

DAP-2660 Version 1.01

802.11ac **Power over Ethernet (PoE) Access Point**

User Manual

Business Class Networking

Table of Contents

Product Overview	4
Introduction	4
Features	5
Package Contents	6
System Requirements	
Hardware Overview	7
LEDs	
Connections	
Basic Installation	R
Hardware Setup	
Method 1 - PoE with PoE Switch or Router	
Method 2 - PoE without PoE Switch or Router	9
Wethod 2 - PoE without PoE Switch or Router.	
	10
Web User Interface	10 11
Web User Interface Wireless	10 11
Web User Interface Wireless Access Point Mode	10 11 11
Web User Interface Wireless Access Point Mode WDS with AP Mode	10 11 11 13 15
Web User Interface Wireless Access Point Mode WDS with AP Mode WDS Mode	10 11 13 13 15 17
Web User Interface Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode	10 11 13 15 17 18
Web User Interface Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode Wireless Security	10 11 13 15 17 18 18
Web User Interface Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode Wireless Security Wireless Security Wired Equivalent Privacy (WEP)	
Web User Interface Wireless Access Point Mode WDS with AP Mode WDS Mode Wireless Client Mode Wireless Security Wireless Security Wired Equivalent Privacy (WEP) Wi-Fi Protected Access (WPA / WPA2)	

24
26
28
30
30
31
32
33
34
35
36
37
38
40
40
41
45
46
47
nly 47
d48
49
50
51
52
53

IP Filter Settings54
MAC Bypass55
DHCP Server56
Dynamic Pool Settings56
Static Pool Setting57
Current IP Mapping List58
Filters59
Wireless MAC ACL
WLAN Partition60
Traffic Control61
Uplink/Downlink Setting61
QoS62
Traffic Manager63
Status64
Status
Device Information65
Device Information65 Client Information66
Device Information65 Client Information66 WDS Information Page67
Device Information
Device Information65Client Information66WDS Information Page67Channel Analyze68Stats Page69Ethernet Traffic Statistics69WLAN Traffic Statistics70Log71View Log71Log Settings72

System Name Settings75
Login Settings75
Console Settings75
SNMP Settings76
Administration77
Central WiFiManager Settings77
Firmware and SSL Upload78
Configuration File Upload79
Time and Date Settings80
Configuration and System81
System Settings82
Help83
Knowledge Base84
Wireless Basics84
Wireless Basics
Wireless Installation Considerations
Wireless Installation Considerations85 Troubleshooting
Wireless Installation Considerations

Product Overview Introduction

D-Link, an industry pioneer in wireless networking, introduces a solution for businesses seeking to deploy next generation 802.11 ac LANs. D-Link unveils its new DAP-2660, designed specifically for environments with high traffic areas such as airports, coffee shops, shopping centers, sporting venues, and school campuses to provide secure and manageable dual band wireless network options for network administrators.

Versatile Access Point

The DAP-2660 Access Point allows network administrators to deploy a highly manageable and extremely robust dual band wireless network. For advanced installations, this new high-speed Access Point has integrated 802.3af Power over Ethernet (PoE) support, allowing installation of this device in areas where power outlets are not readily available. In addition to bridging 802.11ac and 802.11b/g/n wireless networks, the DAP-2660 can bridge to wired networks with its integrated Gigabit (10/100/1000Mbps) Ethernet port.

Enhanced Performance

The DAP-2660 delivers reliable wireless performance with maximum wireless signal rates of up to 1200Mbps. This, coupled with support for Wi-Fi Multimedia[™] (WMM) Quality of Service features, makes it an ideal access point for audio, video, and voice applications.

Security

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

Power Usage

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed. Network Standby: 3.46 watts Switched Off: 0.14 watts

^{*} In Hong Kong, for operation within 5.15 ~ 5.35GHz frequency range, it is restricted to indoor environment.

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

Features

- Provide Ethernet to Wireless LAN bridge fully IEEE 802.3/u/ab compatible on the Ethernet side and fully interoperable with IEEE 802.11ac and b/g/n compliant equipment
- Compatible with IEEE 802.11b high rate standard to provide wireless 11Mbps data rate*
- Compatible with IEEE 802.11g higher speed standard to provide wireless 54Mbps data rate*
- Compatible with IEEE 802.11a higher speed standard to provide wireless 54Mbps data rate*
- Compatible with IEEE 802.11n higher speed standard to provide wireless 300Mbps data rate*
- Compatible with IEEE 802.11ac higher speed standard to provide wireless 900Mbps data rate*
- Operation at 2.4~2.5GHz and 5.15~5.85GHz** frequency band to meet worldwide regulations
- Supports IEEE 802.11ac and b/g/n wireless data encryption with 64/128-bit WEP for security
- Supports enhanced security WPA-PSK and WPA2-PSK, RADIUS client, and Cipher negotiation
- Allows auto fallback data rate for reliability, optimized throughput and transmission range
- Web-based configuration and management
- Supports 802.3af PoE
- Supports 802.3az
- Supports one Gigabit Ethernet port
- AP Mode, WDS Mode, WDS with AP, and Wireless Client Mode
- Supports SNMP v1,v2,v3
- Support Trap server (SNMP v1, v2c)
- Support Central WiFiManager
- Support AP Array and AP Array Setup Tool

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

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

Package Contents

- DAP-2660 802.11ac Power over Ethernet (PoE) Access Point
- Mounting Plate and Hardware
- Ethernet Cable
- CD (with software and user manual)

NOTE no PSU supplied. To power the units use an D-Link PoE switch or the D-Link DPE-101GI PoE injector.

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

System Requirements

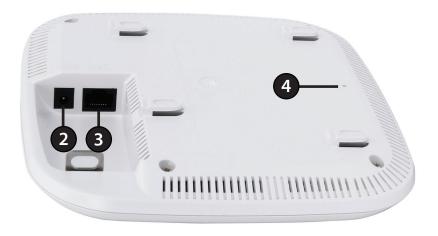
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer Version 7.0, Chrome 12, Safari 4, or Firefox 12 and above (for web-based configuration)

Hardware Overview

Connections



LEDs



		Solid Red	Indicates the access point has malfunctioned.
		Blinking Red	This LED will blink during boot-up.
1	Power/Status	Solid Green	Indicates that the DAP-2660 is working properly.
		Blinking Green	This light will blink green during data transmission.

2	Power Receptor	Connect the supplied power adapter. Power Receptor (*Note no longer used, replaced by PoE)
3	LAN (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router via an Ethernet cable.
4	Reset Button	Press and hold for five seconds to reset the access point to the factory default settings. Press and hold for one second to reboot the access point.

Basic Installation Hardware Setup

To power the access point, you can use one of the following 2 methods:

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

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

Method 1 - PoE with PoE Switch or Router

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

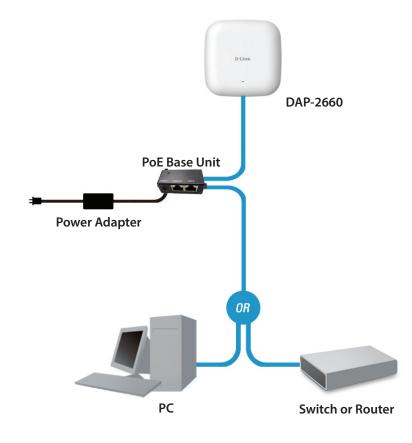
2. Connect the other end into one port on a PoE switch or router.



Method 2 - PoE without PoE Switch or Router

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

- 2. Connect one end of an Ethernet cable into the P+Data Out port on the PoE base unit and the other end into the LAN (PoE) port on the Access Point.
- 3. Use the supplied power adapter. Connect the power adapter to the **Power In** receptor on the PoE adapter.
- 4. Connect the power cable to the power adapter and then connect the other end into a power outlet.
- 5. Purchase separately a DPE-101GI PoE injector if you need to connect the Access Point without a PoE Switch.



Web User Interface

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

Basic Settings Advanced Settings Status Mode Firm Syste Local Syste Up Tr	stem Information Name ware Version em Name tion	DAP-2660 1.00 10:44:03 03 D-Link DAP-2660	8/06/2014	Degout	(?) He
Basic Settings Advanced Settings Status Syste Local Syste Up Tr	el Name ware Version em Name tion	DAP-2660 1.00 10:44:03 03 D-Link DAP-2660			
te-j≌ Status Firmv Syste Loca Syste Up Ti	ware Version em Name tion	1.00 10:44:03 03 D-Link DAP-2660			
Oper MAC MAC	ation Mode(2.4GHz ation Mode(5GHz) Address(2.4GHz) Address(5GHz))		

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.



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 changes. No RADIUS server is required.
- Select **WPA-Enterprise** to secure your network with the inclusion of a RADIUS server.
- Select **802.1X** if your network is using port-based Network Access Control.

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.



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

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

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

- Select Open System to communicate the key across the network.
- Select Shared Key to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.
- Select WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.

WDS Mode

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.

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

D-Link						DAP-2660
🔌 Home 🕺 Main	enance 👻	🚽 Configuration 👻	🤤 s	System 🛛	🖉 Logout	🕐 Help
DAP-2660	Wireles	ss Settings				
Bacic Settings	Wireless Bar Mode Network Nar SSID Visibilit Auto Channel Channel Wild WDS Remote AP 1. 5.	WDs me (SSID) dlink y Enat al Selection Disa th 20 M MAC Address 2. 6.			4. 8.	
	Authenticati	RSSI BSSID	Se	ecurity	SSID	Scan
	Key Settin Encryption Key Type Key Index(: Network Ke Confirm Key	gs (HD 1~4) 1 v y	iisable © Enabl	le Key Size *()_+`-=()[];`\;* ,.	64 Bits •	Save

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, Shared Key, or WPA-Personal.

- Select Open System to communicate the key across the network.
- Select Shared Key to limit communication to only those devices that share the same WEP settings.
- Select WPA-Personal to secure your network using a password and dynamic key changes. No RADIUS server is required.

Wireless Client Mode

Wireless Band:	Select either 2.4 GHz or 5 GHz from the drop-down menu.	D-Link				DAP-2660
		🏠 Home 🌋 Maintenanci	e 👻 🚽 Configura	ation 👻 👙 Sy	/stem 💋 Logou	it 🕐 Help
Mode:	Wireless Client is selected from the drop-down menu.	DAP-2660	Wireless Settings	2.4GHz 👻		
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.	LAN IPv8 Advanced Settings € Status	Mode Network Name (SSID) SSID Visibility Auto Channel Selection Channel Channel Width Site Survey	Vireless Client Vireless Client Client Cnable Cnable Cnable Auto 20/40 MHz V		
SSID Visibility:	This option is unavailable in Wireless Client mode.		CH RSSI	BSSID Sec	urity SSID	Scan
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-2660 is connected to when set to Wireless Client mode.		Authentication Key Settings Encryption Key Type Key Index(1~4) Network Key Confirm Key	Open System Open System Chable HEX I I	Key Size 64 Bits	•
Channel Width:	Use the drop-down menu to choose 20 MHz or Auto 20/40 MHz.		Wireless MAC Clone Enable MAC Source	(0-9,a-z,A-Z,~!@#\$%^&*	()_+`-={}[];'\:" ,,/<>?)	
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.		MAC Address MAC	C Address	: : Scan	_
Authentication:	Will be explained in the next topic.					
						Save

Wireless Security

Wireless security is a key concern for any wireless network installed. Unlike any other networking method wireless networks will broadcast it's presence for anyone to connect to it. Today, wireless security has advanced to a level where it is virtually impenetrable.

There are mainly two forms of wireless encryption and they are called Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first security method developed. It is a low level encryption but better than now encryption. WPA is the newest encryption standard and with the advanced WPA2 standard wireless networks have finally reach a point where the security is strong enough to give users the peace of mind when installing wireless networks.

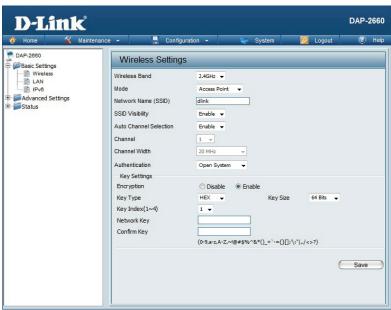
Wired Equivalent Privacy (WEP)

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.

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.

Wireless Setting	S
Wireless Band	2.4GHz 👻
Mode	Access Point 👻
Network Name (SSID)	dlink
SSID Visibility	Enable 🗸
Auto Channel Selection	Enable 👻
Channel	1 -
Channel Width	20 MHz 👻
Authentication	WPA-Personal 👻
PassPhrase Settings	
WPA Mode	AUTO (WPA or WPA2) 🔻
Cipher Type	Auto 👻 Group Key Update Interval 3600 (Seconds)
Manual	Periodical Key Change
Activated From	Sun 🚽 : 00 🚽 : 00 🚽
Time Interval	1 (1~168)hour(s)
PassPhrase	
Confirm PassPhrase	
	notice: 8~63 in ASCII or 64 in Hex. (0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}[];'\:" ,./<>?)
	Save

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: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

Account Server: Enter the IP address of the Account Server

Account Port: Enter the Account port

Account Secret: Enter the Account secret

Home 🕺 Maint	lenance 👻 🔚 Configu	uration 🗕 😴 System 💋 Logout 🖤
AP-2660	Wireless Settings	6
Basic Settings	Wireless Band	2.4GHz 👻
a LAN	Mode	Access Point
Advanced Settings	Network Name (SSID)	dlink
Status		
	SSID Visibility	Enable 🗸
	Auto Channel Selection	Enable 👻
	Channel	1 -
	Channel Width	20 MHz 👻
	Authentication	WPA-Enterprise
	RADIUS Server Settings	
	WPA Mode	AUTO (WPA or WPA2)
	Cipher Type	Auto Group Key Update Interval 3600 (Seconds)
	Network Access Protec	
	Network Access Protection	
	RADIUS Server Mode	
	RADIUS Server	External Internal
	Primary RADIUS Serve	
	RADIUS Server	RADIUS Port 1812
	RADIUS Secret	
		(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}[];\:" ,./<>?)
	Backup RADIUS Server	
	RADIUS Server	RADIUS Port 1812
	RADIUS Secret	
		(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}[];'\:" ,./<>?)
	Primary Accounting Se	erver Setting
	Accounting Mode	Disable 👻
	Accounting Server	Accounting Port 1813
	Accounting Secret	
		(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}[];'\:" ,./<>?)
	Backup Accounting Ser	rver Setting (Optional)
	Accounting Server	Accounting Port 1813
	Accounting Secret	
		(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}[];'\:" ,,/<>?)

LAN

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

- Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2660. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.
- **IP Address:** The default IP address is 192.168.0.50. Assign a static IP address that is within the IP address range of your network.
- Subnet Mask: Enter the subnet mask. All devices in the network must share the same subnet mask.
- **Default Gateway:** Enter the IP address of the gateway/router in your network.
 - **DNS:** Enter a DNS server IP address. This is usually the local IP address of your gateway/router.

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

IPv6

Enable IPv6: Check to enable the IPv6

Get IP From: Auto is chosen here. Choose this option the DAP-2660 can get IPv6 address automatically or use Static to set IPv6 address manually. When Auto is selected, the other fields here will be grayed out.

IP Address: Enter the LAN IPv6 address used here.

Prefix: Enter the LAN subnet prefix length value used here.

Default Gateway: Enter the LAN default gateway IPv6 address used here.

IPv6 Settings	
 Enable IPv6 Get IP From IP Address Prefix Default Gateway 	Auto Static Auto
	Save

Advanced Settings

In the Advanced Settings Section the user 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.

D-Link [®]				DAP-2660
🔅 Home 🕺 Maintenanc	e 👻 📑 Configuration	🝷 🐳 System	💋 Logout	Help
DAP-2660 Basic Settings Advanced Settings Performance Wireless Resource Multi-SSID VLAN Intrusion Schedule Internal RADIUS Server ARP Spoofing Prevention Bandwidth Optimization AP Array Captive Portal DHCP Server Filters Traffic Control Status	Performance Settings Wireless band Wireless Wireless Mode Data Rate Beacon Interval (40-500) DTIM Interval (1-15) Transmit Power WMM (Wi-Fi Multimedia) Ack Time Out (5GHz, 25~200) Short GI IGMP Snooping Multicast Rate Multicast Bandwidth Control Maximum Multicast Bandwidth HT20/40 Coexistence Transfer DHCP Offer to Unicast	SGHz ♥ Off ♥ Mixed 802.11ac ♥ Best(Up to 867) ♥ (Mbps) 100 1 100% ♥ Enable ♥ 25 (µs) Enable ♥ Disable ♥ Disable ♥ 100 kbps Disable ♥ Disable ♥		Save

Performance

On the Performance Settings page the 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 combination 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 (draft) 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.

Wireless band	5GHz 👻	
Wireless	Off 👻	
Wireless Mode	Mixed 802.11ac 👻	
Data Rate	Best(Up to 867) 👻 (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 👻	

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

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

Ack Time Out To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 25 and 200 (2.4 GHZ, 64~200): 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: 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.
- Multicast Bandwidth Adjust the multicast packet data rate here. The multicast rate is supported in AP mode, and WDS with AP mode, including Multi-Control: SSIDs

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

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

Wireless Resource Control

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

Wireless band: Select 2.4GHz or 5GHz.

- Band Steering:Use the drop-down menu to Enable the 5G Preferred
function. When the wireless clients support both
2.4GHz and 5GHz and the 2.4GHz signal is not strong
enough, the device will use 5G as higher priority.
- **Band Steering Age:** Enter the time in seconds to specify the interval of updating information.
 - Band Steering
Difference:The 5G preferred difference value is equal to the
number of 5GHz wireless client connections minus
the number of 2.4GHz wireless client connections.
If the number of 5GHz wireless client connections
minus the number of 2.4GHz wireless client connections
minus the number of 2.4GHz wireless client connections
exceed this value, the extra 5GHz wireless client
connections will be forced to connect to the 2.4GHz
band and not the 5GHz band.
 - Band SteeringEnter the maximum 5G connection attempts allowedRefuse Number:before the 5G preferred function will be disabled for
the wireless station connection.



- 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-2660 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 Preferred:	Use the drop-down menu to Enable the 11n Preferred function. The wireless clients with 802.11n protocol will have higher priority to connect to the device.
Network Utilization:	Set the maximum utilization of this access point for service. The DAP-2660 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.
Aging out:	Use the drop-down menu to select the criteria of disconnecting the wireless clients. Available options are RSSI and Data Rate .
RSSI Threshold:	When RSSI is selected in the Aging out drop-down menu, select the percentage of RSSI here. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients.
Data Rate Threshold:	When Data Rate is selected in the Aging out drop-down menu, select the threshold of data rate here. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients.
ACL RSSI:	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 seven multi-SSIDs. With the Primary SSID, you have a total of eight 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 WMM stands for Wi-Fi Multimedia. Enabling this feature Multimedia): 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, enter the IP address of the RADIUS server. In addition, you must configure RADIUS Port and RADIUS Secret.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

VLAN

VLAN List

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

VLAN Status: 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.

VLAN List Port List Add/Edit VLAN PVID Setting VID VLAN Name Untag VLAN Ports Tag VLAN Ports Edit Delete Mgmt, LAN, Primary(2.4G), S- 1(2.4G), S-2(2.4G), S- 3(2.4G), S-2(2.4G), S- 3(2.4G), S-4(2.4G), S- 5(2.4G), S-4(2.4G), S- 5(2.4G), W-1(2.4G), W- 2(2.4G), W-1(2.4G), W- 2(2.4G), W-3(2.4G), W- 4(2.4G), W-5(2.4G), W- 4(2.4G), W-5(2.4G), W- 4(2.4G), Primary(5G), S- 1(5G), S-2(5G), S- 1(5G), S-2(5G), S- 6(5G), S-7(5G), W- 1(5G), W-2(5G), W- 3(5G), W-4(5G), W-	VLAN Status : Disable Enable VLAN Mode : Static(2.4G), Static(5G)					
Mgmt, LAN, 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- 5(2.4G), W-1(2.4G), W- 2(2.4G), W-1(2.4G), W- 2(2.4G), W-3(2.4G), W- 4(2.4G), W-5(2.4G), W- 1 default 6(2.4G), W-7(2.4G), W- 8(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), W- 1(5G), W-2(5G), W-	VLAN List	Port List	Add/Edit VLAN	PVID Setting		
5(5G), W-6(5G), W- 7(5G), W-8(5G)			Mgmt, LAN, 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), W-1(2.4G), W- 2(2.4G), W-3(2.4G), W- 4(2.4G), W-5(2.4G), W- 6(2.4G), W-7(2.4G), W- 8(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), W- 1(5G), W-2(5G), W- 3(5G), W-4(5G), W- 5(5G), W-6(5G), W-			

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.

VLAN Settings		
VLAN Status : O Disable 💿 Enable	Save	
VLAN Mode : Static(2.4G), Static(5G)		
VLAN List Port List Add/Edit VLAN	PVID Setting	
Port Name Tag VID	Untag VID	PVID
Mgmt	1	1
LAN	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
W-1(2.4G)	1	1
W-2(2.4G)	1	1
W-3(2.4G)	1	1
W-4(2.4G)	1	1
W-5(2.4G)	1	1
W-6(2.4G)	1	1
W-7(2.4G)	1	1
W-8(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
W-1(5G)	1	1
W-2(5G)	1	1
W-3(5G)	1	1
W-4(5G)	1	1
W-5(5G)	1	1
W-6(5G)	1	1
W-7(5G)	1	1
W-8(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	/LAN Settings								
VLAN Status : O Disable VLAN Mode : Static(2.4G) VLAN List Port List	, Static(50		/LAN	P۱	/ID Set	ting	Sav	/e	
Untag Tag Not Member		AN Name Mgmt L O	AN O						1
2.4GHz MSSID Port Untag Tag Not Member	Select A All All All	I Prima o O	ry S-1 • •	S-2 0 0	S-3 • •	S-4 •	S-5 • •	S-6 • •	S-7 •
WDS Port Untag Tag Not Member	Select All All All All	W-1 • •	W-2 • •	W-3	W-4 • •	W-5 • •	W-6 • •	W-7 • •	W-8 • •
- 5GHz MSSID Port Untag Tag	Select A	I Prima O	ry S-1 •	S-2 0	S-3 •	S-4 0	S-5 •	S-6 •	S-7 •
Not Member WDS Port Untag Tag	All Select All All All	•	• W-2 •	• W-3 •	• W-4 •	• W-5 •	• W-6 •	• W-7 •	• W-8 •
Not Member	All	•	•	•	•	•	•	• 	ave

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.

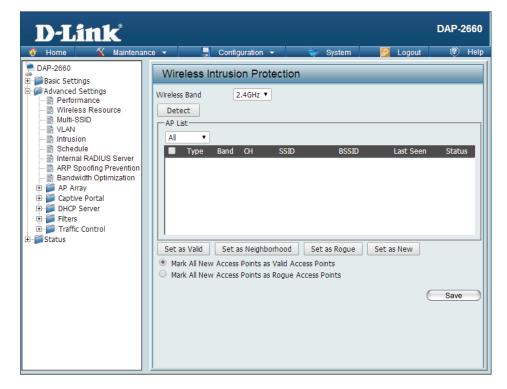
VLAN Status:	Use the radio button to toggle between Enable and Disable.
PVID Auto Assign Status:	Use the radio button to toggle PVID auto assign status to Enable.

VLAN Setting	<u>js</u>		_	_		
VLAN Status : C	tic(2.4G), Static(5	G)			Save	
VLAN List P	ort List Ad	ld/Edit VLAN	PVID	Setting		
PVID Auto Assig	n Status 🛛 🖲 Dis	able 🔍 Er	able			
Port PVID	Mgmt LAN	_	_	_		
2.4GHz						
MSSID Port	Primary S-1	S-2	S-3 S-4	S-5	S-6	S-7
WDS Port	W-1 W-2		W-4 W-5	W-6	u W-7	¥-8
PVID	1 1	1	L 1	1	1	1
- 5GHz						
MSSID Port	Primary S-1	S-2	S-3 S-4	S-5	S-6	S-7
PVID WDS Port	1 1 W-1 W-2		l 1 W-4 W-5	1 W-6	1 W-7	1 W-8
PVID	1 1		l 1	1	1	1
					E	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: Select 2.4GHz or 5GHz.
 - AP List: The choices include All, Valid, Neighbor, Rogue, and New.
 - **Detect:** Click this button to initiate a scan of the network.



Schedule

The Wireless Schedule Settings window is used to add and modify scheduling rules on the device. Click the 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.

D-Link		DAP-2660
🔅 Home 🛛 🔏 Maintenanc	e 🗕 🚽 Configura	ion 🗸 🛛 🐳 System 🛛 🔀 Logout 🛛 🕅 Help
DAP-2660	Wireless Schedule	Settings
Basic Settings Advanced Settings Performance Wireless Resource Wireless Resource Wireless Resource Schedule Intrusion Schedule Bandwidth Optimization AP Array Captive Portal DHCP Server Filters Traffic Control Status	Wireless Schedule Add Schedule Rule Name Index SSID Day(s) All Day(s) Start Time End Time	Disable ▼ Disable ▼
	Schedule Rule List Name SSID Index +: To the end time of th	SSID Day(s) Time Frame Wireless Edit DEL e next day overnight.
		Cave

Internal RADIUS Server

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

User Name: Enter a name to authenticate user access to the **D-Link** DAP-2660 internal RADIUS server. 🚽 Configuration 👻 A Hom Maintenance 👻 Phillip 10 DAP-2660 Password: Enter a password to authenticate user access to the Internal RADIUS Server Basic Settings internal RADIUS server. The length of your password Advanced Settings Add RADIUS Account Performance should be 8~64. Wireless Resource User Name Multi-SSID 🖹 VLAN Password 📄 Intrusion Status: Toggle the drop-down menu between Enable and 📄 Schedule Status Enable • Internal RADIUS Server **RADIUS Account list** Disable. ARP Spoofing Prevention Bandwidth Optimization User Name Delete 🗄 🎬 AP Array 🗄 🧊 Captive Portal **RADIUS Account List:** Displays the list of users. DHCP Server E Filters E Traffic Control 🗉 🎬 Status

Save

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.

D-Link [®]		DAP-2660
🛊 Home 🔏 Maintenand	ce 🕶 📑 Configuration 👻 🤤 System 🛛 🙋 Logout	Image: The second se
DAP-2660	ARP Spoofing Prevention Settings	
Advanced Settings	ARP Spoofing Prevention Disable v	
Wireless Resource	Add Gateway Address	
🗟 VLAN	Gateway IP Address	
Intrusion Schedule	Gateway MAC Address : : : : : : : : : : : : : : : : : :	
Internal RADIUS Server	Add Clear	
Bandwidth Optimization AP Array	Gateway Address List	
Captive Portal DHCP Server	Total Entries: 0	lete All
🕀 🎬 Filters	Gateway IP Address Gateway MAC Address Edit	t Delete
		Save

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			imization
Optimization:	Optimization function.	Enable Bandwidth Optimization	Enable 💌
Downlink Bandwidth:	Enter the downlink bandwidth of the device in	Downlink Bandwidth	80 Mbits/sec
	Mbits per second.	Uplink Bandwidth	80 Mbits/sec
Uplink Bandwidth:	Enter the uplink bandwidth of the device in Mbits	Add Bandwidth O	ptimization Rule
	per second.	Rule Type	Allocate average BW for each station
Alle coto overago DM/	AD will distribute average bandwidth for each	Band	2.4 GHz 💌
Allocate average BW for each station:	AP will distribute average bandwidth for each client.	SSID Index	Primary SSID V
		Downlink Speed	Kbits/sec 💟
Allocate maximum BW	Specify the maximum bandwidth for each	Uplink Speed	Kbits/sec V
for each station:	connected client. Reserve certain bandwidth for future clients.	Readwidth Ontini	Add Clear
		Bandwidth Optimi	CCID
Allocate different BW The weight of 11b/g/n and 11a/n client a	The weight of 11b/g/n and 11a/n client are	Band Type	Index Downlink Speed Uplink Speed Edit Del
for a/b/g/n stations:	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 Allocte		
	specific BW for SSID.		Save

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 the limitation of the downloading speed in either Kbits/sec or Mbits/sec for the rule.
 - **Uplink Speed:** Enter the limitation of the uploading speed in either Kbits/sec or Mbits/sec for the rule.

AP Array

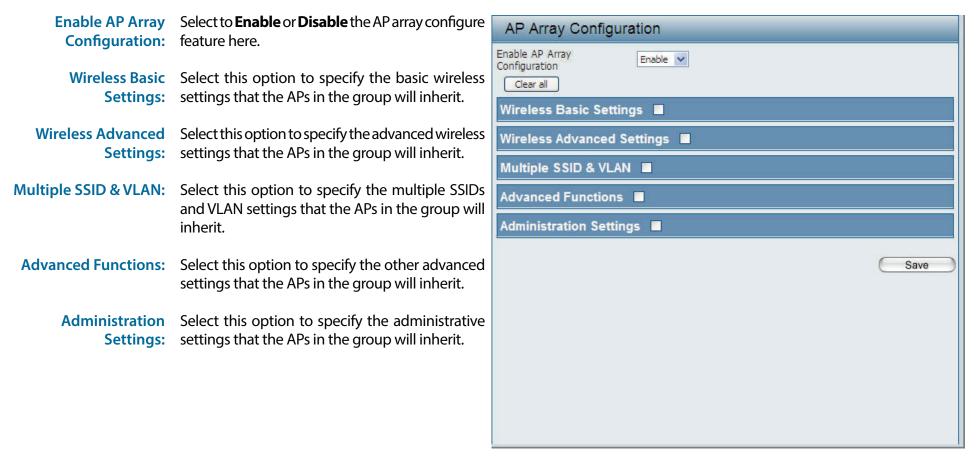
AP Array Scan

The AP Array window is used to create up to 32 APs on a local network to be organized into a single group in order to increase ease of management. Click the **Save** button to let your changes take effect. Central WiFiManager and AP Array are mutually exclusive functions.

Enable AP Array:	Select the check box to enable the AP array function. The three modes that are available are Master , Backup Master , and Slave . APs in the	D-Link Home 🖇 Maintena	DAP-2660 ance 🗸 🔚 Configuration 🖌 🐳 System 💋 Logout 🛞 Help
	same array will use the same configuration. The	DAP-2660	AP Array Scan
	configuration will sync the Master AP to the Slave	Settings Generation	Enable AP Array Version:2.0
	AP and the Backup Master AP when a Slave AP and	Performance	Master Backup Master Slave
	a Backup Master AP join the AP array.	VLAN	AP Array Name d-link AP Array Password
AP Array Name:	Enter an AP array name for the group here.	Internal RADIUS Server ARP Spoofing Prevention Bandwidth Optimization AP Array	Scan AP Array List Scan Connection Status Disconnect AP Array List Image: Connect Conn
AP Array Password:	Enter an AP array password for the group here. This password must be the same on all the APs	AP Array Scan Configuration Settings Auto-RF Load Balance	Array Name Master IP MAC Master Backup Slave Total Master Slave Total
	in the group.		
Scan AP Array List:	Click this button to initiate a scan of all the available APs currently on the network.	Status Sevice Information Client Information Status Client Information Channel Analyze	Current Members Index Role IP Address MAC Address Location
Connection Status:	Display the AP array connection status.	Ethernet	
AP Array List:		,	
	the following parameters: Array Name, Master IP, MAC, Master, Backup Master, Slave, and Total.		Save
Current Members:	This table displays all the current array members. The DAP-2660 AP array feature supports up to eight AP array members.		

Configuration Settings

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



Wireless Basic Settings

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

SSID Visibility: Select this option to enable SSID visibility.

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

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

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

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

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

Wireless Advanced Settings

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

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

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

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

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

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

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

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

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

	Wireless Basic Setting	s 🗹		
	Network Name (SSID)		SSID Visibility	
	Auto Channel Selection		Channel Width	
n.	Security		Captive Profile	v
th.	Band			
un.				

Wireless Advanced Settings 🛛				
Wireless		Wireless Mode		
Data Rate		Beacon Interval		
DTIM Interval		Transmit Power		
WMM (Wi-Fi Multimedia)		Ack Time Out		
Wireless ACL		Short GI		
Link Integrity		Connection Limit		
IGMP Snooping				

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

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

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

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

Multiple SSID & VLAN

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

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

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

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

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

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

Advanced Functions

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

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

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

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

Advanced Functions	2		
Schedule Settings		QoS Settings	
Log Settings		Time and Date Settings	
ARP Spoofing Prevention		Bandwidth Optimization	
Captive Portal		Auto RF	V
Load Balance		DHCP server Settings	

Multiple SSID & VLA	N 🗹		
SSID		SSID Visibility	
Security		WMM	
Captive Profile		VLAN	

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

Bandwidth Select this option to use the same bandwidth optimization settings. **Optimization:**

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

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

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

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

Administration Settings

System Name Settings:Select this option to use the same system name.SNMP Settings:Select this option to use the same SNMP settings.Login Settings:Select this option to use the same login settings.

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

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

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

Administration Setting	5 🗹		
System Name Settings		SNMP Settings	
Login Settings		Console Settings	
Limit Administrator		Ping Control Setting	

Auto-RF

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

Enable: Auto-RF: Select to Enable or Disable the auto-RF feature here.		Auto-RF	
fiere.	here.	Enable Auto-RF	Disable 💌
Initiate Auto-RF:	Click the Auto-RF Optimize button to initiate the	Initiate Auto-RF	Auto-RF Optimize
	auto-RF optimization feature.	Auto-Initiate	Disable 🔛
Auto-Initiate:	Select the Enable or Disable the auto-initiate	Auto-Initiate Period	24 (hours)
Auto Initiate.	feature here.	RSSI Threshold	40%
		RF Report Frequency	10 (Seconds)
Auto-Initiate Period:	After enabling the auto-initiate option, the auto- initiate period value can be entered here. This value must be between 1 and 24 hours.		Save
RSSI Threshold:	Select the RSSI threshold value here. This value is listed in the drop-down menu in increments of 10% from 10% to 100% .		
RF Report Frequency:	Enter the RF report frequency value here.		

Load Balance

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

Enable Load Balance: Select to Enable or Disable the load balance feature here.	Load Balance		
	leature here.	Enable Load Balance	Disable 💌
Active Threshold:	Enter the active threshold value here.	Active Threshold	0
			Save

Captive Portal

Authentication Settings-Web Redirection Only

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

	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.

Session Timeout (1-1440) 60 Minute(s) Band 5GHz SSID Index Primary SSID Authentication Type Web Redirection Only IP Interface Settings Web Redirection State Enable URL Path http:// Save Band SSID Index Captive Profile Edit Deitedite	
SSID Index Primary SSID Authentication Type Web Redirection Only IP Interface Settings Web Redirection State Enable URL Path http:// Save	
Authentication Type Web Redirection Only IP Interface Settings Web Redirection State Enable URL Path http:// Save	
IP Interface Settings Web Redirection State Enable URL Path http:// Save	
Web Redirection State Enable URL Path http:// Save	
URL Path http:// -	
Save	
	lete

Authentication Settings- Username/Password

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

Session	Enter the session timeout value here. This value	
timeout(1-1440): can be from 1 to 1440 minutes. By default, this		Captive P
	value is 60 minutes.	
Band :	Select 2.4GHz or 5GHz.	Band SSID Index
SSID Index :	Select the SSID for this Authentication.	Authentication Ty IP Interface Se Web Redirection
Authentication Type :	Select the captive portal encryption type here. Options to choose from are Web Redirection,	URL Path
	Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the Username/Password option.	Username/Pas Username Password
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.	
Username:	Enter the username for the new account here.	Band
Password:	Enter the password for the new account here.	

60 Minute(s)
5GHz 👻
Primary SSID 🔻
Username/Password 👻
Disable 🗸
http:// v
Add Clear
Username Edit Delete
Save
Save
x 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, user can view and configure the Captive Portal settings. After selecting Passcode as the Authentication Type, we can configure the Passcode authentication that will be applied to each wireless client in this network.

Session	Enter the session timeout value here. This value				
timeout(1-1440) :	can be from 1 to 1440 minutes. By default, this	D-Link		DAP-26	60
	value is 60 minutes.	🔹 Home 🥳 Maintenance	e 🛨 📑 Configura	ition 🗕 👙 System 🛛 🖉 Logout 👘 I	Help
		DAP-2660	Captive Portal Auth	pentication	
Band :	Select 2.4GHz or 5GHz.	Basic Settings Advanced Settings	Session Timeout (1-1440)	60 Minute(s)	
		Performance Wireless Resource	Band	5GHz 🔻	
SSID Index :	Select the SSID for this Authentication.	Multi-SSID	SSID Index	Primary SSID 👻	
		Intrusion	Authentication Type	Passcode 🗸	
Authentication Type :	Select the captive portal encryption type here.	Schedule 	IP Interface Settings Web Redirection State	Disable 🗸	
	Options to choose from are Web Redirection,	ARP Spoofing Prevention Bandwidth Optimization	URL Path	http:// 👻	
	Username/Password, Passcode, Remote	AP Array Gaptive Portal	Passcode Settings		
	RADIUS, LDAP and POP3. In this section we'll	Authentication Settings	Passcode Quantity		
	discuss the Passcode option.	IP Filter Settings MAC Bypass	Duration Last Active Time	Hour Year 2015 Month Jan Day 1 Hour 1:00	
		DHCP Server Filters	User Limit		
Web Redirection State :	Default is Disable or select Enable to enable the	🗈 📁 Traffic Control		Add Clear	
	website redirection feature.		Delete All Passcode Du	uration Last Active Time User Limit Dele	te
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.				
Passcode Quantity:	Enter the number of ticket that will be used			Save	
Passeoue Quantity.	here.		Band SSID In	ndex Captive Profile Edit Dele	te
	here.				
Duration:	Enter the duration value, in hours, for this				
Bulution	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				

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	Enter the session timeout value here. This value				
timeout(1-1440):	can be from 1 to 1440 minutes. By default, this	D-Link		DA	P-2660
	value is 60 minutes.	🚯 Home 🔏 Maintenance	e 👻 📕 Configura	tion 👻 🤤 System 🛛 🖉 Logout	🕐 Help
		DAP-2660	Captive Portal Auth		
Band	Select 2.4GHz or 5GHz.	Basic Settings	Session Timeout (1-1440)	60 Minute(s)	
Dana.	Select 2.4d 12 01 Juli2.	Performance	Band	5GHz V	
			SSID Index	Primary SSID 🔻	
SSID Index :	Select the SSID for this Authentication.	VLAN	Authentication Type	Remote RADIUS	
		Schedule	IP Interface Settings Web Redirection State	Disable 👻	
Authentication Type :	Select the captive portal encryption type here.	ARP Spoofing Prevention	URL Path	http:// v	
	Options to choose from are Web Redirection,	🗈 📁 AP Array	Remote RADIUS Settings		
	Username/Password, Passcode, Remote	Captive Portal Authentication Settings	Radius Server Settings		
	RADIUS, LDAP and POP3. In this section we'll		Radius Server	Radius Port	
	discuss the Remote RADIUS option.	MAC Bypass DHCP Server	Radius Secret Remote RADIUS Type	SPAP V	
	discuss the hemote hhbios option.	Filters Traffic Control	Secondary radius Server	Settings	
Wala Dadina stian State .	Defeult is Dischlass weaks at Englands and his the	E ■ Status	Radius Server	Radius Port	
Web Redirection State :	Default is Disable or select Enable to enable the		Radius Secret	SPAP V	
	website redirection feature.		Remote RADIUS Type Third radius Server Settin		
			Radius Server	Radius Port	
URL Path :	Select whether to use either HTTP or HTTPS		Radius Secret		
	here. After selecting either http:// or https://,		Remote RADIUS Type	SPAP 🗸	
	enter the URL of the website that will be used			S	ave
	in the space provided.		Band SSID In	ndex Captive Profile Edit	Delete
Padius Server	Enter the RADIUS server's IP address here				
Radius Server.					
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.				

Authentication Settings- LDAP

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

	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.	E
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.	
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. Alternat	ivelv



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, user can view and configure the Captive Portal settings. After selecting POP3 as the Authentication Type, we can configure the POP3 authentication that will be applied to each wireless client in this network.

	Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this	D-Link				DAP-2660
	value is 60 minutes.	🔶 Home 🌋 Maintenan	ice 👻 📑 Configura	ation 👻 🐳 System	💋 Logout	🕐 Help
		DAP-2660	Captive Portal Aut	hentication		
Band :	Select 2.4GHz or 5GHz.	Basic Settings Advanced Settings Performance Wireless Resource	Session Timeout (1-1440) Band	60 Minute(s) 5GHz -		
SSID Index :	Select the SSID for this Authentication.		SSID Index Authentication Type IP Interface Settings	Primary SSID V POP3 V		
Authentication Type :	Select the captive portal encryption type here. Options to choose from are Web Redirection,	ARP Spoofing Prevention ARP Spoofing Prevention Bandwidth Optimization P AP Array Captive Portal	Web Redirection State URL Path POP3 Settings	Disable http://		
	Username/Password, Passcode, Remote RADIUS, LDAP and POP3. In this section we'll discuss the POP3 option.	Authentication Settings Cogin Page Upload IP Filter Settings IP Filter	Server Port Connection Type	110 None -	(Save
Web Redirection State :	Default is Disable or select Enable to enable the website redirection feature.	B → Inthe concor	Band SSID In	dex Captive Pro	file E(dit Delete
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.					
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.					

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 In this field the path to the login style file, that will **D-Link** DAP-2660 be uploaded, will be displayed. Alternatively, the Maintenance -Configuration path can be manually entered here. DAP-2660 Login Page Upload Basic Settings Advanced Settings Select the wireless band and login style that will Upload Login Style From Local Hard Drive Performance Upload Login Style from file : Browse ... Upload Wireless Resource be used in each SSID here. Click Download button Multi-SSID The Left space 457216 Byte(s) to download the template file for login page and VLAN Intrusion Schedule Login Page Style List Click Del button to delete the template file. Internal RADIUS Server Wireless Band 5GHz 🗸 ARP Spoofing Prevention ID Style Name Pri S-1 Bandwidth Optimization 1 pages default.tar Ы + AP Array H 2 pages_headerpic.tar E Captive Portal Authentication Settings 3 pages_license.tar Login Page Upload IP Filter Settings MAC Bypass E DHCP Server E Filters 🗄 🍏 Traffic Control Status Save

From Local Hard Drive:

Login Page Style List :

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 :	Wireless Band : Select 2.4GHz or 5GHz.	
IP Address:	IP Address: Enter the IP address or network address	
Subnet Mask:	Subnet Mask: Enter the subnet mask of the IP address or networks address	
Upload IP Filter File:	Upload IP Filter File: To upload a IP filter list file, click Browse and navigate to the IP filter list file saved on the computer, and then click Upload.	
Download IP Filter File:	Download IP Filter File: To download IP Filter list file, click Download and to save the IP Filter list.	

D-Link	DAP-26	60
🔶 Home 🕺 Maintenan	ce 🕶 📕 Configuration 🕶 🐳 System 💋 Logout 📧 H	Help
DAP-2660 Basic Settings Advanced Settings Wireless Resource Wireless Resource Wireless Resource With-SSID VLAN Intrusion Schedule Internal RADIUS Server ARP Spoofing Prevention Bandwidth Optimization Captive Portal Captive Portal Dip IP Filter Settings MAC Bypass DHCP Server Filters DHCP Server Filters DHCP Server Filters DHCP Server	IP Filter Settings Wireless Band SSID Index IP Address Subnet Mask ID IP Address Subnet Mask Delete Upload IP Filter File Upload File :	
⊞- j Status	Download IP Filter File Load IP Filter File Load IP Filter File Hard Driver : Save	

MAC Bypass

The DAP-2660 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.
 Image: Computer of the 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 To download MAC bypass list file, click Download Hard Driver: and to save the MAC bypass list.

MAC Bypass Setti	ngs
Wireless Band SSID Index MAC Address	2.4GHz Primary SSID Add
ID MAC Address	Delete
Upload MAC File	
Upload File :	瀏覽 Upload
Download MAC File	
Load MAC File to Local Hard Driver :	Download
	Save

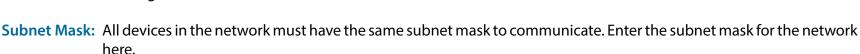
DHCP Server

Dynamic Pool Settings

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. If needed or required in the network, the DAP-2660 is capable of acting as a DHCP server.

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

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



- 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.

D-Link

Dynamic Pool Settings

Disable V

235

dlink-ap

604800

192.168.0.20

255.255.255.0

DHCP Server Control

Function Enable/Disable

Dynamic Pool Settings

The Range of Pool (1-254)

Lease Time (60 - 31536000 sec)

IP Assigned From

Subnet Mask

Domain Name

Gateway

WINS

DNS

DAP-2660

Basic Settings

Advanced Settings

Multi-SSID

VLAN

Intrusion

Schedule

🗄 📁 Captive Portal

E DHCP Server

Filters
 Filters
 Traffic Control

Status

Performance

Wireless Resource

ARP Spoofing Prevention

Bandwidth Optimization

Dynamic Pool Setting:

Current IP Mapping Lis

Static Pool Settings

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.

DAP-2660

Save

Static Pool Setting

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

- Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select Enable to allow the DAP-2660 to function as a DHCP server.
 - 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	
DHCP Server Control	
Function Enable/Disable	Enable 💌
Static Pool Setting	
Host Name	
Assigned IP	
Assigned MAC Address	
Subnet Mask	255.255.255.0
Gateway	
WINS	
DNS	
Domain Name	dlink-ap
	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.

	These are IP address pools the DHCP server has assigned using the dynamic pool setting.	Current IP Mapping List	
Binding MAC Address:	The MAC address of a device on the network that is assigned an IP address from the DHCP dynamic pool.	Host Name Binding MAC Address Current DHCP Static Pools Host Name Binding MAC Address	Assigned IP Address Lease Time Assigned IP Address
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.

Filters

Wireless MAC ACL

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

Wireless Band: Displays the current wireless band rate.

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

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

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

- MAC Address: Enter each MAC address that you wish to include in your filter list, and click Apply.
- MAC Address List: When you enter a MAC address, it appears in this list. Highlight a MAC address and click Delete to remove it from this list.
 - **Current Client** This table displays information about all the current **Information:** connected stations.

Wireless MAC	ACL Se	ttings			
Wireless Band	2,40	GHz 💌			
Access Control List	Acc	ept 💌			
MAC Address	Ĺ]:[]:[]:[]:[bbA []:	
ID MAC Ad	dress		Delete		
Current Client Informat	CARRONAL				
MAC Address 00:1F:3B:AD:35:0B	SSID	Band N	Authenticati OPEN	on Signal 98%	Add
00.1F.3B.AD.33.0B	UIIIK	N	OPEN	9070	
I					
Upload ACL File					4
Upload File :				Browse Upload	l.
Download ACL File					
Load ACL File to Local Driver :	Hard Do	wnload			
				e	Save

WLAN Partition

This page allows the user to configure a WLAN Partition.

Wireless Band: Display	ys 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.

00	Disable
	 Disable Disable Disable
	O Disable
	O Disable
	O Disable
	O Disable

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

D-Link Maintenanc	e 🔻 📙 C	Configuration 🔻	😜 System	💋 Logout	🕐 Help
DAP-2660 Basic Settings Advanced Settings Performance Wireless Resource Multi-SSID	Uplink and D	ownlink Setting	9		
	Ethernet 2.4GHz	Downlink	Uplink		
Hull Sold Schedule Schedule Schedule ARP Spoofing Prevention Bandwidth Optimization Gaptive Portal DHCP Server Fiters Wireless MAC ACL WLAN Partition Traffic Control Status	Downlink Interfa Primary-ssid WDS1 WDS5 Uplink Interface- Primary-ssid Multi-ssid4 WDS1 WDS1 WDS5 Downlink Bandwidth Uplink Bandwidth(1-	Multi-ssid1 Multi-ssid5 WDS2 WDS6 Multi-ssid1 Multi-ssid5 WDS2 WDS6	Multi-ssid2 Multi-ssid6 WDS3 WDS7 Multi-ssid6 WDS3 WDS3 WDS7 Mbits/sec Mbits/sec	Multi-ssid3 Multi-ssid7 WDS4 WDS8 Multi-ssid3 Multi-ssid7 WDS4 WDS8	Save

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-2660 supports four priority levels. Once the desired QoS settings are finished, click the **Save** button to 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: Downlink Bandwidth: The downlink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.
 - Uplink Bandwidth: Uplink Bandwidth: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Enable QoS		_		_	_	_	_	_
Advanced QoS								
Downlink Bandwidth	100 Mbits	s/sec						
Uplink Bandwidth	100 Mbits	s/sec						
ACK/DHCP/ICMP/DNS Priority	Highest Priority	- Lin	nit 100	%	Port	53,63	7,68,5	546,547
Web Traffic Priority	Third Priority	- Lin	nit 100	%	Port	80,44	43,31	28,8080
Mail Traffic Priority	Second Priority	- Lin	nit 100	%	Port	25,11	10,46	5,995
Ftp Traffic Priority	Low Priority	- Lin	nit 100	%	Port	20,21	1	
User Defined-1 Priority	Highest Priority	- Lir	nit 100	%	Port	0		0
User Defined-2 Priority	Second Priority	- Lin	nit 100	%	Port	0		0
User Defined-3 Priority	Third Priority	- Lin	nit 100	%	Port	0	-	0
User Defined-4 Priority	Low Priority	→ Lin	nit 100	%	Port	0		0
Other Traffic Priority	Low Priority	- Lin	nit 100	%				

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

Traffic Manage	r
Traffic Manager	Disable 🔻
Unlisted Clients Traffic	O Deny O Forward
Downlink Bandwidth	100 Mbits/sec
Uplink Bandwidth	100 Mbits/sec
Add Traffic Manag	er Rule
Name	
Client IP(optional)	
Client MAC(optional)	
Downlink Speed	Mbits/sec
Uplink Speed	Mbits/sec
	Add Clear
Traffic Manager R	ules
Name Client	IP Client MAC Downlink Speed Uplink Speed Edit Del
	Save
	Save

Status

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

D-Link [®]			DAP-2660
🛕 Home 🥳 Maintenand	ce 👻 📕 Configuration	👻 👙 System 💋 Logout	🕐 Help
DAP-2660	Device Information		
Basic Settings Wireless LAN Pro Advanced Settings Status Device Information Client Information WDS Information Channel Analyze Statistics Log	Ethernet MAC Address: Wireless MAC Address(2.4GHz): Wireless MAC Address(5GHz): Ethernet IP Address Subnet Mask Gateway DNS Wireless (2.4GHz) Network Name (SSID) Channel Data Rate Security Wireless (5GHz) Network Name (SSID) Channel Data Rate Security	Firmware Version:1.05 70:62:b8:50:d2:40 Primary: 70:62:b8:50:d2:41 ~ 70:62:b8:50:d2:47 Primary: 70:62:b8:50:d2:41 ~ 70:62:b8:50:d2:47 Primary: 70:62:b8:50:d2:49 ~ 70:62:b8:50:d2:4f 192.168.0.50 255.255.255.0 N/A dlink 1 Auto None dlink 149 Auto None	
	AP Array AP Array	d-link	
	Role	Slave	
	Location		
	Device Status		
	CPU Utilization	3%	
	Memory Utilization	24%	

Device Information

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

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

D-Link [®]			DAP-266				
🕎 Home 🏾 🐒 Maintenan	ce 👻 📙 Configuration	👻 👙 System 💋	🛿 Logout 🛛 🕐 He				
DAP-2660	Device Information						
Wireless Wireless LAN Pro Channel Analyze Channel Analyze Log	Device Information Ethernet MAC Address: Wireless MAC Address(2.4GHz): Wireless MAC Address(5GHz): Ethernet IP Address Subnet Mask Gateway DNS Wireless (2.4GHz) Network Name (SSID) Channel Data Rate Security Wireless (5GHz) Network Name (SSID) Channel Data Rate	SSID 1~7: 70:62:b8:50:d2:41 ~ 70:6					
	Security	None					
	AP Array AP Array Role Location Device Status CPU Utilization Memory Utilization Central WiFiManager Connection Status Server IP Service Port Live Port Group ID	d-link Slave 3% 24% Disconnect					

Client Information

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

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

- **SSID:** Displays the SSID of the client.
- MAC: Displays the MAC address of the client.
- **Band:** Displays the wireless band that the client is connected to.
- Authentication: Displays the type of authentication being used.
 - **RSSI:** Displays the client's signal strength.
- **Power Saving Mode:** Displays the status of the power saving feature.

Client Inform	nation				
Client Informatio	n Station as	sociation (2	2.4GHz): 2		
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode
Primary SSID F	8:A4:5F:72:C7	':5C N	OPEN	11%	On
Primary SSID 0	4:FE:31:D5:08	:06 N	OPEN	67%	Off
Client Informatio	n Station as	sociation(5	GHz): 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-2660's Wireless Distribution System network.

WDS Information:	This window displays the Wireless Distribution System information for clients currently connected to the DAP-2660.
Name:	Displays the SSID of the client.
MAC:	Displays the MAC address of the client.
Authentication:	Displays the type of authentication being used.
Signal:	Displays the client's signal strength.
Status:	Displays the status of the power saving feature.

WDS Information				
WDS Information	Channel : 1 (2.412 GHz)			
Name MAC	Authentication	Signal	Status	
WDS Information	Channel : 36 (5.18 GHz)			
Name MAC	Authentication	Signal	Status	

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.

Channel Analy	ze		
Wireless Band Detect Wireless Summary	2.4GHz ▼ 2.4GHz 5GHz		
AP List			
CH AP Num	MRssi(%)	ARssi(%)	Evaluation
* There are only t	hree non-overlapped cha	annels in 2.4G band, resp	ectively 1,6 and 11.

Stats Page Ethernet Traffic Statistics

Displays wired interface network traffic information.

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

D-Link					DAP-2660
🛊 Home 🔏 Maintenar	nce 🔻	Configuration 🔻	🐳 System	💋 Logout	🕐 Help
DAP-2660	Eth	ernet Traffic Statistics	;		
 Basic Settings Advanced Settings Client Information Client Information Client Information Channel Analyze Stats Ethernet WLAN Cog Log Log Settings 	Trans Trans Dropp Recei Recei	mitted Count mitted Packet Count mitted Bytes Count ved Packet Count ved Packet Count ved Bytes Count ved Packet Count	16182 9712778 0 24559 6515872 0	Clea	r Refresh

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.

D-Link			DAP-2660
🔶 Home 🕺 Maintenai	nce 👻 🚽 Configuration 👻	👙 System	💋 Logout 🛛 🕖 Help
DAP-2660 Basic Settings Advanced Settings Status Status Device Information	WLAN Traffic Statistics		
	Transmitted Count	2.4GHz	Clear Refresh 5GHz
Client Information	Transmitted Packet Count	12464	0
	Transmitted Bytes Count	3001368	0
Ethernet	Dropped Packet Count	20537	0
WLAN	Transmitted Retry Count	0	0
⊡ 10g I View Log	Received Count		
Log Settings	Received Packet Count	941	0
	Received Bytes Count	133976	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
	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.

D-Link [®]	DAP-26	60
🛊 Home 🔏 Mainter	nce 🕶 📕 Configuration 🕶 🐳 System 🙋 Logout 🕐 H	lelp
DAP-2660 Basic Settings Advanced Settings Setus Device Information	View Log	
	First Page Last Page Previous Next Clear Page 1 of 3	
Client Information	Time Priority Message	
	Uptime 0 day 04:04:45 [SYSACT] Web login success from 192.168.0.2	
E - 2 Stats Ethernet WLAN E - 2 View Log 2 View Log 2 Log Settings	Uptime 0 day 03:16:01 [Wireless] 2.4G:Deauth:Aging STA F8:A4:5F:72:C7:5C	
	Uptime 0 day 03:09:00 [SYSACT] Web logout from 192.168.0.2	
	Uptime 0 day 03:05:16 [Wireless] 2.4G:Deauth:Aging STA 04:FE:31:D5:08:06	
	Uptime 0 day 03:01:47 [SYSACT] Web login success from 192.168.0.2	
	Uptime 0 day 03:00:05 [Wireless] 2.4G:Association Success:STA 04:FE:31:D5:08:06	
	Uptime 0 day 02:54:35 [SYSACT] Web logout from 192.168.0.2	
	Uptime 0 day 02:51:29 [SYSACT] Web login success from 192.168.0.2	
	Uptime 0 day 02:49:22 [Wireless] 2.4G:Association Success:STA F8:A4:5F:72:C7:5C	
	Uptime 0 day 02:47:01 [SYSACT] Web login success from 192.168.0.2	
	Uptime 0 day 02:09:31 [Wireless] 2.4G:Deauth:Aging STA E8:99:C4:A2:01:D0	1
	Uptime 0 day 02:04:10 [Wireless] 2.4G:Association Success:STA E8:99:C4:A2:01:D0	
	Uptime 0 day 01:23:01 [Wireless] 2.4G:Deauth:Aging STA E8:99:C4:AE:0C:22	
	Uptime 0 day 01:17:46 [Wireless] 2.4G:Deauth:Aging STA 04:FE:31:D5:08:06	Ī
	Uptime 0 day 01:17:33 [Wireless] 2.4G:Association Success:STA E8:99:C4:AE:0C:22	
	Uptime 0 day 01:14:55 [Wireless] 2.4G:Association Success:STA 04:FE:31:D5:08:06	

Log Settings

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

Log Server/IP Address:	Enter the IP address of the server you would like to send the DAP-2660 log to.	D-Link Home Maintenance	e 🔹 📑 Configuration	▼ 👻 System	Logout	DAP-2660
Log Type: E-mail Notification: E-mail Log Schedule:	Check the box for the type of activity you want to log. There are three types: System Activity, Wireless Activity, and Notice. Support Simple Mail Transfer Protocol for log schedule and periodical change key. It can not support Gmail SMTP port 465. Please set to Gmail SMTP port 25 or 587. Use the drop-down menu to set the e-mail log schedule.	DAP-2660 Basic Settings Status Client Information Channel Analyze VULAN Cog Log Settings	Log Settings Log Settings Log Server / IP Address Log Type Email Notification Cutgoing mail server (SMTP) Authentication SSL/TLS From Email Address To Email Address Email Server Address SMTP Port User Name Password Confirm Password	 ✓ System Activity ✓ Wireless Activity ✓ Notice ✓ Enable Internal ▼ Enable Enable Enable Internal Inte		

Email Log Schedule

0 • hours or when Log is full

Schedule

Save

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.

D-Link [®]					DAP-2660
🔶 Home 🏾 🔏 Maintena	nce 👻 🚽 Co	nfiguration 🔻	👙 System	💋 Logout	🕐 Help
Administration Settin Firmware and SSL C Basic Set Configuration File	gs ertification Upload 1form	nation			
Advance(Time and Date		DAP-2660			
	Firmware Version	1.00 10:44:0	03 03/06/2014		
Client Information	System Name	D-Link DAP-2	2660		

Administration Limit Administrator

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

Limit Administrator VLAN Check the box provided and the

- ID: 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.

D-Link [®]		DAP-2660
🛊 Home 🕺 Maintenand	ce 🕶 🔚 Configuration 👻 👻 System 🙋 Logout	🕐 Help
DAP-2660 Advanced Settings Status Client Information WDS Information Status WDS Information Status WLAN Ucg Log Log Settings	Administration Settings	
	Limit Administrator VLAN ID Enable 1 Limit Administrator IP Enable IP Range To:	
	Add Item From To Delete	
	System Name Settings 🔎	
	Login Settings 📕	
	Console Settings 📕	
	SNMP Settings	
	Bing Control Sotting	

System Name Settings

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

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

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

System Name Setti	ngs 🗹	
System Name	D-Link DAP-2553	
Location		

Login Settings

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

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

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

Login Settings 🗹	
Login Name	admin
Old Password	
New Password	
Confirm Password	

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

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

Console Settings

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

- Status: Status is enabled by default. Uncheck the box to disable the console.
- **Console Protocol:** Select the type of protocol you would like to use, Telnet or SSH.

Console Settings 🗹]	
Status	Enable	
Console Protocol	⊙ Telnet ○ SSH	
Timeout	3 Mins 💉	

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

SNMP Settings

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

Status:	Check the box to enable the SNMP	SNMP Settin
	functions. This is enabled by default.	Status
Public Community String:	Enter the public SNMP community string.	Public Commun Private Commun
Private Community String:	Enter the private SNMP community string.	Trap Status Trap Server IP

SNMP Settings 🗹	
Status	Enable
Public Community String	public
Private Community String	private
Trap Status	Enable
Trap Server IP	

Administration

Central WiFiManager Settings

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

Enable Central Select to enable or disable the Central **WiFiManager:** WiFiManager.

Central WiFiManager Setting 🛛

Enable Central WiFiManager Disable 👻

Firmware and SSL Upload

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

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

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

Upload SSL Certification After you have downloaded a SSL

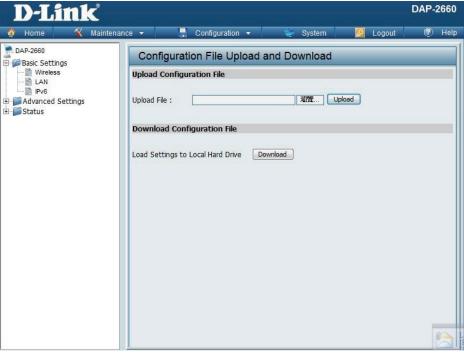
from Local Hard Drive: certification to your local drive, click "Choose File." Select the certification and click "Open" and "Upload" to complete the upgrade.

D-Link [®]		DAP-2660				
🚯 Home 🥳 🔏 Mainte	enance 👻 🔚 Configuration 👻 🐑 System 🛛 💆 Logout	t 🕜 Help				
DAP-2660	Firmware and SSL Certification Upload					
Settings Settings	Update Firmware From Local Hard Drive Firmware Version 1.00					
⊕-∭Advanced Settings ⊕-∭Status	Upload Firmware From File: 瀏覽 Upload					
	Update SSL Certification From Local Hard Drive					
	Upload Certificate From File: 2010 2010 2010 2010 2010 2010 2010 201					
	Upload Key From File: Upload	j				

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.

	You can upload and download configuration files of the access point.	D-Link Home 🔨 Maintena	ance -
Upload Configuration File:	Browse to the saved configuration file you have in local drive and click "Open" and "Upload" to update the configuration.	DAP-2660 Basic Settings Wireless LAN Pv6 ⊕ Marced Settings ⊕ Status	Config Upload Co Upload File Download
.	Click "Download" to save the current configuration file to your local disk. Note that if you save one configuration file with the administrator's password now, after resetting your DAP-2660 and then updating to this saved configuration file, the password will be gone.		Load Setti



Time and Date Settings

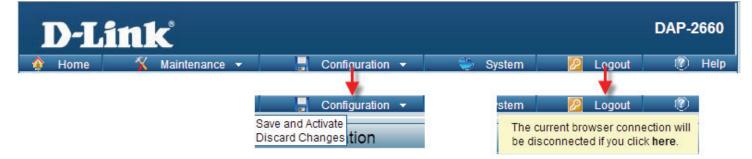
Enter the NTP server IP, choose the time zone, and enable or disable daylight saving time.

Current Time:	Displays the current time and date settings.	
Enable NTP Server:	Check to enable the AP to get system time from an NTP server from the Internet.	
NTP Server:	Enter the NTP server IP address.	÷
Time Zone:	Use the drop-down menu to select your correct Time Zone.	
Enable Daylight Saving:	Check the box to enable Daylight Saving Time.	
Daylight Saving Dates:	Use the drop-down menu to select the correct Daylight Saving offset.	
Set the Date and Time Manually:	A user can either manually set the time for the AP here, or click the Copy Your Computer's Time Settings button to copy the time from the computer in use (Make sure that the computer's time is set correctly).	

D-Link						DAP-26	60
	nance 👻 🔚 C	Configuration 🔻	💝 System		Logout	() I	Help
DAP-2660 Basic Settings Advanced Settings	Time and Da	ate Settings					
	Time Configura	ation					
	Current Time	01/01/1970	04:15:56				
	Automatic Time	e Configuration					
	Enable NTP Server	-					
	NTP Server						
	Time Zone	(GMT+08:00)	Ulaan Bataar			•	•
	Enable Daylight Sa	ving					
	Set the Date ar	nd Time Manually					
	Date And Time	Year 20:	14 Month	Mar 🔻	Day	12 🔻	
	Date And Time	Hour 15	 Minute 	13 🔻	Second	5 🔻	
		Copy Your	Computer's Time	Sottings			
		сору той	Computers film	securgs			-11
					0	Save	

Configuration and System

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



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

Restart the Device:	Click Restart to restart the DAP-2660.	
	Click Restore to restore the DAP-2660 back to factory default settings.	
Clear Language Pack:	Click to clear the current Language pack running.	Ē

D-Lini	Ľ					DAP-2660
🌢 Home 🌱	Maintenance	- Configuratio	on 👻	👙 System	💋 Logout	🕐 Help
DAP-2660 Basic Settings Advanced Settings Status		System Settings				
	R	estart the Device		Restart		
	R	estore to Factory Default Set	ttings	Restore		

Help

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

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

Basic Settings

Wireless Settings

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

Wireless Band

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

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 "dink". The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

SSID Visibility

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

Auto Channel Selection

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

Channel

Indicate the channel setting for the DAP-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 your 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-2660 saves money by providing users with multi-functionality configurable in four different modes.
- Scalability Configurations can be easily changed and range from Peer-to-Peer networks, suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Wireless Installation Considerations

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

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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2660. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows[®] XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 7.0 or higher, Chrome, Firefox, or Safari 4 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows[®] firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
- Configure your Internet settings:

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

Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK. Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.

- Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

What can I do if I forgot my password?

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

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

How to check your IP address?

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

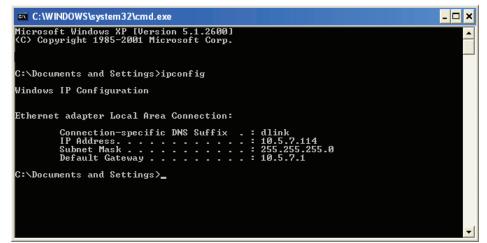
Click on Start > Run. In the run box type cmd and click OK.

At the prompt, type ipconfig and press Enter.

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

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

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



How to statically assign an IP address?

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

Step 1:

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

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

Step 2:

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

Step 3:

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

Step 4:

Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router. Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1). Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5:

Click OK twice to save your settings.

Internet Protocol (TCP/IP) Pr	operties 🛛 🛛 🤶 🔀				
General					
	automatically if your network supports d to ask your network administrator for				
🔘 Obtain an IP address automa	atically				
Ose the following IP address:					
IP address:	192.168.0.52				
Subnet mask:	255 . 255 . 255 . 0				
Default gateway:	192.168.0.1				
O Obtain DNS server address a	automatically				
─⊙ Use the following DNS serve	r addresses:				
Preferred DNS server:	192.168.0.1				
Alternate DNS server:					
	Advanced				
OK Cancel					

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 802.3af
- IEEE 802.3x

Network Management

- Web Browser interface (HTTP, Secure HTTP (HTTPS))
- Central WiFiManager
- SNMP Support (Private MIB)
- Command Line Interface (Telnet, Secure SSH Telnet)

Security

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

Wireless Frequency Range

• 2.4 to 2.4835 GHz and 5.15 to 5.85 GHz**

Operating Voltage

• 802.3af PoE or 12V/1A

Antenna Type

- 2x Detachable 3 dBi Omni antennas @2.4GHz
- 2x Detachable 4 dBi Omni antennas @5GHz

LEDs

• Power/Status

Temperature

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

Humidity

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

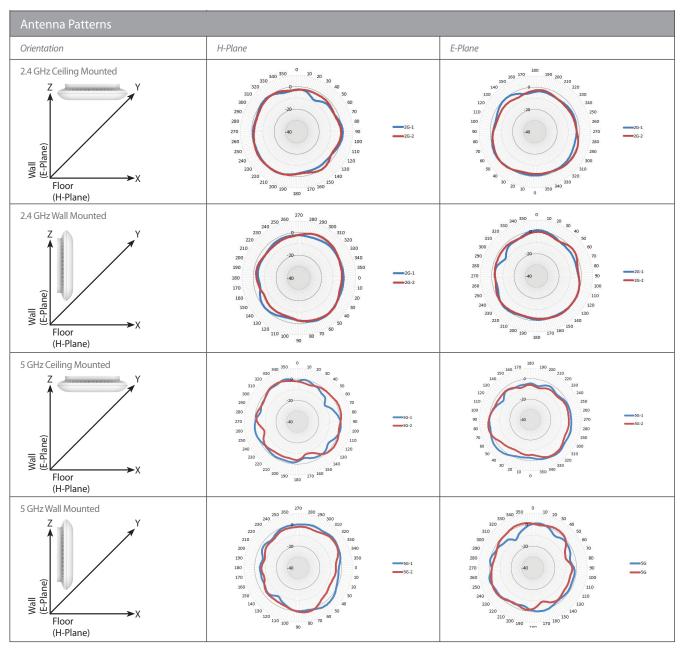
Certifications

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

Dimensions

- L = 170 mm
- W = 170 mm
- H = 28 mm

Antenna Pattern



FREE Central WiFiManager Software

DOWNLOAD NOW

With the easy-to-use web-based interface you can...

- Configure once and apply to multiple Access Points
- Install on Windows PC
- Access on any device using a web-browser, e.g. smartphone or notebook
- Utilise user authentication and access control
- Monitor your entire wireless network in real time¹
- Access detailed reports
- Optimise your bandwidth

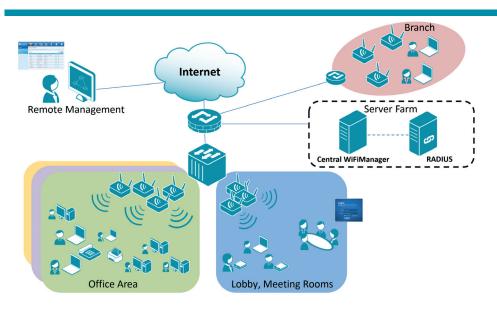


Connect to More www.dlink.com/wifidownload





FREE Central WiFiManager



Available on the following products²:

DAP-2695

Wireless AC1750 Indoor Access Point Designed to support small to medium business or enterprise environments. Secure, manageable dual-band wireless LAN options.



Wireless AC1200 Indoor Ceiling Access Point Providing enhanced speeds of Wireless AC as well as dual-band connectivity to reduce

connectivity to reduce interference, for a faster and more efficient network.



DAP-2310

Wireless N Indoor Access Point

Ideal for creating or expanding capacity of a wireless network; mainly used in high-traffic areas such as airports, coffee shops, sports venues, and university campus deployments.



DAP-2360

Wireless N PoE Access Point

For advanced indoor installations, this highspeed Access Point has integrated PoE support, allowing installation in areas where power outlets are not readily available.



DAP-2690

Wireless N Simultaneous Dual-Band PoE Access Point

Designed for indoor installation where power outlets are not readily available. Enables deployment of a highly manageable, robust and secure wireless network.



DAP-2330 Wireless N PoE

Access Point Ideal for wireless networks in high- traffic areas such as airports, coffee shops, shopping centres, sporting venues, hotels and campus deployments. PoE offers installation where power outlets are not available.





2. Visit dlink.com for selected Hardware & Software versions.

Connect to More www.dlink.com/wifidownload