

# NUCLIAS CONNECT DAP-2695 User Guide

V 2.00

---

# Table of Contents

<b>Nuclias Connect</b> .....	4	IPv6 Settings .....	24
Introduction .....	4	Advanced Settings .....	25
Nuclias Connect Key Features.....	5	Performance .....	26
<b>Setup</b> .....	6	Wireless Resource Control.....	28
Package Contents.....	6	Multi-SSID.....	30
System Requirements.....	6	VLAN.....	32
<b>Hardware Overview</b> .....	7	VLAN List.....	32
LEDs.....	7	Port List.....	33
Connections .....	7	Add/Edit VLAN .....	34
<b>Basic Installation</b> .....	8	PVID Settings.....	35
Hardware Setup .....	8	Intrusion.....	36
Configure the Access Point .....	8	Schedule .....	37
<b>Setup Wizard</b> .....	10	Internal RADIUS Server.....	38
<b>Web User Interface</b> .....	11	ARP Spoofing Prevention .....	39
Wireless .....	12	Bandwidth Optimization .....	40
Access Point Mode .....	12	Captive Portal.....	42
WDS with AP Mode.....	14	Authentication Settings-Web Redirection Only	42
WDS Mode .....	16	Authentication Settings- Username/Password..	44
Wireless Client Mode.....	18	Authentication Settings- Passcode .....	46
Wireless Security .....	19	Authentication Settings- Remote RADIUS.....	48
Wired Equivalent Privacy (WEP) .....	19	Authentication Settings- LDAP.....	50
Wi-Fi Protected Access (WPA / WPA2).....	20	Authentication Settings- POP3.....	52
802.1x.....	22	Login Page Upload.....	54
LAN .....	23	MAC Bypass.....	55
		DHCP Server .....	56
		Dynamic Pool Settings.....	56

Static Pool Setting .....	57	Login Settings .....	76
Current IP Mapping List.....	58	Console Settings .....	77
Filters.....	59	SNMP Settings .....	77
Wireless MAC ACL.....	59	Ping Control Setting .....	77
WLAN Partition .....	60	Nuclias Connect Settings.....	78
IP Filter Settings.....	61	DDP Control Setting .....	78
Traffic Control.....	62	Country Setting .....	78
Uplink/Downlink Setting .....	62	Firmware and SSL Certification Upload.....	79
QoS.....	63	Configuration File Upload .....	80
Traffic Manager.....	64	Time and Date Settings .....	81
Status .....	65	Configuration and System.....	82
Device Information .....	66	System Settings.....	83
Client Information .....	67	Help .....	84
WDS Information Page .....	68	<b>Knowledge Base .....</b>	<b>85</b>
Channel Analyze .....	69	Wireless Basics .....	85
Statistics.....	70	Wireless Installation Considerations.....	86
Ethernet Traffic Statistics.....	70	<b>Troubleshooting .....</b>	<b>87</b>
WLAN Traffic Statistics.....	71	Why can't I access the web-based configuration	
Log .....	72	utility? .....	87
View Log.....	72	What can I do if I forgot my password?.....	87
Log Settings.....	73	How to check your IP address? .....	88
Maintenance Section .....	74	How to statically assign an IP address?.....	89
Administration.....	75	<b>Technical Specifications .....</b>	<b>90</b>
Limit Administrator .....	75		
System Name Settings.....	76		

# 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 (up to 1,000 APs), while retaining a robust and centralized management system. And 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 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 Access Points (APs) without licensing charges, coupled with an inexpensive optional hardware controller (The 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 admins 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 & manage a variety of distributed deployments, including setting & 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, AD
- 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-2695, please refer to the Nuclias Connect User Guide.

# Setup

## Package Contents

- DAP-2695 Access Point
- Six Detachable Antennas
- Power Adapter (Optional)
- Mounting Plate and Hardware
- Ethernet Cable
- Quick Install Guide

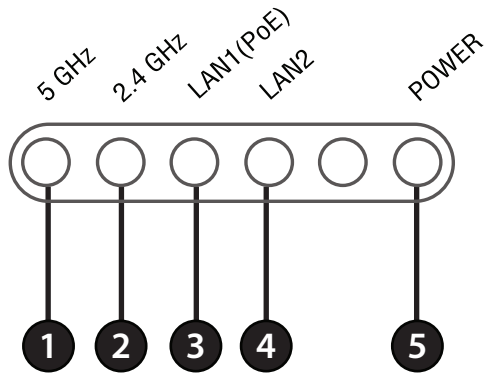
**Note:** *Using a power supply with a different voltage rating than the one included with the DAP-2695 will cause damage and void the warranty for this product.*

## System Requirements

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

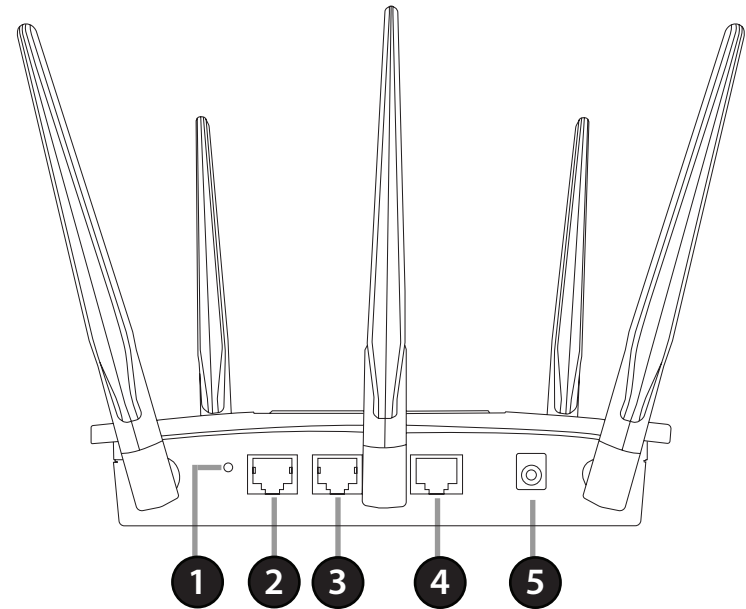
# Hardware Overview

## LEDs



<b>1</b>	5GHz	When lit, the access point is operating at 5GHz. This light will blink when there is wireless traffic.
<b>2</b>	2.4GHz	When lit, the access point is operating at 2.4GHz. This light will blink when there is wireless traffic.
<b>3</b>	LAN1 (PoE)	Solid light when the Ethernet port is connected to a power over Ethernet (PoE) port, such as a router or switch. The light will blink when there is traffic through LAN port.
<b>4</b>	LAN2	Solid light when the Ethernet port is connected to a working port, such as a router or switch. The light will blink when there is traffic through LAN port.
<b>5</b>	Power	The light will blink during boot up. Once solid, the access point is ready.

## Connections



<b>1</b>	Reset Button	Press and hold for six seconds to reset the access point to the factory default settings.
<b>2</b>	Console Port	Connect the supplied console cable to configure using a command line interface.
<b>3</b>	LAN2 Port	Connect to your network with an Ethernet cable.
<b>4</b>	LAN1 (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router.
<b>5</b>	Power Receptor	Connect the supplied power adapter. (*Optional)

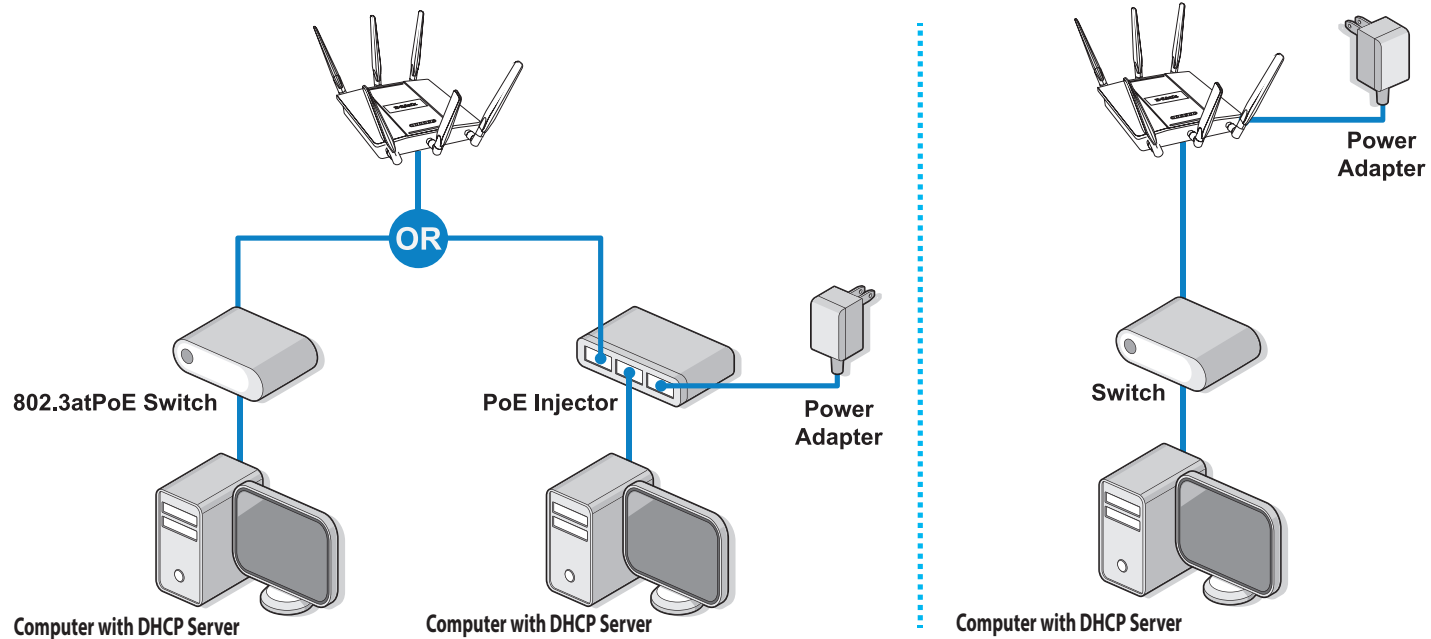
# Basic Installation

## Hardware Setup

To power on the DAP-2695, you can use ONE of the following methods:

1. Plug one end of your Ethernet cable into the LAN port of the DAP-2695, and the other end into a port on a 802.3at PoE switch.
2. Separately purchase a DPE-301GI PoE injector if you need to connect the Access Point without a 802.3at PoE Switch.
3. Separately purchase a power adaptor to plug into the power receptor of the DAP-2695

### Configure the Access Point





To set up and manage the DAP-2695, 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 **dap2695.local** in the address field of your browser.  
Log in to the Administration user interface. The default login information is:  
Username: admin  
Password: admin
2. Connect the access point and your computer via DPE-301GI PoE injector. Manage the access point from the computer.  
Enter **dap2695.local** in the address field of your browser.  
Log in to the Administration user interface. The default login information is:  
Username: admin  
Password: admin
3. Connect the access point and your computer to the same network switch. Manage the access point from the computer.  
Enter **dap2695.local** in the address field on your browser.  
Log in to the Administration user interface. The default login information is:  
Username: admin  
Password: admin

# 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.

Once the settings are configured, click **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(NTP)  
 Manually

System Date

System Time(24 HR)  :

Enable Daylight Saving

DST Start(24 HR)   in  at

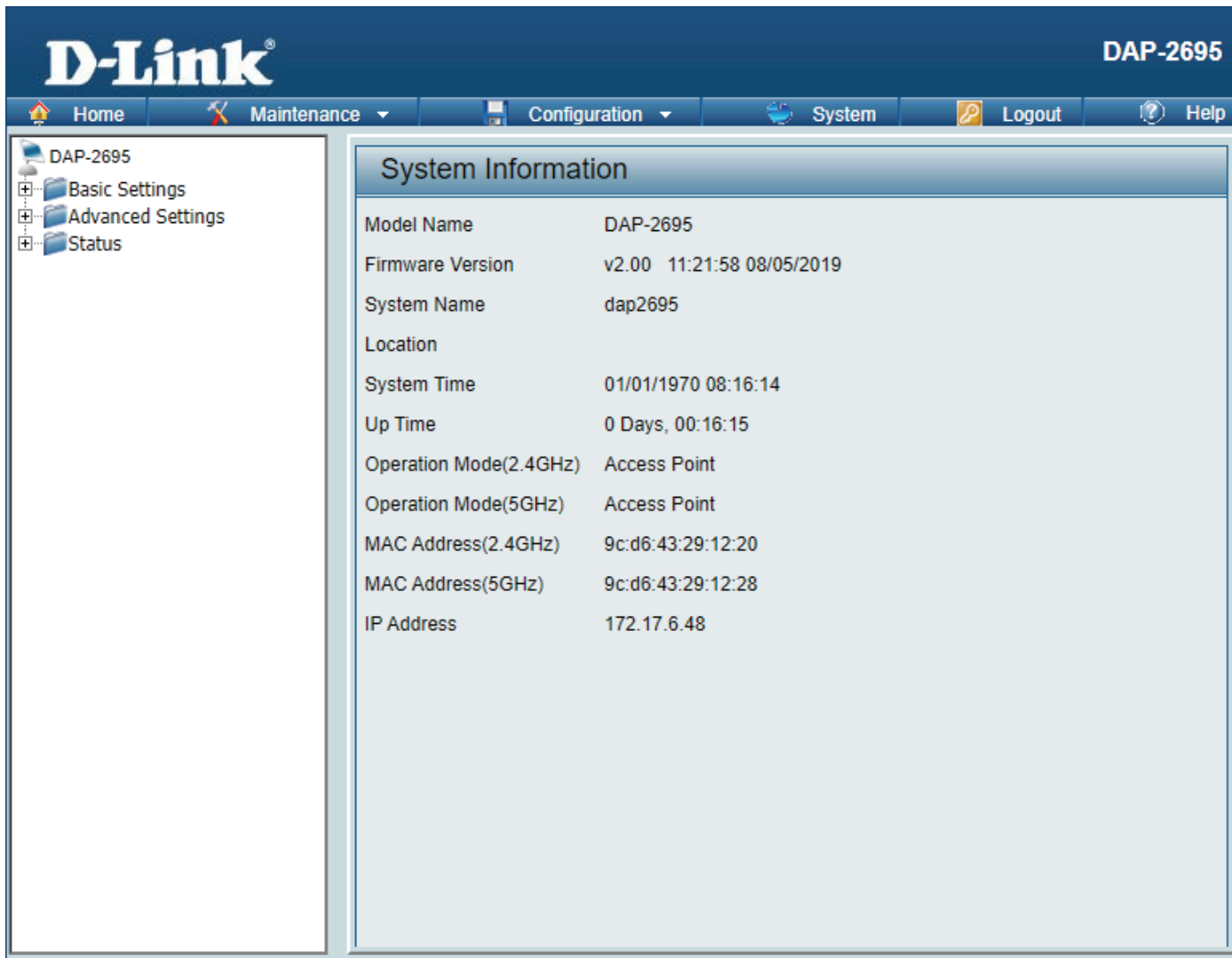
DST End(24 HR)   in  at

Daylight Offset(minutes)

System Country

# Web User Interface

The DAP-2695 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type **dap2695.local** in the address field and then press **Enter** to login. Most of the configurable settings are located in the menu of the left side of the web GUI which contains sections called **Basic Settings**, **Advanced Settings** and **Status**.



The screenshot displays the D-Link DAP-2695 web user interface. The top navigation bar includes the D-Link logo, the device name 'DAP-2695', and menu items: Home, Maintenance, Configuration, System, Logout, and Help. A left sidebar shows a tree view with 'DAP-2695' expanded to show 'Basic Settings', 'Advanced Settings', and 'Status'. The main content area is titled 'System Information' and contains the following data:

Model Name	DAP-2695
Firmware Version	v2.00 11:21:58 08/05/2019
System Name	dap2695
Location	
System Time	01/01/1970 08:16:14
Up Time	0 Days, 00:16:15
Operation Mode(2.4GHz)	Access Point
Operation Mode(5GHz)	Access Point
MAC Address(2.4GHz)	9c:d6:43:29:12:20
MAC Address(5GHz)	9c:d6:43:29:12:28
IP Address	172.17.6.48

# Wireless

On the wireless settings page, you can setup the basic wireless configuration for the access point. The user can choose from 4 different wireless modes:

**Access Point** - Used to create a wireless LAN

**WDS with AP** - Used to connect multiple wireless networks while still functioning as a wireless access point

**WDS** - Used to connect multiple wireless networks

**Wireless Client** - Used when the access point needs to act as a wireless network adapter for an Ethernet enabled device

## Access Point Mode

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

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

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

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

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

The screenshot displays the D-Link DAP-2695 Web User Interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with Basic Settings (Wireless, LAN, IPv6), Advanced Settings, and Status. The main content area is titled "Wireless Settings" and contains the following configuration options:

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

A "Save" button is located at the bottom right of the settings area.

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

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

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

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

## WDS with AP Mode

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

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

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

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

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

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

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

### Wireless Settings

Wireless Band 2.4GHz ▾

Mode WDS with AP ▾

Network Name (SSID)

Auto Channel Selection Enable ▾

Channel 6 ▾

Channel Width 20 MHz ▾

AP MAC Address

Site Survey Scan

CH	RSSI	BSSID	Security	SSID

Authentication Open System ▾

Key Settings

Encryption  Disable  Enable

Key Type Key Size 64 Bits ▾

Key Type HEX ▾

Key Index(1~4) 1 ▾

Network Key

Confirm Key

(0-9,a-z,A-Z,~!@#%&^&\*()\_+`-={[]:~\|,./<>?)

Save

**AP MAC Address:** Enter the MAC addresses of the root AP of this WDS network. If left empty, then this device is the the root AP.

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

**Authentication:** 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.

## WDS Mode

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

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

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

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

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

**Channel:** All devices on the network must share the same channel. To change the channel, use the drop-down menu to make the desired selection.

**Channel Width:** Use the drop-down menu to choose 20 MHz or Auto 20/40 MHz.

**AP MAC Address:** Enter the MAC addresses of the root AP of this WDS network. If left empty, then this device is the the root AP.

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

- Wireless Band: 5GHz
- Mode: WDS
- Network Name (SSID): MESH\_5
- Auto Channel Selection: Enable
- Channel: 44
- Channel Width: Auto 20/40/80 MHz
- AP MAC Address: (empty)

Below the settings is a 'Site Survey' section with a 'Scan' button. A table with the following headers is visible:

CH	RSSI	BSSID	Security	SSID

The 'Authentication' section is set to 'WPA-Personal'. The 'PassPhrase Settings' section includes:

- WPA Mode: WPA2 Only
- Cipher Type: AES
- Group Key Update Interval: 3600 (Sec)
- PassPhrase: (masked with dots)
- Confirm PassPhrase: (masked with dots)

A notice at the bottom of the PassPhrase Settings section reads: 'notice: 8~63 in ASCII or 64 in Hex. (0-9,a-z,A-Z,~!@#%&\*()\_+`-={[]:\';",./<>?)'. A 'Save' button is located at the bottom right of the form.



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

**Authentication:** 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. No RADIUS server is required.

## Wireless Client Mode

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

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

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

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

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

**Channel:** The channel used will be displayed, and matches the AP that the DAP-2695 is connected to when set to Wireless Client mode.

**Channel Width:** Use the drop-down menu to choose 20 MHz or Auto 20/40 MHz.

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

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

### Wireless Settings

Wireless Band 5GHz ▾

Mode Wireless Client ▾

Network Name (SSID)

SSID Visibility Enable ▾

Auto Channel Selection Enable ▾

Channel 44 ▾

Channel Width Auto 20/40/80 MHz ▾

---

Site Survey

CH	RSSI	BSSID	Security	SSID

---

Authentication WPA-Personal ▾

PassPhrase Settings

WPA Mode AUTO (WPA or WPA2) ▾

Cipher Type AES ▾ Group Key Update Interval  (Sec)

PassPhrase

Confirm PassPhrase

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

---

Wireless MAC Clone

Enable

MAC Source Auto ▾

MAC Address  :  :  :  :  :

MAC Address

## 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 no 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:** Use the radio button to disable or enable encryption.

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

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

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

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

\*\*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
- Mode: Access Point
- Network Name (SSID): dlink
- SSID Visibility: Enable
- Auto Channel Selection: Disable
- Channel: 1
- Channel Width: 20 MHz
- Authentication: Open System
- Key Settings:
  - Encryption:  Enable
  - Key Type: HEX
  - Key Size: 64 Bits
  - Key Index(1~4): 1
  - Network Key: [Redacted]
  - Confirm Key: [Redacted]

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

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

WPA was created by the Wi-Fi Alliance to address the limitations and weaknesses found in WEP. This protocol is mainly based on the 802.11i standard. There are also two variations found in WPA called WPA-Personal (PSK) and WPA-Enterprise (EAP).

WPA-EAP requires the user to install a Radius Server on the network for authentication.

WPA-Personal does not require the user to install a Radius Server on the network.

Comparing WPA-PSK with WPA-EAP, WPA-PSK is seen as a weaker authentication but comparing WPA-PSK to WEP, WPA-PSK is far more secure than WEP. WPA-EAP is the highest level of wireless security a user can use for wireless today.

WPA2 is an upgrade of WPA. WPA2 yet again solves some possible security issues found in WPA. WPA2 has two variations called WPA2-Personal (PSK) and WPA2-Enterprise (EAP) which is the same as found with WPA.

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

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

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

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

The screenshot displays the 'Wireless Settings' configuration interface. The settings are as follows:

- Wireless Band: 2.4GHz
- Mode: Access Point
- Network Name (SSID): dlink
- SSID Visibility: Enable
- Auto Channel Selection: Disable
- Channel: 1
- Channel Width: 20 MHz
- Authentication: WPA-Personal
- PassPhrase Settings:
  - WPA Mode: AUTO (WPA or WPA2)
  - Cipher Type: Auto
  - Group Key Update Interval: 1800 (Seconds)
  - Manual:  (Selected)
  - Periodical Key Change:
  - Activated From: Sun 00:00
  - Time Interval: (1~168)hour(s)
  - PassPhrase: [Redacted]
  - Confirm PassPhrase: [Redacted]

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

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

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

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

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

**RADIUS Server Mode:** Choose external or Internal.

**RADIUS Server:** 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.

## 802.1x

802.1x is a standard for passing EAP over a wired or wireless LAN. With 802.1x, you package EAP messages in Ethernet frames and don't use PPP. This is desirable in situations in which the rest of PPP isn't needed, where you're using protocols other than TCP/IP, or where the overhead and complexity of using PPP is undesirable.

802.1x also requires the user to install a Radius Server on the network for authentication.

**Key Update Interval:** Choose interval (in seconds) in which the key is valid.

**RADIUS Server Mode:** Choose external or Internal.

**RADIUS Server:** 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.

The screenshot displays the 'Wireless Settings' configuration page. The 'Authentication' dropdown is set to '802.1X'. Below this, the 'RADIUS Server Settings' section is expanded, showing the following fields:

- Key Update Interval:** 300 (Sec)
- RADIUS Server Mode:** Radio buttons for 'External' (selected) and 'Internal'.
- Primary RADIUS Server Setting:**
  - RADIUS Server: [ ]
  - RADIUS Port: 1812
  - RADIUS Secret: [ ]
- Backup RADIUS Server Setting (Optional):**
  - RADIUS Server: [ ]
  - RADIUS Port: 1812
  - RADIUS Secret: [ ]
- Primary Accounting Server Setting:**
  - Accounting Mode: Disable
  - Accounting Server: [ ]
  - Accounting Port: 1813
  - Accounting Secret: [ ]
- Backup Accounting Server Setting (Optional):**
  - Accounting Server: [ ]
  - Accounting Port: 1813
  - Accounting Secret: [ ]

At the bottom right of the form is a 'Save' button.

## 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-2695. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

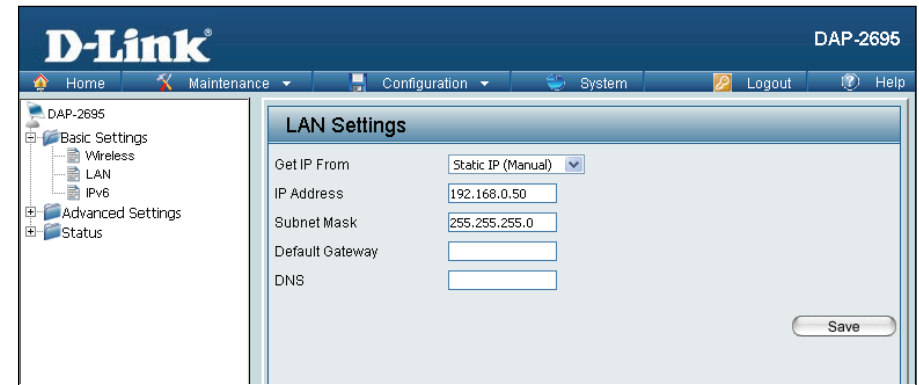
**Get IP From:** **Static IP (Manual)** is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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



The screenshot displays the D-Link web interface for the DAP-2695 device. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view with 'DAP-2695' expanded, containing 'Basic Settings', 'Wireless', 'LAN', 'IPv6', 'Advanced Settings', and 'Status'. The main content area is titled 'LAN Settings' and contains the following fields:

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

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

## IPv6 Settings

This section allows you to enable the IPv6 configuration of the device.

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

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

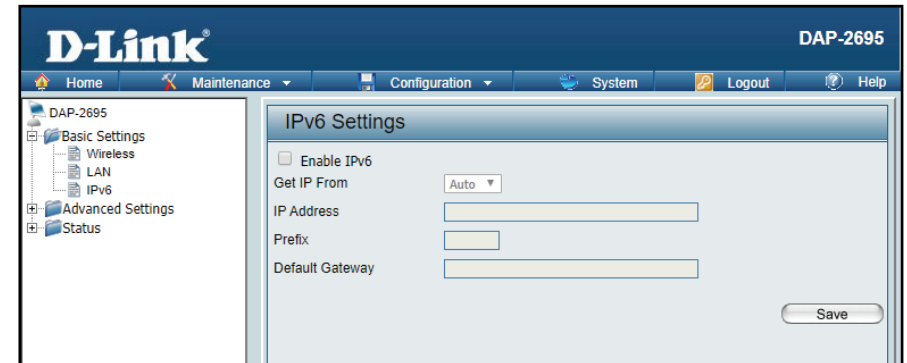
- **Auto:** Choose this option and the device can get IPv6 address automatically. The other fields will be grayed out.
- **Static:** Choose this option to set IPv6 address manually.

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

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

**Default**

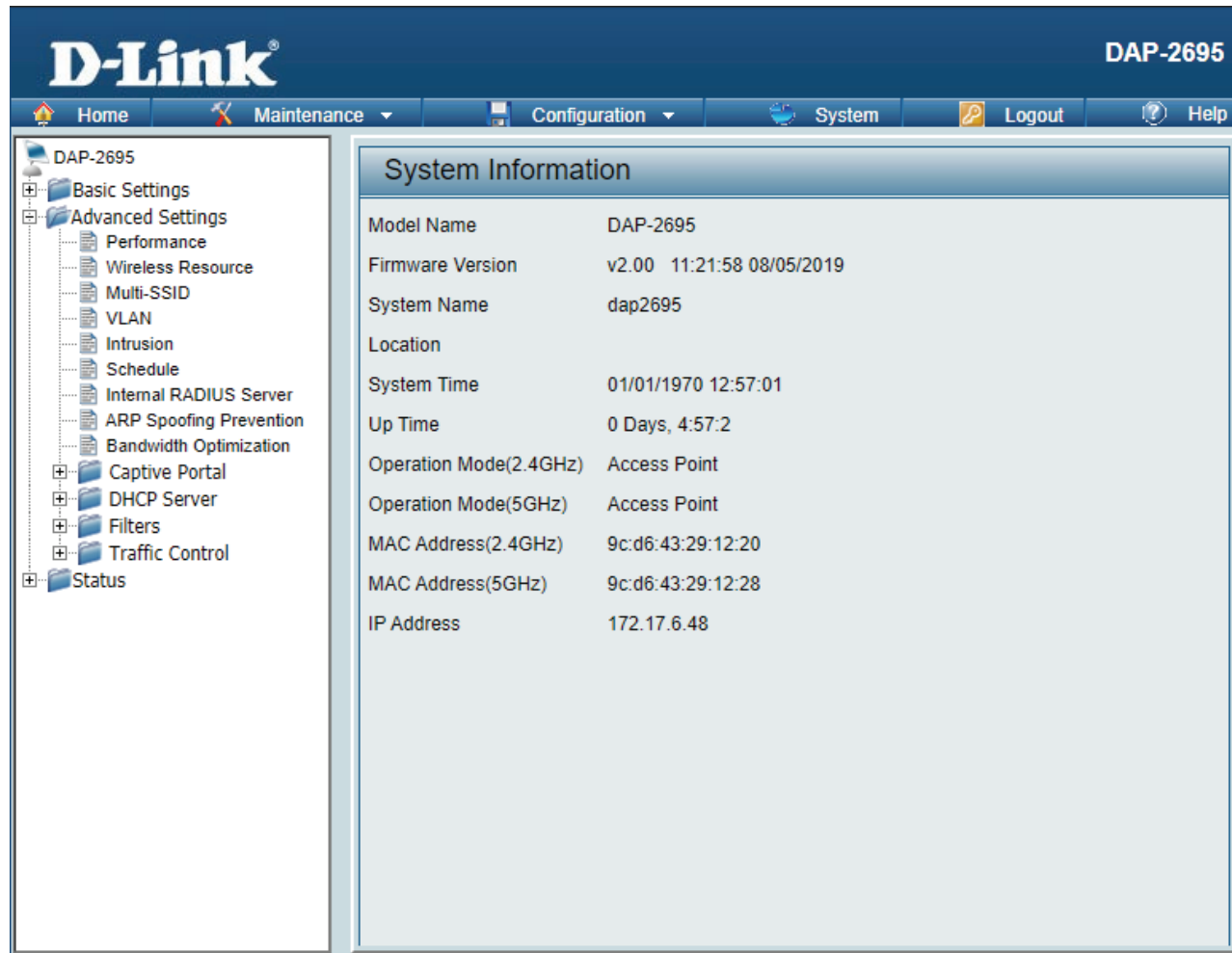
**Gateway:** Enter the LAN default gateway IPv6 address.





# Advanced Settings

In the Advanced Settings Section users can configure advanced settings concerning Performance, Multiple SSID, VLAN, Security, Quality of Service, AP Array, Web Redirection, DHCP Server, Filters and Scheduling. The following pages will explain settings found in the Advanced Settings section in more detail.



The screenshot displays the D-Link DAP-2695 web user interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of settings, with 'Advanced Settings' expanded to show sub-menus like 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 main content area shows the 'System Information' page with the following details:

System Information	
Model Name	DAP-2695
Firmware Version	v2.00 11:21:58 08/05/2019
System Name	dap2695
Location	
System Time	01/01/1970 12:57:01
Up Time	0 Days, 4:57:2
Operation Mode(2.4GHz)	Access Point
Operation Mode(5GHz)	Access Point
MAC Address(2.4GHz)	9c:d6:43:29:12:20
MAC Address(5GHz)	9c:d6:43:29:12:28
IP Address	172.17.6.48

## Performance

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

**Wireless Band:** Select either 2.4GHz or 5GHz.

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

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

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

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

**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.

Performance Settings	
Wireless band	5GHz
Wireless	On
Wireless Mode	Mixed 802.11ac
Data Rate	Best(Up to 1300) (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out (5GHz, 25~200)	25 (µs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable (Mbps)
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Disable
Transfer DHCP Offer to Unicast	Disable

Save

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

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

**Ack Time Out (2.4 GHZ, 64~200):** To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 25 and 200 microseconds for 5 GHz or from 64 to 200 microseconds in the 2.4 GHz in the field provided.

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

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

**Multicast Rate :** Select the multicast rate for 2.4GHz and 5GHz band.

**Maximum Multicast Bandwidth :** Set the multicast packets maximum bandwidth pass through rate from the Ethernet interface to the Access Point.

**Multicast Bandwidth Control :** Adjust the multicast packet data rate here. The multicast rate is supported in AP mode, (2.4 GHZ and 5 GHZ) and WDS with AP mode, including Multi-SSIDs.

**HT20/40 Coexistence :** Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40MHz and there is another wireless network's channel over-lapping and causing interference, the Access Point will automatically change to 20MHz.

**Transfer DHCP Offer to Unicast :** Enable to transfer the DHCP Offer to Unicast from LAN to WLAN, suggest to enable this function if stations number is larger than 30.

**STP Status:** Enable Spanning Tree Protocol Status to help prevent switching loops.

# Wireless Resource Control

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

**Wireless band:** Select **2.4GHz** or **5GHz**.

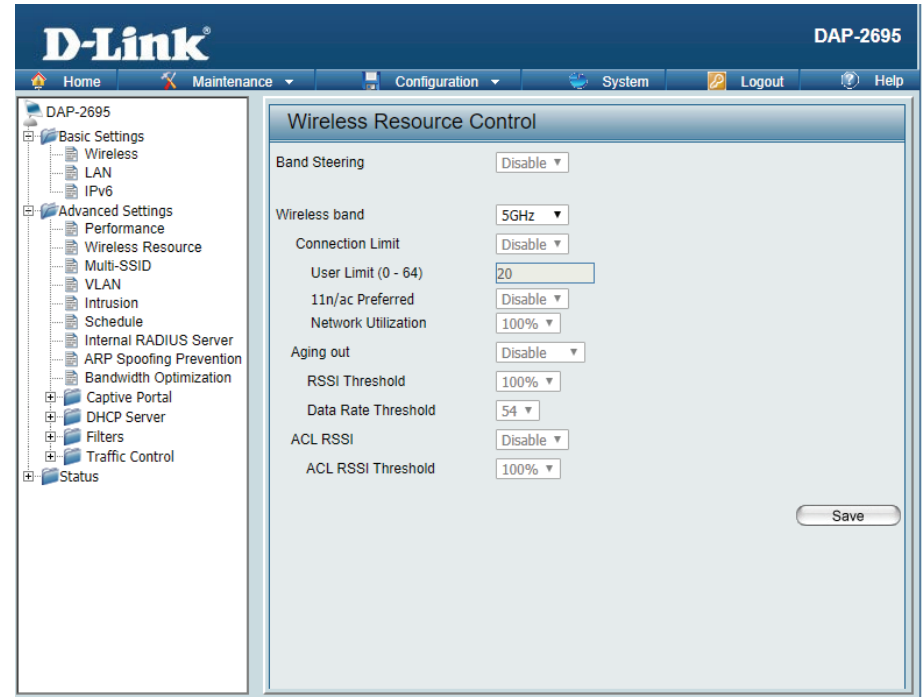
**Connection Limit:** Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled 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-2695 will not allow clients to associate with the AP.

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

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

**Network Utilization:** Set the maximum utilization of this access point for service. The DAP-2695 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.

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



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

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

**ACL RSSI:** Use the drop-down menu to **Enable** the 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:** Set the ACL RSSI Threshold.

## Multi-SSID

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

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

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

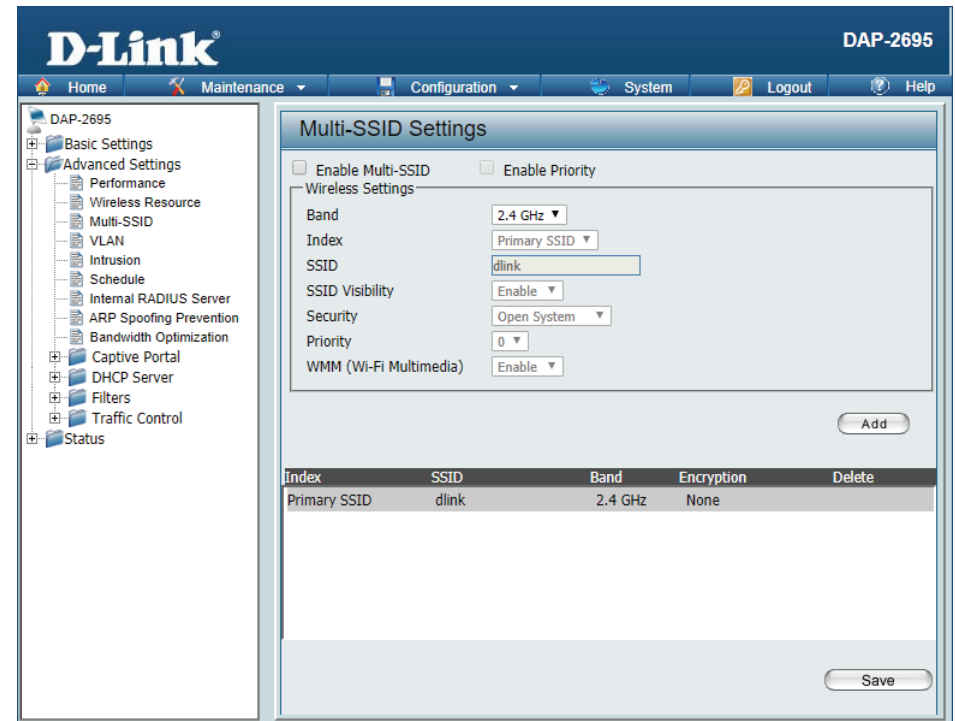
**SSID Visibility:** Enable or Disable SSID visibility. Enabling this feature broadcasts the SSID across the network, thus making it visible to all network users.

**Security:** The Multi-SSID security can be Open System, WPA-Personal, or WPA-Enterprise. For a detailed description of the Open System parameters please go to page 23. For a detailed description of the WPA-Personal parameters please go to page 24. For a detailed description of the WPA-Enterprise parameters please go to page 25.

**Priority:** Select the priority level of the SSID selected.

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

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



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

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

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

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

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

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

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

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

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

**RADIUS Server:** When you select WPA-Enterprise or 802.1x, enter the IP address of the RADIUS server. In addition, you must configure RADIUS Port and RADIUS Secret.

**Key Update Interval:** When you select 802.1x, choose an interval (in seconds) in which the key is valid.

**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.

# VLAN

## VLAN List

The DAP-2695 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-2695 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

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

**VLAN Mode:** The current VLAN mode is displayed.

**D-Link** DAP-2695

Home Maintenance Configuration System Logout Help

DAP-2695

- 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

### VLAN Settings

VLAN Status :  Disable  Enable Save

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

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)		



## Port List

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

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

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

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

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

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

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

## Add/Edit VLAN

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

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

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

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

### VLAN Settings

VLAN Status :  Disable  Enable Save

VLAN Mode : 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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="radio"/>

Save

## PVID Settings

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

**VLAN Status:** Use the radio button to toggle between Enable and Disable.

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

### VLAN Settings

VLAN Status :  Disable  Enable Save

VLAN Mode : 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	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

2.4GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

5GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

Save

## Intrusion

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

**Wireless Band** 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, Neighbor, Rogue, and New**.

The following is a definition of the listed AP categories:

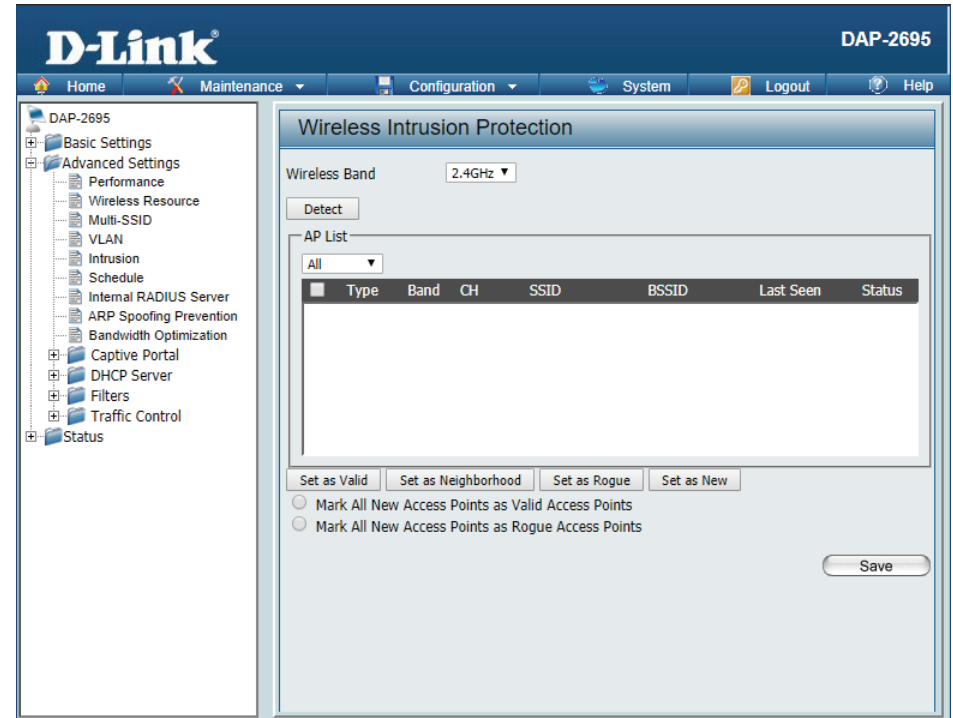
**Valid:** An AP which is authenticated to the network with encryption is classified as valid.

**Neighbor:** 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.



## Schedule

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

**Wireless Schedule:** Use the drop-down menu to enable the device's scheduling feature.

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

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

**SSID:** This read-only field indicates the current SSID in use. To create a new SSID, go to the Wireless Settings window (Basic Settings > Wireless).

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

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

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

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

The screenshot displays the D-Link DAP-2695 web interface for configuring wireless schedules. The left sidebar shows a tree view of settings, with 'Schedule' selected under 'Advanced Settings'. The main panel, titled 'Wireless Schedule Settings', features a 'Wireless Schedule' dropdown menu currently set to 'Disable'. Below this is the 'Add Schedule Rule' section, which includes input fields for 'Name', 'Index' (set to 'Primary SSID 2.4G'), and 'SSID' (set to 'dlink'). The 'Day(s)' section offers two radio button options: 'All Week' and 'Select Day(s)'. Under 'Select Day(s)', there are checkboxes for each day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat). There are also checkboxes for 'All Day(s)', 'Start Time', and 'End Time' (with an 'Overnight' checkbox). 'Add' and 'Clear' buttons are located below the 'Add Schedule Rule' section. A 'Schedule Rule List' table is positioned below, with columns for Name, SSID Index, SSID, Day(s), Time Frame, Wireless Edit, and DEL. The table is currently empty. At the bottom of the interface is a 'Save' button.

## Internal RADIUS Server

The DAP-2695 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the Save button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts to 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:** Toggle the drop-down menu between Enable and Disable.

**RADIUS Account List:** Displays the list of users.

The screenshot displays the D-Link DAP-2695 Web User Interface. The top navigation bar includes the D-Link logo, the device model 'DAP-2695', and menu items: Home, Maintenance, Configuration, System, Logout, and Help. A left-hand navigation tree shows the following structure:

- DAP-2695
  - 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 'Internal RADIUS Server'. It contains two sections:

- Add RADIUS Account:** This section includes three input fields: 'User Name', 'Password', and 'Status'. The 'Status' field is a dropdown menu currently set to 'Enable'.
- RADIUS Account list:** This section contains a table with the following headers: 'User Name', 'Enable', 'Disable', and 'Delete'. The table body is currently empty.

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

## ARP Spoofing Prevention

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

**ARP Spoofing Prevention:** This check box allows you to enable the ARP spoofing prevention function.

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

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

The screenshot displays the D-Link DAP-2695 Web User Interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view of settings categories: 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, and Status. The main content area is titled 'ARP Spoofing Prevention Settings'. It features a 'Disable' dropdown menu for 'ARP Spoofing Prevention'. Below this is the 'Add Gateway Address' section with input fields for 'Gateway IP Address' and 'Gateway MAC Address' (formatted as six boxes separated by colons), and 'Add' and 'Clear' buttons. The 'Gateway Address List' section shows 'Total Entries: 0' and a 'Delete All' button. A table with columns 'Gateway IP Address', 'Gateway MAC Address', 'Edit', and 'Delete' is present but empty. A 'Save' button is located at the bottom right of the settings area.

## Bandwidth Optimization

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

**Enable Bandwidth Optimization:** Use the drop-down menu to Enable the Bandwidth Optimization function.

**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.

**Allocate average BW for each station:** AP will distribute the average bandwidth for each client.

**Allocate maximum BW for each station:** Specify the maximum bandwidth for each connected client. Reserve certain bandwidth for future clients.

**Allocate different BW for a/b/g/n stations:** The weight of 11b/g/n and 11a/n client are 10%/20%/70% ; 20%/80%. AP will distribute different bandwidth for 11a/b/g/n clients.

**Allocate specific BW for SSID:** All clients share the total bandwidth.

**Rule Type:** Use the drop-down menu to select the type that is applied to the rule. Available options are: **Allocate average BW for each station**, **Allocate maximum BW for each station**, **Allocate different BW for 1a/b/g/n stations**, and **Allocate specific BW for SSID**.

### Bandwidth Optimization

Enable Bandwidth Optimization Enable

Downlink Bandwidth  Mbits/sec

Uplink Bandwidth  Mbits/sec

Add Bandwidth Optimization Rule

Rule Type Allocate average BW for each station

Band 2.4 GHz

SSID Index Primary SSID

Downlink Speed  Kbits/sec

Uplink Speed  Kbits/sec

Bandwidth Optimization Rules

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Del



**Band:** Use the drop-down menu to toggle the wireless band between 2.4GHz and 5GHz.

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

**Downlink Speed:** Enter a downloading speed limit in either Kbits/sec or Mbits/sec for the rule.

**Uplink Speed:** Enter an uploading speed limit in either Kbits/sec or Mbits/sec for the rule.

# 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, users 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 here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

**Band :** Select 2.4GHz or 5GHz.

**SSID Index :** Select the SSID for this Authentication.

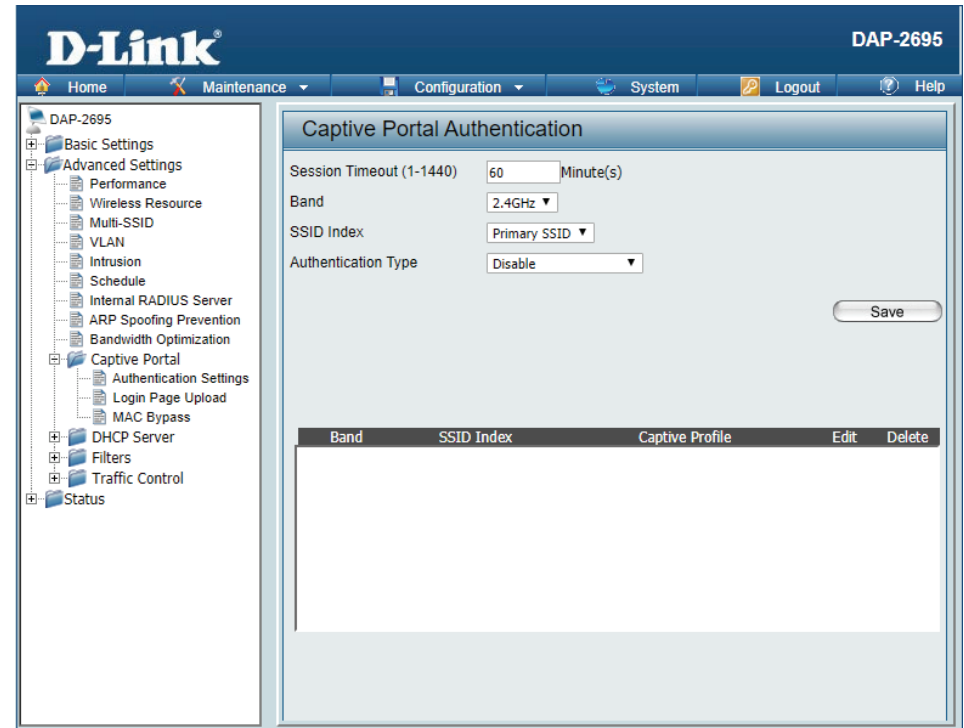
**Authentication Type :** Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Web Redirection option.

**Web Redirection State :** Default setting is **Enable** when select Web Redirection Only.

**URL Path :** Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

**IPIF Status :** Select to Enable or Disable the Captive Portal with its IP interface feature here.

**VLAN Group :** Enter the VLAN Group ID here.



**Get IP From :** Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

**IP Address :** 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.

### 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

## Authentication Settings- Username/Password

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 here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

**Band :** Select 2.4GHz or 5GHz.

**SSID Index :** Select the SSID for this Authentication.

**Authentication Type :** Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Username/Password option.

**Web Redirection State :** Default is Disable or select Enable to enable the website redirection feature.

**URL Path :** Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

**IPIF Status :** Select to Enable or Disable the Captive Portal with its IP interface feature here.

**VLAN Group :** Enter the VLAN Group ID here.

**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

**Username/Password Settings**

Username

Password

Username	Edit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

**Get IP From :** Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

**IP Address :** 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 here.

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

**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

**Username/Password Settings**

Username

Password

Username	Edit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

## 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, users 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 here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

**Band :** Select 2.4GHz or 5GHz.

**SSID Index :** Select the SSID for this Authentication.

**Authentication Type :** Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Passcode option.

**Web Redirection State :** Default is Disable or select Enable to enable the website redirection feature.

**URL Path :** Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

**IPIF Status :** Select to Enable or Disable the Captive Portal with its IP interface feature here.

**VLAN Group :** Enter the VLAN Group ID here.

### 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

**Passcode Settings**

Passcode Quantity

Duration  Hour

Last Active Time Year  Month  Day  Hour

User Limit

Passcode	Duration	Last Active Time	User Limit	Delete

**Get IP From :** Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

**IP Address :** 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 here.

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

**Last Active Day:** Select the last active date for this passcode here. 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

**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

**Passcode Settings**

Passcode Quantity

Duration  Hour

Last Active Time Year  Month  Day  Hour

User Limit

Passcode	Duration	Last Active Time	User Limit	Delete

## 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 here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

**Band :** Select 2.4GHz or 5GHz.

**SSID Index :** Select the SSID for this Authentication.

**Authentication Type :** Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Remote RADIUS option.

**Web Redirection State :** Default is Disable or select Enable to enable the website redirection feature.

**URL Path :** Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

**IPIF Status :** Select to Enable or Disable the Captive Portal with its IP interface feature here.

**VLAN Group :** Enter the VLAN Group ID here.

**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

**Remote RADIUS Settings**

**Radius Server Settings**

Radius Server  Radius Port

Radius Secret

Remote RADIUS Type

**Secondary radius Server Settings**

Radius Server  Radius Port

Radius Secret

Remote RADIUS Type

**Third radius Server Settings**

Radius Server  Radius Port

Radius Secret

Remote RADIUS Type

Band	SSID Index	Captive Profile	Edit	Delete



**Get IP From :** Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

**Subnet Mask :** 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 here

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

**Radius Port:** Enter the RADIUS server's shared secret here

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

**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

**Remote RADIUS Settings**

**Radius Server Settings**

Radius Server  Radius Port

Radius Secret

Remote RADIUS Type

**Secondary radius Server Settings**

Radius Server  Radius Port

Radius Secret

Remote RADIUS Type

**Third radius Server Settings**

Radius Server  Radius Port

Radius Secret

Remote RADIUS Type

Band	SSID Index	Captive Profile	Edit	Delete

## 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, users 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 here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

**Band :** Select 2.4GHz or 5GHz.

**SSID Index :** Select the SSID for this Authentication.

**Authentication Type :** Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the LDAP option.

**Web Redirection State :** Default is Disable or select Enable to enable the website redirection feature.

**URL Path :** Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

**IPIF Status :** Select to Enable or Disable the Captive Portal with its IP interface feature here.

**VLAN Group :** Enter the VLAN Group ID here.

**Get IP From :** Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

**Captive Portal Authentication**

Session Timeout (1-1440) 60 Minute(s)

Band 2.4GHz

SSID Index Primary SSID

Authentication Type LDAP

**Web Redirection Interface Settings**

Web Redirection State Disable

URL Path http://

**IP Interface Settings**

IPIF Status Disable

VLAN Group

Get IP From Static IP(Manual)

IP Address

Subnet Mask

Gateway

DNS

**LDAP Settings**

Server

Port 389

Authenticate Mode Simple

Username

Password

Base DN (ou=,dc=)

Account Attribute (ex.cn)

Identity  Auto Copy

Save

Band	SSID Index	Captive Profile	Edit	Delete

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

**Subnet Mask :** 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 here.

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

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

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

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

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

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

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

## Authentication Settings- POP3

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, users 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 here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

**Band :** Select 2.4GHz or 5GHz.

**SSID Index :** Select the SSID for this Authentication.

**Authentication Type :** Select the captive portal encryption type here. Options to choose from are Web Redirection, Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the POP3 option.

**Web Redirection State :** Default is Disable or select Enable to enable the website redirection feature.

**URL Path :** Select whether to use either HTTP or HTTPS here. After selecting either http:// or https://, enter the URL of the website that will be used in the space provided.

**IPIF Status :** Select to Enable or Disable the Captive Portal with its IP interface feature here.

**VLAN Group :** Enter the VLAN Group ID here.

### 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

**POP3 Settings**

Server

Port

Connection Type

Band	SSID Index	Captive Profile	Edit	Delete

**Get IP From:** Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2695. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

**Subnet Mask:** 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 here.

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

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

**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

POP3 Settings

Server

Port

Connection Type

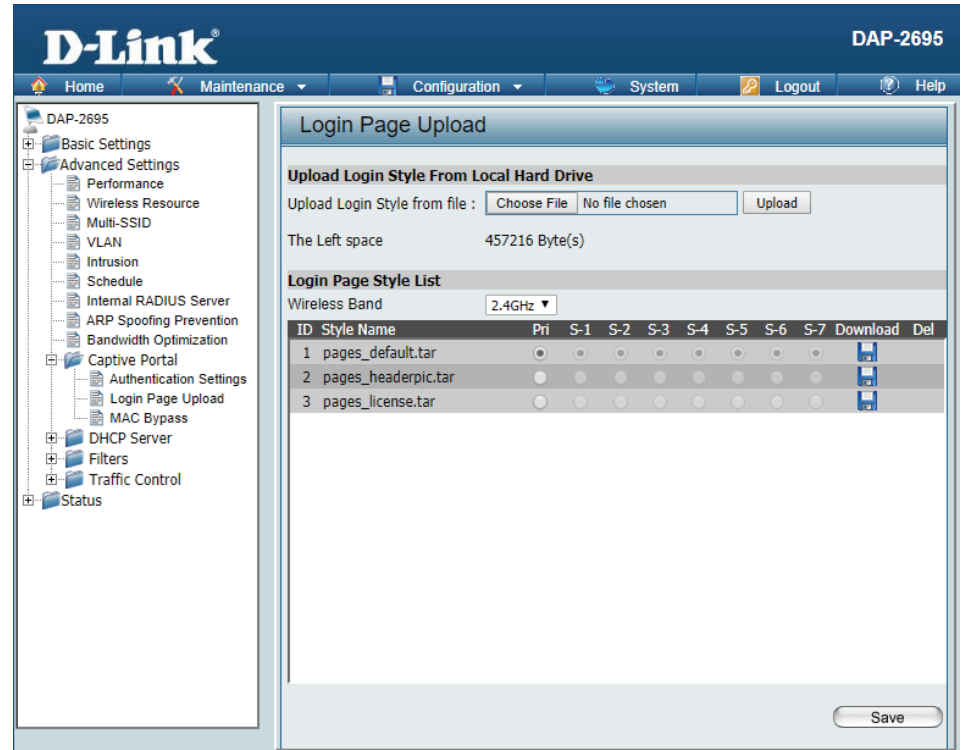
Band	SSID Index	Captive Profile	Edit	Delete

## Login Page Upload

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

**Upload Login Style From Local Hard Drive:** In this field the path to the login style file that will be uploaded will be displayed. Alternatively, the path can be manually entered here.

**Login Page Style List :** Select the wireless band and login style that will be used in each SSID here. Click Download button to download the template file for login page and Click the Del button to delete the template file.



## MAC Bypass

The DAP-2695 features a wireless MAC Bypass. Once a user is finished with these settings, click the Save button to let the changes take effect.

**Wireless Band:** Select the wireless band for MAC Bypass.

**SSID Index:** Select the SSID for 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 this list. Highlight a MAC address and click the Delete icon to remove it from this list.

**Upload 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.

**Load MAC File to Local Hard Driver:** To download the MAC bypass list file, click Download and to save the MAC bypass list.

The screenshot shows the D-Link DAP-2695 Web User Interface. The main content area is titled "MAC Bypass Settings". It contains the following elements:

- Wireless Band:** A dropdown menu set to "2.4GHz".
- SSID Index:** A dropdown menu set to "Primary SSID".
- MAC Address:** A text input field with a colon-separated format (e.g., : : : : : ) and an "Add" button.
- MAC Address List:** A table with columns for "ID", "MAC Address", and "Delete". The table is currently empty.
- Upload MAC File:** A section with a "Choose File" button, a "No file chosen" status, and an "Upload" button.
- Download MAC File:** A section with a "Download" button and the text "Load MAC File to Local Hard Driver".
- Save:** A "Save" button at the bottom right of the settings area.

The left navigation menu includes: DAP-2695, Basic Settings, Advanced Settings (Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization), Captive Portal (Authentication Settings, Login Page Upload, MAC Bypass), DHCP Server, Filters, Traffic Control, and Status.

# 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-2695 is capable of acting as a DHCP server.

**Function Enable/Disable:** Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses. Select Enable to allow the DAP-2695 to function as a DHCP server.

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

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

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

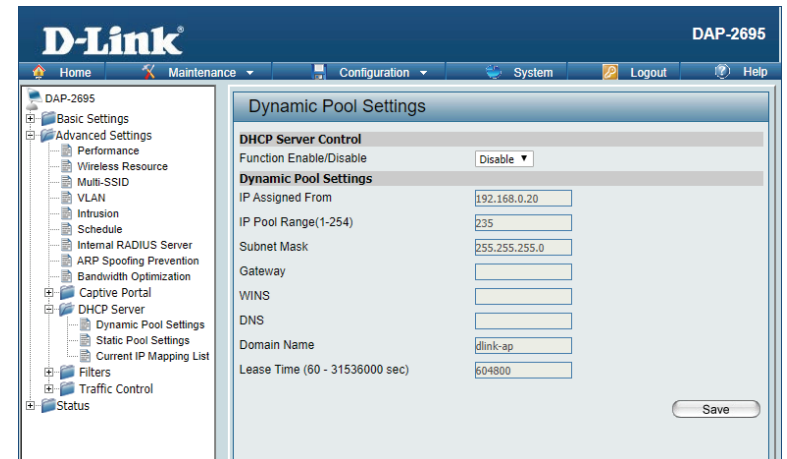
**Gateway:** Enter the IP address of the gateway on the network.

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

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

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

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





## Static Pool Setting

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

**Function Enable/Disable:** Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select Enable to allow the DAP-2695 to function as a DHCP server.

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

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

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

**Gateway:** Specify the Gateway address for the wireless network.

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

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

**Domain Name:** Specify the domain name for the network.

Static Pool Settings					
<b>DHCP Server Control</b>					
Function Enable/Disable	Enable ▾				
<b>Static Pool Setting</b>					
Host Name	<input type="text"/>				
Assigned IP	<input type="text"/>				
Assigned MAC Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Subnet Mask	255.255.255.0				
Gateway	<input type="text"/>				
WINS	<input type="text"/>				
DNS	<input type="text"/>				
Domain Name	dlink-ap				
<input type="button" value="Save"/>					
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 Profile:** These are IP address pools the DHCP server has assigned using the dynamic pool setting.

**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.

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

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

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

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

**Wireless Band:** Specify the current wireless band rate.

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

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

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

**SSID Index:** Choose from dropdown list which SSID to apply filter list to.

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

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

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

#### Wireless MAC ACL Settings

Wireless Band	<input type="text" value="2.4GHz"/>	Total : 512 Used : 0
Access Control List	<input type="text" value="Disable"/>	
SSID Index	<input type="text" value="Primary SSID"/>	
MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="button" value="Add"/>

ID	MAC Address	Delete

**Current Client Information**

MAC Address	SSID	Band	Authentication	Signal	Add

**Upload ACL File**

Upload File :

**Download ACL File**

Load ACL File to Local Hard Driver :

## WLAN Partition

This page allows the user to configure a WLAN Partition.

**Wireless Band:** Displays the current wireless band.

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

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

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

The screenshot shows the 'WLAN Partition' configuration page. It features several settings:

- Wireless Band:** A dropdown menu set to '2.4GHz'.
- Link Integrity:** A dropdown menu set to 'Disable'.
- Ethernet to WLAN Access:** A dropdown menu set to 'Enable'.
- Internal Station Connection:** A section with a table of radio buttons for each SSID type.

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

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

## IP Filter Settings

Enter the IP address or network address that will be used in the IP filter rule. For example, an IP address like 192.168.70.66 or a network address like 192.168.70.0. This IP address or network will be inaccessible to wireless clients in this 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.

**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** icon to remove it from the list.

**Upload IP Filter File:** To upload a IP filter list file, click **Choose File** 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.

### IP Filter Settings

Wireless Band:

SSID Index:

Filter State:

IP Address:

Subnet Mask:

ID	IP Address	Subnet Mask	Delete

**Upload IP Filter File**

Upload File :  No file chosen

**Download IP Filter File**

Load IP Filter File to Local Hard Driver :

# Traffic Control

## Uplink/Downlink Setting

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 the **Save** button to let your changes take effect.

**Downlink Bandwidth:** The downlink bandwidth in Mbits per second.

**Uplink Bandwidth:** The uplink bandwidth in Mbits per second.

The screenshot displays the D-Link DAP-2695 Web User Interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view of configuration options, with 'Traffic Control' expanded to show 'Uplink/Downlink Settings', 'QoS', and 'Traffic Manager'. The main content area is titled 'Uplink and Downlink Setting' and features the following elements:

- LAN1 and LAN2 settings with checkboxes for 'Downlink' and 'Uplink'.
- Radio buttons for '2.4GHz' and '5GHz'.
- 'Downlink Interface' section with checkboxes for 'Primary-ssid' and 'Multi-ssid1' through 'Multi-ssid7'.
- 'Uplink Interface' section with checkboxes for 'Primary-ssid' and 'Multi-ssid1' through 'Multi-ssid7'.
- Input fields for 'Downlink Bandwidth(1~1300)' and 'Uplink Bandwidth(1~1300)', both set to '100' Mbits/sec.
- A 'Save' button at the bottom right.

## QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2695 supports four priority levels. Once the desired QoS settings are finished, click the **Save** button to let your changes take effect.

**Enable QoS:** Check this box to allow QoS to prioritize traffic. Use the drop-down menus to select the four levels of priority. Click the Save button when you are finished.

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

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

**QoS**

Enable QoS

**Advanced QoS**

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 %

Save

## Traffic Manager

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

**Traffic Manager:** Use the drop-down menu to Enable the traffic manager feature.

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

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

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

Traffic Manager Disable ▾

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

---

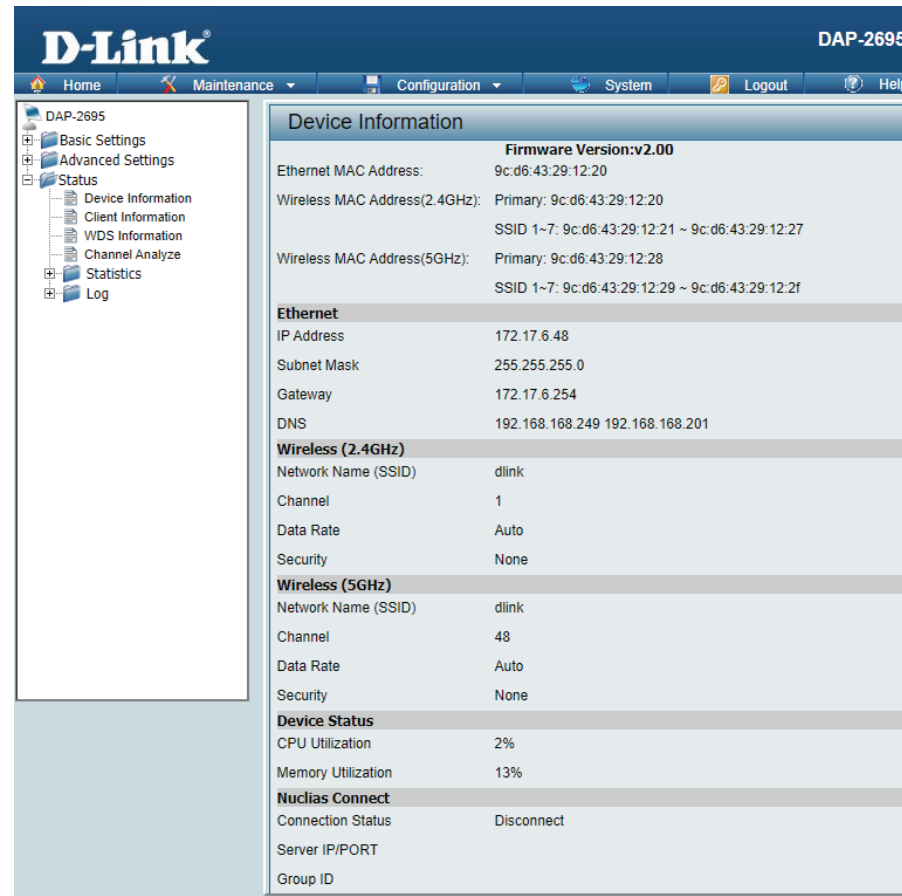
#### Traffic Manager Rules

Name	Client IP	Client MAC	Downlink Speed	Uplink Speed	Edit	Del



# 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-2695 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with categories like Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Channel Analyze, Statistics, and Log. The main content area is titled 'Device Information' and contains the following data:

Device Information	
<b>Firmware Version: v2.00</b>	
Ethernet MAC Address:	9c:d6:43:29:12:20
Wireless MAC Address(2.4GHz):	Primary: 9c:d6:43:29:12:20
	SSID 1~7: 9c:d6:43:29:12:21 ~ 9c:d6:43:29:12:27
Wireless MAC Address(5GHz):	Primary: 9c:d6:43:29:12:28
	SSID 1~7: 9c:d6:43:29:12:29 ~ 9c:d6:43:29:12:2f
Ethernet	
IP Address	172.17.6.48
Subnet Mask	255.255.255.0
Gateway	172.17.6.254
DNS	192.168.168.249 192.168.168.201
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	1
Data Rate	Auto
Security	None
Wireless (5GHz)	
Network Name (SSID)	dlink
Channel	48
Data Rate	Auto
Security	None
Device Status	
CPU Utilization	2%
Memory Utilization	13%
Nuclias Connect	
Connection Status	Disconnect
Server IP/PORT	
Group ID	

## Device Information

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

**Device Information:** This read-only window displays the configuration settings of the DAP-2695, including the firmware version and the device's MAC address.

The screenshot shows the D-Link web interface for a DAP-2695 device. The main content area is titled "Device Information" and contains the following data:

Firmware Version:v2.00	
Ethernet MAC Address:	9c:d6:43:29:12:20
Wireless MAC Address(2.4GHz):	Primary: 9c:d6:43:29:12:20
	SSID 1~7: 9c:d6:43:29:12:21 ~ 9c:d6:43:29:12:27
Wireless MAC Address(5GHz):	Primary: 9c:d6:43:29:12:28
	SSID 1~7: 9c:d6:43:29:12:29 ~ 9c:d6:43:29:12:2f
Ethernet	
IP Address	172.17.6.48
Subnet Mask	255.255.255.0
Gateway	172.17.6.254
DNS	192.168.168.249 192.168.168.201
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	1
Data Rate	Auto
Security	None
Wireless (5GHz)	
Network Name (SSID)	dlink
Channel	48
Data Rate	Auto
Security	None
Device Status	
CPU Utilization	2%
Memory Utilization	13%
Nuclias Connect	
Connection Status	Disconnect
Server IP/PORT	
Group ID	

## Client Information

This page displays the associated clients SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-2695 network.

**Client Information:** This window displays the wireless client information for clients currently connected to the DAP-2695.

**SSID:** Displays the SSID of the client.

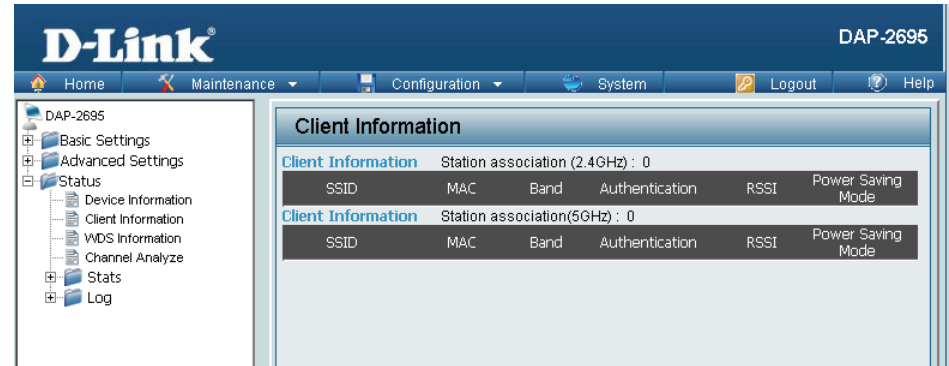
**MAC:** Displays the MAC address of the client.

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

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

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

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



The screenshot shows the D-Link DAP-2695 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with categories like Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Channel Analyze, Stats, and Log. The main content area is titled 'Client Information' and displays two tables for station associations.

Client Information						
Station association (2.4GHz) : 0						
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	
Client Information						
Station association(5GHz) : 0						
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	

## WDS Information Page

This page displays the access points SSID, MAC, band, authentication method, signal strength, and status for the DAP-2695's Wireless Distribution System network.

**WDS Information:** This window displays the Wireless Distribution System information for clients currently connected to the DAP-2695.

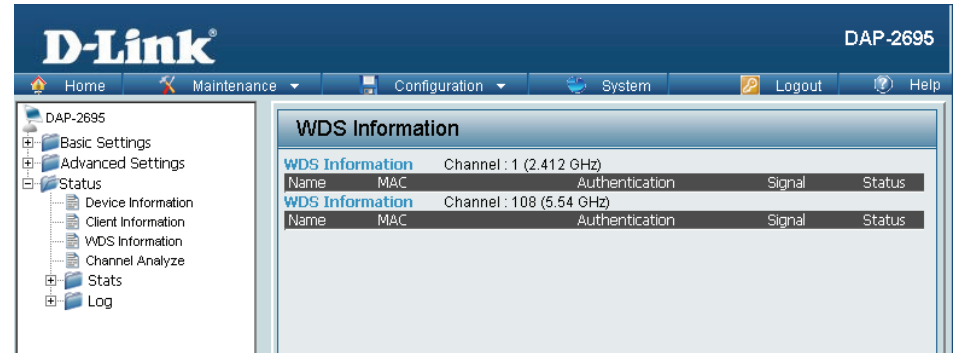
**Name:** Displays the SSID of the client.

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

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

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

**Status:** Displays the status of the power saving feature.

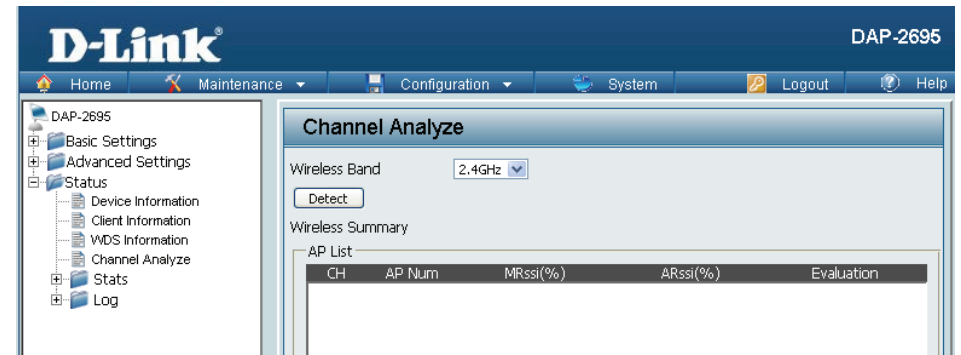


## Channel Analyze

**Wireless Band:** Select either 2.4Ghz or 5GHz.

**Detect:** Click the Detect button to scan.

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

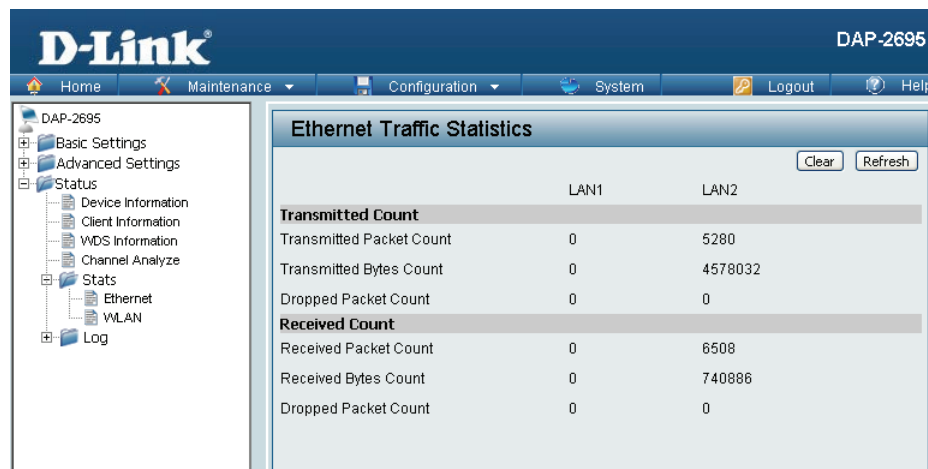


# Statistics

## Ethernet Traffic Statistics

Displays wired interface network traffic information.

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



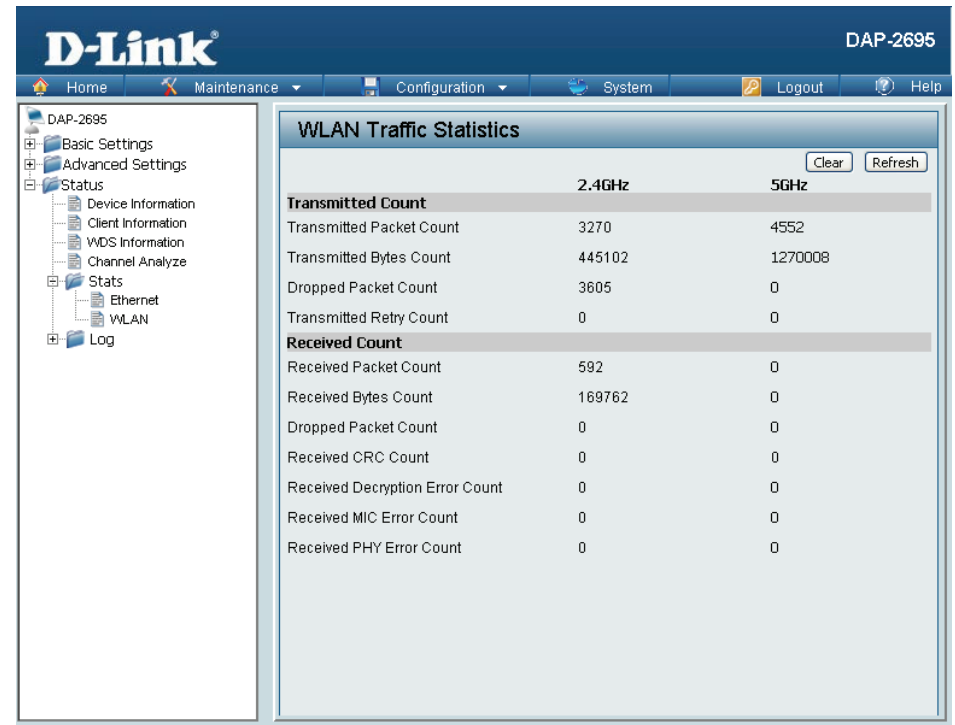
The screenshot shows the D-Link DAP-2695 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of the interface, with Ethernet selected under the Status section. The main content area displays the Ethernet Traffic Statistics page, which includes a table of traffic data for LAN1 and LAN2. The table is divided into Transmitted Count and Received Count sections. The data shows that LAN2 has transmitted 5280 packets and 4578032 bytes, and received 6508 packets and 740886 bytes. LAN1 has zero counts for all metrics.

	LAN1	LAN2
<b>Transmitted Count</b>		
Transmitted Packet Count	0	5280
Transmitted Bytes Count	0	4578032
Dropped Packet Count	0	0
<b>Received Count</b>		
Received Packet Count	0	6508
Received Bytes Count	0	740886
Dropped Packet Count	0	0

## WLAN Traffic Statistics

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

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



The screenshot shows the D-Link DAP-2695 Web User Interface. The page title is "WLAN Traffic Statistics". The interface includes a navigation menu on the left and a main content area with a table of statistics. The table has columns for "2.4GHz" and "5GHz". The statistics are categorized into "Transmitted Count" and "Received Count".

	2.4GHz	5GHz
<b>Transmitted Count</b>		
Transmitted Packet Count	3270	4552
Transmitted Bytes Count	445102	1270008
Dropped Packet Count	3605	0
Transmitted Retry Count	0	0
<b>Received Count</b>		
Received Packet Count	592	0
Received Bytes Count	169762	0
Dropped Packet Count	0	0
Received CRC Count	0	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:** The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.

The screenshot shows the D-Link DAP-2695 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar menu shows the following structure:

- DAP-2695
  - Basic Settings
  - Advanced Settings
  - Status
    - Device Information
    - Client Information
    - WDS Information
    - Channel Analyze
  - Stats
    - Ethernet
    - WLAN
  - Log
    - View Log
    - Log Settings

The main content area is titled "View Log" and shows "Page 1 of 11". The log table contains the following data:

Time	Priority	Message
Uptime 0 day 20:53:02	[Wireless]	2.4G:Deauth:Aging STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:43:29	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:43:07	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:42:55	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:41:03	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
Uptime 0 day 20:32:54	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:32:50	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
Uptime 0 day 20:32:19	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:32:14	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
Uptime 0 day 20:31:43	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:31:38	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
Uptime 0 day 20:31:07	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:31:01	[Wireless]	2.4G:Received disassociate:STA 10:0E:2B:AE:B6:90 (reason 1)
Uptime 0 day 20:30:30	[Wireless]	2.4G:Association Success:STA 10:0E:2B:AE:B6:90
Uptime 0 day 20:06:47	[Wireless]	2.4G:Deauth:Aging STA F0:7D:68:07:2C:B0
Uptime 0 day 19:56:45	[Wireless]	2.4G:Association Success:STA F0:7D:68:07:2C:B0
Uptime 0 day 19:56:45	[Wireless]	2.4G:Received Deauth:STA 00:24:01:AB:C0:10 (reason 6)
Uptime 0 day 19:56:44	[Wireless]	2.4G:Received Deauth:STA 00:24:01:AB:C0:10 (reason 6)



## 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 log type.

**Log Server / IP Address:** Enter the IP address of the EU directive Syslog server.

**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.

**To Email Address:** Enter the email address.

**Email Server Address:** Enter the email server address.

**SMTP Port:** Enter the SMTP port.

**User Name:** Enter the name of the new user entry.

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

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

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

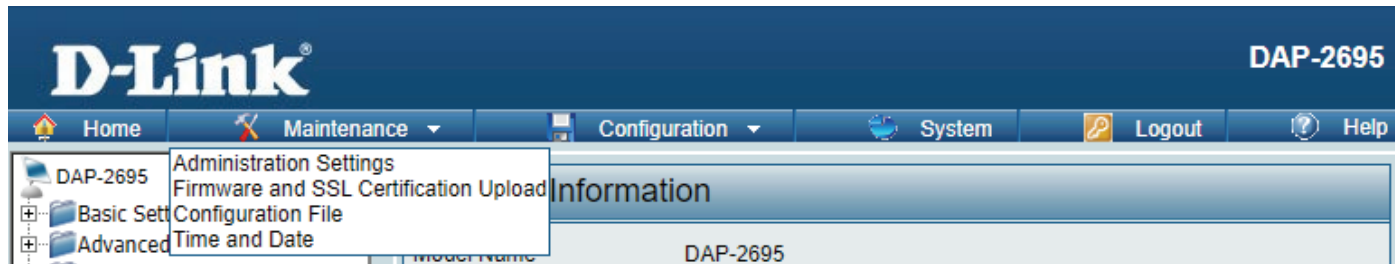
The screenshot shows the D-Link DAP-2695 Web User Interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with categories like Basic Settings, Advanced Settings, Status, Stats, and Log. The main content area is titled 'Log Settings' and contains the following fields:

- Log Settings:**
  - Log Server / IP Address: [Text Input]
  - Log Type:
    - System Activity
    - Wireless Activity
    - Notice
- Email Notification:**
  - Email Notification:  Enable
  - Outgoing mail server (SMTP): [Internal] (Dropdown)
  - Authentication:  Enable
  - SSL/TLS:  Enable
  - From Email Address: [Text Input]
  - To Email Address: [Text Input]
  - Email Server Address: [Text Input]
  - SMTP Port: [Text Input]
  - User Name: [Text Input]
  - Password: [Text Input]
  - Confirm Password: [Text Input]
- Email Log Schedule:**
  - Schedule: [0] (Dropdown) hours or when Log is full

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

# Maintenance Section

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



# Administration

## Limit Administrator

Check one or more of the five main categories to display the various hidden administrator parameters and settings displayed on the next five pages. Each of the five main categories display various hidden administrator parameters and settings. The administrator or users with administration privilege can access the administration management interface. By the default the admin account is not configured with a password. It is highly recommended to create a password before configuring the settings.

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

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

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

The screenshot shows the D-Link DAP-2695 Administration Settings page. The page is titled "Administration Settings" and includes a navigation menu on the left with options: Home, Maintenance, Configuration, System, Logout, and Help. The main content area is divided into several sections:

- Limit Administrator:** This section is checked. It includes:
  - Limit Administrator VLAN ID:** A checkbox labeled "Enable" is checked, and the value "1" is entered in the adjacent text box.
  - Limit Administrator IP:** A checkbox labeled "Enable" is unchecked.
  - IP Range:** Two text boxes labeled "From:" and "To:" are present, with an "Add" button to the right.
  - Table:** A table with columns "Item", "From", "To", and "Delete". The table is currently empty.
- System Name Settings:** A section with a minus sign icon.
- Login Settings:** A section with a minus sign icon.
- Console Settings:** A section with a minus sign icon.
- SNMP Settings:** A section with a minus sign icon.
- Ping Control Setting:** A section with a minus sign icon.
- Central WiFiManager Setting:** A section with a minus sign icon.

A "Save" button is located at the bottom right of the page.

## System Name Settings

**System Name:** Enter the name of the device. The default name is DAP-2695.

**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 dap2680.

System Name Settings <input checked="" type="checkbox"/>	
System Name	<input type="text" value="dap2695"/>
Location	<input type="text"/>
MDNS Name	<input type="text" value="dap2695"/>

## Login Settings

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

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

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

**Apply New Password:** Check to apply new password to devcie.

Login Settings <input checked="" type="checkbox"/>	
Login Name	<input type="text" value="admin"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/> <input type="checkbox"/> Apply New Password

## Console Settings

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

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

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

Console Settings <input checked="" type="checkbox"/>	
Status	<input checked="" type="checkbox"/> Enable
Console Protocol	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH
Timeout	3 Mins <input type="button" value="v"/>

## SNMP Settings

**Status:** Check the box to enable the SNMP functions.

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

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

**Trap Status:** Check the box to enable the trap function.

**Trap Server:** Enter the trap server IP address.

SNMP Settings <input checked="" type="checkbox"/>	
Status	<input type="checkbox"/> Enable
Public Community String	public
Private Community String	private
Trap Status	<input type="checkbox"/> Enable
Trap Server IP	

## Ping Control Setting

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

Ping Control Setting <input checked="" type="checkbox"/>	
Status	<input checked="" type="checkbox"/> Enable

## DDP Control Setting

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

DDP Control Setting <input checked="" type="checkbox"/>	
Status	<input type="checkbox"/> Enable

## Country Setting

**Select a Country:** Choose from drop down list country where device is located.

Country Settings <input checked="" type="checkbox"/>	
Select a Country	Taiwan ▼

## Nuclias Connect Settings

**Enable Nuclias Connect :** Select to enable or disable Nuclias Connect.

Nuclias Connect Setting <input checked="" type="checkbox"/>	
Enable Nuclias Connect	Disable ▼

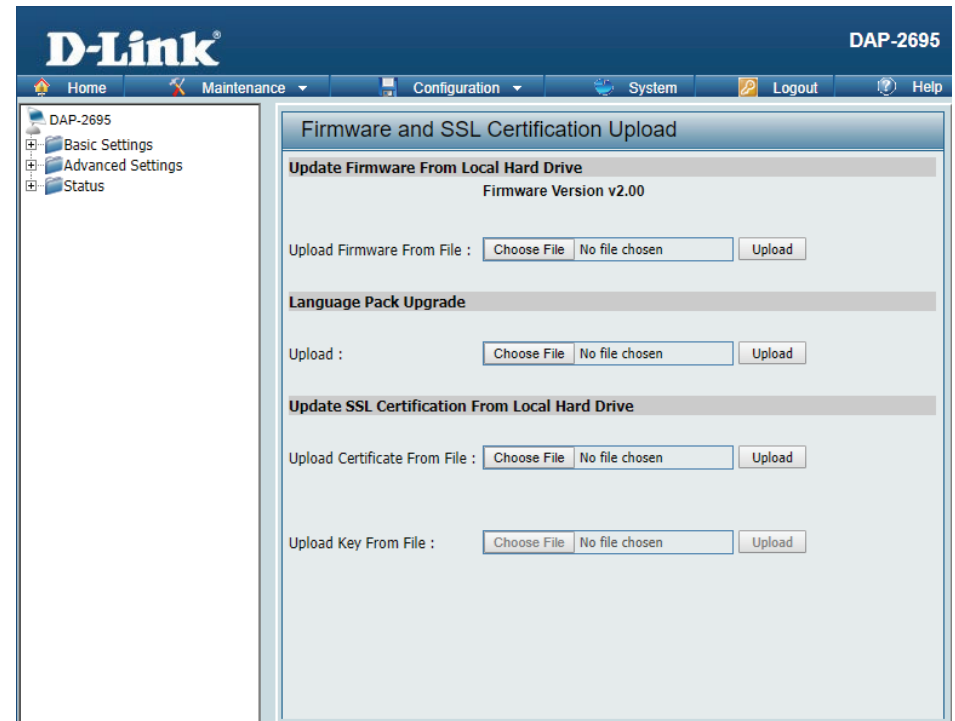
## Firmware and SSL Certification Upload

This page allows users to perform a firmware upgrade. A Firmware upgrade is a function that upgrades the the low-level access point software. 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 new firmware version 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 **Choose File** 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 **Choose File**. 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 **Choose File**. Select the certification and click **Open** and **Upload** to complete the upgrade.



The screenshot shows the D-Link web interface for the DAP-2695 device. The page title is "Firmware and SSL Certification Upload". The current firmware version is displayed as "Firmware Version v2.00". The interface includes three main sections for file uploads:

- Update Firmware From Local Hard Drive:** This section has a label "Upload Firmware From File :" followed by a "Choose File" button, a "No file chosen" status, and an "Upload" button.
- Language Pack Upgrade:** This section has a label "Upload :" followed by a "Choose File" button, a "No file chosen" status, and an "Upload" button.
- Update SSL Certification From Local Hard Drive:** This section has a label "Upload Certificate From File :" followed by a "Choose File" button, a "No file chosen" status, and an "Upload" button.

Below this, there is another section for "Upload Key From File :" with a "Choose File" button, a "No file chosen" status, and an "Upload" button.

The interface also features a navigation menu on the left with options: Home, Maintenance, Configuration, System, Logout, and Help. The top right corner shows the device name "DAP-2695".

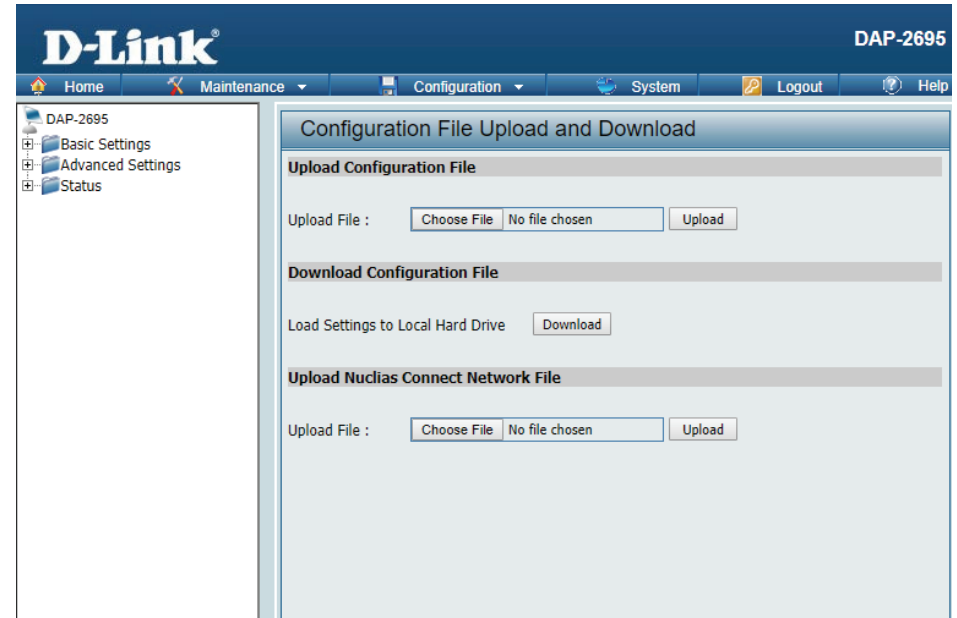
## Configuration File Upload

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

**Upload Configuration File:** After you have a configuration file, click **Choose File**. 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 Nuclias Connect AC1750 Dual Band PoE Access Point 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 **Choose File**. Select the saved Nuclias Connect file and click **Open** and **Upload** to upload the Nuclias Connect file.





## Time and Date Settings

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

**Current Time:** Displays the current time and date settings.

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

**NTP Server:** Enter the NTP server IP address.

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

**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 Daylight Saving Time.

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

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

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

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

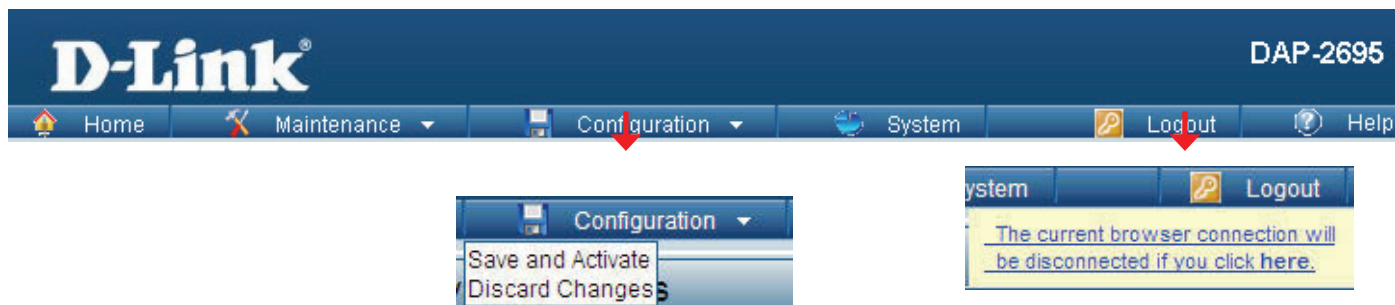
The screenshot shows the D-Link DAP-2695 web interface. The main content area is titled "Time and Date Settings". It is divided into several sections:

- Time Configuration:** Shows the "Current Time" as 01/03/1970 12:09:43.
- Automatic Time Configuration:** Includes a checkbox for "Enable NTP" (unchecked), an empty "NTP Server" input field, and a "Time Zone" dropdown menu set to "(GMT+08:00) Kuala Lumpur, Singapore".
- Set the Date and Time Manually:** Features dropdown menus for "Date And Time" (Year: 2019, Month: Oct, Day: 16, Hour: 15, Minute: 47, Second: 59) and a "Copy Your Computer's Time Settings" button.
- Daylight Configuration:** Includes a checkbox for "Enable Daylight Saving" (unchecked), a "Daylight Saving Offset" dropdown set to 15, and "Daylight Saving Dates" for both DST Start and DST End, each with dropdowns for Month, Week, Day, Hour, and Minute.

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

# Configuration and System

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



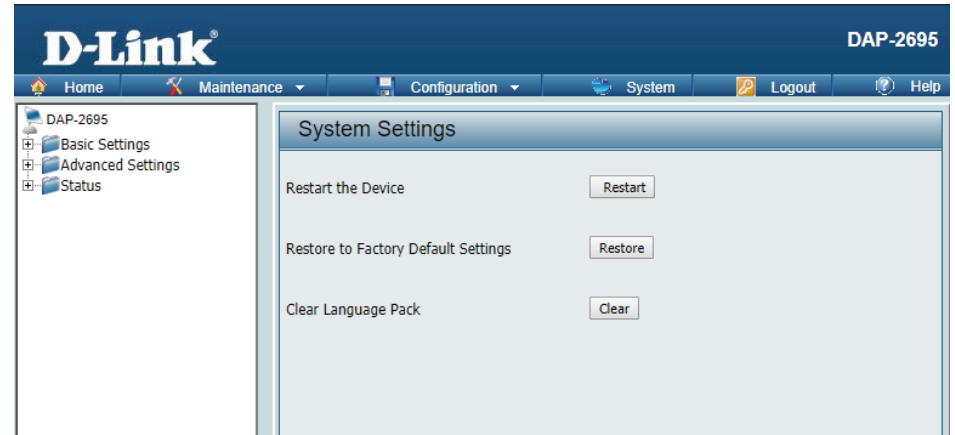
# System Settings

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

**Restart the Device:** Click Restart to restart the DAP-2695.

**Restore to Factory Default Settings:** Click Restore to restore the DAP-2695 back to factory default settings.

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



# Help

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

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

### Basic Settings

#### Wireless Settings

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

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

**Application**  
This option allows the user to choose for indoor or outdoor mode at the 5G Band.

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

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

**SSID Visibility**  
Indicate whether or not the SSID of your wireless network will be broadcasted. The default value of SSID Visibility is set to "Enable," which allows wireless clients to detect the wireless network. By changing this setting to "Disable," wireless clients can no longer detect the wireless network and can only connect if they have the correct SSID entered.

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

**Channel**  
Indicate the channel setting for the DAP-2553. By default, the AP is set to Auto Channel Scan. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

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

#### Authentication

# 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-2695 saves money by providing users with multi-functionality configurable in four different modes.
- **Scalability** - Configurations can be easily changed and range from Peer-to-Peer networks, suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

## Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the access point and other network devices to a minimum. Each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a
3. 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
4. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on the range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
5. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
6. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2695. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link access point (192.168.0.50 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 7.0 or higher, Chrome, Firefox, or Safari 4 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
- Configure your Internet settings:
  - Go to Start > Settings > Control Panel. Double-click the Internet Options Icon. From the Security tab, click the button to restore the settings to their defaults.
  - Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.
  - Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.
  - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

## What can I do if I forgot my password?

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

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

## How to check your IP address?

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

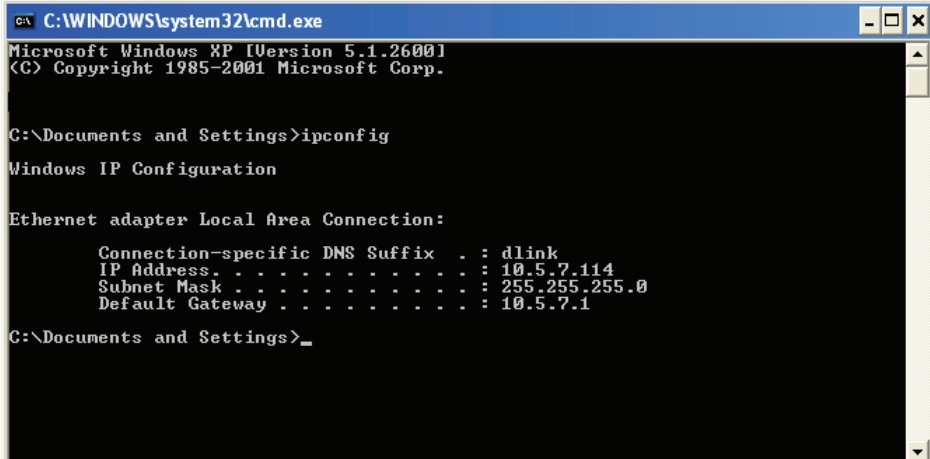
Click on Start > Run. In the run box type cmd and click OK.

At the prompt, type ipconfig and press Enter.

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

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

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



```
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 to statically assign an IP address?

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

### Step 1:

Windows® 2000: Click on Start > Settings > Control Panel > Network Connections

Windows XP: Click on Start > Control Panel > Network Connections

Windows Vista®: Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections

### Step 2:

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

### Step 3:

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

### Step 4:

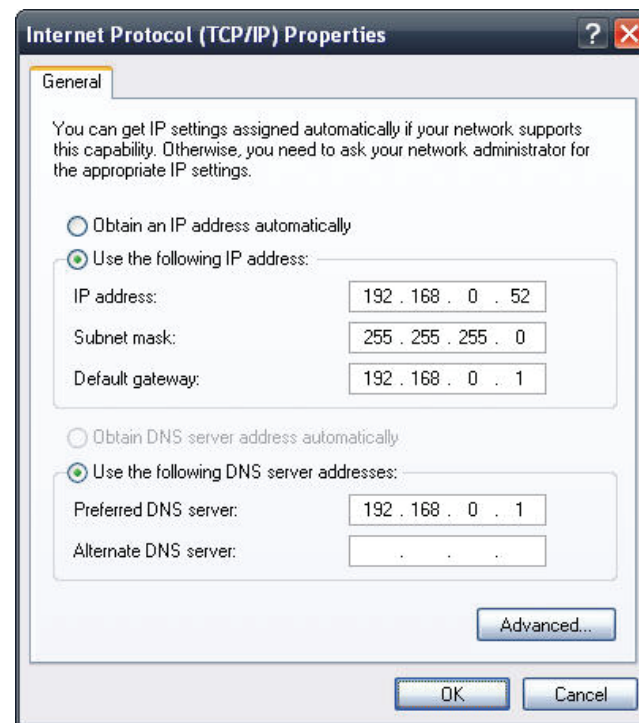
Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

### Step 5:

Click OK twice to save your settings.



# Technical Specifications

## Standards

- IEEE 802.11ac
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3at
- IEEE 802.3x

## Network Management

- Web Browser interface (HTTP, Secure HTTP (HTTPS))
- SNMP v1/v2c/v3
- Command Line Interface (Telnet, Secure SSH Telnet)
- D-Link Nuclias Connect

## Security

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

## Wireless Frequency Range

- 2.4 to 2.4835 GHz and 5.15 to 5.85 GHz\*\*

## Operating Voltage

- 48V/0.5A or 802.3at PoE

## Antenna Type

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

## LEDs

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

## Temperature

- Operating: 0°C to 40°C
- Storing: -20°C to 65°C

## Humidity

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

## Certifications

- FCC Class B
- CE
- UL
- IC
- Wi-Fi

## Dimensions

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