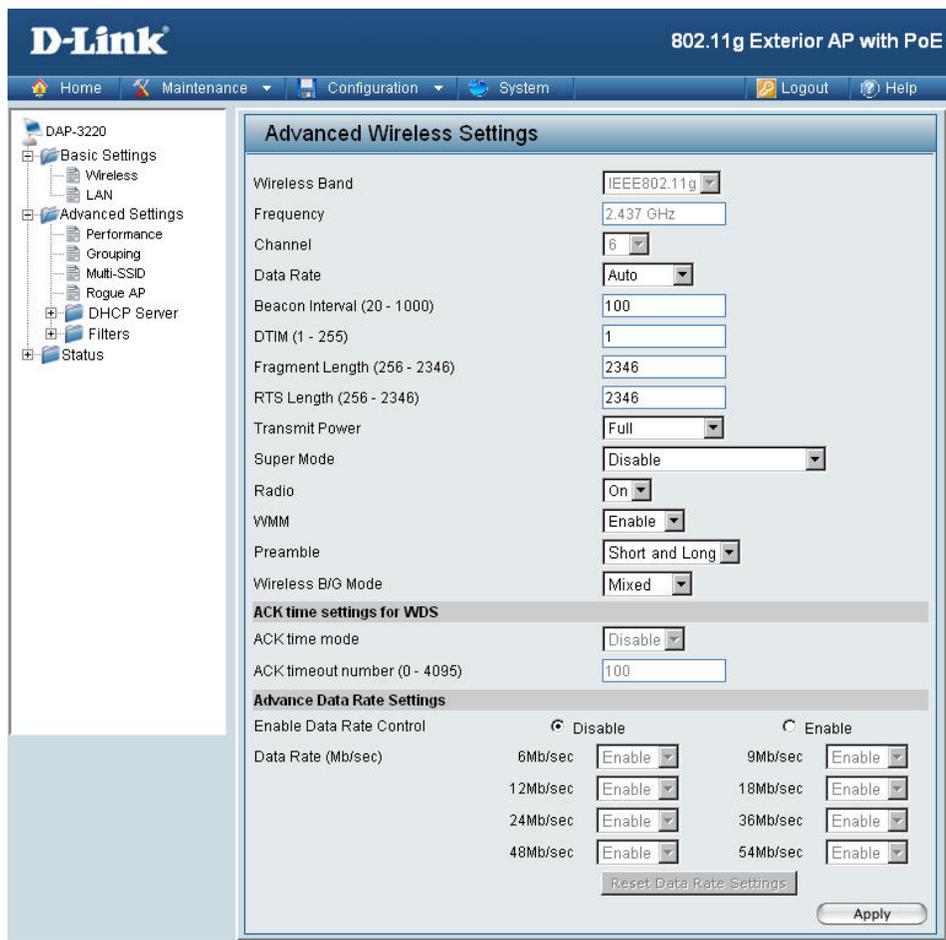
**Get IP From:** Static (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-3220. When DHCP is selected, the other fields here will be greyed out.

**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.

# Home > Advanced Settings > Performance



**Wireless Band:** IEEE 802.11g.

**Frequency:** The frequency reflects the choice of wireless channel. When IEEE 802.11g is chosen, the frequency is 2.437GHz for channel 6.

**Channel:** The default channel for IEEE 802.11g is 6.

**Data Rate\*:** The **Data Rates** are Auto, 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps.

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

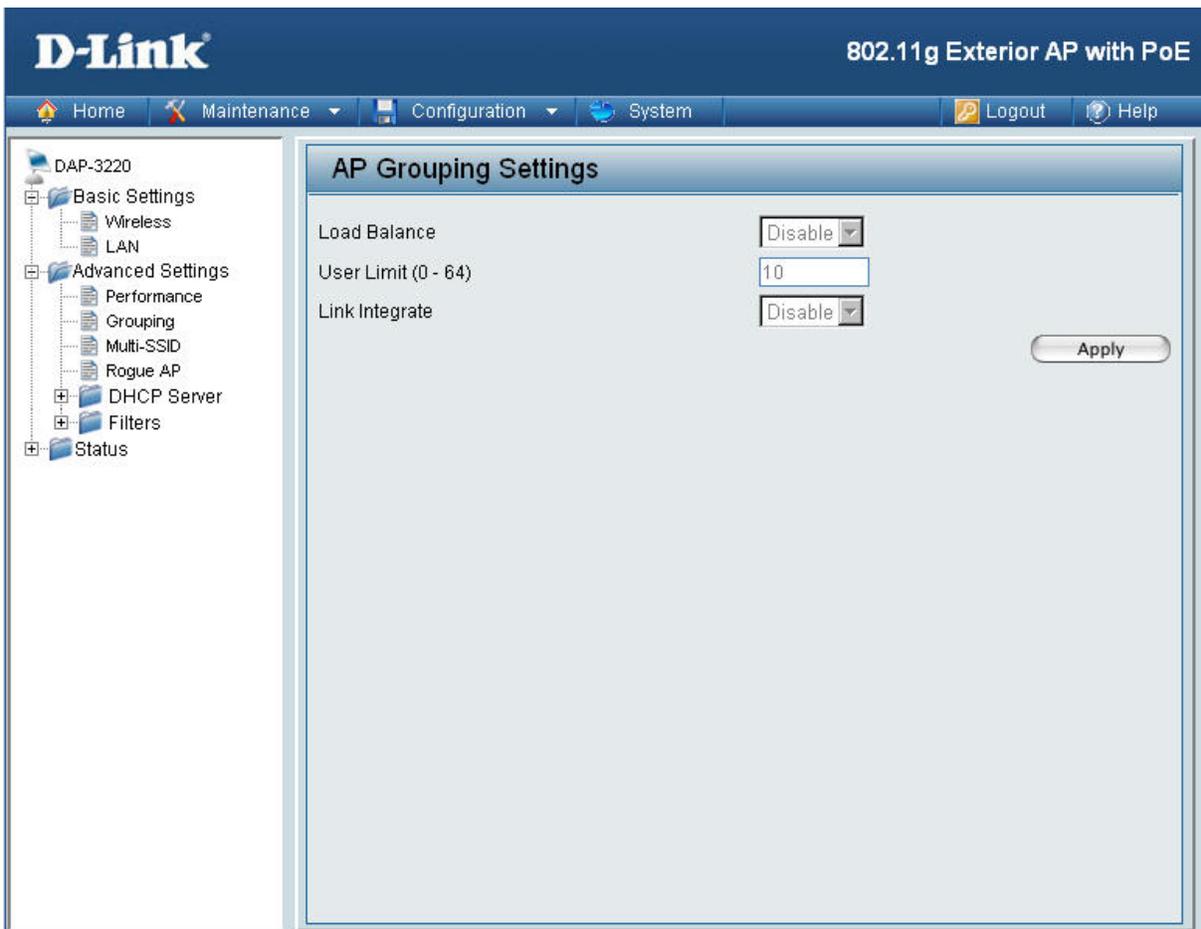
**DTIM:** (*Delivery Traffic Indication Message*) - Select a setting between 1 and 255. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

\*Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput may vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead can lower actual data throughput rate.

<b>Fragment Length:</b>	The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the setting of 2346 bytes will be fragmented before transmission. 2346 is the default setting.
<b>RTS Length:</b>	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.
<b>Transmit Power:</b>	Choose from full, half (-3dB), quarter (-6dB), eighth (-9dB), and minimum power.
<b>Super G Mode:</b>	<p>Super G is a set of performance enhancement features that increase end user application throughput in an 802.11g network, and is backwards compatible with standard 802.11g devices. For top performance, all wireless devices on the network should be Super G capable. Select either <b>Disabled</b>, <b>Super G without Turbo</b>, or <b>Super G with Dynamic Turbo</b>.</p> <p><b>Disabled:</b> Standard 802.11g support, no enhanced capabilities.</p> <p><b>Super G without Turbo:</b> Capable of packet bursting, FastFrames, and compression mode.</p> <p><b>Super G with Dynamic Turbo:</b> 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 G and have Dynamic Turbo enabled.</p>
<b>Radio:</b>	Select <b>On</b> or <b>Off</b> .
<b>WMM:</b>	Select <b>Enable</b> or <b>Disable</b> , <b>Disable</b> is selected by default. WMM stands for Wi-Fi Multimedia, by enabling this feature it will improve the user experience for audio and video applications over a Wi-Fi network.
<b>Preamble:</b>	Select the default value <b>Short and Long</b> , or <b>Long Only</b> .
<b>Wireless B/G Mode:</b>	This function allows you to configure the wireless network with IEEE 802.11g, IEEE 802.11b, or IEEE 802.11g with backward interoperability with IEEE 802.11b.
<b>Ack Ttime Mode:</b>	Select Enable or Disable.
<b>ACK Timeout</b>	Adjusting the ACK time value can improve the throughput when using WDS mode for long distance application. The default value is set to 100.

**Enable data rate control:** Specify the data rates at which the DAP-3220 should transmit signals. Choose from 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps.

## Home > Advanced Settings > Grouping



- Load Balance:** Allows you to balance and share the wireless network traffic and clients using multiple DAP-3220s. Select **Enable** or **Disable**.
- User Limit:** Sets the maximum amount of users that are allowed access (0-64 users).
- Link Integrate:** If the Ethernet connection between the LAN and the DAP-3220 is disconnected, the Link Integrate option will cause the wireless segment associated with the AP to be disconnected from the AP. Select **Enable** or **Disable**.

## Home > Advanced Settings > Multi-SSID

**D-Link** 802.11g Exterior AP with PoE

Home Maintenance Configuration System Logout Help

DAP-3220

- Basic Settings
  - Wireless
  - LAN
- Advanced Settings
  - Performance
  - Grouping
  - Multi-SSID
  - Rogue AP
  - DHCP Server
  - Filters
  - Status

### Multi-SSID Settings

Enable Multi-SSID     Enable VLAN State

**Wireless Settings**

Band: IEEE802.11g

Index: Primary SSID

SSID: dlink

SSID Broadcast: Enable

Security: None

VLAN ID: 1

WMM: Enable

**Key Settings**

Key Type: Hex

Key Size: 64 Bits

Key: 1 [Masked]

Apply

Index	SSID	Band	Encryption	VLAN ID	Delete

If you want to configure the Guest and Internal networks on Virtual LAN (VLAN), the switch and DHCP server you are using must also support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard.

**Enable Multi-SSID:** Check to enable Multi-SSID.

**Enable VLAN State:** Check to enable VLAN.

**Band:** IEEE802.11g is selected.

**Index:** You can select up to 7 multi-SSIDs. The default multi-SSIDs is the primary, which puts the total to 8 multi-SSIDs.

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

- Security:** The Multi-SSIDs security can be WPA/WPA2-Enterprise or WPA-Auto-Enterprise only when the Primary SSID's security is at the same security level. Also. They must also connect to the same RADIUS server.
- VLAN ID:** If you are enabling Guest access and configure Internal and Guest networks on the VLAN, this field will also be enabled.
- Provide a number between 1 and 4094 for the Internal VLAN.
- This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE802.1Q frames. The access point must be able to reach the DHCP server.
- Check with the Administrator in regards to VLAN and DHCP configurations.
- WMM:** Select Enable or Disable .
- Key Type:** Select **Hex** or **ASCII**.
- Key Size:** Select from **64-Bits**, **128-Bits**, and **152-Bits**.
- Key:** Select from the 1st to 4th key to be set as the active key

When Primary SSID is set to any of the following security levels:	Multi-SSID can use any of these security levels:
None Open System (WEP) Shared Key (WEP) WPA-Personal WPA2-Personal WPA-Auto-Personal	None Open System (WEP) Shared Key (WEP) WPA-Personal WPA2-Personal WPA-Auto-Personal
WPA-Enterprise WPA2-Enterprise WPA-Auto-Enterprise	None Open System (WEP) Shared Key (WEP) WPA-Personal WPA2-Personal WPA-Auto-Personal WPA-Enterprise WPA2-Enterprise WPA-Auto-Enterprise

Note: if WPA or WPA2 is being used, it will occupy the key spaces 2 and 3, leaving keys 1 and 4 for other SSIDs to use for WEP.

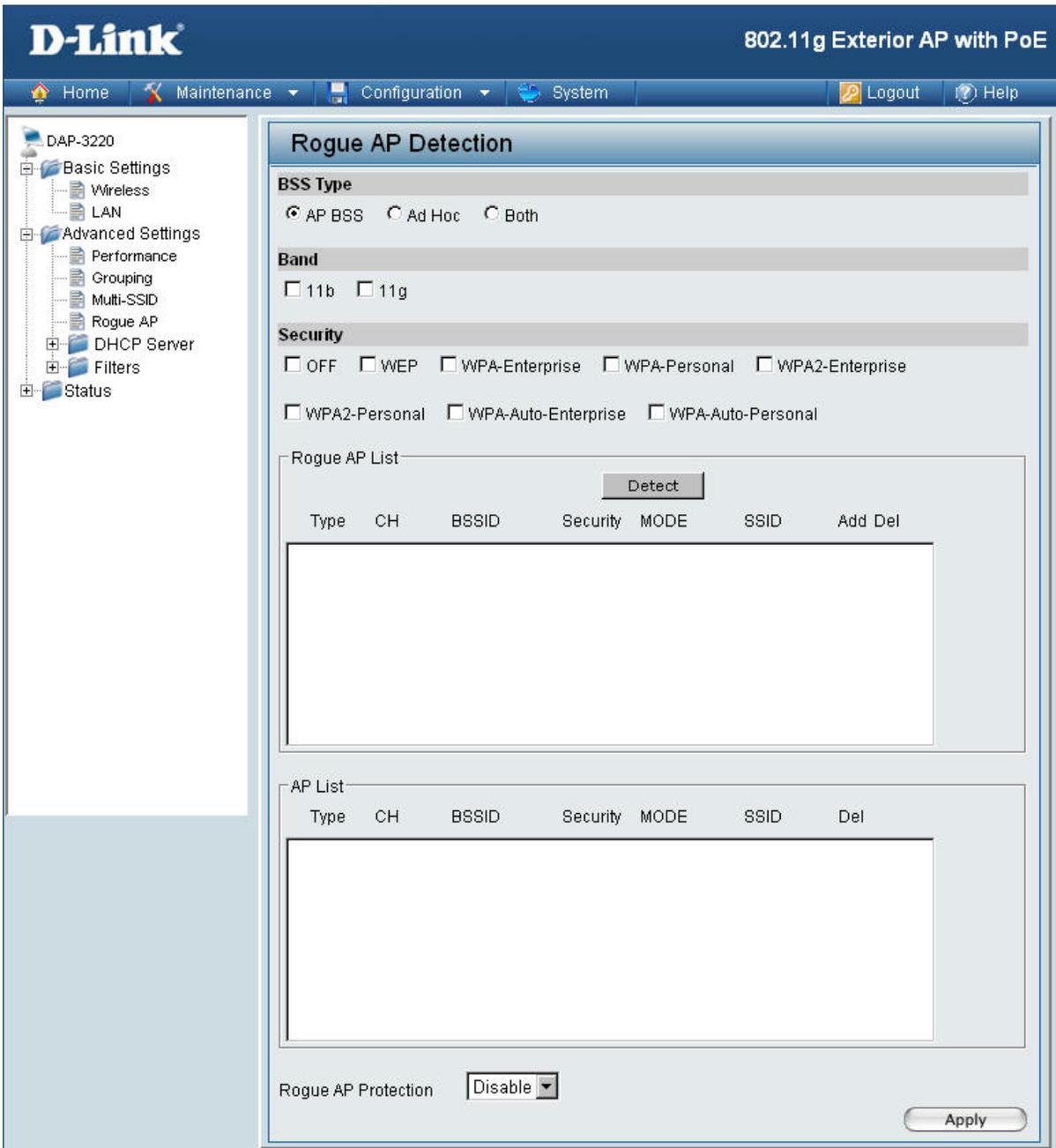
When configuring a Multi-SSID, you must click **Save to Table** and then click **Apply** to save your settings.

**Cipher Type:** When you select **WPA-Personal**, please select **AUTO**, **AES**, 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**, please enter a **PassPhrase** in the corresponding field.

# Home > Advanced Settings > Rogue AP



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

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

---

<b>Security:</b>	Select the Security types <b>OFF</b> , <b>WEP</b> , <b>WPA-Enterprise</b> , <b>WPA-Personal</b> , <b>WPA2-Enterprise</b> , <b>WPA2-Personal</b> , <b>WPA-Auto-Enterprise</b> , and <b>WPA-Auto-Personal</b> that you would like to include during AP detection.
<b>Rogue AP List:</b>	This window shows all of the neighbor APs detected based on your criteria listed above (BSS Type, Band, and Security). If the AP is in the same network, or if you know the AP, just click on “ <b>Add</b> ” to save it to the AP list.
<b>AP List:</b>	This window shows all of the APs that are allowed access on the network.
<b>Rogue AP Protection:</b>	Enable this function to keep the connection with the authorized clients even when there are rogue APs around.

## Home > Advanced Settings > DHCP Server > Dynamic Pool Settings

**D-Link** 802.11g Exterior AP with PoE

Home Maintenance Configuration System Logout Help

DAP-3220

- Basic Settings
  - Wireless
  - LAN
- Advanced Settings
  - Performance
  - Grouping
  - Multi-SSID
  - Rogue AP
  - DHCP Server
    - Dynamic Pool Setting
    - Static Pool Setting
    - Current IP Mapping L
- Filters
- Status

### DHCP Dynamic Pools

**DHCP Server Control**

Function Enable/Disable:

**Dynamic Pool Settings**

IP Assigned From:

The Range of Pool (1-255):

SubMask:

Gateway:

Wins:

DNS:

Domain Name:

Lease Time (60 - 31536000 sec):

Status:

Apply

**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 DAP-3220 to function as a DHCP server.

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

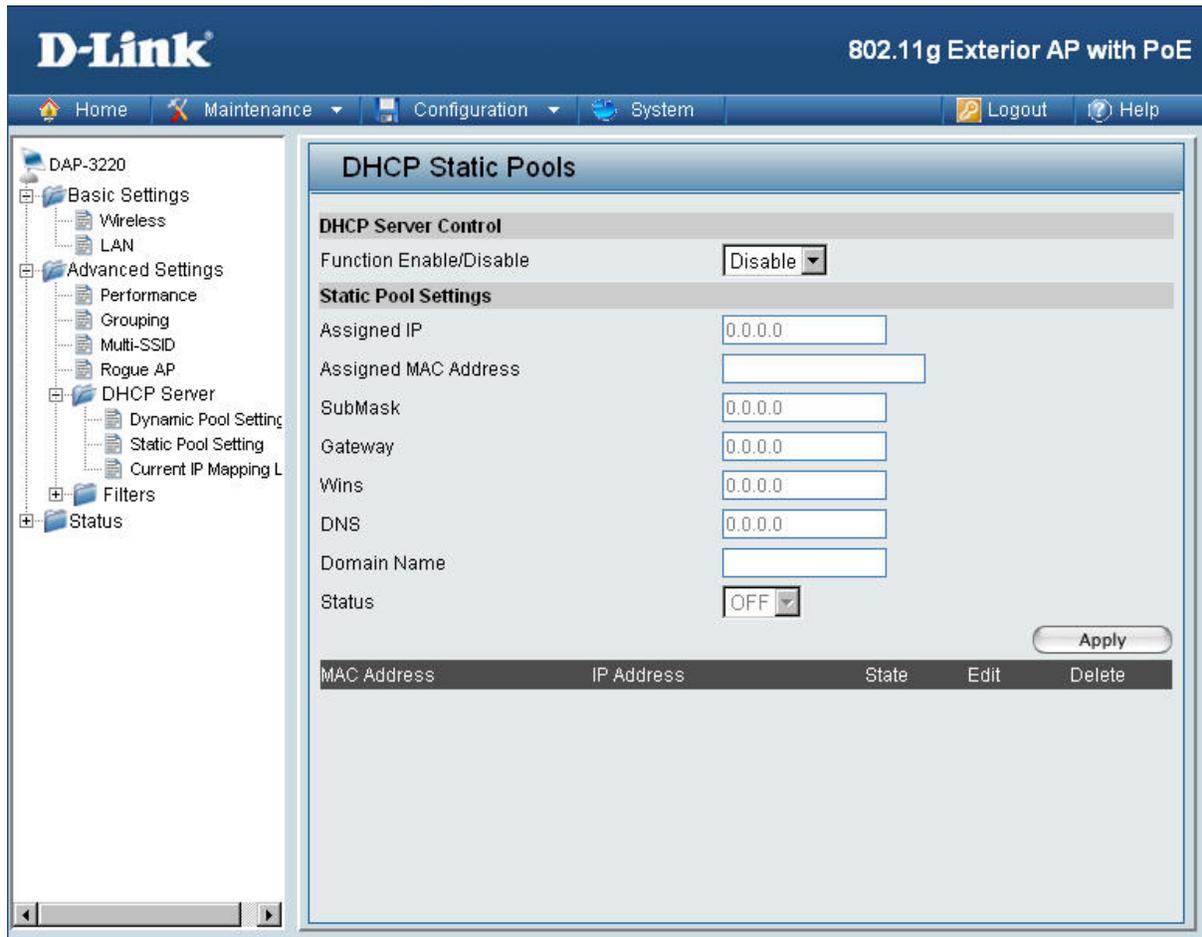
**The Range of Pool (1-255):** Enter the number of IP addresses available for assignment.

**SubMask:** All devices in the network must have the same subnet mask to communicate. Enter the submask for the network here.

---

<b>Gateway:</b>	Enter the IP address of the gateway on the network.
<b>WINS:</b>	<b>Windows Internet Naming Service</b> is a system that determines the IP address of a network computer that has a dynamically assigned IP address.
<b>DNS:</b>	Enter the IP address of the DNS server. The DNS (Domain Name Server) translates domain names such as www.dlink.com into IP addresses.
<b>Domain Name:</b>	Enter the domain name of the DAP-3220, if applicable. (An example of a domain name is: www.dlink.com.)
<b>Lease Time (60-31536000 sec.):</b>	The Lease Time is the period of time before the DHCP server will assign new IP addresses.
<b>Status:</b>	Turn the <b>Dynamic Pool Settings ON</b> or <b>OFF</b> here.

# Home > Advanced Settings > 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 DAP-3220 to function as a DHCP server.

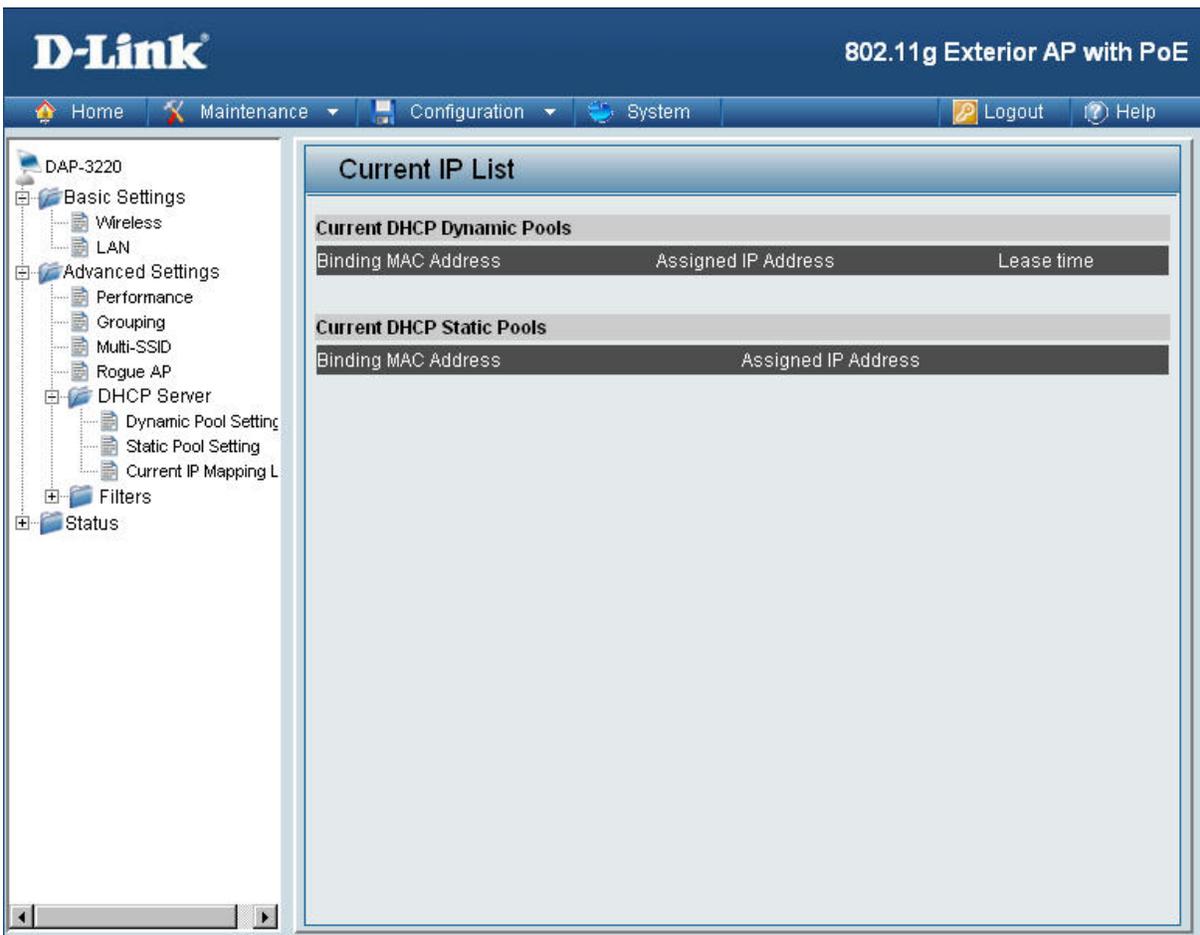
**Assigned IP:** Use the **Static Pool Settings** to assign the same IP address to a device every time you start up. The IP addresses assigned in the Static Pool list must NOT be in the same IP range as the Dynamic Pool. After you have assigned a static IP address to a device via its MAC address, click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

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

---

<b>SubMask:</b>	Enter the subnet mask here.
<b>WINS:</b>	Enter the IP address of the gateway on the network. <b>Windows Internet Naming Service</b> is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.
<b>DNS:</b>	Enter the IP address of the Domain Name Server, if applicable. The DNS translates domain names such as www.dlink.com into IP addresses.
<b>Domain Name:</b>	Enter the domain name of the DAP-3220, if applicable.
<b>Status:</b>	This option turns the Static Pool settings ON or OFF.

## Home > Advanced Settings > DHCP Server > Current IP Mapping List



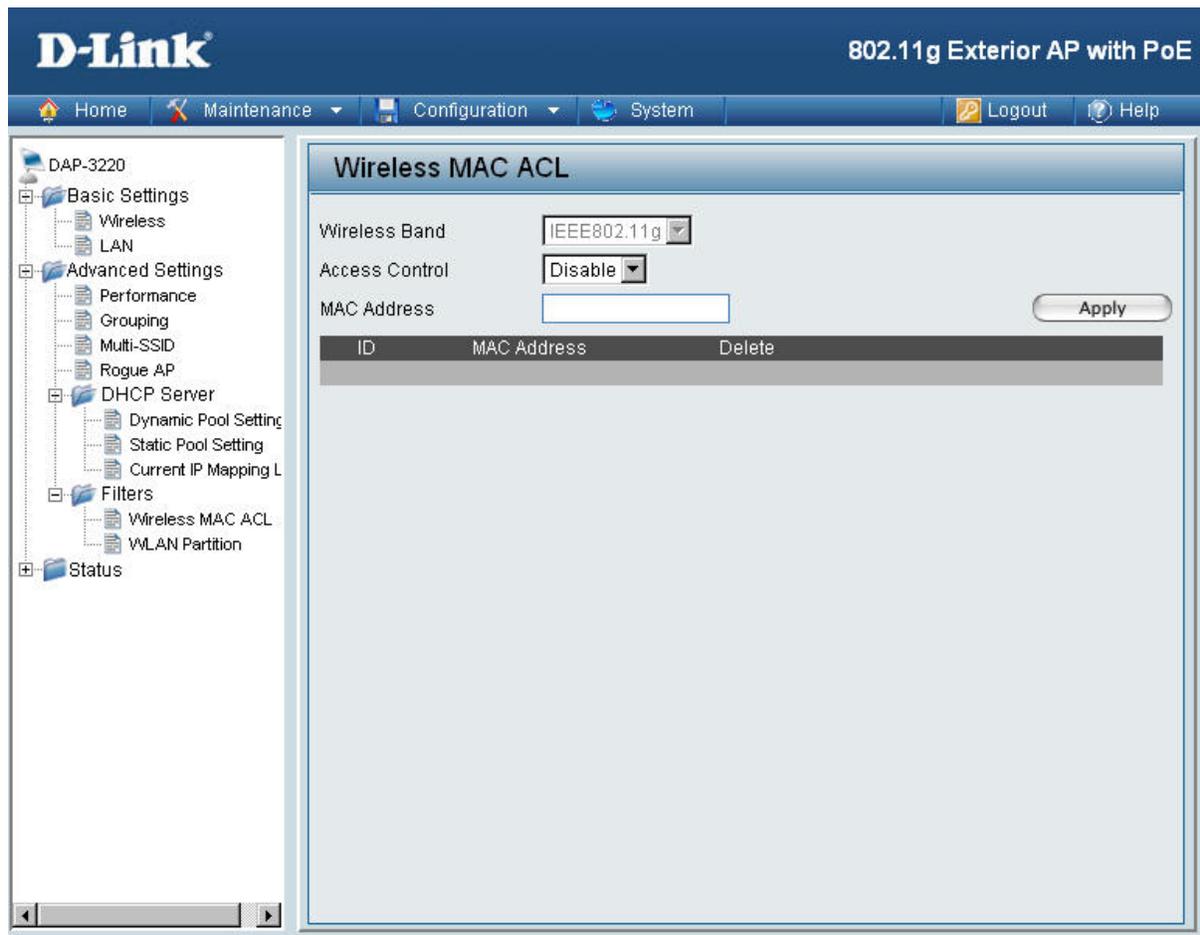
This screen displays information about the current DHCP dynamic and static IP address pools. This information is available when you enable the DHCP function of the DAP-3220 and assign dynamic and static IP address pools.

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

## Home > Advanced Settings > Filters > Wireless MAC ACL



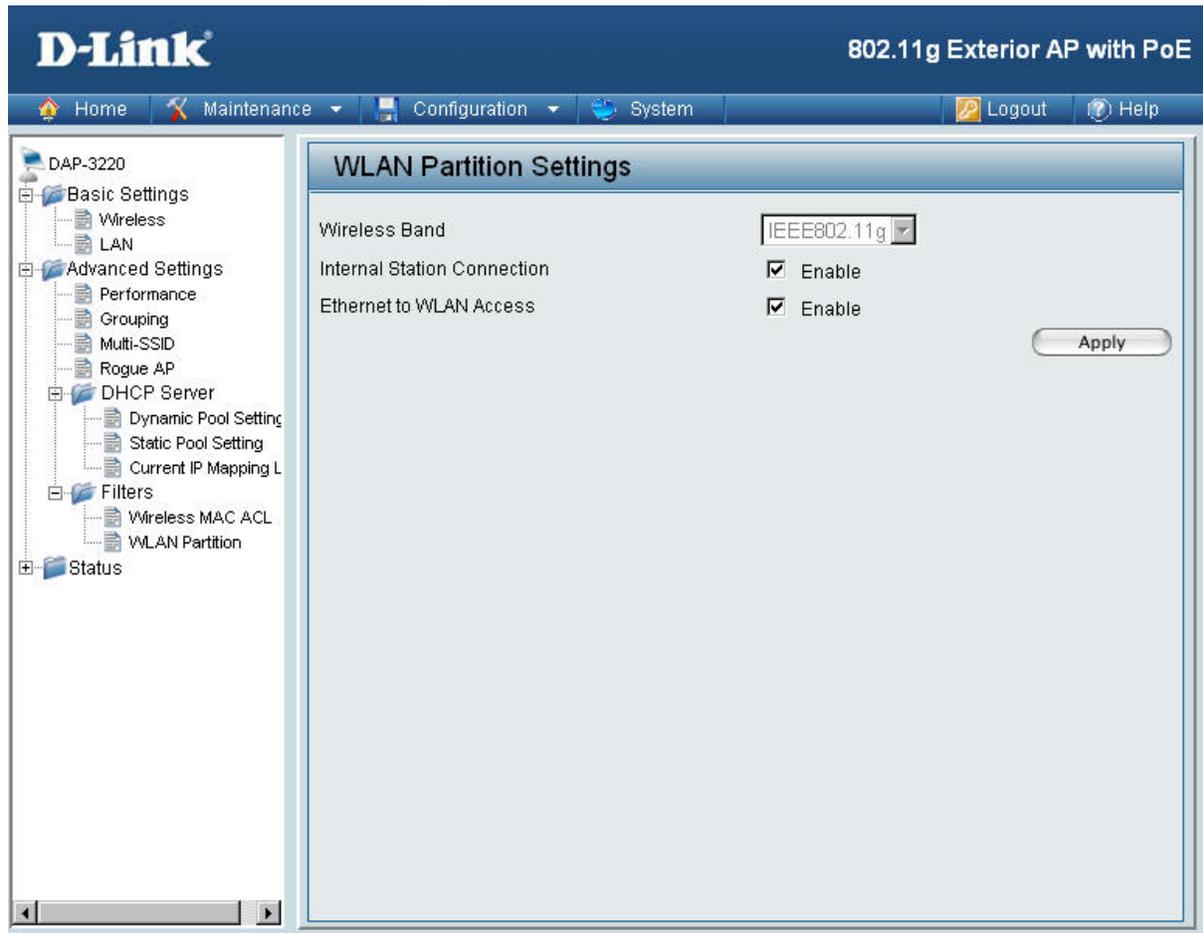
**Wireless Band:** IEEE 802.11g

**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 on the Access Control List.

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

**MAC Address List:** When you enter a MAC address, it appears in this list. Highlight a MAC address and click **Delete** to remove it appears on this list.

## Home > Advanced Settings > Filters > WLAN Partition

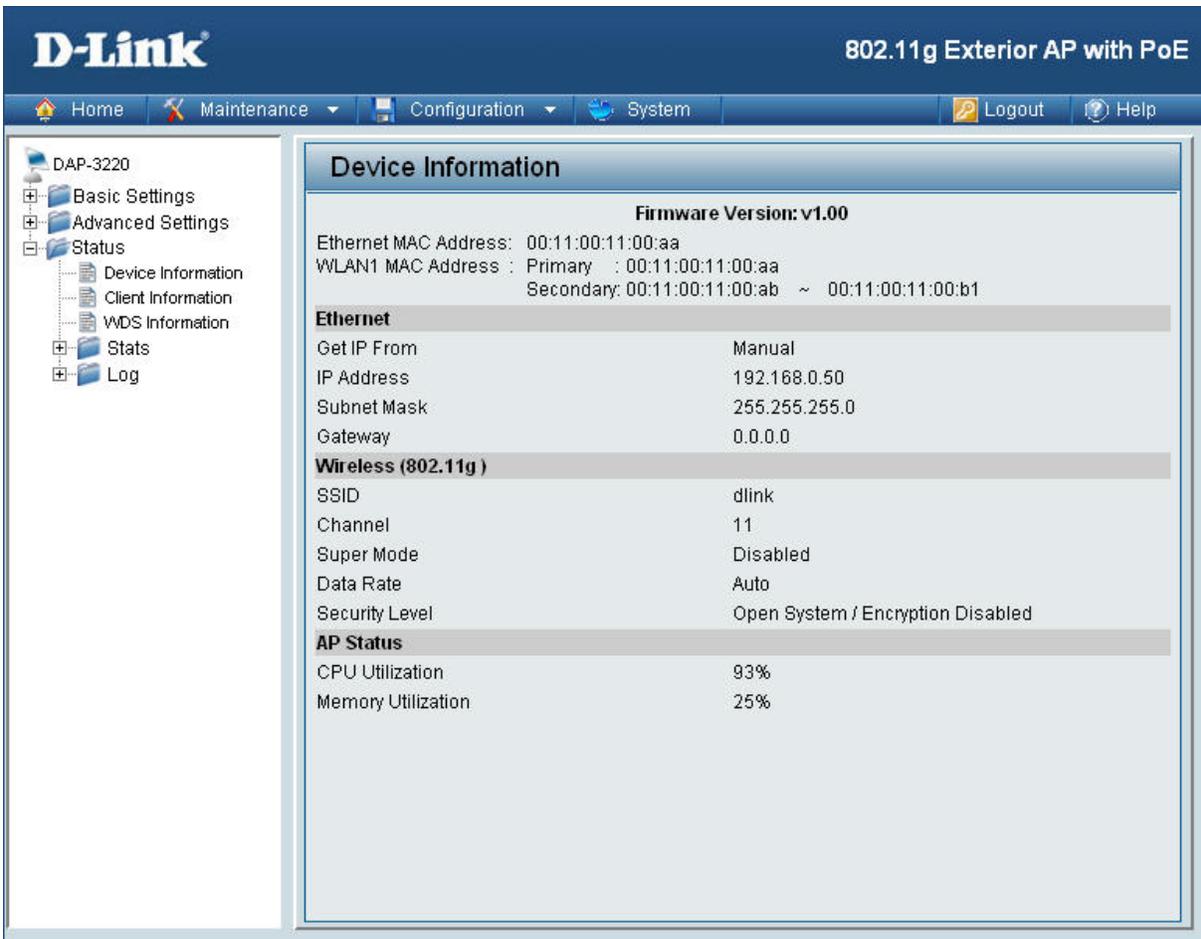


**Wireless Band:** IEEE 802.11g

**Internal Station Connection:** When connection is disabled, wireless stations of the selected band are unable to exchange data through the access point.

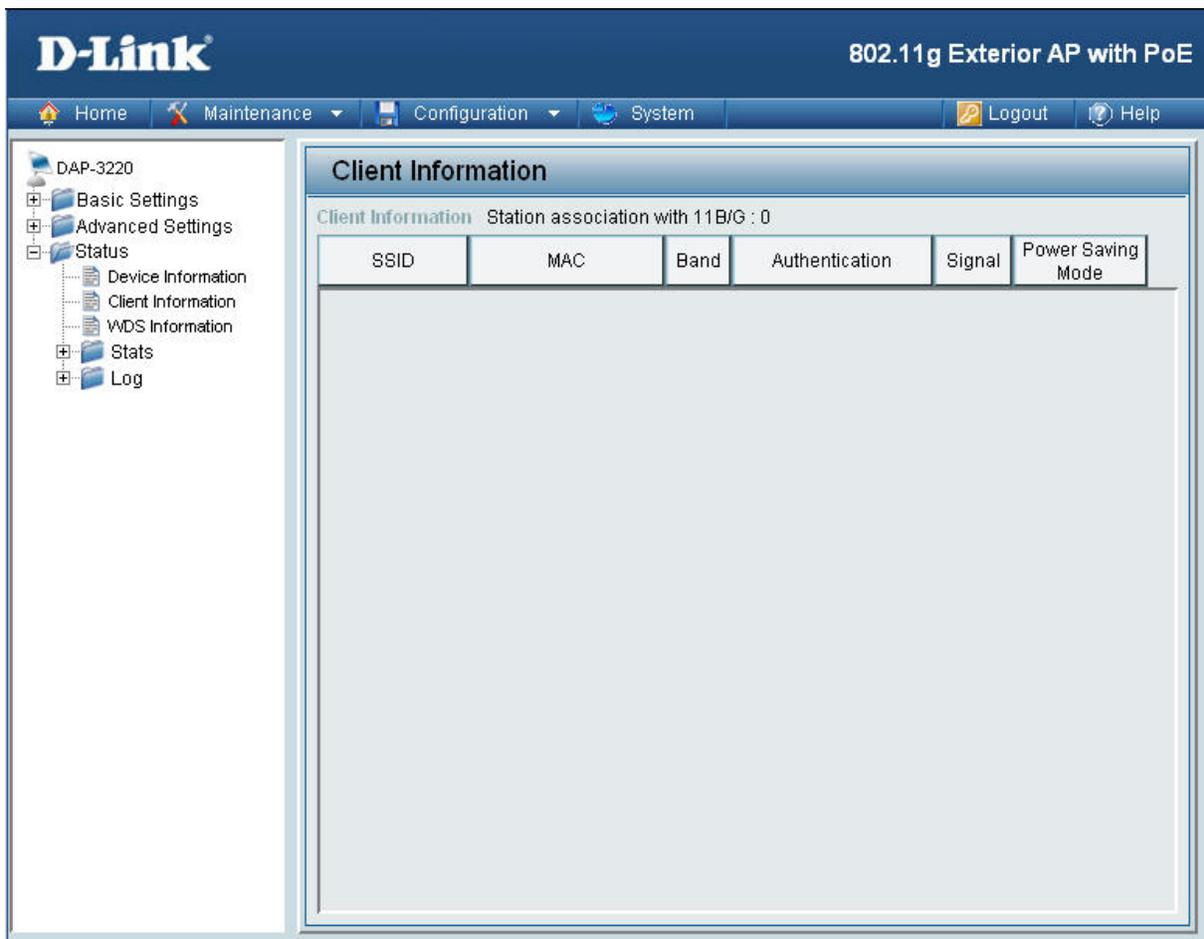
**Ethernet to WLAN Access:** When disabled, all data from the Ethernet to associated wireless devices will be blocked. Wireless devices can still send data to the Ethernet.

## Home > Status > Device Information



**Device Information:** This window displays the configuration settings of the DAP-3220, including the firmware version and the device's MAC address.

## Home > Status > Client Information



**Client Information:** This window displays the wireless client information for clients currently connected to the DAP-3220.

The following information is available for each client communicating with the DAP-3220.

**MAC:** Displays the MAC address of the client.

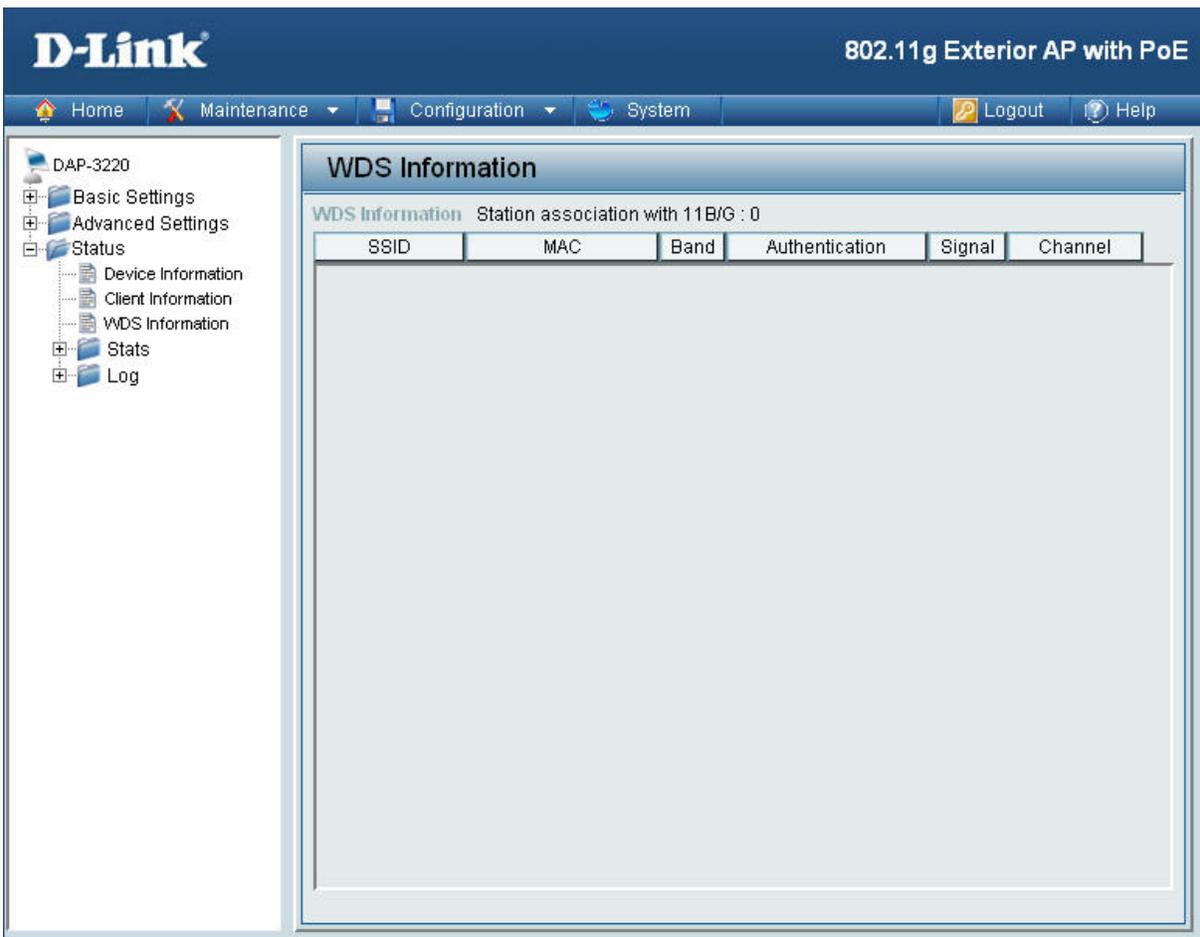
**Band:** Displays the wireless band that the client is connected to.

**Authentication:** Displays the type of authentication being used.

**Signal:** Displays the client's signal strength.

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

## Home > Status > WDS Information



**MAC:** Displays the MAC address of the client.

**Band:** Displays the wireless band that the client is connected to.

**Authentication:** Displays the type of authentication being used.

**Signal:** Displays the client's signal strength.

**Channel:** Displays the wireless channel being used

## Home > Status > Stats > Ethernet

The screenshot shows the D-Link web interface for a DAP-3220 device. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view with 'Status' expanded to 'Stats' and 'Ethernet' selected. The main content area is titled 'Ethernet Traffic Statistics' and contains a table with the following data:

Transmitted Count	
Transmitted Frame Count	1891
Transmitted Bytes Count	51104
Received Count	
Received Frame Count	1116
Received Bytes Count	68897

**Ethernet Traffic Statistics:** This page displays statistics both the transmitted and received count for frames and bytes.

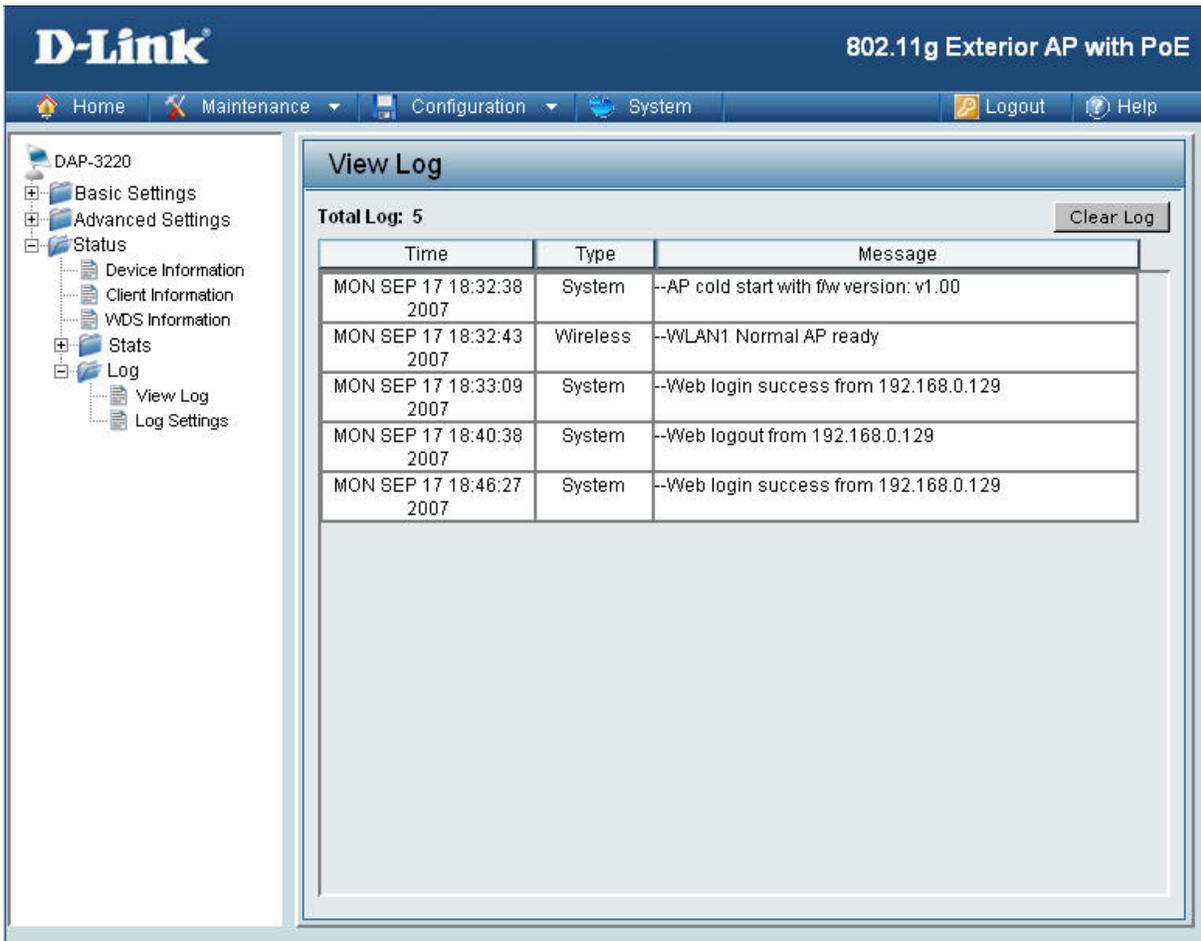
## Home > Status > Stats > WLAN802.11G

The screenshot shows the D-Link web interface for a DAP-3220 device. The page title is "802.11g Exterior AP with PoE". The navigation menu on the left includes: Home, Maintenance, Configuration, System, Logout, and Help. The main content area is titled "WLAN 802.11G Traffic Statistics" and contains a table of statistics. A "Refresh" button is located in the top right corner of the table area.

Throughput	
Transmit Success Rate	70 %
Transmit Retry Rate	0 %
Receive Success Rate	0 %
Receive Duplicate Rate	0 %
RTS Success Count	0
RTS Failure Count	5096
Transmitted Bytes Count	7808
Received Bytes Count	0
Transmitted Frame Count	
Transmitted Frame Count	366
Multicast Transmitted Frame Count	40
Transmitted Error Count	162
Transmitted Total Retry Count	0
Transmitted Multiple Retry Count	0
Received Frame Count	
Received Frame Count	0
Multicast Received Frame Count	0
Received Frame FCS Error Count	5096
Received Frame Duplicate Count	0
ACK RCV failure Count	1282
WEP Frame Error Count	
WEP Excluded Frame Count	0
WEP ICV Error Count	0

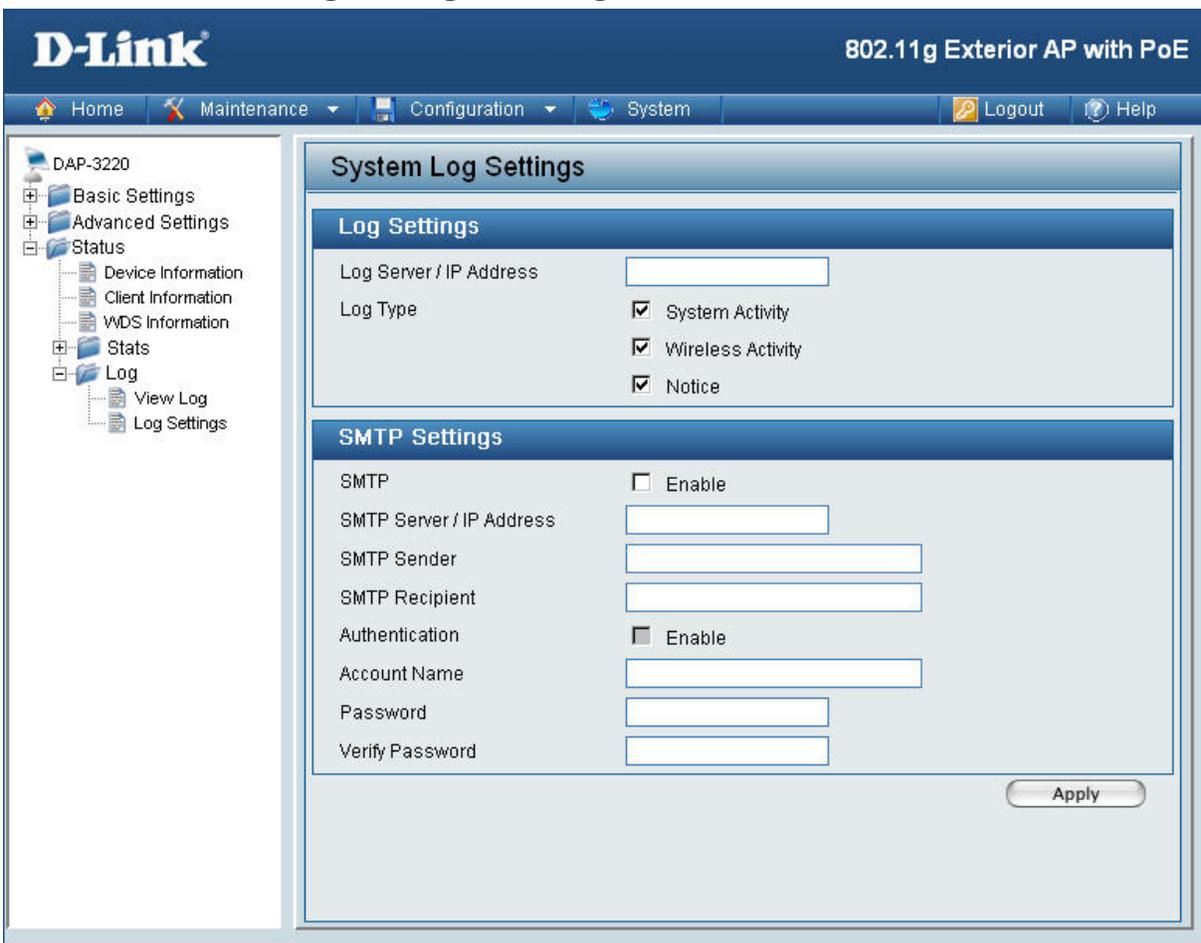
**WLAN 802.11g Traffic Statistics:** This page displays 802.11g wireless network statistics for data throughput, transmitted and received frames, and WEP frame errors.

# Home > Status > Log > View Log



**View Log:** The log displays system and network messages including a time stamp and message type.

## Home > Status > Log > Log Settings



- Log Server / IP Address:** Enter the IP address of the server you would like to send the DAP-3220s log to.
- Log Type:** Check the box for the type of activity you want to log. There are three types: **System**, **Wireless** and **Notice**.
- SMTP:** Check the box to enable SMTP.
- SMTP Server / IP Address:** Enter the IP address of the SMTP server.
- SMTP Sender:** Enter the e-mail address of the SMTP sender.
- SMTP Recipient:** Enter the e-mail address of the SMTP recipient.
- Authentication:** Check this box if your SMTP server requires authentication.
- Account Name:** Enter your account name for sending an e-mail.
- Password:** Re-enter the password associated with the account name in the Verify Password box.

## Maintenance > Administrator Settings

The screenshot shows the D-Link web interface for the 802.11g Exterior AP with PoE. The page is titled "Administrator Settings" and is part of the "Maintenance" menu. The interface includes a navigation sidebar on the left with options like "Basic Settings", "Wireless", "LAN", "Advanced Settings", and "Status". The main content area is divided into several sections:

- Limit Administrator IP:** Contains two checkboxes, "Limit Administrator IP 1" and "Limit Administrator IP 2", each followed by an input field for an IP address.
- Limit Administrator by vlan setting:** Contains a checkbox "Limit Administrator VID" followed by an input field for a VLAN ID.
- Login Settings:** Includes fields for "User Name" (default: admin), "Old Password", "New Password", and "Confirm New Password".
- Console Settings:** Includes a "Status" checkbox (checked), "Console Protocol" (radio buttons for Telnet and SSH), and a "Timeout" dropdown menu (set to 3 Mins).
- SNMP Settings:** Includes a "Status" checkbox (unchecked), "Public Community String" (default: public), "Private Community String" (default: private), "Trap Status" checkbox (unchecked), "Trap Server IP" (default: 0.0.0.0), and "Trap Type" (checkboxes for System Trap and Wireless Trap).

An "Apply" button is located at the bottom right of the configuration area.

**Limit Administrator IP:** Check the box to enable the feature.

**Limit Administrator IP 1:** Enter the IP address that the administrator will be allowed to log in from.

**Limit Administrator IP 2:** Enter a secondary IP address that the administrator will be allowed to log in from.

**Limit Administrator VID:** Enter the specific VLAN ID that the administrator will be allowed to log in from.

### Login Settings

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

**Old Password:** When changing your password, enter the old password here.

**New Password:** When changing your password, enter the new password here.

**Confirm New Password:** Confirm by re-entering your new password here.

### Console Settings

**Status:** Status is Enabled by default. Uncheck the box to disable the console.

**Console Protocol:** Select the type of protocol you would like to use, **Telnet** or **SSH**.

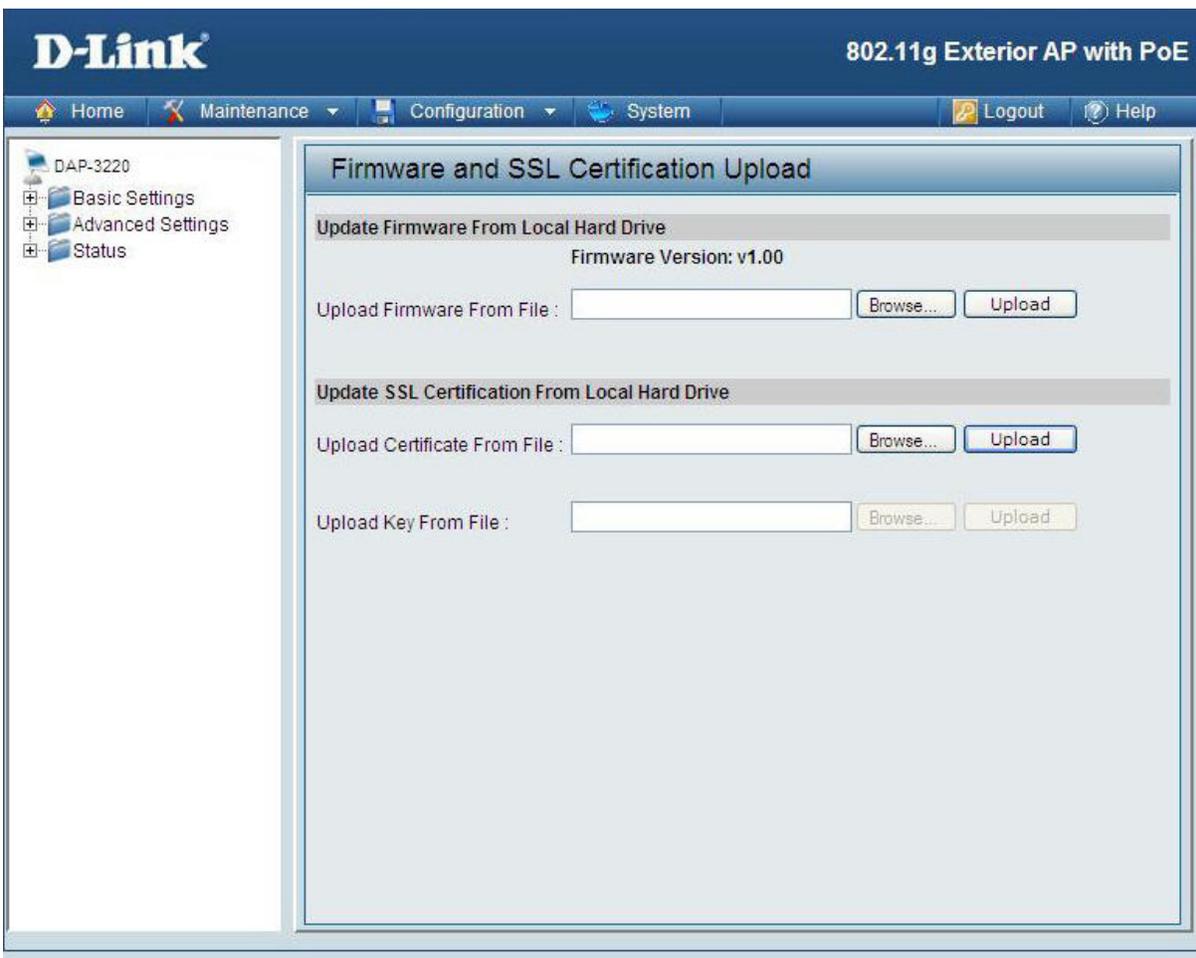
### SNMP Settings

**Status:** Status is Enabled by default. Uncheck the box to disable the SNMP functions.

**Public Community String:** Enter the public SNMP community string.

**Private Community String:** Enter the private SNMP community string.

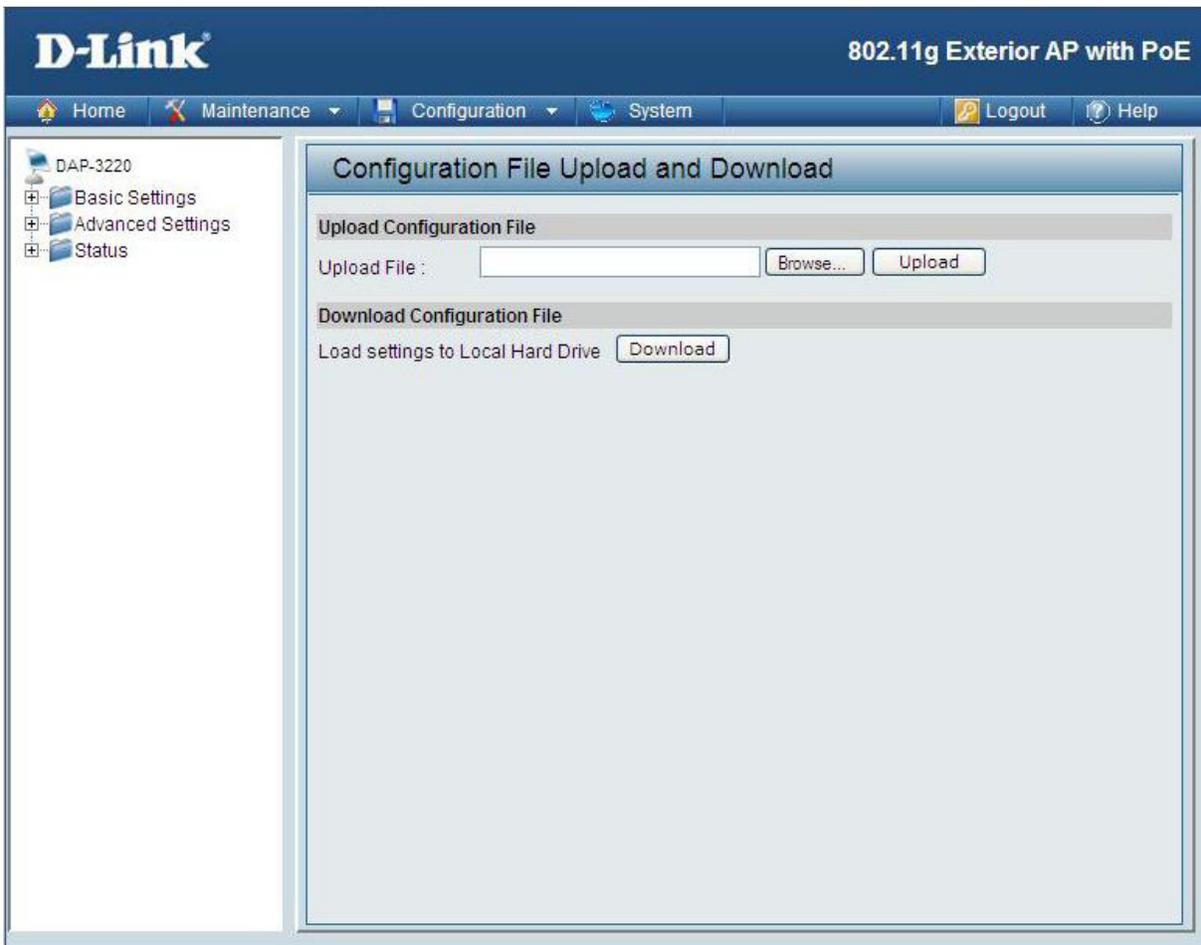
## Maintenance > Firmware and SSL Certification Upload



**Upload Firmware:** After downloading the most recent version of firmware for the DAP-3220 from <http://support.dlink.com> to your local computer, use the **Browse** button to locate the firmware file on your computer. Click **Upload** to update the firmware version.

**Upload SSL Certification:** Click **Browse** to locate the SSL Certification file on your local computer. After selecting and opening the file, click **Upload** to upload the file to the DAP-3220.

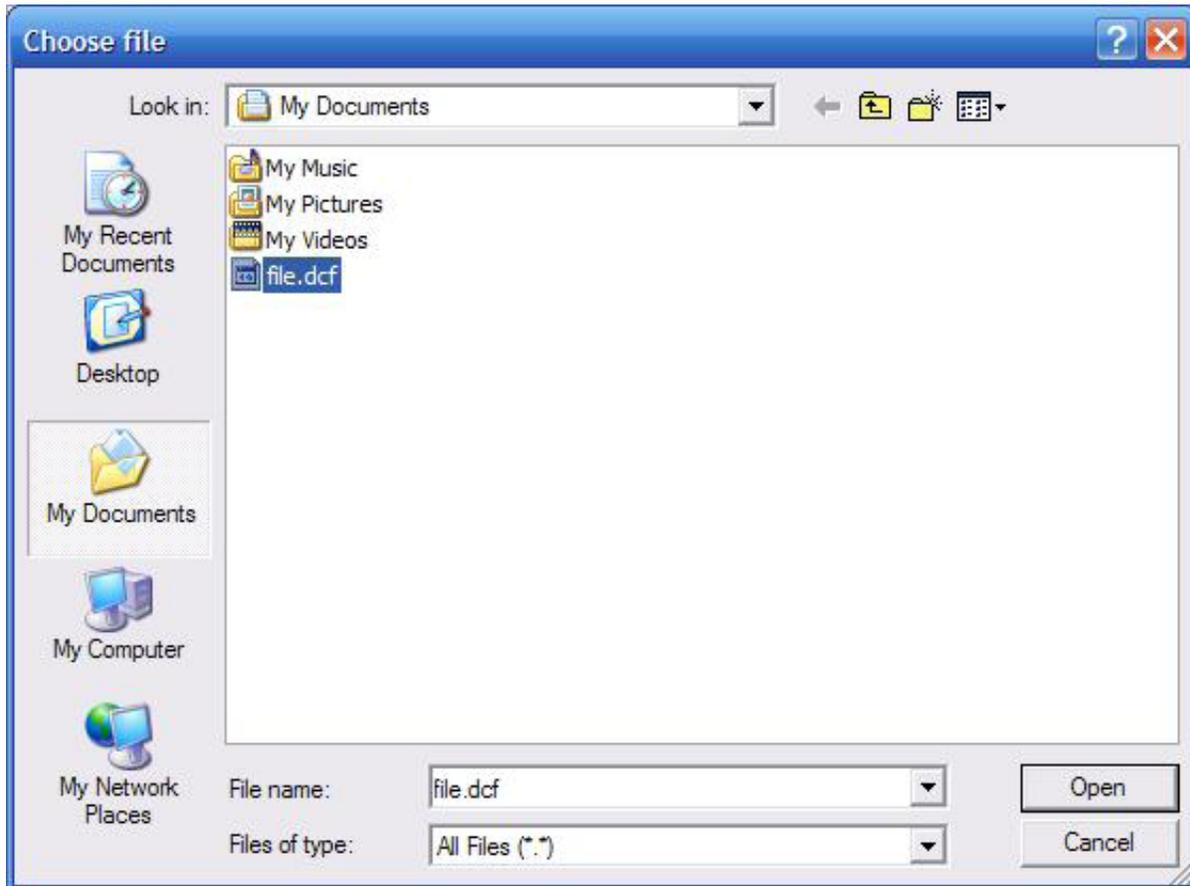
## Maintenance > Configuration File Upload and Download



**Upload File:** Click the **Browse** button to locate a previously saved configuration file on your local computer. After selecting the file, click **Upload** to apply the configuration settings to the DAP-3220.

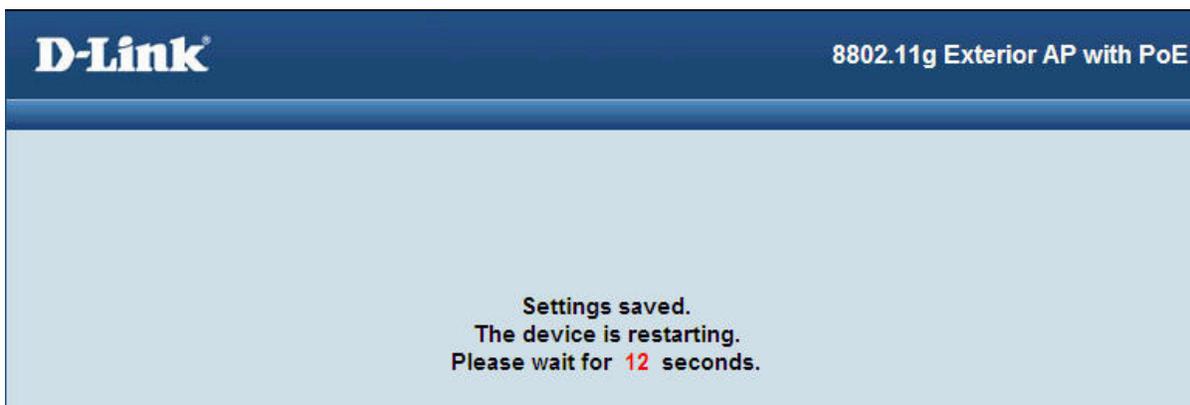
**Download Configuration File:** Click **Download** to save the current DAP-3220 configuration to your local computer.

## Maintenance > Cfg File > Choose file



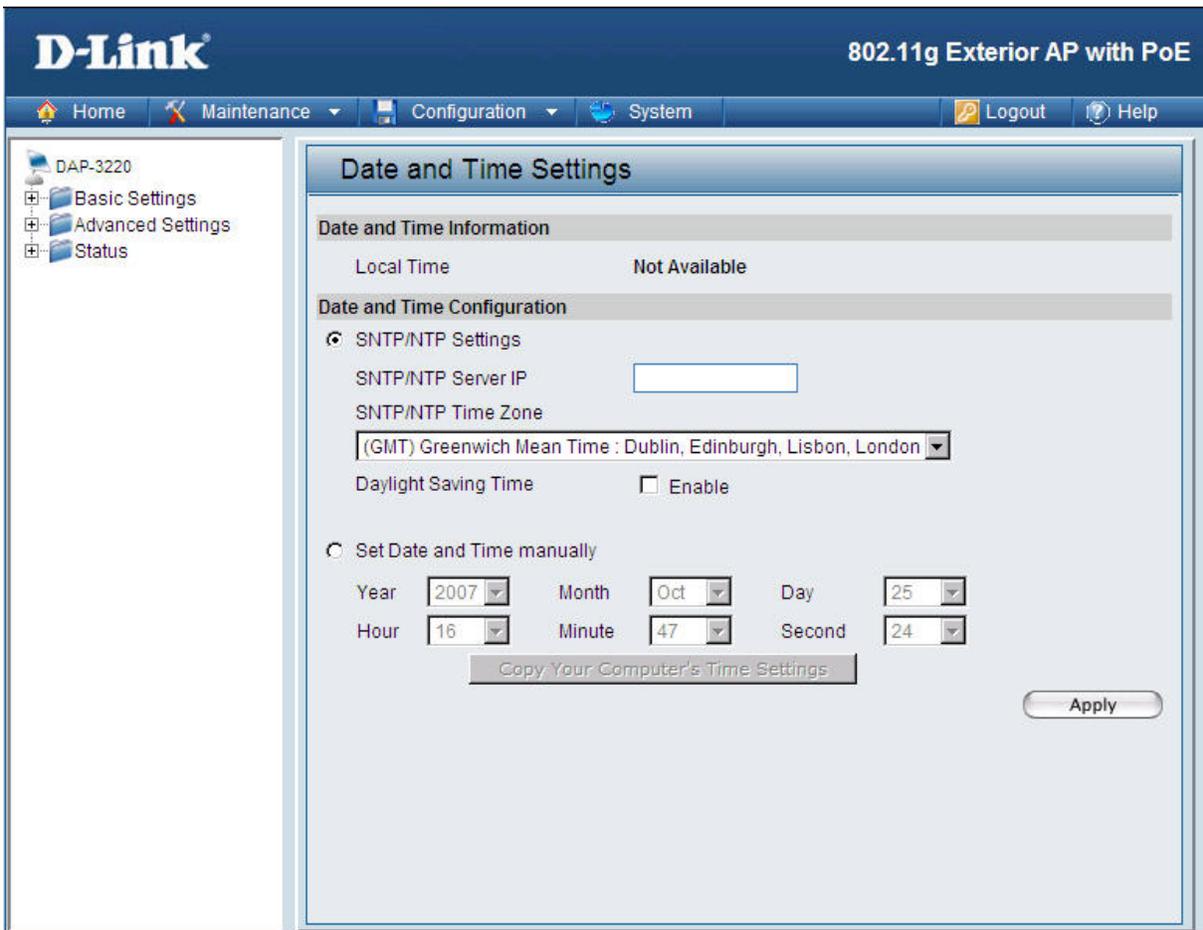
When you click **Browse** in the previous screen, the dialog box shown above appears.

Select the file you wish to download and click **Open**. Click **OK** to begin loading.



Click **Restart** for the settings to take effect. The dialog box above will appear as the device restarts. Please wait for a few seconds.

# Maintenance > Date and Time Settings



**SNTP/NTP Information:**

Displays the current SNTP/NTP settings.

**SNTP/NTP Server IP Address:**

Enter the SNTP/NTP server IP address.

**SNTP/NTP Time Zone:**

Select your correct Time Zone.

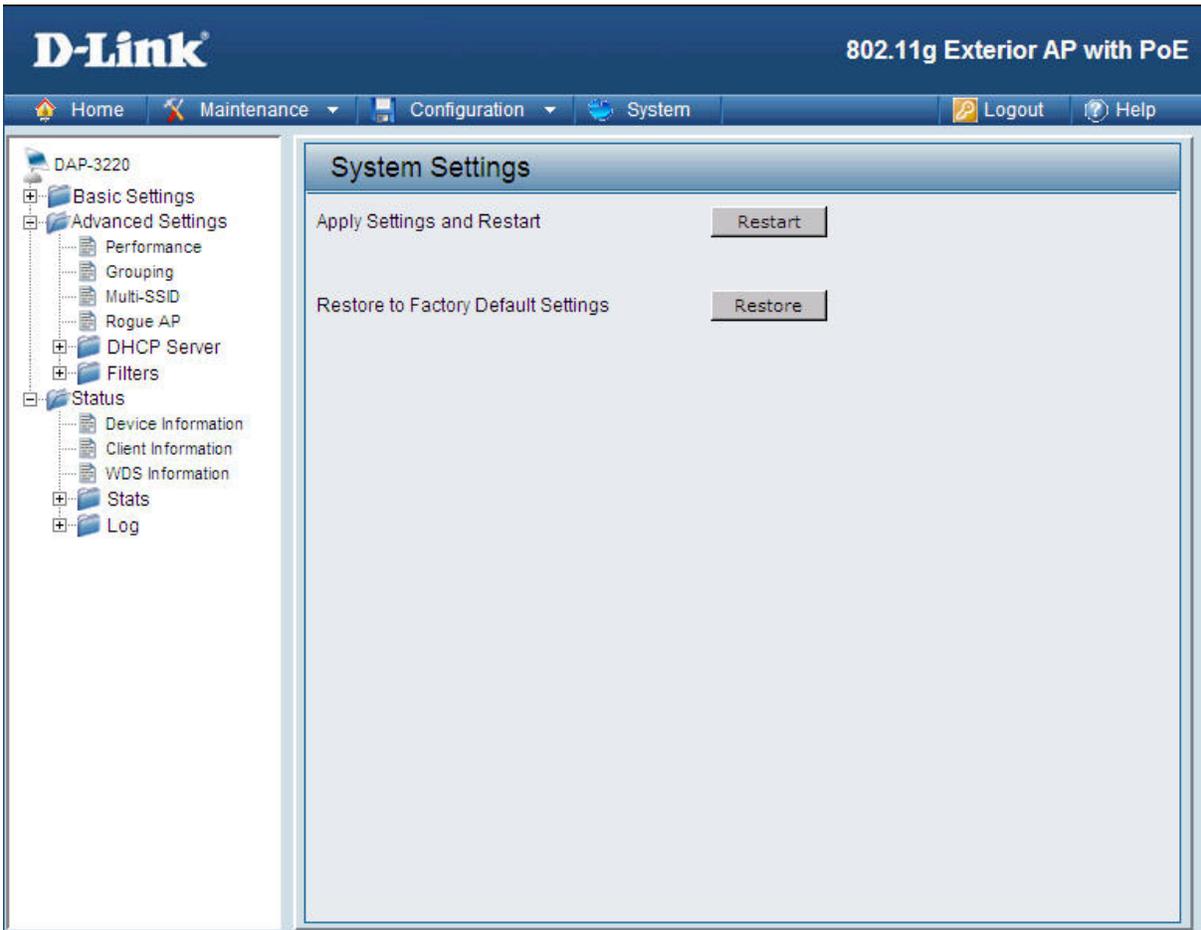
**Daylight Saving Time:**

Check the box to **Enable** Daylight Saving Time.

**Set Date and Time manually:**

You can either manually set the time for your AP here, or you can click the Copy Your Computer's Time Settings button to copy the time from the computer you are using (Make sure that the computer's time is set correctly).

## System > System Settings



Click **Restart** to restart the DAP-3220.

Click **Restore** to restore the DAP-3220 back to factory default settings.

# Help

## Home

### Advanced Settings

#### Performance

You can customize the network radio to fit your needs by tuning radio parameters in performance section. Performance functions are designed for advanced users who are familiar with 802.11 wireless networks and radio configuration.

#### Wireless Band

IEEE 802.11g is supported.

#### Frequency

The operation frequency display will change according to the channel selected.

#### Channel

By default, the AP is set to Auto Channel Scan. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

#### Data Rate

Indicate the base transfer rates based on the speed of wireless adapters on the wireless local area network (WLAN). The default value is set to "Auto" which adjusts the base transfer rate depending on the base rate of the connecting device.

#### 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)

DTIM Interval specifies the number of AP beacons between each Delivery Traffic Indication Message (DTIM). It informs associated stations of the next window for listening to broadcast and multicast messages. You can specify a DTIM value range from 1 to 255. The AP will send the next DTIM with specified DTIM value to stations if there is any buffered broadcast or multicast message. Stations hear the beacons and get ready to receive the broadcast or multicast messages. The default value for DTIM interval is 1.

#### Fragment Length (256-2346)

The default value is 2346 for fragmentation. By fragmenting packets into shorter fragments, the time spent on re-transmissions can be reduced if the packet error rate is high. However, unnecessary short fragment length will result in poor performance due to low transmission efficiency.

#### RTS Interval (1-2346)

The default value for request to send (RTS) threshold is 2346. With smaller RTS length value, the wireless network can recover from interference and collisions quicker since more RTS packets are transmitted. However, more RTS packets also consume more bandwidth, which leads to low throughput. Thus, small RTS Length value is only recommended for heavy loading network or high electromagnetic wireless interference.

**Help:** | Scroll down the Help page for topics and explanations.

# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-3220 Managed Wireless Access Point. We will cover various aspects of the network setup, especially the network adapters. Please read the following if you are having any technical difficulties.

Note: it is recommended that you use an Ethernet connection to **configure the DAP-3220**.

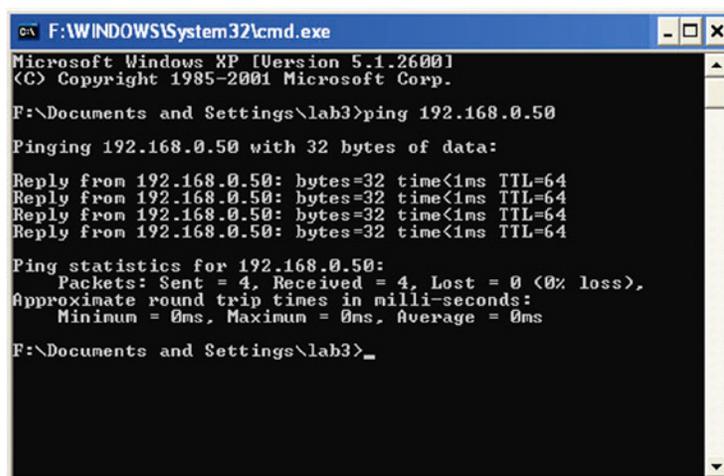
## 1. The computer used to configure the DAP-3220 cannot access the Configuration menu.

- Check if the **Ethernet LED** on the DAP-3220 is **ON**. If the **LED** is not **ON**, check if the cable for the Ethernet connection is securely inserted.
- Check if the Ethernet adapter is working properly. Please see item 3 of this **Troubleshooting** section to check that the drivers for the network adapters are loaded properly.
- Check if the IP address is in the same range and subnet as the DAP-3220. If it is not, please see **Checking the IP Address in Windows® XP** in the **Networking Basics** section of this manual.

Note: the IP address of the DAP-3220 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 DAP-3220 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 DAP-3220.



```
ca 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 within 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 DAP-3220 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; there may be no two devices with 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, then 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. 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 its wireless range. Please refer to the Installation Considerations in the Wireless Basics section of this manual for further information on placement of your D-Link wireless products to obtain best results.

### 4. Why does my wireless connection keep dropping?

- Antenna Orientation - try different antenna orientations for the DAP-3220. 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, or lights, your wireless connection will degrade dramatically or even drop. Try changing the channel of 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.

### 5. Why can't I get a wireless connection?

If you have enabled encryption on the DAP-3220, 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 cannot be established.
- Move the DAP-3220 and the wireless client into the same room and then test the wireless connection.
- Disable all security settings.
- Turn off your DAP-3220 and the client. Turn the DAP-3220 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, or lights, your wireless connection will degrade dramatically or drop altogether. Try changing the channel on your DAP-3220, 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.

# Technical Specifications

---

## Standards

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

## Network Management

- Web Browser interface
  - HTTP
  - Secure HTTP (HTTPS)
- AP Manager II
- SNMP Support
  - D-View Module
  - Private MIB
- Command Line Interface
  - Telnet
  - Secure SSH Telnet

## Data Rates\*

For 802.11g:

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

For 802.11b:

- 11, 5.5, 2, and 1Mbps

## Security

- WPA-Personal
- WPA-Enterprise
- WPA2-Personal
- WPA2-Enterprise
- 64/128/152-bit WEP
- SSID Broadcast Disable
- MAC Address Access Control List

## Wireless Frequency Range

- 2.4GHz to 2.4835GHz

## Operating Voltage

- 48VDC +/- 10% for PoE

## Radio and Modulation Type

For 802.11b:

DSSS:

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

\*Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput may vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead can lower actual data throughput rate.

For 802.11g:

OFDM:

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

DSSS:

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

Maximum Transmit Output Power

17dBm Typically

Receiver Sensitivity

For 802.11b, at 8% PER:

- 2Mbps: -89dBm
- 11Mbps: -83dBm

For 802.11g, at 10% PER:

- 6Mbps: -87dBm
- 9Mbps: -86dBm
- 12Mbps: -85dBm
- 18Mbps: -83dBm
- 24Mbps: -80dBm
- 36Mbps: -76dBm
- 48Mbps: -71dBm
- 54Mbps: -66dBm

Antenna

Embedded 9dBi patch antenna\*\*

LEDs

- Power
- LAN
- WLAN

Temperature

- Operating: -20°C to 60°C
- Storing: -20°C to 65°C

Humidity

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

Certifications

- FCC
- CE
- WiFi
- CSA
- IC
- C-Tick

Dimensions

- L = 10.93 inches (190mm)
- W = 6.10 inches (160mm)
- H = 1.77 inches (55mm)

\*\*DAP-3220 has one embedded panel antenna and one RP-N type connector for optional antenna use. You can only use one antenna at a time; it means if you want to use the optional antenna, the embedded antenna will be disabled automatically.

# 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 DLink 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 DLink 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. DLink 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 NONINFRINGEMENT.

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 NONCONFORMING 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 Corporation/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 ©2007 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.

**FCC Caution:**

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

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

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

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

**IMPORTANT NOTICE:****FCC Radiation Exposure Statement:**

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

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

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

**Industry Canada Notice:**

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

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

**IMPORTANT NOTE:**

**Radiation Exposure Statement:**

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

This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.