

DAP-2330

Version 1.00

Wireless N300
Single Band Gigabit PoE Access Point

User Manual

Business Class Networking

Table of Contents

Product Overview.....	4	IPv6	24
Introduction	4	Advanced Settings	25
Features.....	5	Performance	26
Package Contents.....	6	Wireless Resource Control.....	28
System Requirements	6	Multi-SSID	30
Hardware Overview	7	VLAN.....	32
LEDs	7	VLAN List.....	32
Connections	7	Port List.....	33
Basic Installation.....	8	Add/Edit VLAN	34
Hardware Setup	8	PVID Settings.....	35
Method 1 - PoE with PoE Switch	8	Intrusion.....	36
Method 2 - PoE without PoE Switch or Router.....	9	Schedule	37
Method 3 - No PoE.....	10	Internal RADIUS Server.....	38
Web User Interface	11	ARP Spoofing Prevention	39
Wireless	12	Bandwidth Optimization	40
Access Point Mode	12	AP Array.....	42
WDS with AP Mode	14	AP Array Scan	42
WDS Mode	16	Configuration Settings.....	43
Wireless Client Mode.....	18	Auto-RF	47
Wireless Security	19	Load Balance	48
Wired Equivalent Privacy (WEP)	19	Captive Portal.....	49
Wi-Fi Protected Access (WPA / WPA2).....	20	Authentication Settings - Passcode	49
802.1x Authentication.....	22	Authentication Settings - User Name/Password.....	50
LAN	23	Authentication Settings - Remote RADIUS.....	51
		Authentication Settings - LDAP	52
		Authentication Settings - POP3.....	53

Login Page Upload	54	Console Settings	75
Web Redirection	55	SNMP Settings	76
DHCP Server	56	Administration	77
Dynamic Pool Settings	56	Central WiFiManager Settings	77
Static Pool Setting	57	Firmware and SSL Upload	78
Current IP Mapping List	58	Configuration File Upload	79
Filters	59	Time and Date Settings	80
Wireless MAC ACL	59	Configuration and System	81
WLAN Partition	60	System Settings	82
Traffic Control	61	Help	83
Uplink/Downlink Setting	61	Knowledge Base	84
QoS	62	Wireless Basics	84
Traffic Manager	63	Wireless Installation Considerations	85
Status	64	Troubleshooting	86
Device Information	65	Why can't I access the web-based configuration utility?	86
Client Information	66	What can I do if I forgot my password?	86
WDS Information Page	67	How to check your IP address?	87
Channel Analyze	68	How to statically assign an IP address?	88
Stats Page	69	Technical Specifications	89
Ethernet Traffic Statistics	69	Antenna Pattern	90
WLAN Traffic Statistics	70	Contacting Technical Support	91
Log	71	Warranty	92
View Log	71	Registration	98
Log Settings	72		
Maintenance Section	73		
Administration	74		
Limit Administrator	74		
System Name Settings	75		
Login Settings	75		

Product Overview

Introduction

D-Link, an industry pioneer in wireless networking, introduces a solution for businesses seeking to deploy next generation 802.11n LANs. D-Link unveils its new DAP-2330, designed specifically for environments with high traffic areas such as airports, coffee shops, shopping centers, sporting venues, and school campuses to provide secure and manageable dual band wireless network options for network administrators.

Versatile Access Point

The DAP-2330 Access Point allows network administrators to deploy a highly manageable and extremely robust dual band wireless network. For advanced installations, this new high-speed Access Point has integrated 802.3af Power over Ethernet (PoE) support, allowing installation of this device in areas where power outlets are not readily available. In addition to bridging 802.11b/g/n wireless networks, the DAP-2330 can bridge to wired networks with its integrated Gigabit (10/100/1000Mbps) Ethernet port.

Enhanced Performance

The DAP-2330 delivers reliable wireless performance with maximum wireless signal rates of up to 300Mbps. This, coupled with support for Wi-Fi Multimedia™ (WMM) Quality of Service features, makes it an ideal access point for audio, video, and voice applications.

Security

To help maintain a secure wireless network, the DAP-2330 provides the latest in wireless security technologies by supporting both Personal and Enterprise versions of WPA and WPA2 (802.11i) with support for RADIUS server back end. To further protect your wireless network, MAC Address Filtering, Wireless LAN segmentation, Disable SSID Broadcast, Rogue AP Detection, and Wireless Broadcast Scheduling are also included.

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

Features

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

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

Package Contents

- DAP-2330 Access Point
- Power Adapter
- Mounting Plate and Hardware
- Ethernet Cable
- CD (with software and user manual)
- Quick Installation Guide

Note: *Using a power supply with a different voltage rating than the one included with the DAP-2330 will cause damage and void the warranty for this product.*

System Requirements

- y Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- y Internet Explorer Version 11.0, Chrome 33, Safari 7, or Firefox 28 and above (for web-based configuration)

Hardware Overview

LEDs



1	Power/Status	Solid Red	Indicates the access point has malfunctioned.
		Blinking Red	This LED will blink during boot-up.
		Solid Green	Indicates that the DAP-2330 is working properly.
		Blinking Green	This light will blink green during data transmission.

Connections



2	Power Receptor	Connect the supplied power adapter.
3	LAN (PoE) Port	Connect to a Power over Ethernet (PoE) switch or router via an Ethernet cable.
4	Reset Button	Press and hold for five seconds to reset the access point to the factory default settings. Press and hold for one second to reboot the access point.

Basic Installation

Hardware Setup

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

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

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

Method 3 - Use if you do not have a PoE switch or router and have a power outlet near the location of the access point.

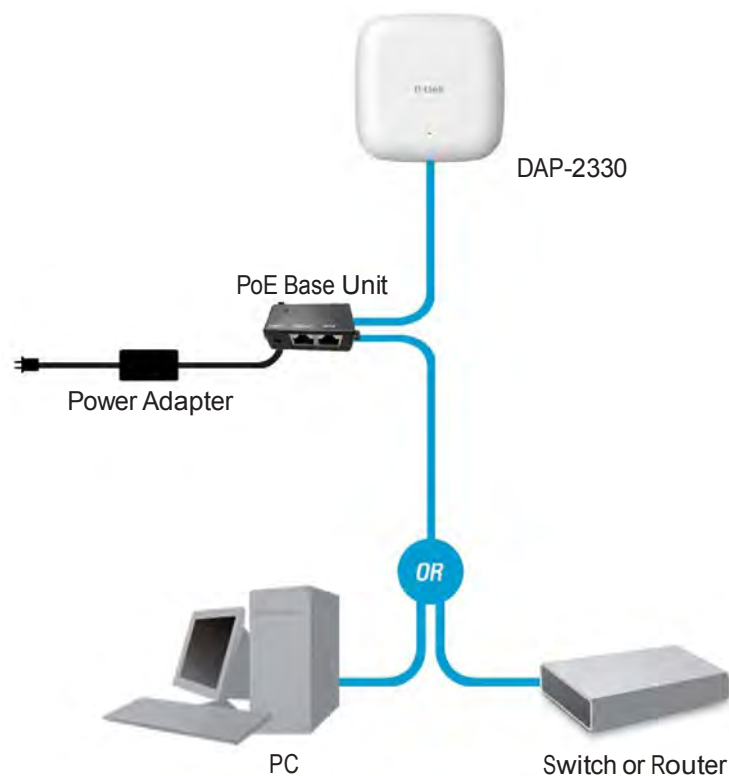
Method 1 - PoE with PoE Switch

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.



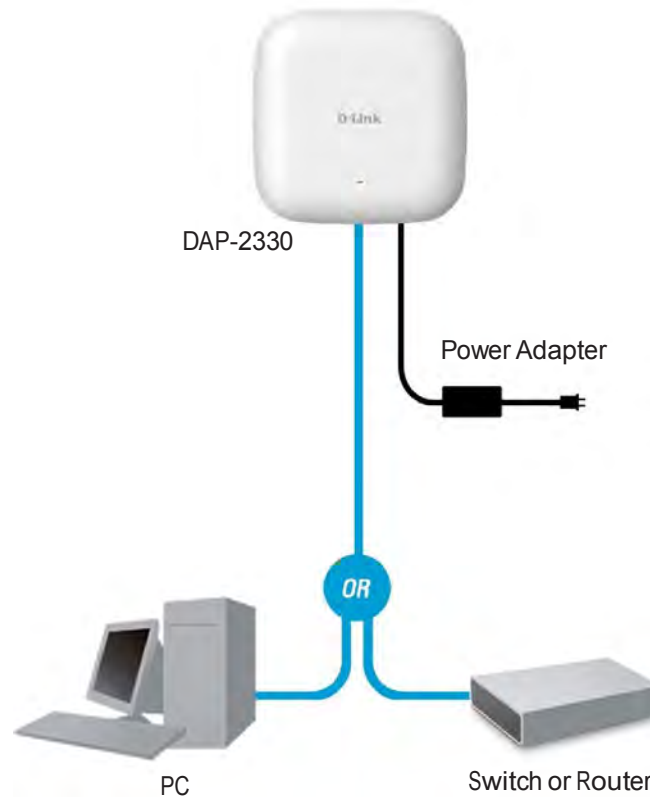
Method 2 - PoE without PoE Switch or Router

1. Connect one end of an Ethernet cable into the **Data In** port on the PoE base unit and the other end into one port on your switch, router, or computer.
2. Connect one end of an Ethernet cable into the **P+Data Out** port on the PoE base unit and the other end into the LAN (PoE) port on the Access Point.
3. Use the supplied power adapter. Connect the power adapter to the **Power In** receptor on the PoE adapter.
4. Connect the power cable to the power adapter and then connect the other end into a power outlet.



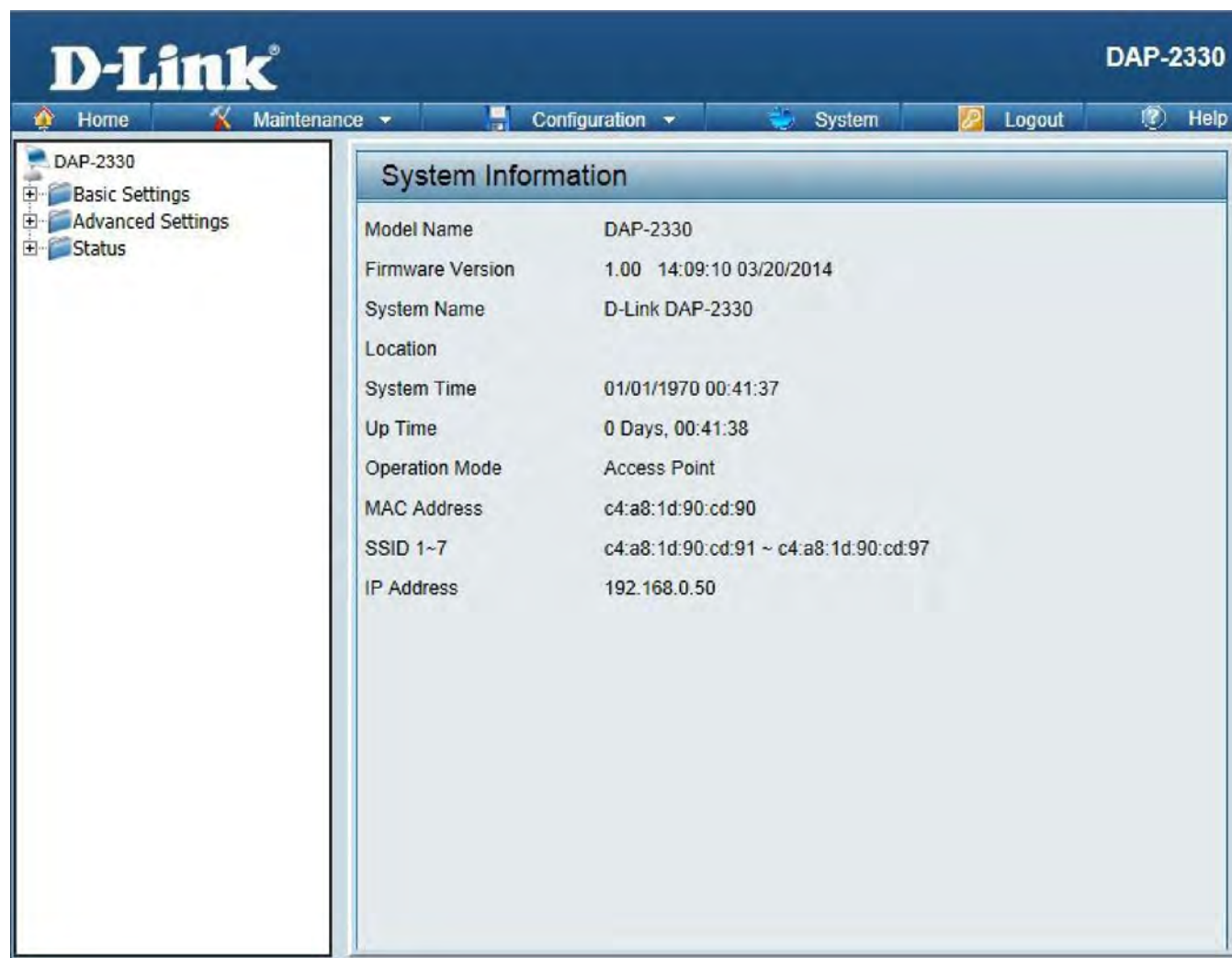
Method 3 - No PoE

1. Connect one end of your Ethernet cable into the LAN (PoE) port and then connect the other end to a switch, router, or computer.
2. Use the supplied power adapter. Connect the power adapter to the Power receptor on the Access Point.
3. Connect the power cable to the power adapter and then connect the other end into a power outlet.



Web User Interface

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



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

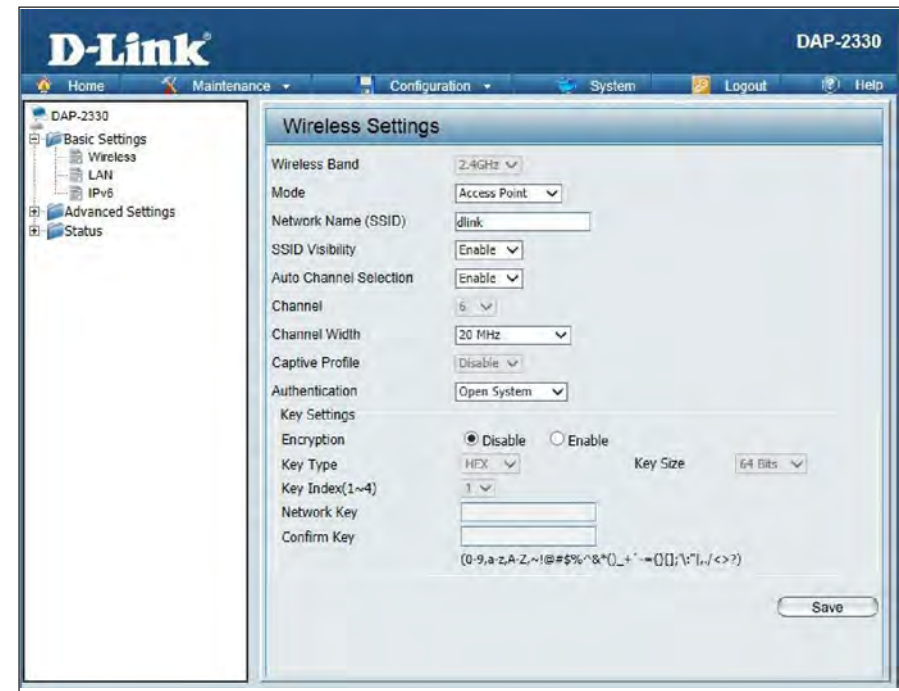
Wireless Band: Select 2.4GHz in default.

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 wireless devices on your network.

Captive Profile: Disable or select a Captive Portal profile for Primary SSID.

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 2.4GHz in default.

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 wireless devices on your network.

The screenshot shows the 'Wireless Settings' configuration page. The 'Wireless Band' is set to '2.4GHz'. The 'Mode' is set to 'WDS with AP'. The 'Network Name (SSID)' is 'dlink'. 'SSID Visibility' is 'Enable'. 'Auto Channel Selection' is 'Disable'. The 'Channel' is '6' and 'Channel Width' is '20 MHz'. The 'Captive Profile' is 'Disable'. Under the 'WDS' section, the 'Remote AP MAC Address' is entered in eight fields (1-8). Below this is a 'Site Survey' section with a table header: CH, RSSI, BSSID, Security, SSID. A 'Scan' button is to the right of the table. The 'Authentication' section is set to 'Open System'. Under 'Key Settings', 'Encryption' is 'Disable', 'Key Type' is 'HEX', 'Key Index(1~4)' is '1', and 'Key Size' is '64 Bits'. There are input fields for 'Network Key' and 'Confirm Key'. A 'Save' button is at the bottom right.

Captive Profile: Disable or select a Captive Portal profile.

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 2.4GHz in default.

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.

Captive Profile: Disable in default.

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 shows the 'Wireless Settings' configuration page. The 'Wireless Band' is set to '2.4GHz', 'Mode' is 'WDS', 'Network Name (SSID)' is 'dlink', 'SSID Visibility' is 'Enable', 'Auto Channel Selection' is 'Disable', 'Channel' is '6', and 'Channel Width' is '20 MHz'. The 'Captive Profile' is set to 'Disable'. Under the 'WDS' section, there are eight input fields for 'Remote AP MAC Address' labeled 1 through 8. Below this is a 'Site Survey' section with a 'Scan' button and a table with columns 'CH', 'RSSI', 'BSSID', 'Security', and 'SSID'. The 'Authentication' section is set to 'Open System'. Under 'Key Settings', 'Encryption' is 'Disable', 'Key Type' is 'HEX', 'Key Index(1~4)' is '1', and 'Key Size' is '64 Bits'. There are input fields for 'Network Key' and 'Confirm Key' with a validation hint below them: '(0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}|:~\|,./<>?)'. A 'Save' button is at the bottom right.

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 2.4GHz in default.

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-2330 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.

Captive Profile: Disable in default.

Will be explained in the next topic.

Authentication:

Wireless Settings

Wireless Band: 2.4GHz
 Mode: Wireless Client
 Network Name (SSID): dlink
 SSID Visibility: Enable
 Auto Channel Selection: Enable
 Channel: 6
 Channel Width: Auto 20/40 MHz
 Captive Profile: Disable

Site Survey [Scan]

CH	RSSI	BSSID	Security	SSID

Authentication Open System

Key Settings

Encryption: ☒ Disable ☐ Enable
 Key Type: HEX Key Size: 64 Bits
 Key Index(1~4): 1
 Network Key:
 Confirm Key:
 (0-9,a-z,A-Z,~!@#\$%^&*()_+`-={}|:~!./<>?)

Wireless MAC Clone

Enable: ☐
 MAC Source: Auto
 MAC Address: : : : : : [Scan]

MAC Address

Wireless Security

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

There are mainly two forms of wireless encryption and they are called Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP was the first security method developed. It is a low level encryption but better than 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.

The screenshot shows the 'Wireless Settings' window. In the 'Key Settings' section, the 'Encryption' radio button is selected. The 'Key Type' is set to 'HEX' and the 'Key Size' is set to '64 Bits'. The 'Key Index(1~4)' is set to '1'. The 'Network Key' and 'Confirm Key' fields are empty, and the password strength indicator below them shows a strength of 0. The 'Save' button is at the bottom right.

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

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

Wi-Fi Protected Access (WPA / WPA2)

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

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

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

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

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

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

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

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

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

Wireless Settings

Wireless Band: 2.4GHz

Mode: Access Point

Network Name (SSID): dlink

SSID Visibility: Enable

Auto Channel Selection: Enable

Channel: 1

Channel Width: 20 MHz

Captive Profile: Disable

Authentication: WPA-Personal

PassPhrase Settings

WPA Mode: AUTO (WPA or WPA2)

Cipher Type: Auto

Group Key Update Interval: 3600 (Seconds)

☒ Manual ☐ Periodical Key Change

Activated From: Sun : 00 : 00

Time Interval: 1 (1~168) hour(s)

PassPhrase:

Confirm PassPhrase:

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

Save

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

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

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

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

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

RADIUS Port: Enter the RADIUS port.

RADIUS Secret: Enter the RADIUS secret.

Account Server: Enter the IP address of the Account Server

Account Port: Enter the Account port

Account Secret: Enter the Account secret

Wireless Settings

Wireless Band: 2.4GHz
 Mode: Access Point
 Network Name (SSID): dlink
 SSID Visibility: Enable
 Auto Channel Selection: Enable
 Channel: 1
 Channel Width: 20 MHz
 Captive Profile: Disable
 Authentication: WPA-Enterprise

RADIUS Server Settings

WPA Mode: AUTO (WPA or WPA2)
 Cipher Type: Auto
 Group Key Update Interval: 3600 (Seconds)
 Network Access Protection: ☒ Disable ☐ Enable
 RADIUS Server Mode: ☒ External ☐ Internal

Primary RADIUS Server Setting

RADIUS Server: 192.168.0.100 RADIUS Port: 1812
 RADIUS Secret: *****
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-={ } [] ; ' " | , . / < > ?)

Backup RADIUS Server Setting (Optional)

RADIUS Server: 192.168.0.101 RADIUS Port: 1812
 RADIUS Secret: *****
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-={ } [] ; ' " | , . / < > ?)

Primary Accounting Server Setting

Accounting Mode: Enable
 Accounting Server: 192.168.0.200 Accounting Port: 1813
 Accounting Secret: *****
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-={ } [] ; ' " | , . / < > ?)

Backup Accounting Server Setting (Optional)

Accounting Server: 192.168.0.201 Accounting Port: 1813
 Accounting Secret: *****
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-={ } [] ; ' " | , . / < > ?)

Save

802.1x Authentication

Key Update Interval : Select the interval during which the group key will be valid (300 is the recommended value). A lower interval may reduce data transfer rates.

RADIUS Server Mode : Select External or Internal RADIUS server

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

Wireless Settings

Wireless Band: 2.4GHz
 Mode: Access Point
 Network Name (SSID): dlink
 SSID Visibility: Enable
 Auto Channel Selection: Enable
 Channel: 6
 Channel Width: 20 MHz
 Captive Profile: Disable
 Authentication: 802.1X

RADIUS Server Settings

Key Update Interval: 300 (Seconds)

RADIUS Server Mode

RADIUS Server: ☒ External ☐ Internal

Primary RADIUS Server Setting

RADIUS Server: RADIUS Port: 1812
 RADIUS Secret:
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-= {} [] ; ' \ : , / < > ?)

Backup RADIUS Server Setting (Optional)

RADIUS Server: RADIUS Port: 1812
 RADIUS Secret:
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-= {} [] ; ' \ : , / < > ?)

Primary Accounting Server Setting

Accounting Mode: Disable
 Accounting Server: Accounting Port: 1813
 Accounting Secret:
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-= {} [] ; ' \ : , / < > ?)

Backup Accounting Server Setting (Optional)

Accounting Server: Accounting Port: 1813
 Accounting Secret:
 (0-9,a-z,A-Z,~!@#\$%^&*()_+ '-= {} [] ; ' \ : , / < > ?)

Save

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-2330. 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-2330. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

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

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

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

LAN Settings

Get IP From: Static IP (Manual) ▼

IP Address: 192.168.0.50

Subnet Mask: 255.255.255.0

Default Gateway:

DNS:

Save

IPv6

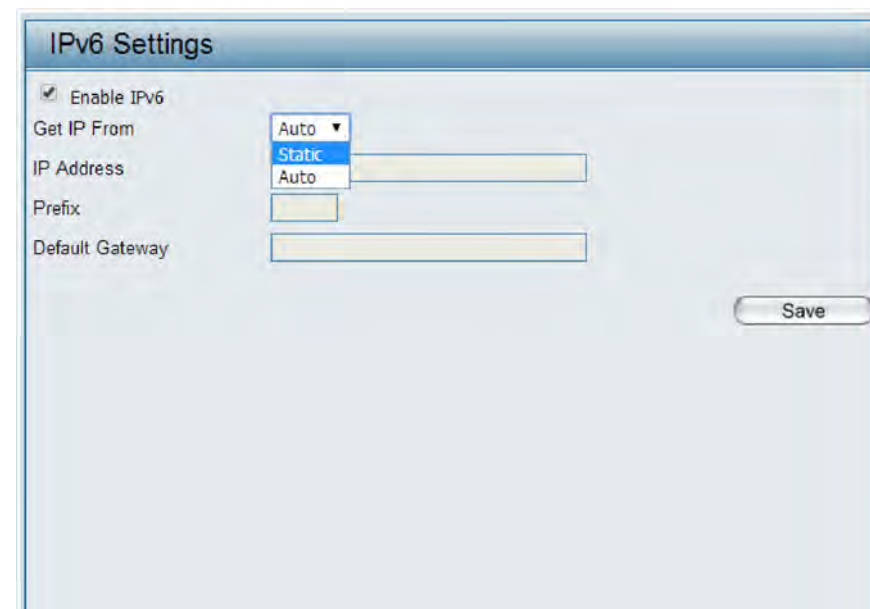
Enable IPv6: Check to enable the IPv6

Get IP From: Auto is chosen here. Choose this option the DAP-2330 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 a web-based configuration window titled "IPv6 Settings". It contains the following elements:

- A checked checkbox labeled "Enable IPv6".
- A dropdown menu labeled "Get IP From" with "Auto" selected. The dropdown list also shows "Static" and "Auto".
- A text input field labeled "IP Address" which is grayed out.
- A text input field labeled "Prefix" which is grayed out.
- A text input field labeled "Default Gateway" which is grayed out.
- A "Save" button 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-2330 web interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of the configuration menu, with 'Advanced Settings' expanded to show 'Performance', 'Wireless Resource', 'Multi-SSID', 'VLAN', 'Intrusion', 'Schedule', 'Internal RADIUS Server', 'ARP Spoofing Prevention', 'Bandwidth Optimization', 'AP Array', 'Captive Portal', 'DHCP Server', 'Filters', 'Traffic Control', and 'Status'. The main content area is titled 'Performance Settings' and contains the following configuration options:

Setting	Value
Wireless band	2.4GHz
Wireless	On
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Data Rate	Best(Up to 300) (Mbps)
Beacon Interval (40-500)	100
DTIM Interval (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out (2.4GHz, 48~200)	48 (μs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable (Mbps)
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT20/40 Coexistence	Enable

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

Performance

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

Wireless Band: Select 2.4Ghz in default.

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

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

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

Beacon Interval (25-500): 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.

The screenshot shows the 'Performance Settings' window with the following configurations:

- Wireless band: 2.4GHz
- Wireless: On
- Wireless Mode: Mixed 802.11n, 802.11g and 802.11b
- Data Rate: Best(Up to 300) (Mbps)
- Beacon Interval (40-500): 100
- DTIM Interval (1-15): 1
- Transmit Power: 100%
- WMM (Wi-Fi Multimedia): Enable
- Ack Time Out (2.4GHz, 48-200): 48 (μs)
- Short GI: Enable
- IGMP Snooping: Disable
- Multicast Rate: Disable (Mbps)
- Multicast Bandwidth Control: Disable
- Maximum Multicast Bandwidth: 100 kbps
- HT20/40 Coexistence: Enable

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

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 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 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

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

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** in default.

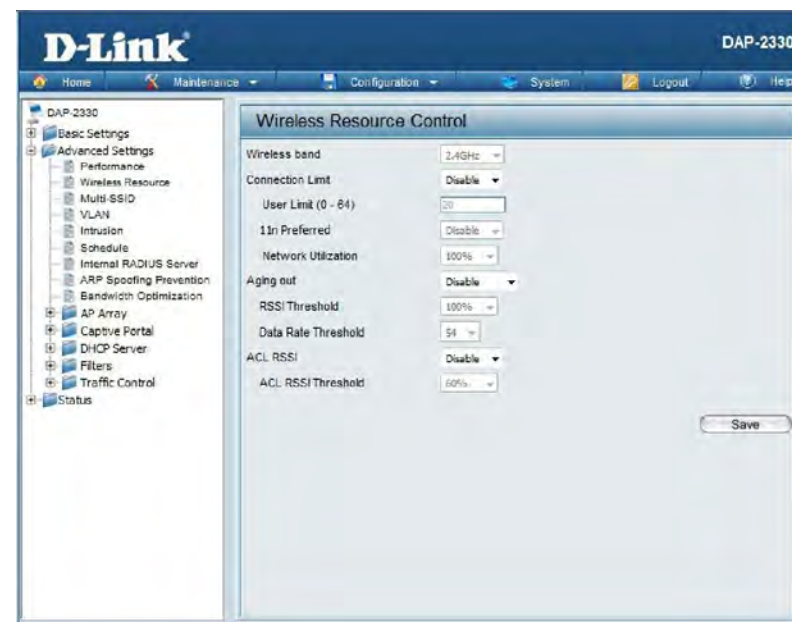
Connection Limit: Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client 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-2330 will not allow clients to associate with the AP.

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

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

Network Utilization: Set the maximum utilization of this access point for service. The DAP-2330 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** in default.

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

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

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

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

Priority: Select the priority level of the SSID selected.

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

Captive Profile: Enable or disable captive port profile for user authentication.



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-2330 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-2330 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

VLAN Mode : Static

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

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

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.

The screenshot shows the 'VLAN Settings' window. At the top, there are radio buttons for 'VLAN Status' (Disable is selected) and 'VLAN Mode' (Static is selected), along with a 'Save' button. Below this is a tabbed interface with four tabs: 'VLAN List', 'Port List' (which is active), 'Add/Edit VLAN', and 'PVID Setting'. The 'Port List' tab contains a table with four columns: 'Port Name', 'Tag VID', 'Untag VID', and 'PVID'. The table lists various ports and their associated VLAN IDs.

Port Name	Tag VID	Untag VID	PVID
Mgmt		1	1
LAN		1	1
Primary		1	1
S-1		1	1
S-2		1	1
S-3		1	1
S-4		1	1
S-5		1	1
S-6		1	1
S-7		1	1
W-1		1	1
W-2		1	1
W-3		1	1
W-4		1	1
W-5		1	1
W-6		1	1
W-7		1	1
W-8		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

VLAN Mode : Static

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

VLAN ID (VID) VLAN Name

Port	Select All	Mgmt	LAN
Untag	All	☐	☐
Tag	All	☐	☐
Not Member	All	☐	☐

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	☐	☐	☐	☐	☐	☐	☐	☐
Tag	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☐	☐	☐	☐	☐	☐	☐	☐

WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	☐	☐	☐	☐	☐	☐	☐	☐
Tag	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☐	☐	☐	☐	☐	☐	☐	☐

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.

The screenshot shows the 'VLAN Settings' window with the 'PVID Setting' tab selected. At the top, 'VLAN Status' is set to 'Disable' and 'VLAN Mode' is 'Static'. Below this, 'PVID Auto Assign Status' is also set to 'Disable'. Three tables are present, each with a 'PVID' row where the value '1' is entered in every column.

Port	Mgmt	LAN
PVID	1	1

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

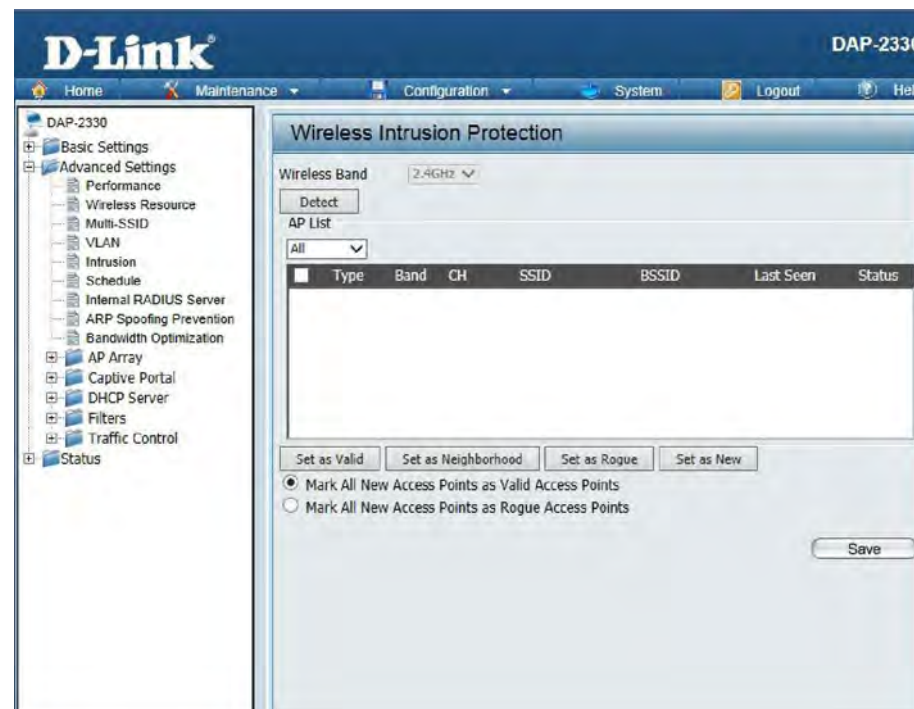
Intrusion

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 in default.

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

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



Schedule

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

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

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

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

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

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

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

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

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

D-Link DAP-2330 Wireless Schedule Settings

Wireless Schedule: Disable

Add Schedule Rule

Name:

Index: Primary SSID

SSID: dlink

Day(s): All Week Select Day(s)

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

All Day(s): ☐

Start Time: : (hour:minute, 24 hour time)

End Time: : (hour:minute, 24 hour time) Overnight

Schedule Rule List

Name	SSID Index	SSID	Day(s)	Time Frame	Wireless Edit	DEL

+: To the end time of the next day overnight.

Internal RADIUS Server

The DAP-2330 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 shows the D-Link DAP-2330 web interface. The left sidebar contains a tree view with categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multicast, 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 'Internal RADIUS Server'. It features an 'Add RADIUS Account' section with input fields for 'User Name', 'Password', and a 'Status' dropdown menu set to 'Enable'. Below this is a 'RADIUS Account list' table with columns for 'User Name', 'Enable', 'Disable', and 'Delete'. The table is currently empty. A 'Save' button is located at the bottom right of the configuration area.

ARP Spoofing Prevention

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

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

Gateway IP Address: Enter a gateway IP address.

Gateway MAC Address: Enter a gateway MAC address.

The screenshot displays the D-Link DAP-2330 web interface. The left sidebar shows a tree view of configuration options, with 'ARP Spoofing Prevention' selected under 'Advanced Settings'. The main content area is titled 'ARP Spoofing Prevention Settings'. It features a dropdown menu for 'ARP Spoofing Prevention' set to 'Disable'. Below this is the 'Add Gateway Address' section, which includes input fields for 'Gateway IP Address' and 'Gateway MAC Address' (formatted as six boxes separated by colons), and 'Add' and 'Clear' buttons. The 'Gateway Address List' section shows 'Total Entries: 0' and a 'Delete All' button. A table with columns 'Gateway IP Address', 'Gateway MAC Address', 'Edit', and 'Delete' is present but empty. A 'Save' button is located at the bottom right of the settings area.

Bandwidth Optimization

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

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

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

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

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

Add Clear

Bandwidth Optimization Rules

Band	Type	SSID Index	Downlink Speed	Uplink Speed	Edit	Del

Save

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

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-2330 AP array feature supports up to eight AP array members.



Configuration Settings

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

Enable AP Array Configuration: Select to **Enable** or **Disable** the AP array configure 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. Below this are five tabs: 'Wireless Basic Settings', 'Wireless Advanced Settings', 'Multiple SSID & VLAN', 'Advanced Functions', and 'Administration Settings'. Each tab has a small square icon next to it. At the bottom right of the window is a 'Save' button.

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 ☒			
Network Name (SSID)	☒	SSID Visibility	☒
Auto Channel Selection	☒	Channel Width	☒
Security	☒	Captive Profile	☒
Band	☒		

Wireless Advanced Settings

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

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

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

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

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

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

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

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

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

Connection Limit: 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 ☒			
SSID	☒	SSID Visibility	☒
Security	☒	WMM	☒
Captive Profile	☒	VLAN	☒

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

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 ☒			
System Name Settings	☒	SNMP Settings	☒
Login Settings	☒	Console Settings	☒
Limit Administrator	☒	Ping Control Setting	☒

Auto-RF

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

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

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. It has a title bar 'Auto-RF' and a light blue background. The settings are as follows:

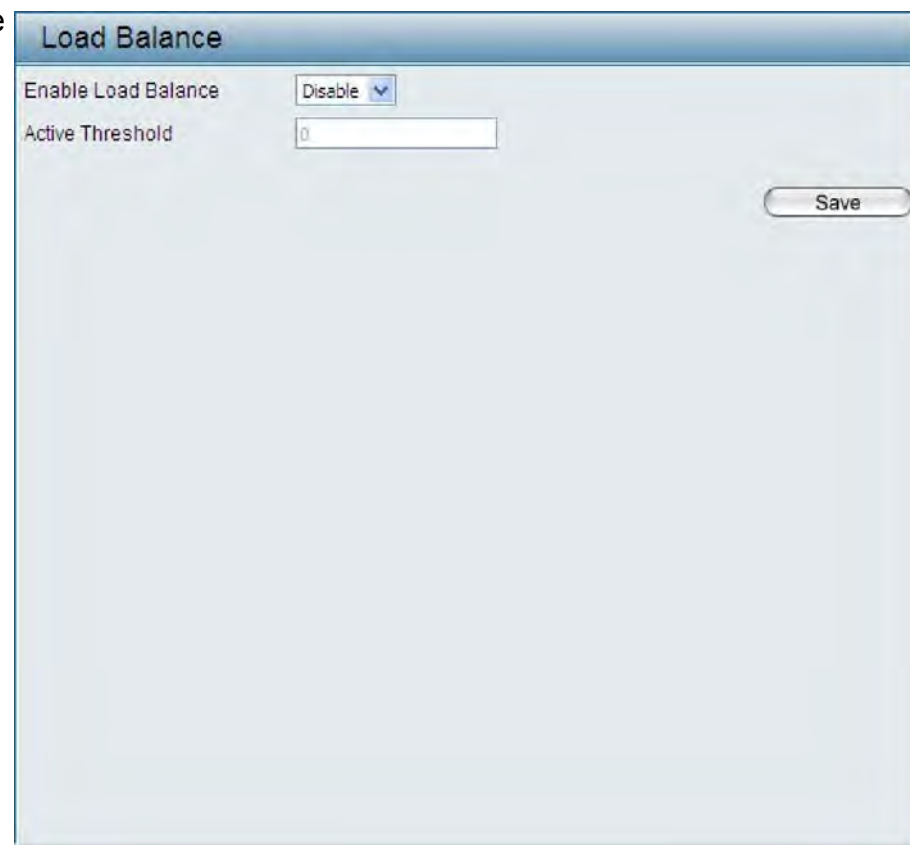
- Enable Auto-RF:** A dropdown menu set to 'Disable'.
- Initiate Auto-RF:** A yellow button labeled 'Auto-RF Optimize'.
- Auto-Initiate:** A dropdown menu set to 'Disable'.
- Auto-Initiate Period:** A text input field containing '24' followed by '(hours)'.
- RSSI Threshold:** A dropdown menu set to '40%'.
- RF Report Frequency:** A text input field containing '10' followed by '(Seconds)'.
- Save:** A rounded button at the bottom right.

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 web-based configuration window titled "Load Balance". Inside the window, there are two 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 - 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. Click the **Add** button to add a new entry. Click the **Delete** or **Delete All** button to remove a specific entry or all the entries configured.

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

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

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

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

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

Captive Portal Authentication

Encryption Type:

Passcode Settings

Passcode Quantity:

Duration: Hours

Last Active Day: Year Month Day

User Limit:

Passcode	Duration	Last Active Day	User Limit	Delete

Captive Profile	Edit	Delete

Authentication Settings - User Name/Password

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

Restricted Subnets: Enter the restricted subnets here. Access to these subnets will be denied to guest accounts. Up to four restricted subnet entries can be defined.

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Group: Select the group for the new account here. Options to choose from are **Manager** and **Guest**. Guest accounts will have limited access.

The screenshot shows the 'Captive Portal Authentication' configuration window. It includes sections for 'Encryption Type' (set to 'Username/Password'), 'Username/Password Settings', 'IP Filter Settings' (with four subnets), 'Username/Password Rule Settings' (with fields for Username, Password, and Group set to 'Manager'), and a table for 'Captive Profile'.

Username	Group	Edit	Delete

Captive Profile	Edit	Delete

Authentication Settings - Remote RADIUS

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

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

RADIUS Server: Enter the RADIUS server's IP address here. Enter

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

RADIUS Secret: RADIUS server's shared secret here. Select to

Accounting Mode: **Enable** or **Disable** the accounting mode here.

Accounting Server: Enter the accounting server's IP address here.

Accounting Port: Enter the accounting server's port number here.

Accounting Secret: Enter the accounting server's shared secret here.

The screenshot shows the 'Captive Portal Authentication' configuration window. It has a title bar and a main content area. The 'Encryption Type' is set to 'Remote RADIUS'. Below it, 'Remote RADIUS Settings' shows 'Remote RADIUS Type' as 'SPAP'. The 'Radius Server Settings' section includes fields for 'Radius Server' (empty), 'Radius Port' (1812), and 'Radius Secret' (empty). The 'Accounting Server Settings' section includes 'Accounting Mode' (Disable), 'Accounting Server' (empty), 'Accounting Port' (1813), and 'Accounting Secret' (empty). An 'Add' button is at the bottom right. A table at the bottom has columns 'Captive Profile', 'Edit', and 'Delete'.

Captive Profile	Edit	Delete
-----------------	------	--------

Authentication Settings - LDAP

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

The screenshot displays the 'Captive Portal Authentication' configuration window. At the top, the 'Encryption Type' is set to 'LDAP'. Below this, the 'LDAP Settings' section contains several fields: 'Server' (empty), 'Port' (389), 'Authenticate Mode' (Simple), 'Username' (empty), 'Password' (empty), 'Base DN' (ou=,dc=), 'Account Attribute' (ex.cn), and 'Identity' (empty). An 'Auto Copy' checkbox is located next to the 'Identity' field. An 'Add' button is positioned at the bottom right of the settings area. Below the settings, there is a table with three columns: 'Captive Profile', 'Edit', and 'Delete'. The table is currently empty.

Authentication Settings - POP3

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

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**.

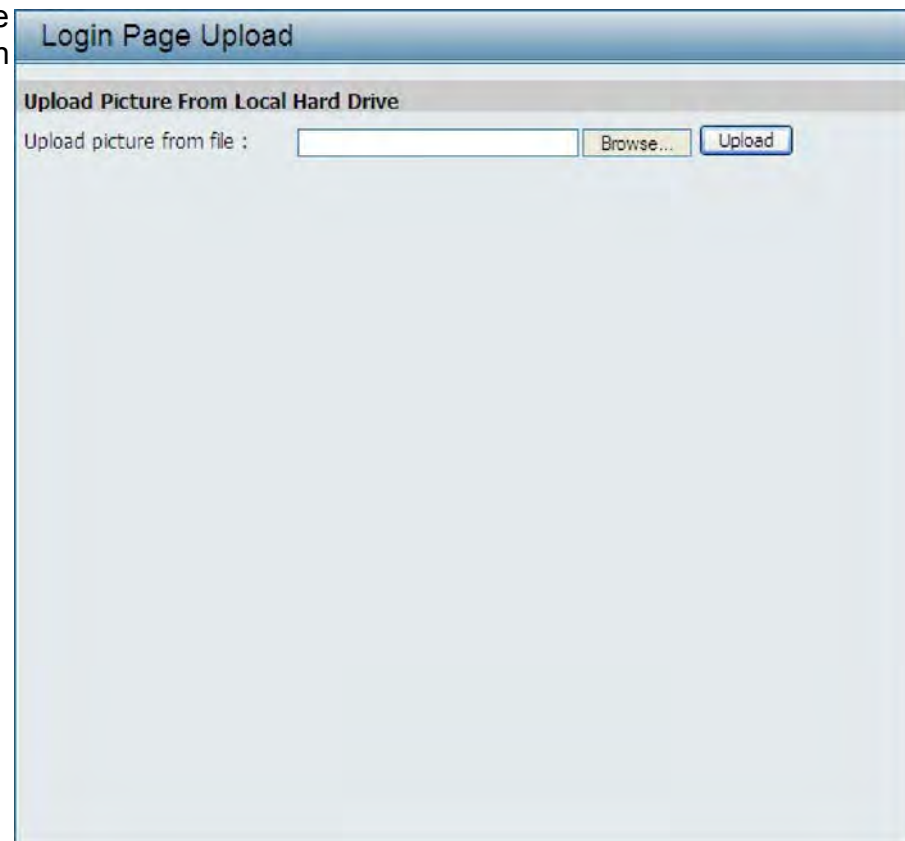
The screenshot shows the 'Captive Portal Authentication' configuration window. It features a title bar with the text 'Captive Portal Authentication'. Below the title bar, there are three main sections: 'Encryption Type' with a dropdown menu set to 'POP3', 'POP3 Settings' with fields for 'Server' (empty), 'Port' (set to '110'), and 'Connection Type' (dropdown set to 'None'), and an 'Add' button. At the bottom, there is a table with three columns: 'Captive Profile', 'Edit', and 'Delete'. The table is currently empty.

Captive Profile	Edit	Delete
-----------------	------	--------

Login Page Upload

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

Upload picture from file: In this field the path to the image file, that will be uploaded, will be displayed. Alternatively, the path can be manually entered here.



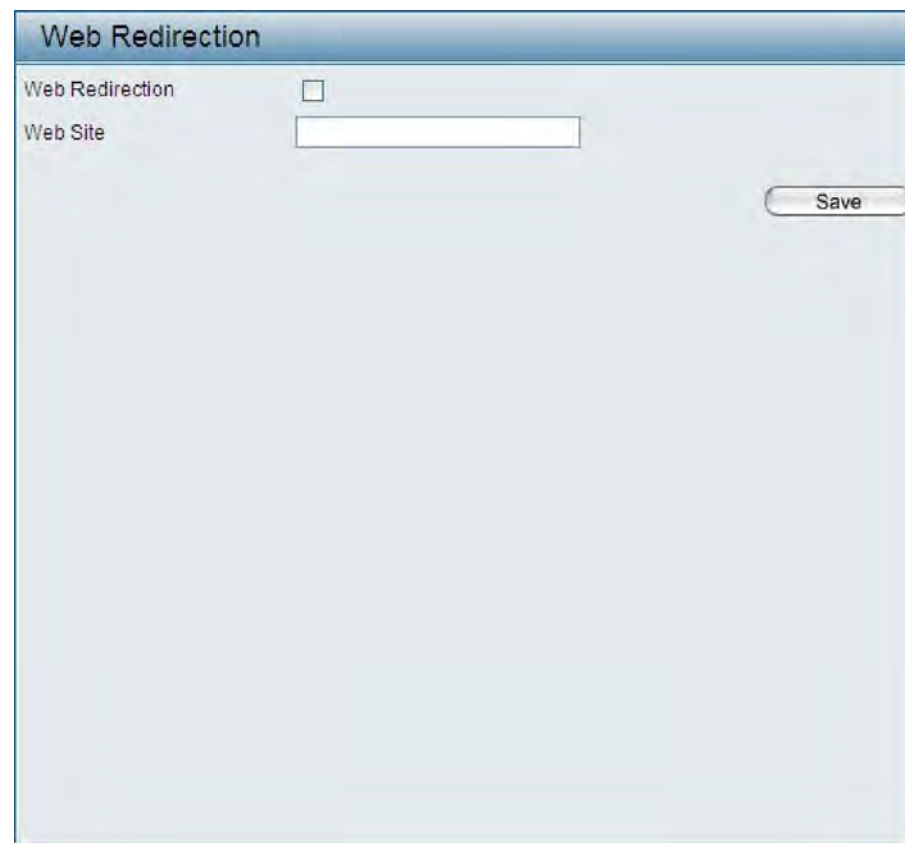
The screenshot shows a web-based configuration window titled "Login Page Upload". Inside the window, there is a section titled "Upload Picture From Local Hard Drive". Below this title, there is a text input field labeled "Upload picture from file :". To the right of the input field are two buttons: "Browse..." and "Upload". The "Browse..." button is highlighted with a yellow border. The rest of the window is a large, empty light blue area.

Web Redirection

In this window, users can view and configure the Web redirection settings for the captive portal hosted by this access point. Wireless clients will be redirected to this web site prior and after authentication. Click the **Save** button to accept the changes made.

Web Redirection: Select this checkbox to enable the Web redirection feature.

Web Site: Enter the destination web site's address here.

A screenshot of a web configuration window titled "Web Redirection". The window has a light blue header bar with the title. Below the header, there are two labels: "Web Redirection" and "Web Site". The "Web Redirection" label is followed by an unchecked checkbox. The "Web Site" label is followed by a text input field. In the bottom right corner of the window, there is a "Save" button.

Web Redirection

Web Redirection ☐

Web Site

Save

DHCP Server

Dynamic Pool Settings

The DHCP address pool defines the range of the IP address that can be assigned to stations in the network. A Dynamic Pool allows wireless stations to receive an available IP with lease time control. If needed or required in the network, the DAP-2330 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-2330 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-2330 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.

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.

The screenshot shows the 'Wireless MAC ACL Settings' web interface. At the top, there's a title bar. Below it, the 'Wireless Band' is set to '2.4GHz'. The 'Access Control List' is set to 'Accept'. There's a 'MAC Address' input field with an 'Add' button. Below this is a table with columns 'ID', 'MAC Address', and 'Delete'. The table is currently empty. Underneath is a section titled 'Current Client Information' containing a table with columns 'MAC Address', 'SSID', 'Band', 'Authentication', 'Signal', and 'Add'. The table has one entry: MAC Address '00:1F:3B:AD:35:0B', SSID 'dlink', Band 'N', Authentication 'OPEN', Signal '98%', and an 'Add' checkbox. At the bottom, there are sections for 'Upload ACL File' (with 'Upload File' and 'Browse...' buttons) and 'Download ACL File' (with a 'Download' button). A 'Save' button is at the very bottom right.

ID	MAC Address	Delete

MAC Address	SSID	Band	Authentication	Signal	Add
00:1F:3B:AD:35:0B	dlink	N	OPEN	98%	☐

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	☒ Enable	☐ Disable	☐ Guest mode
Multi-SSID 1	☒ Enable	☐ Disable	☐ Guest mode
Multi-SSID 2	☒ Enable	☐ Disable	☐ Guest mode
Multi-SSID 3	☒ Enable	☐ Disable	☐ Guest mode
Multi-SSID 4	☒ Enable	☐ Disable	☒ Guest mode
Multi-SSID 5	☒ Enable	☐ Disable	☒ Guest mode
Multi-SSID 6	☒ Enable	☐ Disable	☐ Guest mode
Multi-SSID 7	☒ Enable	☐ Disable	☒ Guest mode
<div>Save</div>			

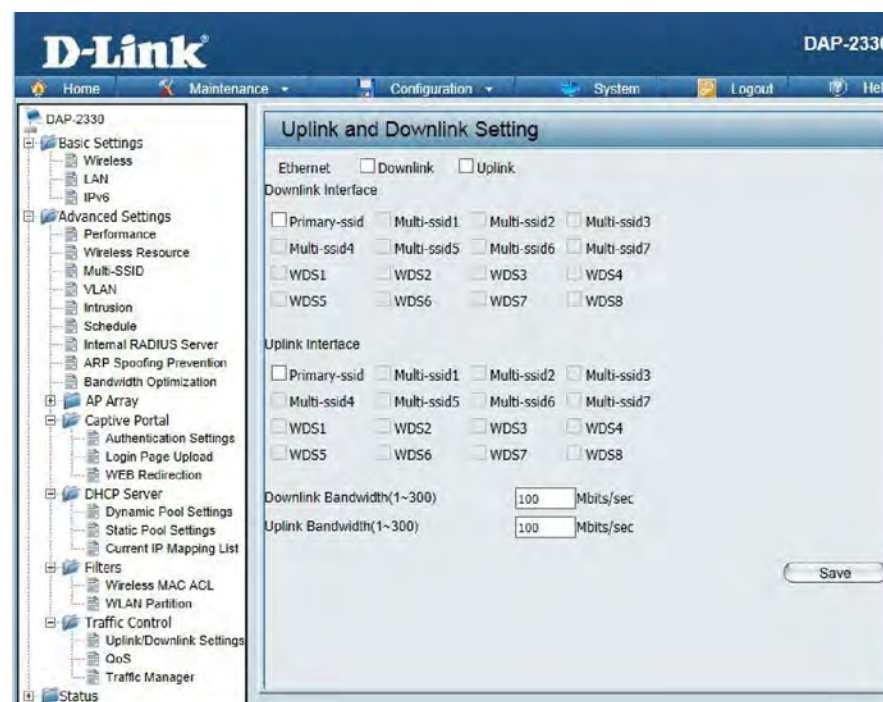
Traffic Control

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-2330 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. At the top, there is a title bar 'QoS'. Below it, a checkbox labeled 'Enable QoS' is checked. The main section is titled 'Advanced QoS'. It contains several settings:

- Downlink Bandwidth:** A text box with '100' and a label 'Mbits/sec'.
- Uplink Bandwidth:** A text box with '100' and a label 'Mbits/sec'.
- ACK/DHCP/ICMP/DNS Priority:** A dropdown menu set to 'Highest Priority', a 'Limit' text box with '100', and a '% Port' text box with '53,67,68,546,547'.
- Web Traffic Priority:** A dropdown menu set to 'Third Priority', a 'Limit' text box with '100', and a '% Port' text box with '80,443,3128,8080'.
- Mail Traffic Priority:** A dropdown menu set to 'Second Priority', a 'Limit' text box with '100', and a '% Port' text box with '25,110,465,995'.
- Ftp Traffic Priority:** A dropdown menu set to 'Low Priority', a 'Limit' text box with '100', and a '% Port' text box with '20,21'.
- User Defined-1 Priority:** A dropdown menu set to 'Highest Priority', a 'Limit' text box with '100', and a '% Port' text box with '0' and a range selector '- 0'.
- User Defined-2 Priority:** A dropdown menu set to 'Second Priority', a 'Limit' text box with '100', and a '% Port' text box with '0' and a range selector '- 0'.
- User Defined-3 Priority:** A dropdown menu set to 'Third Priority', a 'Limit' text box with '100', and a '% Port' text box with '0' and a range selector '- 0'.
- User Defined-4 Priority:** A dropdown menu set to 'Low Priority', a 'Limit' text box with '100', and a '% Port' text box with '0' and a range selector '- 0'.
- Other Traffic Priority:** A dropdown menu set to 'Low Priority', a 'Limit' text box with '100', and a '% Port' text box with '0'.

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

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.

The screenshot shows the 'Traffic Manager' configuration window. At the top, there's a title bar 'Traffic Manager'. Below it, the 'Traffic Manager' status is set to 'Disable' with a dropdown arrow. The 'Unlisted Clients Traffic' section has two radio buttons: 'Deny' (unselected) and 'Forward' (selected). Below these are two input fields for 'Downlink Bandwidth' and 'Uplink Bandwidth', both set to '100' Mbits/sec. The 'Add Traffic Manager Rule' section contains five input fields: 'Name', 'Client IP(optional)', 'Client MAC(optional)', 'Downlink Speed', and 'Uplink Speed', each followed by a unit 'Mbits/sec'. There are 'Add' and 'Clear' buttons at the bottom of this section. The 'Traffic Manager Rules' section features a table with columns: 'Name', 'Client IP', 'Client MAC', 'Downlink Speed', 'Uplink Speed', 'Edit', and 'Del'. A 'Save' button is located at the bottom right of the window.

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.

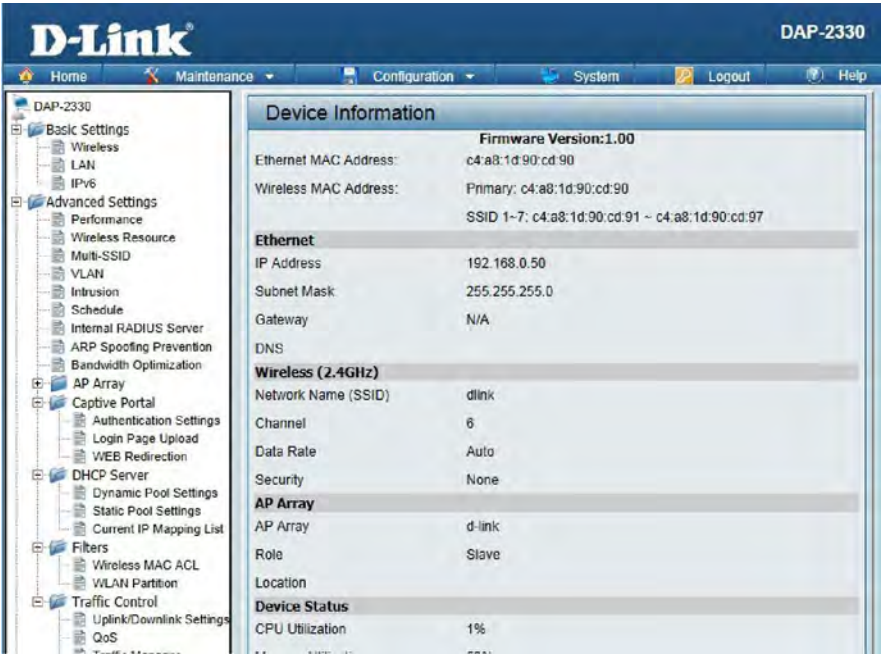
The screenshot displays the D-Link DAP-2330 web interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of the configuration menu, with the 'Status' section expanded. The main content area displays the 'Device Information' page, which includes the following sections:

- Device Information**
 - Firmware Version: 1.00
 - Ethernet MAC Address: c4:a8:1d:90:cd:90
 - Wireless MAC Address: Primary: c4:a8:1d:90:cd:90
 - SSID 1~7: c4:a8:1d:90:cd:91 ~ c4:a8:1d:90:cd:97
- 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: 6
 - Data Rate: Auto
 - Security: None
- AP Array**
 - AP Array: d-link
 - Role: Slave
 - Location
- Device Status**
 - CPU Utilization: 1%
 - Memory Utilization: 52%
- Central WiFiManager**
 - Connection Status: Disconnect
 - Server IP
 - Service Port
 - Live Port

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-2330, including the firmware version and the device's MAC address.



Client Information

This page displays the associated clients SSID, MAC, band, authentication method, signal strength, and power saving mode for the DAP-2330 network.

Client Information: This window displays the wireless client information for clients currently connected to the DAP-2330.

SSID: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

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

Authentication: Displays the type of authentication being used.

RSSI: Displays the client's signal strength.

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



Client Information	Station association (2.4GHz) : 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-2330's Wireless Distribution System network.

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DAP-2330.

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

Status: Displays the status of the power saving feature.

WDS Information				
WDS Information		Channel : 6 (2.437 GHz)		
Name	MAC	Authentication	Signal	Status

Channel Analyze

Wireless Band: Select 2.4GHz in default.

Detect: Click the Detect button to scan.

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

The screenshot shows a web interface titled "Channel Analyze". It features a "Wireless Band" dropdown menu set to "2.4GHz" and a "Detect" button. Below these is a "Wireless Summary" section containing an "AP List" table. The table has five columns: "CH", "AP Num", "MRssi(%)", "ARssi(%)", and "Evaluation". The table is currently empty. At the bottom of the interface, a note states: "* There are only three non-overlapped channels in 2.4G band, respectively 1,6 and 11."

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

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.

WLAN Traffic Statistics

Clear

Refresh

Transmitted Count

Transmitted Packet Count

Transmitted Bytes Count

Dropped Packet Count

Transmitted Retry Count

Received Count

Received Packet Count

Received Bytes Count

Dropped Packet Count

Received CRC Count0

Received Decryption Error Count

Received MIC Error Count

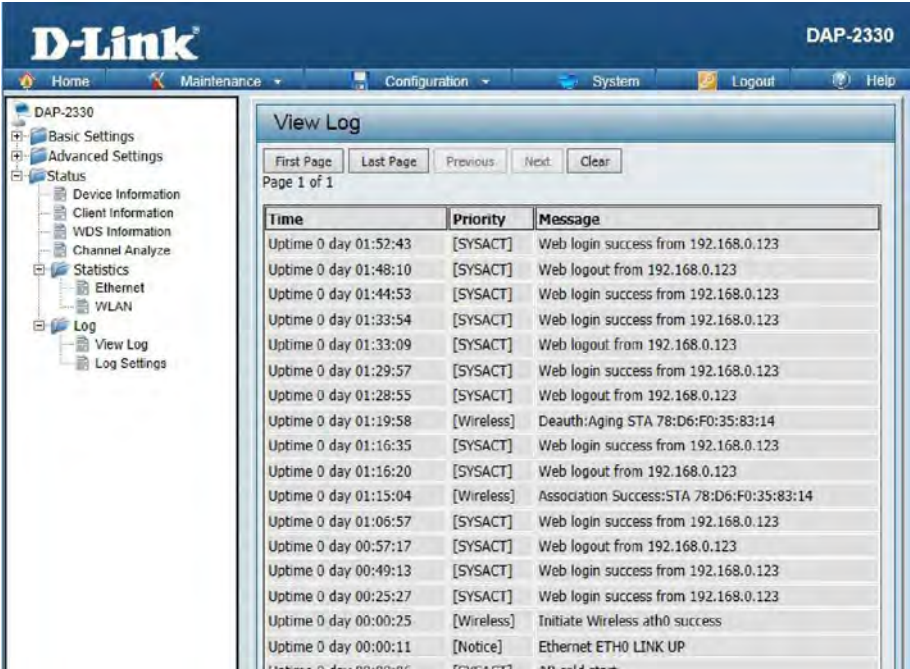
Received PHY Error Count

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.



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-2330 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.

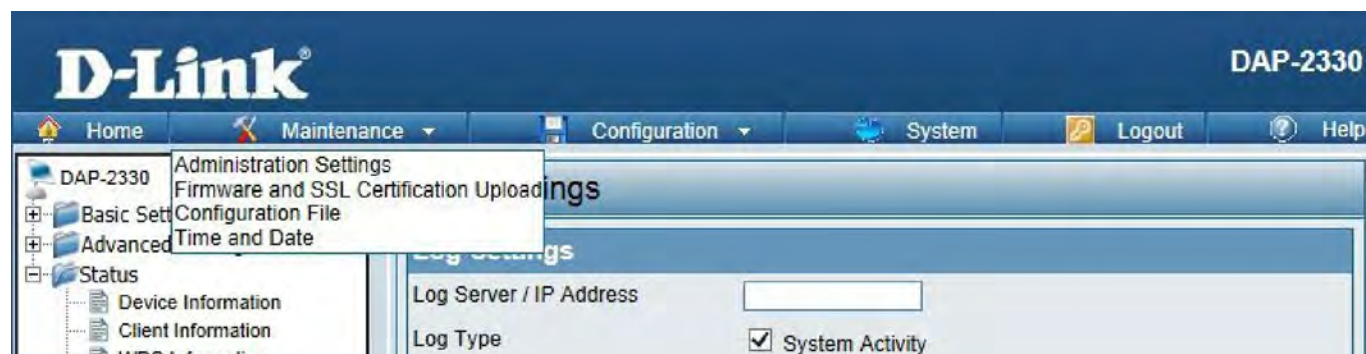
The screenshot shows the D-Link DAP-2330 web interface. The top navigation bar includes Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view with categories like Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Channel Analyze, Statistics, Ethernet, WLAN, Log, View Log, and Log Settings. The main content area is titled 'Log Settings' and contains three sections:

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

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

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

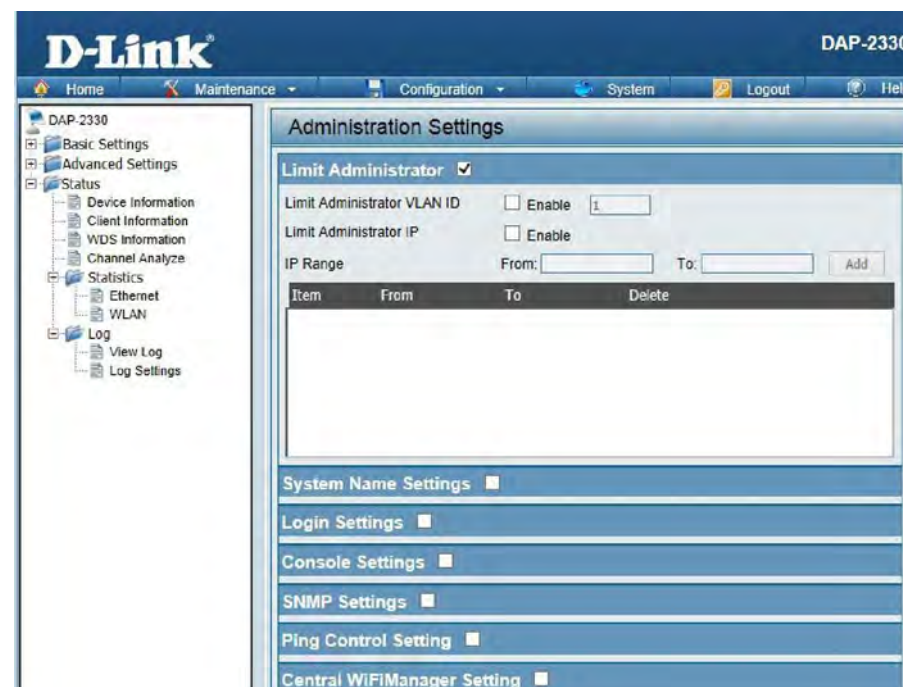
Limit Administrator

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 then 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-2330.

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

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.

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.

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.



The screenshot shows a web-based configuration interface for SNMP settings. The title bar is blue with the text "SNMP Settings" and a green checkmark icon. Below the title bar, there are five rows of settings:

Setting	Value
Status	☐ Enable
Public Community String	public
Private Community String	private
Trap Status	☐ Enable
Trap Server IP	

Administration

Central WiFiManager Settings

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

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



The image shows a web interface for 'Central WiFiManager Setting'. It features a blue header bar with the title and a checkmark icon. Below the header, there is a light blue box containing the text 'Enable Central WiFiManager' followed by a dropdown menu. The dropdown menu is currently set to 'Disable' and has a small downward arrow icon.

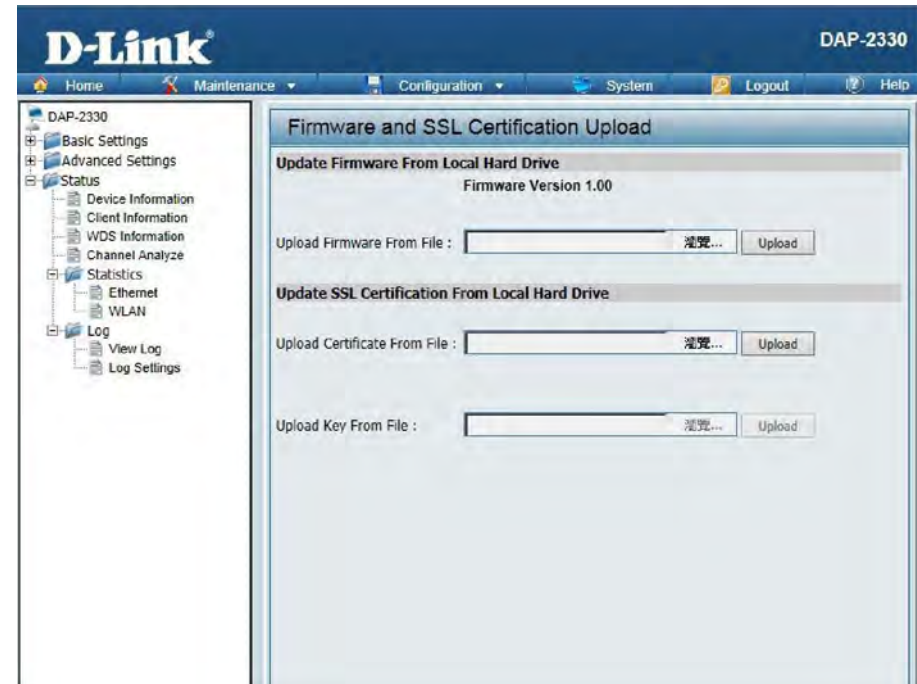
Firmware and SSL Upload

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.



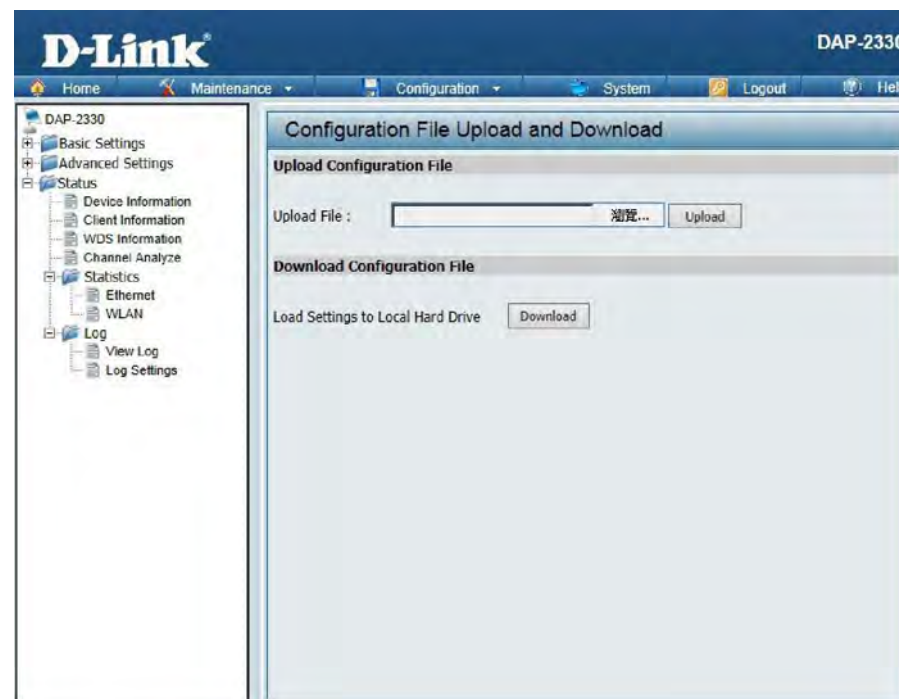
Configuration File Upload

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-2330 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.

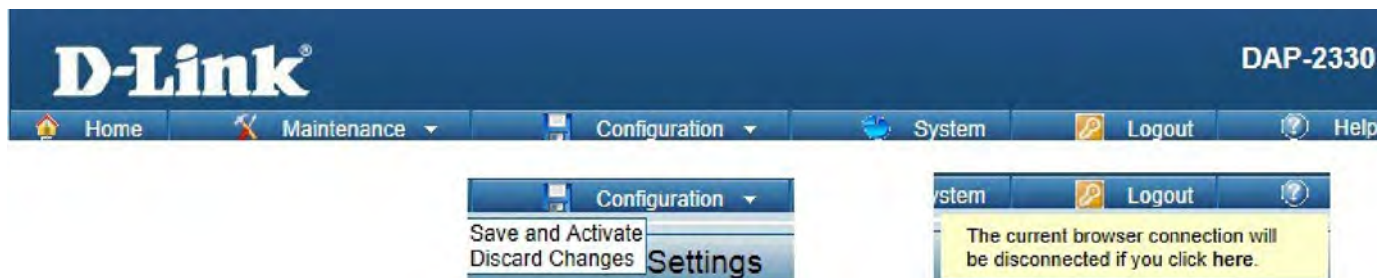
Daylight Saving Dates: Use the drop-down menu to select the correct Daylight Saving offset.

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-2330 web interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. A left sidebar shows a tree view of configuration options: Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Channel Analyze, Statistics, Ethernet, WLAN, Log, View Log, and Log Settings. The main content area is titled 'Time and Date Settings' and contains three sections: 'Time Configuration' showing the current time as 01/01/1970 02:02:25; 'Automatic Time Configuration' with checkboxes for 'Enable NTP Server' and 'Enable Daylight Saving', an 'NTP Server' text field, and a 'Time Zone' dropdown menu currently set to '(GMT+08:00) Ulaan Bataar'; and 'Set the Date and Time Manually' with input fields for Year (2014), Month (Apr), Day (21), Hour (17), Minute (9), and Second (36), along with a 'Copy Your Computer's Time Settings' button. A 'Save' button is located at the bottom right of the configuration area.

Configuration and System

These options are the remaining options 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.



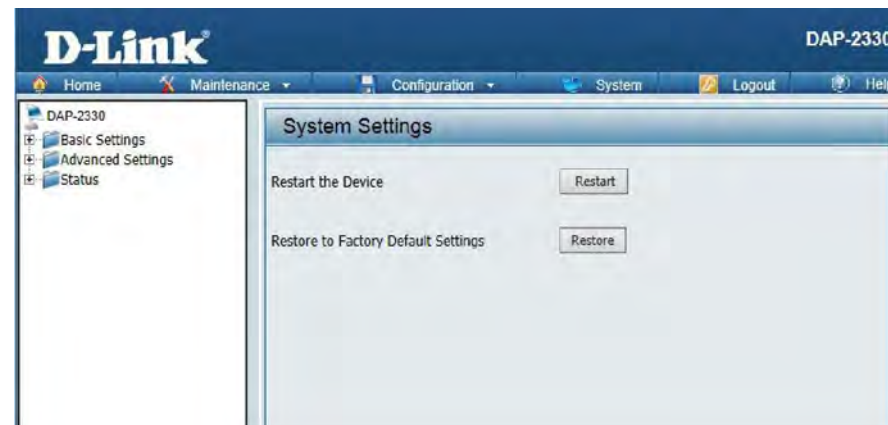
System Settings

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-2330.

Restore to Factory Default Settings: Click Restore to restore the DAP-2330 back to factory default settings.

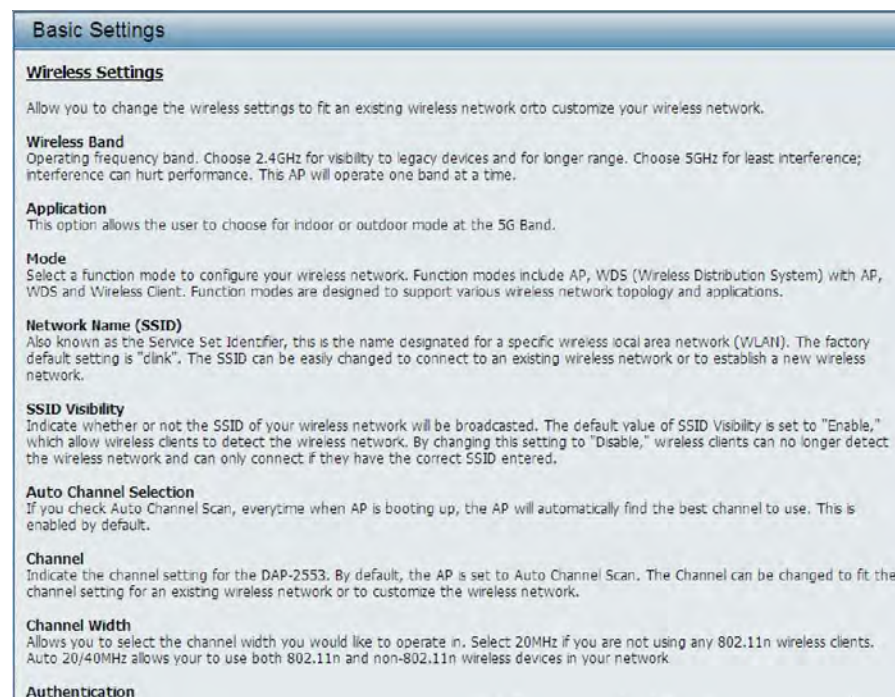
Clear Language Pack: Click to clear the current Language pack running.



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.



Knowledge Base

Wireless Basics

D-Link wireless products are based on industry standards to provide high-speed wireless connectivity that is easy to use within your home, business or public access wireless networks. D-Link wireless products provides you with access to the data you want, whenever and wherever you want it. Enjoy the freedom that wireless networking can bring to you.

WLAN use is not only increasing in both home and office environments, but in public areas as well, such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are allowing people to work and communicate more efficiently. Increased mobility and the absence of cabling and other types of fixed infrastructure have proven to be beneficial to many users.

Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards, allowing wireless users to use the same applications as those used on a wired network.

People use WLAN technology for many different purposes:

- **Mobility** - productivity increases when people can have access to data in any location within the operating range of their WLAN. Management decisions based on real-time information can significantly improve the efficiency of a worker.
- **Low implementation costs** - WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLAN's ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.
- **Installation and network expansion** - by avoiding the complications of troublesome cables, a WLAN system can be fast and easy during installation, especially since it can eliminate the need to pull cable through walls and ceilings. Wireless technology provides more versatility by extending the network beyond the home or office.
- **Inexpensive solution** - wireless network devices are as competitively priced as conventional Ethernet network devices. The DAP-2330 saves money by providing users with multi-functionality configurable in four different modes.
- **Scalability** - Configurations can be easily changed and range from Peer-to-Peer networks, suitable for a small number of users to larger Infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Wireless Installation Considerations

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

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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2330. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

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

What can I do if I forgot my password?

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

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

How to check your IP address?

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

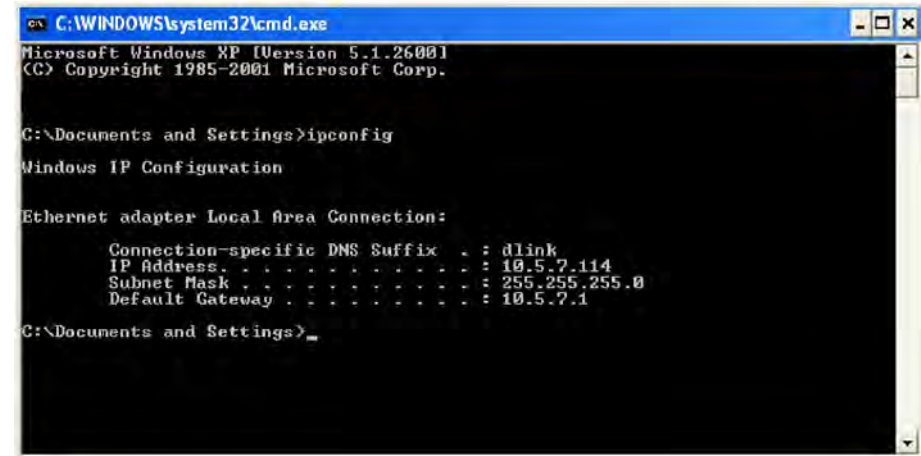
Click on Start > Run. In the run box type cmd and click OK.

At the prompt, type ipconfig and press Enter.

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

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

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . . : 10.5.7.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>
```

How to statically assign an IP address?

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

Step 1:

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

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

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

Step 2:

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

Step 3:

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

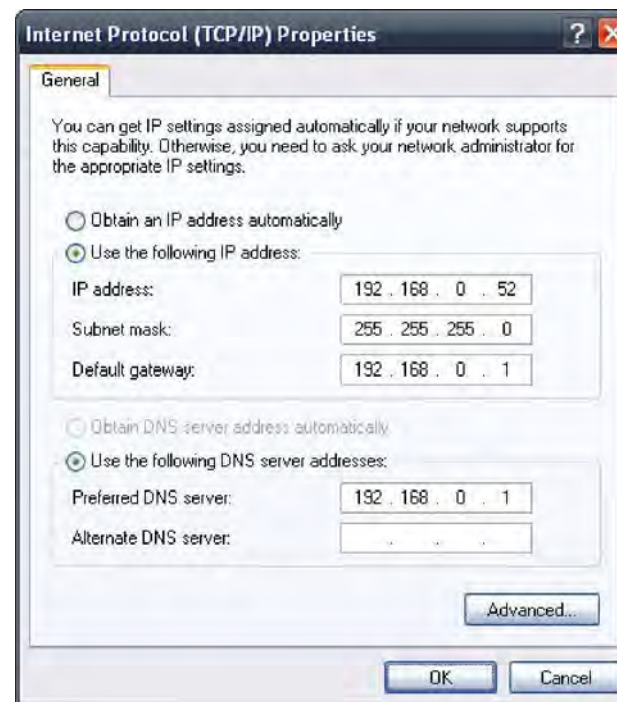
Step 4:

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

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

Step 5:

Click OK twice to save your settings.



Technical Specifications

Standards

- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3b
- IEEE 802.3af
- IEEE 802.3x

Network Management

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

Security

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

Wireless Frequency Range

- 2.4 to 2.4835 GHz

Operating Voltage

- 48V DC +/- 10% for PoE or 12V/1A

LEDs

- Power/Status

Temperature

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

Humidity

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

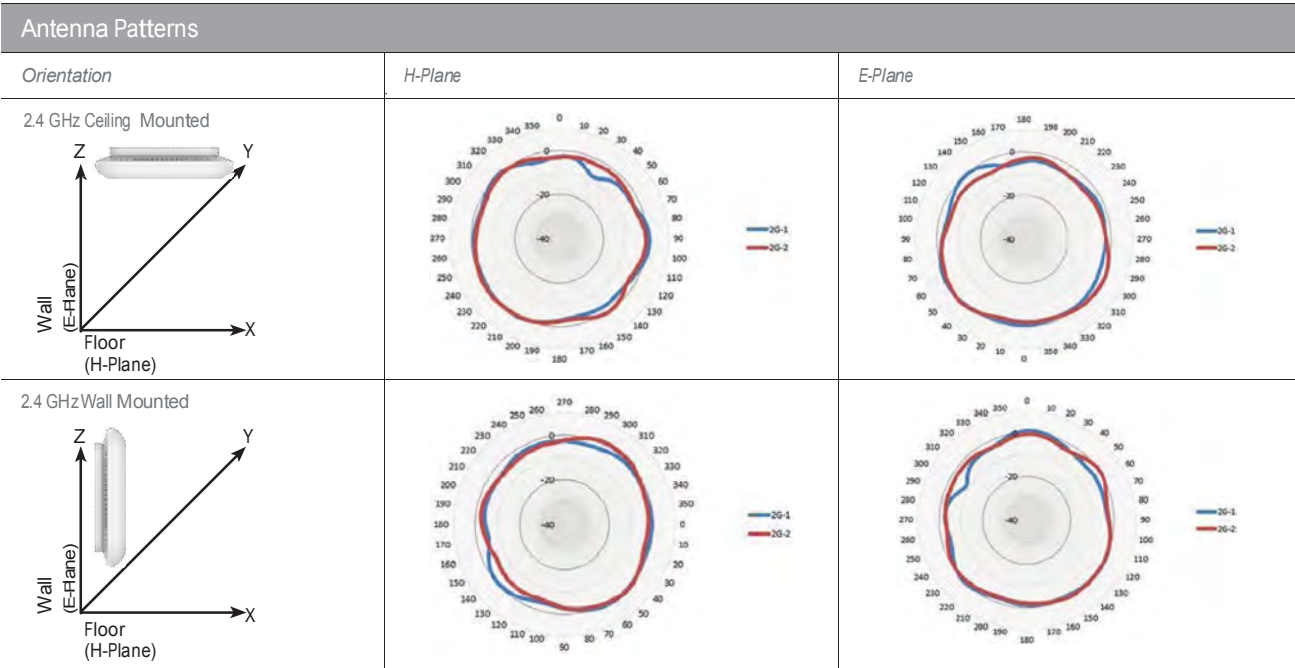
Certifications

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

Dimensions

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

Antenna Pattern



Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DAP-2330)
- Hardware Revision (located on the label on the device (e.g. rev A1))
- Serial Number (s/n number located on the label on the device).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

For customers within the United States:

Phone Support:

(877) 453-5465

Internet Support:

<http://support.dlink.com>

For customers within Canada:

Phone Support:

(800) 361-5265

Internet Support:

<http://support.dlink.ca>

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by DLink in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim:

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support (USA 1-877-453-5465 or Canada 1-800-361-5265), who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form. Enter the assigned Case ID Number at <https://rma.dlink.com/> (USA only) or <https://rma.dlink.ca> (Canada only).

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc.
- **USA residents** send to 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.
- **Canadian residents** send to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming. RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

What Is Not Covered:

The Limited Warranty provided herein by D-Link does not cover:

Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks:

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

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any

derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright ©2011 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Federal Communication Commission Interference Statement

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

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

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.

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.

802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Appendix E - Warranty

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

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

Industry Canada Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

- 1) this device may not cause interference and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

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

Caution:

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

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

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

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

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Registration

Register your product online at registration.dlink.com



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

Version 1.0
May 12, 2014