D-Link
Building Networks for People

DAP-2660

Version 1.00

*Air*Premier

Wireless AC1200 Concurrent Dual Band PoE Access Point

User Manual

Business Class Networking

Table of Contents

Product Overview

Introduction

D-Link, an industry pioneer in wireless networking, introduces a solution for businesses seeking to deploy next generation draft 802.11ac LANs. D-Link unveils its new DAP-2660, designed specifically for business-class environments such as large or enterprise corporations to provide secure and manageable dual band wireless LAN options for network administrators.

Versatile Access Point

The DAP-2660 Access Point allows network administrators to deploy a highly manageable and extremely robust dual band wireless network. All six antennas are detachable and can provide optimal wireless coverage in either 2.4GHz (802.11g and 802.11n) or 5GHz (802.11ac, 802.11a, and 802.11n) bands. Enclosed in a plenum-rated metal chassis, the DAP-2660 Access Point adheres to strict fire codes for placement in air passageways. For advanced installations, this new high-speed Access Point has integrated 802.3af Power over Ethernet (PoE) support, allowing installation of this device in areas where power outlets are not readily available.

Enhanced Performance

The DAP-2660 delivers reliable wireless performance with maximum wireless signal rates of up to 1750Mbps. This, coupled with support for Wi-Fi Multimedia™ (WMM) Quality of Service features, makes it an ideal access point for audio, video, and voice applications. Additionally, the DAP-2660 supports load balance features to ensure maximum performance.

Security

To help maintain a secure wireless network, the DAP-2660 provides the latest in wireless security technologies by supporting both Personal and Enterprise versions of WPA and WPA2 (802.11i) with support for RADIUS server back end. To further protect your wireless network, MAC Address Filtering, Wireless LAN segmentation, Disable SSID Broadcast, Rogue AP Detection, and Wireless Broadcast Scheduling are also included.

The DAP-2660 includes support for up to 16 VLANs for implementing multiple SSIDs to further help segment users on the network. The DAP-2660 also includes a wireless client isolation mechanism, which limits direct client-to-client communication.

* Maximum wireless signal rate derived from IEEE Standard 802.11ac (draft), 802.11g, 802.11a, 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

- Provide Ethernet to Wireless LAN bridge fully IEEE 802.3/u/ab compatible on the Ethernet side and fully interoperable with IEEE 802.11ac and b/g/n/a compliant equipment
- Compatible with IEEE 802.11b high rate standard to provide wireless 11Mbps data rate
- Compatible with IEEE 802.11g higher speed standard to provide wireless 54Mbps data rate
- Compatible with IEEE 802.11a higher speed standard to provide wireless 54Mbps data rate
- Compatible with IEEE 802.11n higher speed standard to provide wireless 450Mbps data rate
- Compatible with draft 802.11ac higher speed standard to provide wireless 1300Mbps data rate
- Operation at 2.4~2.5GHz and 5.15~5.85GHz frequency band to meet worldwide regulations
- Supports IEEE 802.11ac and b/g/n/a wireless data encryption with 64/128-bit WEP for security
- Allows auto fallback data rate for reliability, optimized throughput and transmission range
- Web-based configuration and management
- Supports enhanced security – WPA-PSK and WPA2-PSK, RADIUS client, and Cipher negotiation
- Supports one 802.3af PoE port
- Supports two 10/100/1000M Ethernet ports
- AP Mode, WDS Mode, WDS with AP, and Wireless Client Mode
- Supports SNMP v1,v2,v3
- Support Trap server (SNMP v1, v2c)
- Support AP Manager II and D-View 6.0
- Support AP Array and AP Array Setup Tool
- Support Port Redundancy
- Support one RJ-45 console port for debug

* Maximum wireless signal rate derived from IEEE Standard 802.11ac (draft), 802.11g, 802.11a, 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.

**Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-2660 isn't supported in the 5.25~5.35GHz and 5.47 ~ 5.725GHz frequency ranges in some regions.

Package Contents

- DAP-2660 Access Point
- Six Detachable Antennas
- Power Adapter
- PoE Base Unit
- Mounting Plate and Hardware
- Ethernet Cable
- Console Cable
- CD (with software and user manual)

Note: *Using a power supply with a different voltage rating than the one included with the DAP-2660 will cause damage and void the warranty for this product.*

System Requirements

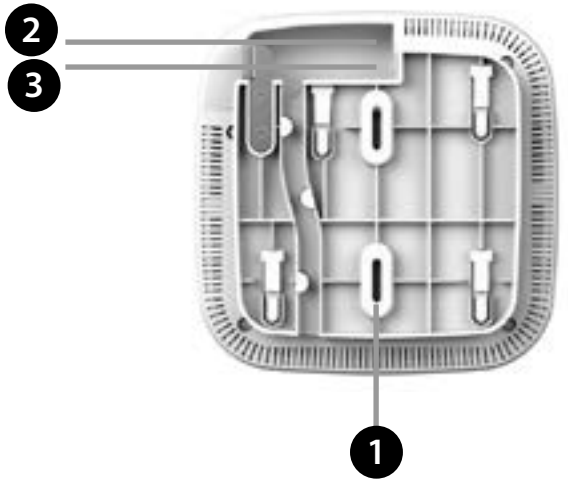
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer Version 7.0 or Firefox 3.0 and Above (for configuration)

Hardware Overview

LEDs

1	Power	The light blinks in red during boot up or malfunction, and lights in solid red when the bootup is failed. The LED lights in solid green when it is ready, and blinks in green when the traffice is passing through.

Connections



1	Reset Button	Press and hold for six seconds to reset the access point to the factory default settings.
2	LAN (PoE) Port	Connect to your network with an Ethernet cable.
3	Power Receptor	Connect the supplied power adapter.

Basic Installation

Hardware Setup

To power the access point, you can use one of the following 3 methods:

Method 1 - Use if you have a PoE switch or router.

Method 2 - Use if you do not have a PoE switch or router and do not have a power outlet near the location of the access point.

Method 3 - Use if you do not have a PoE switch or router and have a power outlet near the location of the access point.

Method 1 - PoE with PoE Switch or Router

1. Connect one end of your Ethernet cable to the LAN1 (PoE) port on the access point.

2. Connect the other end into one port on a PoE switch or router.

Method 2 - PoE without PoE Switch or Router

1. Connect one end of an Ethernet cable into the **Data In** port on the PoE base unit and the other end into one port on your switch, router, or computer.

2. Connect one end of an Ethernet cable into the **P+Data Out** port on the PoE base unit and the other end into the **LAN1 (PoE)** port on the Access Point.

3. Use the supplied power adapter. Connect the power adapter to the **Power In** receptor on the PoE adapter.

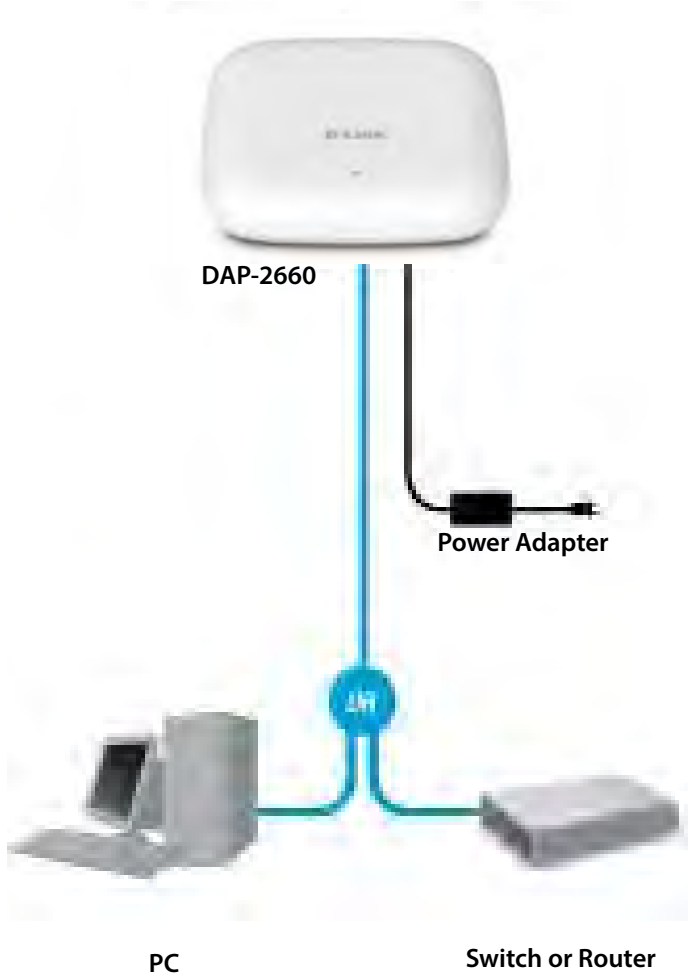
4. Connect the power cable to the power adapter and then connect the other end into a power outlet.

Method 3 - No PoE

1. Connect one end of your Ethernet cable into the **LAN1 (PoE)** or **LAN2** port and then connect the other end to a switch, router, or computer.

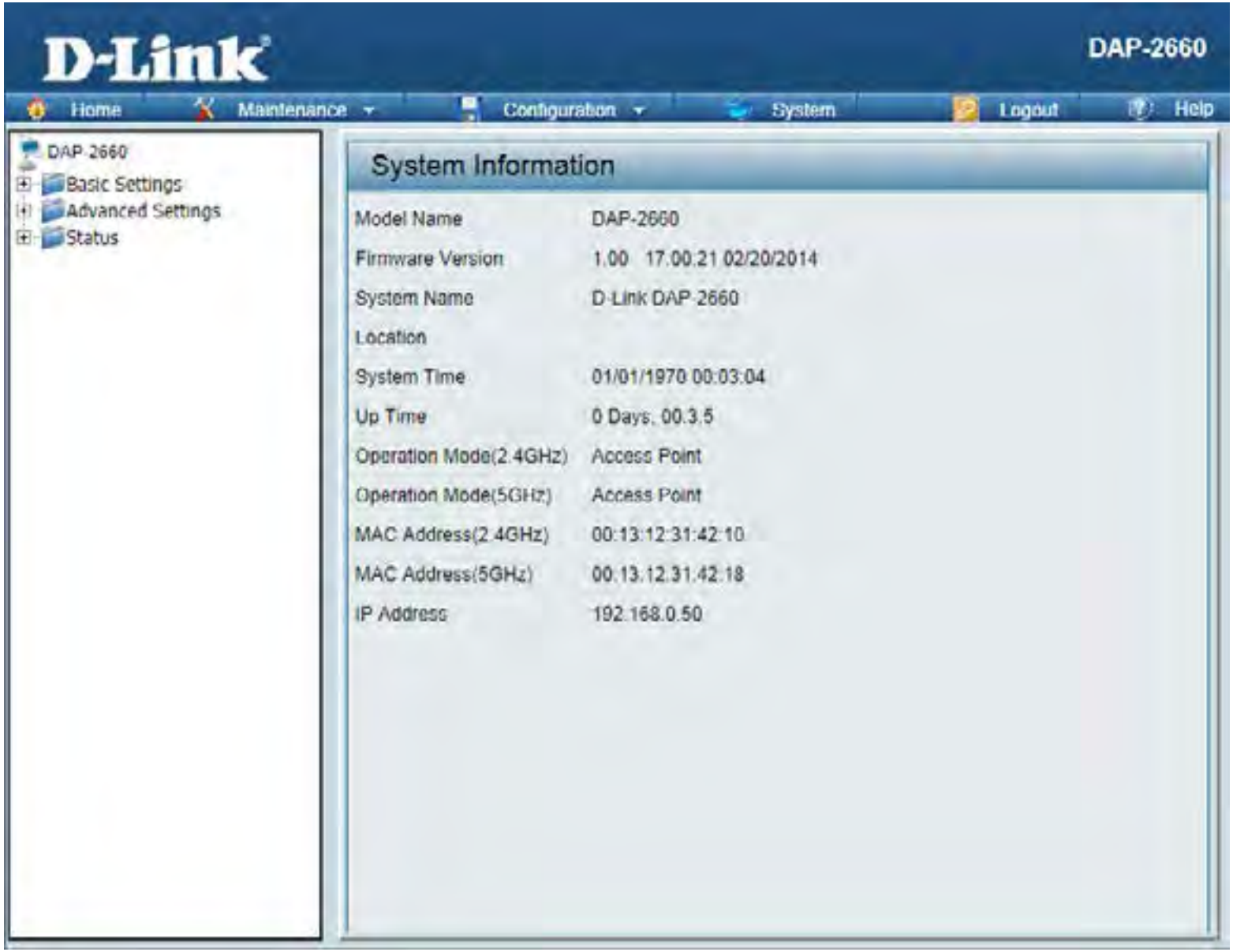
2. Use the supplied power adapter. Connect the power adapter to the Power receptor on the Access Point.

3. Connect the power cable to the power adapter and then connect the other end into a power outlet.



Web User Interface

The DAP-2660 supports an elaborate web user interface where the user can configure and monitor the device. Most of the configurable settings are located in the left menu of the web GUI which contains section called **Basic Settings**, **Advanced Settings** and **Status**.

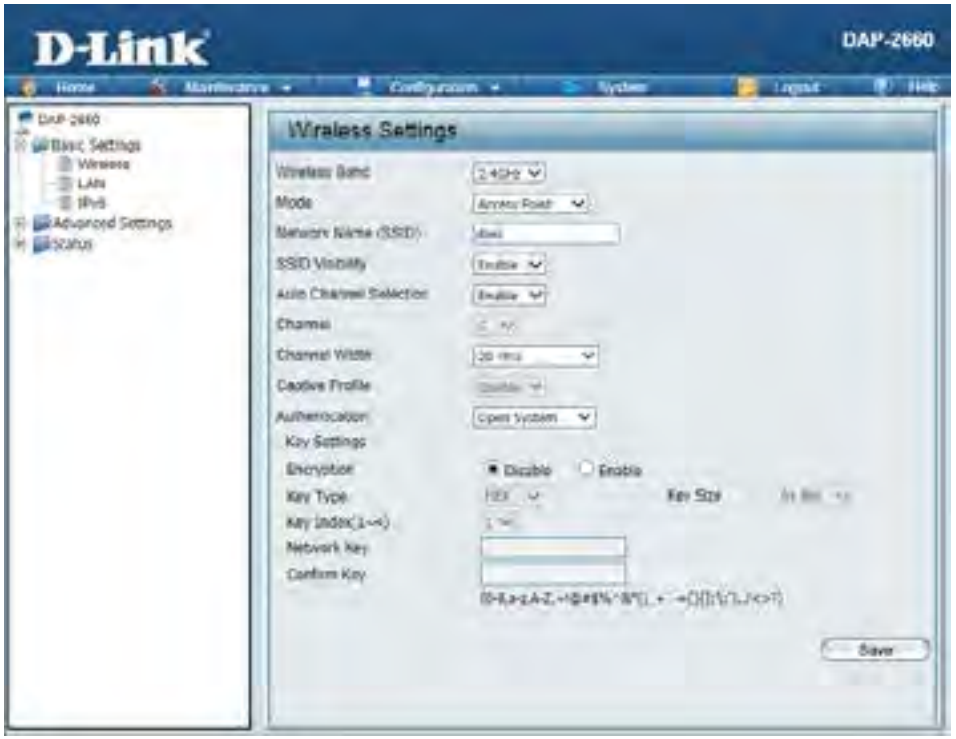


Basic Settings

Wireless

On the wireless settings page, you can setup the basic wireless configuration for the access point. The user can choose from 4 different wireless modes:
Access Point - Used to create a wireless LAN
WDS with AP - Used to connect multiple wireless networks while still functioning as a wireless access point
WDS - Used to connect multiple wireless networks
Wireless Client - Used when the access point needs to act as a wireless network adapter for an Ethernet enabled device

Access Point Mode (2.4GHz) - Open System



Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **2.4GHz** wireless band.

Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **Access Point** wireless mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

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

Auto Channel Selection: Select to **Enable** or **Disable** the auto-channel selection feature here. When enabled, the access point automatically selects the channel that provides the best wireless performance. The channel selection process only occurs when the AP is booting up. To manually select a channel, set this option to **Disable** and select a channel from the drop-down menu.

Channel: To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.

Note: *The wireless adapters will automatically scan and match the wireless settings.*

Channel Width: Select the wireless channel width option here. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

Captive Profile: Select to **Enable** or **Disable** the captive profile feature here.

Wireless security is a key concern for any wireless network installed. Unlike any other networking method wireless networks will broadcast it's presence for anyone to connect to it. Today, wireless security has advanced to a level where it is virtually impenetrable.
There are mainly two forms of wireless encryption and they are called Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first security method developed. It is a low level encryption but better than now encryption. WPA is the newest encryption standard and with the advanced WPA2 standard wireless networks have finally reach a point where the security is strong enough to give users the peace of mind when installing wireless networks.

WEP provides two variations called **Open System** and **Shared Key**.

Open System will send a request to the access point and if the key used matches the one configured on the access point, the access point will return a success message back to the wireless client. If the key does not match the one configured on the access point, the access point will deny the connection request from the wireless client.

Authentication: Select the wireless authentication method to use here. Options to choose from are **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, and **802.1X**. After selecting the **Open System** option, the following parameters will be available for configuration. Open System to communicate the key across the network (WEP).

Encryption: Select to **Enable** or **Disable** wireless encryption here.

Key Type: When the encryption option is enabled, select the key type here. Options to choose from are **HEX** and **ASCII**.

Key Size: When the encryption option is enabled, select the key size here. Options to choose from are **64 Bits** and **128 Bits**.

Key Index (1~4): Select the key index value used here. The keys 1 to 4 can be selected.

Network Key: Enter the wireless WEP key in the space provided here. When HEX was selected as the key type, the network key must consist out of the numbers 0 to 9 and the letters A to F. When ASCII was selected as the key type, the network key can consist out of any ASCII characters.

Confirm Key: Re-enter the wireless WEP key in the space provided. This key must be identical to the network key entered previously.

Access Point Mode (2.4GHz) - Shared Key

Shared Key will send a request to the access point and if the key used matches the one configured on the access point, the access point will send a challenge to the client. The client will then again send a confirmation of the same key back to the access point where the access point will either return a successful or a denial packet back to the wireless client.

Authentication: Select the wireless authentication method to use here. Options to choose from are **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, and **802.1X**. After selecting the **Shared Key** option, the following parameters will be available for configuration. Shared Key will limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.

Encryption: Select to **Enable** or **Disable** wireless encryption here.

Key Type: When the encryption option is enabled, select the key type here. Options to choose from are **HEX** and **ASCII**.

Key Size: When the encryption option is enabled, select the key size here. Options to choose from are **64 Bits** and **128 Bits**.

Key Index (1~4): Select the key index value used here. The keys 1 to 4 can be selected.

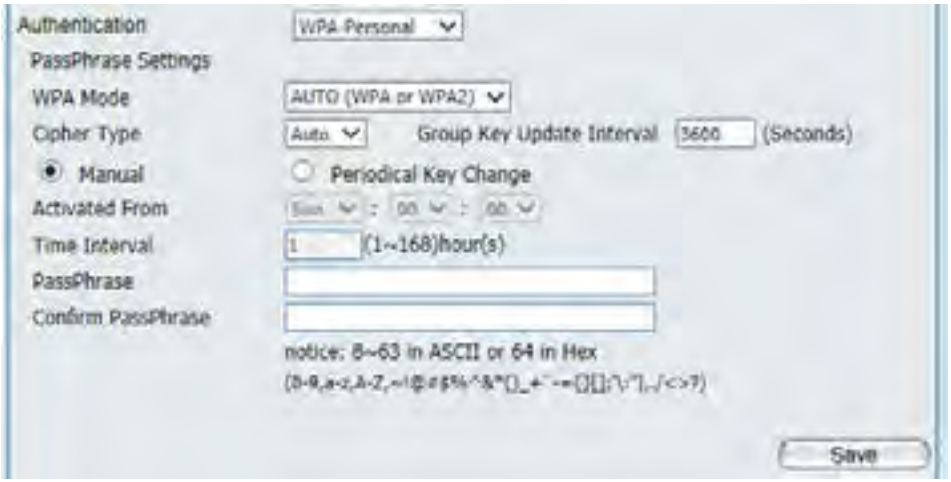
Network Key: Enter the wireless WEP key in the space provided here. When HEX was selected as the key type, the network key must consist out of the numbers 0 to 9 and the letters A to F. When ASCII was selected as the key type, the network key can consist out of any ASCII characters.

Confirm Key: Re-enter the wireless WEP key in the space provided. This key must be identical to the network key entered previously.

Access Point Mode (2.4GHz) - WPA Personal

WPA-Personal (PSK) does not require the user to install a RADIUS server on the network. Wi-Fi Protected Access (WPA) was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

Authentication: Select the wireless authentication method to use here. Options to choose from are **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, and **802.1X**. After selecting the **WPA-Personal** option, the following parameters will be available for configuration. WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.



WPA Mode: Select the WPA mode here. Options to choose from are **AUTO (WPA or WPA2)**, **WPA2 Only**, and **WPA Only**. WPA and WPA2 use different algorithms. AUTO (WPA or WPA2) allows you to use both WPA and WPA2.

Cipher Type: Select the WPA cipher type here. Options to choose from are **AUTO**, **AES**, and **TKIP**..

Group Key Update Interval: Enter the interval during which the group key will be valid. By default, this value is 3600 seconds.

Manual: Information Needed.

Periodical Key Change: Information Needed.

Activated From: Information Needed.

Time Interval: Information Needed.

PassPhrase: Enter the WPA passphrase that will be used here. This passphrase can be in the ASCII or HEX form.

Confirm PassPhrase: Re-enter the WPA passphrase that will be used here. This must be identical to the passphrase enter above.

Access Point Mode (2.4GHz) - WPA Enterprise

WPA-Enterprise (EAP) requires the user to install a RADIUS server on the network for authentication. Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today. WPA2 is an upgrade of WPA. WPA2 yet again solves some possible security issues found in WPA. WPA2 has two variations called WPA2-Personal (PSK) and WPA2-Enterprise (EAP) which is the same as found with WPA.

Authentication: Select the wireless authentication method to use here. Options to choose from are **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, and **802.1X**. After selecting the **WPA-Enterprise** option, the following parameters will be available for configuration.

WPA Mode: Select the WPA mode here. Options to choose from are **AUTO (WPA or WPA2)**, **WPA2 Only**, and **WPA Only**. WPA and WPA2 use different algorithms. AUTO (WPA or WPA2) allows you to use both WPA and WPA2.

Cipher Type: Select the WPA cipher type here. Options to choose from are **AUTO**, **AES**, and **TKIP**..

Group Key Update Interval: Enter the interval during which the group key will be valid. By default, this value is 3600 seconds.

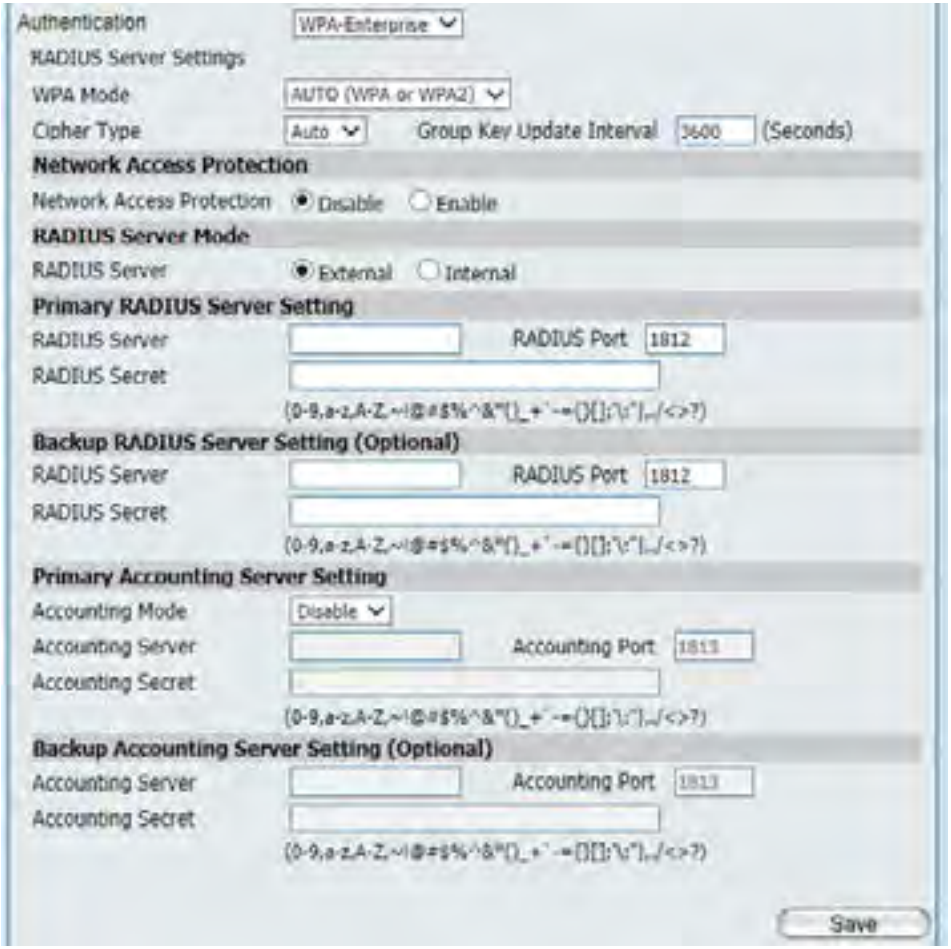
Network Access Protection: Select to **Enable** or **Disable** the network access protection feature here.

RADIUS Server Mode: Select the RADIUS server mode here. Options to choose from are **External** and **Internal**.

Primary RADIUS Server: Enter the primary RADIUS server's IP address or domain name here.

Primary RADIUS Port: Enter the primary RADIUS server's port number here.

Primary RADIUS Secret: Enter the primary RADIUS server's secrect passphrase here. This secrect is in the ASCII form.

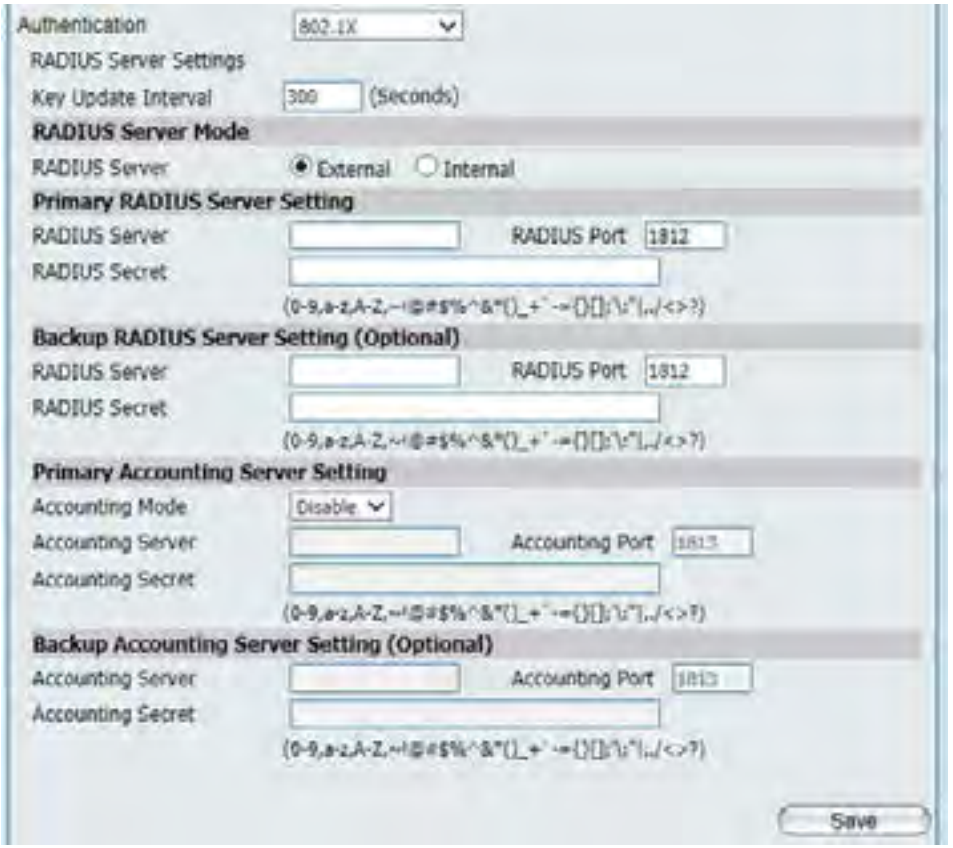


Backup RADIUS Server:	Enter the backup RADIUS server's IP address or domain name here.
Backup RADIUS Port:	Enter the backup RADIUS server's port number here.
Backup RADIUS Secret:	Enter the backup RADIUS server's secrect passphrase here. This secrect is in the ASCII form.
Accounting Mode:	Select to **Enable** or **Disable** the RADIUS accounting mode here.
Primary Accounting Server:	Enter the primary accounting server's IP address or domain name here.
Primary Accounting Port:	Enter the primary accounting server's port number here.
Primary Accounting Secret:	Enter the primary accounting server's secrect passphrase here. This secrect is in the ASCII form.
Backup Accounting Server:	Enter the backup accounting server's IP address or domain name here.
Backup Accounting Port:	Enter the backup accounting server's port number here.
Backup Accounting Secret:	Enter the backup accounting server's secrect passphrase here. This secrect is in the ASCII form.

Access Point Mode (2.4GHz) - 802.1X

802.1X Information
???

Authentication: Select the wireless authentication method to use here. Options to choose from are **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, and **802.1X**. After selecting the **802.1X** option, the following parameters will be available for configuration.



Key Update Interval: Enter the interval during which the key will be valid. By default, this value is 300 seconds.

RADIUS Server: Select the RADIUS server mode here. Options to choose from are **External** and **Internal**.

Primary RADIUS Server: Enter the primary RADIUS server's IP address or domain name here.

Primary RADIUS Port: Enter the primary RADIUS server's port number here.

Primary RADIUS Secret: Enter the primary RADIUS server's secrect passphrase here. This secrect is in the ASCII form.

Backup RADIUS Server: Enter the backup RADIUS server's IP address or domain name here.

Backup RADIUS Port: Enter the backup RADIUS server's port number here.

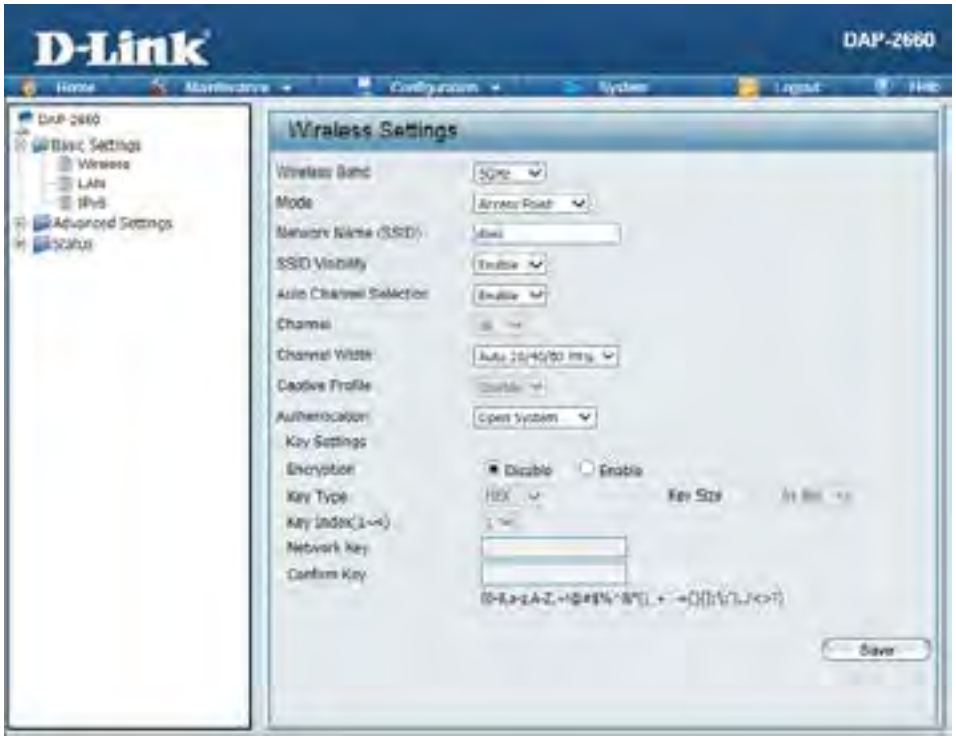
Backup RADIUS Secret: Enter the backup RADIUS server's secrect passphrase here. This secrect is in the ASCII form.

Accounting Mode: Select to **Enable** or **Disable** the RADIUS accounting mode here.

Primary Accounting Server: Enter the primary accounting server's IP address or domain name here.

Primary Accounting Port:	Enter the primary accounting server's port number here.
Primary Accounting Secret:	Enter the primary accounting server's secrect passphrase here. This secrect is in the ASCII form.
Backup Accounting Server:	Enter the backup accounting server's IP address or domain name here.
Backup Accounting Port:	Enter the backup accounting server's port number here.
Backup Accounting Secret:	Enter the backup accounting server's secrect passphrase here. This secrect is in the ASCII form.

Access Point Mode (5GHz)



Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **Access Point** wireless mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

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

Auto Channel Selection: Select to **Enable** or **Disable** the auto-channel selection feature here. When enabled, the access point automatically selects the channel that provides the best wireless performance. The channel selection process only occurs when the AP is booting up. To manually select a channel, set this option to **Disable** and select a channel from the drop-down menu.

Channel: To change the channel, first toggle the *Auto Channel Selection* setting to **Disable**, and then use the drop-down menu to make the desired selection.

Note: *The wireless adapters will automatically scan and match the wireless settings.*

Channel Width: Select the wireless channel width option here. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** and **Auto 20/40/80 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

Captive Profile: Select to **Enable** or **Disable** the captive profile feature here.

Authentication: Select the wireless authentication method to use here. In the **Access Point** mode, the following authentication methods are supported: **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise** and **802.1X**.

For more information about the wireless security, refer to page 14.

WDS with AP Mode (2.4GHz)

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **2.4GHz** wireless band.

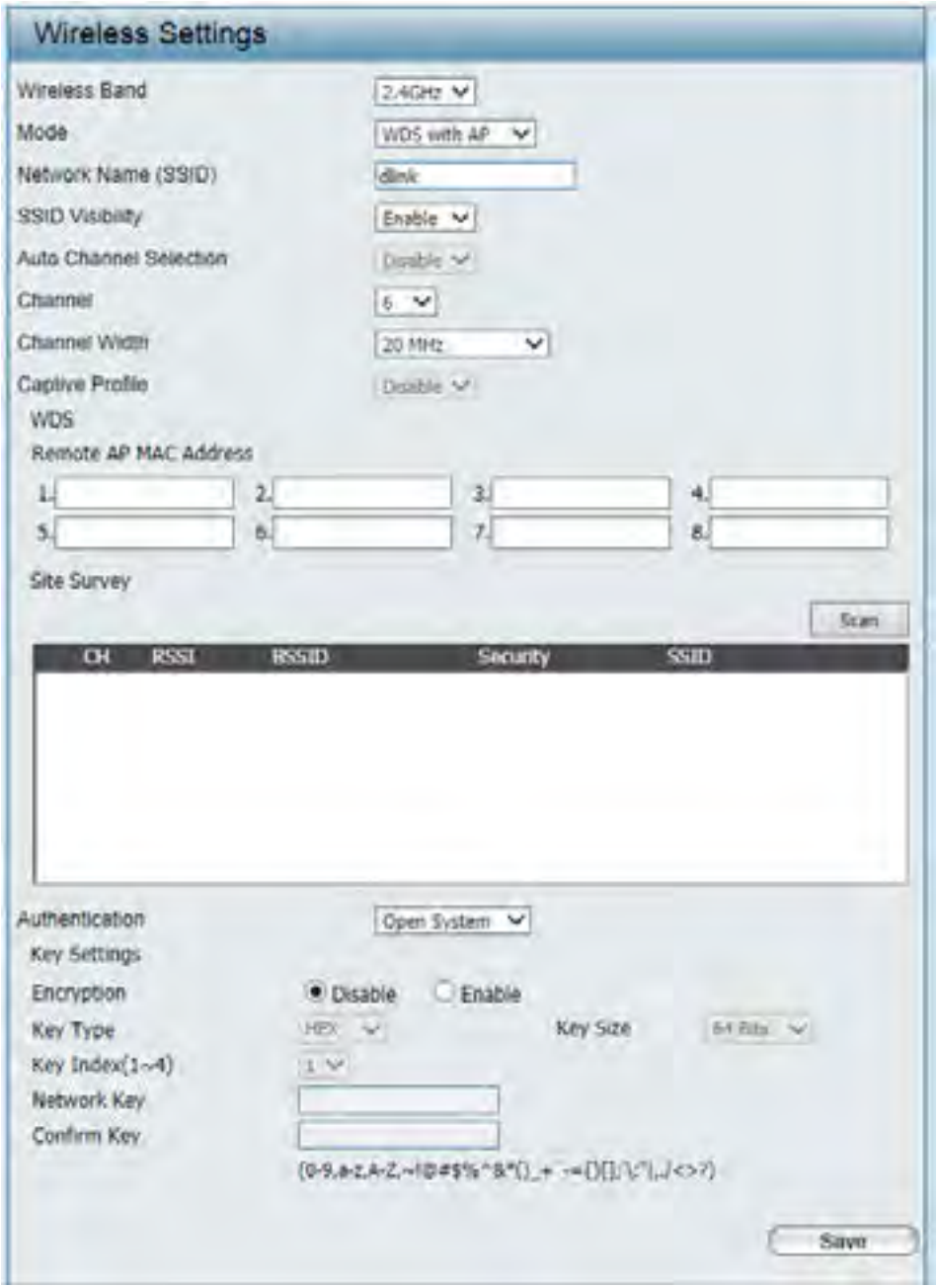
Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **WDS with AP** wireless mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

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

Auto Channel Selection: This feature can only be used in the Access Point mode.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)



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

Captive Profile: Select the enable or disable the captive portal feature here.

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

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

Authentication: Select the wireless authentication method to use here. In the **WDS with AP** mode, the following authentication methods are supported: **Open System** and **WPA-Personal**.

For more information about the wireless security, refer to page 14.

WDS with AP Mode (5GHz)

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

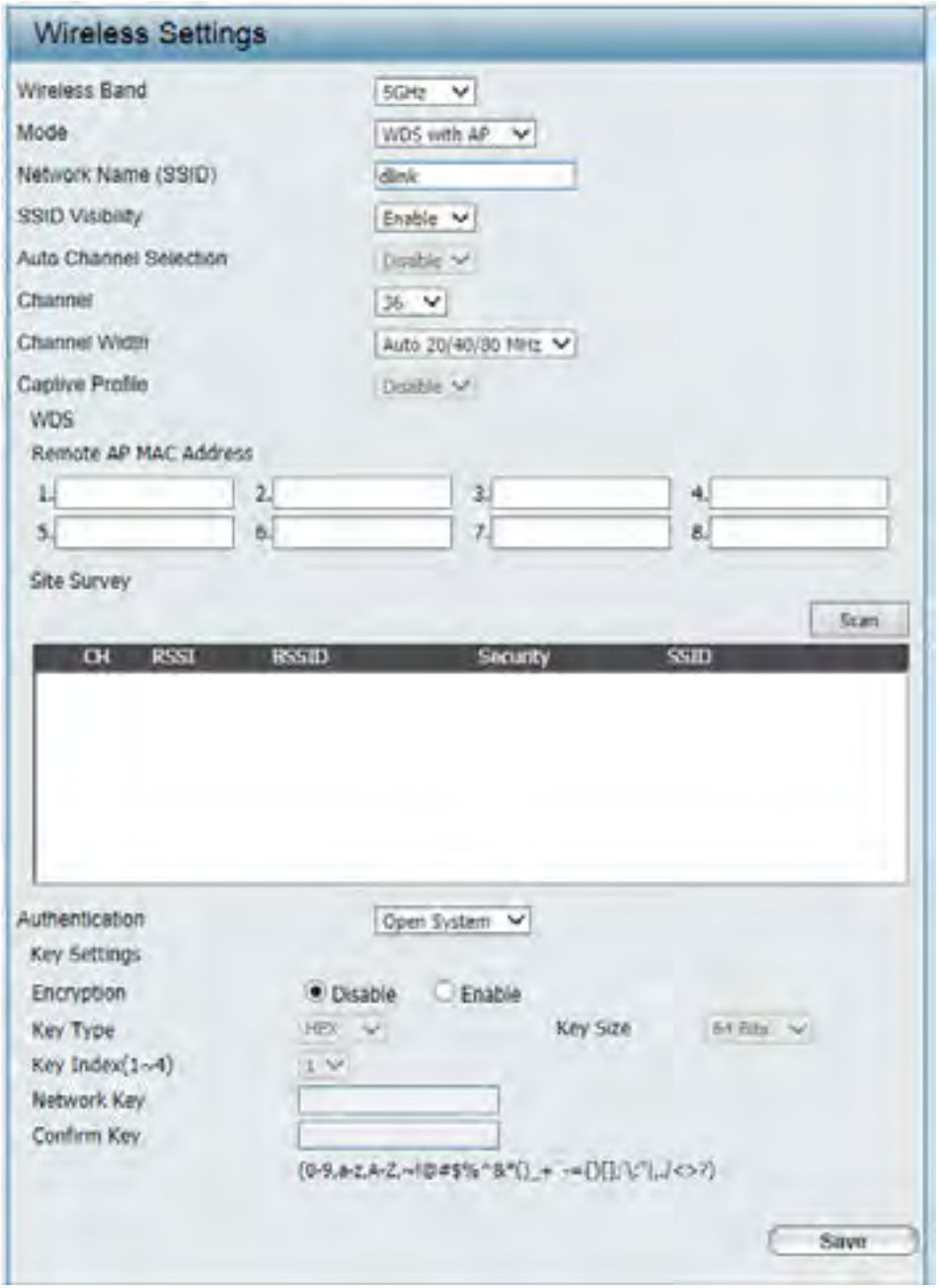
Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **WDS with AP** wireless mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

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

Auto Channel Selection: This feature can only be used in the Access Point mode.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)



Channel Width: Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** and **Auto 20/40/80 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

Captive Profile: Select the enable or disable the captive portal feature here.

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

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

Authentication: Select the wireless authentication method to use here. In the **WDS with AP** mode, the following authentication methods are supported: **Open System** and **WPA-Personal**.

For more information about the wireless security, refer to page 14.

WDS Mode (2.4GHz)

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **2.4GHz** wireless band.

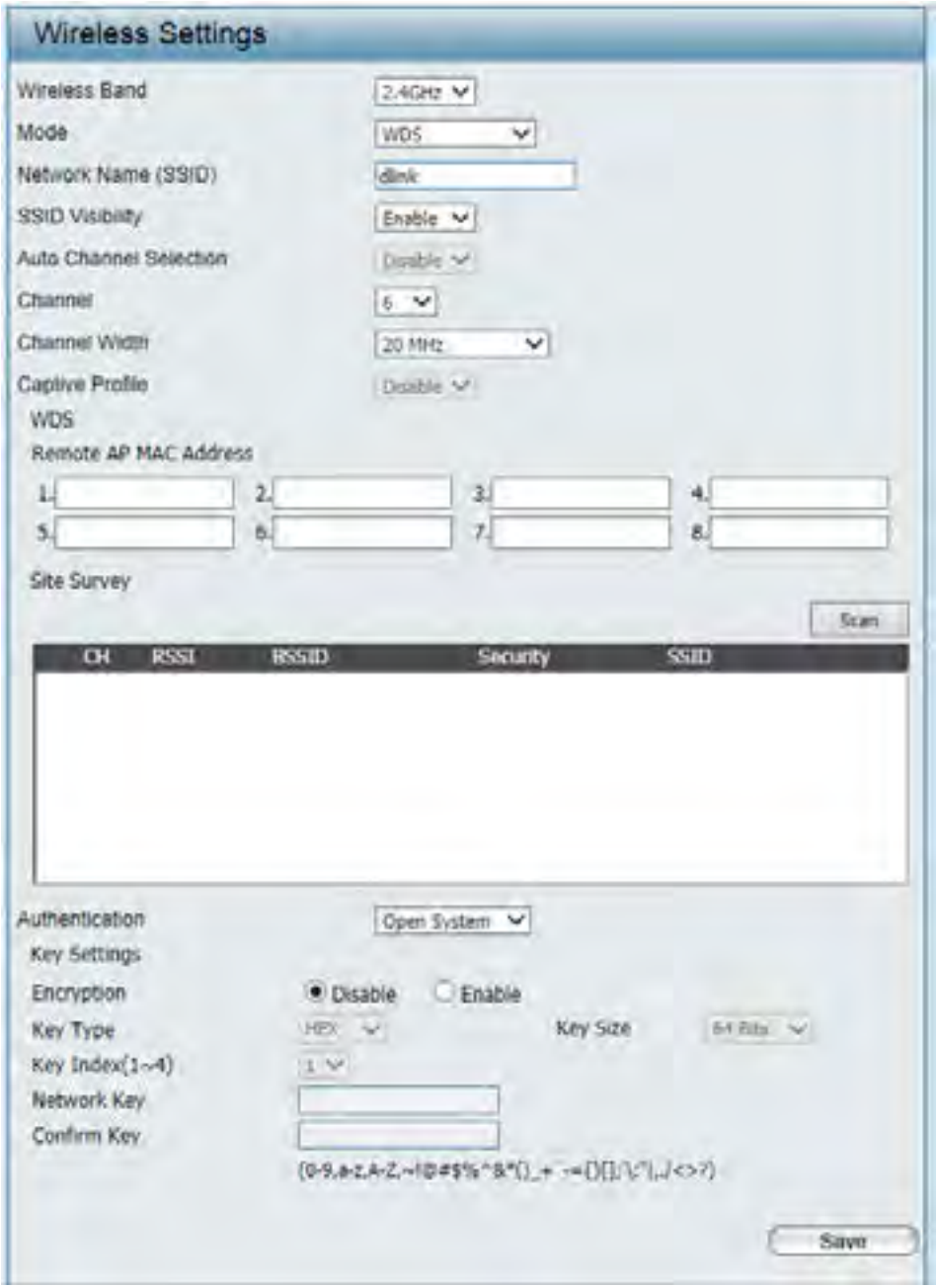
Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **WDS** wireless mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

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

Auto Channel Selection: This feature can only be used in the Access Point mode.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)



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

Captive Profile: Select the enable or disable the captive portal feature here.

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

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

Authentication: Select the wireless authentication method to use here. In the **WDS** mode, the following authentication methods are supported: **Open System** and **WPA-Personal**.

For more information about the wireless security, refer to page 14.

WDS Mode (5GHz)

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

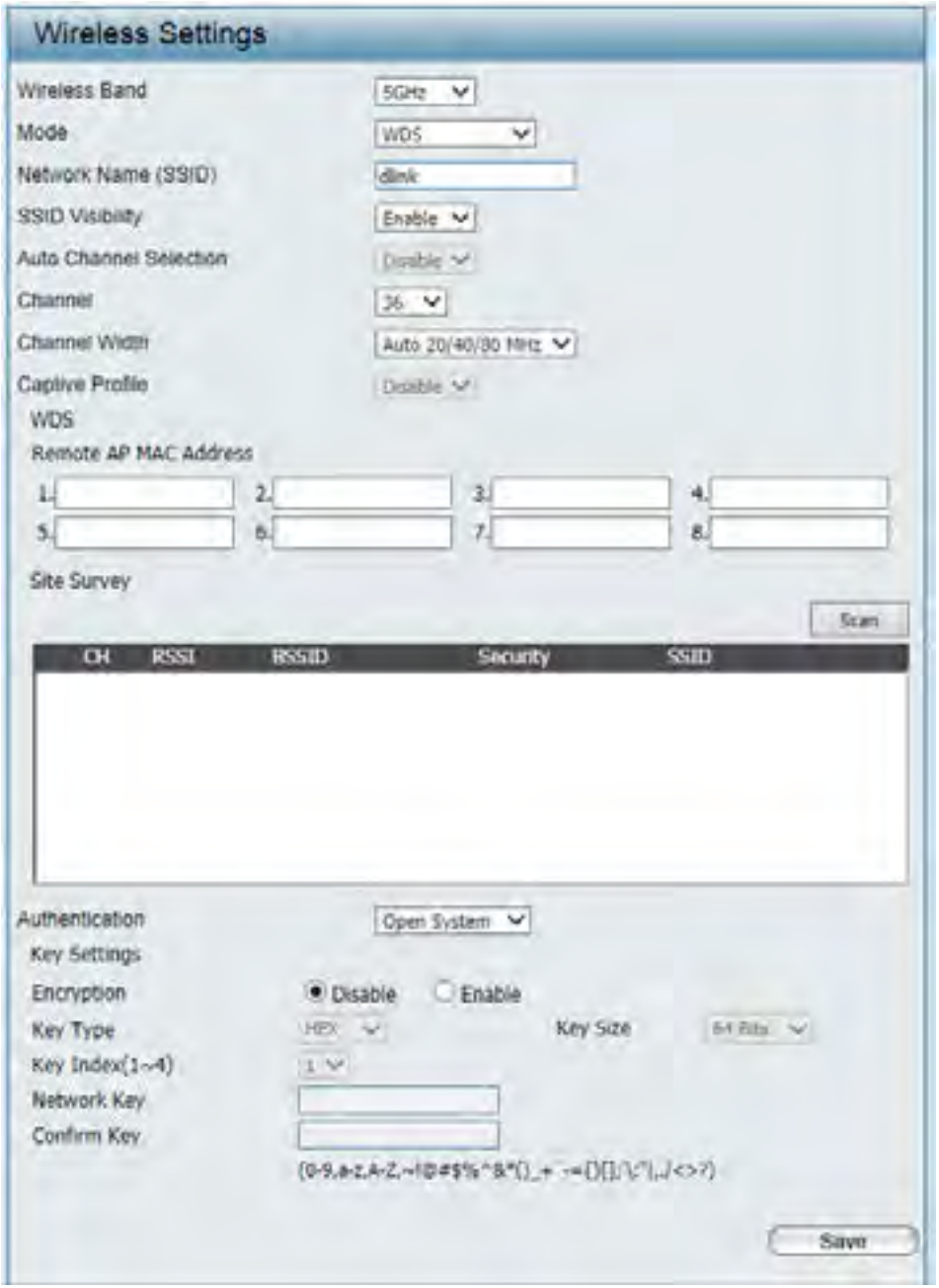
Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **WDS with AP** wireless mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

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

Auto Channel Selection: This feature can only be used in the Access Point mode.

Channel: All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection. (Note: The wireless adapters will automatically scan and match the wireless settings.)



Channel Width: Allows you to select the channel width you would like to operate in. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** and **Auto 20/40/80 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

Captive Profile: Select the enable or disable the captive portal feature here.

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

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

Authentication: Select the wireless authentication method to use here. In the **WDS** mode, the following authentication methods are supported: **Open System** and **WPA-Personal**.

For more information about the wireless security, refer to page 14.

Wireless Client Mode (2.4GHz)

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **2.4GHz** wireless band.

Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **Wireless Client** mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

SSID Visibility: This option is not configurable in the Wireless Client mode.

Auto Channel Selection: This option is not configurable in the Wireless Client mode.

Channel: This option is not configurable in the Wireless Client mode.

Channel Width: This option is not configurable in the Wireless Client mode.

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

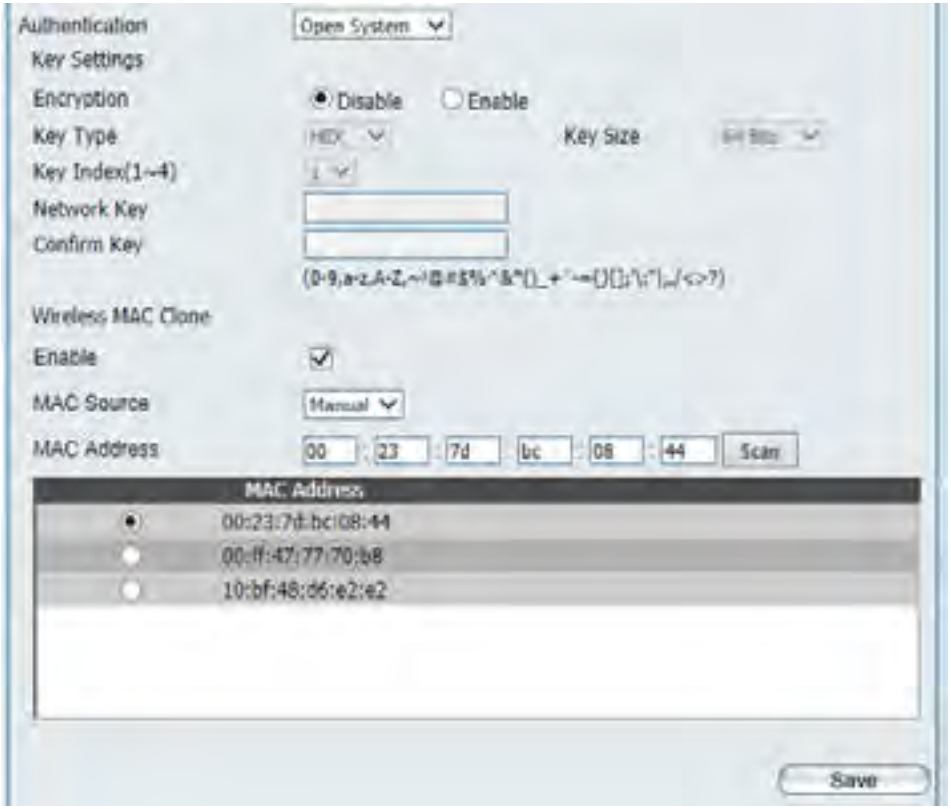
Authentication: Select the wireless authentication method to use here. In the **Wireless Client** mode, the following authentication methods are supported: **Open System** and **WPA-Personal**.

For more information about the wireless security, refer to page 14.

Wireless MAC Clone: Select the **Enable** checkbox to enable the wireless MAC clone option.

MAC Source: After enabling the **Wireless MAC Clone** option, the MAC source can be selected. Options to choose from are **Auto** and **Manual**.

MAC Address: After the **Manual** option was selected as the **MAC Source**, click the **Scan** button to scan for MAC addresses used by the PC connected to the Web UI. After the MAC addresses were found, they will be displayed in the table provided. Selecting one of the entries will automatically clone the MAC address into the MAC Address field. Alternatively, the MAC address can be entered manually in the spaces provided.



Wireless Client Mode (5GHz)

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

Mode: Select wireless mode used here. Options to choose from are **Access Point**, **WDS with AP**, **WDS**, and **Wireless Client**. In this section we'll explain the **Wireless Client** mode.

Network Name (SSID): Enter the Service Set IDentifier (SSID) used here. This name is designated for a specific Wireless Local Area Network (WLAN). By default, the SSID is **dlink**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. The SSID can be up to 32 characters and is case-sensitive.

SSID Visibility: This option is not configurable in the Wireless Client mode.

Auto Channel Selection: This option is not configurable in the Wireless Client mode.

Channel: This option is not configurable in the Wireless Client mode.

Channel Width: This option is not configurable in the Wireless Client mode.

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

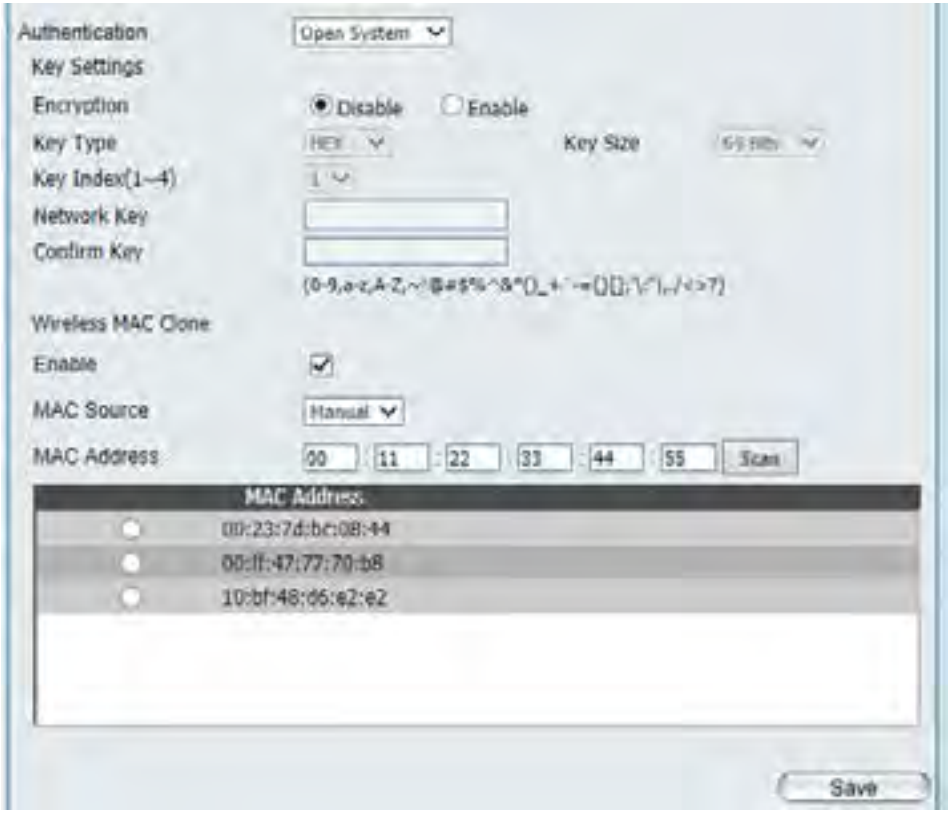
Authentication: Select the wireless authentication method to use here. In the **Wireless Client** mode, the following authentication methods are supported: **Open System** and **WPA-Personal**.

For more information about the wireless security, refer to page 14.

Wireless MAC Clone: Select the **Enable** checkbox to enable the wireless MAC clone option.

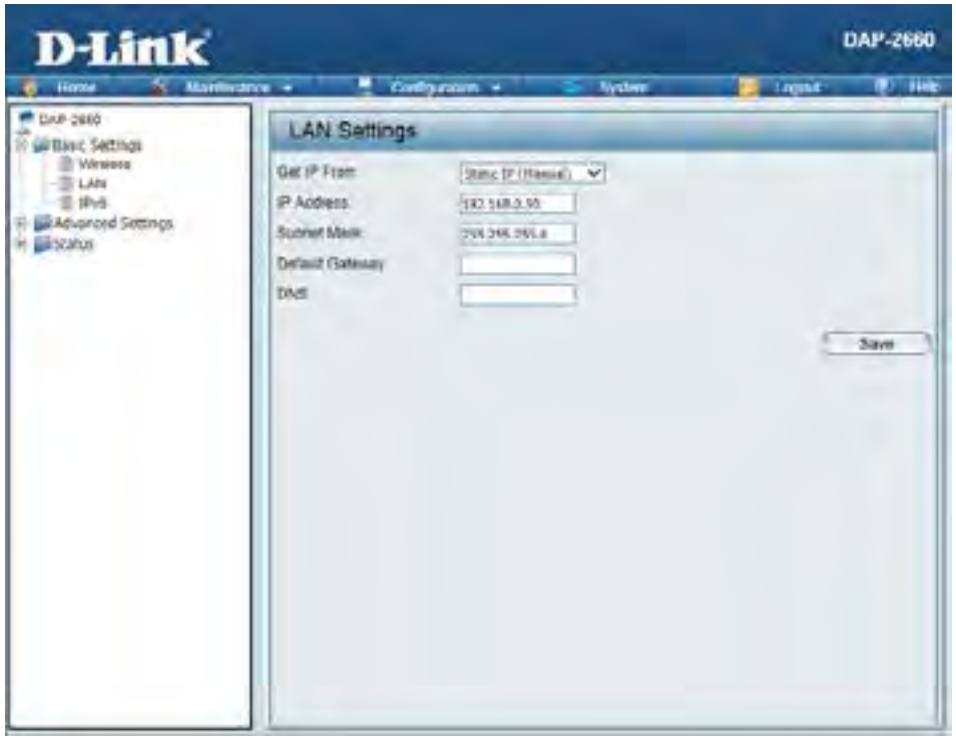
MAC Source: After enabling the **Wireless MAC Clone** option, the MAC source can be selected. Options to choose from are **Auto** and **Manual**.

MAC Address: After the **Manual** option was selected as the **MAC Source**, click the **Scan** button to scan for MAC addresses used by the PC connected to the Web UI. After the MAC addresses were found, they will be displayed in the table provided. Selecting one of the entries will automatically clone the MAC address into the MAC Address field. Alternatively, the MAC address can be entered manually in the spaces provided.



LAN

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DAP-2660. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.



Get IP From: **Static IP (Manual)** is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2660. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

Default Gateway: Enter the IP address of the gateway/router in your network.

DNS: Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

IPv6

This access point is IPv6 ready. An IPv6 address can be manually configured or automatically obtained from a DHCPv6 server. This IPv6 address is only applicable to the LAN side of the local network and is not visible from the Internet.

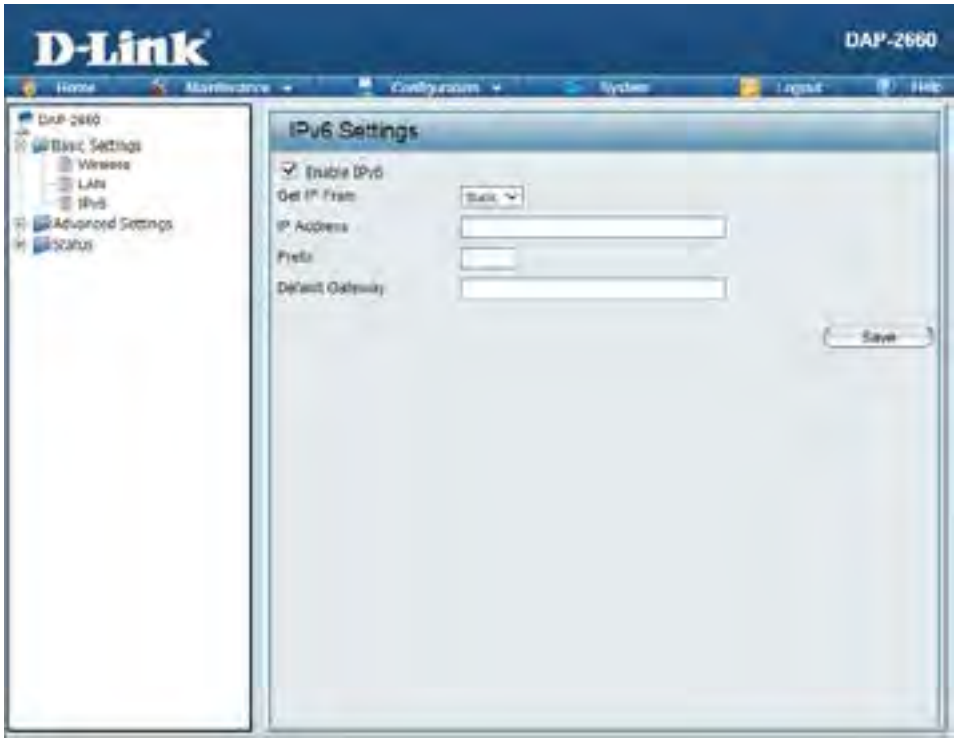
Enable IPv6: Select the checkbox to enable the IPv6 option of this access point.

Get IP From: Select the method that will be used by this access point to obtain an IPv6 address. Options to choose from are **Static** and **Auto**. Select the **Auto** option if this access point can obtain IPv6 settings from a DHCPv6 server on the local network. Select the **Static** option to manually enter the IPv6 settings in the spaces provided.

IP Address: Enter the IPv6 address for this access point here.

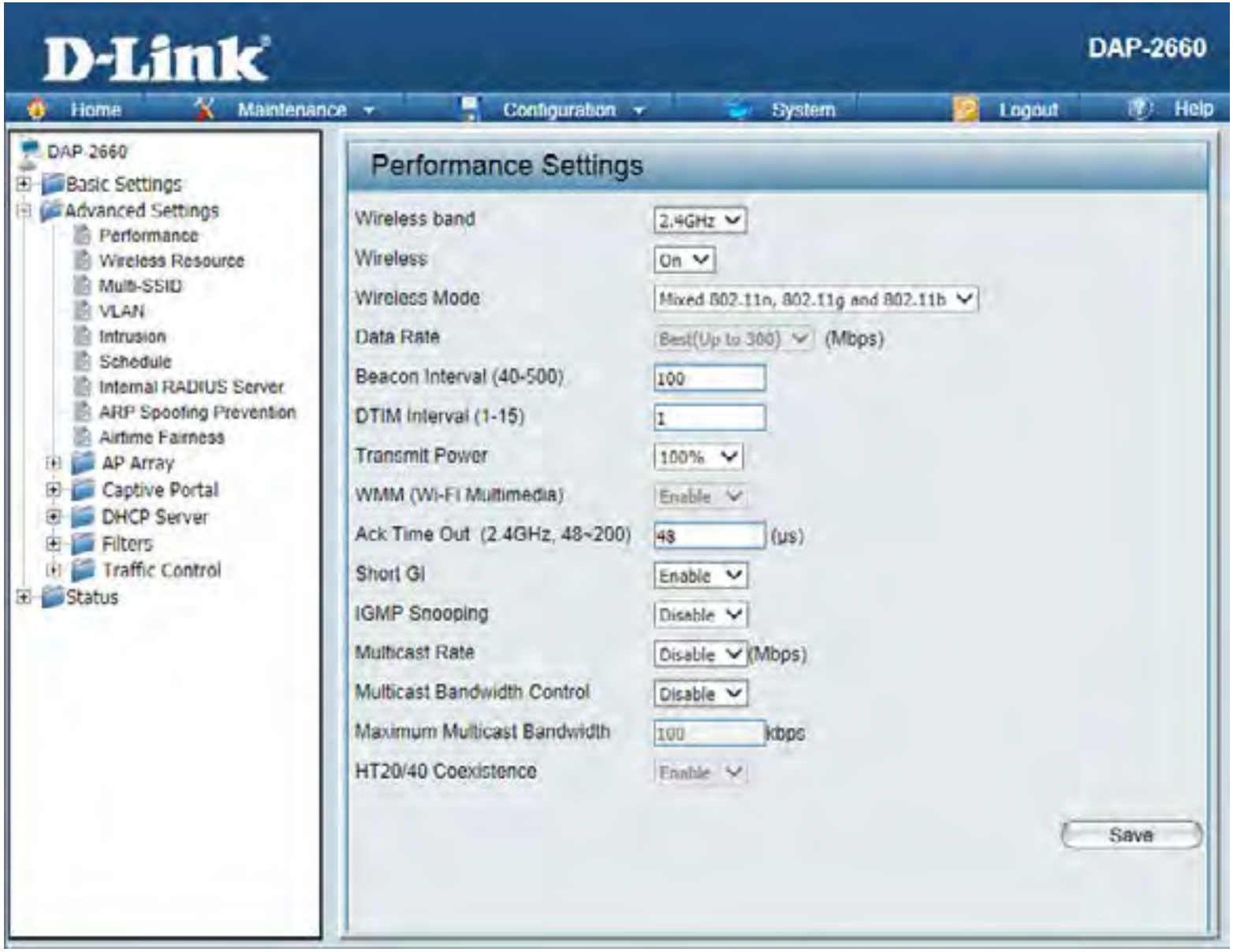
Prefix: Enter the IPv6 prefix value for this access point here.

Default Gateway: Enter the default gateway's IPv6 address here.



Advanced Settings

In the Advanced Settings Section the user can configure advanced settings concerning Performance, Wireless Resources, Multiple SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Airtime Fairness, AP Array, Captive Portal, DHCP Server, Filters and Traffic Control. The following pages will explain settings found in the Advanced Settings section in more detail.



Performance (2.4GHz)

On the Performance Settings page the users can configure more advanced settings concerning the wireless signal and hosting.

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **2.4GHz** wireless band.

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

Wireless Mode: Select the wireless mode here. Options to choose from are **Mixed 802.11n, 802.11g and 802.11b**, **Mixed 802.11g and 802.11b** and **802.11n Only**.

Data Rate*: Only after selecting the **Mixed 802.11g and 802.11b** option as the wireless mode, can the data rate be selected. Select the data rate here. Options to choose from are **54**, **48**, **36**, **24**, **18**, **12**, **11**, **9**, **6**, **5.5**, **2** and **1** Mbps.

Beacon Interval (40-500): Beacons are packets sent by an access point to synchronize a wireless network. Specify a value in milliseconds. The default (100) is recommended. Setting a higher beacon interval can help to save the power of wireless clients, while setting a lower one can help a wireless client connect to an access point faster.

DTM Interval (1-15): Select a Delivery Traffic Indication Message (DTM) setting between 1 and 15. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

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%.

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

WMM (Wi-Fi Multimedia): WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network. This feature is enabled by default and can only be disabled when **Mixed 802.11g and 802.1b** was selected as the **Wireless Mode**.

Ack Time Out (2.4 GHZ, 48~200): To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 48 and 200 microseconds for 2.4 GHz in the field provided.

Short GI: Select **Enable** or **Disable**. Enabling a short Guard Interval (GI) 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. This option cannot be enabled when **Mixed 802.11g and 802.11b** was selected as the **Wireless Mode**.

IGMP Snooping: Select **Enable** or **Disable**. Internet Group Management Protocol (IGMP) 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.

Multicast Rate: Select the multicast packet data rate value here. Options to choose from are **54**, **48**, **36**, **24**, **18**, **12**, **11**, **9**, **6**, **5.5**, **2** and **1** Mbps. The multicast rate is supported in AP mode, (2.4 GHZ and 5 GHZ) and WDS with AP mode, including Multi-SSIDs. This option cannot be configured when **802.11n Only** was selected as the **Wireless Mode**.

Multicast Bandwidth Control : Select to **Enable** or **Disable** the multicast bandwidth control option here.

Maximum Multicast Bandwidth: After enabling the multicast bandwidth control option, enter the maximum multcast bandwidth value here. By default this value is 100 Kbps.

HT20/40 Coexistence : 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 over-lapping and causing interference, the Access Point will automatically change to 20MHz

Performance (5GHz)

On the Performance Settings page the users can configure more advanced settings concerning the wireless signal and hosting.

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

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

Wireless Mode: Select the wireless mode here. Options to choose from are **Mixed 802.11n, 802.11a**, **802.11a Only**, **802.11n Only** and **Mixed 802.11ac**.

Data Rate*: Only after selecting the **802.11a Only** option as the wireless mode, can the data rate be selected. Select the data rate here. Options to choose from are **54**, **48**, **36**, **24**, **18**, **12**, **9**, and **6** Mbps.

Beacon Interval (40-500): Beacons are packets sent by an access point to synchronize a wireless network. Specify a value in milliseconds. The default (100) is recommended. Setting a higher beacon interval can help to save the power of wireless clients, while setting a lower one can help a wireless client connect to an access point faster.

DTM Interval (1-15): Select a Delivery Traffic Indication Message (DTM) setting between 1 and 15. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

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%.

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

WMM (Wi-Fi Multimedia): WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network. This feature is enabled by default and can only be disabled when **802.11a Only** was selected as the **Wireless Mode**.

Ack Time Out (5GHz, 25~200): To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 25 and 200 microseconds for 5GHz in the field provided.

Short GI: Select **Enable** or **Disable**. Enabling a short Guard Interval (GI) 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. This option cannot be enabled when **802.11a Only** was selected as the **Wireless Mode**.

IGMP Snooping: Select **Enable** or **Disable**. Internet Group Management Protocol (IGMP) 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.

Multicast Rate: Select the multicast packet data rate value here. Options to choose from are **54**, **48**, **36**, **24**, **18**, **12**, **11**, **9**, **6**, **5.5**, **2** and **1** Mbps. The multicast rate is supported in AP mode, (2.4 GHZ and 5 GHZ) and WDS with AP mode, including Multi-SSIDs. This option cannot be configured when **802.11n Only** was selected as the **Wireless Mode**.

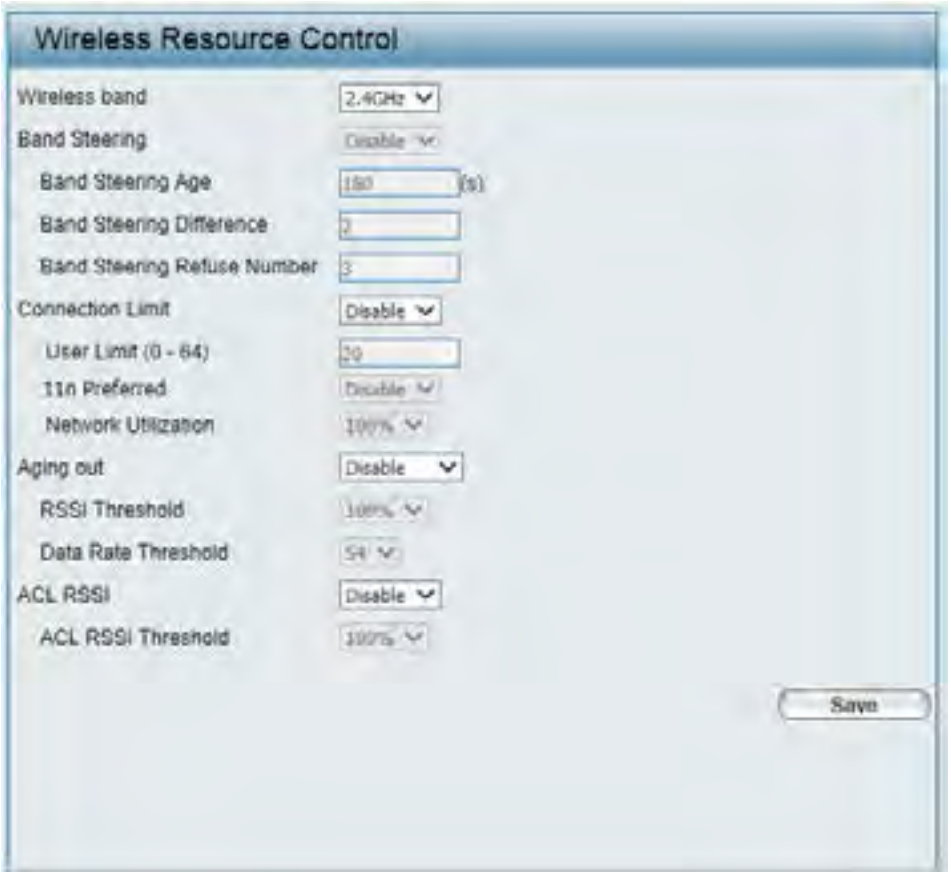
Multicast Bandwidth Control : Select to **Enable** or **Disable** the multicast bandwidth control option here.

Maximum Multicast Bandwidth: After enabling the multicast bandwidth control option, enter the maximum multcast bandwidth value here. By default this value is 100 Kbps.

HT20/40 Coexistence : 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 over-lapping and causing interference, the Access Point will automatically change to 20MHz

Wireless Resource (2.4GHz)

The Wireless Resource Control window is used to configure the wireless connection settings so that the device can detect the better wireless connection in your environment.



Wireless band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **2.4GHz** wireless band.

Band Steering: This parameter can only be configured in the 5GHz band section.

Band Steering Age: This parameter can only be configured in the 5GHz band section.

Band Steering Difference: This parameter can only be configured in the 5GHz band section.

Band Steering Refuse Number: This parameter can only be configured in the 5GHz band section.

Connection Limit: Select to **Enable** or **Disable** the connection limit feature here. 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 below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled and when the number of users exceeds this value, or the network utilization of this AP exceeds the percentage that has been specified, the DAP-2660 will not allow clients to associate with the AP.

User Limit (0-64): Enter the maximum amount of users that are allowed access (0 to 64 users) to the device using the specified wireless band. The default setting is 20.

11n Prefered: Use the drop-down menu to **Enable** or **Disable** the 11n Preferred function. The wireless clients with 802.11n protocol will have higher priority to connect to the device.

Network Utilization: Set the maximum utilization of this access point for service. The DAP-2660 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.

Aging Out: Use the drop-down menu to select the criteria of disconnecting the wireless clients. Available options are **RSSI** and **Data Rate**.

RSSI Threshold: When **RSSI** is selected in the **Aging Out** drop-down menu, select the percentage of RSSI here. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients.

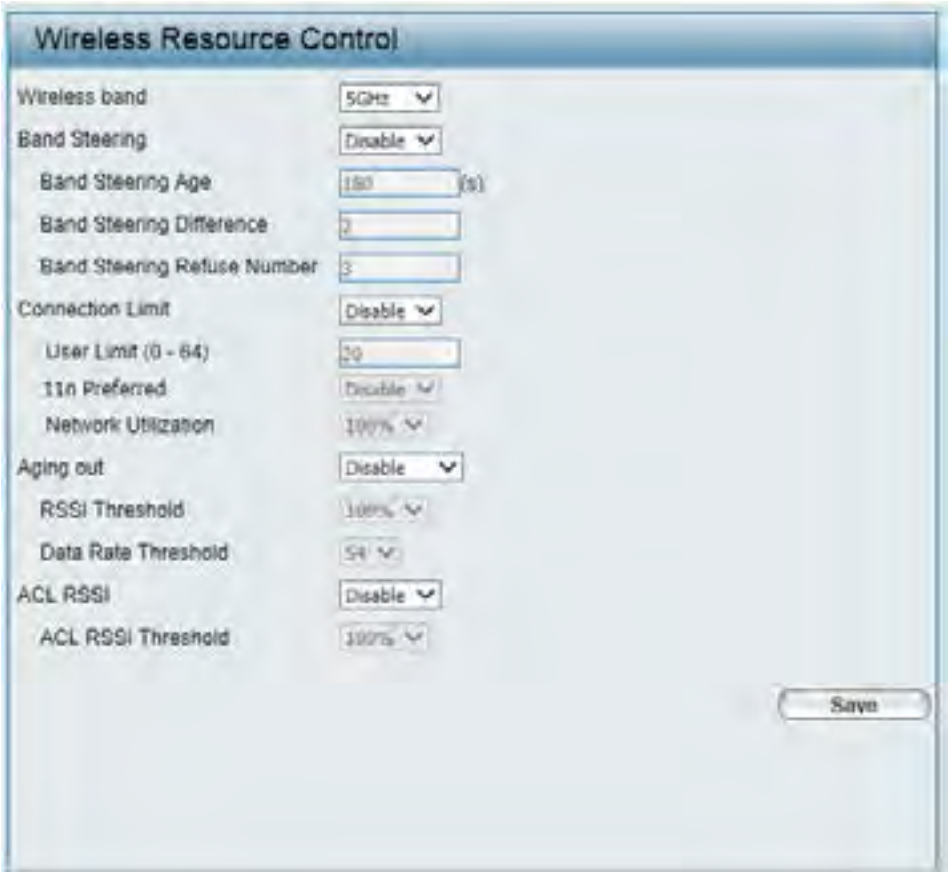
Data Rate Threshold: When **Data Rate** is selected in the **Aging Out** drop-down menu, select the threshold of data rate here. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients.

ACL RSSI: Select to **Enable** or **Disable** the ACL RSSI feature here. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.

ACL RSSI Threshold: Set the ACL RSSI threshold percentage.

Wireless Resource (5GHz)

The Wireless Resource Control window is used to configure the wireless connection settings so that the device can detect the better wireless connection in your environment.



Wireless band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

Band Steering: Select to **Enable** or **Disable** the band steering feature here.

Band Steering Age: Enter the band steering age value, in seconds, in the space provided, to specify the interval of updating information.

Band Steering Difference: Enter the band steering difference value here. The band steering difference value is equal to the number of 5GHz wireless client connections minus the number of 2.4GHz wireless client connections. If the number of 5GHz wireless client connections minus the number of 2.4GHz wireless client connections exceed this value, the extra 5GHz wireless client connections will be forced to connect to the 2.4GHz band and not the 5GHz band.

Band Steering Refuse Number: Enter the maximum 5GHz connection attempts allowed before the 5GHz preferred function will be disabled for the wireless station connection.

Connection Limit: Select to **Enable** or **Disable** the connection limit feature here. 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 below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled and when the number of users exceeds this value, or the network utilization of this AP exceeds the percentage that has been specified, the DAP-2660 will not allow clients to associate with the AP.

User Limit (0-64): Enter the maximum amount of users that are allowed access (0 to 64 users) to the device using the specified wireless band. The default setting is 20.

11n Prefered: Use the drop-down menu to **Enable** or **Disable** the 11n Preferred function. The wireless clients with 802.11n protocol will have higher priority to connect to the device.

Network Utilization: Set the maximum utilization of this access point for service. The DAP-2660 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.

Aging Out: Use the drop-down menu to select the criteria of disconnecting the wireless clients. Available options are **RSSI** and **Data Rate**.

RSSI Threshold: When **RSSI** is selected in the **Aging Out** drop-down menu, select the percentage of RSSI here. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients.

Data Rate Threshold: When **Data Rate** is selected in the **Aging Out** drop-down menu, select the threshold of data rate here. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients.

ACL RSSI: Select to **Enable** or **Disable** the ACL RSSI feature here. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.

ACL RSSI Threshold: Set the ACL RSSI threshold percentage.

Multi-SSID (2.4GHz)

The device supports up to four multiple Service Set Identifiers. You can set the Primary SSID in the Basic > Wireless section. The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Enable Multi-SSID: Select the checkbox to enable the multiple SSID feature.

Enable Priority: Select the checkbox to enable the priority option.

Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **2.4GHz** wireless band.

Index: Select the SSID index value here. The Primary SSID cannot be modified here. After selecting multiple SSIDs 1 to 7, their respective parameters can be configured.

SSID: Enter a unique SSID name for each multiple SSID in the space provided.

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

Security: Select the wireless security method to use for the specified multiple SSID here. For multiple SSIDs, the following wireless security methods are supported: **Open System**, **WPA-Personal**, **WPA Enterprise** and **802.1X**.

For more information about the wireless security, refer to page 14.

Priority: Select the priority level of the SSID selected.

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

Captive Portal: Select to **Enable** or **Disable** the captive portal feature for the specified multi-SSID here.

Multi-SSID (5GHz)

The device supports up to four multiple Service Set Identifiers. You can set the Primary SSID in the Basic > Wireless section. The SSID's factory default setting is dlink. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Enable Multi-SSID: Select the checkbox to enable the multiple SSID feature.

Enable Priority: Select the checkbox to enable the priority option.

Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

Index: Select the SSID index value here. The Primary SSID cannot be modified here. After selecting multiple SSIDs 1 to 7, their respective parameters can be configured.

SSID: Enter a unique SSID name for each multiple SSID in the space provided.

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

Security: Select the wireless security method to use for the specified multiple SSID here. For multiple SSIDs, the following wireless security methods are supported: **Open System**, **WPA-Personal**, **WPA Enterprise** and **802.1X**.

For more information about the wireless security, refer to page 14.

Priority: Select the priority level of the SSID selected.

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

Captive Portal: Select to **Enable** or **Disable** the captive portal feature for the specified multi-SSID here.

VLAN

VLAN List

The DAP-2660 supports VLANs. VLANs can be created with a Name and VID. Mgmt (TCP stack), LAN, Primary/Multiple SSID, and WDS connection can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-2660 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

VLAN Status: Select to **Enable** or **Disable** the VLAN status here.

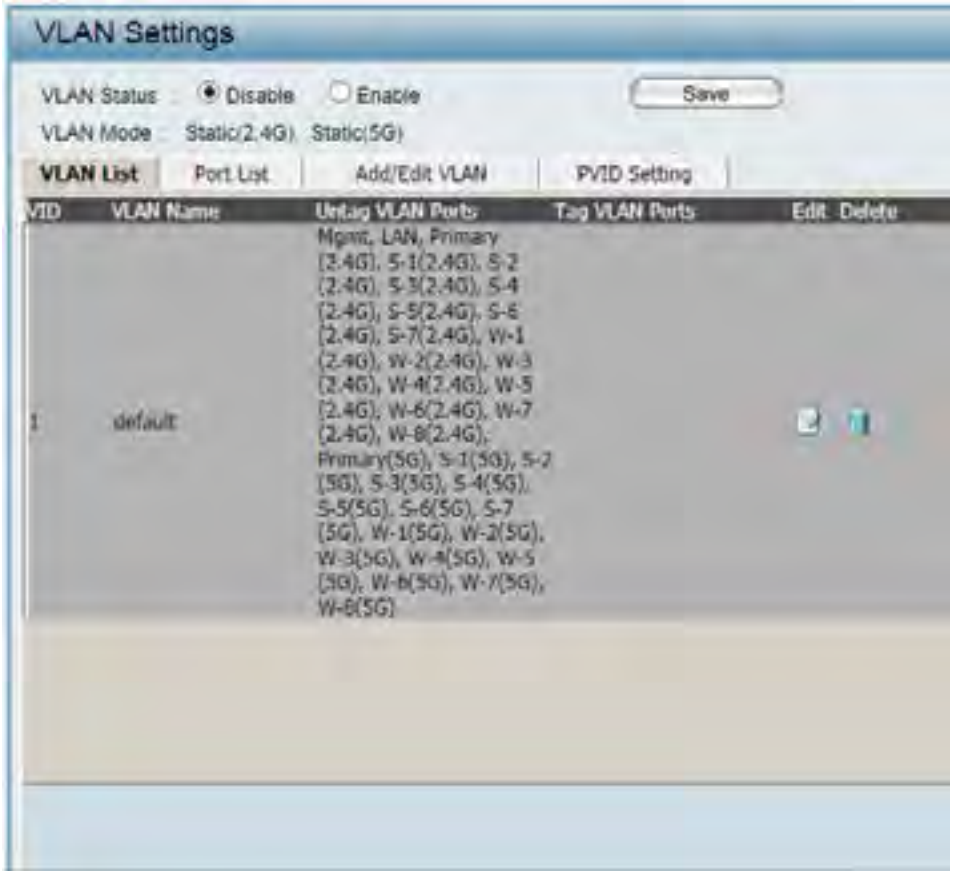
VLAN Mode: The current VLAN mode is displayed.

VLAN List: In this tab, a list of configured VLAN, with their respective parameters will be displayed.

Port List: In this tab, a list of ports, with their respective VLAN configurations, will be displayed.

Add/Edit VLAN: In this tab, we can add or modify VLANs configured on this access point.

PVID Settings:: In the tab, we can configure the PVID settings for the VLANs configured in this access point.



Port List

The Port List tab displays the current ports. If you want to configure the guest and internal networks on a Virtual LAN (VLAN), the switch and DHCP server you are using must also support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

VLAN Status: Select to **Enable** or **Disable** the VLAN status here.

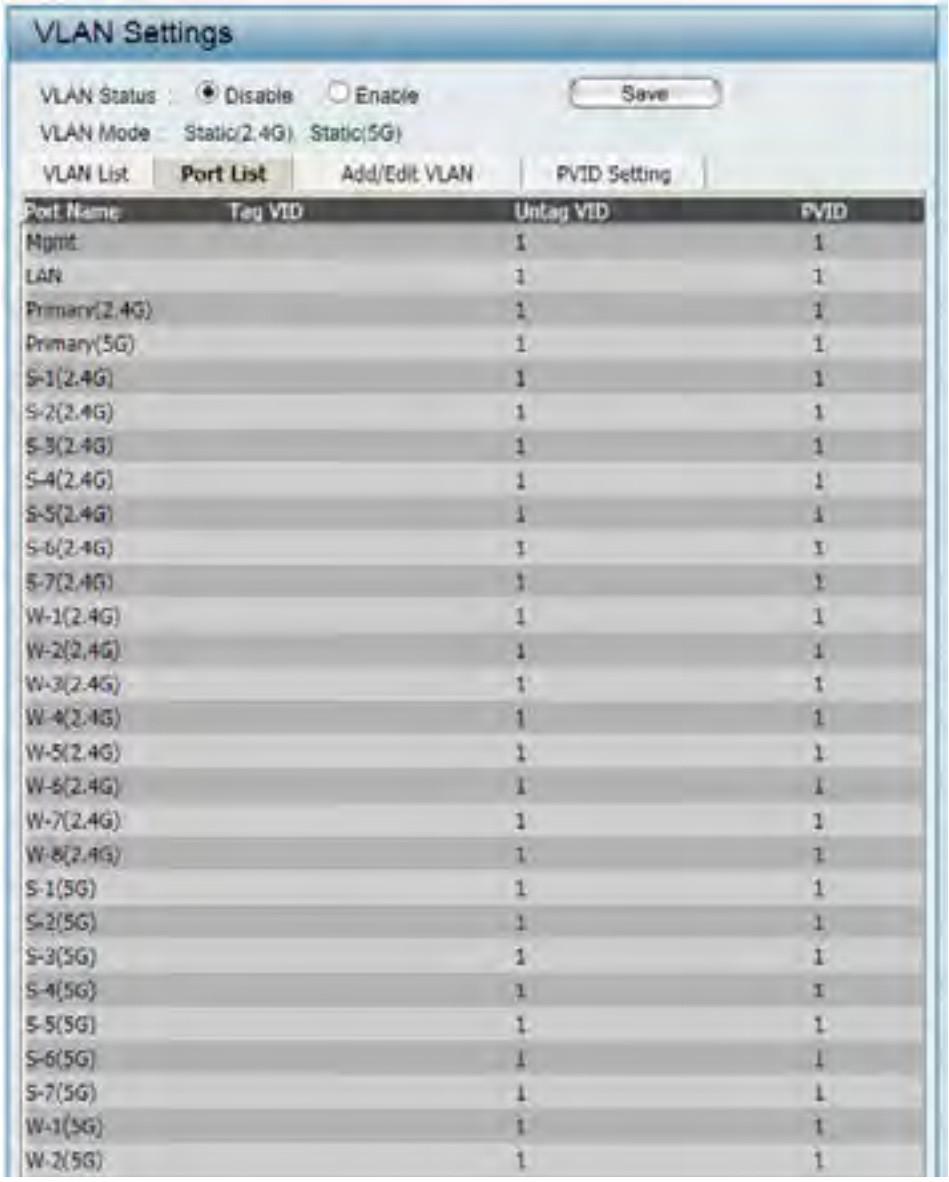
VLAN Mode: The current VLAN mode is displayed.

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

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

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

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



Add/Edit VLAN

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

VLAN Status: Select to **Enable** or **Disable** the VLAN status here.

VLAN Mode: The current VLAN mode is displayed.

VLAN ID (VID): Enter the VLAN ID value here. This value must be between 1 and 4096.

VLAN Name: Enter the VLAN name to add or modify here.

Untag: Select this option to configure the respective port to be untagged in the VLAN.

Tag: Select this option to include the VLAN tag in the packets sent and received through the respective port.

Not Member: Select this option to specify that the respective port in not a member of the VLAN being added/configured.

PVID Settings

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

VLAN Status: Select to **Enable** or **Disable** the VLAN status here.

VLAN Mode: The current VLAN mode is displayed.

PVID Auto Assign Status: Select to **Enable** or **Disable** the option to automatically assign PVIDs for all the ports.

PVID: Enter the PVID value for the respective port in the spaces provided.

Intrusion

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

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**.

Detect: Click this button to initiate a scan for APs on the network.

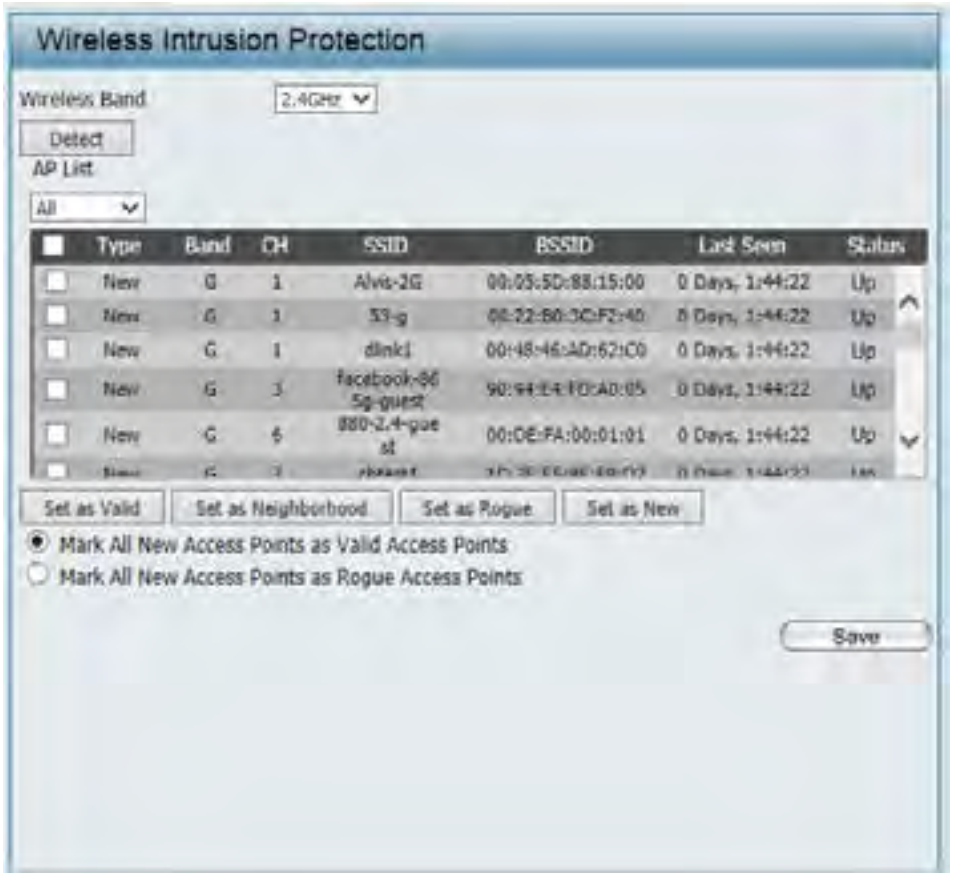
AP List: Select the type of APs to display in the table. Options to choose from are **All**, **Valid**, **Neighbor**, **Rogue**, and **New**.

Set as Valid: Select an AP from the list and click this button configure the selected AP as a valid AP.

Set as Neighborhood: Select an AP from the list and click this button configure the selected AP as part of the neighborhood.

Set as Rogue: Select an AP from the list and click this button configure the selected AP as a rogue AP.

Set as New: Select an AP from the list and click this button configure the selected AP as a new AP.



Schedule

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

Wireless Schedule: Select to **Enable** or **Disable** the wireless schedule feature here.

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

Index: Use the drop-down menu to select the desired SSID.

SSID: This read-only field indicates the current SSID in use.

Day(s): Toggle the radio button between **All Week** and **Select Day(s)**. If the second option is selected, check the specific days you want the rule to be effective on.

All Day(s): Check this box to have your settings apply 24 hours a day.

Start Time: Enter the beginning hour and minute, using a 24-hour clock.

End Time: Enter the ending hour and minute, using a 24-hour clock.

Internal RADIUS Server

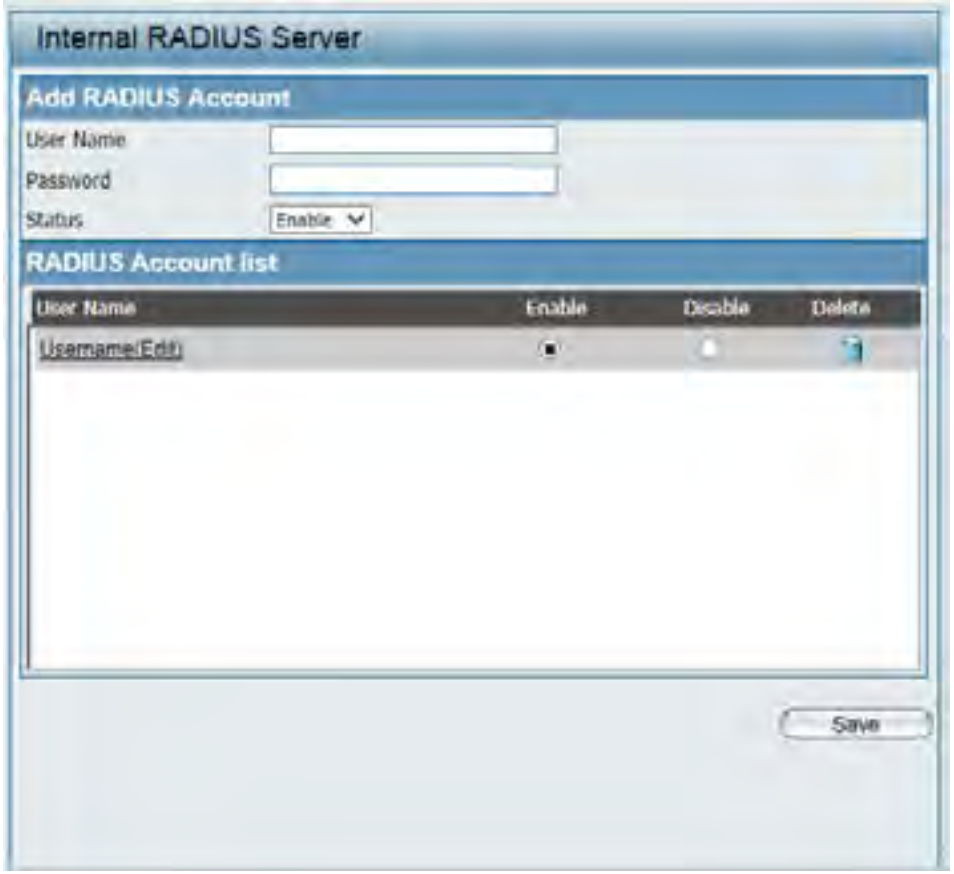
The DAP-2660 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the **Save** button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts below 30.

User Name: Enter the user name for the new RADIUS account here.

Password: Enter the password for the new RADIUS account here. The password must be between 8 and 64 characters long.

Status: Select to Enable or Disable the status of the newly created RADIUS account here.

RADIUS Account List: In this table, a list of configured RADIUS accounts will be displayed. To enable the status of a RADIUS account, select the **Enable** radio button. To disable the status of a RADIUS account, select the **Disable** radio button. To remove a RADIUS account, click on the **Delete** icon.



ARP Spoofing Prevention

The ARP Spoofing Prevention feature allows users to add IP/MAC address mapping to prevent ARP spoofing attacks.

ARP Spoofing Prevention: Select to **Enable** or **Disable** the ARP spoofing prevention feature here.

Gateway IP Address: Enter the gateway IP address here.

Gateway MAC Address: Enter the gateway MAC address here.

Airtime Fairness

The Airtime Fairness window allows the user to manage the bandwidth of the device and arrange the bandwidth for various wireless clients. When the Airtime Fairness rule is finished, click the **Add** button. To discard the Airtime Fairness Rule settings, click the **Clear** button. Click the **Save** button to let your changes take effect.

Enable Airtime Fairness: Select to **Enable** or **Disable** the Airtime Fairness feature here.

Downlink Bandwidth: Enter the downlink bandwidth of the device in Mbits per second.

Uplink Bandwidth: Enter the uplink bandwidth of the device in Mbits per second.

Rule Type: Select the rule type here. Available options are: **Allocate average BW for each station**, **Allocate maximum BW for each station**, **Allocate different BW for 11a/b/g/n stations**, and **Allocate specific BW for SSID**.

Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**. In this section we'll explain the **5GHz** wireless band.

SSID: Select the SSID that will be used for this feature here.

Downlink Speed: Enter the downlink speed limitation value in either Kbits/sec or Mbits/sec for the rule.

Uplink Speed: Enter the uplink speed limitation value in either Kbits/sec or Mbits/sec for the rule.

AP Array

AP Array Scan

The AP Array window allows users to create a set of devices on a network that are organized into a single group in order to increase ease of management. Once a user has made the desired settings, click the **Save** button to let the changes take effect.

Enable AP Array: This check box allows the user to enable the AP array function. The three modes that are available are **Master**, **Backup Master**, and **Slave**. APs in the same array will use the same configuration. The configuration will sync the Master AP to the Slave AP and the Backup Master AP when a Slave AP and a Backup Master AP join the AP array.

AP Array Name: Enter an AP array name for the group here.

AP Array Password: Enter an AP array password for the group here. This password must be the same on all the APs in the group.

Scan AP Array List: Click this button to initiate a scan of all the available APs currently on the network.

AP Array List: This table displays the current AP array status for the following parameters: Array Name, Master IP, MAC, Master, Backup Master, Slave, and Total.

Current Array Members: This table displays all the current array members. The DAP-2660 AP array feature supports up to eight AP array members.

Configuration Settings

In the AP array configuration settings windows, users can specify which settings all the APs in the group will inherit from the master AP. Make the required selection in this window and click the **Save** button to accept the changes made.

Enable AP Array Configuration: Select to **Enable** or **Disable** the AP array configure feature here.

Wireless Basic Settings: Select this option to specify the basic wireless settings that the APs in the group will inherit.

Wireless Advanced Setting: Select this option to specify the advanced wireless settings that the APs in the group will inherit.

Multiple SSID & VLAN: Select this option to specify the multiple SSIDs and VLAN settings that the APs in the group will inherit.

Advanced Functions: Select this option to specify the other advanced settings that the APs in the group will inherit.

Administration Settings: Select this option to specify the administrative settings that the APs in the group will inherit.

Wireless Basic Settings

Network Name (SSID): Select this option to use the same SSID.

SSID Visibility: Select this option to enable SSID visibility.

Auto Channel Selection: Select this option to use auto channel selection.

Channel Width: Select this option to use the same channel width.

Security: Select this option to use the same wireless security.

Captive Profile: Select this option to use the same captive profile settings.

Band: Select this option to use the same wireless band.

Wireless Advanced Settings

Wireless: Select this option to use the same wireless settings.

Wireless Mode: Select this option to use the same wireless mode.

Data Rate: Select this option to use the same data rate.

Beacon Interval: Select this option to use the same beacon interval.

DTIM Interval: Select this option to use the same DTIM interval.

Transmit Power: Select this option to use the same transmit power.

WMM (Wi-Fi Multimedia): Select this option to use the same WMM settings.

Ack Time Out: Select this option to use the same ACK timeout value.

Short GI: Select this option to use the same short GI settings.

Link Integrity: Select this option to use the same link integrity settings.

Connection Limit: Select this option to use the same connection limit value.

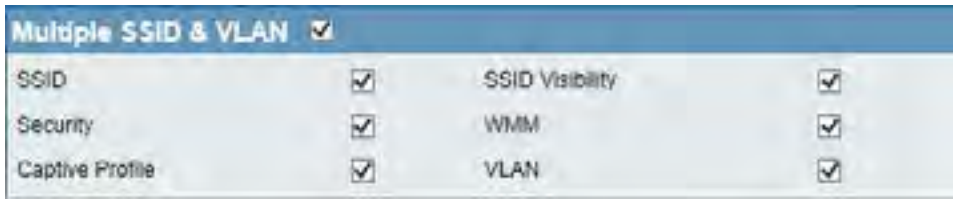
IGMP Snooping: Select this option to use the same IGMP snooping settings.

Multiple SSID & VLAN

SSID: Select this option to use the same multi-SSIDs.

SSID Visibility: Select this option to use the same SSID visible.

Security: Select this option to use the same wireless security settings.



WMM: Select this option to use the same WMM settings.

Captive Profile: Select this option to use the same captive profile settings.

VLAN: Select this option to use the same VLAN settings.

Advanced Functions

Schedule Settings: Select this option to use the same schedule settings.

QoS Settings: Select this option to use the same Quality of Service settings.

Log Settings: Select this option to use the same log settings.

Time and Date Settings: Select this option to use the same time and date settings.

ARP Spoofing Prevention: Select this option to use the same ARP spoofing prevention settings.

Airtime Fairness: Select this option to use the same airtime fairness settings.

Captive Portal: Select this option to use the same captive portal settings.

AP Array Authentication: Select this option to use the same AP array authentication settings.

Auto RF: Select this option to use the same auto-RF settings.

Load Balance: Select this option to use the same load balancing settings.

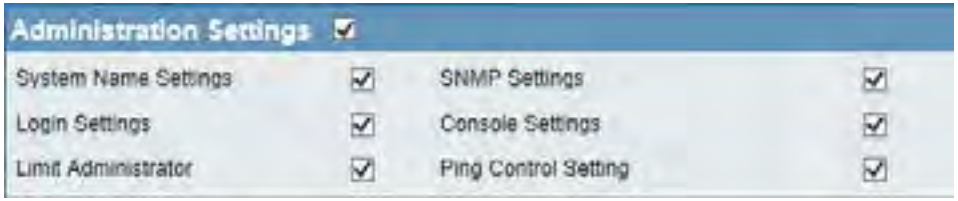
DHCP Server Settings: Select this option to use the same DHCP server settings.

Administration Settings

System Name Settings: Select this option to use the same system name.

SNMP Settings: Select this option to use the same SNMP settings.

Login Settings: Select this option to use the same login settings.



Console Settings: Select this option to use the same console settings.

Limit Administrator: Select this option to use the same limit administrator settings.

Ping Control Settings: Select this option to use the same ping control settings.

Auto-RF

In this windows, users can view and configure the automatic radio frequency settings as well as configure the the auto-initiate period and threshold values. Click the **Save** button to accept the changes made.

Enable: Auto-RF: Select to **Enable** or **Disable** the auto-RF feature here.

Initiate Auto-RF: Click the **Auto-RF Optimize** button to initiate the auto-RF optimization feature.

Auto-Initiate: Select the **Enable** or **Disable** the auto-initiate feature here.

Auto-Initiate Period: After enabling the auto-initiate option, the auto-initiate period value can be entered here. This value must be between 1 and 24 hours.

RSSI Threshold: Select the RSSI threshold value here. This value is listed in the drop-down menu in increments of 10% from **10%** to **100%**.

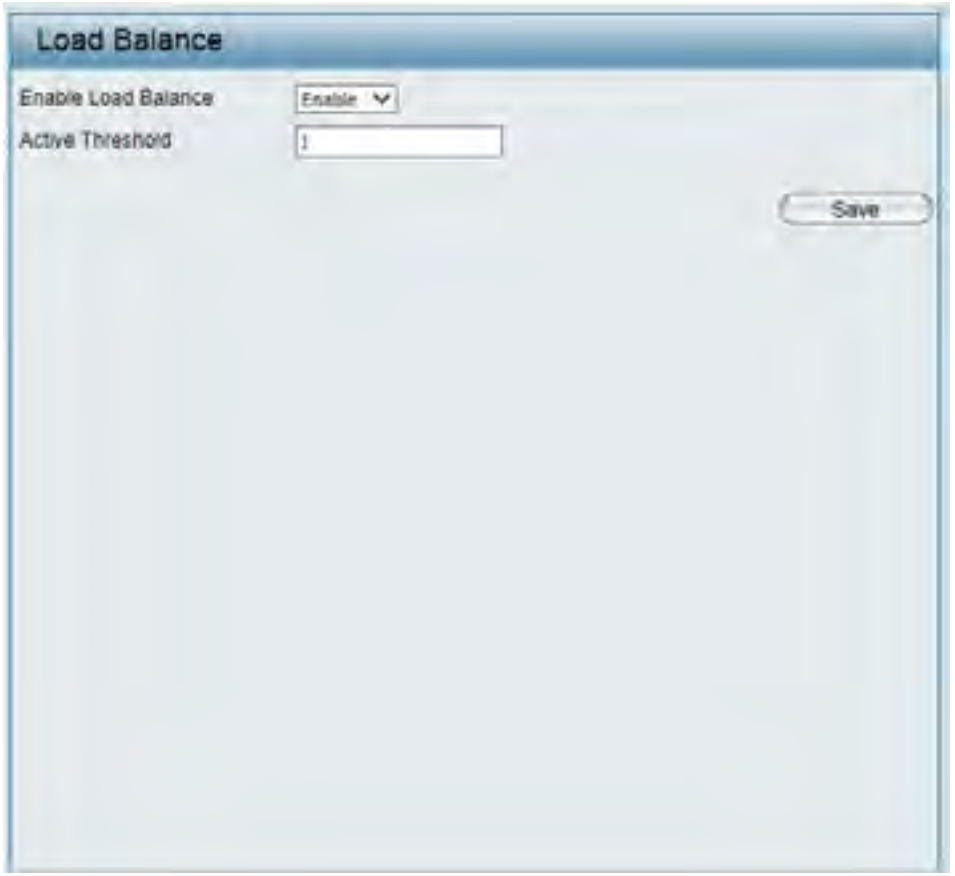
RF Report Frequency: Enter the RF report frequency value here.

Load Balance

In this window, users can view and configure the AP array's load balancing settings. Click the Save button to accept the changes made.

Enable Load Balance: Select to **Enable** or **Disable** the load balance feature here.

Active Threshold: Enter the active threshold value here.



Captive Portal

Authentication Settings - Ticket

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web brower will be redirected to a web authentication page. In this windows, user can view and configure the Captive Portal settings. Click the **Add** button to add a new entry. Click the **Delete** or **Delete All** button to remove a specific entry or all the entries configured.

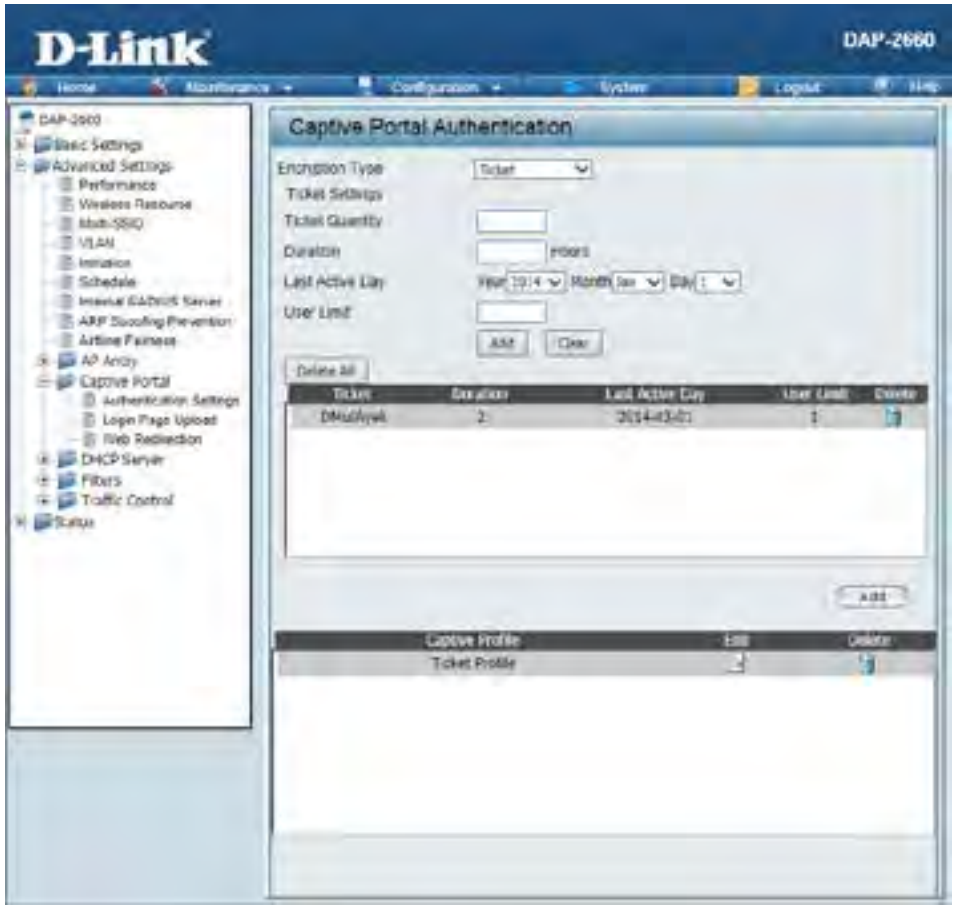
Encryption Type: Select the captive portal encryption type here. Options to choose from are **Ticket**, **User/Password**, **Remote Radius**, **LDAP** and **POP3**. In this section we'll discuss the **Ticket** option.

Ticket Quantity: Enter the number of ticket that will be used here.

Duration: Enter the duration value, in hours, for this ticket.

Last Active Day: Select the last active date for this ticket here. **Year**, **Month** and **Day** selections can be made.

User Limit: Enter the maximum amount of users that can use this ticket at the same time.



Authentication Settings - User/Password

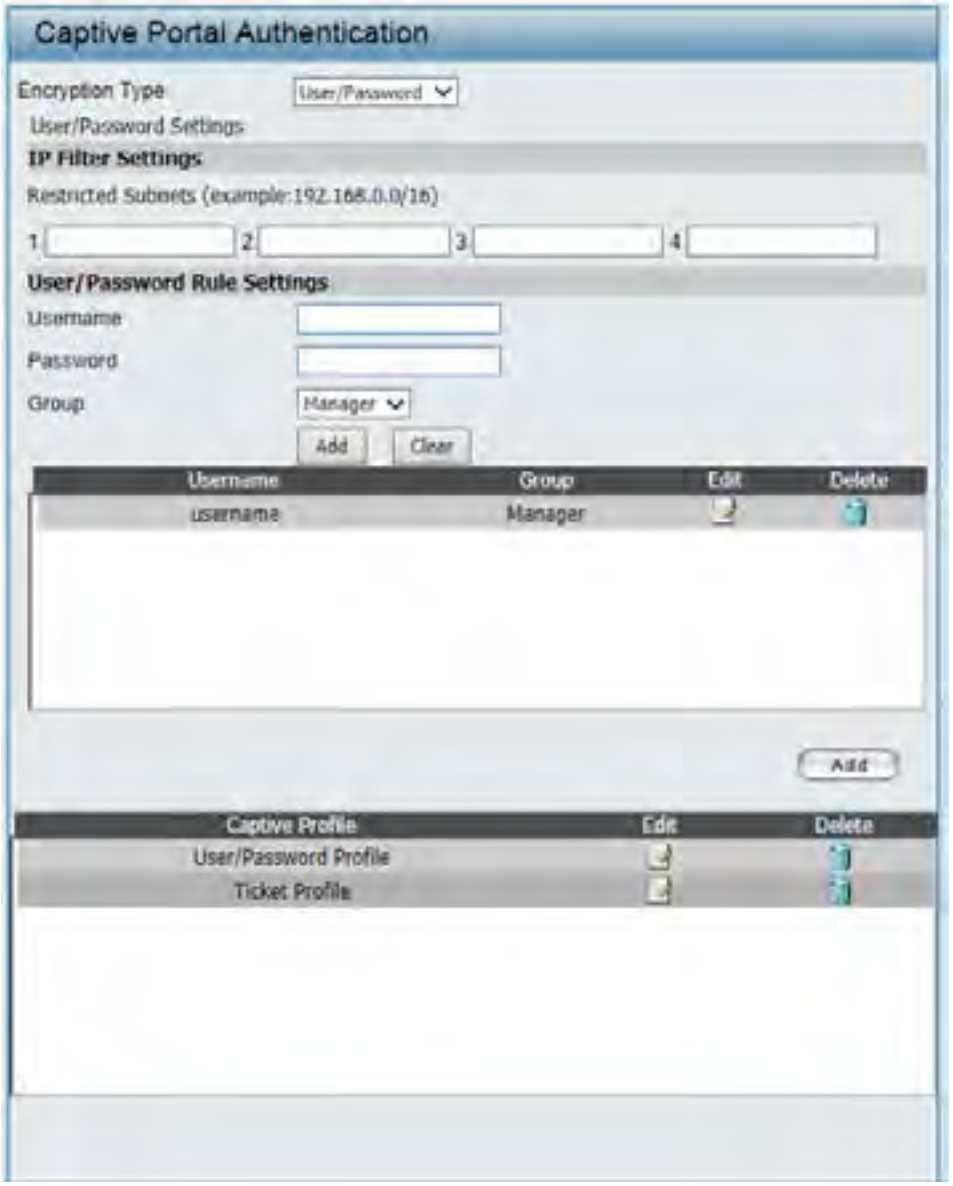
Encryption Type: Select the captive portal encryption type here. Options to choose from are **Ticket**, **User/Password**, **Remote Radius**, **LDAP** and **POP3**. In this section we'll discuss the **User/Password** option.

Restricted Subnets: Enter the restricted subnets here. Access to these subnets will denied to guest accounts. Up to four restricted subnet entries can be defined.

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Group: Select the group for the new account here. Options to choose from are **Manager** and **Guest**. Guest accounts will have limited access.



Authentication Settings - Remote RADIUS

Encryption Type: Select the captive portal encryption type here. Options to choose from are **Ticket**, **User/Password**, **Remote Radius**, **LDAP** and **POP3**. In this section we'll discuss the **Remote Radius** option.

Remote Radius Type: Select the remote RADIUS server type here. Currently, only **SPAP** will be used.

Radius Server: Enter the RADIUS server's IP address here.

Radius Port: Enter the RADIUS server's port number here.

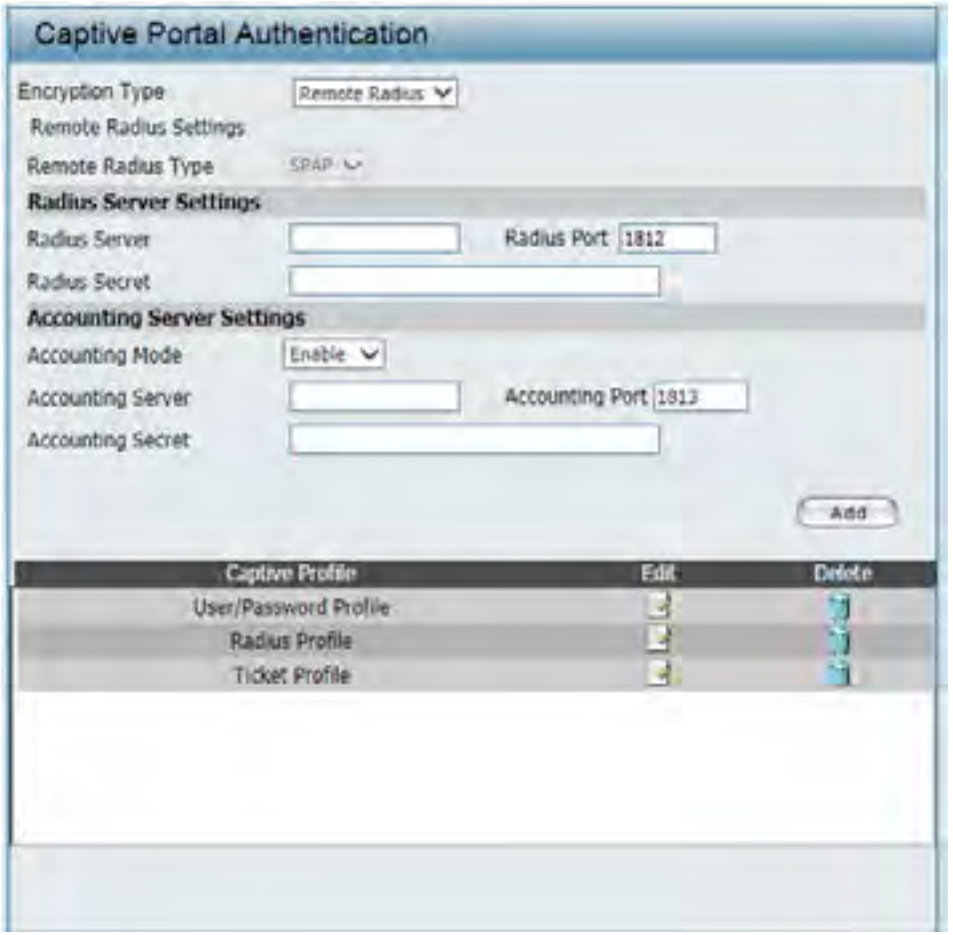
Radius Secret: Enter the RADIUS server's shared secret here.

Accounting Mode: Select to **Enable** or **Disable** the accounting mode here.

Accounting Server: Enter the accounting server's IP address here.

Accounting Port: Enter the accounting server's port number here.

Accounting Secret: Enter the accounting server's shared serect here.



Authentication Settings - LDAP

Encryption Type: Select the captive portal encryption type here. Options to choose from are **Ticket**, **User/Password**, **Remote Radius**, **LDAP** and **POP3**. In this section we'll discuss the **LDAP** option.

Server: Enter the LDAP server's IP address or domain name here.

Port: Enter the LDAP server's port number here.

Authenticate Mode: Select the authentication mode here. Options to choose from are **Simple** and **TLS**.

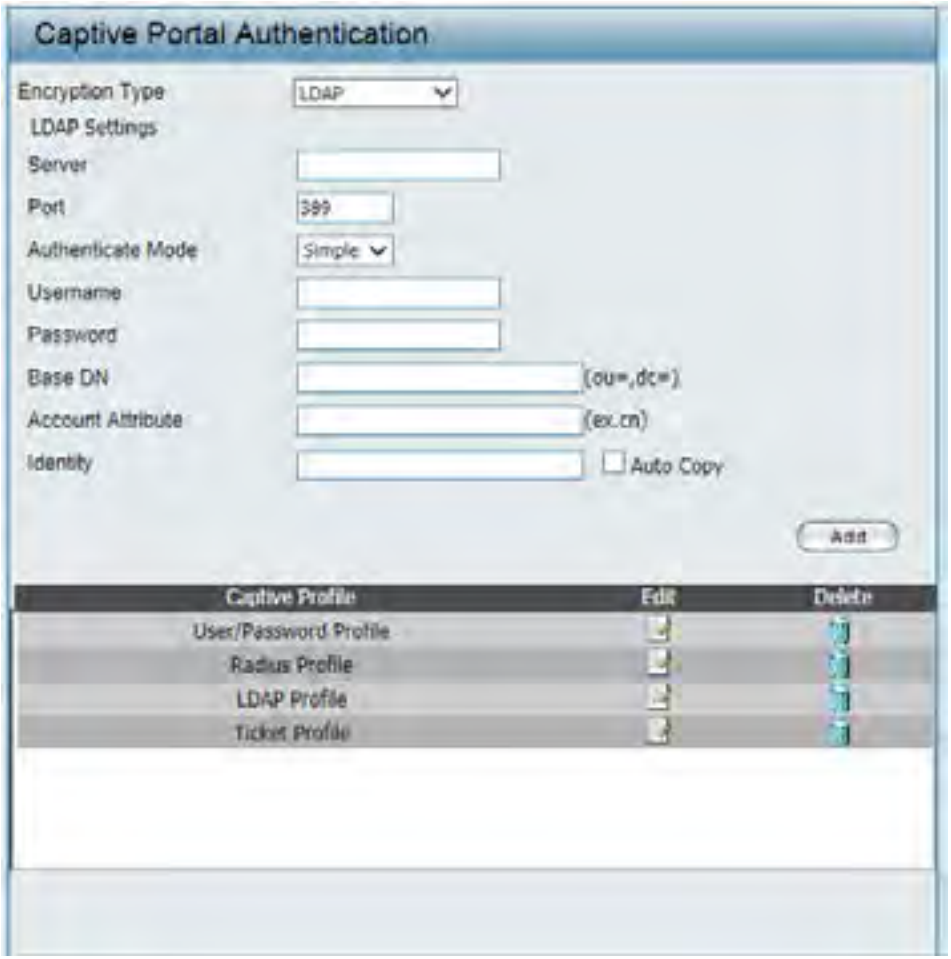
Username: Enter the LDAP server account's username here.

Password: Enter the LDAP server account's password here.

Base DN: Enter the administrator's domain name here.

Account Attribute: Enter the LDAP account attribute string here. This string will be used to search for clients.

Identity: Enter the identity's full path string here. Alternatively, select the **Auto Copy** checkbox to automatically add the generic full path of the web page in the identity field.



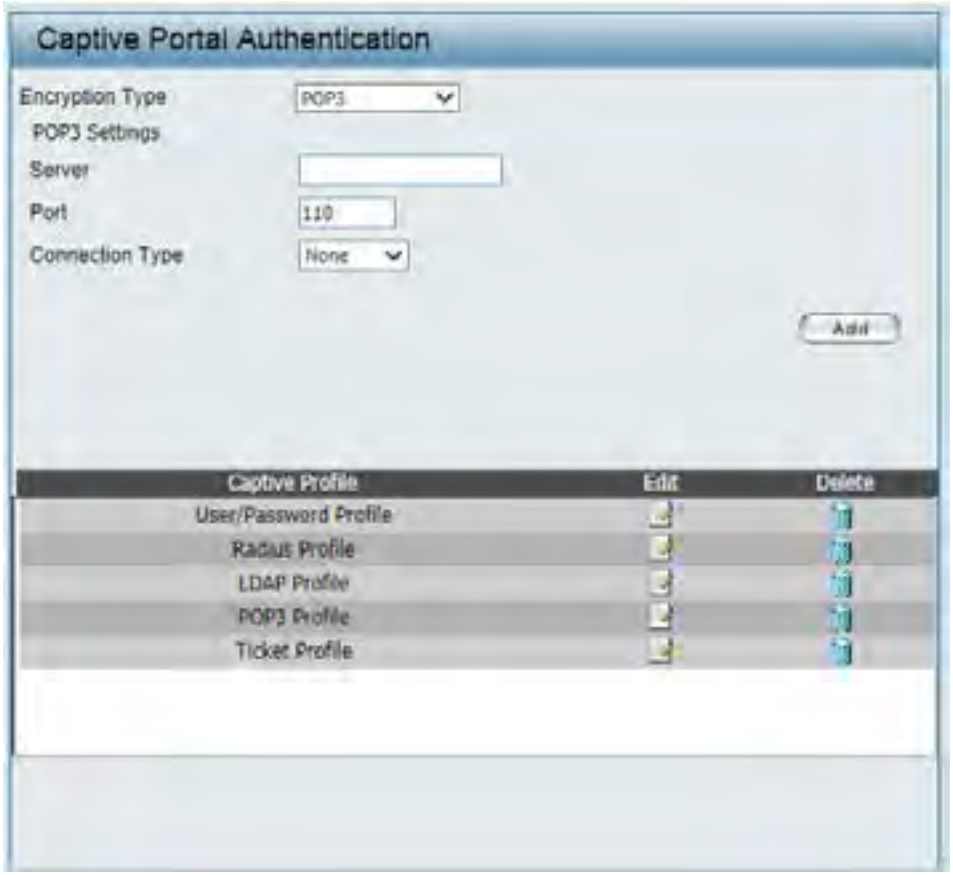
Authentication Settings - POP3

Encryption Type: Select the captive portal encryption type here. Options to choose from are **Ticket**, **User/Password**, **Remote Radius**, **LDAP** and **POP3**. In this section we'll discuss the **Ticket** option.

Server: Enter the POP3 server's IP address or domain name here.

Port: Enter the POP server's port number here.

Connection Type: Select the connection type here. Options to choose from are **None** and **SSL/TLS**.



Login Page Upload

In this window, users can upload a custom login page picture that will be used by the captive portal feature. Click the **Browse** button to navigate to the image file, located on the managing computer and then click the **Upload** button to initiate the upload.

Upload picture from file: In this field the path to the image file, that will be uploaded, will be displayed. Alternatively, the path can be manually entered here.

Web Redirection

In this windows, users can view and configure the Web redirection settings for the captive portal hosted by this access point. Wireless clients will be redirected to this web site prior and after authentication. Click the **Save** button to accept the changes made.

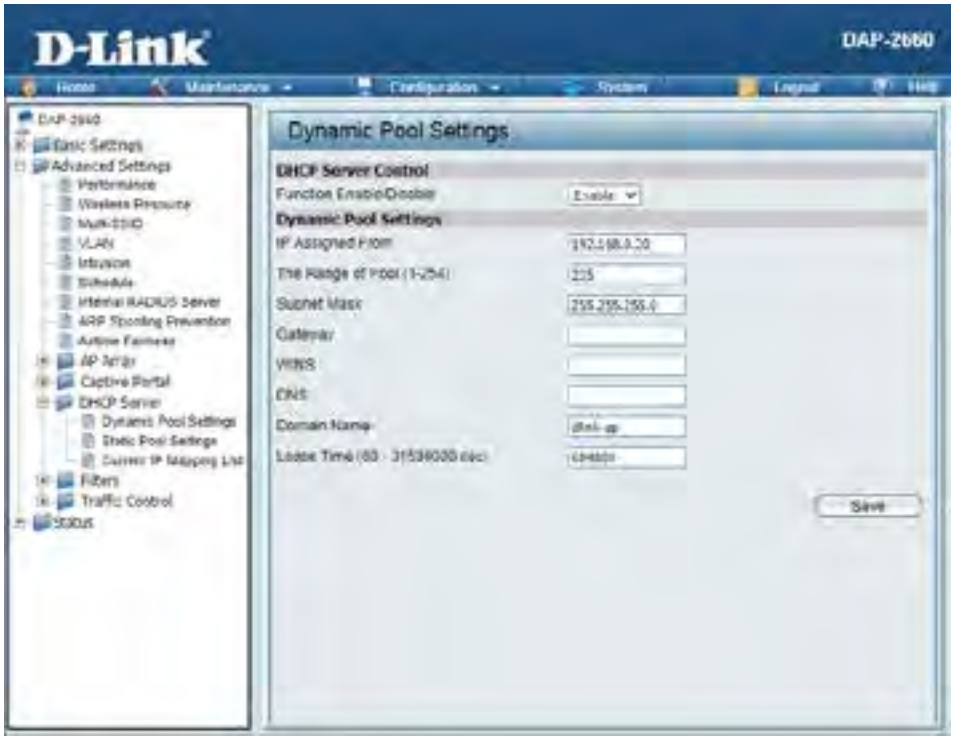
Web Redirection: Select this checkbox to enable the Web redirection feature.

Web Site: Enter the destination web site's address here.

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-2660 is capable of acting as a DHCP server.



Function Enable/ Disable: Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses. Select **Enable** to allow the DAP-2660 to function as a DHCP server.

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

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

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

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

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

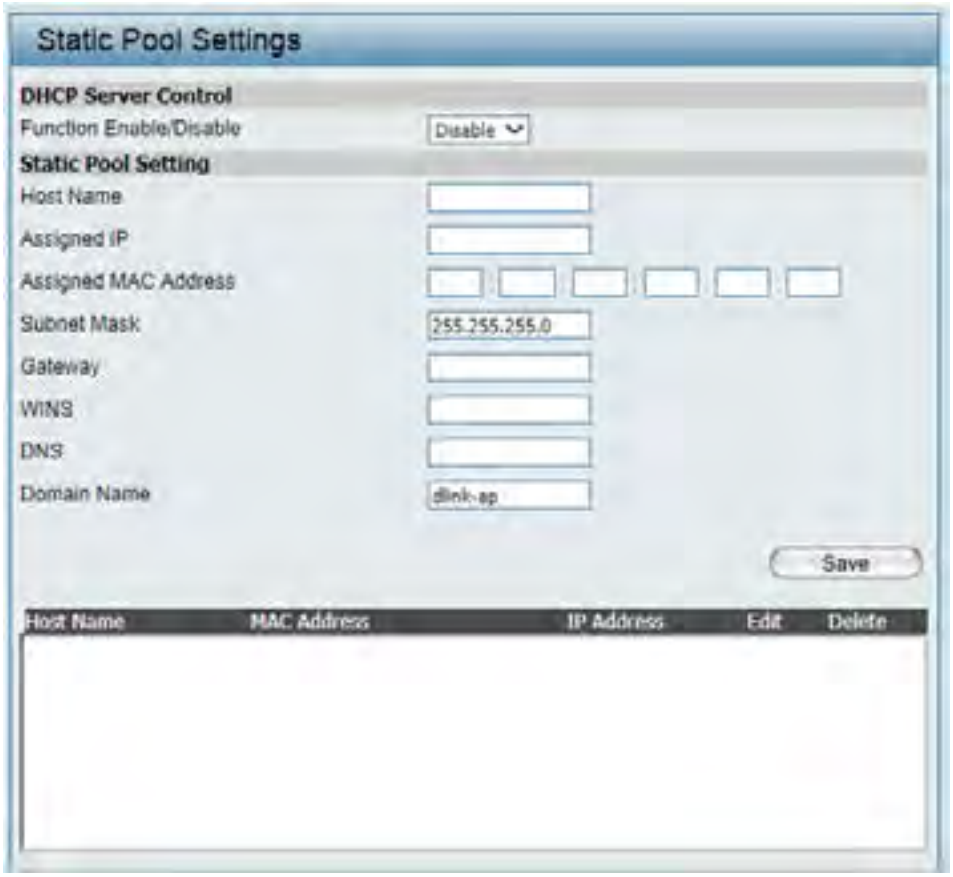
DNS: Enter the IP address of the Domain Name System (DNS) server. The DNS server translates domain names such as www.dlink.com into IP addresses.

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

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

Static Pool Setting

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



Function Enable/ Disable: Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select Enable to allow the DAP-2660 to function as a DHCP server.

Hostname: Enter the hostname of the client here.

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

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

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

Gateway: Specify the Gateway address for the wireless network.

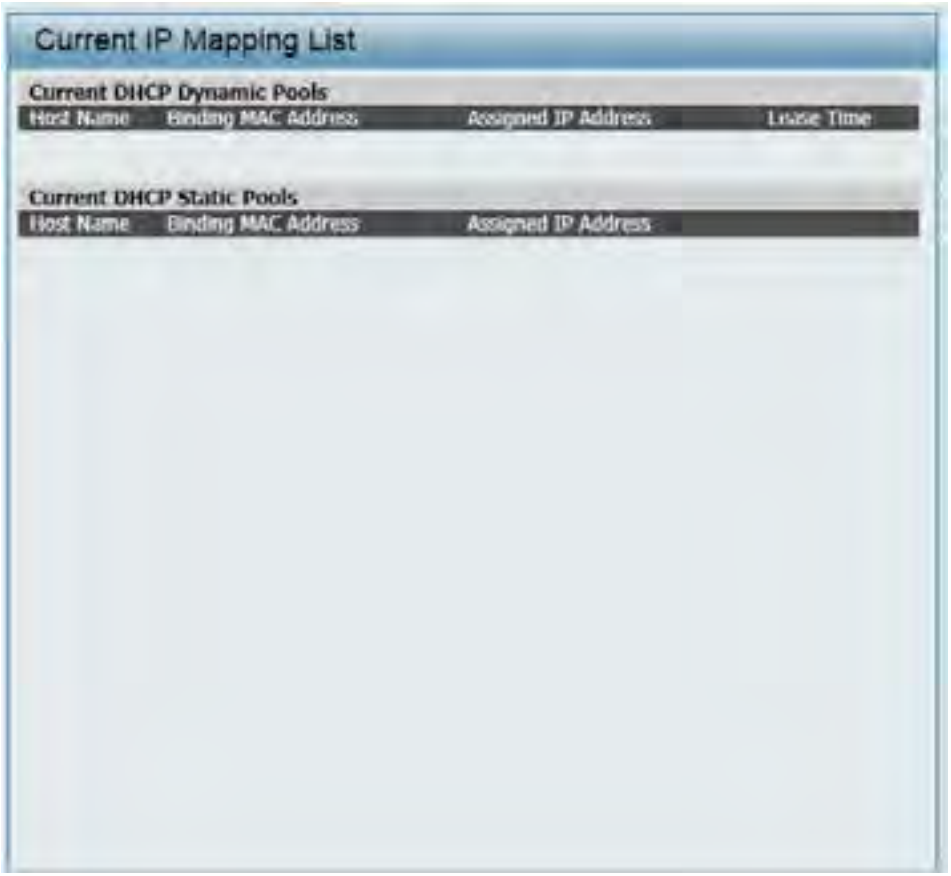
WINS: Specify the Windows Internet Naming Service (WINS) server address for the wireless network. WINS is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

DNS: Enter the DNS server address for your wireless network.

Domain Name: Specify the domain name for the network.

Current IP Mapping List

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



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

Host Name: The host name of a device on the network.

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

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

Lease Time: The length of time that the dynamic IP address will be valid.

Current DHCP Static Pools: These are the IP address pools of the DHCP server assigned through the static pool settings.

Host Name: The host name of a device on the network.

Binding MAC Address: The MAC address of a device on the network that is within the DHCP static IP address pool.

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

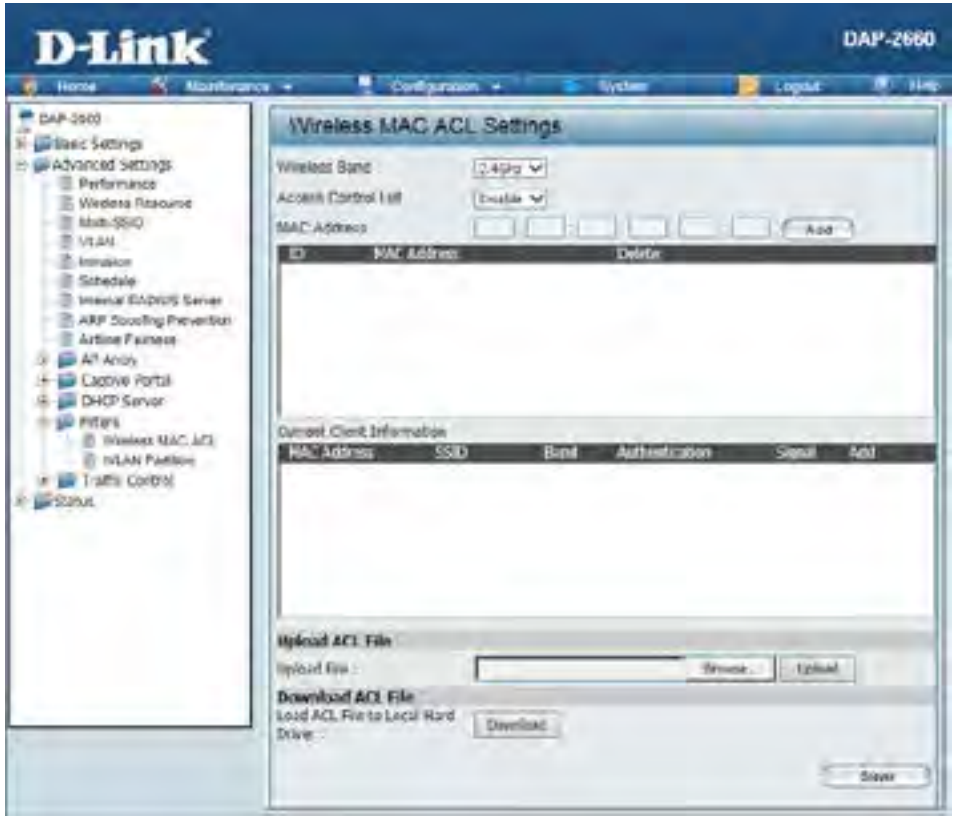
Binding MAC Address: The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.

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

Filters

Wireless MAC ACL

This page allows the user to configure Wireless MAC ACL settings for access control. Click the **Save** button to accept the changes made.



Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**.

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

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

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

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

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

Current Client Information: This table displays information about all the current connected stations.

Upload ACL File: Here users can upload a pre-configured wireless MAC ACL settings configuration file to the access point which will overwrite the current wireless MAC ACL settings. Click the **Browse** button to navigate to the configuation file, located on the local PC, and then click the **Upload** button to initiate the upload.

Load ACL File to Local Hard Drive: Here users can download the current wireless MAC ACL settings, in a configuration file, to the local PC, that serves as a backup when needed. Click the **Download** button and navigate to the destination where the file can be saved on the local PC.

WLAN Partition

In this window, users can view and configure the WLAN partition settings. After the configuration, click the **Save** button to accept the changes made.

Wireless Band: Select the wireless band used here. Options to choose from are **2.4 GHz** and **5 GHz**.

Link Integrity: Select to **Enable** or **Disable** the link integrity feature here. If the Ethernet connection between the LAN and the AP is disconnected, enabling this feature will cause the wireless segment associated with the AP to be disassociated from the AP.

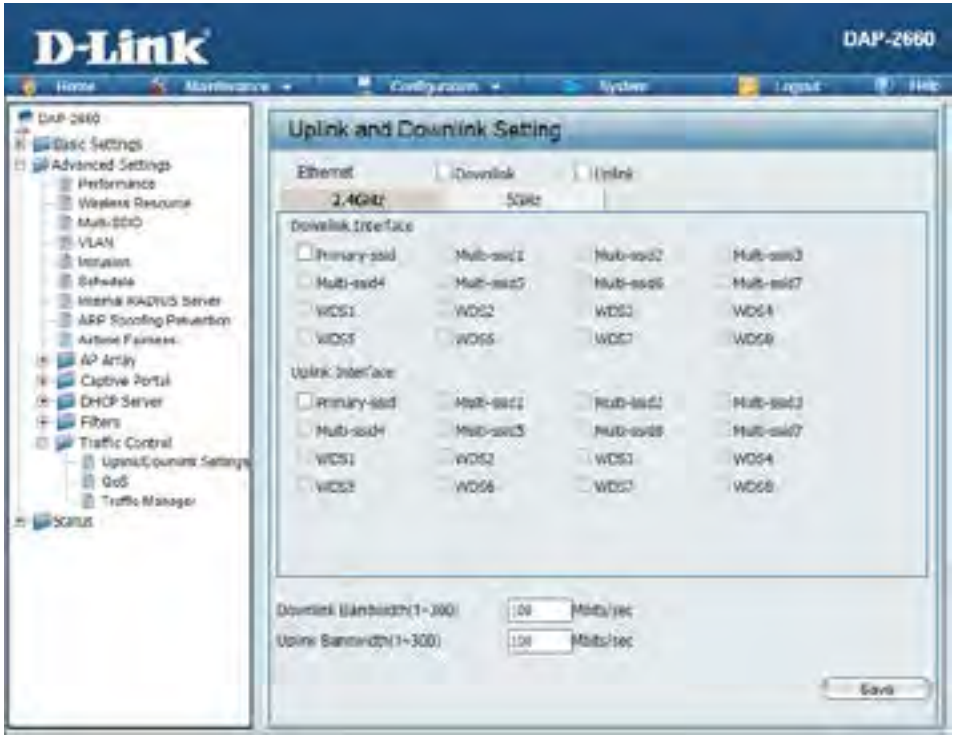
Ethernet to WLAN Access: Select to **Enable** or **Disable** the Ethernet to WLAN access feature here. When disabled, all data from the Ethernet to associated wireless devices will be blocked. Wireless devices can still send data to the Ethernet.

Internal Station Connection: The default value is **Enable**, which allows stations to intercommunicate by connecting to a target AP. When disabled, wireless stations cannot exchange data on the same Multi-SSID. In **Guest mode**, wireless stations cannot exchange data with any station on your network.

Traffic Control

Uplink/Downlink Settings

The uplink/downlink settings allows users to customize the uplink and downlink interfaces including specifying uplink/downlink bandwidth rates in Mbits per second. These values are also used in the QoS and Traffic Manager windows. Once the desired uplink and downlink settings are finished, click the **Save** button accept the changes made.



Downlink: Select this checkbox to configur the download settings.

Uplink: Select this checkbox to configure the uplink settings.

2.4GHz: Select this tab to configure the downlink/uplink settings for the 2.4GHz wireless band.

5GHz: Select this tab to configure the downlink/uplink settings for the 5GHz wireless band.

Downlink Interface: Select the downlink interface(s) that will be configured here.

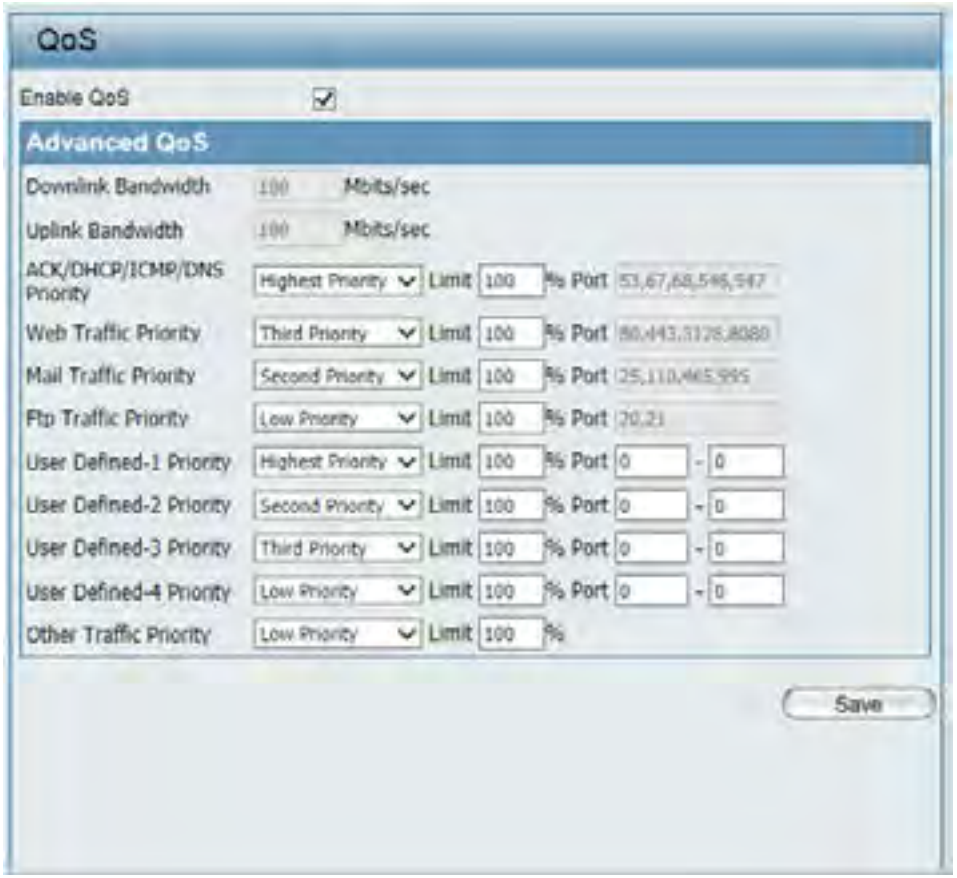
Uplink Interface: Select the uplink interface(s) that will be configured here.

Downlink Bandwidth (1~300): Enter the downlink bandwidth value here. This value must be between 1 and 300 Mbps. By default, this value is 100 Mbps.

Uplink Bandwidth (1~300): Enter the uplink bandwidth value here. This value must be between 1 and 300 Mbps. By default, this value is 100 Mbps.

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2660 supports four priority levels. Once the desired QoS settings are finished, click the **Save** button to accept the changes made.



Enable QoS: Select this checkbox to enable the Quality of Server feature.

Downlink Bandwidth: Here the configured downlink bandwidth value, in Mbps, will be displayed.

Uplink Bandwidth: Here the configured uplink bandwidth value, in Mbps, will be displayed.

Priority: The priority can be selected for each type of traffic available in this window. Options to choose from are **Highest Priority**, **Second Priority**, **Third Priority**, and **Low Priority**.

Limit The limit percentage value can be value can be entered for each type of traffic in the spaces provided next to each traffic type.

Port: For user-defined priority rules, a range of traffic port numbers can manually be entered in the spaces provided.

ACK/DHCP/ICMP/DNS Priority: Select the ACK, DHCP, ICMP and DNS traffic priority here and enter the limit percentage value in the space provided.

Web Traffic Priority: Select the Web traffic priority here and enter the limit percentage value in the space provided.

Mail Traffic Priority: Select the mail traffic priority here and enter the limit percentage value in the space provided.

FTP Traffic Priority: Select the FTP traffic priority here and enter the limit percentage value in the space provided.

User Defined Priority: Select the user-defined traffic priority here and enter the limit percentage value in the space provided. For user-defined priority entries, the traffic port range must also be specified to clarify which type of traffic will be prioritized.

Other Traffic Priority: Lastly, select priority for all other traffic, not defined, here and enter the limit percentage value in the space provided.

Traffic Manager

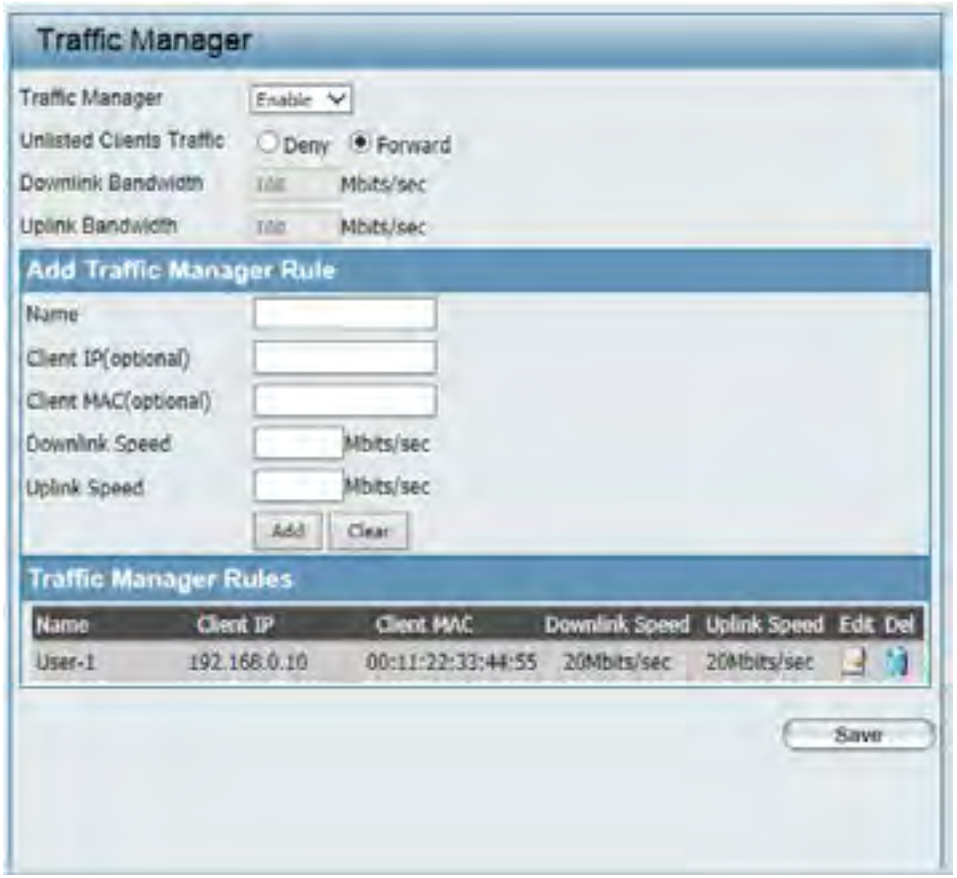
The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/ uplink speed for new traffic manager rules. Click the **Save** button to accept the changes made.

Traffic Manager: Select to **Enable** or **Disable** the traffic manager feature here.

Unlisted Client Traffic: $$$ Select **Deny** or **Forward** to determine how to deal with unlisted client traffic.

Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Uplink Bandwidth: Uplink Bandwidth:The uplink bandwidth in Mbits per second. This value is entered in the Uplink/ Downlink Setting window.



Status

In the Status Section the user can monitor and view configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the Status section in more detail.

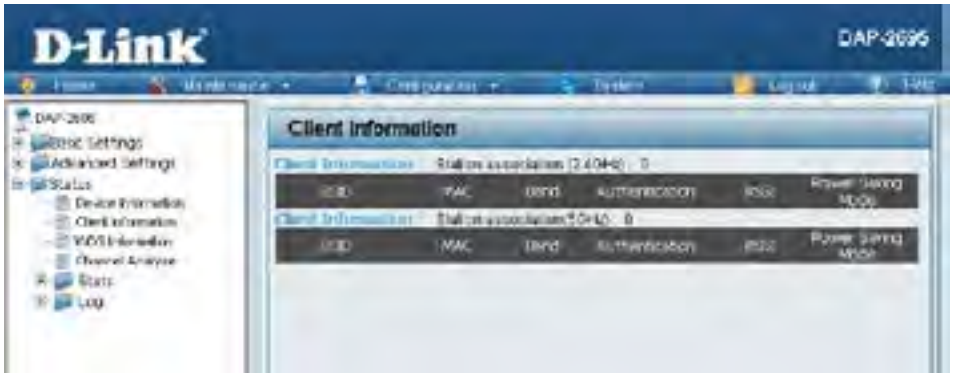
Device Information

This page displays the current information like firmware version, Ethernet and wireless parameters, as well as the information regarding CPU and memory utilization.

Device Information: This read-only window displays the configuration settings of the DAP-2660, including the firmware version and the device's MAC address.

Client Information

This page displays the associated clients SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-2660 network.



Client Information: This window displays the wireless client information for clients currently connected to the DAP-2660.

SSID: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

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

Authentication: Displays the type of authentication being used.

RSSI: Displays the client's signal strength.

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

WDS Information Page

This page displays the access points SSID, MAC, band, authentication method, signal strength, and status for the DAP-2660's Wireless Distribution System network.

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-2660.

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

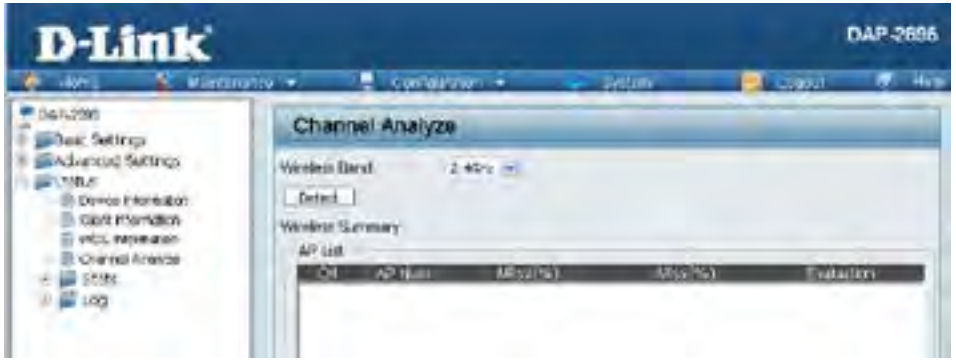
Status: Displays the status of the power saving feature.

Channel Analyze

Wireless Band: Select either 2.4Ghz or 5GHz.

Detect: Click the Detect button to scan.

AP List: This will list the transmitting channels and quality.



Stats Page

Ethernet Traffic Statistics

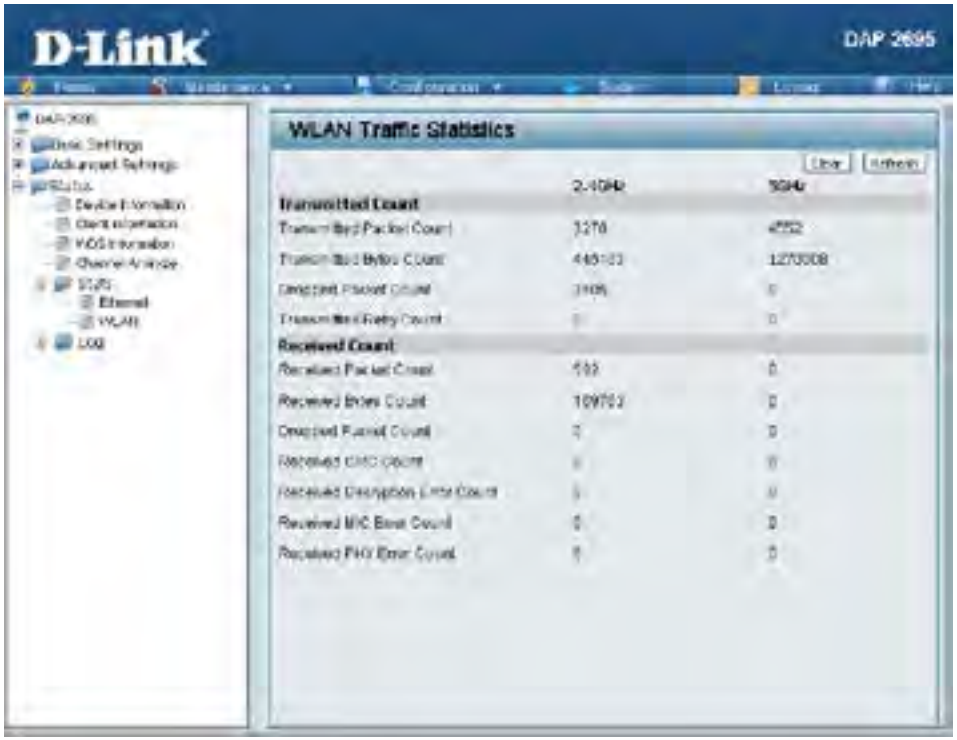
Displays wired interface network traffic information.

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

WLAN Traffic Statistics

Displays throughput, transmitted frame, received frame, and WEP frame error information for the AP network.

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

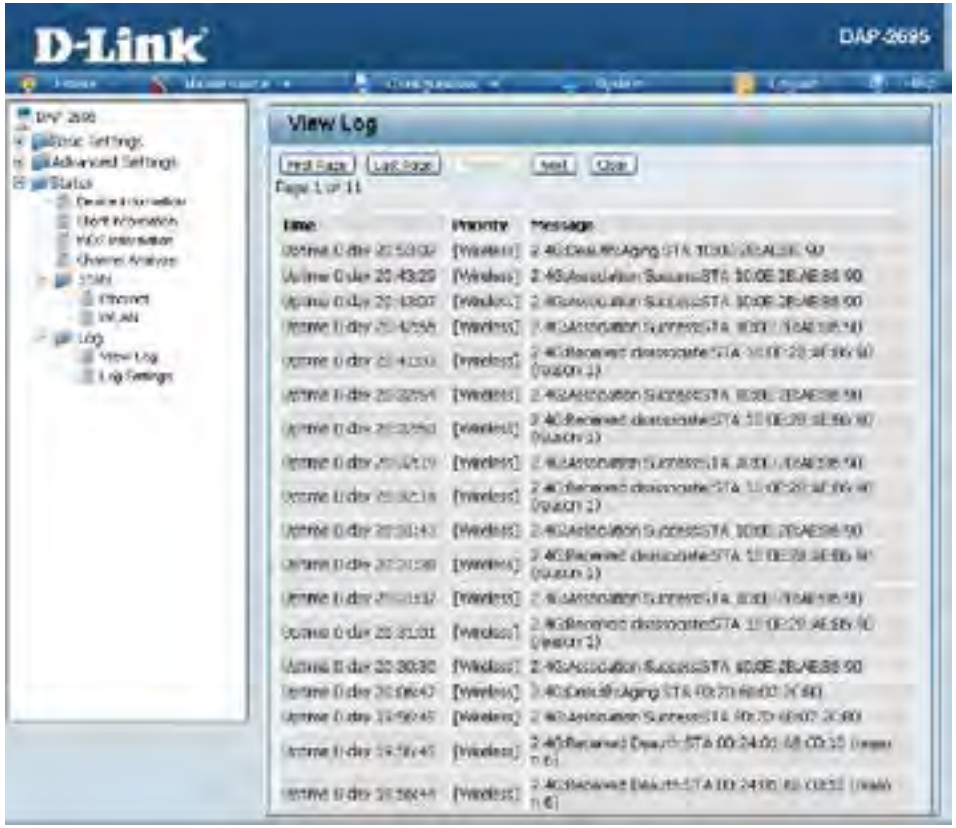


Log

View Log

The AP's embedded memory holds logs here. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.

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



Log Settings

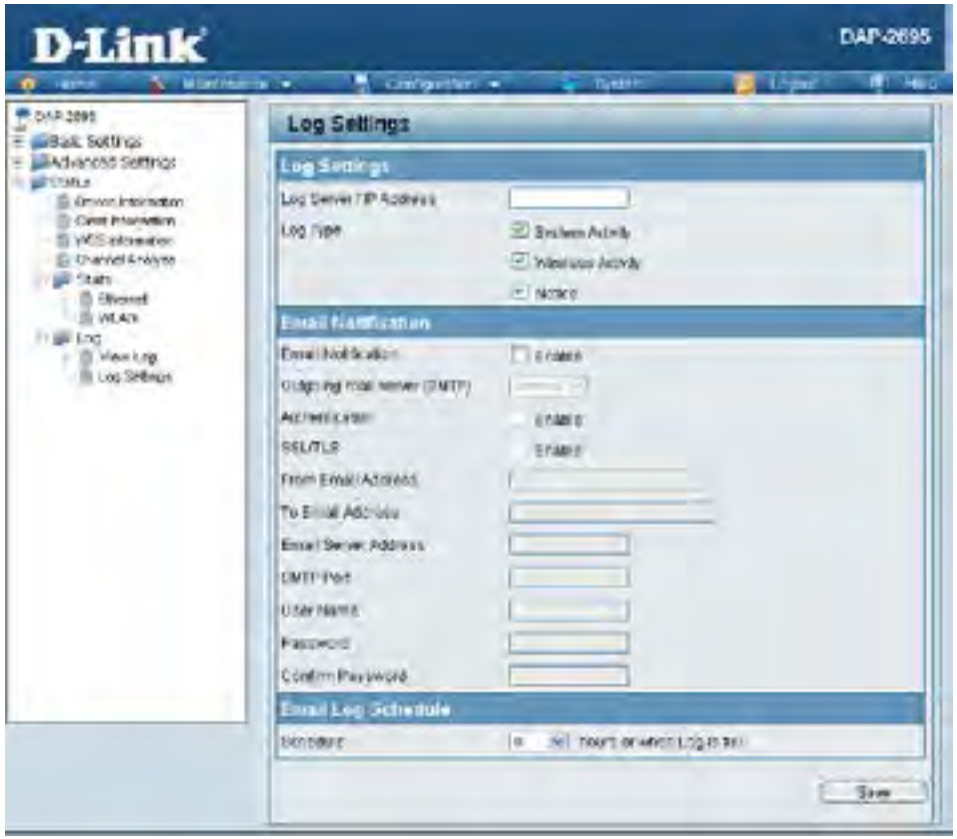
Enter the log server's IP address to send the log to that server. Check or uncheck System Activity, Wireless Activity, or Notice to specify what kind of log type you want it to log.

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-2660 log to.

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

E-mail Notification: Support Simple Mail Transfer Protocol for log schedule and periodical change key. It can not support Gmail SMTP port 465. Please set to Gmail SMTP port 25 or 587.

E-mail Log Schedule: Use the drop-down menu to set the e-mail log schedule.



Maintenance Section

In the Status Section the user can monitor and view configuration settings of the access point. Here the user can also view statistics about client information, WDS information and more. The following pages will explain settings found in the maintenance section in more detail.

Administration

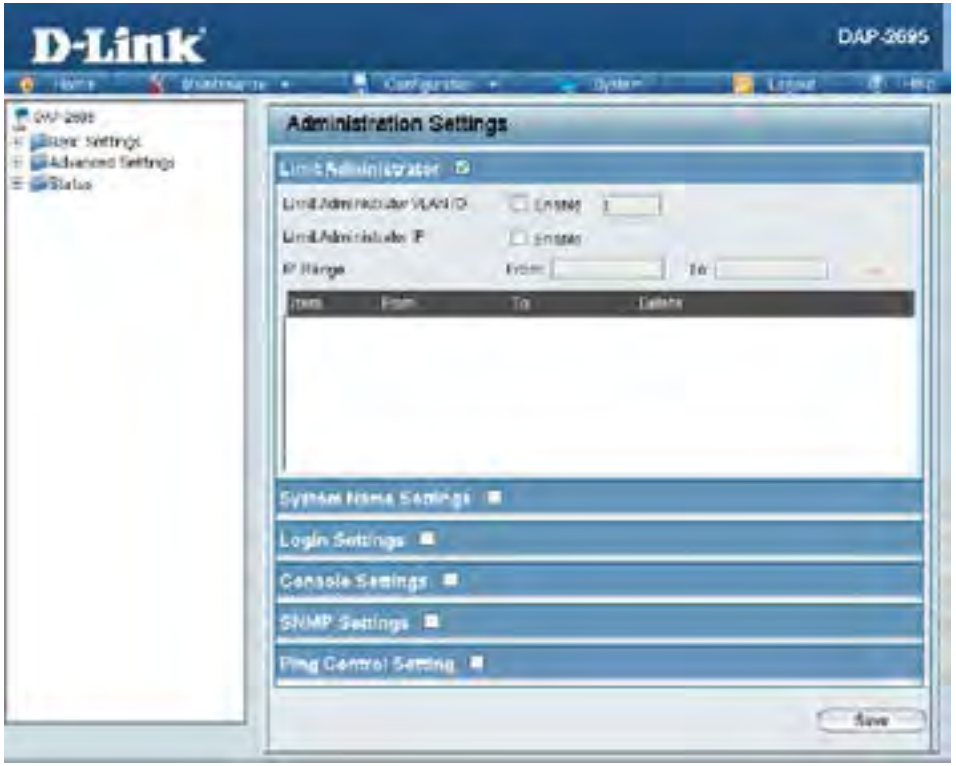
Limit Administrator

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

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

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

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



System Name Settings

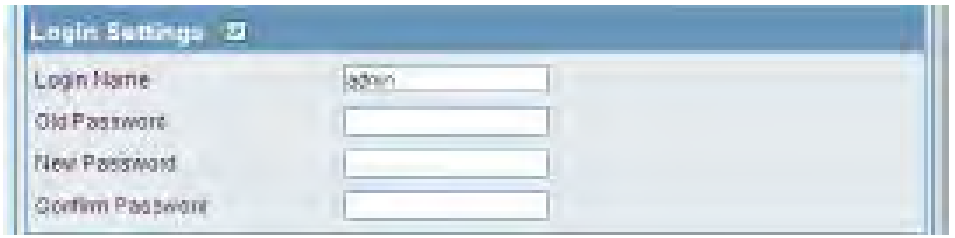
Each of the five main categories display various hidden administrator parameters and settings.

System Name: The name of the device. The default name is D-Link DAP-2660.

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

Login Settings

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



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

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

New Password: When changing your password, enter the new password here. The password is case-sensitive. "A" is a different character than "a." The length should be between 0 and 12 characters.

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

Console Settings

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

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

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

Time-out: Set to 1 Min, 3 Mins, 5 Mins, 10 Mins, 15 Mins or Never.

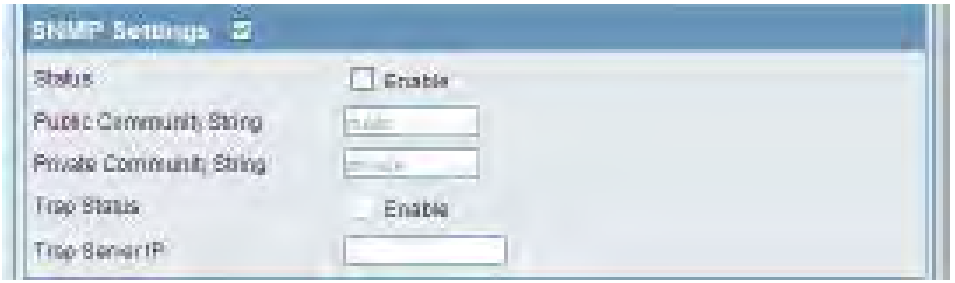
SNMP Settings

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

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

Public Community String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.



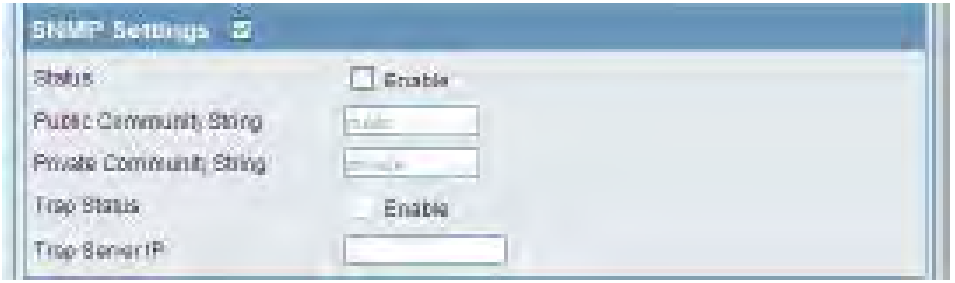
Central WiFiManager Settings

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

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

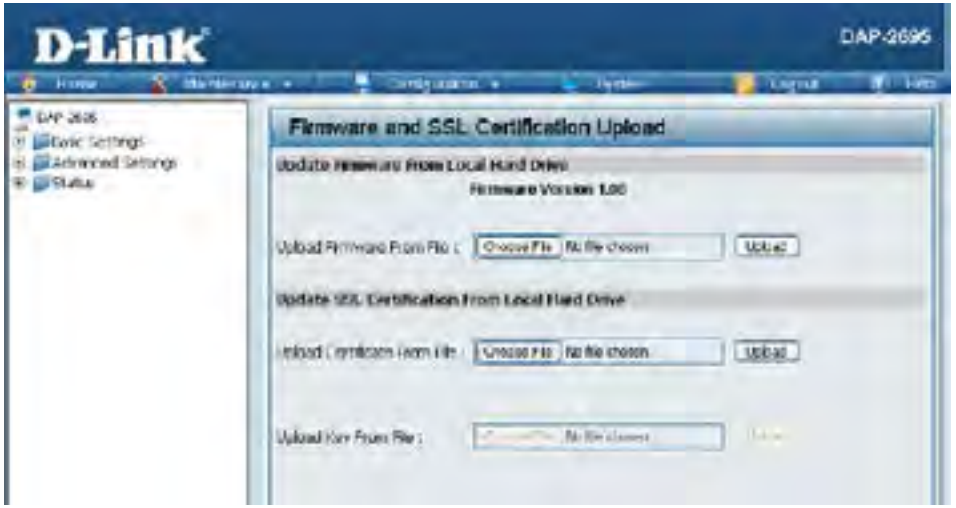
Enter the public SNMP community string.

Enter the private SNMP community string.



Firmware and SSL Upload

This page allows the user to perform a firmware upgrade. A Firmware upgrade is a function that upgrade the running software used by the access point. This is a useful feature that prevents future bugs and allows for new features to be added to this product. Please go to your local D-Link website to see if there is a newer version firmware available.



Firmware and SSL Certification Upload: You can upload files to the access point.

Upload Firmware from Local Hard Drive: The current firmware version is displayed above the file location field. After the latest firmware is downloaded, click on the "Choose File" button to locate the new firmware. Once the file is selected, click on the "Open" and "Upload" button to begin updating the firmware. Please don't turn the power off while upgrading.

Upload SSL Certification from Local Hard Drive: After you have downloaded a SSL certification to your local drive, click "Choose File." Select the certification and click "Open" and "Upload" to complete the upgrade.

Configuration File Upload

This page allows the user to backup and recover the current configuration of the access point in case of a unit failure.

Configuration File Upload and Download: You can upload and download configuration files of the access point.

Upload Configuration File: Browse to the saved configuration file you have in local drive and click "Open" and "Upload" to update the configuration.

Download Configuration File: Click "Download" to save the current configuration file to your local disk. Note that if you save one configuration file with the administrator's password now, after resetting your DAP-2660 and then updating to this saved configuration file, the password will be gone.

Time and Date Settings

Enter the NTP server IP, choose the time zone, and enable or disable daylight saving time.

Current Time: Displays the current time and date settings.

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

NTP Server: Enter the NTP server IP address.

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

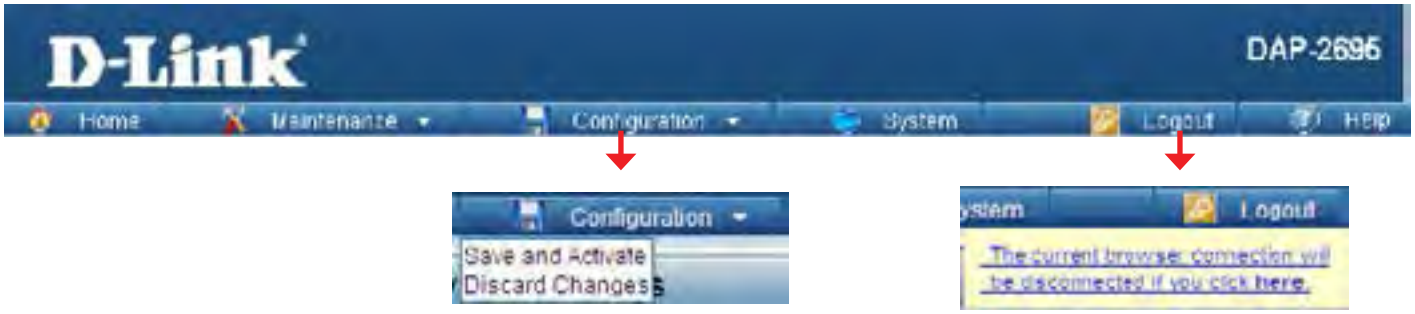
Enable Daylight Saving: Check the box to enable Daylight Saving Time.

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

Set the Date and Time Manually: A user can either manually set the time for the AP here, or click the Copy Your Computer's Time Settings button to copy the time from the computer in use (Make sure that the computer's time is set correctly).

Configuration and System

These options are the remaining option to choose from in the top menu. Configuration allows the user to save and activate or discard the configurations done. System allows the user to restart the unit, perform a factory reset or clear the language pack settings. Logout allows the user to safely log out from the access point's web configuration. Help allows the user to read more about the given options to configure without the need to consult the manual. The following pages will explain settings found in the configuration and system section in more detail.



System Settings

On this page the user can restart the unit, perform a factory reset of the access point or clear the added language pack.

Restart the Device: Click Restart to restart the DAP-2660.

Restore to Factory Default Settings: Click Restore to restore the DAP-2660 back to factory default settings.

Clear Language Pack: Click to clear the current Language pack running.

Help

The help page is useful to view a brief description of a function available on the access point in case the manual is not present.

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

Knowledge Base

Wireless Basics

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

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

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

People use WLAN technology for many different purposes:

- **Mobility** - productivity increases when people can have access to data in any location within the operating range of their WLAN. Management decisions based on real-time information can significantly improve the efficiency of a worker.
- **Low implementation costs** - WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLAN's ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.
- **Installation and network expansion** - by avoiding the complications of troublesome cables, a WLAN system can be fast and easy during installation, especially since it can eliminate the need to pull cable through walls and ceilings. Wireless technology provides more versatility by extending the network beyond the home or office.
- **Inexpensive solution** - wireless network devices are as competitively priced as conventional Ethernet network devices. The DAP-2660 saves money by providing users with multi-functionality configurable in four different modes.
- **Scalability** - Configurations can be easily changed and range from Peer-to-Peer networks, suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Wireless Installation Considerations

The D-Link 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 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
3. 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.
4. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on the range. Try to position access points, wireless routers, 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.
5. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
6. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2660. 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.)

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

When entering the IP address of the D-Link access point (192.168.0.50 for example), 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 a ROM chip in 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:
    - Internet Explorer 7.0 or higher, Chrome, Firefox, or Safari 4 or 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® 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.

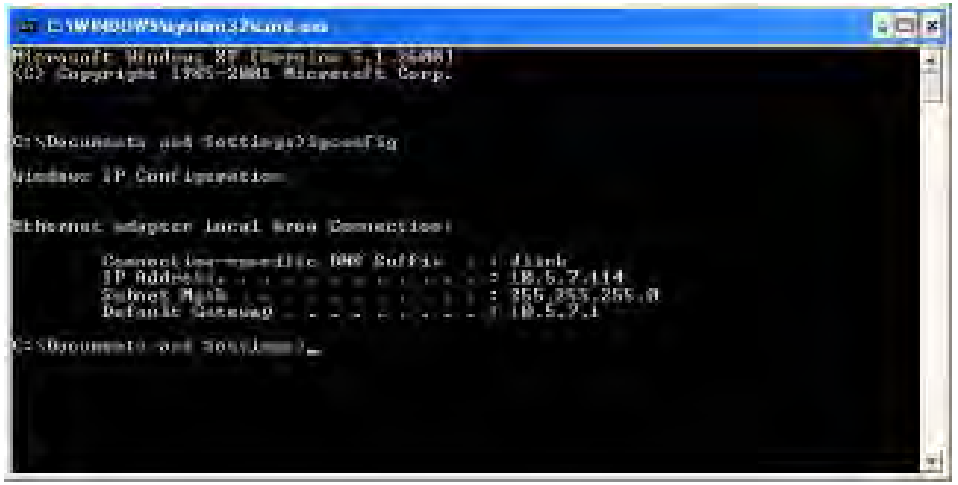
What can I do if I forgot my password?

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.

How to check your IP address?

After you install your network 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.

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.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

How to 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:

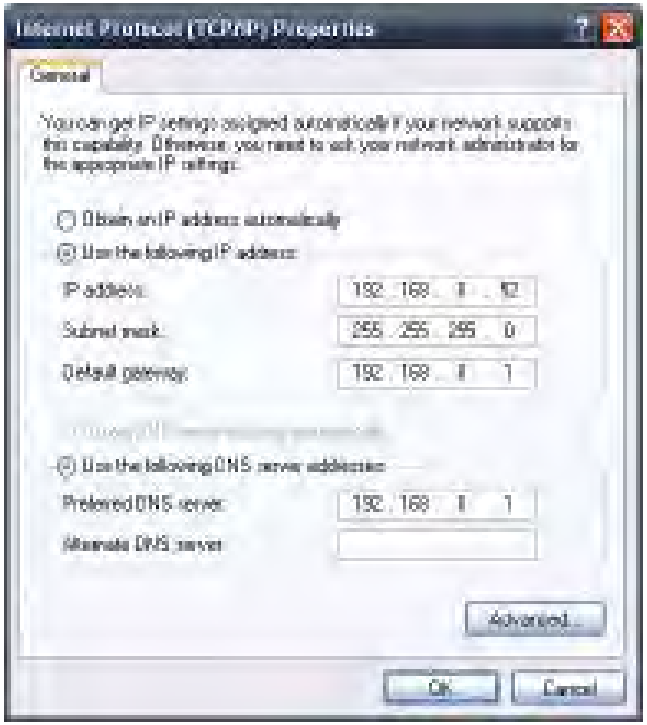
Step 1:
Windows® 2000: Click on Start > Settings > Control Panel > Network Connections
Windows XP: Click on Start > Control Panel > Network Connections
Windows Vista®: Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections

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.

Step 5:
Click OK twice to save your settings.



Technical Specifications

Standards
- IEEE 802.11ac (draft)
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3af
- IEEE 802.3at
- IEEE 802.3x

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

Security
- WPA™ Personal/Enterprise
- WPA2™ Personal/Enterprise
- WEP™ 64-/128-bit

Wireless Frequency Range
- 2.4 to 2.4835 GHz and 5.15 to 5.85 GHz**

Operating Voltage
- 48V DC +/- 10% for PoE or 48V/0.5A

Antenna Type
- 3x Detachable 4 dBi Omni antennas @2.4GHz
- 3x Detachable 6 dBi Omni antennas @5GHz

LEDs
- Power
- LAN1 (PoE)
- LAN2
- 2.4 GHz
- 5 GHz

Temperature
- Operating: 0˚C to 50˚C
- Storing: -20˚C to 65˚C

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

Certifications
- FCC Class B
- CE
- UL
- IC
- C-Tick
- CSA
- Wi-Fi

Dimensions
- L = 198.8 mm
- W = 190 mm
- H = 36.5 mm

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

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

FCC Caution:
Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.
If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted to indoor environments only.
Our products work well for channels 1-11 in the USA and Canada markets. It does not work well with other channels.

IMPORTANT NOTICE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.
The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.
For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

IC statement:
This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.
Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une
utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

NCC 警語

以下警語適用台灣地區

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
5.25-5.35 GHz頻帶內操作之無線資訊傳輸設備，限於室內使用

電磁波曝露量MPE標準值 1mW/cm2，送測產品實測值為：0.406275 mW/cm2