

DAP-2620

Version 1.00

**Wireless AC1200
Wave 2 Dual-Band wall-plate PoE AP**

User Manual

Business Class Networking

Package Contents

- DAP-2620 Access Point
- Mounting Plate and Hardware

Note: *Using a power supply with a different voltage rating than the one included with the DAP-2620 will cause damage and void the warranty for this product.*

System Requirements

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

Basic Installation

Hardware Setup

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

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

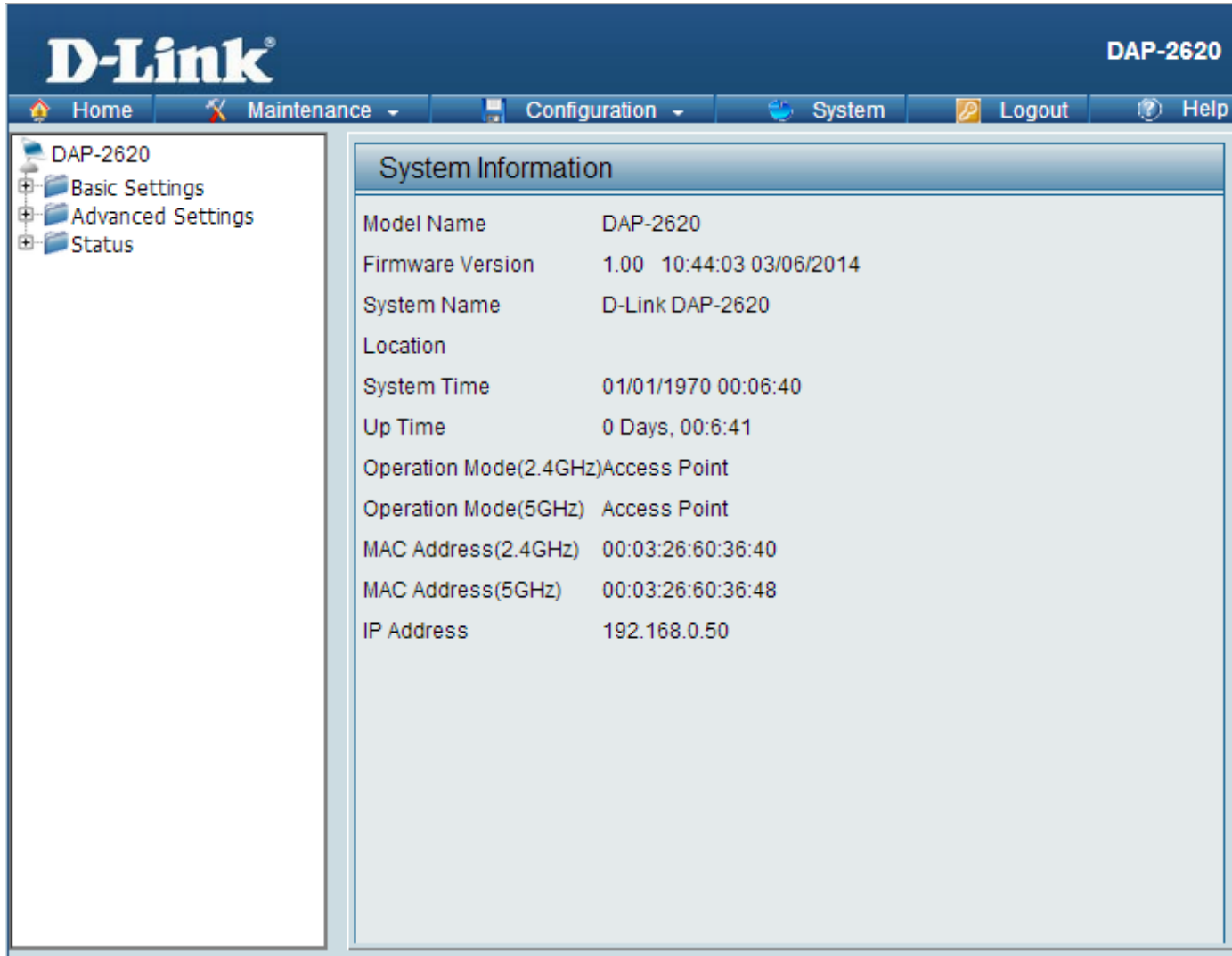
Method 1 - PoE with PoE Switch or Router

1. Connect one end of your Ethernet cable to the LAN (PoE) port on the access point.
2. Connect the other end into one port on a PoE switch or router.



Web User Interface

The DAP-2620 supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type the IP address of the access point (Default setting is <http://192.168.0.50> or <https://192.168.0.50>) and then press Enter to login. Most of the configurable settings are located in the left menu of the web GUI which contains section called **Basic Settings**, **Advanced Settings** and **Status**.



The screenshot displays the web user interface for the D-Link DAP-2620. The interface features a dark blue header with the D-Link logo on the left and the device model 'DAP-2620' on the right. Below the header is a navigation bar with buttons for Home, Maintenance, Configuration, System, Logout, and Help. A left-hand menu shows a tree view with 'DAP-2620' expanded, containing sub-items for Basic Settings, Advanced Settings, and Status. The main content area is titled 'System Information' and displays the following details:

Model Name	DAP-2620
Firmware Version	1.00 10:44:03 03/06/2014
System Name	D-Link DAP-2620
Location	
System Time	01/01/1970 00:06:40
Up Time	0 Days, 00:6:41
Operation Mode(2.4GHz)	Access Point
Operation Mode(5GHz)	Access Point
MAC Address(2.4GHz)	00:03:26:60:36:40
MAC Address(5GHz)	00:03:26:60:36:48
IP Address	192.168.0.50

Wireless

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

Access Point - Used to create a wireless LAN

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

WDS - Used to connect multiple wireless networks

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

Access Point Mode

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

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

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

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

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



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

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

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

Authentication: Use the drop-down menu to choose **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, or **802.1x**.

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

WDS with AP Mode

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

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

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

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

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

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

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

The screenshot displays the 'Wireless Settings' page for a D-Link DAP-2620 device. The interface includes a navigation menu on the left with options like 'Basic Settings', 'Wireless', 'LAN', 'IPv6', 'Advanced Settings', and 'Status'. The main content area is titled 'Wireless Settings' and contains the following configuration options:

- Wireless Band:** 2.4GHz
- Mode:** WDS with AP
- Network Name (SSID):** dlink
- SSID Visibility:** Enable
- Auto Channel Selection:** Disable
- Channel:** 1
- Channel Width:** 20 MHz
- WDS Remote AP MAC Address:** Fields 1 through 8.
- Site Survey:** A 'Scan' button.
- Table:** A table with columns: CH, RSSI, BSSID, Security, SSID.
- Authentication:** Open System
- Key Settings:** Radio buttons for 'Disable' (selected) and 'Enable'.
- Key Type:** HEX
- Key Size:** 64 Bits
- Key Index (1-4):** 1
- Network Key:** [Empty text field]
- Confirm Key:** [Empty text field]

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

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

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

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

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

WDS Mode

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

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

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

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

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

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

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

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

The screenshot displays the 'Wireless Settings' page for a D-Link DAP-2620 device. The interface includes a navigation menu on the left with options like 'Basic Settings', 'Wireless', 'LAN', 'IPv6', 'Advanced Settings', and 'Status'. The main content area is titled 'Wireless Settings' and contains the following configuration options:

- Wireless Band:** 2.4GHz
- Mode:** WDS
- Network Name (SSID):** dlink
- SSID Visibility:** Enable
- Auto Channel Selection:** Disable
- Channel:** 1
- Channel Width:** 20 Mhz
- WDS Remote AP MAC Address:** Eight input fields labeled 1 through 8.
- Site Survey:** A table with columns for CH, RSSI, BSSID, Security, and SSID, and a Scan button.
- Authentication:** Open System
- Key Settings:** Disable (selected)
- Encryption:** Disable
- Key Type:** HEX
- Key Size:** 64 bits
- Key Index(1~4):** 1
- Network Key:** Input field
- Confirm Key:** Input field

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

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

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

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

Wireless Client Mode

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

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

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

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

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

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

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

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

Authentication: Will be explained in the next topic.

The screenshot displays the D-Link DAP-2620 web interface. The main configuration area is titled "Wireless Settings". Key settings include:

- Wireless Band:** 2.4GHz
- Mode:** Wireless Client
- Network Name (SSID):** dlink
- SSID Visibility:** Enable
- Auto Channel Selection:** Enable
- Channel:** 1
- Channel Width:** Auto 20/40 MHz

A "Site Survey" section contains a "Scan" button. Below it is a table for survey results:

CH	RSSI	BSSID	Security	SSID

The "Authentication" section is set to "Open System". Under "Key Settings":

- Encryption:** Disable (selected)
- Key Type:** HEX
- Key Size:** 64 Bits
- Key Index:** 1
- Network Key:** [Empty field]
- Confirm Key:** [Empty field]

The "Wireless MAC Clone" section has "Enable" checked, "MAC Source" set to "Auto", and "MAC Address" fields with a "Scan" button. A "Save" button is located at the bottom right of the page.

Wireless Security

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

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

Wired Equivalent Privacy (WEP)

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

Open System will send a request to the access point and if the key used matches the one configured on the access point, the access point will return a success message back to the wireless client. If the key does not match the one configured on the access point, the access point will deny the connection request from the wireless client.

Shared Key will send a request to the access point and if the key used matches the one configured on the access point, the access point will send a challenge to the client. The client will then again send a confirmation of the same key back to the access point where the access point will either return a successful or a denial packet back to the wireless client.

Encryption: Use the radio button to disable or enable encryption.

Key Type*: Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

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

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



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

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

Wi-Fi Protected Access (WPA / WPA2)

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

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

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

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

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

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

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

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

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

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

- Wireless Band: 2.4GHz
- Mode: Access Point
- Network Name (SSID): dlink
- SSID Visibility: Enable
- Auto Channel Selection: Enable
- Channel: 1
- Channel Width: 20 MHz
- Authentication: WPA-Personal
- PassPhrase Settings:
 - WPA Mode: AUTO (WPA or WPA2)
 - Cipher Type: Auto
 - Group Key Update Interval: 3600 (Seconds)
 - Manual (selected) / Periodical Key Change
 - Activated From: Sun : 00 : 00
 - Time Interval: 1 (1~168)hour(s)
 - PassPhrase: [Empty field]
 - Confirm PassPhrase: [Empty field]

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

Save

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

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

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

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

RADIUS Server: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

Account Server: Enter the IP address of the Account Server

Account Port: Enter the Account port

Account Secret: Enter the Account secret

The screenshot displays the D-Link DAP-2620 configuration interface. The 'Wireless Settings' section is active, showing various configuration options. The 'Wireless Band' is set to 2.4GHz, and the 'Mode' is set to Access Point. The 'Network Name (SSID)' is 'dlink', and 'SSID Visibility' is 'Enable'. 'Auto Channel Selection' is also 'Enable'. The 'Channel' is set to 1, and 'Channel Width' is 20 MHz. 'Authentication' is set to WPA-Enterprise. Under 'RADIUS Server Settings', 'WPA Mode' is 'AUTO (WPA or WPA2)' and 'Cipher Type' is 'Auto'. The 'Group Key Update Interval' is set to 1800 seconds. Below this, there are sections for 'Network Access Protection' (set to Disable), 'RADIUS Server Mode' (set to External), and 'Primary RADIUS Server Setting' (with fields for RADIUS Server, RADIUS Port: 1812, and RADIUS Secret). There are also optional sections for 'Backup RADIUS Server Setting' and 'Primary Accounting Server Setting' (with fields for Accounting Mode: Disable, Accounting Server, Accounting Port: 1813, and Accounting Secret). A 'Save' button is located at the bottom right of the configuration area.

LAN

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DAP-2620. These settings may be referred to as private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

Get IP From: **Static IP (Manual)** is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2620. When **Dynamic IP (DHCP)** is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

The screenshot shows the 'LAN Settings' configuration window. It features a title bar 'LAN Settings' and a light blue background. The settings are as follows:

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

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

IPv6

Enable IPv6: Check to enable the IPv6

Get IP From: Auto is chosen here. Choose this option the DAP-2620 can get IPv6 address automatically or use Static to set IPv6 address manually. When Auto is selected, the other fields here will be grayed out.

IP Address: Enter the LAN IPv6 address used here.

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

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

The screenshot shows the 'IPv6 Settings' window. At the top, there is a title bar. Below it, the 'Enable IPv6' checkbox is checked. The 'Get IP From' dropdown menu is open, showing 'Auto' (selected), 'Static', and 'Auto'. Below the dropdown are input fields for 'IP Address', 'Prefix', and 'Default Gateway', all of which are grayed out. A 'Save' button is located in the bottom right corner.

Advanced Settings

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

The screenshot displays the D-Link DAP-2620 web management interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view of settings categories: Basic Settings, Advanced Settings (expanded), Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, AP Array, Captive Portal, DHCP Server, Filters, Traffic Control, and Status. The main content area is titled 'Performance Settings' and contains the following configuration options:

Setting	Value
Wireless band	5GHz
Wireless	Off
Wireless Mode	Mixed 802.11ac
Data Rate	Best(Up to 867) (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out (5GHz, 25~200)	25 (μs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable (Mbps)
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Disable
Transfer DHCP Offer to Unicast	Disable

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

Performance

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

Wireless Band: Select either 2.4GHz or 5GHz.

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

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

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

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

DTM Interval (1-15): Select a Delivery Traffic Indication Message setting between 1 and 15. 1 is the default setting. DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Performance Settings	
Wireless band	5GHz
Wireless	Off
Wireless Mode	Mixed 802.11ac
Data Rate	Best(Up to 867) (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out (5GHz, 25~200)	25 (μs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable (Mbps)
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Disable
Transfer DHCP Offer to Unicast	Disable

Save

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

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

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

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

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

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

Multicast Bandwidth Control : Adjust the multicast packet data rate here. The multicast rate is supported in AP mode, 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.

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

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

Wireless Resource Control

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

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

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

Band Steering Age: Enter the time in seconds to specify the interval of updating information.

Band Steering Difference: The 5G preferred difference value is equal to the number of 5GHz wireless client connections minus the number of 2.4GHz wireless client connections. If the number of 5GHz wireless client connections minus the number of 2.4GHz wireless client connections exceed this value, the extra 5GHz wireless client connections will be forced to connect to the 2.4GHz band and not the 5GHz band.

Band Steering Refuse Number: Enter the maximum 5G connection attempts allowed before the 5G preferred function will be disabled for the wireless station connection.

Connection Limit: Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled and when the number of users exceeds this value, or the network utilization of this AP exceeds the percentage that has been specified, the DAP-2620 will not allow clients to associate with the AP.

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

Wireless Resource Control	
Wireless band	2.4GHz ▾
Band Steering	Disable ▾
Band Steering Age	180 (s)
Band Steering Difference	2
Band Steering Refuse Number	3
Connection Limit	Disable ▾
User Limit (0 - 64)	20
11n Preferred	Disable ▾
Network Utilization	100% ▾
Aging out	Disable ▾
RSSI Threshold	100% ▾
Data Rate Threshold	54 ▾
ACL RSSI	Disable ▾
ACL RSSI Threshold	60% ▾

Save

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

Network Utilization: Set the maximum utilization of this access point for service. The DAP-2620 will not allow any new clients to associate with the AP if the utilization exceeds the value the user specifies. Select a utilization percentage between 100%, 80%, 60%, 40%, 20%, or 0%. When this network utilization threshold is reached, the device will pause one minute to allow network congestion to dissipate.

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

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

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

ACL RSSI: Use the drop-down menu to **Enable** the function. When enabled, the device denies the connection request from the wireless clients with the RSSI lower than the specified threshold below.

ACL RSSI Threshold: Set the ACL RSSI Threshold.

Multi-SSID

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

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

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

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

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

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

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

Priority: Select the priority level of the SSID selected.

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



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

Key Type: Select HEX or ASCII.

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

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

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

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

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

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

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

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

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

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

VLAN

VLAN List

The DAP-2620 supports VLANs. VLANs can be created with a Name and VID. Mgmt (TCP stack), LAN, Primary/Multiple SSID, and WDS connection can be assigned to VLANs as they are physical ports. Any packet which enters the DAP-2620 without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

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

VLAN Mode: The current VLAN mode is displayed.

VLAN Settings

VLAN Status : Disable Enable Save

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

VLAN List				
VID	VLAN Name	Untag VLAN Ports	Tag VLAN Ports	Edit Delete
1	default	Mgmt, LAN, Primary(2.4G), S-1(2.4G), S-2(2.4G), S-3(2.4G), S-4(2.4G), S-5(2.4G), S-6(2.4G), S-7(2.4G), W-1(2.4G), W-2(2.4G), W-3(2.4G), W-4(2.4G), W-5(2.4G), W-6(2.4G), W-7(2.4G), W-8(2.4G), Primary(5G), S-1(5G), S-2(5G), S-3(5G), S-4(5G), S-5(5G), S-6(5G), S-7(5G), W-1(5G), W-2(5G), W-3(5G), W-4(5G), W-5(5G), W-6(5G), W-7(5G), W-8(5G)		

Port List

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

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

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

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

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

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

VLAN Settings			
VLAN Status : <input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="button" value="Save"/>			
VLAN Mode : Static(2.4G), Static(5G)			
<input type="button" value="VLAN List"/>	<input checked="" type="button" value="Port List"/>	<input type="button" value="Add/Edit VLAN"/>	<input type="button" value="PVID Setting"/>
Port Name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN		1	1
Primary(2.4G)		1	1
Primary(5G)		1	1
S-1(2.4G)		1	1
S-2(2.4G)		1	1
S-3(2.4G)		1	1
S-4(2.4G)		1	1
S-5(2.4G)		1	1
S-6(2.4G)		1	1
S-7(2.4G)		1	1
W-1(2.4G)		1	1
W-2(2.4G)		1	1
W-3(2.4G)		1	1
W-4(2.4G)		1	1
W-5(2.4G)		1	1
W-6(2.4G)		1	1
W-7(2.4G)		1	1
W-8(2.4G)		1	1
S-1(5G)		1	1
S-2(5G)		1	1
S-3(5G)		1	1
S-4(5G)		1	1
S-5(5G)		1	1
S-6(5G)		1	1
S-7(5G)		1	1
W-1(5G)		1	1
W-2(5G)		1	1
W-3(5G)		1	1
W-4(5G)		1	1
W-5(5G)		1	1
W-6(5G)		1	1
W-7(5G)		1	1
W-8(5G)		1	1

Add/Edit VLAN

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

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

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

VLAN Name: Enter the VLAN to add or modify.

VLAN Settings

VLAN Status : Disable Enable Save

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

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

VLAN ID (VID) VLAN Name

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

2.4GHz

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

WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5GHz

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

WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save

PVID Settings

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

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

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

VLAN Settings

VLAN Status : Disable Enable Save

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

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

PVID Auto Assign Status Disable Enable

Port	Mgmt	LAN
PVID	1	1

2.4GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1
WDS Port	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
PVID	1	1	1	1	1	1	1	1

5GHz

MSSID Port	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
PVID	1	1	1	1	1	1	1	1
WDS Port	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
PVID	1	1	1	1	1	1	1	1

Save

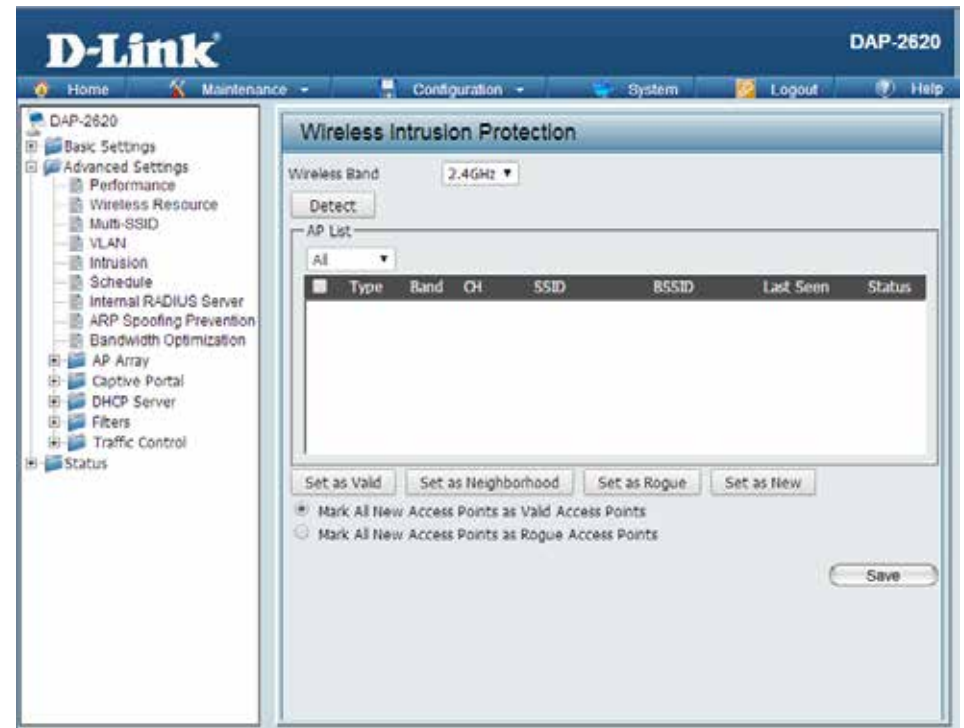
Intrusion

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

Wireless Band: Select 2.4GHz or 5GHz.

AP List: The choices include All, Valid, Neighbor, Rogue, and New.

Detect: Click this button to initiate a scan of the network.



Schedule

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

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

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

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

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

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

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

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

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

The screenshot displays the D-Link DAP-2620 configuration interface. The left sidebar shows a tree view with 'Schedule' selected under 'Advanced Settings'. The main content area is titled 'Wireless Schedule Settings'. At the top, there's a 'Wireless Schedule' dropdown menu currently set to 'Disable'. Below this is the 'Add Schedule Rule' section, which includes a 'Name' text input field, an 'Index' dropdown menu showing 'Primary SSID 2.4G', and an 'SSID' text input field containing 'dlink'. There are two radio button options: 'All Week' (unselected) and 'Select Day(s)' (selected). Under 'Select Day(s)', there are checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. Below these are an 'All Day(s)' checkbox, 'Start Time' and 'End Time' fields (each with hour and minute inputs and a '(hour:minute, 24 hour time)' label), and an 'Overnight' checkbox. 'Add' and 'Clear' buttons are located below the time fields. A 'Schedule Rule List' table is present below, with columns: Name, SSID Index, SSID, Day(s), Time Frame, Wireless Edit, and DEL. The table is currently empty. At the bottom right of the main panel is a 'Save' button. A note at the bottom of the table area reads '+: To the end time of the next day overnight.'

Internal RADIUS Server


The DAP-2620 features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the Save button to let your changes take effect. The newly-created account will appear in this RADIUS Account List. The radio buttons allow the user to enable or disable the RADIUS account. Click the icon in the delete column to remove the RADIUS account. We suggest you limit the number of accounts below 30.

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

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

Status: Toggle the drop-down menu between Enable and Disable.

RADIUS Account List: Displays the list of users.



The screenshot displays the D-Link DAP-2620 web management interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view of configuration options, with 'Internal RADIUS Server' selected under 'Advanced Settings'. The main content area is titled 'Internal RADIUS Server' and contains two sections: 'Add RADIUS Account' and 'RADIUS Account list'. The 'Add RADIUS Account' section has input fields for 'User Name' and 'Password', and a 'Status' dropdown menu set to 'Enable'. The 'RADIUS Account list' section is currently empty, with a table header showing columns for 'User Name', 'Enable', 'Disable', and 'Delete'. A 'Save' button is located at the bottom right of the configuration area.

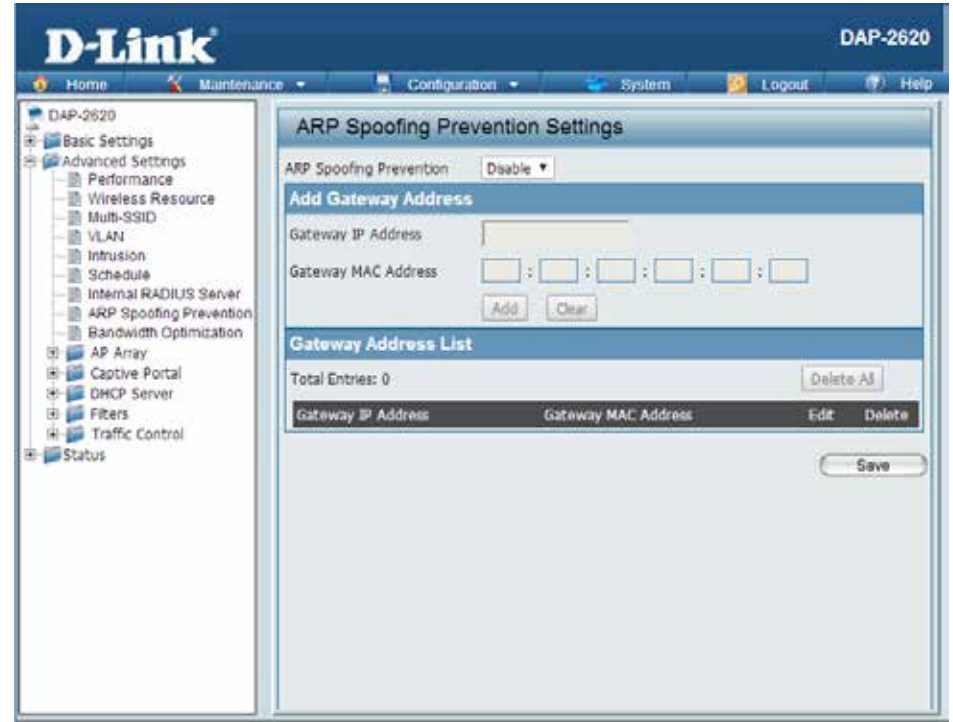
ARP Spoofing Prevention

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

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

Gateway IP Address: Enter a gateway IP address.

Gateway MAC Address: Enter a gateway MAC address.



Bandwidth Optimization

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

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

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

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

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

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

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

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

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

Bandwidth Optimization

Enable Bandwidth Optimization Enable

Downlink Bandwidth Mbits/sec

Uplink Bandwidth Mbits/sec

Add Bandwidth Optimization Rule

Rule Type Allocate average BW for each station

Band 2.4 GHz

SSID Index Primary SSID

Downlink Speed Kbits/sec

Uplink Speed Kbits/sec

Bandwidth Optimization Rules

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Del

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

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

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

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

AP Array

AP Array Scan

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

Enable AP Array: Select the check box to enable the AP array function. The three modes that are available are **Master**, **Backup Master**, and **Slave**. APs in the same array will use the same configuration. The configuration will sync the Master AP to the Slave AP and the Backup Master AP when a Slave AP and a Backup Master AP join the AP array.

AP Array Name: Enter an AP array name for the group here.

AP Array Password: Enter an AP array password for the group here. This password must be the same on all the APs in the group.

Scan AP Array List: Click this button to initiate a scan of all the available APs currently on the network.

Connection Status: Display the AP array connection status.

AP Array List: This table displays the current AP array status for the following parameters: Array Name, Master IP, MAC, Master, Backup Master, Slave, and Total.

Current Members: This table displays all the current array members. The DAP-2620 AP array feature supports up to eight AP array members.

The screenshot shows the D-Link DAP-2620 web interface. The main content area is titled "AP Array Scan". It features a checkbox for "Enable AP Array" (Version 2.0) and three radio buttons for "Master", "Backup Master", and "Slave". Below these are input fields for "AP Array Name" and "AP Array Password", and a "Scan" button. The "Connection Status" is displayed as "Disconnect".

The "AP Array List" table is currently empty. Below it is the "Current Members" table, which is also empty. A "Save" button is located at the bottom right of the page.

Array Name	Master IP	MAC	Master	Backup Master	Slave	Total

Current Members				
Index	Role	IP Address	MAC Address	Location

Configuration Settings

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

- Enable AP Array Configuration:** Select to **Enable** or **Disable** the AP array configuration feature here.
- Wireless Basic Settings:** Select this option to specify the basic wireless settings that the APs in the group will inherit.
- Wireless Advanced Settings:** Select this option to specify the advanced wireless settings that the APs in the group will inherit.
- Multiple SSID & VLAN:** Select this option to specify the multiple SSIDs and VLAN settings that the APs in the group will inherit.
- Advanced Functions:** Select this option to specify the other advanced settings that the APs in the group will inherit.
- Administration Settings:** Select this option to specify the administrative settings that the APs in the group will inherit.

The screenshot shows the 'AP Array Configuration' window. At the top, there is a title bar. Below it, the 'Enable AP Array Configuration' section has a dropdown menu set to 'Enable' and a 'Clear all' button. The main area contains five expandable sections, each with a checkbox: 'Wireless Basic Settings', 'Wireless Advanced Settings', 'Multiple SSID & VLAN', 'Advanced Functions', and 'Administration Settings'. A 'Save' button is located at the bottom right of the window.

Wireless Basic Settings

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

SSID Visibility: Select this option to enable SSID visibility.

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

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

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

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

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

Wireless Basic Settings <input checked="" type="checkbox"/>			
Network Name (SSID)	<input checked="" type="checkbox"/>	SSID Visibility	<input checked="" type="checkbox"/>
Auto Channel Selection	<input checked="" type="checkbox"/>	Channel Width	<input checked="" type="checkbox"/>
Security	<input checked="" type="checkbox"/>	Captive Profile	<input checked="" type="checkbox"/>
Band	<input checked="" type="checkbox"/>		

Wireless Advanced Settings

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

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

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

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

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

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

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

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

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

Wireless Advanced Settings <input checked="" type="checkbox"/>			
Wireless	<input checked="" type="checkbox"/>	Wireless Mode	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="checkbox"/>	Beacon Interval	<input checked="" type="checkbox"/>
DTIM Interval	<input checked="" type="checkbox"/>	Transmit Power	<input checked="" type="checkbox"/>
WMM (Wi-Fi Multimedia)	<input checked="" type="checkbox"/>	Ack Time Out	<input checked="" type="checkbox"/>
Wireless ACL	<input checked="" type="checkbox"/>	Short GI	<input checked="" type="checkbox"/>
Link Integrity	<input checked="" type="checkbox"/>	Connection Limit	<input checked="" type="checkbox"/>
IGMP Snooping	<input checked="" type="checkbox"/>		

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

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

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

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

Multiple SSID & VLAN

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

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

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

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

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

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

Multiple SSID & VLAN <input checked="" type="checkbox"/>			
SSID	<input checked="" type="checkbox"/>	SSID Visibility	<input checked="" type="checkbox"/>
Security	<input checked="" type="checkbox"/>	WMM	<input checked="" type="checkbox"/>
Captive Profile	<input checked="" type="checkbox"/>	VLAN	<input checked="" type="checkbox"/>

Advanced Functions

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

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

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

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

Advanced Functions <input checked="" type="checkbox"/>			
Schedule Settings	<input checked="" type="checkbox"/>	QoS Settings	<input checked="" type="checkbox"/>
Log Settings	<input checked="" type="checkbox"/>	Time and Date Settings	<input checked="" type="checkbox"/>
ARP Spoofing Prevention	<input checked="" type="checkbox"/>	Bandwidth Optimization	<input checked="" type="checkbox"/>
Captive Portal	<input checked="" type="checkbox"/>	Auto RF	<input checked="" type="checkbox"/>
Load Balance	<input checked="" type="checkbox"/>	DHCP server Settings	<input checked="" type="checkbox"/>

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

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

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

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

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

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

Administration Settings

System Name Settings: Select this option to use the same system name.

SNMP Settings: Select this option to use the same SNMP settings.

Login Settings: Select this option to use the same login settings.

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

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

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

Administration Settings <input checked="" type="checkbox"/>			
System Name Settings	<input checked="" type="checkbox"/>	SNMP Settings	<input checked="" type="checkbox"/>
Login Settings	<input checked="" type="checkbox"/>	Console Settings	<input checked="" type="checkbox"/>
Limit Administrator	<input checked="" type="checkbox"/>	Ping Control Setting	<input checked="" type="checkbox"/>

Auto-RF

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

Enable: Auto-RF: Select to **Enable** or **Disable** the auto-RF feature here.

Initiate Auto-RF: Click the **Auto-RF Optimize** button to initiate the auto-RF optimization feature.

Auto-Initiate: Select the **Enable** or **Disable** the auto-initiate feature here.

Auto-Initiate Period: After enabling the auto-initiate option, the auto-initiate period value can be entered here. This value must be between 1 and 24 hours.

RSSI Threshold: Select the RSSI threshold value here. This value is listed in the drop-down menu in increments of 10% from **10%** to **100%**.

RF Report Frequency: Enter the RF report frequency value here.

The screenshot shows the 'Auto-RF' configuration window with the following settings:

Setting	Value
Enable Auto-RF	Disable
Initiate Auto-RF	Auto-RF Optimize
Auto-Initiate	Disable
Auto-Initiate Period	24 (hours)
RSSI Threshold	40%
RF Report Frequency	10 (Seconds)

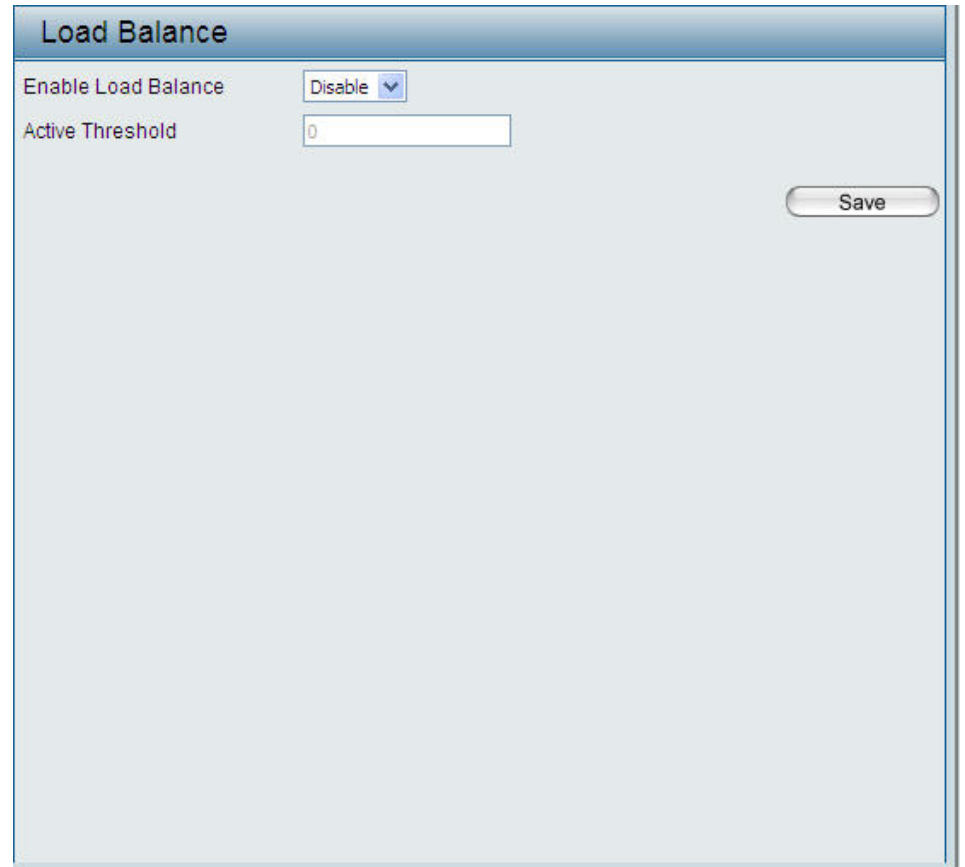
A 'Save' button is located at the bottom right of the window.

Load Balance

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

Enable Load Balance: Select to **Enable** or **Disable** the load balance feature here.

Active Threshold: Enter the active threshold value here.



The screenshot shows a configuration window titled "Load Balance". It contains two main settings: "Enable Load Balance" with a dropdown menu currently set to "Disable", and "Active Threshold" with a text input field containing the value "0". A "Save" button is located in the bottom right corner of the window.

Captive Portal

Authentication Settings-Web Redirection Only

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

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2620. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

Authentication Settings- Username/Password

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

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2620. When Dynamic

The screenshot displays the D-Link DAP-2620 web interface. The left sidebar shows a navigation tree with 'Captive Portal' expanded to 'Authentication Settings'. The main content area is titled 'Captive Portal Authentication' and contains the following settings:

- Session Timeout (1-1440):** 60 Minute(s)
- Band:** 2.4GHz
- SSID Index:** Primary SSID
- Authentication Type:** Username/Password
- Web Redirection Interface Settings:** Web Redirection State is set to Disable. URL Path is http://.
- IP Interface Settings:** IPIF Status is Disable. VLAN Group is empty. Get IP From is Static IP(Manual). IP Address, Subnet Mask, Gateway, and DNS fields are empty.
- Username/Password Settings:** Username and Password fields are empty. Add and Clear buttons are present.

Below the settings are two tables for managing authentication profiles:

Username	Edit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Authentication Settings- Passcode

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

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2620. When Dynamic IP (DHCP) is selected, the other fields here will be

grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

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

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

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

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

Authentication Settings- Remote RADIUS

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

Session timeout(1-1440): Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band: Select 2.4GHz or 5GHz.

SSID Index: Select the SSID for this Authentication.

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

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

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

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

VLAN Group: Enter the VLAN Group ID here

Get IP From: Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2620. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

The screenshot displays the 'Captive Portal Authentication' configuration page for a D-Link DAP-2620 device. The interface includes a navigation menu on the left and a main configuration area on the right. The configuration area is divided into several sections: 'Session Timeout (1-1440)' (60 Minute(s)), 'Band' (2.4GHz), 'SSID Index' (Primary SSID), 'Authentication Type' (Remote RADIUS), 'Web Redirection Interface Settings' (Web Redirection State: Disable, URL Path: http://), 'IP Interface Settings' (IPIF Status: Disable, VLAN Group: , Get IP From: Static IP(Manual), IP Address: , Subnet Mask: , Gateway: , DNS:), 'Remote RADIUS Settings', 'Radius Server Settings' (Radius Server: , Radius Port: 1812, Radius Secret: , Remote RADIUS Type: SPAP), 'Secondary radius Server Settings' (Radius Server: , Radius Port: 1812, Radius Secret: , Remote RADIUS Type: SPAP), and 'Third radius Server Settings' (Radius Server: , Radius Port: 1812, Radius Secret: , Remote RADIUS Type: SPAP). A 'Save' button is located at the bottom right of the configuration area. Below the configuration area, there is a table with columns: Band, SSID Index, Captive Profile, Edit, and Delete.

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 here

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

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

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

Authentication Settings- LDAP

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

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2620. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

The screenshot displays the D-Link DAP-2620 web interface. The left sidebar shows a navigation tree with 'Captive Portal' expanded to 'Authentication Settings'. The main content area is titled 'Captive Portal Authentication' and contains the following settings:

- Session Timeout (1-1440)**: 60 Minute(s)
- Band**: 2.4GHz
- SSID Index**: Primary SSID
- Authentication Type**: LDAP
- Web Redirection Interface Settings**:
 - Web Redirection State**: Disable
 - URL Path**: http://
- IP Interface Settings**:
 - IPIF Status**: Disable
 - VLAN Group**: (empty)
 - Get IP From**: Static IP(Manual)
 - IP Address**: (empty)
 - Subnet Mask**: (empty)
 - Gateway**: (empty)
 - DNS**: (empty)
- LDAP Settings**:
 - Server**: (empty)
 - Port**: 389
 - Authenticate Mode**: Simple
 - Username**: (empty)
 - Password**: (empty)
 - Base DN**: (empty) (ou=,dc=)
 - Account Attribute**: (empty) (ex.cn)
 - Identity**: (empty) Auto Copy

A 'Save' button is located at the bottom right of the settings area. Below the settings is a table with columns: Band, SSID Index, Captive Profile, Edit, and Delete.

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

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

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

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

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

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

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

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

Base DN: Enter the administrator's domain name here

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

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

Authentication Settings- POP3

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

Session timeout(1-1440) : Enter the session timeout value here. This value can be from 1 to 1440 minutes. By default, this value is 60 minutes.

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DAP-2620. When Dynamic IP

The screenshot displays the 'Captive Portal Authentication' configuration page for a D-Link DAP-2620 device. The interface includes a navigation menu on the left and a main configuration area on the right. The configuration area is divided into several sections: 'Session Timeout (1-1440)' with a value of 60 minutes; 'Band' set to 2.4GHz; 'SSID Index' set to Primary SSID; 'Authentication Type' set to POP3; 'Web Redirection Interface Settings' with 'Web Redirection State' set to Disable and 'URL Path' set to http://; 'IP Interface Settings' with 'IPIF Status' set to Disable, 'VLAN Group' empty, 'Get IP From' set to Static IP(Manual), and 'IP Address', 'Subnet Mask', and 'Gateway' fields empty; 'DNS' field empty; 'POP3 Settings' with 'Server' field empty, 'Port' set to 110, and 'Connection Type' set to None. A 'Save' button is located at the bottom right of the configuration area. Below the configuration area is a table with columns: Band, SSID Index, Captive Profile, Edit, and Delete.

Band	SSID Index	Captive Profile	Edit	Delete

(DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

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

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

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

Login Page Upload

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

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

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

The screenshot shows the D-Link DAP-2620 web interface. The main content area is titled "Login Page Upload". It features a section for "Upload Login Style From Local Hard Drive" with a text input field for the file path, a "Browse..." button, and an "Upload" button. Below this, it shows "The Left space" as 457216 Byte(s). There is also a "Login Page Style List" section with a "Wireless Band" dropdown menu set to "5GHz".

ID	Style Name	Pri	S-1	S-2	S-3	S-4	S-5	S-6	S-7	Download	Del
1	pages_default.tar	●	●	●	●	●	●	●	●	Download	Del
2	pages_headerpic.tar	●	●	●	●	●	●	●	●	Download	Del
3	pages_license.tar	●	●	●	●	●	●	●	●	Download	Del

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

IP Filter Settings

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

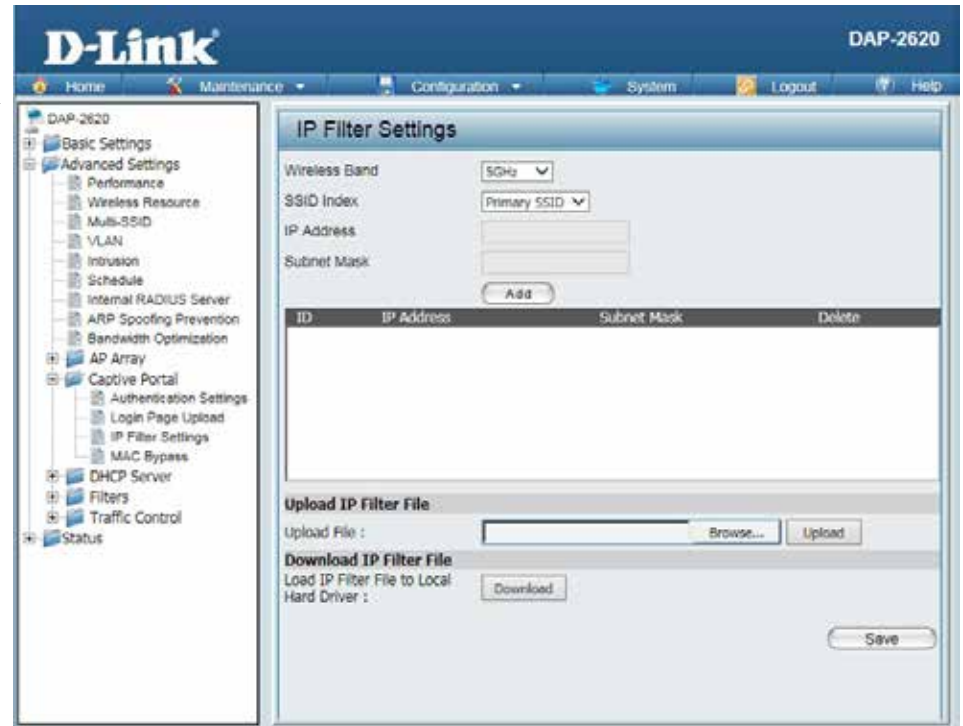
Wireless Band : Wireless Band : Select 2.4GHz or 5GHz.

IP Address: IP Address: Enter the IP address or network address

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

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

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



MAC Bypass

The DAP-2620 features a wireless MAC Bypass. Once a user is finished with these settings, click the Save button to let the changes take effect.

Wireless Band: Select the wireless band for MAC Bypass.

SSID Index: Select the SSID for MAC Bypass.

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

MAC Address List: When a MAC address is entered, it appears in this list.
Highlight a MAC address and click the Delete icon to remove it from this list.

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

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

The screenshot shows the 'MAC Bypass Settings' web interface. At the top, there are three dropdown menus: 'Wireless Band' set to '2.4GHz', 'SSID Index' set to 'Primary SSID', and 'MAC Address' with six empty input boxes and an 'Add' button. Below this is a table with three columns: 'ID', 'MAC Address', and 'Delete'. The table is currently empty. Underneath the table, there are two sections: 'Upload MAC File' with an 'Upload File' input field, a '浏览...' (Browse) button, and an 'Upload' button; and 'Download MAC File' with a 'Load MAC File to Local Hard Driver' input field and a 'Download' button. At the bottom right of the interface is a 'Save' button.

DHCP Server

Dynamic Pool Settings

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. If needed or required in the network, the DAP-2620 is capable of acting as a DHCP server.

Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses. Select Enable to allow the DAP-2620 to function as a DHCP server.

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

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

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

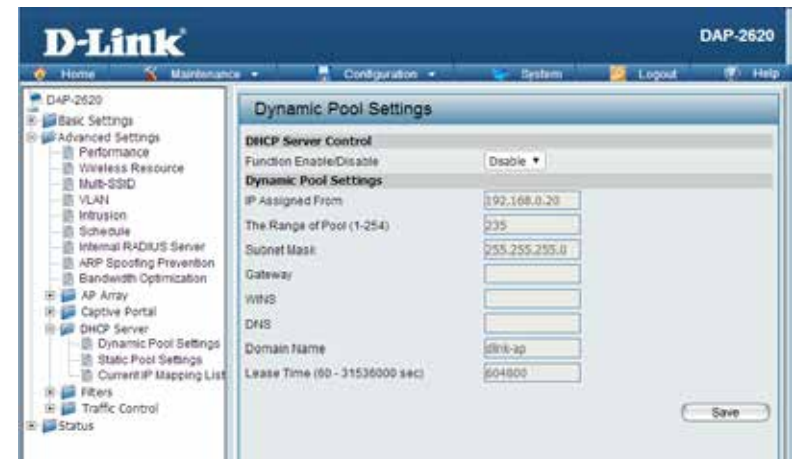
Gateway: Enter the IP address of the gateway on the network.

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

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

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

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



Static Pool Setting

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

Function Enable/Disable: Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses. Select Enable to allow the DAP-2620 to function as a DHCP server.

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

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

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

Gateway: Specify the Gateway address for the wireless network.

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

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

Domain Name: Specify the domain name for the network.

Static Pool Settings

DHCP Server Control

Function Enable/Disable: Enable

Static Pool Setting

Host Name:

Assigned IP:

Assigned MAC Address: : : : : :

Subnet Mask: 255.255.255.0

Gateway:

WINS:

DNS:

Domain Name: dlink-ap

Save

Host Name	MAC Address	IP Address	Edit	Delete

Current IP Mapping List

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

Current DHCP Dynamic Profile: These are IP address pools the DHCP server has assigned using the dynamic pool setting.

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

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

Lease Time: The length of time that the dynamic IP address will be valid.

Current DHCP Static Pools: These are the IP address pools of the DHCP server assigned through the static pool settings.

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

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

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

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

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

Filters

Wireless MAC ACL

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

Wireless Band: Displays the current wireless band rate.

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

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

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

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

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

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

Wireless MAC ACL Settings

Wireless Band: 2.4GHz

Access Control List: Accept

MAC Address: : : : : : Add

ID	MAC Address	Delete

Current Client Information

MAC Address	SSID	Band	Authentication	Signal	Add
00:1F:3B:AD:35:0B	dlink	N	OPEN	98%	<input type="checkbox"/>

Upload ACL File

Upload File : Browse... Upload

Download ACL File

Load ACL File to Local Hard Driver : Download

Save

WLAN Partition

This page allows the user to configure a WLAN Partition.

Wireless Band: Displays the current wireless band.

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

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

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

WLAN Partition		
Wireless Band	2.4GHz ▼	
Link Integrity	Disable ▼	
Ethernet to WLAN Access	Enable ▼	
Internal Station Connection		
Primary SSID	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
Multi-SSID 1	<input type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
Multi-SSID 2	<input type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
Multi-SSID 3	<input type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
Multi-SSID 4	<input type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
Multi-SSID 5	<input type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
Multi-SSID 6	<input type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
Multi-SSID 7	<input type="radio"/> Enable	<input type="radio"/> Disable <input type="radio"/> Guest mode
<input type="button" value="Save"/>		

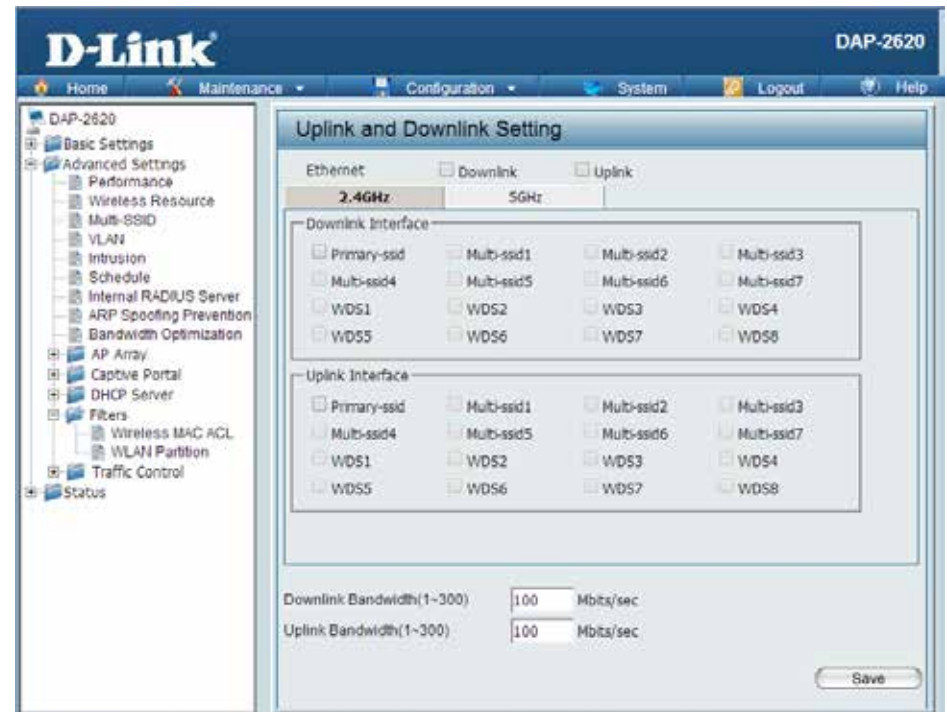
Traffic Control

Uplink/Downlink Setting

The uplink/downlink setting allows users to customize the downlink and uplink interfaces including specifying downlink/uplink bandwidth rates in Mbits per second. These values are also used in the QoS and Traffic Manager windows. Once the desired uplink and downlink settings are finished, click the **Save** button to let your changes take effect.

Downlink Bandwidth: The downlink bandwidth in Mbits per second.

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



QoS

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

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

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

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

The screenshot shows the QoS configuration window with the following settings:

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

A **Save** button is located at the bottom right of the 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. Click the **Save** button to let your changes take effect.

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

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

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

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

Traffic Manager

Traffic Manager Disable ▾

Unlisted Clients Traffic Deny Forward

Downlink Bandwidth Mbits/sec

Uplink Bandwidth Mbits/sec

Add Traffic Manager Rule

Name

Client IP(optional)

Client MAC(optional)

Downlink Speed Mbits/sec

Uplink Speed Mbits/sec

Traffic Manager Rules

Name	Client IP	Client MAC	Downlink Speed	Uplink Speed	Edit	Del

Status

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

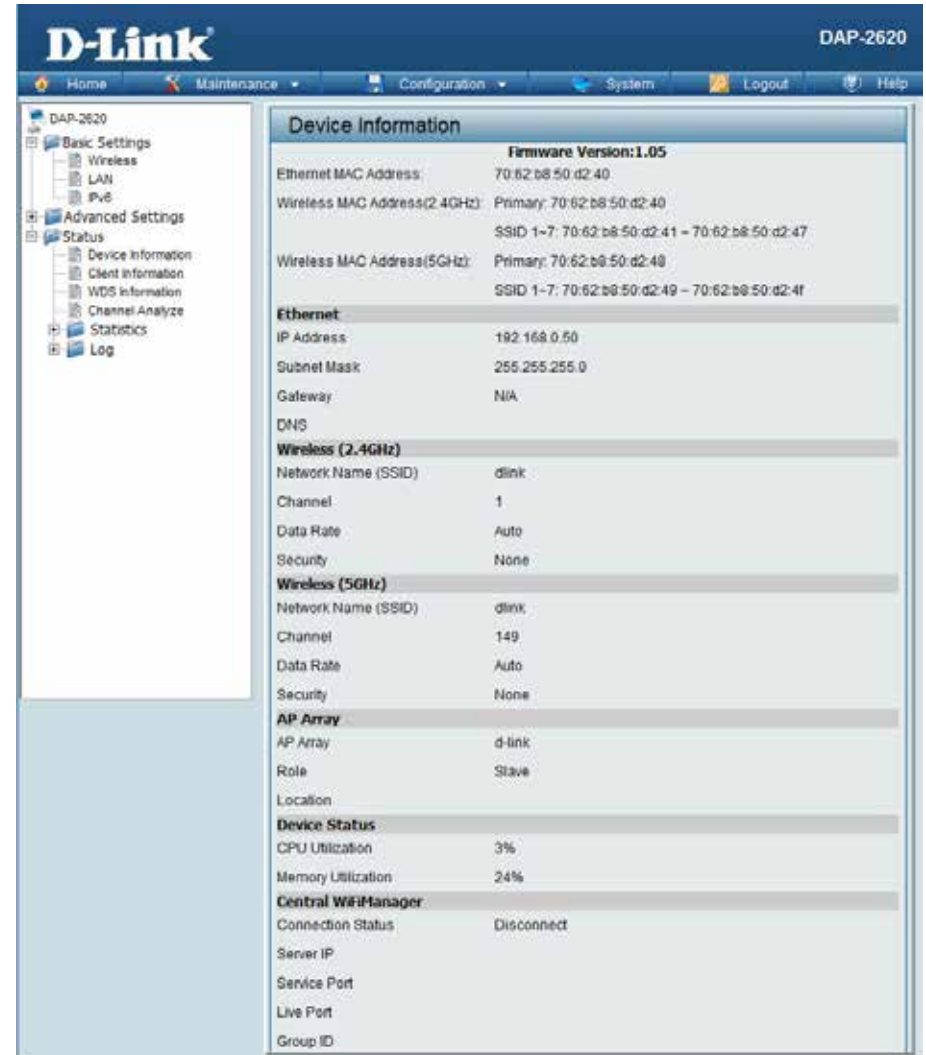
The screenshot displays the D-Link DAP-2620 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with categories: Basic Settings (Wireless, LAN, IPv6), Advanced Settings, Status (Device Information, Client Information, WDS Information, Channel Analyze), Statistics, and Log. The main content area is titled 'Device Information' and contains the following data:

Device Information	
Firmware Version: 1.05	
Ethernet MAC Address:	70:62:b8:50:d2:40
Wireless MAC Address(2.4GHz):	Primary: 70:62:b8:50:d2:40
	SSID 1~7: 70:62:b8:50:d2:41 ~ 70:62:b8:50:d2:47
Wireless MAC Address(5GHz):	Primary: 70:62:b8:50:d2:48
	SSID 1~7: 70:62:b8:50:d2:49 ~ 70:62:b8:50:d2:4f
Ethernet	
IP Address	192.168.0.50
Subnet Mask	255.255.255.0
Gateway	N/A
DNS	
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	1
Data Rate	Auto
Security	None
Wireless (5GHz)	
Network Name (SSID)	dlink
Channel	149
Data Rate	Auto
Security	None
AP Array	
AP Array	d-link
Role	Slave
Location	
Device Status	
CPU Utilization	3%
Memory Utilization	24%

Device Information

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

Device Information: This read-only window displays the configuration settings of the DAP-2620, including the firmware version and the device's MAC address.



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

Device Information	
Firmware Version: 1.05	
Ethernet MAC Address:	70:82:b8:50:d2:40
Wireless MAC Address(2.4GHz):	Primary: 70:82:b8:50:d2:40 SSID 1-7: 70:82:b8:50:d2:41 - 70:82:b8:50:d2:47
Wireless MAC Address(5GHz):	Primary: 70:62:b8:50:d2:48 SSID 1-7: 70:62:b8:50:d2:49 - 70:62:b8:50:d2:4f
Ethernet	
IP Address:	192.168.0.50
Subnet Mask:	255.255.255.0
Gateway:	N/A
DNS	
Wireless (2.4GHz)	
Network Name (SSID):	dlink
Channel:	1
Data Rate:	Auto
Security:	None
Wireless (5GHz)	
Network Name (SSID):	dlink
Channel:	149
Data Rate:	Auto
Security:	None
AP Array	
AP Array:	d-link
Role:	Slave
Location	
Device Status	
CPU Utilization:	3%
Memory Utilization:	24%
Central WiFiManager	
Connection Status:	Disconnect
Server IP:	
Service Port:	
Live Port:	
Group ID:	

Client Information

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

Client Information: This window displays the wireless client information for clients currently connected to the DAP-2620.

SSID: Displays the SSID of the client.

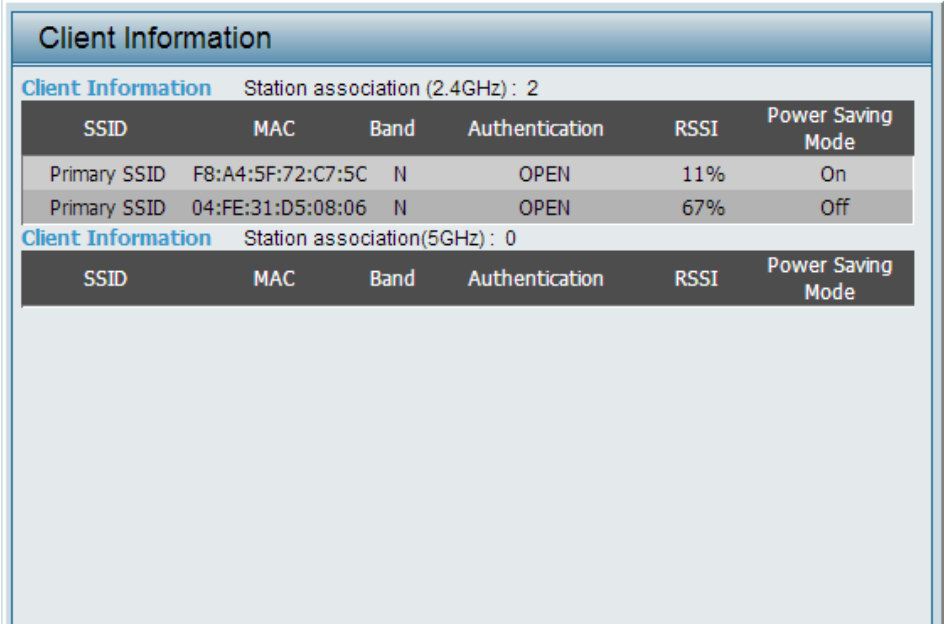
MAC: Displays the MAC address of the client.

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

Authentication: Displays the type of authentication being used.

RSSI: Displays the client's signal strength.

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



The screenshot shows a window titled "Client Information" with two sections. The first section is "Station association (2.4GHz) : 2" and the second is "Station association(5GHz) : 0". Each section contains a table with columns for SSID, MAC, Band, Authentication, RSSI, and Power Saving Mode.

Client Information					
Station association (2.4GHz) : 2					
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode
Primary SSID	F8:A4:5F:72:C7:5C	N	OPEN	11%	On
Primary SSID	04:FE:31:D5:08:06	N	OPEN	67%	Off
Station association(5GHz) : 0					
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode

WDS Information Page

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

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-2620.

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

Status: Displays the status of the power saving feature.



The screenshot shows a window titled "WDS Information" containing two tables. The first table is for Channel 1 (2.412 GHz) and the second is for Channel 36 (5.18 GHz). Both tables have columns for Name, MAC, Authentication, Signal, and Status.

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

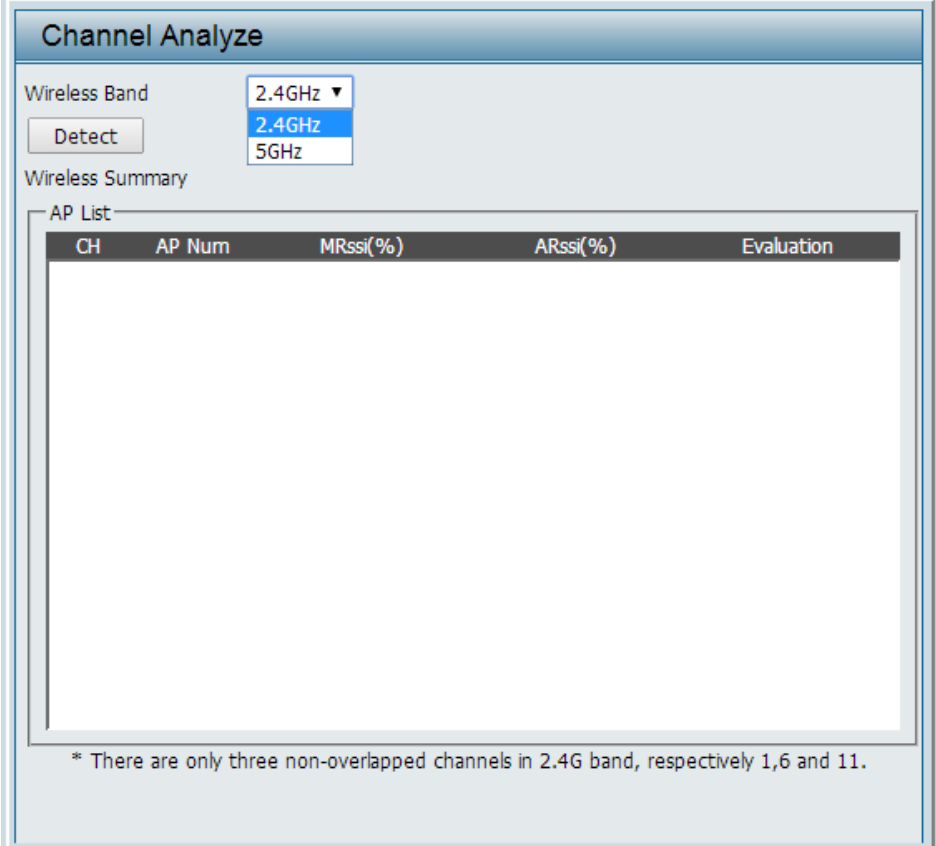
WDS Information				
Channel : 36 (5.18 GHz)				
Name	MAC	Authentication	Signal	Status

Channel Analyze

Wireless Band: Select either 2.4Ghz or 5GHz.

Detect: Click the Detect button to scan.

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



Channel Analyze

Wireless Band: 2.4GHz ▾
2.4GHz
5GHz

Detect

Wireless Summary

AP List

CH	AP Num	MRssi(%)	ARssi(%)	Evaluation
----	--------	----------	----------	------------

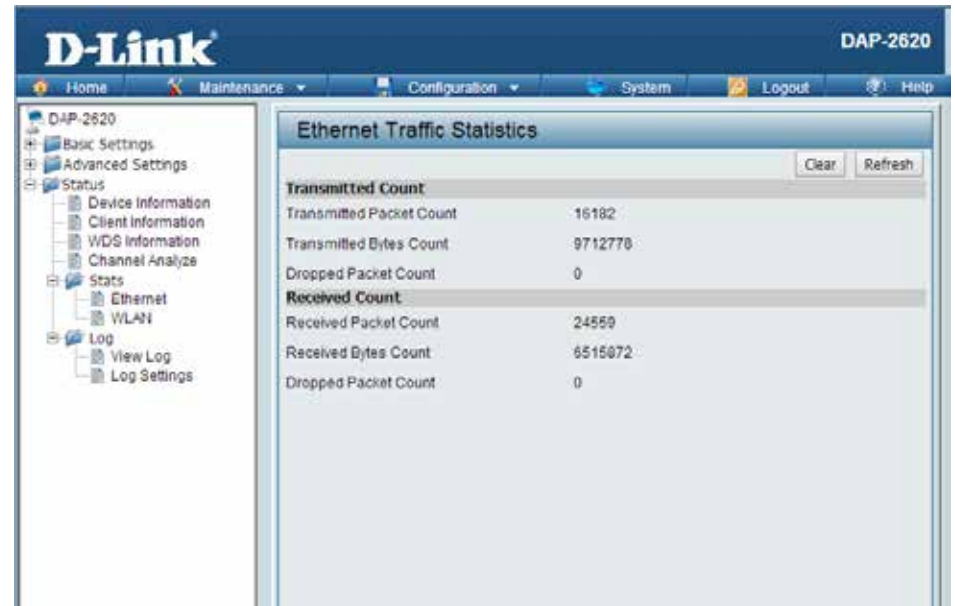
* There are only three non-overlapped channels in 2.4G band, respectively 1,6 and 11.

Stats Page

Ethernet Traffic Statistics

Displays wired interface network traffic information.

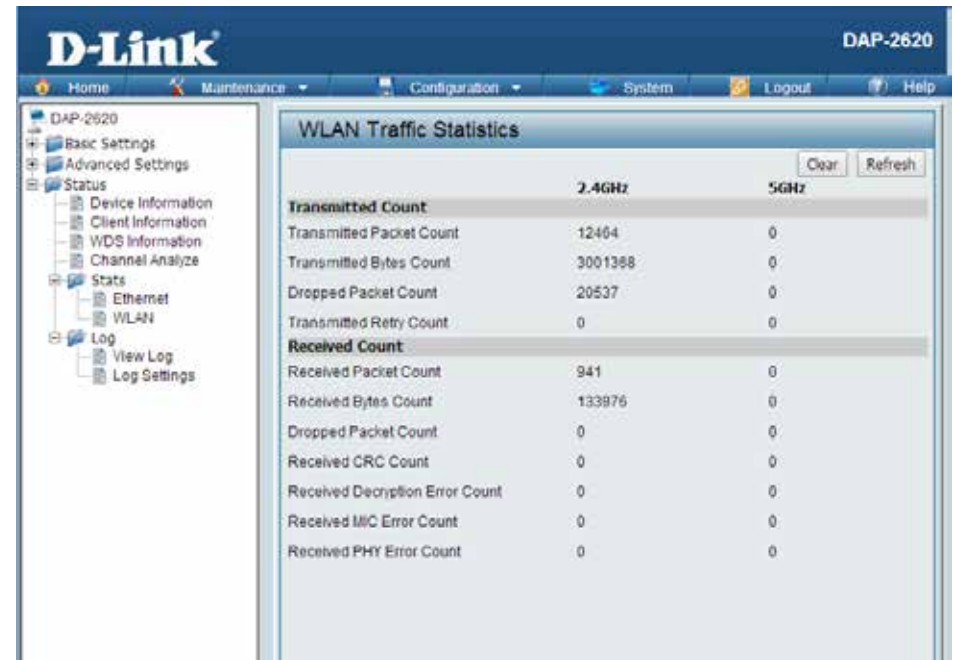
Ethernet Traffic Statistics: This page displays transmitted and received count statistics for packets and bytes.



WLAN Traffic Statistics

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

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



The screenshot shows the D-Link DAP-2620 web interface. The navigation menu on the left includes: DAP-2620, Basic Settings, Advanced Settings, Status (Device Information, Client Information, WDS Information, Channel Analyze), Stats (Ethernet, WLAN), Log (View Log, Log Settings). The main content area is titled "WLAN Traffic Statistics" and features a table with columns for "2.4GHz" and "5GHz". The table is divided into "Transmitted Count" and "Received Count" sections. The "Transmitted Count" section includes: Transmitted Packet Count (12464), Transmitted Bytes Count (3001388), Dropped Packet Count (20537), and Transmitted Retry Count (0). The "Received Count" section includes: Received Packet Count (941), Received Bytes Count (133976), Dropped Packet Count (0), Received CRC Count (0), Received Decryption Error Count (0), Received MIC Error Count (0), and Received PHY Error Count (0). There are "Clear" and "Refresh" buttons in the top right of the table area.

	2.4GHz	5GHz
Transmitted Count		
Transmitted Packet Count	12464	0
Transmitted Bytes Count	3001388	0
Dropped Packet Count	20537	0
Transmitted Retry Count	0	0
Received Count		
Received Packet Count	941	0
Received Bytes Count	133976	0
Dropped Packet Count	0	0
Received CRC Count	0	0
Received Decryption Error Count	0	0
Received MIC Error Count	0	0
Received PHY Error Count	0	0

Log

View Log

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

View Log: The AP's embedded memory displays system and network messages including a time stamp and message type. The log information includes but is not limited to the following items: cold start AP, upgrading firmware, client associate and disassociate with AP, and web login. The web page holds up to 500 logs.

The screenshot shows the D-Link DAP-2620 web interface. The left sidebar contains a navigation tree with the following items: DAP-2620, Basic Settings, Advanced Settings, Status (Device Information, Client Information, WDS Information, Channel Analyze), Stats (Ethernet, WLAN), Log (View Log, Log Settings). The main content area is titled "View Log" and includes navigation buttons: First Page, Last Page, Previous, Next, and Clear. Below the buttons, it indicates "Page 1 of 3". The log entries are as follows:

Time	Priority	Message
Uptime 0 day 04:04:45	[SYSACT]	Web login success from 192.168.0.2
Uptime 0 day 03:16:01	[Wireless]	2.4G:Deauth:Aging STA F8:A4:5F:72:C7:5C
Uptime 0 day 03:09:00	[SYSACT]	Web logout from 192.168.0.2
Uptime 0 day 03:05:16	[Wireless]	2.4G:Deauth:Aging STA 04:FE:31:D5:08:06
Uptime 0 day 03:01:47	[SYSACT]	Web login success from 192.168.0.2
Uptime 0 day 03:00:05	[Wireless]	2.4G:Association Success:STA 04:FE:31:D5:08:06
Uptime 0 day 02:54:35	[SYSACT]	Web logout from 192.168.0.2
Uptime 0 day 02:51:29	[SYSACT]	Web login success from 192.168.0.2
Uptime 0 day 02:49:22	[Wireless]	2.4G:Association Success:STA F8:A4:5F:72:C7:5C
Uptime 0 day 02:47:01	[SYSACT]	Web login success from 192.168.0.2
Uptime 0 day 02:09:31	[Wireless]	2.4G:Deauth:Aging STA E8:99:C4:A2:01:D0
Uptime 0 day 02:04:10	[Wireless]	2.4G:Association Success:STA E8:99:C4:A2:01:D0
Uptime 0 day 01:23:01	[Wireless]	2.4G:Deauth:Aging STA E8:99:C4:AE:0C:22
Uptime 0 day 01:17:46	[Wireless]	2.4G:Deauth:Aging STA 04:FE:31:D5:08:06
Uptime 0 day 01:17:33	[Wireless]	2.4G:Association Success:STA E8:99:C4:AE:0C:22
Uptime 0 day 01:14:55	[Wireless]	2.4G:Association Success:STA 04:FE:31:D5:08:06

Log Settings

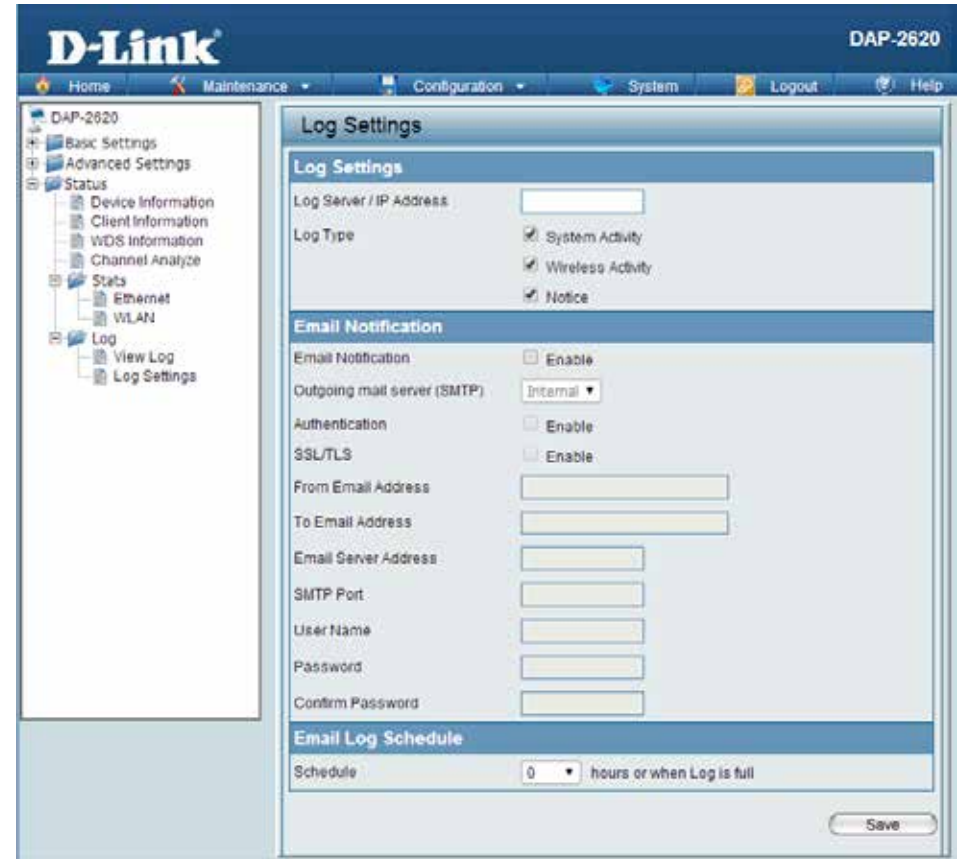
Enter the log server's IP address to send the log to that server. Check or uncheck System Activity, Wireless Activity, or Notice to specify what kind of log type you want it to log.

Log Server/IP Address: Enter the IP address of the server you would like to send the DAP-2620 log to.

Log Type: Check the box for the type of activity you want to log. There are three types: System Activity, Wireless Activity, and Notice.

E-mail Notification: Support Simple Mail Transfer Protocol for log schedule and periodical change key. It can not support Gmail SMTP port 465. Please set to Gmail SMTP port 25 or 587.

E-mail Log Schedule: Use the drop-down menu to set the e-mail log schedule.



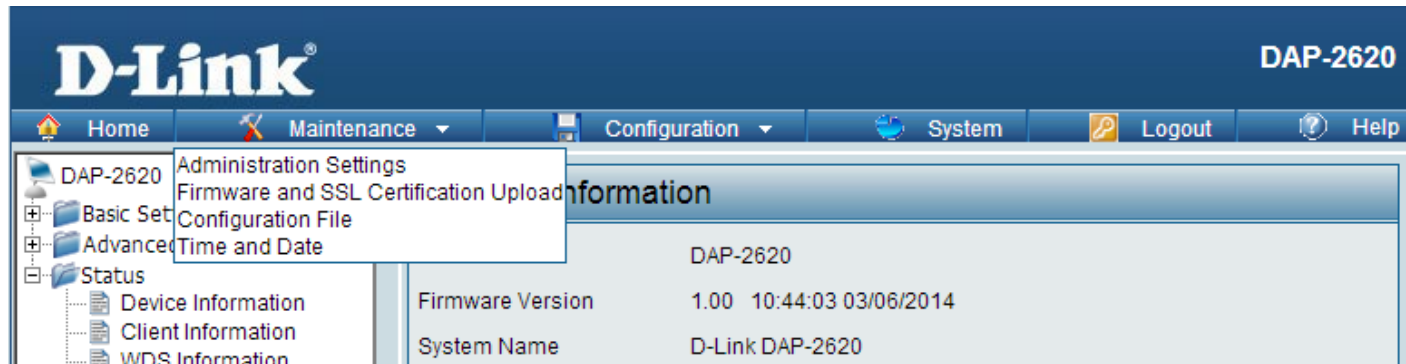
The screenshot displays the D-Link DAP-2620 web interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows a tree view with categories: 'DAP-2620', 'Basic Settings', 'Advanced Settings', 'Status', 'Stats', 'Log', and 'View Log'. The 'Log' category is expanded, showing 'Log Settings'. The main content area is titled 'Log Settings' and contains the following fields:

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

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

Maintenance Section

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



Administration

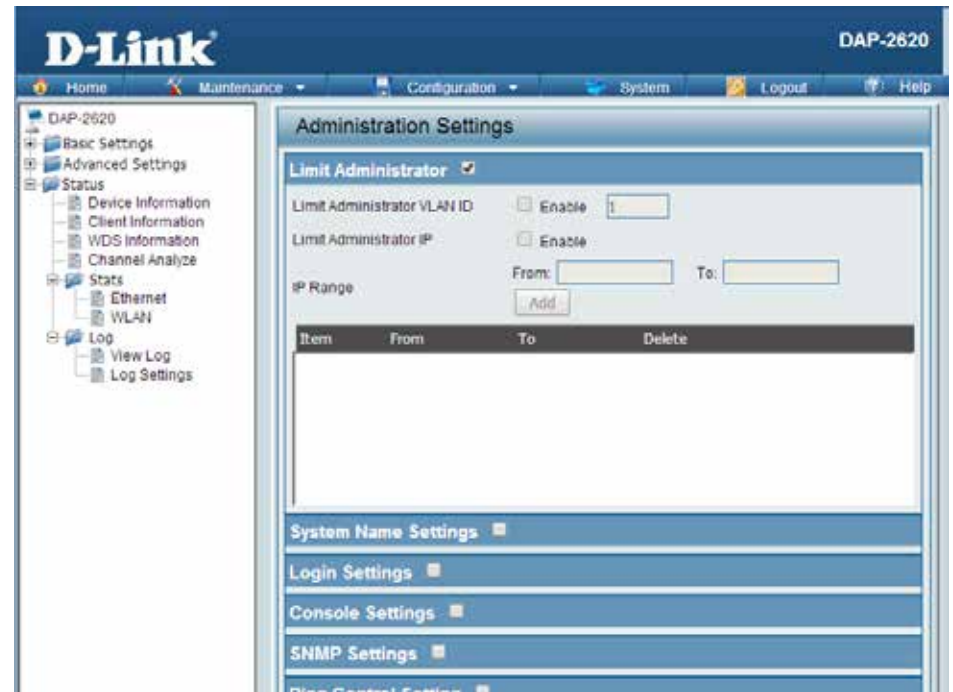
Limit Administrator

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

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

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

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



System Name Settings

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

System Name: The name of the device. The default name is D-Link DAP-2620.

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

System Name Settings <input checked="" type="checkbox"/>	
System Name	<input type="text" value="D-Link DAP-2620"/>
Location	<input type="text"/>

Login Settings

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

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

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

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

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

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

Console Settings

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

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

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

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

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

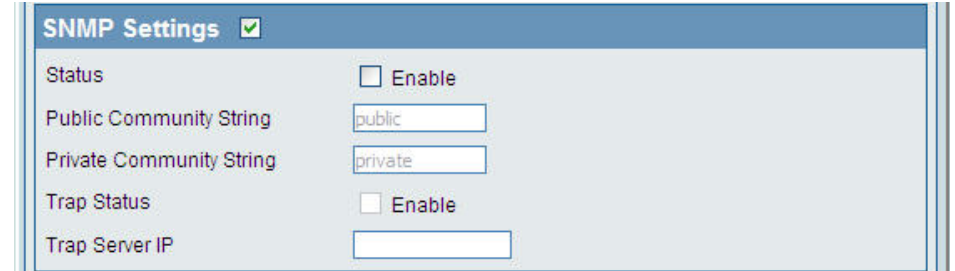
SNMP Settings

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

Status: Check the box to enable the SNMP functions. This is enabled by default.

Public Community String: Enter the public SNMP community string.

Private Community String: Enter the private SNMP community string.



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

Administration

Central WiFiManager Settings

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

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



The screenshot shows a web interface for 'Central WiFiManager Setting'. It features a blue header bar with the title and a checked checkbox. Below the header, there is a light gray area containing the text 'Enable Central WiFiManager' followed by a dropdown menu currently displaying 'Disable'.

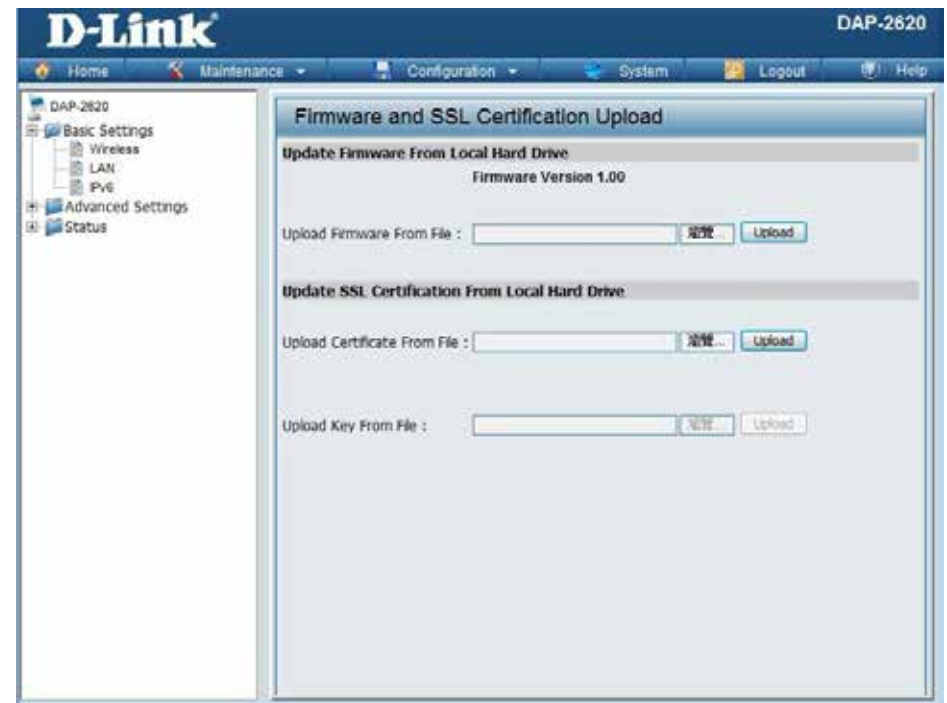
Firmware and SSL Upload

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

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

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

Upload SSL Certification 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.



Configuration File Upload

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

Configuration File Upload and Download: You can upload and download configuration files of the access point.

Upload Configuration File: Browse to the saved configuration file you have in local drive and click "Open" and "Upload" to update the configuration.

Download Configuration File: Click "Download" to save the current configuration file to your local disk. Note that if you save one configuration file with the administrator's password now, after resetting your DAP-2620 and then updating to this saved configuration file, the password will be gone.



Time and Date Settings

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

Current Time: Displays the current time and date settings.

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

NTP Server: Enter the NTP server IP address.

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

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

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

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

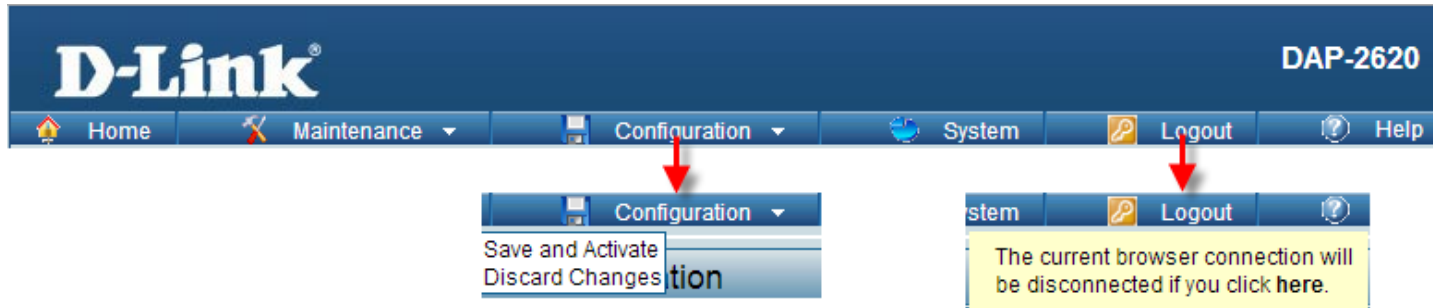
The screenshot displays the D-Link DAP-2620 web interface. The top navigation bar includes 'Home', 'Maintenance', 'Configuration', 'System', 'Logout', and 'Help'. The left sidebar shows 'DAP-2620' with sub-items: 'Basic Settings', 'Advanced Settings', and 'Status'. The main content area is titled 'Time and Date Settings' and contains the following sections:

- Time Configuration:** Shows 'Current Time' as 01/01/1970 04:15:56.
- Automatic Time Configuration:** Includes a checkbox for 'Enable NTP Server', an 'NTP Server' text input field, a 'Time Zone' dropdown menu (set to '(GMT+08:00) Ulaan Batair'), and a checkbox for 'Enable Daylight Saving'.
- Set the Date and Time Manually:** Features a 'Date And Time' section with dropdown menus for Year (2014), Month (Mar), Day (12), Hour (15), Minute (13), and Second (5). Below these is a button labeled 'Copy Your Computer's Time Settings'.

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

Configuration and System

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



System Settings

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

Restart the Device: Click Restart to restart the DAP-2620.

Restore to Factory Default Settings: Click Restore to restore the DAP-2620 back to factory default settings.

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



Help

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

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

Basic Settings

Wireless Settings

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

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

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

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

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

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

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

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

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

Authentication

Federal Communication Commission Interference Statement

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

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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

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 24cm between the radiator & your body.

Registration

Register your product online at www.onlineregister.com/dlink



Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.00
March 19, 2019