

# NUCLIAS CONNECT DAP-2620 User Guide

V 1.00

# Table of Contents

<b>Table of Contents</b> .....	<b>2</b>	LAN .....	23
<b>Nuclias Connect</b> .....	<b>4</b>	IPv6 .....	24
Introduction .....	4	Advanced Settings .....	25
Nuclias Connect Key Features.....	5	Performance .....	26
Package Contents.....	6	Wireless Resource Control .....	28
System Requirements .....	6	Multi-SSID .....	30
<b>Hardware Overview</b> .....	<b>7</b>	VLAN.....	33
LEDs.....	7	VLAN List .....	33
Connections .....	7	Port List.....	34
<b>Basic Installation</b> .....	<b>8</b>	Add / Edit VLAN .....	35
Hardware Setup .....	8	PVID Settings.....	36
Configure the Access Point .....	8	Intrusion.....	37
<b>Setup Wizard</b> .....	<b>10</b>	Schedule .....	38
<b>Web User Interface</b> .....	<b>11</b>	Internal RADIUS Server .....	39
Basic Settings .....	12	ARP Spoofing Prevention .....	40
Wireless Settings.....	12	Bandwidth Optimization .....	41
Access Point Mode .....	12	Captive Portal.....	43
WDS with AP Mode .....	14	Authentication Settings - Web Redirection Only	43
WDS Mode.....	16	Authentication Settings - Username/Password..	45
Wireless Client Mode .....	18	Authentication Settings - Passcode .....	47
Wireless Security .....	20	Authentication Settings - Remote RADIUS.....	49
Wired Equivalent Privacy (WEP) .....	20	Authentication Settings - LDAP .....	51
Wi-Fi Protected Access (WPA / WPA2) .....	21	Authentication Settings - POP3.....	53
		Login Page Upload .....	55
		MAC Bypass.....	56
		DHCP Server .....	57

Dynamic Pool Settings.....	57	Country Settings .....	80
Static Pool Settings .....	59	DDP Control Settings .....	80
Current IP Mapping List.....	60	Nuclias Connect Settings .....	80
Filters.....	61	Firmware and SSL Certification Upload.....	81
Wireless MAC ACL .....	61	Configuration File .....	82
WLAN Partition .....	62	Time and Date Settings .....	83
IP Filter Settings.....	63	Configuration.....	84
Traffic Control.....	64	System .....	85
Uplink/Downlink Settings .....	64	Logout .....	86
QoS.....	65	Help .....	87
Traffic Manager.....	66	<b>Knowledge Base .....</b>	<b>88</b>
Status .....	67	Wireless Basics .....	88
Device Information .....	68	Wireless Installation Considerations.....	89
Client Information .....	69	<b>Troubleshooting .....</b>	<b>90</b>
WDS Information .....	70	Why can't I access the web-based configuration utility?.....	90
Statistics .....	71	What can I do if I forgot my password? .....	91
Ethernet.....	71	How to check your IP address? .....	91
WLAN Traffic Statistics.....	72	How do I assign a static IP address?.....	92
Log .....	73	<b>Technical Specifications .....</b>	<b>93</b>
View Log.....	73	<b>Antenna Pattern .....</b>	<b>94</b>
Log Settings.....	74		
Maintenance .....	76		
Administration Settings .....	77		
Limit Administrator .....	78		
System Name Settings .....	78		
Login Settings .....	79		
Console Settings .....	79		
Ping Control Settings .....	79		
LED Settings.....	80		

# Nuclias Connect

## Introduction

Nuclias Connect is D-Link's centralized management solution for Small-to-Medium-Sized Business (SMB) networks. Nuclias Connect makes it easier to analyze, automate, configure, optimize, scale, and secure your network — delivering the convenience of an Enterprise-wide management solution, at an SMB price. Nuclias Connect gives you the financial and technical flexibility to expand from a small network to a larger one of up to 1,000 Access Points APs, while retaining a robust and centralized management system. With its intuitive Graphical User Interface (GUI), a wealth of enhanced AP features, and a setup wizard that supports 11 languages, Nuclias Connect minimizes the hassle of deployment, configuration, and administration tasks.

Deployable on a Windows server (or Linux via Docker), PC, or Smartphone (via lite management app) the Nuclias Connect free-to-download software is capable of managing up to 1,000 APs without licensing charges, coupled with an inexpensive optional hardware controller (DNH-100 Nuclias Connect Hub) suitable for remote locations. Through software-based monitoring and remote management of all wireless Access Points (APs) on your network, Nuclias Connect offers tremendous flexibility compared to traditional hardware-based unified management systems. Configuration can be done remotely. Network traffic analytics are available at a glance (in whole or in part). Load Balancing, Airtime Fairness, and Localized Throttling are enabled.

Nuclias Connect supports multi-tenancy, so network administrators can grant localized management authority for local networks. In addition, because APs can support 8 SSIDs per radio (16 SSIDs per dual band APs), administrators have the option of using one SSID to create a guest network for visitors.

Nuclias Connect provides direct AP discovery and provisioning when it shares the same Layer-2/Layer-3 network with a given AP, allowing users to find APs and import profiles with minimum effort, which can be applied as needed to groups or individual APs for even more effective configuration.

Since Nuclias Connect's software operates transparently on the network, an AP can be deployed anywhere in an NAT environment. Admins can provide and manage a variety of distributed deployments, including setting and admin account configuration for each deployment.

Nuclias Connect allows for multiple user authentications while enabling specific access control configurations for each SSID, giving admins the option of configuring separate internal networks for different subnets, while enabling more advanced Value-Added Services, such as Captive Portal or Wi-Fi Hotspot.

## Nuclias Connect Key Features

- Free-to-Download Management Software
- Searchable Event Log and Change Log
- License-Free Access Points
- Traffic Reporting & Analytics
- Authentication via Customizable Captive Portal, 802.1x and RADIUS Server, POP3, LDAP
- Backwards-Compatibility
- Remote Config. & Batch Config.
- Multilingual Support
- Intuitive Interface
- Multi-Tenant & Role-Based Administration
- Payment Gateway (Paypal) Integration and Front-Desk Ticket Management

For more information on how to use Nuclias Connect with DAP-2620, please refer to the Nuclias Connect User Guide.

## Package Contents

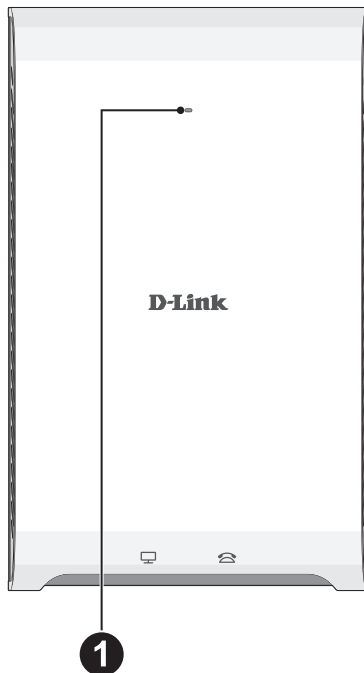
- DAP-2620 802.11ac Power over Ethernet (PoE) Access Point
- Mounting Brackets
- Quick Setup Guide

## System Requirements

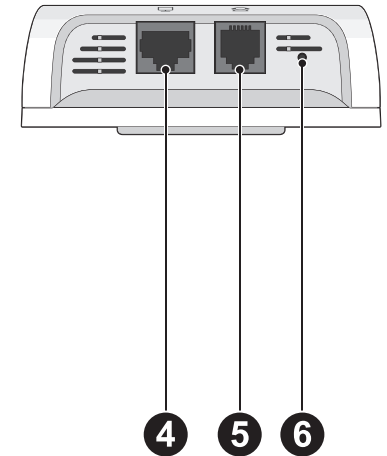
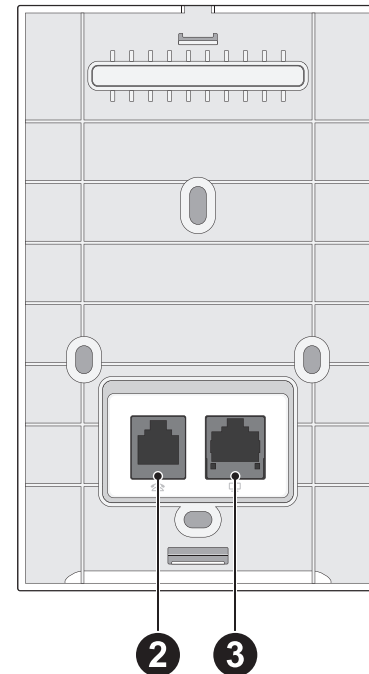
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer 11, Safari 7, Firefox 28, or Google Chrome 33 and above (for configuration)

# Hardware Overview

## LEDs



## Connections



No.	Item	LED Color	Description
1	Power/Status LED	Red (Flashing)	Indicates device booting up/device malfunctioned.
		Red (Solid)	Indicates the access point has malfunctioned.
		Green (Solid)	Indicates that the DAP-2620 is working properly.

No.	Item	Description
2	RJ11 Uplink Port	Connect to a Private Automatic Branch Exchange (PABX) or telephone line.
3	LAN (PoE) Port	Connect to a Power over Ethernet (PoE) switch via an Ethernet cable.
4	LAN Port	Connect to computer, IP cam or Set-Top Box
5	RJ11 Downlink Port	Connect to a phone via a phone cable.
6	Reset Button	Press and hold for 10 seconds to factory reset the device.

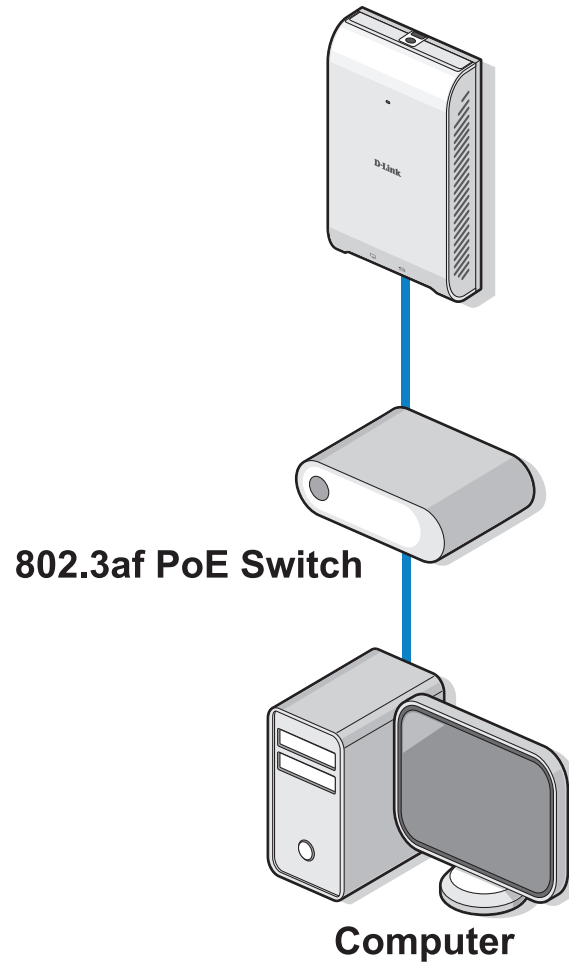
# Basic Installation

## Hardware Setup

To power on the DAP-2620, you can use the following method:

Plug in one end of your Ethernet cable into the LAN port of the DAP-2620's back panel, and the other end into the port on a switch.

### Configure the Access Point





To set up and manage the DAP-2620, use one of the following methods:

1. Connect the access point and your computer to the same PoE switch. Manage the access point from the computer.

Enter **dap2620.local** in the address field of your browser.

Log in to the Administration Web pages. The default login information is:

Username: admin

Password: admin

2. On your smart device, search for the Nuclias Connect app, or scan the QR codes below.



3. Download the Nuclias Connect app.
4. Open the Nuclias Connect app and follow the onscreen instructions to discover and setup your device.

# Setup Wizard

The first login instance displays the System Settings window which requires a change in password. Additional settings include the System Time and System Country functions.

After logging in to the user interface, fill in the New Password and Confirm New Password fields.

In the System Time function, select **Using Network Time Protocol (NTP)** or **Manually** to define the system time. If required, click the Daylight Saving Offset drop-down menu and select the value (minutes).

- Setting NTP System Time: Before trying to configure NTP check perform a ping test with the NTP server. In the NTP Server field, enter the NTP server to use. Then click the Time Zone drop-down menu and select the appropriate time zone.
- Setting System Time Manually: From the System Date drop-down menu, select the Year, Month, and Day along with the Hour and Minutes appropriate for the AP.
- Enable Daylight Saving: Click the radio button to enable the daylight savings time (DST) function. Set the DST start (24 hours) and end (24 hours) time by clicking on the drop-down menus and setting the Month, Week, Day, Hour, and Minute of the DST starting days.
- System Country: Click the drop-down menu to select the country.

Once the settings are configured, click the **Update** button to accept the configuration and proceed to the main interface menu page.

Provide system Settings...

**These settings apply to this access point**

New Password

Confirm new password

System Time  Using Network Time Protocol  
 Manually

System Date

System Time(24 HR)  :

Enable Daylight Saving

DST Start(24 HR)   in  at  :

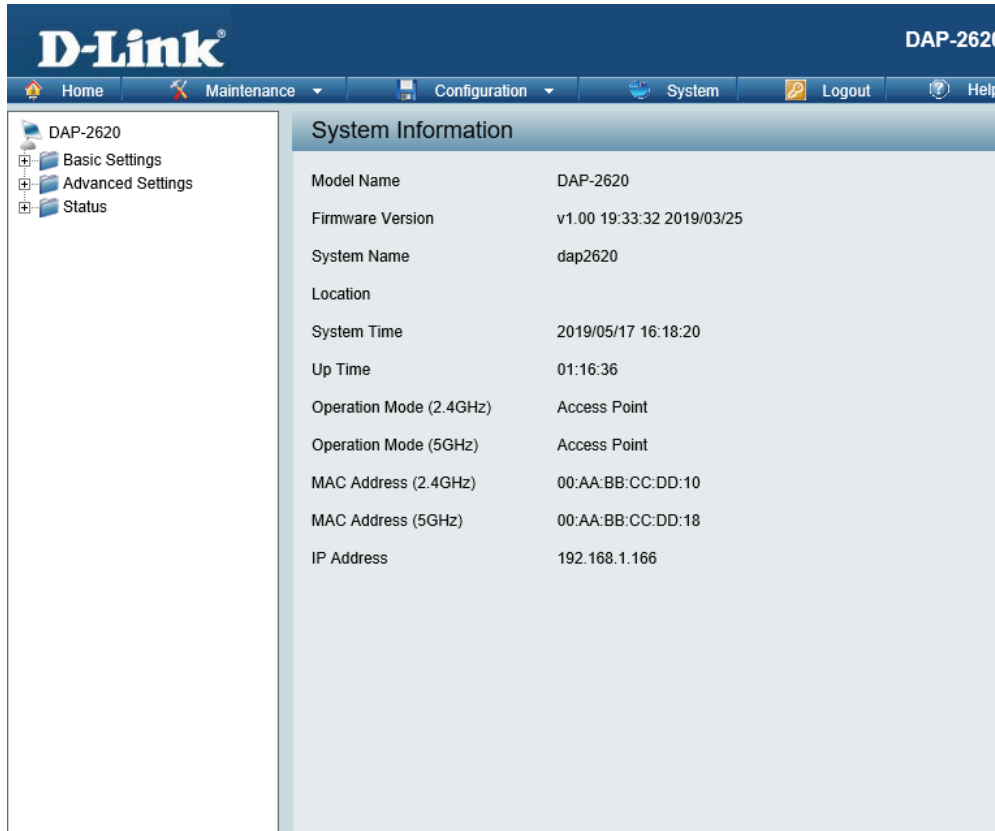
DST End(24 HR)   in  at  :

DST Offset(minutes)

System Country

# Web User Interface

The DAP-2620 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type **dap2620.local** in the address field and then press **Enter** to login. 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**.



The screenshot displays the D-Link DAP-2620 web user interface. The top navigation bar includes the D-Link logo, the device name "DAP-2620", and a menu with options: Home, Maintenance, Configuration, System, Logout, and Help. A left sidebar menu shows "DAP-2620" with sub-items: Basic Settings, Advanced Settings, and Status. The main content area is titled "System Information" and lists the following details:

Model Name	DAP-2620
Firmware Version	v1.00 19:33:32 2019/03/25
System Name	dap2620
Location	
System Time	2019/05/17 16:18:20
Up Time	01:16:36
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	00:AA:BB:CC:DD:10
MAC Address (5GHz)	00:AA:BB:CC:DD:18
IP Address	192.168.1.166

# Basic Settings

## Wireless Settings

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

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Operation Mode** Click the drop-down menu to select **Access Point**.

**Network Name (SSID)** Enter the name of Service Set Identifier (SSID) up to 32 characters and is case-sensitive.

**SSID Visibility** Click the drop-down menu to enable or disable broadcast the SSID across the network.

**Auto Channel Selection** Click the drop-down menu to enable automatically selects the channel that provides the best wireless performance. The channel selection process only occurs when the AP is booting up.

**Channel** Click the drop-down menu to select the desired channel. The function is only available when **Auto Channel Selection** is **Disable**.

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

The screenshot shows the 'Wireless Settings' configuration page. The settings are as follows:

- Wireless Band: 2.4GHz
- Operation Mode: Access Point
- Network Name (SSID): dlink
- SSID Visibility: Enable
- Auto Channel Selection: Enabled
- Channel: 6
- Channel Width: Auto 20/40 MHz
- Authentication: Open System
- Key Settings: Disable (selected)
- Encryption: Disable (selected)
- Key Type: ASCII
- Key Size: 64 Bits
- Key Index (1~4): 1
- Network Key: [Empty field]
- Confirm Key: [Empty field]

A 'Save' button is located at the bottom right of the form.

**Channel Width** Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. 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.

**Authentication** Click the drop-down menu to select **Open System**, **Shared Key**, **WPA-Personal**, **WPA-EAP**, or **802.1X**.

- Select **Open System** to communicate the key across the network (WEP).
- Select **Shared Key** to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.
- Select **WPA-Personal** to secure your network using a password and dynamic key changes. No RADIUS server is required.
- Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.
- Select **802.1X** if your network is using port-based Network Access Control.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## WDS with AP Mode

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Operation Mode** Click the drop-down menu to select **WDS with AP**.

**Network Name (SSID)** Enter the name of Service Set Identifier (SSID) up to 32 characters and is case-sensitive.

**Auto Channel Selection** This option is unavailable in WDS with AP mode.

**Channel** Click the drop-down menu to select the desired channel. The function is only available when **Auto Channel Selection** is **Disable**.

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

**Channel Width** Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. 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.

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

The screenshot shows the 'Wireless Settings' page. The 'Operation Mode' is set to 'WDS with AP'. The 'Network Name (SSID)' is 'dlinkwds'. 'Auto Channel Selection' is 'Enabled'. The 'Channel' is '6' and 'Channel Width' is 'Auto 20/40 MHz'. Under the 'WDS' section, the 'AP MAC Address' field is empty. A 'Site Survey' section contains a 'Scan' button. Below this is a table header with columns: Ch, Signal (%), MAC Address, Security, and SSID. A message below the header says 'You can click Scan button to start.' At the bottom, 'Authentication' is 'Open System', 'Key Settings' has 'Disable' selected, and 'Key Type' is 'ASCII' with 'Key Size' set to '64 Bits'.

**Authentication** Click the drop-down menu to select **Open System**, or **WPA-Personal**.

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

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## WDS Mode

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Operation Mode** Click the drop-down menu to select **WDS**.

**Network Name (SSID)** Enter the name of Service Set Identifier (SSID) up to 32 characters and is case-sensitive.

**Auto Channel Selection** This option is unavailable in WDS mode.

**Channel** Click the drop-down menu to select the desired channel. The function is only available when **Auto Channel Selection** is **Disable**.

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

**Channel Width** Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. 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.

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

**Wireless Settings**

Wireless Band: 2.4GHz

Operation Mode: WDS

Network Name (SSID): dlinkwds

Auto Channel Selection: Enabled

Channel: 6

Channel Width: Auto 20/40 MHz

WDS

AP MAC Address: [Empty]

Site Survey

Scan

Ch	Signal (%)	MAC Address	Security	SSID
You can click Scan button to start.				

Authentication: Open System

Key Settings

Encryption:  Disable  Enable

Key Type: ASCII Key Size: 64 Bits



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

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

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Wireless Client Mode

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Operation Mode** Click the drop-down menu to select **Wireless Client**.

**Network Name (SSID)** Enter the name of Service Set Identifier (SSID) up to 32 characters and is case-sensitive.

**SSID Visibility** This option is unavailable in Wireless Client mode.

**Auto Channel Selection** Click the drop-down menu to select the desired channel. The function is only available when **Auto Channel Selection** is **Disable**.

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

**Channel** The channel used will be displayed, and matches the AP that the DAP-2620 is connected to when set to Wireless Client mode.

**Channel Width** Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. 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.

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

**Authentication** Will be explained in the next topic.

**Enable** Check the box to enable the Wireless MAC Clone function.

**MAC Source** Click the drop-down menu to select **Auto** or **Manual**.

**Wireless Settings**

Wireless Band: 2.4GHz

Operation Mode: Wireless Client

Network Name (SSID):

SSID Visibility: Enable

Auto Channel Selection: Enabled

Channel: 6

Channel Width: Auto 20/40 MHz

Site Survey: Scan

Ch	Signal (%)	MAC Address	Security	SSID
You can click Scan button to start.				

Authentication: Open System

Key Settings

Encryption:  Disable  Enable

Key Type: ASCII Key Size: 64 Bits

Key Index (1-4): 1

**MAC Address** When **MAC Source** is set to **Manual**, click **Scan** to find the MAC address to clone.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Wireless Security

Wireless security is a key concern for any wireless network installed. Unlike any other networking method wireless networks will broadcast its 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.

### Wired Equivalent Privacy (WEP)

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.
- **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.

**Encryption** Click the radio button to disable or enable encryption.

**Key Type** Click the drop-down menu to select **HEX\*** or **ASCII\*\***.

**Key Size** Click the drop-down menu to select **64 Bits** or **128 Bits**.

**Key Index (1~4)** Click the drop-down menu to select the 1st through the 4th key to be the active key.

**Network Key** Input the characters which will define the network key.

**Confirm Key** Re-enter the value as entered in the Network Key to confirm the setting.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

\* Hexadecimal (HEX) digits consist of the numbers 0-9 and the letters A-F.

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

The screenshot shows the 'Wireless Settings' configuration page. The settings are as follows:

- Wireless Band: 2.4GHz
- Operation Mode: Access Point
- Network Name (SSID): dlink
- SSID Visibility: Enable
- Auto Channel Selection: Enabled
- Channel: 6
- Channel Width: Auto 20/40 MHz
- Authentication: Open System
- Key Settings:
  - Encryption:  Disable  Enable
  - Key Type: ASCII
  - Key Size: 64 Bits
  - Key Index (1~4): 1
  - Network Key: [Empty text box]
  - Confirm Key: [Empty text box]

At the bottom right, there is a 'Save' button. Below the confirm key field, there is a character set restriction: (0-9,a-z,A-Z,~!@#%&\*\_+~=-{}|:~!<=>?)

## Wi-Fi Protected Access (WPA / WPA2)

The WPA protocol is based on the 802.11i standard. WPA offers two variations called WPA-Personal (PSK) and WPA-Enterprise (EAP). WPA-EAP requires the user to install a Radius Server on the network for authentication, while WPA-Personal does not. In comparison, WPA-PSK is seen as a weaker authentication variation than WPA-EAP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

WPA2 is an upgrade of WPA and solves security issues found in WPA. WPA2 also offers two variations called WPA2-Personal (PSK) and WPA2-Enterprise (EAP) similar to WPA.

**WPA Mode** When **Authentication** setting is set to **WPA-Personal**, click the drop-down menu to select one of the following: **Auto (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**.

Auto (WPA or WPA2) allows the device to select either setting to match the client configuration.

**Cipher Type** Click the drop-down menu to select the cipher type for the WPA setting, type: **Auto**, **AES**, or **TKIP**.

**Group Key Update Interval** Enter the interval period in seconds in which the interval period is valid.

**Encryption key** Select the method to define the cipher type encryption key: **Manual** or **Periodical Key Change**.

- **Manual:** Enter the PassPhrase encryption key. The minimum and maximum number of characters is 8 to 63 ASCII characters and 64 characters in HEX. In the Confirm PassPhrase field enter the same key to confirm.
- **Periodical Key Change:** Select the option to have each client negotiate an unique encryption key between the client and the access point.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

The screenshot displays the 'Wireless Settings' configuration interface. Key settings include:

- Wireless Band:** 2.4GHz
- Operation Mode:** Access Point
- Network Name (SSID):** dlink
- SSID Visibility:** Enable
- Auto Channel Selection:** Enabled
- Channel:** 6
- Channel Width:** Auto 20/40 MHz
- Authentication:** WPA-Personal
- PassPhrase Settings:**
  - WPA Mode:** AUTO (WPA or WPA2)
  - Cipher Type:** Auto
  - Group Key Update Interval:** 3600 (Sec)
  - Time Interval:** 1 (1~168)hour(s)
- PassPhrase:** [Empty field]
- Confirm PassPhrase:** [Empty field]

Notice: 8~63 in ASCII or 64 in Hex.  
(0-9,a-z,A-Z,~!@#%&\*()\_+~=-{}|:~",./<>?)

Save

**WPA Mode** When **Authentication** setting is set to **WPA-EAP**, click the drop-down menu to select one of the following: **Auto (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**.

Auto (WPA or WPA2) allows the device to select either setting to match the client configuration.

**Cipher Type** Click the drop-down menu to select the cipher type for the WPA setting, type: **Auto**, **AES**, or **TKIP**.

**Group Key Update Interval** Enter the interval period in seconds in which the interval period is valid.

**RADIUS Server** Enter the IP address of the RADIUS server to be used to authenticate.

**Radius Port** Enter the RADIUS port.

**RADIUS Secret** Enter the shared secret to be used between the radius server and the DAP to authenticate.

**Accounting Mode** Click the drop-down menu to enable or disable the accounting mode.

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

**Accounting Port** Enter the accounting port.

**Accounting Secret** Enter the accounting secret.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## 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-2620. 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** Click the drop-down menu to select IP address setting mode.

- **Static IP (Manual):** Select this setting to assign a static IP address to the device.
- **Dynamic IP (DHCP):** Select this setting to obtain an IP address from a DHCP server on the network.

**IP Address** Enter the IP address to assign a static IP address

**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.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

The screenshot shows the 'LAN Settings' configuration page. It features a title bar 'LAN Settings' and a list of configuration items, each with a text input field:

- Get IP From:** A dropdown menu currently set to 'Dynamic IP (DHCP)'.
- IP Address:** A text box containing '192.168.1.166'.
- Subnet Mask:** A text box containing '255.255.255.0'.
- Default Gateway:** A text box containing '192.168.1.1'.
- DNS:** A text box containing '192.168.1.201'.

A 'Save' button is positioned at the bottom right of the form area.

## IPv6

**Enable IPv6** Check to enable the IPv6.

**Get IP From** Click the drop-down menu to select IPv6 address setting mode.

- **Auto:** Choose this option the DAP-2620 can get IPv6 address automatically. The other fields will be grayed out.
- **Static:** to set IPv6 address manually.

**IP Address** Enter the LAN IPv6 address used.

**Prefix** Enter the LAN subnet prefix length value used.

**Default Gateway** Enter the LAN default gateway IPv6 address used.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.



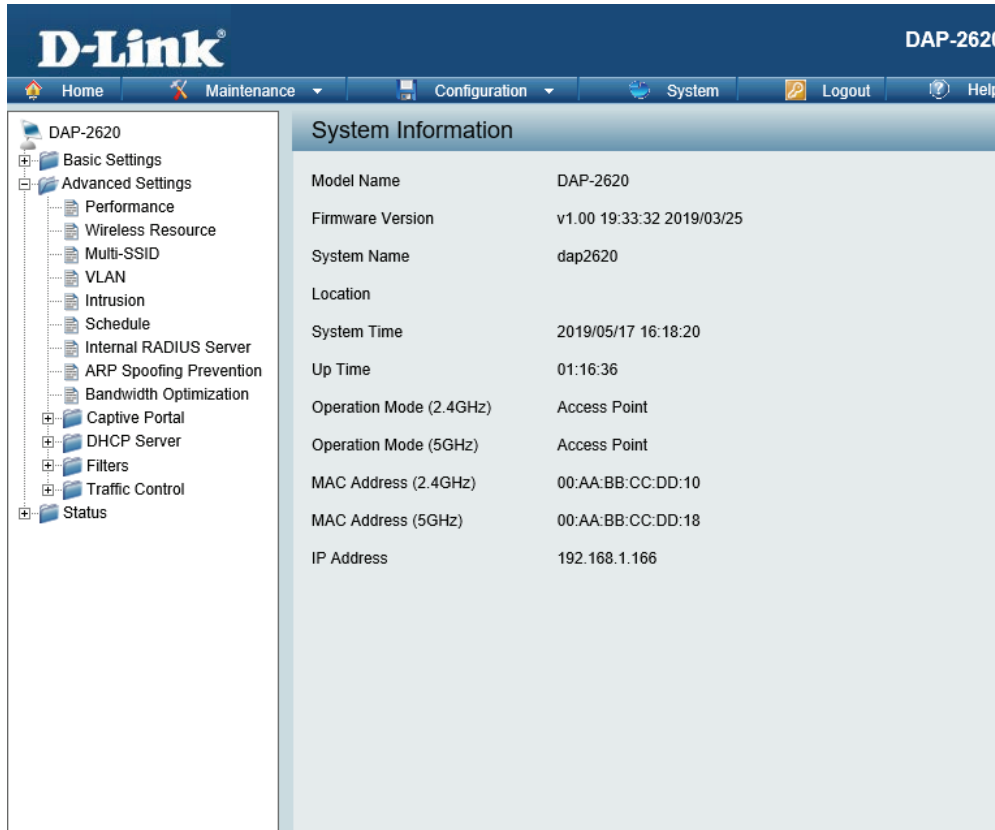
The screenshot shows the 'IPv6 Settings' configuration page. It features a header 'IPv6 Settings' and a 'Save' button. The settings include:

- Enable IPv6
- Get IP From: Auto (dropdown menu)
- IP Address: [text input field]
- Prefix: [text input field]
- Default Gateway: [text input field]



# Advanced Settings

In the Advanced Settings Section the user can configure advanced settings concerning Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Captive Portal, DHCP Server, Filters and Traffic Control. The following pages will explain settings found in the Advanced Settings section in more detail.



The screenshot displays the D-Link DAP-2620 Web User Interface. The top navigation bar includes the D-Link logo, the model name "DAP-2620", and menu items for Home, Maintenance, Configuration, System, Logout, and Help. A left-hand navigation tree shows the following structure:

- DAP-2620
  - Basic Settings
  - Advanced Settings
    - Performance
    - Wireless Resource
    - Multi-SSID
    - VLAN
    - Intrusion
    - Schedule
    - Internal RADIUS Server
    - ARP Spoofing Prevention
    - Bandwidth Optimization
  - Captive Portal
  - DHCP Server
  - Filters
  - Traffic Control
  - Status

The main content area is titled "System Information" and displays the following details:

Model Name	DAP-2620
Firmware Version	v1.00 19:33:32 2019/03/25
System Name	dap2620
Location	
System Time	2019/05/17 16:18:20
Up Time	01:16:36
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	00:AA:BB:CC:DD:10
MAC Address (5GHz)	00:AA:BB:CC:DD:18
IP Address	192.168.1.166

## Performance

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

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Wireless** Click the drop-down menu to enable or disable the wireless function.

**Wireless Mode** Click the drop-down menu to select the wireless mode.

- 2.4GHz band supports: **Mixed 802.11b, 802.11g, 802.11n; Mixed 802.11b, 802.11g; and 802.11n Only.**
- 5GHz band supports: **Mixed 802.11n, 802.11a; 802.11a Only; 802.11n Only; and Mixed 802.11ac.**

Please note that when backwards compatibility is enabled for legacy (802.11a/g/b) clients, degradation of 802.11n wireless performance is expected.

**Data Rate\*** When **Wireless Mode** is set to **Mixed 802.11b, 802.11g** (for 2.4GHz) and **802.11a Only** (for 5GHz), click the drop-down menu to indicate the base transfer rate of wireless adapters on the wireless LAN. The AP will adjust the base transfer rate depending on the base rate of the connected device. If there are obstacles or interference, the AP will derate the transfer rate.

**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.

Performance Settings	
Wireless Band	2.4GHz
Wireless	On
Wireless Mode	Mixed 802.11b, 802.11g, 802.11n
Data Rate	Best(Up to 300) Mbps
Beacon Interval (40-500)	100
DTIM Period (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out	64 (μs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable Mbps
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT 20/40 Coexistence	Enable
Transfer DHCP Offer to Unicast	Disable
STP (Spanning tree)	Disable

Save

- DTM Interval (1-15)** Select a Delivery Traffic Indication Message 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** Use the drop-down menu to 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.
- WMM (Wi-Fi Multimedia)** This function is available for Mixed 802.11g and 802.11b in 2.4GHz and 802.11a Only in 5GHz wireless bands. Click the drop-down menu to enable or disable the WMM function. WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.
- Ack Time Out** To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 25 and 200 microseconds for 5GHz or between 48 and 200 microseconds in the 2.4GHz in the field provided.
- Short GI** Click the drop-down menu to enable or disable the short GI function. Enabling a short guard interval can increase throughput. However, be aware that it can also increase the error rate in some installations due to increased sensitivity to radio-frequency installations.
- IGMP Snooping** Click the drop-down menu to enable or disable the IGMP Snooping function. Internet Group Management Protocol allows the AP to recognize IGMP queries and reports sent between routers and an IGMP host (wireless STA). When IGMP snooping is enabled, the AP will forward multicast packets to an IGMP host based on IGMP messages passing through the AP.
- Multicast Rate** Click the drop-down menu to select the multicast rate to adjust multicast packet data rates.
- Multicast Bandwidth Control** Adjust the multicast packet data rate. The multicast rate is supported in AP mode, (2.4GHz and 5GHz) and WDS with AP mode, including Multi-SSIDs.
- Maximum Multicast Bandwidth** Set the multicast packets maximum bandwidth pass through rate from the Ethernet interface to the Access Point. The function is only available when **Multicast Bandwidth Control** is **Enable**.
- HT20/40 Coexistence** Click the drop-down menu to enable the function to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel over-lapping and causing interference, the Access Point will automatically change to 20 MHz.
- Transfer DHCP Offer to Unicast** Click the drop-down menu to enable the function to transfer the DHCP Offer to Unicast from LAN to WLAN, suggest to enable this function if stations number is larger than 30.
- STP (Spanning tree)** Click the drop-down menu to enable the spanning tree function.
- Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Wireless Resource Control

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.

**Airtime Fairness** Click the drop-down menu to enable or disable the airtime fairness function.

**Band Steering** Click the drop-down menu to enable the Band Steering function. When the wireless clients support both 2.4GHz and 5GHz and the 2.4GHz signal is not strong enough, the device will use 5GHz as higher priority.

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Connection Limit** Click the drop-down menu to enable or disable the connection limit function. The option is for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled 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-2620 will not allow clients to associate with the AP.

**User Limit (1 - 64)** This function is only available when Connection Limit is enabled. Set the maximum amount of users that are allowed access (1 - 64 users) to the device using the specified wireless band.

**11n Preferred** This function is only available when Connection Limit is enabled. Use the drop-down menu to enable the 11n Preferred function. The wireless clients with 802.11n protocol will have higher priority to connect to the device.

The screenshot shows the 'Wireless Resource Control' configuration window. It contains the following settings:

Setting	Value
Airtime Fairness	Disable
Bandsteering	Disable
Wireless Band	2.4GHz
Connection Limit	Disable
User Limit (0 - 64)	20
11n Preferred	Disable
Network Utilization	100%
Aging out	Disable
RSSI Threshold	100%
Data Rate Threshold	54
ACL RSSI	Disable
ACL RSSI Threshold	60%

A 'Save' button is located at the bottom right of the window.

- Network Utilization** Click the drop-down menu to set the maximum utilization of this access point for service. The DAP-2620 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. 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.
- RSSI Threshold** When **Aging out** is **RSSI**, click the drop-down menu to select the percentage of RSSI. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients. The function is only available when **Aging out** is **RSSI**.
- Data Rate Threshold** When **Aging out** is **Data Rate**, click the drop-down menu to select the threshold of data rate. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients. The function is only available when **Aging out** is **Data Rate**.
- ACL RSSI** Click the drop-down menu to enable the ACL RSSI function. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.
- ACL RSSI Threshold** Click the drop-down menu to set the ACL RSSI Threshold.
- Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Multi-SSID

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

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

**Enable Priority** Check to enable the **Priority** function.

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

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

**SSID** This function is only available when Index is not set to Primary SSID. Enter the Service Set Identifier (SSID) designated for a specific wireless local area network (WLAN). The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

**SSID Visibility** This function is only available when Index is not set to Primary SSID. Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

**Security** This function is only available when Index is not set to Primary SSID. Click the drop-down menu to select the security encryption, options include: WPA-Personal, WPA-EAP, or 802.1X.

**Priority** This function is only available when Enable Priority is selected. Click the drop-down menu to select the priority level of the SSID selected. The function is only available when **Enable Priority** is checked.

**Multi-SSID Settings**

Enable Multi-SSID       Enable Priority

**Wireless Settings**

Band: 2.4GHz

Index: Primary SSID

SSID: dlink

SSID Visibility: Enable

Security: Open System

Priority: 0

WMM (Wi-Fi Multimedia): Enable

**Key Settings**

Encryption:  Disable     Enable

Key Type: ASCII    Key Size: 64 Bits

Key Index (1~4): 1

Network Key:

Confirm Key:

(0-9,a-z,A-Z,~!@#\$\$%^&\*()\_+\*=00;:;,./<>?)

Add

Index	SSID	Band	Authentication Method	Encryption Type	Delete
-------	------	------	-----------------------	-----------------	--------

- WMM (Wi-Fi Multimedia)** This function is only available when WMM under Performance Settings is enabled. Click the drop-down menu to enable or disable the WMM function. WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.
- Encryption** This function is only available when multi-SSID is enabled and Index is an SSID other than Primary SSID. Click the radio button to enable or disable the encryption. If **Enable** is selected the following configurations are required: Key Type, Key Size, Key Index (1~4), Network Key, and Confirm Key.
- Key Type** Click the drop-down menu to select **HEX** or **ASCII**.
- Key Size** Click the drop-down menu to select **64 Bits** or **128 Bits**.
- Key Index (1~4)** Click the drop-down menu to select from the 1st to 4th key to be set as the active key.
- Network Key** Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.
- Confirm Key** Re-enter the value as entered in the Network Key to confirm the setting.
- WPA Mode** When **Security** setting is set to **WPA-Personal** or **WPA-EAP**, click the drop-down menu to select a WPA mode [Options: Auto (WPA or WPA2), WPA2 Only, or WPA1 Only]. Auto (WPA or WPA2) allows you to use both WPA and WPA2. In addition, you must configure Cipher Type, and Group Key Update Interval.
- Cipher Type** When **Security** is **WPA-Personal** or **WPA-EAP**, click the drop-down menu to select **Auto**, **AES**, or **TKIP**.
- Group Key Update Interval** Enter the interval during which the group key will be valid.
- Encryption key** Select the means to define a unique encryption key for the defined cipher type.
- **Manual:** Select the manual option to define the PassPhrase encryption key. The minimum and maximum number of characters is 8 to 63 ASCII characters and 64 characters in HEX. In the Confirm PassPhrase field enter the same key to confirm the setting.
  - **Periodical Key Change:** Select the option to have each client negotiate a very unique encryption key between the client and the access point.
- Time Interval** Enter the variable in hours to set the interval.
- PassPhrase** When **Security** is set to **WPA-Personal**, enter a pass phrase in the corresponding field.
- Confirm PassPhrase** Retype the Pass Phrase entry to confirm the Pass Phrase.
- RADIUS Server** When **Security** is set to **WPA-EAP**, enter the IP address of the RADIUS server.
- Radius Port** Enter the RADIUS port.
- RADIUS Secret** Enter the RADIUS secret.
- Accounting Mode** Click the drop-down menu to enable or disable the accounting mode.
- Accounting Server** Enter the IP address of the accounting server.

**Accounting Port** Enter the accounting port.

**Accounting Secret** Enter the accounting secret.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.



# VLAN

## VLAN List

The DAP-2620 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-2620 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

**VLAN Status** Click the radio button to enable or disable VLAN status. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the VLAN List tab.

**VLAN Status** Displays the current VLAN status.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

**VID** Displays the VID of the VLAN.

**VLAN Name** Displays the name of the VLAN.

**Untag VLAN Ports** Displays the untagged ports.

**Tag VLAN Ports** Displays the tagged ports.

**Edit** Click **Edit** to edit the current VLAN.

**Delete** Click **Delete** to delete the current VLAN.

**VLAN Settings**

VLAN Status :  Disable  Enable Save

VLAN Status : Static(2.4G), Static(5G)

**VLAN List** | Port List | Add/Edit VLAN | PVID Setting

VID	VLAN Name	Untag VLAN Ports	Tag VLAN Ports	Edit	Delete
1	default	Mgmt, LAN1, LAN2, Primary (2.4G), S-1(2.4G), S-2(2.4G), S-3(2.4G), S-4(2.4G), S-5 (2.4G), S-6(2.4G), S-7(2.4G),	Primary(5G), S-1(5G), S-2 (5G), S-3(5G), S-4(5G), S-5 (5G), S-6(5G), S-7(5G)	<span>Edit</span>	<span>Delete</span>

## 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** Click the radio button to enable or disable VLAN status. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the VLAN List tab.

**VLAN Mode** Displays the current VLAN mode.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

**Port Name** Displays the name of the port.

**Tag VID** Displays the tagged VID of the port.

**Untag VID** Displays the untagged VID of the port.

**PVID** Displays the PVID of the port.

**VLAN Settings**

VLAN Status :  Disable  Enable Save

VLAN Status : Static(2.4G), Static(5G)

VLAN List **Port List** Add/Edit VLAN PVID Setting

Port Name	Tag VID	Untag VID	PVID
Mgmt	1	1	1
LAN1	1	1	1
LAN2	1	1	1
Primary(2.4G)	1	1	1
Primary(5G)	1	1	1
S-1(2.4G)	1	1	1
S-2(2.4G)	1	1	1
S-3(2.4G)	1	1	1
S-4(2.4G)	1	1	1
S-5(2.4G)	1	1	1
S-6(2.4G)	1	1	1
S-7(2.4G)	1	1	1
S-1(5G)	1	1	1
S-2(5G)	1	1	1
S-3(5G)	1	1	1
S-4(5G)	1	1	1
S-5(5G)	1	1	1
S-6(5G)	1	1	1
S-7(5G)	1	1	1

## Add / Edit VLAN

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

**VLAN Status** Click the radio button to enable or disable VLAN status. By default this feature is disabled.

**VLAN Mode** Displays the current VLAN mode.

**VLAN ID** Enter a value (1-4094) for the Internal VLAN.

**VLAN Name** Enter the VLAN name to add or modify.

**Save** Click to save the updated configuration.  
To make the updates permanent, click **Configuration > Save and Activate**.

From the Port fields, select the radio button to set Untag/Tag/Not Member settings to the Mgmt (management) and LAN ports. The port configuration functions are also available for the defined 2.4GHz and 5GHz ports.

Untagged ports are used for connecting to client devices, such as a computer host. While tagged ports are designated for VLAN trunk links.

VLAN Settings

VLAN Status :  Disable  Enable Save

VLAN Status : Static(2.4G), Static(5G)

VLAN List | Port List | **Add/Edit VLAN** | PVID Setting

VLAN ID (VID)  VLAN Name

Port	Select All	Mgmt	LAN1	LAN2
Untag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.4GHz

MSSID Port	Select All	Primary S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5GHz

MSSID Port	Select All	Primary S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 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 **Save** for the changes to take effect.

**VLAN Status** Click the radio button to enable or disable VLAN status. By default this feature is disabled.

**VLAN Mode** Displays the current VLAN mode.

**PVID Auto Assign Status** Click the radio button to enable or disable PVID auto assign status.

For each untagged port, set the PVID of the port to its assigned VLAN ID. For example, if ports 1, 2, 3, 4, and 5 are untagged members of VLAN 10, ports 1, 2, 3, 4, and 5 would be configured with a PVID of 10.

For better system consistency, the following are recommended:

- set MSSID ports S1 and S2 to 16 and 17, respectively
- set switch port trunk native VLAN 1 for trunk port 1

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

**VLAN Settings**

VLAN Status :  Disable  Enable Save

VLAN Status : Static(2.4G), Static(5G)

VLAN List | Port List | Add/Edit VLAN | **PVID Setting**

PVID Auto Assign Status  Disable  Enable

Port	Mgmt	LAN1	LAN2
PVID	1	1	1

2.4GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

5GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1

Save

## Intrusion

The Wireless Intrusion Protection window is used to classify APs as Valid, Neighborhood, Rogue, or a New group. Click **Save** for the changes to take effect.

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Detect** Click **Detect** to initiate a scan of the network.

**AP List** Click the drop-down menu to select **All**, **Valid**, **Neighborhood**, **Rogue**, and **New**.

The following is a definition of the listed AP categories:

- **Valid:** An AP which is authenticated to the network with encryption is classified as valid.
- **Neighborhood:** A detected AP with a weak signal strength is classified as a suspect neighbor.
- **Rogue:** An AP that has been installed on the secure network with out explicit authorization.
- **New:** An alternative category.

From the AP List select a detected AP and click **Set as Valid**, **Set as Neighborhood**, **Set as Rogue**, or **Set as New** to manually define the category type for the AP. Alternatively, click the radio button to mark all new access points as valid or rogue.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Wireless Intrusion Protection

Wireless Band

AP List

Type	Band	CH	SSID	BSSID	Last Seen	Status
You can click Scan button to start.						

Mark All New Access Points as Valid Access Points

Mark All New Access Points as Rogue Access Points

## Schedule

The Wireless Schedule Settings window is used to add and modify schedule rules on the device. Click **Save** for the changes to take effect.

- Wireless Schedule** Click the drop-down menu to enable the device's schedule feature.
- Name** Enter a name for the new schedule rule in the field provided.
- SSID Index** Click the drop-down menu to select the desired SSID.
- SSID** Displays the current SSID.  
To create a new SSID, go to the Wireless Settings window (**Basic Settings > Wireless**).
- Day(s)** Click the radio button to select **All Week** and **Select Day(s)**. If **Select Day(s)** 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.
- Overnight** Check this box to set an overnight schedule.  
Note, in an overnight schedule the Start Time designates the beginning period in the evening.
- Save** Click to save the updated configuration.  
To make the updates permanent, click **Configuration > Save and Activate**.

**Wireless Schedule Settings**

Wireless Schedule Disable ▾

**Add Schedule Rule**

Name

SSID Index Primary SSID 2.4G ▾

SSID

Day(s) 
 All Week  Selects Day(s)

Sun  Mon  Tue  Wed  Thu  Fri  Sat

All Day(s)

Start Time  :  (hour:minute, 24 hour time)

End Time  :  (hour:minute, 24 hour time)  Overnight

**Schedule List**

Name	SSID Index	SSID	Day(s)	Time Frame	Wireless	Edit	DEL
+: To the end time of the next day overnight.							

## Internal RADIUS Server

The DAP-2620 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click **Save** 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 a name to authenticate user access to the internal RADIUS server.

**Password** Enter a password to authenticate user access to the internal RADIUS server. The length of your password should be 8 ~ 64.

**Status** Click the drop-down menu to enable the internal RADIUS server status.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Internal RADIUS Server

**RADIUS Accounts (Max: 256 users)**

User Name  (4-16Characters)

Password  (6-32Characters)

Status  ▾

**RADIUS Account list**

User Name	Enable	Disable	Delete
No user entries			

## ARP Spoofing Prevention

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

**ARP Spoofing Prevention** Click the drop-down menu to enable the ARP spoofing prevention function. By default this feature is disabled.

**Gateway IP Address** Enter a gateway IP address.

**Gateway MAC Address** Enter a gateway MAC address.

**Add** Click to create a defined rule.

**Clear** Click to remove the settings from the menu interface.

**Delete All** Click to delete all gateway entries.

**Edit** Click to edit the selected gateway entry.

**Delete** Click to delete the gateway entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

### ARP Spoofing Prevention Settings

ARP Spoofing Prevention Disable ▾

---

#### Add Gateway Address

Gateway IP Address

Gateway MAC Address  :  :  :  :  :

---

#### Gateway Address List

Total Entries: 0

Gateway IP Address	Gateway MAC Address	Edit	Delete
<input type="button" value="Save"/>			



## Bandwidth Optimization

The Bandwidth Optimization window allows the user to manage the bandwidth of the device and arrange the bandwidth for wireless clients. After defining the Bandwidth Optimization rule, click **Add**. To discard the settings, click **Clear**. Click **Save** for the changes to take effect.

**Enable Bandwidth Optimization** Click the drop-down menu to enable the Bandwidth Optimization function. By default this feature is disabled.

**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** Click the drop-down menu to select a rule:

- **Allocate average BW for each station:** AP will distribute average bandwidth for each client.
- **Allocate maximum BW for each station:** Specify the maximum bandwidth for each connected client.
- **Allocate different BW for 11a/b/g/n stations:** The weight of 11b/g/n and 11a/n client are 10%/20%/70%; 20%/80%. The AP distributes different bandwidth for 11a/b/g/n clients.
- **Allocate specific BW for SSID:** All clients share the total bandwidth.

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for the specified wireless band.

**Downlink Speed** Enter the limitation of the download speed in either Kbits/sec or Mbits/sec for the rule.

**Uplink Speed** Enter the limitation of the upload speed in either Kbits/sec or Mbits/sec for the rule.

**Add** Click to create a defined rule.

**Bandwidth Optimization**

Enable Bandwidth Optimization

Downlink Bandwidth  Mbits/sec

Uplink Bandwidth  Mbits/sec

**Add Bandwidth Optimization Rule**

Rule Type

Band

SSID Index

Downlink Speed  Kbits/sec

Uplink Speed  Kbits/sec

**Bandwidth Optimization Rules**

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Delete
<input type="button" value="Save"/>						

**Clear** Click to remove the settings from the menu interface.

**Edit** Click to edit the selected gateway entry.

**Delete** Click to delete the gateway entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

# Captive Portal

## Authentication Settings - Web Redirection Only

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Web Redirection Only as the Authentication Type, we can configure the redirection website URL that will be applied to each wireless client in this network.

**Session Timeout (1-1440)** Enter the session timeout value (1-1440).

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for this Authentication.

**Authentication Type** By default the function is set to **Disable**.

For this example, click the drop-down menu to select **Web Redirection Only**.

**Web Redirection State** When **Authentication Type** is **Web Redirection Only**, click the drop-down menu to enable web redirection state.

**URL Path** Click the drop-down menu to select **http://** or **https://**, then enter the URL of the website that will be used in the space provided.

**IPIF Status** Click the drop-down menu to enable or disable the Captive Portal with its IP interface feature.

**VLAN Group** Enter the VLAN Group ID.

**Captive Portal Authentication**

Session Timeout (1-1440)  Minute(s)

Band

SSID Index

Authentication Type

**Web Redirection Interface Settings**

Web Redirection State

URL Path

**IP Interface Settings**

IPIF Status

VLAN Group

Get IP From

IP Address

Subnet Mask

Gateway

DNS

Band	SSID Index	Captive Profile	Edit	Delete
------	------------	-----------------	------	--------

**Get IP From** Click the drop-down menu to select IP address setting mode.

- **Static IP (Manual):** 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-2620.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

**IP Address** 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.

**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.

**Edit** Click to edit the selected entry.

**Delete** Click to delete the selected entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Authentication Settings - Username/Password

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Username/Password as the Authentication Type, we can configure the Username/Password authentication that will be applied to each wireless client in this network.

**Session Timeout (1-1440)** Enter the session timeout value (1-1440).

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for this Authentication.

**Authentication Type** By default the function is set to **Disable**. For this example, click the drop-down menu to select **Username/Password**.

**Web Redirection State** When **Authentication Type** is **Username/Password**, click the drop-down menu to enable web redirection state.

**URL Path** Click the drop-down menu to select **http://** or **https://**, then enter the URL of the website that will be used in the space provided.

**IPIF Status** Click the drop-down menu to enable or disable the Captive Portal with its IP interface feature.

**VLAN Group** Enter the VLAN Group ID.

**Get IP From** Click the drop-down menu to select IP address setting mode.

- **Static IP (Manual):** 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-2620.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

**IP Address** 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.

**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.

**Username** Enter the username for the new account.

**Password** Enter the password for the new account.

**Add** Click to create a defined rule.

**Clear** Click to remove the settings from the menu interface.

**Edit** Click to edit the selected entry.

**Delete** Click to delete the selected entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Authentication Settings - Passcode

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Passcode as the Authentication Type, we can configure the Passcode authentication that will be applied to each wireless client in this network.

**Session Timeout (1-1440)** Enter the session timeout value (1-1440).

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for this Authentication.

**Authentication Type** By default the function is set to **Disable**. For this example, click the drop-down menu to select **Passcode**.

**Web Redirection State** When **Authentication Type** is **Passcode**, click the drop-down menu to enable web redirection state.

**URL Path** Click the drop-down menu to select **http://** or **https://**, then enter the URL of the website that will be used in the space provided.

**IPIF Status** Click the drop-down menu to enable or disable the Captive Portal with its IP interface feature.

**VLAN Group** Enter the VLAN Group ID.

**Get IP From** Click the drop-down menu to select IP address setting mode.

- **Static IP (Manual):** 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-2620.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

The screenshot shows the 'Captive Portal Authentication' configuration window. It is organized into several sections:

- Session Timeout (1-1440):** A text input field containing '60' followed by 'Minute(s)'.
- Band:** A dropdown menu currently showing '2.4GHz'.
- SSID Index:** A dropdown menu currently showing 'Primary SSID'.
- Authentication Type:** A dropdown menu currently showing 'Passcode'.
- Web Redirection Interface Settings:**
  - Web Redirection State:** A dropdown menu currently showing 'Enable'.
  - URL Path:** A dropdown menu showing 'http://' followed by an empty text input field.
- IP Interface Settings:**
  - IPIF Status:** A dropdown menu currently showing 'Disable'.
  - VLAN Group:** An empty text input field.
  - Get IP From:** A dropdown menu currently showing 'Static IP (Manual)'.
  - IP Address:** An empty text input field.
  - Subnet Mask:** An empty text input field.
  - Gateway:** An empty text input field.
  - DNS:** An empty text input field.
- Passcode Settings:**
  - Passcode Quantity:** An empty text input field.
  - Duration:** A text input field containing 'Hour'.
- Last Active Time:** A series of dropdown menus for 'Year' (2015), 'Month' (Jan), 'Day' (1), and 'Hour' (1:00).

**IP Address** 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.

**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.

**Passcode Quantity** Enter the number of ticket that will be used.

**Duration** Enter the duration value, in hours, for this passcode.

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

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

**Add** Click to create a defined rule.

**Clear** Click to remove the settings from the menu interface.

**Delete All** Click to delete all passcode setting entries.

**Edit** Click to edit the selected entry.

**Delete** Click to delete the selected entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.



## Authentication Settings - Remote RADIUS

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting Remote RADIUS as the Authentication Type, we can configure the Remote RADIUS authentication that will be applied to each wireless client in this network.

**Session Timeout (1-1440)** Enter the session timeout value (1-1440).

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for this Authentication.

**Authentication Type** By default the function is set to **Disable**. For this example, click the drop-down menu to select **Remote RADIUS**.

**Web Redirection State** When **Authentication Type** is **Remote RADIUS**, click the drop-down menu to enable web redirection state.

**URL Path** Click the drop-down menu to select **http://** or **https://**, then enter the URL of the website that will be used in the space provided.

**IPIF Status** Click the drop-down menu to enable or disable the Captive Portal with its IP interface feature.

**VLAN Group** Enter the VLAN Group ID.

**Get IP From** Click the drop-down menu to select IP address setting mode.

- **Static IP (Manual):** 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-2620.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

The screenshot shows the 'Captive Portal Authentication' configuration window. It is divided into several sections:

- Session Timeout (1-1440):** A text input field containing '60' followed by 'Minute(s)'.
- Band:** A dropdown menu currently showing '2.4GHz'.
- SSID Index:** A dropdown menu currently showing 'Primary SSID'.
- Authentication Type:** A dropdown menu currently showing 'Remote RADIUS'.
- Web Redirection Interface Settings:**
  - Web Redirection State:** A dropdown menu currently showing 'Enable'.
  - URL Path:** A dropdown menu showing 'http://' followed by an empty text input field.
- IP Interface Settings:**
  - IPIF Status:** A dropdown menu currently showing 'Disable'.
  - VLAN Group:** An empty text input field.
  - Get IP From:** A dropdown menu currently showing 'Static IP (Manual)'.
  - IP Address:** An empty text input field.
  - Subnet Mask:** An empty text input field.
  - Gateway:** An empty text input field.
  - DNS:** An empty text input field.
- Remote RADIUS Settings:**
  - RADIUS Server:** An empty text input field.
  - Radius Port:** A text input field containing '1812'.
  - Shared Secret:** An empty text input field.

**IP Address** 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.

**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.

**Radius Server** Enter the RADIUS server's IP address.

**Radius Port** Enter the RADIUS server's port number.

**Radius Secret** Enter the RADIUS server's shared secret.

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

**Edit** Click to edit the selected entry.

**Delete** Click to delete the selected entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Authentication Settings - LDAP

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting LDAP as the Authentication Type, we can configure the LDAP authentication that will be applied to each wireless client in this network.

**Session Timeout (1-1440)** Enter the session timeout value (1-1440).

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for this Authentication.

**Authentication Type** By default the function is set to **Disable**. For this example, click the drop-down menu to select **LDAP**.

**Web Redirection State** When **Authentication Type** is **LDAP**, click the drop-down menu to enable web redirection state.

**URL Path** Click the drop-down menu to select **http://** or **https://**, then enter the URL of the website that will be used in the space provided.

**IPIF Status** Click the drop-down menu to enable or disable the Captive Portal with its IP interface feature.

**VLAN Group** Enter the VLAN Group ID.

**Get IP From** Click the drop-down menu to select IP address setting mode.

- **Static IP (Manual):** 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-2620.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

The screenshot shows the 'Captive Portal Authentication' configuration interface. It is organized into several sections:

- Session Timeout (1-1440):** A text input field containing '60' followed by 'Minute(s)'.
- Band:** A dropdown menu currently showing '2.4GHz'.
- SSID Index:** A dropdown menu currently showing 'Primary SSID'.
- Authentication Type:** A dropdown menu currently showing 'LDAP'.
- Web Redirection Interface Settings:**
  - Web Redirection State:** A dropdown menu currently showing 'Enable'.
  - URL Path:** A dropdown menu showing 'http://' followed by an empty text input field.
- IP Interface Settings:**
  - IPIF Status:** A dropdown menu currently showing 'Disable'.
  - VLAN Group:** An empty text input field.
  - Get IP From:** A dropdown menu currently showing 'Static IP (Manual)'.
  - IP Address:** An empty text input field.
  - Subnet Mask:** An empty text input field.
  - Gateway:** An empty text input field.
  - DNS:** An empty text input field.
- LDAP Settings:**
  - Server:** An empty text input field.
  - Port:** A text input field containing '389'.
  - Authenticate Mode:** A dropdown menu currently showing 'Simple'.

**IP Address** 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.

**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.

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

**Port** Enter the LDAP server's port number.

**Authenticate Mode** Click the drop-down menu to select the authentication mode.

**Username** Enter the LDAP server account's username.

**Password** Enter the LDAP server account's password.

**Base DN** Enter the administrator's domain name.

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

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

**Edit** Click to edit the selected entry.

**Delete** Click to delete the selected entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Authentication Settings - POP3

The Captive Portal is a built-in web authentication server. When a station connects to an AP, the web browser will be redirected to a web authentication page. In this window, user can view and configure the Captive Portal settings. After selecting POP3 as the Authentication Type, we can configure the POP3 authentication that will be applied to each wireless client in this network.

**Session Timeout (1-1440)** Enter the session timeout value (1-1440).

**Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for this authentication.

**Authentication Type** By default the function is set to **Disable**. For this example, click the drop-down menu to select **POP3**.

**Web Redirection State** When **Authentication Type** is **POP3**, click the drop-down menu to enable web redirection state.

**URL Path** Click the drop-down menu to select **http://** or **https://**, then enter the URL of the website that will be used in the space provided.

**IPIF Status** Click the drop-down menu to enable or disable the Captive Portal with its IP interface feature.

**VLAN Group** Enter the VLAN Group ID.

**Get IP From** Click the drop-down menu to select IP address setting mode.

- **Static IP (Manual):** 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-2620.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

The screenshot shows the 'Captive Portal Authentication' configuration window. It is divided into several sections:

- Session Timeout (1-1440):** 60 Minute(s)
- Band:** 2.4GHz
- SSID Index:** Primary SSID
- Authentication Type:** POP3
- Web Redirection Interface Settings:**
  - Web Redirection State: Enable
  - URL Path: http://
- IP Interface Settings:**
  - IPIF Status: Disable
  - VLAN Group: (empty)
  - Get IP From: Static IP (Manual)
  - IP Address: (empty)
  - Subnet Mask: (empty)
  - Gateway: (empty)
  - DNS: (empty)
- POP3 Settings:**
  - Server: (empty)
  - Port: 110
  - Connection Type: None

**IP Address** 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.

**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.

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

**Port** Enter the POP server's port number.

**Connection Type** Click the drop-down menu to select the connection type, options include: None or SSL/TLS.

**Edit** Click to edit the selected entry.

**Delete** Click to delete the selected entry.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Login Page Upload

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

**Upload Login Style from file** After you have a saved login style file, click **Browse....** Select the saved login style file and click **Open** and **Upload** to upload the login style file.

**Login Page Style List** Click the drop-down menu to select the wireless band and login style that will be used in each SSID here. Click **Download** to download the template file for the login page and click **Delete** to delete the template file.

**Note:** *The Left space field indicates the available memory in Bytes on the device.*

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate.**

**Login Page Upload**

**Upload Login Style From Local Hard Drive**

Upload Login Style from file :

The Left space 742400 Byte(s)

**Login Page Style List**

Wireless Band

ID	Style Name	Pri	S-1	S-2	S-3	S-4	S-5	S-6	S-7	Download	Del
1	pages_default.tar	1	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="Download"/>	<input type="button" value="Del"/>
2	pages_headerpic.tar	2	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="Download"/>	<input type="button" value="Del"/>
3	pages_license.tar	3	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="Download"/>	<input type="button" value="Del"/>

## MAC Bypass

The DAP-2620 features a wireless MAC Bypass mechanism that allows clients in a network to access the Internet without the need for Captive Portal authentication.

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for the MAC bypass.

**MAC Address** Enter each MAC address that you wish to include in your bypass list, and click **Add**.

**MAC Address List** When a MAC address is entered, it appears in the list.

Highlight a MAC address and click **Delete** icon to remove it from the list.

**Upload MAC File** To upload a MAC bypass list file, click **Browse...** and navigate to the MAC bypass list file saved on the computer, and then click **Upload**.

**Download MAC File** To download MAC bypass list file, click **Download** and to save the MAC bypass list.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

The screenshot shows the 'MAC Bypass Settings' web interface. It features a header with the title 'MAC Bypass Settings'. Below the header, there are several configuration options: 'Wireless Band' with a dropdown menu set to '2.4GHz', 'SSID Index' with a dropdown menu set to 'Primary SSID', and 'MAC Address' with a series of input fields and an 'Add' button. Below these options is a table with two columns: 'ID' and 'MAC Address', and a 'Delete' button. Underneath the table, there are two sections: 'Upload MAC File' and 'Download MAC File'. The 'Upload MAC File' section has an 'Upload File:' label, an input field, a 'Browse...' button, and an 'Upload' button. The 'Download MAC File' section has a 'Load MAC File to Local Hard Driver:' label and a 'Download' button. At the bottom right of the interface, there is a 'Save' button.



# 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-2620 is capable of acting as a DHCP server.

**Function Enable/Disable** Click the drop-down menu to enable or disable the DAP-2620 functions as a DHCP server. By default this feature is disabled.

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.

**IP Assigned From** Enter the first IP address available for assignment on your network.

**IP Pool Range (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** Enter the subnet mask for the network. All devices in the network must have the same subnet mask to communicate.

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

**WINS** Enter 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.

Dynamic Pool Settings	
<b>DHCP Server Control</b>	
Function Enable/Disable	Disabled ▾
<b>Dynamic Pool Settings</b>	
IP Assigned From	192.168.1.20
IP Pool Range(1-254)	235
Subnet Mask	255.255.255.0
Gateway	
WINS	
DNS	
Domain Name	dlink-ap
Lease Time (60 - 31536000 sec)	604800
<input type="button" value="Save"/>	

**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** Enter the lease time that the period of time before the DHCP server will assign new IP addresses.  
**(60 - 31536000 sec)**

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## Static Pool Settings

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

**Function Enable/Disable** Click the drop-down menu to enable or disable the DAP-2620 functions as a DHCP server. By default this feature is disabled.

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.

**Host Name** Enter the name of the host entry. Spaces are not valid character options.

**Assigned IP** Enter the IP address of the device requesting association.

**Assigned MAC Address** Enter the MAC address of the device requesting association.

**Subnet Mask** Enter the subnet mask of the IP address specified in the "IP Assigned From" field.

**Gateway** Enter the gateway address for the wireless network.

**WINS** Enter 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** Enter the domain name for the network.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Static Pool Settings

**DHCP Server Control**

Function Enable/Disable

**Static Pool Settings**

Host Name

Assigned IP

Assigned MAC Address  :  :  :  :

Subnet Mask

Gateway

WINS

DNS

Domain Name

Host Name	MAC Address	IP Address	Edit	Delete
-----------	-------------	------------	------	--------

## 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 settings.

**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.

**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.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Current IP Mapping List			
Current DHCP Dynamic Pools			
Host Name	Binding MAC Address	Assigned IP Address	Lease Time
Current DHCP Static Pools			
Host Name	Binding MAC Address	Assigned IP Address	

## Filters

### Wireless MAC ACL

The page allows the user to configure Wireless MAC ACL settings for access control.

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Access Control List** Click the drop-down menu to select the access control list. By default this feature is disabled.

- Select **Disable** to disable the filters function.
- Select **Allow** to accept only those devices with MAC addresses in the Access Control List. All other devices not on the list will be rejected.
- Select **Deny** to reject the devices with MAC addresses on the Access Control List. All other devices not on the list will be accepted.

**SSID Index** Click the drop-down menu to select the SSID for the specified wireless band.

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

**MAC Address List** When a MAC address is entered, it is added to the following index. Highlight a listing and click **Delete** to remove it from the index.

**Current Client Information** Displays information about all the current connected stations.

**Upload File** To upload a ACL list file, click **Browse...** and navigate to the ACL list file saved on the computer, and then click **Upload**.

**Load ACL File to Local Hard Drive** To download ACL list file, click **Download** and to save the ACL list.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

## WLAN Partition

The page allows the user to configure a WLAN Partition.

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**Ethernet to WLAN Access** Click the drop-down menu to enable or disable the Ethernet devices to communicate with wireless clients. 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** Click the radio button to a specific mode. The modes are defined as follows:

- **Enable:** Allows communication between wireless clients connected to the same SSID and wireless clients connected to different SSIDs configured on this access point.
- **Disable:** Disallows communication between wireless clients connected to the same SSID, while allowing communication between wireless clients configured on this access point which are connected to different SSIDs.
- **Guest:** Disallows communication between wireless clients configured on the access point even when connected to the same or different SSIDs.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

SSID	Enable	Disable	Guest mode
Primary SSID	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-SSID 1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-SSID 2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-SSID 3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-SSID 4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-SSID 5	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-SSID 6	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-SSID 7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## IP Filter Settings

Enter the IP address or network address that will be used in the IP filter rule. In the following example, if the IP addresses 192.168.70.66 or 192.168.70.0 are entered, they would be inaccessible to wireless clients on the same network.

**Wireless Band** Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

**SSID Index** Click the drop-down menu to select the SSID for the IP filter..

**Filter State** Click the drop-down menu to enable or disable the filter state. By default this feature is disabled.

**IP Address** Enter the IP address or network address to apply the filter settings.

**Subnet Mask** Enter the subnet mask of the IP address or networks address.

**IP Address List** When an IP address is entered, it appears in the list.  
Highlight a IP address and click **Delete** to remove it from the list.

**Upload IP Filter File** To upload a IP filter list file, click **Browse...** and navigate to the IP filter list file saved on the computer, and then click **Upload**.

**Download IP Filter File** To download IP Filter list file, click **Download** and to save the IP filter list.

**Save** Click to save the updated configuration.  
To make the updates permanent, click **Configuration > Save and Activate**.

The screenshot shows the 'IP Filter Settings' page. At the top, there are several configuration options: 'Wireless Band' set to '2.4GHz', 'SSID Index' set to 'Primary SSID', and 'Filter State' set to 'Disable'. Below these are input fields for 'IP Address' and 'Subnet Mask', both currently empty, with an 'Add' button underneath. A table with columns 'ID', 'IP Address', 'Subnet Mask', and 'Delete' is present but empty. Below the table are sections for 'Upload IP Filter File' (with an 'Upload File' label, an empty text box, a 'Browse...' button, and an 'Upload' button) and 'Download IP Filter File' (with a 'Load IP Filter File to Local Hard Driver' label and a 'Download' button). A 'Save' button is located at the bottom right of the form.

# Traffic Control

## Uplink/Downlink Settings

The uplink/downlink setting allows users to customize the downlink and uplink interfaces including specifying downlink/uplink 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 **Save** to let your changes take effect.

**Ethernet** Check the box to specify the Downlink or Uplink settings.

**Downlink Bandwidth** Enter the downlink bandwidth in Mbits per second.

**Uplink Bandwidth** Enter the uplink bandwidth in Mbits per second.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

### Uplink and Downlink Settings

Ethernet1	<input type="checkbox"/> Downlink	<input type="checkbox"/> Uplink
Ethernet2	<input type="checkbox"/> Downlink	<input type="checkbox"/> Uplink

2.4GHz
5GHz

**Downlink Interface**

<input type="checkbox"/> Primary-ssid	<input type="checkbox"/> Multi-ssid1	<input type="checkbox"/> Multi-ssid2	<input type="checkbox"/> Multi-ssid3
<input type="checkbox"/> Multi-ssid4	<input type="checkbox"/> Multi-ssid5	<input type="checkbox"/> Multi-ssid6	<input type="checkbox"/> Multi-ssid7

**Uplink Interface**

<input type="checkbox"/> Primary-ssid	<input type="checkbox"/> Multi-ssid1	<input type="checkbox"/> Multi-ssid2	<input type="checkbox"/> Multi-ssid3
<input type="checkbox"/> Multi-ssid4	<input type="checkbox"/> Multi-ssid5	<input type="checkbox"/> Multi-ssid6	<input type="checkbox"/> Multi-ssid7

Downlink Bandwidth(1~867)  Mbits/sec

Uplink Bandwidth(1~867)  Mbits/sec



## QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2620 supports four priority levels. Once the desired QoS settings are finished, click **Save** to let your changes take effect.

**Note:** *Bandwidth Optimization is disabled if QoS is enabled.*

**Enable QoS** Check the box to allow QoS to prioritize traffic. By default this feature is disabled.

**Downlink Bandwidth** Enter the downlink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.

**Uplink Bandwidth** Enter the uplink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.

**ACK/DHCP/ICMP/DNS Priority** Click the drop-down menu to select the level of priority for the selected rule.

**Web Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.

**Mail Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.

**Ftp Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.

**User Defined-1/2/3/4 Priority** Click the drop-down menu to select the level of priority for the selected rule.

**Other Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

The screenshot shows the QoS configuration window. At the top, there is a section for 'QoS' with an 'Enable QoS' checkbox that is currently unchecked. Below this is the 'Advanced QoS' section, which is expanded. It contains several rows of settings:

- Downlink Bandwidth:** 100 Mbits/sec
- Uplink Bandwidth:** 100 Mbits/sec
- ACK/DHCP/ICMP/DNS Priority:** Highest Priority, Limit 100%, Port 53,67,68,546,547
- Web Traffic Priority:** Third Priority, Limit 100%, Port 80,443,3128,8080
- Mail Traffic Priority:** Second Priority, Limit 100%, Port 25,110,465,995
- Ftp Traffic Priority:** Low Priority, Limit 100%, Port 20,21
- User Defined-1 Priority:** Highest Priority, Limit 100%, Port 0 - 0
- User Defined-2 Priority:** Second Priority, Limit 100%, Port 0 - 0
- User Defined-3 Priority:** Third Priority, Limit 100%, Port 0 - 0
- User Defined-4 Priority:** Low Priority, Limit 100%, Port 0 - 0
- Other Traffic Priority:** Low Priority, Limit 100%

A 'Save' button is located at the bottom right of the configuration area.

## 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 **Save** for the changes to take effect.

**Note:** *Bandwidth Optimization is disabled if QoS is enabled.*

**Traffic Manager** Click the drop-down menu to enable the traffic manager feature. By default this feature is disabled.

**Unlisted Clients Traffic** Click the radio button to select **Deny** or **Forward** to determine how to deal with unlisted client traffic.

**Downlink Bandwidth** Enter the downlink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.

**Uplink Bandwidth** Enter the uplink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.

**Name** Enter the name of the traffic manager rule.

**Client IP (optional)** Enter the client IP address of the traffic manager rule.

**Client MAC (optional)** Enter the client MAC address of the traffic manager rule.

**Downlink Speed** Enter the downlink speed in Mbits per second.

**Uplink Speed** Enter the uplink speed in Mbits per second.

**Traffic Manager Rules List** When a rule is entered, it is added to the following index. Click **Edit** or **Delete** to alter the current rule.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

**Traffic Manager**

Traffic Manager  ▾

Unlisted Clients Traffic  Deny  Forward

Downlink Bandwidth  Mbits/sec

Uplink Bandwidth  Mbits/sec

**Add Traffic Manager Rule**

Name

Client IP(optional)

Client MAC(optional)

Downlink Speed  Mbits/sec

Uplink Speed  Mbits/sec

**Traffic Manager Rules**

Name	Client IP	Client MAC	Downlink Speed	Uplink Speed	Edit	Delete
<input type="button" value="Save"/>						

# 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.



The screenshot displays the D-Link DAP-2620 Web User Interface. The top navigation bar includes the D-Link logo, the device model 'DAP-2620', and menu items: Home, Maintenance, Configuration, System, Logout, and Help. A left sidebar shows a tree view with 'DAP-2620' expanded, containing sub-items: Basic Settings, Advanced Settings, Status (selected), Device Information, Client Information, WDS Information, Statistics, and Log. The main content area is titled 'System Information' and displays the following details:

Model Name	DAP-2620
Firmware Version	v1.00 19:33:32 2019/03/25
System Name	dap2620
Location	
System Time	2019/05/17 16:18:20
Up Time	01:16:36
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	00:AA:BB:CC:DD:10
MAC Address (5GHz)	00:AA:BB:CC:DD:18
IP Address	192.168.1.166

## Device Information

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

- Ethernet MAC Address** Displays the Ethernet MAC address.
- Wireless MAC Address (2.4GHz)** Displays the 2.4GHz wireless MAC address.
- Wireless MAC Address (5GHz)** Displays the 5GHz wireless MAC address.
- IP Address** Displays the assigned IP address.
- Subnet Mask** Displays the assigned subnet mask.
- Gateway** Displays the assigned gateway.
- DNS** Displays the assigned DNS.
- Network Name (SSID)** Displays the SSID of 2.4GHz network.
  - Channel** Displays the channel of 2.4GHz network.
  - Data Rate** Displays the data rate of 2.4GHz network.
  - Security** Displays the security of 2.4GHz network.
- Network Name (SSID)** Displays the SSID of 5GHz network.
  - Channel** Displays the channel of 5GHz network.
  - Data Rate** Displays the data rate of 5GHz network.
  - Security** Displays the security of 5GHz network.
- CPU Utilization** Displays the current CPU utilization.
- Memory Utilization** Displays the current memory utilization.
- Connection Status** Displays the current connection status.
  - Server IP** Displays the current server IP address.
  - Server Port** Displays the current server port.

Device Information	
<b>Firmware Version:v1.00</b>	
Ethernet MAC Address	00:AA:BB:CC:DD:10
Wireless MAC Address(2.4GHz):	Primary: 00:AA:BB:CC:DD:10
	SSID 1~7: 00:AA:BB:CC:DD:11~00:AA:BB:CC:DD:17
Wireless MAC Address(5GHz):	Primary: 00:AA:BB:CC:DD:18
	SSID 1~7: 00:AA:BB:CC:DD:19~00:AA:BB:CC:DD:1F
<b>Ethernet</b>	
IP Address	192.168.1.166
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS	192.168.1.201
<b>Wireless(2.4GHz)</b>	
Network Name (SSID)	dlink
Channel	Ch 7 + 11 (Auto)
Data Rate	Best(Up to 300) Mbps
Security	No Authentication / No Encryption
<b>Wireless(5GHz)</b>	
Network Name (SSID)	dlink
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Data Rate	Best(Up to 867) Mbps

## Client Information

The page displays the associated clients SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-2620 network.

**SSID** Displays the associated clients SSID for the network.

**MAC** Displays the associated clients MAC address for the network.

**Band** Displays the associated clients band for the network.

**Authentication** Displays the associated authentication method for the network.

**RSSI** Displays the associated clients RSSI for the network.

**Power Saving Mode** Displays the associated clients power saving mode for the network.

**System Info** Displays the associated clients information for the network.

Client Information						
<b>Client Information</b>		Station association (2.4GHz) : 0				
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info
No wireless client						
<b>Client Information</b>		Station association (5GHz) : 0				
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info
No wireless client						

## WDS Information

The page displays the access points SSID, MAC, band, authentication method, signal strength, and status for the DAP-2620's Wireless Distribution System network.

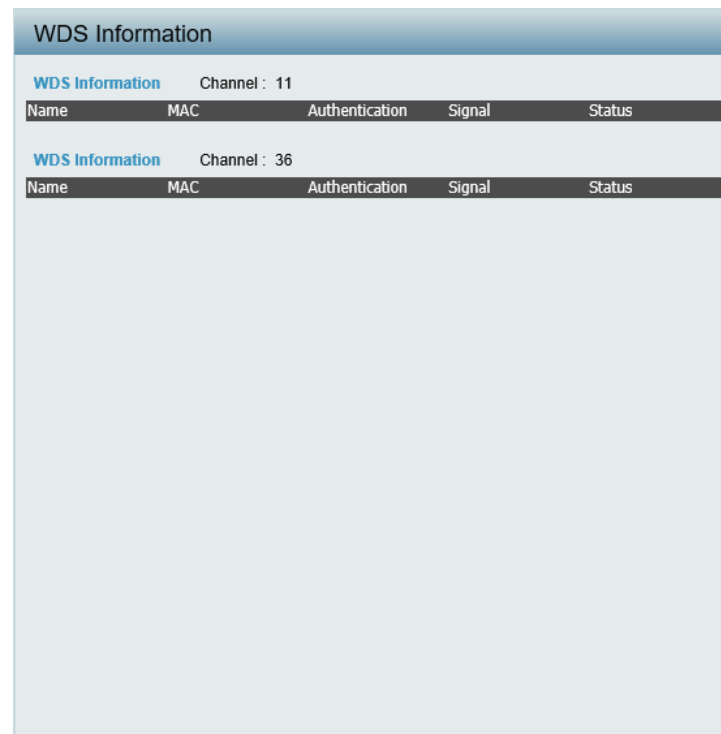
**Name** Displays the AP SSID for the network.

**MAC** Displays the AP MAC address for the network.

**Authentication** Displays the AP authentication method for the network.

**Signal** Displays the AP signal for the network.

**Status** Displays the AP status for the network.



The screenshot shows the 'WDS Information' page with two tables. The first table is for Channel 11 and the second is for Channel 36. Both tables have the same headers: Name, MAC, Authentication, Signal, and Status. The tables are currently empty.

WDS Information				
Channel : 11				
Name	MAC	Authentication	Signal	Status

WDS Information				
Channel : 36				
Name	MAC	Authentication	Signal	Status

## Statistics

### Ethernet

Displays wired interface network traffic information for LAN1 (Bottom) and LAN2 (Rear).

**Transmitted Packet Count** Displays the transmitted packet count.

**Transmitted Bytes Count** Displays the transmitted bytes count.

**Dropped Packet Count** Displays the dropped packet count.

**Received Packet Count** Displays the received packet count.

**Received Bytes Count** Displays the received bytes count.

**Dropped Packet Count** Displays the dropped packet count.

**Refresh** Click **Refresh** to update the Ethernet traffic statistics list.

Ethernet Traffic Statistics		
	LAN1	LAN2
<b>Transmitted Count</b>		
Transmitted Packet Count	2877	22427
Transmitted Bytes Count	313866	22246815
Dropped Packet Count	0	0
<b>Received Count</b>		
Received Packet Count	0	24220
Received Bytes Count	0	2398891
Dropped Packet Count	0	0

## WLAN Traffic Statistics

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

- Transmitted Packet Count** Displays the transmitted packet count.
- Transmitted Bytes Count** Displays the transmitted bytes count.
- Dropped Packet Count** Displays the dropped packet count.
- Transmitted Retry Count** Displays the transmitted retry count.
- Received Packet Count** Displays the received packet count.
- Received Bytes Count** Displays the received bytes count.
- Dropped Packet Count** Displays the dropped packet count.
- Received CRC Count** Displays the received CRC count.
- Received Decryption Error Count** Displays the received decryption error count.
- Received MIC Error Count** Displays the received MIC error count.
- Received PHY Error Count** Displays the received PHY error count.
- Refresh** Click **Refresh** to update the WLAN traffic statistics list.

WLAN Traffic Statistics		
	2.4GHz	5GHz
<input type="button" value="Refresh"/>		
<b>Transmitted Count</b>		
Transmitted Packet Count	0	0
Transmitted Bytes Count	0	0
Dropped Packet Count	2674	0
Transmitted Retry Count	0	0
<b>Received Count</b>		
Received Packet Count	0	0
Received Bytes Count	0	0
Dropped Packet Count	0	0
Received CRC Count	27155	0
Received Decryption Error Count	0	0
Received MIC Error Count	0	0
Received PHY Error Count	0	0



# 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** Displays the AP's embedded memory holds logs, up to 500 logs.

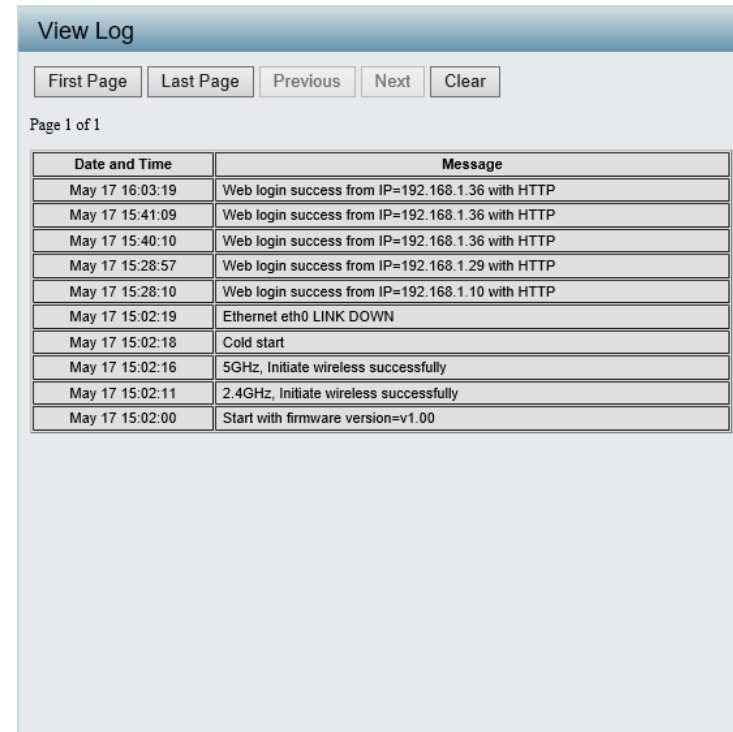
**First Page** Click to display the home View Log page.

**Last Page** Click to display the last View Log page.

**Previous** Click to display the page occurring before in order.

**Next** Click to display the page occurring after in order.

**Clear** Click to remove all listings from the View Log page.



The screenshot shows the 'View Log' web interface. At the top, there are navigation buttons: 'First Page', 'Last Page', 'Previous', 'Next', and 'Clear'. Below the buttons, it indicates 'Page 1 of 1'. The main content is a table with two columns: 'Date and Time' and 'Message'. The table contains the following log entries:

Date and Time	Message
May 17 16:03:19	Web login success from IP=192.168.1.36 with HTTP
May 17 15:41:09	Web login success from IP=192.168.1.36 with HTTP
May 17 15:40:10	Web login success from IP=192.168.1.36 with HTTP
May 17 15:28:57	Web login success from IP=192.168.1.29 with HTTP
May 17 15:28:10	Web login success from IP=192.168.1.10 with HTTP
May 17 15:02:19	Ethernet eth0 LINK DOWN
May 17 15:02:18	Cold start
May 17 15:02:16	5GHz, Initiate wireless successfully
May 17 15:02:11	2.4GHz, Initiate wireless successfully
May 17 15:02:00	Start with firmware version=v1.00

## 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 log server.

**Log Type** Check the boxes to select the activity to log. There are three types: System Activity, Attacks, and Notice.

**Log Server / IP Address** Enter the EU directive Syslog Server IP address or Domain Name to use for the log settings.

**Email Notification** Check the box to enable sending email notification.

**Outgoing mail server (SMTP)** Click the drop-down menu to select the SMTP server type, options include: Internal, Gmail, Hotmail.

**Authentication** Check the box to enable the authentication of the email notification.

**SSL/TLS** Check the box to enable the SSL/TLS function.

**From Email Address** Enter the email address of the account you would like to send the log.

**To Email Address** Enter the email address of the account you would like to send the log.

**Email Server Address** Enter the IP address of the server you would like to send the log.

**SMTP Port** Enter the SMTP port of the email server.

**Account** Enter the user name of the of the listed email address.

**Password** Enter the password set for the email notification.

**Confirm Password** Retype the password entry to confirm the password.

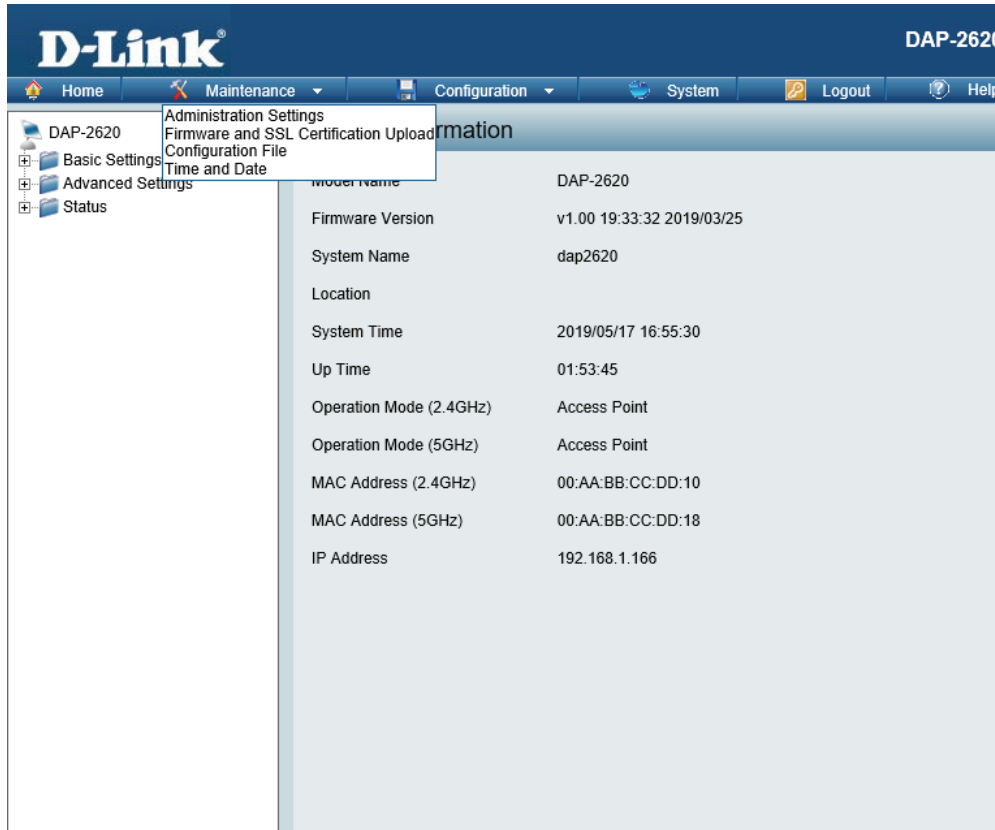
The screenshot shows the 'Log Settings' configuration page. It is divided into two main sections: 'Log Settings' and 'Email Notification'.  
 In the 'Log Settings' section:  
 - There is a text input field for 'Log Server / IP Address'.  
 - The 'Log Type' section has three checkboxes: 'System Activity' (checked), 'Attacks' (checked), and 'Notice' (checked).  
 - Below that is another text input field for 'EU directive Syslog Server Settings / Log Server / IP Address'.  
 In the 'Email Notification' section:  
 - The 'Email Notification' checkbox is unchecked.  
 - The 'Outgoing mail server (SMTP)' dropdown menu is set to 'Internal'.  
 - There are text input fields for 'Authentication', 'SSL/TLS', 'From Email Address', 'To Email Address', 'Email Server Address', 'SMTP Port', 'Account', and 'Password'.

**Schedule** Click the drop-down menu to set email log schedule.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

# Maintenance

In the Maintenance 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.



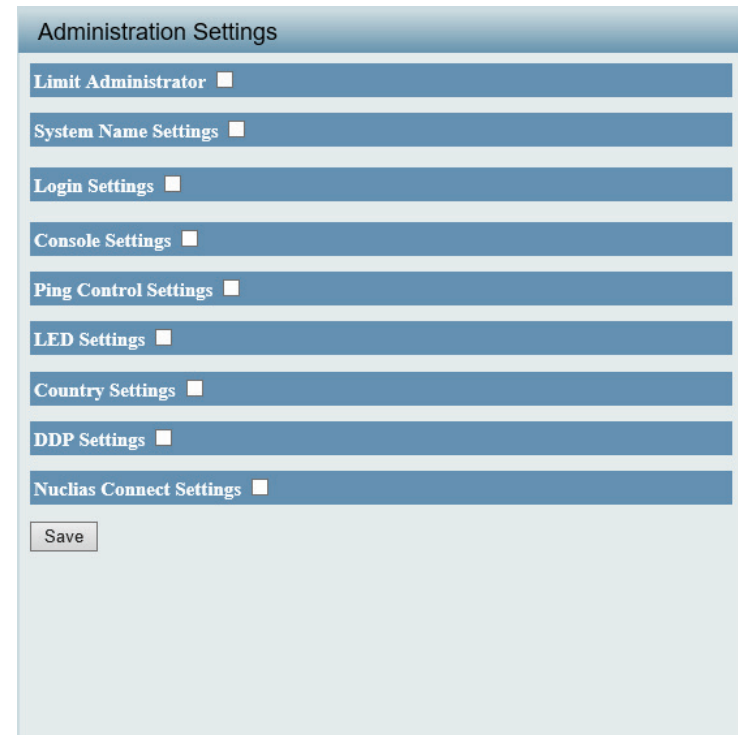
The screenshot displays the D-Link DAP-2620 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with DAP-2620, Basic Settings, Advanced Settings, and Status. The main content area is titled 'Information' and displays the following system details:

Model Name	DAP-2620
Firmware Version	v1.00 19:33:32 2019/03/25
System Name	dap2620
Location	
System Time	2019/05/17 16:55:30
Up Time	01:53:45
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	00:AA:BB:CC:DD:10
MAC Address (5GHz)	00:AA:BB:CC:DD:18
IP Address	192.168.1.166

## Administration Settings

The administrator or users with administration privilege can access the administration management interface.

After any setting modification, the updated configuration must be saved to the device through the Configuration function, otherwise, the settings will not be saved to the firmware.



## Limit Administrator

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

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

### VLAN ID

**Limit Administrator IP** Check the box 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 **Add**.

**Note:** To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

Item	From	To	Delete
------	------	----	--------

## System Name Settings

**System Name** Enter the name of the device. The default name is D-Link dap2620.

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

**MDNS Name** Enter the name of the multicast DNS. The default name is dap2620.

**Note:** To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

## Login Settings

**Login Name** Enter a user name.

**New Password** Enter the new password. The password is case-sensitive. "A" is a different character than "a." The length should be between 4 to 32 characters.

**Confirm Password** Enter the new password a second time for confirmation purposes. Check the box to apply and update the password.

**Note:** To save the new configuration settings to the firmware, click **Configuration** > **Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

## Console Settings

**Status** Check the box to enable the console.

**Console Protocol** Click the radio button to select the type of protocol.

**Timeout** Click the drop-down menu to select the timeout.

**Note:** To save the new configuration settings to the firmware, click **Configuration** > **Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

## Ping Control Settings

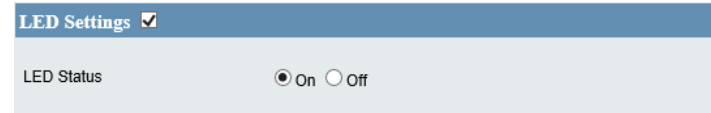
**Status** Check the box to enable the ping control setting.

**Note:** To save the new configuration settings to the firmware, click **Configuration** > **Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

## LED Settings

**LED Status** Click the radio button to select the LED on or off.

**Note:** To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.



## Country Settings

**Select a Country** Click the drop-down menu to select a country.

**Note:** To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

**Note:** The function is region dependent.



## DDP Control Settings

**Status** Check the box to enable the DDP control setting.

**Note:** To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.

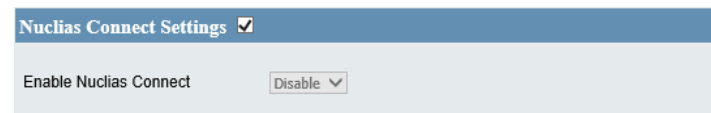


## Nuclias Connect Settings

The Nuclias Connect section is used to create a set of APs on the Internet to be organized into a single group in order to increase ease of management. Nuclias Connect and AP Array are mutually exclusive functions.

**Enable Nuclias Connect** Click the drop-down menu to enable or disable the Nuclias Connect.

**Note:** To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.





## Firmware and SSL Certification Upload

The 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.

**Update Firmware From Local Hard Drive** The current firmware version is displayed above the file location field. After the latest firmware is downloaded, click **Browse...** to locate the new firmware. Once the file is selected, click **Open** and **Upload** to begin updating the firmware. Please don't turn the power off while upgrading.

**Language Pack Upgrade** After you have downloaded a language pack to your local drive, click **Browse....** Select the language pack and click **Open** and **Upload** to complete the upgrade.

**Update SSL Certification From Local Hard Drive** After you have downloaded a SSL certification to your local drive, click **Browse....** Select the certification and click **Open** and **Upload** to complete the upgrade.

The screenshot displays a web interface titled "Firmware and SSL Certification Upload". It is divided into three main sections, each with a header bar:

- Update Firmware From Local Hard Drive:** This section shows the current "Firmware Version v1.00". Below this, there is a label "Upload Firmware From File:" followed by a text input field, a "Browse..." button, and an "Update" button.
- Language Pack Upgrade:** This section has a label "Upload:" followed by a text input field, a "Browse..." button, and an "Update" button.
- Update SSL Certification From Local Hard Drive:** This section contains two identical rows. The first row is labeled "Upload Certificate From File:" and the second is labeled "Upload Key From File:". Each row includes a text input field, a "Browse..." button, and an "Update" button.

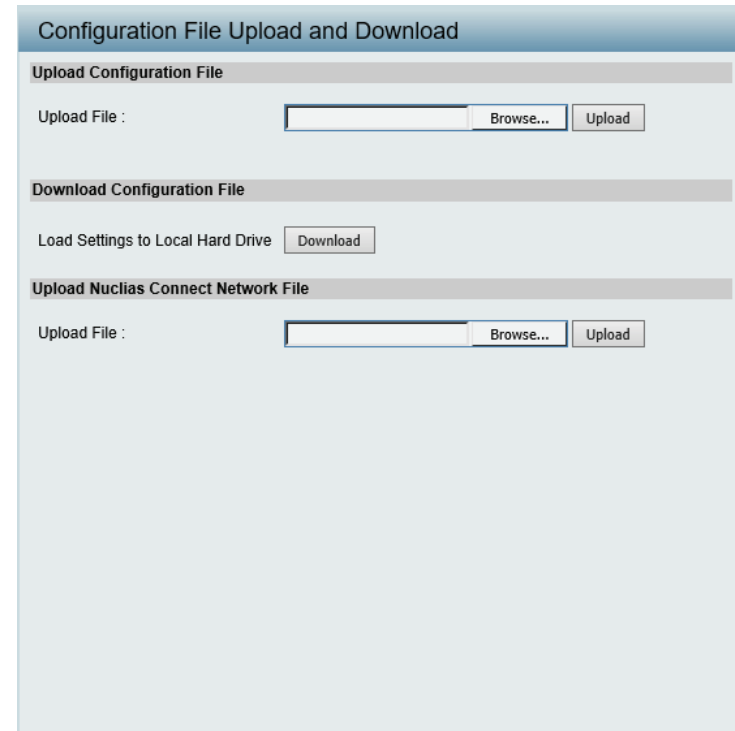
## Configuration File

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

**Upload Configuration File** After you have a configuration file, click **File Browse....** Select the configuration file 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-2620 and then updating to this saved configuration file, the password will be gone.

**Upload Nuclias Connect Network File** After you have a saved Nuclias Connect file, click **File Browse....** Select the saved Nuclias Connect file and click **Open** and **Upload** to upload the Nuclias Connect file.



The screenshot shows a web interface titled "Configuration File Upload and Download". It is divided into three sections:

- Upload Configuration File:** This section contains a text input field labeled "Upload File:" followed by a "Browse..." button and an "Upload" button.
- Download Configuration File:** This section contains a "Load Settings to Local Hard Drive" button and a "Download" button.
- Upload Nuclias Connect Network File:** This section contains a text input field labeled "Upload File:" followed by a "Browse..." button and an "Upload" button.

## 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.

**Enable NTP** Check the box 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** Click the drop-down menu to select your correct time zone.

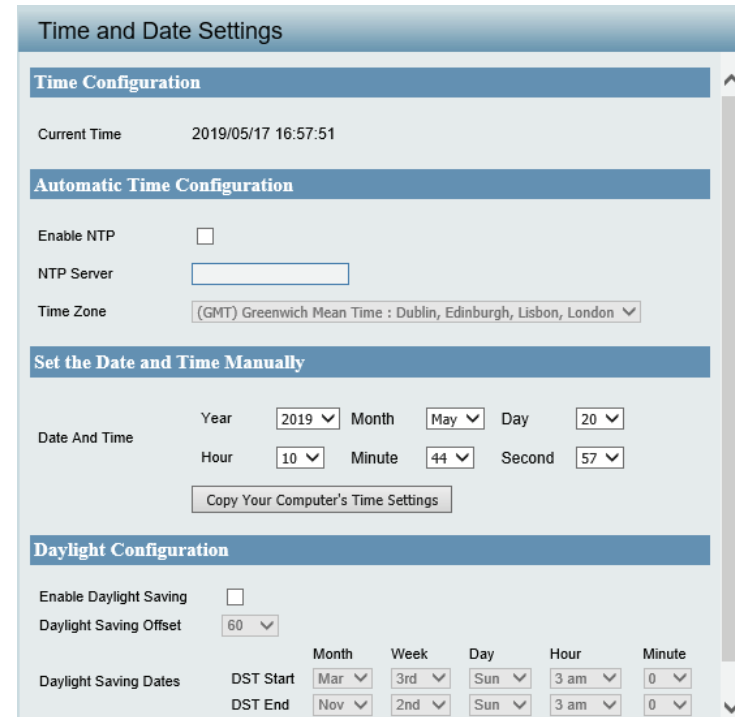
**Date And Time** Set the time for the AP or click **Copy Your Computer's Time Settings** to copy the time from the computer in use (Make sure that the computer's time is set correctly).

**Enable Daylight Saving** Check the box to enable the daylight saving time settings.

**Daylight Saving Offset** Click the drop-down menu to select the offsetting variable in minutes to adjust for daylight saving time.

**Daylight Saving Dates** Click the drop-down menu to designate the start/end date and time for daylight saving time.

**Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.



**Time and Date Settings**

**Time Configuration**

Current Time 2019/05/17 16:57:51

**Automatic Time Configuration**

Enable NTP

NTP Server

Time Zone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

**Set the Date and Time Manually**

Date And Time

Year 2019 Month May Day 20

Hour 10 Minute 44 Second 57

Copy Your Computer's Time Settings

**Daylight Configuration**

Enable Daylight Saving

Daylight Saving Offset 60

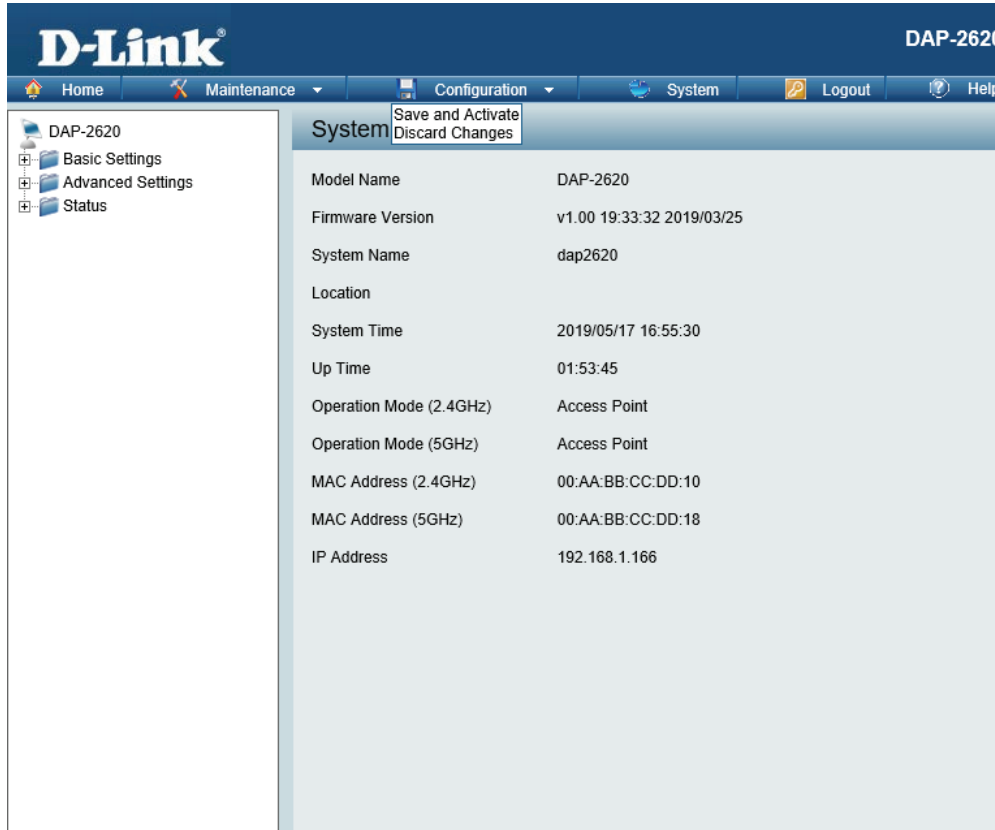
Daylight Saving Dates

	Month	Week	Day	Hour	Minute
DST Start	Mar	3rd	Sun	3 am	0
DST End	Nov	2nd	Sun	3 am	0

# Configuration

Configuration allows the user to save and activate or discard the configurations done.

- Save and Activate: Click **Save and Activate** to have configuration changes you have made to be saved across a system reboot.
- Discard Changes: Click **Discard Changes** to discard the settings you have made.



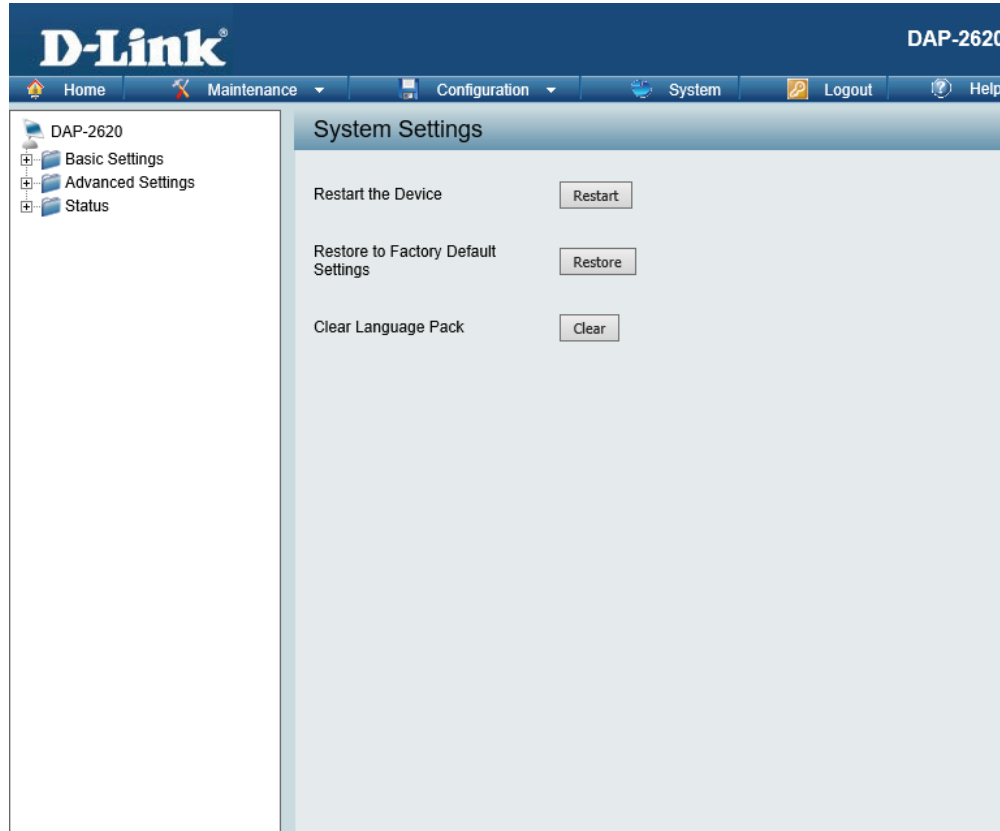
The screenshot displays the D-Link DAP-2620 Web User Interface. The top navigation bar includes the D-Link logo, the device name 'DAP-2620', and menu items: Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with 'DAP-2620' expanded, containing 'Basic Settings', 'Advanced Settings', and 'Status'. The main content area is titled 'System' and features a table of system information. Above the table, there are two buttons: 'Save and Activate' and 'Discard Changes'.

Parameter	Value
Model Name	DAP-2620
Firmware Version	v1.00 19:33:32 2019/03/25
System Name	dap2620
Location	
System Time	2019/05/17 16:55:30
Up Time	01:53:45
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	00:AA:BB:CC:DD:10
MAC Address (5GHz)	00:AA:BB:CC:DD:18
IP Address	192.168.1.166

# System

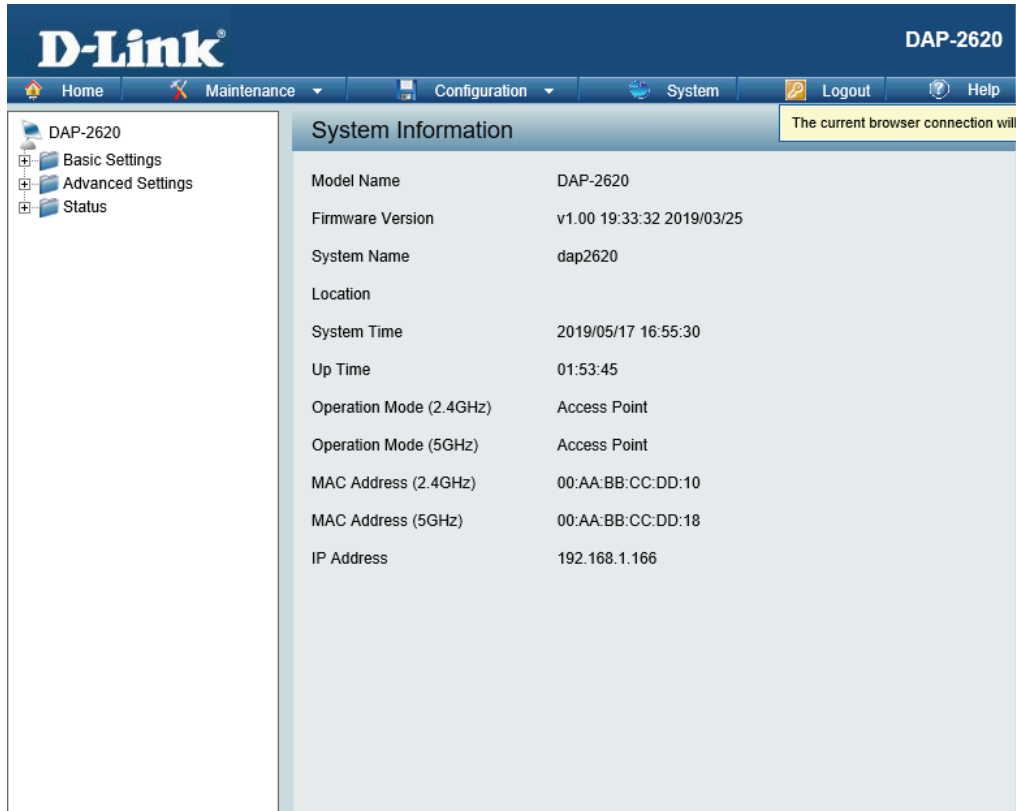
The System page allows the user to restart the unit, perform a factory reset or clear the language pack settings.

- Restart the Device: Click **Restart** to restart the device.
- Restore to Factory Default Settings: Click **Restore** to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save.
- Clear Language Pack: Click **Clear** to reset language to default settings.



# Logout

Click **Logout** to allow the user to safely log out from the access point's web configuration. Click **The current browser connection will be disconnected if you click here** to logout.



The screenshot displays the D-Link web configuration interface for a DAP-2620 access point. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The main content area is titled "System Information" and contains a table of system details. A yellow warning box at the top right of the main content area states "The current browser connection will be disconnected if you click here".

Parameter	Value
Model Name	DAP-2620
Firmware Version	v1.00 19:33:32 2019/03/25
System Name	dap2620
Location	
System Time	2019/05/17 16:55:30
Up Time	01:53:45
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	00:AA:BB:CC:DD:10
MAC Address (5GHz)	00:AA:BB:CC:DD:18
IP Address	192.168.1.166

# 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.

### Basic Settings

Change the wireless settings on the device for an existing network or create a new network.

**Wireless Band**  
This is the operating frequency band. This Access Point (AP), operates within 2 bands, 2.4GHz and 5GHz. 2.4GHz works best with legacy devices and suitable for longer ranges. Select 5GHz for least interference and better performance.

**Mode**  
Select between Access Point, Wireless Distribution System (WDS) with AP, WDS and Wireless Client mode.

**Network Name/Service Set Identifier (SSID)**  
The SSID factory default is "dlink". Change the SSID to connect to existing wireless networks or establish a new wireless network.

**SSID Visibility**  
The SSID Visibility signal is enabled by default. Select Disable to make the Access Point invisible to all client devices.

**Auto Channel Selection**  
Enabled by default, when the device boots up, to automatically search for the best available channel.

**Channel**  
Auto Channel Selection is set as default. Settings for the channel can be configured to work with existing wireless networks or customized a new wireless network.

**Channel Width**  
Setup the Channel bandwidths. Use 20MHz and Auto 20/40MHz for 802.11n and non-802.11n wireless devices. Connect Mixed 802.11b/g/n for 2.4GHz and Mixed 802.11a/n for 5GHz. Configure Auto 20/40/80 MHz for 802.11ac and non 802.11ac wireless devices, and Mixed 802.11ac for 5GHz. When using Auto 20/40 MHz channel settings data can be transmitted using 40MHz and when using Auto 20/40/80MHz data can be transmitted using 80MHz.

# 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-2620 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 (0.5 meters).
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 is not in use.

# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2620. 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 **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
  - Click **Connection** tab and set the dial-up option to Never Dial a Connection. Click **LAN Settings**. 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.

1. Click on **Start > Run**. In the run box type `cmd` and click **OK**.
2. 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.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

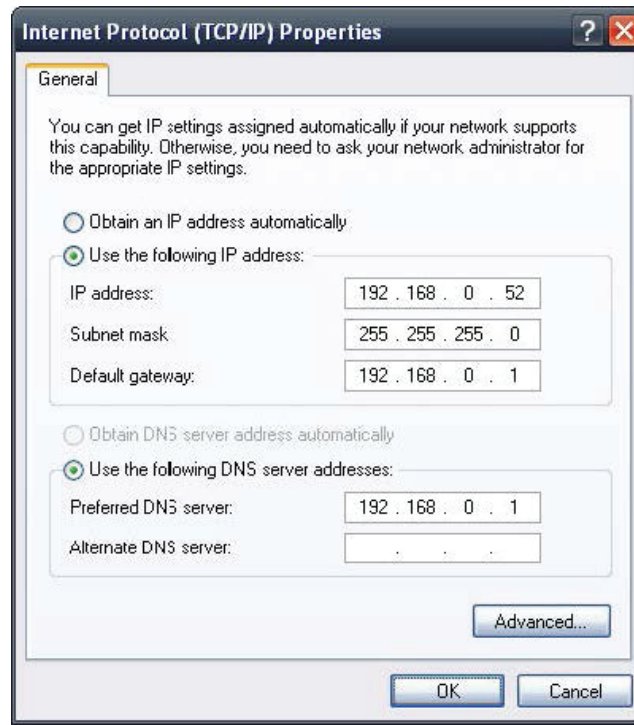
    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . .               : 10.5.7.114
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 10.5.7.1

C:\Documents and Settings>_
    
```

## How do I assign a static 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:

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**.
2. Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.
3. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
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.
5. Click **OK** twice to save your settings.



# Technical Specifications

- Standards**
- IEEE 802.11a/b/g/n/ac
  - IEEE 802.3i/u/ab

- Network Management**
- Telnet
  - Web (HTTP)
  - Secure Socket Layer (SSL)
  - Traffic control
  - D-Link Nuclias Connect

- Security**
- WPA™ Personal/Enterprise
  - WPA2™ Personal/Enterprise
  - WEP™ 64/128-bit encryption
  - SSID broadcast disable
  - MAC address access control
  - Internal RADIUS server

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

**Antenna Type** Two Dual Dand Internal Antennas (2.4 GHz 2 dBi & 5 GHz 2 dBi)

- Temperature**
- Operating: 0°C to 40°C (32°F to 104°F)
  - Storing: -20°C to 65°C (-4°F to 149)

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

- Certifications**
- FCC
  - CE

**Dimensions (L x W x H)** 153.5 x 94.65 x 35.8 mm (6.04 x 3.73 x 1.41 in)

- Weight**
- 212 g (0.47 lbs) without mounting bracket
  - 250.9 g (0.55 lbs) with mounting bracket

# Antenna Pattern

