

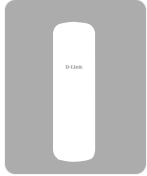
User Manual

5 km Long Range 802.11ac Wireless Bridge

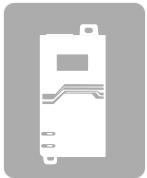
Table of Contents

Product Overview	3		
Package Contents.....	3		
System Requirements	4		
Introduction	5		
Features.....	6		
Hardware Overview.....	7		
Connection	7		
LED Indicators.....	8		
Installation	9		
Preparation before Installation.....	9		
Powering the Access Point.....	10		
Cable Requirements	10		
Configuring the First DAP-3711 in Access Point Mode	10		
Configuring the Second DAP-3711 in Client Mode.....	11		
Wireless Installation Considerations.....	13		
Mounting the Device	15		
Checking the Signal Strength	15		
Mounting on a Pole	15		
Configuration.....	16		
Factory Default Setting	16		
Web-based Configuration.....	17		
Wizard.....	20		
Basic Settings.....	25		
Wireless	25		
Network.....	32		
		In the Network tab, you can set up the DAP-3711's network mode and IP address.	32
		QoS.....	34
		Service	37
		System	40
		Status	42
		Info.....	42
		Statistics	44
		Network.....	45
		Syslog Info	46
		Tools	47
		Ping IP	47
		Traceroute	48
		Link Test.....	49
		Antenna Alignment	50
		Spectrum Analyzer.....	51
		Technical Specifications	52

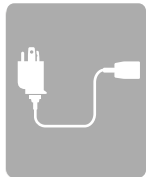
Package Contents



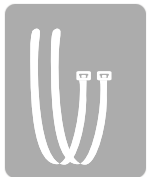
DAP-3711 5 km Long Range 802.11ac Wireless Bridge



24V PoE Injector



Power cord



Mounting ties



Quick Start Guide

Note: Using a PoE Injector with a different voltage rating or PoE injector than the one included with the DAP-3711 will cause damage and void the warranty for this product.

System Requirements

**Web-based Configuration
Requirements**

Computer with the following:

- Microsoft Windows®, Apple Mac OS, or a Linux-based operating system

Browser Requirements:

- Microsoft Edge, Firefox 60.0, Safari ,or Chrome 68.0.3440.106

Introduction

DAP-3711 is a powerful WIFI Bridge/AP device, which allows WIFI access and video/audio/data transmission device, enables long-range, fast speed and robust wireless connections. DAP-3711 has the advantages of long-distance, high-throughput, and between point-to-multi-point performances.

DAP-3711 also support TDMA. TDMA technology solves the problems of hidden-node problem in the 802.11 network. ACK Time-Out Auto Adjust can automatically detect the distances of the DAP-3711 devices, and thus adjust the wireless parameters to achieve the best wireless link quality.

The best transmission range and max speed of DAP-3711 is up to 867Mbps¹, making it suitable for many applications of WIFI Bridge, especially point-to-multi-point communication.

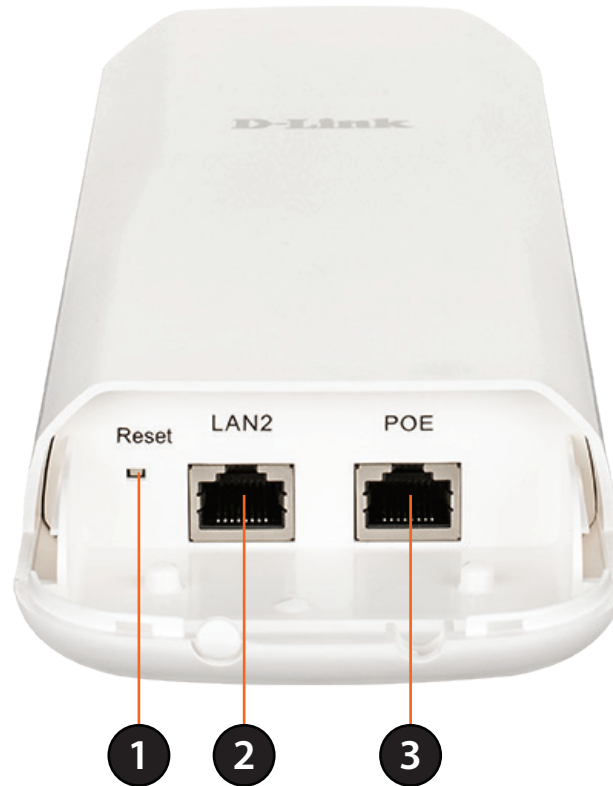
¹ Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Features

- High-performance 802.11ac 2×2 chip
- Max. transmission range: 5 km
- Max. transmission throughput: up to 867 Mbps
- Integrated TDMA, intelligent rate control, and Auto ACK timeout
- TDMA solves the problems of hidden-node problem in the 802.11 network, thus having better long-distance and PTMP performance
- Supports 4 operation modes: Access Point, Client, WDS Access Point, WDS Client
- Supports point-to-point and point-to-multipoint connections
- Unique RF and antenna design enable long-range transmission
- Wireless multimedia optimization technology guarantees video/audio transmission QoS
- User-friendly web-based UI makes the installation and setup processes much easier
- Reliable PoE power supply
- Waterproof housing and protection from weather
- Web-based configuration, easy to use
- Support dual backup firmware, maintenance operation will be safer and more reliable
- Web based working scenario selection makes the installation and setting much easier

Hardware Overview

Connection

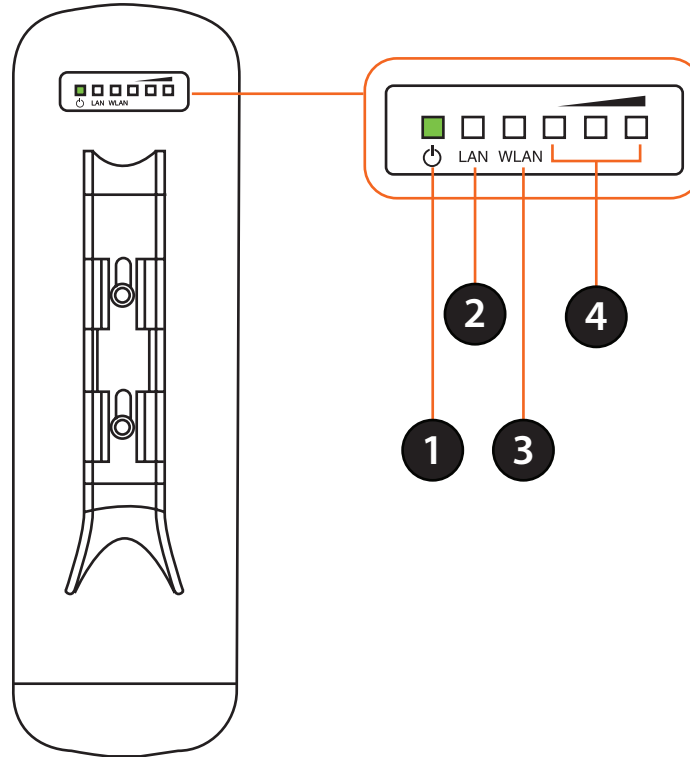


1	Reset Button	Resets the device to its factory settings.
2	LAN 2 Port	Uses a standard Ethernet cable to connect to devices such as computers and switches.
3	PoE LAN Port	Uses a standard Ethernet cable to connect the device to a PoE power source such as a PoE switch or PoE injector.

Note: The DAP-3711 uses a proprietary PoE injector which is needed to function correctly. Only use the included PoE injector as other power sources such as 3rd party PoE injectors or hubs may damage the DAP-3711 or cause it to operate unreliably and will also void the warranty.

Hardware Overview

LED Indicators

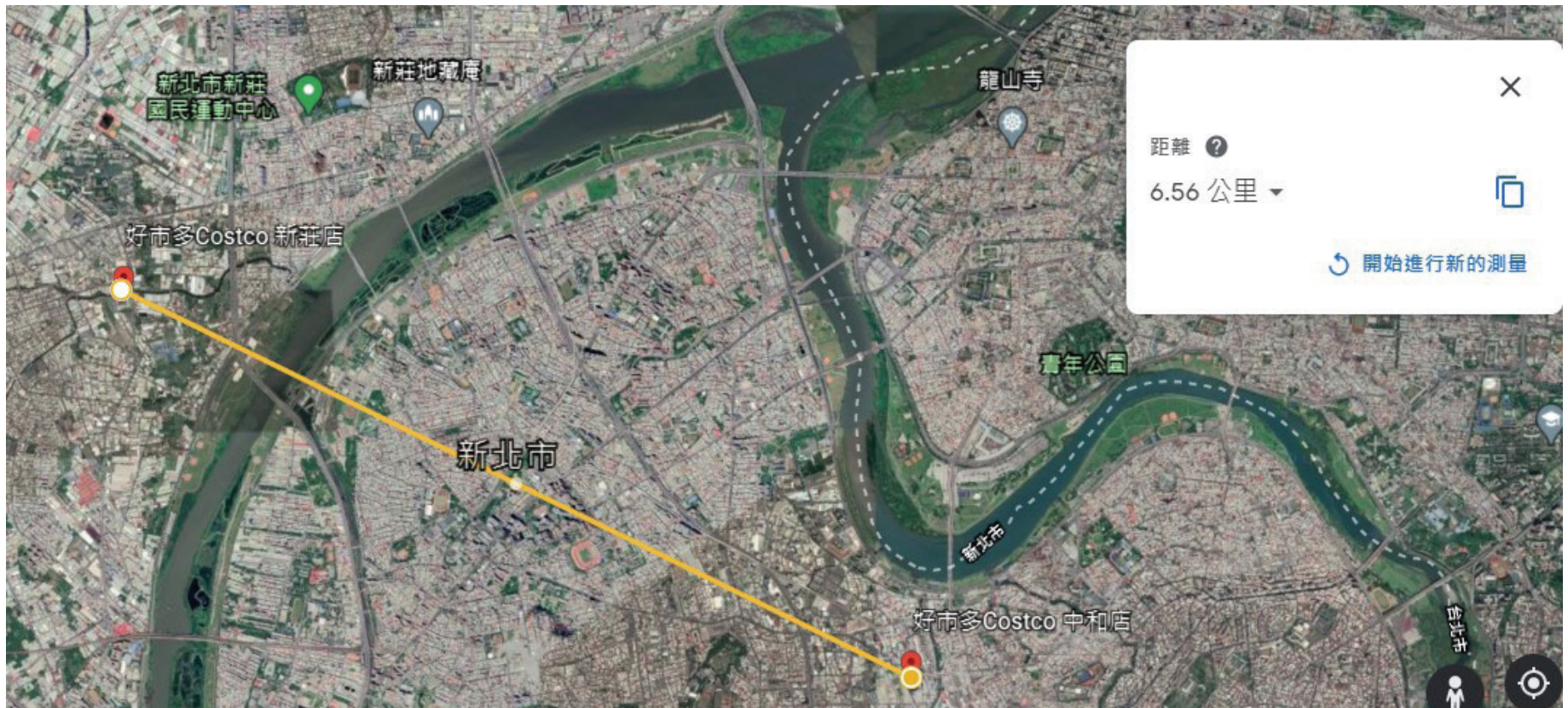


1	Power	Power indicator. Green light indicates the power is on.
2	LAN	Network connection light. A steady green light indicates the LAN port of the PoE power supply is connected to a network device. A flashing green light indicates data is being transmitted.
3	WLAN	Wireless indicator. Lights up to indicate wireless activation. Flashes when data is being transmitted.
4	Signal Strength	Signal strength indicator. A red light indicates a weak signal. Red and yellow together indicates a medium signal. Yellow, red and green together indicates a strong signal.

Installation

Preparation before Installation

Before installing the DAP-3711, check the distance between the two sides and ensure that they are within wireless signal range of each other. It may be helpful to use a Graphic Information System (GIS) program such as Google Earth to check for obstructions between the two sites. If there is an obstruction, it may help to install the DAP-3711 as high as possible to prevent the signal from being blocked.



Note: Ensure that both devices have the same model number and are running the same firmware version. The radiation pattern and wireless protocol of the DAP-3711 is designed for high-performance bridge connectivity. Using different models or models with mismatched firmware versions may cause problems, such as performance degradation or a reduction in coverage area.

Powering the Access Point

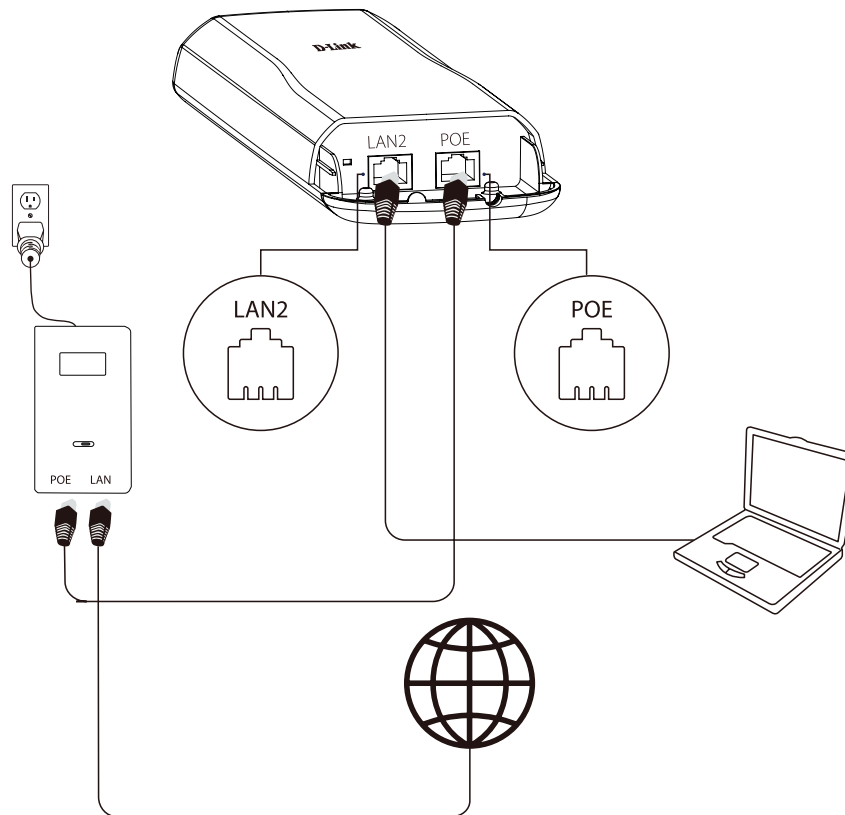
To power the DAP-3711, use a standard Ethernet cable to connect the PoE port on the DAP-3711 to a 24V PoE injector.

Cable Requirements

Use a CAT 5 cable with an even sheath. The Ethernet ports on the DAP-3711 access point cannot accept a CAT 5 cable that has an uneven sheath; the RJ-45 connector on the cable will not fit properly into the receptacle on the access point.

Configuring the First DAP-3711 in Access Point Mode

1. Use an Ethernet cable to connect the LAN 2 port on the DAP-3711 to the management computer.



2. Ensure the computer is configured with the static IP address 192.168.0.2 and a subnet mask of 255.255.255.0.

3. Launch a web browser. Enter 192.168.0.50 in the address field of your browser.

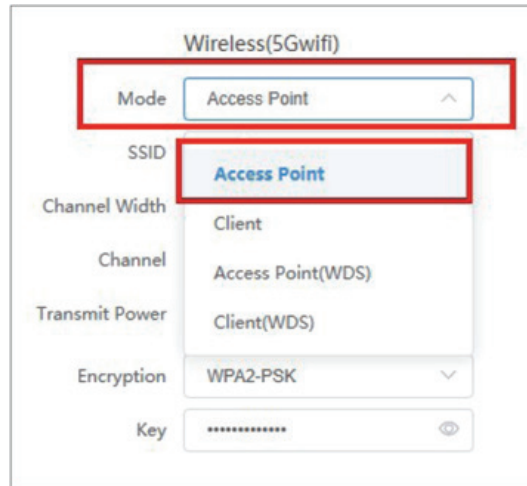
4. Log in to the administration user interface.

The default login information is:

Username: **admin**

Password: **admin**

5. Follow the Setup Wizard's instructions to configure the device in Access Point Mode.

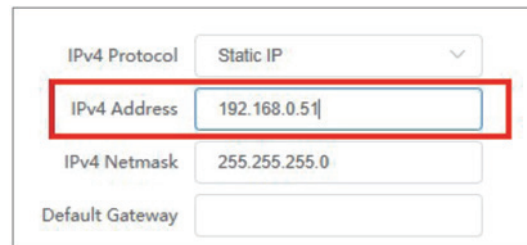


The screenshot shows the 'Wireless(5Gwifi)' configuration page. The 'Mode' dropdown menu is open, and 'Access Point' is selected. The other fields are: SSID (empty), Channel Width (Client), Channel (Access Point(WDS)), Transmit Power (Client(WDS)), Encryption (WPA2-PSK), and Key (masked with asterisks).

Configuring the Second DAP-3711 in Client Mode

1. Follow steps 1-4 of the instructions above to power on the device. Launch the Setup Wizard to configure the device in Client Mode.

2. To avoid an IP address conflict, change the IPv4 address so that it is different from the first DAP-3711's IP address (for instance, by changing it to 192.168.0.51, as in the following screenshot).



The screenshot shows the IPv4 configuration page. The 'IPv4 Protocol' is set to 'Static IP'. The 'IPv4 Address' field is highlighted with a red box and contains the value '192.168.0.51'. The 'IPv4 Netmask' is set to '255.255.255.0' and the 'Default Gateway' field is empty.

- On step four of the Setup Wizard (Wireless), select Client from the dropdown list. Enter the same SSID and key that you entered when configuring the first device.

Wireless(5Gwifi)

1 Mode Client

2 SSID dlink

Channel Width Auto

Channel Auto

Transmit Power 8

Encryption WPA2-PSK

3 Key *****

- To confirm that wireless connectivity between the two devices is configured correctly, navigate to the Status page and check the information under Associated Stations (shown below).

D-Link DAP-3711 admin Wizard Save Logout

Wireless

WiFi1

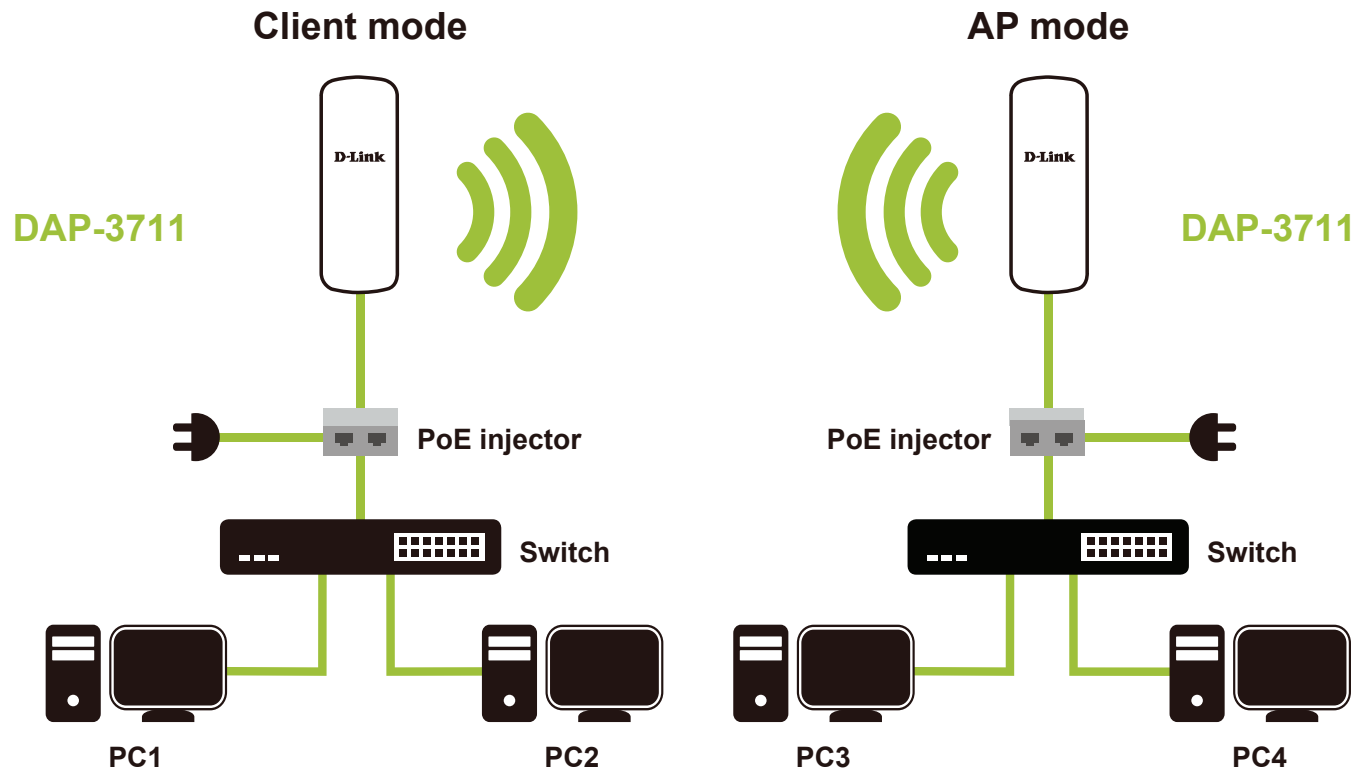
SSID: SunnyTest Distance: 0.15 km
Mode: Client CCQ / Noise Floor: 100% / -100 dBm
BSSID: 9C:B7:93:F3:CA:72 Signal Noise Ratio: -52 / -100 dBm
Country: United Kingdom Transmit Power: 8 dBm
Channel Width: 80MHz
Channel: 5500 MHz (100)
802.11 Mode: 802.11ac
Encryption: WPA2-PSK

Associated Stations

SSID	RSSI/Noise	IPv4 Address	Encryption	MAC	TX/RX Rate	CCQ	802.11 Mode	Association Time
SunnyTest	-52/-100	0.194.134	WPA2-PSK	9C:B7:93:F3:CA:72	866.7 Mbps / 866.7 Mbps	undefined%	802.11ac	00:00:34

©2020 Dlink Digital Technology Co., Ltd. All Rights Reserved.

Once completed, your network will resemble the following diagram.



Wireless Installation Considerations

The D-Link Long Range 802.11ac Wireless Bridge lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

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

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless access points, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 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 2.4 Hz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Mounting the Device

If you plan to install the DAP-3711 on a pole, orient the front of the access point (the side without the LEDs) toward the intended coverage area. The radio antennas transmit through the front of the access point but not through the reverse side (where the bracket is).

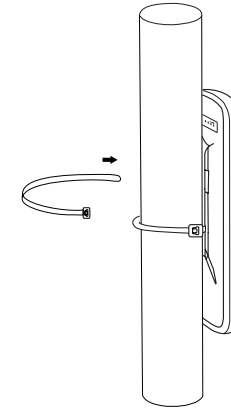
Be sure to install the device at a height that ensures that the alignment between the devices is visible and there is no obstruction in the middle.

Checking the Signal Strength

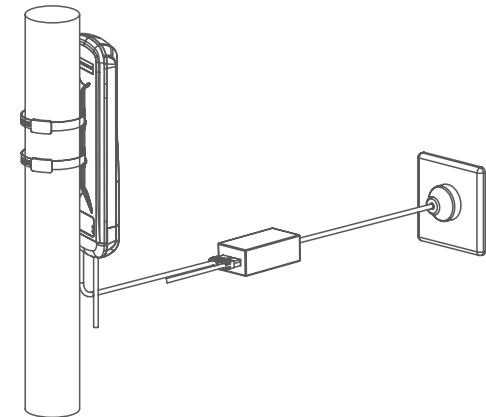
Before fixing the device in place, slowly pan the DAP-3711 from side to side and check the LED indicator to find the position where the signal is strongest.

Mounting on a Pole

1. Connect an Ethernet cable to the LAN port on the DAP-3711.
2. Place the DAP-3711 against the pole where you want it to be positioned.



3. Wrap the metal mounting ties around the pole and thread them through the holes on the DAP-3711



Configuration

This section will show you how to configure your new D-Link Long Range 802.11ac Wireless Bridge using the web-based configuration utility.

Factory Default Setting

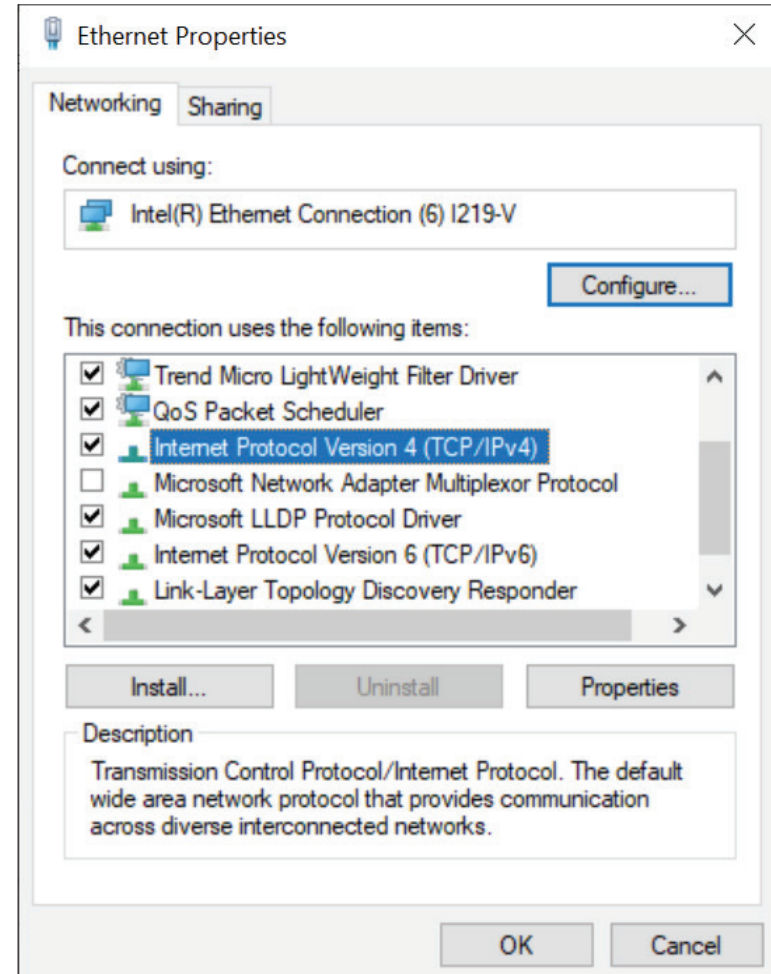
The following table shows the DAP-3711's default settings.

Features	Factory Default Setting
Username	admin
Password	admin
Operation Mode	Bridge
Wi-Fi Mode	Access Point
SSID	dlink
Encryption	WPA2-PSK
Key	1234567890abc
LAN	IP: 192.168.0.50 Subnet: 255.255.255.0 Gateway: 192.168.0.1
DHCP Server	disable
802.11 mode	802.11 ac
Channel	auto
Bandwidth	80 MHz
TDMA	disable

Web-based Configuration

To log in the DAP-3711 web interface, you will need to configure your computer's TCP/IP settings:

1. Right-click the **Local Area Connection** icon on your computer and click **Properties**, then click **Continue**. The **Local Area Connection Properties** dialog box will appear, as seen below.



2. Select **Internet Protocol (TCP/IP)** and click the **Properties** button, and the following dialog box will appear:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 216 . 104 . 64 . 5

Alternate DNS server: 216 . 104 . 72 . 5

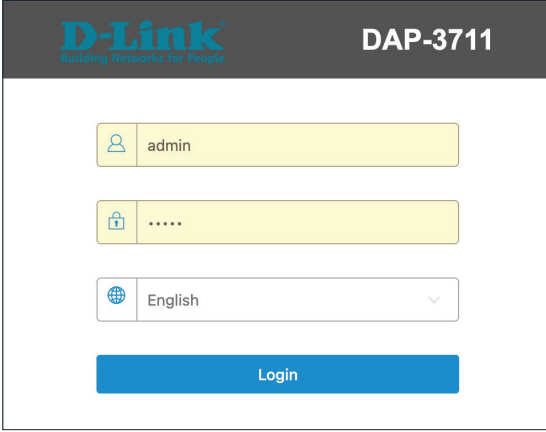
Validate settings upon exit

Advanced...

OK Cancel

3. In the above figure, the **IP address** should be set to **192.168.0.***. Here, * can be any number between 1-255 (but not 50, since the DAP-3711's default IP address is **192.168.0.50**).

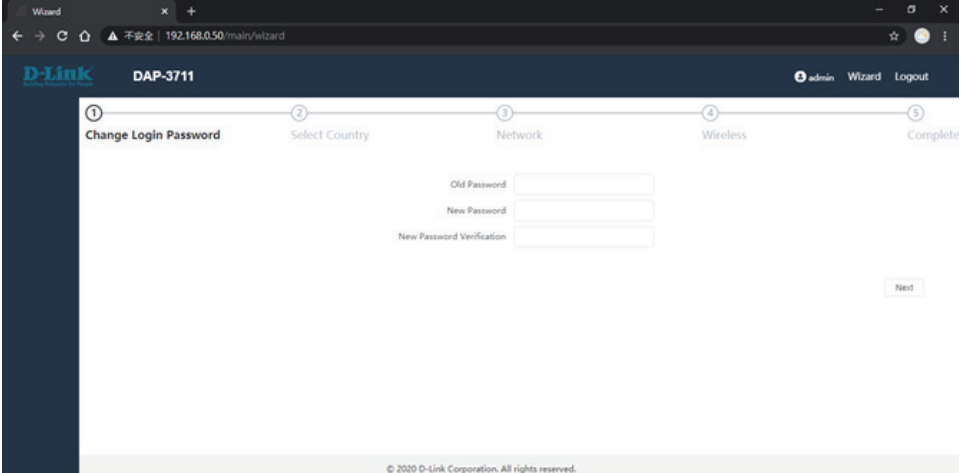
4. When you are done configuring the IP settings above, enter the default IP address (**192.168.0.50**) into the address bar of your web browser, and the following login interface will appear.



The screenshot shows the login page for the D-Link DAP-3711. At the top left is the D-Link logo with the tagline "Building Networks for People". At the top right is the model number "DAP-3711". Below the header, there are three input fields: a username field containing "admin", a password field with masked characters "*****", and a language selection dropdown menu currently set to "English". At the bottom of the form is a blue "Login" button.

5. Enter the username (Default: **admin**) and password (Default: admin) respectively and click "**Login**" to login the main page of DAP-3711. As you can see, this management interface will enter the wizard mode to take you through the initial settings.

Note: The password supports 4~31 digits of upper and lower case letters, numbers, and special symbols
`~!@#\$%^&*()-_+=+



The screenshot shows the wizard mode of the D-Link DAP-3711 management interface. The browser address bar shows "192.168.0.50/main/wizard". The page has a dark blue header with the D-Link logo, "DAP-3711", and user information "admin Wizard Logout". A progress bar at the top indicates five steps: 1. Change Login Password (active), 2. Select Country, 3. Network, 4. Wireless, and 5. Complete. The main content area contains three password input fields: "Old Password", "New Password", and "New Password Verification". A "Next" button is located at the bottom right of the form. The footer contains the copyright notice "© 2020 D-Link Corporation. All rights reserved."

Wizard

When you log into the DAP-3711 for the first time, the Wizard page will automatic pop-up. You can also click **Wizard** in the top right corner.

The screenshot displays the D-Link DAP-3711 configuration interface. At the top, the D-Link logo and 'DAP-3711' are on the left, and 'admin', 'Wizard', and 'Logout' are on the right. The 'Wizard' link is highlighted with a red box. Below the header is a progress bar with five steps: 1. Change Login Password (active), 2. Select Country, 3. Network, 4. Wireless, and 5. Compli. The main content area shows three password input fields: 'Old Password', 'New Password', and 'New Password Verification'. A 'Next' button is located at the bottom right of the form.

Section 3 - Configuration

Change Login Password

If you log in to DAP-3711 for the first time, you need to change the password. The default password is admin. The device login password supports 4~31 digits of upper and lower case letters, numbers, and special symbols `~!@#\$%^&*()-_+=

Old Password	<input type="password" value="....."/>
New Password	<input type="password" value="....."/>
New Password Verification	<input type="password" value="....."/>

Select Country

Select the country where the device is located. Only allow the device to work on channels allowed in a specific country.

WIFI(5G)

Country Code	<input type="text" value="United Kingdom"/>
--------------	---

Network

This helps to set the network parameters. The default mode is Bridge mode and the default LAN IP address is 192.168.0.50. Please change 192.168.0.50 to other IP.

IP Protocol: If you select "Static IP", you have to specify a static IP address, subnet mask, default gateway and DNS server for your local area network which connects to the LAN port of DAP-3711. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

DHCPv4 Client: Select "DHCPv4 Client" to allow the DHCP server within your local area network to assign an IP address automatically.

DHCPv6 Client: Select "DHCPv6 Client" to allow the DHCP server within your local area network to assign an IP address automatically.

IP Protocol	<input type="text" value="Static IP"/>
IPv4 Address	<input type="text" value="192.168.0.50"/>
IPv4 Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.0.1"/>

Wireless

This is for Access Point wireless related settings. Select the operating mode corresponding to the desired mode, and then click “Next” to complete the wizard. After confirming that the operating mode will be changed, the AP will reboot and be ready for use when it is completed.

Wireless Mode: DAP-3711 has four different operating modes, making it adaptable to any situation. Before setting, please determine which Wireless Model (**Access Point, Client, Access Point (WDS), Client (WDS)**) you want to set the DAP-3711 to, and then follow the wizard’s instructions to set it up step by step.

Access Point: The DAP-3711 connects directly to the main Ethernet LAN and receives connectivity from other wireless devices. In access point (AP) mode, 802.11a/n/ac compliant device can connect to the wireless network.

Client: DAP-3711 is connected to the remote AP in it. When there are more than two APs with identical SSID and encryption in the environment, it will automatically connect to them. You can also check the connected AP information in the “**Station List**” on the “**Status**” page.

Access Point (WDS): Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. Access Point (WDS) mode expands current wireless coverage and allows device to connect to the network. It means this device is a AP in WDS mode.

The screenshot shows the 'Wireless(5Gwifi)' configuration interface. It includes the following settings:

- Wireless Mode:** Access Point (dropdown menu)
- SSID:** dlink (text input)
- Channel Width:** 80 MHz (dropdown menu)
- Frequency(Channel):** auto (dropdown menu)
- Transmit Power:** 23 (slider control)
- Encryption:** WPA2-PSK (dropdown menu)
- Key:** (password input with visibility toggle)

Client (WDS): Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. Client (WDS) means this device is a client in WDS mode.

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

Channel Width: Channel width basically controls how broad the signal is for transferring data. Select what you need according to your environment. Default 80 MHz in Access Point mode. DAP-3711 supports 10MHz/20MHz/40MHz/80MHz bandwidth.

Frequency (Channel): Indicates the channel setting for the DAP-3711. In Access Point or Access Point (WDS) mode, the channel can be changed to fit the channel settings of the existing wireless network or to customize the wireless network.

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.

Encryption: The key is required and only sharing the same key with other wireless devices can the communication be established.

OPEN: It allows any device to join the network without performing any security check.

- WPA-PSK:** It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.
- WPA2-PSK:** As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.
- WPA/WPA2 Hybrid-PSK:** It provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

Key: Only 8 to 63 bits of upper and lower case English letters, numbers and special symbols are supported
`~!@#\$%^&*()-_+=

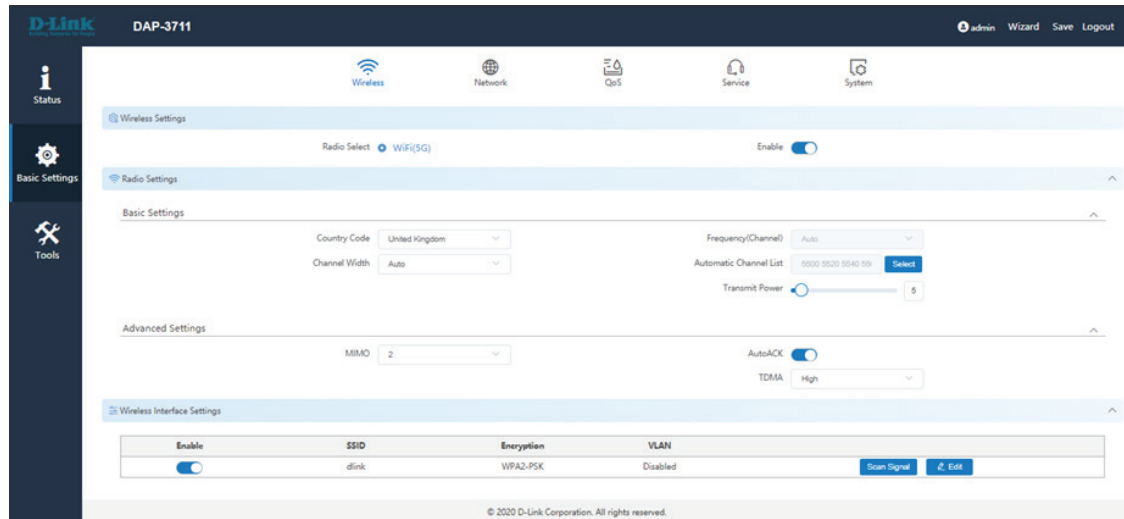
Complete

After the data input is completed, press Next to complete the above setting procedure, and the device will automatically reboot.

Basic Settings

The DAP-3711 provides three main options in the black bar on the left, which are **Status**, **Basic Settings** and **Tools**. This section will introduce how to navigate the **Basic Settings** page. In Basic settings page, there are five tabs: **Wireless**, **Network**, **QoS**, **Service**, and **System**.

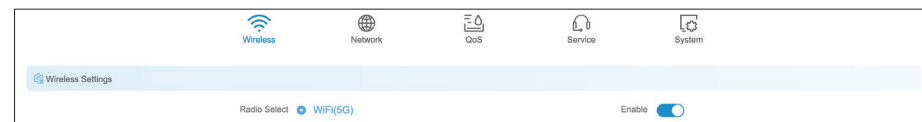
After making changes, click **Save** to apply them.



Wireless

In the **Wireless** tab, you can configure the DAP-3711's Wi-Fi and radio settings.

Wireless Settings: Toggle the button to enable or disable Wi-Fi.



Radio Setting: In this section, users can set up basic and advanced Wi-Fi and radio settings.

Basic Settings

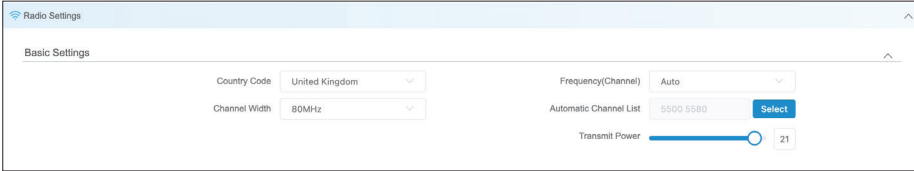
Country Code: Use this to select the country where the DAP-3711 is installed.

Channel Width: Use this to change the AP's channel width. The default is 80 MHz. (in Access Point model or Access Point (WDS) mode)

Frequency: Use this to specify the Wi-Fi channel to use, or select Auto to determine this automatically. Default is Auto.

Automatic Channel List: If the auto channel is selected in Frequency, user can decide channels which DAP-3711 can run. After clicking the **Select**, user can select the channels which DAP-3711 can run in their country.

Transmit Power: The device's output power. When the output power is increased, the signal distance and signal strength will be improved.



The screenshot displays the 'Radio Settings' window with the 'Basic Settings' tab selected. The settings are as follows:

Setting	Value
Country Code	United Kingdom
Channel Width	80MHz
Frequency(Channel)	Auto
Automatic Channel List	5500 5580 Select
Transmit Power	21

Advanced Settings

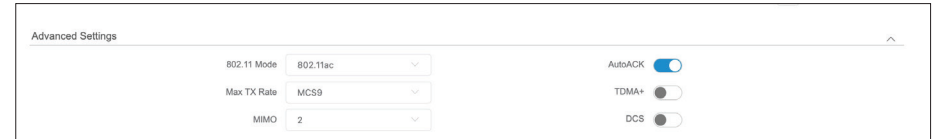
802.11 Mode: You can select the 802.11 mode which the DAP-3711 should use. It is suggested to keep this setting at 802.11ac to provide an optimal transmission rate.

MIMO: The DAP-3711 supports 2T2R Multi-Input-Multi-Output. In high-interference environments, you can set this to 1T1R to reduce the noise.

Auto ACK: Enabling this function will automatically detect the distance between the two DAP-3711 units and optimize the link quality. Enabling this is recommended. If you disable this function, you will need to manually enter the distance between the two units.

TDMA: To use TDMA, you will need to enable TDMA mode in both DAP-3711 units. TDMA can prevent 802.11 hidden node issues. When setting up PTMP, enabling TDMA is recommended. The TDMA function can only work between two DAP-3711 units.

When TDMA is enabled, you can also decide whether you want to enable JTrans. JTrans can help prevent an internal wireless attack. The client and access point must be turned on at the same time when JTrans is enabled.



Wireless Interface Settings

In this section, you can change the settings for the DAP-3711's Wi-Fi operation mode, SSID, encryption, and site survey.

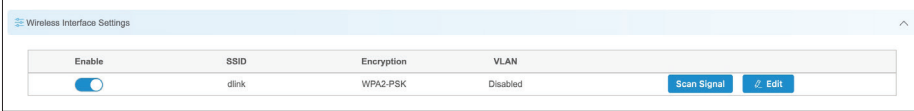
Scan Signal: When you click **Scan Signal**, the device will conduct a site survey to find the SSIDs that the DAP-3711 can detect. If you select an SSID, the DAP-3711 will switch to client mode and connect to the SSID you selected. Click the **Edit** button to set up encryption (if required).

Rescan: Click this to perform a site survey again.

Select: Click this to select which SSID the DAP-3711 should connect to.

Lock: Use this to select which SSID and MAC address the DAP-3711 should connect to. If you enable this, the DAP-3711 will only connect to the AP you specify.

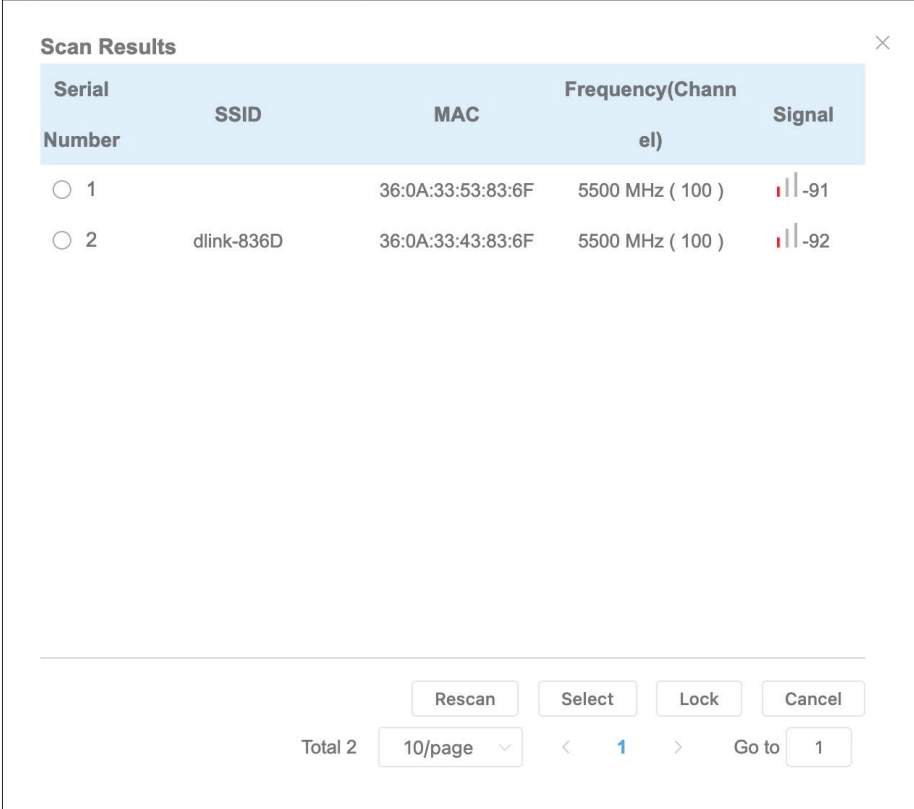
Cancel: Click this to cancel the scan.



Wireless Interface Settings

Enable	SSID	Encryption	VLAN
<input checked="" type="checkbox"/>	dlink	WPA2-PSK	Disabled

[Scan Signal](#) [Edit](#)



Scan Results

Serial Number	SSID	MAC	Frequency(Channel)	Signal
<input type="radio"/> 1		36:0A:33:53:83:6F	5500 MHz (100)	▬ -91
<input type="radio"/> 2	dlink-836D	36:0A:33:43:83:6F	5500 MHz (100)	▬ -92

[Rescan](#) [Select](#) [Lock](#) [Cancel](#)

Total 2 < 1 > Go to

Edit: Click this to change the DAP-3711's operation mode, encryption and key. The following page will pop up:

SSID: To set the SSID which the DAP-3711 will broadcast when it operates in **Access Point** or **Access Point (WDS)** or **SSID** mode, or the SSID that the DAP-3711 will attempt to connect to when it operates in **Client** or **Client (WDS)** mode.

Hidden SSID: When the DAP-3711 is in **Access Point** or **Access Point (WDS)** mode, this function will be displayed. Use this to hide the broadcast name of the wireless network to avoid being connected to others. Check this function; others will not be able to search the SSID

Wireless Mode: DAP-3711 has four different operating modes, making it adaptable to any situation. Before setting, please determine which Wireless Model (**Access Point**, **Client**, **Access Point (WDS)**, **Client (WDS)**) you want to set the DAP-3711 to

Access Point: The DAP-3711 connects directly to the main Ethernet LAN and receives connectivity from other wireless devices. In access point (AP) mode, 802.11a/n/ac compliant device can connect to the wireless network.

Client: DAP-3711 is connected to the remote AP in it. When there are more than two APs with identical SSID and encryption in the environment, it will automatically connect to them. You can also check the connected AP information in the "**Station List**" on the "**Status**" page.

The screenshot shows the configuration page for the DAP-3711. It is divided into two sections: Basic Settings and Advanced Settings. In the Basic Settings section, the SSID is set to 'dlink', the Wireless Mode is 'Access Point', the Encryption is 'WPA2-PSK', and the Key is a series of dots. In the Advanced Settings section, Client Isolation, Speed Limit, and MAC Filtering are all disabled. The VLAN ID is set to 0 and the Max Users is set to 127. At the bottom right, there are 'Cancel' and 'Complete' buttons.

This screenshot shows the same configuration page as the previous one, but with the Wireless Mode dropdown menu open. The menu lists four options: 'Access Point' (which is highlighted in blue), 'Client', 'Access Point(WDS)', and 'Client(WDS)'. The other settings in the page remain the same as in the previous screenshot.

- Access Point (WDS):** Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. Access Point (WDS) mode expands current wireless coverage and allows device to connect to the network. It means this device is an AP in WDS mode.
- Client (WDS):** Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. Client (WDS) means this device is a client in WDS mode.

Encryption: The key is required and only sharing the same key with other wireless devices can the communication be established.

- OPEN:** It allows any device to join the network without performing any security check.
- WPA-PSK:** It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.
- WPA2-PSK:** As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

The screenshot displays a configuration window for wireless settings, divided into 'Basic Settings' and 'Advanced Settings' sections.

Basic Settings:

- SSID: sunnytest
- Hide SSID:
- Wireless Mode: Access Point
- Encryption: WPA2-PSK

Advanced Settings:

- Client Isolation:
- Speed Limit:
- MAC Filtering:
- Type: Off the list
- MAC List:

Key Selection Panel:

- Key: OPEN
- Key: WPA-PSK
- Key: WPA2-PSK (highlighted)
- VLAN ID: WPA2-PSK
- Max Users: WPA/WPA2 Hybrid-PSK
- Max Users: IEEE802.1X

Buttons at the bottom: Cancel, Complete.

WPA/WPA2 Hybrid-PSK: You can select the 802.11 mode which the DAP-3711 should use. It is suggested to keep this setting at 802.11ac to provide an optimal transmission rate.

Key: Only 8 to 63 bits of upper and lower case English letters, numbers and special symbols are supported
`~!@#\$%^&*()-_+=

Client Isolation: When you enable this function, the clients which are connected to the DAP-3711 will not be able to communicate with each other.

Speed Limit: When you enable this function, you will be able to set up a maximum upload/download speed for each client.

VLAN ID: Use this to set up the VLAN ID for the SSID.

Max. Users: Use this to set up the maximum number of clients that can connect to the DAP-3711.

MAC Filtering: Use this to set up a list of MAC addresses that you want to allow or disallow to connect to DAP-3711.

The screenshot displays the configuration interface for the D-Link DAP-3711, divided into two sections: Basic Settings and Advanced Settings.

Basic Settings:

- SSID: sunnytest
- Hide SSID:
- Wireless Mode: Access Point
- Encryption: WPA2-PSK
- Key:

Advanced Settings:

- Client Isolation:
- Speed Limit:
- MAC Filtering:
- Type: Off the list
- MAC List:
- VLAN ID: 0
- Max Users: 127

At the bottom right, there are two buttons: "Cancel" and "Complete".

Network

In the **Network** tab, you can set up the DAP-3711's network mode and IP address.

Network Mode: Select either Bridge Mode or Router Mode.

Bridge Mode: In this mode, the DAP-3711's LAN Port and Wi-Fi will bridge together.

Router Mode: In this mode, the DAP-3711 will act as a router.

Management VLAN: Use this to set up a management VLAN ID tag and IP address. When the VLAN is enabled, the DAP-3711 can only be accessed with this VLAN tag and IP address.

In **Bridge Mode**, users can configure the DAP-3711's LAN interface.

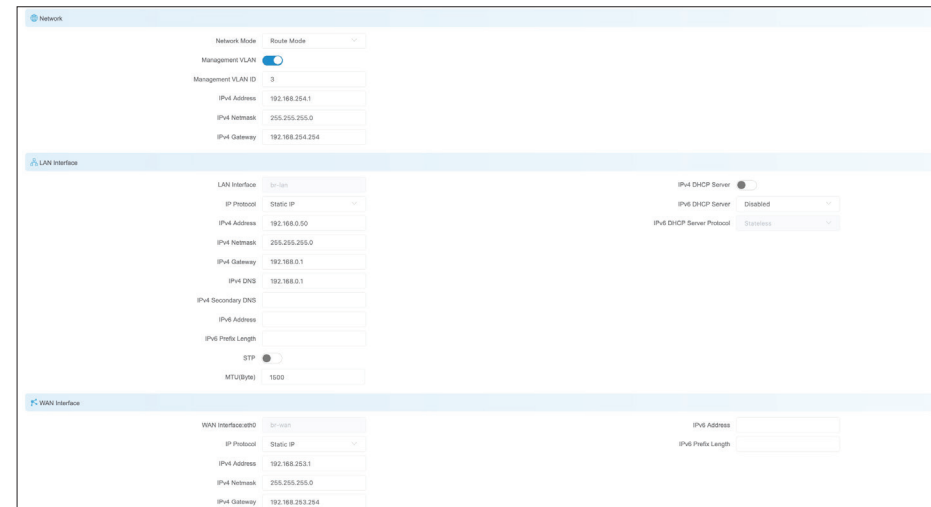
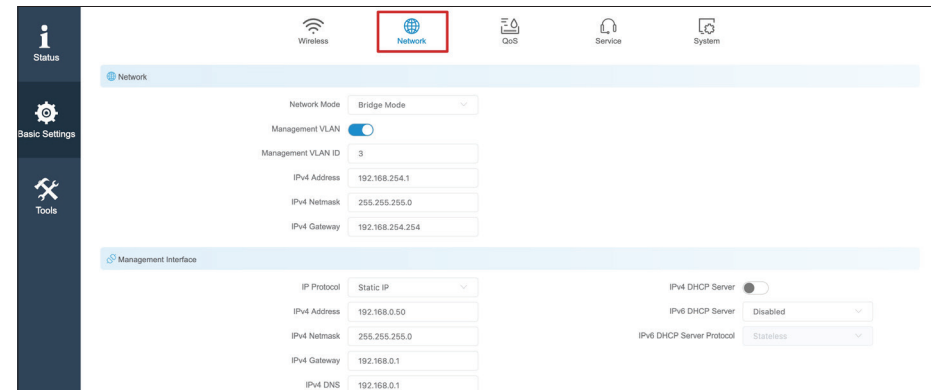
IP Protocol: Use this setting to select either Static IP or DHCP IP.

IPv4/IPv6 DHCP Server: Enabling this function in bridge mode is not recommended. When you enable this function, you need to make sure there are no DHCP servers in the DAP-3711's network.

In **Router Mode**, you need to configure the LAN and WAN interface of the DAP-3711.

LAN interface: You can set the IP addresses of the devices which can be accessed via Wi-Fi using this setting. DAP-3711 supports two LAN ports, in Router Mode, the LAN Interface here represents the LAN2 port.

WAN Interface: In router mode, the physical LAN port becomes the WAN port. You need to enter the IP address or configure DHCP clients to get the IP address as well as PPPoE.



Advanced Settings: In this section, you can configure settings such as static routes. In general, users will not need to configure anything in this section.

Bridge Interface Setting: This displays and controls the DAP-3711's bridge policy.

VLAN: This displays the DAP-3711 VLAN ID tag.

Ethernet Interface Setting: Use this to select the LAN port's speed negotiation mode.

IPv4/IPv6 Static Route: Use this to add the Static Route rule for the DAP-3711.

Interface Isolation: After enabling this function, the two wired interfaces of the device cannot ping each other

The screenshot shows the 'Advanced Settings' page with the following sections:

- Bridge Interface Settings:** A table with columns: Bridge Name, STP, Port, Comment, and an Add button.

Bridge Name	STP	Port	Comment	Add
br-lan	Disabled	ath1		
br-wan		eth0		
- VLAN:** A table with columns: Enable, Interface, VLAN ID, Comment, and an Add button.
- Ethernet Interface Settings:** A table with columns: Interface, Mode, Speed, Duplex.

Interface	Mode	Speed	Duplex
eth0	Negotiate		
- IPv4 Static Routes:** A table with columns: Interface, Destination, Netmask, IPv4 Gateway, Metric, MTU, and an Add button.
- IPv6 Static Routes:** A table with columns: Interface, Destination, Prefix Length, IPv6 Gateway, Metric, MTU, and an Add button.

The screenshot shows the 'Advanced Settings' page with the following sections:

- Interface Isolation:** A table with columns: Interface, Enable.

Interface	Enable
Wired Ethernet	<input type="checkbox"/>

Below the screenshot, there are input fields for:

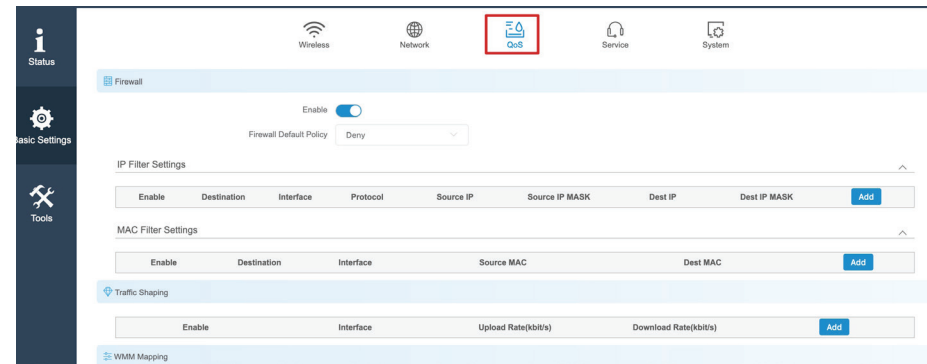
- IPv6 Address:
- IPv6 Prefix Length:
- STP:
- MTU(Byte):

QoS

In the QoS tab, there are four sections on this page: **Firewall**, **Traffic Shaping**, **WMM**, and **QoS Priority**.

Firewall: When the firewall is enabled, the device will only allow certain devices to connect to it.

Firewall Default Policy: **Accept:** Only accept the devices listed in **IP Filter Settings** and **MAC Filter Settings**.
Deny: Deny the devices listed in **IP Filter Settings** and **MAC Filter Settings**.



IP Filter Settings: Click **Add** to add a new IP address to allow or deny.

IP Filter Settings

Enable

Destination

Interface

Protocol

Source IP

Source IP MASK

Dest IP

Dest IP MASK

MAC Filter Settings: Click **Add** to add a new MAC address to accept or deny.

MAC Filter Settings

Enable

Destination

Interface

Source MAC

Dest MAC

Traffic Shaping: Traffic shaping is used to control the upload/download traffic on each network port.

Interface: Select the Interface: eth0 (LAN), eth1(LAN2), ath1(wireless)

Upload Rate: Enter the maximum upload speed.

Download Rate: Enter the maximum download speed.

WMM Mapping: WMM (Wi-Fi Multimedia) allows wireless communication to define a priority limit on the basis of data type. Time-sensitive data (like video/audio data) can be assigned a higher priority than other data. For WMM to be enabled, the wireless client must support it as well.

Enable	802.1p Priority	WMM Access Category
<input type="checkbox"/>	0	BE
<input type="checkbox"/>	1	BK
<input type="checkbox"/>	2	BK
<input type="checkbox"/>	3	BE
<input type="checkbox"/>	4	VI
<input type="checkbox"/>	5	VI
<input type="checkbox"/>	6	VO
<input type="checkbox"/>	7	VO

QoS Priority: Use this setting to set the QoS settings on the LAN port.

Enable	Target CoS	Target DSCP	Source MAC	Dest MAC	VLAN ID	CoS	Eth Type	DSCP	IP Type	Source IP	Dest IP	Source Port	Dest Port	Add

Service

In the service tab, you can configure the following settings: **Time**, **Automatic Restart**, **External System Log Server**, **Ping Watchdog** and **LED Settings**.

Time: Here you can configure the DAP-3711's time settings.

Time Zone: Use this to select the Time Zone in your location.

Calibration Type: If **Manual** is selected, you can change the time, or click **Synchronize** to sync the DAP-3711's time with user's PC.

If **NTP** is selected, the DAP-3711 will sync with a dedicated NTP server. Internet access is required if this setting is enabled.

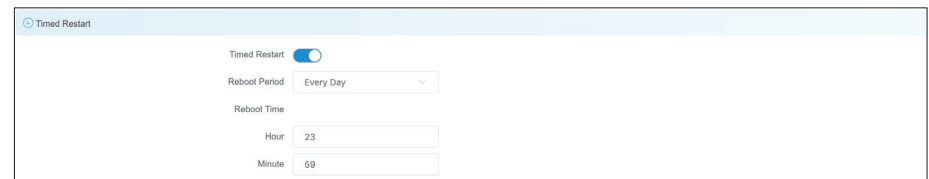
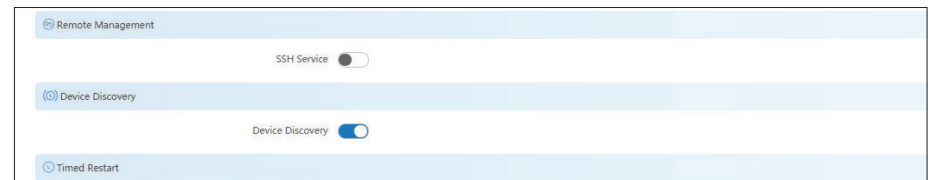
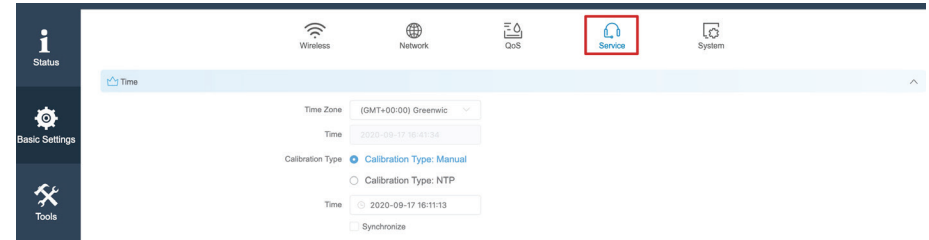
Remote Management: To enable the SSH service. Default is disable.

SSH Service: If user enable this service, the device is accepted to remote access by SSH.

Device Discovery: The process in which the device will search within its range to find other active devices that have registered themselves as visible to other devices.

Time Restart: When this function is enabled, the DAP-3711 will automatically restart according to a schedule that you set.

Reboot Period: There are three items can be selected: **Every Day**, **Every Week**, and **Once**.



External System Log Server Settings: When this is enabled and a server IP is also set here, the log information will be saved to the Syslog server automatically.

Ping Watchdog: The Ping Watchdog sets the DAP-3711 to continuously ping a user-defined IP address (for example, the IP address of the AP that the client is connecting to). If it is unable to ping using the settings that you entered, the DAP-3711 will automatically reboot. It is highly recommended that you enable this feature when using Access Point / Access Point (WDS) Mode.

Ping IP: Specify the IP address of the target which will be monitored using ping. If this feature is enabled in Client/Client (WDS) mode, the IP address should be the IP address of the AP that the client is connecting to.

Ping Interval: Specify the time interval (in seconds) that the Ping Watchdog should wait between ping requests.

Startup Delay: Specify the initial time delay (in seconds) before the first ping request should be sent by the Ping Watchdog.

Ping Failure: Specify the number of ping replies to wait for. If the designated number of ping replies is not received, the Ping Watchdog will reboot the device.

The screenshot shows a web interface with two sections. The top section, titled 'External System Log Server Settings', contains three input fields: 'External System Log Server IP' (empty), 'External System Log Server Port' (set to 514), and 'Log Output Level' (set to Info). The bottom section, titled 'Ping Watchdog', has an 'Enable' toggle switch turned on. Below it are four input fields: 'Ping IP' (empty), 'Ping Interval (Seconds)' (set to 3), 'Start Delay (Seconds)' (set to 60), and 'Ping Failed Times' (set to 20).

Note: If you want to modify the parameters of the Ping Watchdog, please disable it first and then apply the desired settings. When the web page shows that Ping Watchdog is disabled, users will be able to re-enable it with modified parameters.

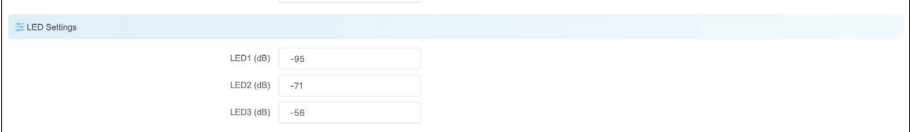
LED Configuration: LED1, LED2, and LED3 light up to indicate the DAP-3711's signal strength. The default ranges are:

LED1: -95 dBm to -1 dBm

LED2: -71 dBm to -1 dBm

LED3: -56 dBm to -1 dBm

When the signal strength is higher than -95dB and below -71dBm, LED1 light; when the signal strength is higher than -71dB and below -56dBm, both LED1 and LED2 light; when the signal strength is higher than -56dBm, all the 3 LEDs light.



The screenshot shows a web interface titled "LED Settings". It contains three rows of configuration options, each with a label and a text input field. The first row is "LED1 (dB)" with the value "-95". The second row is "LED2 (dB)" with the value "-71". The third row is "LED3 (dB)" with the value "-56".

Label	Value
LED1 (dB)	-95
LED2 (dB)	-71
LED3 (dB)	-56

System

There are three subsections in the **System** section: **System**, **Firmware Management**, and **Account Management**.

Device Name: Enter the device name here.

Login Timeout: Enter the time (in minutes) before users should be automatically logged out of the web UI.

Backup Syslog: Click to back up the current system configuration settings and download them as a file.

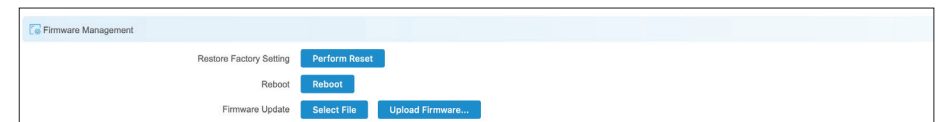
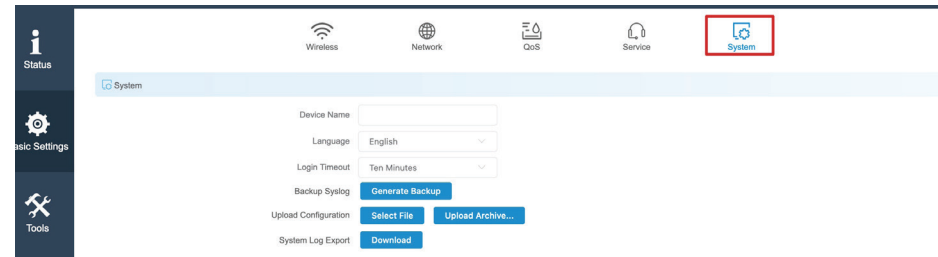
Upload Configuration: Click **Browse** to choose the backup configuration file and then click Upload to apply the settings.

System Log Export: Click to download a backup of the current system log.

Restore Factory Settings: Click the **Reset** button to restore the device to the factory default settings.

Reboot: Click the button to reboot the DAP-3711.

Firmware Update: Click the **Browse** button and choose a firmware file, then click the **Update** button to upgrade the firmware to the latest version.



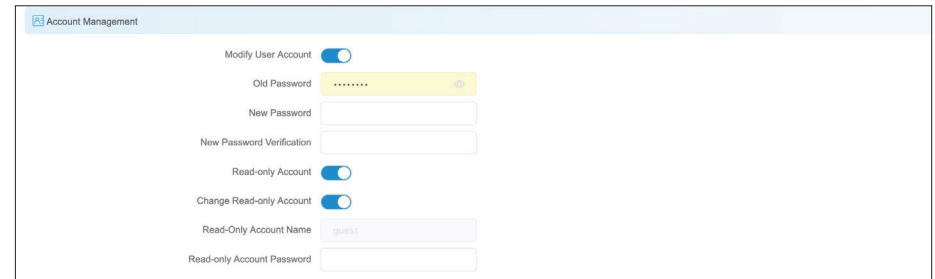
Section 3 - Configuration

Account Management: In this section you can change the admin password or set up a Read Only account.

Modify User Account: Use this to change the admin account's password

Read-Only Account: Use this to enable a Read Only guest account

Change Read-Only Account: Use this to change the guest account's password



The screenshot shows the 'Account Management' configuration page. It includes the following settings:

- Modify User Account:** A toggle switch that is turned on.
- Old Password:** A text input field containing seven dots, with a visibility icon on the right.
- New Password:** A text input field.
- New Password Verification:** A text input field.
- Read-only Account:** A toggle switch that is turned on.
- Change Read-only Account:** A toggle switch that is turned on.
- Read-Only Account Name:** A text input field containing the value 'guest'.
- Read-only Account Password:** A text input field.

Status

There are four tabs in the **Status** section. This page displays the **System**, **Network**, **Wireless** and **Station List** for the DAP-3711.

Info

In the **Info** tab, information about the device is displayed.

Device Name: Device Name: The name of the device

Device Model: Device Model: The model (DAP-3711)

Firmware Version: The software version number

Uptime: The length of time that the device has been powered on

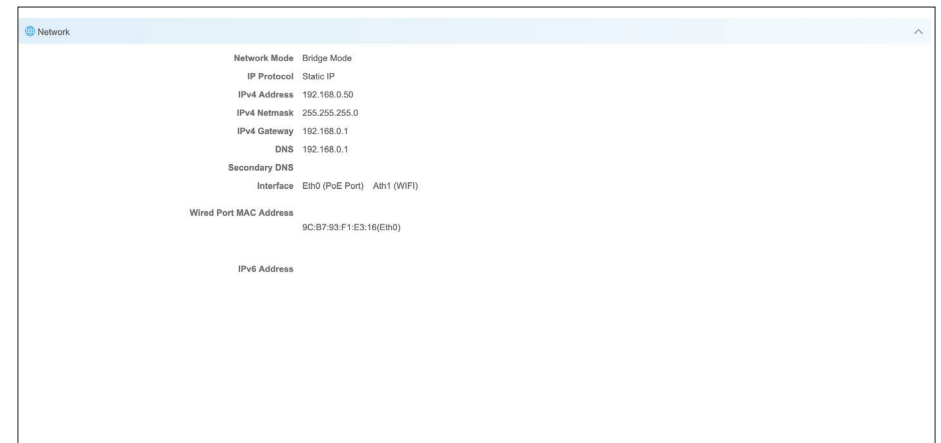
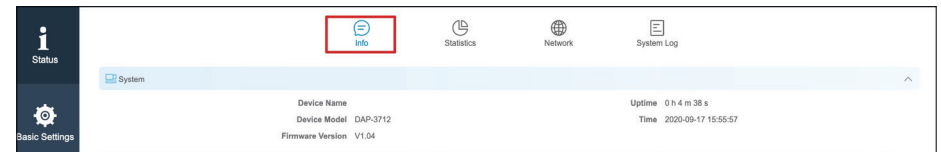
Time: The current time

Network: This displays the DAP-3711's network status

Network Mode: This indicates whether the device is in Router Mode or Bridge Mode

IP Protocol: This indicates whether the device is configured with a Static IP or DHCP

Wired Port MAC Address: This displays the device's LAN MAC Address



SSID: SSID: Displays the device's SSID

Wireless Mode: This displays the device's mode: Access Point, Client, Access Point (WDS), or Client (WDS)

BSSID: This displays the device's Wi-Fi MAC address

Country Code: This displays the device's country code

Channel Width: This displays the device's current operating channel width (10/20/40/80 MHz)

Frequency (Channel): Displays the device's current operating channel

802.11 Mode: This displays the device's current 802.11 mode: 802.11ac or 802.11 a/n

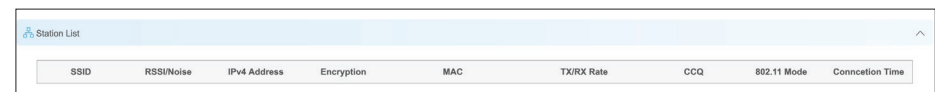
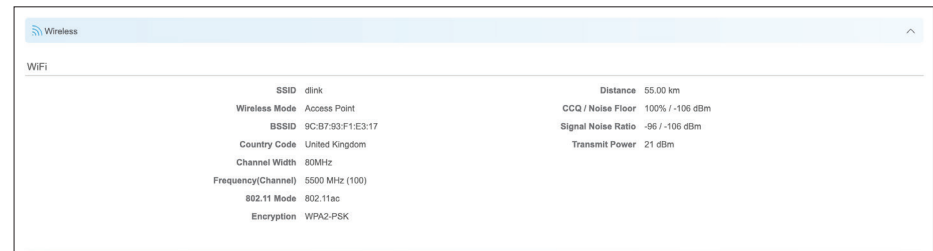
Encryption: Displays the current Wi-Fi encryption

Distance: Shows distance between the two associated devices

Noise Floor: Displays the current noise floor value. In order to achieve the best results, a value of less than -95dBm is recommended

Transmit Power: Displays the DAP-3711's current Wi-Fi power output

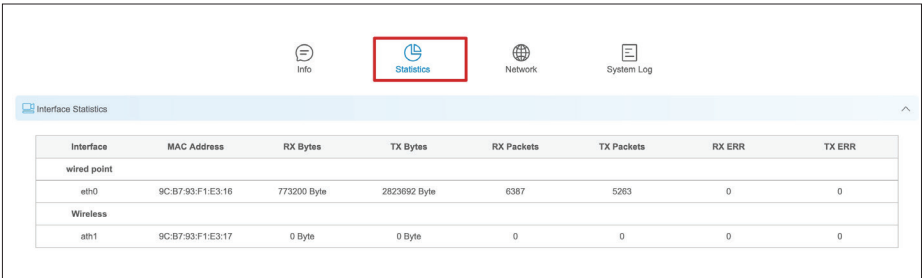
Station List Info: This will list all of the client devices which are connected to the DAP-3711.



Statistics

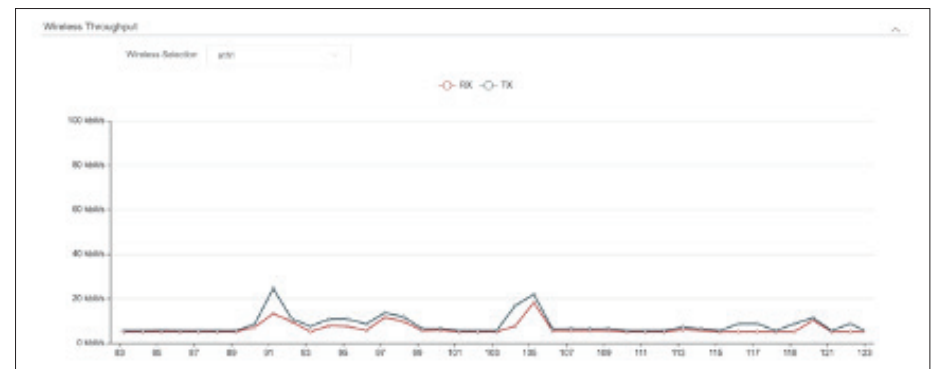
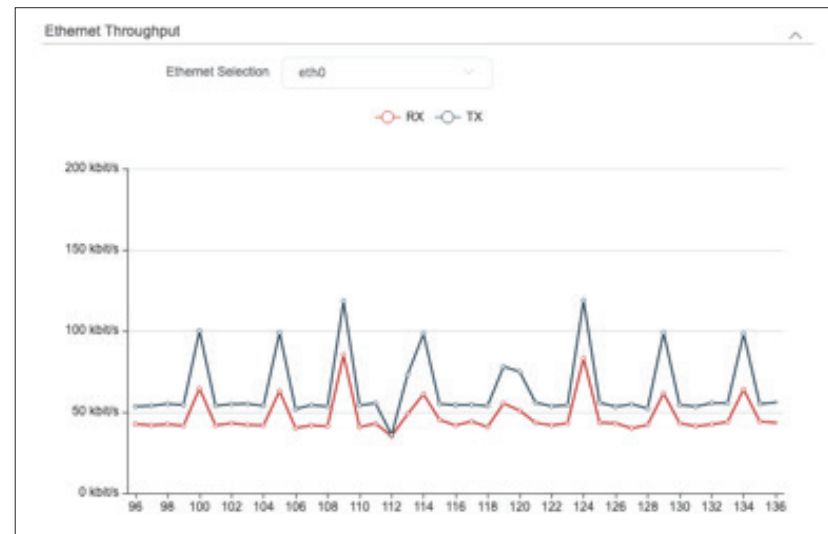
There are two subsections: **Interface Statics** and **Throughput**.

Interface Statics: Displays the DAP-3711's traffic



Interface	MAC Address	RX Bytes	TX Bytes	RX Packets	TX Packets	RX ERR	TX ERR
wired point							
eth0	9C:B7:93:F1:E3:16	773200 Byte	2823692 Byte	6387	5263	0	0
Wireless							
ath1	9C:B7:93:F1:E3:17	0 Byte	0 Byte	0	0	0	0

Throughput: Displays the current Ethernet and wireless traffic



Network

In this tab, you can see the current IPv4 route table, APR table and bridge table.

The screenshot displays the Network configuration page with a navigation bar at the top containing icons for Info, Statistics, Network (highlighted with a red box), and System Log. Below the navigation bar are three expandable sections:

- IPv4 Routes Table:** A table with columns: Destination, Netmask, Gateway, Interface, and Metric.
- ARP Table:** A table with columns: IPv4 Address, MAC Address, and Interface.
- Bridge Table:** A table with columns: MAC Address and Ageing Timer.

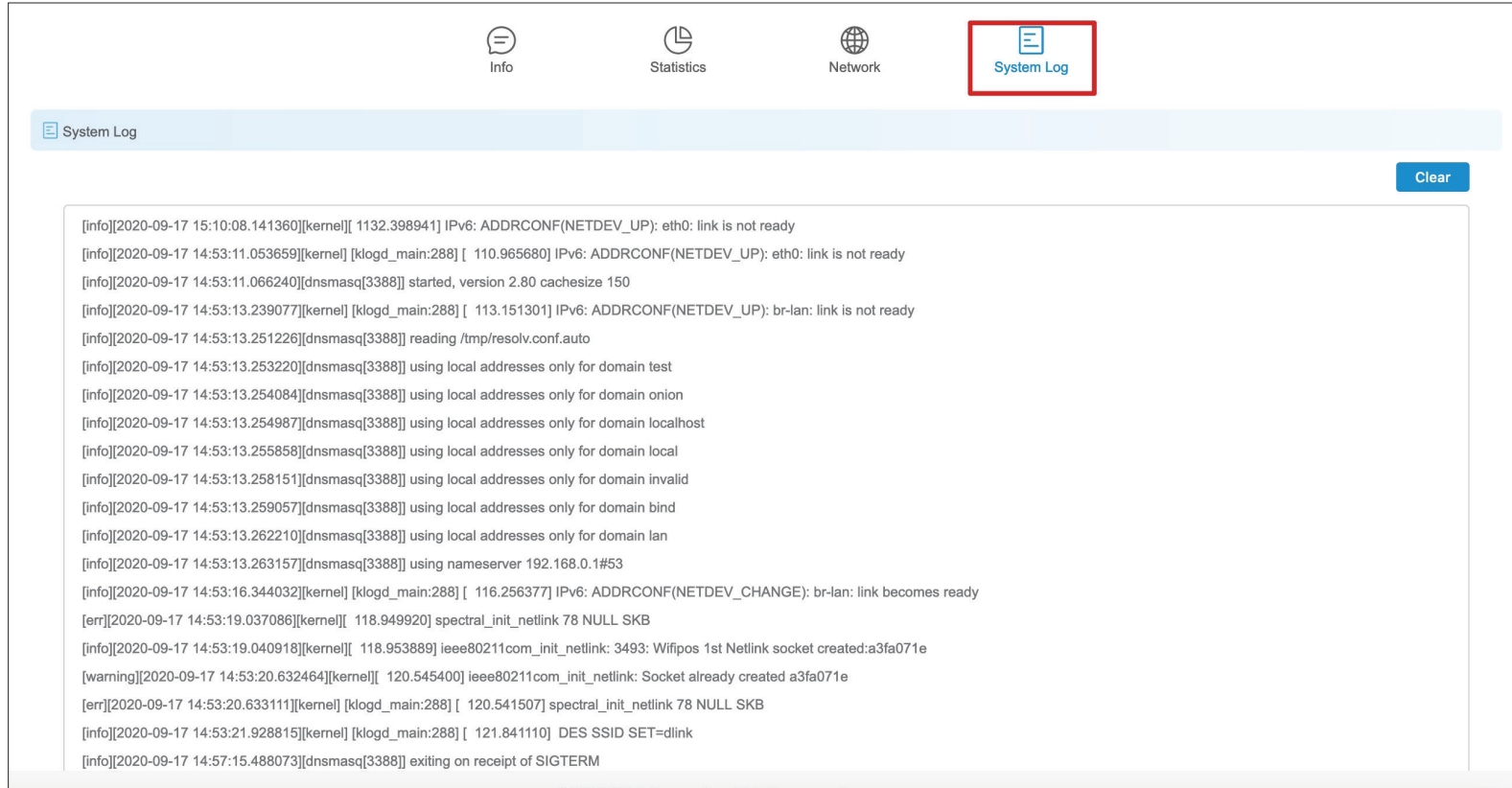
Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.0.1	br-lan	0
192.168.0.0	255.255.255.0	0.0.0.0	br-lan	0
224.0.0.0	240.0.0.0	0.0.0.0	br-lan	0

IPv4 Address	MAC Address	Interface
192.168.0.12	00:E0:4C:68:00:2E	br-lan
192.168.0.1	00:00:00:00:00:00	br-lan

MAC Address	Ageing Timer
9C:B7:93:F1:E3:17	0s
9C:B7:93:F1:E3:16	0s
00:E0:4C:68:00:2E	0s

Syslog Info

This tab shows the current syslog. Click the Clear button to **Clear** the log.



The screenshot displays the 'System Log' interface. At the top, there are four navigation icons: 'Info', 'Statistics', 'Network', and 'System Log' (which is highlighted with a red box). Below the navigation bar, the 'System Log' title is shown on the left, and a 'Clear' button is on the right. The main area contains a list of log entries, each starting with a timestamp and a log level in brackets, followed by the message text.

```
[info][2020-09-17 15:10:08.141360][kernel][ 1132.398941] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[info][2020-09-17 14:53:11.053659][kernel][klogd_main:288][ 110.965680] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[info][2020-09-17 14:53:11.066240][dnsmasq[3388]] started, version 2.80 cachesize 150
[info][2020-09-17 14:53:13.239077][kernel][klogd_main:288][ 113.151301] IPv6: ADDRCONF(NETDEV_UP): br-lan: link is not ready
[info][2020-09-17 14:53:13.251226][dnsmasq[3388]] reading /tmp/resolv.conf.auto
[info][2020-09-17 14:53:13.253220][dnsmasq[3388]] using local addresses only for domain test
[info][2020-09-17 14:53:13.254084][dnsmasq[3388]] using local addresses only for domain onion
[info][2020-09-17 14:53:13.254987][dnsmasq[3388]] using local addresses only for domain localhost
[info][2020-09-17 14:53:13.255858][dnsmasq[3388]] using local addresses only for domain local
[info][2020-09-17 14:53:13.258151][dnsmasq[3388]] using local addresses only for domain invalid
[info][2020-09-17 14:53:13.259057][dnsmasq[3388]] using local addresses only for domain bind
[info][2020-09-17 14:53:13.262210][dnsmasq[3388]] using local addresses only for domain lan
[info][2020-09-17 14:53:13.263157][dnsmasq[3388]] using nameserver 192.168.0.1#53
[info][2020-09-17 14:53:16.344032][kernel][klogd_main:288][ 116.256377] IPv6: ADDRCONF(NETDEV_CHANGE): br-lan: link becomes ready
[err][2020-09-17 14:53:19.037086][kernel][ 118.949920] spectral_init_netlink 78 NULL SKB
[info][2020-09-17 14:53:19.040918][kernel][ 118.953889] ieee80211com_init_netlink: 3493: Wifipos 1st Netlink socket created:a3fa071e
[warning][2020-09-17 14:53:20.632464][kernel][ 120.545400] ieee80211com_init_netlink: Socket already created a3fa071e
[err][2020-09-17 14:53:20.633111][kernel][klogd_main:288][ 120.541507] spectral_init_netlink 78 NULL SKB
[info][2020-09-17 14:53:21.928815][kernel][klogd_main:288][ 121.841110] DES SSID SET=dlink
[info][2020-09-17 14:57:15.488073][dnsmasq[3388]] exiting on receipt of SIGTERM
```

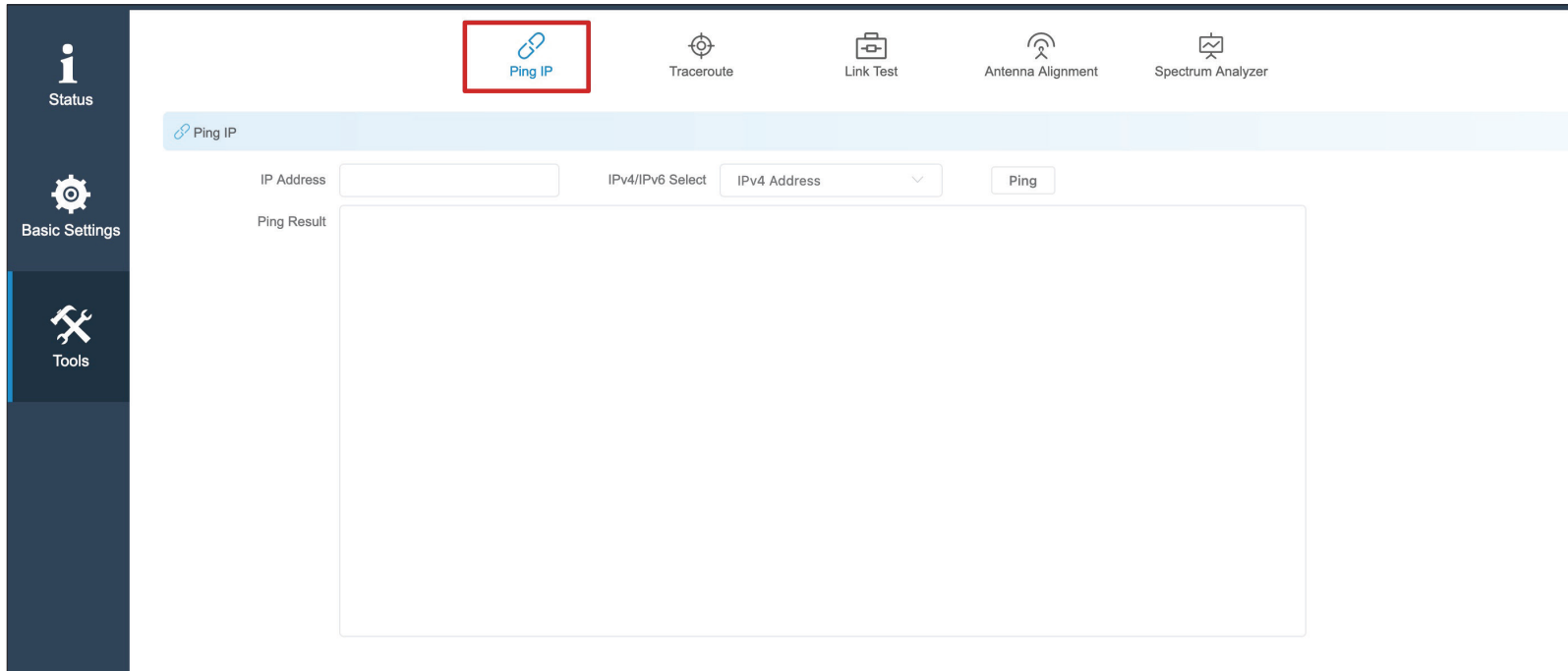
Tools

The DAP-3711 has many useful tools built in to help you manage the device and your network. These tools include **Ping IP**, **Traceroute**, **Link Test**, **Antenna Alignment** and **Spectrum Analyzer**.

Ping IP

You can type in an IP address and check the ping result.

IP Address: Enter the IP address that you would like to ping.



Traceroute

This allows the user to traceroute an IP address.

IP Address: Enter the IP address to traceroute

The screenshot shows a web management console interface with a top navigation bar containing five icons: Ping IP, Traceroute (highlighted with a red box), Link Test, Antenna Alignment, and Spectrum Analyzer. Below the navigation bar is a light blue header with a 'Traceroute' tab icon. The main content area contains the following elements:

- An 'IP Address' text input field.
- An 'IPv4/IPv6 Select' dropdown menu currently set to 'IPv4 Address'.
- A 'Traceroute' button.
- A large, empty rectangular area labeled 'Traceroute Result' for displaying the output.

Link Test

The DAP-3711 has a built-in Iperf function. Users can configure the DAP-3711 in **Iperf Server Mode**. Then the Iperf client can connect to the Iperf server to verify the speed between the two links. In client mode, you can assign an Iperf server IP address to check the speed between the two links.

Iperf Type: Select Client or Server

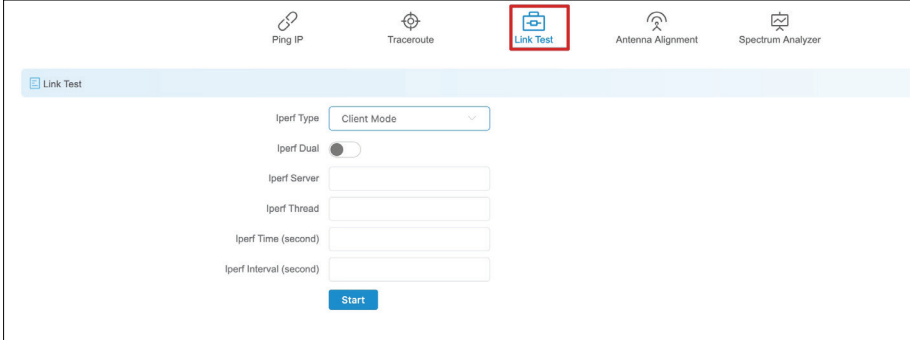
Iperf Dual: If you select Iperf Dual, the DAP-3711 will conduct a bi-directional speed test. Otherwise, it only test the speed of transmission from the Iperf client to the Iperf server.

Iperf Server: Enter the Iperf server's IP address.

Iperf Thread: Enter the number of threads during the test.

Iperf Time: Enter how long the speed test should last.

Iperf Interval: Enter the interval to wait between the tests.



The screenshot shows the 'Link Test' configuration page. At the top, there are five navigation icons: Ping IP, Traceroute, Link Test (highlighted with a red box), Antenna Alignment, and Spectrum Analyzer. Below the navigation bar, the 'Link Test' page has a title bar. The configuration options are as follows:

- Iperf Type:** A dropdown menu set to 'Client Mode'.
- Iperf Dual:** A toggle switch that is currently turned off.
- Iperf Server:** An empty text input field.
- Iperf Thread:** An empty text input field.
- Iperf Time (second):** An empty text input field.
- Iperf Interval (second):** An empty text input field.

At the bottom right of the configuration area, there is a blue 'Start' button.

Antenna Alignment

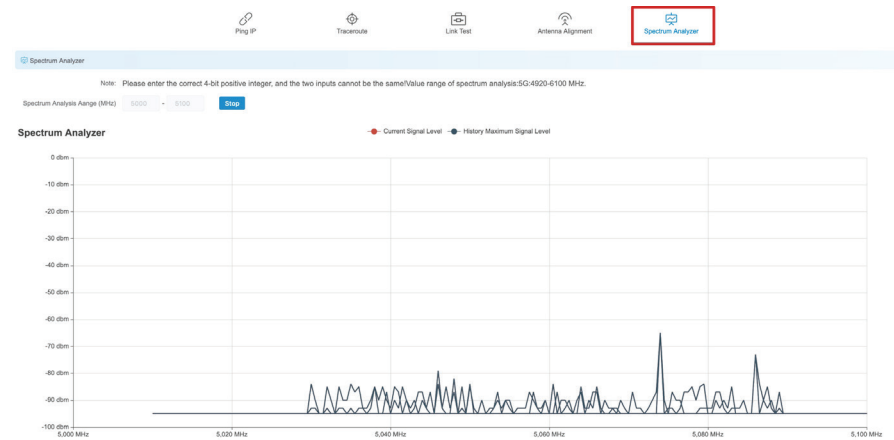
When you select this, the DAP-3711 will recalibrate its signal strength. You can check which angle has the best antenna alignment when you install the DAP-3711.

The screenshot shows a web interface for configuring the DAP-3711. At the top, there is a navigation bar with five icons: Ping IP, Traceroute, Link Test, Antenna Alignment (highlighted with a red box), and Spectrum Analyzer. Below this is a light blue header bar with a menu icon and the text "Antenna Alignment". Underneath the header, there is a "Radio Select" dropdown menu currently set to "ath1" and a blue "Stop" button. The main area of the page is a large empty graph with a vertical axis on the left labeled with signal strength values: 0 dBm, -20 dBm, -40 dBm, -60 dBm, and -80 dBm. The graph area is currently blank, indicating that the alignment process has not yet started or no data is being displayed.

Spectrum Analyzer

You can use the Spectrum Analyzer to scan for the best channels. When performing the scan, the DAP-3711 Wi-Fi may disconnect.

Spectrum Analysis Range: Enter the frequency range to conduct spectrum analysis on. It will take a few seconds to finish the scan.



Technical Specifications

Standards

802.11a/n/ac

Device Interfaces

2 x 100/1000 Mbps Ethernet port, reset button

LEDs

Power, WLAN, LAN, Signal strength

Antenna Type

Directional

Antenna Gain

15 dBi

Beamwidth

H: 40°, V: 15°

Standards

802.11a/n/ac

Protection

8 kV ESD Protection

Enclosure

ABS, IP66 compliant

Operation Modes

AP, Station, WDS AP, WDS Station

Operating Frequency

5180~5320 MHz, 5745~5825 MHz

Max. Transmit Power¹

27 dBm

Wireless Speed

Up to 867 Mbps

Bandwidth Support

20/40/80 MHz

Wireless Configuration

Auto channel support, transmit power selection, SSID broadcast enabling/disabling

Security

802.11i 128-bit AES Personal / Enterprise

System Tools

Ping, traceroute, NTP, ping watchdog, syslog, spectrum analyzer, throughput testing (lperf)

Smart Wireless Technology

TDMA, Auto ACK, intelligent rate control, co-channel interference avoidance

Advanced Features

Max. station limit

¹Range will vary depending on country's maximum transmit power output regulation. Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

LAN Type

Static, DHCP

VLAN Support

Yes

Firewall

IP / MAC filter

Monitors

Throughput, interfaces, routes table, bridge table, ARP table, AP information, syslog

Firmware Upgrade

Web-based upgrade

Power Input

24V Passive PoE

Power Consumption

≤ 15 W

Operating Temperature

-40°C to 65°C

Storage Temperature

-40°C to 85°C

Operating Humidity

0% to 90%

Storage Humidity

0% to 90%

Weight

600g (1.3 lbs)

Dimensions

288 x 88 x 45 mm (11.3 x 3.4 x 1.8 in)

Certifications

CE

FCC

Trademarks:

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright ©2020 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.