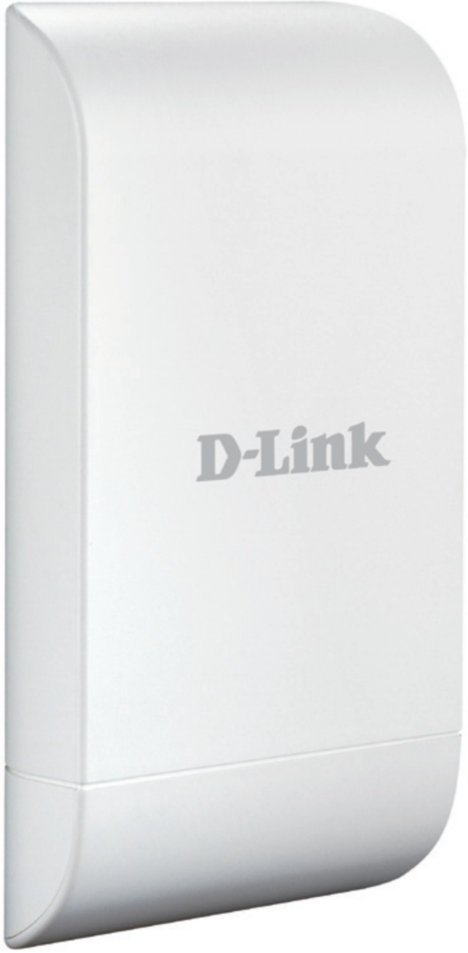
Version 3.0 | 21/05/2014



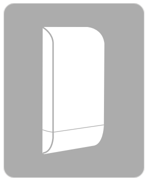
User Manual

Wireless N Exterior Access Point

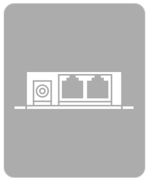
DAP-3410

Table of Contents

Package Contents

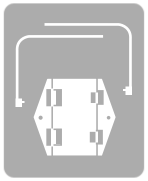


DAP-3410 Wireless N Exterior Access Point



Power Over Ethernet Injector

Power Adapter



Wall Mount

Quick Installation Guide

Note: Using a power supply with a different voltage rating or PoE injector than the one included with the DAP-3410 will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based Network • IEEE 802.11a/n wireless clients (AP Mode) • IEEE 802.11a/n wireless network (AP Mode)
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 and higher • Mozilla Firefox 12.0 and higher • Google™ Chrome 20.0 and higher • Apple Safari 4 and higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

D-Link, an industry leader in networking, introduces the new D-Link DAP-3410 Wireless N Exterior Access Point. With the ability to transfer files with a maximum wireless signal rate of up to 300 Mbps[1], the DAP-3410 gives you ability to add high-speed wireless network access to places outside of your internal networking environment. Additional operation modes such as WDS and WISP also make the DAP-3410 perfect for those needing to span longer distances wirelessly.

The DAP-3410 is Wi-Fi IEEE 802.11n compliant, meaning that it can connect and interoperate with other 802.11n compatible wireless client devices. The DAP-3410 is also compatible with devices that comply with the 802.11a standard. With its Setup Wizard, the DAP-3410 ensures that you will be up and running a wireless network in just a matter of minutes.

The DAP-3410 features Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) to provide an enhanced level of security for wireless data communications. The DAP-3410 also includes additional security features to keep your wireless connection safe from unauthorized access.

[1] 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.

Ultimate Performance

The D-Link Wireless N Exterior Access Point (DAP-3410) is an 802.11n compliant device that delivers real world performance of up to 300 Mbps[2], much faster than an 802.11g wireless connection (also faster than a 100 Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage outside of your normal internal networking environment. Built to withstand harsh environments, the DAP-3410 also excels in connecting separate networks that cannot be joined physically using traditional medium. The built-in 15dBi sector antenna is designed to deliver high powered performance, ensuring that wireless coverage will cover even hard to reach locations.

Multiple Operation Modes

The DAP-3410 features seven different operation modes, allowing it to adapt to any situation. As a standard wireless access point (AP) the DAP-3410 can connect to a wide range of devices that are 802.11 a/n compliant. In wireless distribution system (WDS) mode it can expand current wireless coverage without the need for a wired backbone link. As a wireless client it can connect to an existing AP, and expand the network physically with the two built-in 10/100 Ethernet ports. Repeater mode will extend current wireless coverage eliminating dead spots and weak signals.

Also built into the DAP-3410 is WISP mode, which expands functionality for long range communications by including the ability to function as a client or repeater. In WISP Repeater mode, the AP wirelessly connects to a WISP (Wireless Internet Service Provider) AP and repeats the signal received from the WISP. In this mode, the AP also acts as a router for both wireless and wired clients on your LAN. In WISP Client Router mode, the AP wirelessly connects to a WISP (Wireless Internet Service Provider) AP and acts as a router for wired clients on the LAN, to allow the client to still access the Internet even though it is using wireless technology.

Total Security

The DAP-3410 supports 64/128-bit WEP data encryption and WPA/WPA2 security functions. In addition, it provides MAC Address Filtering to control user access, and the Disable SSID Broadcast function to limit unauthorized access to the internal network. Network administrators have multiple options for managing the DAP-3410, including Web (HTTP) or Secured Web (HTTPS). For advanced network management, administrators can use SNMP v1, v2c, v3 to configure and manage access points.

[2] Maximum wireless signal rate derived from IEEE Standard 802.11g and 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-3410 provides an up to 300 Mbps[2] 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.

- **Compatible with IEEE802.11a/n Devices -** The DAP-3410 is still fully compatible with the 802.11a/n standards, so it can connect with existing 802.11a/n adapters.

- **Built-in High Gain Sector Antenna -** The DAP-3410 comes equipped with a high powered 15 dBi antenna that helps to provide better wireless coverage and increases signal strength.

- **PoE Passthrough -** The DAP-3410 supports PoE (Power over Ethernet) which enables it to be supplied with Ethernet over a power cable. It can also power D-Link surveillance cameras such as the DCS-3716, DCS-6113, and DCS-7110.

- **Convenient Installation -** The DAP-3410 features a wall/pole mount in the rear for easy setup on poles or walls.

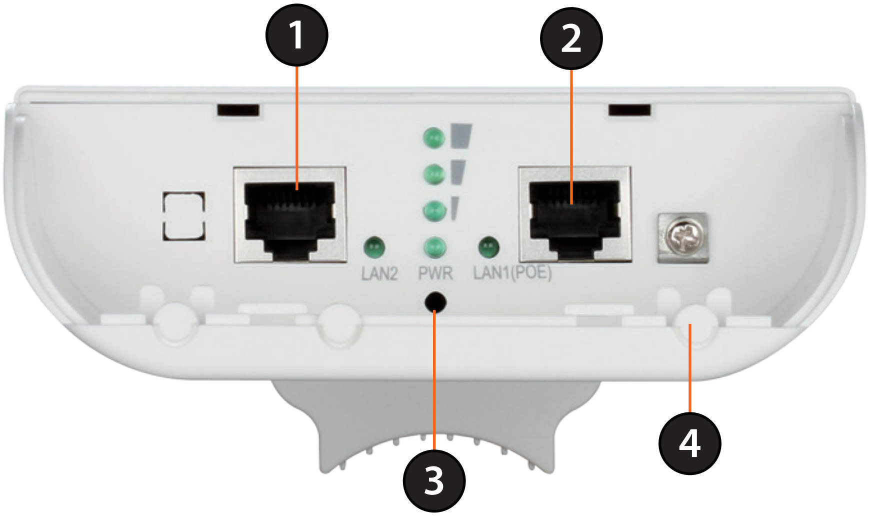
- **Rugged Construction -** The DAP-3410 is built to withstand harsh environments, and is compliant with the Waterproof IPX6 Standard.[3]

[2] Maximum wireless signal rate derived from IEEE Standard 802.11g and 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.

[3] IPX6 standard means the device is protected from low pressure jets of water from all directions - limited ingress permitted. It is recommended to place this device under a roof, shelter or in weather-proof box when in severe weather environment.

Hardware Overview

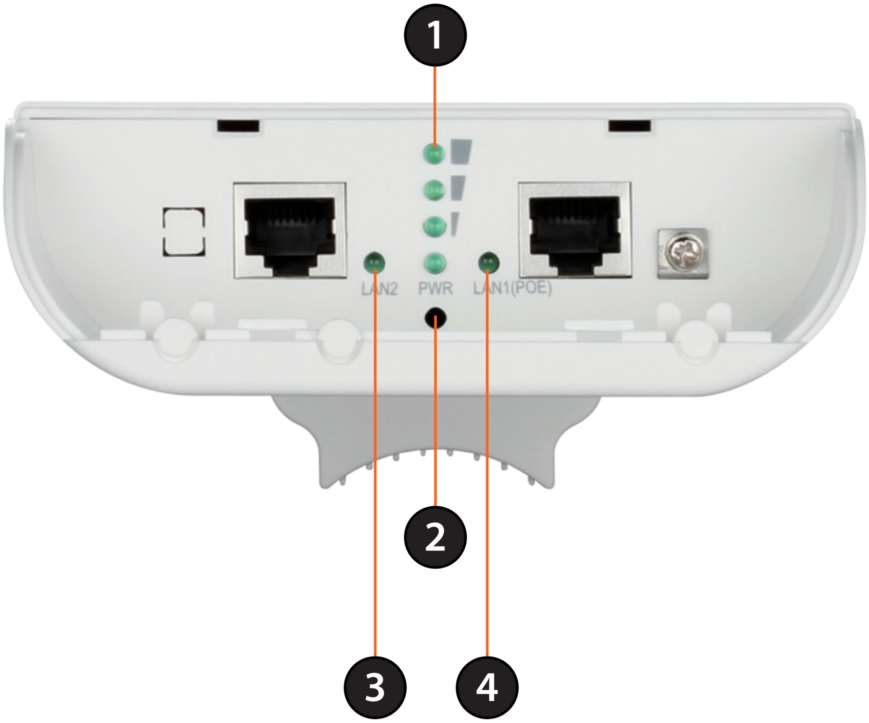
Connections



1	**LAN Port**	Connects to 10/100 Ethernet devices such as computers, switches, and hubs.
2	**LAN (PoE) Port**	Power is supplied through the LAN cable connected in this port via the Power over Ethernet Injector. Please see "Installation" on page 11 for more details on how to correctly power the DAP-3410 and connect to other networking devices.
3	**Reset Button**	Hold the reset button for at least 5 seconds to reset the device back to the factory default settings. All the LEDs will turn on for 2 second and then begin the reboot process.
4	**Grounding Wire Connector**	Connects to a grounding wire.

Note: The DAP-3410 uses a proprietary PoE injector which is needed to function correctly. Only use the included PoE injector as other power sources such as 3rd party PoE injectors or PoE switches or hubs may damage the DAP-3410 or cause it to operate unreliably, and will also void the warranty.

Hardware Overview
LEDs



1	Wireless Signal Strength LED	Shows different signal strength levels. (Only supported in Wireless Client, Repeater, WDS, and WISP mode)
2	Power LED	A solid green light indicates the device is powered and ready.
3	LAN LED	A solid green light indicates the LAN port connection is OK. A blinking green light indicates that the unit is transmitting data over that port.
4	LAN LED (PoE)	A solid green light indicates the LAN port (PoE) connection is OK. A blinking green light indicates that the unit is transmitting data over that port.

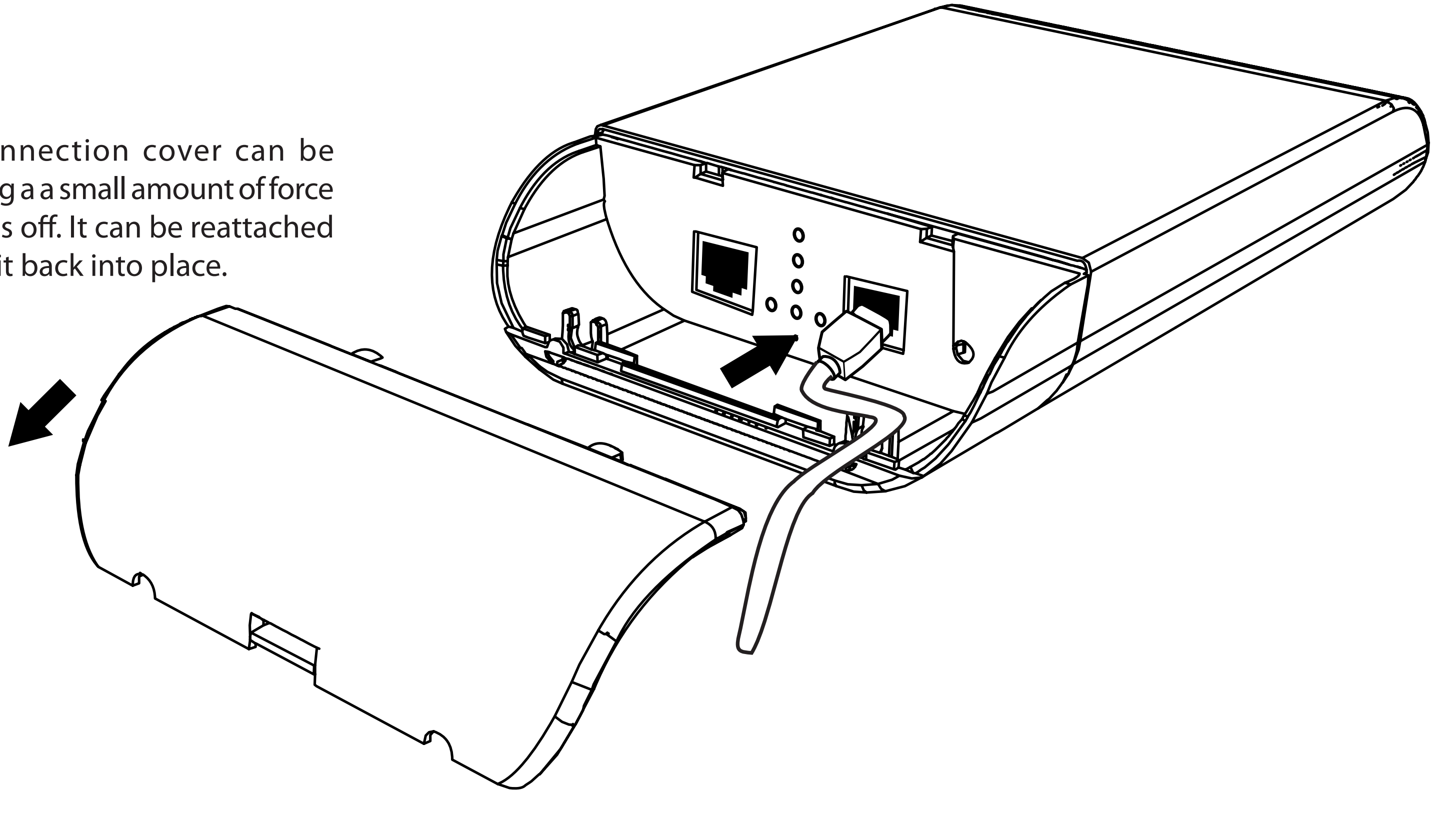
Installation

First, you will need to configure the DAP-3410 with a computer connected directly to the unit. The following pages explains how to set up the DAP-3410 in order to be properly configured and then tested to work as desired.

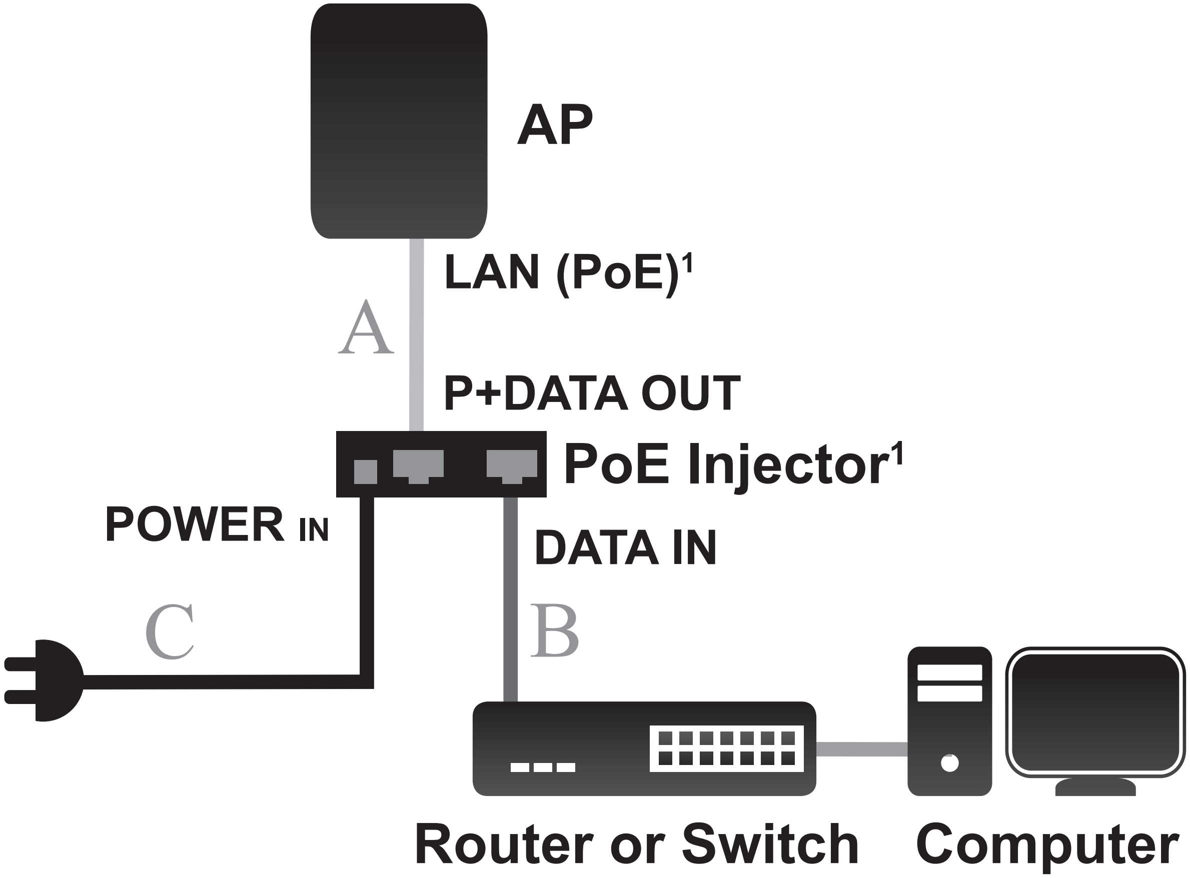
The DAP-3410 acts as a central connection point for any device (client) that has a 802.11n or a 802.11a wireless network interface and is within range of the AP. Clients must use the same SSID (wireless network name) and channel as the AP in order to connect. If wireless security is enabled on the AP, the client will need to enter a password to connect to the AP. In Access Point mode, multiple clients can connect to the AP at the same time.

STEP 1: Connect an Ethernet Cable to the LAN (PoE) Port on the AP.

The port connection cover can be removed using a a small amount of force so that it pops off. It can be reattached by snapping it back into place.



STEP 2: Connect the AP to Your Network



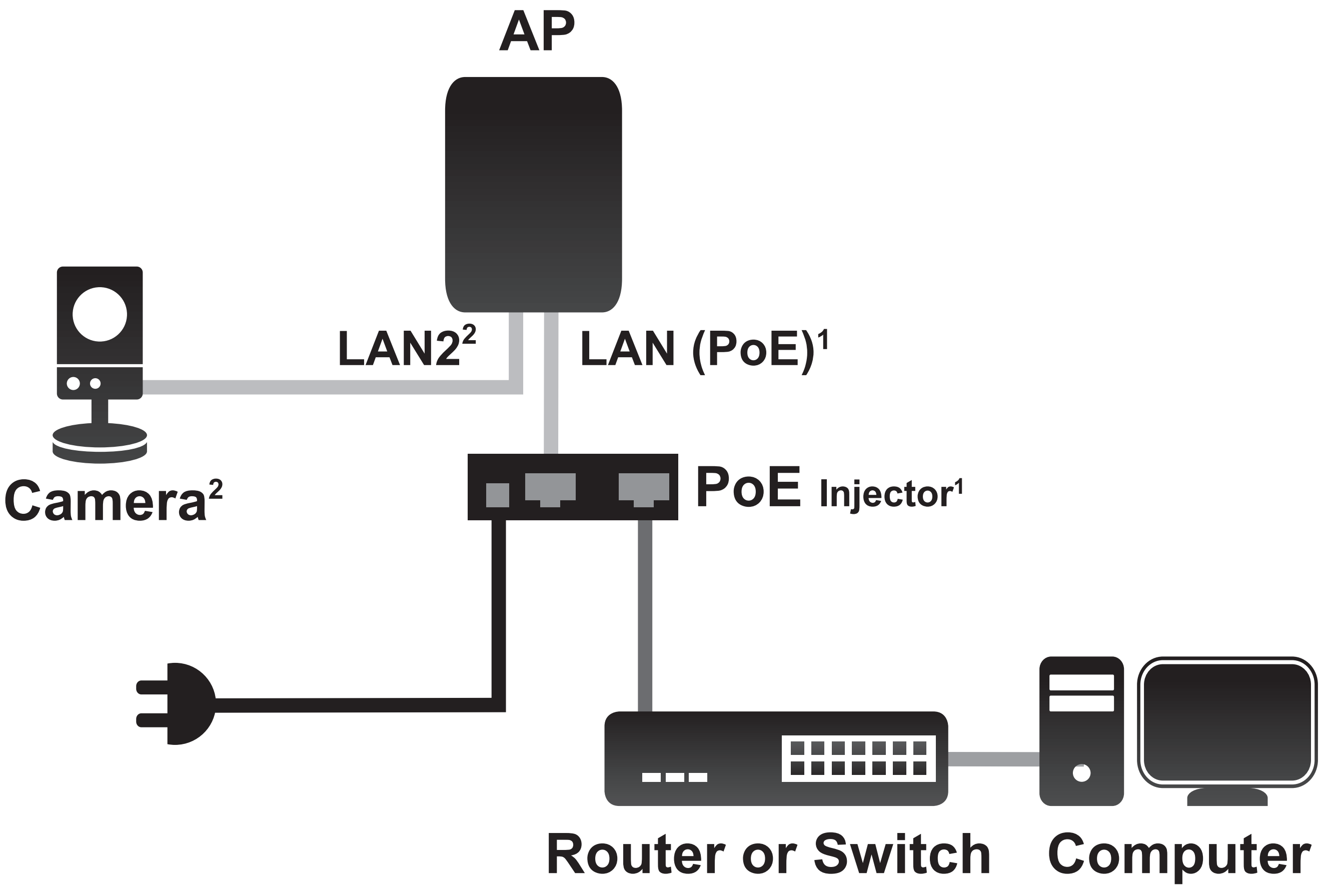
A. Connect the Ethernet cable that is connected to the AP from STEP 1 to the P+DATA OUT port on the PoE Injector.

B. Connect an Ethernet cable from a router, switch, or PC to the DATA IN port on the PoE Injector.

C. Attach the power adapter to the connector labeled POWER IN on the PoE Injector, and plug it into an electrical outlet.

[1] This product uses a proprietary PoE design and can only be used with the included PoE injector.

PoE Passthrough



A. Power on the AP through the PoE kit (as in STEP 4) and connect the camera to the LAN 2 port.

B. Log in to the web UI and enable PoE Passthrough in Maintenance to power on the camera.*

[2] The LAN 2 port can be connected to D-Link cameras that require up to 7 watts, such as the DCS-3716, DCS-6113, and DCS-7110. It can also be connected to a router or a switch.

Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link access point and other network devices to a minimum. Each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters). Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless access points, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

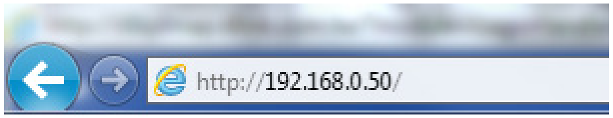
5. If you are using 5 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 5 Hz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Configuration

This section will show you how to configure your new D-Link Wireless N Exterior Access Point using the web-based configuration utility.

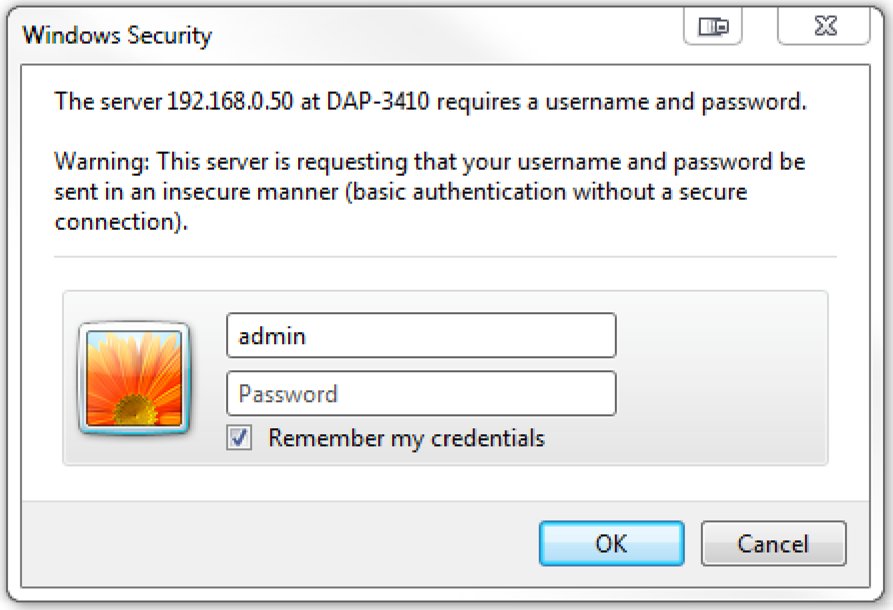
Web-based Configuration Utility

If you wish to change the default settings or optimise the performance of the DAP-3410, you may use the web-based configuration utility.



http://192.168.0.50/

To access the configuration utility, open a web browser such as Internet Explorer and enter **http://192.168.0.50**



Windows Security

The server 192.168.0.50 at DAP-3410 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

Password

☑ Remember my credentials

Select **admin** and then enter your password. Leave the password blank by default.

If you get a Page Cannot be Displayed error, please refer to “**Troubleshooting**” on page 77 for assistance.

Operating Modes

The DAP-3410 features seven different operating modes, allowing it to adapt to any situation. Select the operating mode by clicking on the radio button, that correspondes to the desired mode then click on **Change Mode**. After confirming that the operating mode will be changed, the AP will reboot and will be ready for use after 40 seconds.

Access Point: In access point (AP) mode, 802.11n/g/b compliant devices can connect to the wireless network.

WDS with AP: Wireless distribution system (WDS) with AP mode expands current wireless coverage and also allows devices to connect to the network.

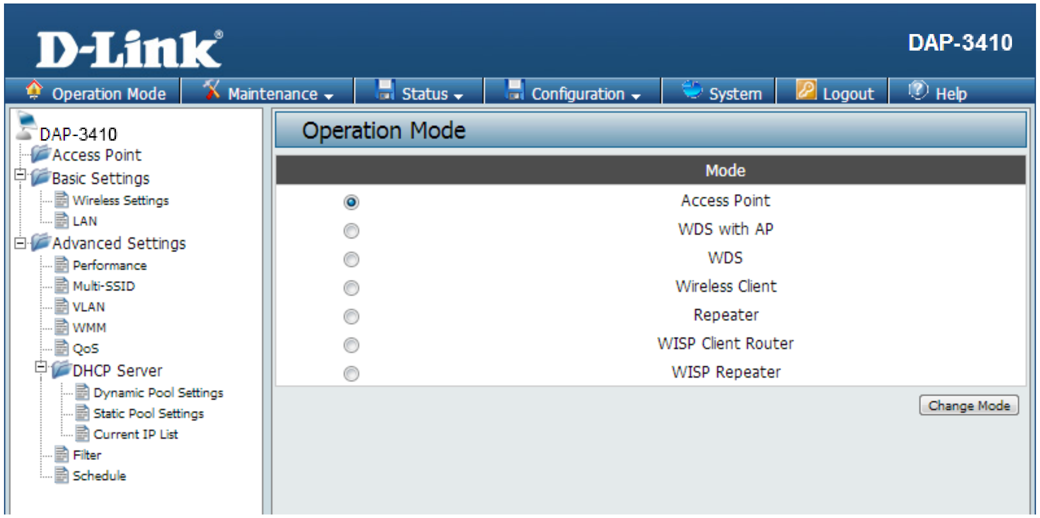
WDS: Wireless distribution system (WDS) mode expands current wireless coverage from other Wireless AP devices that are in WDS mode.

Wireless Client: As a wireless client the DAP-3410 can connect to an existing AP and expand the network physically with the two built-in 10/100 Ethernet ports.

Repeater: Repeater mode will extend current wireless coverage, alleviating dead spots and weak signals.

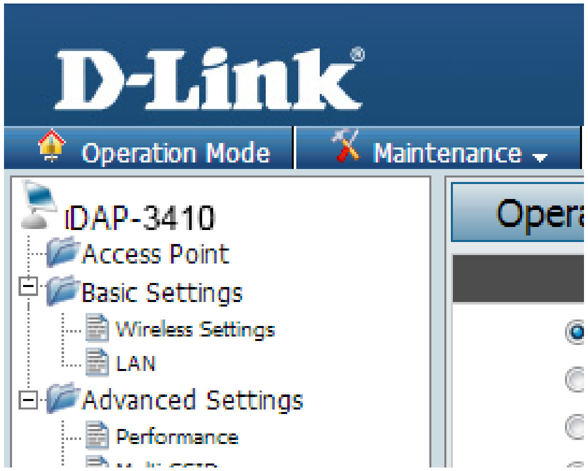
WISP Client Router: WISP Client Router mode allows for the sharing of a WISP connection using the two built-in 10/100 Ethernet ports.

WISP Repeater: WISP Repeater mode will extend an existing WISP's network coverage area.



Operation Mode

	Mode
●	Access Point
○	WDS with AP
○	WDS
○	Wireless Client
○	Repeater
○	WISP Client Router
○	WISP Repeater

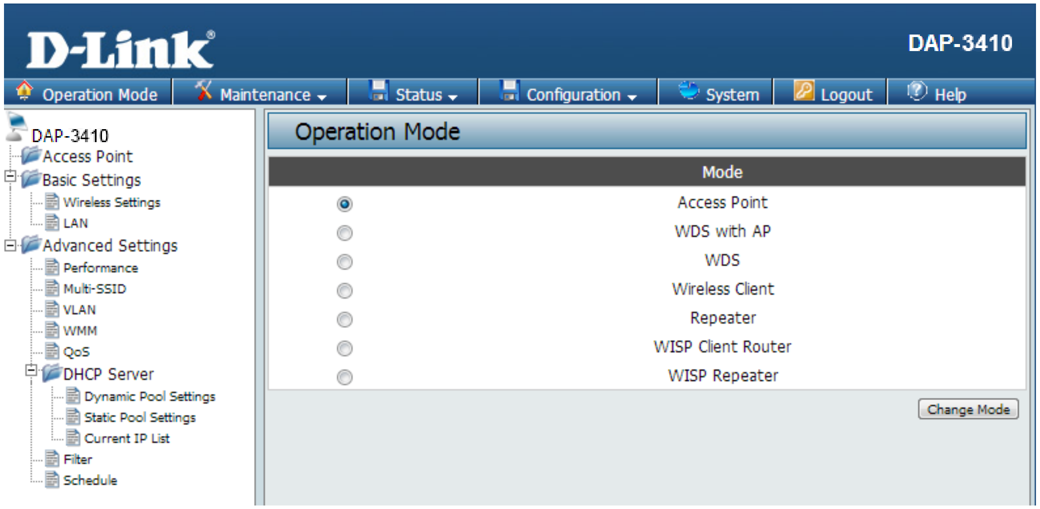


Note: The current operating mode will be listed under the device's name in the configuration menu tree.

Basic Settings

The image to the right shows a configuration menu tree for when the AP is in Access Point mode. If you need help determining which operating mode the AP is currently in, please see "Operating Modes" on page 16.

Note: The DAP-3410 has different configuration options depending on the current operating mode. Please be aware that some screens and menus will not be present unless the AP is operating in an applicable operating mode.

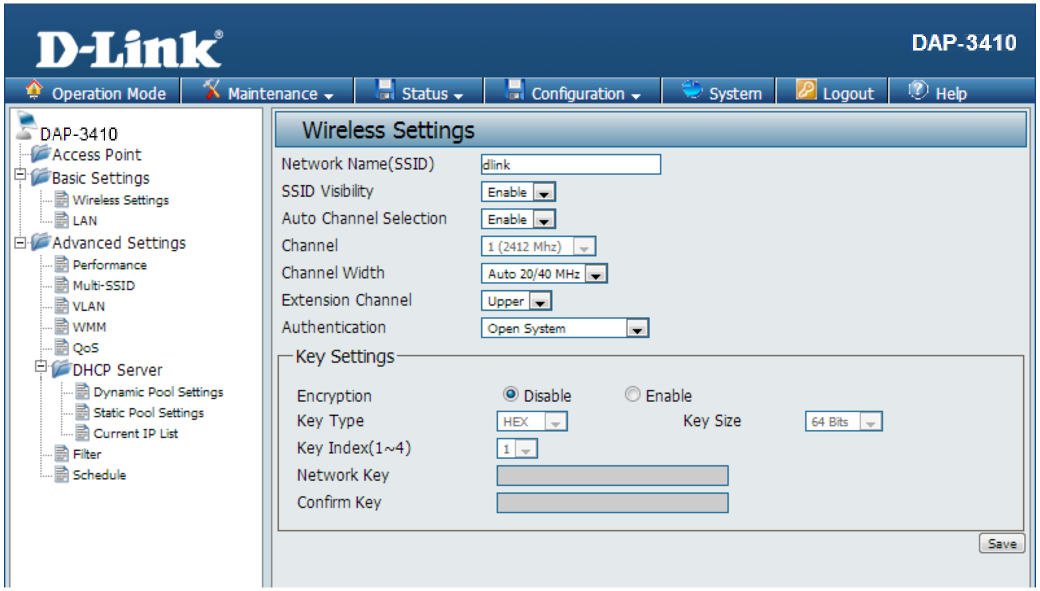


Operation Mode

Mode
● Access Point
○ WDS with AP
○ WDS
○ Wireless Client
○ Repeater
○ WISP Client Router
○ WISP Repeater

Wireless Settings

This page will allow you to configure the wireless connection for the DAP-3410. Please be aware that some menu options will change depending on which type of security setting is used.



Wireless Settings

Network Name(SSID): dlink
SSID Visibility: Enable
Auto Channel Selection: Enable
Channel: 1 (2412 Mhz)
Channel Width: Auto 20/40 MHz
Extension Channel: Upper
Authentication: Open System

Key Settings

Encryption: ● Disable ○ Enable
Key Type: HEX   Key Size: 64 Bits
Key Index(1~4): 1
Network Key:
Confirm Key:

Network Name (SSID): Enter a name for your wireless network (SSID). For security purposes, it is highly recommended to change from the default network name.

SSID Visibility: Select **Disabled** if you do not want the SSID of your wireless network to be broadcasted by the DAP-3410. Your wireless clients will have to know the SSID of your DAP-3410 in order to connect to it.

Auto Channel Selection: The Auto Channel Scan setting can be selected to allow the DAP-3410 to choose the channel with the least amount of interference.

Channel: Indicates the channel setting for the DAP-3410. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Scan, this option will be grayed out.

Channel Width: Auto 20/40 - Select if you are using both 802.11n and non-802.11n wireless devices. 20MHz - Select if you are not using any 802.11n wireless clients.

Extension Channel: Used only when **Channel width** is set to 40 MHz. Select the desired channel bonding for control.

Authentication: Refer to “Wireless Security” on page 62 of this manual for a detailed explanation of the wireless security options.

Open System/Shared Key Authentication

If you selected Open System as your Authentication, you will see these settings:

Encryption: Use the radio button to disable or enable encryption. (Encryption option only available with Open System setting)

Key Type: Select either **HEX** or **ASCII** as the key type.

Key Size: Select **64 Bits** or **128 Bits** for your key size.

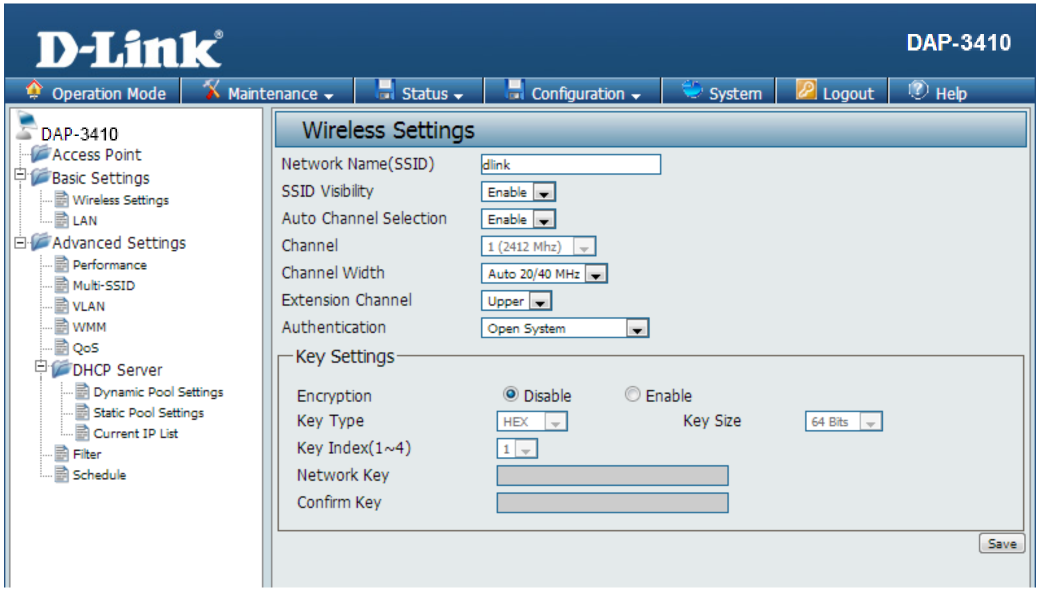
Key Index: Select which key you want to be the active key.

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

Confirm Key: Confirm the network key.

Click **Save** to commit your changes.

Note: 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.



Wireless Settings

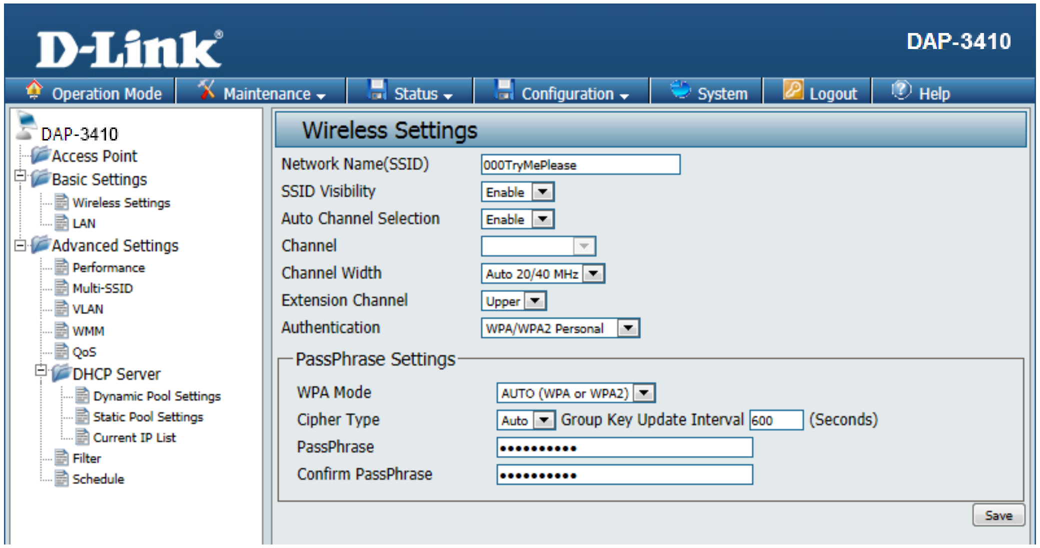
Network Name(SSID)	dlink
SSID Visibility	Enable
Auto Channel Selection	Enable
Channel	1 (2412 Mhz)
Channel Width	Auto 20/40 MHz
Extension Channel	Upper
Authentication	Open System

Key Settings

Encryption	● Disable	○ Enable	
Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			

WPA/WPA2-Personal Authentication

If you selected WPA/WPA2-Personal Authentication as your Authentication, you will see these settings:



Wireless Settings

Network Name(SSID)	000TryMePlease
SSID Visibility	Enable
Auto Channel Selection	Enable
Channel	
Channel Width	Auto 20/40 MHz
Extension Channel	Upper
Authentication	WPA/WPA2 Personal

PassPhrase Settings

WPA Mode	AUTO (WPA or WPA2)
Cipher Type	Auto Group Key Update Interval 600 (Seconds)
PassPhrase	••••••••••
Confirm PassPhrase	••••••••••

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: Select the interval during which the group key will be valid. The default value of **1800** is recommended. Select **Manual** to enter your key (Passphrase).

Passphrase / Confirm Passphrase: When you select **WPA-Personal**, please enter a Passphrase in the corresponding fields.

WPA/WPA2-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.

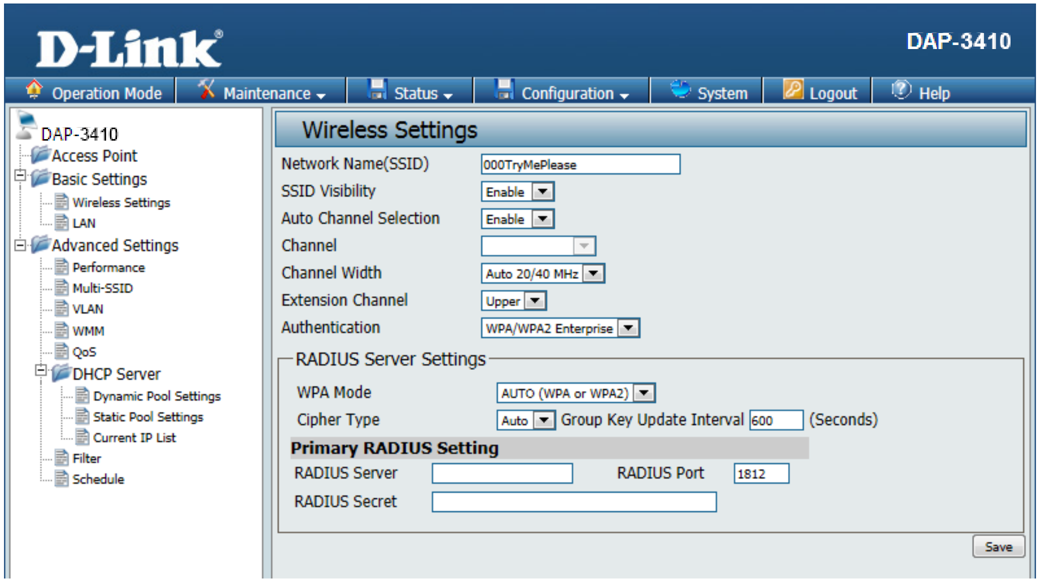
Cipher Type: When WPA-Enterprise is selected, you must also select a cipher type from the drop-down menu: Auto, AES, or TKIP.

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

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

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.



Wireless Settings

Network Name(SSID): 000TryMePlease
SSID Visibility: Enable
Auto Channel Selection: Enable
Channel:
Channel Width: Auto 20/40 MHz
Extension Channel: Upper
Authentication: WPA/WPA2 Enterprise

RADIUS Server Settings

WPA Mode: AUTO (WPA or WPA2)
Cipher Type: Auto Group Key Update Interval 600 (Seconds)

Primary RADIUS Setting

RADIUS Server: RADIUS Port 1812
RADIUS Secret:

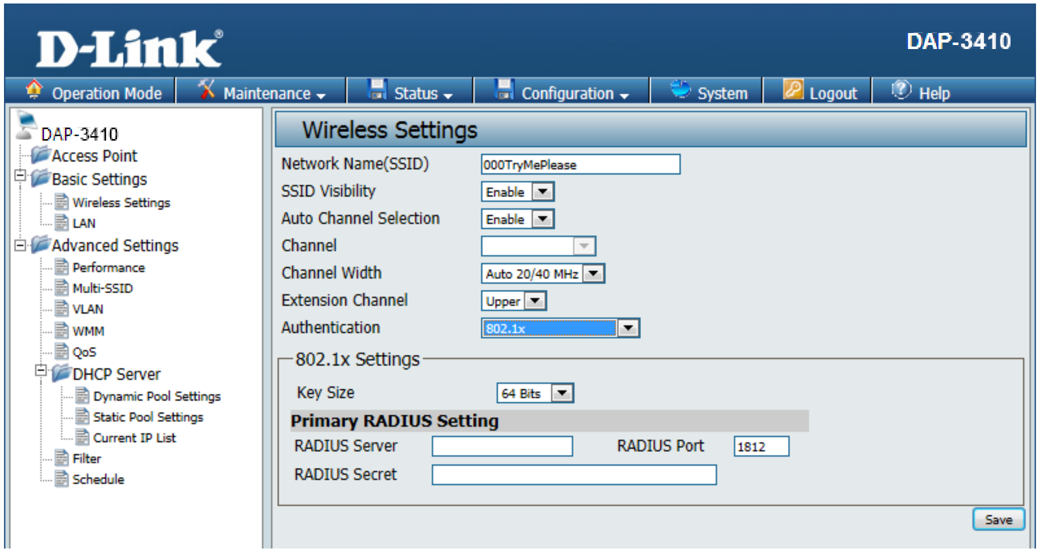
802.1x Authentication

Key Size: Select **64 Bits** or **128 Bits** for your key size.

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

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.



Wireless Settings

Network Name(SSID)	000TryMePlease
SSID Visibility	Enable
Auto Channel Selection	Enable
Channel	
Channel Width	Auto 20/40 MHz
Extension Channel	Upper
Authentication	802.1x

802.1x Settings

Key Size: 64 Bits

Primary RADIUS Setting

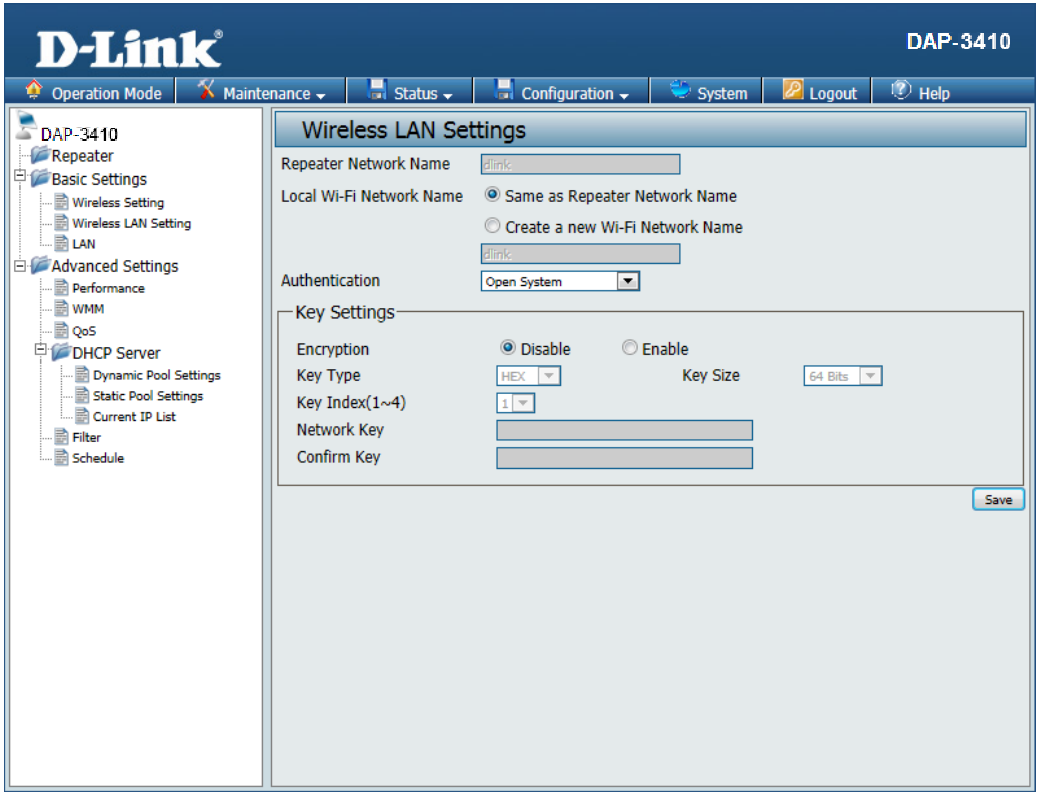
RADIUS Server:

RADIUS Port: 1812

RADIUS Secret:

Wireless LAN Settings

This page will allow you to change the wireless LAN settings of the AP. This function is used when there are multiple access points that are connected to increase wireless coverage over an area.



Wireless LAN Settings

Repeater Network Name: dlink

Local Wi-Fi Network Name: ● Same as Repeater Network Name ○ Create a new Wi-Fi Network Name dlink

Authentication: Open System

Key Settings

Encryption: ● Disable ○ Enable

Key Type: HEX Key Size: 64 Bits

Key Index(1~4): 1

Network Key:

Confirm Key:

Repeater Network Name: Set this to the SSID of the wireless network that the DAP-3410 will be connecting to.

Local Wi-Fi Network Name: This option can either be set to rebroadcast the wireless network that the DAP-3410 is connected to, or it can broadcast a different SSID.

Authentication: The wireless LAN security can be **Open System**, **WPA-Persona**l, **WPA-Enterprise, or 802.1x**.

For a detailed description of the Open System parameters, please go to page 19.

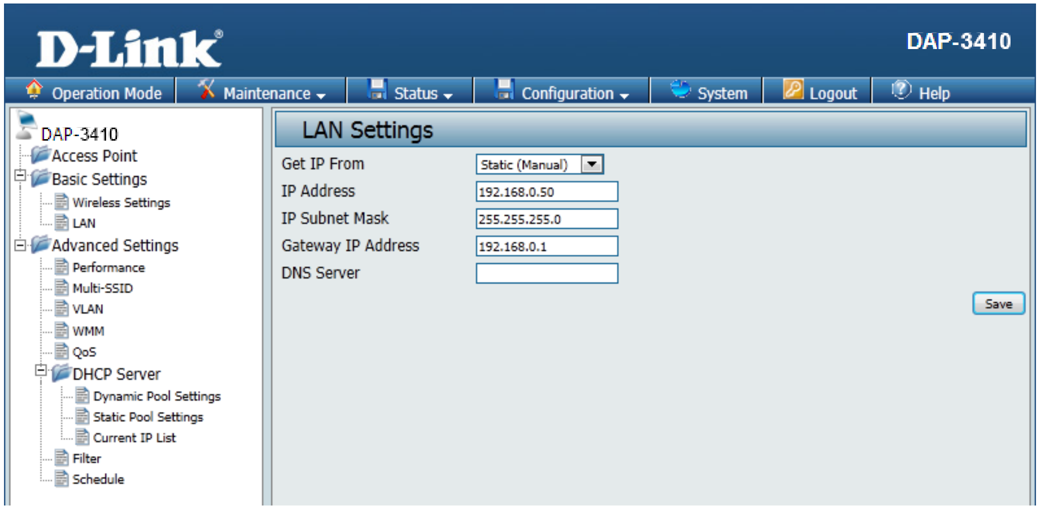
For a detailed description of the WPA-Personal parameters, please go to page 20.

For a detailed description of the WPA-Enterprise parameters, please go to page 21.

For a detailed description of the 802.1x parameters, please go to page 22.

LAN Settings

This section will allow you to change the local network settings of the DAP-3410. After making your changes, click the **Save** button.



LAN Settings

Get IP From	Static (Manual)
IP Address	192.168.0.50
IP Subnet Mask	255.255.255.0
Gateway IP Address	192.168.0.1
DNS Server	

Get IP From: Select an option to choose how the AP will obtain an IP address to use on the local network. If this is set to **Static**, you will need to manually enter the necessary information.

IP Address: Enter the IP address of the router. The default IP address is 192.168.0.50. If you change the IP address, once you click Save, you will need to enter the new IP address in your browser to get back into the configuration utility.

IP Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

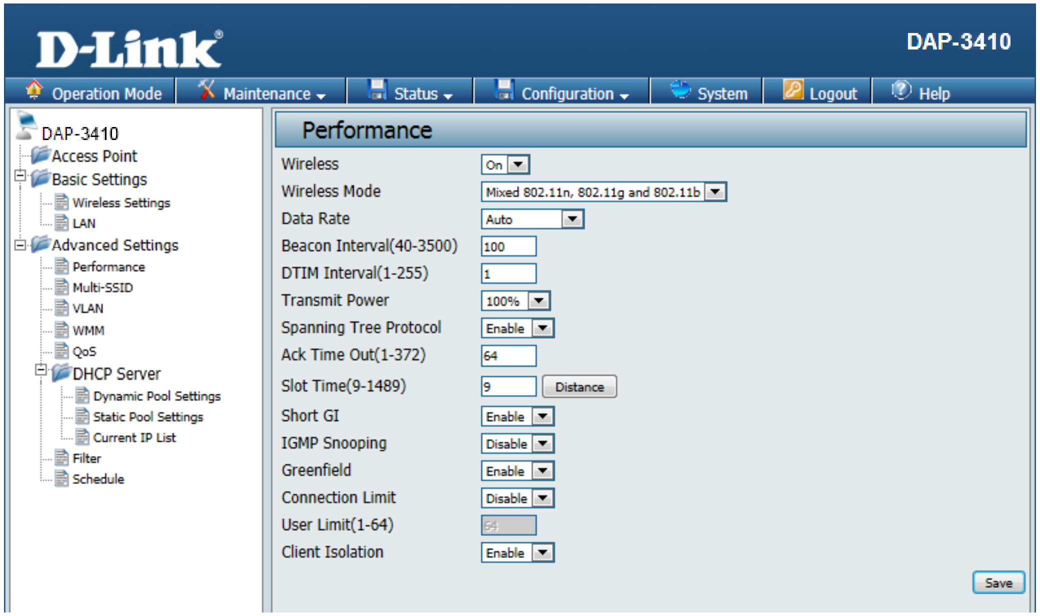
Gateway IP Address: Enter the gateway IP Address for your local network.

DNS Server Configure the IP address of the preferred DNS server.

Advanced Settings

Performance

This options on this page will allow you to fine tune the wireless connectivity of the access point.



Performance

Wireless	On
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Data Rate	Auto
Beacon Interval(40-3500)	100
DTIM Interval(1-255)	1
Transmit Power	100%
Spanning Tree Protocol	Enable
Ack Time Out(1-372)	64
Slot Time(9-1489)	9
Short GI	Enable
IGMP Snooping	Disable
Greenfield	Enable
Connection Limit	Disable
User Limit(1-64)	64
Client Isolation	Enable

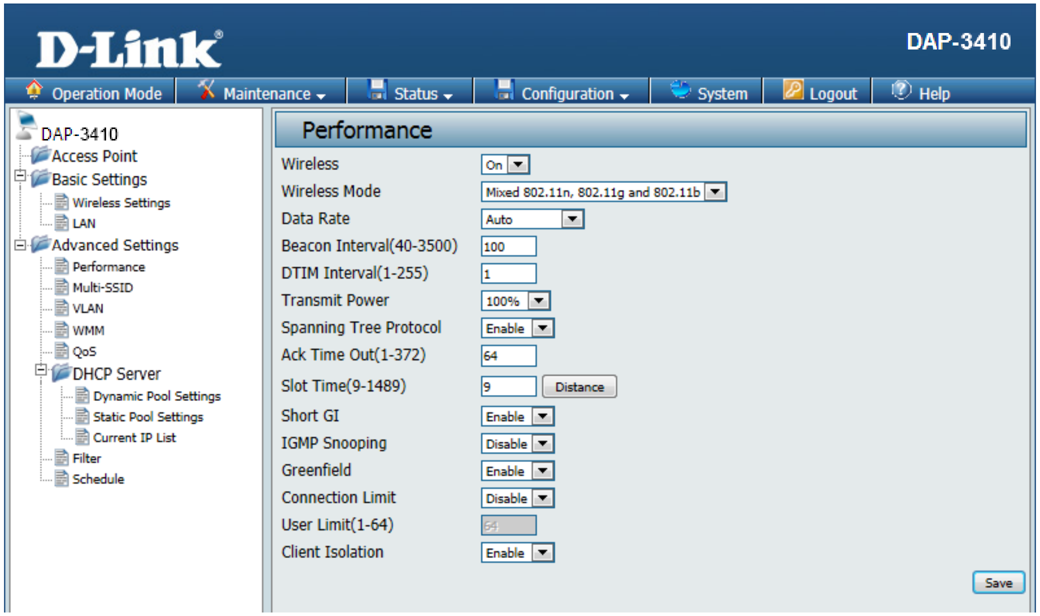
Wireless: Use the drop-down menu to turn the wireless function **On** or **Off**.

Wireless Mode: The different combination of clients that can be supported include **Mixed 802.11n**, and **802.11n Only**.

Data Rate: Set 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. This option is enabled in **Mixed 802.11g and 802.11b** mode. The choices available are **Best (Up to 54)**, **54**, **48**, **36**, **24**, **18**, **12**, **9**, **6**, **11**, **5.5**, **2** or **1**.

Beacon Interval: 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 Set a Delivery Traffic Indication Message setting between 1 and 255. The default value is 1. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.



Performance

Wireless	On
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Data Rate	Auto
Beacon Interval(40-3500)	100
DTIM Interval(1-255)	1
Transmit Power	100%
Spanning Tree Protocol	Enable
Ack Time Out(1-372)	64
Slot Time(9-1489)	9
Short GI	Enable
IGMP Snooping	Disable
Greenfield	Enable
Connection Limit	Disable
User Limit(1-64)	64
Client Isolation	Enable

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%.

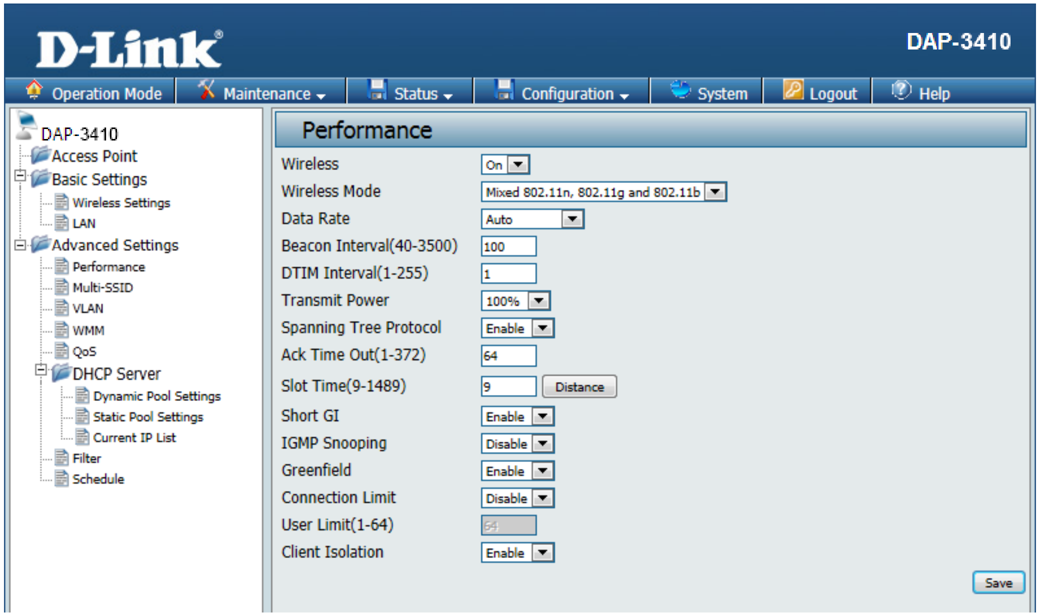
Spanning Tree Protocol: Select **Enable** or **Disable**. Enabling this option will help prevent bridge loops and will provide nearby AP's with the information needed to reliably route the network should one of the other devices fail.

Ack Time Out: To effectively optimize throughput over long distance links, enter a value for Acknowledgement Time Out from 1 to 372 microseconds in the 2.4 GHz in the field provided.

Slot Time: This setting is used to specify an amount of time the AP will wait after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which will increase throughput.

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.



Performance

Wireless	On
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Data Rate	Auto
Beacon Interval(40-3500)	100
DTIM Interval(1-255)	1
Transmit Power	100%
Spanning Tree Protocol	Enable
Ack Time Out(1-372)	64
Slot Time(9-1489)	9 Distance
Short GI	Enable
IGMP Snooping	Disable
Greenfield	Enable
Connection Limit	Disable
User Limit(1-64)	64
Client Isolation	Enable

Save

Greenfield: Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40MHz and there is another wireless network's channel overlapping and causing interference, the router will automatically change to 20MHz.

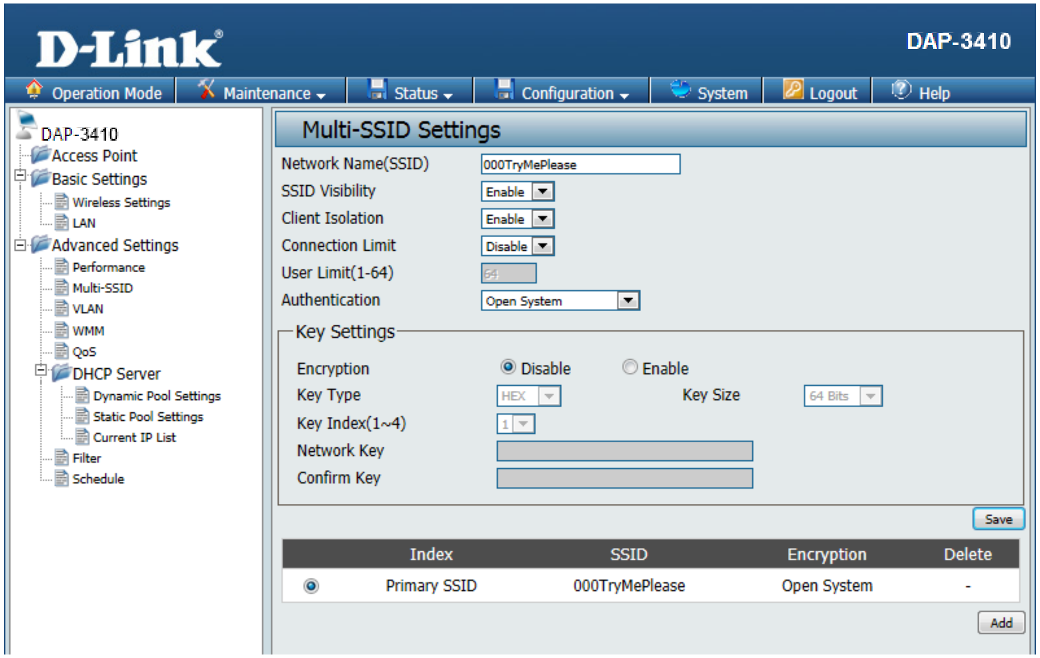
Connection Limit: Select **Enable** or **Disable**. This is an option for load balancing, and determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field. If this function is enabled and the number of users exceeds this value, the DAP-3410 will not allow any additional clients to associate with the AP.

User Limit: Set the maximum amount of users that are allowed access (1-64 users). To use this feature, the Connection Limit above must be enabled. For most networks, a limit of 10 is recommended. The default setting is 20.

Client Isolation: If this option is enabled, connected clients will not be able to view or access each other.

Multi-SSID

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



Multi-SSID Settings

Network Name(SSID)	000TryMePlease
SSID Visibility	Enable
Client Isolation	Enable
Connection Limit	Disable
User Limit(1-64)	64
Authentication	Open System

Key Settings

Encryption	● Disable ○ Enable		
Key Type	HEX	Key Size	64 Bits
Key Index(1~4)	1		
Network Key			
Confirm Key			

	Index	SSID	Encryption	Delete
●	Primary SSID	000TryMePlease	Open System	-

Network Name(SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN).

SSID Visibility: **Enable** or **Disable** SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

Client Isolation: If this option is enabled, the connected clients will not be able to view or access each other.

Connection Limit: This option allows for load balancing on the AP. It sets a limit on the number of connections that can be used across all of the broadcasted SSIDs.

User Limit: If **Connection Limit** is enabled, this option will allow you to input the maximum number of connected clients.

Authentication: The Multi-SSID security can be **Open System**, **WPA-Persona**l, **WPA-Enterprise, or 802.1x**.

For a detailed description of the Open System parameters, please go to page 19.

For a detailed description of the WPA-Personal parameters, please go to page 20.

For a detailed description of the WPA-Enterprise parameters, please go to page 21.

For a detailed description of the 802.1x parameters, please go to page 22.

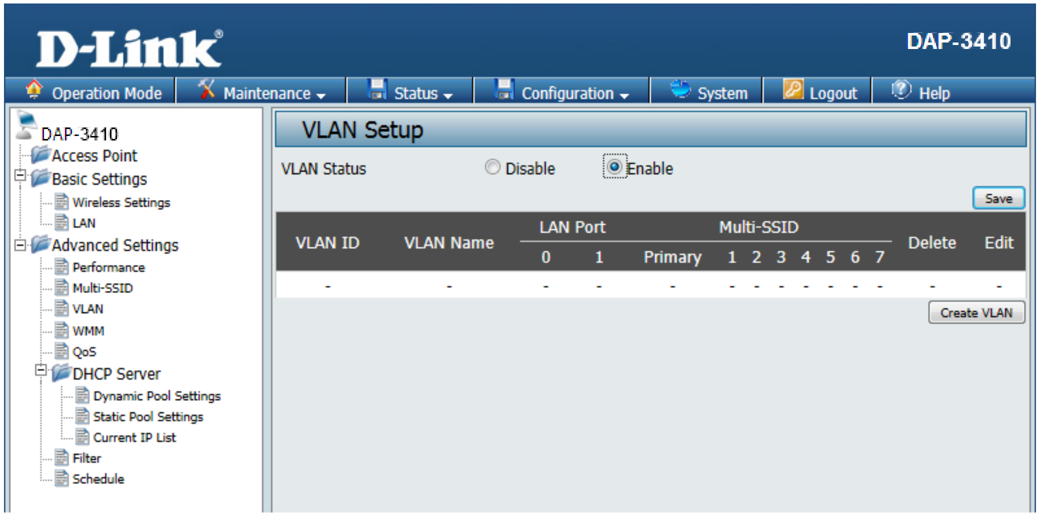
VLAN

The VLAN List tab displays the current VLANs. Clicking on **Create VLAN** will allow you to create a new Virtual LAN with a Name and ID. The LAN ports and the Multi-SSID function can be assigned to a VLAN.

VLAN Status: Use the radio button to toggle between **Enable** or **Disable**. After changing the option, you will need to click on **Save** to add or edit VLANs.

To remove or modify a VLAN, click on the **Delete** or **Edit** button.

To add a VLAN, click on the **Create VLAN** button.



VLAN Setup

VLAN Status ○ Disable ● Enable

VLAN ID	VLAN Name	LAN Port		Multi-SSID								Delete	Edit
		0	1	Primary	1	2	3	4	5	6	7		
-	-	-	-	-	-	-	-	-	-	-	-	-	-

Add/Edit VLAN

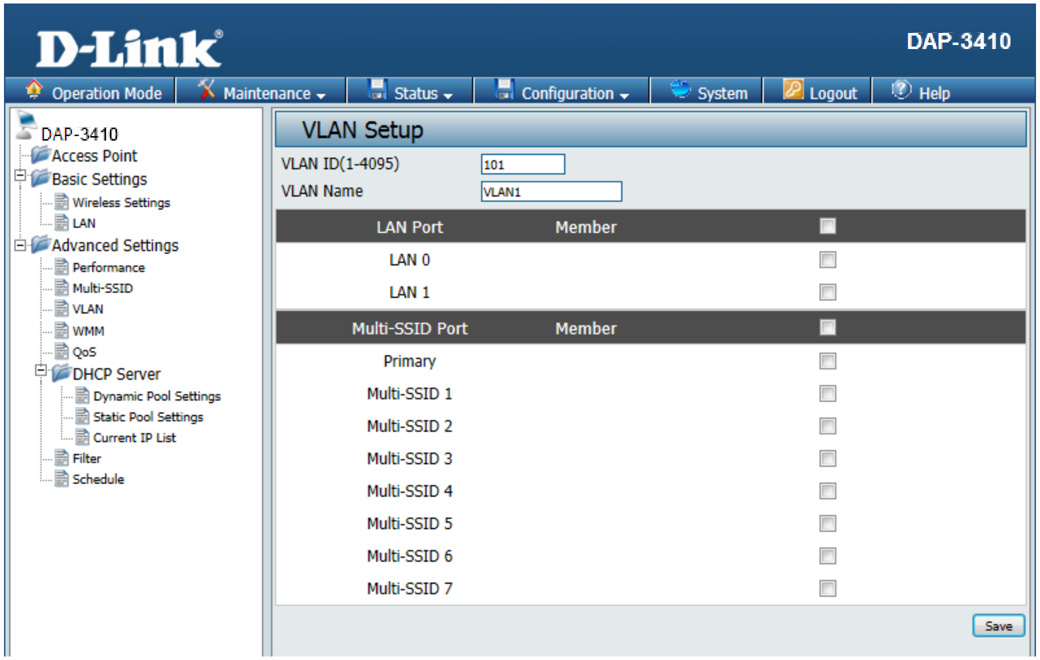
The **VLAN Setup** tab is used to configure VLANs. Once you have made the desired changes, click the **Save** button to let your changes take effect.

VLAN ID: Provide a number between 1 and 4094 for the Internal VLAN.

VLAN Name: Enter the VLAN to add or modify.

LAN Port: Select a LAN port to bind to the SSID.

Multi-SSID Port: Select the corresponding SSID to bind to the LAN port in order to create a VLAN. You can find more information about setting up multiple SSID's by referring to "Multi-SSID" on page 28.



VLAN Setup

VLAN ID(1-4095): 101

VLAN Name: VLAN1

LAN Port	Member ☐
LAN 0	☐
LAN 1	☐

Multi-SSID Port	Member ☐
Primary	☐
Multi-SSID 1	☐
Multi-SSID 2	☐
Multi-SSID 3	☐
Multi-SSID 4	☐
Multi-SSID 5	☐
Multi-SSID 6	☐
Multi-SSID 7	☐

WMM

This page will allow you to change the settings that control the WMM feature, which provides QoS for any devices that are connected via wireless to the AP.

WMM: Select whether to **Enable** or **Disable** the WMM functionality of the access point.

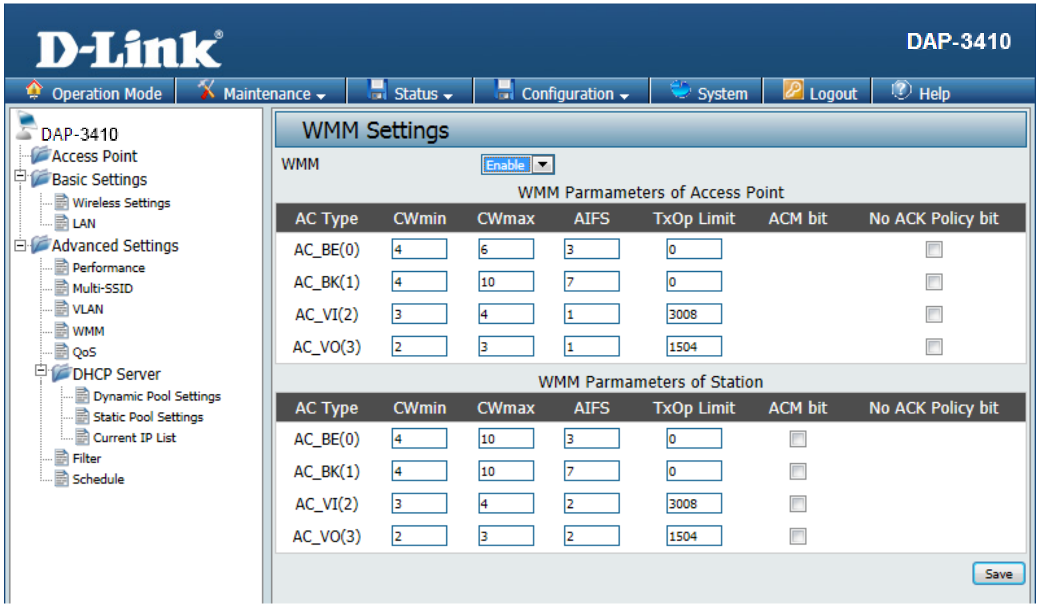
AC Type: A different type of data is associated with each queue. The queue and associated priorities and parameters for transmission are as follows:

(Best Effort, BE): Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

(Background, BK): Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

(Video, VI): High priority queue, minimum delay. Time-sensitive data such as video and other streaming media are automatically sent to this queue.

(Voice, VO): Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.



WMM Settings

WMM: Enable

WMM Parmameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	6	3	0		□
AC_BK(1)	4	10	7	0		□
AC_VI(2)	3	4	1	3008		□
AC_VO(3)	2	3	1	1504		□

WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	10	3	0	□	
AC_BK(1)	4	10	7	0	□	
AC_VI(2)	3	4	2	3008	□	
AC_VO(3)	2	3	2	1504	□	

CWmin: The value specified for the Minimum Contention Window is the lower limit of a range for the initial random backoff wait time. Setting this value gives the DAP-3410 a starting point before beginning to double the window size when a collision is detected.

CWMax: The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

AIFS: The Arbitration Inter-Frame Spacing (AIFs) specifies a wait time (in milliseconds) for data frames. The AIFs ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free.

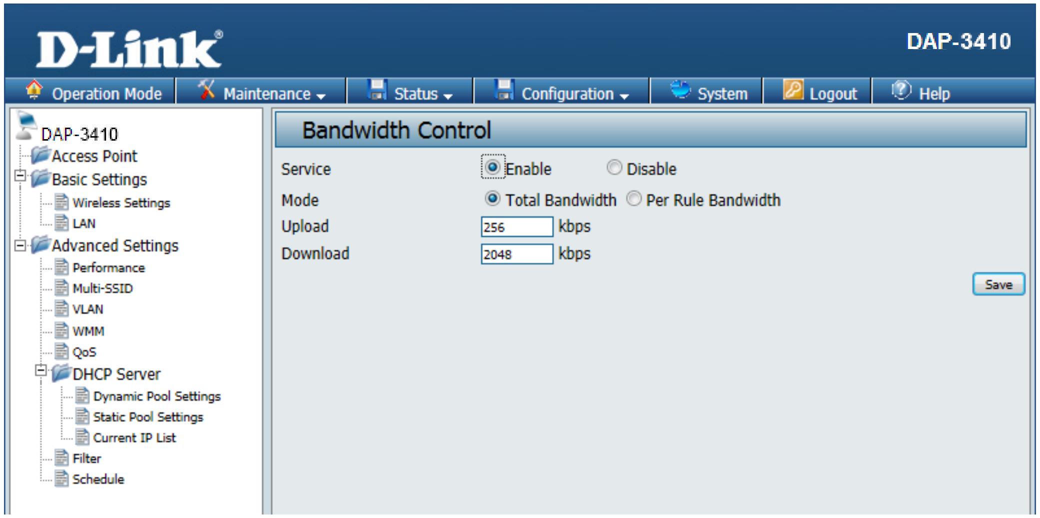
TxOp Limit: The Transmission Opportunity (TXOP) is an interval of time when a WMM client station has the right to initiate transmissions onto the wireless medium.

ACM BIT: Enabling this checkbox will allow the AP to broadcast the admission control bit.

No ACK Policy bit: When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange.

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 type of traffic and will adjust the amount of bandwidth used based on the settings defined here.



Bandwidth Control

Service	● Enable ○ Disable
Mode	● Total Bandwidth ○ Per Rule Bandwidth
Upload	256 kbps
Download	2048 kbps

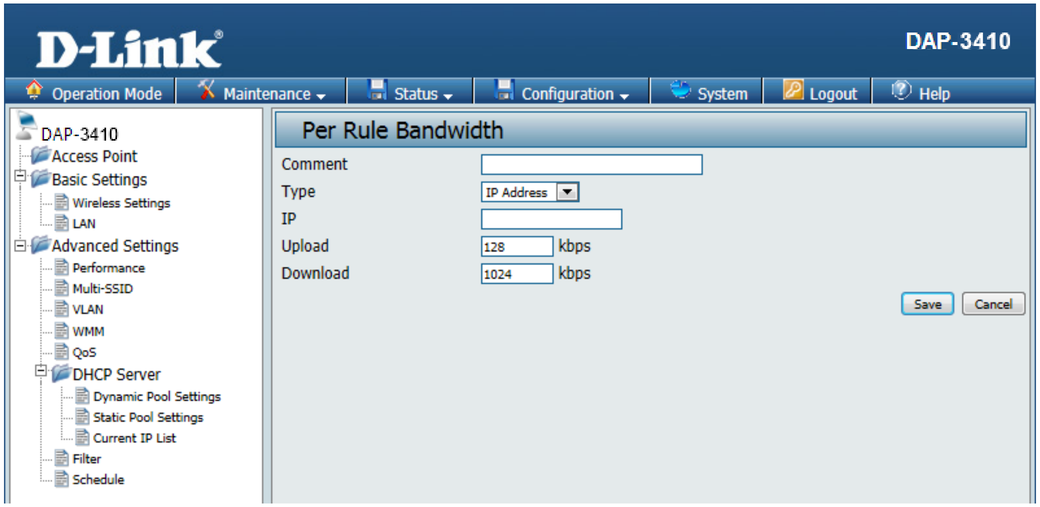
Service: Enable this option if you want to allow QoS to prioritize your traffic.

Mode: Select whether QoS should be based on total bandwidth or on a per rule basis.

Upload: Set the QoS limit for upload bandwidth.

Download: Set the Qos limit for download bandwidth.

If the Per Rule Bandwidth option is selected, the following choices will become available.



Per Rule Bandwidth

Comment	
Type	IP Address
IP	
Upload	128 kbps
Download	1024 kbps

Comment: You can enter a comment to easily identify your rule.

Type: Select whether the rule should apply to an IP address, IP segment, a destination port or a MAC address. The following field will change accordingly.

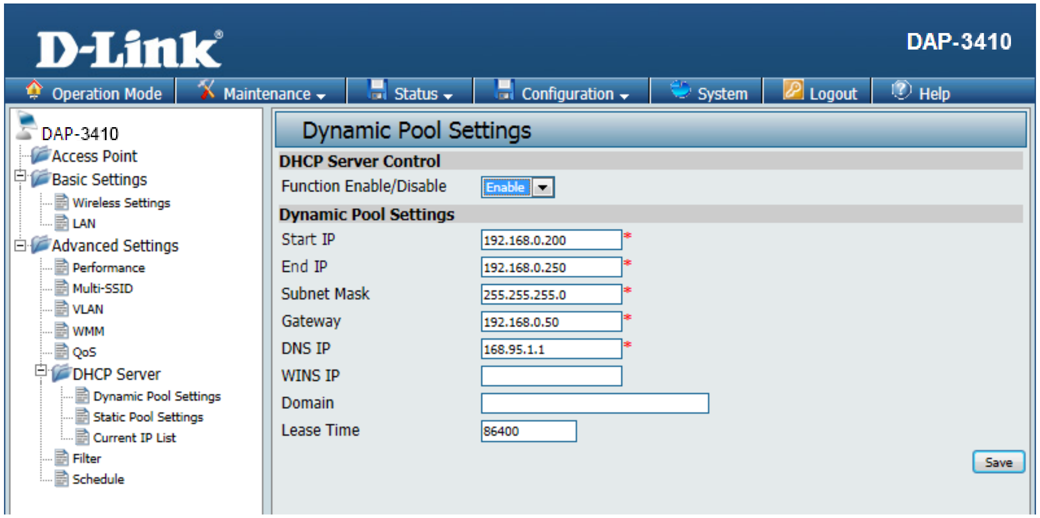
Upload: Set the QoS limit for upload bandwidth.

Download: Set the QoS limit for download bandwidth.

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. If needed or required in the network, the DAP-3410 is capable of acting as a DHCP server.



Dynamic Pool Settings

DHCP Server Control

Function Enable/Disable	Enable

Dynamic Pool Settings

Start IP	192.168.0.200 *
End IP	192.168.0.250 *
Subnet Mask	255.255.255.0 *
Gateway	192.168.0.50 *
DNS IP	168.95.1.1 *
WINS IP	
Domain	
Lease Time	86400

Function Enable/ Disable: Select **Enable** to allow the DAP-3410 to function as a DHCP server.

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

End IP: Input the last IP address available for assignment on your network.

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

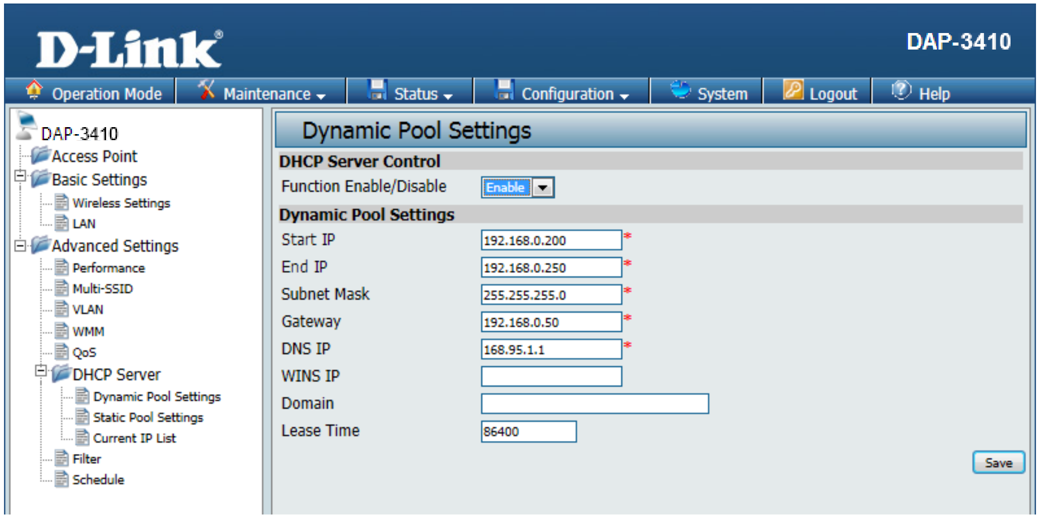
Gateway: Enter the IP address of the gateway on the network.

DNS IP: 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.

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.

Domain: Enter the domain name of the network, if applicable. (An example of a domain name is: www.dlink.com.)

Least Time The lease time is the period of time before the DHCP server will assign new IP addresses.



Dynamic Pool Settings

DHCP Server Control

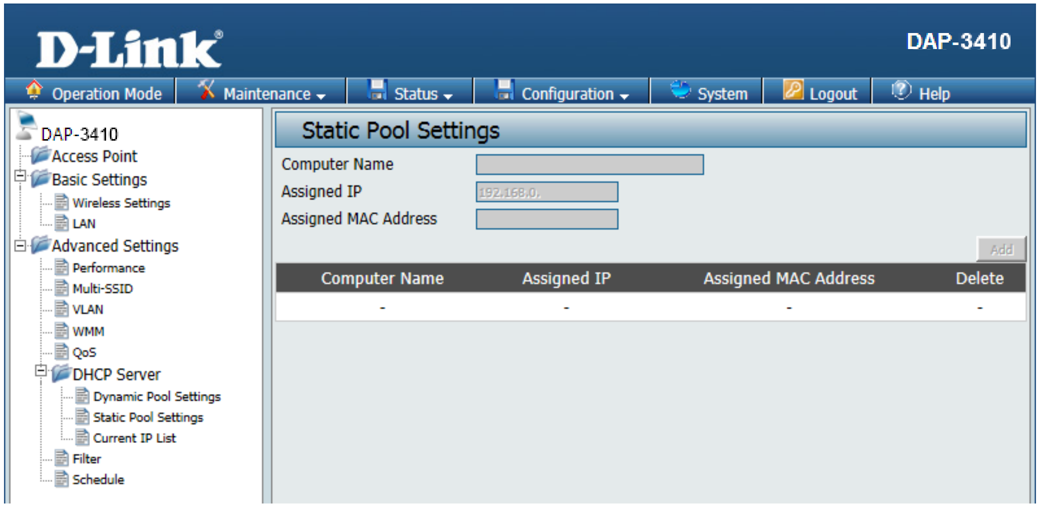
Function Enable/Disable	Enable

Dynamic Pool Settings

Start IP	192.168.0.200 *
End IP	192.168.0.250 *
Subnet Mask	255.255.255.0 *
Gateway	192.168.0.50 *
DNS IP	168.95.1.1 *
WINS IP	
Domain	
Lease Time	86400

Static Pool Settings

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.



Static Pool Settings

Computer Name	
Assigned IP	192.168.0.
Assigned MAC Address	

Computer Name	Assigned IP	Assigned MAC Address	Delete
-	-	-	-

Computer Name: Enter a name for the computer or device that will be used to identify the IP address and assigned MAC address.

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.

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

After you have assigned a static IP address to a device via its MAC address, click **Save**; 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.

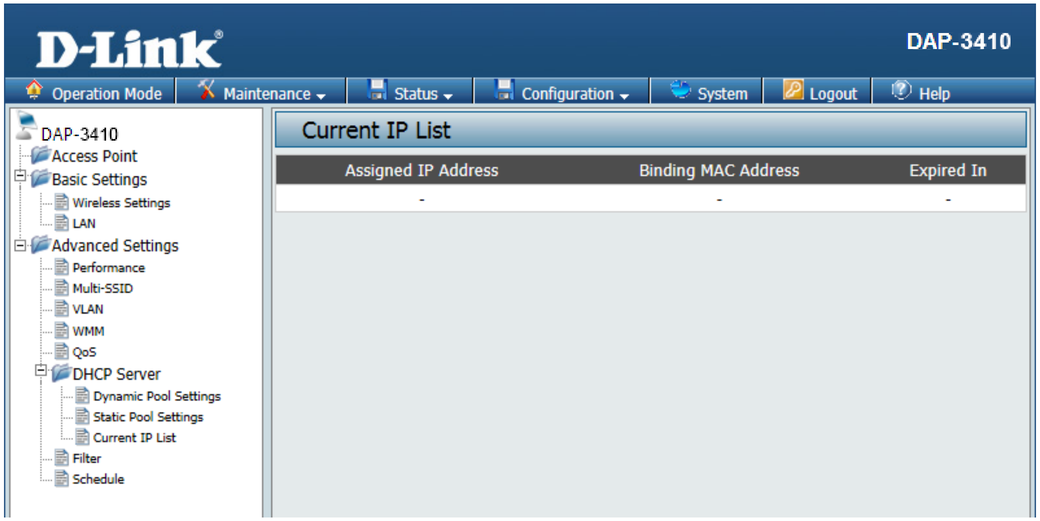
Current IP List

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.

Assigned IP Address: The current corresponding DHCP-assigned IP address of the device.

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

Expired In: The length of time until the dynamic IP address will be invalid.



Current IP List

Assigned IP Address	Binding MAC Address	Expired In
-	-	-

Filter

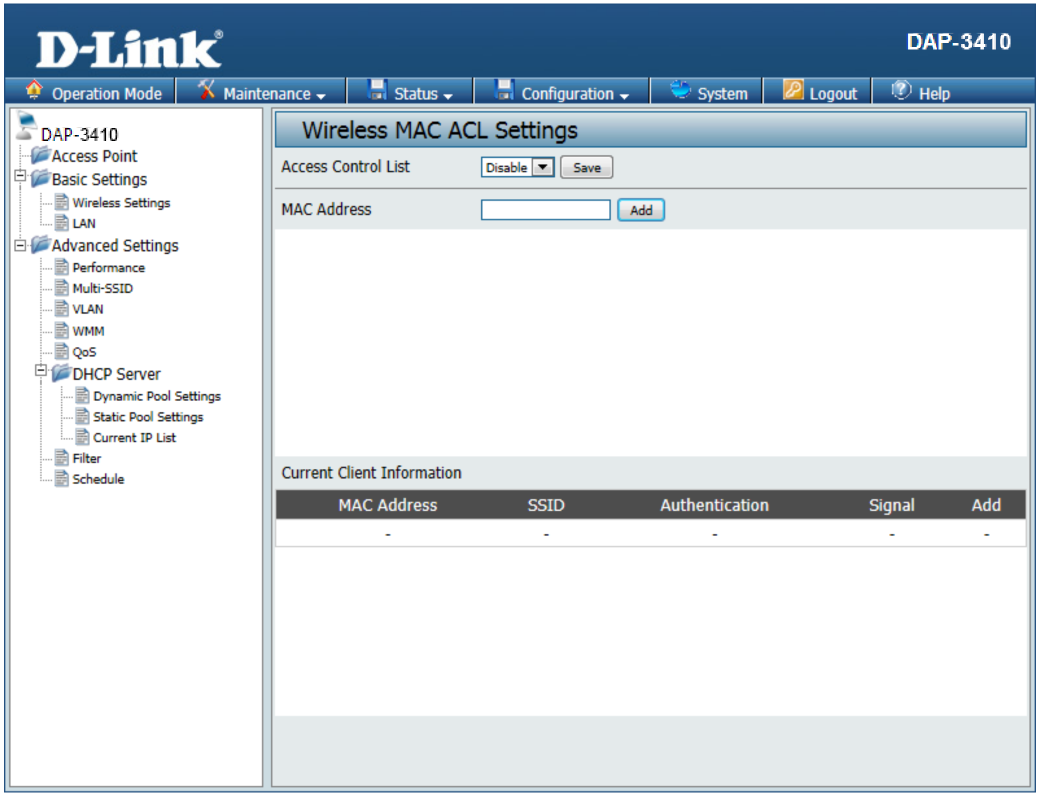
The Access Control filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

Access Control List: When **Disabled** is selected, MAC addresses are not used to control network access. When **Enabled** is selected, only computers with MAC addresses listed in the MAC Address List are granted network access.

MAC Address: Click the **Add** button to add the new MAC address to be filtered. Filtered MAC addresses will be listed in the section below.

Current Client Information

This section shows currently connected clients, and gives you the option to add them to the MAC address access control list



Wireless MAC ACL Settings

Access Control List: Disable

MAC Address:

Current Client Information

MAC Address	SSID	Authentication	Signal	Add
-	-	-	-	-

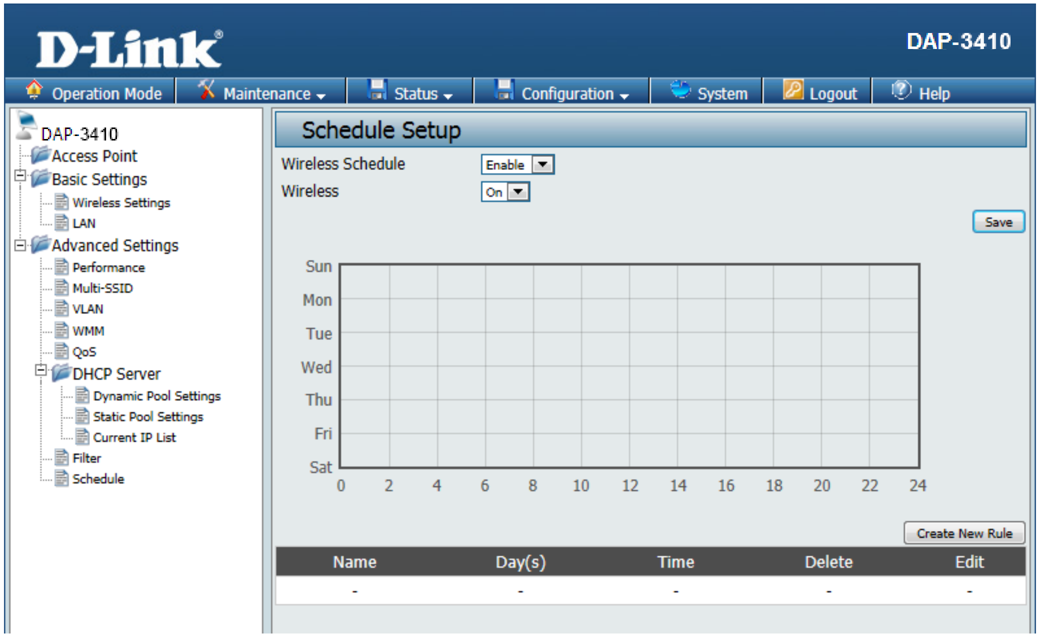
Schedule

This page will allow you to setup access schedules for the device. This will enable or disable clients from connecting to the device during specified times.

Wireless Schedule: **Enable** or **Disable** wireless access based on a predetermined schedule by selecting an option from the drop down box.

Wireless: Select whether the schedule will either turn the wireless network **on**, or **off**. Once you have determined the wireless state to be controlled by scheduling, click **Create New Rule** to continue.

Wireless Schedule List: The list of schedules will be listed below the weekly graph. Click the **Edit** icon to make changes or click the **Delete** icon to remove the schedule.



Schedule Setup

Wireless Schedule: Enable

Wireless: On

Name	Day(s)	Time	Delete	Edit
-	-	-	-	-

If you create a new rule or edit an existing one, you will see these settings:

Name: Enter a name to identify the rule being created.

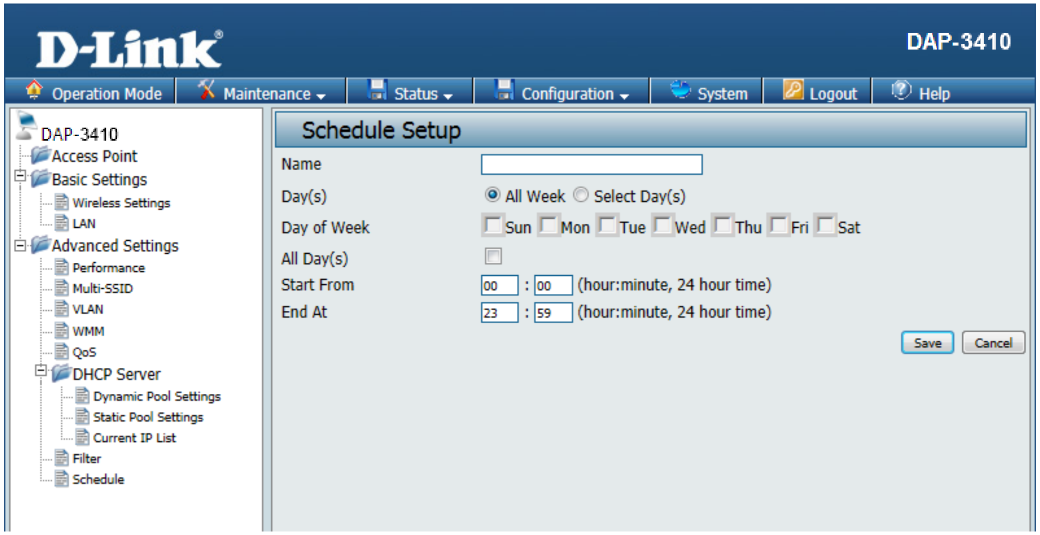
Day(s): All Week, or choose Select Day(s) to specify what days the rule should be active on.

Day of Week: Select the days that the rule will be active.

All Day(s): Select this checkbox if the rule should be active all day for the days specified.

Start From: This should be set to the time when the rule will become active.

End At: This should be set to the time when the rule will become inactive.



Schedule Setup

Name	
Day(s)	● All Week ○ Select Day(s)
Day of Week	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
All Day(s)	□
Start From	00 : 00 (hour:minute, 24 hour time)
End At	23 : 59 (hour:minute, 24 hour time)

DMZ

DMZ is short for Demilitarized Zone. If an application has trouble working from behind the router, you can expose a computer to the Internet and run the application on that computer.

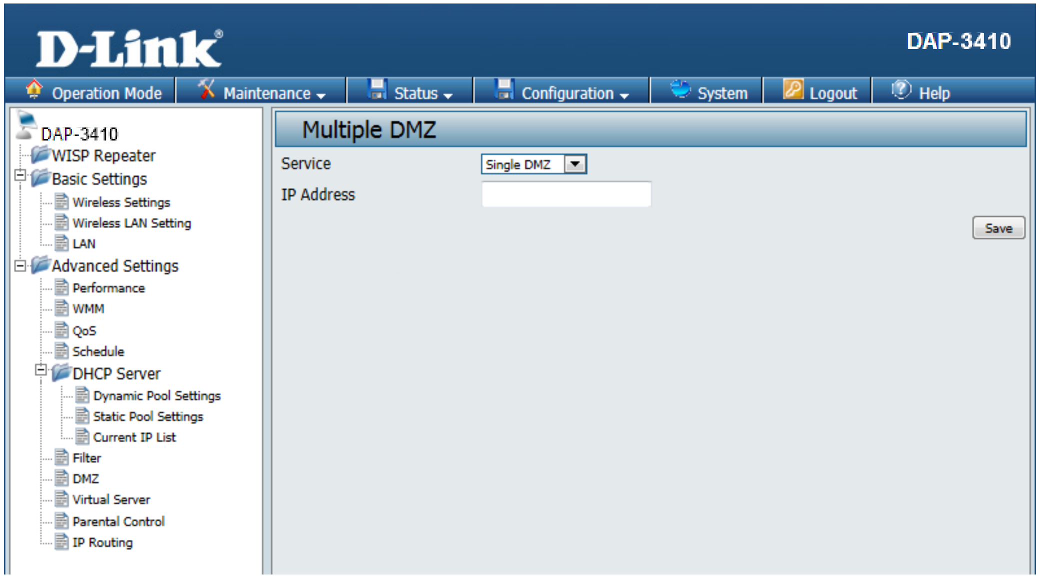
Service: You can select either **Single DMZ** or **Multiple DMZ**. This will allow you to choose whether to expose a single IP address via DMZ, or to expose multiple IP addresses.

Note: Placing a computer in the DMZ may expose that computer to a variety of security risks.

IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains it's IP address automatically using DHCP, be sure to make a static reservation on the **DHCP Server** > **Static Pool Settings** page so that the IP address of the DMZ machine does not change.

Public WAN IP Address: If the Multiple DMZ option is selected, this field will be available. This should be set to the external IP address that will be assigned to an internal IP address of a computer or device.

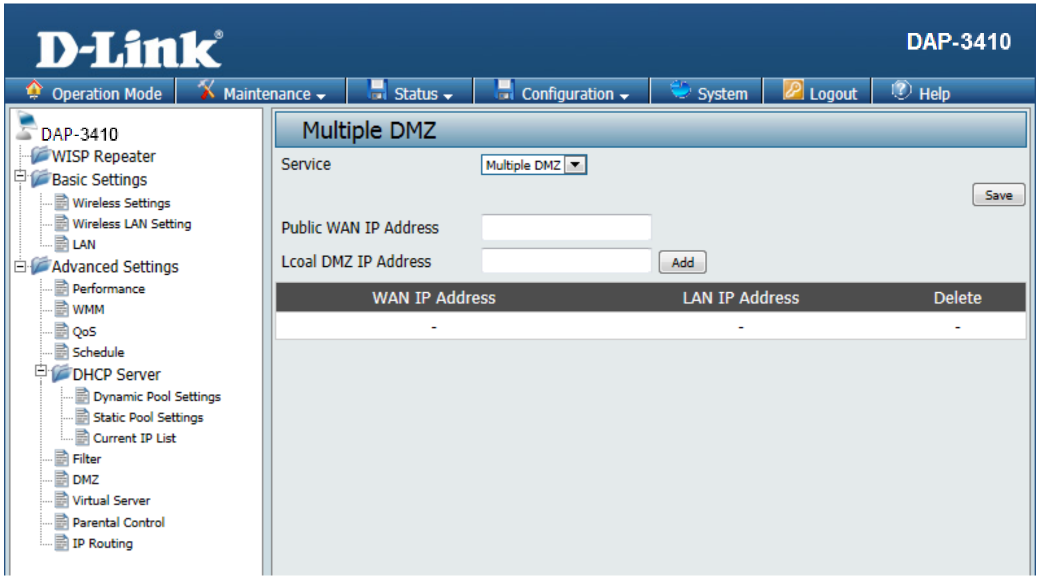
Local DMZ IP Address: If the Multiple DMZ option is selected, this field will be available. This should be set to the internal IP address of a computer or device that will be assigned to an external IP address.



Multiple DMZ

Service: Single DMZ

IP Address:



Multiple DMZ

Service: Multiple DMZ

Public WAN IP Address:

Lcoal DMZ IP Address:

WAN IP Address	LAN IP Address	Delete
-	-	-

Virtual Server

This will allow you to open a single port. This allows a computer or device to provide external access to services or applications that are otherwise blocked by the built-in firewall. To create a virtual server, click on **Create New Virtual Server**, and the following settings will appear:

Service: Select to either **Disable** or **Enable** the rule.

Description: Enter a name for the rule.

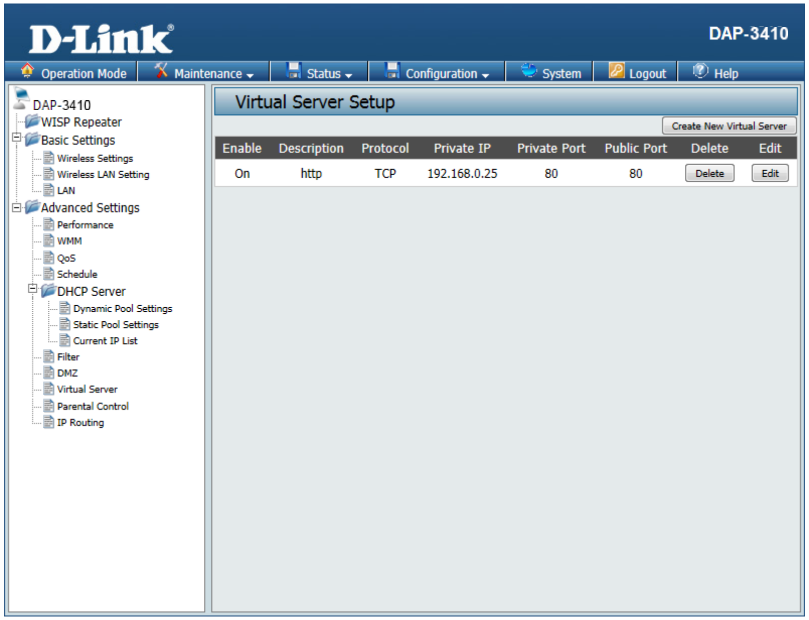
Private IP: Enter the IP address of the computer on your local network that you want to allow the incoming service to.

Protocol Type: Select either **TCP** or **UDP**.

Private Port: Enter the port that you want to open for the computer or device on the internal network.

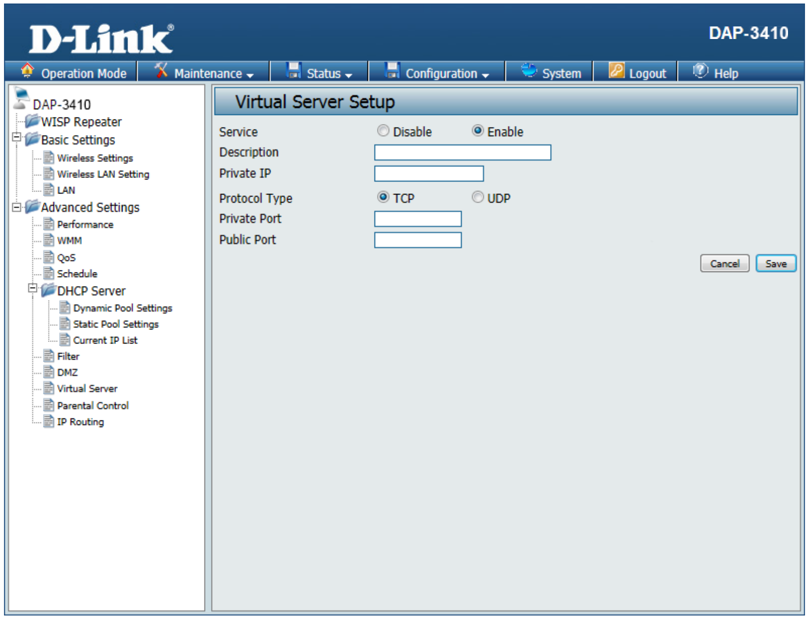
Public Port: Enter the port that you want to open for the external network.

Note: The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer or device within your local network.



Virtual Server Setup

Enable	Description	Protocol	Private IP	Private Port	Public Port	Delete	Edit
On	http	TCP	192.168.0.25	80	80	Delete	Edit

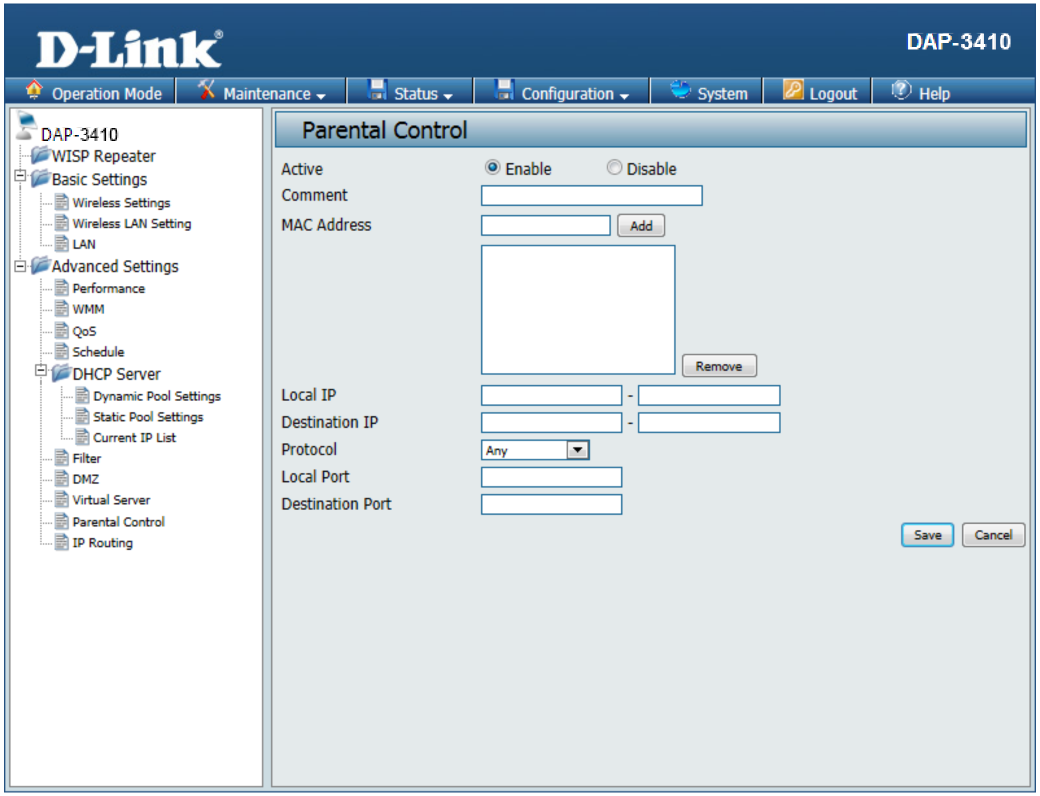


Virtual Server Setup

Service	○ Disable	● Enable
Description		
Private IP		
Protocol Type	● TCP	○ UDP
Private Port		
Public Port		

Parental Control

Parental Control is used to allow you to set up a range of IP Addresses that can be either be blacklisted or whitelisted to certain MAC addresses on the network.



Parental Control

Active ● Enable ○ Disable
Comment
MAC Address
Local IP -
Destination IP -
Protocol Any
Local Port
Destination Port

Active: Select to either **Disable** or **Enable** the Parental Control feature.

Comment: You can enter a comment here for each rule that is created.

MAC Address: Enter the MAC address to be monitored and click **Save** to add it to the parental control list.

Local IP: Enter the start and end of an IP address range that you would like to filter on the local network. This is normally used to prevent access to certain parts of the internal network.

Destination IP: Enter the start and end of an IP address range that you would like to filter on the destination network. This is normally used to prevent access to certain parts of the external network.

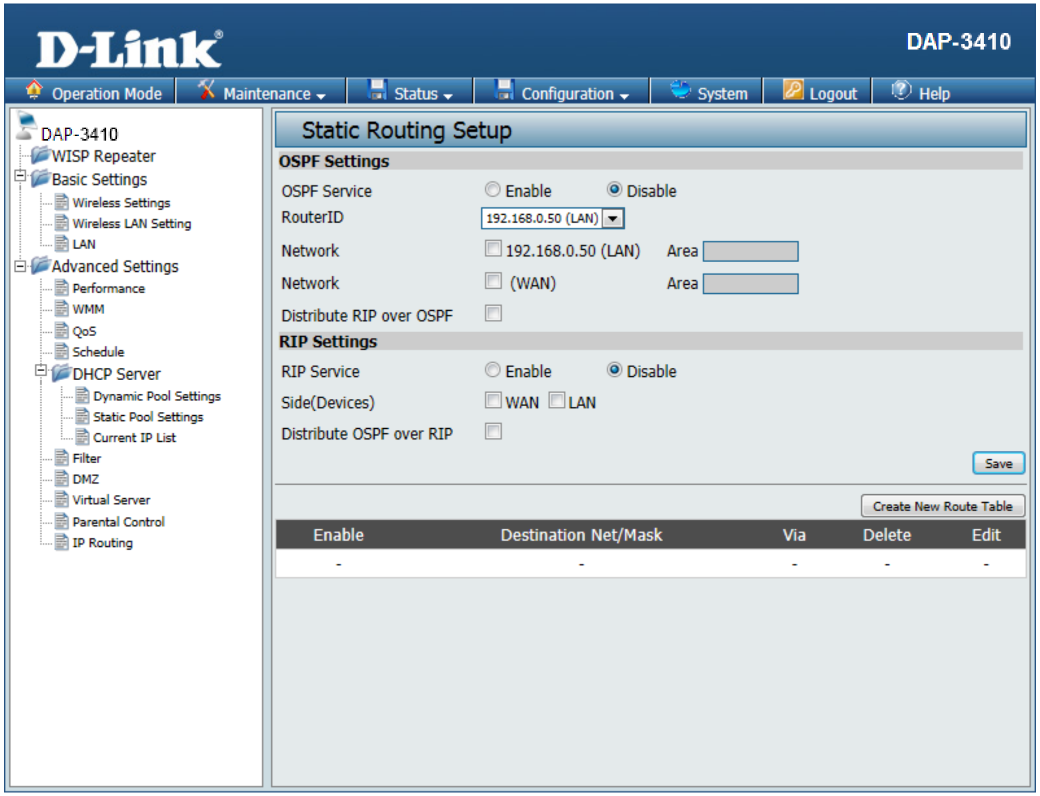
Protocol: Specify which protocol to filter.

Local Port: Enter the specific port to filter on the local network.

Destination Port: Enter the specific port to filter on the destination network.

IP Routing

Static Routing Setup



Static Routing Setup

OSPF Settings

OSPF Service ○ Enable ● Disable

RouterID 192.168.0.50 (LAN)

Network □ 192.168.0.50 (LAN) Area

Network □ (WAN) Area

Distribute RIP over OSPF □

RIP Settings

RIP Service ○ Enable ● Disable

Side(Devices) □ WAN □ LAN

Distribute OSPF over RIP □

Enable	Destination Net/Mask	Via	Delete	Edit
-	-	-	-	-

This page will allow you to configure the built-in routing protocols that the DAP-3410 allows when in certain operating modes.

OSPF Service Select to either **Disable** or **Enable** the AP from offering OSPF service.

RouterID: Select the interface that the AP will broadcast OSPF from. This should be the main interface that will connect to the local network.

Network (Internal): Selecting this checkbox will allow you to enter an area that will be used by the static routing setup on the internal network.

Network (External): Selecting this checkbox will allow you to enter an area that will be used by the static routing setup on the external network

Distribute RIP over OSPF: Enabling this option will allow the router to broadcast the RIP routing protocol over OSPF.

RIP Service: Select to either **Disable** or **Enable** the AP from offering RIP routing services.

Side (Devices): Select the checkbox for the interface that will allow clients to connect to.

Distribute OSPF over RIP: Enabling this option will allow the router to broadcast the OSPF routing protocol over the RIP service.

Click **Create New Route Table** to define specific routes that will be handled by the AP.

This page will allow you to define specific routes that will be broadcasted by the AP and made available to the clients that connect to it.

Mode: Select whether the route being offered is either **Disabled** or **Enabled**.

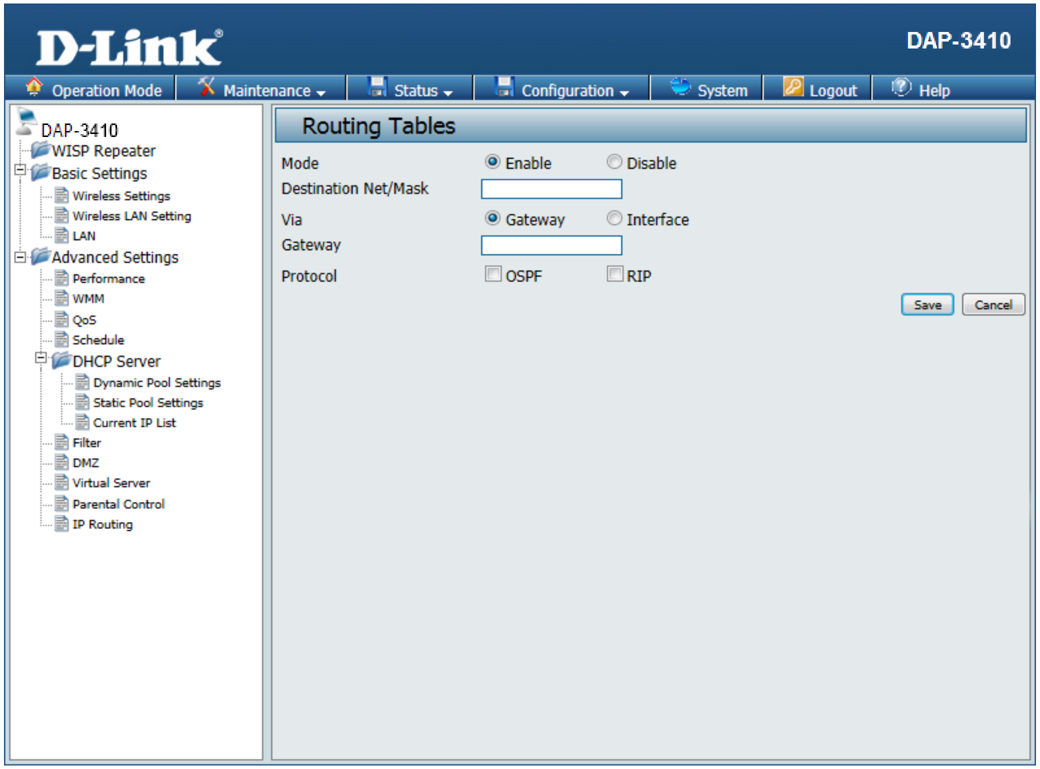
Destination Net/Mask: Enter either the destination network, or the subnet mask that will be used in the static route.

Via: Select whether the static route will be controlled by an existing gateway, or if the interface on the AP should route the traffic.

Gateway: This option becomes available if **Gateway** is selected. Enter the gateway IP address.

Interface: This option becomes available if **Interface** is selected. Enter the interface on the AP that will be used with the static route.

Protocol: Select the checkmark for the routing protocol that will be used to advertise this static route to other routers on the network.



Routing Tables

Mode	● Enable	○ Disable
Destination Net/Mask		
Via	● Gateway	○ Interface
Gateway		
Protocol	□ OSPF	□ RIP

Maintenance

Administration Settings

This page will allow you to change a number of settings that are used by the device administrator such as changing the password used to access the device, as well as the method of accessing the device remotely and from what IP address the device can be remotely managed from.

Limit Administrator IP: Check this to limit administrator access to specific IP ranges only.

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

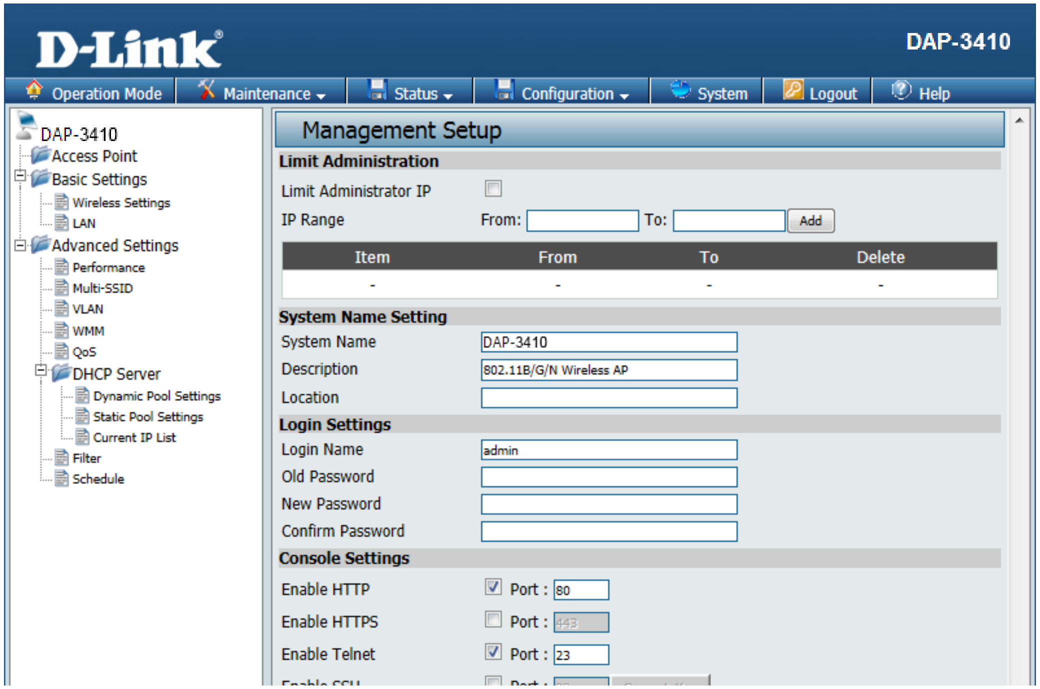
System Name: Enter a name for the device. The default name is D-Link DAP-3410.

Description: Enter a description for the device and its role.

Location: Enter the physical location of the device, e.g. 72nd Floor, D-Link HQ.

Login Name: Enter a user name. The default is admin.

Old Password / New Password: You can change your password by entering the old password, then entering the new password and entering it again to confirm it. The password is case-sensitive and should be between 0 and 12 characters.



Management Setup

Limit Administration

Limit Administrator IP □

IP Range From: To: Add

Item	From	To	Delete
-	-	-	-

System Name Setting

System Name: DAP-3410

Description: 802.11B/G/N Wireless AP

Location:

Login Settings

Login Name: admin

Old Password:

New Password:

Confirm Password:

Console Settings

Enable HTTP ☑ Port : 80

Enable HTTPS □ Port : 443

Enable Telnet ☑ Port : 23

Enable HTTP: Select this checkbox to enable access to the console via HTTP. The port which the console will use for connections can also be specified.

Enable HTTPS: Select this checkbox to enable access to the console via HTTPS. The port which the console will use for connections can also be specified.

Enable Telnet: Select this checkbox to enable access to the console via Telnet. The port which the console will use for connections can also be specified.

Enable SSH: Select this checkbox to enable access to the console via SSH. The port which the console will use for connections can also be specified. In order to use this feature, you will need to click on the Generate Key button to create an SSH key.

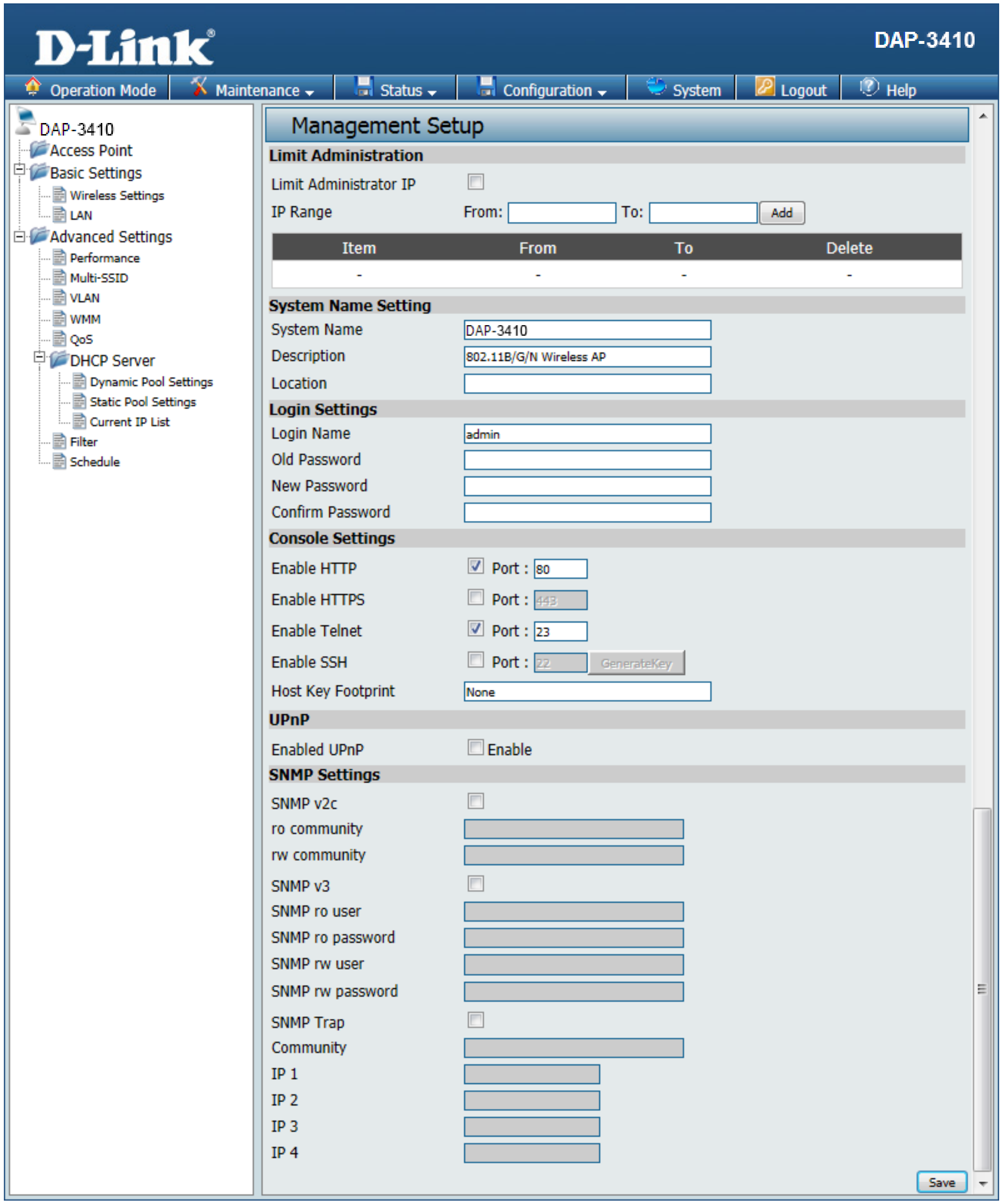
Host Key Footprint: This will display the SSH key generated by the AP.

Enable UPnP: Select this checkbox to enable UPnP support for the management console on the AP.

SNMP v2c: Check the box to enable the SNMP v2c functions. This option is disabled by default.

RO Community: Enter the read only community string.

RW Community: Enter the read & write community string.



Management Setup

Limit Administration

Limit Administrator IP □

IP Range From: To:

Item	From	To	Delete
-	-	-	-

System Name Setting

System Name: DAP-3410
Description: 802.11B/G/N Wireless AP
Location:

Login Settings

Login Name: admin
Old Password:
New Password:
Confirm Password:

Console Settings

Enable HTTP ☑ Port : 80
Enable HTTPS □ Port : 443
Enable Telnet ☑ Port : 23
Enable SSH □ Port : 22
Host Key Footprint: None

UPnP

Enabled UPnP □ Enable

SNMP Settings

SNMP v2c □
ro community
rw community
SNMP v3 □
SNMP ro user
SNMP ro password
SNMP rw user
SNMP rw password
SNMP Trap □
Community
IP 1
IP 2
IP 3
IP 4

SNMP v3: Check the box to enable the SNMP v3 functions. This option is disabled by default.

SNMP ro user: Enter the username for read only SNMP access.

SNMP ro password: Enter the password for read only SNMP access.

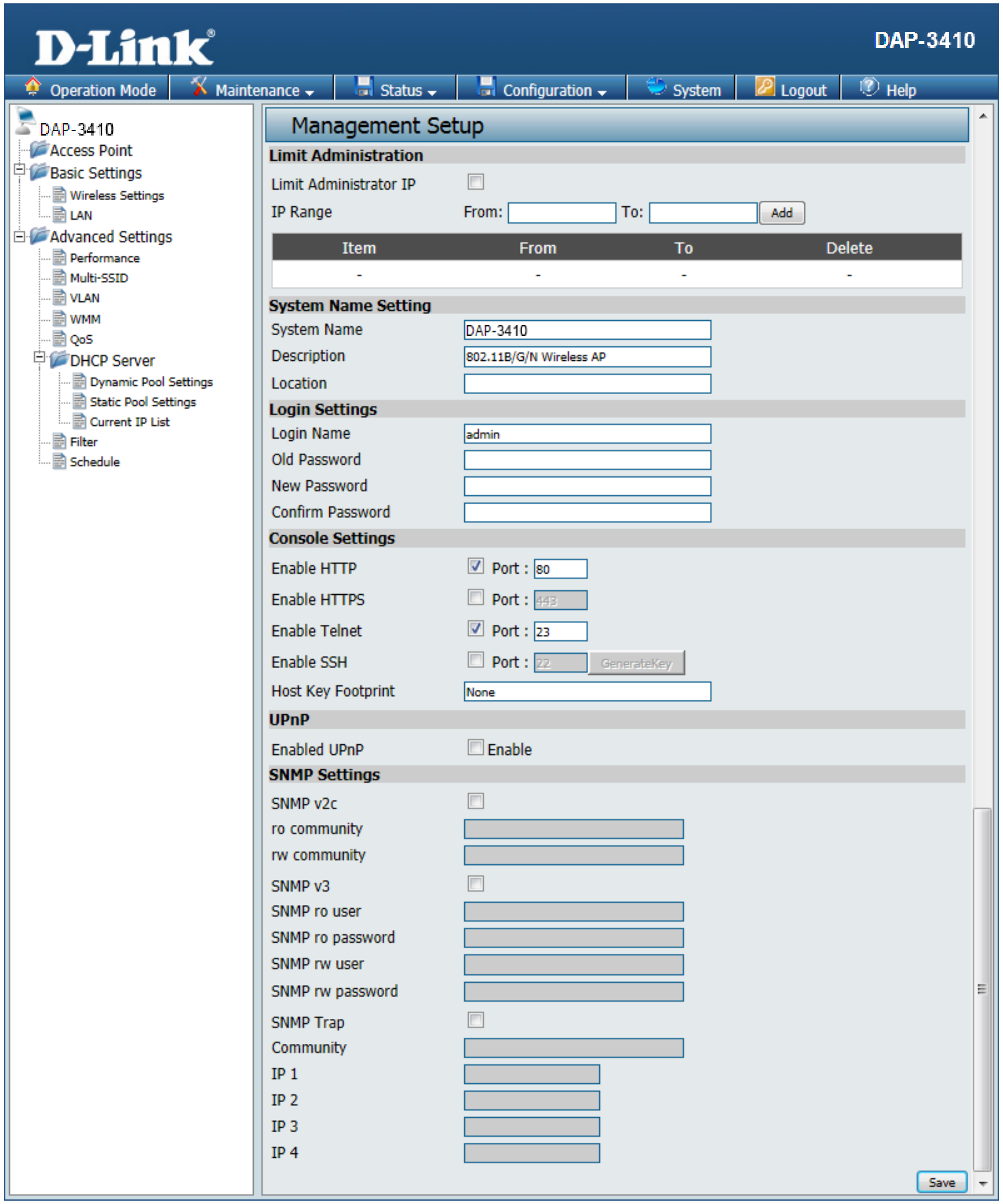
SNMP rw user: Enter the username for read/write SNMP access.

SNMP rw password: Enter the password for read/write SNMP access.

SNMP Trap: Check the box to enable the sending of Trap Status messages.

Community: Set a community string required by the remote host computer that will receive trap messages or notices send by the system.

IP 1 to 4: Enter the IP addresses of the remote hosts to receive trap messages.



Management Setup

Limit Administration

Limit Administrator IP □

IP Range From: To:

Item	From	To	Delete
-	-	-	-

System Name Setting

System Name: DAP-3410

Description: 802.11B/G/N Wireless AP

Location:

Login Settings

Login Name: admin

Old Password:

New Password:

Confirm Password:

Console Settings

Enable HTTP ☑ Port : 80

Enable HTTPS □ Port : 443

Enable Telnet ☑ Port : 23

Enable SSH □ Port : 22

Host Key Footprint: None

UPnP

Enabled UPnP □ Enable

SNMP Settings

SNMP v2c □

ro community

rw community

SNMP v3 □

SNMP ro user

SNMP ro password

SNMP rw user

SNMP rw password

SNMP Trap □

Community

IP 1

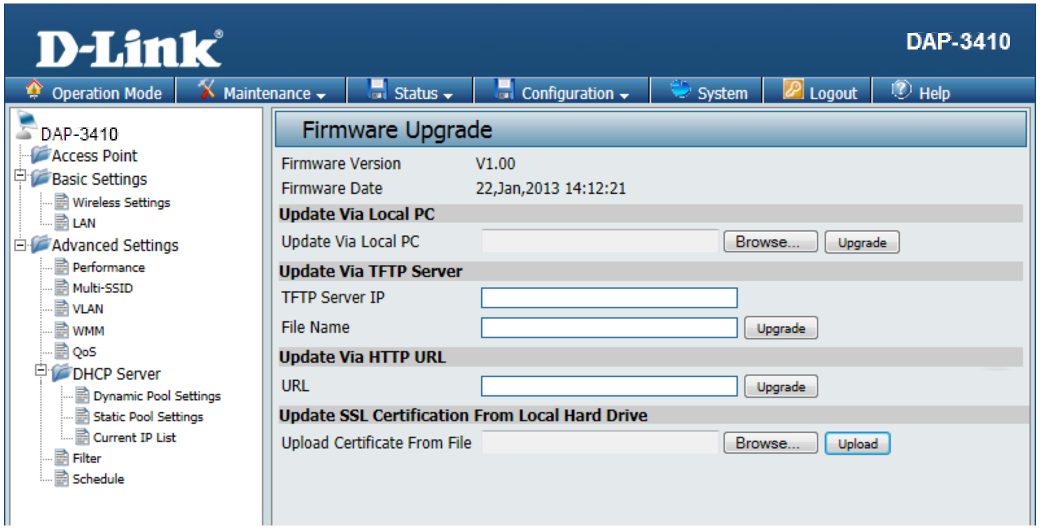
IP 2

IP 3

IP 4

Firmware and SSL Certification Upload

This page allows you to upgrade the firmware of the access point as well as upload an SSL certificate to secure the connections made to the DAP-3410. Make sure the firmware or SSL certificate you want to use is on the local hard drive of the computer. Please check the D-Link support website for firmware updates by visiting **http://support.dlink.com**. The DAP-3410 includes a number of ways to update the firmware such as a direct connection over the LAN, via a TFTP server, or via HTTP. SSL certificates must be updated via the LAN connection.



Firmware Upgrade

Firmware Version V1.00

Firmware Date 22,Jan,2013 14:12:21

Update Via Local PC

Update Via Local PC

Update Via TFTP Server

TFTP Server IP

File Name

Update Via HTTP URL

URL

Update SSL Certification From Local Hard Drive

Upload Certificate From File

Update Via Local PC: Click on **Browse** to locate the firmware file to be used for the update. Click on **Upgrade** to start the process of updating the firmware.

TFTP Server IP: Enter the IP address of the TFTP server that will be used to upgrade the AP.

File Name: Enter the filename of the firmware hosted on the TFTP server. Click on **Upgrade** to start the process of updating the firmware.

Update Via HTTP URL: Enter the URL of the HTTP server that will be used to upgrade the AP. This should be the address of the server and the location of the hosted firmware. Click on **Upgrade** to start the process of updating the firmware.

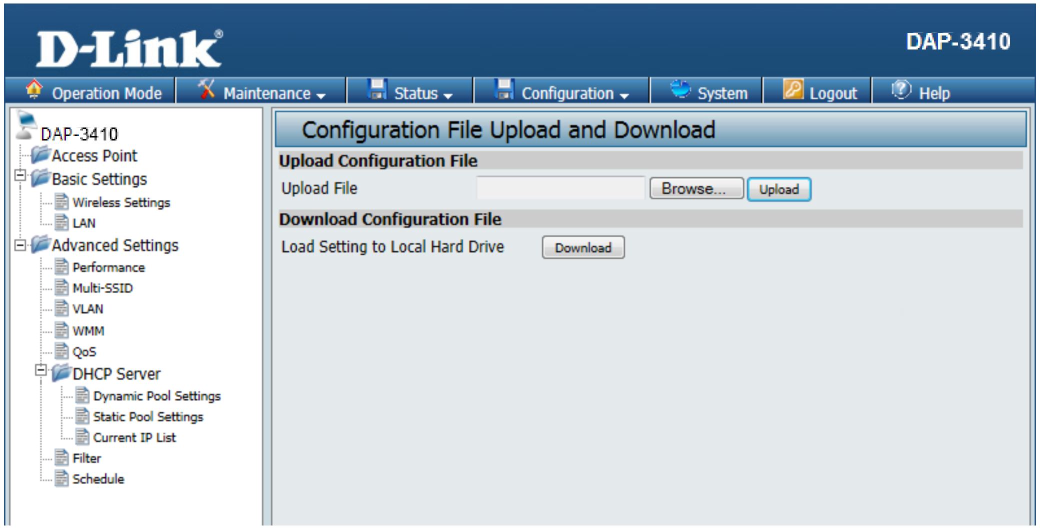
Upload Certification From File: Click on **Browse** to locate the certificate file to be used. Click on **Upload** to start the process of transferring the certificate to the AP.

Configuration File

This page will allow you to upload or download a configuration file for the DAP-3410.

Upload File: Use this option to load a previously saved configuration. Click **Browse** to find a previously saved configuration file. Then, click the **Upload Settings** button to transfer those settings to the access point.

Load Setting to Local Hard Drive: Use this option to save the current access point configuration settings to a file on the hard disk of the computer you are using. Click the **Download** button. You will then see a file dialog where you can select a location and file name for the settings.



Configuration File Upload and Download

Upload Configuration File

Upload File [Browse...] [Upload]

Download Configuration File

Load Setting to Local Hard Drive [Download]

Ping Watchdog

This page will allow you to configure the Ping Watchdog function of the AP. Ping Watchdog works by sending ICMP "echo request" packets to a target host and listens for ICMP echo response replies. Ping Watchdog is enabled by default.

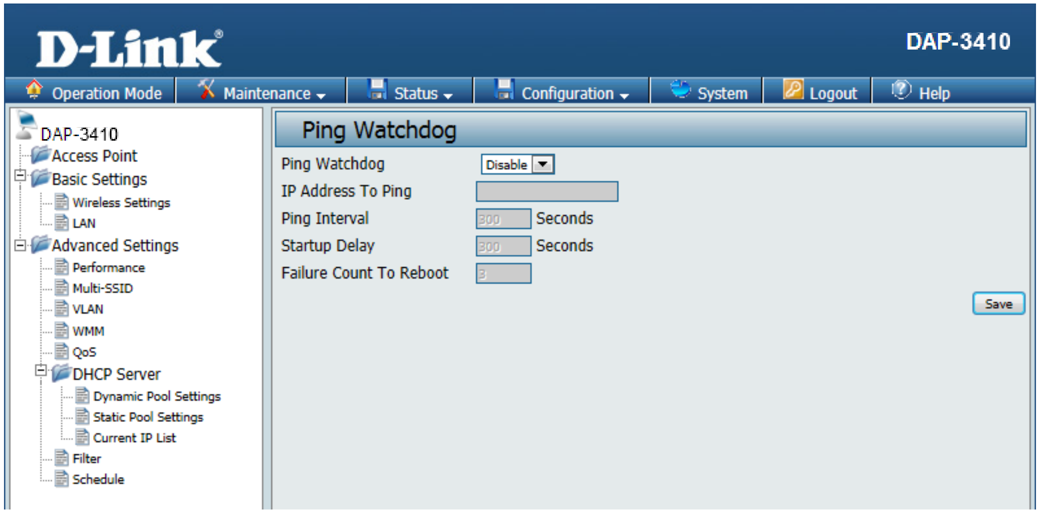
Ping Watchdog: Select whether the ping watchdog function is **Disabled** or **Enabled**.

IP Address to Ping: Enter the IP address that will be used for the AP to ping.

Ping Interval: Set the amount of time in seconds that the AP will wait between pings.

Startup Delay: Set the amount of time in seconds that the AP will wait before beginning to ping the target host.

Failure Count to Reboot: Set the number of times that the ping will fail before the ping watchdog will force the AP to reboot.

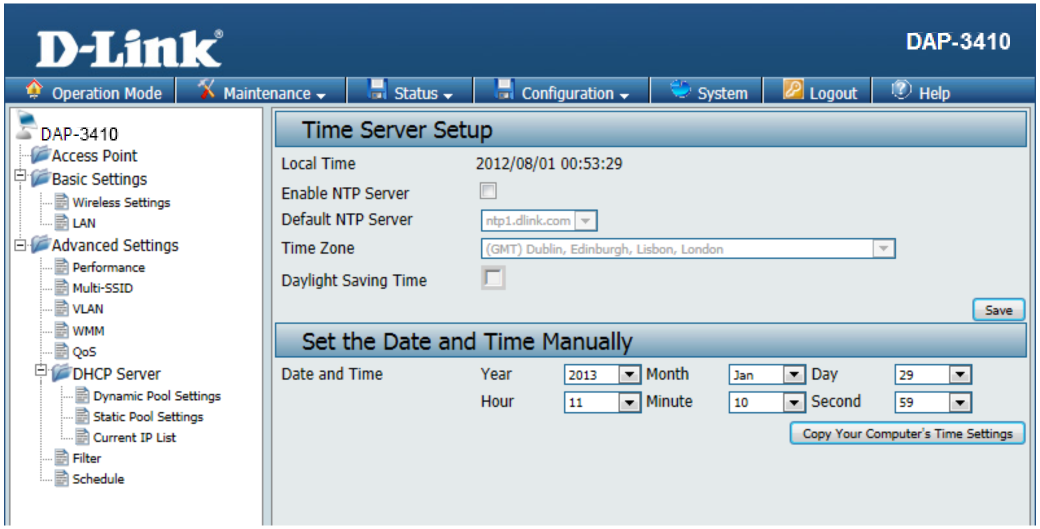


Ping Watchdog

Ping Watchdog	Disable
IP Address To Ping	
Ping Interval	300 Seconds
Startup Delay	300 Seconds
Failure Count To Reboot	3

Time and Date

The Time Server Setup page allows you to configure, update, and maintain the correct time on the internal system clock. In this section you can set the time zone that you are in. Daylight Saving can also be configured to automatically adjust the time when needed.



Time Server Setup

Local Time 2012/08/01 00:53:29

Enable NTP Server □

Default NTP Server ntp1.dlink.com

Time Zone (GMT) Dublin, Edinburgh, Lisbon, London

Daylight Saving Time □

Save

Set the Date and Time Manually

Date and Time Year 2013 Month Jan Day 29

Hour 11 Minute 10 Second 59

Copy Your Computer's Time Settings

Enable NTP Server: NTP is short for Network Time Protocol. This allows the system clock to be updated automatically by using an NTP server.

NTP Server Used: Enter the NTP server or select one from the drop-down menu.

Time Zone: Select the Time Zone from the drop-down menu.

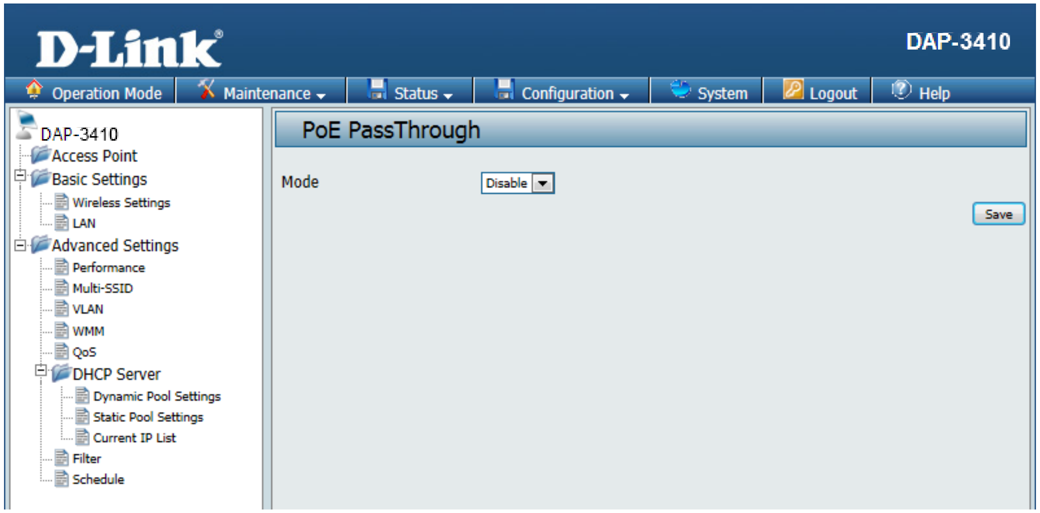
Daylight Saving Time: To set Daylight Saving time manually, click the Daylight Saving Time check box. Next, use the drop-down menu to select a Daylight Saving Offset and then enter a start date and an end date for daylight saving time.

Date and Time: To manually set the time, enter the Year, Month, Day, Hour, Minute, and Second and then click **Save**. To avoid having to manually set the time, you can also click the **Copy Your Computer's Time Settings** button at the bottom of the page to have the DAP-3410 automatically set the time based on the system clock of the computer being used to configure the DAP-3410.

PoE PassThrough

This page will allow you to change the PoE pass through setting of the AP. If this is enabled, the LAN port will allow D-Link surveillance cameras such as the DCS-3716, DCS-6113, and DCS-7110 to be powered through the secondary LAN port.

Mode: Select whether the PoE pass through function is **Disabled** or **Enabled**.



PoE PassThrough

Mode: Disable

Status

Device Information

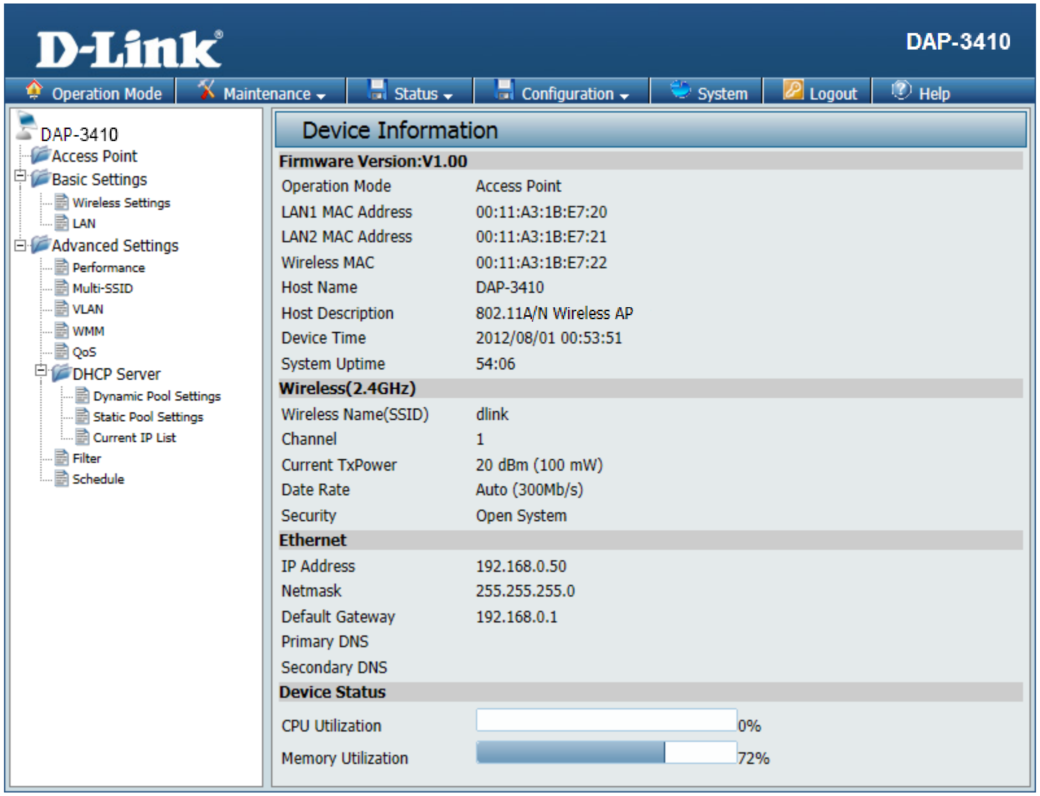
This page displays the current LAN, wireless LAN and important device information for the DAP-3410.

Firmware Version: Displays the access point's time and firmware version. Also displays the current operating mode and hardware address (MAC), which may be needed by a network administrator.

Wireless: Displays the wireless your wireless settings such as SSID and Channel along with the current power output of the antennae, data throughput, and wireless security method.

Ethernet: Displays the private (local) IP settings for the two built in LAN ports on the access point.

Device Status: Displays current system utilization of the access point.



Device Information

Firmware Version:V1.00	
Operation Mode	Access Point
LAN1 MAC Address	00:11:A3:1B:E7:20
LAN2 MAC Address	00:11:A3:1B:E7:21
Wireless MAC	00:11:A3:1B:E7:22
Host Name	DAP-3410
Host Description	802.11A/N Wireless AP
Device Time	2012/08/01 00:53:51
System Uptime	54:06
Wireless(2.4GHz)	
Wireless Name(SSID)	dlink
Channel	1
Current TxPower	20 dBm (100 mW)
Date Rate	Auto (300Mb/s)
Security	Open System
Ethernet	
IP Address	192.168.0.50
Netmask	255.255.255.0
Default Gateway	192.168.0.1
Primary DNS	
Secondary DNS	
Device Status	
CPU Utilization	0%
Memory Utilization	72%

Client Information

This window displays the wireless client information for clients currently connected to the DAP-3410.

MAC Address: Displays the MAC address of the client.

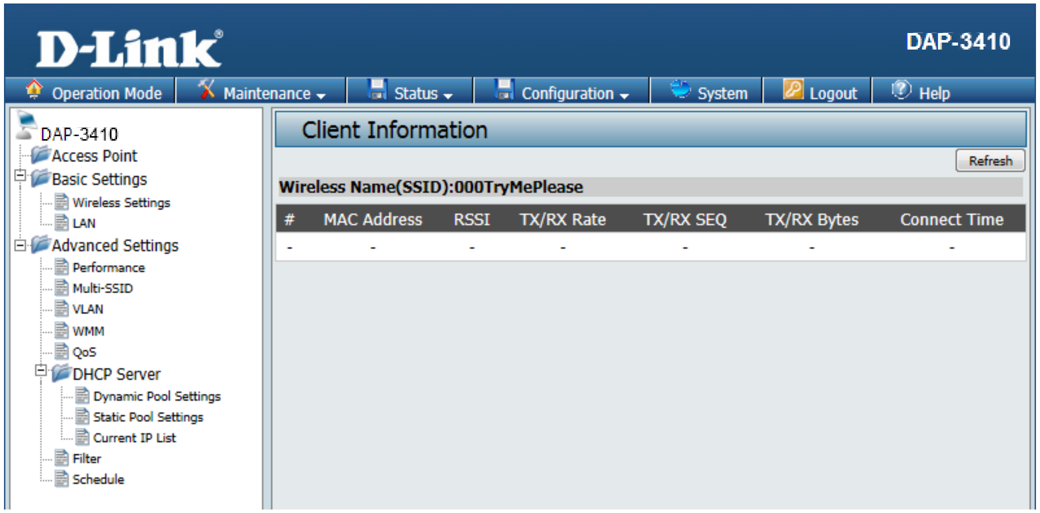
RSSI: Displays the client's signal strength (received signal strength indicator).

TX/RX Rate: Displays the current wireless speed that the client is connected with.

TX/RX SEQ: This indicates the TX/RX sequence of the respective WDS's link

TX/RX Bytes: Displays the current amount of data that the client has trasferred since it connected.

Connect Time: Displays the total amount of time that the client has been connected.

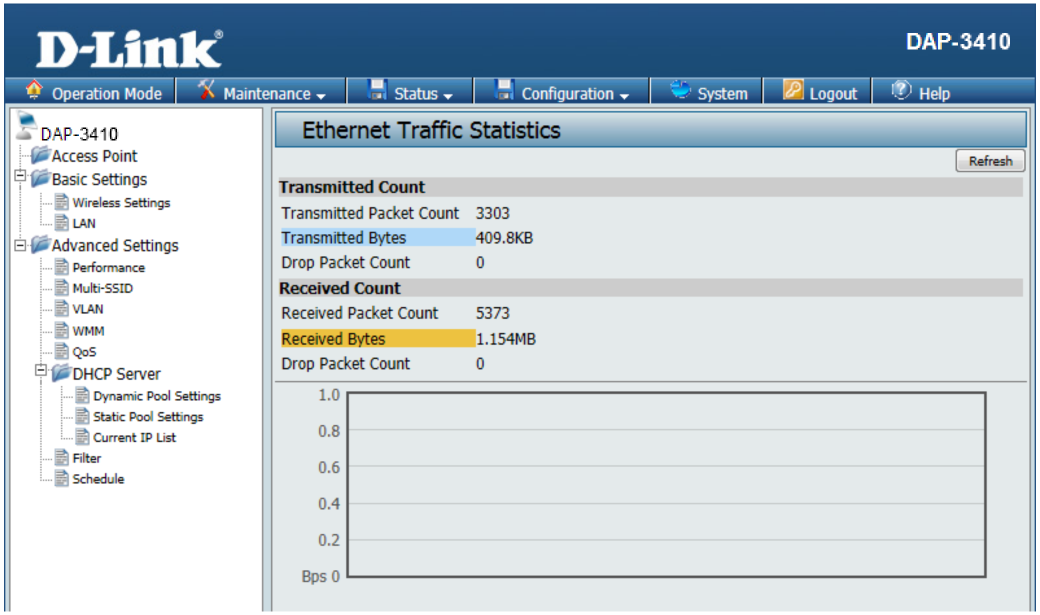


Wireless Name(SSID):000TryMePlease

#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	TX/RX Bytes	Connect Time
-	-	-	-	-	-	-

Ethernet Information

The DAP-3410 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the access point is rebooted.

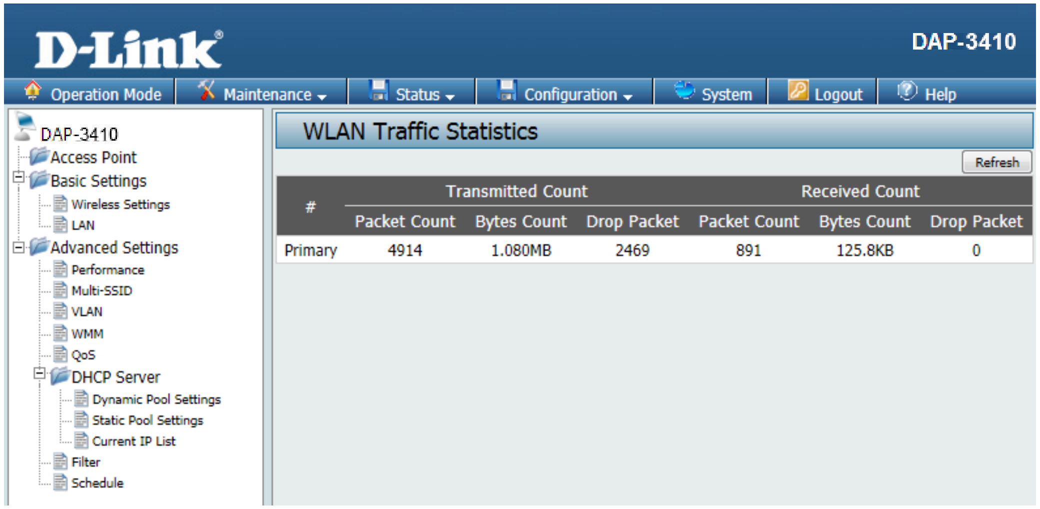


Ethernet Traffic Statistics

Transmitted Count	
Transmitted Packet Count	3303
Transmitted Bytes	409.8KB
Drop Packet Count	0
Received Count	
Received Packet Count	5373
Received Bytes	1.154MB
Drop Packet Count	0

WLAN Information

This window displays wireless network statistics for data throughput, transmitted and received frames, and frame errors. The traffic counter will reset if the access point is rebooted.



WLAN Traffic Statistics

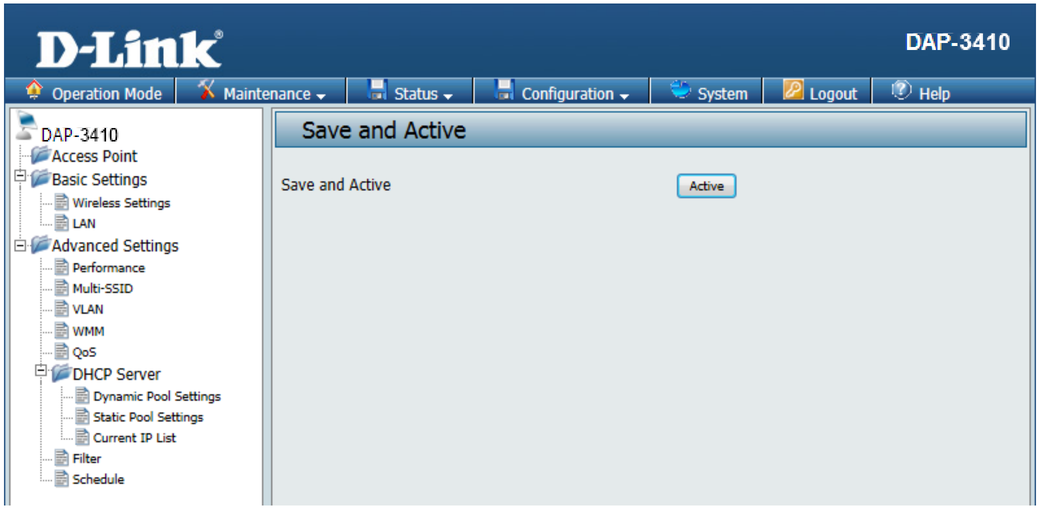
#	Transmitted Count			Received Count		
	Packet Count	Bytes Count	Drop Packet	Packet Count	Bytes Count	Drop Packet
Primary	4914	1.080MB	2469	891	125.8KB	0

Configuration

Save and Active

When making changes on most of the configuration screens it is best to use the **Save** button at the bottom of each screen to save (not activate) your configuration changes.

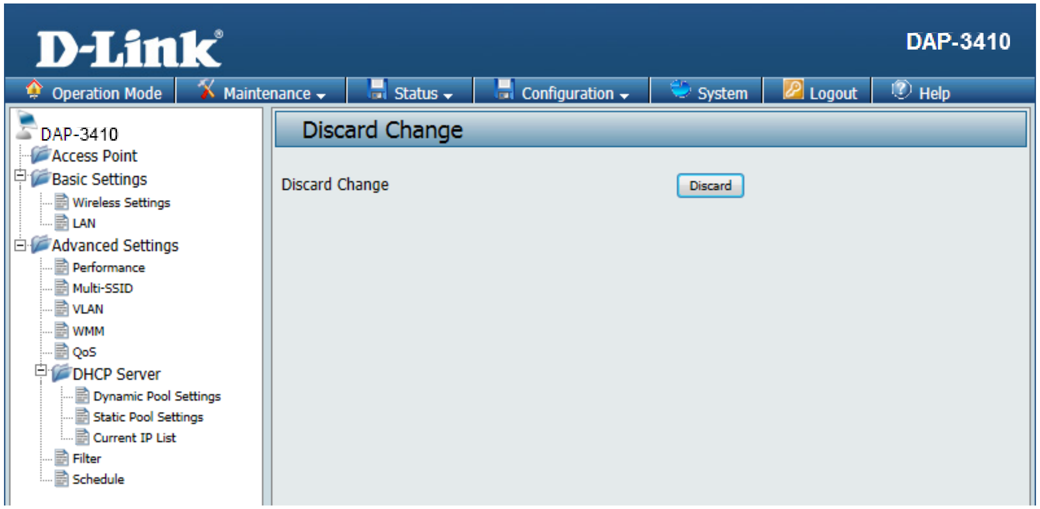
You may change settings to multiple pages before activating. Once you are finished, click the **Configuration** button located at the top of the page and then click **Save and Activate**. You can then click **Activate** here to enable your changes.



Discard Changes

When making changes on most of the configuration screens it is best to use the **Save** button at the bottom of each screen to save (not activate) your configuration changes.

If you wish to discard all of the changes you have made, and not yet activated, you may click the **Discard** button.

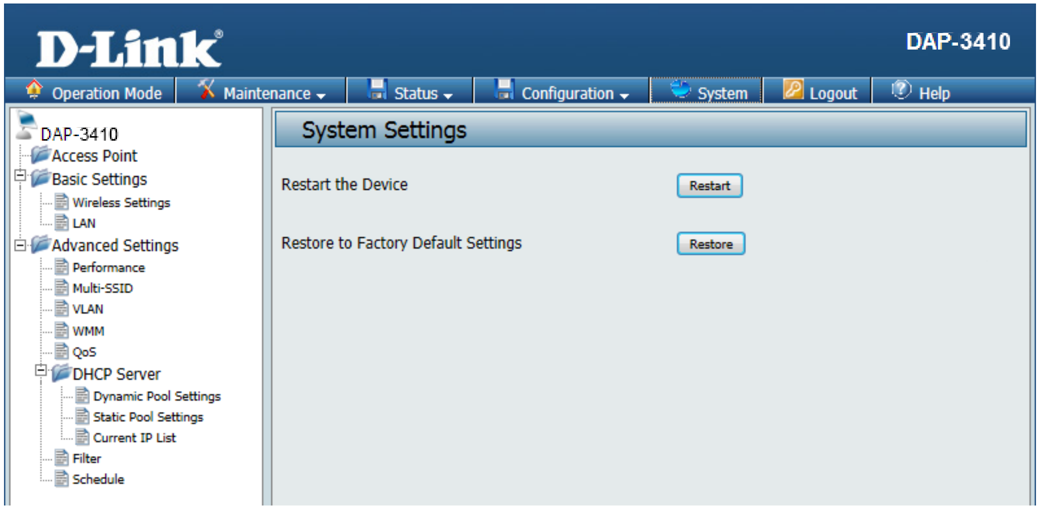


System

This page will allow you to restart the AP, or restore its settings to the factory defaults.

Click the **Restart** button to reboot the device.

Click the **Restore** button to reset all settings back to the factory defaults. Please note that this will erase all settings and changes made to the device's configuration.



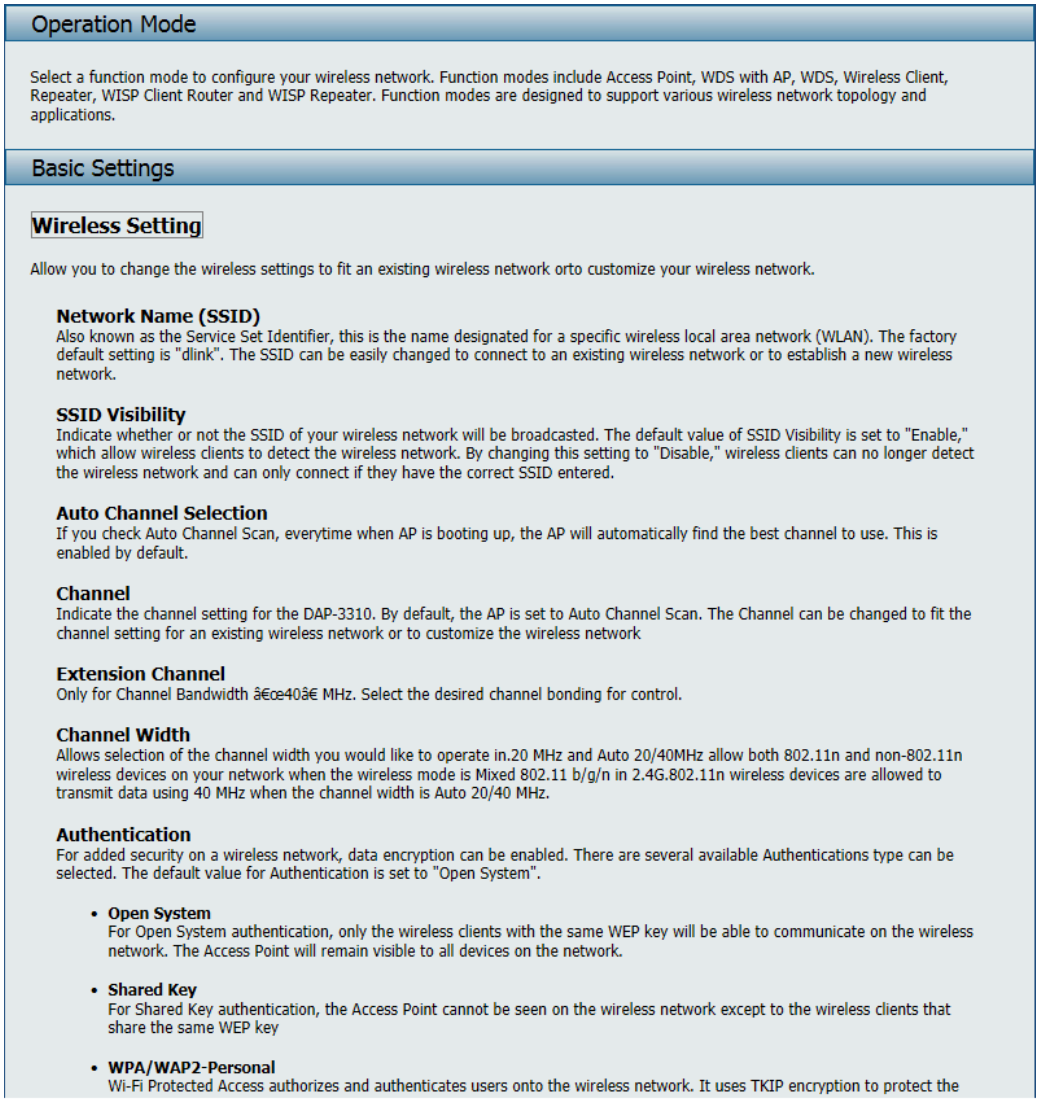
System Settings

Restart the Device

Restore to Factory Default Settings

Help

Further information and in depth help can be found anytime from the AP's online help function. Scroll down the Help page for topics and explanations.



Operation Mode

Select a function mode to configure your wireless network. Function modes include Access Point, WDS with AP, WDS, Wireless Client, Repeater, WISP Client Router and WISP Repeater. Function modes are designed to support various wireless network topology and applications.

Basic Settings

Wireless Setting

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

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-3310. 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

Extension Channel
Only for Channel Bandwidth â€œ40â€ MHz. Select the desired channel bonding for control.

Channel Width
Allows selection of the channel width you would like to operate in.20 MHz and Auto 20/40MHz allow both 802.11n and non-802.11n wireless devices on your network when the wireless mode is Mixed 802.11 b/g/n in 2.4G.802.11n wireless devices are allowed to transmit data using 40 MHz when the channel width is Auto 20/40 MHz.

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/WAP2-Personal**
  Wi-Fi Protected Access authorizes and authenticates users onto the wireless network. It uses TKIP encryption to protect the

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-3410 offers the following types of security:

- WEP (Wired Equivalent Privacy)
- WPA-Personal (Wi-Fi Protected Access)
- WPA-Enterprise (Wi-Fi Protected Access)

What is WEP?

WEP, or Wired Equivalent Privacy, is a Wi-Fi security protocol that encrypts transmitted data. WEP is an older protocol that is not believed to be as effective anymore.

WEP uses a passphrase or key to authenticate your wireless connection. For 64-Bit WEP, the key is an alpha-numeric password that is 10 hex digits or an ASCII password consisting of 5 text characters. The hex digits are either numbers from 0 to 9 or letters from A to F. For 128-Bit WEP, the key is an alpha-numeric password that is 26 hex digits or an ASCII password with 13 text characters.

Configure WEP

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (dlinkap. local). Click on **Setup** and then click **Wireless Setup** on the left side.

2. Next to *Security Mode*, select **WEP**.
   Note: Choosing WEP means the device will only operate in Legacy wireless mode (802.11B/G) and will not provide 802.11N performance.

3. Next to *WEP Encryption*, select **64Bit(10 hex digits)**, **64Bit(5 ASCII characters)**, **128Bit(26 hex digits)** or **128Bit(13 ASCII characters)**.

4. Next to *WEP Key 1*, enter a set of digits or letters from A to F, or a string of text.

5. Next to *Authentication,* select **Both** or **Shared Key**.

6. Click **Save Settings** at the top of the window to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the access point.

What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (dlinkap.local). Click on **Setup** and then click **Wireless Setup** on the left side.

2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *WPA Mode*, select **Auto(WPA or WPA2)**, **WPA2 only**, or **WPA only**.

4. Next to *Cipher Type*, select **TKIP**, **AES**, or **TKIP and AES**.

5. Next to *Pre-Shared Key,* enter a key. The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The passphrase must be between 8-63 characters.

6. Click **Save Settings** at the top of the window to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the access point.

Configure WPA/WPA2 Enterprise

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point (dlinkap.local). Click on **Setup** and then click **Wireless Setup** on the left side.

2. Next to *Security Mode*, select **WPA-Enterprise**.

3. Next to *WPA Mode*, select **Auto(WPA or WPA2)**, **WPA2 only**, or **WPA only**.

4. Next to *Cipher Mode*, select **TKIP**, **AES**, or **Auto**.

5. Next to *RADIUS Server IP Address*, enter the IP Address of your RADIUS server.

6. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.

7. Next to *RADIUS Server Shared Secret*, enter the security key.

8. Click **Advanced** to enter settings for a secondary RADIUS Server.

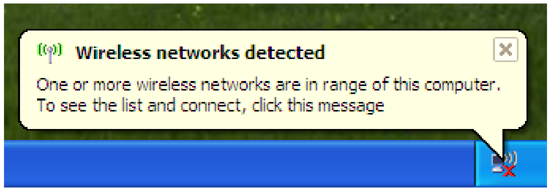
9. Click **Save Settings** to save your settings.

Connect to a Wireless Network

Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

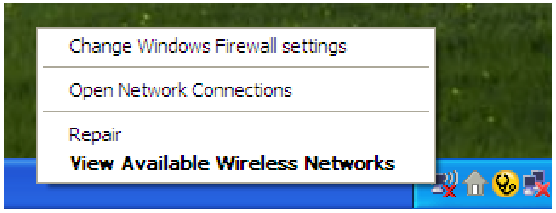


Wireless networks detected

One or more wireless networks are in range of this computer.
To see the list and connect, click this message

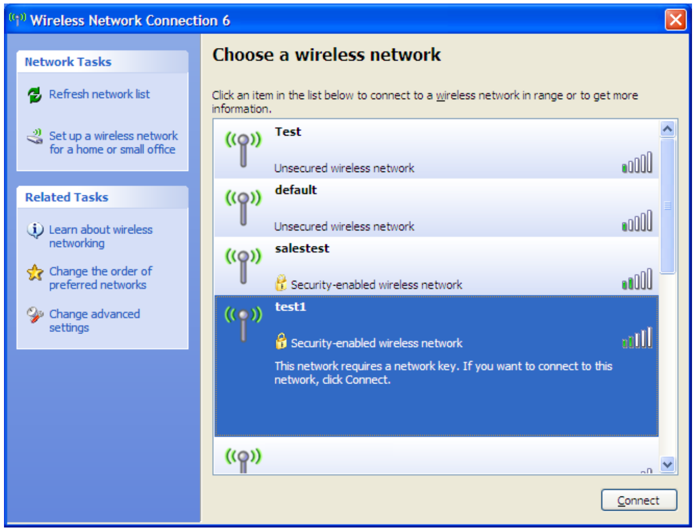
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

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



Wireless Network Connection 6

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

salestest
Security-enabled wireless network

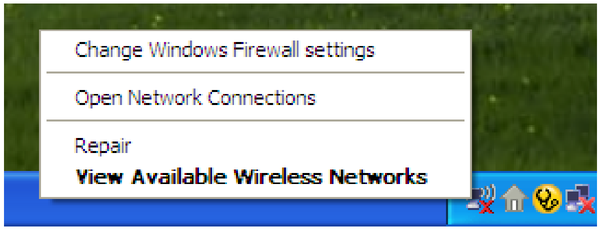
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

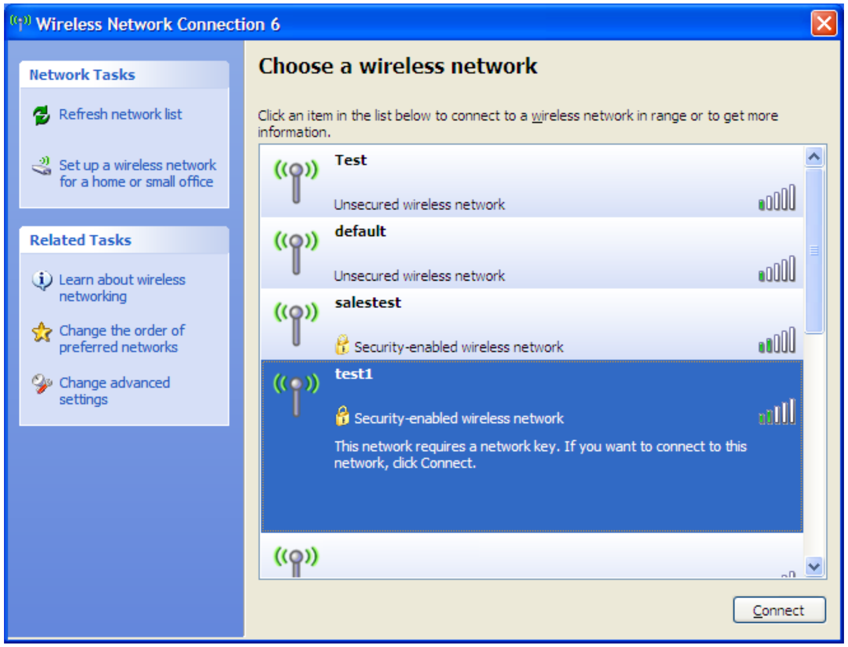
Configure WPA-PSK

It is recommended to enable WEP on your wireless bridge or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks.**


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

2. Highlight the wireless network (SSID) you would like to connect to and click **Connect.**


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

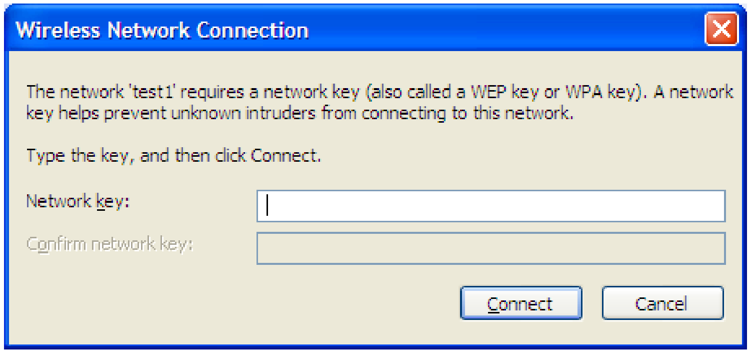
default
Unsecured wireless network

salestest
Security-enabled wireless network

test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect.**

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


Wireless Network Connection

The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

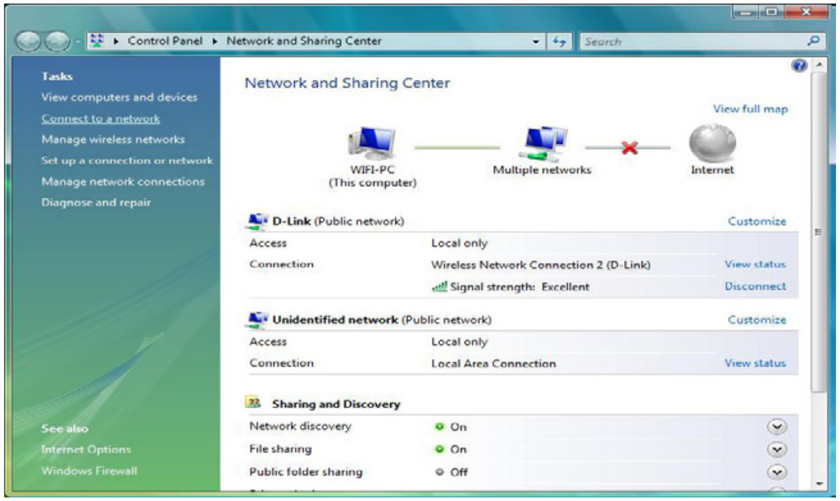
Network key:

Confirm network key:

Using Windows Vista®

Windows Vista® users may use the convenient, built-in wireless utility. Follow these instructions:

From the Start menu, go to Control Panel, and then click on **Network and Sharing Center**.



Network and Sharing Center

D-Link (Public network)

Access	Local only
Connection	Wireless Network Connection 2 (D-Link)
	Signal strength: Excellent

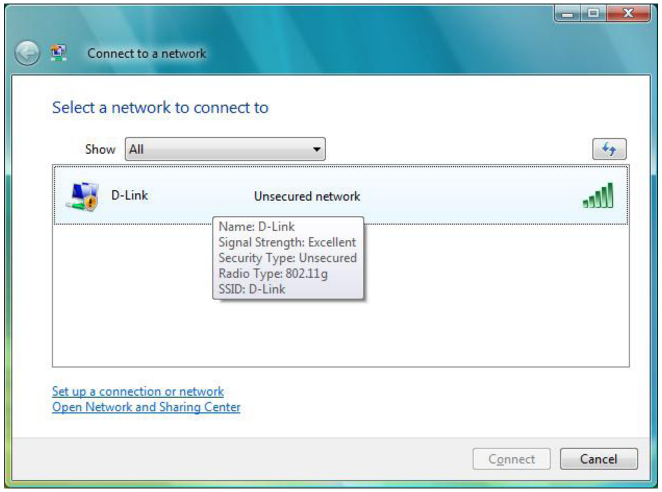
Unidentified network (Public network)

Access	Local only
Connection	Local Area Connection

Sharing and Discovery

Network discovery	● On
File sharing	● On
Public folder sharing	○ Off

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) under Select a network to connect to and then click the **Connect** button.


Connect to a network
Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

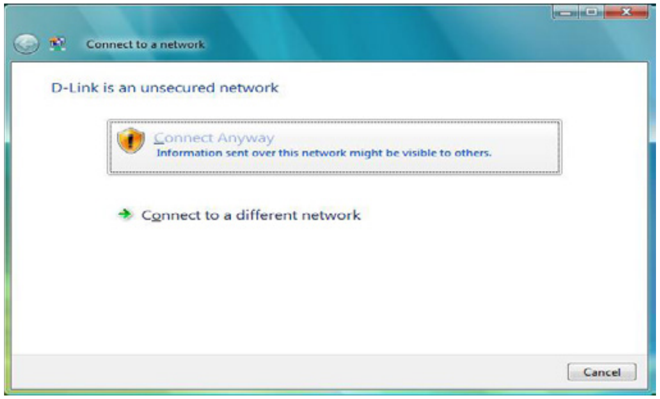
Select a network to connect to

Show: All

D-Link Unsecured network

Name: D-Link
Signal Strength: Excellent
Security Type: Unsecured
Radio Type: 802.11g
SSID: D-Link

Click **Connect Anyway** to continue.

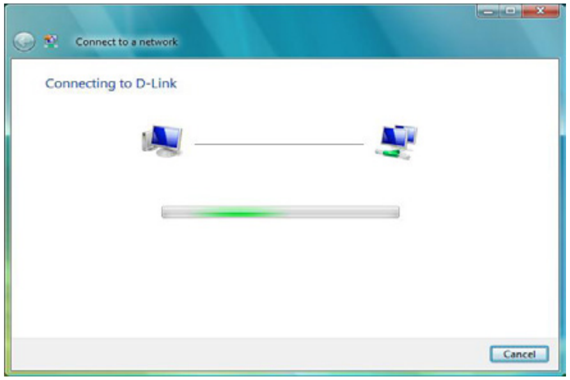


D-Link is an unsecured network

Connect Anyway
Information sent over this network might be visible to others.

Connect to a different network

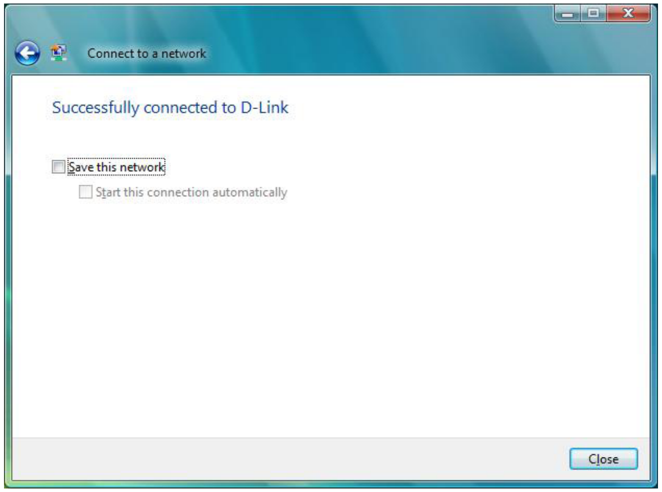
The utility will display the following window to indicate a connection is being made.



Connecting to D-Link

The final window indicates the establishment of a successful connection.

The next two pages display the windows used to connect to either a WEP or a WPA-PSK wireless network.



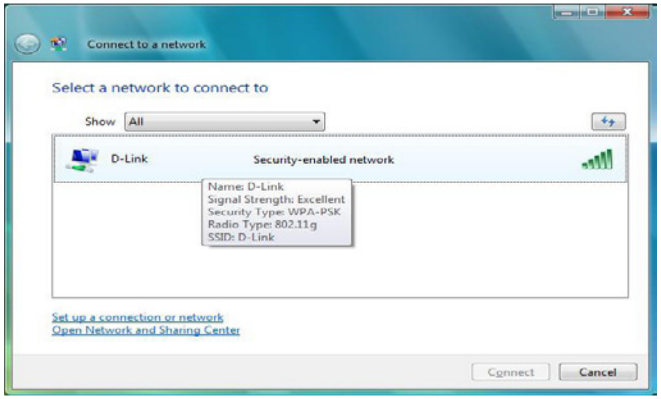
Successfully connected to D-Link

□ Save this network
□ Start this connection automatically

Configure WPA-PSK

It is recommended to enable WEP on your wireless bridge or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

Click on a network (displayed using the SSID) using WPA-PSK under Select a network to connect to and then click the **Connect** button.



Connect to a network

Select a network to connect to

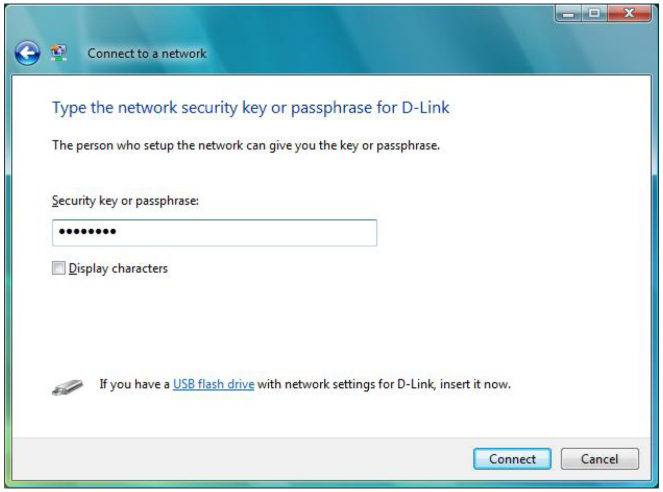
Show: All

D-Link Security-enabled network

Name: D-Link
Signal Strength: Excellent
Security Type: WPA-PSK
Radio Type: 802.11g
SSID: D-Link

Set up a connection or network
Open Network and Sharing Center

Enter the appropriate security key or passphrase in the field provided and then click the **Connect** button.



Connect to a network

Type the network security key or passphrase for D-Link

The person who setup the network can give you the key or passphrase.

Security key or passphrase: ••••••••

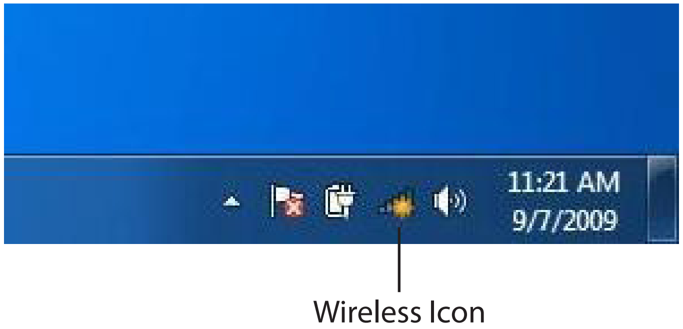
□ Display characters

If you have a USB flash drive with network settings for D-Link, insert it now.

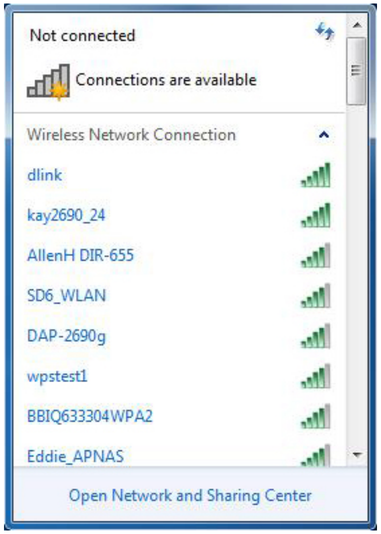
Using Windows® 7

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



2. The utility will display any available wireless networks in your area.


Not connected

Connections are available

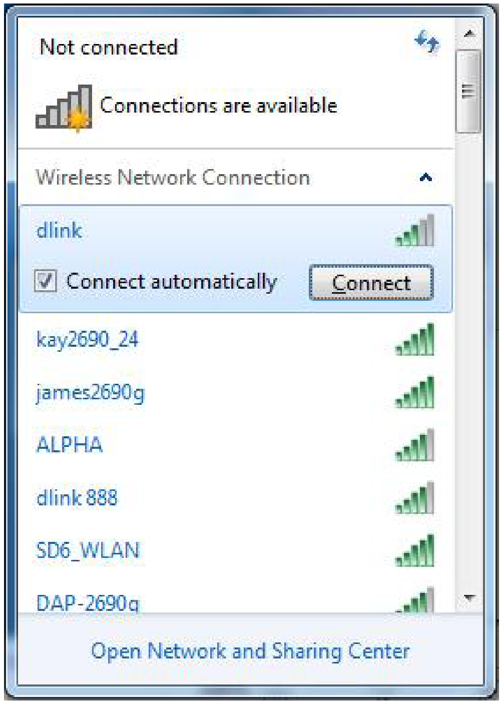
Wireless Network Connection

- dlink
- kay2690_24
- AllenH DIR-655
- SD6_WLAN
- DAP-2690g
- wpstest1
- BBIQ633304WPA2
- Eddie_APNAS

Open Network and Sharing Center

3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

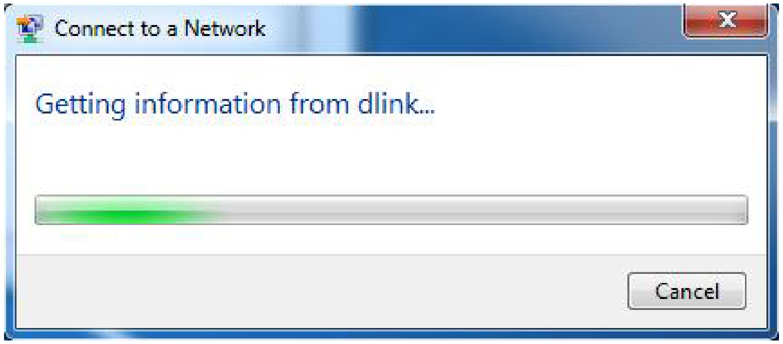
   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



Not connected

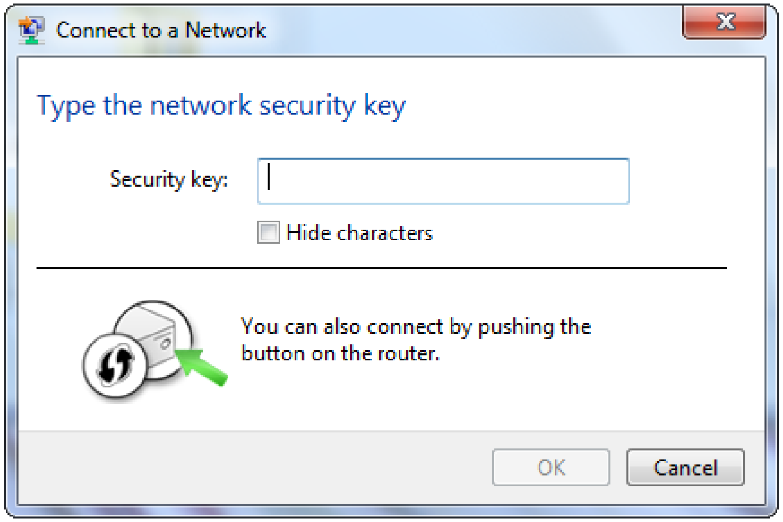
Connections are available

4. The following window appears while your computer tries to connect to the router.



Getting information from dlink...

5. Enter the same security key or passphrase that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.



You can also connect by pushing the button on the router.

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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-3410. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link access point (**dlinkapwxyz.local** for example, with **wxyz** the last four digits of the AP's MAC Address), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:

  - Microsoft Internet Explorer® 7 and higher
  - Mozilla Firefox 12.0 and higher
  - Google™ Chrome 20.0 and higher
  - Apple Safari 4 and higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:

  - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** Icon. From the Security tab, click the button to restore the settings to their defaults.

  - Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.

  - Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.

  - Close your web browser (if open) and open it.

- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.

- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

If you forgot your password, you must reset your access point. Unfortunately this process will change all your settings back to the factory defaults.

To reset the access point, locate the reset button (hole) on the rear panel of the unit. With the access point powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the access point will go through its reboot process. Wait about 30 seconds to access the access point. The default IP address is 192.168.0.50. When logging in, the username is Admin and leave the password box empty.

3. Why can’t I connect to certain sites or send and receive emails when connecting through my access point?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

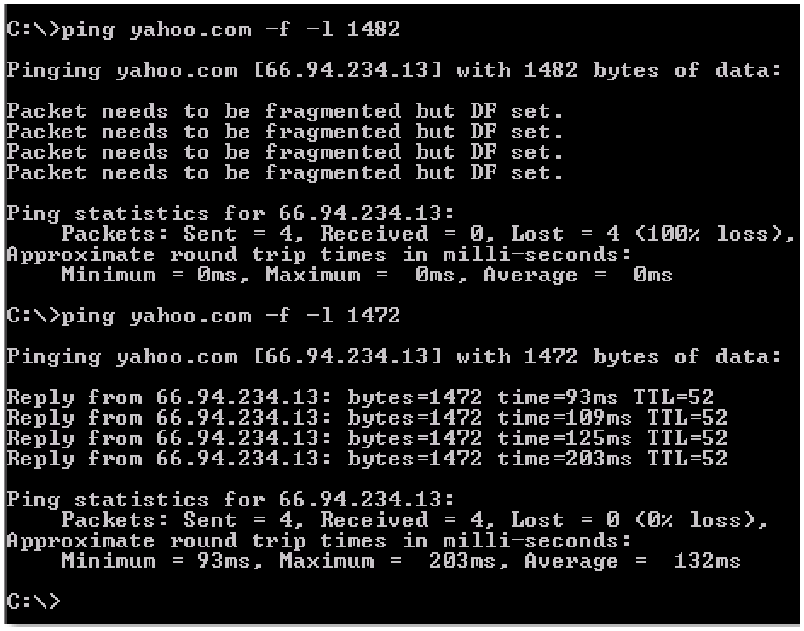
Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you’ll have to do a special ping of the destination you’re trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in command (Windows® NT, 2000, and XP users type in cmd) and press **Enter** (or click **OK**).
- Once the window opens, you’ll need to do a special ping. Use the following syntax:

  ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**



```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your access point with the proper MTU size.

To change the MTU rate on your access point follow the steps below:

- Open your browser, enter the IP address of your access point (192.168.0.50) and click **OK.**
- Enter your username (Admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure.**
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

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

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Access point is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office.

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your access point or Access Point

Make sure you place the bridge/access point in a centralized location within your network for the best performance. Try to place the bridge/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a Repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, wireless speakers, and televisions as far away as possible from the bridge/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don’t let your next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the access point. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure –** All wireless clients will connect to an access point or wireless bridge.
- **Ad-Hoc –** Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless bridge. All the wireless devices, or clients, will connect to the wireless bridge or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP address

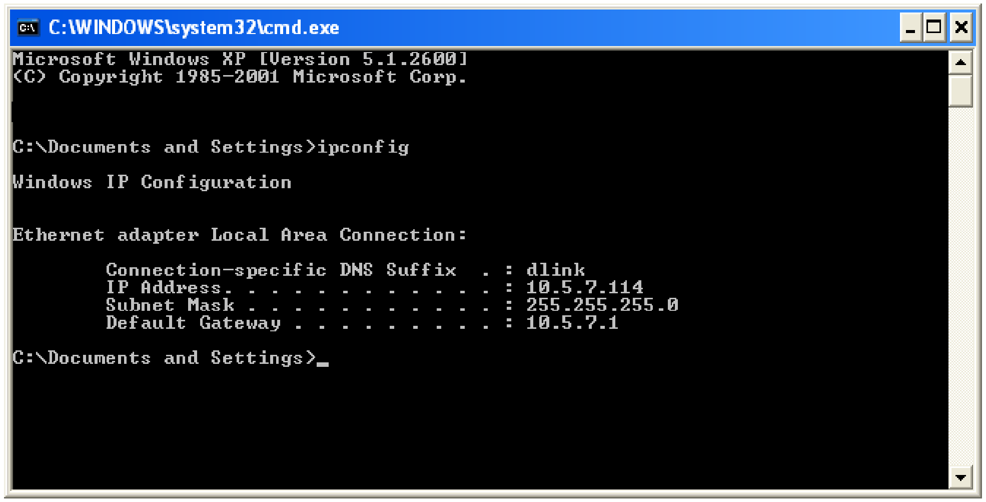
After you install your adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on Start > Run. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type cmd in the Start Search box.)

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.


C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : dlink
        IP Address. . . . . . . . . . . . : 10.5.7.114
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.5.7.1

C:\Documents and Settings>_
```

Statically Assign an IP address

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

Step 1

Windows® 7 - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change Adapter Setting.**

Windows Vista® - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections.**

Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2

Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

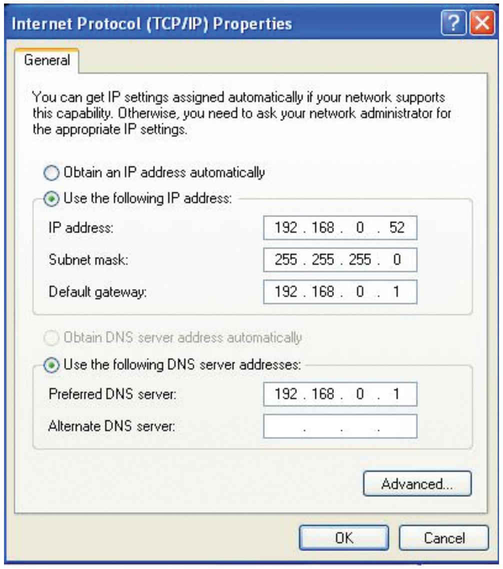
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 52

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

Step 5

Click **OK** twice to save your settings.

Technical Specifications

Standards

- IEEE 802.11a/n
- IEEE 802.3
- IEEE 802.3u

Network Management

- Web Browser Interface
- HTTP - Secure HTTP (HTTPS)
- SNMP v1, v2c, and v3

Security

- WPA-Personal & Enterprise
- WPA2-Personal & Enterprise
- WEP 64/128 bit Encryption
- 802.1X

Wireless Frequencyt

- 5.15 GHz - 5.825 GHz

Operational Modes

- Access Point
- Wireless Distribution System
- Wireless Distribution System with AP
- Wireless Client
- Repeater
- WISP Repeater
- WISP Client

Antenna

- Built-in 15 dBi Sector Antenna

Maximum Transmit Power Ouput[1]

- 29 dBm (800 mW)

Maximum Power Input

- 48 V/ 0.5 A

Maximum Power Consumption

- 15.9 watts

LEDs

- Wireless Signal Strength LED
- Power
- LAN
- Wireless

Operating Temperature

- Operating: -20 to 60 °C (-4 to 140 °F)
- Storage: -20 to 85 °C (-4 to 185 °F)

Humidity

- Operating: 0 to 90% (non-condensing)
- Storage: 5 to 95% (non-condensing)

Safety & Emissions

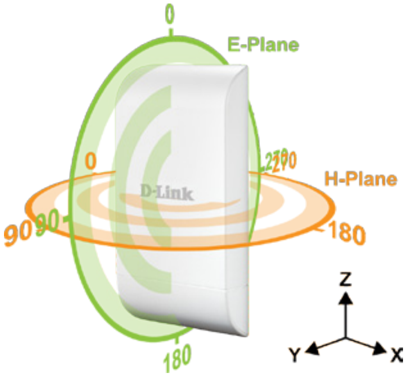
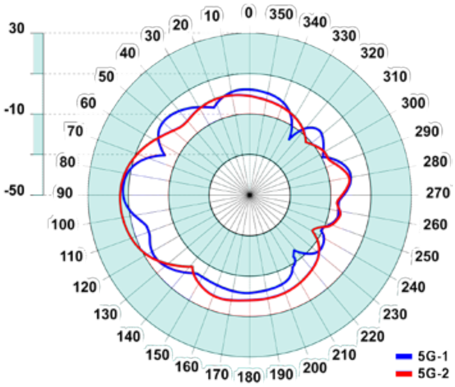
- FCC
- CE

Dimensions (L x W x H)

- 118 x 56 x 195 mm (4.64 x 2.2 x 7.67 inches)

[1] Range will vary depending on country's maximum transmit power output regulation. Maximum wireless signal rate derived from IEEE Standard 802.11g and 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.

Antenna Pattern

Antenna Patterns	
Orientation	*H-Plane*
5 GHz Wall Mounted 	

E-Plane
H-Plane
D-Link
Z
Y
X

30
-10
-50
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250
260
270
280
290
300
310
320
330
340
350
5G-1
5G-2