

NUCLIAS CONNECT

DAP-3666 User Guide

V 1.00

Table of Contents

Table of Contents	2	WDS with AP Mode	17
Nuclias Connect	4	WDS Mode.....	19
Introduction	4	Wireless Client Mode	21
Nuclias Connect Key Features.....	5	Wireless Security	23
Setup	6	Wired Equivalent Privacy (WEP)	23
Package Contents.....	6	Wi-Fi Protected Access (WPA / WPA2)	24
System Requirements	6	LAN	28
Hardware Overview.....	7	Advanced Settings.....	29
Rear.....	7	Performance	30
LEDs.....	8	Wireless Resource	32
Connections	8	Multi-SSID.....	34
Wireless Basics	9	VLAN.....	37
Four Operational Modes	9	VLAN List.....	37
Connect to your Network.....	10	Port List.....	38
Installation	12	Add / Edit VLAN	39
Installation Considerations	12	PVID Settings.....	40
Setup Wizard	13	Intrusion.....	41
Web User Interface	14	Schedule	42
Basic Settings	15	Internal RADIUS Server	43
Wireless Settings.....	15	ARP Spoofing Prevention	44
Access Point Mode	15	Bandwidth Optimization	45
		Hotspot 2.0.....	47
		Hotspot.....	47
		Interworking.....	48
		WAN Metrics	49
		LIST	50

OSU	51	Log	83
Captive Portal.....	53	View Log.....	83
Authentication Settings - Web Redirection Only	53	Log Settings.....	84
Authentication Settings - Username/Password..	55	Maintenance	85
Authentication Settings - Passcode	57	Administration Settings	86
Authentication Settings - Remote RADIUS.....	59	Limit Administrator	87
Authentication Settings - LDAP.....	61	System Name Settings	87
Authentication Settings - POP3.....	63	Login Settings	88
Login Page Upload	65	Console Settings	88
MAC Bypass.....	66	Ping Control Settings	88
DHCP Server	67	LED Settings.....	89
Dynamic Pool Settings.....	67	Country Settings	89
Static Pool Settings	69	DDP Control Settings	89
Current IP Mapping List.....	70	Nuclias Connect Settings	89
Filters.....	71	Firmware and SSL Certification Upload.....	90
Wireless MAC ACL	71	Configuration File	91
WLAN Partition	72	Time and Date Settings	92
IP Filter Settings.....	73	Configuration.....	93
Traffic Control.....	74	System	94
Uplink/Downlink Settings	74	Logout	95
QoS.....	75	Help	96
Traffic Manager.....	76	Troubleshooting	97
Status	77	Antenna Pattern	102
Device Information	78	Technical Specifications	103
Client Information	79		
WDS Information	80		
Statistics	81		
Ethernet.....	81		
WLAN Traffic Statistics.....	82		

Nuclias Connect

Introduction

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

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

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

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

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

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

Nuclias Connect Key Features

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

For more information on how to use Nuclias Connect with DAP-3666, please refer to the Nuclias Connect User Guide.

Setup

Package Contents

- DAP-3666 Nuclias Connect AC1200 Wave 2 Outdoor Access Point
- Installation Guide
- Mounting kit (Wall/Pole Mount)
- Stainless steel mount base x 1
- Stainless tie back straps x 2
- Wall screw x 4
- Wall plug x 4
- Stainless mount screw (hexagonal hole)
- Hexagon Socket Spanner (Security screw)
- Two LAN Port Waterproof Enclosure
- Grounding Wire

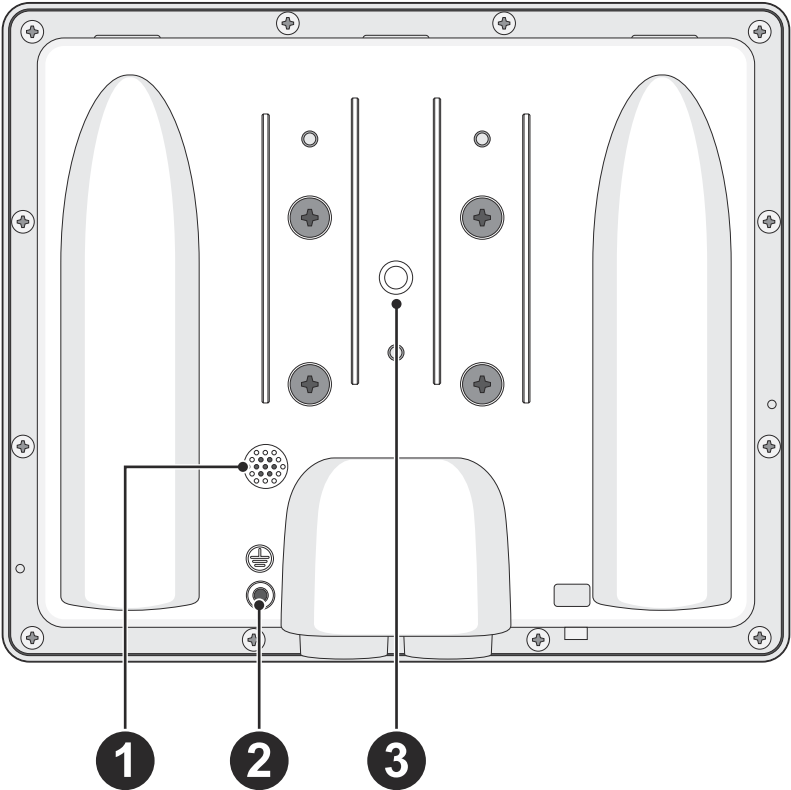
Note: No PSU supplied. To power the units use a D-Link 802.3af PoE switch or the D-Link DPE-301GI, DPE-311GI PoE injector.

System Requirements

Network Requirements	<ul style="list-style-type: none">• IEEE 802.11n/g wireless clients (AP/bridge modes)• IEEE 802.11n/g wireless router or access point (client mode)
Web-based Configuration Utility Requirements	Computer with the following: <ul style="list-style-type: none">• Windows®, Macintosh, or Linux-based operating system Browser Requirements: <ul style="list-style-type: none">• Internet Explorer 11, Chrome 33, Safari 7, or Firefox 28 and above (for web-based configuration)

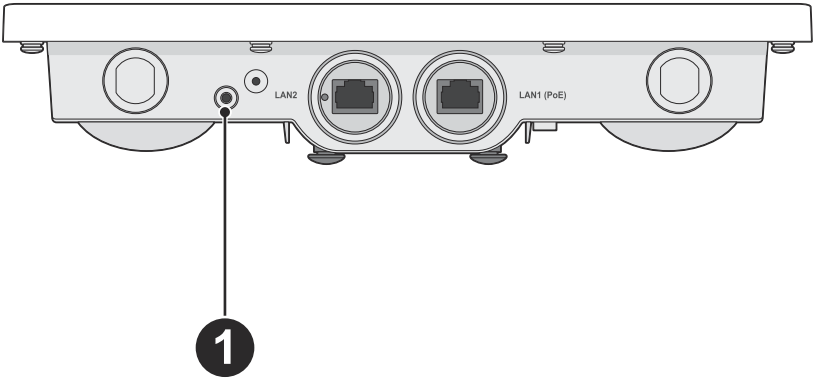
Hardware Overview

Rear



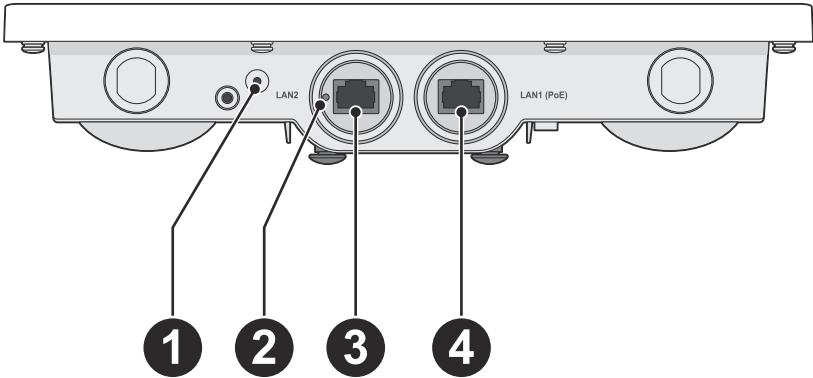
No.	Item	Description
1	Gore-Tex®	Ventilation for heat and humidity dissipation.
2	Grounding Point	Attach a ground wire to the conductor to connect the access point to a grounding electrode.
3	Wall/Pole Mount	Location used to mount on a wall or a pole location.

LEDs



No.	Item	LED Color	Description
1	Power/ Status LED	Red (Solid)	Indicates that the DAP-3666 has malfunctioned.
		Red (Flashing)	Indicates the DAP-3666 is booting up or malfunctioning.
		Green (Solid)	Indicates that the DAP-3666 is working properly.

Connections



No.	Item	Description
1	Mounting Lock	Connector for the mount screw.
2	Reset Button	Press and hold for 10 seconds to factory reset the device.
3	LAN Port	Connect to a switch or router via an Ethernet cable.
4	LAN (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router via an Ethernet cable.

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-3666 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.

Four Operational Modes

Operation Mode (Only support 1 mode at a time)	Function
Access Point (AP)	Create a wireless LAN
WDS with AP	Wirelessly connect multiple networks while still functioning as a wireless AP
WDS	Wirelessly connect multiple networks
Wireless Client	AP acts as wireless network adapter for your Ethernet enabled device

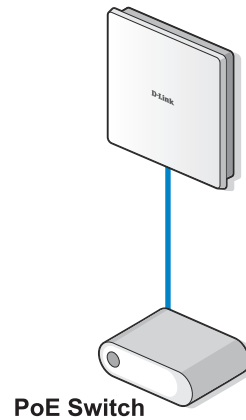
Connect to your Network

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

- Method 1 - Power on by PoE switch.
- Method 2 - Power on by PoE kit.

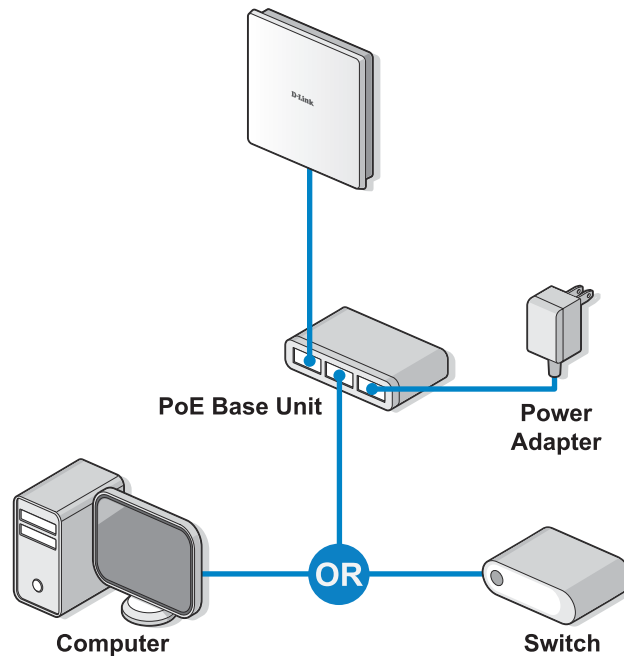
Method 1 - Powered by PoE switch

1. Connect one end of your Ethernet cable into the LAN1 (PoE) port on the DAP-3666 and then connect the other end to your PoE switch.



Method 2 - Powered by PoE kit

1. Connect one end of an Ethernet cable into the **Data In** port on the PoE injector and the other end into one port on your switch, router, or computer.
2. Connect one end of an Ethernet cable into the **P+Data Out** port on the PoE base unit and the other end into the **LAN1 (PoE)** port on the DAP-3666 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.



Installation

Installation Considerations

The D-Link wireless device 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 device 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 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.
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 2.4 GHz 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 GHz 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.

Setup Wizard

The following methods illustrate the setup options required for managing the DAP-3666:

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

Enter **dap3666.local** in the address field on your browser.

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

Username: admin

Password: admin

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

Enter **dap3666.local** in the address field of your browser.

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

Username: admin

Password: admin

3. Connect the access point and your computer via DPE-301GI PoE injector. Manage the access point from the computer.

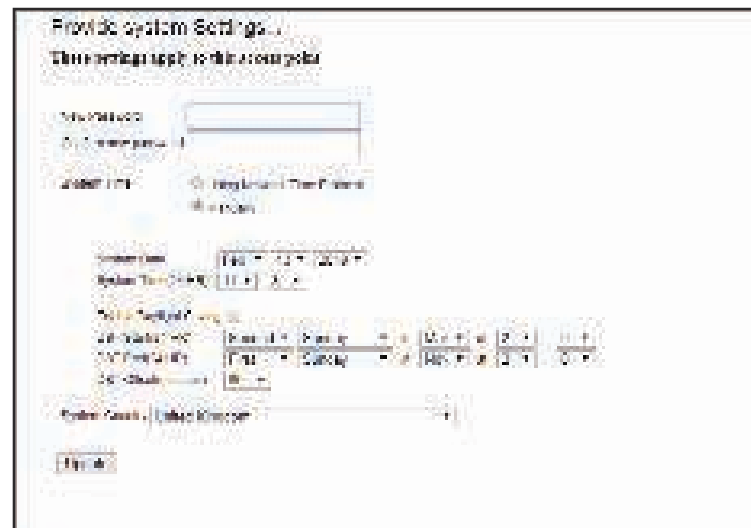
Enter **dap3666.local** in the address field of your browser.

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

Username: admin

Password: admin

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



Web User Interface

The DAP-3666 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type **dap3666.local** in the address field and then press **Enter** to login. Most of the configurable settings are located in the left menu of the web GUI which contains section called **Basic Settings**, **Advanced Settings** and **Status**.



Basic Settings

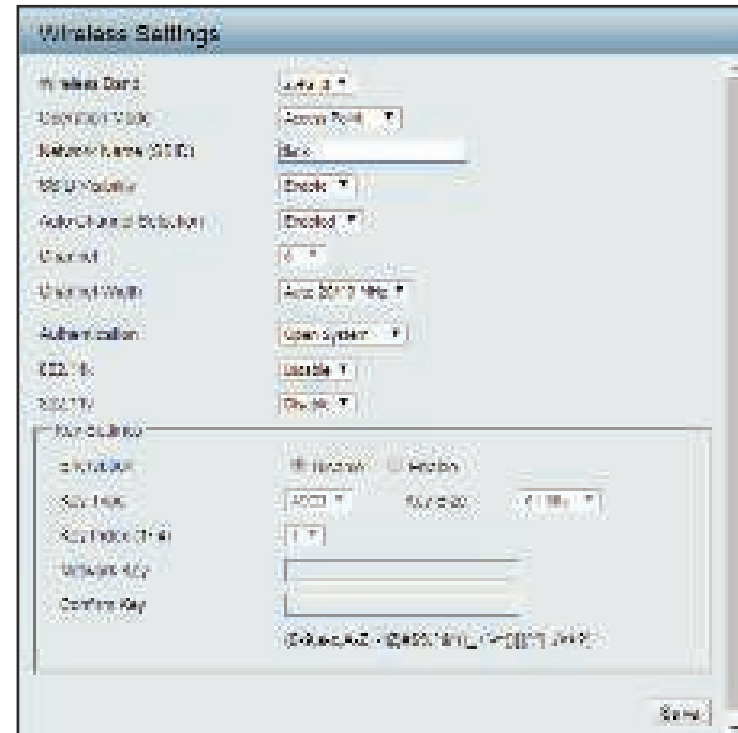
Wireless Settings

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

- **Access Point** - Used to create a wireless LAN
- **WDS with AP** - Used to connect multiple wireless networks while still functioning as a wireless access point
- **WDS** - Used to connect multiple wireless networks
- **Wireless Client** - Used when the access point needs to act as a wireless network adapter for an Ethernet enabled device

Access Point Mode

- | | |
|-------------------------------|--|
| Wireless Band | Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz. |
| Operation Mode | Click the drop-down menu to select Access Point . |
| Network Name (SSID) | Enter the name of Service Set Identifier (SSID) up to 32 characters and is case-sensitive. |
| SSID Visibility | Click the drop-down menu to enable or disable broadcast the SSID across the network. |
| Auto Channel Selection | Click the drop-down menu to enable automatically selects the channel that provides the best wireless performance. The channel selection process only occurs when the AP is booting up. |
| Channel | Click the drop-down menu to select the desired channel. The function is only available when Auto Channel Selection is Disable . |
- Note:** The wireless adapters will automatically scan and match the wireless settings.



Channel Width Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

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

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

802.11k/v/r Use the drop-down menu to choose to enable or disable 802.11k/v/r

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

WDS with AP Mode

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

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

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

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

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

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

Channel Width Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

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

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

The screenshot shows the 'Wireless Settings' page. The 'Wireless Band' is set to 'Auto'. The 'Operation Mode' is set to 'WDS with AP'. The 'Network Name (SSID)' is 'Default'. 'Auto Channel Selection' is 'Disable'. The 'Channel' is '11'. The 'Channel Width' is 'Auto 20/40 MHz'. The 'WDS' section has an 'AP MAC Address' field. The 'WDS List' section has a 'Scan' button and a table with columns: Ch, Channel, MAC Address, Security, and SSID. The table is currently empty. The 'Authentication' section has a 'Open System' dropdown. The 'Force Channel' section has a 'Broadcast' dropdown.

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

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

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

WDS Mode

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

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

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

Auto Channel Selection This option is unavailable in WDS mode.

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

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

Channel Width Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

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

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

The screenshot shows the 'Wireless Settings' page in a web browser. The 'Operation Mode' is set to 'WDS'. The 'Network Name (SSID)' is 'Default'. The 'Auto Channel Selection' is 'Disable'. The 'Channel' is '11'. The 'Channel Width' is 'Auto 20/40 MHz'. The 'WDS' section has an 'AP MAC Address' field. The 'WDS List' section has a 'Scan' button and a table with columns: Ch, Channel, MAC Address, Security, and SSID. The table is currently empty. The 'Authentication' section has a 'Open System' dropdown. The 'Page Controls' section has 'Back', 'Forward', and 'Cancel' buttons.

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

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

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

Wireless Client Mode

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

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

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

SSID Visibility This option is unavailable in Wireless Client mode.

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

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

Channel The channel used will be displayed, and matches the AP that the DAP-3666 is connected to when set to Wireless Client mode.

Channel Width Click the drop-down menu to select **20 MHz**, **Auto 20/40 MHz** or **Auto 20/40/80 MHz**. Select **20 MHz** if you are not using any 802.11n wireless clients. **Auto 20/40 MHz** allows you to connect to both 802.11n and 802.11b/g or 802.11a wireless devices on your network.

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

Authentication Will be explained in the next topic. "Wireless Security" on page 23

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

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

The screenshot shows the 'Wireless Settings' page. The 'Wireless Band' is set to '2.4GHz'. The 'Operation Mode' is set to 'Wireless Client'. The 'Network Name (SSID)' field is empty. The 'SSID Visibility' is set to 'Hidden'. The 'Channel' is set to 'Auto'. The 'Channel Width' is set to 'Auto 20/40 MHz'. The 'Site Survey' section shows a table with columns: Ch, Channel, MAC Address, Security, and SSID. Below the table, it says 'Wireless Client: Scan button is disabled'. The 'Authentication' section shows 'Authentication Mode' set to 'Open System'. The 'Encryption' section shows 'Encryption' set to 'Disable' and 'Key Type' set to 'Any Size'. The 'MAC Clone' section shows 'Enable' checked and 'MAC Source' set to 'Auto'.

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

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

Wireless Security

Wireless security is a key concern for any wireless network. Wireless networks broadcasts 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: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first security method developed. WPA is the newest encryption standard and with the advancements of WPA2, standard wireless networks have finally reach a point where the security is strong enough to give users the peace of mind when installing wireless networks.

Wired Equivalent Privacy (WEP)

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

- **Open System** will send a request to the access point and if the key used matches the one configured on the access point, the access point will return a success message back to the wireless client. If the key does not match the one configured on the access point, the access point will deny the connection request from the wireless client.
- **Shared Key** will send a request to the access point and if the key used matches the one configured on the access point, the access point will send a challenge to the client. The client will then again send a confirmation of the same key back to the access point where the access point will either return a successful or a denial packet back to the wireless client.

Encryption Click the radio button to disable or enable encryption.

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

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

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

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

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

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

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

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

Wi-Fi Protected Access (WPA / WPA2)

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

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

802.11k Click the drop-down menu to enable the 802.11k function.

802.11v Click the drop-down menu to enable the 802.11v function.

802.11r Click the drop-down menu to enable the 802.11r function.

Mobility Domain Enter a name for the mobility domain. The function is only available when **802.11r** is set to **Enable**.

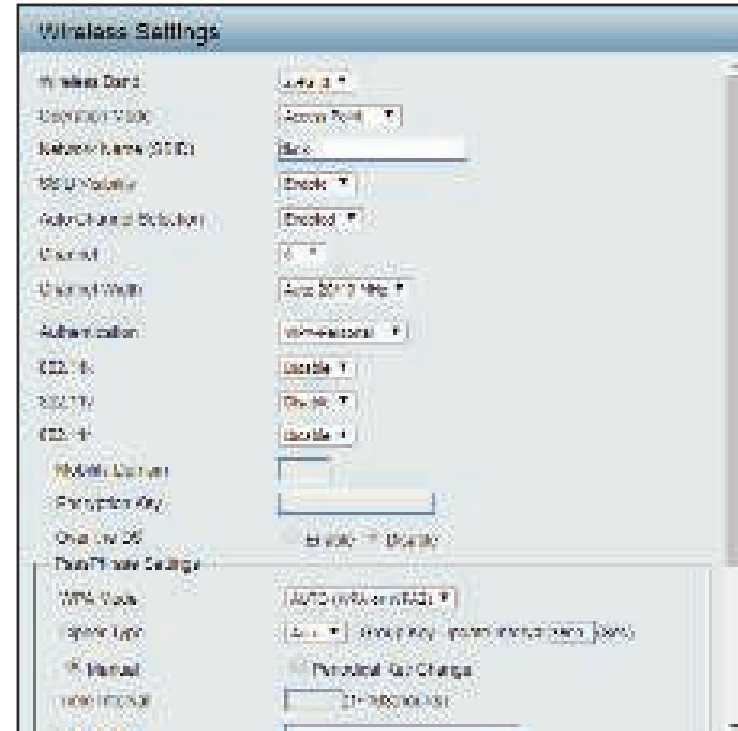
Encryption Key Enter an encryption key to access the wireless network. The function is only available when **802.11r** is set to **Enable**.

Over the DS Click the radio button to disable or enable the function. The function is only available when **802.11r** is set to **Enable**.

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

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

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



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

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

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

802.11k Click the drop-down menu to enable the 802.11k function.

802.11v Click the drop-down menu to enable the 802.11v function.

802.11r Click the drop-down menu to enable the 802.11r function.

Mobility Domain Enter a name for the mobility domain. The function is only available when **802.11r** is set to **Enable**.

Encryption Key Enter an encryption key to access the wireless network. The function is only available when **802.11r** is set to **Enable**.

Over the DS Click the radio button to disable or enable the function. The function is only available when **802.11r** is set to **Enable**.

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

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

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

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

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

Radius Port Enter the RADIUS port.

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

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

Accounting Server Enter the IP address of the accounting server.

Accounting Port Enter the accounting port.

Accounting Secret Enter the accounting secret.

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

LAN

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DAP-3666. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

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

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

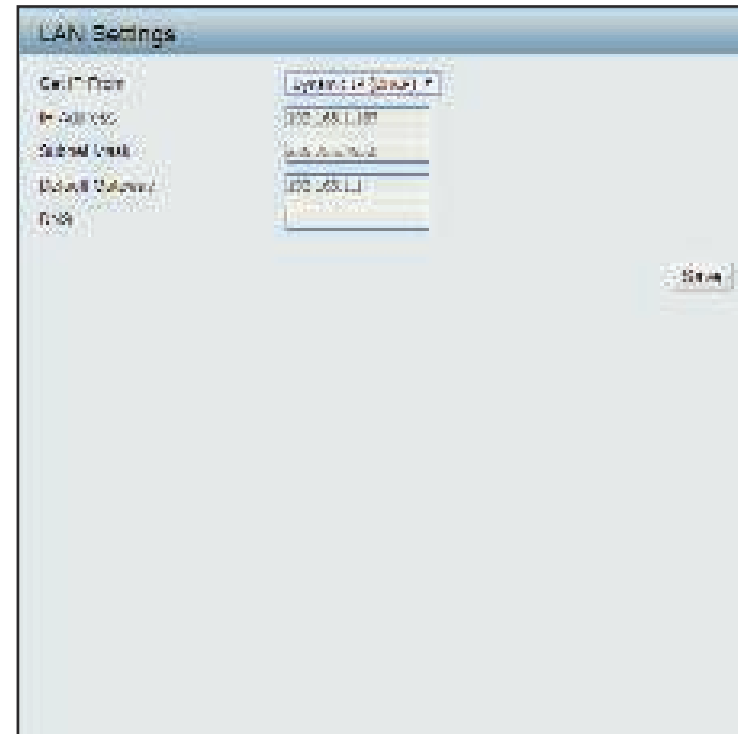
IP Address Enter the IP address to assign a static IP address

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

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

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

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



The screenshot shows the 'LAN Settings' web interface. It features a table with the following fields: 'Get IP From' (set to 'Dynamic IP (DHCP)'), 'IP Address' (192.168.1.100), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.1.1), and 'DNS'. A 'Save' button is located at the bottom right of the form.

Get IP From	IP Address	Subnet Mask	Default Gateway	DNS
Dynamic IP (DHCP)	192.168.1.100	255.255.255.0	192.168.1.1	

Save

Advanced Settings

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



Performance

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

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

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

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

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

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

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

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

- DTM Interval (1-15)** Select a Delivery Traffic Indication Message setting between 1 and 15. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- Transmit Power** Use the drop-down menu to determine the power level of the wireless transmission. Transmitting power can be adjusted to eliminate overlapping of wireless area coverage between two access points where interference is a major concern. For example, if wireless coverage is intended for half of the area, then select 50% as the option.
- WMM (Wi-Fi Multimedia)** This function is available for Mixed 802.11g and 802.11b in 2.4GHz and 802.11a only in 5GHz wireless bands. Click the drop-down menu to enable or disable the WMM function. WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.
- Ack Time Out** To effectively optimize throughput over long distance links enter a value for Acknowledgement Time Out between 25 and 200 microseconds for 5GHz or between 48 and 200 microseconds in the 2.4GHz in the field provided.
- Short GI** Click the drop-down menu to enable or disable the short GI function. Enabling a short guard interval can increase throughput. However, be aware that it can also increase the error rate in some installations due to increased sensitivity to radio-frequency installations.
- IGMP Snooping** Click the drop-down menu to enable or disable the IGMP Snooping function. Internet Group Management Protocol allows the AP to recognize IGMP queries and reports sent between routers and an IGMP host (wireless STA). When IGMP snooping is enabled, the AP will forward multicast packets to an IGMP host based on IGMP messages passing through the AP.
- Multicast Rate** Click the drop-down menu to select the multicast rate to adjust multicast packet data rates.
- Multicast Bandwidth Control** Adjust the multicast packet data rate. The multicast rate is supported in AP mode, (2.4GHz and 5GHz) and WDS with AP mode, including Multi-SSIDs.
- Maximum Multicast Bandwidth** Set the multicast packets maximum bandwidth pass through rate from the Ethernet interface to the Access Point. The function is only available when **Multicast Bandwidth Control** is set to **Enable**.
- HT20/40 Coexistence** Click the drop-down menu to enable the function to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel overlapping and causing interference, the Access Point will automatically change to 20 MHz.
- Transfer DHCP Offer to Unicast** Click the drop-down menu to enable the function to transfer the DHCP Offer to Unicast from LAN to WLAN. Recommended if stations number is larger than 30.
- STP (Spanning tree)** Click the drop-down menu to disable or enable the STP function.
- PMF** Click the drop-down menu to disable or enable the PMF function.
- Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Wireless Resource

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

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

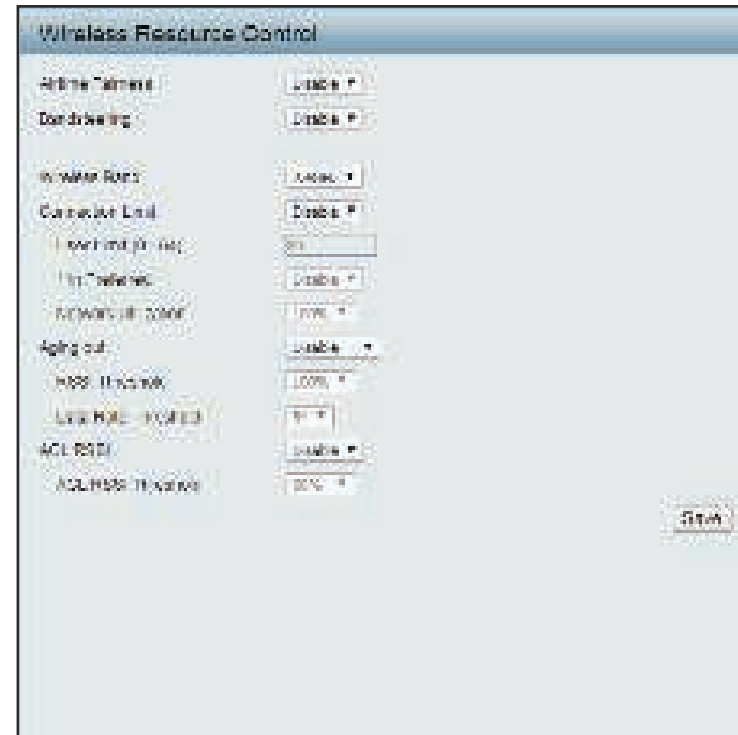
Bandsteering Click the drop-down menu to enable the Band Steering function. When the wireless clients support both 2.4GHz and 5GHz and the 2.4GHz signal is not strong enough, the device will use 5GHz as the higher priority.

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

Connection Limit Click the drop-down menu to enable or disable the connection limit function. This determines whether to limit the number of users accessing this device, effective for load balancing. The exact number is entered in the User Limit field below. This feature allows users to share their wireless network traffic and clients 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-3666 will not allow clients to associate with the AP.

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

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



- Network Utilization** Enter a value to set the maximum utilization of this access point for service. The DAP-3666 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. The function is only available when **Connection Limit** is **Enabled**.
- Aging out** Use the drop-down menu to select the criteria of disconnecting the wireless clients.
- RSSI Threshold** When **Aging out** is **RSSI**, click the drop-down menu to select the percentage of RSSI. When the RSSI of wireless clients is lower than the specified percentage, the device disconnects the wireless clients. The function is only available when **Aging out** is **RSSI**.
- Data Rate Threshold** When **Aging out** is **Data Rate**, click the drop-down menu to select the threshold of data rate. When the data rate of wireless clients is lower than the specified number, the device disconnects the wireless clients. The function is only available when **Aging out** is **Data Rate**.
- ACL RSSI** Click the drop-down menu to enable the ACL RSSI function. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.
- ACL RSSI Threshold** Click the drop-down menu to set the ACL RSSI Threshold.
- Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

Multi-SSID

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

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

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

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

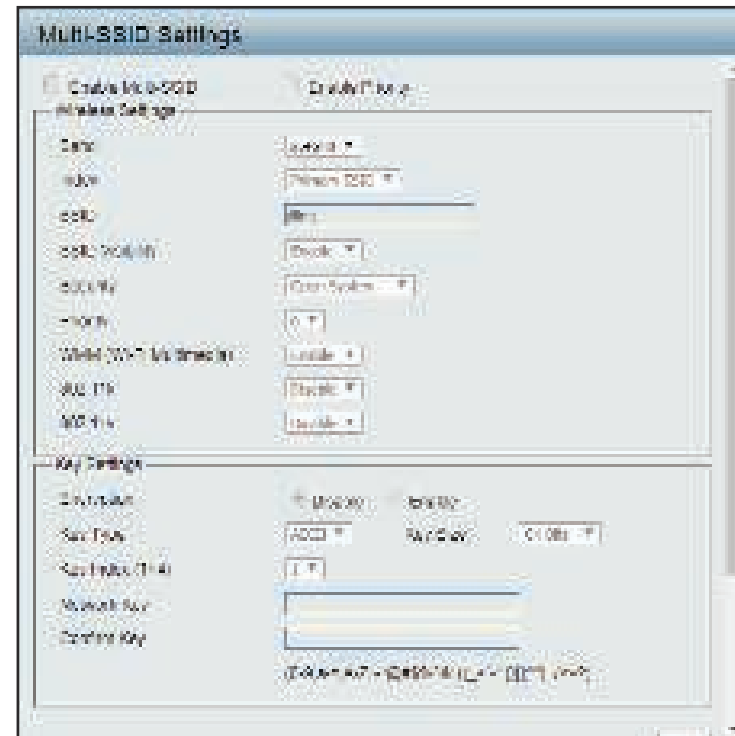
Index You can select up to three multi-SSIDs. With the Primary SSID, you have a total of four multi-SSIDs.

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

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

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

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



- WMM (Wi-Fi Multimedia)** This function is only available when WMM under Performance Settings is enabled. Click the drop-down menu to enable or disable the WMM function. WMM stands for Wi-Fi Multimedia. Enabling this feature will improve the user experience for audio and video applications over a Wi-Fi network.
- 802.11k** Click the drop-down menu to enable the 802.11k function.
- 802.11v** Click the drop-down menu to enable the 802.11v function.
- 802.11r** Click the drop-down menu to enable the 802.11r function. The function is only available when **Security** is **WPA-Personal** or **WPA-Enterprise**.
- Mobility Domain** Enter a name for the mobility domain. The function is only available when **802.11r** is **Enable**.
- Encryption Key** Enter a encryption key to access the wireless network. The function is only available when **802.11r** is **Enable**.
- Over the DS** Click the radio button to disable or enable the function. The function is only available when **802.11r** is **Enable**.
- Encryption** This function is only available when multi-SSID is enabled and Index is an SSID other than Primary SSID. Click the radio button to enable or disable the encryption. If **Enable** is selected the following configurations are required: Key Type, Key Size, Key Index (1~4), Network Key, and Confirm Key.
- Key Type** Click the drop-down menu to select **HEX** or **ASCII**.
- Key Size** Click the drop-down menu to select **64 Bits** or **128 Bits**.
- Key Index (1~4)** Click the drop-down menu to select from the 1st to 4th key to be set as the active key.
- Network Key** Input up to four keys for encryption. You will select one of these keys in the Key Index drop-down menu.
- Confirm Key** Re-enter the value as entered in the Network Key to confirm the setting.
- WPA Mode** When **Security** setting is set to **WPA-Personal** or **WPA-EAP**, click the drop-down menu to select a WPA mode [Options: Auto (WPA or WPA2), WPA2 Only, or WPA1 Only]. Auto (WPA or WPA2) allows you to use both WPA and WPA2. In addition, you must configure Cipher Type, and Group Key Update Interval.
- Cipher Type** When **Security** is **WPA-Personal** or **WPA-EAP**, click the drop-down menu to select **Auto**, **AES**, or **TKIP**.
- Group Key Update Interval** Enter the interval during which the group key will be valid.
- Encryption key** Select the means to define a unique encryption key for the defined cipher type.
- **Manual:** Select the manual option to define the PassPhrase encryption key. The minimum and maximum number of characters is 8 to 63 ASCII characters and 64 characters in HEX. In the Confirm PassPhrase field enter the same key to confirm the setting.
 - **Periodical Key Change:** Select the option to have each client negotiate a very unique encryption key between the client and the access point.
- Time Interval** Enter the variable in hours to set the interval.
- PassPhrase** When **Security** is set to **WPA-Personal**, enter a pass phrase in the corresponding field.

Confirm PassPhrase Retype the Pass Phrase entry to confirm the Pass Phrase.

RADIUS Server When **Security** is set to **WPA-EAP**, enter the IP address of the RADIUS server.

Radius Port Enter the RADIUS port.

RADIUS Secret Enter the RADIUS secret.

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

Accounting Server Enter the IP address of the accounting server.

Accounting Port Enter the accounting port.

Accounting Secret Enter the accounting secret.

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

VLAN

VLAN List

The DAP-3666 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-3666 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

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

VLAN Mode Displays the current VLAN mode.

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

VID Displays the VID of the VLAN.

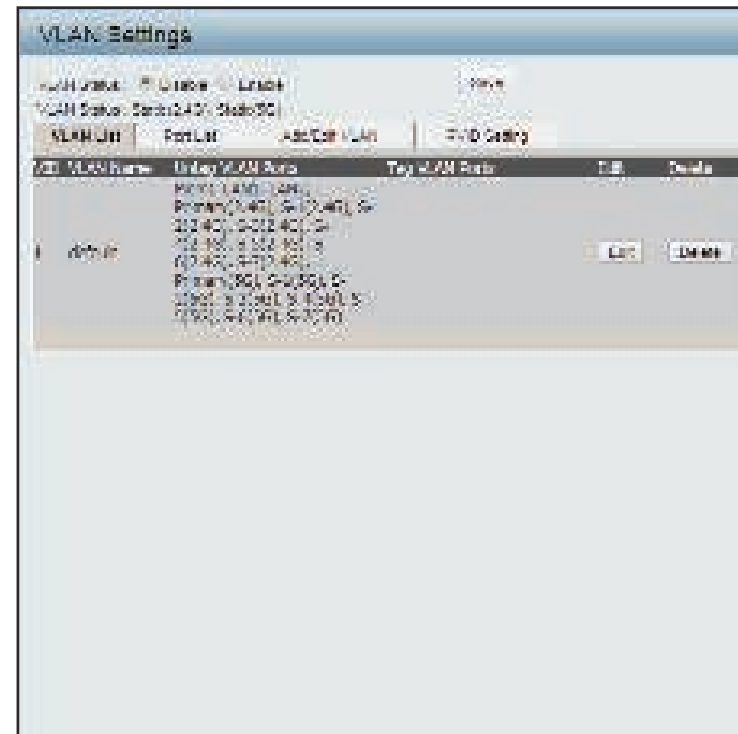
VLAN Name Displays the name of the VLAN.

Untag VLAN Ports Displays the untagged ports.

Tag VLAN Ports Displays the tagged ports.

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

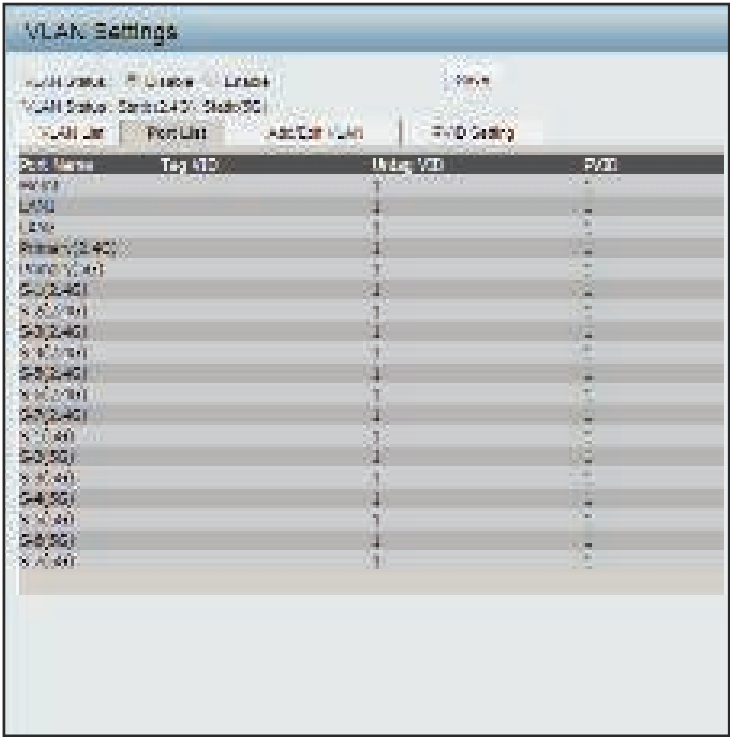
Delete Click **Delete** to delete the current VLAN.



Port List

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

- VLAN Status** Click the radio button to enable or disable VLAN status. Next, go to the **Add/Edit VLAN** tab to add or modify an item on the VLAN List tab.
- VLAN Mode** Displays the current VLAN mode.
 - Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.
- Port Name** Displays the name of the port.
- Tag VID** Displays the tagged VID of the port.
- Untag VID** Displays the untagged VID of the port.
- PVID** Displays the PVID of the port.



Add / Edit VLAN

The Add / Edit VLAN tab is used to configure VLANs.

- VLAN Status** Click the radio button to enable or disable VLAN status. By default this feature is disabled.
- VLAN Mode** Displays the current VLAN mode.
- VLAN ID** Enter a value (1-4094) for the Internal VLAN.
- VLAN Name** Enter the VLAN name to add or modify.
- Save** Click to save the updated configuration.
To make the updates permanent, click **Configuration > Save and Activate**.

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

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

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.

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

VLAN Mode Displays the current VLAN mode.

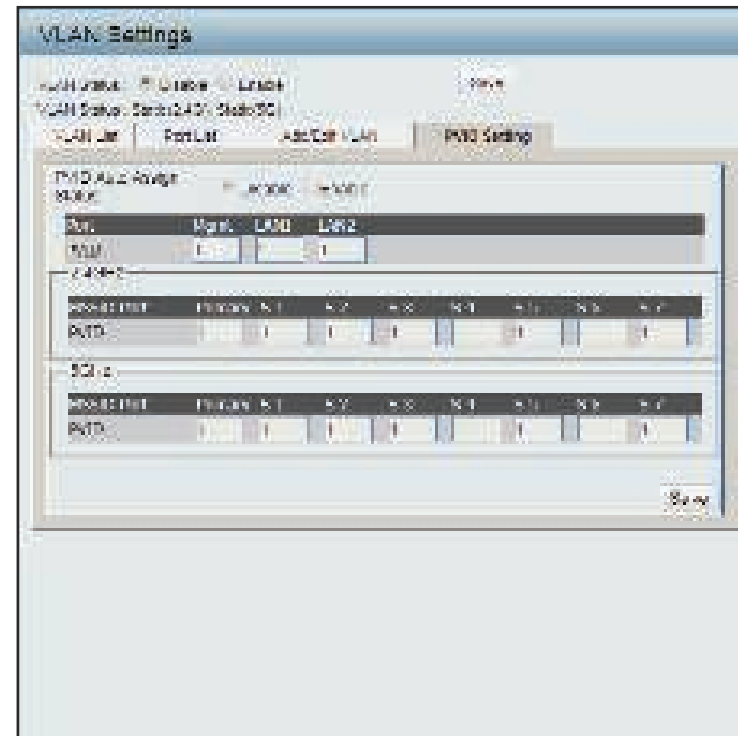
PVID Auto Assign Status Click the radio button to enable or disable PVID auto assign status.

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

For better system consistency, the following configuration settings are recommended:

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

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



Intrusion

The Wireless Intrusion Protection window is used to classify APs as Valid, Neighborhood, Rogue, or a New group.

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

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

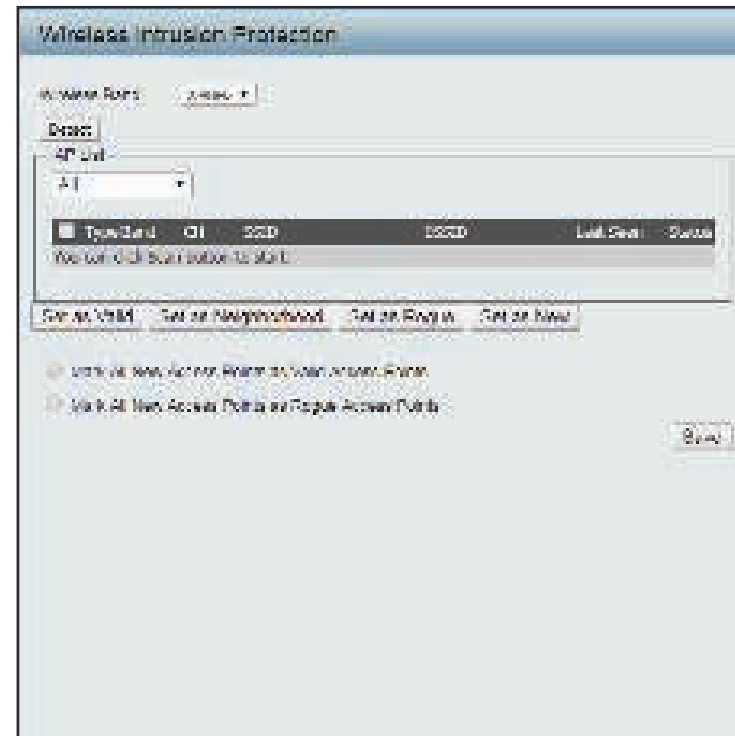
AP List Click the drop-down menu to select **All**, **Valid**, **Neighbor**, **Rogue**, and **New**.

The following is a definition of the listed AP categories:

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

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

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



Schedule

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

- Wireless Schedule** Click the drop-down menu to enable the device's schedule feature.
- Name** Enter a name for the new schedule rule in the field provided.
- SSID Index** Click the drop-down menu to select the desired SSID.
- SSID** Displays the current SSID.
To create a new SSID, go to the Wireless Settings window (**Basic Settings** > **Wireless**).
- Day(s)** Click the radio button to select **All Week** and **Select Day(s)**. If **Select Day(s)** is selected, check the specific days you want the rule to be effective on.
- All Day(s)** Check this box to have your settings apply 24 hours a day.
- Start Time** Enter the beginning hour and minute, using a 24-hour clock.
- End Time** Enter the ending hour and minute, using a 24-hour clock.
- Save** Click to save the updated configuration.
To make the updates permanent, click **Configuration** > **Save and Activate**.

Internal RADIUS Server

The DAP-3666 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click **Save** to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. It is recommended you limit the number of accounts to below 30.

User Name Enter a name to authenticate user access to the internal RADIUS server.

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

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

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



The screenshot shows the 'Internal RADIUS Server' configuration interface. At the top, there is a title bar 'Internal RADIUS Server'. Below it, a blue header bar reads 'RADIUS Accounts (Total: 20 accounts)'. The main configuration area contains three fields: 'User Name' with a text input box and a '(1~32 Characters)' label, 'Password' with a text input box and a '(8~64 Characters)' label, and 'Status' with a 'Enable' radio button and a 'Disable' radio button. Below these fields is another blue header bar 'RADIUS Account List'. Underneath is a table with columns 'User Name', 'Enable', 'Disable', and 'Delete'. The table is currently empty. A 'Save' button is located at the bottom right of the interface.

ARP Spoofing Prevention

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

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

Gateway IP Address Enter a gateway IP address.

Gateway MAC Address Enter a gateway MAC address.

Add Click to create a defined rule.

Clear Click to remove the settings from the menu interface.

Delete All Click to delete all gateway entries.

Edit Click to edit the selected gateway entry.

Delete Click to delete the gateway entry.

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

The screenshot shows the 'ARP Spoofing Prevention Settings' web interface. At the top, there is a toggle switch for 'ARP Spoofing Prevention' which is currently set to 'Disable'. Below this is a section titled 'Add Gateway Address' containing a 'Gateway IP Address' text field and a 'Gateway MAC Address' field with a segmented input for hexadecimal values. There are 'Add' and 'Clear' buttons below these fields. A section titled 'Gateway Address List' contains a table with columns for 'Gateway IP Address', 'Gateway MAC Address', 'Edit', and 'Delete'. The table is currently empty. A 'Save' button is located at the bottom right of the interface.

Bandwidth Optimization

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

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

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

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

Rule Type Click the drop-down menu to select a rule:

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

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

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

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

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

Add Click to create a defined rule.

The screenshot shows the 'Bandwidth Optimization' configuration page. At the top, there's a section to 'Enable Bandwidth Optimization' with a dropdown menu. Below that are input fields for 'Downlink Bandwidth' and 'Uplink Bandwidth'. The main section is 'Add Bandwidth Optimization Rule', which contains a dropdown for 'Rule Type' (set to 'Allocate average BW for each station'), a dropdown for 'Band' (set to '2.4GHz'), a dropdown for 'SSID Index' (set to 'Primary SSID'), and input fields for 'Downlink Speed' and 'Uplink Speed'. There are 'Add' and 'Clear' buttons. Below this is a table titled 'Bandwidth Optimization Rule' with columns: Name, Type, SSID Index, Downlink Speed, Uplink Speed, Edit, and Delete. The table is currently empty. A 'Save' button is located at the bottom right of the page.

Clear Click to remove the settings from the menu interface.

Edit Click to edit the selected gateway entry.

Delete Click to delete the gateway entry.

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

Hotspot 2.0

Hotspot 2.0 (HS2) is a new networking standard designed to make the process of connecting to public wireless hotspots easier and more secure with seamless authentication and encryption between your device and access points. This is based on the IEEE 802.11u standard and uses WPA2-Enterprise for authentication between clients and access points.

Band: Specify Either 2.4 GHz or 5 GHz from the drop down list.

SSID Index: Specify from drop down list the SSID index.

Hotspot

Hotspot 2.0: Choose enable to turn on hotspot 2.0 function.

OSEN: Enable OSU Server-only authenticated layer-2 Encryption Network (OSEN) to indicate that the hotspot uses a OSEN network type.

Allow Cross Connection: Choose enable to allow cross connection for clients.

Manage P2P: Choose enable to allow P2P.

DGAF: This option configures the Downstream Group Addressed Forwarding. Choose enable to allow AP to forward downstream group-addressed frames.

Proxy ARP: Choose enable to allow proxy ARP.

L2TIF: Choose enable to allow Layer 2 Traffic Inspection and Filtering.

The screenshot shows the 'Hotspot 2.0' configuration page. At the top, there are two dropdown menus: 'Band' set to '2.4GHz' and 'SSID Index' set to 'Primary SSID'. Below these are five tabs: 'Hotspot', 'Interworking', 'WPA2/Network', 'LBT', and 'OSU'. The 'Hotspot' tab is selected. Inside this tab, there is a list of settings, each with a label and a dropdown menu:

Setting	Value
Hotspot 2.0	Disable
OSEN	Disable
Allow Cross Connection	Disable
Manage P2P	Disable
DGAF	Enable DGAF
Proxy ARP	Disable
L2TIF	Disable

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

Interworking

Interworking: Choose enable to turn on interworking function.

Access Network Type: Specify type of network.

Internet: Choose to enable or disable Internet access for this network.

ASRA: Choose enable if the network has Additional Steps required for Access.

ESR: Choose enable to indicate that emergency services are reachable through this device.

Venue Group: Specify group venue belongs to.

Venue Type: Specify type of venue.

Venue Name: Specify name of venue. Choose from the drop down list a language used in the name.

HESSID: Specify a homogenous extended service set (ESS) ID that can be used to identify a specific service provider network.

The screenshot shows the 'Hotspot 2.0' configuration interface. At the top, there are dropdown menus for 'Band' (set to 2.4GHz) and 'SSID Index' (set to Primary SSID). Below these are five tabs: 'Hotspot', 'Interworking' (which is selected), 'WPA Metrics', 'LIST', and 'OSU'. The 'Interworking' tab contains several settings, each with a 'Disable' button: 'Interworking', 'Access Network Type', 'Internet', 'ASRA', 'ESR', and 'UEBA'. Below these are three text input fields: 'Venue Group', 'Venue Type', and 'Venue Name' (which has a dropdown menu set to 'English' and a text field containing 'CHT W-R'). At the bottom of the form is a 'HESSID' text input field. A 'Save' button is located in the bottom right corner.

WAN Metrics

- WAN Link Status:** Information about the status of the Access Point's WAN connection.
- WAN Symmetric Link:** Set to 1 if the WAN link is symmetric (upload and download speeds are the same), or set to 0 if not.
- WAN At Capacity:** Set to 1 if the Access Point or the network is at its max capacity, or set to 0 if not.
- WAN Metrics DL Speed:** The downlink speed of the WAN connection set in kbps. If the downlink speed is not known, set to 0.
- WAN Metrics UL Speed:** The uplink speed of the WAN connection set in kbps. If the uplink speed is not known set to 0.

The screenshot shows the 'Hotspot 2.0' configuration interface. At the top, there are dropdown menus for 'Band' (set to 2.4GHz) and 'SSID Index' (set to Primary SSID). Below these are five tabs: 'Hotspot', 'Interworking', 'WAN Metrics' (which is selected and highlighted), 'LIST', and 'DSU'. The 'WAN Metrics' section contains five rows, each with a label and a text input field: 'WAN Link Status' (0), 'WAN Symmetric Link' (0), 'WAN At Capacity' (0), 'WAN Metrics DL Speed' (0), and 'WAN Metrics UL Speed' (0). A 'Save' button is located at the bottom right of the page.

LIST

Network Auth Type: Identifies whether this is an unsecured network.

IP Address Type Availability: Identifies IP address version and type that the Hotspot Operator uses and that would be allocated and available to a mobile device after it authenticates to the network.

Domain Name List: List one or more domain names for the entity operating the AP.

Roaming Consortium: Identifies service providers or groups of roaming partners whose security credentials can be used to connect to a network.

Nai Realm List: List of all NAI realms available through the BSS.

3gpp Cellular Network: Identifies the 3GPP cellular networks available through the AP.

Connection Capability: Identifies the availability of common IP protocols (TCP, UDP, IPsec) and ports (21, 80, 443, 5060).

Operator Friendly Name: Identifies the Hotspot venue operator.

QoS Map: Bit set to indicate support for QoS mapping from 802.11 to external networks.

Hotspot 2.0

Band: 2.4GHz

SSID Index: Primary SSID

Hotspot | Interworking | VLAN Metrics | **LIST** | QoS

List

Network Auth Type	84	
IP Address Type Availability	4	
Domain Name List	example.com	+ -
Roaming Consortium	888443	+ -
Nai Realm List	8.vlan.mmc892.mcc466.3gpp.net	+ -
3gpp Cellular Network	466.092	+ -
Connection Capability	8.88.1	+ -
Operator Friendly Name	English JCHT Wi-Fi	+ -
QoS Map		+ -

Save

OSU

OSU SSID: Specify the SSID that the device will associate and connect to when accessing the OSU server.

OSU Server URI: Specify the Uniform Resource Identifier (URI) of the OSU Server.

OSU Method List: Specify preferred list of encoding methods that the OSU server supports in order of priority.

OSU Config: Choose from drop down list which configuration set to use.

OSU language: Choose from drop down list language to use.

OSU Friendly Name: Specify a list of one or more names in different languages which will allow the device to display the OSU Friendly Name in alternative languages based on the language selected in the setting of the mobile device.

OSU Nai: Specify OSU Network Access Identifier.

OSU Service Description: Choose the service description language from drop down list. Specify the service provider's description of service offering.

OSU Icon Language: Choose icon language from drop down list.

The screenshot shows the 'Hotspot 2.0' configuration page with the 'OSU' tab selected. The page contains the following fields and controls:

- Band:** A dropdown menu set to '2.4GHz'.
- SSID Index:** A dropdown menu set to 'Primary SSID'.
- Tabs:** A row of tabs including 'Hotspot', 'Interworking', 'WAN Metrics', 'LIST', and 'OSU' (which is active).
- OSU Section:**
 - OSU SSID:** A text input field.
 - OSU Server URI:** A text input field.
 - OSU Method List:** A text input field.
 - OSU Config:** A dropdown menu set to 'Config1'.
 - OSU language:** A dropdown menu set to 'Language'.
 - OSU Friendly Name:** A text input field.
 - OSU Nai:** A text input field.
 - OSU Service Description:** A dropdown menu set to 'Language' followed by a text input field.
 - OSU Icon Language:** A dropdown menu set to 'Language'.
 - OSU Icon Name:** A text input field.
 - OSU Icon Width:** A text input field with a numeric value.
 - OSU Icon Height:** A text input field with a numeric value.
 - OSU Icon Type:** A text input field.
 - OSU Icon File Path:** A text input field.
- Save:** A button located at the bottom right of the form.

OSU Icon Name: Specify icon name.

OSU Icon Width: Specify width of the icon, in pixels.

OSU Icon Height: Specify length of the icon, in pixels.

OSU Icon Type: Specify icon file type, where the icon type is any mim-type graphic format.

OSU Icon File Path: Specify location of icon file.

Captive Portal

Authentication Settings - Web Redirection Only

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

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

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

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

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

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

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

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

VLAN Group Enter the VLAN Group ID.

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

- **Static IP (Manual):** Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-3666.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

Edit Click to edit the selected entry.

Delete Click to delete the selected entry.

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

Authentication Settings - Username/Password

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

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

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

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

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

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

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

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

VLAN Group Enter the VLAN Group ID.

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

- **Static IP (Manual):** Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-3666.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

Username Enter the username for the new account.

Password Enter the password for the new account.

Add Click to create a defined rule.

Clear Click to remove the settings from the menu interface.

Edit Click to edit the selected entry.

Delete Click to delete the selected entry.

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

Authentication Settings - Passcode

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

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

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

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

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

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

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

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

VLAN Group Enter the VLAN Group ID.

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

- **Static IP (Manual):** Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-3666.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

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

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

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

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

Add Click to create a defined rule.

Clear Click to remove the settings from the menu interface.

Delete All Click to delete all passcode setting entries.

Edit Click to edit the selected entry.

Delete Click to delete the selected entry.

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

Authentication Settings - Remote RADIUS

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

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

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

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

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

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

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

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

VLAN Group Enter the VLAN Group ID.

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

- **Static IP (Manual):** Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-3666.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

Radius Server Enter the RADIUS server's IP address.

Radius Port Enter the RADIUS server's port number.

Radius Secret Enter the RADIUS server's shared secret.

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

Edit Click to edit the selected entry.

Delete Click to delete the selected entry.

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

Authentication Settings - LDAP

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

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

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

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

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

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

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

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

VLAN Group Enter the VLAN Group ID.

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

- **Static IP (Manual):** Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-3666.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

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

Port Enter the LDAP server's port number.

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

Username Enter the LDAP server account's username.

Password Enter the LDAP server account's password.

Base DN Enter the administrator's domain name.

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

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

Edit Click to edit the selected entry.

Delete Click to delete the selected entry.

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

Authentication Settings - POP3

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

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

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

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

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

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

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

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

VLAN Group Enter the VLAN Group ID.

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

- **Static IP (Manual):** Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-3666.
- **Dynamic IP (DHCP):** The other fields will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

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

Port Enter the POP server's port number.

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

Edit Click to edit the selected entry.

Delete Click to delete the selected entry.

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

Login Page Upload

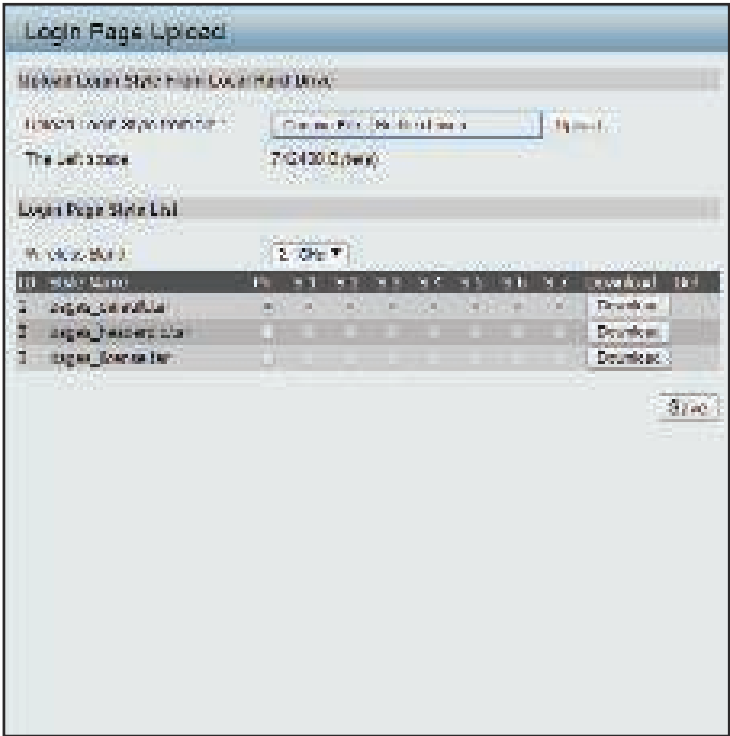
In this window, users can upload a custom login web page that will be used by the captive portal feature. Click **Browse**, to navigate to the custom login file, then click **Upload**.

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

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

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

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



MAC Bypass

The DAP-3666 features a wireless MAC Bypass mechanism that allows clients in a network to access the Internet without the need for Captive Portal authentication.

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

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

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

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

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

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

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

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

The screenshot shows the 'MAC Bypass Settings' web interface. It includes the following elements:

- Wireless Band:** A drop-down menu with '2.4GHz' selected.
- SSID Index:** A drop-down menu with 'Primary SSID' selected.
- MAC Address:** A text input field with a placeholder '00:00:00:00:00:00' and an 'Add' button.
- MAC Address List:** A table with columns 'MAC Address' and 'Delete'. It currently contains one entry: '00:00:00:00:00:00'.
- Upload MAC File:** A section with a 'Choose File' button and an 'Upload' button.
- Download MAC File:** A section with a 'Download' button.
- Save:** A 'Save' button located at the bottom right of the interface.

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-3666 is capable of acting as a DHCP server.

Function Enable/Disable Click the drop-down menu to enable or disable the DAP-3666 functions as a DHCP server. By default this feature is disabled.

Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

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

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

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

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

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

The screenshot shows the 'Dynamic Pool Settings' configuration page. At the top, there's a 'DHCP Server Control' section with a dropdown menu currently set to 'Disable'. Below this is the 'Dynamic Pool Settings' section, which contains several configuration fields: 'IP Assigned From' is set to '192.168.1.1', 'IP Pool Range (1-254)' is set to '255', 'Subnet Mask' is set to '255.255.255.0', 'Gateway' is an empty text box, 'WINS' is an empty text box, 'DHCP Server' is a checkbox that is checked, and 'Lease Time (Sec: 0-1440000)' is set to '3600'. A 'Save' button is located at the bottom right of the form.

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

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

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

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

Static Pool Settings

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

Function Enable/Disable Click the drop-down menu to enable or disable the DAP-3666 functions as a DHCP server. By default this feature is disabled.

Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

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

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

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

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

Gateway Enter the gateway address for the wireless network.

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

DNS Enter the DNS server address for your wireless network.

Domain Name Enter the domain name for the network.

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

Current IP Mapping List

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

- Current DHCP Dynamic Profile

These are IP address pools the DHCP server has assigned using the dynamic pool settings.
- Binding MAC Address

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

The current corresponding DHCP-assigned IP address of the device.
- Lease Time

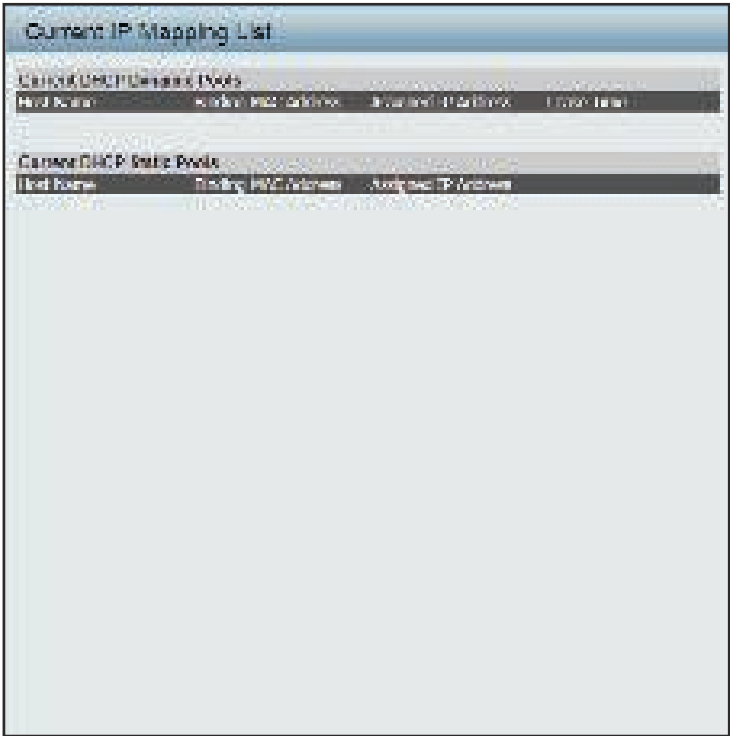
The length of time that the dynamic IP address will be valid.
- Current DHCP Static Pools

These are the IP address pools of the DHCP server assigned through the static pool settings.
- Binding MAC Address

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

The current corresponding DHCP-assigned static IP address of the device.
- Save

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



Filters

Wireless MAC ACL

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

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

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

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

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

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

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

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

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

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

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

The screenshot shows the 'Wireless MAC ACL Settings' page. At the top, there's a title bar. Below it, the 'Wireless Band' is set to '2.4GHz'. The 'Access Control List' is set to 'Allow'. The 'SSID Index' is set to 'Primary SSID'. There are buttons for 'Add', 'Delete', and 'Save'. Below this, there's a table with columns 'ID', 'MAC Address', and 'Delete'. The table is currently empty. Below the table, there's a section for 'Current Client Information' with columns 'MAC Address', 'SSID', 'Signal', and 'RSSI'. Below this, there's a section for 'Upload ACL File' with a 'Choose File' button and an 'Upload' button. At the bottom, there's a 'Download ACL File to Local Hard Drive' button and a 'Save' button.

WLAN Partition

The page allows the user to configure a WLAN Partition.

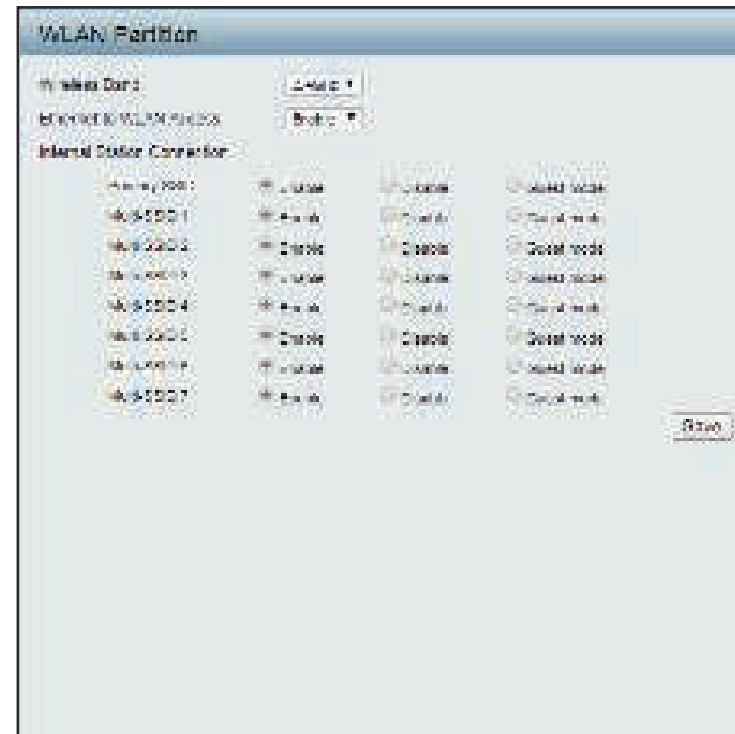
Wireless Band Click the drop-down menu to select the wireless band, 2.4GHz or 5GHz.

Link Integrity Click the drop-down menu to enable or disable the link Integrity function. 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.

Internal Station Connection Click the radio button to a specific mode. The modes are defined as follows:

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

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



IP Filter Settings

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

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

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

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

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

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

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

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

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

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

IP Filter Settings

Wireless Band: 2.4GHz
 SSID Index: Primary SSID
 Filter State: Disable
 IP Address:
 Subnet Mask:

ID	IP Address	Subnet Mask	Delete
1	192.168.70.66	255.255.255.0	Delete
2	192.168.70.0	255.255.255.0	Delete

Upload IP Filter File

Upload File:

Download IP Filter File

Download IP Filter File:

Traffic Control

Uplink/Downlink Settings

The uplink/downlink setting allows users to customize the downlink and uplink interfaces including specifying downlink/uplink bandwidth rates in Mbits per second. These values are also used in the QoS and Traffic Manager windows.

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

Downlink Bandwidth Enter the downlink bandwidth in Mbits per second.

Uplink Bandwidth Enter the uplink bandwidth in Mbits per second.

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

The screenshot shows the 'Uplink and Downlink Settings' web interface. At the top, there are tabs for 'General', 'Uplink', and 'Downlink'. The 'Uplink' tab is currently selected. Below the tabs, there are two sections: 'Downlink Settings' and 'Uplink Settings'. Each section contains a 'Primary' and 'Secondary' bandwidth setting, with a 'Save' button next to each. At the bottom of the page, there are two input fields for 'Downlink Bandwidth (Mbps)' and 'Uplink Bandwidth (Mbps)', each with a 'Save' button. A large 'Save' button is also located at the bottom right of the page.

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DAP-3666 supports four priority levels.

Note: Bandwidth Optimization is disabled if QoS is enabled.

- Enable QoS** Check the box to allow QoS to prioritize traffic. By default this feature is disabled.
- Downlink Bandwidth** Enter the downlink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.
- Uplink Bandwidth** Enter the uplink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.
- ACK/DHCP/ICMP/DNS Priority** Click the drop-down menu to select the level of priority for the selected rule.
- Web Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.
- Mail Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.
- Ftp Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.
- User Defined-1/2/3/4 Priority** Click the drop-down menu to select the level of priority for the selected rule.
- Other Traffic Priority** Click the drop-down menu to select the level of priority for the selected rule.
- Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

The screenshot shows the QoS configuration window. At the top, there's a 'QoS' title bar. Below it, a 'Disable QoS' checkbox is present. The main section is titled 'Activated QoS' and contains a table with the following data:

Traffic Type	Priority	Limit	% Prio.
ACK/DHCP/ICMP/DNS	Highest Priority	Limit 100	% Prio. 25.0000000000
Web Traffic	First Priority	Limit 100	% Prio. 25.0000000000
Mail Traffic	Second Priority	Limit 100	% Prio. 25.0000000000
User Defined-1	Low Priority	Limit 100	% Prio. 25.0000000000
User Defined-2	Second Priority	Limit 100	% Prio. 25.0000000000
User Defined-3	Third Priority	Limit 100	% Prio. 25.0000000000
User Defined-4	Low Priority	Limit 100	% Prio. 25.0000000000
Other Traffic	Low Priority	Limit 100	% Prio. 25.0000000000

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

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.

Note: Bandwidth Optimization is disabled if QoS is enabled.

- Traffic Manager** Click the drop-down menu to enable the traffic manager feature. By default this feature is disabled.
- Unlisted Clients Traffic** Click the radio button to select **Deny** or **Forward** to determine how to deal with unlisted client traffic.
- Downlink Bandwidth** Enter the downlink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.
- Uplink Bandwidth** Enter the uplink bandwidth in Mbits per second. This value is entered in the **Uplink/Downlink Settings** window.
- Name** Enter the name of the traffic manager rule.
- Client IP (optional)** Enter the client IP address of the traffic manager rule.
- Client MAC (optional)** Enter the client MAC address of the traffic manager rule.
- Downlink Speed** Enter the downlink speed in Mbits per second.
- Uplink Speed** Enter the uplink speed in Mbits per second.
- Traffic Manager Rules List** When a rule is entered, it is added to the following index. Click **Edit** or **Delete** to alter the current rule.
- Save** Click to save the updated configuration. To make the updates permanent, click **Configuration > Save and Activate**.

The screenshot shows the 'Traffic Manager' configuration window. At the top, there's a 'Traffic Manager' dropdown menu set to 'Disable'. Below it are radio buttons for 'Unlisted Clients Traffic' (set to 'Deny') and 'Forward'. There are input fields for 'Downlink Bandwidth' (set to '100') and 'Uplink Bandwidth' (set to '100'). A section titled 'Add Traffic Manager Rule' contains input fields for 'Name', 'Client IP (optional)', 'Client MAC (optional)', 'Downlink Speed' (set to '100'), and 'Uplink Speed' (set to '100'). Below this is a table titled 'Traffic Manager Rules' with columns: 'Name', 'Client IP', 'Client MAC', 'Downlink Speed', 'Uplink Speed', 'Edit', and 'Delete'. The table contains two rows of rules. At the bottom right is a 'Save' button.

Name	Client IP	Client MAC	Downlink Speed	Uplink Speed	Edit	Delete
Rule1	192.168.1.100	08:00:27:00:00:00	100Mbps	100Mbps	Edit	Delete
Rule2	192.168.1.101	08:00:27:00:00:01	100Mbps	100Mbps	Edit	Delete

Status

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



Device Information

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

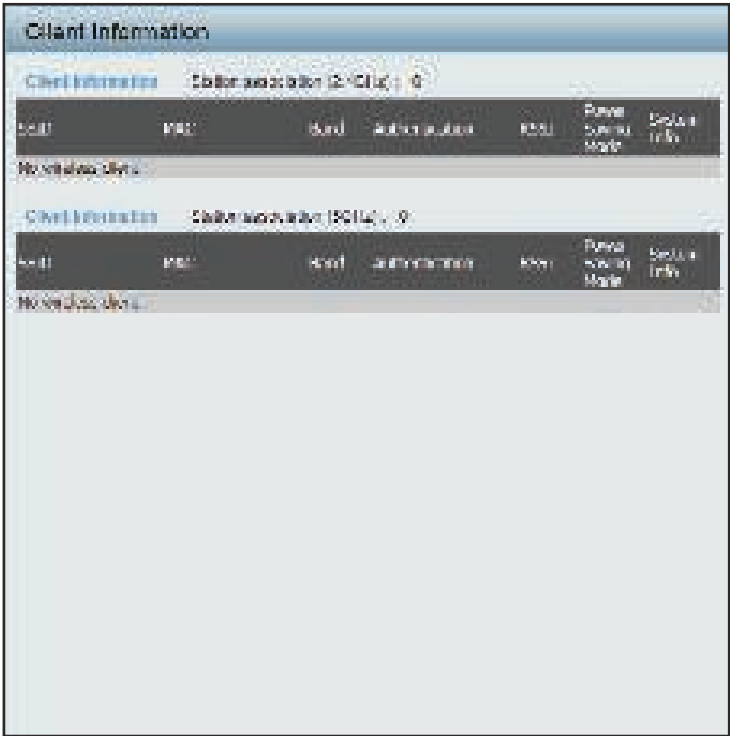
- Ethernet MAC Address** Displays the Ethernet MAC address.
- Wireless MAC Address (2.4GHz)** Displays the 2.4GHz wireless MAC address.
- Wireless MAC Address (5GHz)** Displays the 5GHz wireless MAC address.
- IP Address** Displays the assigned IP address.
- Subnet Mask** Displays the assigned subnet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

Device Information	
Firmware Version: v1.00	
Ethernet MAC Address:	00:14:10:00:00:00
Wireless MAC Address (2.4GHz):	Primary: 00:14:10:00:00:00
	Secondary: 00:14:10:00:00:00
Wireless MAC Address (5GHz):	Primary: 00:14:10:00:00:00
	Secondary: 00:14:10:00:00:00
Ethernet	
IP Address:	192.168.1.100
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
DNS:	---
Wireless 2.4GHz	
Network Name (SSID):	Link
Channel:	CH1 (Auto)
Data Rate:	Auto (Up to 300 Mbps)
Security:	WPA-PSK (TKIP) / WPA-PSK (AES)
Wireless 5GHz	
Network Name (SSID):	Link
Channel:	CH 100 + 104 + 108 + 112 (Auto)
Data Rate:	Auto (Up to 400 Mbps)

Client Information

The page displays the associated clients SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-3666 network.

- SSID** Displays the associated clients SSID for the network.
- MAC** Displays the associated clients MAC address for the network.
- Band** Displays the associated clients band for the network.
- Authentication** Displays the associated authentication method for the network.
- RSSI** Displays the associated clients RSSI for the network.
- Power Saving Mode** Displays the associated clients power saving mode for the network.
- System Info** Displays the associated clients information for the network.



WDS Information

The page displays the access points SSID, MAC, band, authentication method, signal strength, and status for the DAP-3666's Wireless Distribution System network.

- Name** Displays the AP SSID for the network.
- MAC** Displays the AP MAC address for the network.
- Authentication** Displays the AP authentication method for the network.
- Signal** Displays the AP signal for the network.
- Status** Displays the AP status for the network.

WDS Information				
WDS Information Channel : 5				
Name	MAC	Authentication	Signal	Status
WDS Information Channel : 100				
Name	MAC	Authentication	Signal	Status

Statistics

Ethernet

Displays wired interface network traffic information.

- Transmitted Packet Count

Displays the transmitted packet count.
- Transmitted Bytes Count

Displays the transmitted bytes count.
- Dropped Packet Count

Displays the dropped packet count.
- Received Packet Count

Displays the received packet count.
- Received Bytes Count

Displays the received bytes count.
- Dropped Packet Count

Displays the dropped packet count.
- Refresh

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

Ethernet Traffic Statistics		
	LAN1	LAN2
Transmitted Count		
Transmitted Packet Count	24152	10159
Transmitted Bytes Count	34325632	8463136
Dropped Packet Count	0	0
Received Count		
Received Packet Count	22159	0
Received Bytes Count	2711157	0
Dropped Packet Count	0	0

WLAN Traffic Statistics

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

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

	24GHz	5GHz
Transmitted Count		
Transmitted Packet Count	0	0
Transmitted Bytes Count	0	0
Dropped Packet Count	2977	0
Transmitted Retry Count	0	0
Received Count		
Received Packet Count	0	0
Received Bytes Count	0	0
Dropped Packet Count	0	0
Received CRC Count	11831	0
Received Decryption Error Count	0	0
Received MIC Error Count	0	0
Received PHY Error Count	0	0

Log

View Log

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

- View Log** Displays the AP's embedded memory holds logs, up to 500 logs.
- First Page** Click to display the home View Log page.
- Last Page** Click to display the last View Log page.
- Previous** Click to display the page occurring before in order.
- Next** Click to display the page occurring after in order.
- Clear** Click to remove all listings from the View Log page.

View Log				
First Page	Last Page	Page 2 of 2	Next	Close
Date and Time		Message		
Feb 13 13:40:54		Ethernet0 LINK DOWN		
Feb 13 13:41:01		Ethernet0 LINK UP		
Feb 13 13:41:02		Ethernet0 LINK UP		
Feb 13 13:41:05		Ethernet0 LINK DOWN		
Feb 13 13:42:42		Ethernet0 LINK UP		
Feb 13 13:42:45		Ethernet0 LINK DOWN		
Feb 13 13:42:50		Ethernet0 LINK UP		
Feb 13 13:42:54		Ethernet0 LINK DOWN		
Feb 13 13:43:01		Ethernet0 LINK DOWN		
Feb 13 13:43:01		Ethernet0 LINK DOWN		
Feb 13 13:43:02		Ethernet0 LINK DOWN		
Feb 13 13:43:03		Ethernet0 LINK UP		
Feb 13 13:43:07		Ethernet0 LINK DOWN		
Feb 13 13:43:08		Ethernet0 LINK DOWN		
Feb 13 13:43:09		Ethernet0 LINK DOWN		
Feb 13 13:43:10		Ethernet0 LINK DOWN		
Feb 13 13:43:11		Ethernet0 LINK DOWN		
Feb 13 13:43:12		Ethernet0 LINK DOWN		
Feb 13 13:43:13		Ethernet0 LINK DOWN		
Feb 13 13:43:14		Ethernet0 LINK DOWN		
Feb 13 13:43:15		Ethernet0 LINK DOWN		
Feb 13 13:43:16		Ethernet0 LINK DOWN		
Feb 13 13:43:17		Ethernet0 LINK DOWN		
Feb 13 13:43:18		Ethernet0 LINK DOWN		
Feb 13 13:43:19		Ethernet0 LINK DOWN		
Feb 13 13:43:20		Ethernet0 LINK DOWN		
Feb 13 13:43:21		Ethernet0 LINK DOWN		
Feb 13 13:43:22		Ethernet0 LINK DOWN		
Feb 13 13:43:23		Ethernet0 LINK DOWN		
Feb 13 13:43:24		Ethernet0 LINK DOWN		
Feb 13 13:43:25		Ethernet0 LINK DOWN		
Feb 13 13:43:26		Ethernet0 LINK DOWN		
Feb 13 13:43:27		Ethernet0 LINK DOWN		
Feb 13 13:43:28		Ethernet0 LINK DOWN		
Feb 13 13:43:29		Ethernet0 LINK DOWN		
Feb 13 13:43:30		Ethernet0 LINK DOWN		
Feb 13 13:43:31		Ethernet0 LINK DOWN		
Feb 13 13:43:32		Ethernet0 LINK DOWN		
Feb 13 13:43:33		Ethernet0 LINK DOWN		
Feb 13 13:43:34		Ethernet0 LINK DOWN		
Feb 13 13:43:35		Ethernet0 LINK DOWN		
Feb 13 13:43:36		Ethernet0 LINK DOWN		
Feb 13 13:43:37		Ethernet0 LINK DOWN		
Feb 13 13:43:38		Ethernet0 LINK DOWN		
Feb 13 13:43:39		Ethernet0 LINK DOWN		
Feb 13 13:43:40		Ethernet0 LINK DOWN		
Feb 13 13:43:41		Ethernet0 LINK DOWN		
Feb 13 13:43:42		Ethernet0 LINK DOWN		
Feb 13 13:43:43		Ethernet0 LINK DOWN		
Feb 13 13:43:44		Ethernet0 LINK DOWN		
Feb 13 13:43:45		Ethernet0 LINK DOWN		
Feb 13 13:43:46		Ethernet0 LINK DOWN		
Feb 13 13:43:47		Ethernet0 LINK DOWN		
Feb 13 13:43:48		Ethernet0 LINK DOWN		
Feb 13 13:43:49		Ethernet0 LINK DOWN		
Feb 13 13:43:50		Ethernet0 LINK DOWN		
Feb 13 13:43:51		Ethernet0 LINK DOWN		
Feb 13 13:43:52		Ethernet0 LINK DOWN		
Feb 13 13:43:53		Ethernet0 LINK DOWN		
Feb 13 13:43:54		Ethernet0 LINK DOWN		
Feb 13 13:43:55		Ethernet0 LINK DOWN		
Feb 13 13:43:56		Ethernet0 LINK DOWN		

Log Settings

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

Log Server / IP Address Enter the IP address of the log server.

Log Type Check the boxes to select the log type.

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

Email Notification Check the box to enable sending email notification.

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

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

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

From Email Address Enter the email address.

To Email Address Enter the email address.

Email Server Address Enter the email server address.

SMTP Port Enter the SMTP port.

Account Enter the name of the new user entry.

Password Enter the password set for the email notification.

Confirm Password Retype the password entry to confirm the password.

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

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

Maintenance

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



Administration Settings

The administrator or users with administration privilege can access the administration management interface. By the default the admin account is not configured with a password. It is highly recommended to create a password before configuring the settings.

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



Limit Administrator

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

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

Limit Administrator IP Check the box to enable the limit administrator IP address.

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

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

System Name Settings

System Name Enter the name of the device. The default name is D-Link DAP-3666.

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

MDNS Name Enter the name of the multicast DNS. The default name is dap3666.

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

Login Settings

Login Name Enter a user name.

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

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

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

Console Settings

Status Check the box to enable the console.

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

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

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

Ping Control Settings

Status Check the box to enable the ping control setting.

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

LED Settings

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

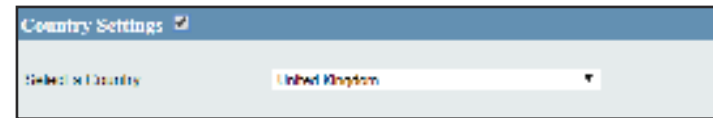
Note: To save the new configuration settings to the firmware, click **Configuration > Save and Activate**, otherwise click **Discard Changes** to delete any setting change.



Country Settings

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

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



DDP Control Settings

Status Check the box to enable the DDP control setting.

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



Nuclias Connect Settings

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

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

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



Firmware and SSL Certification Upload

This page allows the user to perform a firmware upgrade which is an essential tool 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 updated firmware version available.

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

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

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

The screenshot shows a web interface titled "Firmware and SSL Certification Upload". It contains three main sections, each with a "Choose File" button, an "No file chosen" text, and an "Upload" button. The first section is for "Upload Firmware From File", the second is for "Language Pack Upload", and the third is for "Update SSL Certification From Local Hard Drive".

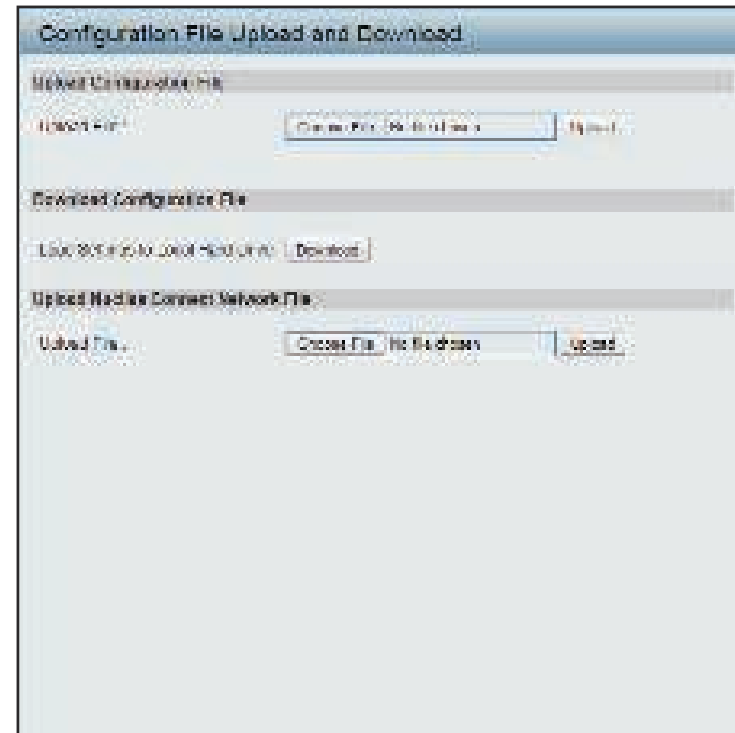
Configuration File

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

Upload Configuration File If have a configuration file, click **Choose File**. Select the configuration file and click **Open** and **Upload** to update the configuration.

Download Configuration File Click **Download** to save the current configuration file to your local disk. if you save a configuration file that contains an administrator's password, after resetting your DAP-3666 and then updating to this saved configuration file, the password will be gone.

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



Time and Date Settings

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

Current Time Displays the current time and date.

Enable NTP Check the box to enable the AP to get the system time from an NTP server over the Internet.

NTP Server Enter the NTP server IP address.

Time Zone Click the drop-down menu to select your correct time zone.

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

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

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

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

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

The screenshot shows the 'Time and Date Settings' page. It includes sections for 'Time Configuration' (Current Time: 2015/02/10 14:04:53), 'Automatic Time Configuration' (Enable NTP checkbox, NTP Server IP field, Time Zone dropdown), 'Set the Date and Time Manually' (Time and Date input fields, a 'Copy Your Computer's Time Settings' button), and 'Daylight Configuration' (Enable Daylight Saving checkbox, Daylight Saving Offset dropdown, and a table for Daylight Saving Dates with columns for Month, Year, Day, Hour, and Minute).

Configuration

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

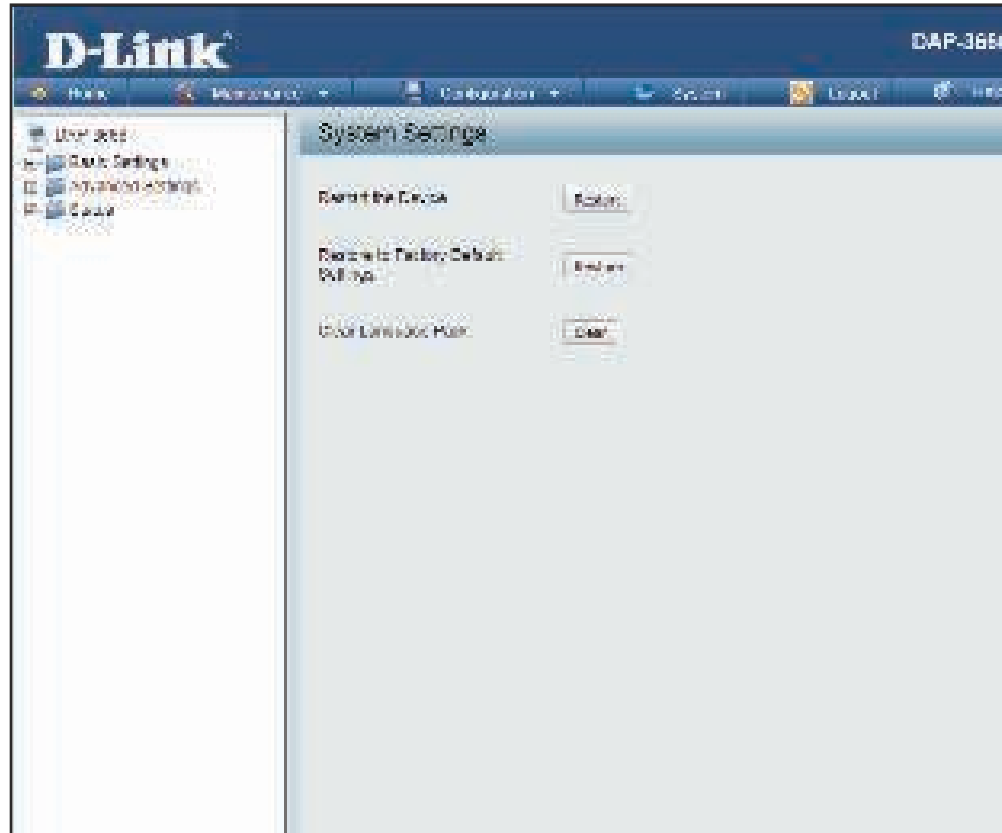
- Save and Activate: Click **Save and Activate** to have configuration changes you have made to be saved across a system reboot.
- Discard Changes: Click **Discard Changes** to discard the settings you have made.



System

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

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



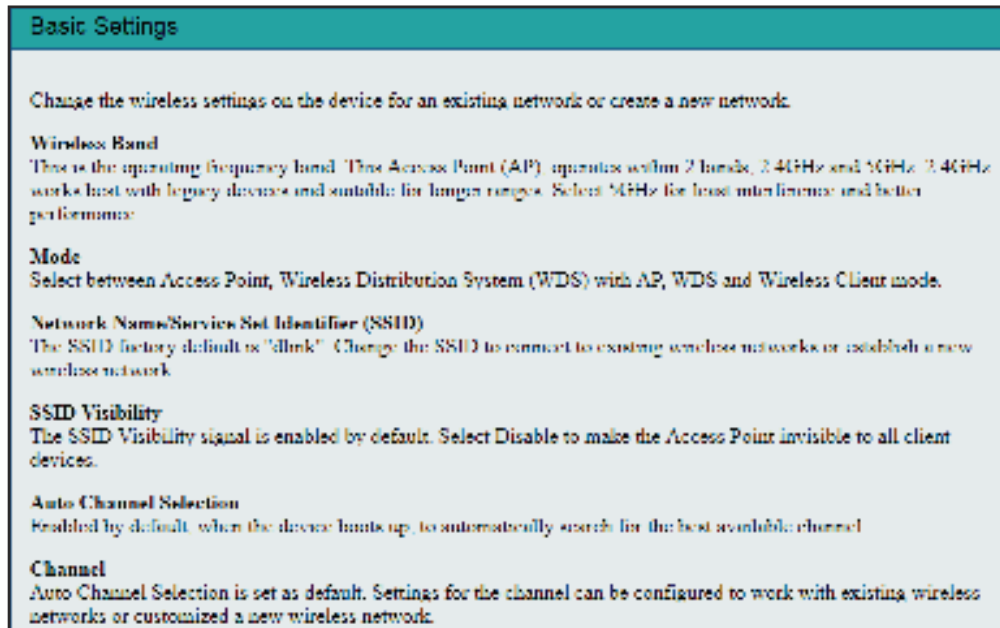
Logout

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



Help

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-3666. We will cover various aspects of the network setup, especially the network adapters. Please read the following if you are having any technical difficulties.

Note: *It is recommended that you use an Ethernet connection to configure the DAP-3666.*

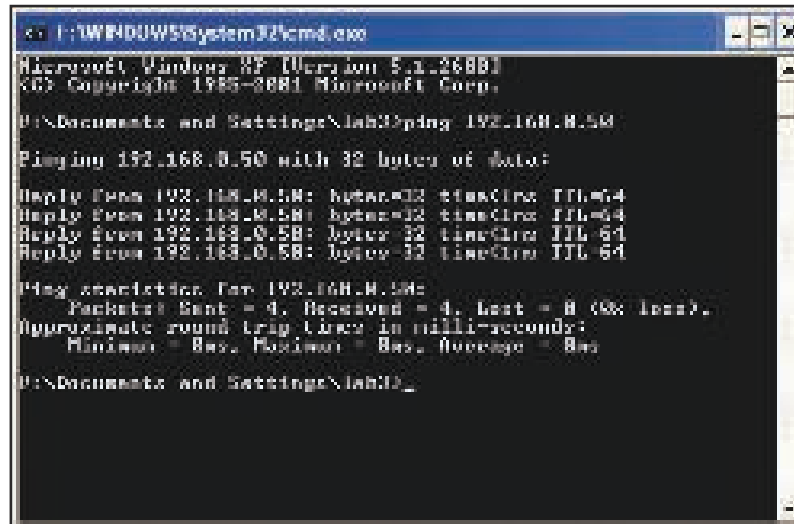
The computer used to configure the DAP-3666 cannot access the Configuration menu.

- Check if the Power LED on the DAP-3666 is ON. If the LED is not ON, check if the cable for the Ethernet connection is securely inserted.

Note: *The default LAN settings for the DAP-3666 is set to DHCP. If the DHCP server does not provide an IP address for the AP, you can use the following settings to access the AP: 192.168.0.50 or type dap3666.local in the web browser's address bar.*

- Perform a Ping test to make sure that the DAP-3666 is responding. Go to **Start > Run**, type `cmd`, and then press **Enter**. At the DOS prompt, type `ping 192.168.0.50`. A successful ping will show four replies.

Note: *If you have changed the default IP address, make sure to ping the correct IP address assigned to the DAP-3666.*



```

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

D:\Documents and Settings\lab\ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Reply from 192.168.0.50: bytes=32 time=64ms TTL=64
Reply from 192.168.0.50: bytes=32 time=64ms TTL=64
Reply from 192.168.0.50: bytes=32 time=64ms TTL=64
Reply from 192.168.0.50: bytes=32 time=64ms TTL=64

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 64ms, Maximum = 64ms, Average = 64ms

D:\Documents and Settings\lab>
  
```

The wireless client cannot access the Internet within Infrastructure mode.

Make sure the wireless client is associated and joined with the correct access point. To check this connection, right-click on the Local Area Connection icon in the taskbar and select **View Available Wireless Networks**. The Connect to Wireless Network screen will appear. Please make sure you have selected the correct available network, as shown in the illustrations below.



- Check that the IP address assigned to the wireless adapter is within the same IP address range as the access point and gateway. Since the DAP-3666 has an IP address of 192.168.0.50, wireless adapters must have an IP address in the same range, e.g. 192.168.0.x. Each device must have a unique IP address; there may be no two devices with the same IP address. The subnet mask must be the same for all the computers on the network. To check the IP address assigned to the wireless adapter, double-click the Local Area Connection icon in the taskbar, then select the Support tab and the IP address will be displayed.
- If it is necessary, assign a Static IP Address to the wireless adapter. If you are entering a DNS Server address, you must also enter the Default Gateway Address. Remember that if you have a DHCP-capable router, you will not need to assign a static IP address.

What variables may cause my wireless products to lose reception?

D-Link products let you access your network from virtually anywhere you want, however, the positioning of the products within your environment will affect its wireless range.

Why does my wireless connection keep dropping?

- If you are using 2.4 GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, or lights, your wireless connection will degrade dramatically or even drop. Try changing the channel of your router, access point and wireless adapter to a different channel to avoid interference.
- Keep your product away - at least 3-6 feet - from electrical devices that generate RF noise like microwaves, monitors, electric motors, etc.

Why can't I get a wireless connection?

If you have enabled encryption on the DAP-3666, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- Make sure that the SSID on the AP and the wireless client are exactly the same. If they are not, wireless connection cannot be established.
- Move the DAP-3666 and the wireless client into the same room and then test the wireless connection.
- Disable all security settings.
- Power off your DAP-3666 and the client. Turn the DAP-3666 back on again, and then turn on the client.
- Make sure that all devices are set to Infrastructure mode.
- Check that the LED indicators are indicating normal activity. If not, check that the AC power and Ethernet cables are firmly connected.
- Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network.
- If you are using 2.4 GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection will degrade dramatically or drop altogether. Try changing the channel on your DAP-3666, and on all the devices in your network to avoid interference.
- Keep your product away - at least 3-6 feet - from electrical devices that generate RF noise like microwaves, monitors, electric motors, etc.

What should I do if I forget 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 bottom 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. Make sure the AP is connected to the DHCP server and obtain the address as set for the network. By the default, the AP's LAN settings are configured to DHCP. In the event that the DHCP server does not provide an IP address, type either of the following in the web browser's address bar to access the AP: 192.168.0.50 or dap3666.local.

How do I check my IP address?

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

1. Click on **Start > Run**. In the run box type `cmd` and click **OK**.
2. At the prompt, type `ipconfig` and press **Enter**.

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

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

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



```

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

C:\Documents and Settings\jagcon01>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

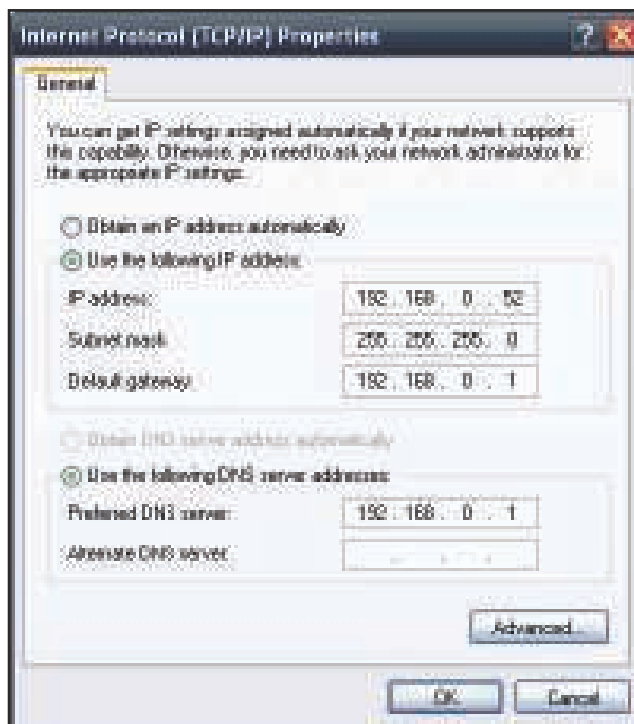
   Connection-specific DNS Suffix . : 
   IP Address . . . . . : 10.5.7.104
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings\jagcon01>
  
```

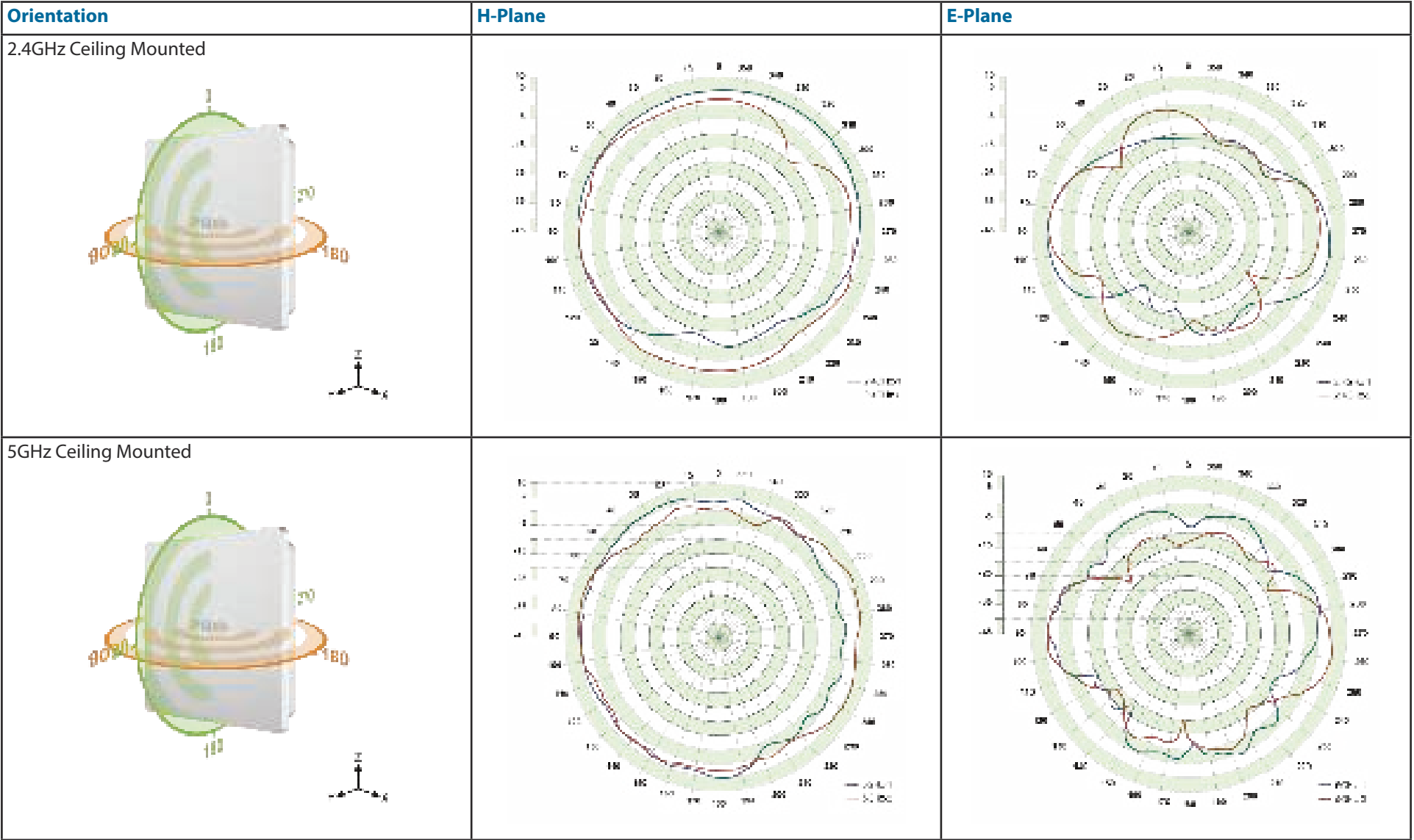
How do I assign a static IP address?

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

1. Windows 10®: Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.
4. Highlight **Internet Protocol (TCP/(IPv4/IPv6))** and click **Properties**.
5. 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.
6. Click **OK** twice to save your settings.



Antenna Pattern



Technical Specifications

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

- Network Management**
- Web Browser interface (HTTP, Secure HTTP [HTTPS])
 - Nuclias Connect APP
 - Command Line Interface (Telnet, Secure SSH Telnet)

- Security**
- WPA™ Personal/Enterprise
 - WPA2™ Personal/Enterprise
 - WEP™ 64-/128-bit
 - SSID Broadcast Disable
 - MAC Address Access Control

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

Operating Voltage 56V/0.54A Power Adapter or 802.3af PoE

- Antenna Type**
- Two embedded 6 dBi gain @ 2.4 GHz
 - Two embedded 7 dBi gain @ 5 GHz

- LEDs**
- Power
 - Status

- Temperature**
- Operating: -30 to 60 °C (-22 to 140 °F)
 - Storing: -30 to 65 °C (-22 to 149 °F)

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

- Certifications**
- FCC
 - IC
 - CE
 - C-Tick
 - UL
 - IP68

Dimensions (L x W x H) 277 x 240 x 50 mm (10.91" x 9.45" x 1.97")

* Please note that operating frequency ranges vary depending on the regulations of individual countries and jurisdictions. The DAP-3666 isn't supported in the 5.25~5.35 GHz and 5.47 ~ 5.725 GHz frequency ranges in some regions.

Federal Communication Commission Interference Statement

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

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

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

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

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 23 cm between the radiator & your body.

FCC NOTICE: To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

IC Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

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

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.

Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Dynamic Frequency Selection (DFS) for devices operating in the bands 5250- 5350 MHz, 5470-5600 MHz and 5650-5725 MHz.

Sélection dynamique de fréquences (DFS) pour les dispositifs fonctionnant dans les bandes 5250-5350 MHz, 5470-5600 MHz et 5650-5725 MHz.

The maximum antenna gain permitted (for devices in the bands 5250-5350 MHz and 5470-5725 MHz) to comply with the e.i.r.p.

limit. le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5470-5725 MHz doit se conformer à la limite de p.i.r.e.

Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

IMPORTANT NOTE:**IC Radiation Exposure Statement:**

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 23 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 23 cm de distance entre la source de rayonnement et votre corps.

This radio transmitter (Model: DAP-3666A1) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (Model: DAP-3666A1) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Antenna list:

Ant.	Brand	P/N	Antenna Type	Connector	Gain (dBi)	
					2.4GHz	5GHz
1	Grand-Tek	OA-58-06-03	Embedded Antenna	I-PEX	-	7.4
2	Grand-Tek	OA-58-05-02	Embedded Antenna	I-PEX	-	5.8
3	Grand-Tek	OA-24-05-06	Embedded Antenna	I-PEX	6.2	-
4	Grand-Tek	OA-24-04-02	Embedded Antenna	I-PEX	3.7	-

Note: The EUT has four antennas.

NCC警語:

- (1) 「經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得自變更頻率、加大功率或變更原設計之特性及功能」。
- (2) 「低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依 電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾」。
- (3) 「不致造成違反低功率電波輻射性電機管理辦法之所有控制、調整及開關之使用方法」。
- (4) 「對任何可能造成違反管理辦法規定之調整予以警告，或建議由具有發射機維修專長之技術人員執行或由其直接監督及負責」。
- (5) 「對任何可能造成違反管理辦法之零件(晶體、半導體等)置換之警告」。
- (6) 「電磁波曝露量MPE標準值 $1\text{mW}/\text{cm}^2$ ，本產品使用時建議應距離人體：23 cm」。