

NUCLIAS CONNECT DIS-2650AP User Guide

V 1.00

Table of Contents

Nuclias Connect	4	Wired Equivalent Privacy (WEP)	24
Introduction	4	Wi-Fi Protected Access (WPA / WPA2).....	25
Nuclias Connect Key Features.....	5	LAN	27
Package Contents.....	6	IPv6	28
System Requirements	6	Advanced Settings	29
Hardware Overview	7	Performance	30
Front Panel	7	Wireless Resource Control	32
Side Panel	7	Multi-SSID.....	34
Basic Installation.....	8	VLAN.....	36
Hardware Setup	8	VLAN List.....	36
Mounting the Device on a Wall	8	Port List.....	37
Installing the Device on a DIN Rail	9	Add/Edit VLAN	38
Installing the Device into a Rack	10	PVID Settings.....	39
Grounding the Device.....	11	Intrusion.....	40
Powering the Device	11	Schedule	41
Using the Terminal Connections.....	11	Internal RADIUS Server	42
Connecting Devices.....	13	ARP Spoofing Prevention	43
Setup Wizard	15	Bandwidth Optimization	44
Web User Interface	16	Hotspot 2.0.....	46
Wireless	17	Hotspot.....	46
Access Point Mode	17	Interworking.....	47
WDS with AP Mode	19	WAN Metrics	48
WDS Mode	21	LIST.....	49
Wireless Client Mode	23	OSU	50
Wireless Security	24	Captive Portal.....	52
		Authentication Settings-Web Redirection Only	52
		Authentication Settings- Username/Password..	54

Authentication Settings- Passcode	56	Administration.....	84
Authentication Settings- Remote RADIUS.....	58	Limit Administrator.....	84
Authentication Settings- LDAP.....	60	System Name Settings.....	85
Authentication Settings- POP3.....	62	Login Settings	85
Login Page Upload	64	Console Settings	86
MAC Bypass.....	65	Ping Control Settings	86
DHCP Server	66	LED Settings.....	86
Dynamic Pool Settings.....	66	Country Settings	86
Static Pool Setting	67	DDP Settings	87
Current IP Mapping List.....	68	Nuclias Connect Settings.....	87
Filters.....	69	Firmware and SSL Upload.....	88
Wireless MAC ACL	69	Configuration File Upload	89
IP Filter Settings.....	70	Time and Date Settings	90
WLAN Partition	71	Configuration and System.....	91
Traffic Control.....	72	System Settings.....	92
Uplink/Downlink Setting	72	Help	93
QoS.....	73	Knowledge Base	94
Traffic Manager.....	74	Wireless Basics	94
Status	75	Wireless Installation Considerations.....	95
Device Information	76	Troubleshooting	96
Client Information	77	Why can't I access the web-based configuration utility?	96
WDS Information Page	78	What can I do if I forgot my password?.....	96
Statistics.....	79	How to check your IP address?	97
Ethernet Traffic Statistics.....	79	How to statically assign an IP address?.....	98
WLAN Traffic Statistics.....	80	Technical Specifications	99
Log	81	Antenna Patterns	100
View Log.....	81		
Log Settings.....	82		
Maintenance Section	83		

Nuclias Connect

Introduction

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

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

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

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

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

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

Nuclias Connect Key Features

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

For more information on how to use Nuclias Connect with DIS-2650AP, please refer to the Nuclias Connect User Guide.

Package Contents

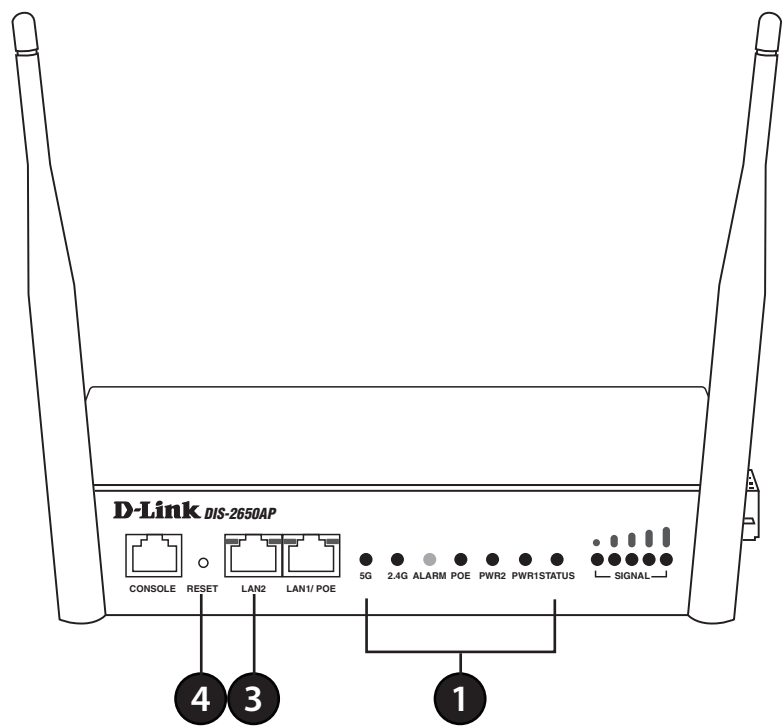
- DIS-2650AP
- Quick Installation Guide
- DIN rail mounting kit
- 4 installation screws (3 x 7 mm)
- Bracket

System Requirements

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

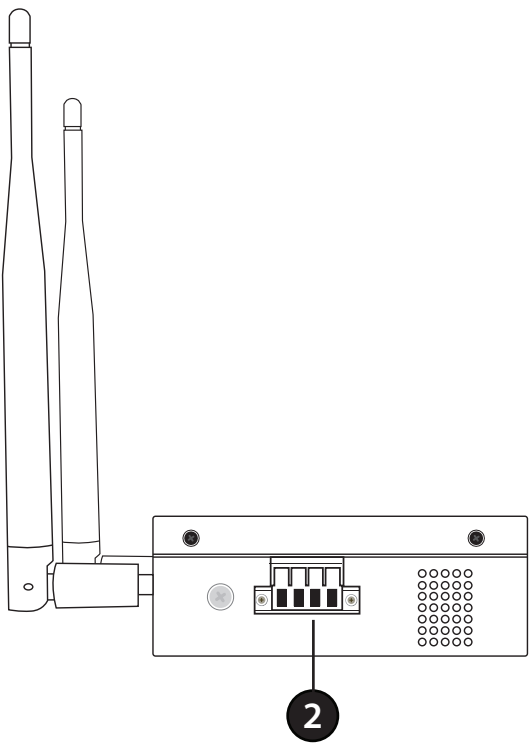
Hardware Overview

Front Panel



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 DIS-2650AP is working properly.

Side Panel



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.

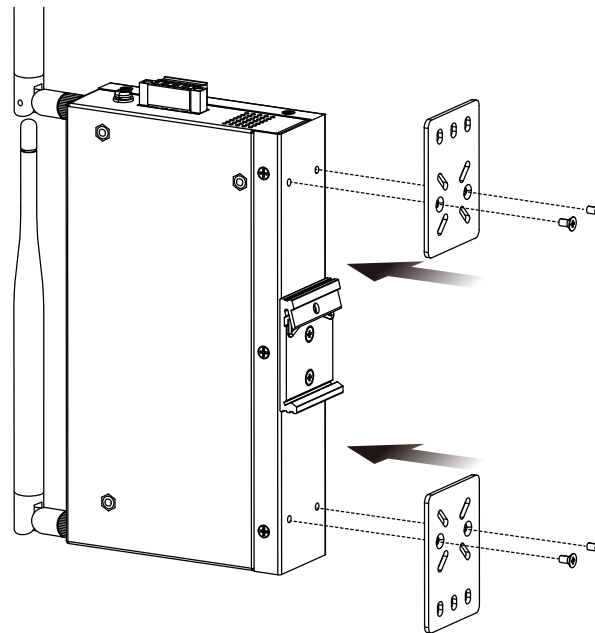
Basic Installation

Hardware Setup

Mounting the Device on a Wall

The DIS-2650AP can be installed on a solid surface by using the included wall mounting plates attached to the back of the device. Use the following instructions to install the DIS-2650AP on a wall:

1. Align the cross-section of the mounting plates with the openings on the back of the device. Secure the plates with the included mounting screws.



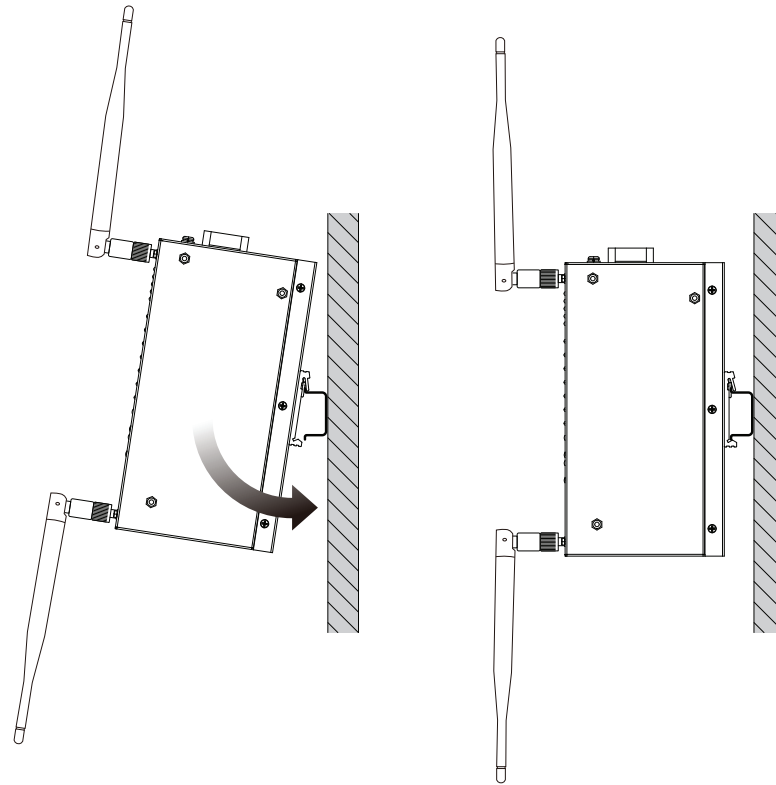
2. Remove the DIN rail mounting clip from the back of the device (if present).
3. Place the mounting brackets (attached to the device) on the location where you want to mount it, and use the brackets as a guide to mark where to drill the screw holes.
4. Drill holes on the marks and insert wall anchors appropriate for the material of the wall.
5. Align the device with the wall anchors and secure it to the wall using appropriate screws for the wall anchors.

Installing the Device on a DIN Rail

The DIS-2650AP can be mounted on a standard DIN rail using the included DIN mounting kit.

Use the following instructions to install the DIS-2650AP on a rail:

1. Check that the DIN rail is installed properly using at least two screws on each end.
2. Fasten the DIN mounting clip to the rear panel of the device using the included mounting screws.

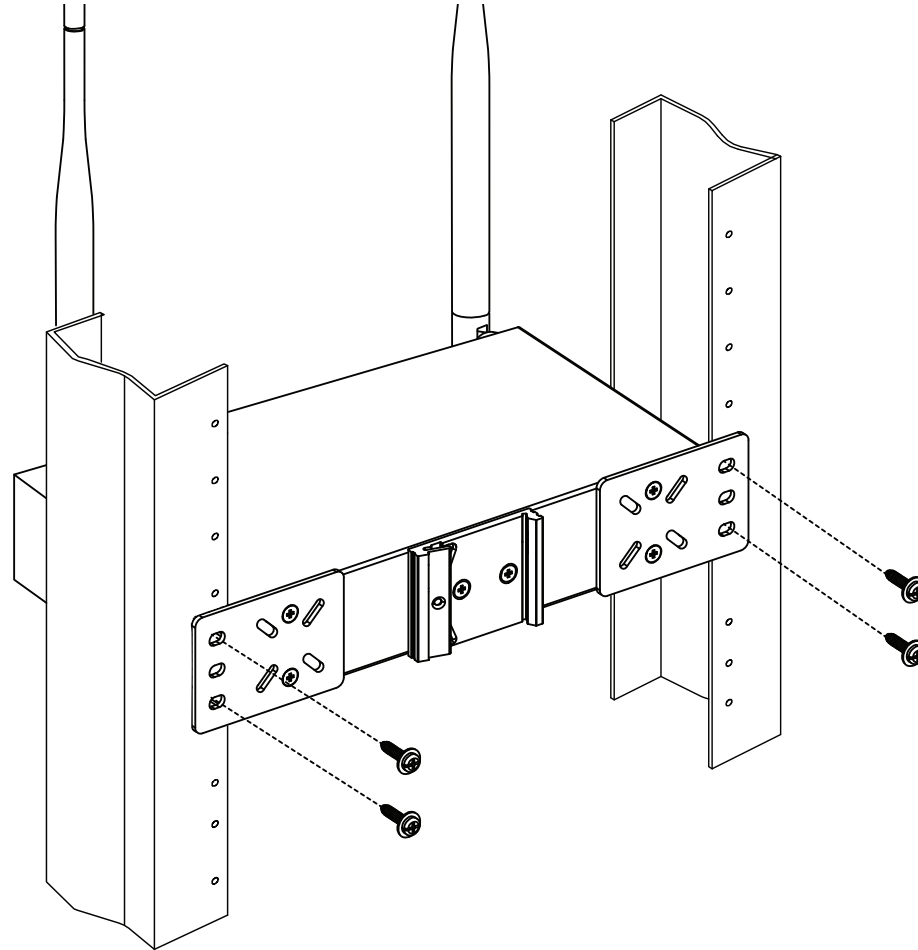


3. Position the DIS-2650AP against the rail, then tilt it upwards and hook the DIN rail clip on the back of the device against the rail. Snap the device into place to complete the installation.

Installing the Device into a Rack

The DIS-2650AP can be mounted on a standard rack using the included mounting plates. To install the device on a rack:

1. Attach the mounting brackets to the rear panel of the device using the provided installation screws.



2. Use the provided screws to attach the two rear mounting plates to the rack.

Grounding the Device

To use the DIS-2650AP safely, it needs to be grounded. Please complete these steps before powering on the device.

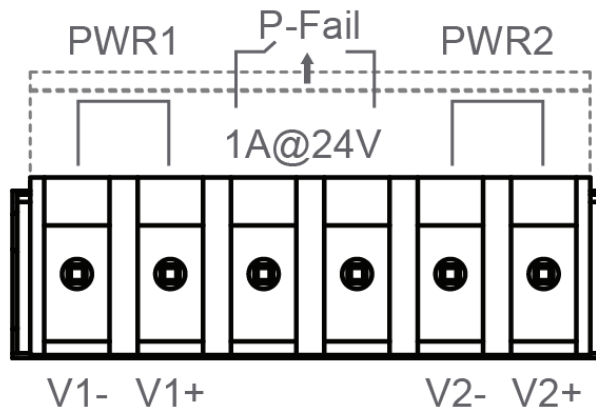
1. Remove the grounding screw from the top of the DIS-2650AP and place the grounding cable lug ring on top of the grounding screw opening.
2. Insert the grounding screw back into the grounding screw opening and use a screwdriver to tighten the grounding screw, securing the grounding cable to the DIS-2650AP.
3. Attach the terminal lug ring at the other end of the grounding cable to an appropriate grounding source.

Powering the Device

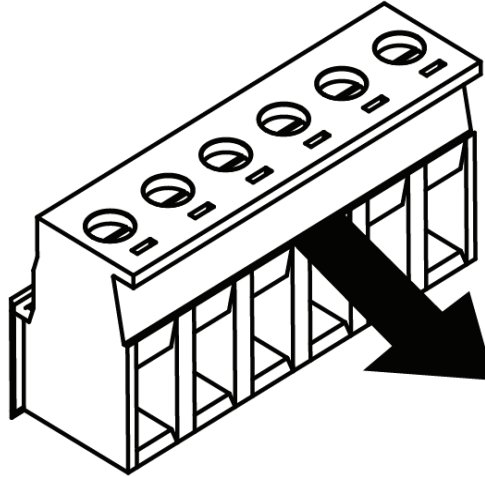
The DIS-2650AP can be powered with an 802.3at PoE source or by using the built-in terminal adapter. This allows dual power inputs using wires from the power source(s) to be screwed into the terminal connections.

Using the Terminal Connections

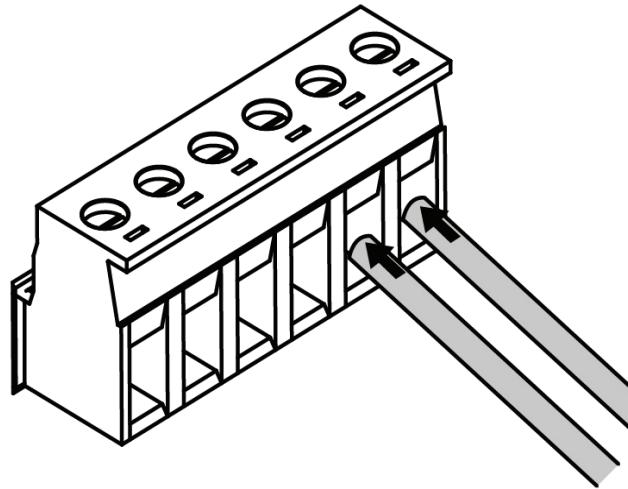
1. Before continuing, consult the diagram below to decide which wires from the power source need to connect to which contacts on the terminal block. Note that two power sources can be used; one inserted into V1-/V1+ (labeled PWR 1) and the other inserted into V2-/V2+ (labeled PWR2).



2. Use a lever to remove the terminal block from the switch.



3. Use a flat head screwdriver to unscrew the terminal connections that you wish to use.
4. Insert the wires into the terminal connection and use the screwdriver to tighten the screws to secure the wires.



5. Re-insert the terminal block into the socket on the device.

Connecting Devices

The Ethernet port can be connected to an end device. Use a standard Category 5/5e/6 RJ-45 Ethernet cable to connect the end device to the DIS-2650AP.

The port will auto-negotiate to the highest possible port speed based on the connected device.

To set up and manage the DIS-2650AP, use one of the following methods:

1. Connect the access point and your computer to the same PoE switch. Manage the access point from the computer.
Enter ***dis2650ap.local*** in the address field of your browser.
Log in to the Administration user interface. The default login information is:
Username: admin
Password: admin
2. Connect the access point and your computer via DPE-311GI PoE injector. Manage the access point from the computer.
Enter ***dis2650ap.local*** in the address field of your browser.
Log in to the Administration user interface. The default login information is:
Username: admin
Password: admin
3. Connect the access point and your computer to the same network switch. Manage the access point from the computer.
Enter ***dis2650ap.local*** in the address field on your browser.
Log in to the Administration user interface. The default login information is:
Username: admin
Password: admin

Setup Wizard

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

After logging in to the user interface, fill in the New Password and Confirm New Password fields.

In the System Time function, select **Using Network Time Protocol (NTP)** or **Manually** to define the system time. If required, click the Daylight Saving Offset drop-down menu and select the value (minutes).

- Setting NTP System Time: Before trying to configure NTP check, perform a ping test with the NTP server. In the NTP Server field, enter the NTP server to use. Then click the Time Zone drop-down menu and select the appropriate time zone.
- Setting System Time Manually: From the System Date drop-down menu, select the Year, Month, and Day along with the Hour and Minutes appropriate for the AP.
- Enable Daylight Saving: Click the radio button to enable the daylight savings time (DST) function. Set the DST start (24 hours) and end (24 hours) time by clicking on the drop-down menus and setting the Month, Week, Day, Hour, and Minute of the DST starting days.

Once the settings are configured, click **Update** button to accept the configuration and proceed to the main interface menu page.

PROVIDE SYSTEM SETTINGS ...

These settings apply to this access point.

New Password

Confirm New Password

System Time

☐ Using Network Time Protocol(NTP)
☒ Manually

System Date

2019 February 20

System Time(24 HR)

12 : 12

Enable Daylight Saving

☐

DST Start(24 HR)

First Sunday in January at 00 0

DST End(24 HR)

First Sunday in January at 00 0

Daylight Offset(minutes)

0

System Country

----Select a Country----

Update

Web User Interface

The DIS-2650AP supports an elaborate web user interface where the user can configure and monitor the device. Launch a web browser, type in `http://dis2650ap.local` and then press Enter to login. The default username and password is: admin Most of the configurable settings are located in the menu on the left side of the web GUI which contains sections called **Basic Settings**, **Advanced Settings** and **Status**.

The screenshot displays the D-Link DIS-2650AP web user interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar contains a tree view of the configuration menu, organized into three main sections: Basic Settings (Wireless, LAN, IPv6), Advanced Settings (Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Hotspot 2.0, Captive Portal, DHCP Server, Filters, Traffic Control), and Status (Device Information, Client Information, WDS Information, Statistics, Log). The main content area is titled 'System Information' and displays the following details:

Model Name	DIS-2650AP
Firmware Version	v1.00 10:02:39 2020/12/16
System Name	dis2650ap
Location	
System Time	2021/01/19 15:12:01
Up Time	00:28:19
Operation Mode (2.4GHz)	Access Point
Operation Mode (5GHz)	Access Point
MAC Address (2.4GHz)	F0:B4:D2:B2:91:F0
MAC Address (5GHz)	F0:B4:D2:B2:91:F8
IP Address	172.17.5.29

Wireless

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

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

Access Point Mode

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

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

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

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

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

The screenshot displays the D-Link Web User Interface for a DIS-2650AP. 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 'Wireless' selected under 'Basic Settings'. The main content area is titled 'Wireless Settings' and contains the following configuration options:

- Wireless Band:** 2.4GHz (dropdown)
- Operation Mode:** Access Point (dropdown)
- Network Name (SSID):** dlink (text input)
- SSID Visibility:** Enable (dropdown)
- Auto Channel Selection:** Enabled (dropdown)
- Channel:** 6 (dropdown)
- Channel Width:** Auto 20/40 MHz (dropdown)
- Authentication:** Open System (dropdown)
- 802.11k/v/r:** Disable (dropdown)
- Key Settings:**
 - Encryption:** ☒ Disable ☐ Enable
 - Key Type:** ASCII (dropdown)
 - Key Size:** 64 Bits (dropdown)
 - Key Index (1~4):** 1 (dropdown)
 - Network Key:** (text input)
 - Confirm Key:** (text input)

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

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

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

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

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

- Select **Open System** to communicate the key across the network (WEP).
- Select **Shared Key** to limit communication to only those devices that share the same WEP settings. If multi-SSID is enabled, this option is not available.
- Select **WPA-Personal** to secure your network using a password and dynamic key. 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.

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

WDS with AP Mode

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

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

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

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

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

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

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

DIS-2650AP

[Home](#)
[Maintenance](#)
[Configuration](#)
[System](#)
[Logout](#)
[Help](#)

DIS-2650AP

- Basic Settings
 - Wireless
 - LAN
 - IPv6
- Advanced Settings
 - Performance
 - Wireless Resource
 - Multi-SSID
 - VLAN
 - Intrusion
 - Schedule
 - Internal RADIUS Server
 - ARP Spoofing Prevention
 - Bandwidth Optimization
 - Hotspot 2.0
 - Captive Portal
 - DHCP Server
 - Filters
 - Traffic Control
 - Status
 - Device Information
 - Client Information
 - WDS Information
 - Statistics
 - Log

Wireless Settings

Wireless Band

2.4GHz

Operation Mode

WDS with AP

Network Name (SSID)

dlink

Auto Channel Selection

Enabled

Channel

6

Channel Width

Auto 20/40 MHz

WDS

AP MAC Address

Site Survey

Ch

Signal (%)

MAC Address

Security

SSID

You can click Scan button to start.

Scan

Authentication

Open System

Key Settings

Encryption

☒ Disable
 ☐ Enable

Key Type

ASCII

Key Size

64 Bits

Key Index (1~4)

1

Network Key

Confirm Key

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

Save

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, or WPA-Personal**.

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

WDS Mode

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

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

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

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

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

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

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

D-Link DIS-2650AP

Home Maintenance Configuration System Logout Help

Wireless Settings

Wireless Band: 2.4GHz

Operation Mode: WDS

Network Name (SSID): dlink

Auto Channel Selection: Enabled

Channel: 6

Channel Width: Auto 20/40 MHz

WDS

AP MAC Address:

Site Survey [Scan]

Ch	Signal (%)	MAC Address	Security	SSID
You can click Scan button to start.				

Authentication: Open System

Key Settings

Encryption: ☒ Disable ☐ Enable

Key Type: ASCII Key Size: 64 Bits

Key Index (1~4): 1

Network Key:

Confirm Key:

(0-9,a-z,A-Z,~!@#\$%^&*()_+~=:[]{}|,./<>?)

[Save]

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

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

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

Wireless Client Mode

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

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

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

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

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

Channel: The channel used will be displayed, and matches the AP that the DIS-2650AP is connected to when set to Wireless Client mode.

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

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

Authentication: Will be explained in the next topic.

The screenshot displays the D-Link DIS-2650AP Web User Interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of settings categories: Basic Settings (Wireless, LAN, IPv6), Advanced Settings (Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Hotspot 2.0), Captive Portal, DHCP Server, Filters, Traffic Control, Status (Device Information, Client Information, WDS Information, Statistics, Log), and a Log section.

The main content area is titled "Wireless Settings". It contains the following configuration options:

- Wireless Band:** 2.4GHz (dropdown)
- Operation Mode:** Wireless Client (dropdown)
- Network Name (SSID):** (text input field)
- SSID Visibility:** Enable (dropdown)
- Auto Channel Selection:** Enabled (dropdown)
- Channel:** 6 (dropdown)
- Channel Width:** Auto 20/40 MHz (dropdown)

Below these settings is a "Site Survey" section with a "Scan" button. A table header is visible with columns: Ch, Signal (%), MAC Address, Security, and SSID. Below the header, it says "You can click Scan button to start."

The "Authentication" section is set to "Open System" (dropdown). Below it is a "Key Settings" section with the following options:

- Encryption:** Disable (selected radio button), Enable (radio button)
- Key Type:** ASCII (dropdown), Key Size: 64 Bits (dropdown)
- Key Index (1~4):** 1 (dropdown)
- Network Key:** (text input field)
- Confirm Key:** (text input field)

Below the key settings is a "Wireless MAC Clone" section with the following options:

- Enabled:** (checkbox, currently unchecked)
- MAC Source:** Manual (dropdown)
- MAC Address:** 00 : 00 : 00 : 00 : 00 : 00 (text input fields)
- Scan:** (button)

At the bottom of the MAC Address section, there is a label "MAC Address" above a dark bar.

Wireless Security

Wireless security is a key concern for any wireless network installed. 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 no encryption. WPA is the newest encryption protocol. 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 sends 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 sends a request to the access point and if the key used matches the one configured on the access point, the access point will send a challenge to the client. The client will then again send a confirmation of the same key back to the access point where the access point will either return a successful or a denial packet back to the wireless client.

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

Key Type*,:** Select HEX or ASCII.

Key Size: Select 64 Bits or 128 Bits.

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

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

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

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

The screenshot displays the D-Link DIS-2650AP configuration interface. The 'Wireless Settings' tab is active. On the left, a tree menu shows categories like Basic Settings, Advanced Settings, and Status. The 'Wireless' option under Basic Settings is selected. The main panel on the right contains the following settings:

- Wireless Band:** 2.4GHz
- Operation Mode:** Access Point
- Network Name (SSID):** (empty text field)
- SSID Visibility:** Enable
- Auto Channel Selection:** Enabled
- Channel:** 6
- Channel Width:** Auto 20/40 MHz
- Authentication:** Open System
- 802.11k/v/r:** Disable
- Key Settings:**
 - Encryption:** ☒ Enable
 - Key Type:** ASCII
 - Key Size:** 64 Bits
 - Key Index (1~4):** 1
 - Network Key:** (empty text field)
 - Confirm Key:** (empty text field)

A legend at the bottom of the Key Settings section indicates valid characters: (0-9,a-z,A-Z,-!@#%&*()_+~=:[]{}|.,/<>?). A 'Save' button is located at the bottom right.

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

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

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

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

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

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

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

The screenshot displays the 'Wireless Settings' web interface. The 'Authentication' is set to 'WPA-Personal'. Below this, the 'PassPhrase Settings' section is expanded, showing 'WPA Mode' set to 'AUTO (WPA or WPA2)', 'Cipher Type' set to 'Auto', and 'Group Key Update Interval' set to '3600 (Sec)'. The 'Time Interval' is set to '1 (1~168) hour(s)'. There are input fields for 'PassPhrase' and 'Confirm PassPhrase'. A notice at the bottom states: 'notice: 8~63 in ASCII or 64 in Hex. (0-9,a-z,A-Z,~,!@#\$%^&*()_+~=:[]{}|,./<>?)'. A 'Save' button is located at the bottom right of the settings area.

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 Band	2.4GHz ▼	
Operation Mode	Access Point ▼	
Network Name (SSID)	dlink	
SSID Visibility	Enable ▼	
Auto Channel Selection	Enabled ▼	
Channel	6 ▼	
Channel Width	Auto 20/40 MHz ▼	
Authentication	WPA-Enterprise ▼	
802.11k/v/r	Disable ▼	
RADIUS Server Settings		
WPA Mode	AUTO (WPA or WPA2) ▼	
Cipher Type	Auto ▼	Group Key Update Interval 3600 (Sec)
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	Enable ▼	
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		

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 DIS-2650AP. 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: **Dynamic IP (DHCP)** is chosen here. Choose this option if you have a DHCP server in your network. 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. If you wish to assign a static IP address to the DIS-2650AP, choose **Static IP (Manual)**.

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

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

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	Dynamic IP (DHCP) ▼
IP Address	192.168.0.102
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS	192.168.0.1
Save	

IPv6

Enable IPv6: Check to enable the IPv6

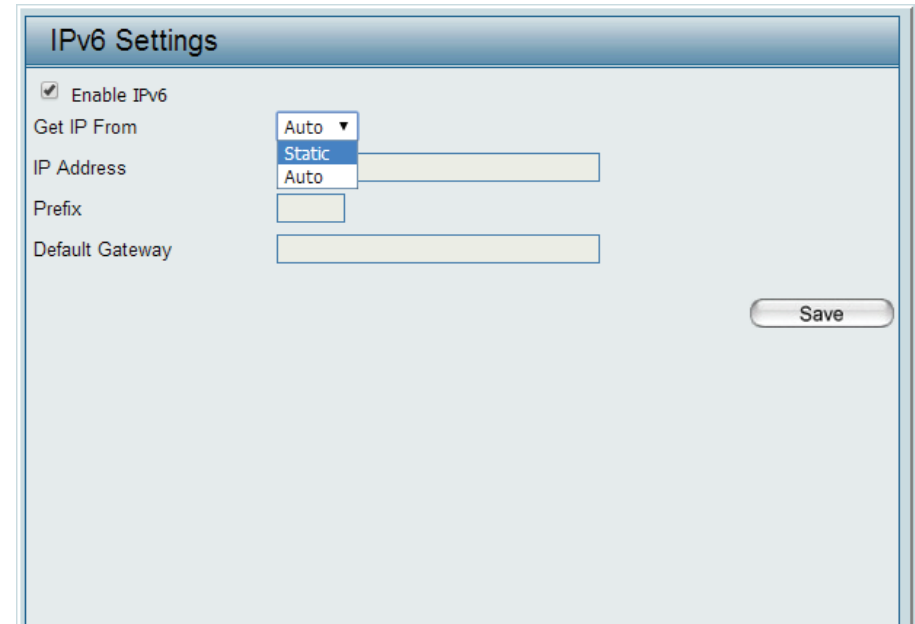
Get IP From: Auto is chosen here. Choose this option the DIS-2650AP can get IPv6 address automatically or use Static to set IPv6 address manually.

Other fields here will be grayed out when Auto is selected.

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 interface 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 menu is open, showing "Auto", "Static", and "Auto" as options.
- 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 users 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 DIS-2650AP Web User Interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. A left sidebar shows a tree view of settings categories: Basic Settings, Advanced Settings (selected), Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Hotspot 2.0, 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 802.11b, 802.11g, 802.11n
Data Rate	Best(Up to 300) Mbps
Beacon Interval (40-500)	100
DTIM Period (1-15)	1
Transmit Power	100%
WMM (Wi-Fi Multimedia)	Enable
Ack Time Out	64 (μs)
Short GI	Enable
IGMP Snooping	Disable
Multicast Rate	Disable Mbps
Multicast Bandwidth Control	Disable
Maximum Multicast Bandwidth	100 kbps
HT 20/40 Coexistence	Enable
Transfer DHCP Offer to Unicast	Disable

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

Performance

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

Wireless Band: Select either 2.4GHz or 5GHz.

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

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

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

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

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

The screenshot displays the 'Performance Settings' interface. It features a list of configuration items on the left and their corresponding values or controls on the right. The items include: Wireless band (5GHz), Wireless (Off), Wireless Mode (Mixed 802.11ac), Data Rate (Best(Up to 867) Mbps), Beacon Interval (40-500) (100), DTIM Interval (1-15) (1), Transmit Power (100%), WMM (Wi-Fi Multimedia) (Enable), Ack Time Out (5GHz, 25~200) (25 μs), Short GI (Enable), IGMP Snooping (Disable), Multicast Rate (Disable Mbps), Multicast Bandwidth Control (Disable), Maximum Multicast Bandwidth (100 kbps), HT20/40 Coexistence (Disable), and Transfer DHCP Offer to Unicast (Disable). A 'Save' button is located at the bottom right of the settings area.

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

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

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

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

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

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

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

Multicast Bandwidth Control : Adjust the multicast packet data rate here. The multicast rate is supported in AP mode, and WDS with AP mode, including Multi-SSIDs

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

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

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

PMF: Enable this option to help protect clients against forged management frames spoofed from other devices that might otherwise disrupt a valid user session.

Wireless Resource Control

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

Airtime Fairness: Enable airtime fairness to help regulate downlink airtime.

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

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

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

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

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

Connection Limit: Select **Enable** or **Disable**. This is an option for load balancing. This determines whether to limit the number of users accessing this device. The exact number is entered in the User Limit field below. This feature allows the user to share the wireless network traffic and the client using multiple APs. If this function is enabled and when the number of users exceeds this value, or the network utilization of this AP exceeds the percentage that has been specified, the DIS-2650AP will not allow clients to associate with the AP.



The screenshot shows the 'Wireless Resource Control' configuration window. It contains the following settings:

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

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

- 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 DIS-2650AP 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

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

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

Enable Priority: Check to enable support for SSID priority level.

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

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

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

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

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

Priority: Select the priority level of the SSID selected.

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

The screenshot shows the configuration interface for a D-Link DIS-2650AP. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. A left sidebar lists various settings categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Hotspot 2.0, Captive Portal, DHCP Server, Filters, Traffic Control, and Status.

Multi-SSID Settings

- ☐ Enable Multi-SSID
- ☐ Enable Priority

Wireless Settings

Band	2.4GHz ▾
Index	Primary SSID ▾
SSID	dlink
SSID Visibility	Enable ▾
Security	Open System ▾
Priority	0 ▾
WMM (Wi-Fi Multimedia)	Enable ▾
802.11k/v/r	Disable ▾

Key Settings

Encryption: ☒ Disable ☐ Enable

Key Type: ASCII ▾ Key Size: 64 Bits ▾

Key Index (1~4): 1 ▾

Network Key:

Confirm Key:

(0-9,a-z,A-Z,-!@#\$%^&*()_+~`~'~,./<>?)

[Add]

Index	SSID	Band	Authentication Method	Encryption Type	Delete
Primary SSID	dlink	2.4G Hz	No Authentication	No Encryption	

[Save]

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 DIS-2650AP 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 DIS-2650AP without a VLAN tag will have a VLAN tag inserted with a PVID. The VLAN List tab displays the current VLANs.

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

VLAN Mode: The current VLAN mode is displayed.

VLAN Settings

VLAN Status : ☒ Disable ☐ Enable Save

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

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

Port List

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

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

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

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

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

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

The screenshot displays the 'VLAN Settings' configuration page. At the top, there are radio buttons for 'VLAN Status' (set to 'Disable') and a 'Save' button. Below this, the 'VLAN Mode' is set to 'Static(2.4G), Static(5G)'. The interface has four tabs: 'VLAN List', 'Port List' (which is active), 'Add/Edit VLAN', and 'PVID Setting'. The 'Port List' tab contains a table with the following data:

Port Name	Tag VID	Untag VID	PVID
Mgmt	1		1
LAN	1		1
Primary(2.4G)	1		1
Primary(5G)	1		1
S-1(2.4G)	1		1
S-2(2.4G)	1		1
S-3(2.4G)	1		1
S-4(2.4G)	1		1
S-5(2.4G)	1		1
S-6(2.4G)	1		1
S-7(2.4G)	1		1
S-1(5G)	1		1
S-2(5G)	1		1
S-3(5G)	1		1
S-4(5G)	1		1
S-5(5G)	1		1
S-6(5G)	1		1
S-7(5G)	1		1

Add/Edit VLAN

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

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

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

VLAN Name: Enter the VLAN to add or modify.

VLAN Settings

VLAN Status : ☒ Disable ☐ Enable
Save

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

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

VLAN ID (VID)
VLAN Name

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

2.4GHz

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	☐	☐	☐	☐	☐	☐	☐	☐

5GHz

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	☐	☐	☐	☐	☐	☐	☐	☐

Save

PVID Settings

The PVID Setting tab is used to enable/disable the Port VLAN Identifier Auto Assign Status as well as to configure various types of PVID settings. Click **Save** button to have 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 displays the 'VLAN Settings' web interface. At the top, there are radio buttons for 'VLAN Status' (Disable is selected) and 'VLAN Mode' (Static(2.4G), Static(5G)). A 'Save' button is located to the right. Below this is a tabbed interface with four tabs: 'VLAN List', 'Port List', 'Add/Edit VLAN', and 'PVID Setting' (which is currently selected). Under the 'PVID Setting' tab, there is a section for 'PVID Auto Assign Status' with 'Disable' selected. Below this are two tables for configuring PVID settings for 2.4GHz and 5GHz bands. Each table has columns for 'MSSID Port', 'Primary', and seven secondary ports (S-1 to S-7). The 'PVID' row in both tables shows the value '1' for all ports. A 'Save' button is at the bottom right of the interface.

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

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

Intrusion

The Wireless Intrusion Protection window is used to classify APs as Valid, Neighborhood, Rogue, or a New group. Click **Save** for the changes to take effect.

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

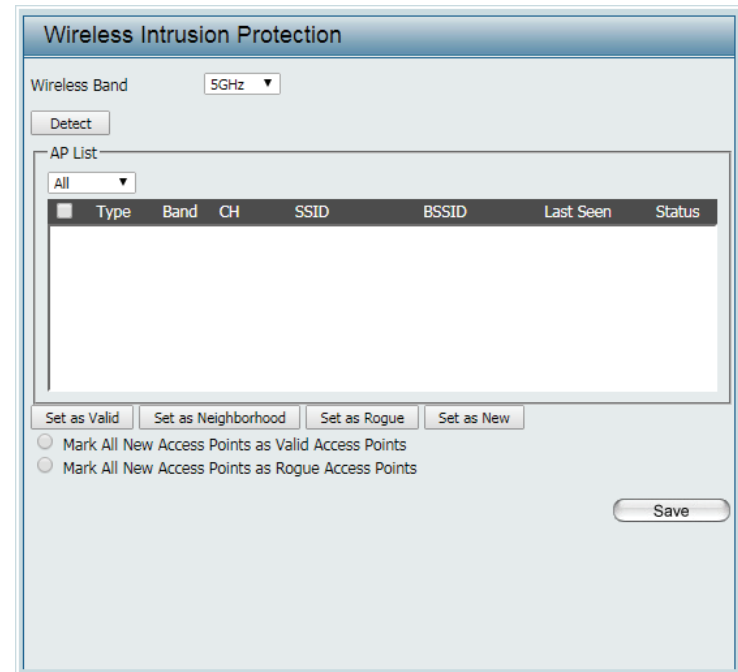
Detect: Click **Detect** to initiate a scan of the network.

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

The following is a definition of the listed AP categories:

- Valid: An AP which is authenticated to the network with encryption is classified as valid.
- Neighbor: A detected AP with a weak signal strength is classified as a suspect neighbor.
- Rogue: An AP that has been installed on the secure network without explicit authorization.
- New: An alternative category.

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



The screenshot shows the 'Wireless Intrusion Protection' window. At the top, there's a title bar. Below it, a 'Wireless Band' dropdown menu is set to '5GHz'. A 'Detect' button is located below the dropdown. The 'AP List' section features a dropdown menu currently set to 'All'. Below this is a table with columns: Type, Band, CH, SSID, BSSID, Last Seen, and Status. The table is currently empty. Below the table, there are four buttons: 'Set as Valid', 'Set as Neighborhood', 'Set as Rogue', and 'Set as New'. At the bottom, there are two radio buttons: 'Mark All New Access Points as Valid Access Points' and 'Mark All New Access Points as Rogue Access Points'. A 'Save' button is positioned at the bottom right of the window.

Schedule

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

Wireless Schedule Settings

Wireless Schedule: Disable

Add Schedule Rule

Name:

SSID Index: Primary SSID 2.4G

SSID: dlink

Day(s): ☐ All Week ☒ Selects 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 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 DIS-2650AP features a built-in RADIUS server. Once you have finished adding a RADIUS account, click the **Save** to have 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 to below 30.

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

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

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

RADIUS Account List: Displays the list of users.

The screenshot displays the D-Link DIS-2650AP Web User Interface. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of configuration options, with 'Internal RADIUS Server' selected under 'Advanced Settings'. The main content area is titled 'Internal RADIUS Server' and contains two sections: 'RADIUS Accounts (Max: 256 users)' and 'RADIUS Account list'.

In the 'RADIUS Accounts' section, there are input fields for 'User Name' (4-16 characters) and 'Password' (6-32 characters), and a 'Status' dropdown menu currently set to 'Enable'.

The 'RADIUS Account list' section shows a table with columns for 'User Name', 'Enable', 'Disable', and 'Delete'. The table is currently empty, displaying 'No user entries'. A 'Save' button is located at the bottom right of the list.

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 Web User Interface for the DIS-2650AP device. The left sidebar shows a navigation tree with 'Advanced Settings' expanded, and 'ARP Spoofing Prevention' selected. The main content area is titled 'ARP Spoofing Prevention Settings'. It features a 'Disable' dropdown menu for 'ARP Spoofing Prevention'. Below this is an 'Add Gateway Address' section with input fields for 'Gateway IP Address' and 'Gateway MAC Address' (formatted as four pairs of boxes separated by dots), and 'Add' and 'Clear' buttons. A 'Gateway Address List' section shows 'Total Entries: 0' and a 'Delete All' button. Below this is a table with columns 'Gateway IP Address', 'Gateway MAC Address', 'Edit', and 'Delete'. A 'Save' button is located at the bottom right of the settings area.

Gateway IP Address	Gateway MAC Address	Edit	Delete
--------------------	---------------------	------	--------

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 **Save** button to have 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 the average bandwidth for each client.
- Allocate maximum BW for each station:** Specify the maximum bandwidth for each connected client. Reserve certain bandwidth for future clients.
- Allocate different BW for a/b/g/n stations:** The weight of 11b/g/n and 11a/n client are 10%/20%/70% ; 20%/80%. AP will distribute different bandwidth for 11a/b/g/n clients.
- Allocate specific BW for SSID:** All clients share the total bandwidth.
- Rule Type:** Use the drop-down menu to select the type that is applied to the rule. Available options are: **Allocate average BW for each station, Allocate maximum BW for each station, Allocate different BW for 1a/b/g/n stations, and Allocte specific BW for SSID.**

Bandwidth Optimization

Enable Bandwidth Optimization

Enable

Downlink Bandwidth

80

Mbits/sec

Uplink Bandwidth

80

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 and 5GHz.

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

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

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

Hotspot 2.0

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

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

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

Hotspot

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

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

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

Manage P2P: Choose enable to allow P2P.

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

Proxy ARP: Choose enable to allow proxy ARP.

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

The screenshot shows the 'Hotspot 2.0' configuration page. At the top, there are two dropdown menus: 'Band' set to '2.4GHz' and 'SSID Index' set to 'Primary SSID'. Below these is a tabbed interface with five tabs: 'Hotspot' (selected), 'Interworking', 'WAN Metrics', 'LIST', and 'OSU'. The 'Hotspot' tab contains a list of settings, each with a dropdown menu: 'Hotspot 2.0' (Disable), 'OSEN' (Disable), 'Allow Cross Connection' (Disable), 'Manage P2P' (Disable), 'DGAF' (Enable DGAF), 'Proxy ARP' (Disable), and 'L2TIF' (Disable). A 'Save' button is located at the bottom right of the configuration area.

Hotspot	Interworking	WAN Metrics	LIST	OSU
Hotspot				
Hotspot 2.0				
OSEN				
Allow Cross Connection				
Manage P2P				
DGAF				
Proxy ARP				
L2TIF				

Interworking

Interworking: Choose enable to turn on interworking function.

Access Network Type: Specify type of network.

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

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

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

Venue Group: Specify group venue belongs to.

Venue Type: Specify type of venue.

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

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

The screenshot shows the 'Hotspot 2.0' configuration interface. At the top, there are two dropdown menus: 'Band' set to '2.4GHz' and 'SSID Index' set to 'Primary SSID'. Below these is a tabbed interface with five tabs: 'Hotspot', 'Interworking' (which is selected and highlighted), 'WAN Metrics', 'LIST', and 'OSU'. The 'Interworking' tab contains a list of configuration items, each with a label and a control element (either a dropdown menu or a text input field). The items are: 'Interworking' (Disable), 'Access Network Type' (0), 'Internet' (Disable), 'ASRA' (Disable), 'ESR' (Disable), 'UESA' (Disable), 'Venue Group' (0), 'Venue Type' (0), 'Venue Name' (English dropdown and CHT Wi-Fi text input), and 'HESSID' (empty text input). To the right of the 'Venue Name' input field are '+' and '-' buttons. At the bottom right of the form is a 'Save' button.

Hotspot	Interworking	WAN Metrics	LIST	OSU
Interworking				
Interworking				
Access Network Type				
Internet				
ASRA				
ESR				
UESA				
Venue Group				
Venue Type				
Venue Name				
HESSID				

WAN Metrics

WAN Link Status: Information about the status of the Access Point's WAN connection.

WAN Symmetric Link: Set to 1 if the WAN link is symmetric (upload and download speeds are the same), or set to 0 if not.

WAN At Capacity: Set to 1 if the Access Point or the network is at its max capacity, or set to 0 if not.

WAN Metrics DL Speed: The downlink speed of the WAN connection set in kbps. If the downlink speed is not known, set to 0.

WAN Metrics UL Speed: The uplink speed of the WAN connection set in kbps. If the uplink speed is not known set to 0.

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

Hotspot	Interworking	WAN Metrics	LIST	OSU
WAN Metrics				
WAN Link Status 0				
WAN Symmetric Link 0				
WAN At Capacity 0				
WAN Metrics DL Speed 0				
WAN Metrics UL Speed 0				

Save

LIST

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

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

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

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

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

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

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

Operator Friendly Name: Identifies the Hotspot venue operator.

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

Hotspot 2.0

Band
2.4GHz
SSID Index
Primary SSID

Hotspot
Interworking
WAN Metrics
LIST
OSU

List

Network Auth Type
04
IP Address Type Availability
4
Domain Name List
emome.net
Roaming Consortium
000A43
Nai Realm List
0,wlan.mnc092.mcc466.3gppne
3gpp Cellular Network
466,092
Connection Capability
6:80:1
Operator Friendly Name
English
CHT Wi-Fi
QoS Map

+ -
+ -
+ -
+ -
+ -
+ -

Save

OSU

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

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

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

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

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

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

OSU Nai: Specify OSU Network Access Identifier.

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

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

Hotspot 2.0

Band
2.4GHz

SSID Index
Primary SSID

Hotspot
Interworking
WAN Metrics
LIST
OSU

OSU

OSU SSID

OSU Server URI

OSU Method List

OSU Config
Config1

OSU language
Language

OSU Friendly Name

OSU Nai

OSU Service Description
Language

OSU Icon Language
Language

OSU Icon Name

OSU Icon Width
0

OSU Icon Height
0

OSU Icon Type

OSU Icon File Path

Save

OSU Icon Name: Specify icon name.

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

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

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

OSU Icon File Path: Specify location of icon file.

Captive Portal

Authentication Settings-Web Redirection Only

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

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

Select 2.4GHz or 5GHz.

Band : Select the SSID for this Authentication.

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

Authentication Type :

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

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

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

VLAN Group : Enter the VLAN Group ID here.

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DIS-2650AP. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

The screenshot displays the D-Link web interface for the DIS-2650AP. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of configuration options, with 'Captive Portal' selected. The main content area is titled 'Captive Portal Authentication' and contains the following settings:

- Session Timeout (1-1440):** 60 Minute(s)
- Band:** 2.4GHz
- SSID Index:** Primary SSID
- Authentication Type:** Web Redirection Only
- Web Redirection Interface Settings:**
 - Web Redirection State:** Enable
 - URL Path:** http://
- IP Interface Settings:**
 - IPIF Status:** Disable
 - VLAN Group:** (empty field)
 - Get IP From:** Static IP (Manual)
 - IP Address:** (empty field)
 - Subnet Mask:** (empty field)
 - Gateway:** (empty field)
 - DNS:** (empty field)

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

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

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

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

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

Authentication Settings- Username/Password

After selecting Username/Password as the Authentication Type, we can configure the Username/Password authentication that will be applied to each wireless client in this network.

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

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here.

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DIS-2650AP. When Dynamic

D-Link DIS-2650AP

Home Maintenance Configuration System Logout Help

Captive Portal Authentication

Session Timeout (1-1440) Minute(s)

Band

SSID Index

Authentication Type

Web Redirection Interface Settings

Web Redirection State

URL Path

IP Interface Settings

IPIF Status

VLAN Group

Get IP From

IP Address

Subnet Mask

Gateway

DNS

Username/Password Settings

Username

Password

Username	Edit	Delete

Band	SSID Index	Captive Profile	Edit	Delete

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

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

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

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

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

Username: Enter the username for the new account here.

Password: Enter the password for the new account here.

Authentication Settings- Passcode

After selecting Passcode as the Authentication Type, we can configure the Passcode authentication that will be applied to each wireless client in this network.

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

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DIS-2650AP. When Dynamic IP (DHCP) is selected, the other fields here will be

D-Link DIS-2650AP

Home Maintenance Configuration System Logout Help

DIS-2650AP

- Basic Settings
- Advanced Settings
 - Performance
 - Wireless Resource
 - Multi-SSID
 - VLAN
 - Intrusion
 - Schedule
 - Internal RADIUS Server
 - ARP Spoofing Prevention
 - Bandwidth Optimization
 - Hotspot 2.0
- Captive Portal
 - Authentication Settings
 - Login Page Upload
 - MAC Bypass
- DHCP Server
- Filters
- Traffic Control
- Status

Captive Portal Authentication

Session Timeout (1-1440): Minute(s)

Band:

SSID Index:

Authentication Type:

Web Redirection Interface Settings

Web Redirection State:

URL Path:

IP Interface Settings

IPIF Status:

VLAN Group:

Get IP From:

IP Address:

Subnet Mask:

Gateway:

DNS:

Passcode Settings

Passcode Quantity:

Duration: Hour

Last Active Time: Year Month Day Hour

User Limit:

Passcode	Duration	Last Active Time	User Limit	Delete

Band SSID Index Captive Profile Edit Delete

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

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

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

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

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

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

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

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

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

Authentication Settings- Remote RADIUS

After selecting Remote RADIUS as the Authentication Type, we can configure the Remote RADIUS authentication that will be applied to each wireless client in this network.

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

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DIS-2650AP. 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.

D-Link DIS-2650AP

Home Maintenance Configuration System Logout Help

DIS-2650AP

- Basic Settings
- Advanced Settings
 - Performance
 - Wireless Resource
 - Multi-SSID
 - VLAN
 - Intrusion
 - Schedule
 - Internal RADIUS Server
 - ARP Spoofing Prevention
 - Bandwidth Optimization
 - Hotspot 2.0
 - Captive Portal
 - Authentication Settings
 - Login Page Upload
 - MAC Bypass
- DHCP Server
- Filters
- Traffic Control
- Status

Captive Portal Authentication

Session Timeout (1-1440): 60 Minute(s)

Band: 2.4GHz

SSID Index: Primary SSID

Authentication Type: Remote RADIUS

Web Redirection Interface Settings

Web Redirection State: Enable

URL Path: http://

IP Interface Settings

IPIF Status: Disable

VLAN Group:

Get IP From: Static IP (Manual)

IP Address:

Subnet Mask:

Gateway:

DNS:

Remote RADIUS Settings

Radius Server Settings

RADIUS Server: Radius Port: 1812

Shared Secret:

Remote RADIUS Type: SPAP

Secondary radius Server Settings

RADIUS Server: Radius Port: 1812

Shared Secret:

Remote RADIUS Type: SPAP

Third radius Server Settings

RADIUS Server: Radius Port: 1812

Shared Secret:

Remote RADIUS Type: SPAP

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

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

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

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

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

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

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

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

Authentication Settings- LDAP

After selecting LDAP as the Authentication Type, we can configure the LDAP authentication that will be applied to each wireless client in this network.

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

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here.

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DIS-2650AP. When Dynamic IP (DHCP) is selected, the other fields here will be grayed out. Please allow about 2 minutes for the DHCP client to be functional once this selection is made.

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

The screenshot displays the D-Link DIS-2650AP web interface. The left sidebar shows a navigation tree with categories like Basic Settings, Advanced Settings, and Captive Portal. The main content area is titled 'Captive Portal Authentication'. It includes fields for Session Timeout (1-1440) set to 60, Band set to 2.4GHz, and SSID Index set to Primary SSID. The Authentication Type is set to LDAP. Below this, the 'Web Redirection Interface Settings' section shows Web Redirection State set to Enable and a URL Path field. The 'IP Interface Settings' section shows IPIF Status set to Disable, and other fields for VLAN Group, Get IP From (Static IP (Manual)), IP Address, Subnet Mask, Gateway, and DNS. The 'LDAP Settings' section includes fields for Server, Port (389), Authenticate Mode (Simple), User Name, Password, Base DN (with a hint '(ou=,dc=)'), Account Attribute (with a hint '(ex.cn)'), and Identity, along with an 'Auto Copy' checkbox. A 'Save' button is at the bottom right. At the very bottom, there is a table header with columns: Band, SSID Index, Captive Profile, Edit, and Delete.

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

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

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

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

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

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

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

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

Base DN: Enter the administrator's domain name here.

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

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

Authentication Settings- POP3

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

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

Band : Select 2.4GHz or 5GHz.

SSID Index : Select the SSID for this Authentication.

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

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

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

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

VLAN Group : Enter the VLAN Group ID here.

Get IP From : Static IP (Manual) is chosen here. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to the DIS-2650AP. When Dynamic IP

The screenshot displays the D-Link DIS-2650AP web interface. The left sidebar shows a navigation tree with 'Captive Portal' expanded, leading to 'Authentication Settings'. The main content area is titled 'Captive Portal Authentication' and contains the following settings:

- Session Timeout (1-1440):** 60 Minute(s)
- Band:** 2.4GHz
- SSID Index:** Primary SSID
- Authentication Type:** POP3
- Web Redirection Interface Settings:**
 - Web Redirection State:** Enable
 - URL Path:** http://
- IP Interface Settings:**
 - IPIF Status:** Disable
 - VLAN Group:** (empty field)
 - Get IP From:** Static IP (Manual)
 - IP Address:** (empty field)
 - Subnet Mask:** (empty field)
 - Gateway:** (empty field)
 - DNS:** (empty field)
- POP3 Settings:**
 - Server:** (empty field)
 - Port:** 110
 - Connection Type:** None

At the bottom right, there is a 'Save' button. Below the settings area, a table header is visible with columns: Band, SSID Index, Captive Profile, Edit, and Delete.

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

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

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

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

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

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

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

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

Login Page Upload

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

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

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

The screenshot shows the D-Link Web User Interface for a DIS-2650AP device. The left sidebar contains a tree view of configuration options: Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Hotspot 2.0, Captive Portal, Authentication Settings, Login Page Upload, MAC Bypass, DHCP Server, Filters, Traffic Control, and Status. The main content area is titled "Login Page Upload" and includes a section for "Upload Login Style From Local Hard Drive" with a "Choose File" button and an "Upload" button. Below this is a "Login Page Style List" table with columns for ID, Style Name, Pri, S-1, S-2, S-3, S-4, S-5, S-6, S-7, Download, and Del. The table lists four styles: pages_default_wifi4eu.tar, pages_default.tar, pages_headerpic.tar, and pages_license.tar. The "Wireless Band" is set to 2.4GHz. A "Save" button is located at the bottom right of the table.

ID	Style Name	Pri	S-1	S-2	S-3	S-4	S-5	S-6	S-7	Download	Del
1	pages_default_wifi4eu.tar									Download	
2	pages_default.tar									Download	
3	pages_headerpic.tar									Download	
4	pages_license.tar									Download	

MAC Bypass

The DIS-2650AP features a wireless MAC Bypass. Once a user is finished with these settings, click **Save** for changes to take effect.

Wireless Band: Select the wireless band for MAC Bypass.

SSID Index: Select the SSID for MAC Bypass.

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

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

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

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

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

The screenshot shows the 'MAC Bypass Settings' web interface. At the top, there's a title bar. Below it, the 'Wireless Band' is set to '2.4GHz' and the 'SSID Index' is set to 'Primary SSID'. The 'MAC Address' field is empty, with an 'Add' button next to it. Below this is a table with three columns: 'ID', 'MAC Address', and 'Delete'. The table is currently empty. Under the table, there's a section for 'Upload MAC File' with an 'Upload File' label, a text input field, a 'Browse...' button, and an 'Upload' button. Below that is a section for 'Download MAC File' with a 'Load MAC File to Local Hard Driver' label and a 'Download' button. At the bottom right, there is a 'Save' button.

ID	MAC Address	Delete
----	-------------	--------

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 DIS-2650AP 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 DIS-2650AP 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.

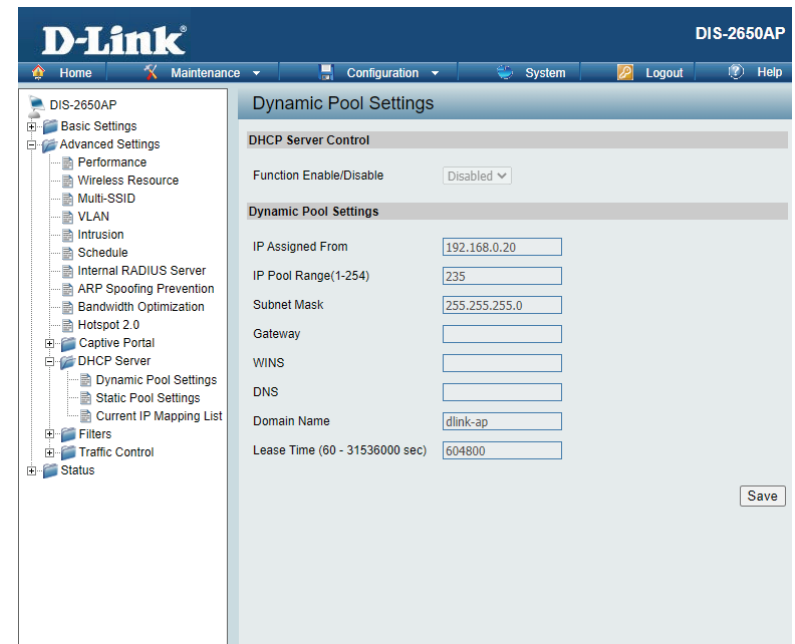
Gateway: Enter the IP address of the gateway on the network.

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.



The screenshot displays the D-Link Web User Interface for the DIS-2650AP. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. The left sidebar shows a tree view of settings categories: Basic Settings, Advanced Settings (Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Hotspot 2.0), Captive Portal, DHCP Server (Dynamic Pool Settings, Static Pool Settings, Current IP Mapping List), Filters, Traffic Control, and Status. The main content area is titled "Dynamic Pool Settings" and contains a "DHCP Server Control" section with a "Function Enable/Disable" dropdown set to "Disabled". Below this is the "Dynamic Pool Settings" section with the following fields: "IP Assigned From" (192.168.0.20), "IP Pool Range(1-254)" (235), "Subnet Mask" (255.255.255.0), "Gateway" (empty), "WINS" (empty), "DNS" (empty), "Domain Name" (dlink-ap), and "Lease Time (60 - 31536000 sec)" (604800). A "Save" button is located at the bottom right of the settings area.

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 DIS-2650AP to function as a DHCP server.

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

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

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

Gateway: Specify the Gateway address for the wireless network.

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

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

Domain Name: Specify the domain name for the network.

Static Pool Settings				
DHCP Server Control				
Function Enable/Disable	Enable ▼			
Static Pool Setting				
Host Name				
Assigned IP				
Assigned MAC Address	: : : : :			
Subnet Mask	255.255.255.0			
Gateway				
WINS				
DNS				
Domain Name	dlink-ap			
Save				
Host Name	MAC Address	IP Address	Edit	Delete

Current IP Mapping List

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

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

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

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

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

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

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

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

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

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

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

Filters

Wireless MAC ACL

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

Wireless Band: Displays the current wireless band rate.

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

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

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

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

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

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

Upload ACL File: Upload the user's own ACL File here.

Download ACL File: Download currenty ACL list to local hard drive.

The screenshot shows the 'Wireless MAC ACL Settings' page. At the top, there's a title bar. Below it, the 'Wireless Band' is set to '2.4GHz' and 'Access Control List' is set to 'Disable'. The 'SSID Index' is 'Primary SSID'. The 'MAC Address' field is empty with an 'Add' button. A table shows 'Current Client Information' with columns for 'MAC Address', 'SSID', 'Signal (%)', and 'Add'. Below this, there's an 'Upload ACL File' section with a 'Choose File' button and an 'Upload' button. The 'Download ACL File' section has a 'Download' button. A 'Save' button is at the bottom right.

ID	MAC Address	Delete	
Current Client Information			
MAC Address	SSID	Signal (%)	Add

IP Filter Settings

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

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

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

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

IP Address: Enter the IP address or network address.

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

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

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

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

The screenshot shows the 'IP Filter Settings' web interface. It features a form with the following fields: 'Wireless Band' (set to 2.4GHz), 'SSID Index' (set to Primary SSID), 'Filter State' (set to Disable), 'IP Address' (empty text box), and 'Subnet Mask' (empty text box). Below these fields is an 'Add' button. Underneath the form is a table with four columns: 'ID', 'IP Address', 'Subnet Mask', and 'Delete'. The table is currently empty. Below the table are two sections: 'Upload IP Filter File' with 'Choose File' and 'Upload' buttons, and 'Download IP Filter File' with a 'Download' button. A 'Save' button is located at the bottom right of the interface.

ID	IP Address	Subnet Mask	Delete
----	------------	-------------	--------

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
Save			

Traffic Control

Uplink/Downlink Setting

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

Downlink Bandwidth: The downlink bandwidth in Mbits per second.

Uplink Bandwidth: The uplink bandwidth in Mbits per second.

The screenshot displays the D-Link web management interface for a DIS-2650AP device. The left sidebar shows a navigation tree with categories like Basic Settings, Advanced Settings, Performance, Wireless Resource, Multi-SSID, VLAN, Intrusion, Schedule, Internal RADIUS Server, ARP Spoofing Prevention, Bandwidth Optimization, Hotspot 2.0, Captive Portal, DHCP Server, Filters, Traffic Control, and Status. The 'Traffic Control' category is expanded, showing 'Uplink/Downlink Settings', 'QoS', and 'Traffic Manager'. The main content area is titled 'Uplink and Downlink Settings'. It features checkboxes for Ethernet1 and Ethernet2, each with 'Downlink' and 'Uplink' options. Below these are tabs for '2.4GHz' and '5GHz'. The '2.4GHz' tab is active, showing two sections: 'Downlink Interface' and 'Uplink Interface'. Each section contains checkboxes for 'Primary-ssid' and seven 'Multi-ssid' options (Multi-ssid1 through Multi-ssid7). At the bottom, there are input fields for 'Downlink Bandwidth(1~867)' and 'Uplink Bandwidth(1~867)', both set to '100' Mbits/sec. A 'Save' button is located at the bottom right of the settings area.

QoS

Quality of Service (QoS) enhances the experience of using a network by prioritizing the traffic of different applications. The DIS-2650AP supports four priority levels. Once the desired QoS settings are finished, click the **Save** to have 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 section titled 'QoS' with a sub-section 'Enable QoS' containing a checkbox. Below this is the 'Advanced QoS' section. It includes fields for 'Downlink Bandwidth' and 'Uplink Bandwidth', both set to '100' Mbits/sec. There are several rows for traffic priorities, each with a dropdown menu for priority, a 'Limit' field set to '100', and a '% Port' field. The priorities and their corresponding port ranges are: ACK/DHCP/ICMP/DNS Priority (Highest Priority, 53,67,68,546,547), Web Traffic Priority (Third Priority, 80,443,3128,8080), Mail Traffic Priority (Second Priority, 25,110,465,995), Ftp Traffic Priority (Low Priority, 20,21), User Defined-1 Priority (Highest Priority, 0 - 0), User Defined-2 Priority (Second Priority, 0 - 0), User Defined-3 Priority (Third Priority, 0 - 0), User Defined-4 Priority (Low Priority, 0 - 0), and Other Traffic Priority (Low Priority, %). A 'Save' button is located at the bottom right of the window.

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

Traffic Manager

The traffic manager feature allows users to create traffic management rules that specify how to deal with listed client traffic and specify downlink/uplink speed for new traffic manager rules. Click the **Save** to have 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: The uplink bandwidth in Mbits per second. This value is entered in the Uplink/Downlink Setting window.

Name: Enter the name of the traffic manager rule.

Client IP (optional): Enter the client IP address of the traffic manager rule.

Client MAC (optional): Enter the client MAC address of the traffic manager rule.

Downlink Speed: Enter the downlink speed in Mbits per second.

Uplink Speed: Enter the uplink speed in Mbits per second.

Traffic Manager

Traffic Manager

Unlisted Clients Traffic
☐ Deny
☒ Forward

Downlink Bandwidth
 Mbits/sec

Uplink Bandwidth
 Mbits/sec

Add Traffic Manager Rule

Name

Client IP(optional)

Client MAC(optional)

Downlink Speed
 Mbits/sec

Uplink Speed
 Mbits/sec

Traffic Manager Rules

Name	Client IP	Client MAC	Downlink Speed	Uplink Speed	Edit	Del
Save						

Status

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

D-Link DIS-2650AP

Home Maintenance Configuration System Logout Help

DIS-2650AP

- Basic Settings
- Advanced Settings
 - Performance
 - Wireless Resource
 - Multi-SSID
 - VLAN
 - Intrusion
 - Schedule
 - Internal RADIUS Server
 - ARP Spoofing Prevention
 - Bandwidth Optimization
 - Hotspot 2.0
- Captive Portal
- DHCP Server
- Filters
- Traffic Control
 - Uplink/Downlink Settings
 - QoS
 - Traffic Manager
- Status**
 - Device Information**
 - Client Information
 - WDS Information
 - Statistics
 - Log

Device Information

Firmware Version: v1.00

Ethernet MAC Address: F0:B4:D2:B2:91:F0

Wireless MAC Address(2.4GHz): Primary: F0:B4:D2:B2:91:F0
SSID 1~7: F0:B4:D2:B2:91:F1~F0:B4:D2:B2:91:F7

Wireless MAC Address(5GHz): Primary: F0:B4:D2:B2:91:F8
SSID 1~7: F0:B4:D2:B2:91:F9~F0:B4:D2:B2:91:FF

Ethernet

IP Address: 172.17.5.29 [Refresh](#)

Subnet Mask: 255.255.255.0

Default Gateway: 172.17.5.254

DNS: 192.168.168.249
192.168.168.250, 192.168.168.201

Wireless(2.4GHz)

Network Name (SSID): dlink

Channel: Ch 4 (Auto)

Data Rate: Best(Up to 300) Mbps

Security: No Authentication / No Encryption

Wireless(5GHz)

Network Name (SSID): dlink

Channel: Ch 36 + 40 + 44 + 48 (Auto)

Data Rate: Best(Up to 867) Mbps

Security: No Authentication / No Encryption

Device Status

CPU Utilization: 6%

Memory Utilization: 64%

Nuclias Connect

Connection Status: Disconnected

Server IP:

Server 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 DIS-2650AP, including the firmware version and the device's MAC address.

D-Link DIS-2650AP

Home Maintenance Configuration System Logout Help

Device Information

Firmware Version: v1.00

Ethernet MAC Address: F0:B4:D2:B2:91:F0

Wireless MAC Address(2.4GHz): Primary: F0:B4:D2:B2:91:F0
SSID 1~7: F0:B4:D2:B2:91:F1~F0:B4:D2:B2:91:F7

Wireless MAC Address(5GHz): Primary: F0:B4:D2:B2:91:F8
SSID 1~7: F0:B4:D2:B2:91:F9~F0:B4:D2:B2:91:FF

Ethernet

IP Address: 172.17.5.29 [Refresh](#)

Subnet Mask: 255.255.255.0

Default Gateway: 172.17.5.254

DNS: 192.168.168.249
192.168.168.250, 192.168.168.201

Wireless(2.4GHz)

Network Name (SSID): dlink

Channel: Ch 4 (Auto)

Data Rate: Best(Up to 300) Mbps

Security: No Authentication / No Encryption

Wireless(5GHz)

Network Name (SSID): dlink

Channel: Ch 36 + 40 + 44 + 48 (Auto)

Data Rate: Best(Up to 867) Mbps

Security: No Authentication / No Encryption

Device Status

CPU Utilization: 6%

Memory Utilization: 64%

Nuclias Connect

Connection Status: Disconnected

Server IP:

Server Port:

Navigation Menu:

- DIS-2650AP
 - Basic Settings
 - Advanced Settings
 - Performance
 - Wireless Resource
 - Multi-SSID
 - VLAN
 - Intrusion
 - Schedule
 - Internal RADIUS Server
 - ARP Spoofing Prevention
 - Bandwidth Optimization
 - Hotspot 2.0
 - Captive Portal
 - DHCP Server
 - Filters
 - Traffic Control
 - Uplink/Downlink Settings
 - QoS
 - Traffic Manager
 - Status
 - Device Information
 - Client Information
 - WDS Information
 - Statistics
 - Log

Client Information

This page displays the associated clients SSID, MAC, band, authentication method, signal strength, RSSI, and power saving mode for the DIS-2650AP network.

Client Information: This window displays the wireless client information for clients currently connected to the DIS-2650AP.

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						
Client Information		Station association (2.4GHz) : 0				
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info
No wireless client						

Client Information		Station association (5GHz) : 0				
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	System Info
No wireless client						

WDS Information Page

This page displays the access points SSID, MAC, band, authentication method, signal strength, and status for the DIS-2650AP's Wireless Distribution System network.

WDS Information: This window displays the Wireless Distribution System information for clients currently connected to the DIS-2650AP.

Name: Displays the SSID of the client.

MAC: Displays the MAC address of the client.

Authentication: Displays the type of authentication being used.

Signal: Displays the client's signal strength.

Status: Displays the status of the power saving feature.

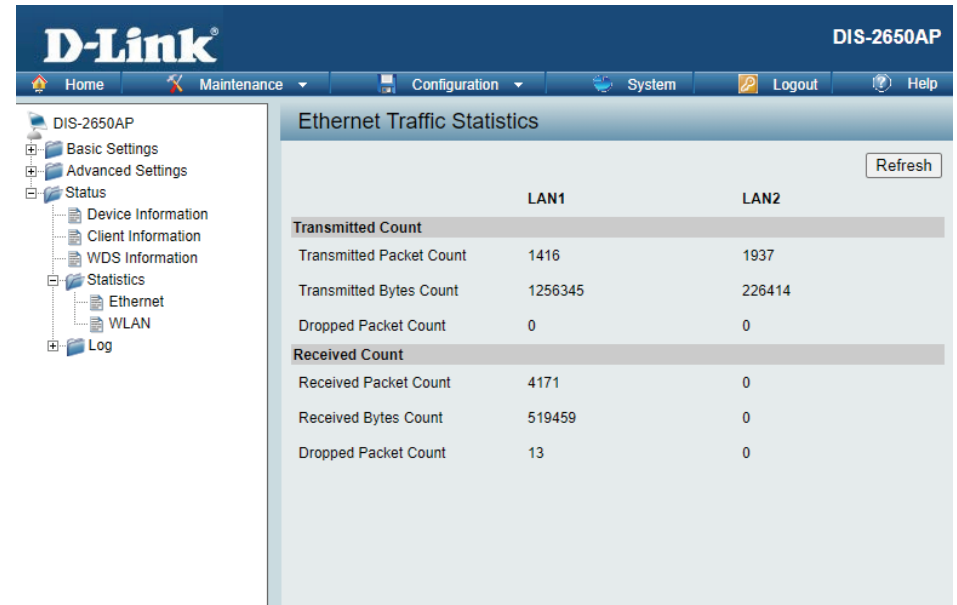
WDS Information				
WDS Information		Channel : 1 (2.412 GHz)		
Name	MAC	Authentication	Signal	Status
WDS Information		Channel : 36 (5.18 GHz)		
Name	MAC	Authentication	Signal	Status

Statistics

Ethernet Traffic Statistics

Displays wired interface network traffic information.

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



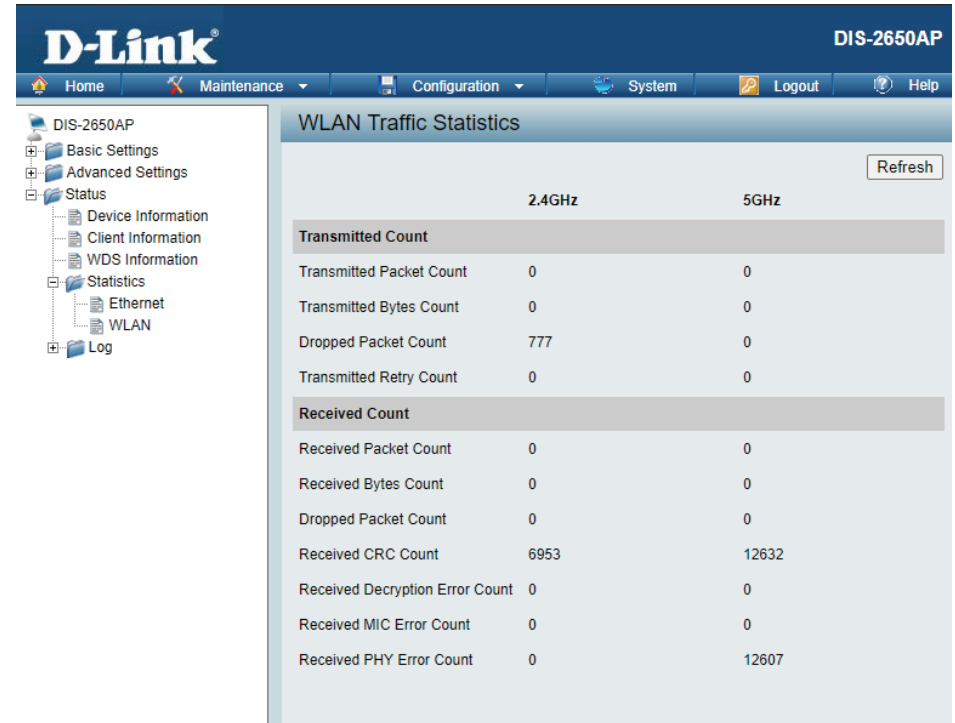
The screenshot shows the D-Link Web User Interface for a DIS-2650AP device. The left sidebar contains a navigation menu with the following items: DIS-2650AP, Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Statistics (selected), Ethernet, WLAN, and Log. The main content area is titled "Ethernet Traffic Statistics" and includes a "Refresh" button. The statistics are presented in a table with columns for LAN1 and LAN2.

	LAN1	LAN2
Transmitted Count		
Transmitted Packet Count	1416	1937
Transmitted Bytes Count	1256345	226414
Dropped Packet Count	0	0
Received Count		
Received Packet Count	4171	0
Received Bytes Count	519459	0
Dropped Packet Count	13	0

WLAN Traffic Statistics

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

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



The screenshot shows the D-Link Web User Interface for a DIS-2650AP. The left sidebar contains a navigation menu with options: Home, Maintenance, Configuration, System, Logout, and Help. Under the Configuration menu, there is a tree view showing: Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Statistics, Ethernet, WLAN, and Log. The main content area is titled 'WLAN Traffic Statistics' and includes a 'Refresh' button. The table displays statistics for 2.4GHz and 5GHz bands, categorized into Transmitted Count and Received Count.

	2.4GHz	5GHz
Transmitted Count		
Transmitted Packet Count	0	0
Transmitted Bytes Count	0	0
Dropped Packet Count	777	0
Transmitted Retry Count	0	0
Received Count		
Received Packet Count	0	0
Received Bytes Count	0	0
Dropped Packet Count	0	0
Received CRC Count	6953	12632
Received Decryption Error Count	0	0
Received MIC Error Count	0	0
Received PHY Error Count	0	12607

Log

View Log

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

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

D-Link®

DIS-2650AP

HomeMaintenanceConfigurationSystemLogoutHelp

DIS-2650AP

- Basic Settings
- Advanced Settings
- Status
 - Device Information
 - Client Information
 - WDS Information
- Statistics
- Log
 - View Log
 - Log Settings

View Log

First PageLast PagePreviousNextClear

Page 1 of 4

Date and Time	Message
Jan 22 15:31:03	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:30:58	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:29:47	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:29:42	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:29:37	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:28:31	Web login success from IP=192.168.0.22 with HTTP
Jan 22 15:28:26	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:28:21	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:28:16	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:27:37	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:27:32	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:27:27	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:27:04	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:26:59	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:26:54	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:26:39	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER
Jan 22 15:26:34	DHCP, Client (MAC=f0:b4:d2:b2:91:f0) sends DISCOVER

81

Log Settings

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

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

Log Type: Check the boxes to select the log type.

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

Email Notification: Check the box to enable sending email notification.

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

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

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

From Email Address: Enter the email address.

To Email Address: Enter the email address.

Email Server Address: Enter the email server address.

SMTP Port: Enter the SMTP port.

User Name: Enter the name of the new user entry.

Password: Enter the password set for the email notification.

Confirm Password: Retype the password entry to confirm the password.

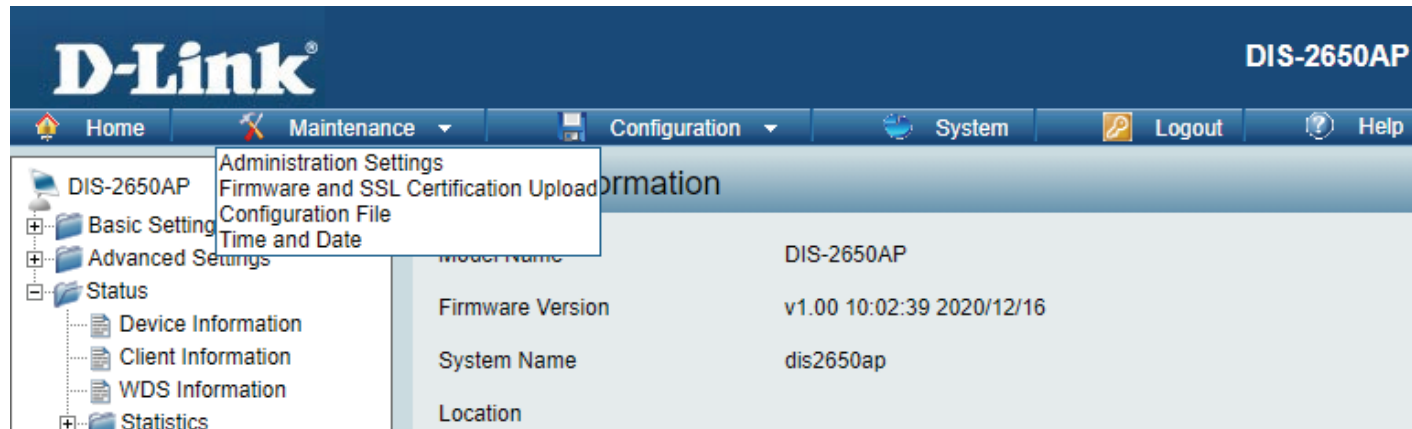
Schedule: Click the drop-down menu to set email log schedule.

The screenshot displays the D-Link Web User Interface for the DIS-2650AP device. The 'Log Settings' page is active, showing a sidebar menu with options like Basic Settings, Advanced Settings, Status, Device Information, Client Information, WDS Information, Statistics, Log, View Log, and Log Settings. The main content area is divided into several sections:

- Log Settings:** Contains 'Log Server / IP Address' (text input) and 'Log Type' (checkboxes for System Activity, Attacks, and Notice, all of which are checked).
- EU directive Syslog Server Settings:** Contains 'Log Server / IP Address' (text input).
- Email Notification:** Contains 'Email Notification' (checkbox), 'Outgoing mail server (SMTP)' (dropdown menu set to 'Internal'), 'Authentication' (checkbox), 'SSL/TLS' (checkbox), 'From Email Address' (text input), 'To Email Address' (text input), 'Email Server Address' (text input), 'SMTP Port' (text input), 'Account' (text input), 'Password' (text input), and 'Confirm Password' (text input).
- Email Log Schedule:** Contains 'Schedule' (dropdown menu set to '0' hours or when Log is full) and a 'Save' button.

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 nine main categories display various hidden administrator parameters and settings. Click **Save** when done.

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.

D-Link® DIS-2650AP

Home Maintenance Configuration System Logout Help

Administration Settings

Limit Administrator ☒

Limit Administrator VLAN ID ☐ Enable

Limit Administrator IP ☐ Enable

IP Range From To

Item	From	To	Delete
System Name Settings			
Login Settings			
Console Settings			
Ping Control Settings			
Country Settings			
DDP Settings			
Nuclias Connect Settings			

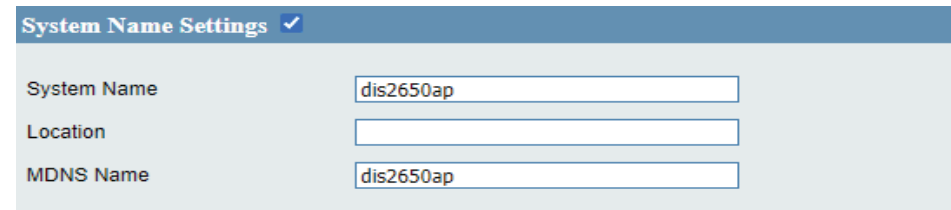
System Name Settings

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 DIS-2650AP.

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

MDNS Name: Enter the name of the multicast DNS. The default name is dis2650ap.



The screenshot shows the 'System Name Settings' page with a blue header bar containing the title and a checkmark icon. Below the header, there are three input fields: 'System Name' with the value 'dis2650ap', 'Location' which is empty, and 'MDNS Name' with the value 'dis2650ap'.

Login Settings

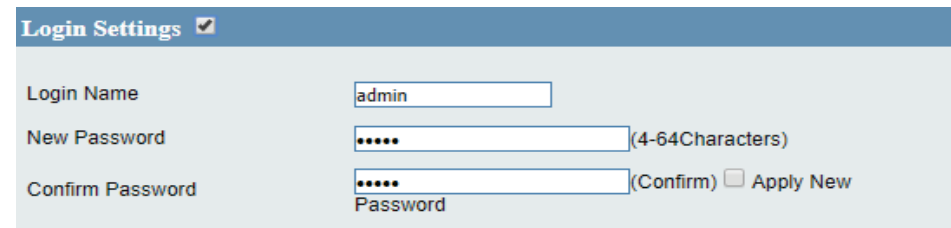
Each of the five main categories display various hidden administrator parameters and settings.

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.



The screenshot shows the 'Login Settings' page with a blue header bar containing the title and a checkmark icon. Below the header, there are three input fields: 'Login Name' with the value 'admin', 'New Password' with masked characters '.....' and a '(4-64Characters)' label, and 'Confirm Password' with masked characters '.....' and a '(Confirm)' label. There is also an 'Apply New' checkbox.

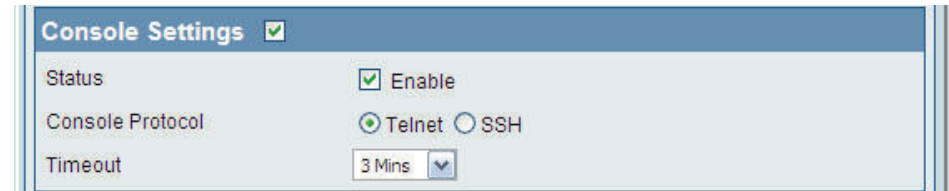
Console Settings

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.

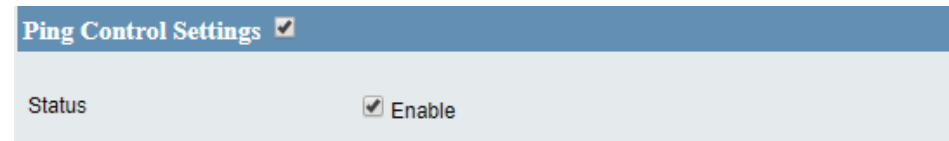


The screenshot shows the 'Console Settings' section with a title bar containing a checkmark. Below the title bar, there are three settings: 'Status' with a checked checkbox and the text 'Enable'; 'Console Protocol' with two radio buttons, 'Telnet' (selected) and 'SSH'; and 'Timeout' with a dropdown menu showing '3 Mins'.

Ping Control Settings

Choose to enable or disable ping function.

Enable: Click to disable. (By default it is enabled.)

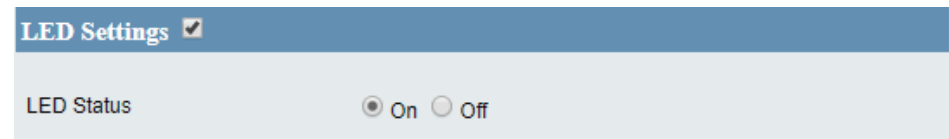


The screenshot shows the 'Ping Control Settings' section with a title bar containing a checkmark. Below the title bar, there is one setting: 'Status' with a checked checkbox and the text 'Enable'.

LED Settings

Choose to enable or disable LED status.

LED Status: Choose corresponding radio button to enable or disable LED Status.



The screenshot shows the 'LED Settings' section with a title bar containing a checkmark. Below the title bar, there is one setting: 'LED Status' with two radio buttons, 'On' (selected) and 'Off'.

Country Settings

Select your country.

Select a Country: Choose from the drop down list the country your device is located.



The screenshot shows the 'Country Settings' section with a title bar containing a checkmark. Below the title bar, there is one setting: 'Select a Country' with a dropdown menu showing 'Taiwan'.

DDP Settings

Choose to enable or disable DDP.

Status: Click to disable. (By default it is enabled.)

DDP Settings 

Status ☒ Enable

Nuclias Connect Settings

Choose to enable or disable Nuclias Connect.

Enable Nuclias Connect: Choose from drop down list to enable or disable Nuclias Connect.

Nuclias Connect Settings 

Enable Nuclias Connect

Disable ▾

Firmware and SSL Upload

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

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 "Update" button to begin updating the firmware. Please don't turn the power off while upgrading.

Language Pack Upgrade:

You can upload an updated language pack from the device here. Click on the "Choose File" button to locate the new language pack. Once the file is selected, click on the "Open" and "Update" button to begin updating the language files.

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. You can upload a SSL Key in the same way.

The screenshot displays the D-Link web interface for the DIS-2650AP device. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. A sidebar on the left lists navigation options: DIS-2650AP, Basic Settings, Advanced Settings, and Status. The main content area is titled "Firmware and SSL Certification Upload". It contains three sections: "Update Firmware From Local Hard Drive" showing the current "Firmware Version v1.00" and a file upload field with "Choose File" and "no file selected" buttons, followed by an "Update" button; "Language Pack Upgrade" with a similar file upload field and "Update" button; and "Update SSL Certification From Local Hard Drive" with two file upload fields (one for the certificate and one for the key) and "Update" buttons.

Configuration File Upload

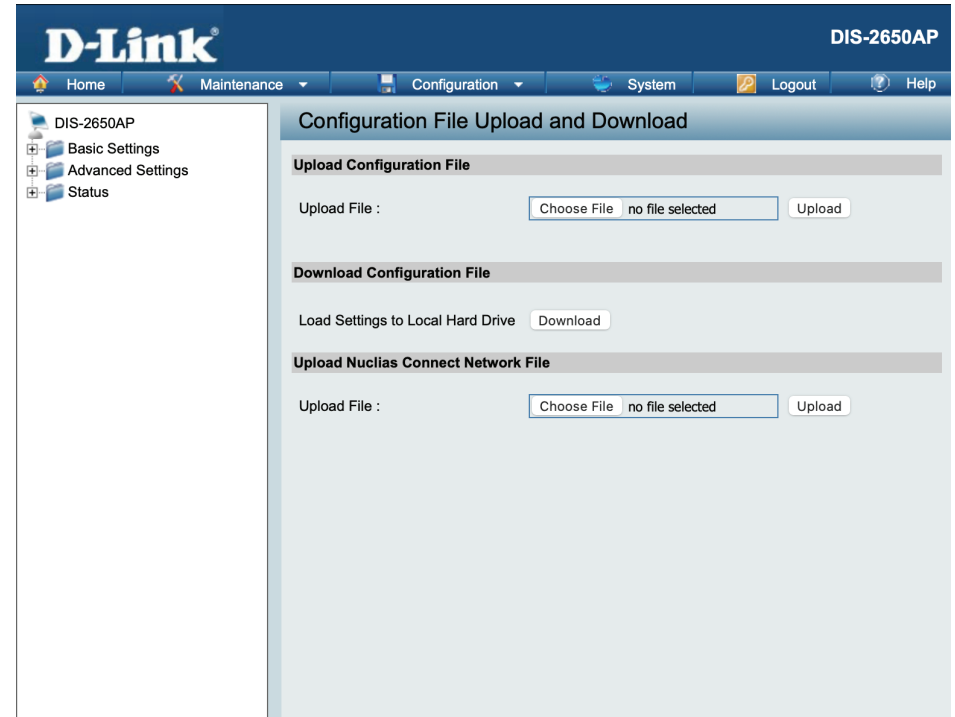
This page allows the user to backup and recover the current configuration of the access point in case of a unit failure.

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 DIS-2650AP and then updating to this saved configuration file, the password will be gone.

Upload Nuclias Connect Network File: Browse to the saved configuration file you have in local drive and click “Open” and “Upload” to update the Nuclias Connect Network file.



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.

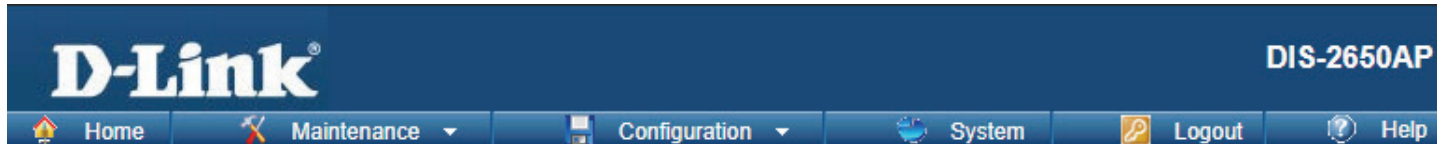
Set the Date and Time Manually: A user can either manually set the time for the AP here, or click the Copy Your Computer's Time Settings button to copy the time from the computer in use (Make sure that the computer's time is set correctly).

The screenshot displays the D-Link Web User Interface for the DIS-2650AP device. The top navigation bar includes links for Home, Maintenance, Configuration, System, Logout, and Help. A left sidebar menu shows options for Basic Settings, Advanced Settings, and Status. The main content area is titled 'Time and Date Settings' and contains several sections:

- Time Configuration:** Shows the 'Current Time' as 2021/01/22 16:16:21.
- Automatic Time Configuration:** Includes a checkbox for 'Enable NTP', an 'NTP Server' input field, and a 'Time Zone' dropdown menu currently set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'.
- Set the Date and Time Manually:** Features a 'Date And Time' section with dropdowns for Year (2021), Month (Feb), Day (22), Hour (11), Minute (47), and Second (10). Below this is a button labeled 'Copy Your Computer's Time Settings'.
- Daylight Configuration:** Includes a checkbox for 'Enable Daylight Saving', a 'Daylight Saving Offset' dropdown set to 60, and a 'Daylight Saving Dates' section. The dates are configured with DST Start on Mar 3rd Sun at 3 am and DST End on Nov 2nd Sun at 3 am. A 'Save' button is located at the bottom right of this section.

Configuration and System

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



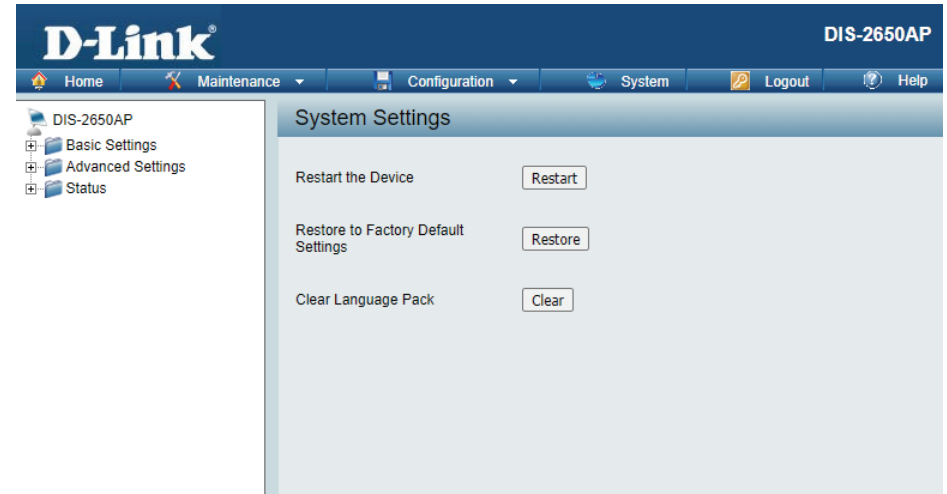
System Settings

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

Restart the Device: Click Restart to restart the DIS-2650AP.

Restore to Factory Default Settings: Click Restore to restore the DIS-2650AP back to factory default settings.

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



Help

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

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

Basic Settings

Wireless Settings

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

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

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

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

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

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

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

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

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

Authentication

Knowledge Base

Wireless Basics

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

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

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

People use WLAN technology for many different purposes:

- **Mobility** - productivity increases when people can have access to data in any location within the operating range of their WLAN. Management decisions based on real-time information can significantly improve the efficiency of a worker.
- **Low implementation costs** - WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLAN's ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.
- **Installation and network expansion** - by avoiding the complications of troublesome cables, a WLAN system can be fast and easy during installation, especially since it can eliminate the need to pull cable through walls and ceilings. Wireless technology provides more versatility by extending the network beyond the home or office.
- **Inexpensive solution** - wireless network devices are as competitively priced as conventional Ethernet network devices. The DIS-2650AP 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 DIS-2650AP. 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.

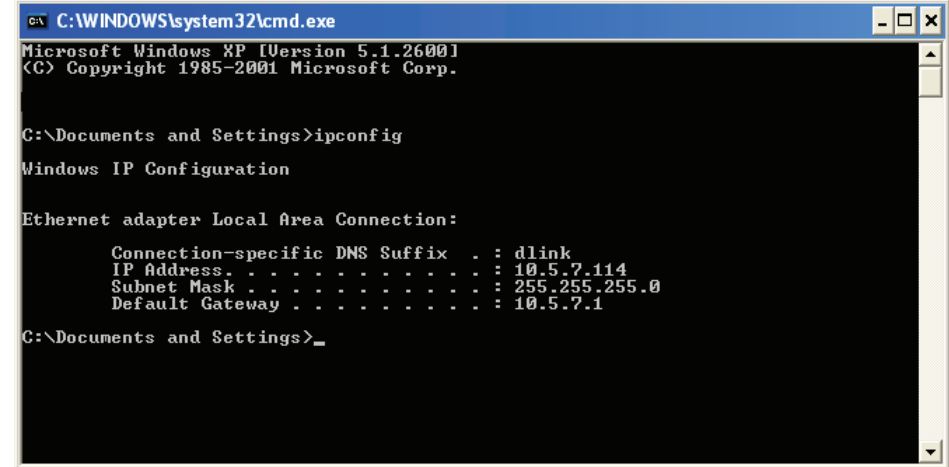
Click on Start > Run. In the run box type cmd and click OK.

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:

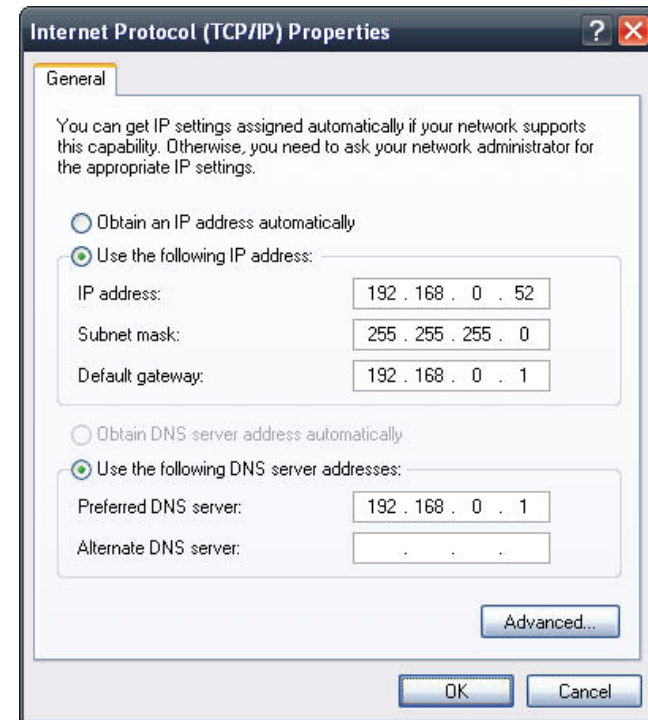
Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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 802.11ac
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3b
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3az
- IEEE 802.3af

Network Management

- Web Browser interface (HTTP, Secure HTTP (HTTPS))
- Nuclias Connect

Security

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

Wireless Frequency Range

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

Power Input

- 12 to 48 V DC terminal block dual input
- 802.3at PoE

Antenna Type

- 2x Detachable 2.5 dBi Omni antennas @2.4GHz
- 2x Detachable 3 dBi Omni antennas @5GHz

LED Displays

- PWR1/PWR2/POE/ALARM/2.4G/5G/STATUS/SIGNAL

Temperature

- Operating: -20°C to 65°C
- Storing: -40°C to 80°C

Humidity

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

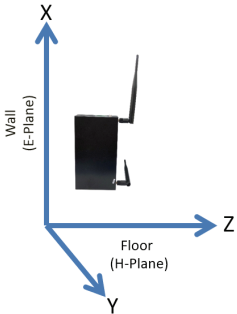
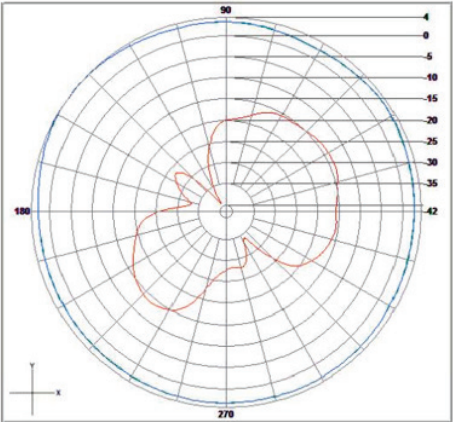
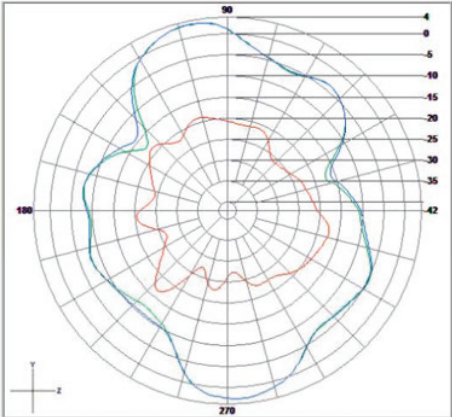
Certifications

- FCC
- CE
- NCC

Dimensions

- L = 196.2 mm
- W = 105.9 mm
- H = 40 mm

Antenna Patterns

Antenna Patterns		
Orientation	H-Plane	E-Plane
2.4 GHz Wall/DIN-rail Mounted 		
5 GHz Wall/DIN-rail Mounted 