D-Link®

Version 1.0 | 02/28/2014

User Manual

Wireless AC1200

Dual Band Gigabit Range Extender

DAP-1650

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
1.0	February 28, 2014	• Initial release for Revision A1

Trademarks

Table of Contents

Product Overview

Package Contents

DAP-1650 Wireless AC1200 Dual Band Gigabit Range Extender

Ethernet Cable

Power Adapter

Wi-Fi Configuration Card

Quick Install Guide

If any of the above items are missing, please contact your reseller.

Note: *Using a power supply with a different voltage rating than the one included with the DAP-1650 will cause damage and void the warranty for this product.*

Minimum Requirements

Network Requirements	• An Ethernet-based Network • IEEE 802.11ac/n/g/a wireless clients (AP/Extender Mode) • IEEE 802.11ac/n/g/a wireless network (Extender/Media Bridge Mode) • 10/100/1000 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows® 8, 7, Vista®, XP (SP3), Mac OS® X (10.5 or higher) • An installed Ethernet adapter or Wireless adapter **Browser Requirements:** • Internet Explorer® 7.0 or higher • Firefox® 20.0 or higher • Chrome™ 20.0 or higher • Safari® 5.0 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
Mobile App Requirements	• QRS Mobile App requires iOS 4.3 or Android 2.0
For Internet Access	• A Router • Broadband Internet Connection

Introduction

The DAP-1650 Wireless AC1200 Dual Band Gigabit Range Extender gives you the ability to transfer files at a maximum combined wireless signal rate of up to 1200 Mbps[1], delivering high-speed wireless network access for your home or office.

The DAP-1650 is compliant with the latest draft IEEE 802.11ac standard, meaning that it can connect with other 802.11ac compatible wireless client devices. It is also backward compatible with 802.11g and 802.11n devices. It can be flexibly configured to operate in three different modes: *Access Point*, *Extender,* and *Media Bridge*.

The DAP-1650 features Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) providing an enhanced level of security for wireless data communications. The DAP-1650 also supports Wi-Fi Protected Setup (WPS), using either the PIN or Push Button methods.

[1] Maximum wireless signal rate derived from draft 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range. Wireless range and speed rates are D-Link RELATIVE performance measurements based on the wireless range and speed rates of a standard Wireless N product from D-Link.

Features

- **Faster Wireless Networking -** The DAP-1650 provides combined wireless speeds of up to 1200 Mbps[1]. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Flexible Operation Modes -** The DAP-1650 can operate as an Extender, Access Point or Media Bridge, meaning that you can customize its operation to suit your specific networking requirements.

- **Gigabit Ethernet Ports** - The built-in Gigabit Ethernet ports facilitate a wired connection of up to 1 Gbps, meaning that wired devices can also take advantage of the DAP-1650's high-speed wireless capabilities.

- **Compatible with IEEE 802.11n**, **802.11g**, and **802.11a Devices -** The DAP-1650 is still fully compatible with the 802.11n/g/a standards, so it can connect with existing wireless adapters found on older devices.

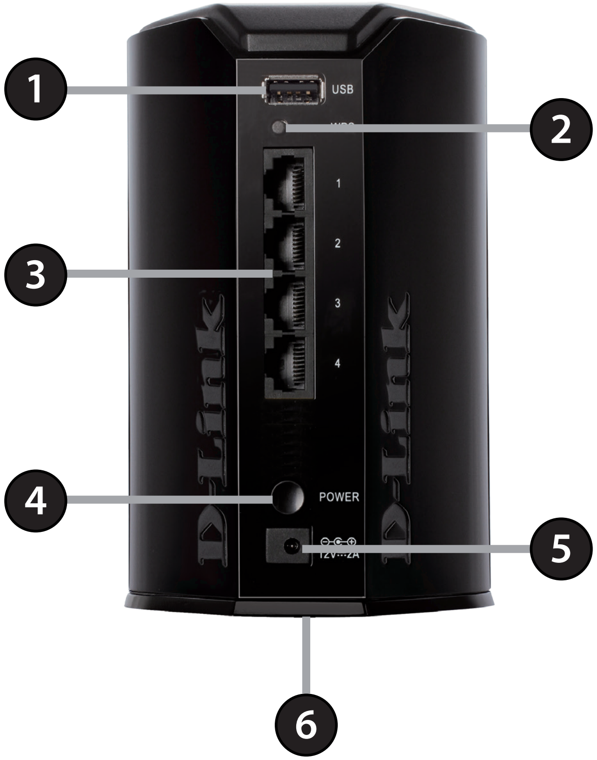
- **Robust Security -** Use WPS (Wi-Fi Protected Setup™) to create a secure connection to new devices in a matter of seconds by simply pushing a button or entering a PIN. There's also WPA/WPA2 security encryption, allowing you to customize your network's security.

- **User-friendly Setup Wizard -** Through its easy-to-use web-based user interface, the DAP-1650 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server.

[1] Maximum wireless signal rate derived from draft 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range. Wireless range and speed rates are D-Link RELATIVE performance measurements based on the wireless range and speed rates of a standard Wireless N product from D-Link.

Hardware Overview

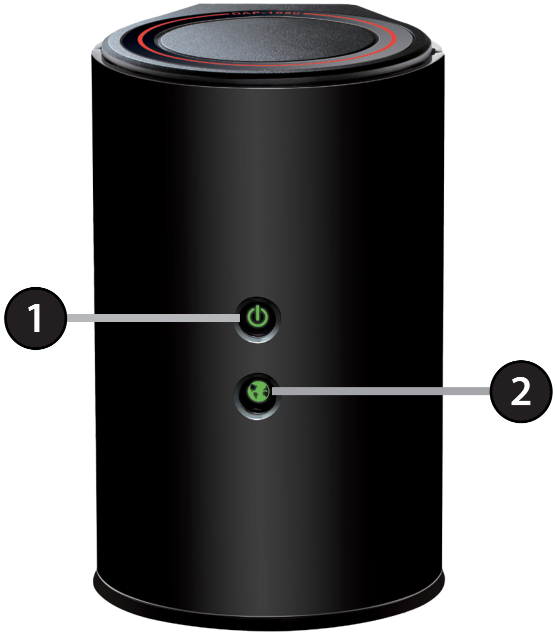
Connections



1	**USB Port**	Connect a USB storage device to share files. (Only in *Access Point* mode.)
2	**WPS Button**	Use WPS (Wi-Fi Protected Setup) to easily create a secure connection to new devices.
3	**Ethernet Ports (1-4)**	Connect Ethernet devices such as computers, switches, gaming consoles, network storage (NAS), and media players to your wireless network.
4	**Power Switch**	Press to power the device on or off.
5	**Power Port**	Plug the supplied power adapter into the power port, and connect to a power outlet.
6	**Reset Button (bottom)**	Press and hold the reset button for a minimum of six seconds to return the device back to the factory default settings.

Hardware Overview

LEDs



LED	Color	Status	Description
Power LED	Orange	Solid	The DAP-1650 is powering on or booting up.
		Blinking	The device is in recovery mode.
	Green	Solid	The device is on and functioning properly.
		Blinking	The WPS button has been pushed and the device is processing a connection.
Internet LED	Green	Solid	A successful connection has been established.*
	Orange	Blinking	Either the device is not establishing a connection with the router or a firmware upgrade is in progress.
	Off		The device is being reset to the factory default settings.

Note: *When the LED turns solid green, this indicates that the DAP-1650 is securely connected to your wireless router or access point.*

Operation Modes

The DAP-1650 features three operational modes, enabling you to customize the device to your networking requirements. Refer to the following pages to determine which mode is best for you.

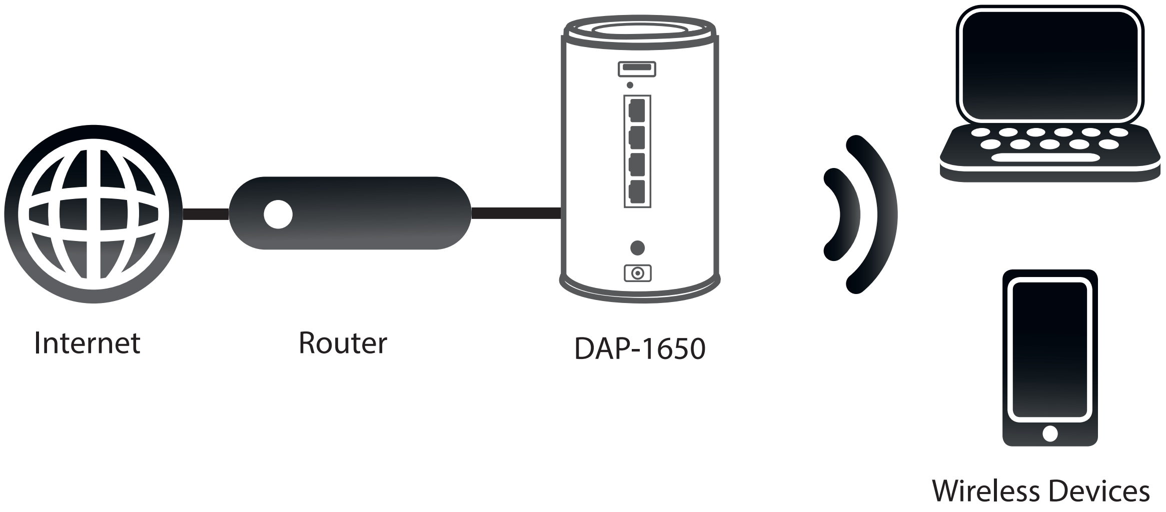
- Access Point mode - page 11
- Extender mode - page 12
- Media Bridge mode - page 13

Access Point Mode

Use *Access Point* (AP) mode to connect wireless clients (like laptops, tablets and smartphones) to your existing wired network. Multiple clients can connect wirelessly to the network at the same time.

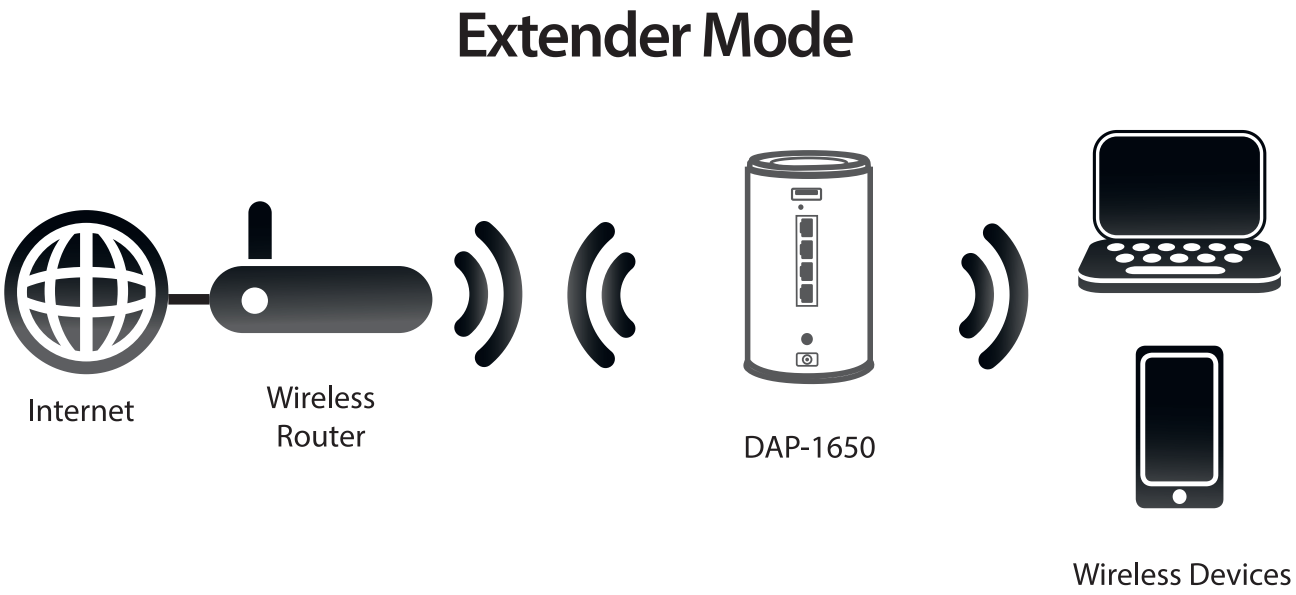
The DAP-1650 acts as a central connection point for any wireless client that has an 802.11ac or backward compatible 802.11n, 802.11g, or 802.11a wireless network interface, and is within range of the AP. From your wireless device, go to the **Wireless Utility** and select the **Wi-Fi Network Name** (SSID) broadcast by the access point in order to wirelessly access the network. If wireless security is enabled on the AP, you must enter a password to connect to the Wi-Fi Network.

AP Mode



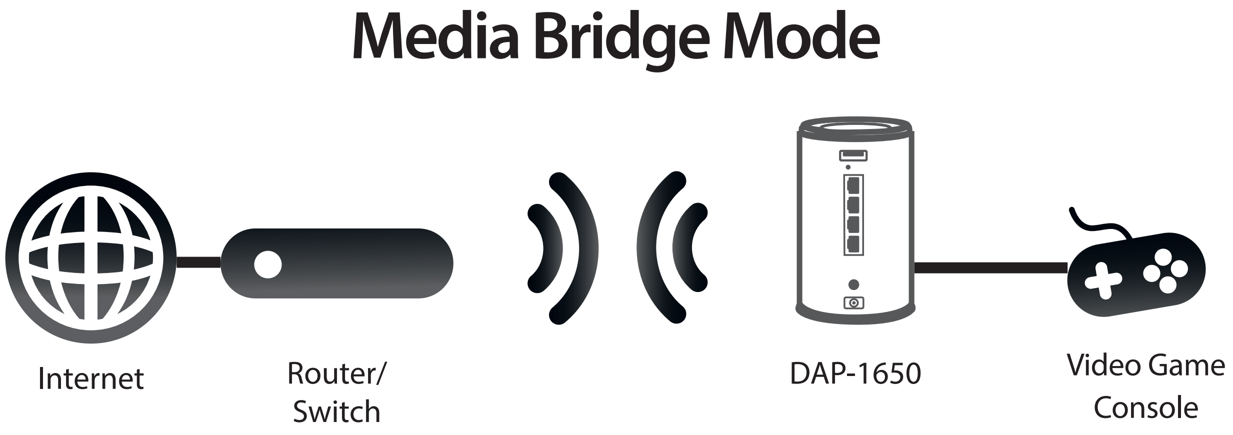
Extender Mode

Use *Extender* mode, to extend the range of your existing wireless network by repeating the wireless signal of another access point or wireless router. The DAP-1650 and wireless router (if used) must be within range of each other. The extended wireless network can use the same Wi-Fi Network Name (SSID) and security settings as the existing network, or you can choose to specify a new network name and security method.



Media Bridge Mode

In *Media Bridge* mode, the DAP-1650 creates a wireless link between two existing networks, enabling you to attach a wired device to a wireless network. The two networks must be within wireless reach of one another in order for *Media Bridge* mode to be effective.



Wireless Installation Considerations

The DAP-1650 lets you access your network using a wireless connection from virtually anywhere within the operating range of the device. 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:

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

- Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it appears 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.

- Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

- If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may also be affected. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Configuration

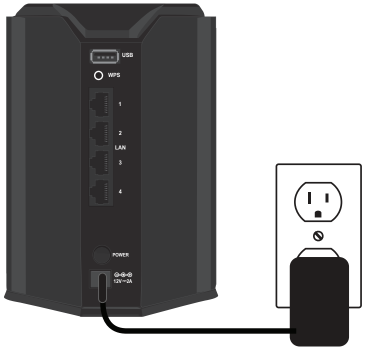
There are three options for configuring your DAP-1650:

- WPS (Wi-Fi Protected Setup) for *Extender* Mode only
- Web-based Configuration
- QRS Mobile (Refer to "QRS Mobile App Setup" on page 29.)

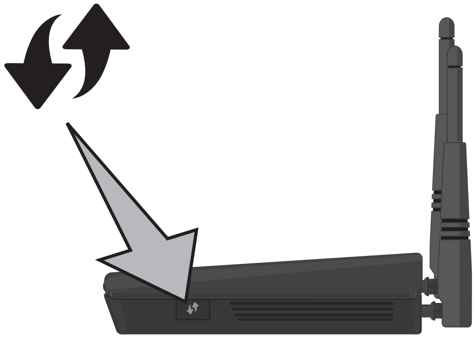
Connect to Your Router Using WPS

By default, your DAP-1650 will be set to *Extender* Mode. WPS is a simple and secure way to connect the extender to your router.

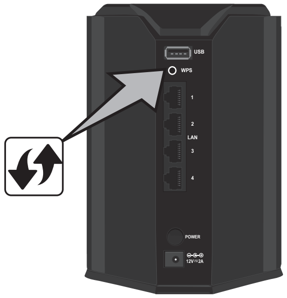
Find an available outlet near your wireless router. Plug in the DAP-1650 and wait until the Power LED turns solid green.



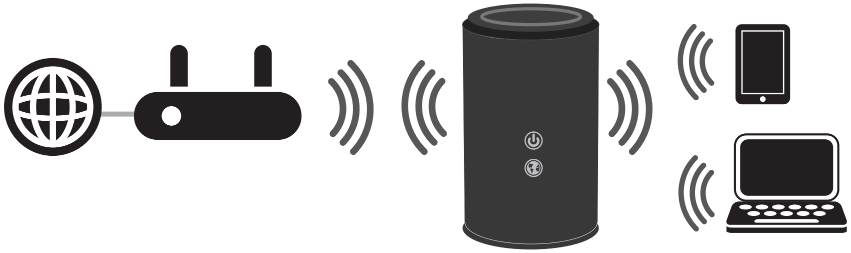
Press the WPS button on your wireless router. (Refer to the user manual for the router you want to connect to make sure you understand how to enable WPS.)



Within one minute, press the WPS button on the DAP-1650. The Power LED will start to blink. The Power and Internet LEDs will be solid green when a successful connection has been established with the router and the device is functioning properly.

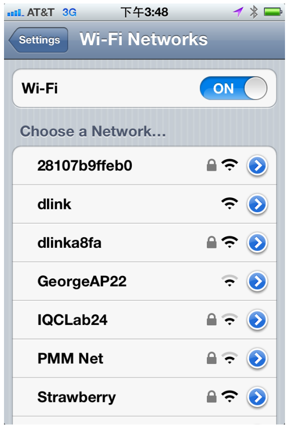


You can now unplug and move the DAP-1650 to a location between your wireless router and the area that you need wireless coverage.



Connect Your Wireless Devices

From your wireless device, go to the **Wireless Utility** to display the available networks and select the new **Wi-Fi Name** (SSID) that appears.



AT&T 3G 下午3:48

Settings Wi-Fi Networks

Wi-Fi ON

Choose a Network...

28107b9ffeb0
dlink
dlinka8fa
GeorgeAP22
IQCLab24
PMM Net
Strawberry

When using WPS to connect to the router, the SSID on the DAP-1650 will automatically be assigned the following:

- 2.4GHz (Your Router's SSID) - EXT
- 5GHz (Your Router's SSID) - EXT5G
-

The **Wi-Fi Password** for your router will be the same for the DAP-1650.

Repeat this process to connect additional Wi-Fi devices to the DAP-1650.

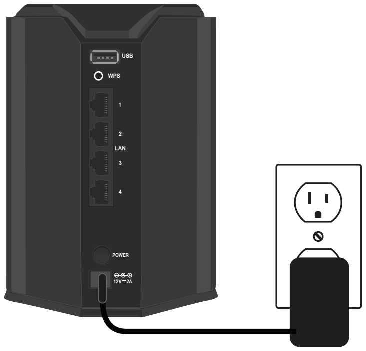
In order to change the default settings or adjust the configuration of the DAP-1650, use the web-based configuration utility. Refer to page 18 for more information.

Configure the DAP-1650 Using a Web Browser

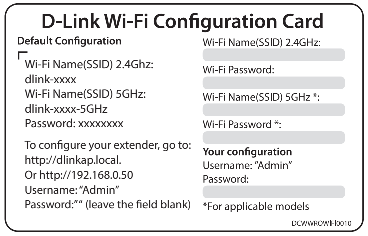
Use the web-based configuration utility on the DAP-1650 to do the following:

- Run the Setup Wizard
- Change the Wireless and Network Settings

Plug the DAP-1650 into an available outlet near your router. You may move it to a more suitable location after configuration.



Open the wireless utility on your wireless device or computer. Select the **Wi-Fi Name** (from the *Wi-Fi Configuration Card*) and enter the **password**.



D-Link Wi-Fi Configuration Card

Default Configuration

Wi-Fi Name(SSID) 2.4Ghz:
dlink-xxxx
Wi-Fi Name(SSID) 5GHz:
dlink-xxxx-5GHz
Password: xxxxxxxx

To configure your extender, go to:
http://dlinkap.local.
Or http://192.168.0.50
Username: "Admin"
Password:"" (leave the field blank)

Wi-Fi Name(SSID) 2.4GHz:

Wi-Fi Password:

Wi-Fi Name(SSID) 5GHz *:

Wi-Fi Password *:

Your configuration
Username: "Admin"
Password:

*For applicable models

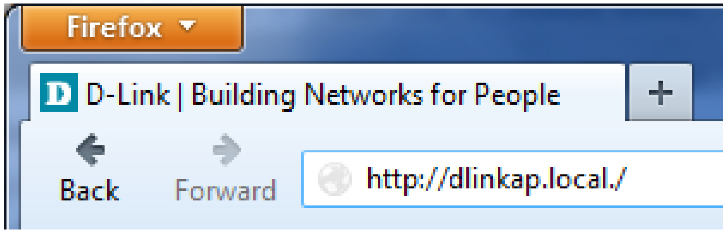
DCWWROWIFI0010

Web-based Configuration Utility

In order to change the default settings or adjust the configuration of the DAP-1650, use the web-based configuration utility. By default, your DAP-1650 will be set to Extender mode.

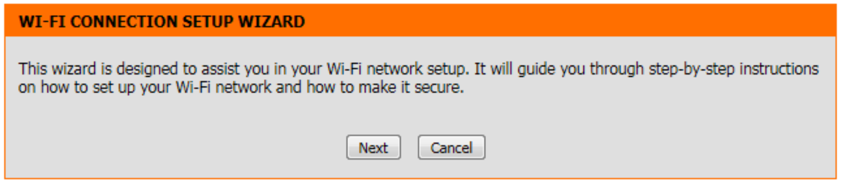
Open a web browser (e.g., Internet Explorer, Firefox, Safari, or Chrome) and enter **http://dlinkap.local./**. You may also enter the IP address* of the DAP-1650. Windows XP users should enter **http://dlinkap**.

** The default IP address is 192.168.0.50. Once the DAP-1650 connects to your router, it will get assigned a new IP address based on your router/network's DHCP settings. You need to log in to your router and view the DHCP table to see what IP address was assigned to the DAP-1650. The MAC address is printed on the label on the DAP-1650.*



http://dlinkap.local./

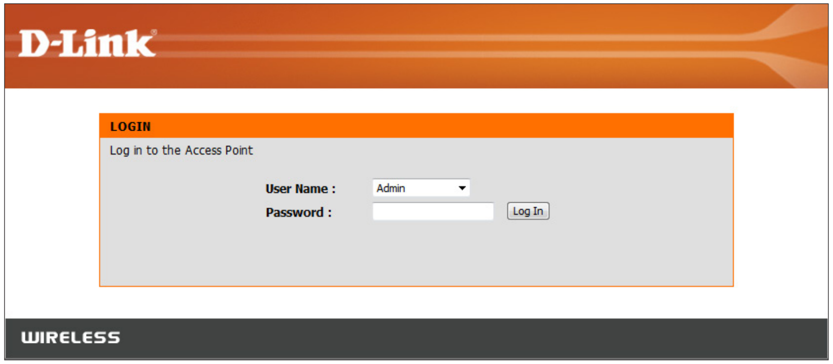
The first time you connect, the DAP-1650 will automatically launch the *Wi-Fi Connection Setup Wizard*. Instructions for the wizard begin on the next page.



WI-FI CONNECTION SETUP WIZARD

This wizard is designed to assist you in your Wi-Fi network setup. It will guide you through step-by-step instructions on how to set up your Wi-Fi network and how to make it secure.

Note:** The next time you go to the configuration utility, you will see the login screen. By default the password is blank. Click **Log in.



LOGIN

Log in to the Access Point

User Name : Admin

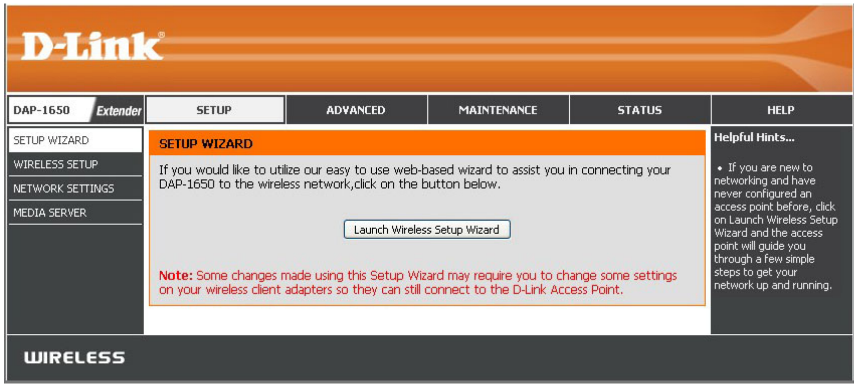
Password :

If you get a *Page Cannot be Displayed* error, refer to "Troubleshooting" on page 103 for assistance.

Wireless Setup Wizard

From **Setup** > **Setup Wizard**, click **Launch Wireless Setup Wizard** to configure your DAP-1650.

If you want to configure the device manually without running the wizard, skip to ”Manual Configuration” on page 30.



SETUP WIZARD

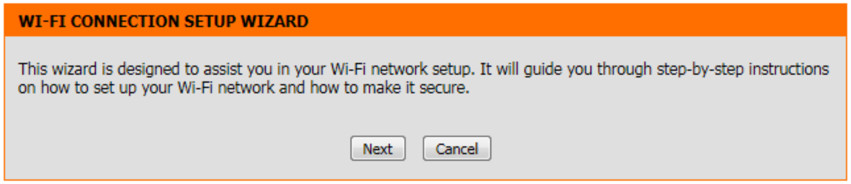
If you would like to utilize our easy to use web-based wizard to assist you in connecting your DAP-1650 to the wireless network,click on the button below.

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Access Point.

Helpful Hints...

- If you are new to networking and have never configured an access point before, click on Launch Wireless Setup Wizard and the access point will guide you through a few simple steps to get your network up and running.

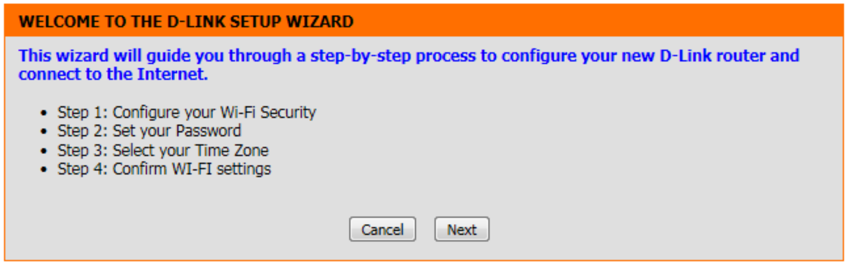
Click **Next** to continue.



WI-FI CONNECTION SETUP WIZARD

This wizard is designed to assist you in your Wi-Fi network setup. It will guide you through step-by-step instructions on how to set up your Wi-Fi network and how to make it secure.

Click **Next** to continue.



WELCOME TO THE D-LINK SETUP WIZARD

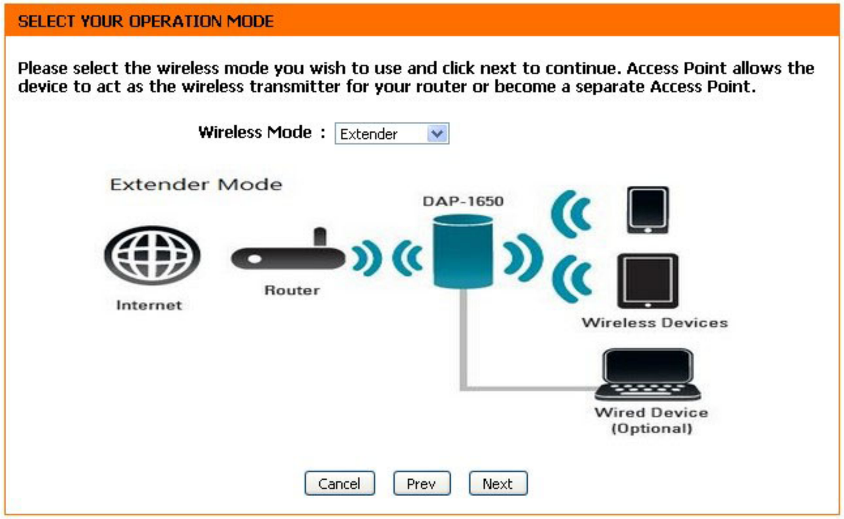
This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

- Step 1: Configure your Wi-Fi Security
- Step 2: Set your Password
- Step 3: Select your Time Zone
- Step 4: Confirm WI-FI settings

Extender Mode

The DAP-1650 can be configured to operate in three different modes: *Access Point*, *Extender* and *Media Bridge*. By default, the device will be set to **Extender** mode, extending the range of your existing wireless network. For *Access Point* mode, refer to "Access Point Mode" on page 23. For *Media Bridge* mode, refer to "Media Bridge Mode" on page 26.

Extender is the default *Wireless Mode*. Click **Next** to continue.



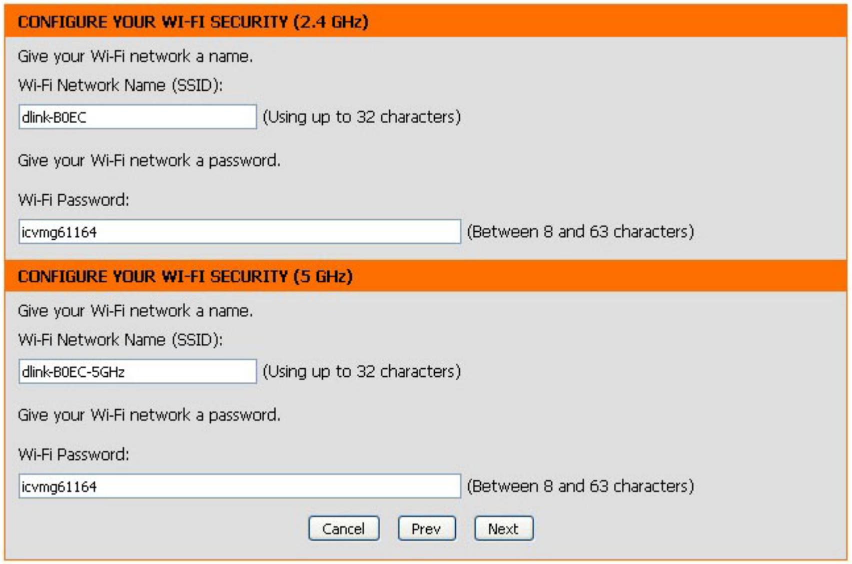
SELECT YOUR OPERATION MODE

Please select the wireless mode you wish to use and click next to continue. Access Point allows the device to act as the wireless transmitter for your router or become a separate Access Point.

Wireless Mode : Extender

The configuration screen will allow you to enter a **Wi-Fi Network Name** (SSID) and a **Wi-Fi Password** for your wireless network. Specify an SSID for both the 2.4GHz and 5GHz bands. While it is possible to use the same wireless security password for both networks, we recommend that you use a different password for each.

Click **Next** to continue.



CONFIGURE YOUR WI-FI SECURITY (2.4 GHz)

Give your Wi-Fi network a name.

Wi-Fi Network Name (SSID): dlink-B0EC (Using up to 32 characters)

Give your Wi-Fi network a password.

Wi-Fi Password: icvmg61164 (Between 8 and 63 characters)

CONFIGURE YOUR WI-FI SECURITY (5 GHz)

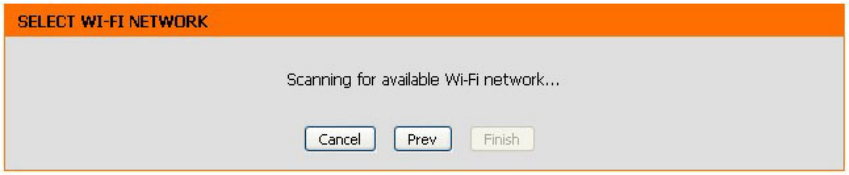
Give your Wi-Fi network a name.

Wi-Fi Network Name (SSID): dlink-B0EC-5GHz (Using up to 32 characters)

Give your Wi-Fi network a password.

Wi-Fi Password: icvmg61164 (Between 8 and 63 characters)

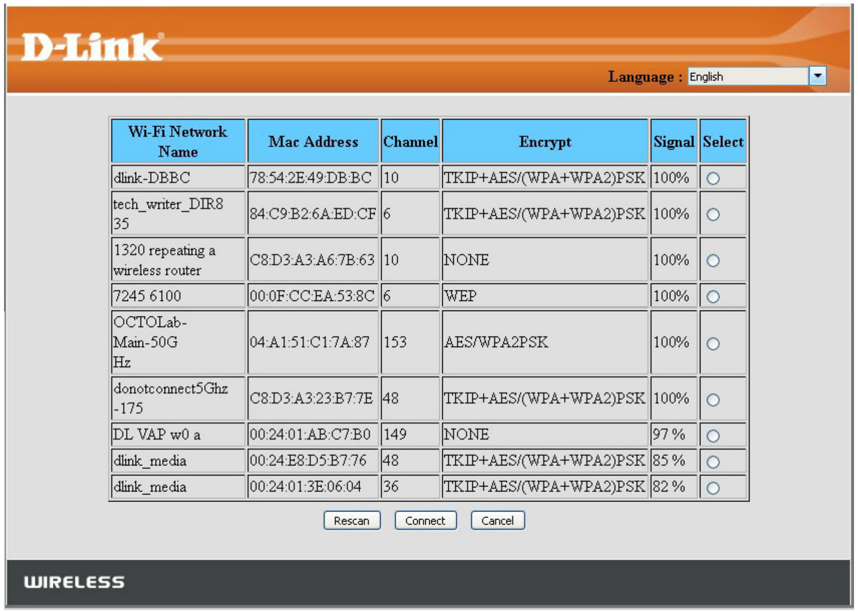
The wizard will scan for available wireless networks.



SELECT WI-FI NETWORK

Scanning for available Wi-Fi network...

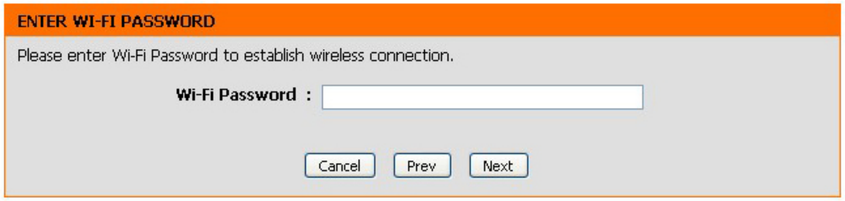
Select the **Wi-Fi Network** you wish to connect to and click **Connect**.



Language : English

Wi-Fi Network Name	Mac Address	Channel	Encrypt	Signal	Select
dlink-DBBC	78:54:2E:49:DB:BC	10	TKIP+AES/(WPA+WPA2)PSK	100%	○
tech_writer_DIR8 35	84:C9:B2:6A:ED:CF	6	TKIP+AES/(WPA+WPA2)PSK	100%	○
1320 repeating a wireless router	C8:D3:A3:A6:7B:63	10	NONE	100%	○
7245 6100	00:0F:CC:EA:53:8C	6	WEP	100%	○
OCTOLab-Main-50G Hz	04:A1:51:C1:7A:87	153	AES/WPA2PSK	100%	○
donotconnect5Ghz -175	C8:D3:A3:23:B7:7E	48	TKIP+AES/(WPA+WPA2)PSK	100%	○
DL VAP w0 a	00:24:01:AB:C7:B0	149	NONE	97 %	○
dlink_media	00:24:E8:D5:B7:76	48	TKIP+AES/(WPA+WPA2)PSK	85 %	○
dlink_media	00:24:01:3E:06:04	36	TKIP+AES/(WPA+WPA2)PSK	82 %	○

If the wireless network is password protected, enter your **Password** for that wireless network and click **Next**.



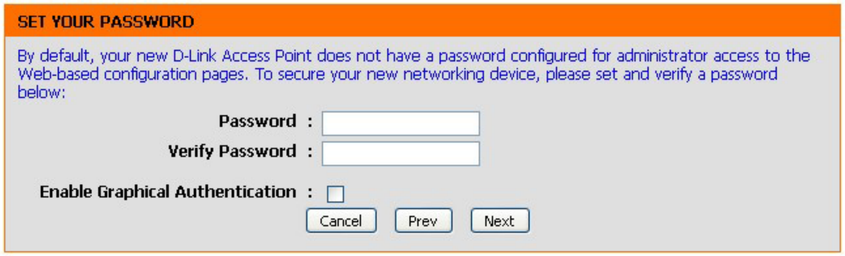
ENTER WI-FI PASSWORD

Please enter Wi-Fi Password to establish wireless connection.

Wi-Fi Password :

Create a **Password** for administrator access to the web-based configuration utility.

Check the **Enable Graphical Authentication** box to enable CAPTCHA authentication for added security. Click **Next** to continue.



SET YOUR PASSWORD

By default, your new D-Link Access Point does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:

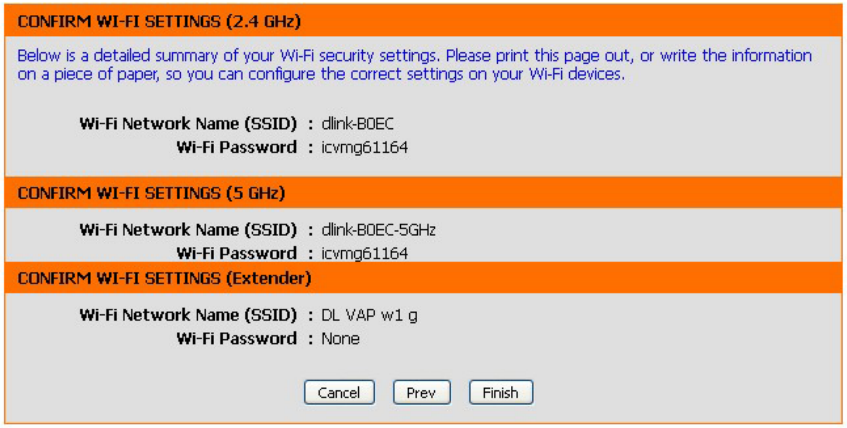
Password :

Verify Password :

Enable Graphical Authentication : □

A summary page will be displayed, showing the current settings for your 2.4GHz and 5GHz wireless networks. Make a note of this information for future reference.

Click **Finish** to save your network settings.



CONFIRM WI-FI SETTINGS (2.4 GHz)

Below is a detailed summary of your Wi-Fi security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your Wi-Fi devices.

Wi-Fi Network Name (SSID) : dlink-B0EC
Wi-Fi Password : icvmg61164

CONFIRM WI-FI SETTINGS (5 GHz)

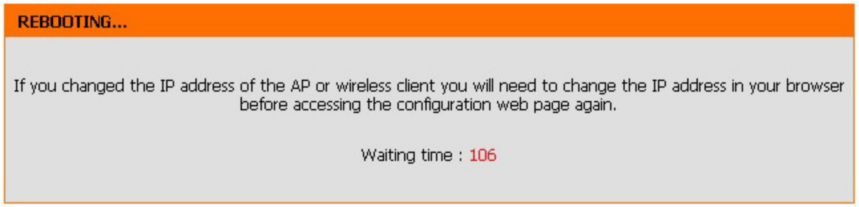
Wi-Fi Network Name (SSID) : dlink-B0EC-5GHz
Wi-Fi Password : icvmg61164

CONFIRM WI-FI SETTINGS (Extender)

Wi-Fi Network Name (SSID) : DL VAP w1 g
Wi-Fi Password : None

In order for your network settings to take effect the extender will reboot automatically.

When the device has finished rebooting the main screen will display.



REBOOTING...

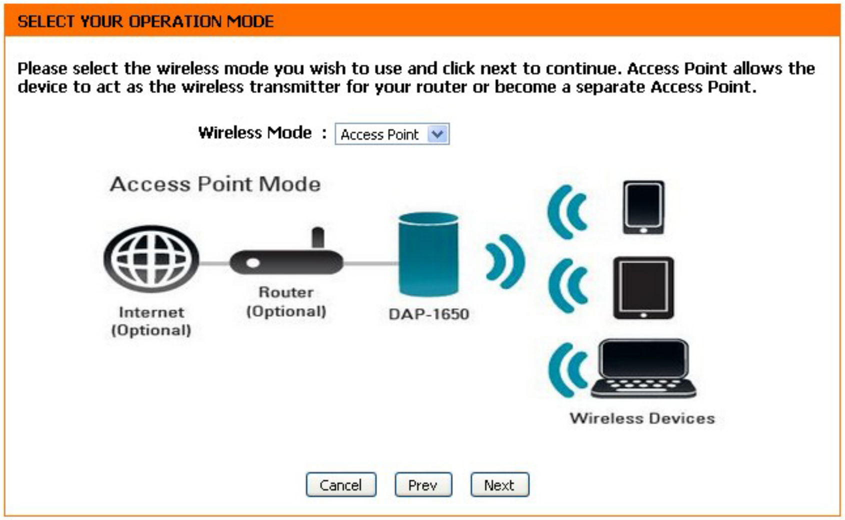
If you changed the IP address of the AP or wireless client you will need to change the IP address in your browser before accessing the configuration web page again.

Waiting time : 106

Access Point Mode

The DAP-1650 can be configured to operate in three different modes: *Access Point*, *Extender* and *Media Bridge*. Select **Access Point** (AP) mode to connect wireless clients (like laptops, tablets and smartphones) to your existing wired network.

Select **Access Point** from the drop-down menu. Then, click **Next** to continue.



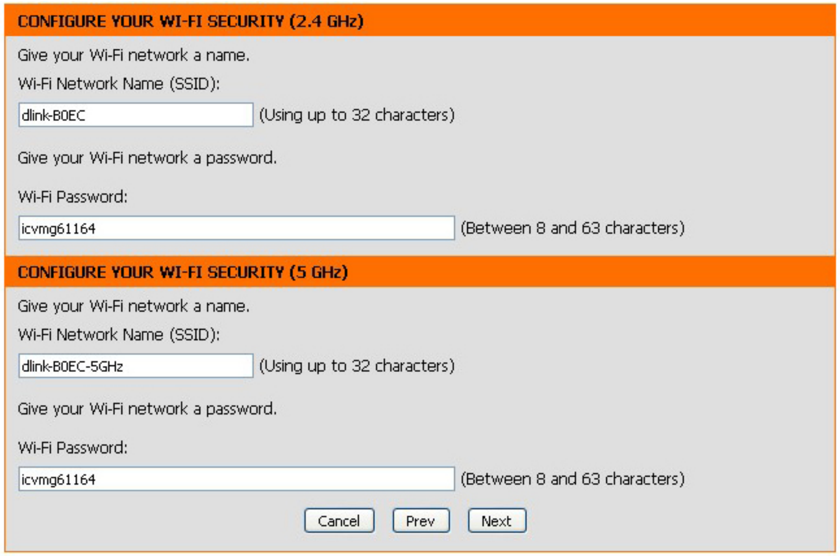
SELECT YOUR OPERATION MODE

Please select the wireless mode you wish to use and click next to continue. Access Point allows the device to act as the wireless transmitter for your router or become a separate Access Point.

Wireless Mode : Access Point

This screen will allow you to enter a **Wi-Fi Network Name** (SSID) and a **Wi-Fi Password** for your wireless network. Specify an SSID for both the 2.4GHz and 5GHz bands. While it is possible to use the same wireless security password for both networks, we recommend that you use a different password for each.

Click **Next** to continue.



CONFIGURE YOUR WI-FI SECURITY (2.4 GHz)

Give your Wi-Fi network a name.

Wi-Fi Network Name (SSID):

dlink-B0EC (Using up to 32 characters)

Give your Wi-Fi network a password.

Wi-Fi Password:

icvmg61164 (Between 8 and 63 characters)

CONFIGURE YOUR WI-FI SECURITY (5 GHz)

Give your Wi-Fi network a name.

Wi-Fi Network Name (SSID):

dlink-B0EC-5GHz (Using up to 32 characters)

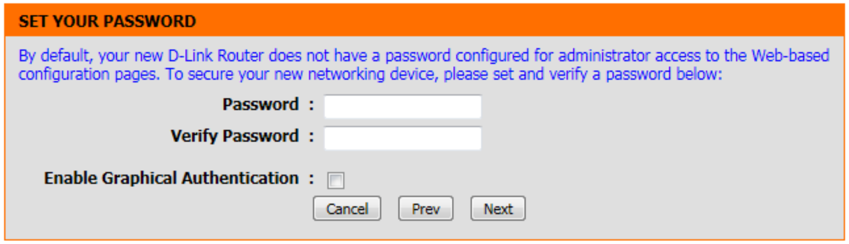
Give your Wi-Fi network a password.

Wi-Fi Password:

icvmg61164 (Between 8 and 63 characters)

Create a **Password** for administrator access to the web-based configuration utility.

Check the **Enable Graphical Authentication** box to enable CAPTCHA authentication for added security. Click **Next** to continue.



SET YOUR PASSWORD

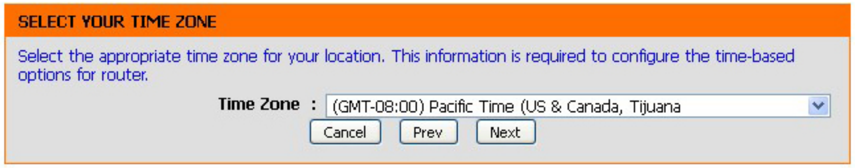
By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

Enable Graphical Authentication : □

Select your **Time Zone** from the drop-down menu and click **Next** to continue.



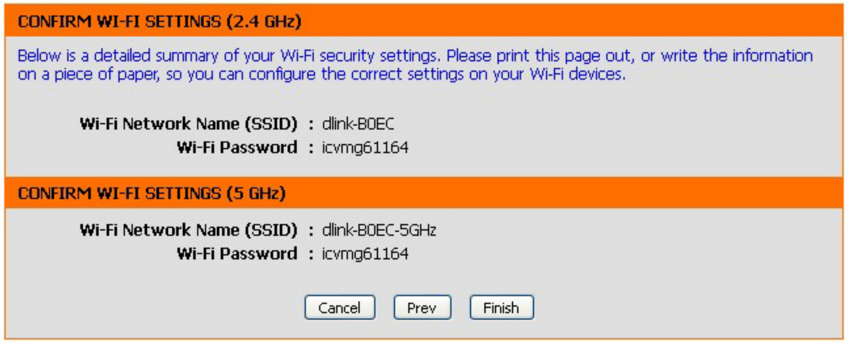
SELECT YOUR TIME ZONE

Select the appropriate time zone for your location. This information is required to configure the time-based options for router.

Time Zone : (GMT-08:00) Pacific Time (US & Canada, Tijuana

A summary page will be displayed, showing the current settings for your 2.4GHz and 5GHz wireless networks. Make a note of this information for future reference.

Click **Finish** to save your network settings.



CONFIRM WI-FI SETTINGS (2.4 GHz)

Below is a detailed summary of your Wi-Fi security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your Wi-Fi devices.

Wi-Fi Network Name (SSID) : dlink-B0EC

Wi-Fi Password : icvmg61164

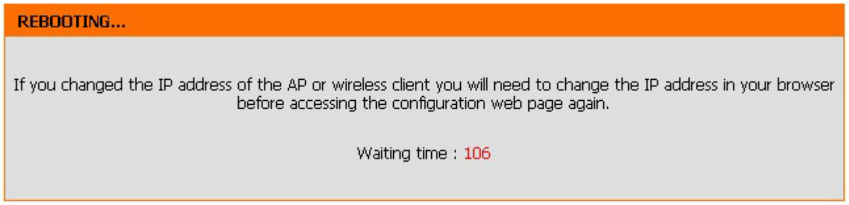
CONFIRM WI-FI SETTINGS (5 GHz)

Wi-Fi Network Name (SSID) : dlink-B0EC-5GHz

Wi-Fi Password : icvmg61164

In order for your network settings to take effect the AP will reboot automatically.

When the device has finished rebooting the main screen will display.



REBOOTING...

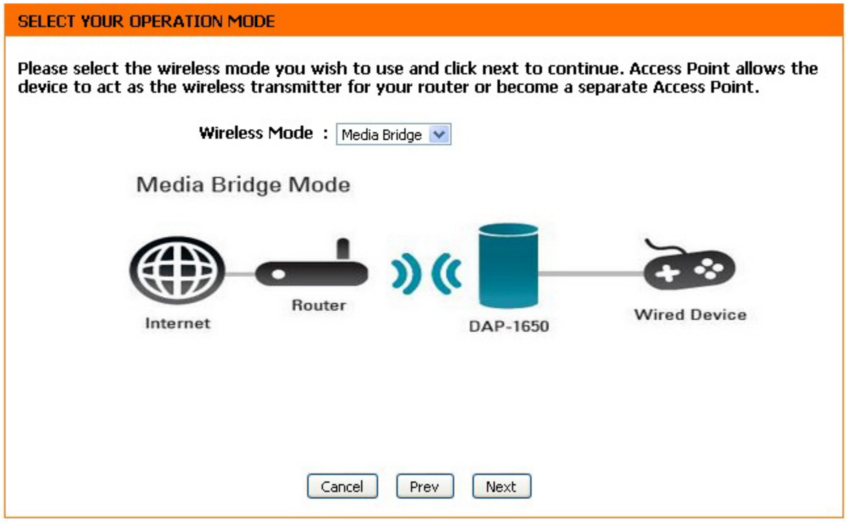
If you changed the IP address of the AP or wireless client you will need to change the IP address in your browser before accessing the configuration web page again.

Waiting time : 106

Media Bridge Mode

The DAP-1650 can be configured to operate in three different modes: *Access Point*, *Extender* and *Media Bridge*. Select **Media Bridge** to attach a wired device to a wireless network.

Select **Media Bridge** from the drop-down menu. Click **Next** to continue.

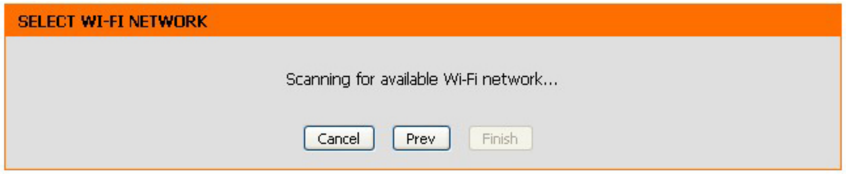


SELECT YOUR OPERATION MODE

Please select the wireless mode you wish to use and click next to continue. Access Point allows the device to act as the wireless transmitter for your router or become a separate Access Point.

Wireless Mode : Media Bridge

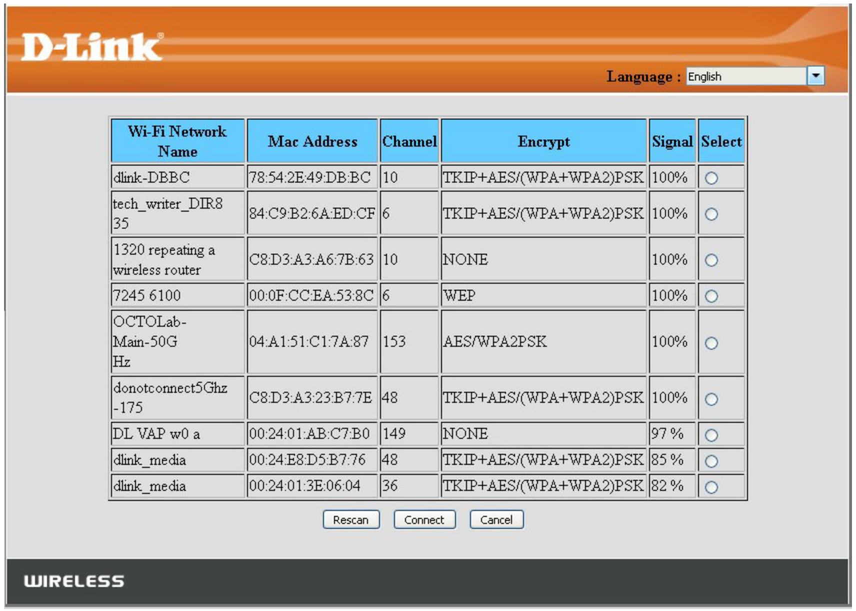
The wizard will scan for available wireless networks.



SELECT WI-FI NETWORK

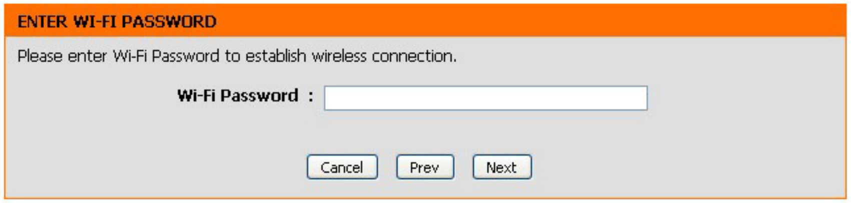
Scanning for available Wi-Fi network...

Select the **Wi-Fi Network** you wish to connect to and click **Connect**.



Wi-Fi Network Name	Mac Address	Channel	Encrypt	Signal	Select
dlink-DBBC	78:54:2E:49:DB:BC	10	TKIP+AES/(WPA+WPA2)PSK	100%	○
tech_writer_DIR835	84:C9:B2:6A:ED:CF	6	TKIP+AES/(WPA+WPA2)PSK	100%	○
1320 repeating a wireless router	C8:D3:A3:A6:7B:63	10	NONE	100%	○
7245 6100	00:0F:CC:EA:53:8C	6	WEP	100%	○
OCTOLab-Main-50GHz	04:A1:51:C1:7A:87	153	AES/WPA2PSK	100%	○
donotconnect5Ghz-175	C8:D3:A3:23:B7:7E	48	TKIP+AES/(WPA+WPA2)PSK	100%	○
DL VAP w0 a	00:24:01:AB:C7:B0	149	NONE	97 %	○
dlink_media	00:24:E8:D5:B7:76	48	TKIP+AES/(WPA+WPA2)PSK	85 %	○
dlink_media	00:24:01:3E:06:04	36	TKIP+AES/(WPA+WPA2)PSK	82 %	○

If the wireless network is password protected, enter your **Password** for that wireless network and click **Next**.

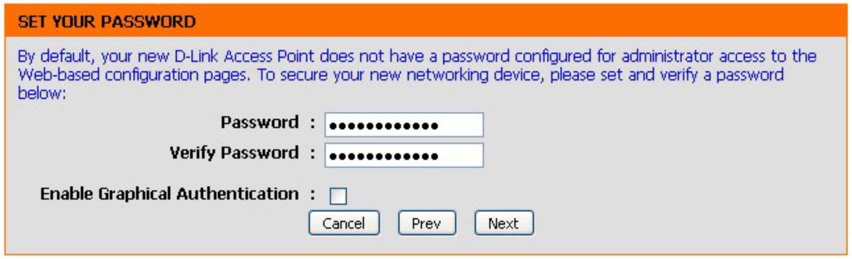


Please enter Wi-Fi Password to establish wireless connection.

Wi-Fi Password :

Create a **Password** for administrator access to the web-based configuration utility.

Check the **Enable Graphical Authentication** box to enable CAPTCHA authentication for added security. Click **Next** to continue.



By default, your new D-Link Access Point does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:

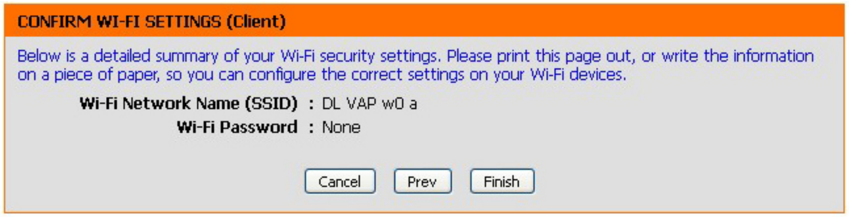
Password : •••••••••••••

Verify Password : •••••••••••••

Enable Graphical Authentication : □

A summary page will be displayed, showing the current settings for your wireless network. Make a note of this information for future reference.

Click **Finish** to save your network settings.



CONFIRM WI-FI SETTINGS (Client)

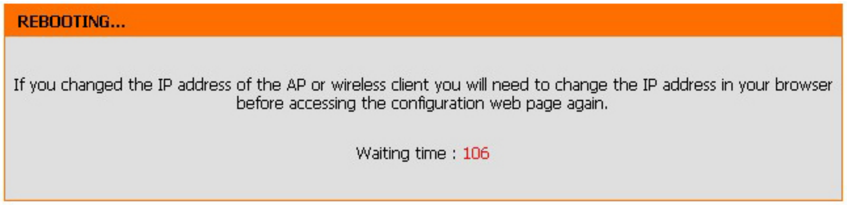
Below is a detailed summary of your Wi-Fi security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your Wi-Fi devices.

Wi-Fi Network Name (SSID) : DL VAP w0 a

Wi-Fi Password : None

In order for your network settings to take effect the media bridge will reboot automatically.

When the device has finished rebooting the main screen will display.



REBOOTING...

If you changed the IP address of the AP or wireless client you will need to change the IP address in your browser before accessing the configuration web page again.

Waiting time : 106

QRS Mobile App Setup

The DAP-1650 can be set up from your iOS or Android smartphone or tablet device using the QRS Mobile app.

From your mobile device, search for **QRS Mobile** in the App Store or Google Play. You may also find the app by scanning the QR codes on the right with a QR code reader.

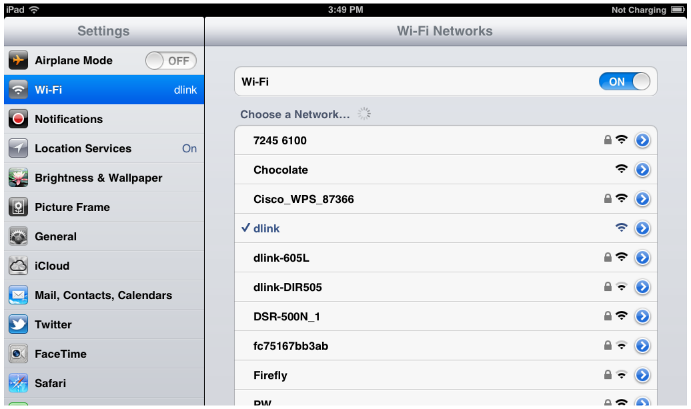
Download the **QRS Mobile** app from the App Store for your iOS device, or from Google Play for your Android device.

For iOS

For Android

Use the wireless utility on your device to connect to the Wi-Fi network that is displayed on the *Wi-Fi Configuration Card* included in the package with your DAP-1650 (ex: **dlink-a8fa).** Then, enter the Wi-Fi password also printed on the *Wi-Fi Configuration Card* (ex: **akbdj1936).**

Once you connect, launch the **QRS Mobile** app and it will guide you through the configuration of your DAP-1650.



iPad 3:49 PM Not Charging

Settings

Airplane Mode OFF
Wi-Fi dlink
Notifications
Location Services On
Brightness & Wallpaper
Picture Frame
General
iCloud
Mail, Contacts, Calendars
Twitter
FaceTime
Safari

Wi-Fi Networks

Wi-Fi ON

Choose a Network...

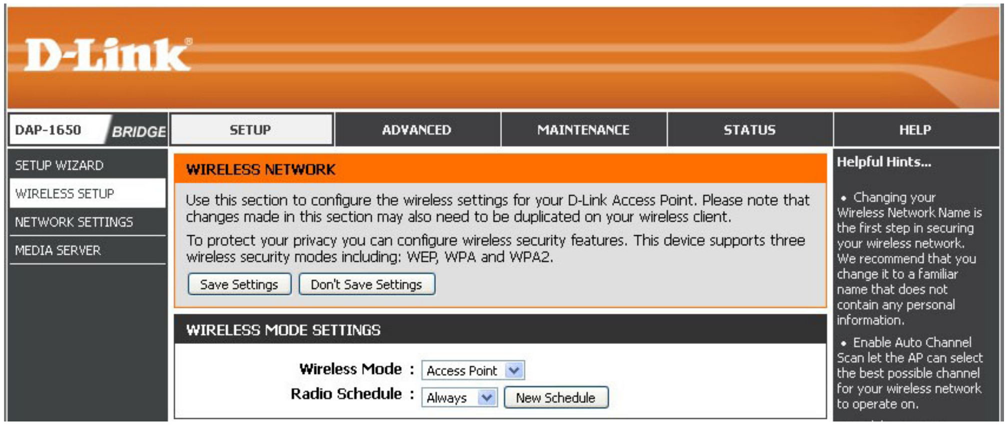
7245 6100
Chocolate
Cisco_WPS_87366
✓ dlink
dlink-605L
dlink-DIR505
DSR-500N_1
fc75167bb3ab
Firefly

Manual Configuration

Wireless Setup

Configure your DAP-1650 manually by navigating to **Setup** > **Wireless Setup**. Refer to the following pages for detailed instructions on how to manually configure the DAP-1650 for your preferred mode of operation.

- Access Point Mode - page 31
- Extender Mode - page 35
- Media Bridge Mode - page 39



WIRELESS NETWORK

Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made in this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

WIRELESS MODE SETTINGS

Wireless Mode : Access Point

Radio Schedule : Always

Helpful Hints...

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enable Auto Channel Scan let the AP can select the best possible channel for your wireless network to operate on.

Access Point Mode

2.4 GHz Band

Select **Access Point** (AP) mode to connect wireless clients (like laptops, tablets and smartphones) to your existing wired network.

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

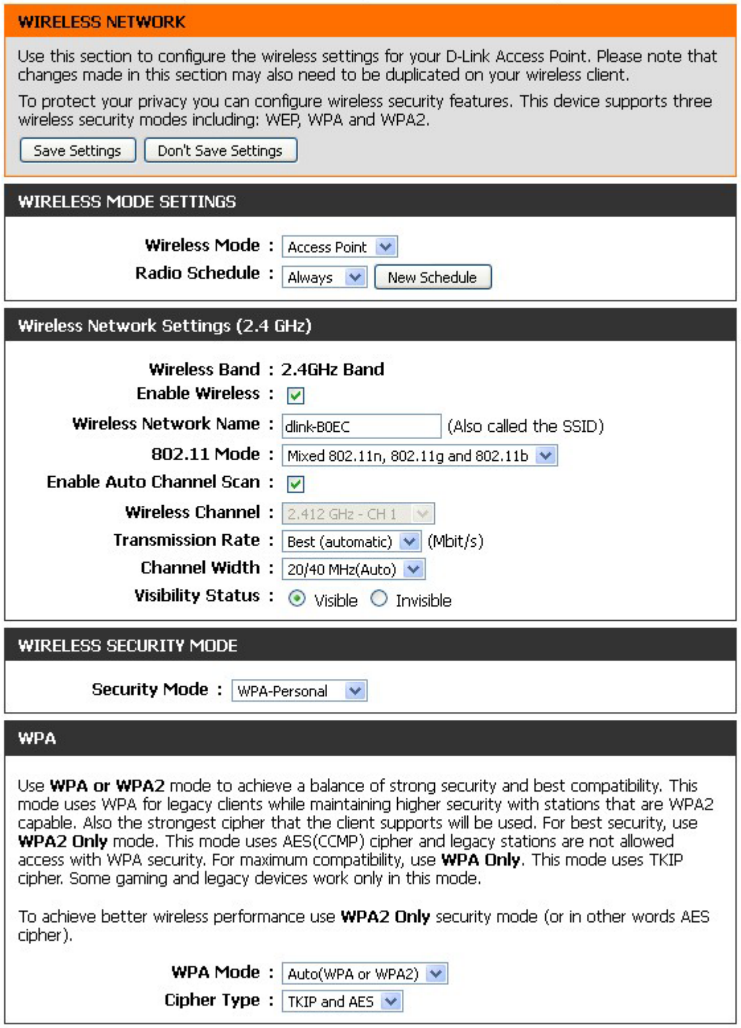
Radio Schedule: You may set up a specific schedule. Select a schedule from the drop-down menu or click **New Schedule** to create a new schedule. By default, the schedule is set to **Always**.

Enable Wireless: Check the box to **Enable** the wireless function for the **2.4GHz** band. You may uncheck the box to disable all wireless functions.

Wireless Network Name: Specify a **Network Name** (SSID) to identify the 2.4GHz network. This is the network name that wireless clients will search for when connecting to your wireless network.

802.11 Mode: Select one of the following:
802.11g Only - Select if you are only using 802.11g wireless clients.
802.11n Only - Select if you are only using 802.11n wireless clients.
Mixed 802.11g and 802.11b - Select if you are using a mix of 802.11g and 802.11b wireless clients.
Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 802.11g wireless clients.
Mixed 802.11n, 802.11g and 802.11b - Select if you are using a mix of 802.11n, 802.11g, and 802.11b wireless clients.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan**. This will allow the DAP-1650 to automatically choose the channel with the least amount of interference.



WIRELESS NETWORK

Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made in this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

WIRELESS MODE SETTINGS

Wireless Mode : Access Point
Radio Schedule : Always

Wireless Network Settings (2.4 GHz)

Wireless Band : 2.4GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC (Also called the SSID)
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan : ☑
Wireless Channel : 2.412 GHz - CH 1
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

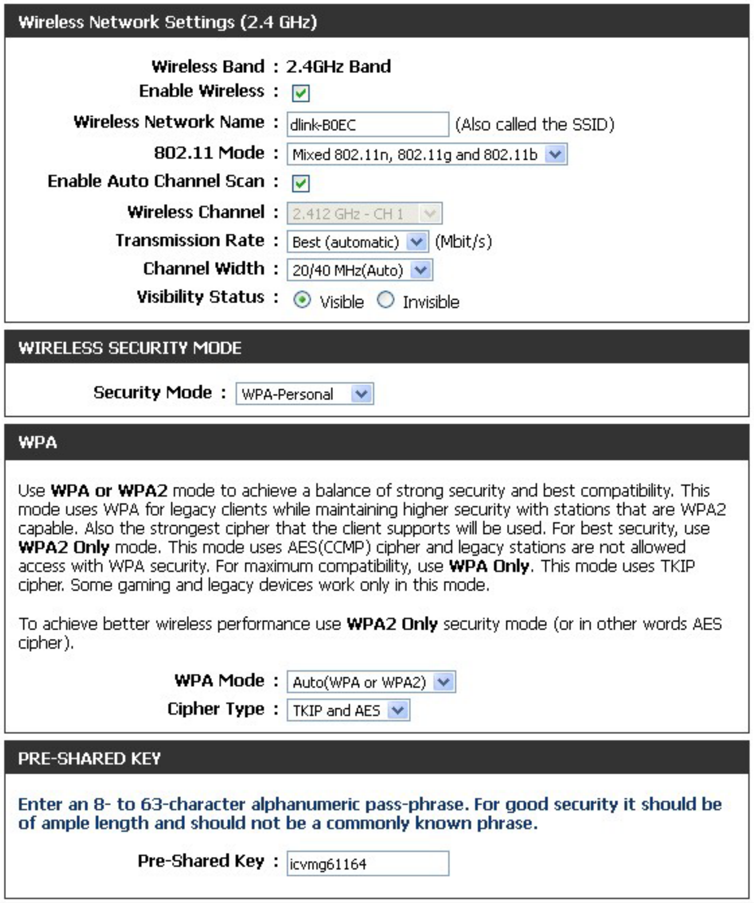
Wireless Channel: Indicates the channel setting for the DAP-1650. The channel can be changed to fit the channel setting for an existing wireless network or to reduce interference in congested areas. If **Auto Channel Scan** is enabled, this option will not be available.

Transmission Rate: Use the drop-down menu to select the appropriate transmission rate in Mbits per second. The default setting is **Best (automatic)**.

Channel Width: Select the channel width:
20/40 MHz(Auto) - Select if you are using both 802.11n and non-802.11n wireless devices.
20 MHz - Select if you are not using any 802.11n wireless clients.

Visibility Status: Select whether you would like the network name (SSID) of your wireless network to be **Visible** or **Invisible** to wireless clients. If **Invisible**, the SSID of the DAP-1650 will not be shown by Site Survey utilities. Therefore the SSID of your wireless network will have to be manually entered so wireless clients can connect to it.

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 40.



Wireless Network Settings (2.4 GHz)

Wireless Band : 2.4GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC (Also called the SSID)
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan : ☑
Wireless Channel : 2.412 GHz - CH 1
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

5 GHz Band

Enable Wireless: Check the box to **Enable** the wireless function for the **5GHz** band. You may uncheck the box to disable all wireless functions.

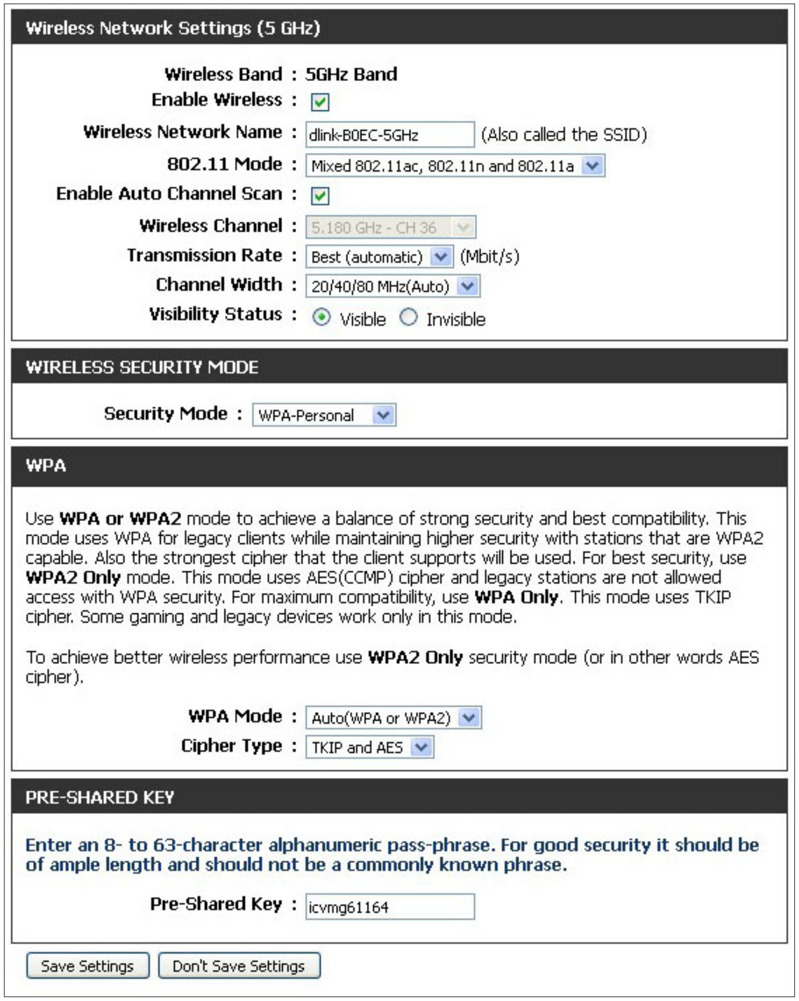
Wireless Network Name: Specify a **Network Name** (SSID) to identify the 5GHz network. This is the network name that wireless clients will search for when connecting to your wireless network. This name should be different than that of the 2.4GHz network above.

802.11 Mode: Select one of the following:
802.11n Only - Select if you are only using 802.11n wireless clients.
802.11ac Only - Select if you are only using 802.11ac wireless clients.
Mixed 802.11a and 802.11n - Select if you are using a mix of 802.11a and 802.11n wireless clients.
Mixed 802.11ac and 802.11n - Select if you are using a mix of 802.11ac and 802.11n wireless clients.
Mixed 802.11ac, 802.11n and 802.11a - Select if you are using a mix of 802.11ac, 802.11n, and 802.11a wireless clients.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan.** This will allow the DAP-1650 to automatically choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DAP-1650. The channel can be changed to fit the channel setting for an existing wireless network or to reduce interference in congested areas. If you enable **Auto Channel Scan**, this option will not be available.

Transmission Rate: Use the drop-down menu to select the appropriate transmission rate in Mbits per second. The default setting is **Best (automatic)**.



Wireless Network Settings (5 GHz)

Wireless Band : 5GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC-5GHz (Also called the SSID)
802.11 Mode : Mixed 802.11ac, 802.11n and 802.11a
Enable Auto Channel Scan : ☑
Wireless Channel : 5.180 GHz - CH 36
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40/80 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

Channel Width: Select the channel width:

20/40/80 MHz(Auto) - Select this option if you are using a combination of 802.11ac, 802.11n, and other wireless devices.

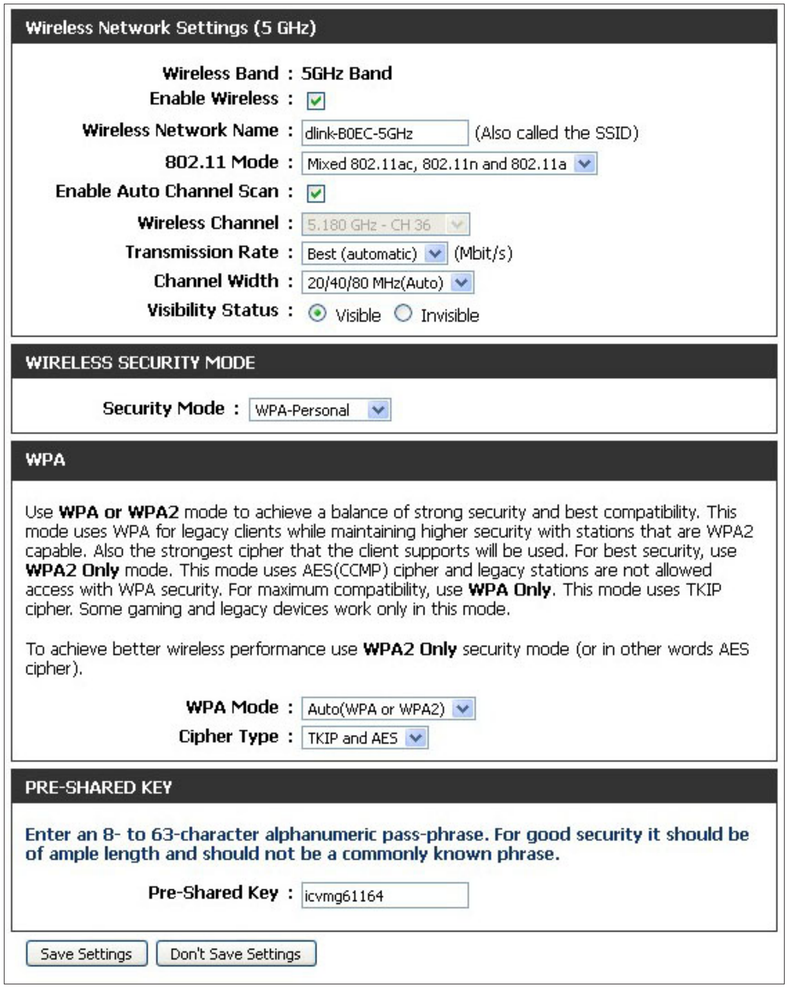
20/40 MHz(Auto) - Select if you are using both 802.11n and non-802.11n wireless devices.

20 MHz - Select if you are not using any 802.11n wireless clients.

Visibility Status: Select whether you would like the network name (SSID) of your wireless network to be **Visible** or **Invisible** to wireless clients. If **Invisible**, the SSID of the DAP-1650 will not be shown by Site Survey utilities. Therefore, the SSID of your wireless network will have to be manually entered so wireless clients can connect to it.

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 40.

Click **Save Settings** at the bottom of the page to save the current configuration.



Wireless Network Settings (5 GHz)

Wireless Band : 5GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC-5GHz (Also called the SSID)
802.11 Mode : Mixed 802.11ac, 802.11n and 802.11a
Enable Auto Channel Scan : ☑
Wireless Channel : 5.180 GHz - CH 36
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40/80 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

Extender Mode

Select **Extender** mode to extend the range of your existing wireless network and increase coverage. The existing wireless signal will be extended by the DAP-1650 using both the 2.4 GHz and 5 GHz bands.

2.4 GHz Band

Wireless Mode: Select **Extender** from the drop-down menu.

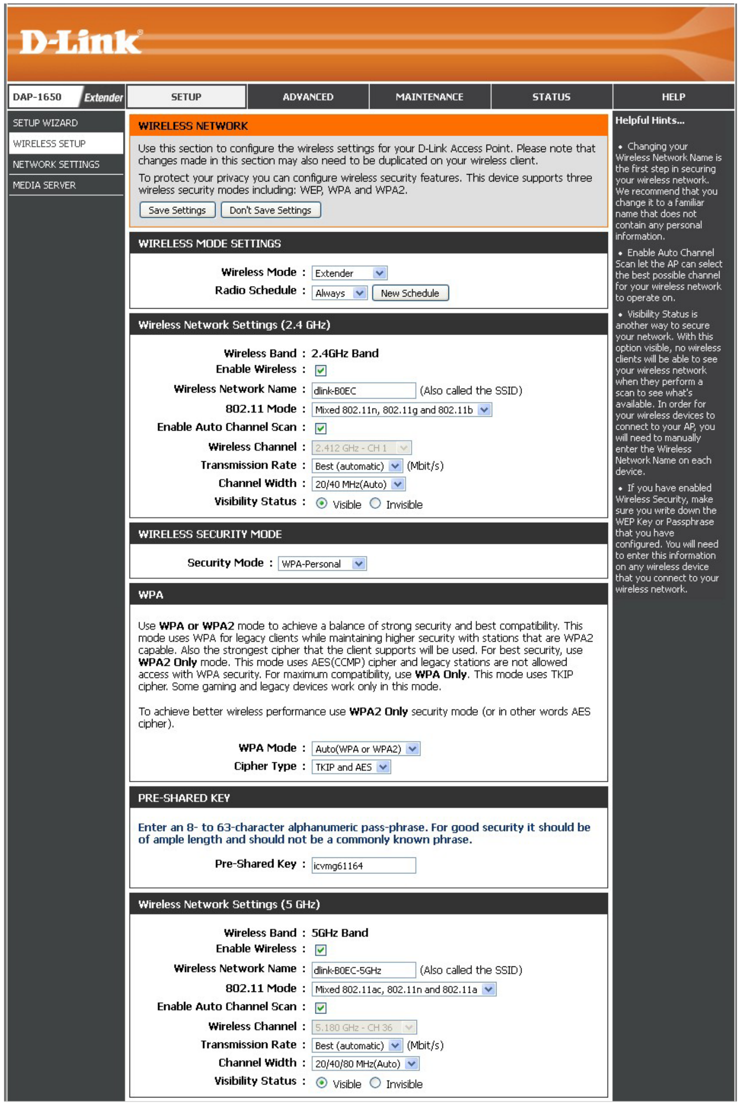
Radio Schedule: You may set up a specific schedule. Select a schedule from the drop-down menu or click **New Schedule** to create a new schedule. By default, the schedule is set to **Always**.

Enable Wireless: Check the box to **Enable** the wireless function for the 2.4GHz band. You can uncheck the box to disable all wireless functions.

Wireless Network Name: Specify a **Network Name** (SSID) to identify the 2.4GHz network. This is the network name that wireless clients will search for when connecting to your wireless network. This name should be different to that of the 5GHz network configured below.

802.11 Mode: Select one of the following:
802.11g Only - Select if you are only using 802.11g wireless clients.
802.11n Only - Select if you are only using 802.11n wireless clients.
Mixed 802.11g and 802.11b - Select if you are using a mix of 802.11g and 802.11b wireless clients.
Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 802.11g wireless clients.
Mixed 802.11n, 802.11g and 802.11b - Select if you are using a mix of 802.11n, 802.11g, and 802.11b wireless clients.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan.** This will allow the DAP-1650 to automatically choose the channel with the least amount of interference.



WIRELESS NETWORK

Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made in this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

WIRELESS MODE SETTINGS

Wireless Mode : Extender
Radio Schedule : Always

Wireless Network Settings (2.4 GHz)

Wireless Band : 2.4GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC (Also called the SSID)
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan : ☑
Wireless Channel : 2.412 GHz - CH 1
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

Wireless Network Settings (5 GHz)

Wireless Band : 5GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC-5GHz (Also called the SSID)
802.11 Mode : Mixed 802.11ac, 802.11n and 802.11a
Enable Auto Channel Scan : ☑
Wireless Channel : 5.180 GHz - CH 36
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40/80 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

Helpful Hints...

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enable Auto Channel Scan let the AP can select the best possible channel for your wireless network to operate on.
- Visibility Status is another way to secure your network. With this option visible, no wireless clients will be able to see your wireless network when they perform a scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down the WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Wireless Channel: Indicates the channel setting for the DAP-1650. The channel can be changed to fit the channel setting for an existing wireless network or to reduce interference in congested areas. If you enable **Auto Channel Scan**, this option will not be available.

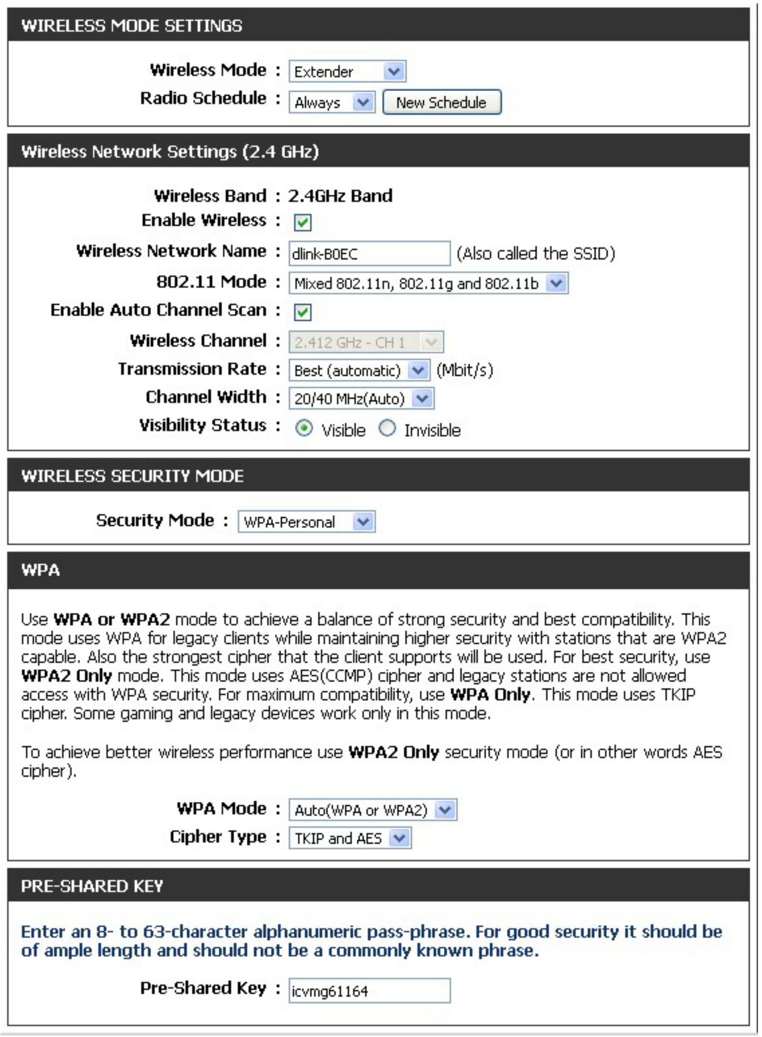
Transmission Rate: Use the drop-down menu to select the appropriate **Transmission Rate** in Mbits per second. The default setting is *Best (automatic)*.

Channel Width: Select the channel width:
20/40 MHz(Auto) - Select if you are using both 802.11n and non-802.11n wireless devices.
20 MHz - Select if you are not using any 802.11n wireless clients.

Visibility Status: Select whether you would like the network name (SSID) of your wireless network to be **Visible** or **Invisible** to wireless clients. If **Invisible**, the SSID of the DAP-1650 will not be shown by Site Survey utilities. Therefore, the SSID of your wireless network will have to be manually entered so wireless clients can connect to it.

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 40.

Click **Save Settings** at the bottom of the page to save the current configuration.



WIRELESS MODE SETTINGS

Wireless Mode : Extender
Radio Schedule : Always

Wireless Network Settings (2.4 GHz)

Wireless Band : 2.4GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC (Also called the SSID)
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan : ☑
Wireless Channel : 2.412 GHz - CH 1
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

5 GHz Band

Wireless Mode: Make sure **Extender** is selected at the top of the screen.

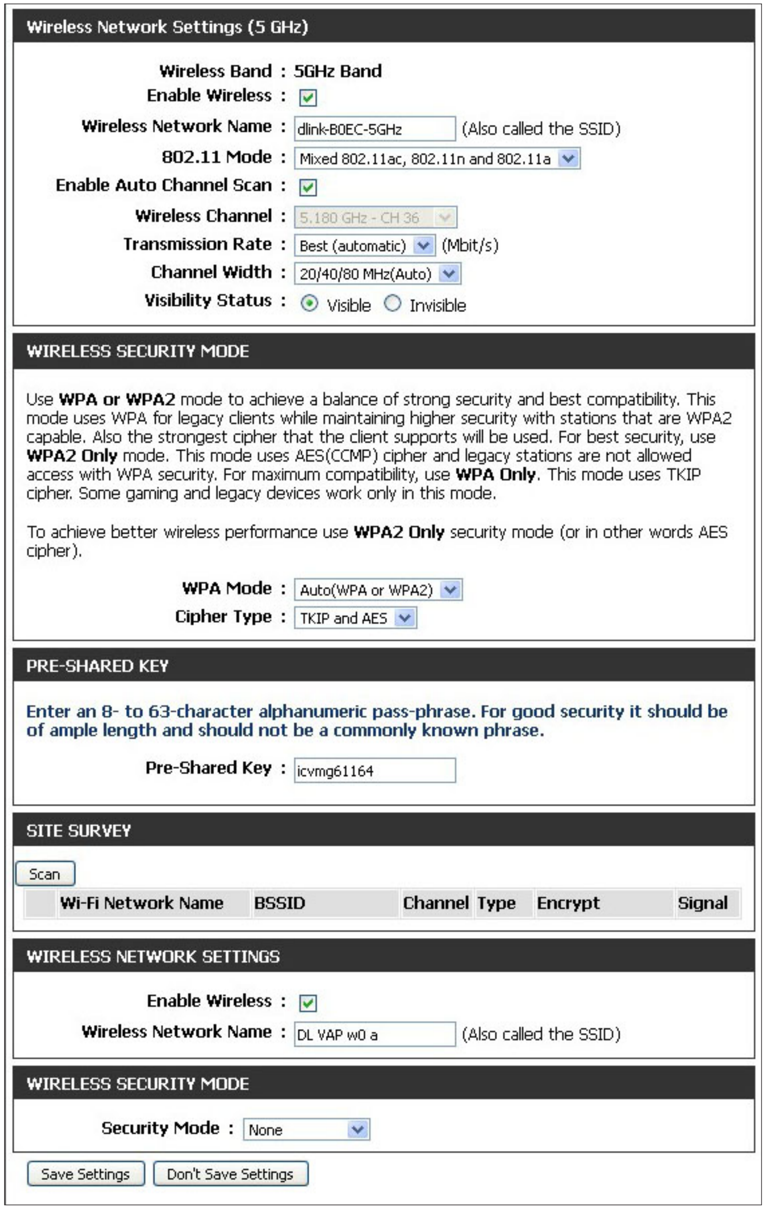
Enable Wireless: Check the box to **Enable** the wireless function for the 5GHz band. If you do not want to use wireless, uncheck the box to disable all wireless functions.

Wireless Network Name: Specify a **Network Name** (SSID) to identify the 5GHz network. This is the network name that wireless clients will search for when connecting to your wireless network. This name should be different than that of the 2.4 GHz network configured above.

802.11 Mode: Select one of the following:
802.11n Only - Select if you are only using 802.11n wireless clients.
802.11ac Only - Select if you are only using 802.11ac wireless clients.
Mixed 802.11a and 802.11n - Select if you are using a mix of 802.11a and 802.11n wireless clients.
Mixed 802.11ac and 802.11n - Select if you are using a mix of 802.11ac and 802.11n wireless clients.
Mixed 802.11ac, 802.11n and 802.11a - Select if you are using a mix of 802.11ac, 802.11n, and 802.11a wireless clients.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan.** This will allow the DAP-1650 to automatically choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DAP-1650. The channel can be changed to fit the channel setting for an existing wireless network or to reduce interference in congested areas. If you enable **Auto Channel Scan**, this option will not be available.



Wireless Network Settings (5 GHz)

Wireless Band : 5GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC-5GHz (Also called the SSID)
802.11 Mode : Mixed 802.11ac, 802.11n and 802.11a
Enable Auto Channel Scan : ☑
Wireless Channel : 5.180 GHz - CH 36
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40/80 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

SITE SURVEY

	Wi-Fi Network Name	BSSID	Channel	Type	Encrypt	Signal

WIRELESS NETWORK SETTINGS

Enable Wireless : ☑
Wireless Network Name : DL VAP w0 a (Also called the SSID)

WIRELESS SECURITY MODE

Security Mode : None

Transmission Rate: Use the drop-down menu to select the appropriate **Transmission Rate** in Mbits per second. The default setting is **Best (automatic)**.

Channel Width: Select the channel width:
20/40/80 Mhz(Auto) - Select this option if you are using a combination of 802.11ac, 802.11n, and other wireless devices.
20/40 MHz(Auto) - Select if you are using both 802.11n and non-802.11n wireless devices.
20 MHz - Select if you are not using any 802.11n wireless clients.

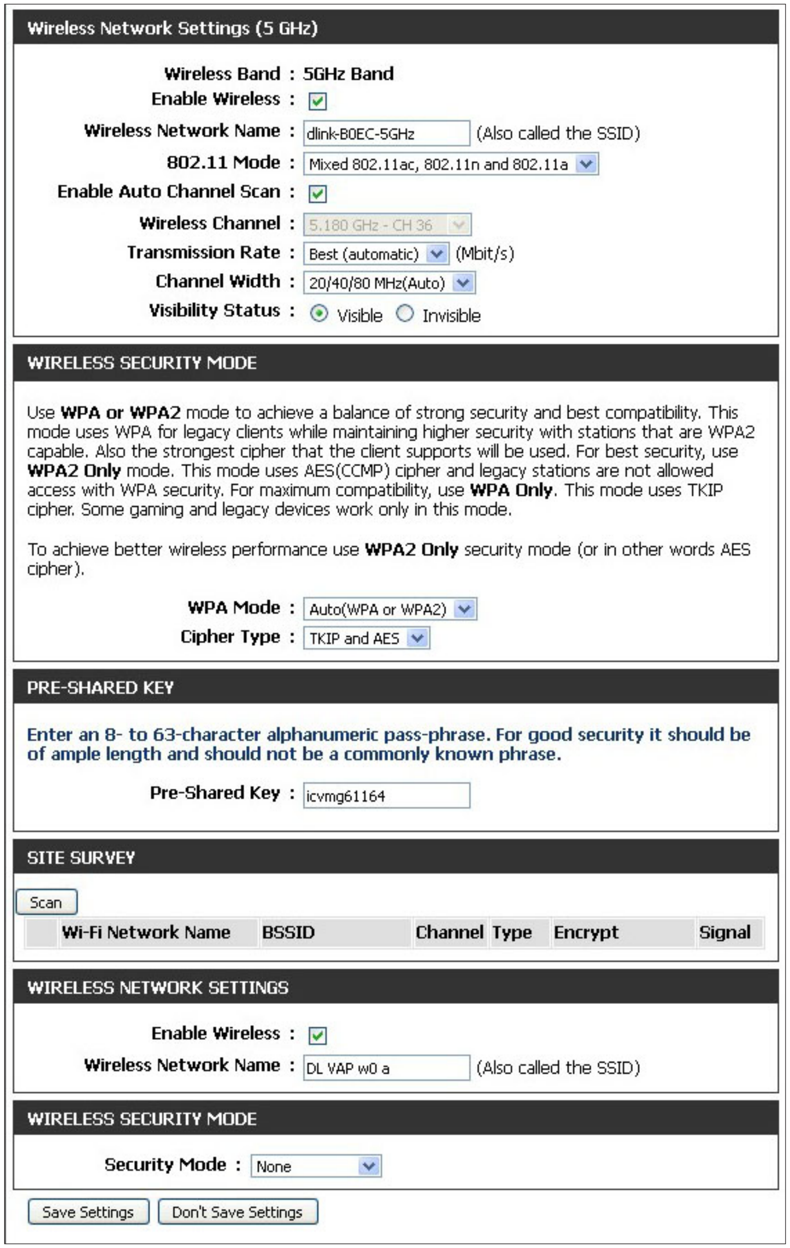
Visibility Status: Select whether you would like the network name (SSID) of your wireless network to be **Visible** or **Invisible** to wireless clients. If **Invisible**, the SSID of the DAP-1650 will not be shown by Site Survey utilities. Therefore the SSID of your wireless network will have to be manually entered so wireless clients can connect to it.

Site Survey: Click the **Scan** button under the *Site Survey* heading to see a list of wireless networks in your area. You may select a wireless network to connect to. It's name will automatically be added to the *Wireless Network Settings* below.

Wireless Network Name: Displays the selected *Wireless Network Name* (SSID).

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 40.

Click **Save Settings** at the bottom of the page to save the current configuration.



Wireless Network Settings (5 GHz)

Wireless Band : 5GHz Band
Enable Wireless : ☑
Wireless Network Name : dlink-B0EC-5GHz (Also called the SSID)
802.11 Mode : Mixed 802.11ac, 802.11n and 802.11a
Enable Auto Channel Scan : ☑
Wireless Channel : 5.180 GHz - CH 36
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20/40/80 MHz(Auto)
Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)
Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

SITE SURVEY

Wi-Fi Network Name	BSSID	Channel	Type	Encrypt	Signal

WIRELESS NETWORK SETTINGS

Enable Wireless : ☑
Wireless Network Name : DL VAP w0 a (Also called the SSID)

WIRELESS SECURITY MODE

Security Mode : None

Media Bridge Mode

Wireless Mode: Select **Media Bridge** from the drop-down menu.

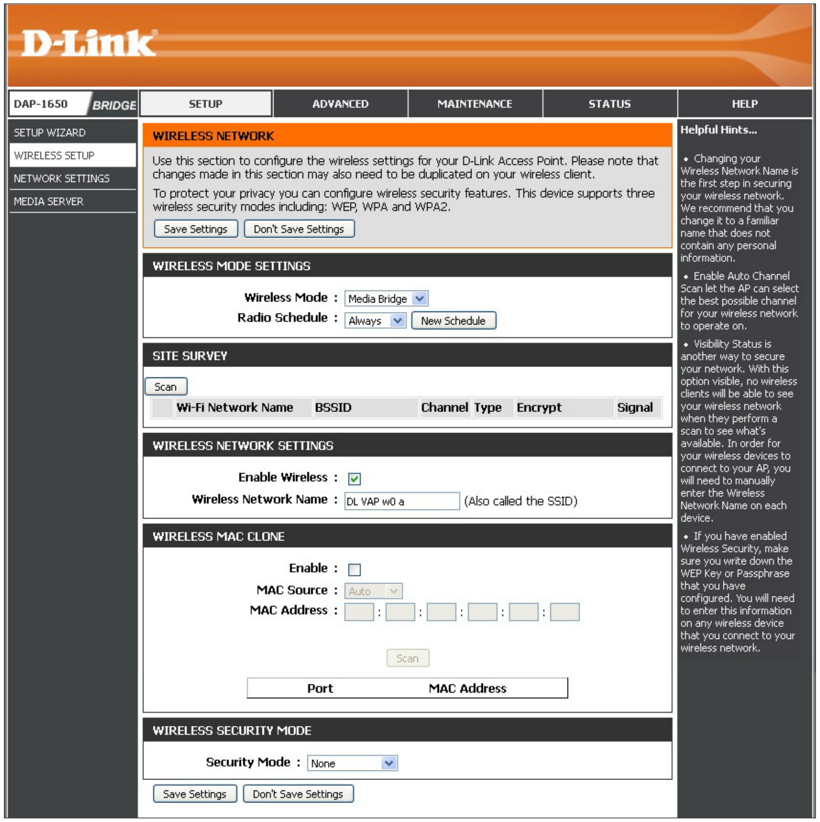
Radio Schedule: You may set up a specific schedule. Select a schedule from the drop-down menu or click **New Schedule** to create a new schedule. By default, the schedule is set to **Always**.

Site Survey: Click the **Scan** button to scan for wireless networks. Select the wireless network you want the bridge to use and it's name will automatically be added to the *Wireless Network Settings*. All APs on the bridge must be using the same wireless channel.

Enable Wireless: Check the box to **Enable** the wireless function. If you do not want to use wireless, uncheck the box to disable all wireless functions.

Wireless Network Name: Displays the selected *Wireless Network Name* (SSID).

Wireless MAC Clone: Check the box to **Enable** the *MAC Clone* function. (A screen shot with this option enabled is shown below right.)



WIRELESS NETWORK

Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made in this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Save Settings | Don't Save Settings

WIRELESS MODE SETTINGS

Wireless Mode : Media Bridge

Radio Schedule : Always | New Schedule

SITE SURVEY

Scan

	Wi-Fi Network Name	BSSID	Channel	Type	Encrypt	Signal

WIRELESS NETWORK SETTINGS

Enable Wireless : ☑

Wireless Network Name : DL VAP w0 a (Also called the SSID)

WIRELESS MAC CLONE

Enable : □

MAC Source : Auto

MAC Address : __ : __ : __ : __ : __ : __

Scan

Port	MAC Address

WIRELESS SECURITY MODE

Security Mode : None

Save Settings | Don't Save Settings

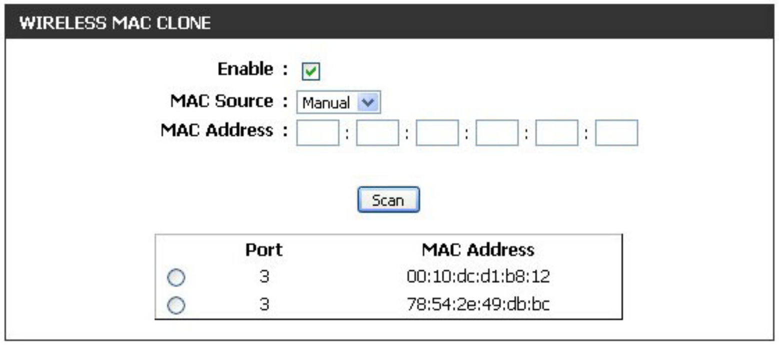
Helpful Hints...

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enable Auto Channel Scan let the AP can select the best possible channel for your wireless network to operate on.
- Visibility Status is another way to secure your network. With this option visible, no wireless clients will be able to see your wireless network when they perform a scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down the WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

MAC Source: If you select **Manual** from the drop down menu, you will be able to click on **Scan**. Select the **MAC Address** from the scanned results and the **MAC Address** will automatically be added.

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 40.

Click **Save Settings** at the bottom of the page to save the current configuration.



WIRELESS MAC CLONE

Enable : ☑

MAC Source : Manual

MAC Address : __ : __ : __ : __ : __ : __

Scan

	Port	MAC Address
○	3	00:10:dc:d1:b8:12
○	3	78:54:2e:49:db:bc

Note: *The Media Bridge mode is not completely specified in the Wi-Fi or IEEE standards. This mode will work with other DAP-1650 units. Communication with other APs (even other D-Link APs) is not guaranteed.*

Configuring Wireless Security

Wireless security encryption prevents unauthorized users from accessing your wireless network. Although the DAP-1650 provides two methods of wireless security encryption from which to select, we recommend that you use WPA, since it is more secure than the older WEP standard. For more details about wireless security, refer to "Wireless Security" on page 88.

***Note:** Unless otherwise specified, the security configuration process is the same for both the 2.4GHz and 5GHz bands.*

WPA-Personal

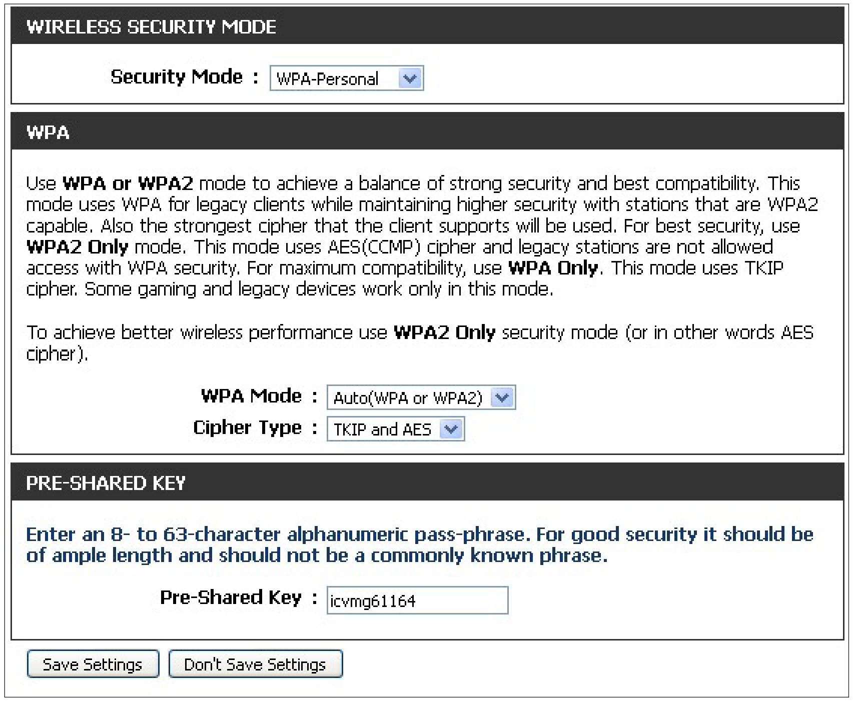
Security Mode: Select **WPA-Personal** from the drop-down menu.

WPA Mode: There are two versions of WPA supported by the DAP-1650: WPA and WPA2. We recommended that you select **Auto(WPA or WPA2)** so that the WPA2 version will be used if connecting wireless clients support it.

Cipher Type: Choose a **Cipher Type** from the drop-down menu.

Pre-Shared Key: Enter the **Pre-Shared Key** (password) for the wireless network. Wireless clients will need this key in order to connect to your wireless network.

Click **Save Settings** at the bottom of the page to save the current configuration.



WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)

Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : icvmg61164

WPA-Enterprise

WPA-Enterprise uses a RADIUS authentication server to provide centralized authentication for wireless access. If you are missing any of the information required for this setup, contact your network administrator.

Security Mode: Select **WPA-Enterprise** from the drop-down menu.

WPA Mode: There are two versions of WPA supported by the DAP-1650: WPA and WPA2. We recommended that you select **Auto(WPA or WPA2)** so that the WPA2 version will be used if connecting wireless clients support it.

Cipher Type: Choose a **Cipher Type** from the drop-down menu.

RADIUS Server IP Address: Enter the **IP Address** for your network's RADIUS authentication server.

RADIUS server Port: Enter the port for the RADIUS authentication server.

Radius Server Shared Secret: Enter the **Shared Secret** required by the RADIUS authentication server.

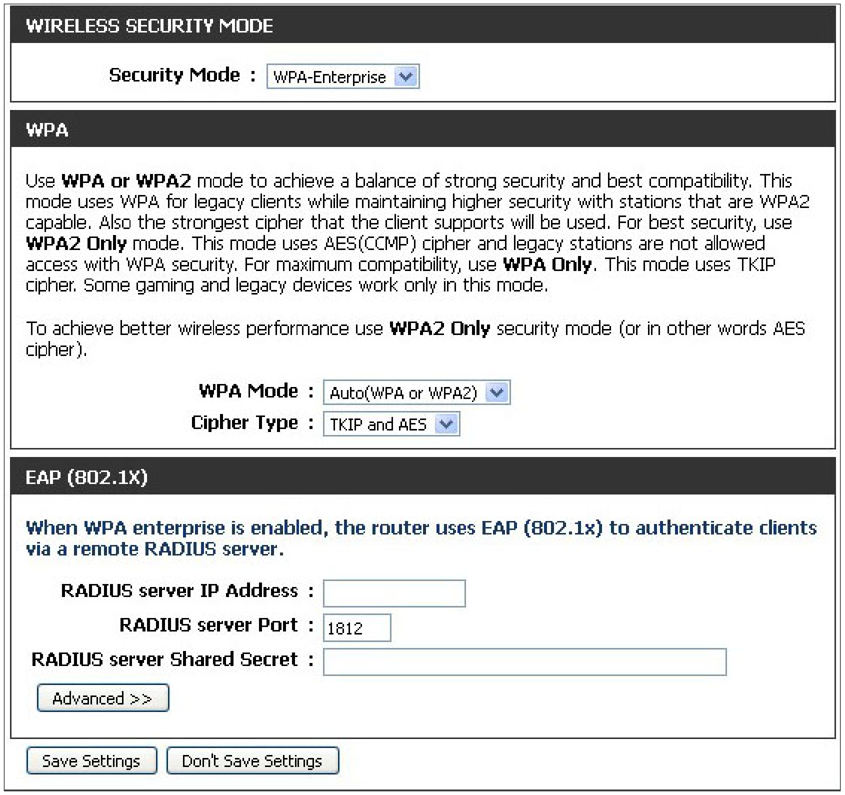
Advanced: Click on the **Advanced** button to display the setup options for an optional backup RADIUS server configuration.

Second RADIUS Server IP Address: Enter the **IP Address** for your network's backup RADIUS authentication server.

Second RADIUS Server Port: Enter the port for the backup RADIUS authentication server.

Second RADIUS Server Shared Secret: Enter the **Shared Secret** required by the backup RADIUS authentication server.

Click **Save Settings** at the bottom of the page to save the current configuration.



WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto(WPA or WPA2)

Cipher Type : TKIP and AES

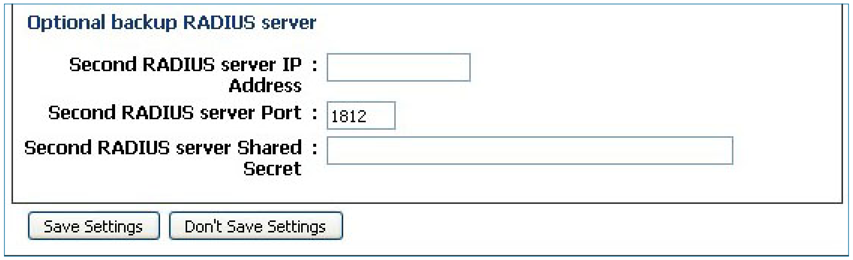
EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port : 1812

RADIUS server Shared Secret :



Optional backup RADIUS server

Second RADIUS server IP Address :

Second RADIUS server Port : 1812

Second RADIUS server Shared Secret :

Network Settings

The Network Settings screen allows you to configure the Local Area Network (LAN) settings for the DAP-1650.

Device Name: You can change the name of your DAP-1650 to make it easier to identify. Enter a name for the device in the field provided. If you change the device name, you may enter this name in your web browser address bar to access the web-based configuration utility. Example: http://devicename

My LAN Connection is: Select how you would like to configure the device's IPv4 mode settings from the drop-down menu:
Dynamic IP (DHCP) - The device will request an IP address from the DHCP server that it is connected to. (If you select this option, skip to the next page for further instructions.)
Static IP - If you select this option, you can manually specify the IP address settings for the device as described below:

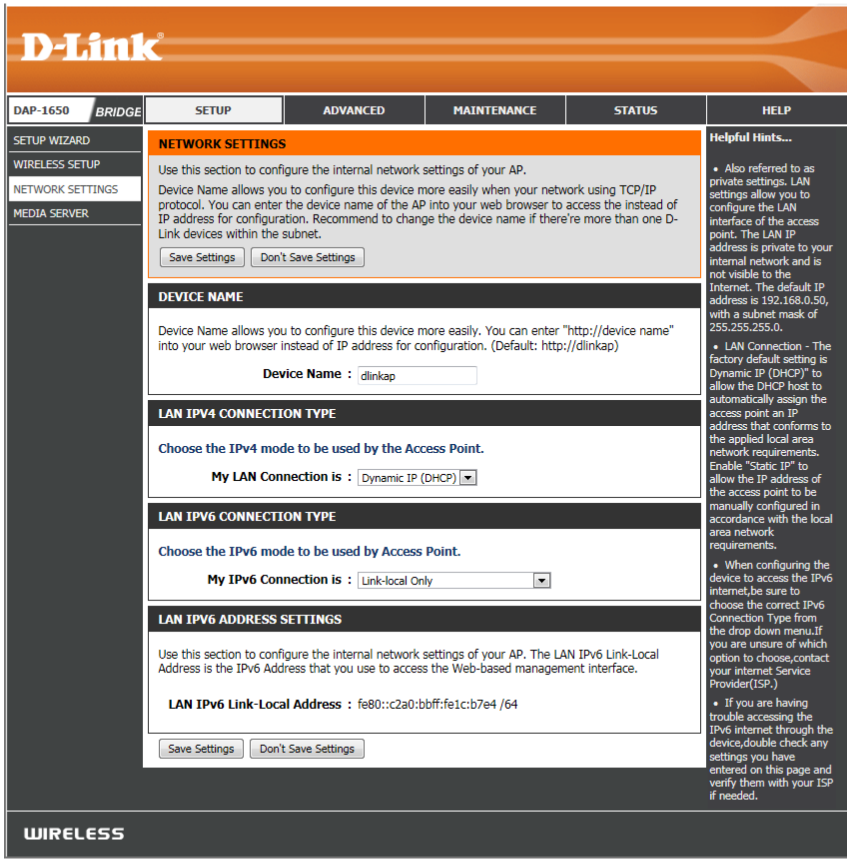
IP Address: Enter the **IP Address** that you want to specify for the device (Static IP only).

Subnet Mask: Enter the **Subnet Mask** to be used by the device(Static IP only).

Gateway Address: Enter the default **Gateway Address** to be used by the access point (Static IP only).

Primary DNS Server: Enter the **Primary DNS Server** address to be used by the access point (Static IP only).

Secondary DNS Server: Enter the **Secondary DNS Server** address to be used by the access point (Static IP only).



NETWORK SETTINGS

Use this section to configure the internal network settings of your AP.

Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. Recommend to change the device name if there're more than one D-Link devices within the subnet.

Save Settings | Don't Save Settings

DEVICE NAME

Device Name allows you to configure this device more easily. You can enter "http://device name" into your web browser instead of IP address for configuration. (Default: http://dlinkap)

Device Name : dlinkap

LAN IPV4 CONNECTION TYPE

Choose the IPv4 mode to be used by the Access Point.

My LAN Connection is : Dynamic IP (DHCP)

LAN IPV6 CONNECTION TYPE

Choose the IPv6 mode to be used by Access Point.

My IPv6 Connection is : Link-local Only

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your AP. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface.

LAN IPv6 Link-Local Address : fe80::c2a0:bbff:fe1c:b7e4 /64

Save Settings | Don't Save Settings

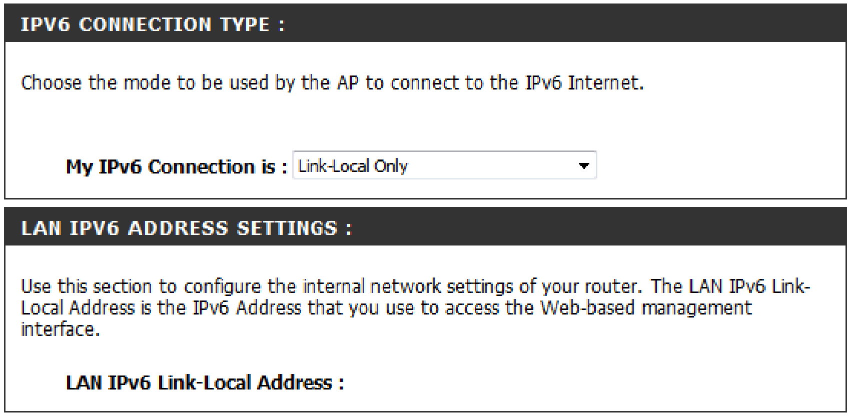
Helpful Hints...

- Also referred to as private settings. LAN settings allow you to configure the LAN interface of the access point. The LAN IP address is private to your internal network and is not visible to the Internet. The default IP address is 192.168.0.50, with a subnet mask of 255.255.255.0.
- LAN Connection - The factory default setting is Dynamic IP (DHCP)" to allow the DHCP host to automatically assign the access point an IP address that conforms to the applied local area network requirements. Enable "Static IP" to allow the IP address of the access point to be manually configured in accordance with the local area network requirements.
- When configuring the device to access the IPv6 internet,be sure to choose the correct IPv6 Connection Type from the drop down menu.If you are unsure of which option to choose,contact your internet Service Provider(ISP.)
- If you are having trouble accessing the IPv6 internet through the device,double check any settings you have entered on this page and verify them with your ISP if needed.

My IPv6 Connection is: Select **Link-Local Only** from the drop-down menu. This will set the device’s local IPv6 address.

LAN IPv6 Link-Local Address: The device’s local IPv6 address will be displayed here. This address may be used to access the web-based configuration utility through the IPv6 protocol.

Click **Save Settings** at the bottom of the page to save the current configuration.



IPV6 CONNECTION TYPE :

Choose the mode to be used by the AP to connect to the IPv6 Internet.

My IPv6 Connection is : Link-Local Only

LAN IPV6 ADDRESS SETTINGS :

Use this section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface.

LAN IPv6 Link-Local Address :

My IPv6 Connection is: Selecting **Static IPv6** from the drop-down menu will allow you to assign a static IPv6 address to the device.

LAN IPv6 Address: The device’s local IPv6 address will be displayed here. This address may be used to access the web-based configuration utility through the IPv6 protocol.

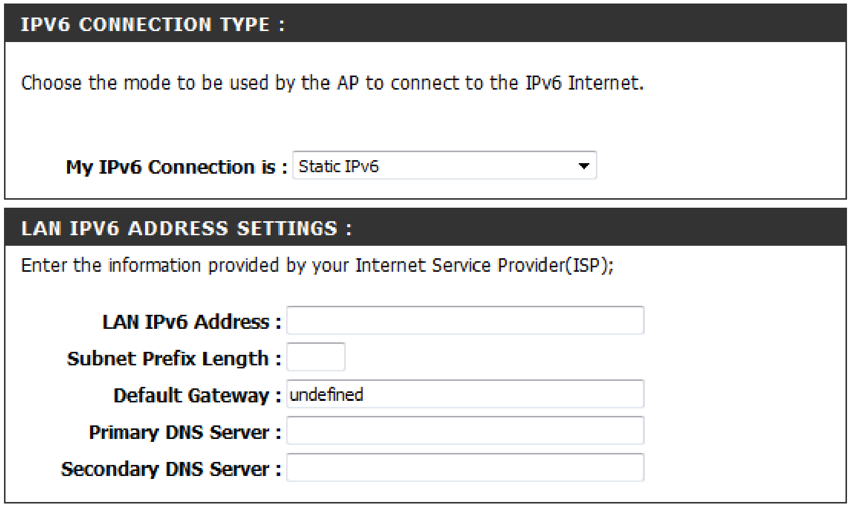
Subnet Prefix Length: Enter the **Prefix Length** for IPv6 IP addresses on your network.

Default Gateway: Enter the default IPv6 gateway address for your network.

Primary DNS Server: Enter the primary IPv6 DNS server address for your network.

Secondary DNS Server: Enter the secondary IPv6 DNS server address for your network.

Click **Save Settings** at the bottom of the page to save the current configuration.



IPV6 CONNECTION TYPE :

Choose the mode to be used by the AP to connect to the IPv6 Internet.

My IPv6 Connection is : Static IPv6

LAN IPV6 ADDRESS SETTINGS :

Enter the information provided by your Internet Service Provider(ISP);

LAN IPv6 Address :

Subnet Prefix Length :

Default Gateway : undefined

Primary DNS Server :

Secondary DNS Server :

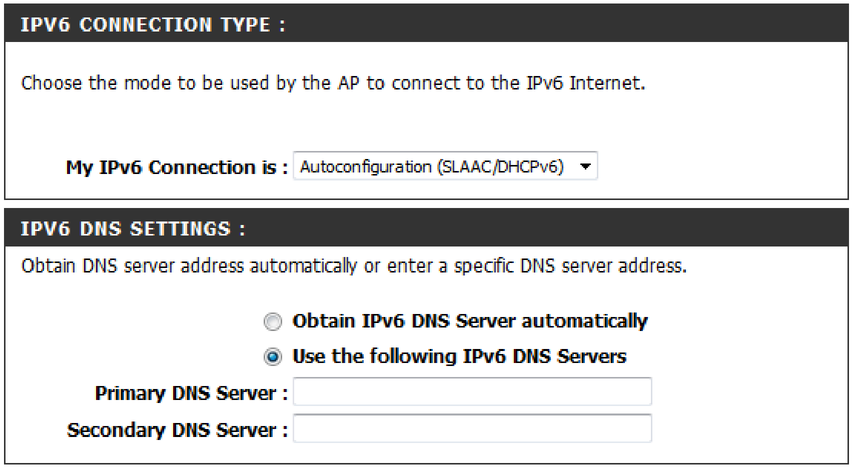
My IPv6 Connection is: Select **Autoconfiguration (SLAAC/DHCPv6)** from the drop-down menu. The device will request IPv6 settings from a DHCPv6 server on your network.

IPv6 DNS Settings: You may choose to have the device automatically obtain DNS server settings from the DHCP server, or you can specify IPv6 DNS server settings to be used. If you select **Obtain IPv6 DNS automatically**, no further configuration is required.

Primary DNS Server: If you select **Use the following IPv6 DNS Servers**, enter the primary IPv6 DNS server address to be used.

Secondary DNS Server: If you select **Use the following IPv6 DNS Servers**, enter the secondary IPv6 DNS server address to be used.

Click **Save Settings** at the bottom of the page to save the current configuration.



IPV6 CONNECTION TYPE :

Choose the mode to be used by the AP to connect to the IPv6 Internet.

My IPv6 Connection is : Autoconfiguration (SLAAC/DHCPv6)

IPV6 DNS SETTINGS :

Obtain DNS server address automatically or enter a specific DNS server address.

○ **Obtain IPv6 DNS Server automatically**

● **Use the following IPv6 DNS Servers**

Primary DNS Server :

Secondary DNS Server :

Media Server

The Media Server screen allows you to enable a DLNA Media Server. DLNA (Digital Living Network Alliance) is the standard for the interoperability of Network Media Devices (NMDs). The user can enjoy multimedia applications (music, pictures and videos) on your network connected PC or media devices. If you choose to share media with devices, any computer or device that connects to your network can play your shared music, pictures and videos.

Note: *The shared media may not be secure. Allowing any devices to stream is recommended only on secure networks.*

DLNA Server: Click the radio button to **Enable** or **Disable** the DLNA Media Server functions.

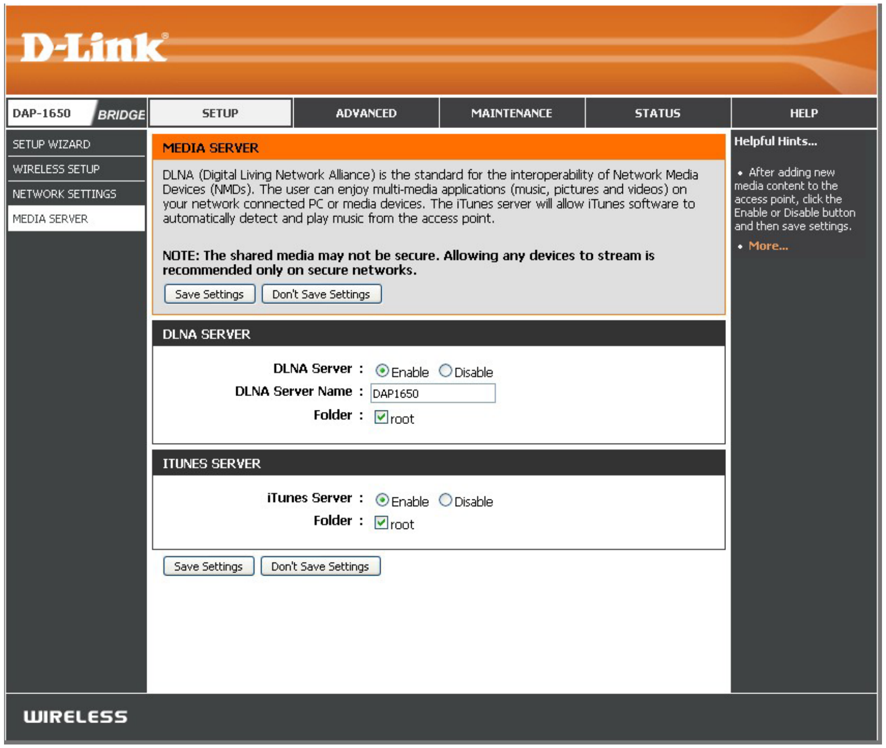
DLNA Server Name: Enter a name for your DLNA media server so that it can be found.

Folder: Choose the location of the folder you wish to share or check the box to use the root folder of the entire drive.

iTunes Server: Click the radio button to **Enable** or **Disable** the iTunes Server functions.

Folder: Choose the location of the iTunes Library folder you wish to share or check the box to use the root folder if it is located on the root folder of the connected drive.

Click **Save Settings** at the bottom of the page to save the current configuration.



MEDIA SERVER

DLNA (Digital Living Network Alliance) is the standard for the interoperability of Network Media Devices (NMDs). The user can enjoy multi-media applications (music, pictures and videos) on your network connected PC or media devices. The iTunes server will allow iTunes software to automatically detect and play music from the access point.

NOTE: The shared media may not be secure. Allowing any devices to stream is recommended only on secure networks.

DLNA SERVER

DLNA Server : ● Enable ○ Disable
DLNA Server Name : DAP1650
Folder : ☑ root

ITUNES SERVER

iTunes Server : ● Enable ○ Disable
Folder : ☑ root

Helpful Hints...

- After adding new media content to the access point, click the Enable or Disable button and then save settings.

Advanced

This section allows you to configure the advanced features of your DAP-1650. There are different options available for configuration based on the mode in which your device is operating. Detailed instructions for *Access Point* mode begins below. Refer page 52 for details about *Extender* mode, and to page 54 for details about *Media Bridge* mode.

Access Point Mode

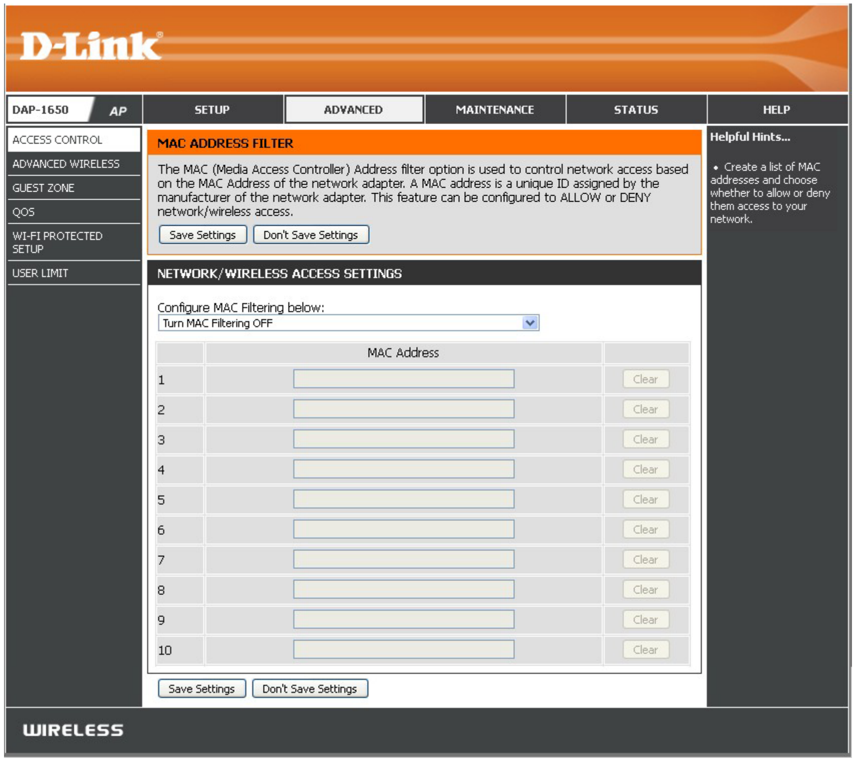
Access Control

MAC filtering allows you to control wireless access to your network according to clients' MAC addresses.

Configure MAC Filtering: Use the drop-down menu to select your desired MAC filtering method:
Turn MAC Filtering OFF - No MAC filtering will be implemented.
Turn MAC Filtering ON and ALLOW computer listed to access the network - MAC filtering will be turned on, and only MAC addresses listed in the table below will be allowed access.
Turn MAC Filtering ON and DENY computer listed to access the network - MAC filtering will be turned on, and only MAC addresses listed in the table below will be denied access.

MAC Address: Enter the **MAC Address** of the client that you wish to filter. If you would like to delete a MAC Address, click on **Clear**.

Click **Save Settings** at the bottom of the page to save the current configuration.



MAC ADDRESS FILTER

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/wireless access.

Helpful Hints...

- Create a list of MAC addresses and choose whether to allow or deny them access to your network.

NETWORK/WIRELESS ACCESS SETTINGS

Configure MAC Filtering below:
Turn MAC Filtering OFF

	MAC Address	
1		Clear
2		Clear
3		Clear
4		Clear
5		Clear
6		Clear
7		Clear
8		Clear
9		Clear
10		Clear

Advanced Wireless

This section allows you to adjust the advanced wireless settings for each wireless band. The first five fields are the same for the 2.4GHz and the 5GHz bands.

Transmit Power: For each wireless band, select the preferred transmission power of the wireless radio from the drop-down menu.

WMM Enable: Check the box to **Enable** wireless multimedia (WMM), a QoS engine that may help reduce lag and latency when transmitting multimedia over your wireless connection.

Short GI: Enabling a short guard interval (GI) may increase throughput. However, it can also increase error rate due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

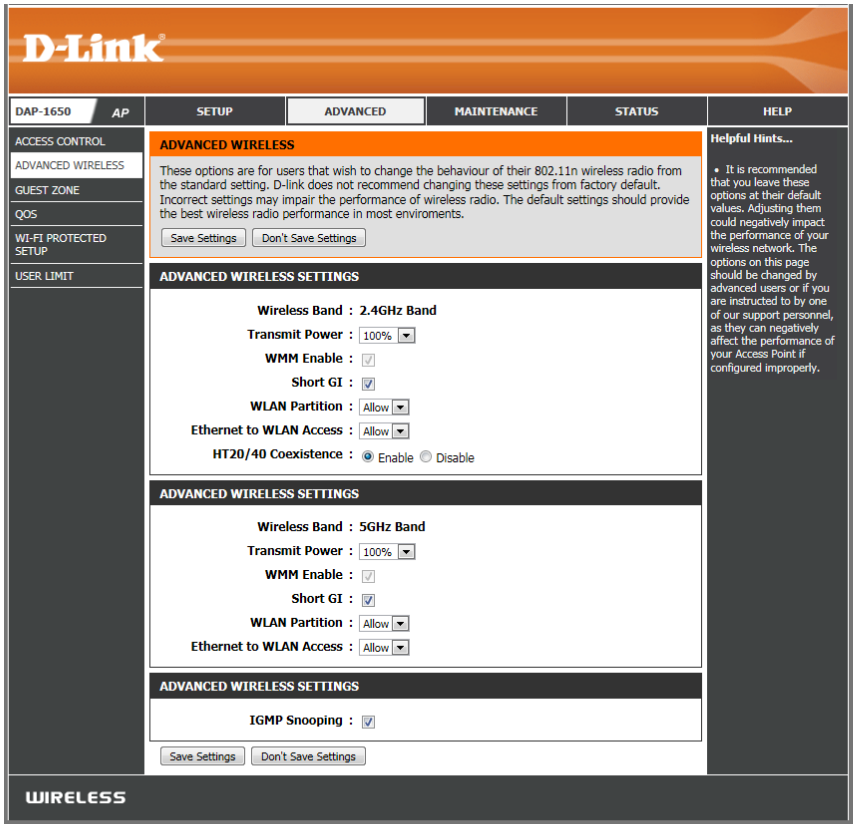
WLAN Partition: Enabling this option means that connected wireless clients will not be able to communicate with each other, but will still have access to network resources such as the Internet.

Ethernet to WLAN Access: When this option is enabled, there is no barrier to data flow from the Ethernet to wireless devices using the access point. If this is disabled, wireless devices can still send data to the Ethernet, but all data from the Ethernet to associated wireless devices is blocked.

HT 20/40 Coexistance: For the 2.4GHz band only, you can click **Enable** to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel causing interference, the AP will automatically change to 20 MHz.

IGMP Snooping: Enable this option to allow the AP to listen for internet group management protocol (IGMP) traffic, which may help detect clients that require multicast streams.

Click **Save Settings** at the bottom of the page to save the current configuration.



ADVANCED WIRELESS

These options are for users that wish to change the behaviour of their 802.11n wireless radio from the standard setting. D-link does not recommend changing these settings from factory default. Incorrect settings may impair the performance of wireless radio. The default settings should provide the best wireless radio performance in most enviroments.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz Band
Transmit Power : 100%
WMM Enable : ☑
Short GI : ☑
WLAN Partition : Allow
Ethernet to WLAN Access : Allow
HT20/40 Coexistence : ● Enable ○ Disable

ADVANCED WIRELESS SETTINGS

Wireless Band : 5GHz Band
Transmit Power : 100%
WMM Enable : ☑
Short GI : ☑
WLAN Partition : Allow
Ethernet to WLAN Access : Allow

ADVANCED WIRELESS SETTINGS

IGMP Snooping : ☑

Helpful Hints...

- It is recommended that you leave these options at their default values. Adjusting them could negatively impact the performance of your wireless network. The options on this page should be changed by advanced users or if you are instructed to by one of our support personnel, as they can negatively affect the performance of your Access Point if configured improperly.

Guest Zone

The guest zone feature allows you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network.

Enable Guest Zone: For each wireless band, check the box to **Enable** the guest zone feature. You can select a schedule for when the guest zone will be active. The schedule may be set to **Always**, which allows the service to always be enabled. Click on **New Schedule** to create your own schedule.

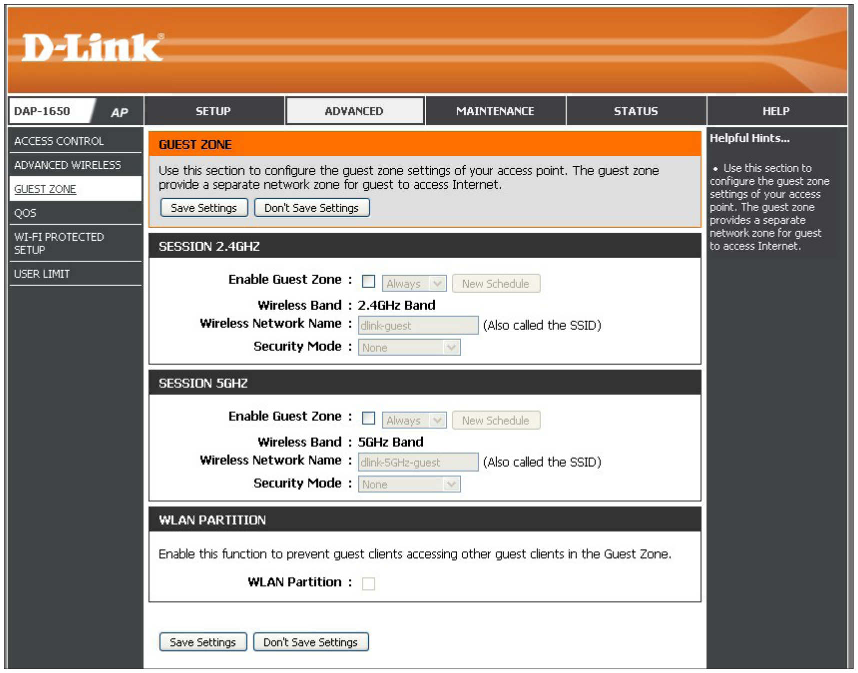
Wireless Band: Displays the *Wireless Band* you are creating a zone for.

Wireless Network Name: Enter a **Wireless Network Name** (SSID) that is different from your main wireless network.

Security Mode: Refer to "Wireless Security" on page 88 for more information.

WLAN Partition: Check the check box to create a *WLAN Partition*, preventing guest clients from accessing other guest clients in the guest zone.

Click **Save Settings** at the bottom of the page to save the current configuration.



GUEST ZONE

Use this section to configure the guest zone settings of your access point. The guest zone provide a separate network zone for guest to access Internet.

SESSION 2.4GHZ

Enable Guest Zone : □ Always
Wireless Band : 2.4GHz Band
Wireless Network Name : dlink-guest (Also called the SSID)
Security Mode : None

SESSION 5GHZ

Enable Guest Zone : □ Always
Wireless Band : 5GHz Band
Wireless Network Name : dlink-5GHz-guest (Also called the SSID)
Security Mode : None

WLAN PARTITION

Enable this function to prevent guest clients accessing other guest clients in the Guest Zone.

WLAN Partition : □

Helpful Hints...

- Use this section to configure the guest zone settings of your access point. The guest zone provides a separate network zone for guest to access Internet.

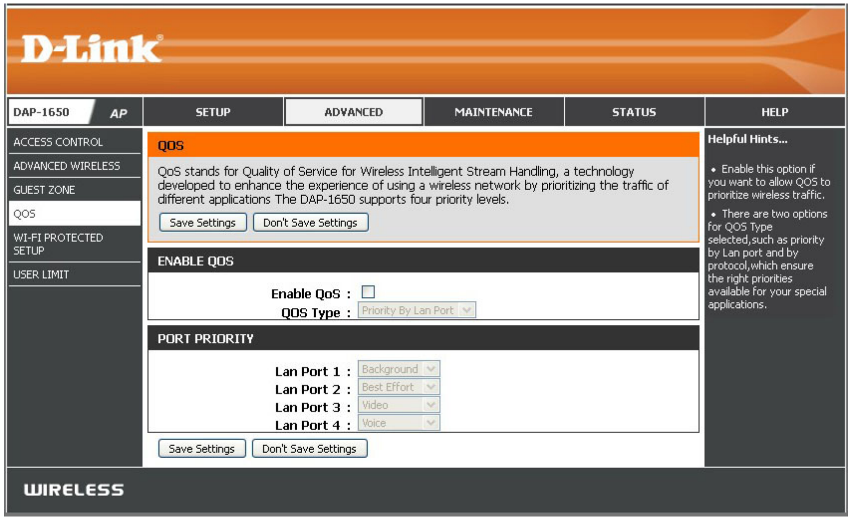
QoS

Enabling QoS (Quality of Service) can improve your network gaming performance by prioritizing applications. By default the QoS engine settings are disabled. Enable QoS if you would like to prioritize wireless traffic.

Enable QoS Engine: This option is disabled by default. Check the box to **Enable**, for better performance with online games and other interactive applications, such as VoIP.

QoS Type: Select **Priority by Lan Port** or by **Priority by Protocol**. If you select the second option, you will see the *Advanced QoS* panel as shown in the bottom right corner.

Lan Port 1-4: If you selected **Priority by Lan Port**, select the type of traffic you would like to prioritize from the drop-down menu for each **Lan Port**.



QOS

QoS stands for Quality of Service for Wireless Intelligent Stream Handling, a technology developed to enhance the experience of using a wireless network by prioritizing the traffic of different applications The DAP-1650 supports four priority levels.

ENABLE QOS

Enable QoS : □

QOS Type : Priority By Lan Port

PORT PRIORITY

Lan Port 1 : Background

Lan Port 2 : Best Effort

Lan Port 3 : Video

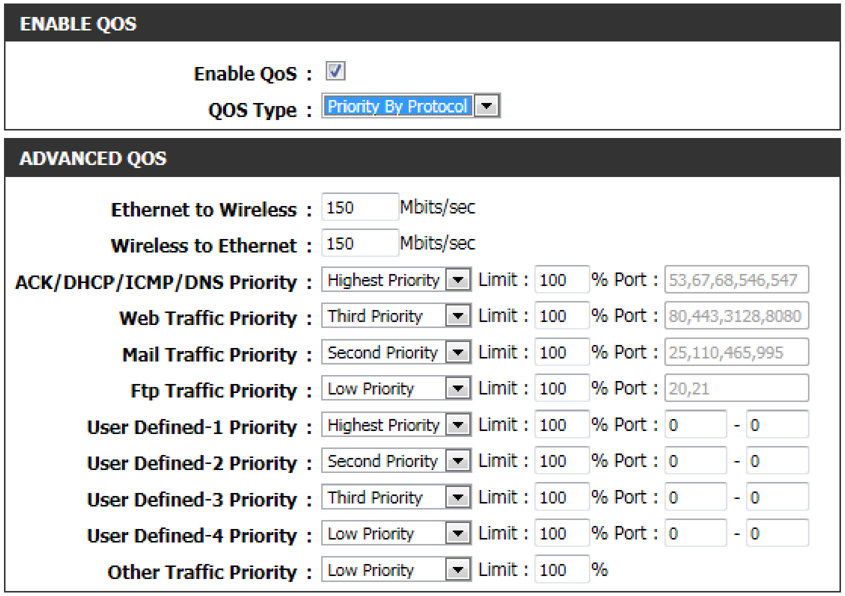
Lan Port 4 : Voice

Helpful Hints...

- Enable this option if you want to allow QOS to prioritize wireless traffic.
- There are two options for QOS Type selected,such as priority by Lan port and by protocol,which ensure the right priorities available for your special applications.

Advanced QoS: If you selected **Priority by Protocol**, use the *Advanced QoS* panel to fine-tune your network traffic prioritization.

Click **Save Settings** at the bottom of the page to save the current configuration.



ENABLE QOS

Enable QoS : ☑

QOS Type : Priority By Protocol

ADVANCED QOS

Ethernet to Wireless :	150 Mbits/sec					
Wireless to Ethernet :	150 Mbits/sec					
ACK/DHCP/ICMP/DNS Priority :	Highest Priority	Limit :	100	% Port :	53,67,68,546,547	
Web Traffic Priority :	Third Priority	Limit :	100	% Port :	80,443,3128,8080	
Mail Traffic Priority :	Second Priority	Limit :	100	% Port :	25,110,465,995	
Ftp Traffic Priority :	Low Priority	Limit :	100	% Port :	20,21	
User Defined-1 Priority :	Highest Priority	Limit :	100	% Port :	0	- 0
User Defined-2 Priority :	Second Priority	Limit :	100	% Port :	0	- 0
User Defined-3 Priority :	Third Priority	Limit :	100	% Port :	0	- 0
User Defined-4 Priority :	Low Priority	Limit :	100	% Port :	0	- 0
Other Traffic Priority :	Low Priority	Limit :	100	%		

Wi-Fi Protected Setup

The Wi-Fi Protected Setup screen allows you select the method to be used for Wi-Fi Protected Setup (WPS) to create a secure wireless connection.

Note: *Clients must support WPS in order for this method to be used.*

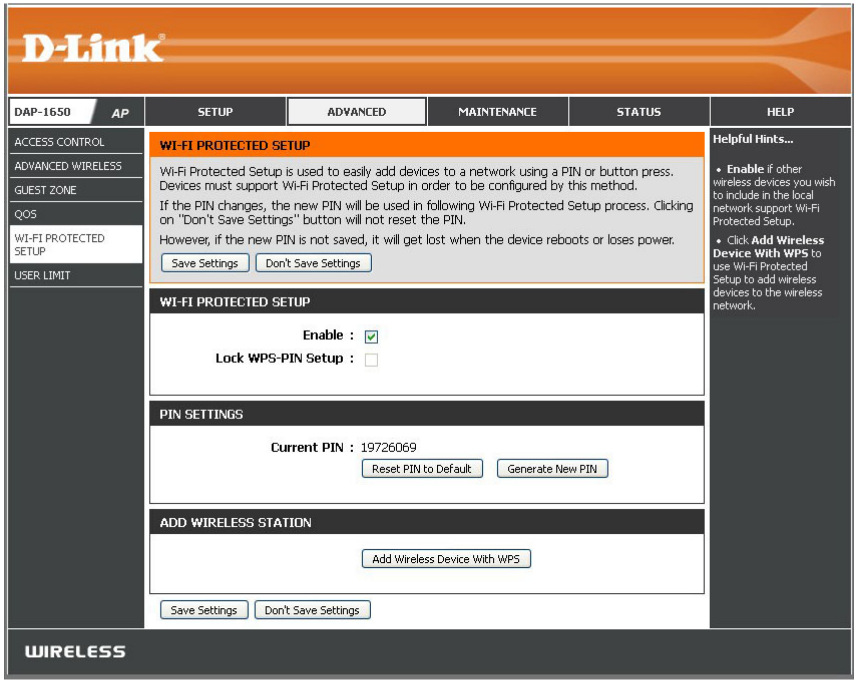
Enable: Check the box to **Enable** WPS.

Lock WPS-PIN Setup: Check the box to disable WPS using the PIN method. If this option is selected, wireless clients will only be able to use the WPS-PBC (push-button connection) method.

Current PIN: Displays the *Current PIN,* which can be used by wireless clients to connect to the access point. Click **Reset PIN to Default** to return the PIN to its factory default. Click **Generate New PIN** to randomly generate a new PIN.

Click **Add Wireless Device With WPS** to activate the WPS-PBC (push-button) method. You will then have 120 seconds to press the WPS button on the new device that you wish to connect.

Click **Save Settings** at the bottom of the page to save the current configuration.



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

WI-FI PROTECTED SETUP

Enable : ☑

Lock WPS-PIN Setup : □

PIN SETTINGS

Current PIN : 19726069

ADD WIRELESS STATION

Helpful Hints...

- **Enable** if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup.
- Click **Add Wireless Device With WPS** to use Wi-Fi Protected Setup to add wireless devices to the wireless network.

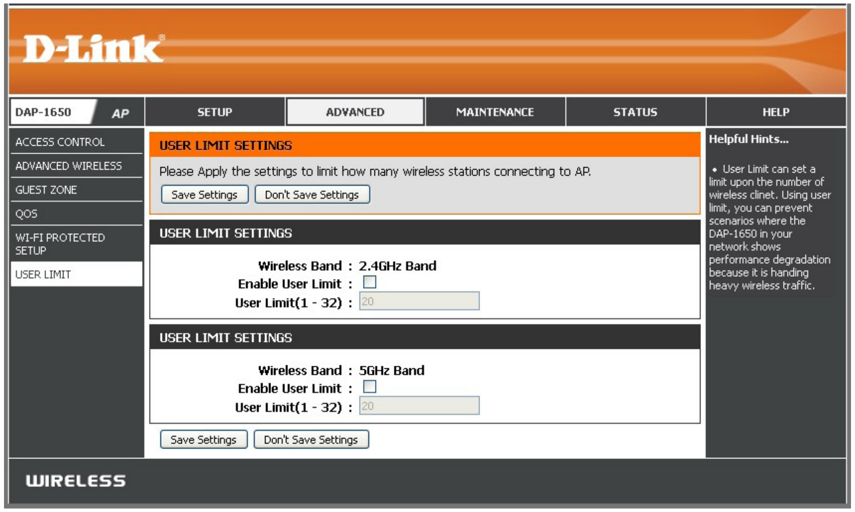
User Limit

The User Limit screen allows you to set a maximum number of wireless clients that can be connected to the access point at any one time for each wireless band.

Enable User Limit: For each wireless band, check the box to **Enable** the user limit option.

User Limit: Enter a number of users (indicates the number of wireless stations, between 1-32).

Click **Save Settings** at the bottom of the page to save the current configuration.



USER LIMIT SETTINGS

Please Apply the settings to limit how many wireless stations connecting to AP.

USER LIMIT SETTINGS

Wireless Band : 2.4GHz Band
Enable User Limit : □
User Limit(1 - 32) : 20

USER LIMIT SETTINGS

Wireless Band : 5GHz Band
Enable User Limit : □
User Limit(1 - 32) : 20

Helpful Hints...

- User Limit can set a limit upon the number of wireless clinet. Using user limit, you can prevent scenarios where the DAP-1650 in your network shows performance degradation because it is handing heavy wireless traffic.

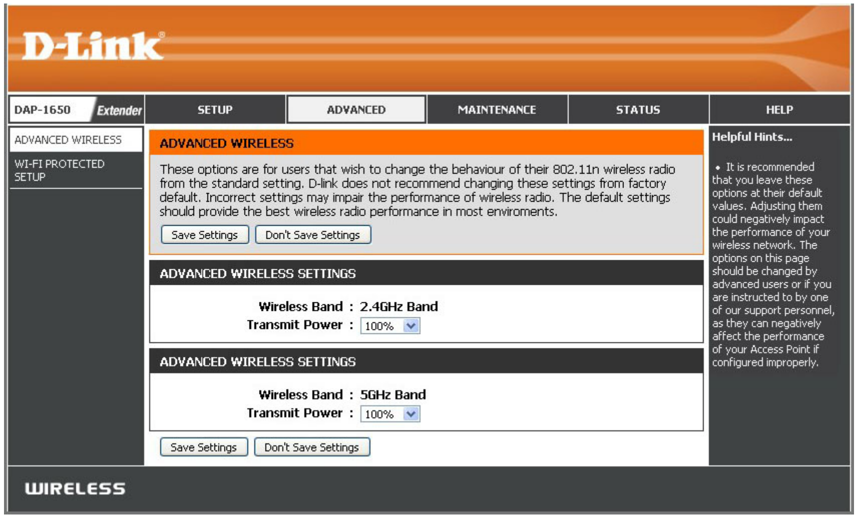
Extender Mode

Advanced Wireless

The Advanced Wireless screen allows you to adjust the advanced wireless settings for each wireless band.

Transmit Power: For each wireless band, select the preferred transmission power of the wireless radio from the drop-down menu.

Click **Save Settings** at the bottom of the page to save the current configuration.



ADVANCED WIRELESS

These options are for users that wish to change the behaviour of their 802.11n wireless radio from the standard setting. D-link does not recommend changing these settings from factory default. Incorrect settings may impair the performance of wireless radio. The default settings should provide the best wireless radio performance in most enviroments.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz Band
Transmit Power : 100%

ADVANCED WIRELESS SETTINGS

Wireless Band : 5GHz Band
Transmit Power : 100%

Helpful Hints...

- It is recommended that you leave these options at their default values. Adjusting them could negatively impact the performance of your wireless network. The options on this page should be changed by advanced users or if you are instructed to by one of our support personnel, as they can negatively affect the performance of your Access Point if configured improperly.

Wi-Fi Protected Setup

The Wi-Fi Protected Setup screen allows you select the method to be used for Wi-Fi Protected Setup (WPS) to create a secure wireless connection.

***Note:** Clients must support WPS in order for this method to be used.*

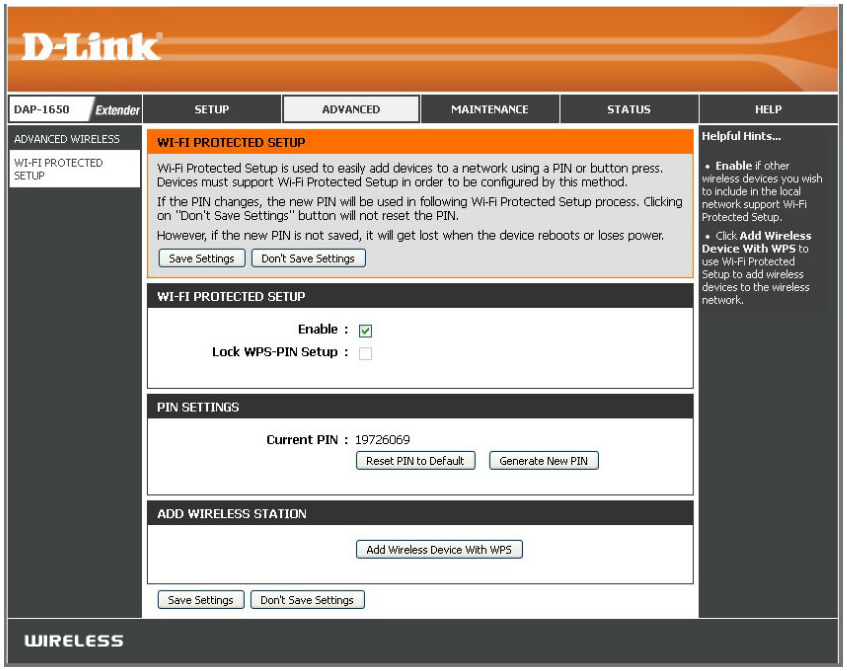
Enable: Check the box to **Enable** WPS.

Lock WPS-PIN Setup: Check the box to disable WPS using the PIN method. If this option is selected, wireless clients will only be able to use the WPS-PBC (push-button connection) method.

Current PIN: Displays the *Current PIN* which can be used by wireless clients to connect to the extender. Click **Reset PIN to Default** to return the PIN to its factory default. Click **Generate New PIN** to randomly generate a new PIN.

Add Wireless Device with WPS: Click **Add Wireless Device With WPS** to activate the WPS-PBC (push-button) method. You will then have 120 seconds to press the WPS button on the new device that you wish to connect.

Click **Save Settings** at the bottom of the page to save the current configuration.



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

WI-FI PROTECTED SETUP

Enable : ☑

Lock WPS-PIN Setup : □

PIN SETTINGS

Current PIN : 19726069

ADD WIRELESS STATION

Helpful Hints...

- **Enable** if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup.
- Click **Add Wireless Device With WPS** to use Wi-Fi Protected Setup to add wireless devices to the wireless network.

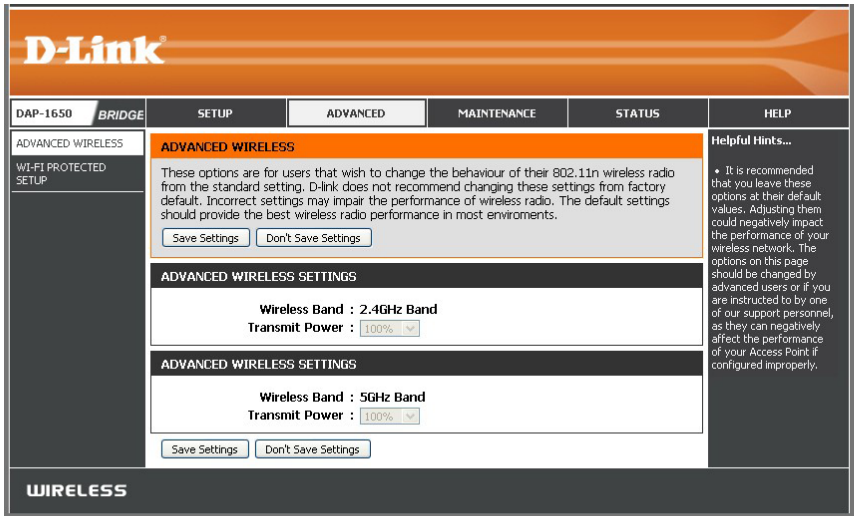
Media Bridge Mode

Advanced Wireless

The Advanced Wireless screen allows you to adjust the advanced wireless settings for each wireless band.

Transmit Power: For each wireless band, select the preferred transmission power of the wireless radio from the drop-down menu.

Click **Save Settings** at the bottom of the page to save the current configuration.



ADVANCED WIRELESS

These options are for users that wish to change the behaviour of their 802.11n wireless radio from the standard setting. D-link does not recommend changing these settings from factory default. Incorrect settings may impair the performance of wireless radio. The default settings should provide the best wireless radio performance in most enviroments.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz Band
Transmit Power : 100%

ADVANCED WIRELESS SETTINGS

Wireless Band : 5GHz Band
Transmit Power : 100%

Helpful Hints...

- It is recommended that you leave these options at their default values. Adjusting them could negatively impact the performance of your wireless network. The options on this page should be changed by advanced users or if you are instructed to by one of our support personnel, as they can negatively affect the performance of your Access Point if configured improperly.

Wi-Fi Protected Setup

The Wi-Fi Protected Setup screen allows you to use Wi-Fi Protected Setup (WPS) to create a secure wireless connection with a wireless router.

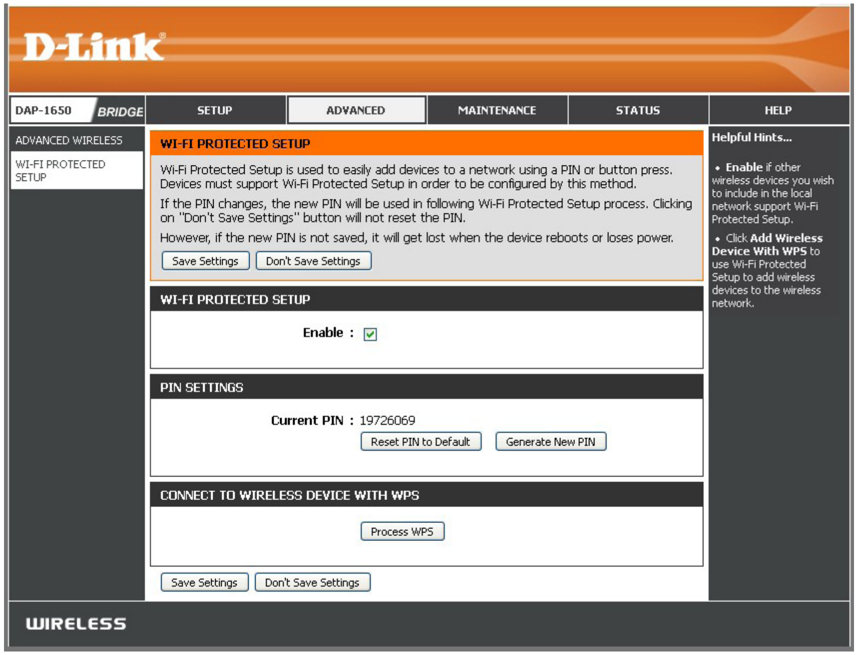
Note: *Router must support WPS in order for this method to be used.*

Enable: Check the box to **Enable** WPS.

Current PIN: Displays the *Current PIN* which can be used by a wireless router to connect to the media bridge. Click **Reset PIN to Default** to return the PIN to its factory default. Click **Generate New PIN** to randomly generate a new PIN.

Click **Add Wireless Device With WPS** to activate the WPS-PBC (push-button) method. You will then have 120 seconds to press the WPS button on the router that you wish to connect.

Click **Save Settings** at the bottom of the page to save the current configuration.



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

WI-FI PROTECTED SETUP

Enable : ☑

PIN SETTINGS

Current PIN : 19726069

CONNECT TO WIRELESS DEVICE WITH WPS

Helpful Hints...

- **Enable** if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup.
- Click **Add Wireless Device With WPS** to use Wi-Fi Protected Setup to add wireless devices to the wireless network.

Maintenance

The Maintenance section allows you to adjust the administrative settings for the DAP-1650, like time, date, and administrator password. You can also update the device's firmware, add or remove language packs, as well as configure the internal system clock.

Access Point Mode

Admin

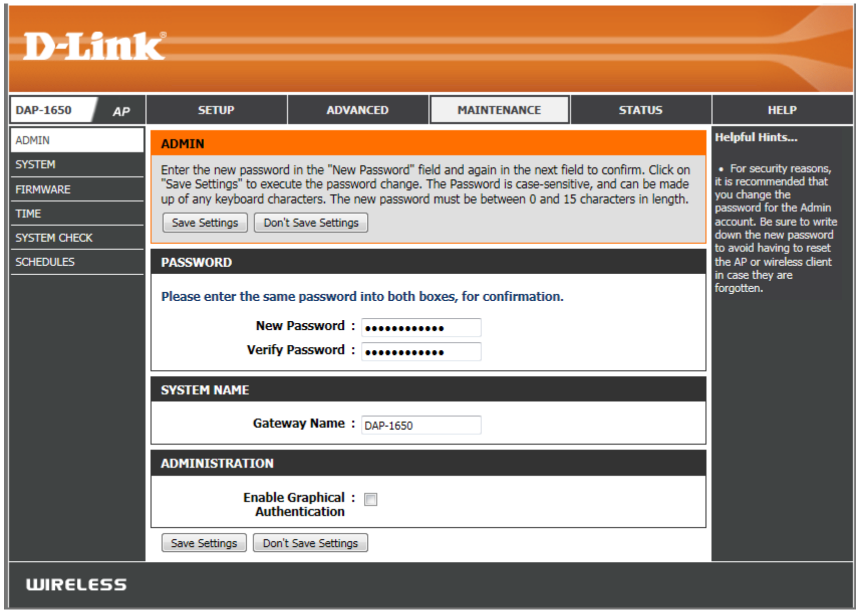
New Password: Enter a **New Password** for the web-based configuration utility's admin account.

Verify Password: Re-enter the **New Password** in this field.

Gateway Name: You can create a user-friendly name for your device.

Enable Graphical Authentication: Check the box to **Enable** CAPTCHA authentication for added security.

Click **Save Settings** at the bottom of the page to save the current configuration.



ADMIN

Enter the new password in the "New Password" field and again in the next field to confirm. Click on "Save Settings" to execute the password change. The Password is case-sensitive, and can be made up of any keyboard characters. The new password must be between 0 and 15 characters in length.

PASSWORD

Please enter the same password into both boxes, for confirmation.

New Password : ••••••••••••
Verify Password : ••••••••••••

SYSTEM NAME

Gateway Name : DAP-1650

ADMINISTRATION

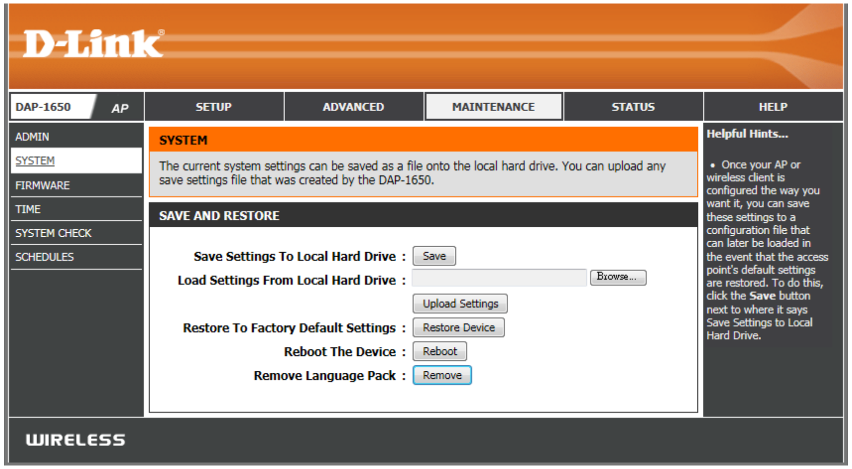
Enable Graphical Authentication : □

Helpful Hints...

- For security reasons, it is recommended that you change the password for the Admin account. Be sure to write down the new password to avoid having to reset the AP or wireless client in case they are forgotten.

System

The System screen allows you to save and restore the device's configuration, as well as restore the factory default settings.



SYSTEM

The current system settings can be saved as a file onto the local hard drive. You can upload any save settings file that was created by the DAP-1650.

SAVE AND RESTORE

Save Settings To Local Hard Drive : Save
Load Settings From Local Hard Drive : Upload Settings
Restore To Factory Default Settings : Restore Device
Reboot The Device : Reboot
Remove Language Pack : Remove

Helpful Hints...

- Once your AP or wireless client is configured the way you want it, you can save these settings to a configuration file that can later be loaded in the event that the access point's default settings are restored. To do this, click the **Save** button next to where it says Save Settings to Local Hard Drive.

Save Settings to Local Hard Drive: Click **Save** to save the DAP-1650's current configuration to a file on your local computer. A *Save File* dialog box will appear, prompting you to save the configuration file on your computer.

Load Settings From Local Hard Drive: Click **Browse** to locate a previously saved configuration file on your local computer. Once the file has been located, click **Upload Settings** to apply the configuration in the file to the access point.

Note: *This will overwrite any current configuration.*

Restore to Factory Default Settings: Click **Restore Device** to reset the DAP-1650's settings to the factory default settings.

Warning: *This will erase all current settings and cannot be undone.*

Reboot the Device: Click to **Reboot** the device. You will need to log in to the device again once the reboot has been completed.

Remove Language Pack: Click to **Remove** a language pack from the device.

Firmware

Use the Firmware page to update the device's firmware, and to add or remove language packs. Make sure the firmware you want to use is on the local hard drive of your computer.

Firmware Information: Displays the DAP-1650's *Current Firmware Version* and *Current Firmware Time*.

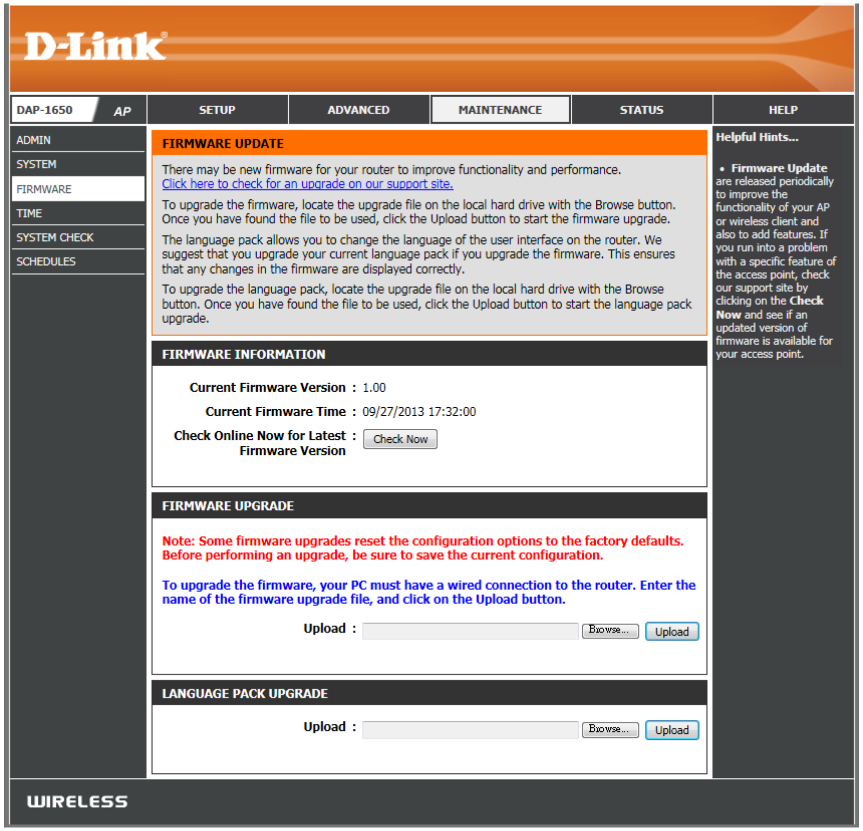
Note: *The access point must have an active Internet connection to check for firmware and language pack updates.*

Check Online Now for Latest Firmware Version: If you click on **Check Now** to check for an upgrade, and updates are detected, the details will be displayed here. Click **Download** to download the upgrade files to your computer.

Firmware Upgrade: Click **Browse** to locate a firmware file on your computer. Once located, click **Upload** to start the firmware upgrade process. It is recommended that you save your AP's current configuration using the System page before you begin a firmware upgrade.

Warning: *You must use a wired connection to the access point to update the firmware.*

Language Pack Upgrade: Click **Browse** to locate a language pack file on your computer. Once located, click **Upload** to start the language pack upgrade process.



FIRMWARE UPDATE

There may be new firmware for your router to improve functionality and performance.
Click here to check for an upgrade on our support site.

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the firmware upgrade.

The language pack allows you to change the language of the user interface on the router. We suggest that you upgrade your current language pack if you upgrade the firmware. This ensures that any changes in the firmware are displayed correctly.

To upgrade the language pack, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the language pack upgrade.

FIRMWARE INFORMATION

Current Firmware Version : 1.00
Current Firmware Time : 09/27/2013 17:32:00
Check Online Now for Latest Firmware Version : Check Now

FIRMWARE UPGRADE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

LANGUAGE PACK UPGRADE

Upload :

Helpful Hints...

- **Firmware Update** are released periodically to improve the functionality of your AP or wireless client and also to add features. If you run into a problem with a specific feature of the access point, check our support site by clicking on the **Check Now** and see if an updated version of firmware is available for your access point.

Time

Use the Time page to configure, update and maintain the correct time on the internal system clock. You can also configure daylight saving and synchronize the AP's clock and calendar with an internet-based network time protocol (NTP) server.

Time: Displays the DAP-1650's current *Date* and *Time*.

Time Zone: Select your **Time Zone** from the drop-down menu.

Enable Daylight Saving: Check the box if you want to **Enable** manual entry of daylight saving time.

Daylight Saving Offset: If you enabled Daylight Saving, you will be able to select a **Daylight Saving Offset**. The offset value is one hour by default.

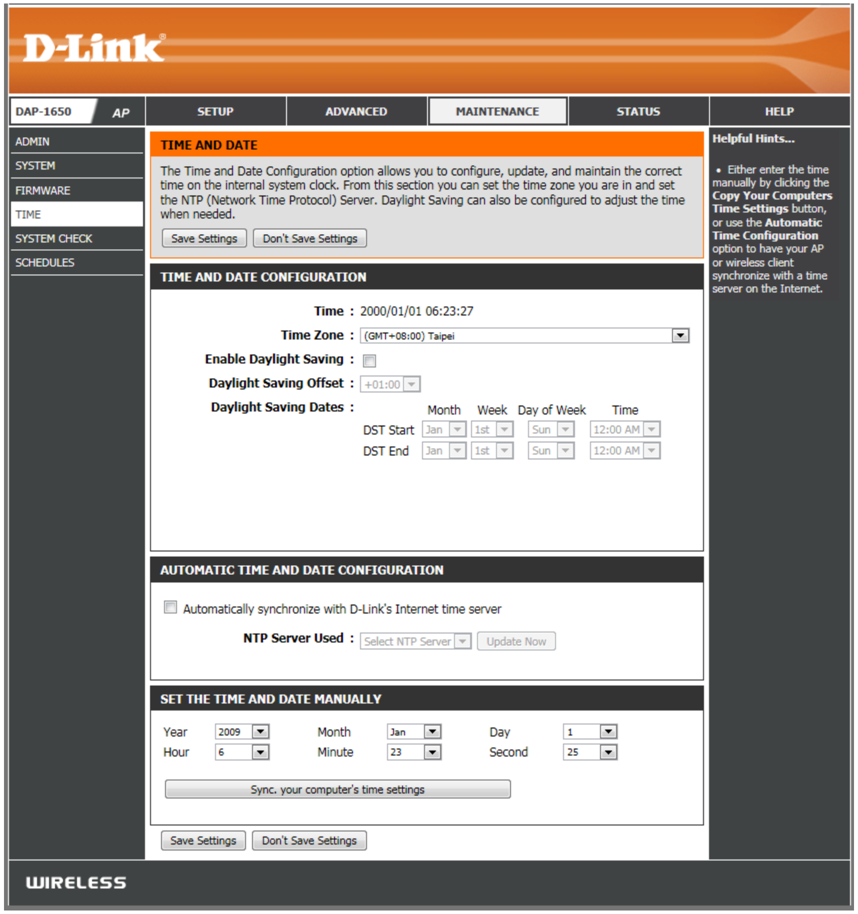
Daylight Saving Dates: Use the drop-down menus to set the **Start** and **End** dates for daylight saving time.

Automatically Synchronize with D-Link's Internet Time Server: Check the box to have the access point automatically synchronize its clock and calendar with D-Link's Internet time server.

NTP Server Used: Enter the address of the NTP server you would like to use, or choose a pre-determined server from the drop-down menu and click **Update Now** to populate the field.

Set the Time and Date Manually: Use the drop-down menus to manually enter the time and date. This option will not be available if **Automatically synchronize...** is checked above.

You can also click **Sync. Your Computer's Time Settings** to synchronize the date and time with your computer's time settings. Click **Save Settings** at the bottom of the page to save the current configuration.



TIME AND DATE

The Time and Date Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.

TIME AND DATE CONFIGURATION

Time : 2000/01/01 06:23:27
Time Zone : (GMT+08:00) Taipei
Enable Daylight Saving : □
Daylight Saving Offset : +01:00
Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Jan	1st	Sun	12:00 AM
DST End	Jan	1st	Sun	12:00 AM

AUTOMATIC TIME AND DATE CONFIGURATION

□ Automatically synchronize with D-Link's Internet time server

NTP Server Used : Select NTP Server

SET THE TIME AND DATE MANUALLY

Year	2009	Month	Jan	Day	1
Hour	6	Minute	23	Second	25

Helpful Hints...

- Either enter the time manually by clicking the **Copy Your Computers Time Settings** button, or use the **Automatic Time Configuration** option to have your AP or wireless client synchronize with a time server on the Internet.

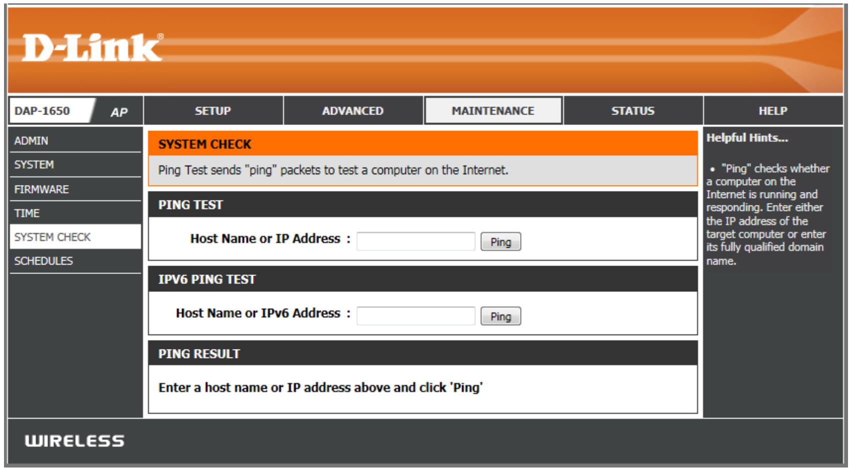
System Check

The System Check page allows you to send Ping packets to test whether or not a computer is on the Internet.

Host Name or IP Address: Enter the **Host Name** or **IP Address** for which you wish to conduct a ping test.

Host Name or IPv6 Address: Enter the **Host Name** or **IPv6 Address** for which you wish to conduct a ping test.

Ping Result: Displays *Results* of the ping test.



SYSTEM CHECK

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Host Name or IP Address :

IPV6 PING TEST

Host Name or IPv6 Address :

PING RESULT

Enter a host name or IP address above and click 'Ping'

Helpful Hints...

- "Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.

Schedules

The Schedule screen can be used to create schedules for use with enforcing rules for various access point functions. Schedules created here will be available for selection from drop-down menus throughout the configuration utility.

Name: Enter a **Name** to identity the new schedule rule.

Day(s): Click **All Week** to make the rule active for every day of the week, or click **Select Day(s)** to specify days on which to activate the rule. Check the box by the day of the week to indicate which days.

All Day - 24 hrs: Check the box to make the rule active *All Day* for the days selected above.

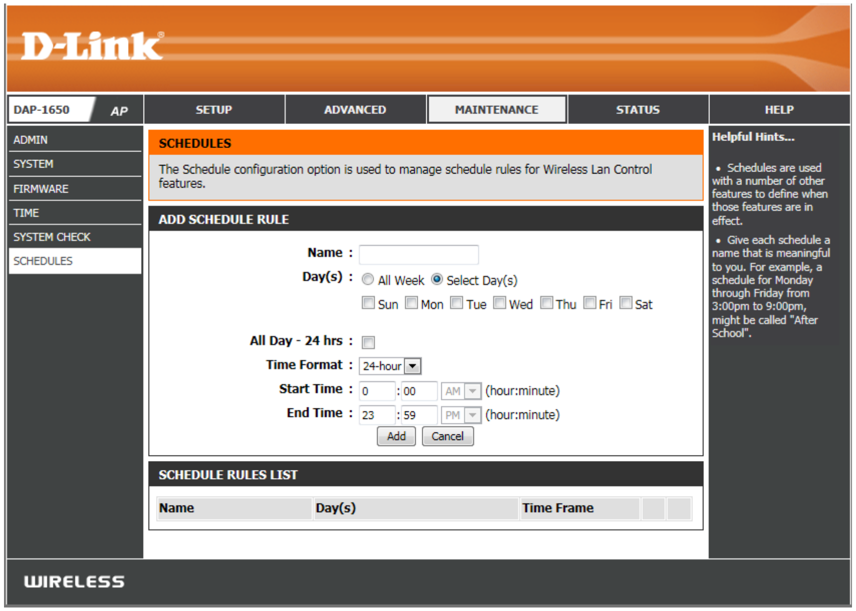
Time format: Select whether you would like to use **24-hour** or **12-hour** time format.

Start Time: Enter the **Time** for the rule to become active on each of the days selected above.

End Time: Enter the **Time** for the rule to become inactive on each of the days selected above.

Click **Add** to add the rule to the Schedule Rules List. Click **Cancel** to clear all fields.

Schedule Rules List: This table displays a summary of all current *Schedule Rules*. Click on the **Edit** icon to edit the rule, or click on the **Trash** icon to delete the rule from the list.



SCHEDULES

The Schedule configuration option is used to manage schedule rules for Wireless Lan Control features.

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Time Format : 24-hour

Start Time : 0 : 00 AM (hour:minute)

End Time : 23 : 59 PM (hour:minute)

SCHEDULE RULES LIST

Name	Day(s)	Time Frame		

Helpful Hints...

- Schedules are used with a number of other features to define when those features are in effect.
- Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

Extender Mode

Admin

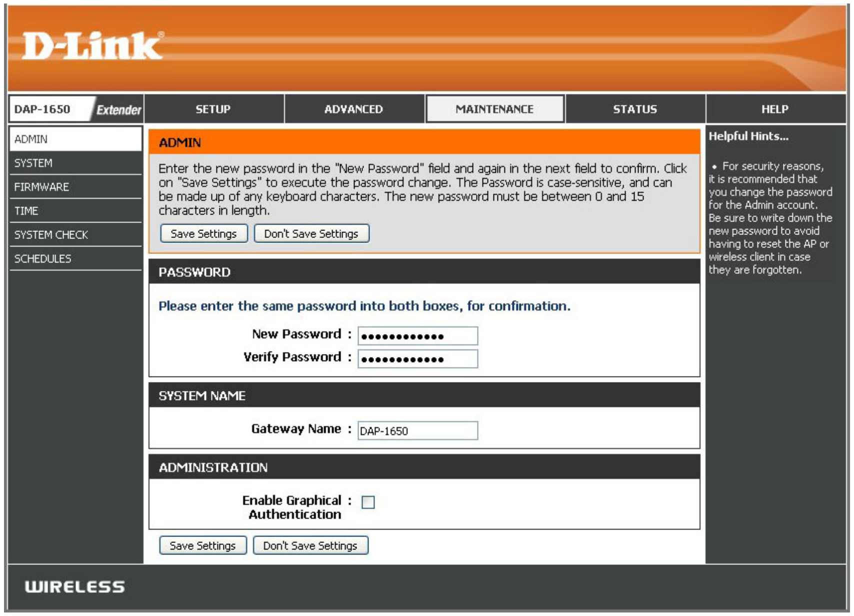
New Password: Enter a **New Password** for the web-based configuration utility's admin account.

Verify Password: Re-enter the **New Password** in this field.

Gateway Name: You can create a user-friendly name for your device.

Enable Graphical Authentication: Check the box to **Enable** CAPTCHA authentication for added security.

Click **Save Settings** at the bottom of the page to save the current configuration.



ADMIN

Enter the new password in the "New Password" field and again in the next field to confirm. Click on "Save Settings" to execute the password change. The Password is case-sensitive, and can be made up of any keyboard characters. The new password must be between 0 and 15 characters in length.

PASSWORD

Please enter the same password into both boxes, for confirmation.

New Password : ••••••••••••

Verify Password : ••••••••••••

SYSTEM NAME

Gateway Name : DAP-1650

ADMINISTRATION

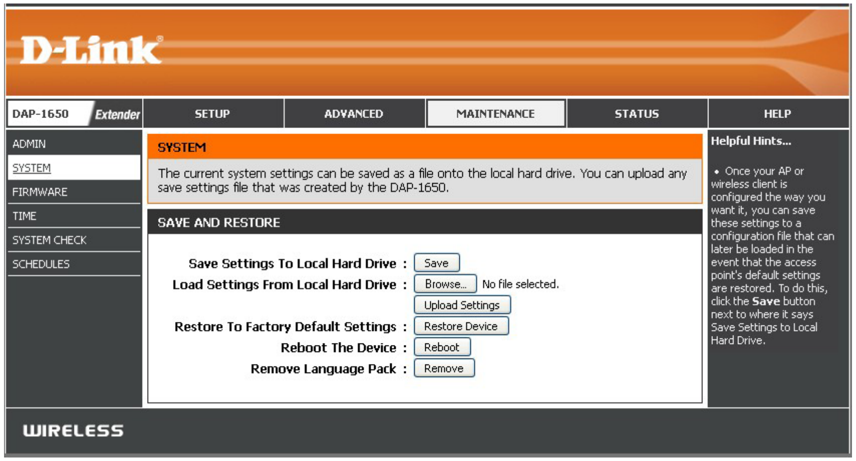
Enable Graphical Authentication : □

Helpful Hints...

- For security reasons, it is recommended that you change the password for the Admin account. Be sure to write down the new password to avoid having to reset the AP or wireless client in case they are forgotten.

System

The System screen allows you to save and restore the device's configuration, as well as restore the factory default settings.



The current system settings can be saved as a file onto the local hard drive. You can upload any save settings file that was created by the DAP-1650.

Save Settings To Local Hard Drive :
Load Settings From Local Hard Drive : No file selected.
Restore To Factory Default Settings :
Reboot The Device :
Remove Language Pack :

- Once your AP or wireless client is configured the way you want it, you can save these settings to a configuration file that can later be loaded in the event that the access point's default settings are restored. To do this, click the **Save** button next to where it says Save Settings to Local Hard Drive.

Save Settings to Local Hard Drive: Click **Save** to save the DAP-1650's current configuration to a file on your local computer. A *Save File* dialog box will appear, prompting you to save the configuration file on your computer.

Load Settings From Local Hard Drive: Click **Browse** to locate a previously saved configuration file on your local computer. Once the file has been located, click **Upload Settings** to apply the configuration in the file to the extender.

Note: *This will overwrite any current configuration.*

Restore to Factory Default Settings: Click **Restore Device** to reset the DAP-1650's settings to the factory default settings.

Warning: *This will erase all current settings and cannot be undone.*

Reboot the Device: Click to **Reboot** the device. You will need to log in to the device again once the reboot has been completed.

Remove Language Pack: Click to **Remove** a language pack from the device.

Firmware

Use the Firmware page to update the device's firmware, and to add or remove language packs. Make sure the firmware you want to use is on the local hard drive of your computer.

Firmware Information: Displays the DAP-1650's *Current Firmware Version* and *Current Firmware Time*.

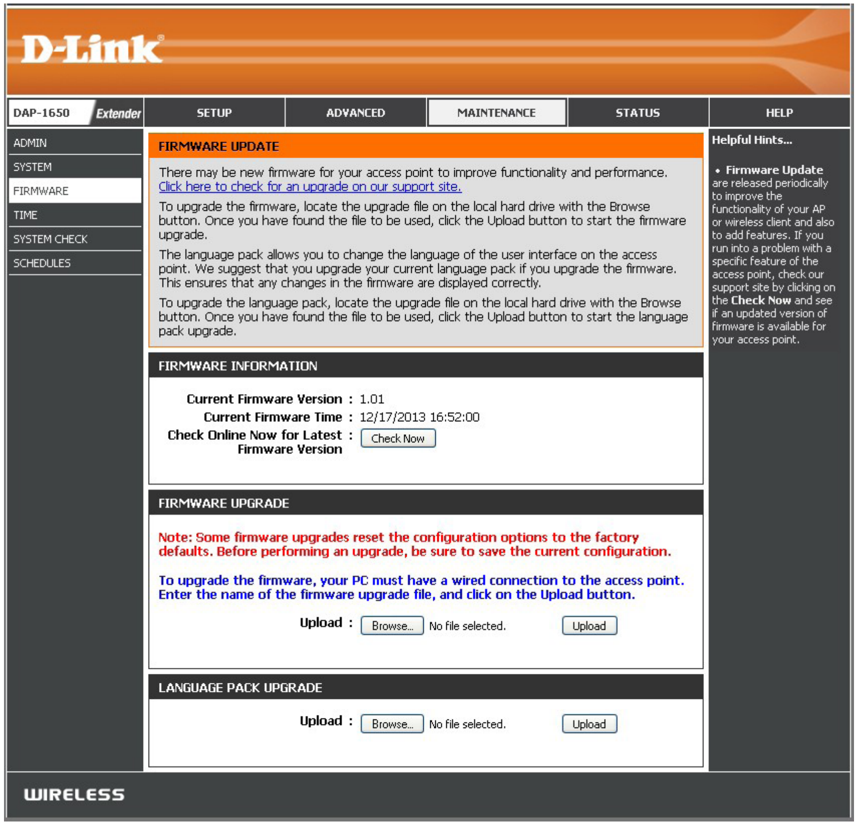
Note: *The extender must have an active Internet connection to check for firmware and language pack updates.*

Check Online Now for Latest Firmware Version: If you click on **Check Now** to check for an upgrade, and updates are detected, the details will be displayed here. Click **Download** to download the upgrade files to your computer.

Firmware Upgrade: Click **Browse** to locate a firmware file on your computer. Once located, click **Upload** to start the firmware upgrade process. It is recommended that you save your device's current configuration using the System page before you begin a firmware upgrade.

Warning: *You must use a wired connection to the device to update the firmware.*

Language Pack Upgrade: Click **Browse** to locate a language pack file on your computer. Once located, click **Upload** to start the language pack upgrade process.



FIRMWARE UPDATE

There may be new firmware for your access point to improve functionality and performance.
Click here to check for an upgrade on our support site.

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the firmware upgrade.

The language pack allows you to change the language of the user interface on the access point. We suggest that you upgrade your current language pack if you upgrade the firmware. This ensures that any changes in the firmware are displayed correctly.

To upgrade the language pack, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the language pack upgrade.

FIRMWARE INFORMATION

Current Firmware Version : 1.01
Current Firmware Time : 12/17/2013 16:52:00
Check Online Now for Latest Firmware Version : Check Now

FIRMWARE UPGRADE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.

To upgrade the firmware, your PC must have a wired connection to the access point. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload : Browse... No file selected. Upload

LANGUAGE PACK UPGRADE

Upload : Browse... No file selected. Upload

Helpful Hints...

- **Firmware Update** are released periodically to improve the functionality of your AP or wireless client and also to add features. If you run into a problem with a specific feature of the access point, check our support site by clicking on the **Check Now** and see if an updated version of firmware is available for your access point.

Time

Use the Time page to configure, update and maintain the correct time on the internal system clock. You can also configure daylight saving and synchronize the device's clock and calendar with an internet-based network time protocol (NTP) server.

Time: Displays the DAP-1650's current *Date* and *Time*.

Time Zone: Select your **Time Zone** from the drop-down menu.

Enable Daylight Saving: Check the box if you want to **Enable** manual entry of daylight saving time.

Daylight Saving Offset: If you enabled Daylight Saving, you will be able to select a **Daylight Saving Offset**. The offset value is one hour by default.

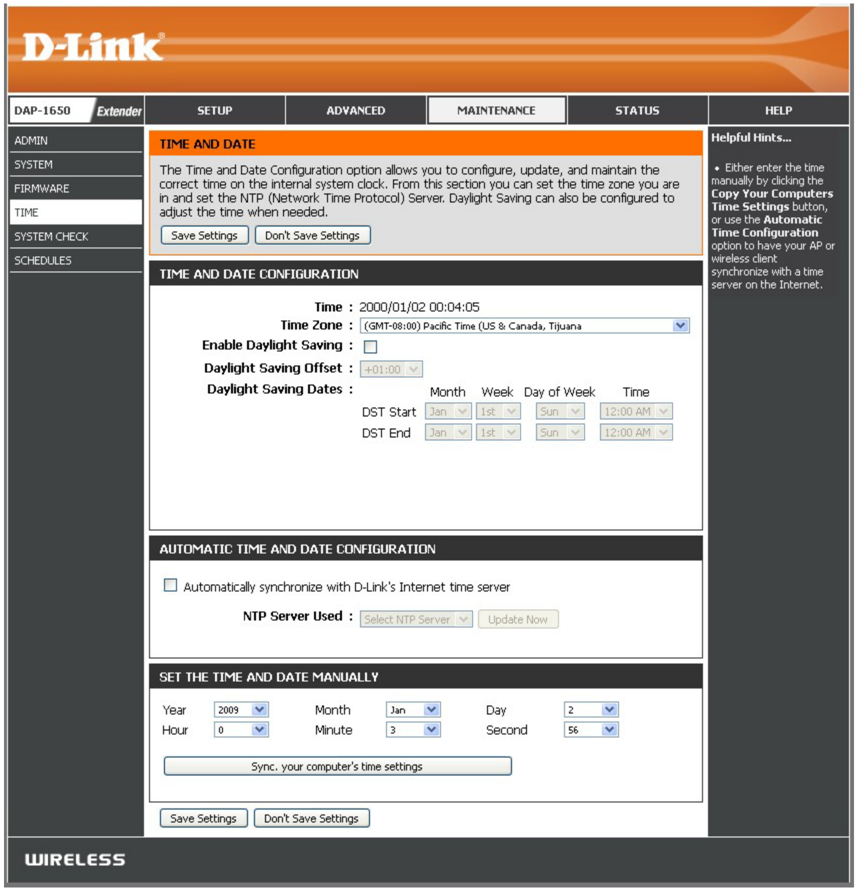
Daylight Saving Dates: Use the drop-down menus to set the **Start** and **End** dates for daylight saving time.

Automatically Synchronize with D-Link's Internet Time Server: Check the box to have the extender automatically synchronize its clock and calendar with D-Link's Internet time server.

NTP Server Used: Enter the address of the NTP server you would like to use, or choose a pre-determined server from the drop-down menu and click **Update Now** to populate the field.

Set the Time and Date Manually: Use the drop-down menus to manually enter the time and date. This option will not be available if **Automatically synchronize...** is checked above.

You can also click **Sync. Your Computer's Time Settings** to synchronize the date and time with your computer's time settings. Click **Save Settings** at the bottom of the page to save the current configuration.



TIME AND DATE

The Time and Date Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.

TIME AND DATE CONFIGURATION

Time : 2000/01/02 00:04:05
Time Zone : (GMT-08:00) Pacific Time (US & Canada, Tijuana
Enable Daylight Saving : □
Daylight Saving Offset : +01:00
Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Jan	1st	Sun	12:00 AM
DST End	Jan	1st	Sun	12:00 AM

AUTOMATIC TIME AND DATE CONFIGURATION

□ Automatically synchronize with D-Link's Internet time server
NTP Server Used : Select NTP Server

SET THE TIME AND DATE MANUALLY

Year	2009	Month	Jan	Day	2
Hour	0	Minute	3	Second	56

Helpful Hints...

- Either enter the time manually by clicking the **Copy Your Computers Time Settings** button, or use the **Automatic Time Configuration** option to have your AP or wireless client synchronize with a time server on the Internet.

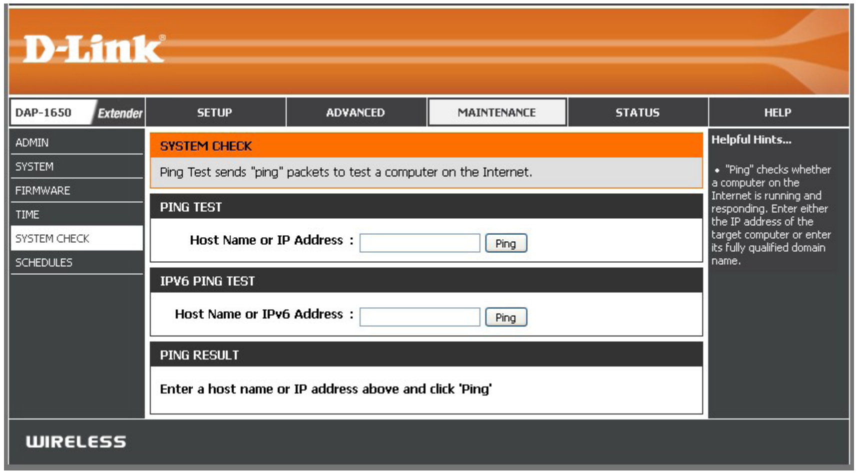
System Check

The System Check page allows you to send Ping packets to test whether or not a computer is on the Internet.

Host Name or IP Address: Enter the **Host Name** or **IP Address** for which you wish to conduct a ping test.

Host Name or IPv6 Address: Enter the **Host Name** or **IPv6 Address** for which you wish to conduct a ping test.

Ping Result: Displays *Results* of the ping test.



SYSTEM CHECK

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Host Name or IP Address :

IPV6 PING TEST

Host Name or IPv6 Address :

PING RESULT

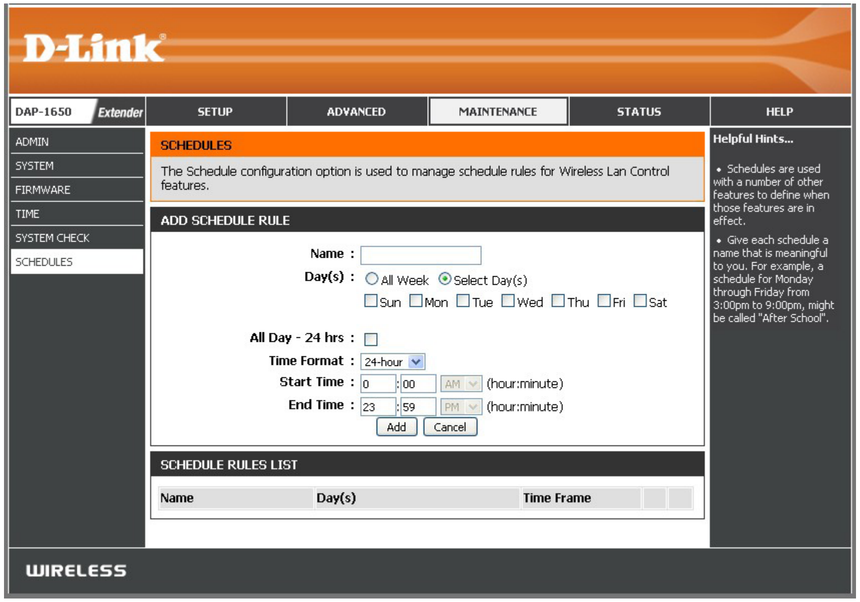
Enter a host name or IP address above and click 'Ping'

Helpful Hints...

- "Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.

Schedules

The Schedule screen can be used to create schedules for use with enforcing rules for various extender functions. Schedules created here will be available for selection from drop-down menus throughout the configuration utility.



SCHEDULES

The Schedule configuration option is used to manage schedule rules for Wireless Lan Control features.

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Time Format : 24-hour

Start Time : 0 : 00 AM (hour:minute)

End Time : 23 : 59 PM (hour:minute)

Add Cancel

SCHEDULE RULES LIST

Name	Day(s)	Time Frame		

Helpful Hints...

- Schedules are used with a number of other features to define when those features are in effect.
- Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

Name: Enter a **Name** to identity the new schedule rule.

Day(s): Click **All Week** to make the rule active for every day of the week, or click **Select Day(s)** to specify days on which to activate the rule. Check the box by the day of the week to indicate which days.

All Day - 24 hrs: Check the box to make the rule active *All Day* for the days selected above.

Time format: Select whether you would like to use **24-hour** or **12-hour** time format.

Start Time: Enter the **Time** for the rule to become active on each of the days selected above.

End Time: Enter the **Time** for the rule to become inactive on each of the days selected above.

Click **Add** to add the rule to the Schedule Rules List. Click **Cancel** to clear all fields.

Schedule Rules List: This table displays a summary of all current *Schedule Rules*. Click on the **Edit** icon to edit the rule, or click on the **Trash** icon to delete the rule from the list.

Media Bridge Mode

Admin

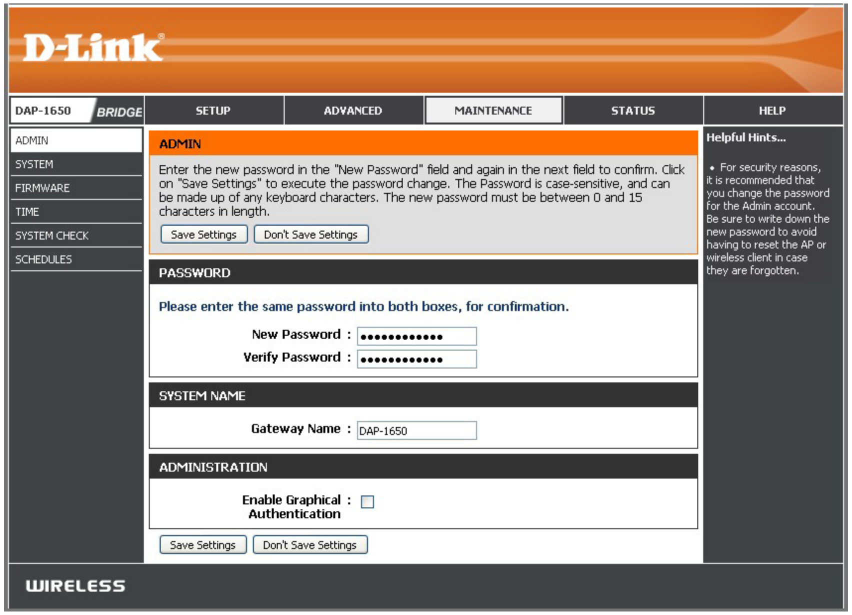
New Password: Enter a **New Password** for the web-based configuration utility's admin account.

Verify Password: Re-enter the **New Password** in this field.

Gateway Name: You can create a user-friendly name for your device.

Enable Graphical Authentication: Check the box to **Enable** CAPTCHA authentication for added security.

Click **Save Settings** at the bottom of the page to save the current configuration.



ADMIN

Enter the new password in the "New Password" field and again in the next field to confirm. Click on "Save Settings" to execute the password change. The Password is case-sensitive, and can be made up of any keyboard characters. The new password must be between 0 and 15 characters in length.

PASSWORD

Please enter the same password into both boxes, for confirmation.

New Password : ••••••••••••

Verify Password : ••••••••••••

SYSTEM NAME

Gateway Name : DAP-1650

ADMINISTRATION

Enable Graphical Authentication : □

Helpful Hints...

- For security reasons, it is recommended that you change the password for the Admin account. Be sure to write down the new password to avoid having to reset the AP or wireless client in case they are forgotten.

System

The System screen allows you to save and restore the device's configuration, as well as restore the factory default settings.

Save Settings to Local Hard Drive: Click **Save** to save the DAP-1650's current configuration to a file on your local computer. A *Save File* dialog box will appear, prompting you to save the configuration file on your computer.

Load Settings From Local Hard Drive: Click **Browse** to locate a previously saved configuration file on your local computer. Once the file has been located, click **Upload Settings** to apply the configuration in the file to the device.

.

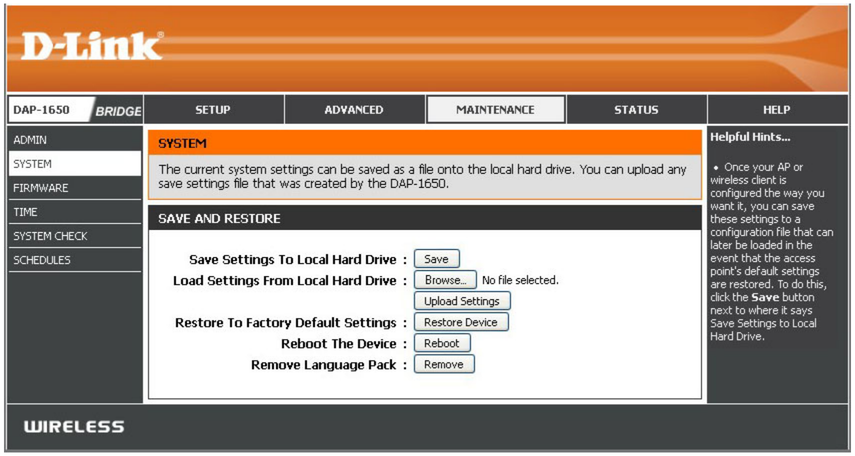
Note: *This will overwrite any current configuration.*

Restore to Factory Default Settings: Click **Restore Device** to reset the DAP-1650's settings to the factory defaults.

Warning: *This will erase all current settings and cannot be undone.*

Reboot the Device: Click **Reboot** to reboot the device. You will need to log in to the device again once the reboot has been completed.

Remove Language Pack: Click to **Remove** a language pack from the device.



SYSTEM

The current system settings can be saved as a file onto the local hard drive. You can upload any save settings file that was created by the DAP-1650.

SAVE AND RESTORE

Save Settings To Local Hard Drive : Save
Load Settings From Local Hard Drive : Browse... No file selected.
Upload Settings
Restore To Factory Default Settings : Restore Device
Reboot The Device : Reboot
Remove Language Pack : Remove

Helpful Hints...

- Once your AP or wireless client is configured the way you want it, you can save these settings to a configuration file that can later be loaded in the event that the access point's default settings are restored. To do this, click the **Save** button next to where it says Save Settings to Local Hard Drive.

Firmware

Use the Firmware page to update the device's firmware, and to add or remove language packs. Make sure the firmware you want to use is on the local hard drive of your computer.

Firmware Information: Displays the DAP-1650's *Current Firmware Version* and *Current Firmware Time*.

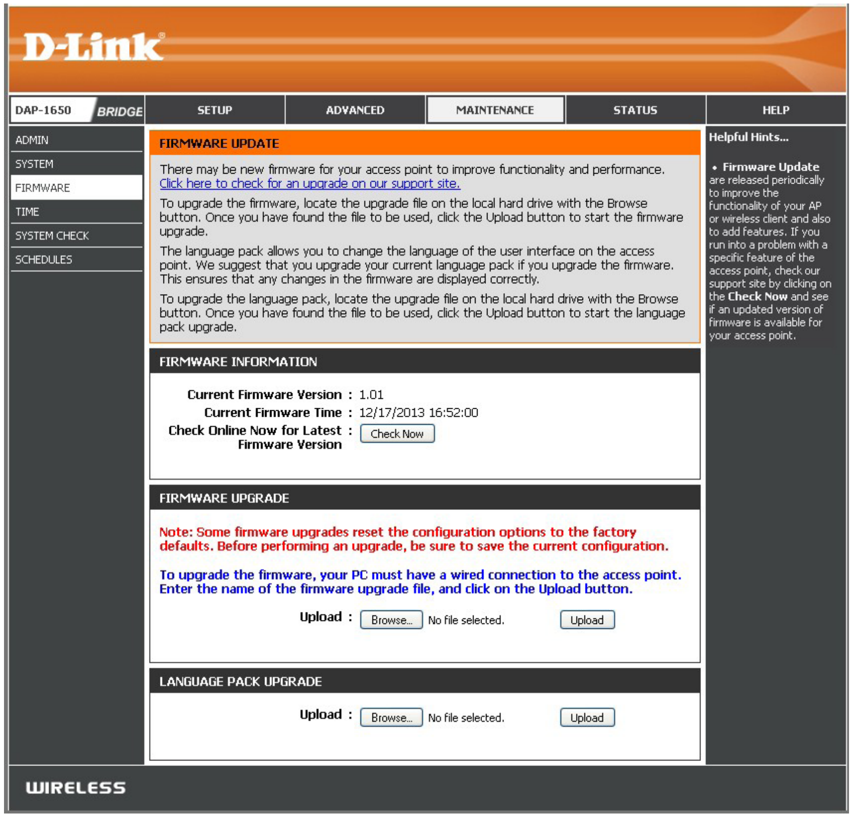
Note: *The media bridge must have an active Internet connection to check for firmware and language pack updates.*

Check Online Now for Latest Firmware Versions: If you click on **Check Now** to check for an upgrade, and updates are detected, the details will be displayed here. Click **Download** to download the upgrade files to your computer.

Firmware Upgrade: Click **Browse** to locate a firmware file on your computer. Once located, click **Upload** to start the firmware upgrade process. It is recommended that you save your device's current configuration using the System page before you begin a firmware upgrade.

Warning: *You must use a wired connection to the device to update the firmware.*

Language Pack Upgrade: Click **Browse** to locate a language pack file on your computer. Once located, click **Upload** to start the language pack upgrade process.



FIRMWARE UPDATE

There may be new firmware for your access point to improve functionality and performance.
Click here to check for an upgrade on our support site.

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the firmware upgrade.

The language pack allows you to change the language of the user interface on the access point. We suggest that you upgrade your current language pack if you upgrade the firmware. This ensures that any changes in the firmware are displayed correctly.

To upgrade the language pack, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the language pack upgrade.

FIRMWARE INFORMATION

Current Firmware Version : 1.01
Current Firmware Time : 12/17/2013 16:52:00
Check Online Now for Latest Firmware Version : Check Now

FIRMWARE UPGRADE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.

To upgrade the firmware, your PC must have a wired connection to the access point. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload : Browse... No file selected. Upload

LANGUAGE PACK UPGRADE

Upload : Browse... No file selected. Upload

Helpful Hints...

- **Firmware Update** are released periodically to improve the functionality of your AP or wireless client and also to add features. If you run into a problem with a specific feature of the access point, check our support site by clicking on the **Check Now** and see if an updated version of firmware is available for your access point.

Time

Use the Time page to configure, update and maintain the correct time on the internal system clock. You can also configure daylight saving and synchronize the device's clock and calendar with an internet-based network time protocol (NTP) server.

Time: Displays the DAP-1650's current *Date* and *Time*.

Time Zone: Select your **Time Zone** from the drop-down menu.

Enable Daylight Saving: Check the box if you want to **Enable** manual entry of daylight saving time.

Daylight Saving Offset: If you enabled Daylight Saving, you will be able to select a **Daylight Saving Offset**. The offset value is one hour by default.

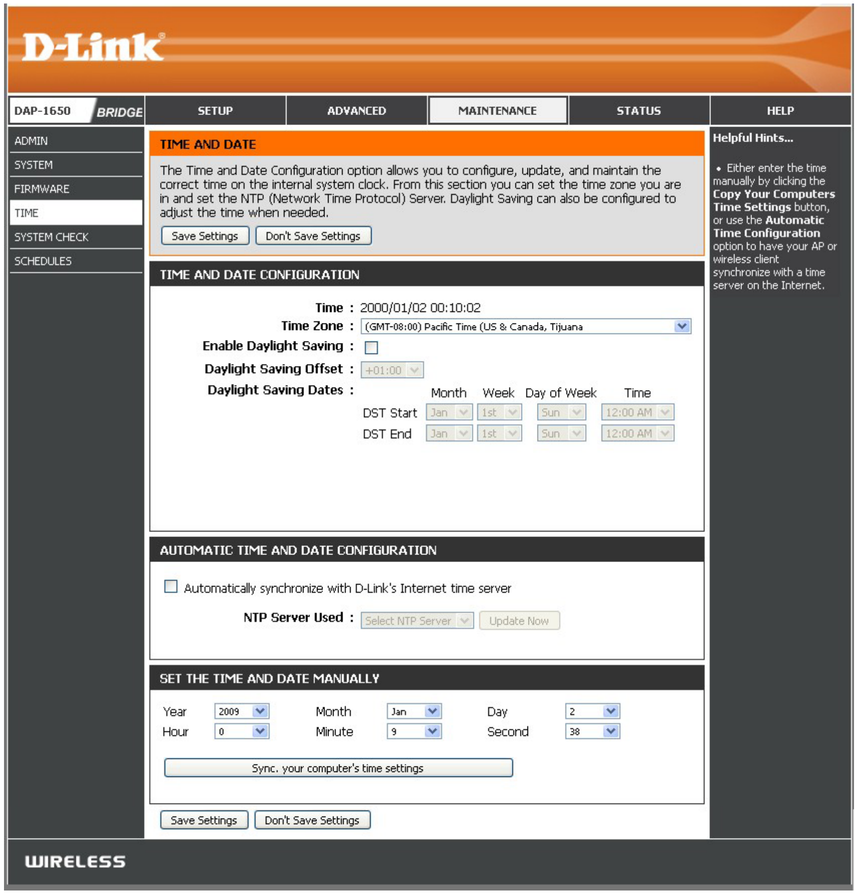
Daylight Saving Dates: Use the drop-down menus to set the **Start** and **End** dates for daylight saving time.

Automatically Synchronize with D-Link's Internet Time Server: Check the box to have the device automatically synchronize its clock and calendar with D-Link's Internet time server.

NTP Server Used: Enter the address of the NTP server you would like to use, or choose a pre-determined server from the drop-down menu and click **Update Now** to populate the field.

Set the Time and Date Manually: Use the drop-down menus to manually enter the time and date. This option will not be available if **Automatically synchronize...** is checked above.

You can also click **Sync. Your Computer's Time Settings** to synchronize the date and time with your computer's time settings. Click **Save Settings** at the bottom of the page to save the current configuration.



TIME AND DATE

The Time and Date Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.

Save Settings | Don't Save Settings

TIME AND DATE CONFIGURATION

Time : 2000/01/02 00:10:02

Time Zone : (GMT-08:00) Pacific Time (US & Canada, Tijuana

Enable Daylight Saving : □

Daylight Saving Offset : +01:00

Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Jan	1st	Sun	12:00 AM
DST End	Jan	1st	Sun	12:00 AM

AUTOMATIC TIME AND DATE CONFIGURATION

□ Automatically synchronize with D-Link's Internet time server

NTP Server Used : Select NTP Server | Update Now

SET THE TIME AND DATE MANUALLY

Year	2009	Month	Jan	Day	2
Hour	0	Minute	9	Second	38

Sync. your computer's time settings

Save Settings | Don't Save Settings

Helpful Hints...

- Either enter the time manually by clicking the **Copy Your Computers Time Settings** button, or use the **Automatic Time Configuration** option to have your AP or wireless client synchronize with a time server on the Internet.

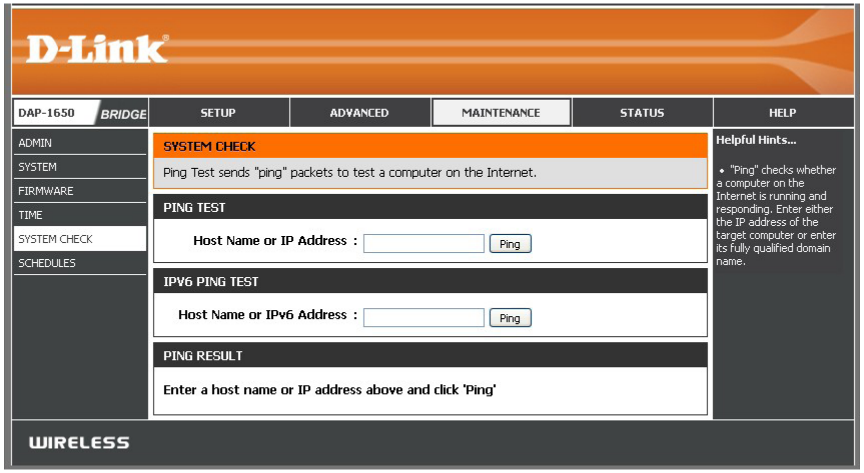
System Check

The System Check page allows you to send Ping packets to test whether or not a computer is on the Internet.

Host Name or IP Address: Enter the **Host Name** or **IP Address** for which you wish to conduct a ping test.

Host Name or IPv6 Address: Enter the **Host Name** or **IPv6 Address** for which you wish to conduct a ping test.

Ping Result: Displays *Results* of the ping test.



SYSTEM CHECK

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Host Name or IP Address :

IPV6 PING TEST

Host Name or IPv6 Address :

PING RESULT

Enter a host name or IP address above and click 'Ping'

Helpful Hints...

- "Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.

Schedules

The Schedule screen can be used to create schedules for use with enforcing rules for various media bridge functions. Schedules created here will be available for selection from drop-down menus throughout the configuration utility.

Name: Enter a **Name** to identity the new schedule rule.

Day(s): Click **All Week** to make the rule active for every day of the week, or click **Select Day(s)** to specify days on which to activate the rule. Check the box by the day of the week to indicate which days.

All Day - 24 hrs: Check the box to make the rule active *All Day* for the days selected above.

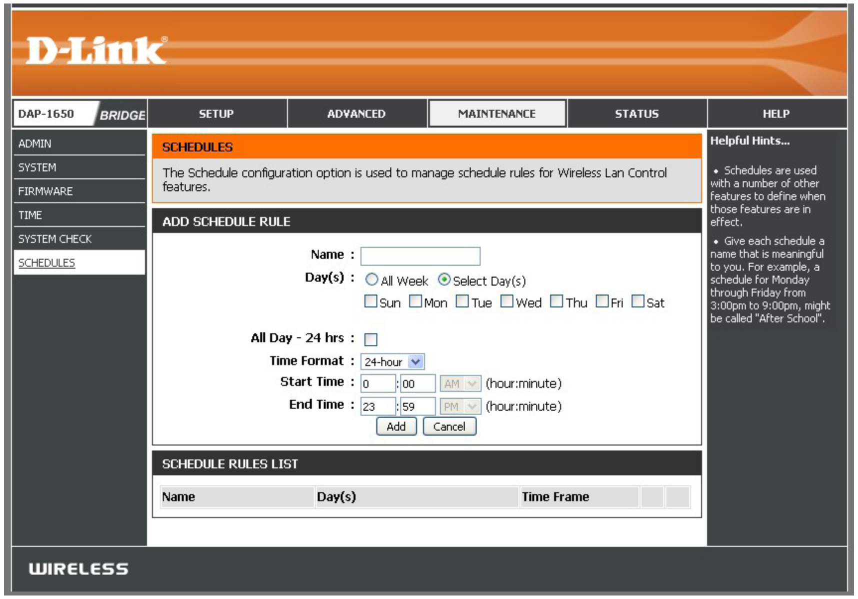
Time format: Select whether you would like to use **24-hour** or **12-hour** time format.

Start Time: Enter the **Time** for the rule to become active on each of the days selected above.

End Time: Enter the **Time** for the rule to become inactive on each of the days selected above.

Click **Add** to add the rule to the Schedule Rules List. Click **Cancel** to clear all fields.

Schedule Rules List: This table displays a summary of all current *Schedule Rules*. Click on the **Edit** icon to edit the rule, or click on the **Trash** icon to delete the rule from the list.



SCHEDULES

The Schedule configuration option is used to manage schedule rules for Wireless Lan Control features.

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Time Format : 24-hour

Start Time : 0 : 00 AM (hour:minute)

End Time : 23 : 59 PM (hour:minute)

SCHEDULE RULES LIST

Name	Day(s)	Time Frame		

Helpful Hints...

- Schedules are used with a number of other features to define when those features are in effect.
- Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

Status

This section displays the current information for the DAP-1650, such as device info, current log of events, and traffic statistics.

Access Point Mode

Device Info

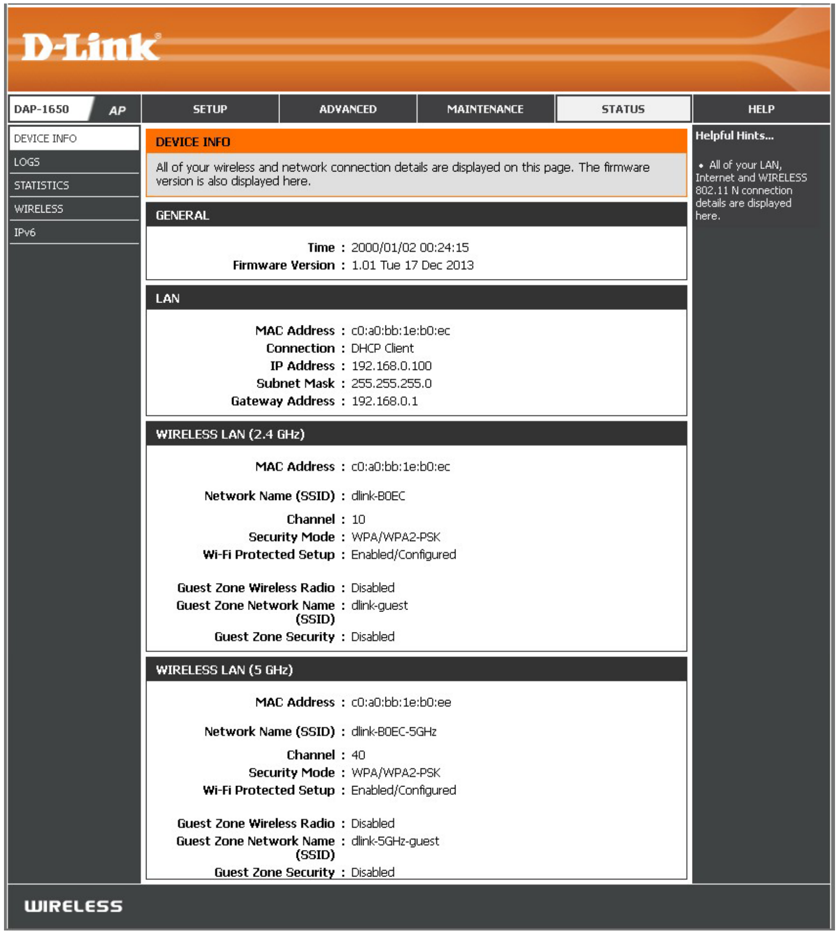
This screen displays the current information for the DAP-1650, such as LAN and wireless LAN details.

General: Displays the DAP-1650’s *Time* and *Firmware Version*.

LAN: Displays the *MAC Address* and the private (local) IP settings for the access point.

Wireless LAN (2.4GHz): Displays the wireless *MAC Address* and wireless settings such as SSID and *Channel* for the 2.4GHz wireless band.

Wireless LAN (5GHz): Displays the wireless *MAC Address* and wireless settings such as SSID and *Channel* for the 5GHz wireless band.



DEVICE INFO

All of your wireless and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : 2000/01/02 00:24:15
Firmware Version : 1.01 Tue 17 Dec 2013

LAN

MAC Address : c0:a0:bb:1e:b0:ec
Connection : DHCP Client
IP Address : 192.168.0.100
Subnet Mask : 255.255.255.0
Gateway Address : 192.168.0.1

WIRELESS LAN (2.4 GHz)

MAC Address : c0:a0:bb:1e:b0:ec
Network Name (SSID) : dlink-B0EC
Channel : 10
Security Mode : WPA/WPA2-PSK
Wi-Fi Protected Setup : Enabled/Configured
Guest Zone Wireless Radio : Disabled
Guest Zone Network Name (SSID) : dlink-guest
Guest Zone Security : Disabled

WIRELESS LAN (5 GHz)

MAC Address : c0:a0:bb:1e:b0:ee
Network Name (SSID) : dlink-B0EC-5GHz
Channel : 40
Security Mode : WPA/WPA2-PSK
Wi-Fi Protected Setup : Enabled/Configured
Guest Zone Wireless Radio : Disabled
Guest Zone Network Name (SSID) : dlink-5GHz-guest
Guest Zone Security : Disabled

Helpful Hints...

- All of your LAN, Internet and WIRELESS 802.11 N connection details are displayed here.

Logs

The DAP-1650 keeps a running log of events and activities occurring on the access point. When the device is rebooted, the logs will automatically be cleared.

Log Type: Select what type of event you would like to be logged: **System Activity, Debug Information, Attacks, Dropped Packets,** and **Notice**. Click **Apply Log Settings Now** to update the log options.

First Page: This button directs you to the first page of the log.

Last Page: This button directs you to the last page of the log.

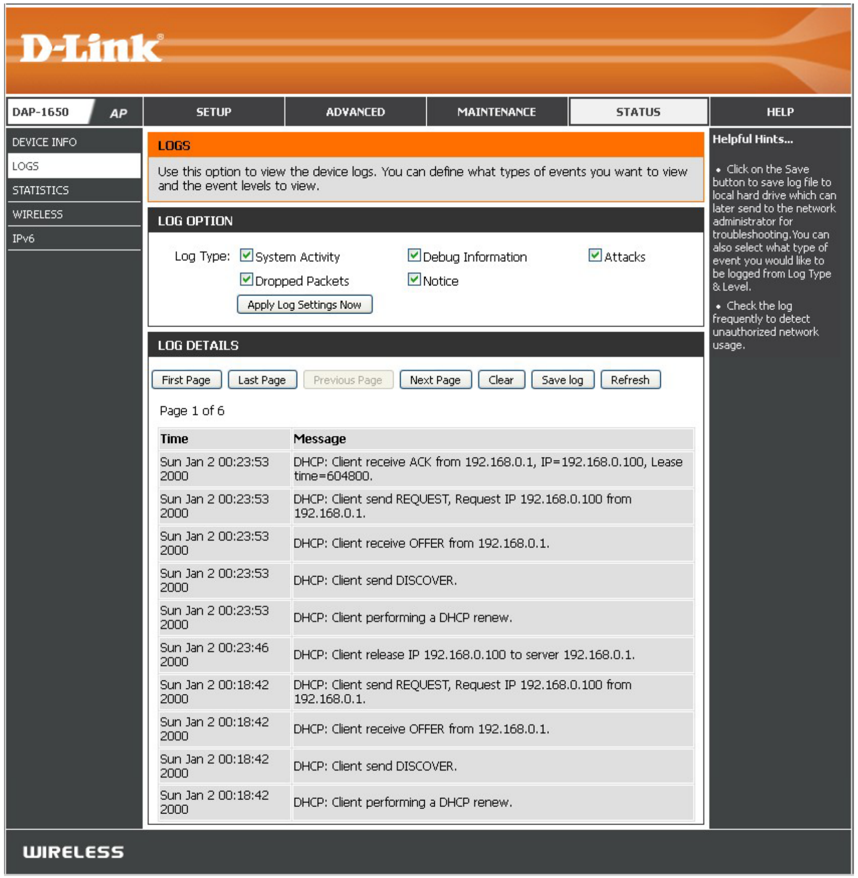
Previous Page: This button directs you to the previous page of the log.

Next Page: This button directs you to the next page of the log.

Clear Log: This button clears all current log content.

Save Log: This button allows you to save the current log to a file on the local hard drive of your computer.

Refresh: This button refreshes the log.



LOGS

Use this option to view the device logs. You can define what types of events you want to view and the event levels to view.

LOG OPTION

Log Type: ☑ System Activity ☑ Debug Information ☑ Attacks ☑ Dropped Packets ☑ Notice

Apply Log Settings Now

LOG DETAILS

First Page | Last Page | Previous Page | Next Page | Clear | Save log | Refresh

Page 1 of 6

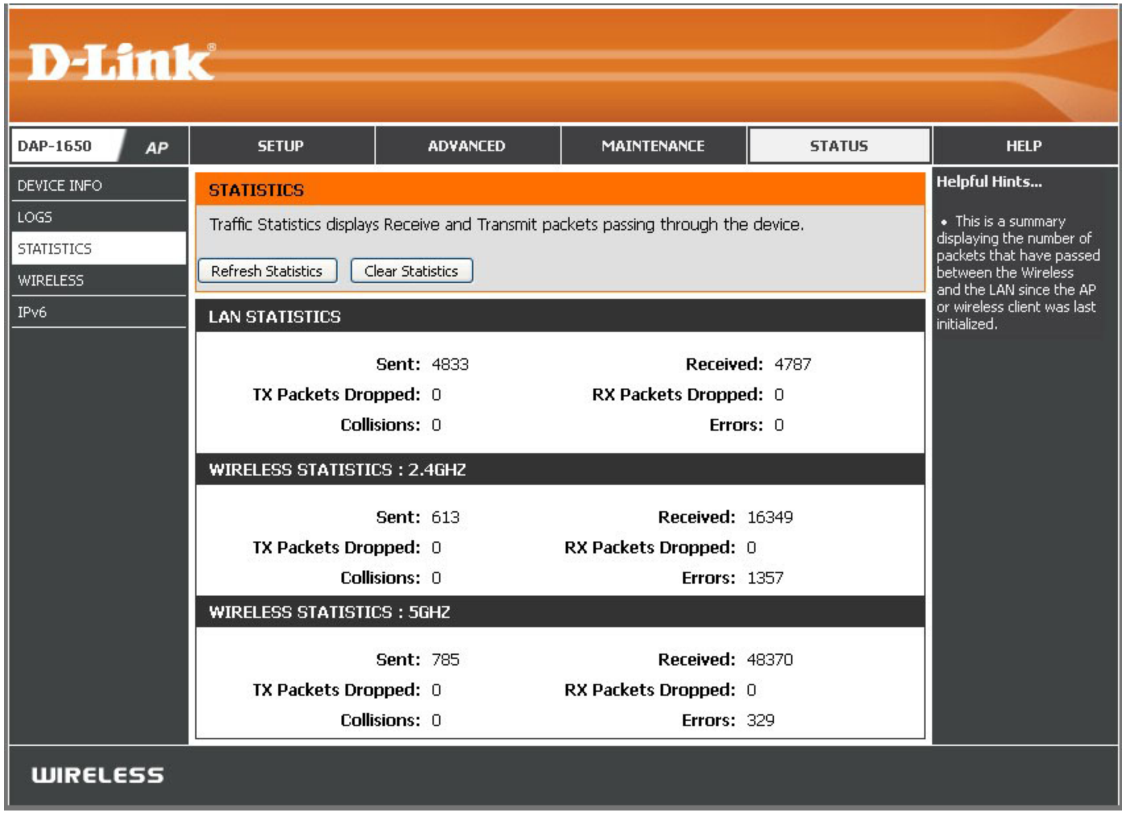
Time	Message
Sun Jan 2 00:23:53 2000	DHCP: Client receive ACK from 192.168.0.1, IP=192.168.0.100, Lease time=604800.
Sun Jan 2 00:23:53 2000	DHCP: Client send REQUEST, Request IP 192.168.0.100 from 192.168.0.1.
Sun Jan 2 00:23:53 2000	DHCP: Client receive OFFER from 192.168.0.1.
Sun Jan 2 00:23:53 2000	DHCP: Client send DISCOVER.
Sun Jan 2 00:23:53 2000	DHCP: Client performing a DHCP renew.
Sun Jan 2 00:23:46 2000	DHCP: Client release IP 192.168.0.100 to server 192.168.0.1.
Sun Jan 2 00:18:42 2000	DHCP: Client send REQUEST, Request IP 192.168.0.100 from 192.168.0.1.
Sun Jan 2 00:18:42 2000	DHCP: Client receive OFFER from 192.168.0.1.
Sun Jan 2 00:18:42 2000	DHCP: Client send DISCOVER.
Sun Jan 2 00:18:42 2000	DHCP: Client performing a DHCP renew.

Helpful Hints...

- Click on the Save button to save log file to local hard drive which can later send to the network administrator for troubleshooting.You can also select what type of event you would like to be logged from Log Type & Level.
- Check the log frequently to detect unauthorized network usage.

Statistics

The DAP-1650 keeps statistics for the traffic that passes through it. You can view the number of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the device is rebooted. Use the buttons at the top of the page to **Refresh** or **Clear** the statistics.



STATISTICS

Traffic Statistics displays Receive and Transmit packets passing through the device.

LAN STATISTICS

Sent:	4833	Received:	4787
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	0

WIRELESS STATISTICS : 2.4GHZ

Sent:	613	Received:	16349
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	1357

WIRELESS STATISTICS : 5GHZ

Sent:	785	Received:	48370
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	329

Helpful Hints...

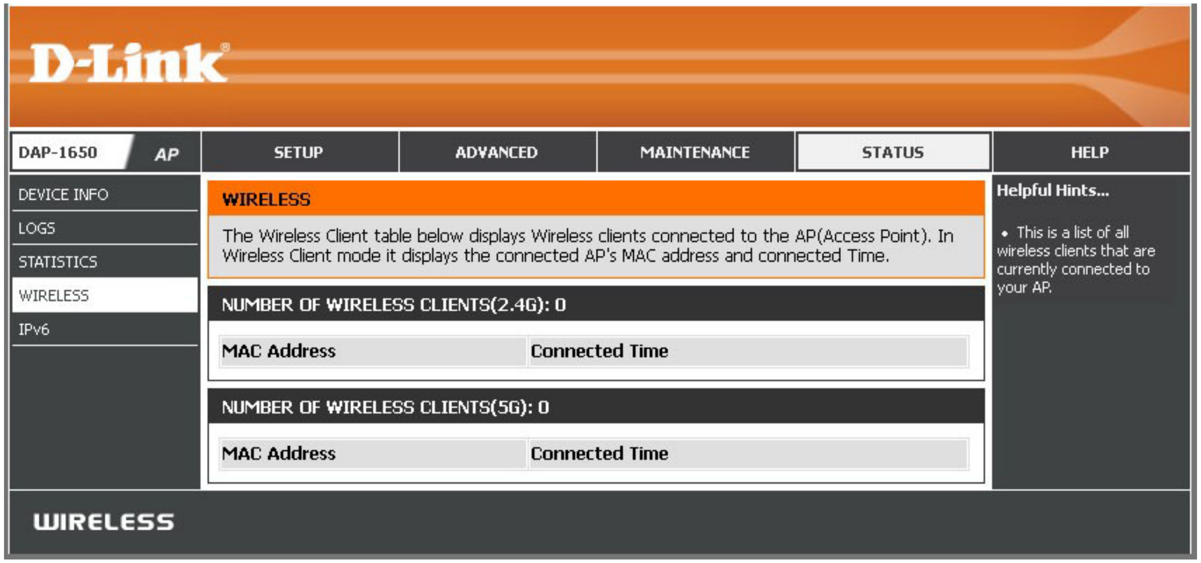
- This is a summary displaying the number of packets that have passed between the Wireless and the LAN since the AP or wireless client was last initialized.

Wireless

The wireless section allows you to view the details for the wireless clients that are connected to your access point.

MAC Address: Displays the Ethernet ID (*MAC Address*) of the wireless client.

Connected Time: Displays the amount of time the wireless client has been connected to the access point.



WIRELESS

The Wireless Client table below displays Wireless clients connected to the AP(Access Point). In Wireless Client mode it displays the connected AP's MAC address and connected Time.

NUMBER OF WIRELESS CLIENTS(2.4G): 0

MAC Address	Connected Time

NUMBER OF WIRELESS CLIENTS(5G): 0

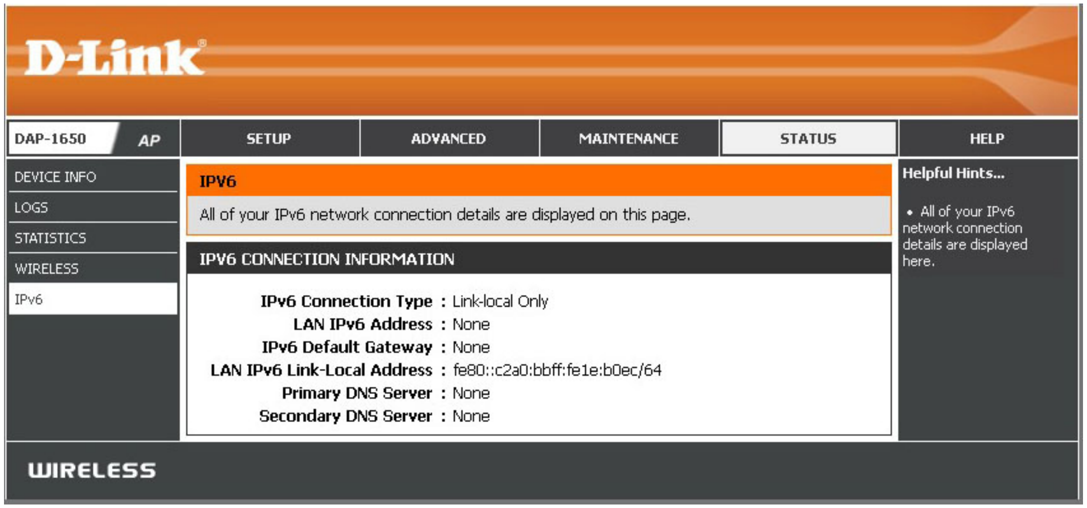
MAC Address	Connected Time

Helpful Hints...

- This is a list of all wireless clients that are currently connected to your AP.

IPv6

The IPv6 section displays a summary of the current IPv6 configuration.



IPV6

All of your IPv6 network connection details are displayed on this page.

IPV6 CONNECTION INFORMATION

```
      IPv6 Connection Type : Link-local Only
          LAN IPv6 Address : None
      IPv6 Default Gateway : None
LAN IPv6 Link-Local Address : fe80::c2a0:bbff:fe1e:b0ec/64
        Primary DNS Server : None
      Secondary DNS Server : None
```

Helpful Hints...

- All of your IPv6 network connection details are displayed here.

IPv6 Connection Type: Displays the DAP-1650's currently configured *IPv6 Connection Type*.

LAN IPv6 Address: If configured, this field displays the current *IPv6 Address* of the device.

IPv6 Default Gateway: If configured, this field will display the details of the default IPv6 gateway.

LAN IPv6 Link-Local Address: Displays the device's local IPv6 address.

Primary DNS Server: If configured this field will display the details of the primary IPv6 DNS server address to be used.

Secondary DNS Server: If configured this field will display the details of the secondary IPv6 DNS server address to be used.

Extender Mode

Device Info

This screen displays the current information for the DAP-1650, such as LAN and wireless LAN details.

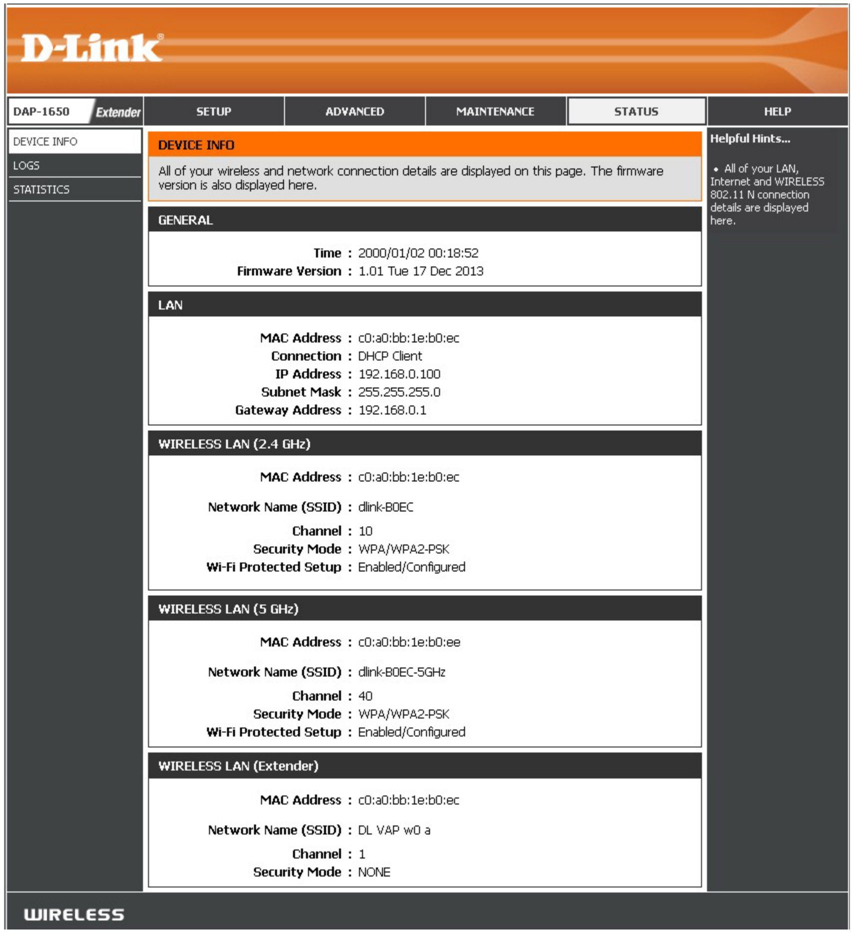
General: Displays the DAP-1650's *Time* and *Firmware Version*.

LAN: Displays the *MAC Address* and the private (local) IP settings for the extender.

Wireless LAN (2.4GHz): Displays the wireless *MAC Address* and wireless settings such as SSID and *Channel* for the 2.4GHz wireless band.

Wireless LAN (5GHz): Displays the wireless *MAC Address* and wireless settings such as SSID and *Channel* for the 5GHz wireless band.

Wireless LAN (Extender): Displays connection details.



DEVICE INFO

All of your wireless and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : 2000/01/02 00:18:52
Firmware Version : 1.01 Tue 17 Dec 2013

LAN

MAC Address : c0:a0:bb:1e:b0:ec
Connection : DHCP Client
IP Address : 192.168.0.100
Subnet Mask : 255.255.255.0
Gateway Address : 192.168.0.1

WIRELESS LAN (2.4 GHz)

MAC Address : c0:a0:bb:1e:b0:ec
Network Name (SSID) : dlink-B0EC
Channel : 10
Security Mode : WPA/WPA2-PSK
Wi-Fi Protected Setup : Enabled/Configured

WIRELESS LAN (5 GHz)

MAC Address : c0:a0:bb:1e:b0:ee
Network Name (SSID) : dlink-B0EC-5GHz
Channel : 40
Security Mode : WPA/WPA2-PSK
Wi-Fi Protected Setup : Enabled/Configured

WIRELESS LAN (Extender)

MAC Address : c0:a0:bb:1e:b0:ec
Network Name (SSID) : DL VAP w0 a
Channel : 1
Security Mode : NONE

Helpful Hints...

- All of your LAN, Internet and WIRELESS 802.11 N connection details are displayed here.

Logs

The DAP-1650 keeps a running log of events and activities occurring on the extender. When the device is rebooted, the logs will automatically be cleared.

Log Type: Select what type of event you would like to be logged: **System Activity, Debug Information, Attacks, Dropped Packets,** and **Notice**. Click **Apply Log Settings Now** to update the log options.

First Page: This button directs you to the first page of the log.

Last Page: This button directs you to the last page of the log.

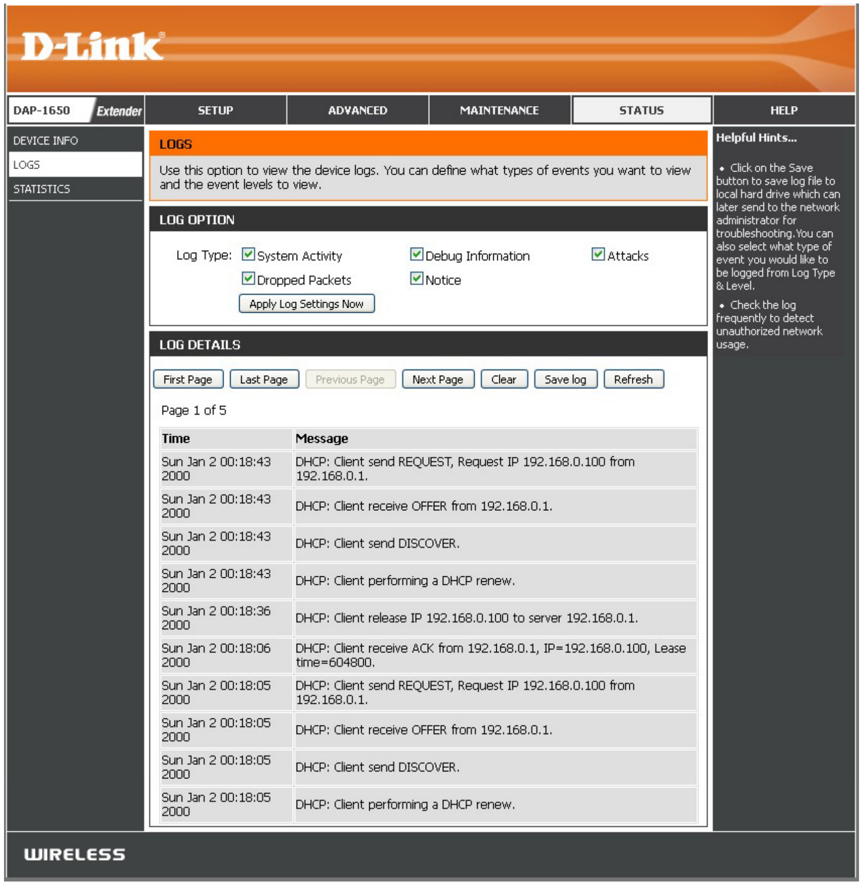
Previous Page: This button directs you to the previous page of the log.

Next Page: This button directs you to the next page of the log.

Clear Log: This button clears all current log content.

Save Log: This button allows you to save the current log to a file on the local hard drive of your computer.

Refresh: This button refreshes the log.



LOGS

Use this option to view the device logs. You can define what types of events you want to view and the event levels to view.

LOG OPTION

Log Type: ☑ System Activity ☑ Debug Information ☑ Attacks ☑ Dropped Packets ☑ Notice

Apply Log Settings Now

LOG DETAILS

First Page | Last Page | Previous Page | Next Page | Clear | Save log | Refresh

Page 1 of 5

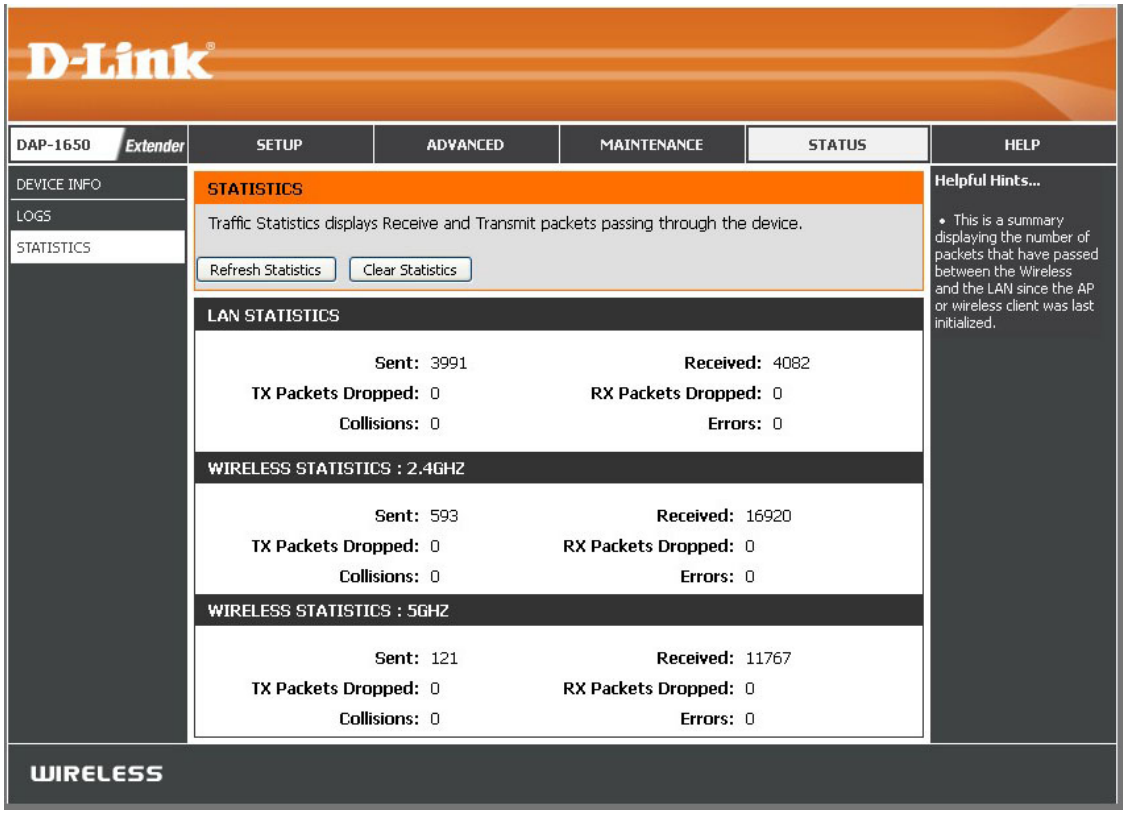
Time	Message
Sun Jan 2 00:18:43 2000	DHCP: Client send REQUEST, Request IP 192.168.0.100 from 192.168.0.1.
Sun Jan 2 00:18:43 2000	DHCP: Client receive OFFER from 192.168.0.1.
Sun Jan 2 00:18:43 2000	DHCP: Client send DISCOVER.
Sun Jan 2 00:18:43 2000	DHCP: Client performing a DHCP renew.
Sun Jan 2 00:18:36 2000	DHCP: Client release IP 192.168.0.100 to server 192.168.0.1.
Sun Jan 2 00:18:06 2000	DHCP: Client receive ACK from 192.168.0.1, IP=192.168.0.100, Lease time=604800.
Sun Jan 2 00:18:05 2000	DHCP: Client send REQUEST, Request IP 192.168.0.100 from 192.168.0.1.
Sun Jan 2 00:18:05 2000	DHCP: Client receive OFFER from 192.168.0.1.
Sun Jan 2 00:18:05 2000	DHCP: Client send DISCOVER.
Sun Jan 2 00:18:05 2000	DHCP: Client performing a DHCP renew.

Helpful Hints...

- Click on the Save button to save log file to local hard drive which can later send to the network administrator for troubleshooting. You can also select what type of event you would like to be logged from Log Type & Level.
- Check the log frequently to detect unauthorized network usage.

Statistics

The DAP-1650 keeps statistics for the traffic that passes through it. You can view the number of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the device is rebooted. Use the buttons at the top of the page to **Refresh** or **Clear** the statistics.



STATISTICS

Traffic Statistics displays Receive and Transmit packets passing through the device.

LAN STATISTICS

Sent:	3991	Received:	4082
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	0

WIRELESS STATISTICS : 2.4GHZ

Sent:	593	Received:	16920
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	0

WIRELESS STATISTICS : 5GHZ

Sent:	121	Received:	11767
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	0

Helpful Hints...

- This is a summary displaying the number of packets that have passed between the Wireless and the LAN since the AP or wireless client was last initialized.

Media Bridge Mode

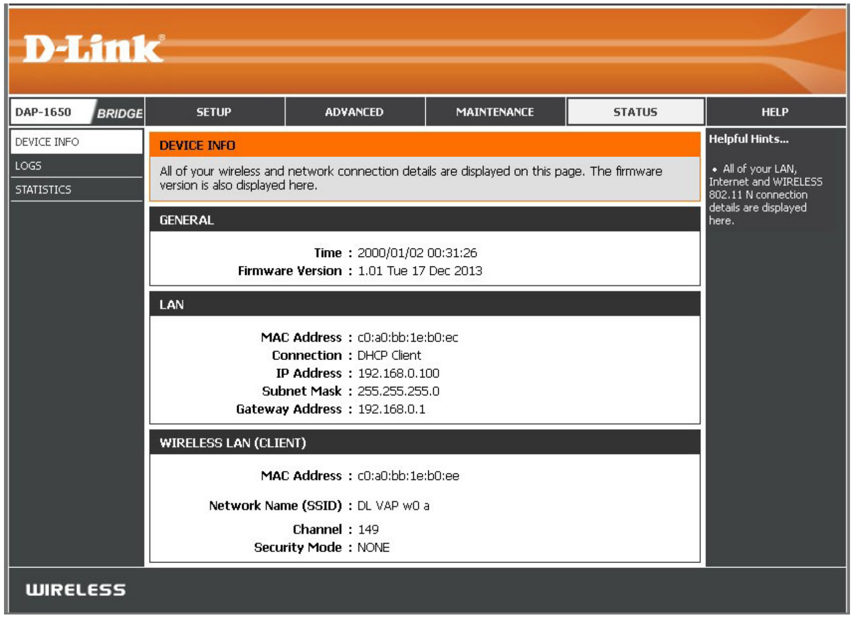
Device Info

This screen displays the current information for the DAP-1650, such as LAN and wireless LAN details.

General: Displays the DAP-1650's *Time* and *Firmware Version*.

LAN: Displays the *MAC Address* and the private (local) IP settings for the device.

Wireless LAN (Client): Displays the wireless *MAC Address* and details for the client.



DEVICE INFO

All of your wireless and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : 2000/01/02 00:31:26
Firmware Version : 1.01 Tue 17 Dec 2013

LAN

MAC Address : c0:a0:bb:1e:b0:ec
Connection : DHCP Client
IP Address : 192.168.0.100
Subnet Mask : 255.255.255.0
Gateway Address : 192.168.0.1

WIRELESS LAN (CLIENT)

MAC Address : c0:a0:bb:1e:b0:ee
Network Name (SSID) : DL VAP w0 a
Channel : 149
Security Mode : NONE

Helpful Hints...

- All of your LAN, Internet and WIRELESS 802.11 N connection details are displayed here.

Logs

The DAP-1650 keeps a running log of events and activities occurring on the media bridge. When the device is rebooted, the logs will automatically be cleared.

Log Type: Select what type of event you would like to be logged: **System Activity, Debug Information, Attacks, Dropped Packets,** and **Notice**. Click **Apply Log Settings Now** to update the log options.

First Page: This button directs you to the first page of the log.

Last Page: This button directs you to the last page of the log.

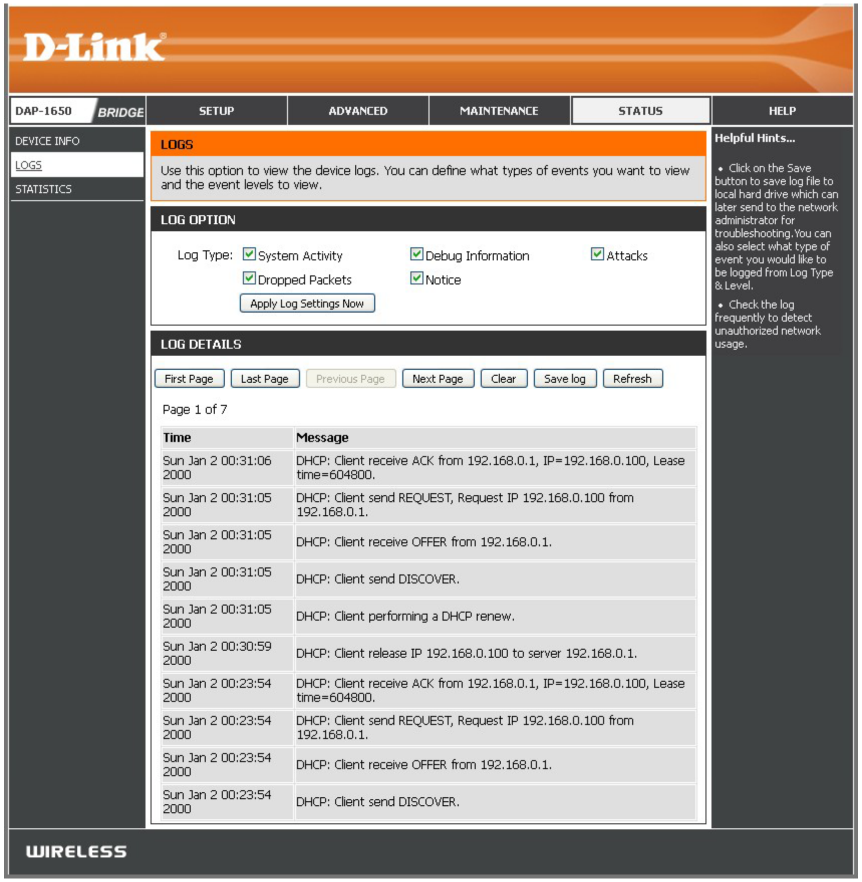
Previous Page: This button directs you to the previous page of the log.

Next Page: This button directs you to the next page of the log.

Clear: This button clears all current log content.

Save Log: This button allows you to save the current log to a file on the local hard drive of your computer.

Refresh: This button refreshes the log.



LOGS

Use this option to view the device logs. You can define what types of events you want to view and the event levels to view.

LOG OPTION

Log Type: ☑ System Activity ☑ Debug Information ☑ Attacks
☑ Dropped Packets ☑ Notice

Apply Log Settings Now

LOG DETAILS

Page 1 of 7

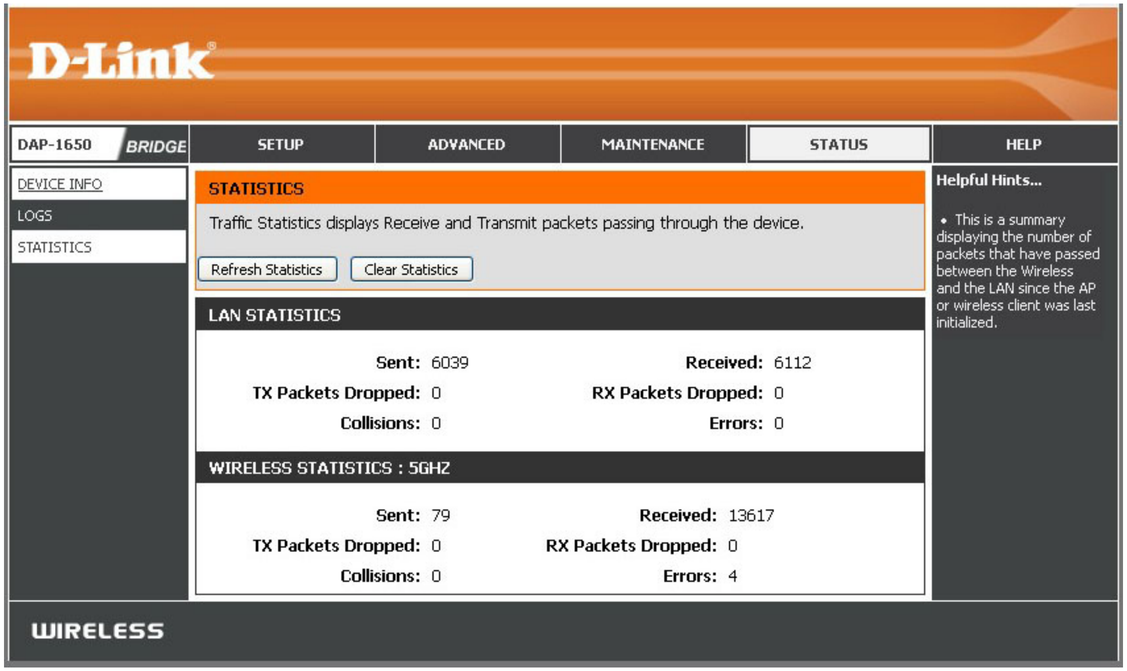
Time	Message
Sun Jan 2 00:31:06 2000	DHCP: Client receive ACK from 192.168.0.1, IP=192.168.0.100, Lease time=604800.
Sun Jan 2 00:31:05 2000	DHCP: Client send REQUEST, Request IP 192.168.0.100 from 192.168.0.1.
Sun Jan 2 00:31:05 2000	DHCP: Client receive OFFER from 192.168.0.1.
Sun Jan 2 00:31:05 2000	DHCP: Client send DISCOVER.
Sun Jan 2 00:31:05 2000	DHCP: Client performing a DHCP renew.
Sun Jan 2 00:30:59 2000	DHCP: Client release IP 192.168.0.100 to server 192.168.0.1.
Sun Jan 2 00:23:54 2000	DHCP: Client receive ACK from 192.168.0.1, IP=192.168.0.100, Lease time=604800.
Sun Jan 2 00:23:54 2000	DHCP: Client send REQUEST, Request IP 192.168.0.100 from 192.168.0.1.
Sun Jan 2 00:23:54 2000	DHCP: Client receive OFFER from 192.168.0.1.
Sun Jan 2 00:23:54 2000	DHCP: Client send DISCOVER.

Helpful Hints...

- Click on the Save button to save log file to local hard drive which can later send to the network administrator for troubleshooting.You can also select what type of event you would like to be logged from Log Type & Level.
- Check the log frequently to detect unauthorized network usage.

Statistics

The DAP-1650 keeps statistics for the traffic that passes through it. You can view the number of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the device is rebooted. Use the buttons at the top of the page to **Refresh** or **Clear** the statistics.



STATISTICS

Traffic Statistics displays Receive and Transmit packets passing through the device.

LAN STATISTICS

Sent:	6039	Received:	6112
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	0

WIRELESS STATISTICS : 5GHZ

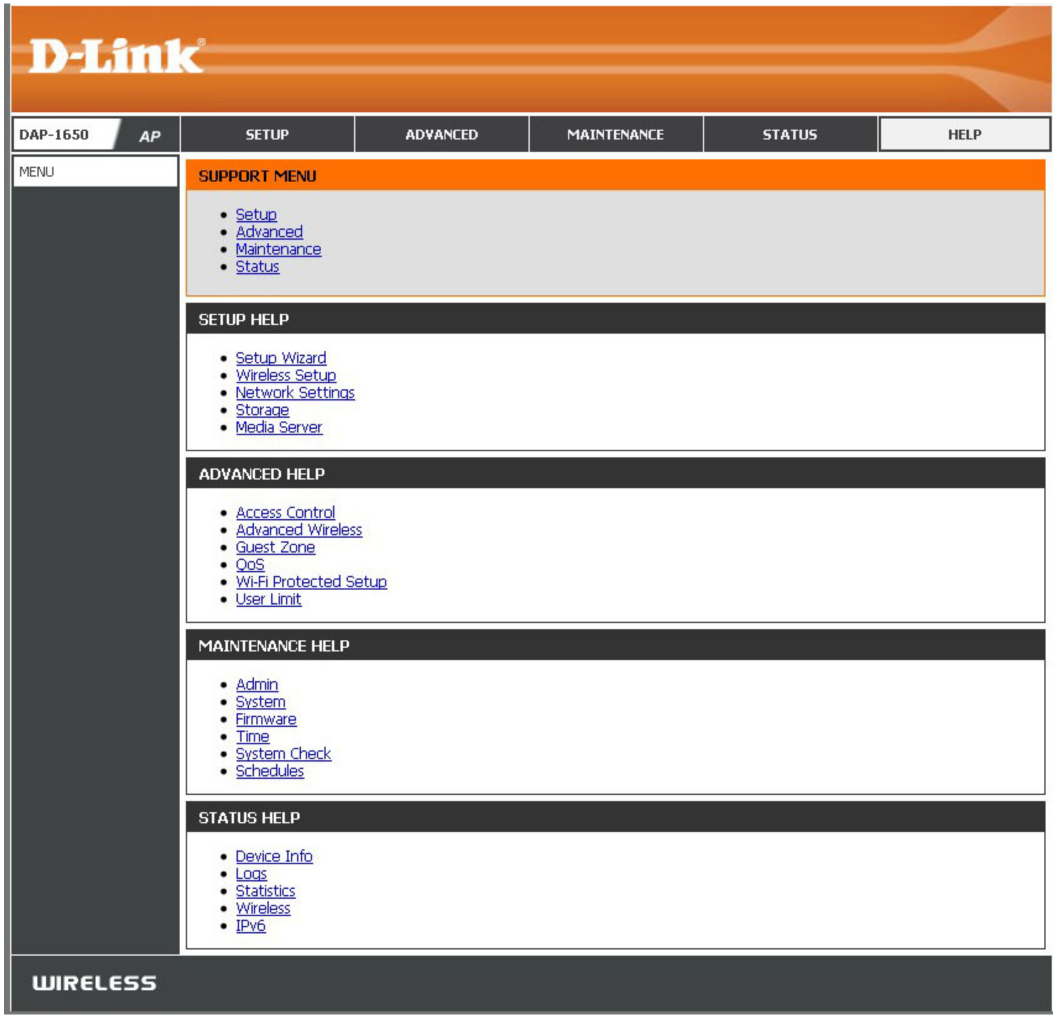
Sent:	79	Received:	13617
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	4

Helpful Hints...

- This is a summary displaying the number of packets that have passed between the Wireless and the LAN since the AP or wireless client was last initialized.

Help

Access Point Mode



SUPPORT MENU

- Setup
- Advanced
- Maintenance
- Status

SETUP HELP

- Setup Wizard
- Wireless Setup
- Network Settings
- Storage
- Media Server

ADVANCED HELP

- Access Control
- Advanced Wireless
- Guest Zone
- QoS
- Wi-Fi Protected Setup
- User Limit

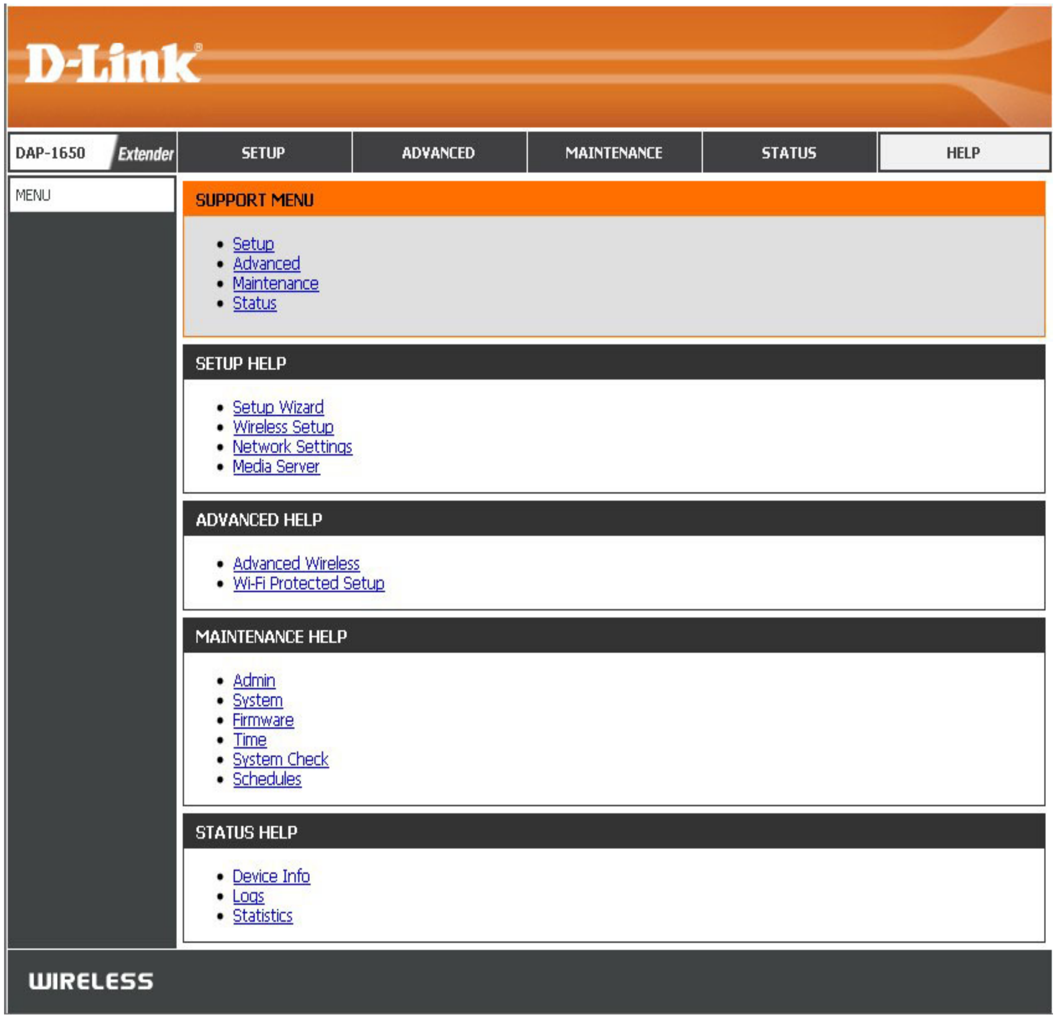
MAINTENANCE HELP

- Admin
- System
- Firmware
- Time
- System Check
- Schedules

STATUS HELP

- Device Info
- Logs
- Statistics
- Wireless
- IPv6

Extender Mode



SUPPORT MENU

- Setup
- Advanced
- Maintenance
- Status

SETUP HELP

- Setup Wizard
- Wireless Setup
- Network Settings
- Media Server

ADVANCED HELP

- Advanced Wireless
- Wi-Fi Protected Setup

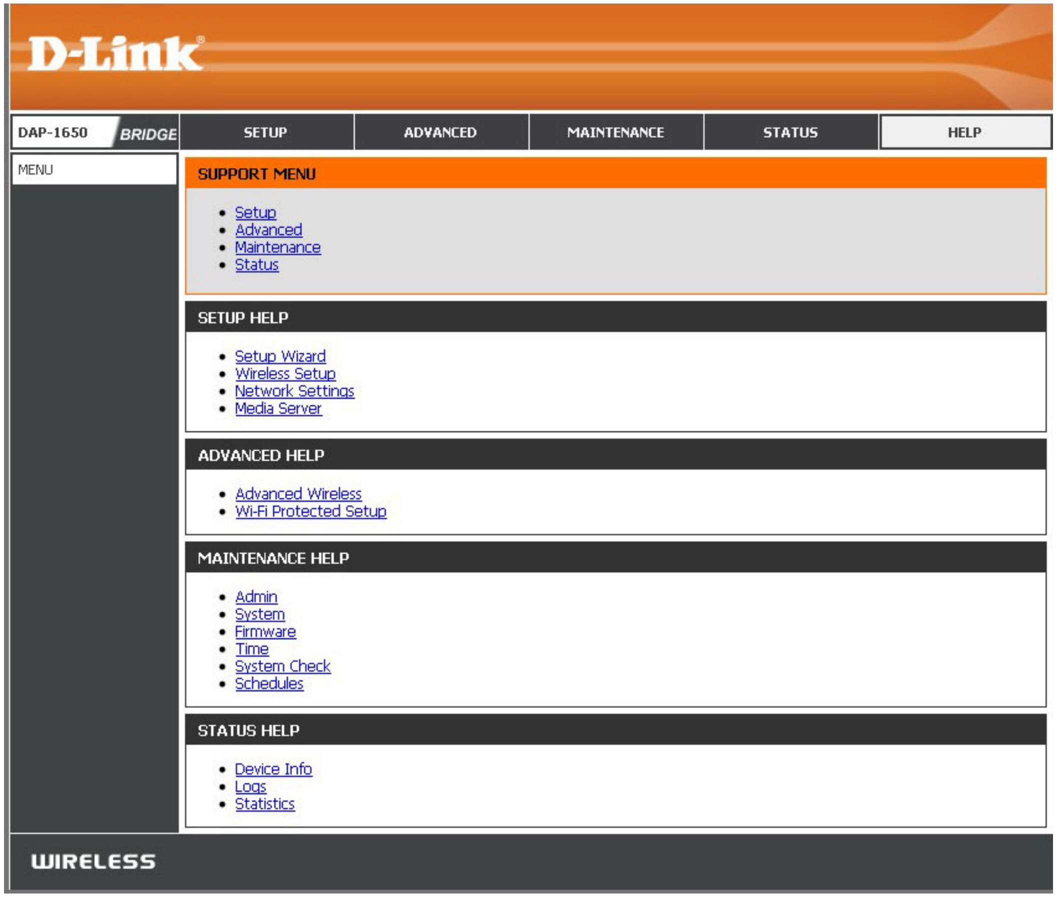
MAINTENANCE HELP

- Admin
- System
- Firmware
- Time
- System Check
- Schedules

STATUS HELP

- Device Info
- Logs
- Statistics

Media Bridge Mode



SUPPORT MENU

- Setup
- Advanced
- Maintenance
- Status

SETUP HELP

- Setup Wizard
- Wireless Setup
- Network Settings
- Media Server

ADVANCED HELP

- Advanced Wireless
- Wi-Fi Protected Setup

MAINTENANCE HELP

- Admin
- System
- Firmware
- Time
- System Check
- Schedules

STATUS HELP

- Device Info
- Logs
- Statistics

Wireless Security

This section will explain the different types of security you can use to protect your wireless network from intruders. Please note that some security methods may not be available for all operation modes. The DAP-1650 offers the following types of security:

- Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA/WPA2)
  - WPA - Personal
  - WPA - Enterprise

What is WPS?

Wi-Fi Protected Setup (WPS) allows you to quickly and easily create a secure wireless connection between devices using a push-button or a PIN code. This method alleviates the need for users to change settings on their wireless devices, or remember security passwords. Many wireless devices have a physical push-button located somewhere on the exterior casing, while others may have a software button located within the device's configuration software. Please refer to your wireless device's documentation for further information on how to connect to the DAP-1650 using WPS.

What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless bridge or access point. WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

WPA/WPA2 has two main security levels; Personal, and Enterprise:

- **WPA/WPA2 - Personal** is sufficient for most home networks and uses a pre-shared key as described above to authenticate users and encrypt data.
- **WPA/WPA2 - Enterprise** is designed for medium-to-large scale networking environments and uses a centralized RADIUS server for authentication. Users must be registered and authorized by the RADIUS server in order to access the wireless network.

Connecting to a Wireless Client

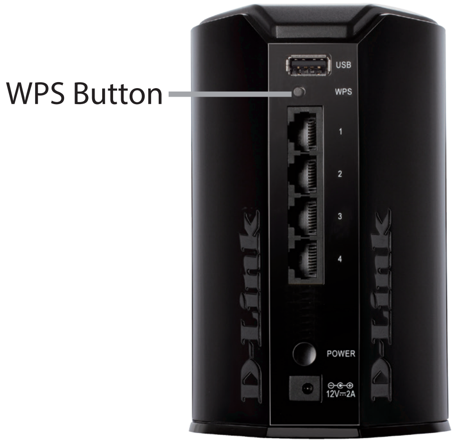
WPS Button

WPS (Wi-Fi Protected Setup) is a simple and secure way to connect your wireless devices with the DAP-1650. Most wireless devices such as wireless routers, media players, printers, and cameras will have a WPS button (or a software utility with WPS). Refer to the user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the **WPS** button on the DAP-1650 for a minimum of one second. The Power LED on the device will start to blink green.

Step 2 - Within 120 seconds, press the **WPS** button on your wireless device.

Step 3 - Allow up to one minute to connect. When the Power LED stops blinking and the Internet LED turns solid green, you will be connected and your wireless connection will be secured with WPA2.

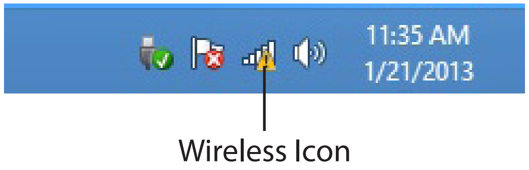


Connect to a Wireless Network

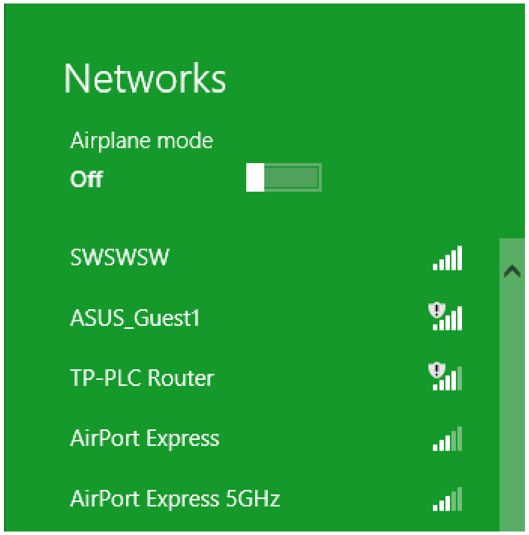
Windows® 8

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

To join an existing network, locate the wireless network icon in the taskbar, next to the time display.

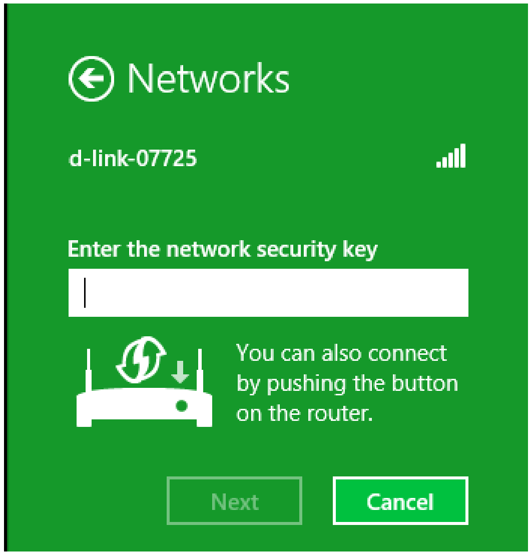


Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.



You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router at this point to enable the WPS function.



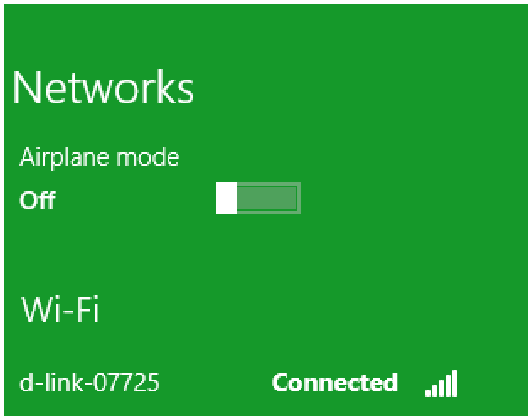
Networks

d-link-07725

Enter the network security key

You can also connect by pushing the button on the router.

When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



Networks

Airplane mode

Off

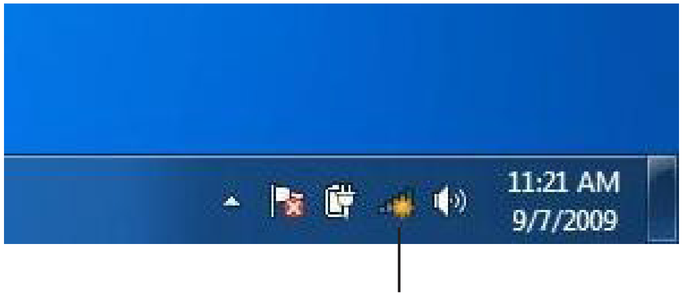
Wi-Fi

d-link-07725 Connected

Windows® 7

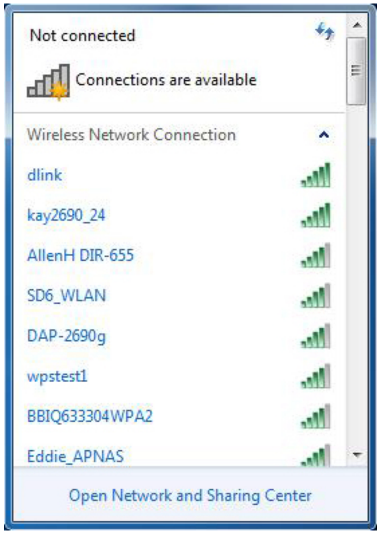
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



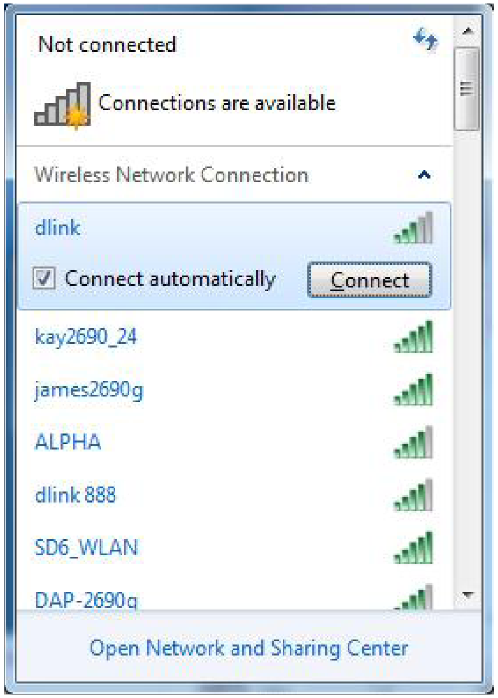
Wireless Icon

2. The utility will display any available wireless networks in your area.

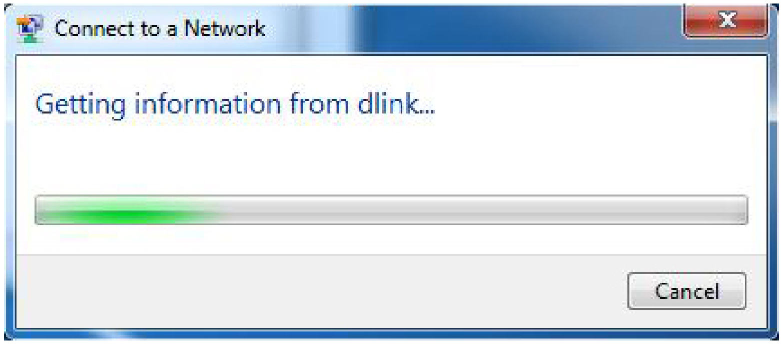


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

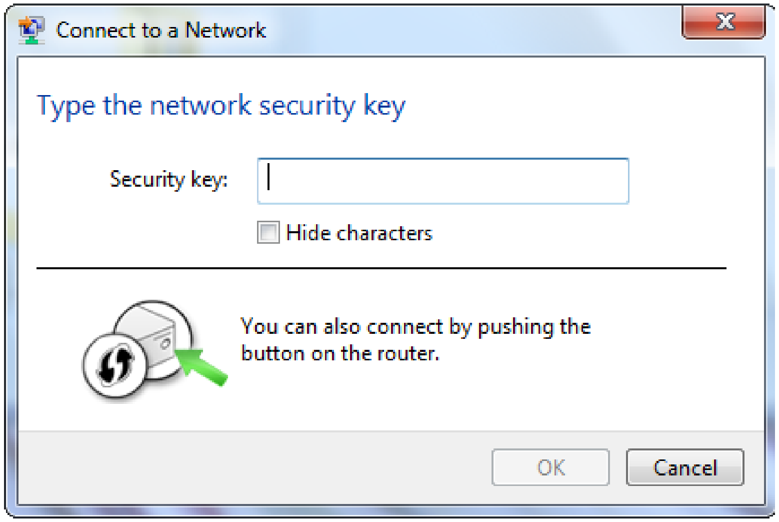


4. The following window appears while your computer tries to connect to the router.



Getting information from dlink...

5. Enter the same security key or passphrase that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.



Security key:

□ Hide characters

You can also connect by pushing the button on the router.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

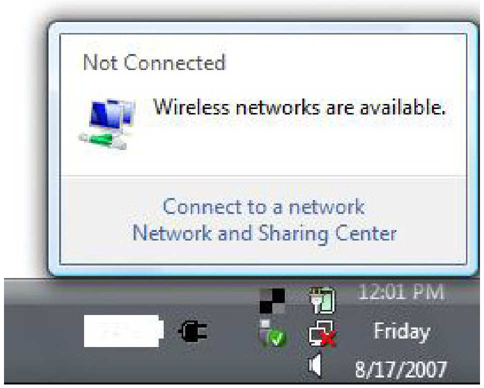
Windows Vista®

Windows Vista users may use the built-in wireless utility. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.

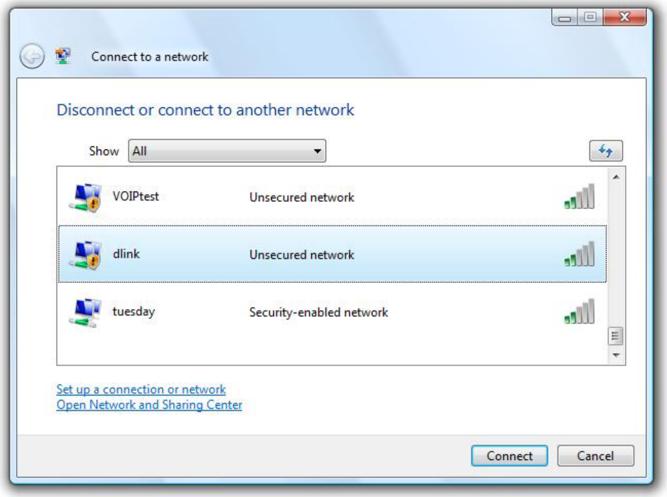


Not Connected

Wireless networks are available.

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings of your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



Connect to a network

Disconnect or connect to another network

Show: All

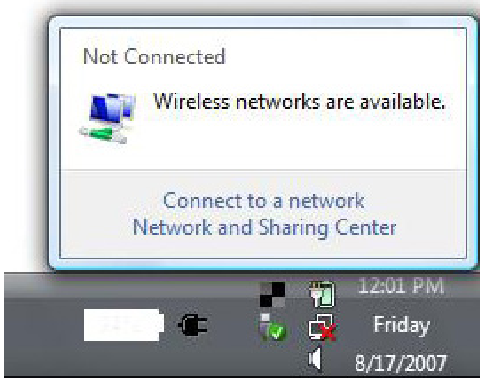
VOIPtest	Unsecured network
dlink	Unsecured network
tuesday	Security-enabled network

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

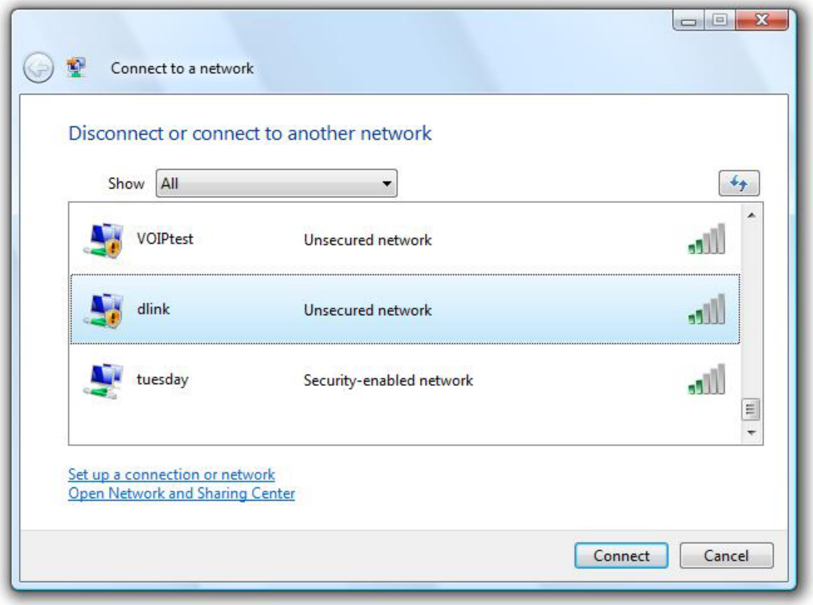
1. Open the Windows Vista Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



Not Connected

Wireless networks are available.

2. Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.



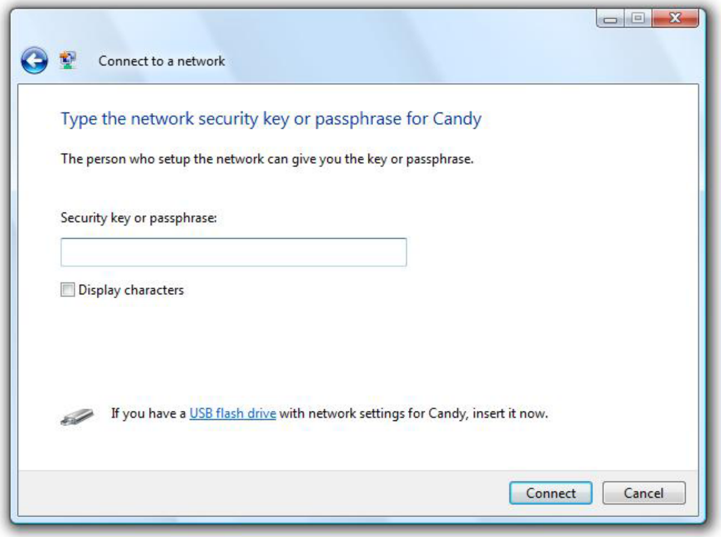
Disconnect or connect to another network

Show All

VOIPtest	Unsecured network
dlink	Unsecured network
tuesday	Security-enabled network

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.



Connect to a network

Type the network security key or passphrase for Candy

The person who setup the network can give you the key or passphrase.

Security key or passphrase:

□ Display characters

If you have a USB flash drive with network settings for Candy, insert it now.

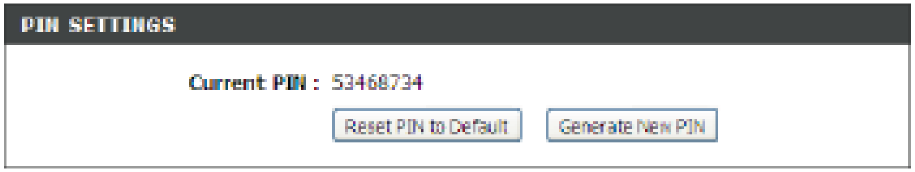
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

WPS/WCN 2.0

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista. The following instructions for setting this up depends on whether you are using Windows Vista to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and unconfigured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista, log into the router and click the **Enable** checkbox in the **Basic** > **Wireless** section. Use the Current PIN that is displayed on the **Advanced** > **Wi-Fi Protected Setup** section or choose to click the **Generate New PIN** button or **Reset PIN to Default** button.



PIN SETTINGS

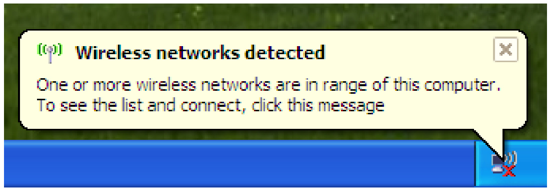
Current PIN : 53468734

If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility).

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

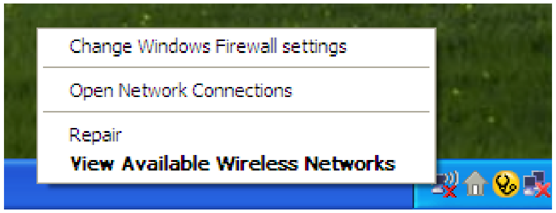


Wireless networks detected

One or more wireless networks are in range of this computer. To see the list and connect, click this message

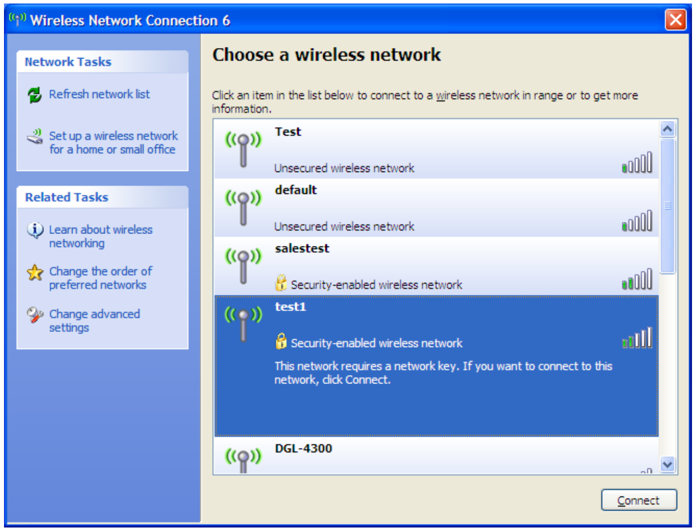
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

If you get a good signal but cannot access the Internet, check the TCP/IP settings of your wireless adapter. Refer to the Networking Basics section in this manual for more information.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

salestest
Security-enabled wireless network

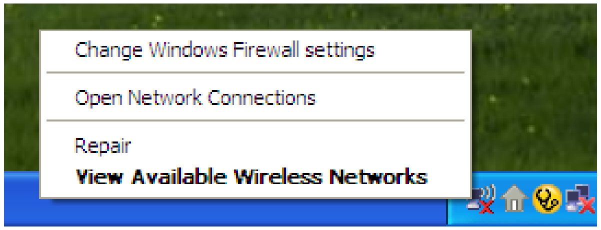
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

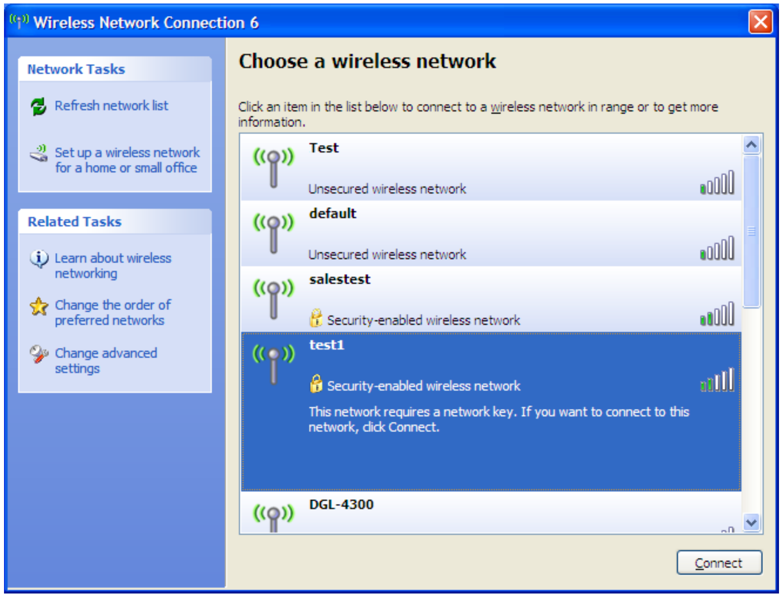
Configure WPA-PSK

It is recommended to enable WEP on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

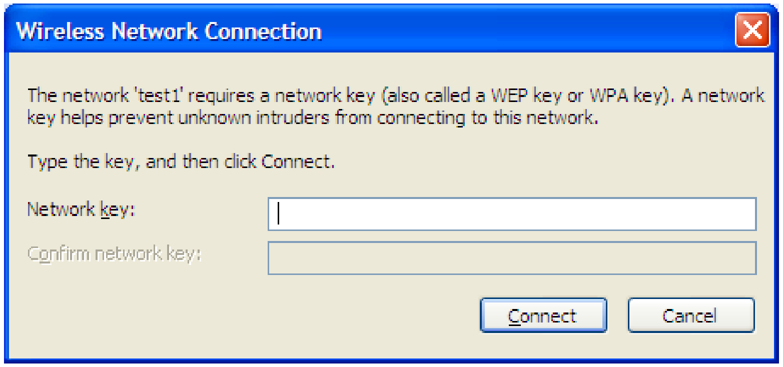
salestest
Security-enabled wireless network

test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.


Wireless Network Connection

The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-1650. Read the following descriptions if you are having problems.

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

When entering the name or IP address of the D-Link access point (**http://dlinkap.local./** 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:
  - Microsoft Internet Explorer® 7.0 or higher
  - Mozilla Firefox® 20.0 or higher
  - Google Chrome™ 20.0 or higher
  - Apple Safari® 5.0 or higher

- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP 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 DAP-1650 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.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your DAP-1650. Unfortunately this process will change all your settings back to the factory default settings.

To reset the device, locate the reset button (hole) on the bottom of the unit. With the device powered on, use a paperclip to hold the button down for about 10 seconds. Release the button and the device will go through its reboot process.

Wait about 30 seconds to access the device. The default address is **http://dlinkap.local./** When logging in, the username is Admin and leave the password field empty.

3. Why can't I connect to certain sites or send and receive emails when connecting through my access point?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

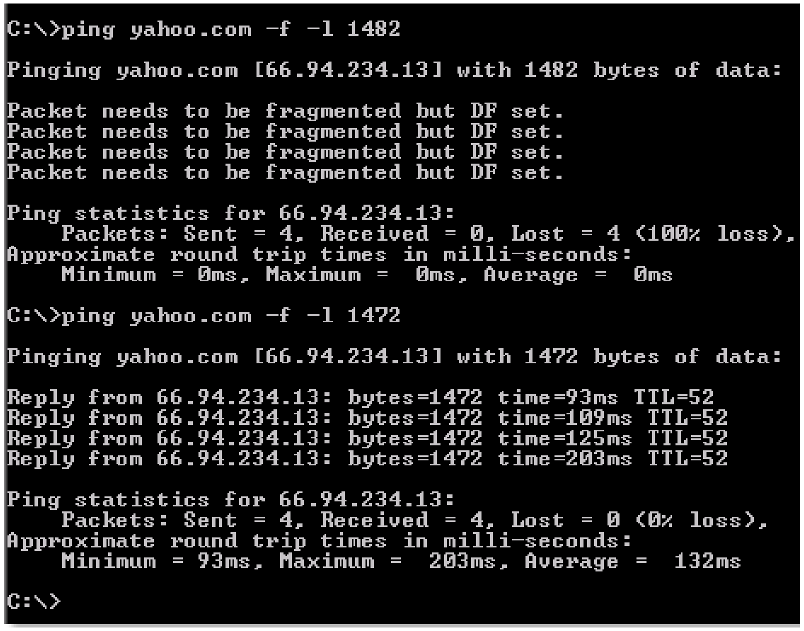
Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and ME users type in *command* (Windows® NT, 2000, and XP users type in cmd) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

  ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**



```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your access point with the proper MTU size.

To change the MTU rate on your access point follow the steps below:

- Open your browser, enter the IP address of your access point (**192.168.0.50**) and click **OK.**
- Enter your username (Admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure.**
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely and conveniently access your network. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapters used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A wireless router is a device used to provide this link.

Networking Basics

Check your IP address

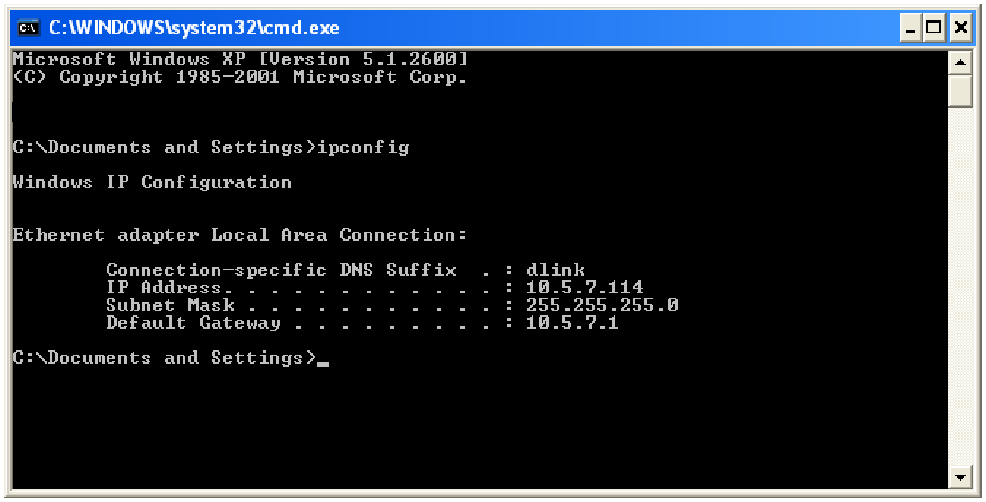
After you install your adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on Start > Run. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type cmd in the Start Search box.)

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.



```
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>_
```

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® 7 - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change Adapter Setting.**

Windows Vista® - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections.**

Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2

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

Step 3

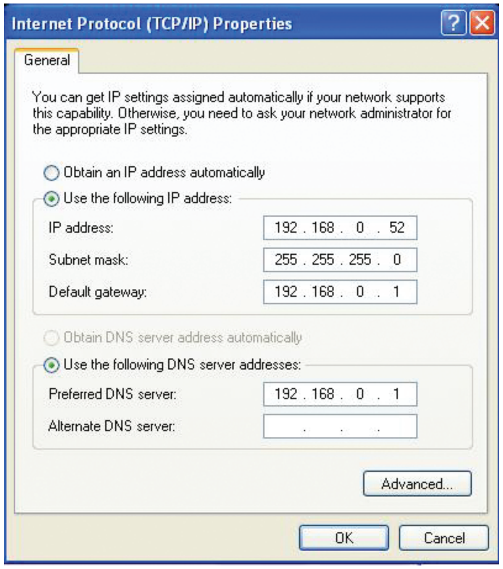
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

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.



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

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 52
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server: . . .

Step 5

Click **OK** twice to save your settings.

Technical Specifications

General		
Device Interfaces	• 802.11 a/b/g/n/ac wireless LAN • Four 10/100/1000 Gigabit LAN ports	• USB 2.0 port
Antenna Type	• 2x2 (2.4 GHz) and 2x2 (5 GHz) internal antennas	
Standards	• IEEE 802.11ac (draft) • IEEE 802.11n • IEEE 802.11g • IEEE 802.11b	• IEEE 802.11a • IEEE 802.3 • IEEE 802.3u
Minimum System Requirements	• Windows® 8/7/Vista®/XP (SP3), or Mac OS® X (10.5 or higher) • Microsoft Internet Explorer 7 or higher, Firefox 12 or higher, or other Java-enabled browser	• CD-ROM • Ethernet network interface
Functionality		
Advanced Features	• Guest zone • Web file access • Multi-language web setup wizard • Green Ethernet	• DLNA media server support • QoS • MAC address filter
Mobile App Support	• SharePort Mobile	• QRS Mobile
Wireless Security	• WPA & WPA2 (Wi-Fi Protected Access)	• Wi-Fi Protected Setup (WPS) PIN/PBC

Physical		
Dimensions	• 3.7 x 4.6 x 5.76 inches (93 x 116 x 145 mm)	
Weight	• 0.73lbs (330 grams)	
Power	• Input: 100 to 240V AC, 50/60 Hz	• Output: 12V DC, 2 A
Temperature	• Operating: 32 to 104 °F (0 to 40 °C)	• Storage: -4 to 149 °F (-20 to 65 °C)
Humidity	• Operating: 0% to 90% non-condensing	• Storage: 5% to 95% non-condensing
Certifications	• FCC Class B • CE Class B • C-Tick • DLNA • IPv6 Ready	• Wi-Fi Certified • Wi-Fi Protected Setup (WPS) • Wi-Fi Multimedia (WMM) • Compatible with Windows 8

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

[2] All Maximum transmission power values expressed are for dual-chain mode. Maximum transmission power and included antennas may vary depending on regional regulations.

[3] Range may vary depending on regional regulations.

Contacting Technical Support

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

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

- Model number of the product (e.g. DAP-1650)
- Hardware Revision (located on the label on the device (e.g. rev A1))
- Serial Number (s/n number located on the label on the device).

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

For customers within the United States:

Phone Support:
(877) 453-5465

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(800) 361-5265

Internet Support:
http://support.dlink.ca

GPL Code Statement

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

http://tsd.dlink.com.tw/GPL.asp

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPLsource code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Please direct all inquiries to:
Email: GPLCODE@DLink.com
Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Systems, Inc.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work’s System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and non-commercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.
"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work). You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor’s “contributor version”.

A contributor’s “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor’s essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient’s use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation. If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

Warranty

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

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

Limited Warranty:

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

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

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

Limited Software Warranty:

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

Non-Applicability of Warranty:

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

Submitting A Claim (USA):

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

Submitting A Claim (Canada):

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

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-800-361-5265, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.ca/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

- RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

What Is Not Covered:

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

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

Disclaimer of Other Warranties:

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

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

Limitation of Liability:

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

Governing Law:

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

Trademarks:

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

Copyright Statement:

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

CE Mark Warning:

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

FCC Statement:

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

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

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

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

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

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:
This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

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

Declaration d'exposition aux radiations:
Cet equipement est conforme aux limites d'exposition aux rayonnements IC etablies pour un environnement non controle. Cet equipement doit etre installe et utilise avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Registration

Register your product online at registration.dlink.com

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

Version 1.0
February 28, 2014