D-Link®
Building Networks for People

DAP-3520

Version I.I

*Air*Premier N

Dual Band Exterior PoE Access Point

User Manual

Business Class Networking

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
1.1	March 5, 2009	DAP-3520 Revision A1 with firmware version 1.10

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2009 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Table of Contents

Preface i
- Manual Revisions i
- Trademarks i

Product Overview 1
- Package Contents 1
- System Requirements 2
- Introduction 3
- Features 4
- Five Operational Modes 5
- Connecting PoE (Power over Ethernet) 6
- Hardware Overview 7
  - Connections 7

Configuration 8
- Web-based Configuration Utility 8
  - Wireless Settings 11
    - WDS with AP mode 13
    - WDS mode 15
    - Wireless Client Mode 17
    - WISP Client Router Mode 19
  - WEP Encryption 21
  - WPA-Personal Authentication 22
  - WPA-Enterprise Authentication 23
  - LAN 24
  - Advanced Settings 25
    - Performance 25
    - Multi-SSID 27
- VLAN 30
  - Port List 31
  - Add/Edit VLAN 32
  - PVID Setting 33
- Intrusion 34
- Schedule 35
- QoS 36
- DHCP Server 38
  - Dynamic Pool Settings 38
  - Static Pool Setting 40
  - Current IP Mapping List 42
- Filters 43
  - Wireless MAC ACL 43
  - WLAN Partition 44
- Router Settings 45
  - Parental Control 45
  - Advance Port Forwarding 46
  - MAC Filter 47
  - Firewall & DMZ 48
  - Advanced Network 49
- Status 50
  - Device Information 50
  - Client Information 51
  - WDS Information 52
- Stats 53
  - Ethernet 53
  - WLAN 54

Log 55
View Log 55
Log Settings 56
Maintenance 58
Administrator Settings 58
Limit Administrator 59
System Name Settings 60
Login Settings 61
Console Settings 62
SNMP Settings 63
Ping Control Setting 64
Firmware and SSL Certification Upload 65
Configuration File 66
Time and Date 67
System 68
System Settings 68
Help 69

Troubleshooting 70

Technical Specifications 73

Warranty 75

Technical Support 81

Registration 82

Package Contents

D-Link DAP-3520 Access Point		**Mounting Plate**	
Power Adapter with Power Cord		**Power over Ethernet Base Unit**	
4M Ethernet Cable		**Grounding Wire**	
CD-ROM		**Screws**	

Note: Using a power supply with a different voltage rating than the one included with the access point will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n-draft or 802.11g wireless clients • IEEE 802.11a wireless clients • 10/100/1000 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 7.0 or later • Firefox 3.0 or later • Chrome 1.0.154.36 or later **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	**Computer with the following:** • Windows® XP with Service Pack 2 or Vista • An installed Ethernet adapter • CD-ROM drive

Introduction

The DAP-3520 802.11a/n or b/g/n switchable AP increases productivity by allowing you to work faster and more efficiently. With the DAP-3520, bandwidth-intensive applications like graphics or multimedia will benefit significantly because large files are now able to move across the network quickly.

The DAP-3520 is capable of operating in one of five different wireless networking modes: access point, WDS (Wireless Distribution System) with AP, WDS, Wireless Client, or WISP (Wireless Internet Service Provider) Client Router mode.

Use less wiring, enjoy increased flexibility, save time and money with PoE (Power over Ethernet). With PoE, the DAP-3520 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 DAP-3520 provides data transfer rates up to 300Mbps*. (The 802.11n standard is backwards compatible with 802.11a, 802.11g, and 802.11b devices.)

* Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a and Draft 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Features

- **Faster Wireless Networking** - The DAP-3520 provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11n wireless router gives you the freedom of wireless networking at speeds 14x faster than 802.11g.

- **Compatible with 802.11a and 802.11g Devices** - The DAP-3520 is still fully compatible with the IEEE 802.11a/g standard, so it can connect with existing 802.11a/b/g PCI, USB and Cardbus adapters.

- **Five Different Operation Modes** - Capable of operating in one of five different operation modes to meet your wireless networking needs: **Access Point**, **WDS with AP**, **WDS**, **Wireless Client**, or **WISP Client Router**.

- **Better security with WPA** - The DAP-3520 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.

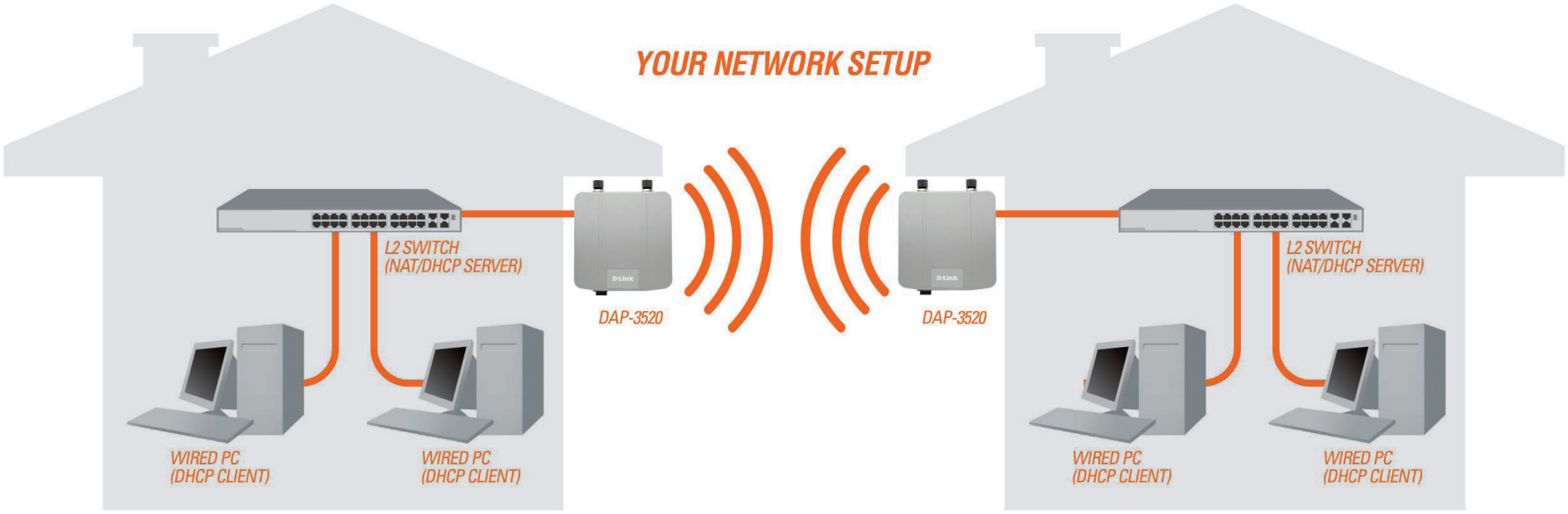
- **AP Manager II Management Software** - The real-time display of the network's topology and AP's information makes network configuration and management quick and simple.

- **SNMP for Management** - The DAP-3520 is not just fast, but also supports SNMP v.3 for better network management. Superior wireless AP manager software is bundled with the DAP-3520 for network configuration and firmware upgrade. Systems administrators can also set up the DAP-3520 easily with the Web-based configuration. A D-Link D-View 6.0 module will be downloadable for network administration and real-time network traffic monitoring with the D-View 6.0 software.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11g, and Draft 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

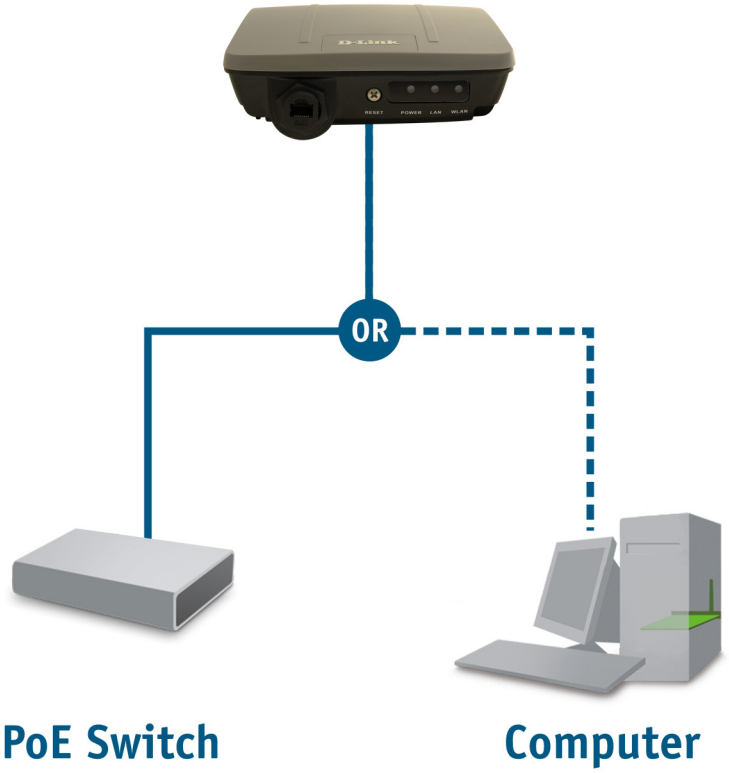
Five Operational Modes

Operation Mode (Only supports 1 mode at a time)	**Function**
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. See the diagram below.
Wireless Client	AP acts as a wireless network adapter for your Ethernet-enabled device
WISP Client Router	Transforms your wireless AP into a WISP Client router, which will get the Internet link wirelessly from your Wireless Internet Service Provider. In this mode, WAN is the wireless port and LAN is the wired port.



Example of a typical setup using WDS mode.

Connecting PoE (Power over Ethernet)



Connect one end of an Ethernet cable (included with your package) to the LAN port on the DAP-3520 and the other end of the Ethernet cable to either your computer or to your PoE switch. The AP can be powered on by a PoE switch or by the power adapter shipped with the AP.

Hardware Overview
Connections

LED	Color	Status	Description
Power	Green	Solid Green	The device is ready.
		Light Off	The device is powering off.
	Red	Blinking Red	The device is booting up.
LAN	Green	Solid Green	The link is up.
		Blinking Green	Data is being transmitted.
		Light Off	The link is down.
WLAN	Green	Solid Green	Wireless is ready.
		Blinking Green	Data is being transmitted.
		Light Off	Wireless is off.

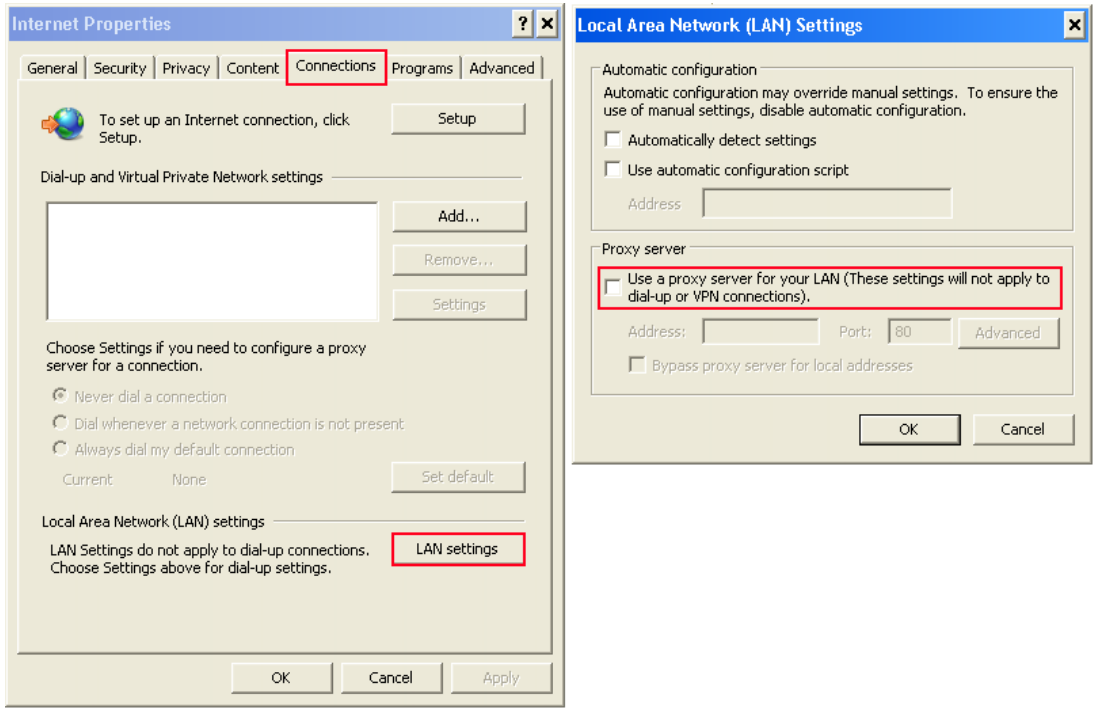
Configuration

This section will show you how to configure your D-Link wireless access point using the web-based configuration utility. If you would like to use the AP Manager II software, please refer to the documentation located on the D-Link CD.

Web-based Configuration Utility

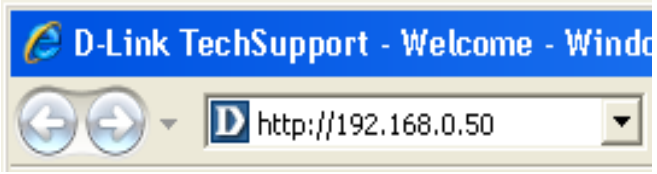
To configure the DAP-3520, use a computer which is connected to the DAP-3520 with an Ethernet cable (see the Network Layout diagram).

First, disable the option of accessing 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. Click **OK**.



Start your web browser (Internet Explorer, Mozilla Firefox).

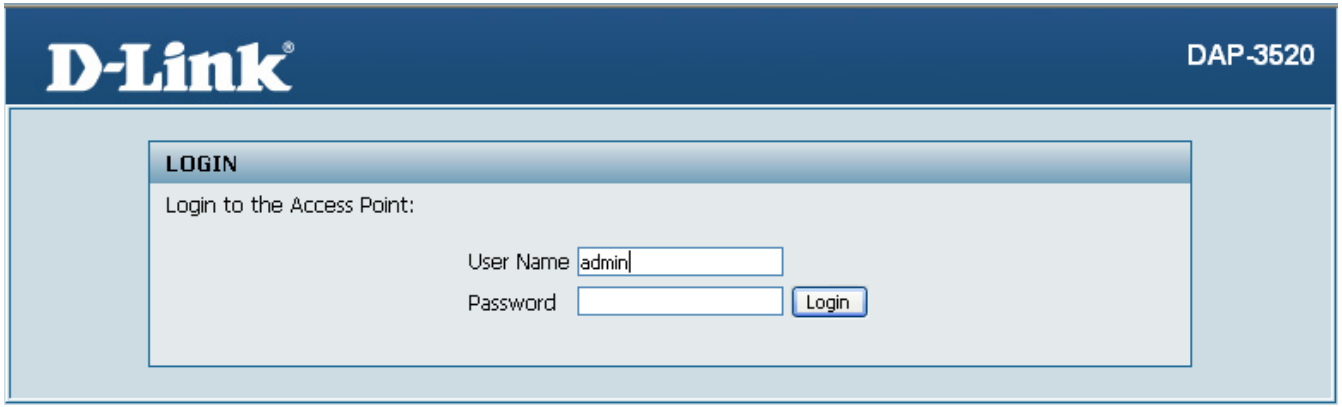
Type the IP address of the DAP-3520 in the address field (**http://192.168.0.50**) and press **Enter**. Make sure that the IP addresses of the DAP-3520 and your computer are in the same subnet.



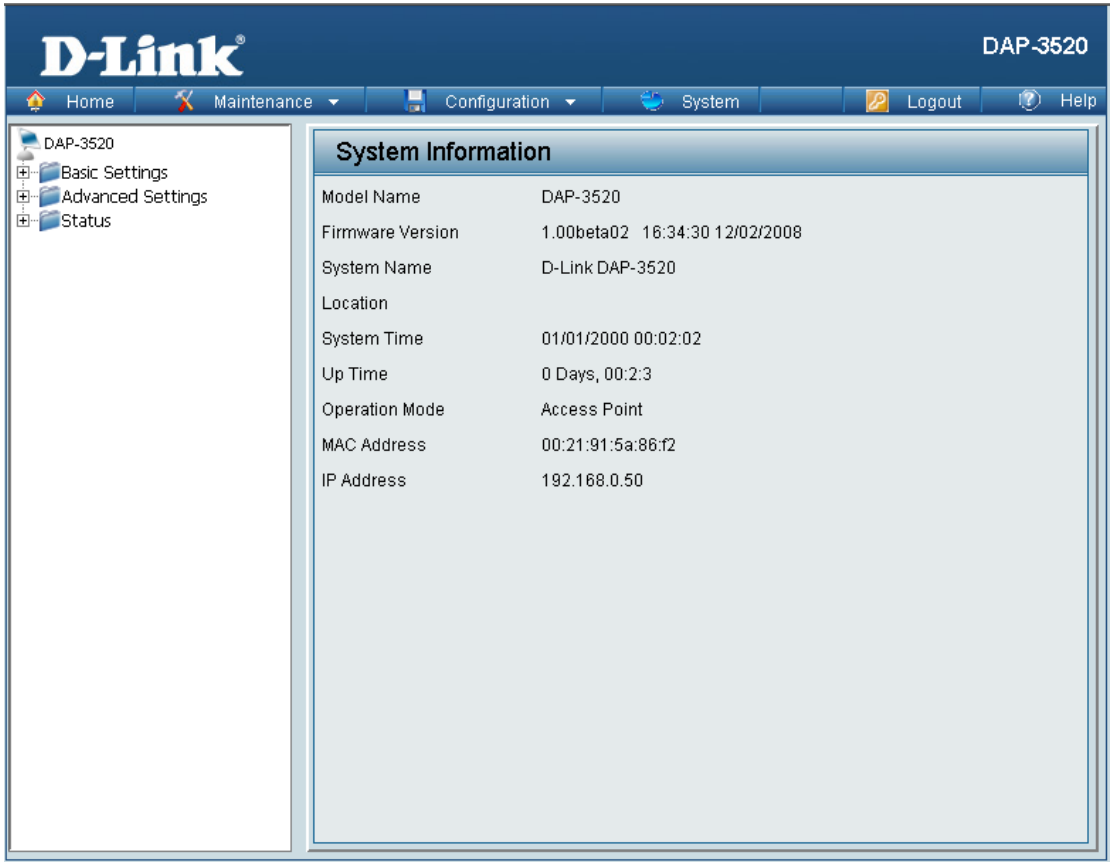
After the connection is established, you will see the user identification window as shown.

Note: *If you have changed the default IP address assigned to the DAP-3520, make sure to enter the correct IP address.*

- Type "**admin**" in the **User Name** field.
- Leave the **Password** field blank.
- Click the **Login** button.



After successfully logging into the DAP-3520, 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.

Wireless Settings

Wireless Band:
Select either 2.4GHz or 5.0GHz from the drop-down menu.

Mode:
Select **Access Point** from the drop-down menu. The other four choices are **WDS with AP**, **WDS**, **Wireless Client**, and **WISP Client Router**.

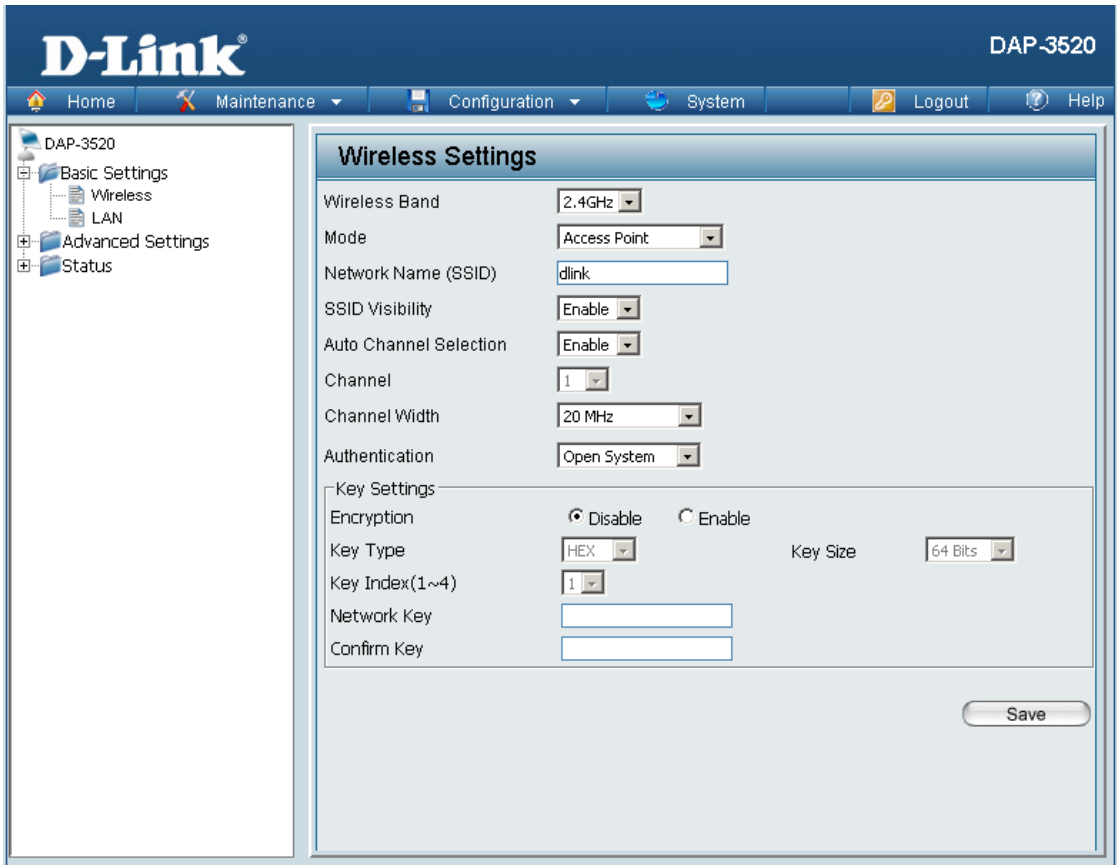
Network Name (SSID):
Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to establish a new wireless network. The SSID can be up to 32 characters and is case sensitive.

SSID Visibility:
Select **Enable** to broadcast the SSID across the network, thus making it visible to all network users. Select **Disable** to hide the SSID from wireless users.

Auto Channel Selection:
Enabling this feature automatically selects the channel that provides the best wireless performance. **Enable** is set by default. The channel selection process only occurs when the AP is booting up.

Channel:
All devices on the network must share the same channel. To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.

Note: *Wireless clients will automatically scan and match the wireless channel of the DAP-3520.*



Channel Width:
Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients or select **Auto 20/40 MHz** to use both 802.11n and non-802.11n wireless devices on your network.

Authentication:
Use the drop-down menu to choose **Open System**, **Shared Key**, **WPA-Personal**, or **WPA-Enterprise**.

- 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. If multi-SSID is enabled, this option is not available.
- Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.
- Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.

WDS with AP mode

In WDS with AP mode, the DAP-3520 wirelessly connects multiple networks while still functioning as a wireless AP at the same time.

Wireless Band:
Select either **2.4 GHz** or **5 GHz** from the drop-down menu.

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

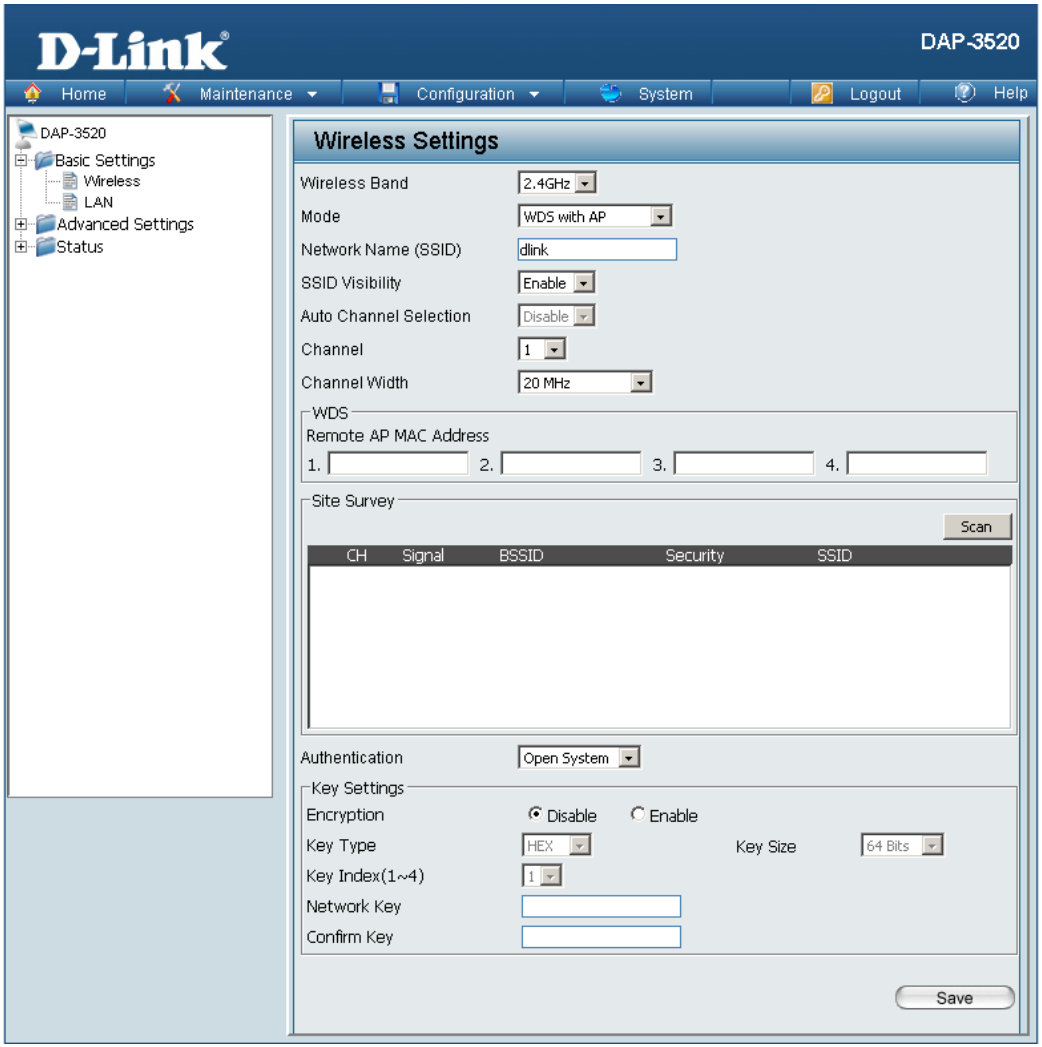
Network Name (SSID):
Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility:
Select **Enable** to broadcast the SSID across the network, thus making it visible to all network users. Select **Disable** to hide the SSID from wireless users.

Auto Channel Selection:
Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS with AP mode. The channel selection process only occurs when the AP is booting up.

Channel:
All devices on the network must share the same channel. To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.

Note: *Wireless clients will automatically scan and match the wireless channel of the DAP-3520.*



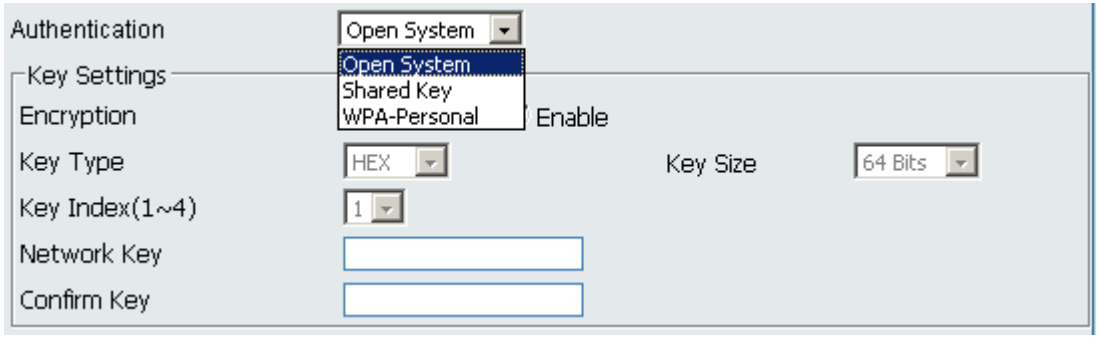
Channel Width:
Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients or select **Auto 20/40 MHz** to use both 802.11n and non-802.11n wireless devices on your network.

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

Site Survey:
Site Survey will display available wireless networks. Click on the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication:
Use the drop-down menu to choose **Open System**, **Shared Key**, or **WPA-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. If multi-SSID is enabled, this option is not available.
- Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.



WDS mode

In WDS mode, the DAP-3520 wirelessly connects multiple networks, without functioning as a wireless AP.

Wireless Band:
Select either **2.4GHz** or **5GHz** from the drop-down menu.

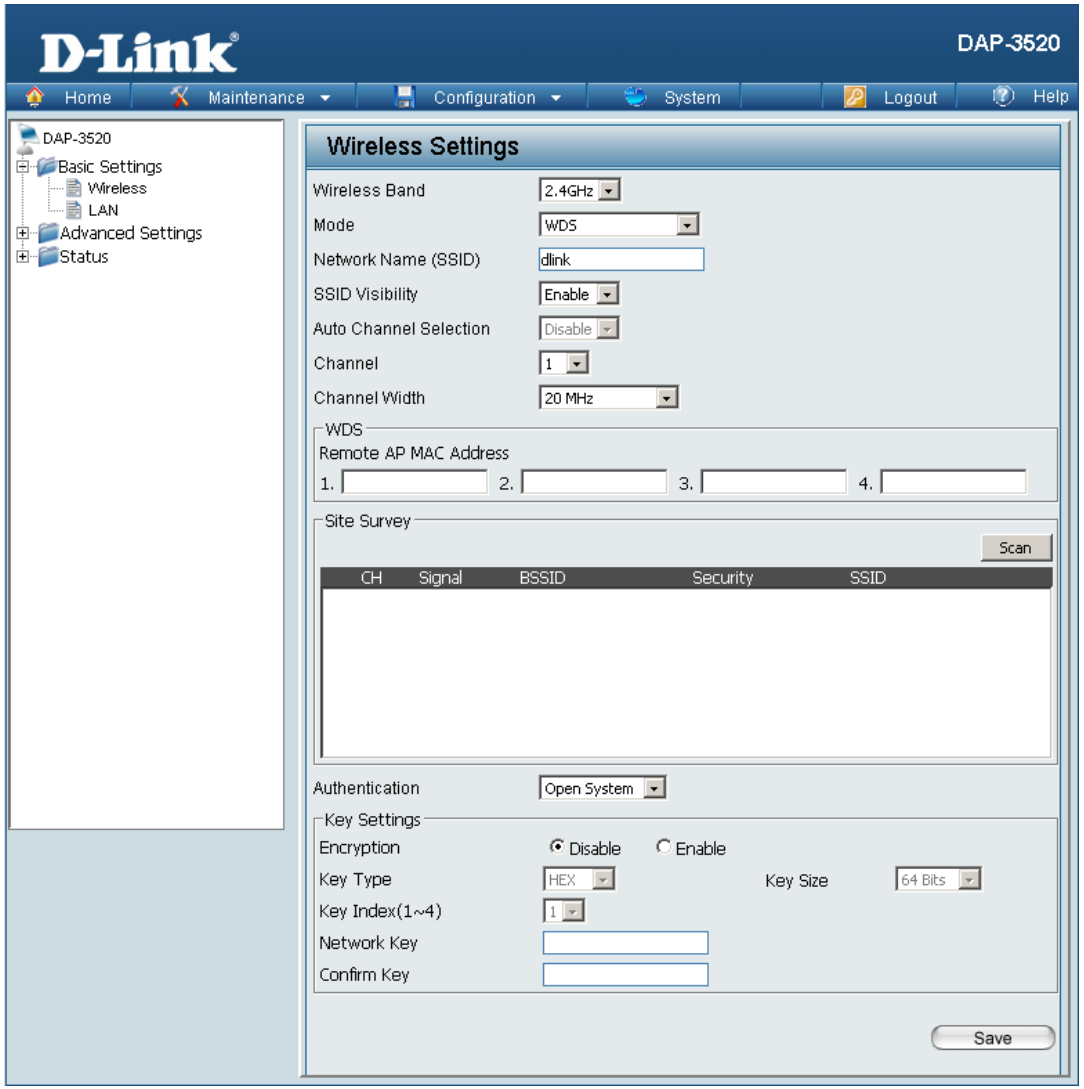
Mode:
WDS mode is selected from the drop-down menu. Access points using WDS must be on the same channel in order to establish connectivity.

Network Name (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 Visibility:
Select **Enable** to broadcast the SSID across the network, thus making it visible to all network users. Select **Disable** to hide the SSID from wireless users.

Auto Channel Selection:
Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in WDS mode.

Channel:
All devices on the network must share the same channel. To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.



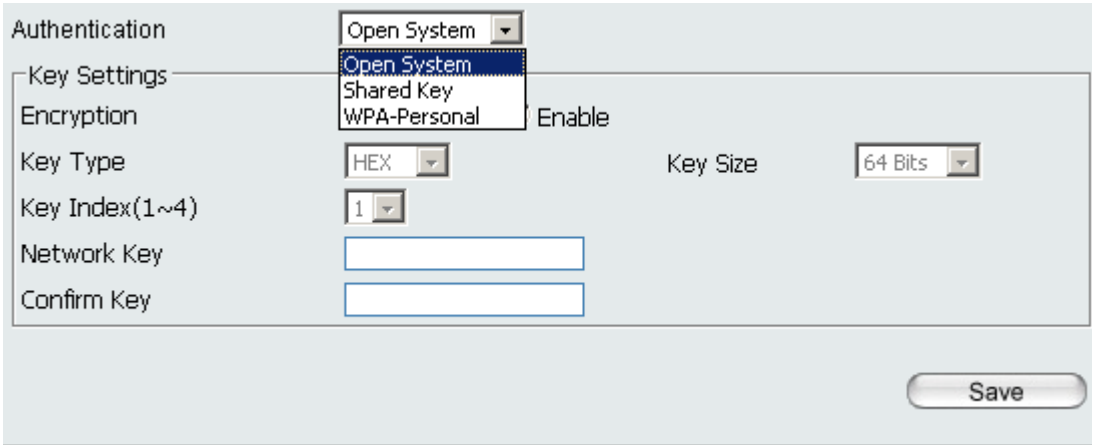
Channel Width:
Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients or select **Auto 20/40 MHz** to use both 802.11n and non-802.11n wireless devices on your network.

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

Site Survey:
Site Survey will display available wireless networks. Click on the **Scan** button to search for available wireless networks, then click on the available network that you want to connect with.

Authentication:
Use the drop-down menu to choose **Open System**, **Shared Key**, or **WPA-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. If multi-SSID is enabled, this option is not available.
- Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.



Wireless Client Mode

Wireless Band:
Select either **2.4GHz** or **5GHz** from the drop-down menu.

Mode:
Wireless Client mode is selected from the drop-down menu.

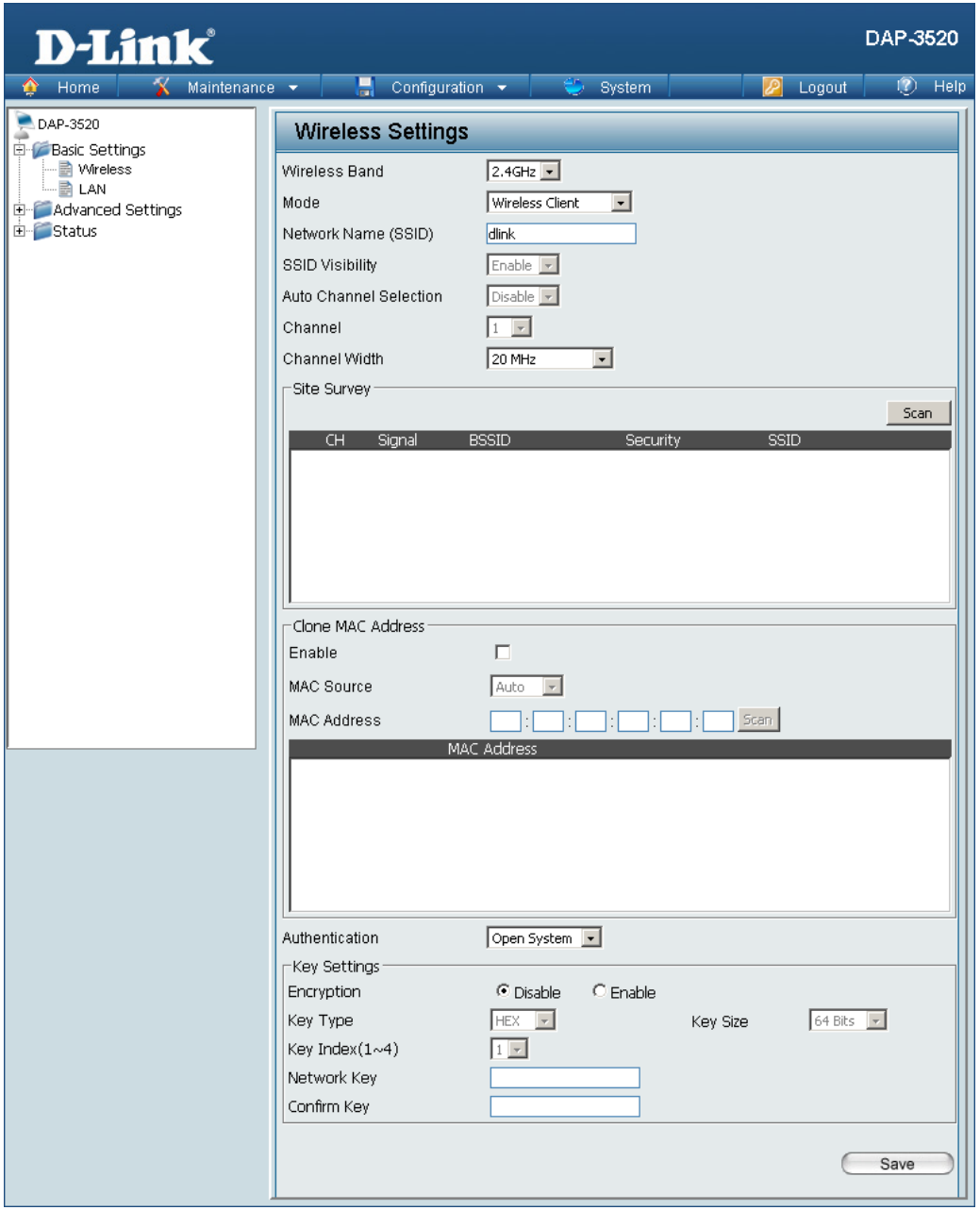
Network Name (SSID):
Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility:
This option is unavailable in wireless client mode.

Auto Channel Selection:
Enabling this feature automatically selects the channel that will provide the best wireless performance. This feature is not supported in Wireless Client mode.

Channel:
The channel will be determined by the access point that the DAP-3520 is connected to.

Channel Width:
Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows both 802.11n and non-802.11n wireless devices on your network.



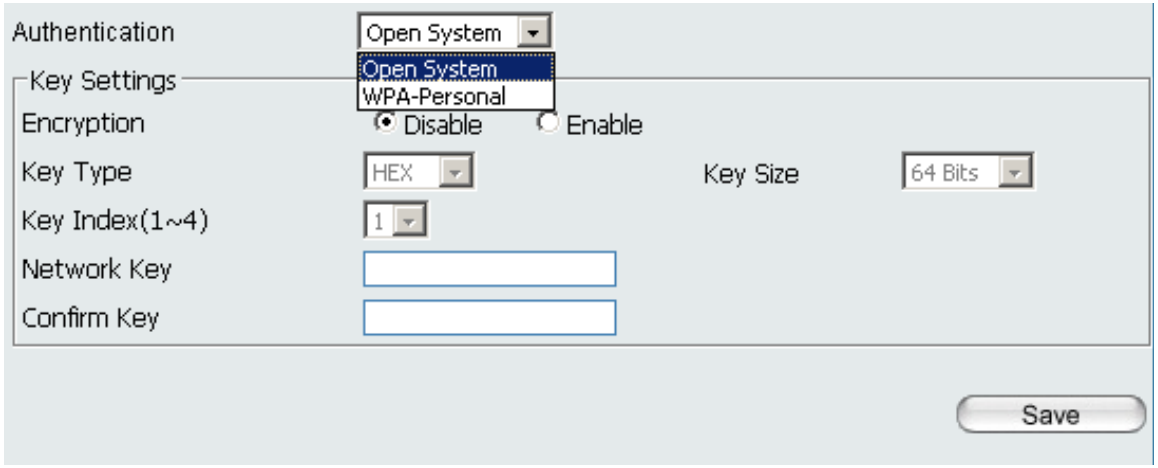
Site Survey:
Site Survey will display available wireless networks. Click on the **Scan** button to search for available wireless networks, then click on the name of the wireless network that you want to connect to.

Clone MAC Address:
Click **Enable** to allow you to clone a MAC address to the access point. If you select **Auto** from the *MAC Source* drop-down, it will copy the first MAC address found in the LAN port.

Next to **MAC Address**, enter the MAC address you would like to clone.

Authentication:
Use the drop-down menu to choose **Open System** or **WPA-Personal**.

- Select **Open System** to communicate the key across the network.
- Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.



WISP Client Router Mode

In WISP Client Router mode, the DAP-3520 wirelessly connects to a WISP (Wireless Internet Service Provider) access point. In this mode, the DAP-3520 also acts as a router for wired clients on your LAN and provides NAT (Network Address Translation) and a DHCP server to generate IP addresses for wired clients. NAT and the DHCP server allow many computers to share the same wireless Internet connection.

Wireless Band:
Select either **2.4GHz** or **5GHz** from the drop-down menu.

Mode:
WISP Client Router mode is selected from the drop-down menu.

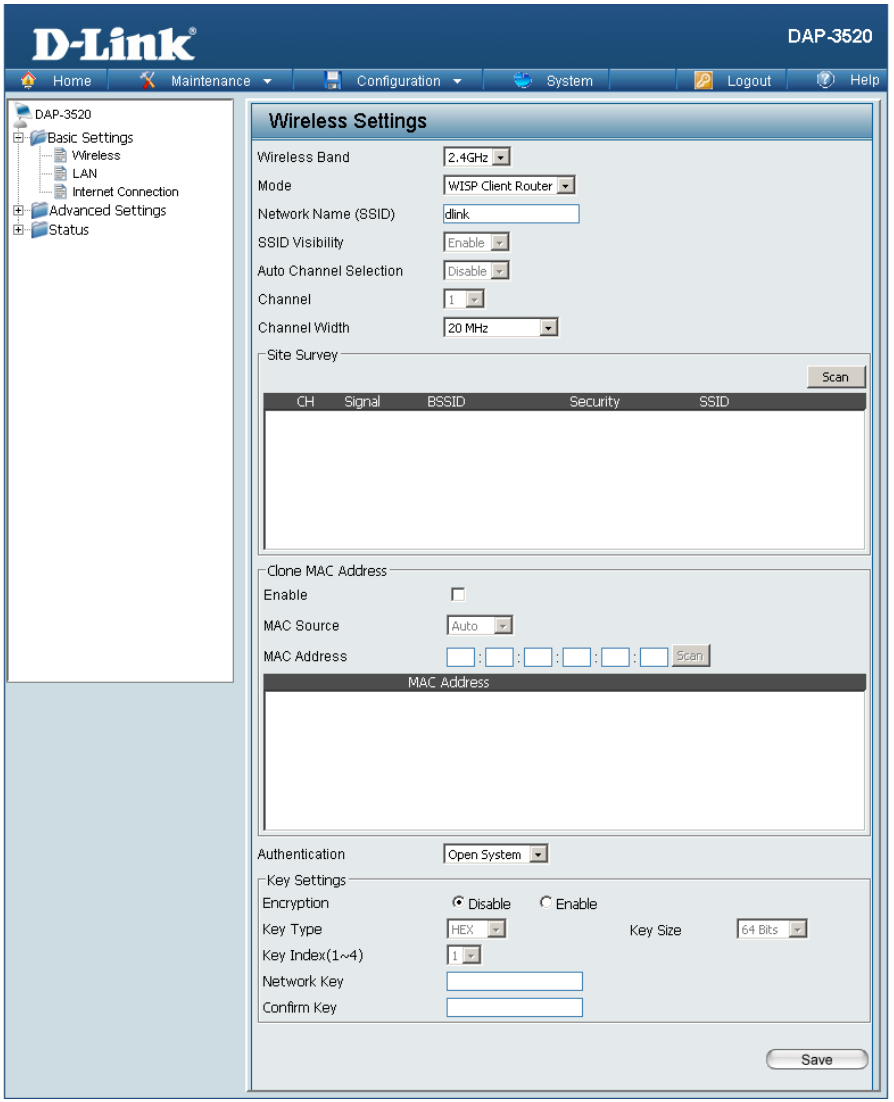
Network Name (SSID):
Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility:
This option is unavailable in WISP Client Router mode.

Auto Channel Selection:
This feature is not supported in WISP Client Router mode.

Channel:
The channel will be determined by the access point that the DAP-3520 is connected to.

Channel Width:
Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows both 802.11n and non-802.11n wireless devices on your network.



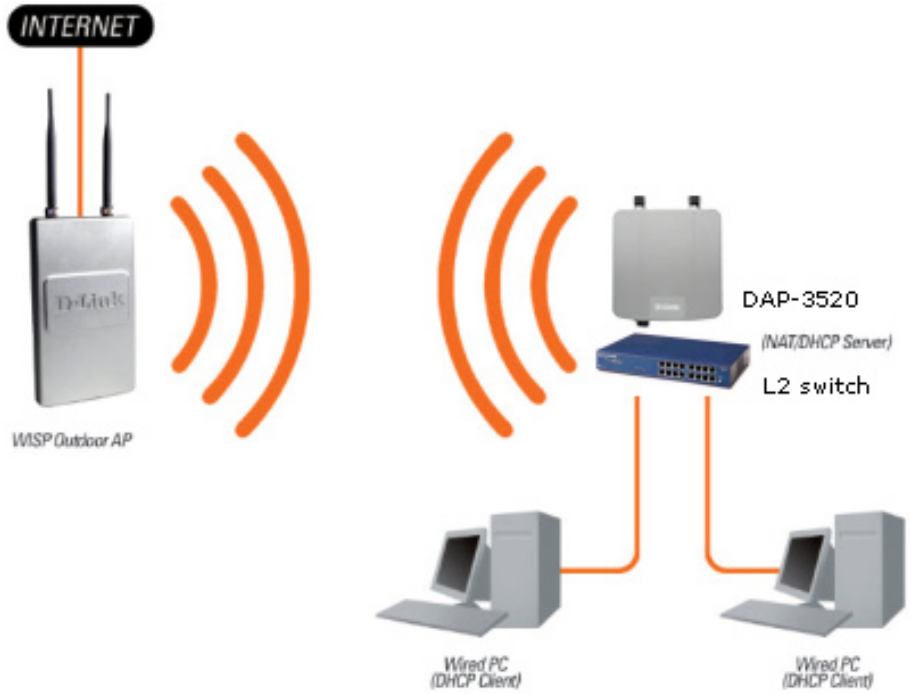
Site Survey:
Site Survey will display available wireless networks. Click on the **Scan** button to search for available wireless networks, then click on the name of a wireless network that you want to connect to.

Clone MAC Address:
Click **Enable** to allow you to clone a MAC address to the access point. If you select **Auto** from the *MAC Source* drop-down, it will copy the first MAC address found in the LAN port.

Next to **MAC Address**, enter the MAC address you would like to clone.

Authentication:
Use the drop-down menu to choose **Open System** or **WPA-Personal**.

- Select **Open System** to communicate the key across the network.
- Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.



WEP Encryption

Authentication:
Select either **Open System** or **Shared Key**.

Encryption:
Click to Enable or Disable Encryption.

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

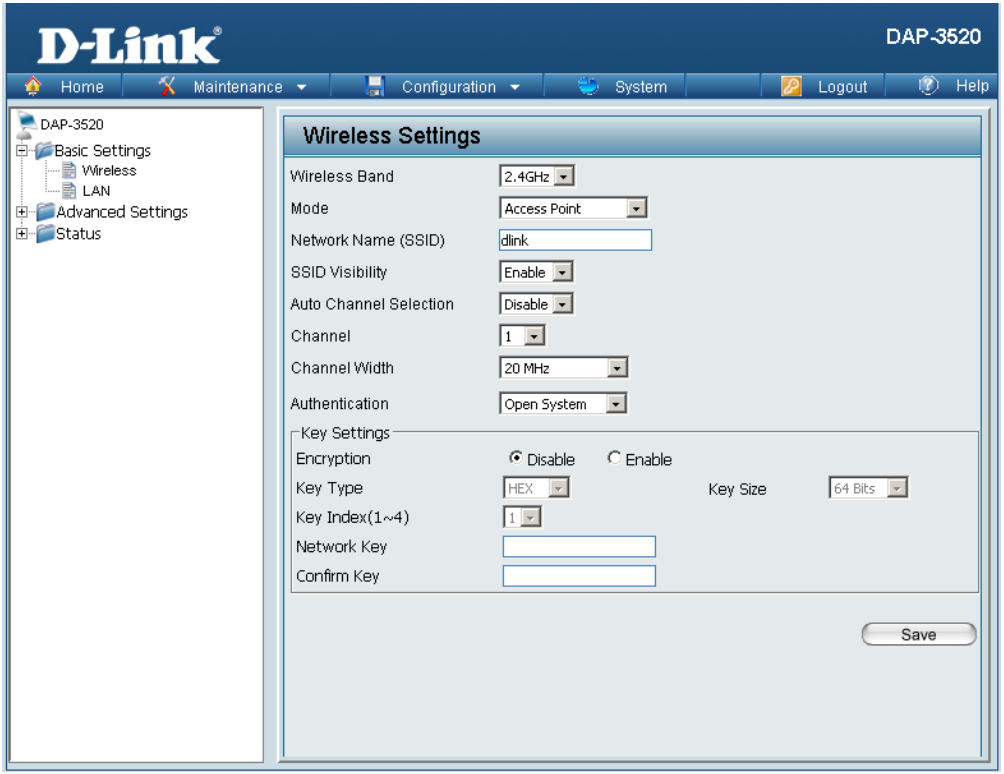
Key Size:
Select **64-bit** or **128-bit** Encryption.

Key Index (1-4):
Select the 1st through the 4th key to be the active key.

Key:
Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.

Network Key:
Enter the WEP encryption key.

Confirm Key:
Retype the network key.



**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.*

WPA-Personal Authentication

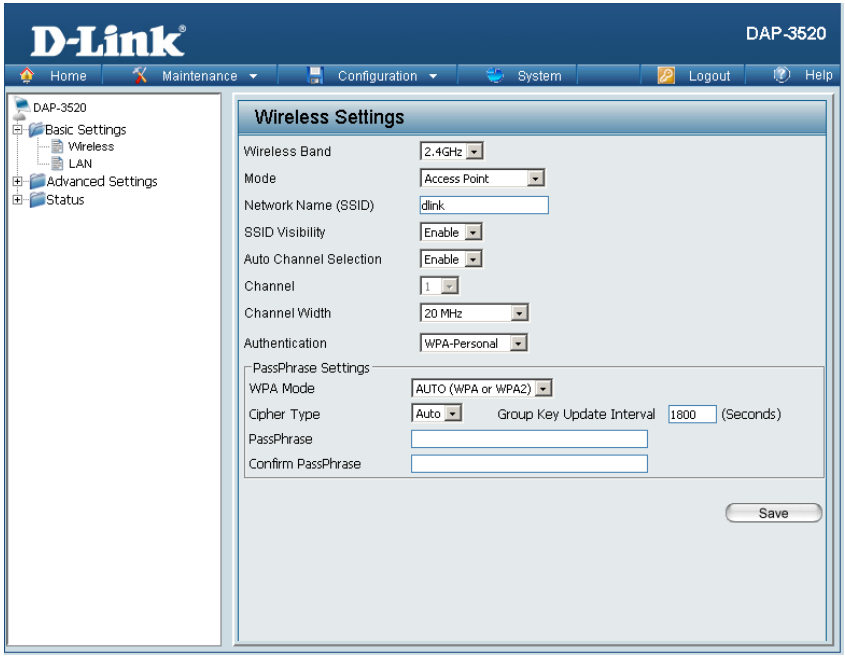
WPA Mode:
When **WPA-Personal** is selected for Authentication type, you must also select a WPA mode from the drop-down menu: **AUTO (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. WPA and WPA2 use different algorithms. **AUTO (WPA or WPA2)** allows you to use both WPA and WPA2.

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

Group Key Update Inverval:
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.

Confirm PassPhrase:
Retype the PassPhrase in the corresponding field.



WPA-Enterprise Authentication

WPA Mode:
When **WPA-Enterprise** is selected, you must also select a WPA mode from the drop-down menu: **AUTO (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. WPA and WPA2 use different algorithms. **AUTO (WPA or WPA2)** allows you to use both WPA and WPA2.

Cipher Type:
When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: **Auto**, **AES**, or **TKIP**.

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

Network Access Protection:
Enable or disable Microsoft Network Access Protection.

RADIUS Server:
Enter the IP address of the primary RADIUS server. You must also configure RADIUS port and RADIUS secret. In addition to a primary RADIUS server, the AP allows you to set up an optional backup RADIUS server.

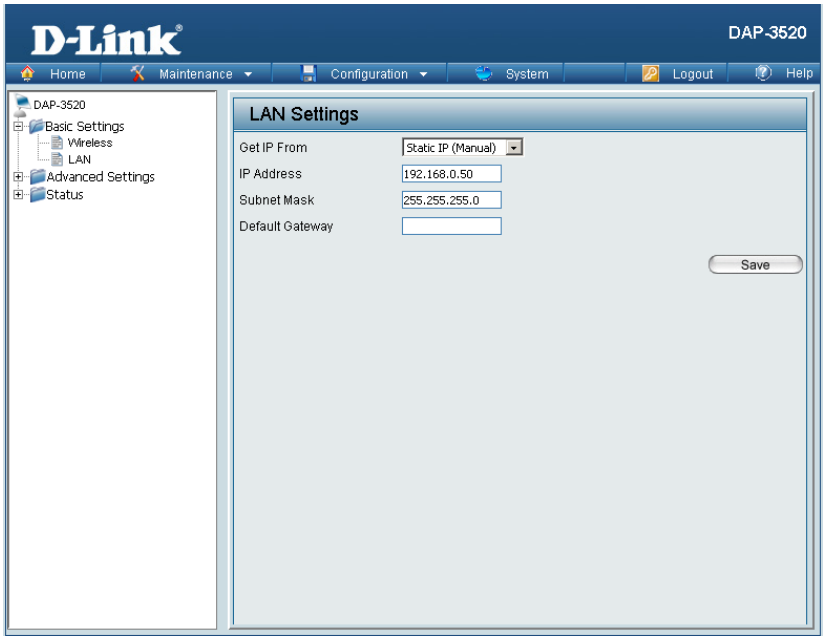
RADIUS Port:
Enter the RADIUS port.

RADIUS Secret:
Enter the RADIUS secret.

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-3520. 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 IP (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-3520.

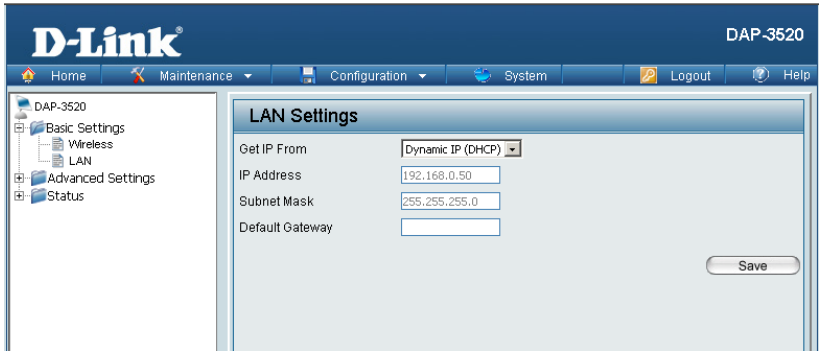


IP Address:
The default IP address is **192.168.0.50**. Assign a static IP address that is within the IP address range of your network.

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.

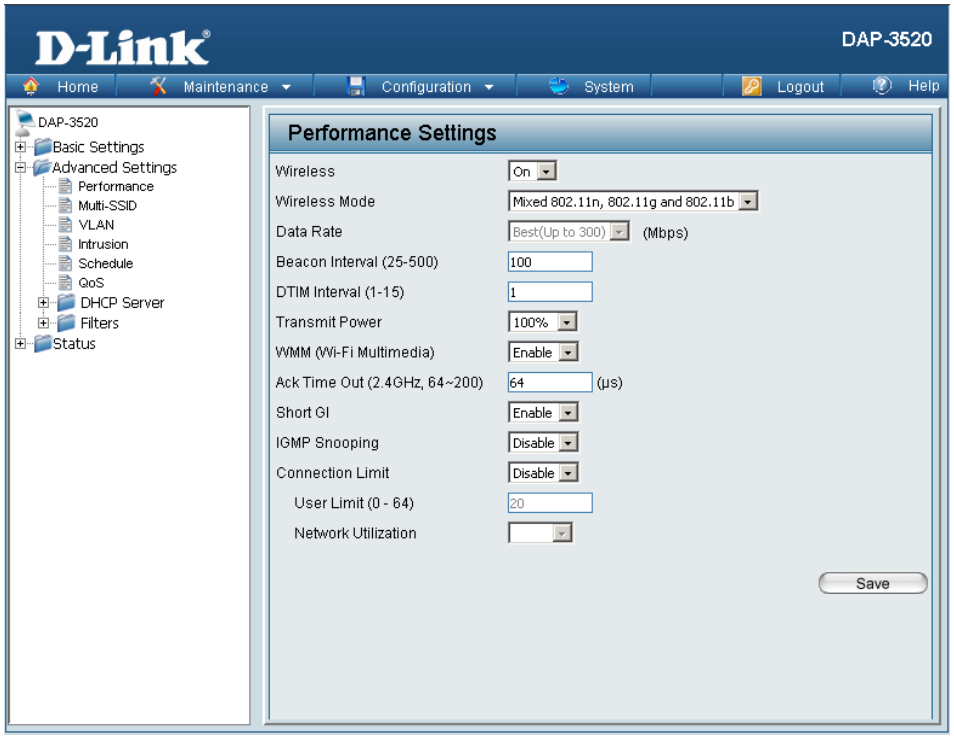
Get IP From:
Dynamic IP (DHCP) is chosen here. Choose this option if you have a DHCP server in your network. When **Dynamic** is selected, the other fields here will be grayed out. Please allow about two minutes for the DHCP client to be functional once this selection is made.



Advanced Settings

Performance

Wireless:
Use the drop-down menu to turn the wireless function **On** or **Off**.



Wireless Mode:
The different combination of clients that can be supported include **Mixed 802.11n, 802.11g and 802.11b**, **Mixed 802.11g and 802.11b** in the 2.4 GHz band and **Mixed 802.11n, 802.11a** and **802.11a only** in the 5 GHz band. Please note that when backwards compatibility is enabled for legacy (802.11a/g/b) clients, degradation of 802.11n wireless performance is expected.

Data Rate*:
Indicate the base transfer rate of wireless adapters on the wireless LAN. The AP will adjust the base transfer rate depending on the base rate of the connected device. If there are obstacles or interference, the AP will step down the rate. This option is enabled in **Mixed 802.11g and 802.11b** mode (for 2.4 GHz) and **802.11a only** mode (for 5 GHz). The choices available are **Best (Up to 54)**, **54**, **48**, **36**, **24**, **18**, **12**, **9**, **6** for 5 GHz and **Best (Up to 54)**, **54**, **48**, **36**, **24**, **18**, **12**, **9**, **6, 11**, **5.5**, **2** or **1** for 2.4 GHz.

Beacon Interval (25-500):
Beacons are packets sent by an access point to synchronize a wireless network. Specify a value in milliseconds. The default (**100**) is recommended. Setting a higher beacon interval can help to save the power of wireless clients, while setting a lower one can help a wireless client connect to an access point faster.

DTIM Interval (1-15):
Select a Delivery Traffic Indication Message setting between **1** and **15**. The default setting is 1. 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 802.11 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 throughout rate.

Transmit Power:
This setting determines the power level of the wireless transmission. Transmitting power can be adjusted to eliminate overlapping of wireless area coverage between two access points where interference is a major concern. For example, if wireless coverage is intended for half of the area, then select **50%** as the option. Use the drop-down menu to select **100%**, **50%**, **25%**, or **12.5%**.

WMM (Wi-Fi Multimedia):
WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.

Ack Time Out (2.4 GHz, 64~200) or Ack Time Out (5 GHz, 50~200):
To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between **50** and **200** microseconds for 5 GHz or from **64** to **200** microseconds in the 2.4 GHz in the field provided.

Short GI:
Select **Enable** or **Disable**. Enabling a short guard interval can increase throughput. However, be aware that it can also increase the error rate in some installations due to increased sensitivity to radio-frequency installations.

IGMP Snooping:
Select **Enable** or **Disable**. Internet Group Management Protocol allows the AP to recognize IGMP queries and reports sent between routers and an IGMP host (wireless STA). When IGMP snooping is enabled, the AP will forward multicast packets to an IGMP host based on IGMP messages passing through the AP.

Connection Limit:
Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled, when the number of users exceeds this value, the DAP-3520 will not allow clients to associate with the AP.

User Limit (0 - 64):
Set the maximum amount of users that are allowed access (**0**-**64** users).To use this feature, the Connection Limit above must be enabled. For most users, a limit of **10** is recommended. The default setting is **20**.

Network Utilization:
Select a utilization percentage between **180**, **60**, **40**, **20**, or **0**. When this network utilization threshold is reached, the device will pause one minute to allow for network congestion to dissipate.

Multi-SSID

The device supports up to four multiple Service Set Identifiers. You can set the Primary SSID in the **Basic** > **Wireless** section. 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.

Enable Multi-SSID:
Check to enable support for multiple SSIDs.

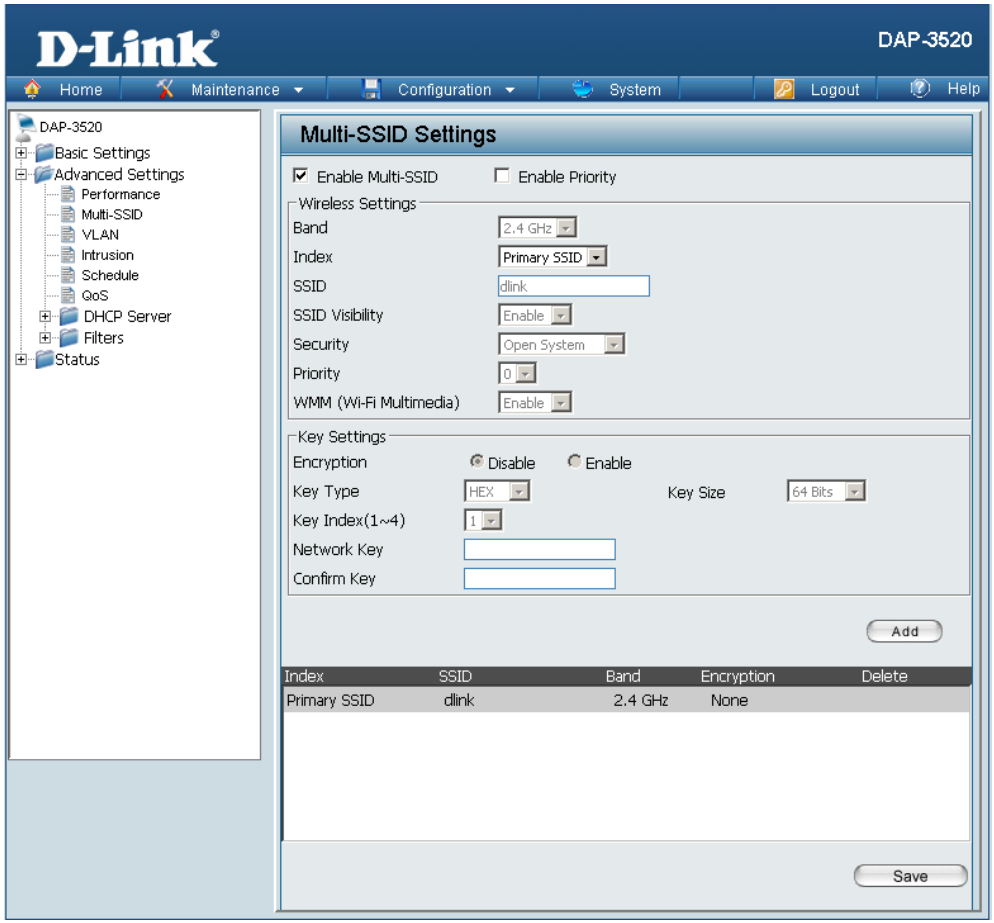
Band:
Displays the current band.

Index:
You can select up to three multi-SSIDs. With the Primary SSID, you have a total of four 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.

SSID Visibility:
Select **Enable** to broadcast the SSID across the network, thus making it visible to all network users. Select **Disable** to hide the SSID from wireless users.

Security:
The Multi-SSID security can be **Open System**, **Shared Key**, **WPA-Personal**, or **WPA-Enterprise**. For a detailed description of the Open System parameters, please go to page 26. For a detailed description of the WPA-Personal parameters please go to page 27. For a detailed description of the WPA-Enterprise parameters, please go to pages 28-29.



Priority:
Select the desired priority from the drop-down menu.

WMM (Wi-Fi Multimedia):
Select **Enable** or **Disable**.

Encryption:
When you select **Open System** or **Shared Key**, toggle between **Enable** and **Disable**. If **Enable** is selected, the Key Type, Key Size, Key Index (1~4), Network Key, and Confirm Keys must also be configured.

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

Key Size:
Select **64 Bits** or **128 Bits**.

Key Index (1~4):
Select from the 1st to the 4th key to be set as the active key.

Network Key:
Enter a network key, otherwise known as a password.

Confirm Key:
Retype the network key.

WPA Mode:
When you select either **WPA-Personal** or **WPA-Enterprise**, you must also choose a WPA mode from the drop-down menu: **AUTO (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. WPA and WPA2 use different algorithms. **AUTO (WPA or WPA2)** allows you to use both WPA and WPA2. In addition, you must configure Cipher Type, and Group Key Update Interval.

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

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

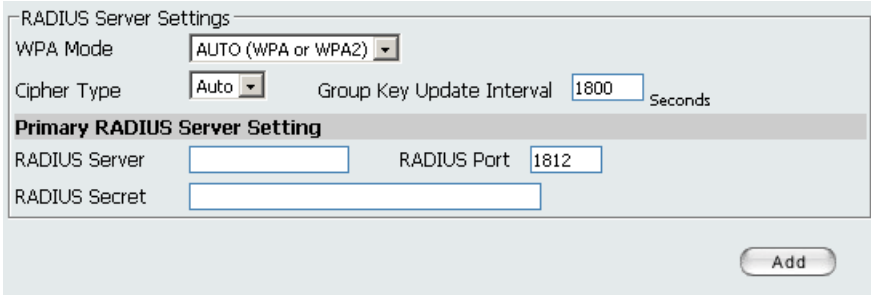
PassPhrase:
When you select **WPA-Personal**, please enter a PassPhrase in the corresponding field.

Confirm PassPhrase:
When you select **WPA-Personal**, please re-enter the PassPhrase entered in the previous item in the corresponding field.

RADIUS Server:
When you select **WPA-Enterprise**, enter the IP address of the primary RADIUS server. You must also configure RADIUS port and RADIUS secret. In addition to a primary RADIUS server, the AP allows you to set up an optional backup RADIUS server.

RADIUS Port:
Enter the RADIUS port.

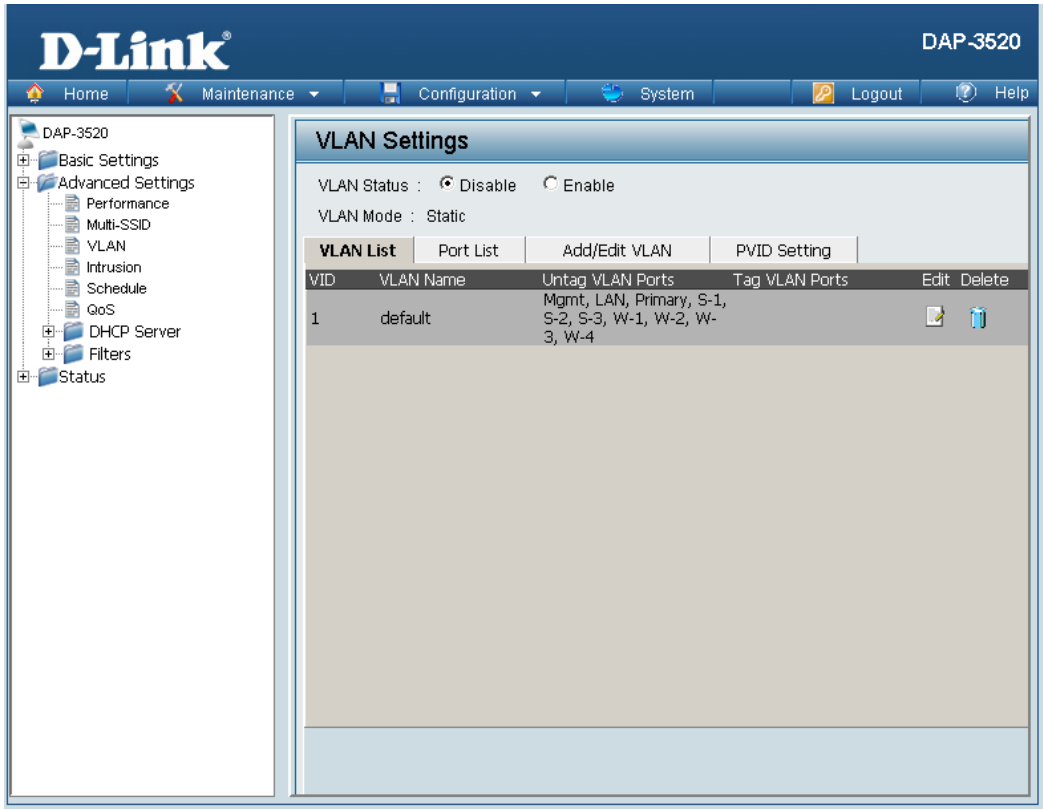
RADIUS Secret:
Enter the RADIUS secret.



VLAN

The DAP-3520 supports VLANs. VLANs can be created with a Name and VID. Mgmt (TCP stack), LAN, Primary/Multiple SSID, and WDS connection can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-3520 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

VLAN Status:
Use the radio button to toggle to Enable. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the **VLAN List** tab.



Port List

The Port List tab displays the current ports. If you want to configure the guest and internal networks on a 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 IEEE 802.1Q standard.

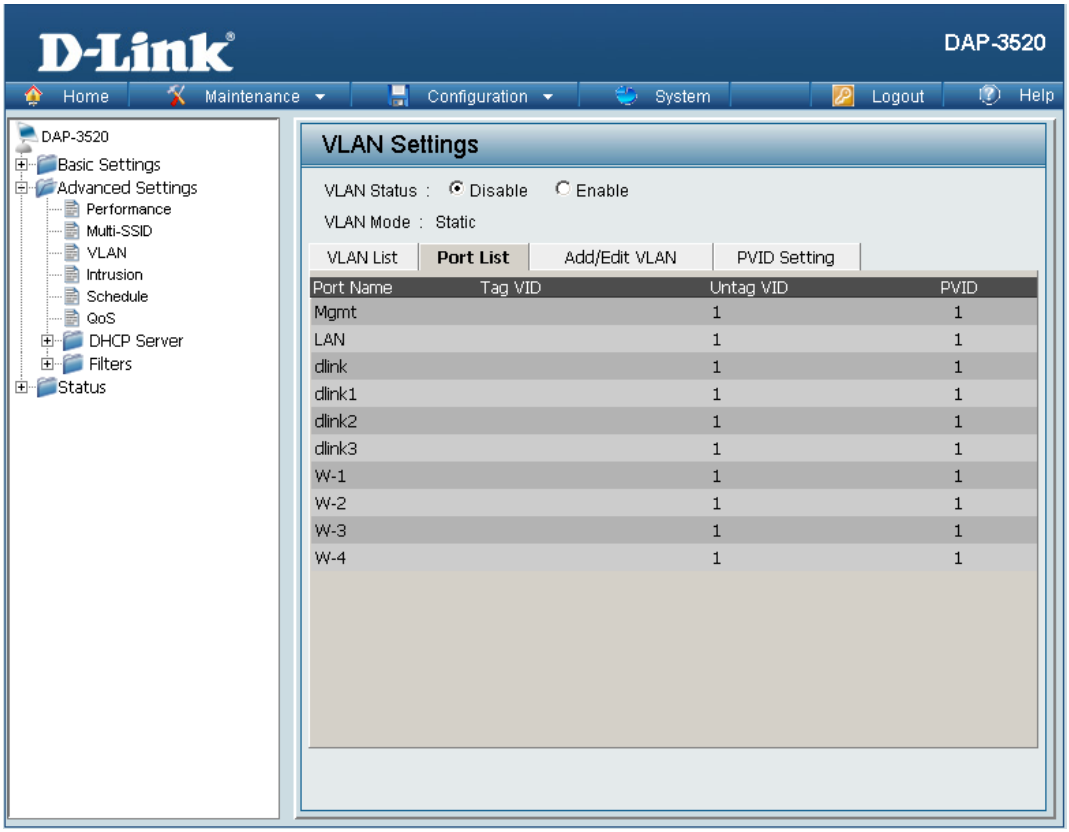
VLAN Status:
Use the radio button to toggle to **Enable**. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the **VLAN List** tab.

Port Name:
The name of the port is displayed in this column.

Tag VID:
The Tagged VID is displayed in this column.

Untag VID:
The Untagged VID is displayed in this column.

PVID:
The Port VLAN Identifier is displayed in this column.



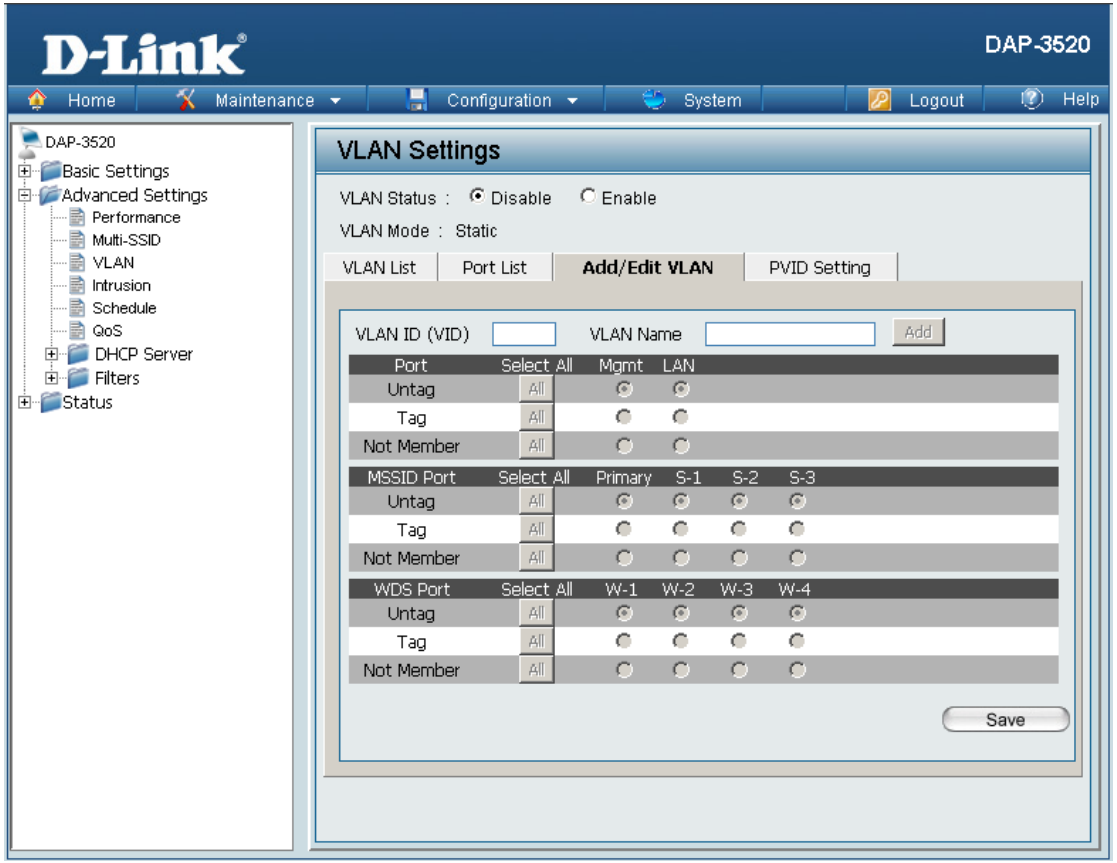
Add/Edit VLAN

The Add/Edit VLAN tab is used to configure VLANs. Once you have made the desired changes, click the **Apply** button to let your changes take effect.

VLAN Status:
Use the radio button to toggle to Enable.

VLAN ID (VID):
Provide a number between **1** and **4094** for the Internal VLAN.

VLAN Name:
Enter the VLAN to add or modify.

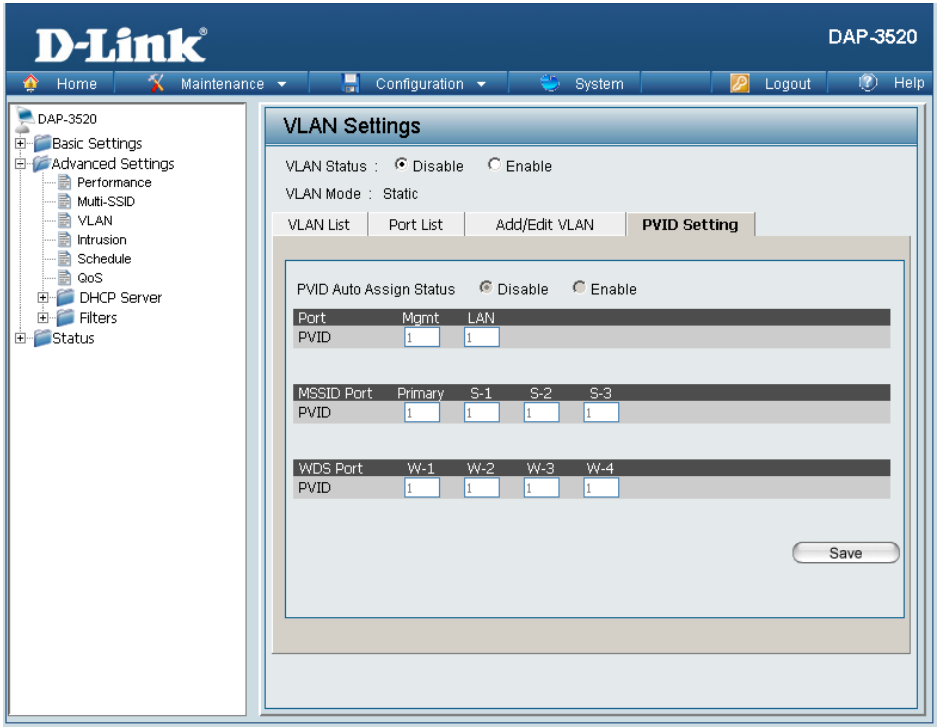


PVID Setting

The PVID Setting tab is used to enable/disable the Port VLAN Identifier Auto Assign Status as well as to configure various types of PVID settings. Click the **Apply** button to let your changes take effect.

VLAN Status:
Use the radio button to toggle to Enable.

PVID Auto Assign Status:
Use the radio button to toggle PVID auto assign status to Enable.

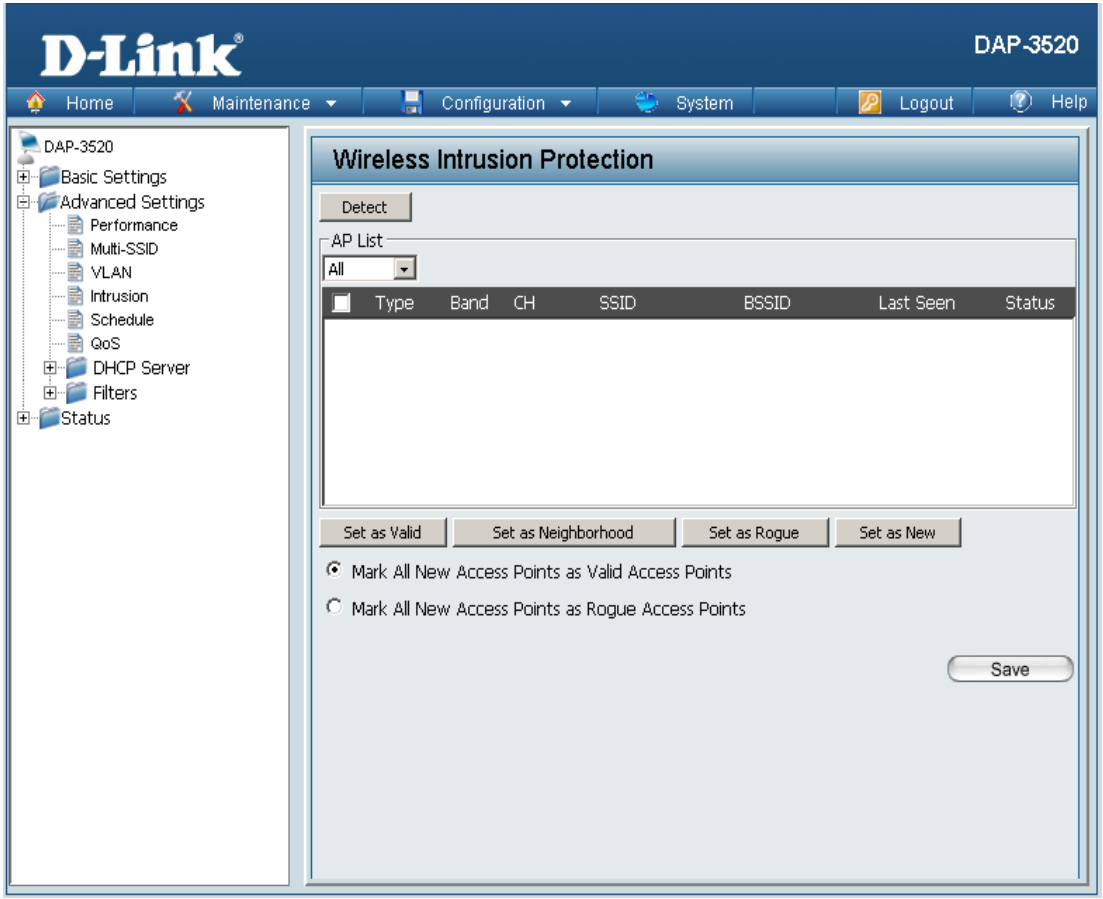


Intrusion

The Wireless Intrusion Protection window is used to set APs as **All**, **Valid**, **Neighborhood**, **Rogue**, and **New**. Click the **Apply** button to let your changes take effect.

AP List:
The choices include **All**, **Valid**, **Neighbor**, **Rogue**, and **New**.

Detect:
Click this button to initiate a scan of the network.



Schedule

The Wireless Schedule Settings window is used to add and modify scheduling rules on the device. Click the **Apply** button to let your changes take effect.

Wireless Schedule:
Select **Enable** or **Disable** from the drop-down menu.

Name:
Enter a name for your schedule rule.

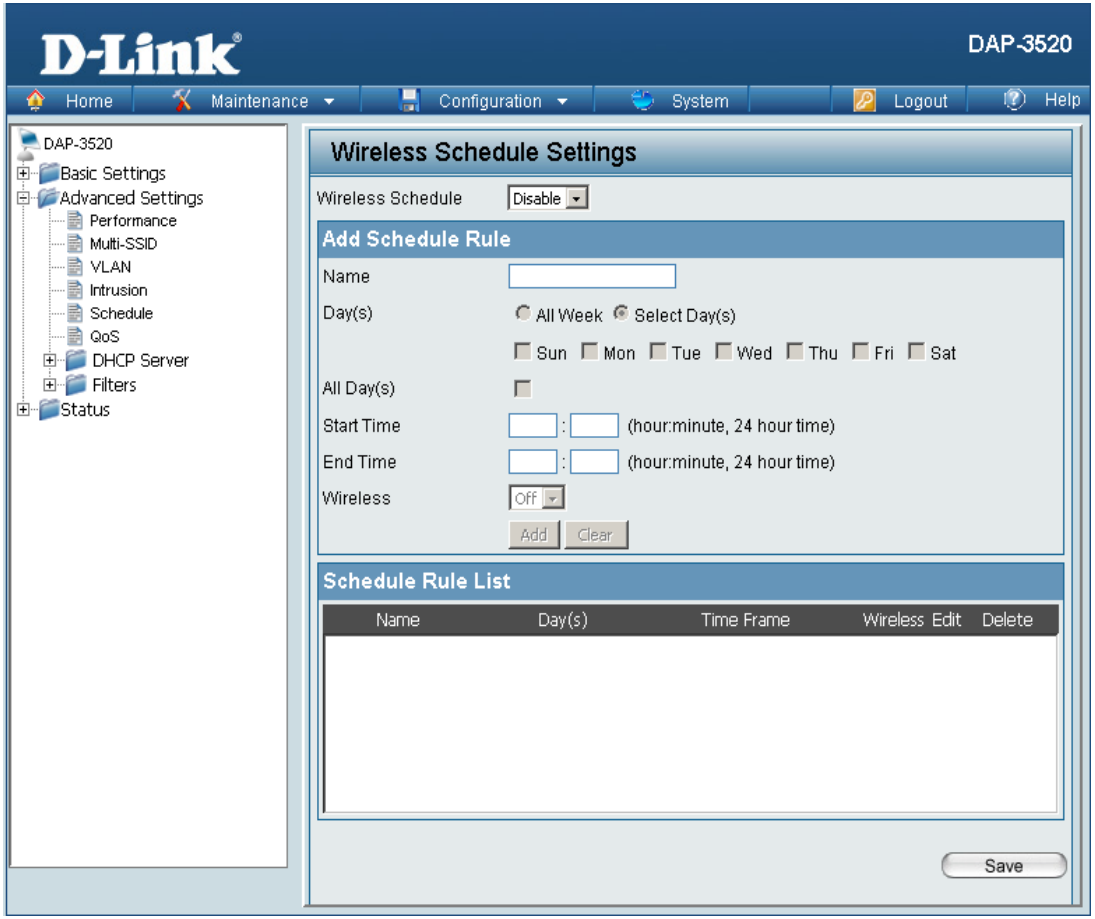
Day(s):
Select **All Week** or **Select Days(s)**. If **Select Day(s)** is selected, check the specific days you want the rule to be effective on.

All Days(s):
Check this box to select all days.

Start Time:
Enter the start time for the rule.

End Time:
Enter the end time for the rule.

Wireless:
Select **Off** and **On**.



QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications.

A QoS Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific QoS Rules are not required.

QoS supports overlaps between rules. If more than one rule matches a specific message flow, the rule with the highest priority will be used.

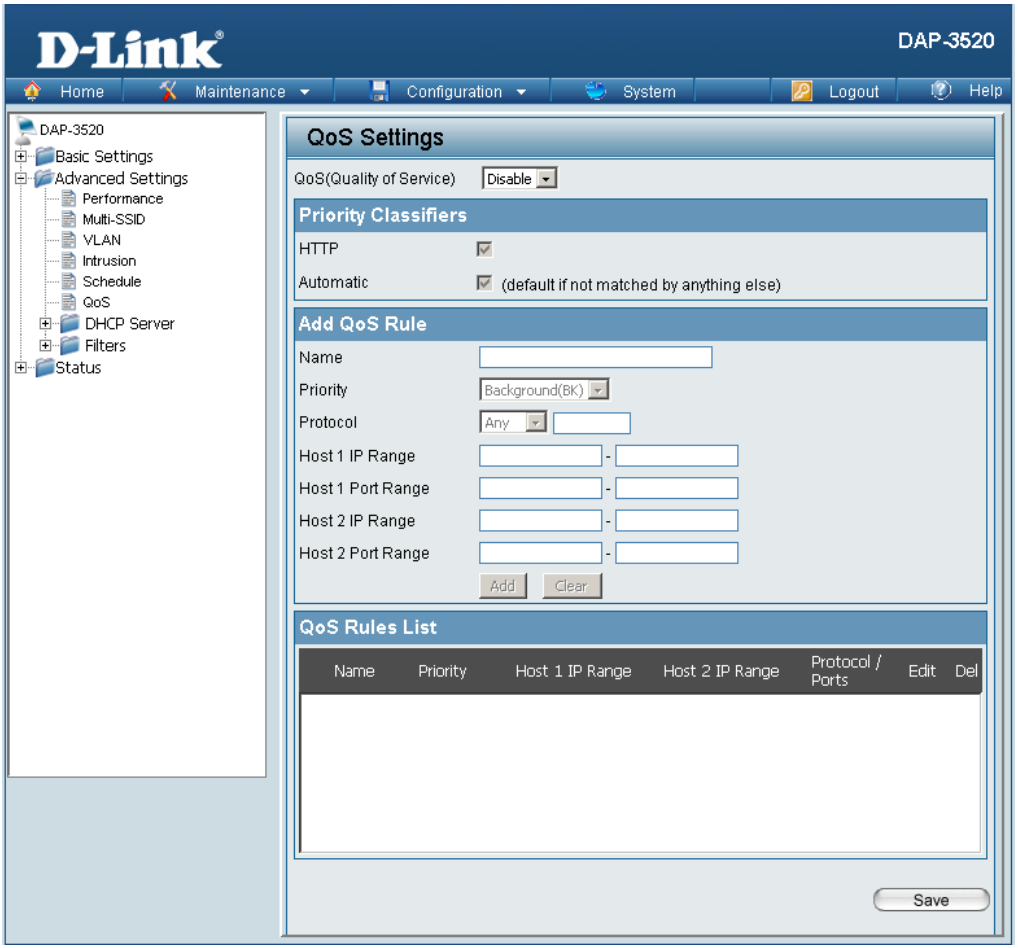
QoS (Quality of Service):
Enable this option if you want to allow QoS to prioritize your traffic Priority Classifiers.

HTTP:
Allows the access point to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Automatic:
When enabled, this option causes the access point to automatically attempt to prioritize traffic streams that it does not otherwise recognize, based on the behavior that the streams exhibit. This acts to de-prioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

Name:
Enter a name for the new QoS rule in the field provided.

Priority:
Use the drop-down menu to select the desired priority: **Background (BK)**, **Best Effort (BE)**, **Video (VI)**, or **Voice (VO)**.



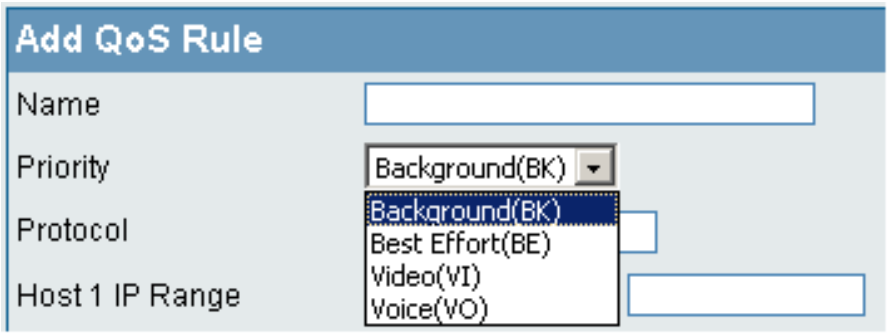
Protocol:
Use the drop-down menu to choose the appropriate protocol used by the messages: **Any**, **TCP**, **UDP**, **Both**, **IMCP**, or **Other**.

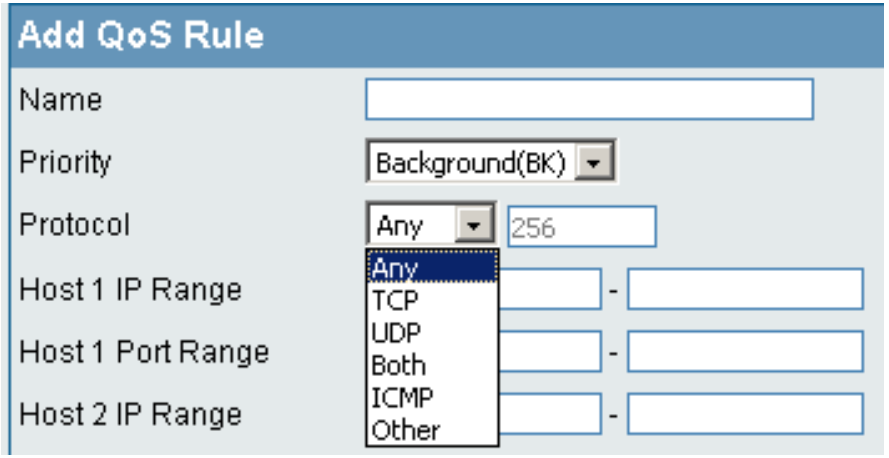
Host 1 IP Range:
The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host 1 Port Range:
The rule applies to a flow of messages for which host 1's port number is within the range set here when the Protocol is set to **TCP**, **UDP**, or **Both**.

Host 2 IP Range:
The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.

Host 2 Port Range:
The rule applies to a flow of messages for which host 2's port number is within the range set here when the Protocol is set to **TCP**, **UDP**, or **Both**.





DHCP Server

Dynamic Pool Settings

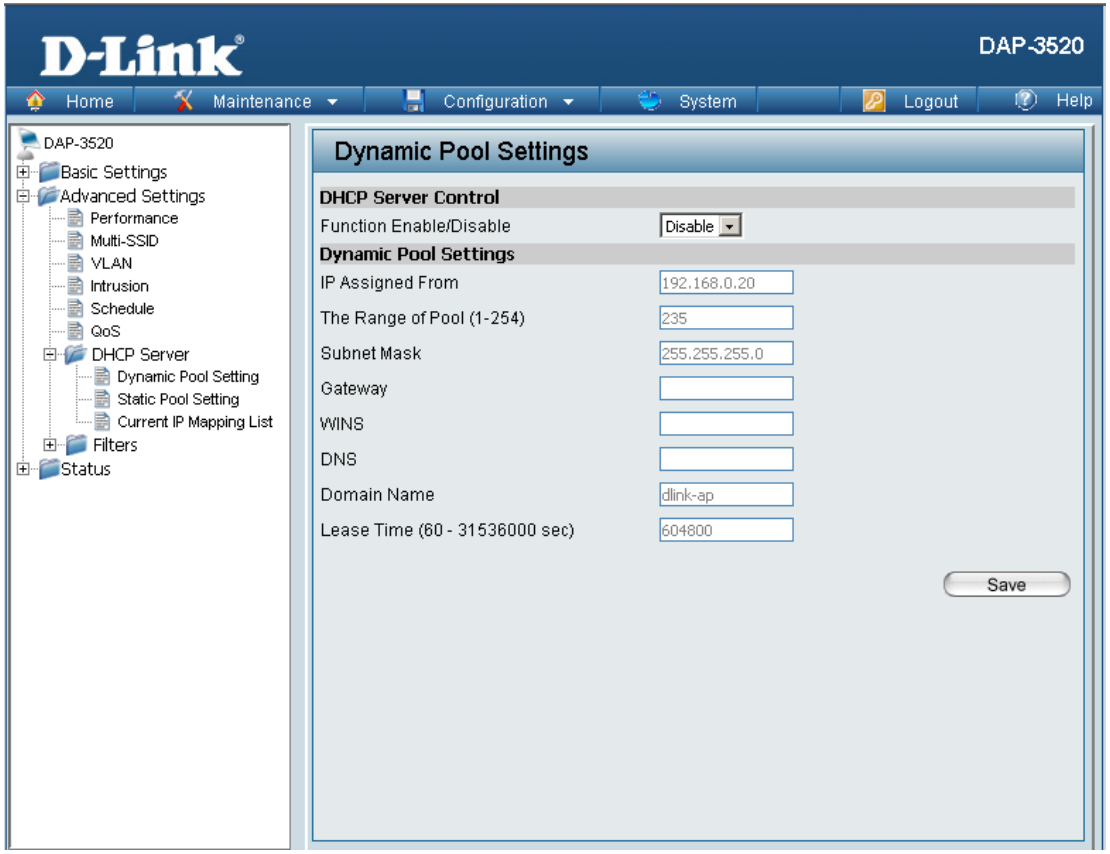
The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control.

Function Enable/Disable:
Dynamic Host Configuration Protocol (DHCP) 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-3520 to function as a DHCP server.

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

The Range of Pool (1-254):
Enter the number of IP addresses available for assignment. IP addresses are increments of the IP address specified in the “IP Assigned From” field.

Subnet Mask:
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:
Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer that has a dynamically assigned IP address.

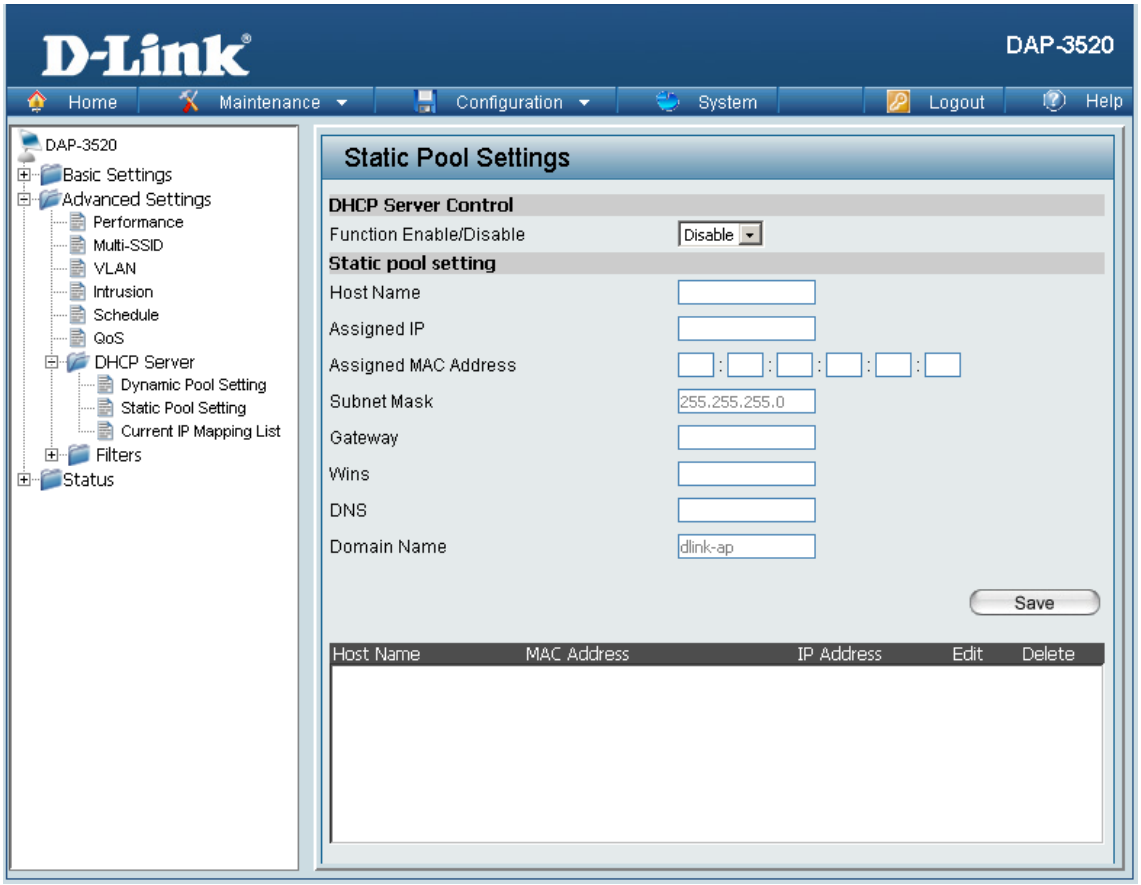
DNS:
Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as www.dlink.com into IP addresses.

Domain Name:
Enter the domain name of the network, 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.

Static Pool Setting

The DHCP address pool defines the range of IP addresses that can be assigned to stations on the network. A static pool allows specific wireless stations to receive a fixed IP without time control.



Function Enable/Disable:
Dynamic Host Configuration Protocol (DHCP) 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-3520 to function as a DHCP server.

Host Name:
Enter a name for the assigned client.

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 requesting association here.

Subnet Mask:
Define the submask of the IP address specified in the "IP Assigned From" field.

Gateway:
Specify the Gateway address for the wireless network.

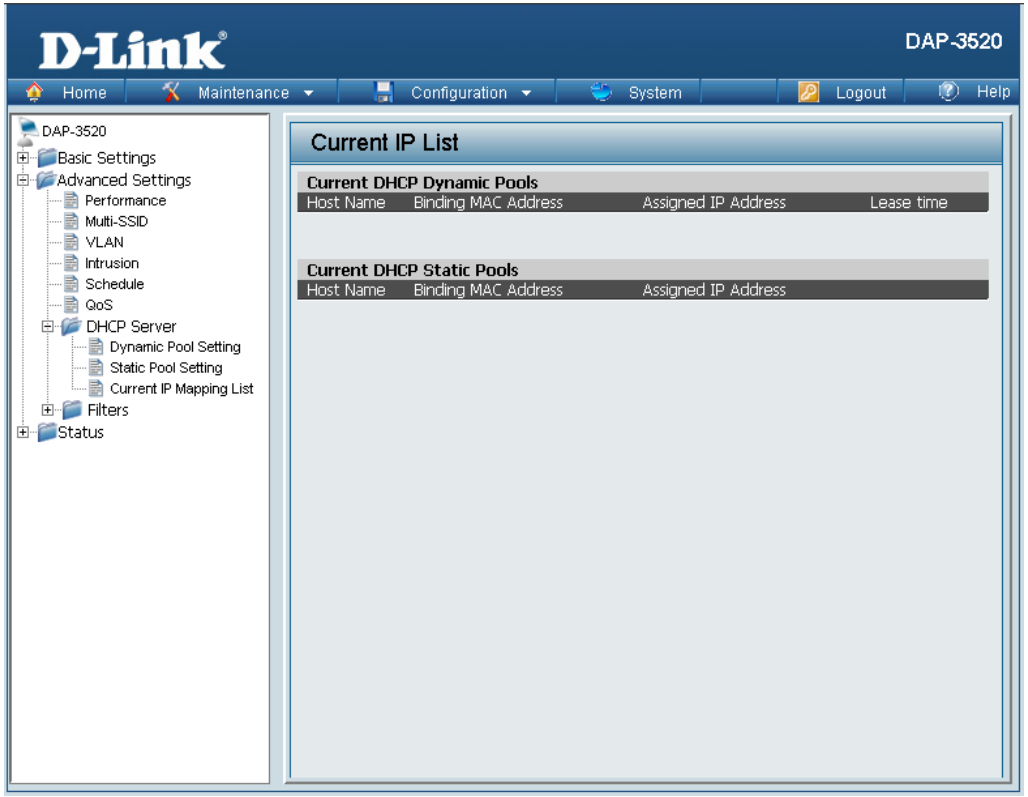
WINS:
Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

DNS:
Enter the Domain Name System (DNS) server address for the wireless network. The DNS server translates domain names such as www.dlink.com into IP addresses.

Domain Name:
Specify the domain name for the network.

Current IP Mapping List

This window displays information about the current assigned DHCP dynamic and static IP address pools. This information is available when you enable DHCP server on the AP and assign dynamic and static IP address pools.



Current DHCP Dynamic Pools:
These are IP address pools the DHCP server has assigned using the dynamic pool setting.

Host Name:
The host name of the client.

Binding MAC Address:
The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.

Assigned IP Address:
The current corresponding DHCP-assigned 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 the IP address pools of the DHCP server assigned through the static pool settings.

Host Name:
The host name of the client.

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.

Filters

Wireless MAC ACL

Wireless Band:
Displays the current wireless band rate.

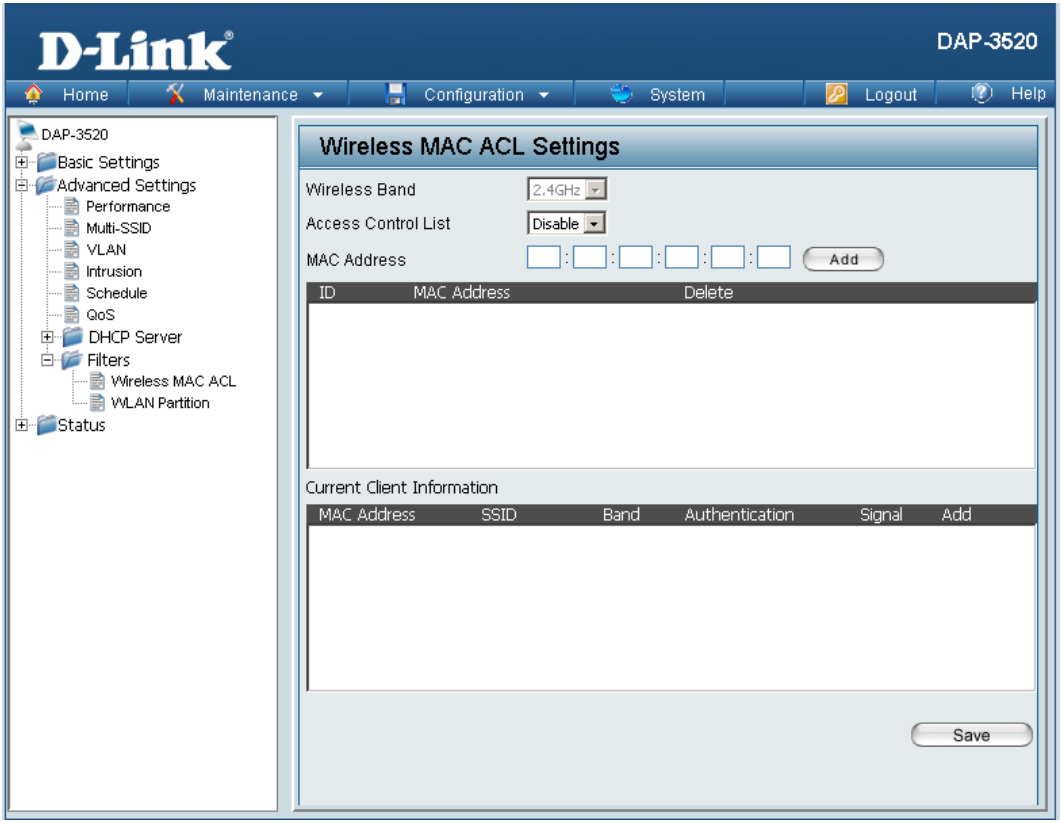
Access Control List:
Select **Disable** to disable the filters function.

Select **Accept** to accept only those devices with MAC addresses in the Access Control List. All other devices not on the list will be rejected.

Select **Reject** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

MAC Address:
Enter each MAC address that you wish to include in your filter list, and click **Apply**.

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



WLAN Partition

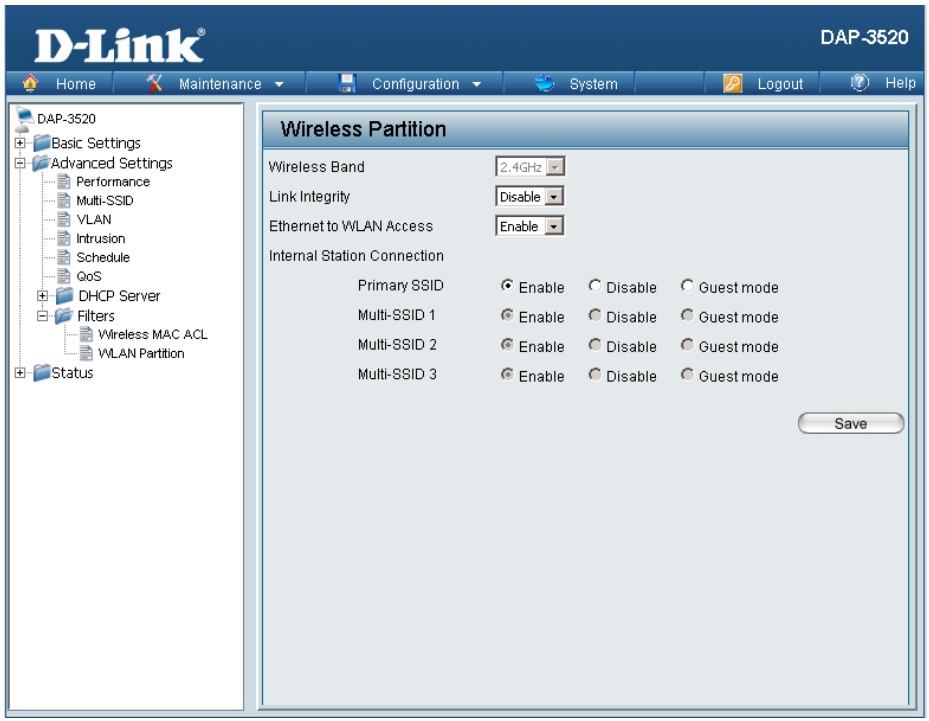
Wireless Band:
Displays the current wireless band rate.

Link Integrity:
Select **Enable** or **Disable**.

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

Internal Station Connection:
The default value is **Enable**, which allows stations to inter-communicate by connecting to a target AP. When disabled, wireless stations cannot exchange data through the AP.

Guest mode is for creating a hotspot. Clients connecting to this SSID will not be able to see other wireless devices on this wireless network. They will only be able to network to devices connected via the Ethernet port on the DAP-3520.



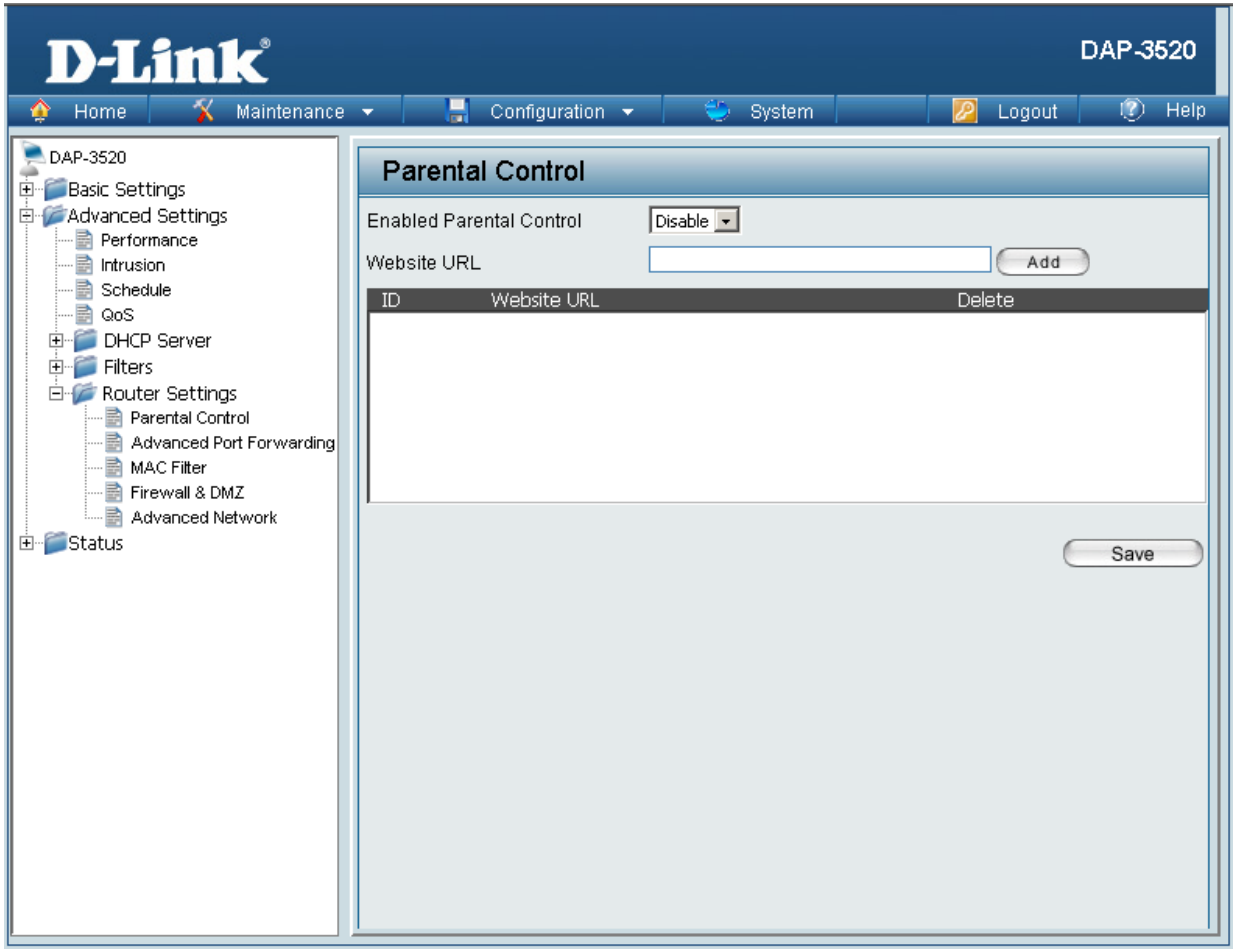
Router Settings

Parental Control

Note: *The following features are only available when in WISP Client Router Mode.*

Enabled Parental Control:
Select **Allow** to allow computers access to these sites only, select **Deny** to deny computers access to these sites only, or **Disable** to turn off the parental control feature.

Website URL:
Enter the keywords or URLs that you want to block (or allow). Any URL with the keyword in it will be blocked.



Advance Port Forwarding

Note: *The following features are only available when in WISP Client Router Mode.*

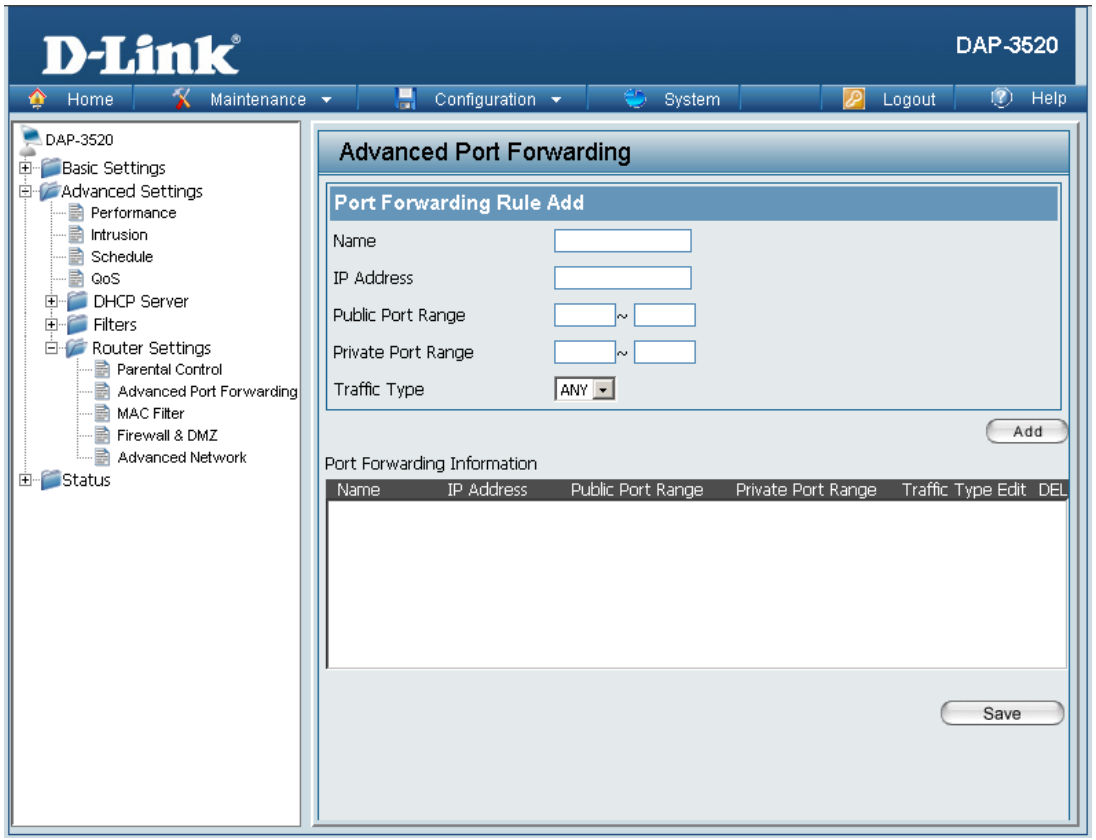
Name:
Enter a name for the rule.

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

Public Port Range:
Enter the public port or ports that you want to open. If you want to open one public port, enter the same port in both boxes.

Private Port Range:
Enter the private port or ports that you want to open. If you want to open one private port, enter the same port in both boxes.

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

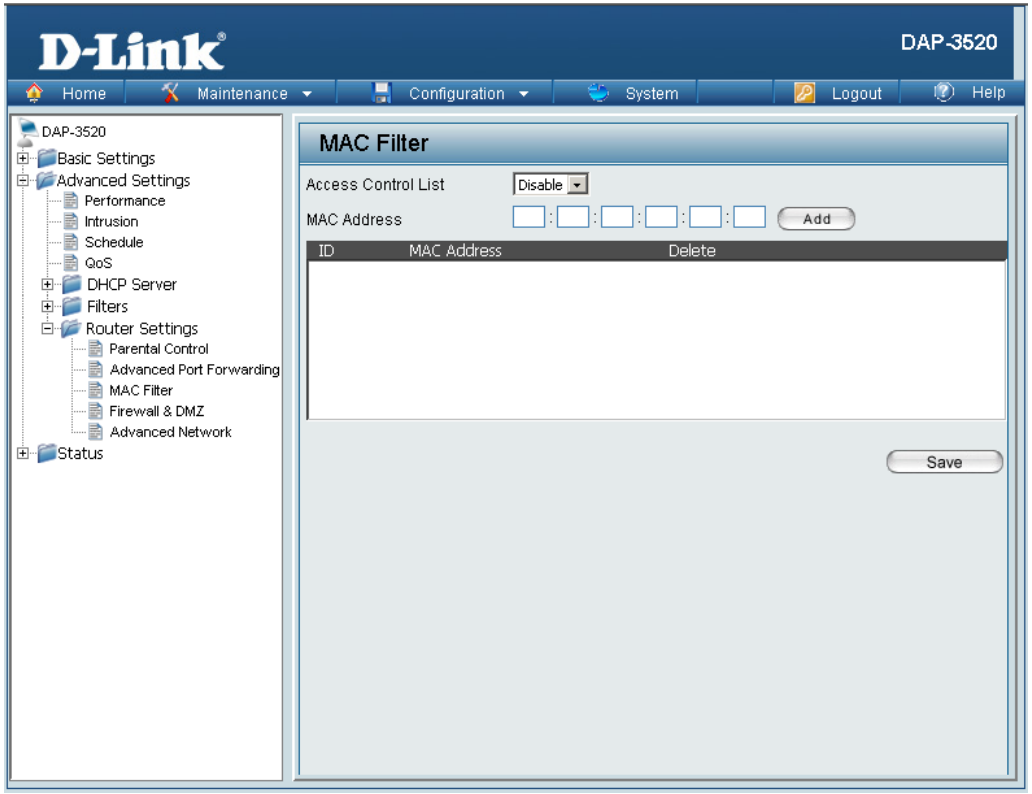


MAC Filter

Note: *The following features are only available when in WISP Client Router Mode.*

MAC Control List:
Select **Enable** or **Disable**

MAC Address:
Enter the MAC that you wish to be filtered out and click **Add** to add it to the list.



Firewall & DMZ

Note: *The following features are only available when in WISP Client Router Mode.*

Enable DMZ:
Check this box to enable DMZ.

DMZ IP Address:
Enter the IP address of the computer you would like to open all ports to.

Enable SPI:
Check this box to enable Stateful Packet Inspection (SPI).

Name:
Choose a name for the firewall rule.

Source Interface:
Toggle among **Source**, **LAN**, and **WAN**. This is the TCP/UDP port on either the LAN or WAN side.

Source IP:
Enter a beginning and ending source IP address.

Protocol:
Select the transport protocol that will be used for the filter rule (**All**, **TCP**, **UDP**, or **ICMP**).

Action:
Select to **Allow** or **Deny** transport of the data packets according to the criteria defined in the rule.

Destination Interface:
Toggle among **Dest**, **LAN**, and **WAN**. This is the TCP/UDP port on either the LAN or WAN side.

Destination IP:
Enter a beginning and ending destination IP address.

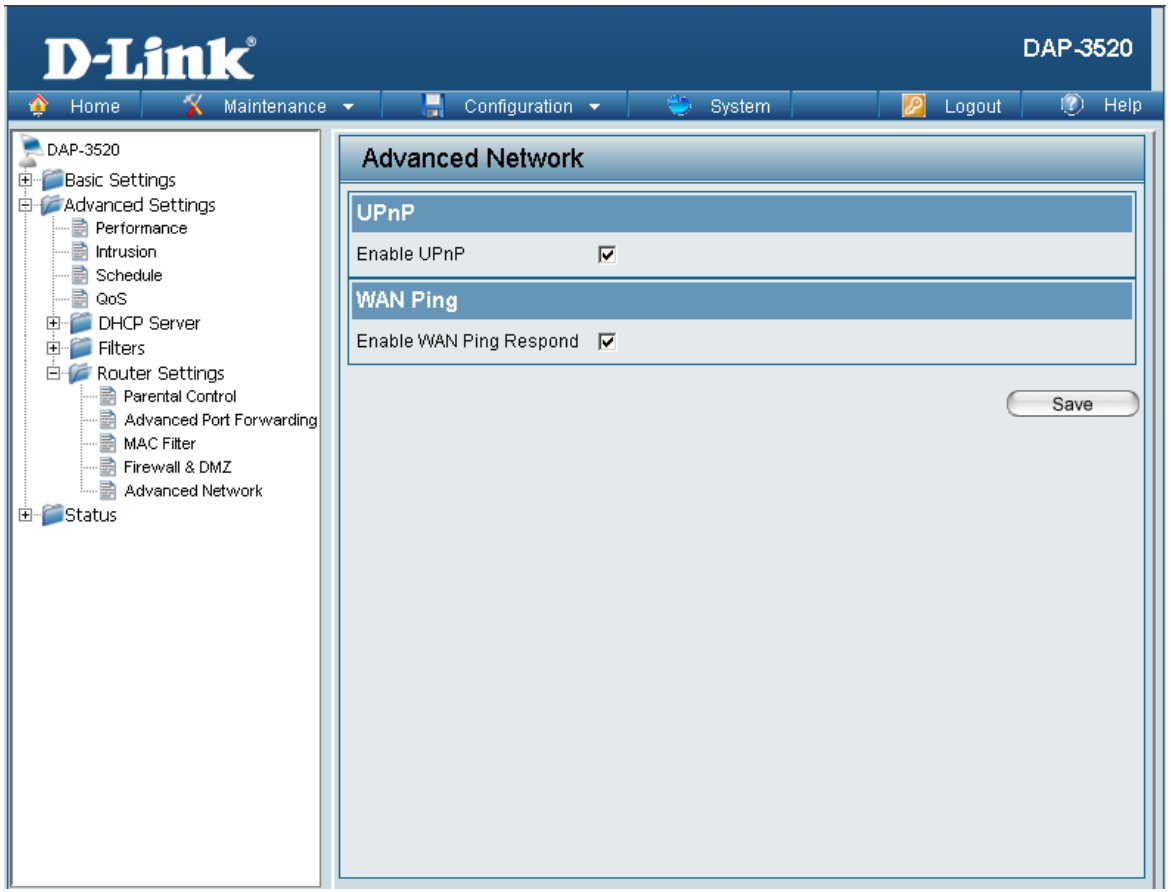
Port Range:
Enter the desired port range for the filter rule.

Advanced Network

Note: *The following features are only available when in WISP Client Router Mode.*

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

Enable WAN Ping Respond:
Unchecking the box will not allow the DAP-3520 to respond to Pings. Blocking the Ping may provide some extra security from hackers. Tick this check box to allow the WAN port to be “Pinged”.

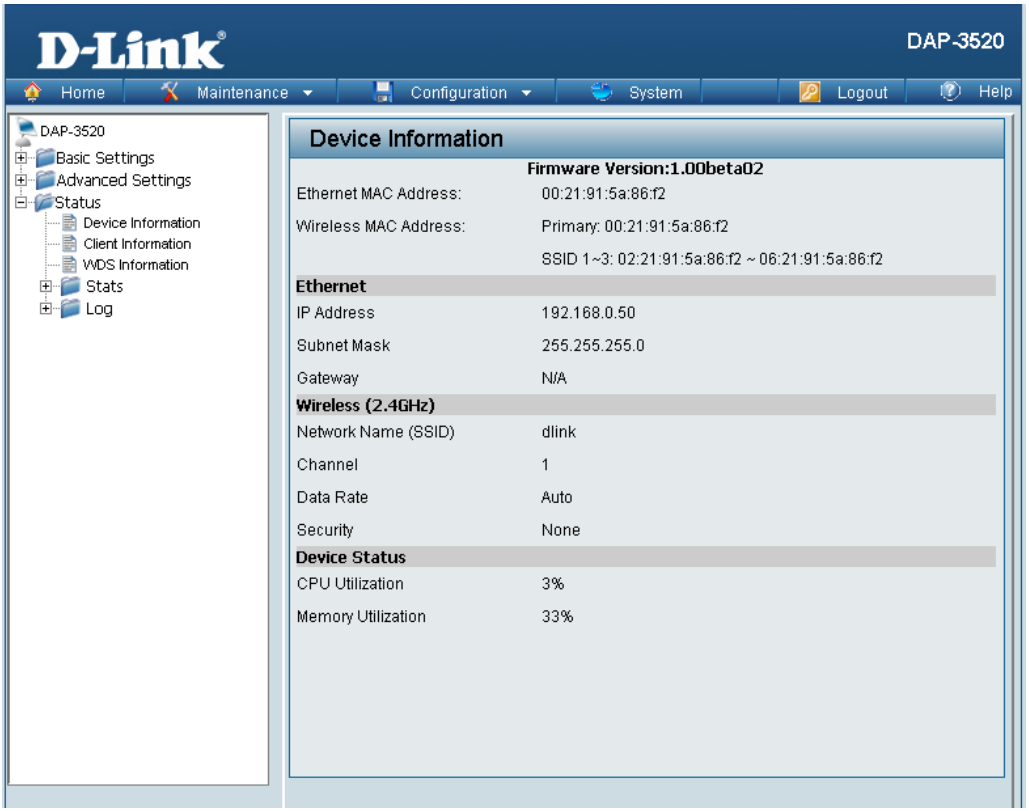


Status

Device Information

Device Information:

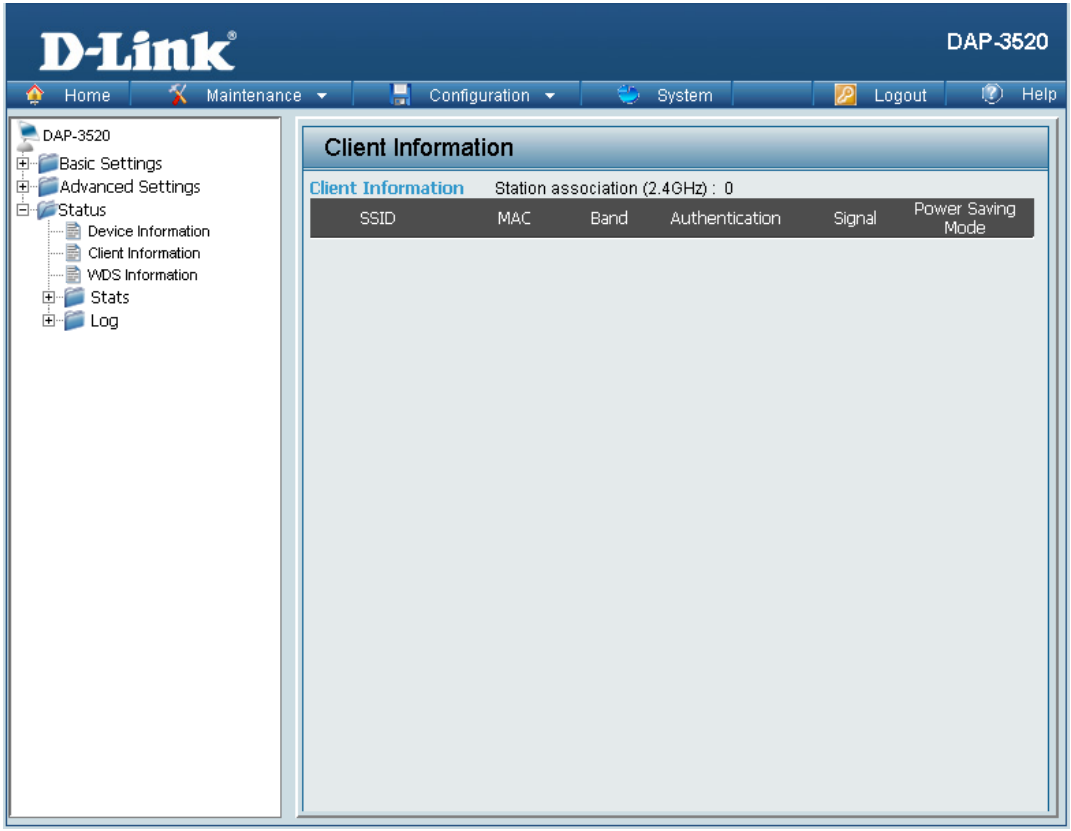
This read-only window displays the configuration settings of the DAP-3520, including the firmware version and the device's MAC address.



Client Information

Client Information:
This window displays the wireless client information for clients currently connected to the DAP-3520.

The following information is available for each client communicating with the DAP-3520.



SSID:
Displays the SSID of the client.

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.

WDS Information

WDS Information:
This window displays the Wireless Distribution System information for clients currently connected to the DAP-3520.

The following information is available for each client communicating with the DAP-3520.

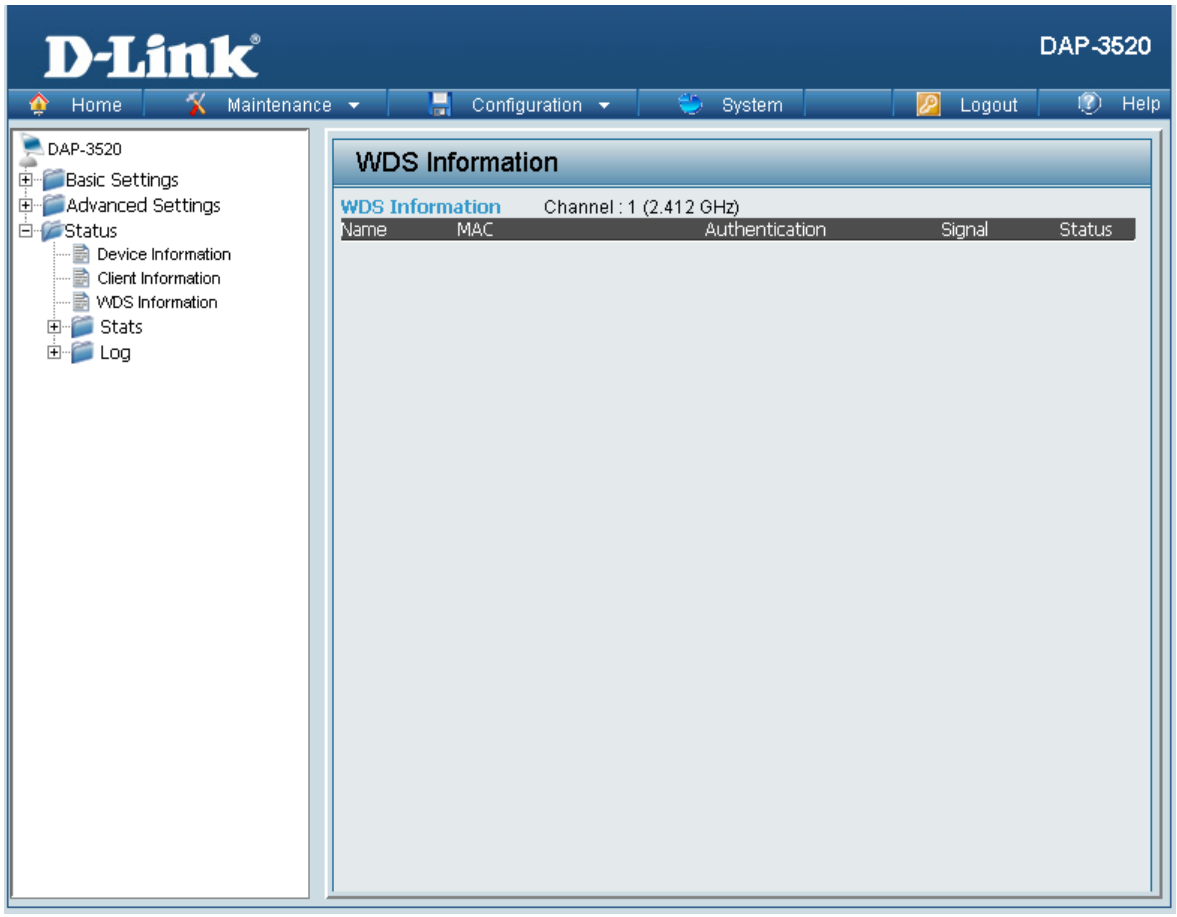
Name:
Displays the name of the client.

MAC:
Displays the MAC address of the client.

Authentication:
Displays the type of authentication being used.

Signal:
Displays the WDS link signal strength.

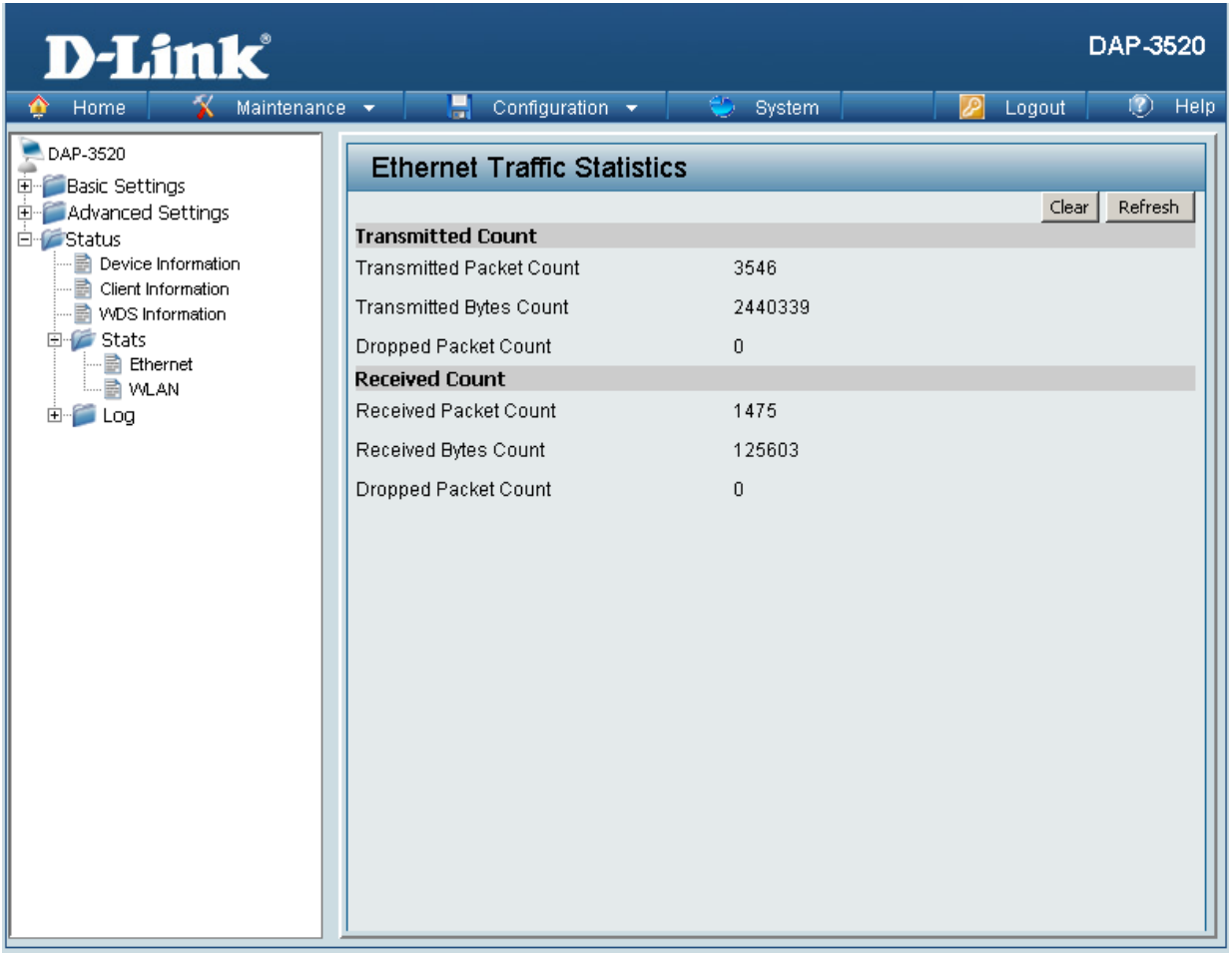
Status:
Displays the status of the power saving feature.



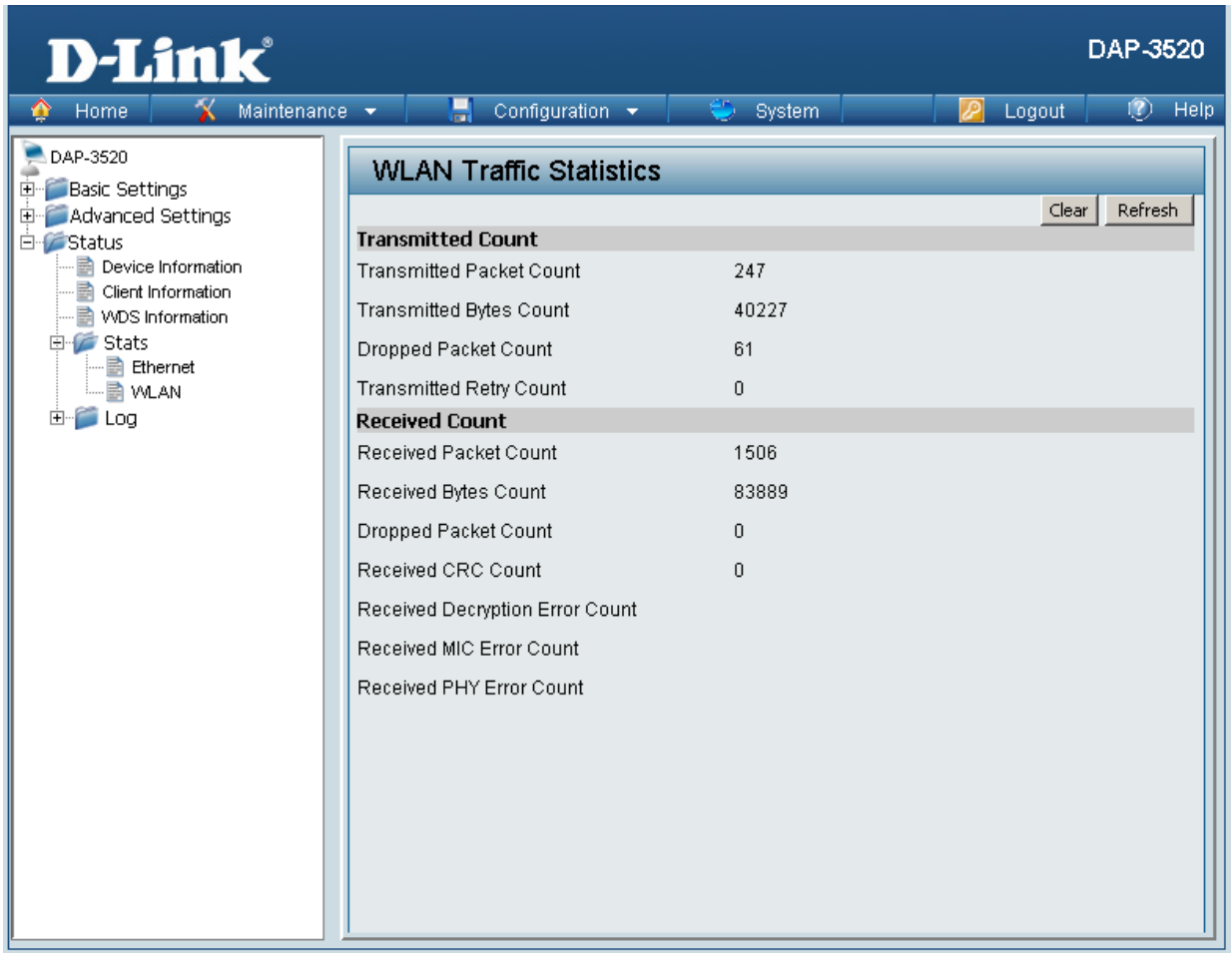
Stats

Ethernet

Ethernet Traffic Statistics:
This page displays transmitted and received count statistics for packets and bytes.



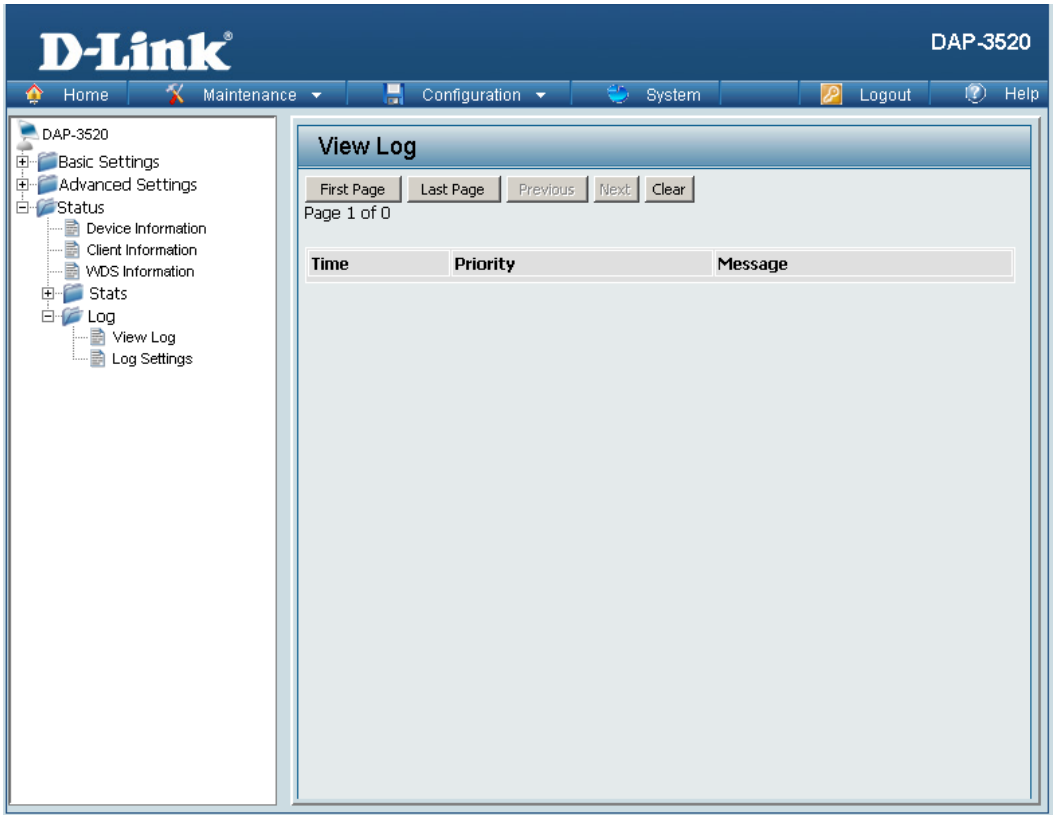
WLAN Traffic Statistics:
This page displays wireless network statistics for data throughput, transmitted and received frames, and frame errors.



Log

View Log

View Log:
The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.



Log Settings

Log Server/IP Address:
Enter the IP address of the server you would like to send the DAP-3520 log to.

Log Type:
Check the box for the type of activity you want to log. There are three types: System Activity, Wireless Activity, and Notice.

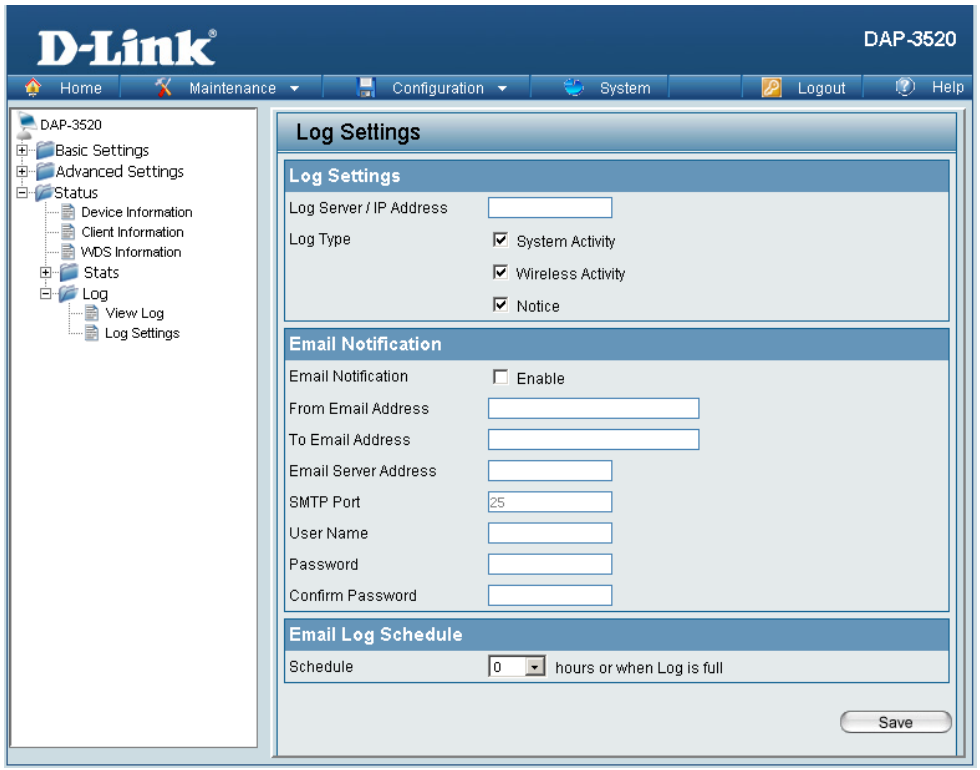
Email Notification:
Click to Enable email notification.

From Email Address:
Enter the sender's e-mail address. This field does not require a valid e-mail address. However, if your e-mail client is filtering spam, make sure you allow this address to be received.

To Email Address:
Enter the e-mail address you want to send alerts to. This address must correspond with the SMTP server configured above.

Email Server Address:
Enter the IP address of the server you would like to send the DAP-3520 log to.

SMTP Port:
Enter a TCP port number to relay outbound mail to your mail server. The default port is **25**.

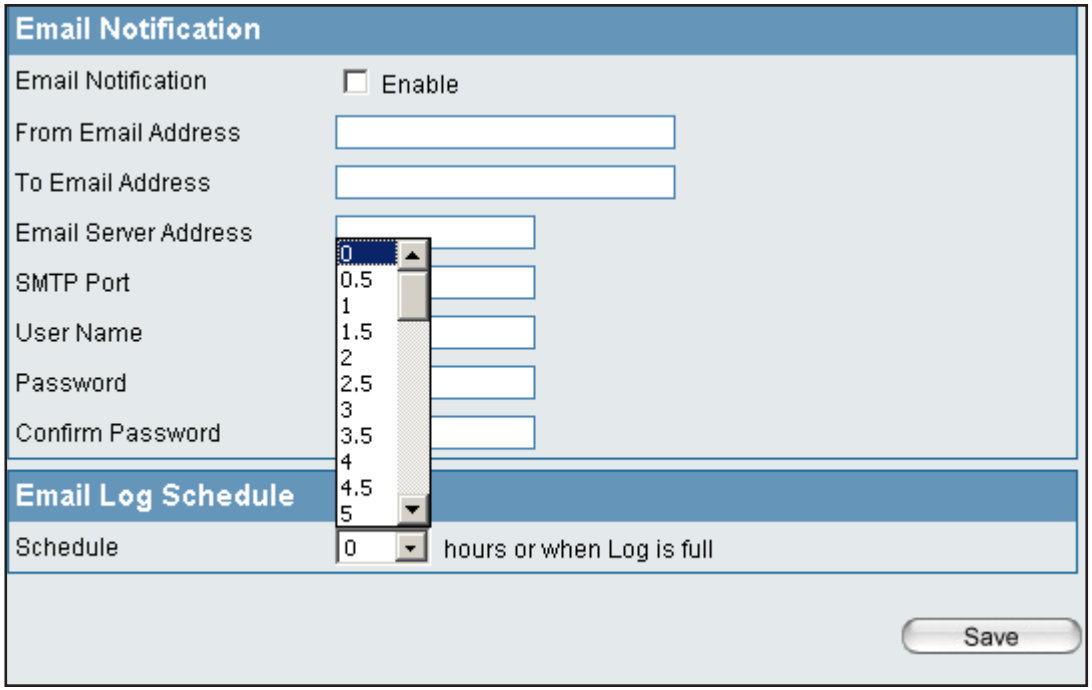


User Name:
Enter an appropriate user name for your e-mail account.

Password:
Enter an appropriate password for your e-mail account.

Confirm Password:
Retype the password for your e-mail account.

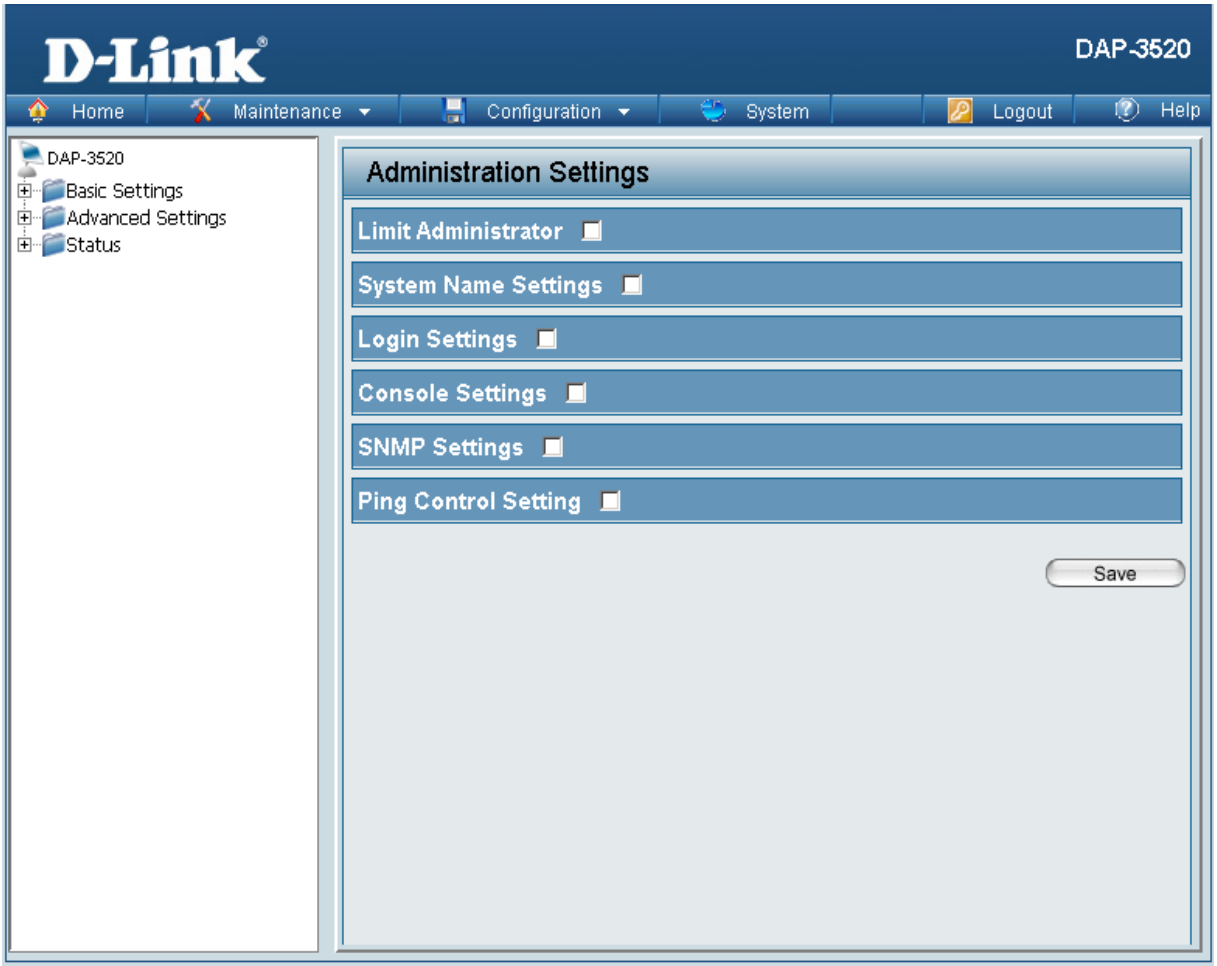
Schedule:
Use the drop-down menu to select the number of hours before mail will be sent to the server. For example, if a value of **2** is selected, mail will be sent to the server every two hours. However, if the log entry is full between 0 and 2 hours, mail will also be sent to the server and then the log entry will be automatically cleared.



Maintenance

Administrator Settings

Check one or more of the six main categories to display the various hidden administrator parameters and settings displayed on the next five pages.

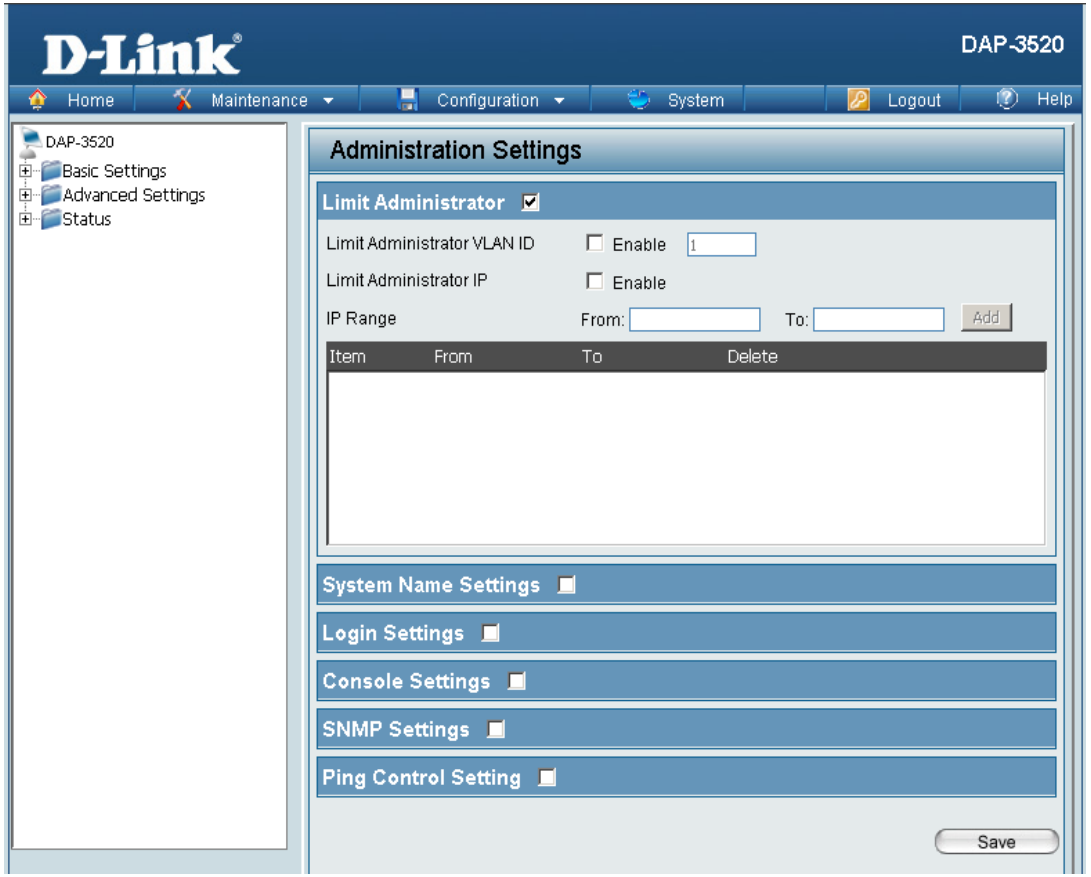


Limit Administrator

Limit Administrator VLAN ID:
Check the box provided and then enter the specific VLAN ID that the administrator will be allowed to log in from.

Limit Administrator IP:
Check to enable the Limit Administrator IP address.

IP Range:
Enter the IP address range that the administrator will be allowed to log in from and then click the **Add** button.

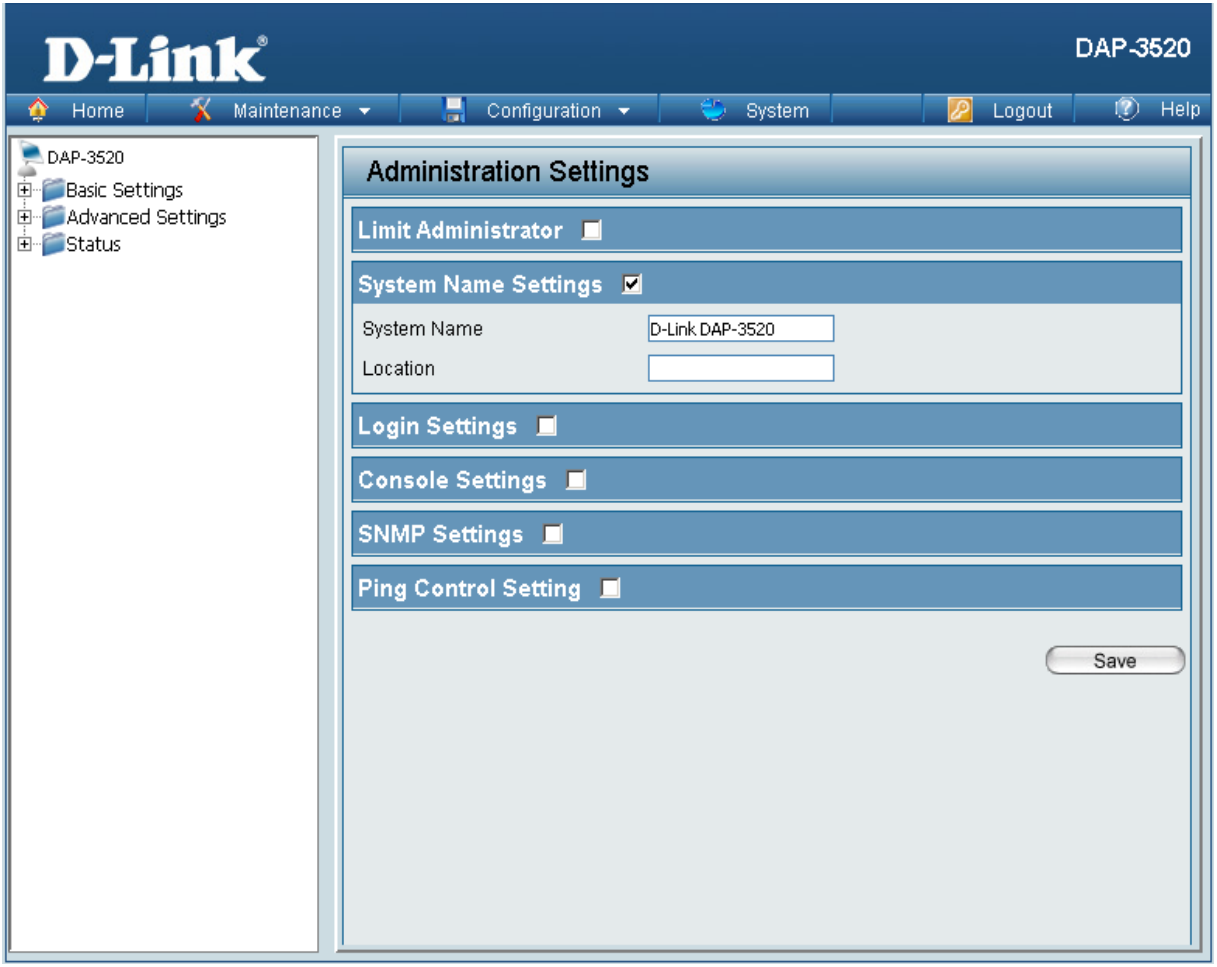


System Name Settings

System Name Settings:
Each of the six main categories display various hidden administrator parameters and settings.

System Name:
The name of the device. The default name is **D-Link DAP-3520**.

Location:
The physical location of the device, e.g. office.



Login Settings

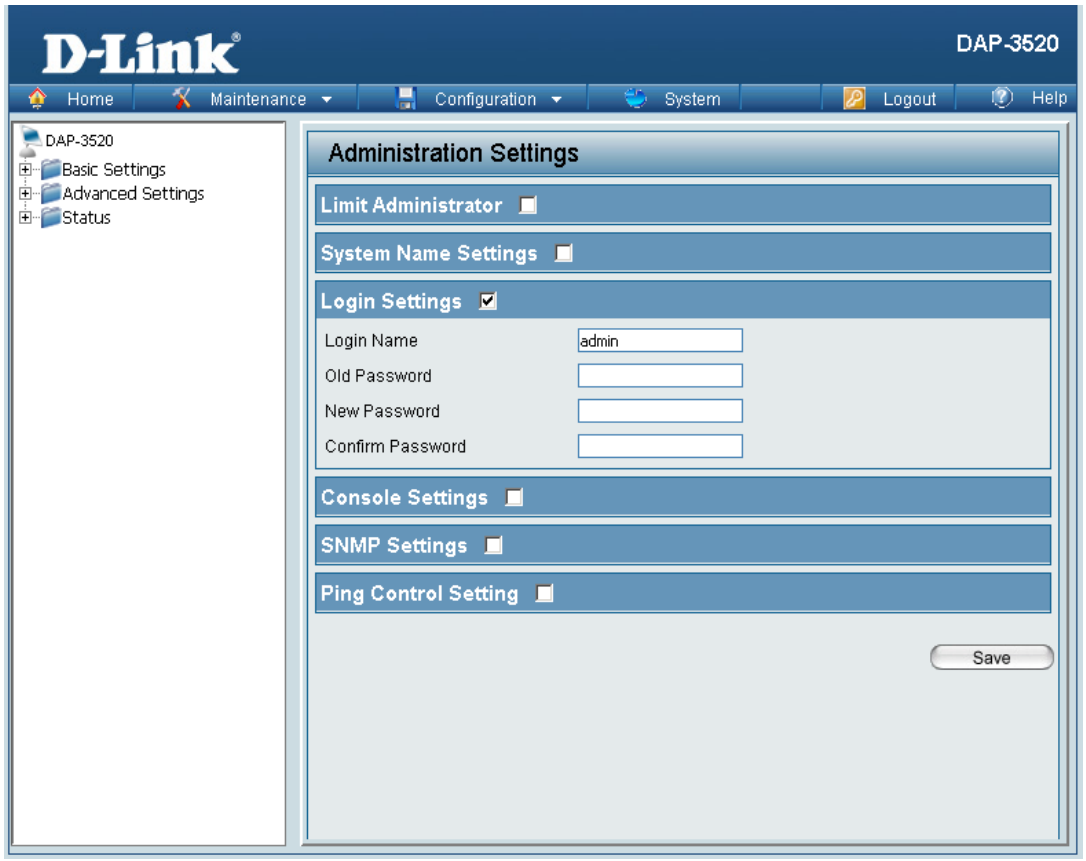
Each of the six main categories display various hidden administrator parameters and settings.

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. The password is case-sensitive. “A” is a different character than “a.” The length should be between 0 and 12 characters.

Confirm Password:
Enter the new password a second time for confirmation purposes.



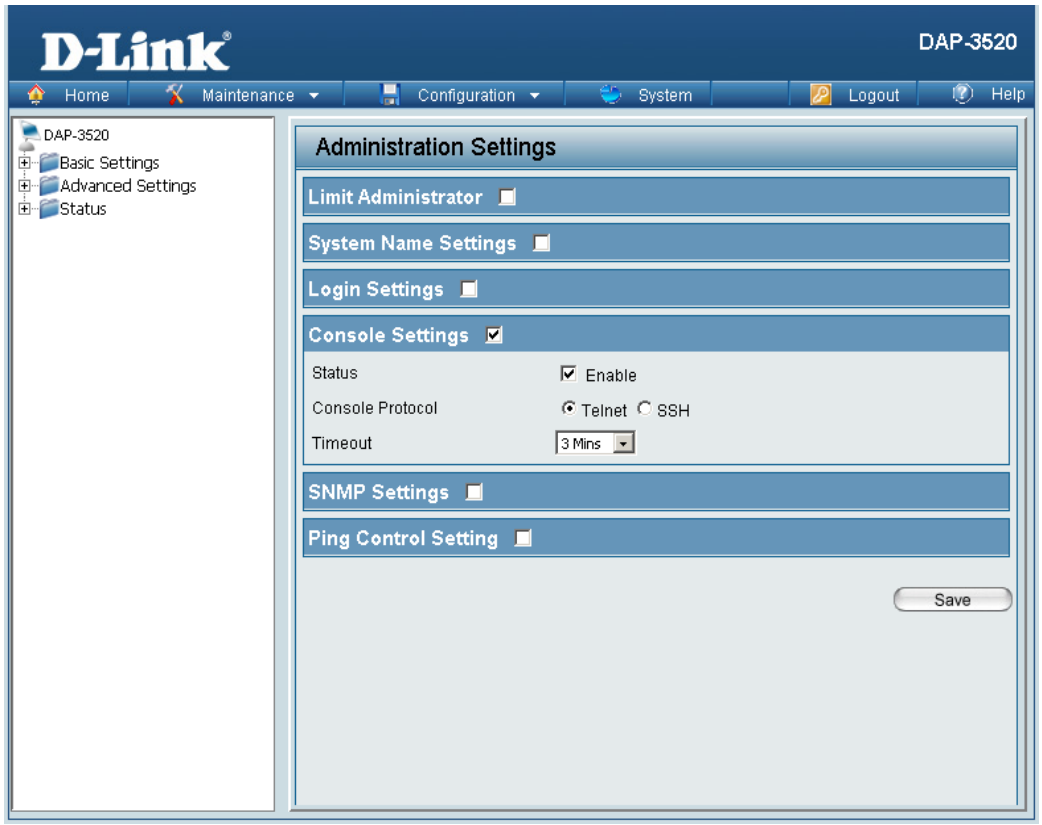
Console Settings

Each of the six main categories display various hidden administrator parameters and settings.

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

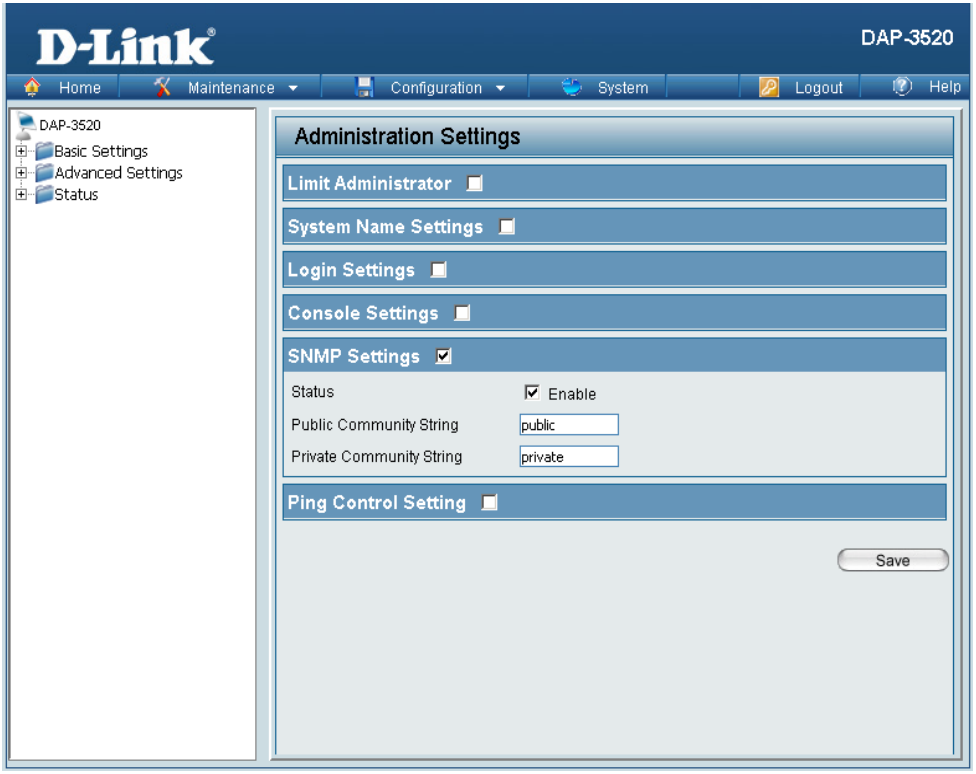
Console Protocol:
Select the type of protocol you would like to use, **Telnet** or **SSH.**

Timeout:
Set to **1 Min**, **3 Mins**, **5 Mins**, **10 Mins**, **15 Mins** or **Never**.



SNMP Settings

Each of the six main categories display various hidden administrator parameters and settings.



Status:
Check the box to enable the SNMP functions. This is enabled by default.

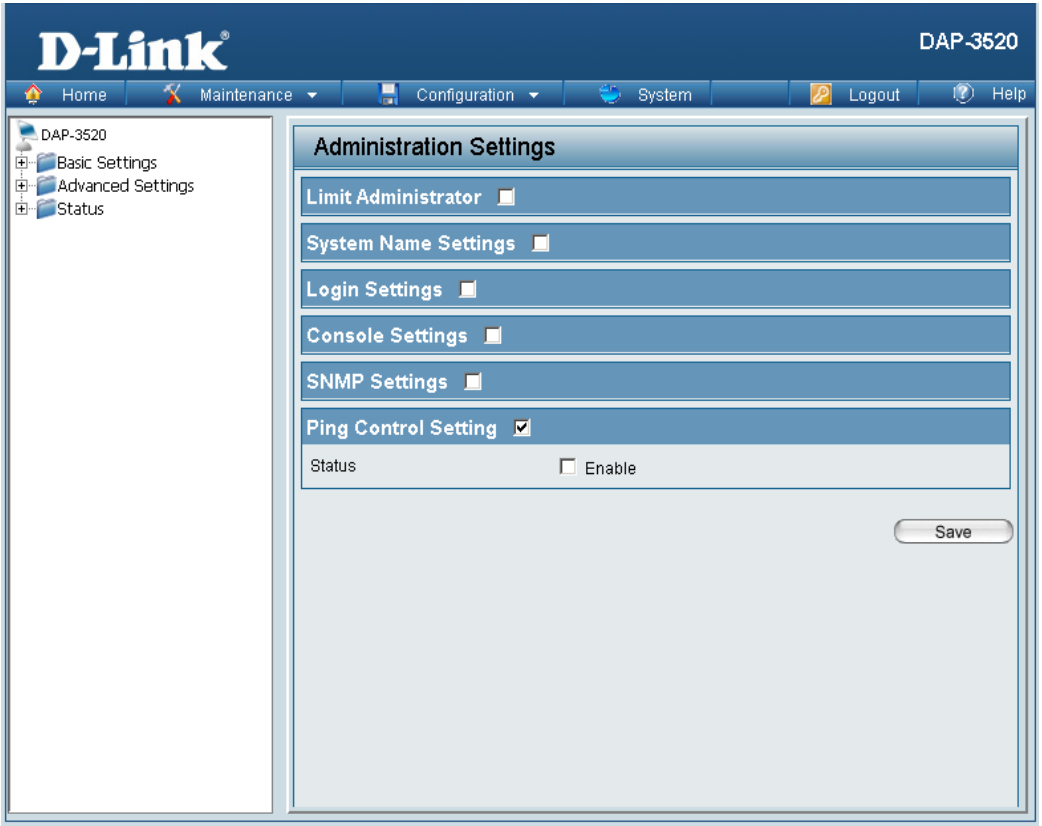
Public Community String:
Enter the public SNMP community string.

Private Community String:
Enter the private SNMP community string.

Ping Control Setting

Each of the six main categories display various hidden administrator parameters and settings.

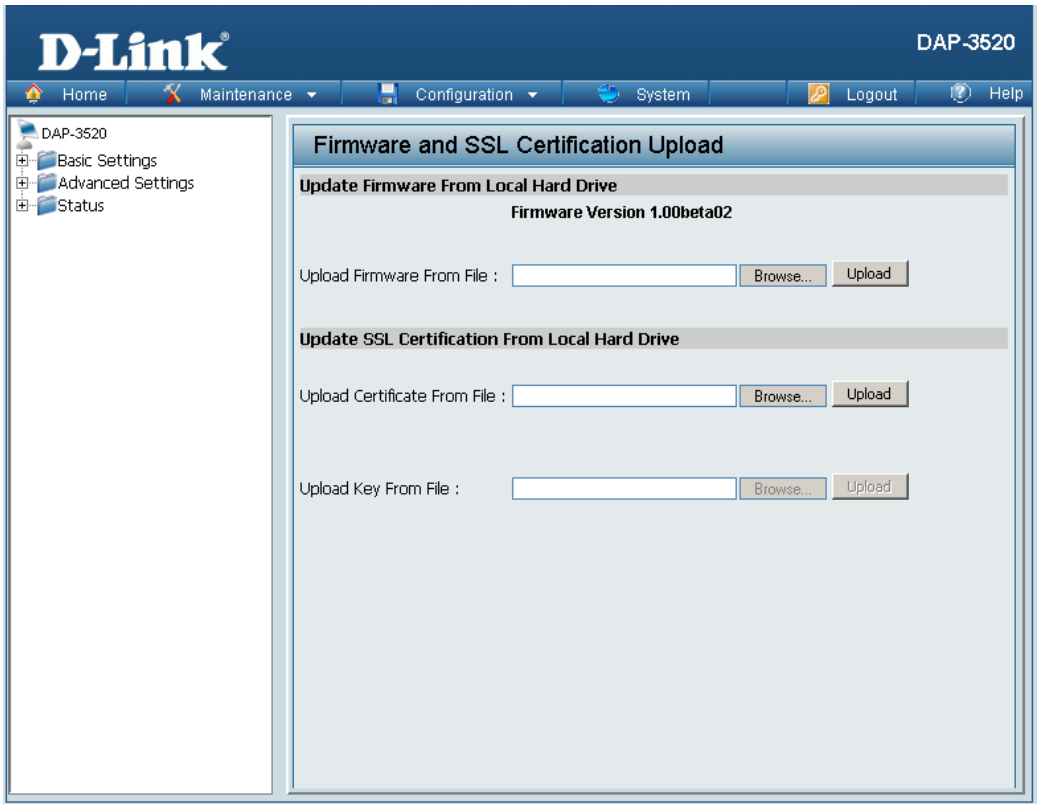
Status:
Check the box to enable Ping control.



Firmware and SSL Certification Upload

Upload Firmware From Local Hard Drive:
The current firmware version is displayed above the file location field. After downloading the most recent version of firmware for the DAP-3520 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. Please do not turn the power off while upgrading.

Upload SSL Certification From Local Hard Drive:
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-3520.

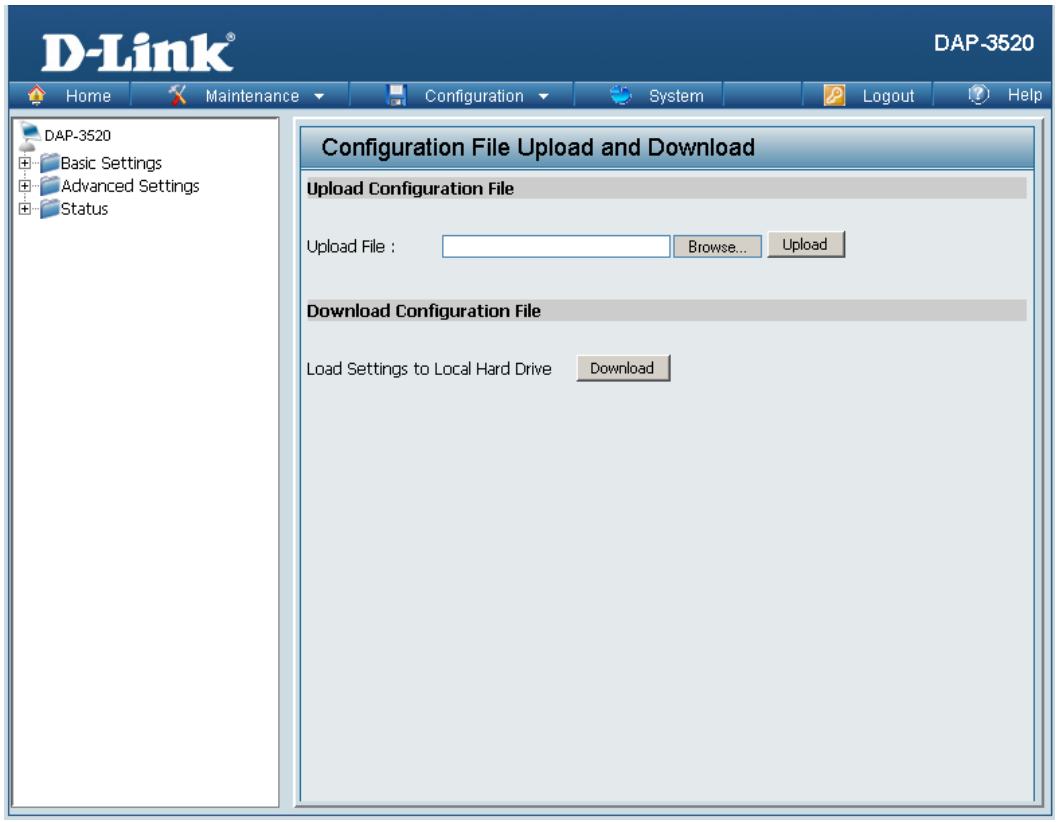


Configuration File

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-3520.

Download Configuration File:
Click **Download** to save the current DAP-3520 configuration to your local computer.

Note that if you save one configuration with the administrator's password now, after resetting your DAP-3520, and then updating to this saved configuration file, the password will be gone.



Time and Date

Current Time:
Displays the current time and date settings.

Time Zone:
Use the drop-down menu to select your correct Time Zone.

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

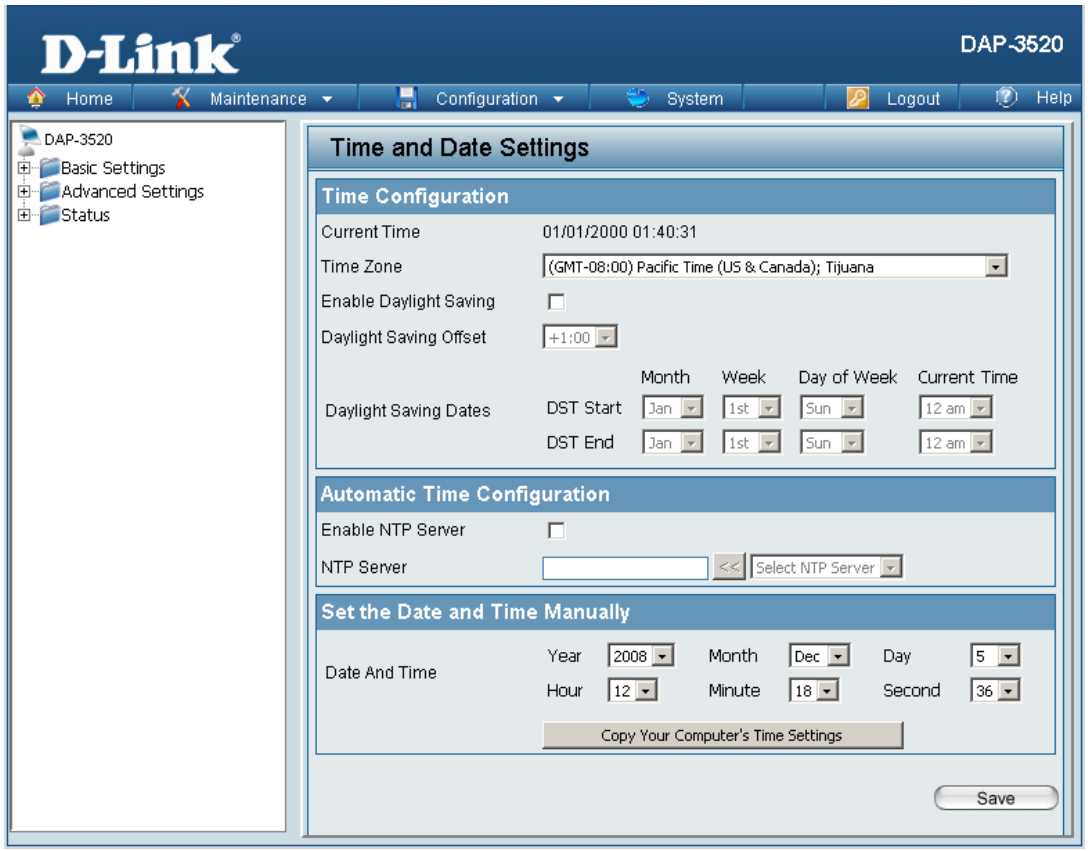
Daylight Saving Offset:
Use the drop-down menu to select the correct Daylight Saving offset.

Daylight Saving Dates:
Use the drop-down menu to select the correct Daylight Saving offset.

Enable NTP Server:
Check to enable the AP to get system time from an NTP server.

NTP Server:
Enter the NTP server IP address.

Set the 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).

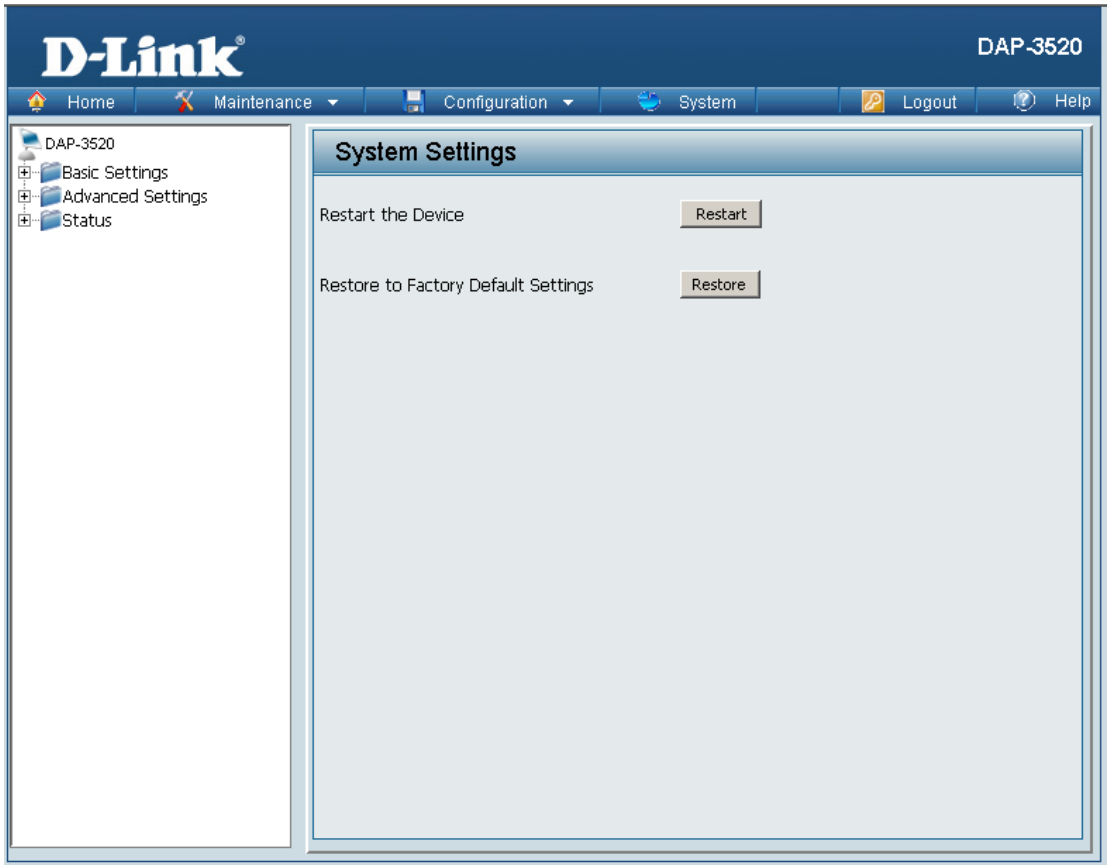


System

System Settings

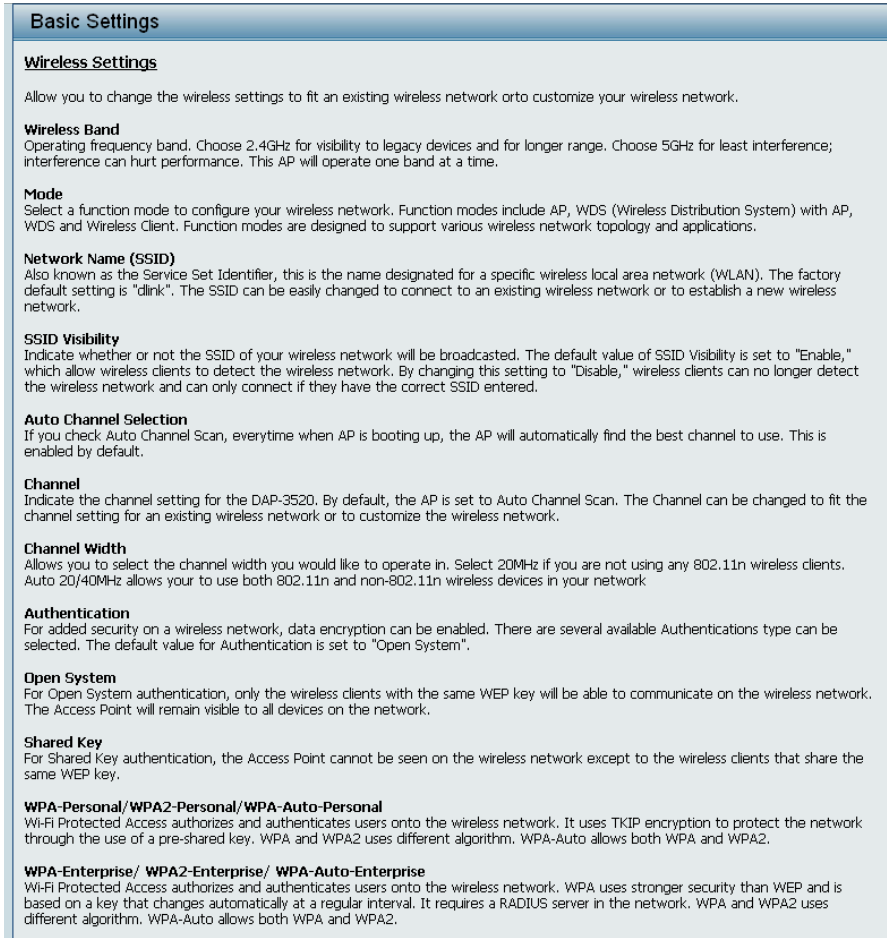
Restart the Device:
Click **Restart** to restart the DAP-3520.

Restore to Factory Default Settings:
Click **Restore** to restore the DAP-3520 back to factory default settings.



Help

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



Basic Settings

Wireless Settings

Allow you to change the wireless settings to fit an existing wireless network orto customize your wireless network.

Wireless Band
Operating frequency band. Choose 2.4GHz for visibility to legacy devices and for longer range. Choose 5GHz for least interference; interference can hurt performance. This AP will operate one band at a time.

Mode
Select a function mode to configure your wireless network. Function modes include AP, WDS (Wireless Distribution System) with AP, WDS and Wireless Client. Function modes are designed to support various wireless network topology and applications.

Network Name (SSID)
Also known as the Service Set Identifier, this is the name designated for a specific wireless local area network (WLAN). The 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 Visibility
Indicate whether or not the SSID of your wireless network will be broadcasted. The default value of SSID Visibility is set to "Enable," which allow wireless clients to detect the wireless network. By changing this setting to "Disable," wireless clients can no longer detect the wireless network and can only connect if they have the correct SSID entered.

Auto Channel Selection
If you check Auto Channel Scan, everytime when AP is booting up, the AP will automatically find the best channel to use. This is enabled by default.

Channel
Indicate the channel setting for the DAP-3520. 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.

Channel Width
Allows you to select the channel width you would like to operate in. Select 20MHz if you are not using any 802.11n wireless clients. Auto 20/40MHz allows your to use both 802.11n and non-802.11n wireless devices in your network

Authentication
For added security on a wireless network, data encryption can be enabled. There are several available Authentications type can be selected. The default value for Authentication is set to "Open System".

Open System
For Open System authentication, only the wireless clients with the same WEP key will be able to communicate on the wireless network. The Access Point will remain visible to all devices on the network.

Shared Key
For Shared Key authentication, the Access Point cannot be seen on the wireless network except to the wireless clients that share the same WEP key.

WPA-Personal/WPA2-Personal/WPA-Auto-Personal
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. It uses TKIP encryption to protect the network through the use of a pre-shared key. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

WPA-Enterprise/ WPA2-Enterprise/ WPA-Auto-Enterprise
Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. WPA uses stronger security than WEP and is based on a key that changes automatically at a regular interval. It requires a RADIUS server in the network. WPA and WPA2 uses different algorithm. WPA-Auto allows both WPA and WPA2.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-3520 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-3520.

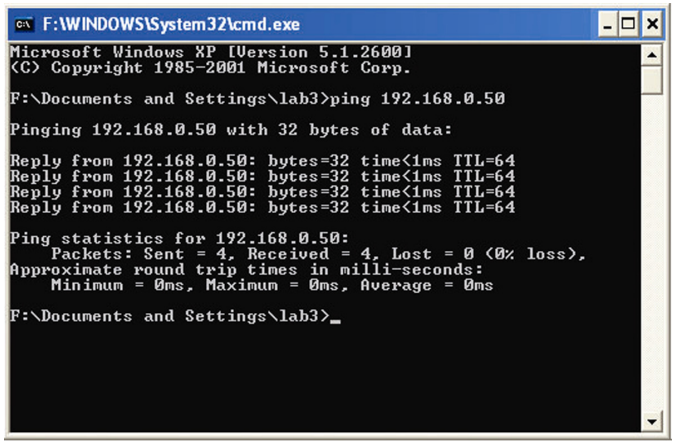
1. The computer used to configure the DAP-3520 cannot access the Configuration menu.

- Check if the LAN LED on the DAP-3520 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-3520.

Note: The default IP address of the DAP-3520 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.

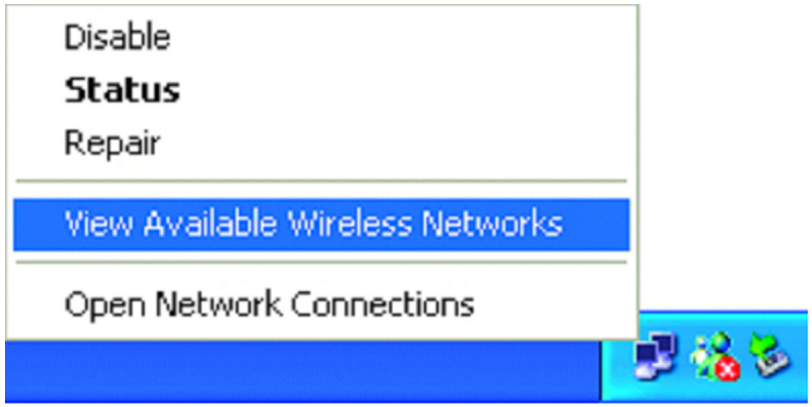
- Do a Ping test to make sure that the DAP-3520 is responding. Go to **Start**>**Run**>Type **Command**>Type **ping 192.168.0.50.** A successful ping will show four replies.

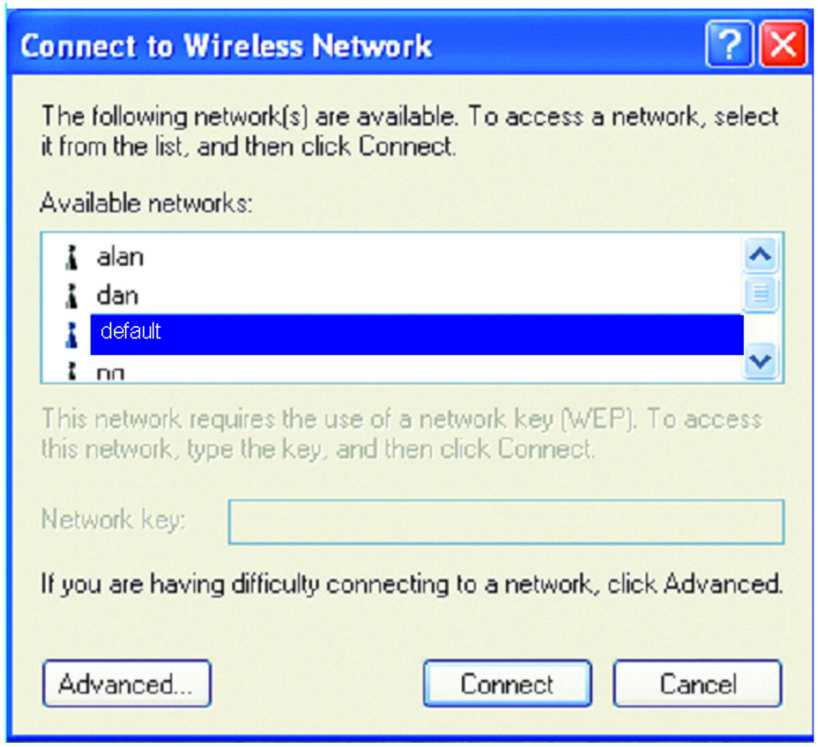
Note: If you have changed the default IP address, make sure to ping the correct IP address assigned to the DAP-3520.



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-3520 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 the **Local Area Connection** icon in the taskbar, then select the **Support** tab and the IP address will be displayed.

- If it is necessary to assign a Static IP Address to the wireless adapter. 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.*

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.

4. Why does my wireless connection keep dropping?

- Antenna Orientation - try different antenna orientations for the DAP-3520. 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-3520, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- Make sure that the SSID on the AP and the wireless client are exactly the same. If they are not, wireless connection cannot be established.
- Move the DAP-3520 and the wireless client into the same room and then test the wireless connection.
- Disable all security settings.
- Turn off your DAP-3520 and the client. Turn the DAP-3520 back on again, and then turn on the client.
- 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 2.4 GHz 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-3520, 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 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3af

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 802.11a:
- 54, 48, 36, 24, 18, 12, 9, and 6 Mbps

For 802.11b:
- 11, 5.5, 2, and 1 Mbps

For 802.11g:
- 54, 48, 36, 24, 18, 12, 9, and 6 Mbps

For 802.11n (draft): HT20/HT40
- 144.4/300, 130/270, 117/243, 104/216, 78/162, 66/135, 58.5/121.5, 52/108, 39/81, 26/54, 19.5/40.5, 12/27, and 6.5/13.5 Mbps

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

Operating Modes
- Access Point (AP)
- WDS with AP
- WDS
- Wireless Client
- WISP (Wireless Internet Service Provider) Client Router

LAN Port Speed
- 10/100/1000 Mbps

Wireless Frequency Range**

For 802.11a:
- 5.15 ~ 5.85GHz

For 802.11b/g:
- 2.4 ~ 2.4835GHz

For 802.11n:
- 2.4GHz Band: 2.4 ~ 2.4835GHz
- 5GHz Band: 5.15 ~ 5.85GHz

Operating Voltage
- PoE 48VDC +/-10%

Maximum Power Consumption
- 12.95 Watts

*Maximum wireless signal rate derived from IEEE Standard 802.11 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 throughout rate.

**Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-3520 is not supported in the 5.25~5.35GHz and 5.47 ~ 5.725GHz frequency ranges in some regions.

Radio and Modulation Type

For 802.11a/g/n:

- BPSK, QPSK, 16QAM, and 64QAM with OFDM

For 802.11b:

- DQPSK, DBPSK, DSSS, and CCK

Embedded Directional Antenna Peak Gain

- 8dBi Gain @2.4GHz
- 10dBi Gain @5GHz

Maximum Transmit Output Power

- 17 dBm@ 2.4 GHz
- 16 dBm @5 GHz

Maximum Effective Isotropic Radiated Power (EIRP)

- 28dBm @ 2.4 GHz
- 29dBm @5 GHz

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 Class B
- CE
- UL 60950
- IC
- C-Tick
- CSA
- Wi-Fi®

Ingress Protection Rating

- IP65

Weight

- 1.58 lbs (717g)

Dimensions

- L = 198 mm
- W = 163 mm
- H = 58 mm

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 1-877-354-6555, 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 ©2009 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 10dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50ohms.

Technical Support

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

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

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:
(877) 354-6555

D-Link Technical Support over the Internet:
http://support.dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:
(877) 354-6560

D-Link Technical Support over the Internet:
http://support.dlink.com

Registration

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

Version 1.1
March 5, 2009