D-Link®

Version 1.00

User Manual

Wireless Range Extender N300

DAP-1320

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	October 19, 2012	• Initial release

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

This purpose of this product is to create a constant network connection for your devices. As such, it does not have a standby mode or use a power management mode. If you wish to power down this product, please simply unplug it from the power outlet.

Table of Contents

Package Contents

DAP-1320 Wireless Range Extender N300

Wi-Fi Configuration Card

Quick Installation Guide

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

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n or 802.11g wireless clients
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • Wireless card **Browser Requirements:** • Internet Explorer 7 or later • Firefox 12.0 or later • Safari 4 or later • Google Chrome 20.0 or later **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

TOTAL PERFORMANCE

Combines wireless repeater features and Wireless N300 technology to provide the best wireless performance.

TOTAL COVERAGE

Provides greater wireless signal rates even at farther distances for best-in-class whole home coverage.

ULTIMATE PERFORMANCE

The D-Link Wireless N300 Range Extender (DAP-1320) lets you extend a secure wireless network throughout your home. Connect the DAP-1320 to a router and share your high-speed Internet access with everyone on the network.

TOTAL NETWORK SECURITY

The DAP-1320 supports wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA/WPA2 standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices.

* Maximum wireless signal rate derived from IEEE Standard 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.

Features

- **Faster Wireless Networking** - The DAP-1320 provides a wireless connection of up to 300 Mbps* with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

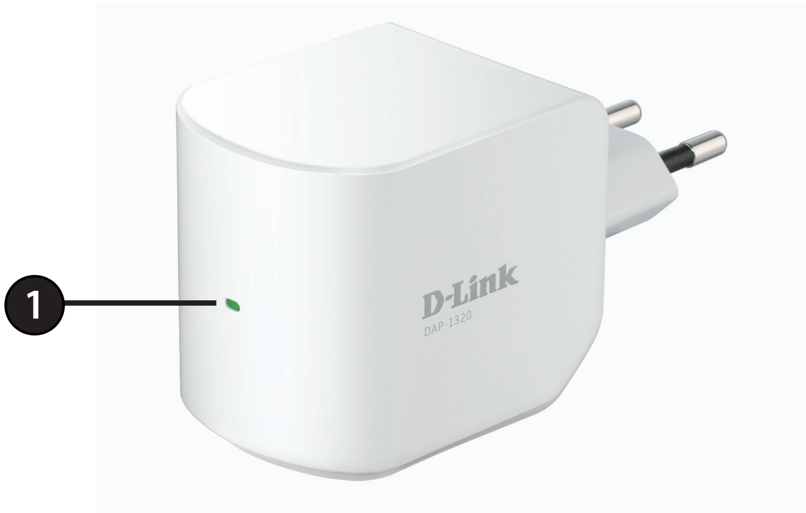
- **Compatible with 802.11g/b Devices** - The DAP-1320 is still fully compatible with the IEEE 802.11g/b standards, so it can connect with existing 802.11g/b devices.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DAP-1320 lets you control what information is accessible to those on the wireless network. Configure your repeater to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 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.

Hardware Overview

Front/Top

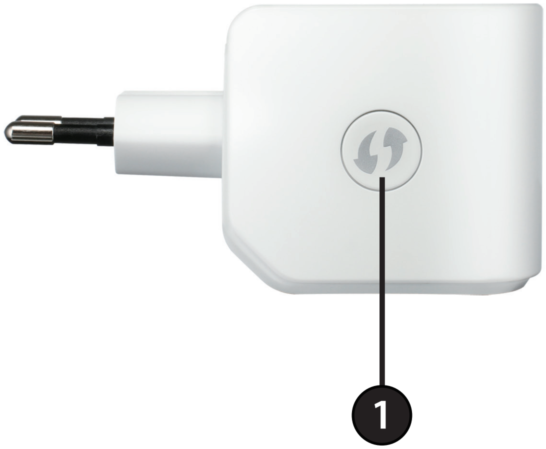


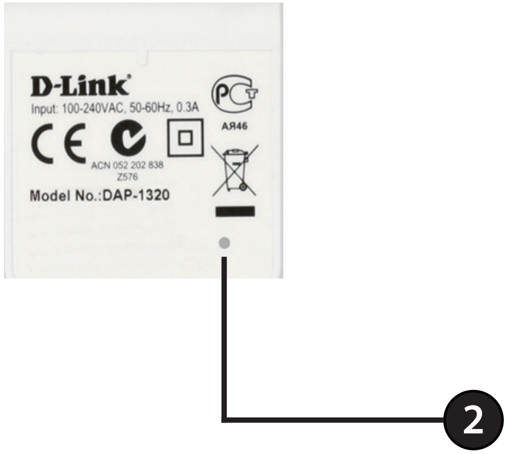
1	LED Indicator	This indicates the current status of the DAP-1320, as detailed in the table below.

LED Indicator	Color	Status	Description
Power/Status	Green	Solid Green	The device is powered ON and operating properly
		Blinking Green	The device is processing WPS
		Light off	The device is powered off
	Red	Solid Red	During the Power ON process or if system is defective
		Blinking Red	The device is under Recovery Mode or the device has malfunctioned
		Light off	The device is powered off
	Orange	Blinking Orange	Cannot connect or provision an IP address from the uplink router
		Light Off	The device is powered off

Hardware Overview

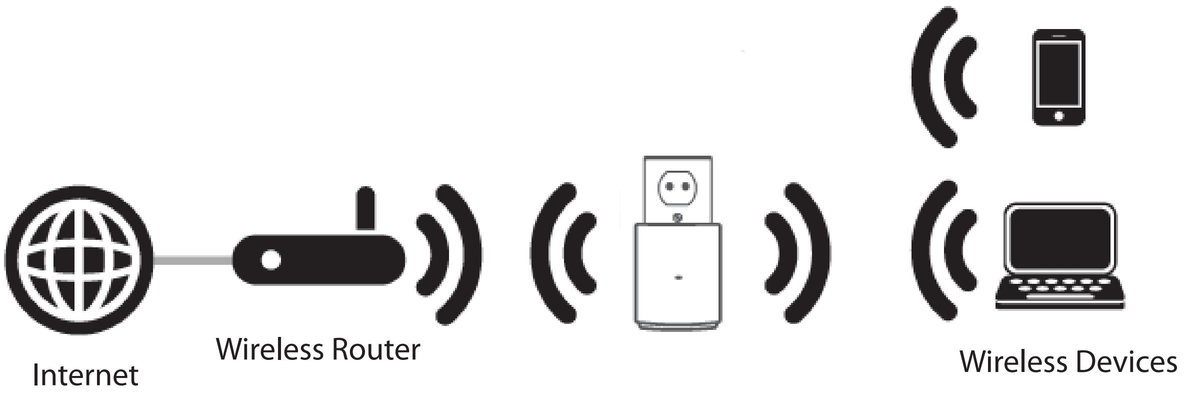
Side and Bottom





1	WPS Button	1. Pressing the WPS button for 5 seconds allows you to set up the DAP-1320 through One-Touch AP Configutation. 2. Pressing the WPS button for 1 second allows you to connect with Wi-Fi clients.
2	Reset Button	Pressing the Reset Button allows you to reset the DAP-1320 to factory default settings.

The DAP-1320 acts as a repeater to extend the range of an existing wireless network to provide better signal for parts of your home or office that may have poor reception.



Wireless Installation Factors

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

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

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

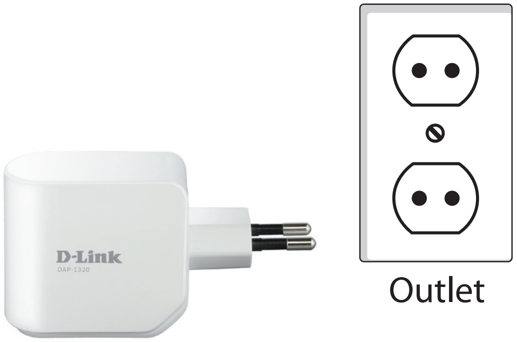
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation,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

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

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

Setting Up Your DAP-1320

1. Take the DAP-1320 and plug it into a power outlet. Verify that the power LED has turned blinking amber before continuing.



There are three ways to configure your DAP-1320 - using the One-Touch AP configuration method, using the QRS Mobile app on your smartphone or tablet device, or using the Web GUI on your computer.

For detailed information on the three methods for configuring your DAP-1320, refer to the following sections of the manual:

- One-Touch AP Configuration on page 10
- Web-based Configuration on page 11
- QRS Mobile App Configuration on page 12

One-Touch AP Configuration

The DAP-1320 supports One-Touch AP configuration using the WPS (Wi-Fi Protected Setup) button to connect to a wireless router to extend the Wi-Fi network in your home, as well as for connecting devices to the DAP-1320's extended wireless network. **Note:** To use One-Touch AP Configuration to connect to a wireless router, please make sure the router features a WPS button.

1. Plug the DAP-1320 into a wall outlet and wait until the power LED is blinking amber.

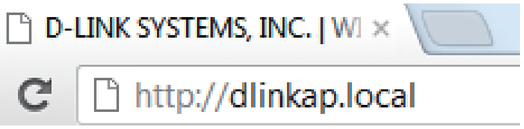
2. Push the WPS button on the wireless Router, and then push and hold the WPS button on the DAP-1320 for about **5 seconds** or until the green LED starts to flash. Please allow up to two minutes for the process to finish.

The LED will become solid green when the DAP-1320 has connected successfully to the wireless router or AP. The DAP-1320 is then ready for you to share a Wi-Fi network with your PCs and mobile devices by using the network name (SSID) and password located on your Wi-Fi Configuration Card.

Note: To connect devices to the DAP-1320, you just push the WPS button on the DAP-1320 for 1 second, then repeat the process on the device. If the connection fails (amber LED still flashes), move your DAP-1320 closer to your wireless router and repeat steps 1 and 2.

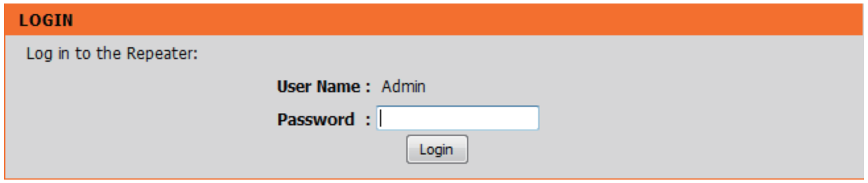
Web-based Configuration

To access the configuration utility for the DAP-1320 on your PC, first connect to the DAP-1320 wirelessly using the network name (SSID) and password located on your Wi-Fi Configuration Card. Then open a web browser and enter **http://dlinkap.local** in the address bar.



Note: If you have multiple DAP-1320 devices on the network, you can access web-based configuration via **http://dlinkapwxyz.local.** as shown in the included Wi-Fi Configuration Card, with "wxyz" being the last four digits of the DAP-1320's MAC address.

Enter your password. By default, Admin is selected as the username and cannot be changed, and by default, the password is blank.



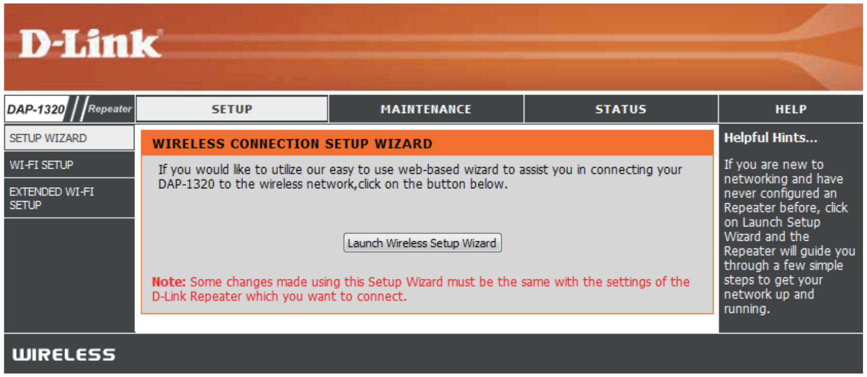
LOGIN

Log in to the Repeater:

User Name : Admin

Password :

The configuration interface will open, and you can configure the different settings of the DAP-1320.



WIRELESS CONNECTION SETUP WIZARD

If you would like to utilize our easy to use web-based wizard to assist you in connecting your DAP-1320 to the wireless network,click on the button below.

Note: Some changes made using this Setup Wizard must be the same with the settings of the D-Link Repeater which you want to connect.

Helpful Hints...

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

For detailed information on setting up your DAP-1320 to extend a network, refer to **Wireless Connection Settings** on page 15.

QRS Mobile App Setup

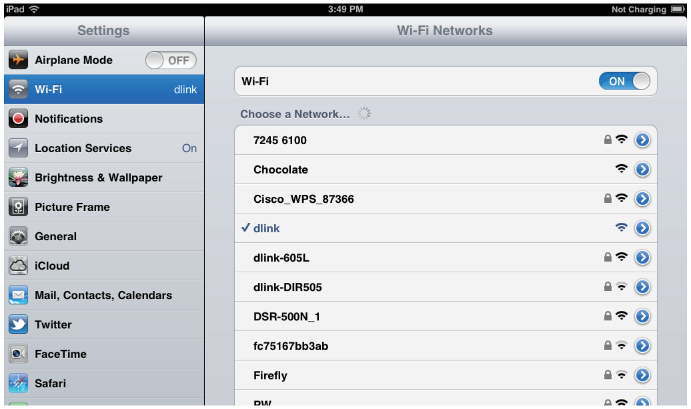
The DAP-1320 can be set up from your iOS or Android smartphone or tablet device using the QRS Mobile app.

1. Use your mobile device to scan a QR code to download the **QRS Mobile** app from the App Store (left) for your iOS device, or from Google Play (right) for your Android device.

For iOS

For Android

2. Connect to the Wi-Fi network that is displayed on the Wi-Fi Configuration Card included in your package (ex: **dlink-a8fa).** Then, enter the Wi-Fi password also printed on the Wi-Fi Configuration Card **(akbdj1936).**



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

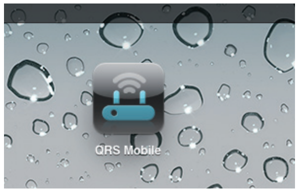
Wi-Fi Networks

Wi-Fi: ON

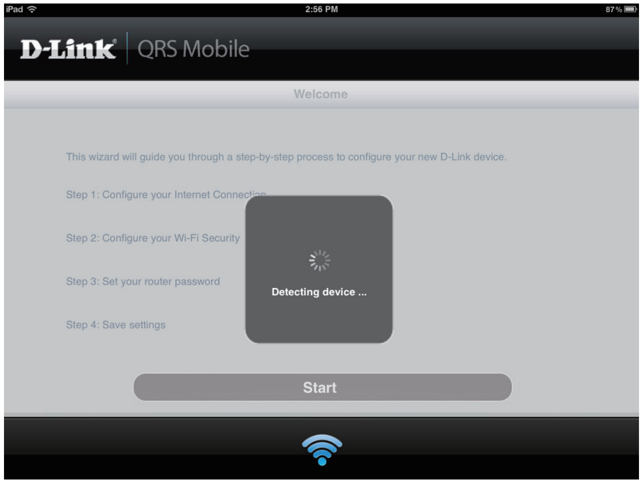
Choose a Network...

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

3. Once your mobile device is connected, tap on the **QRS Mobile** icon.



4. Click **Start** to continue.



This wizard will guide you through a step-by-step process to configure your new D-Link device.

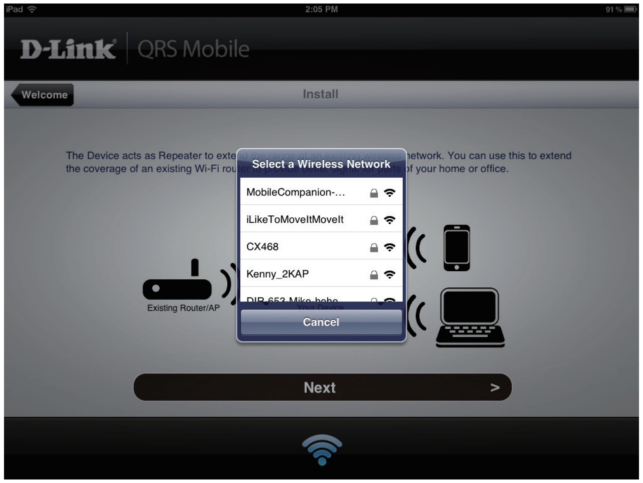
Step 1: Configure your Internet Connection

Step 2: Configure your Wi-Fi Security

Step 3: Set your router password

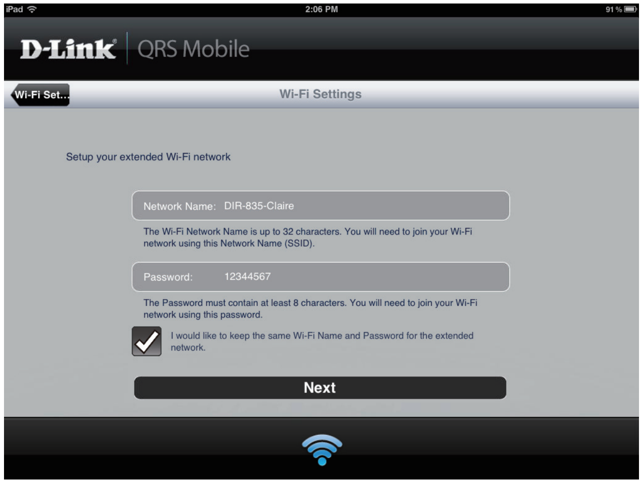
Step 4: Save settings

5. QRS Mobile will first detect your DAP-1320, then scan for available Wi-Fi networks. Select the network you wish to extend and enter the password if required.



The Device acts as Repeater to extend the range of an existing wireless network. You can use this to extend the coverage of an existing Wi-Fi router to provide better signal for parts of your home or office.

6. Enter a network name (SSID) and password for the extended Wi-Fi network. You may keep the existing SSID and password if you wish. Click **Next** to continue.



Setup your extended Wi-Fi network

Network Name: DIR-835-Claire

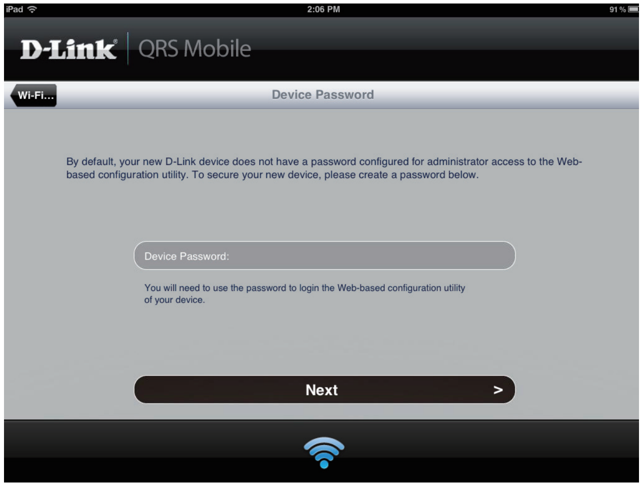
The Wi-Fi Network Name is up to 32 characters. You will need to join your Wi-Fi network using this Network Name (SSID).

Password: 12344567

The Password must contain at least 8 characters. You will need to join your Wi-Fi network using this password.

☑ I would like to keep the same Wi-Fi Name and Password for the extended network.

7. Create an admin password for the DAP-1320's Web-based configuration utility. Click **Next** to continue.

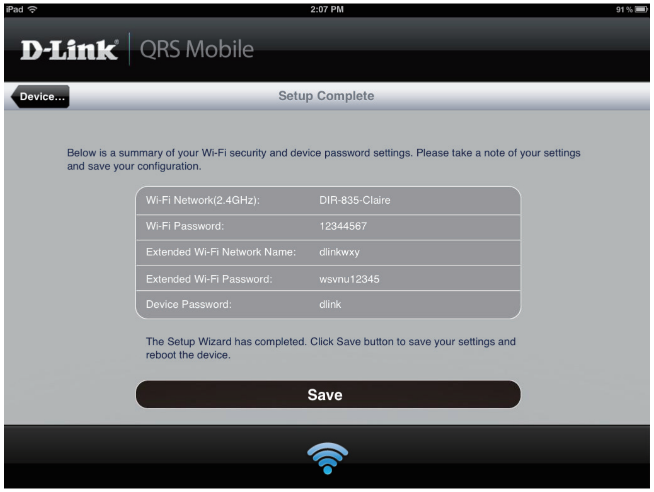


By default, your new D-Link device does not have a password configured for administrator access to the Web-based configuration utility. To secure your new device, please create a password below.

Device Password:

You will need to use the password to login the Web-based configuration utility of your device.

8. A summary of your settings will be displayed. Click **Save** to reboot the device and to complete the setup.



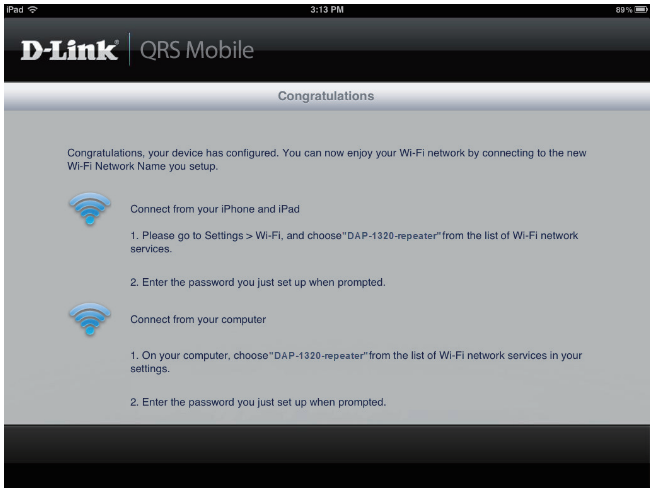
Setup Complete

Below is a summary of your Wi-Fi security and device password settings. Please take a note of your settings and save your configuration.

Wi-Fi Network(2.4GHz):	DIR-835-Claire
Wi-Fi Password:	12344567
Extended Wi-Fi Network Name:	dlinkwxy
Extended Wi-Fi Password:	wsvnu12345
Device Password:	dlink

The Setup Wizard has completed. Click Save button to save your settings and reboot the device.

9. After the Setup Wizard is complete, the following screen will appear. You can now change your mobile device and laptop Wi-Fi settings to the wireless network name and password you just created.



Congratulations

Congratulations, your device has configured. You can now enjoy your Wi-Fi network by connecting to the new Wi-Fi Network Name you setup.

Connect from your iPhone and iPad

1. Please go to Settings > Wi-Fi, and choose"DAP-1320-repeater"from the list of Wi-Fi network services.

2. Enter the password you just set up when prompted.

Connect from your computer

1. On your computer, choose"DAP-1320-repeater"from the list of Wi-Fi network services in your settings.

2. Enter the password you just set up when prompted.

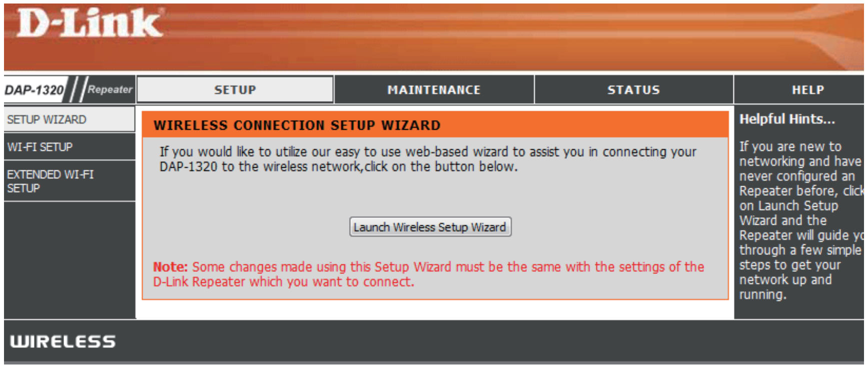
Web-based Configuration

Setup

Setup Wizard

If you want to configure your repeater to connect to the Internet using a setup wizard, click **Launch Wireless Setup Wizard**, and continue to the next step below.

If you already have a Wi-Fi network set up and you want to configure your Wi-Fi network settings manually, go to **Wi-Fi Setup** on the left and refer to "Wi-Fi Setup" on page 21 for more details, or go to **Extended Wi-Fi Setup** and refer to "Extended Wi-Fi Setup" on page 23 for more details.



WIRELESS CONNECTION SETUP WIZARD

If you would like to utilize our easy to use web-based wizard to assist you in connecting your DAP-1320 to the wireless network,click on the button below.

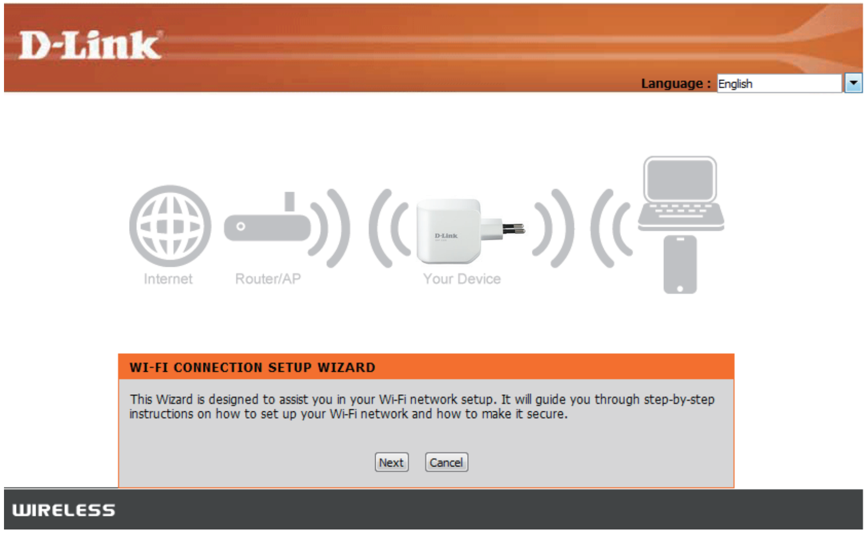
Note: Some changes made using this Setup Wizard must be the same with the settings of the D-Link Repeater which you want to connect.

Helpful Hints...

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

This wizard is designed to guide you through a step-by-step process to configure your new D-Link wireless range extender to extend your wireless network and connect to the Internet.

Click **Next** to continue.

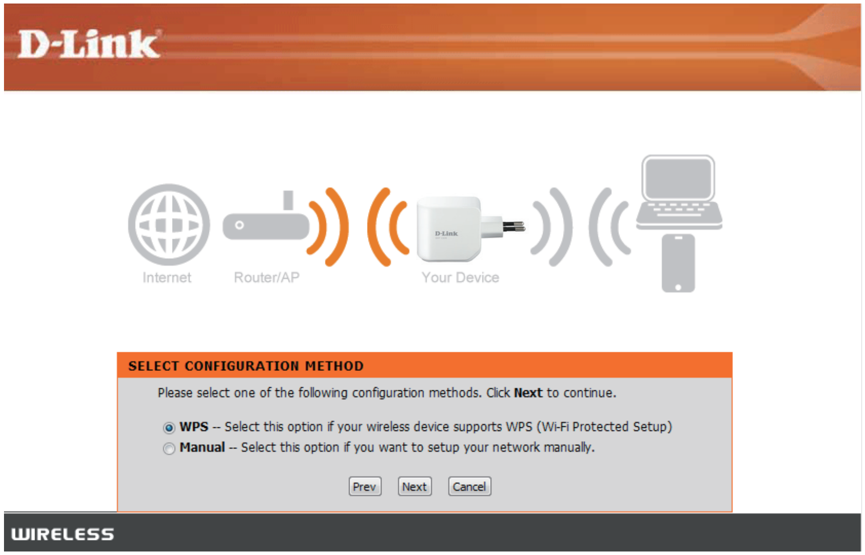


WI-FI CONNECTION SETUP WIZARD

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.

Select whether you want to use the WPS (Wireless Protected Setup) method or the Manual method to set up an extended wireless network using your DAP-1320 and click Next.

These two methods are described in the following sections in the following pages.



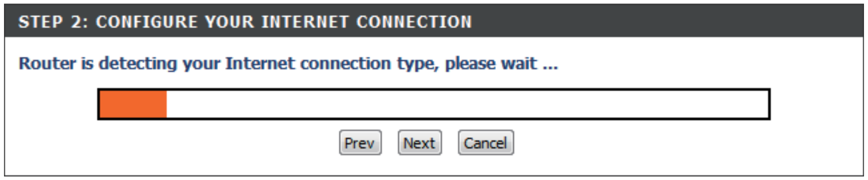
SELECT CONFIGURATION METHOD

Please select one of the following configuration methods. Click **Next** to continue.

● **WPS** -- Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)
○ **Manual** -- Select this option if you want to setup your network manually.

Using the WPS method

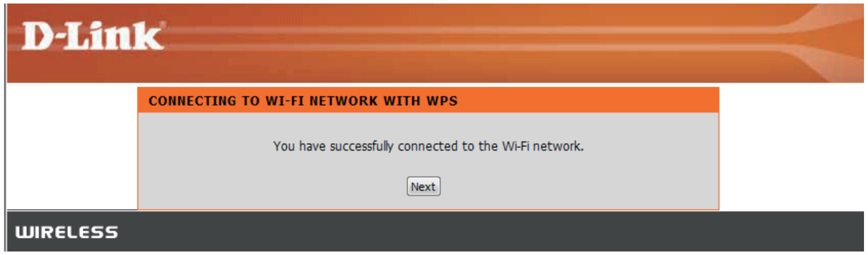
The DAP-1320 uses the Push-button method for WPS. After selecting WPS, the DAP-1320 will ask you to press the WPS Push button on the AP (access point) or router you want to connect to. You have 120 seconds to press the button on your AP or router.



STEP 2: CONFIGURE YOUR INTERNET CONNECTION

Router is detecting your Internet connection type, please wait ...

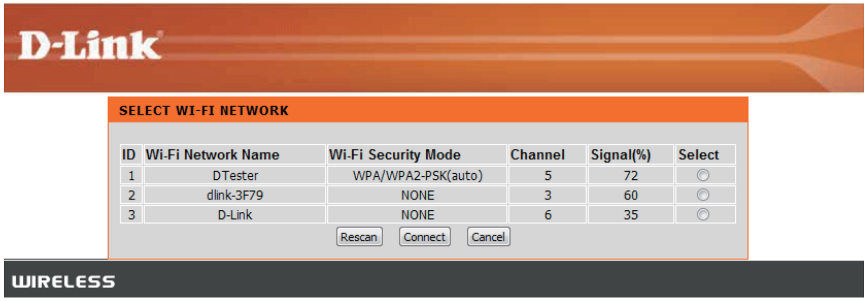
If a connection has been successfully made, you will see a notice on the screen. Click **Next** to continue.



CONNECTING TO WI-FI NETWORK WITH WPS

You have successfully connected to the Wi-Fi network.

The DAP-1320 will first scan for available Wi-Fi networks and list the networks it has found. If the network you would like to connect to isn't listed, click **Rescan** for the DAP-1320 to perform another scan. Select your network and click **Connect**.

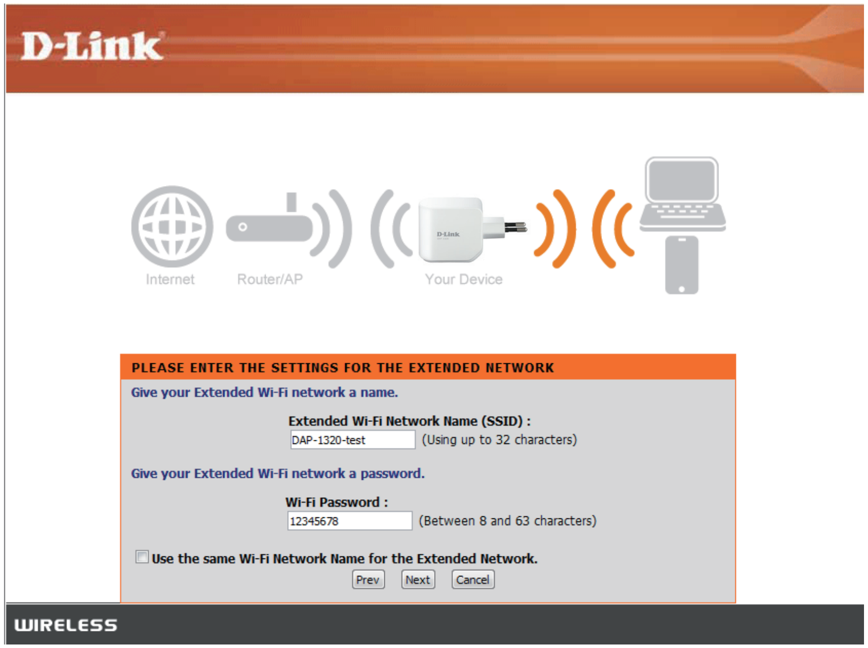


SELECT WI-FI NETWORK

ID	Wi-Fi Network Name	Wi-Fi Security Mode	Channel	Signal(%)	Select
1	DTester	WPA/WPA2-PSK(auto)	5	72	○
2	dlink-3F79	NONE	3	60	○
3	D-Link	NONE	6	35	○

Enter the Wi-Fi network name (SSID) and password for your extended network. If you would like the same Wi-Fi network name for the extended network, click on the Use the same Wi-Fi Network Name for the Extended Network box.

Click **Next** to continue.
Click **Prev** to return to the previous step.



PLEASE ENTER THE SETTINGS FOR THE EXTENDED NETWORK

Give your Extended Wi-Fi network a name.

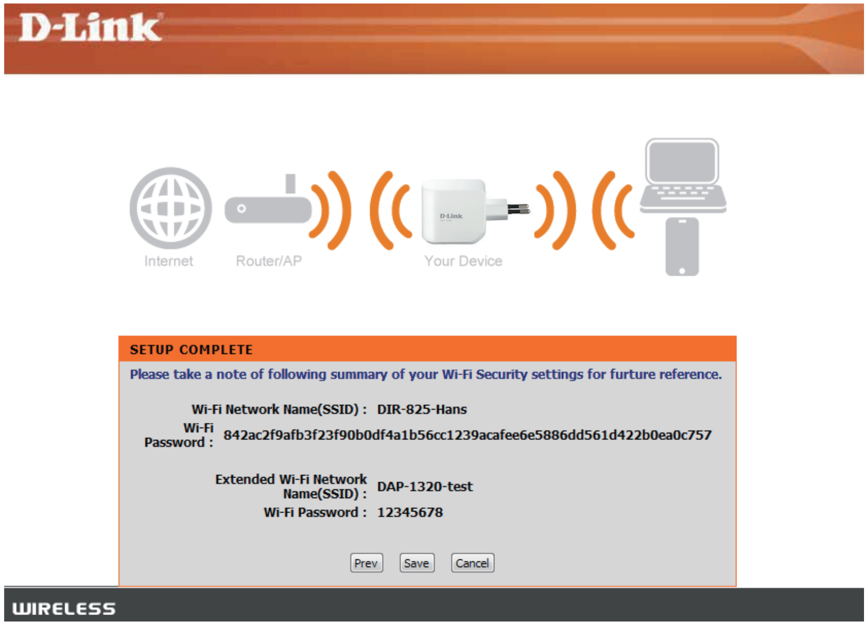
Extended Wi-Fi Network Name (SSID) : DAP-1320-test (Using up to 32 characters)

Give your Extended Wi-Fi network a password.

Wi-Fi Password : 12345678 (Between 8 and 63 characters)

□ Use the same Wi-Fi Network Name for the Extended Network.

Setup is complete, and your wireless network name and password will be displayed. It is recommended that you write this information down for future reference. Click **Next** to save your settings and reboot the repeater for your settings to take effect.



SETUP COMPLETE

Please take a note of following summary of your Wi-Fi Security settings for furture reference.

Wi-Fi Network Name(SSID) : DIR-825-Hans

Wi-Fi Password : 842ac2f9afb3f23f90b0df4a1b56cc1239acafee6e5886dd561d422b0ea0c757

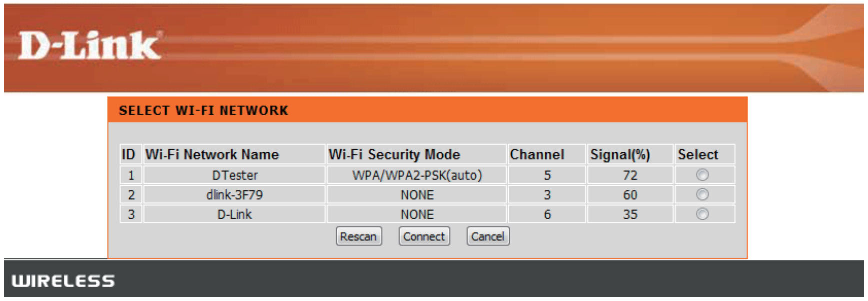
Extended Wi-Fi Network Name(SSID) : DAP-1320-test

Wi-Fi Password : 12345678

Using the manual method

The DAP-1320 will first scan for available Wi-Fi networks and list the networks it has found. If the network you would like to connect to isn't listed, click **Rescan** for the DAP-1320 to perform another scan. Select your network and click **Connect**.

Click **Next** to continue.

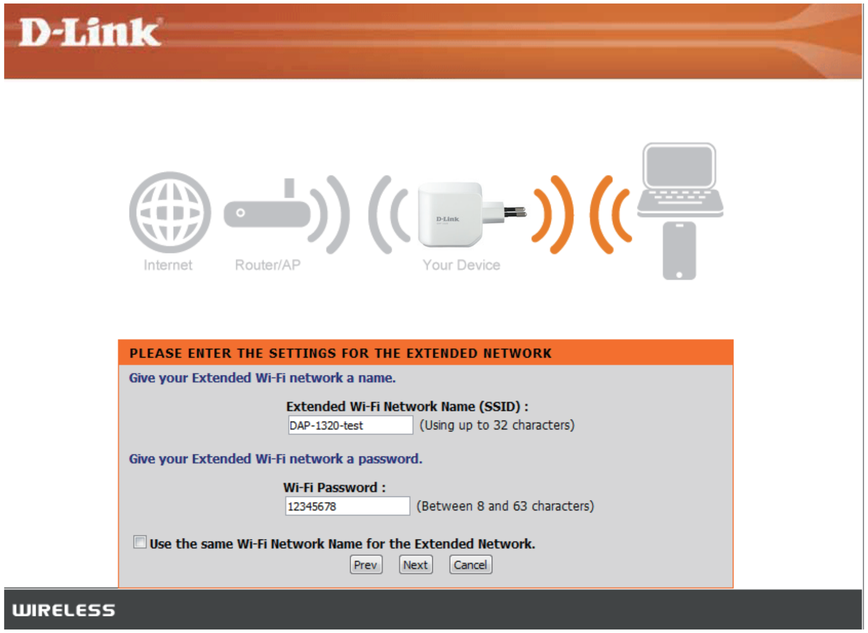


SELECT WI-FI NETWORK

ID	Wi-Fi Network Name	Wi-Fi Security Mode	Channel	Signal(%)	Select
1	DTester	WPA/WPA2-PSK(auto)	5	72	○
2	dlink-3F79	NONE	3	60	○
3	D-Link	NONE	6	35	○

Enter the Wi-Fi network name (SSID) and password for your extended network. If you would like the same Wi-Fi network name for the extended network, click on the Use the same Wi-Fi Network Name for the Extended Network box.

Click **Next** to continue.
Click **Prev** to return to the previous step.



PLEASE ENTER THE SETTINGS FOR THE EXTENDED NETWORK

Give your Extended Wi-Fi network a name.

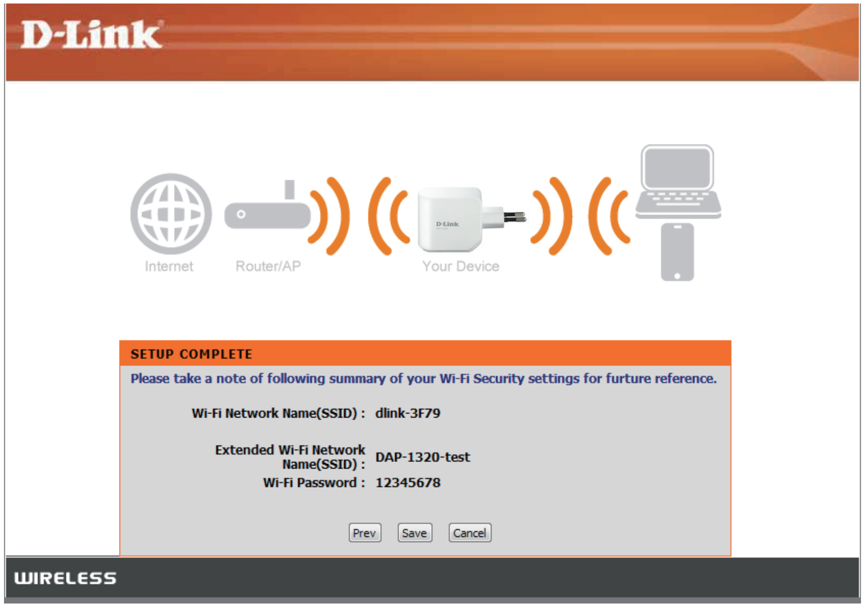
Extended Wi-Fi Network Name (SSID) : DAP-1320-test (Using up to 32 characters)

Give your Extended Wi-Fi network a password.

Wi-Fi Password : 12345678 (Between 8 and 63 characters)

□ Use the same Wi-Fi Network Name for the Extended Network.

Setup is complete, and your wireless network name and password will be displayed. It is recommended that you write this information down for future reference. Click **Save** to save your settings and reboot the repeater.



SETUP COMPLETE

Please take a note of following summary of your Wi-Fi Security settings for furture reference.

Wi-Fi Network Name(SSID) : dlink-3F79

Extended Wi-Fi Network Name(SSID) : DAP-1320-test

Wi-Fi Password : 12345678

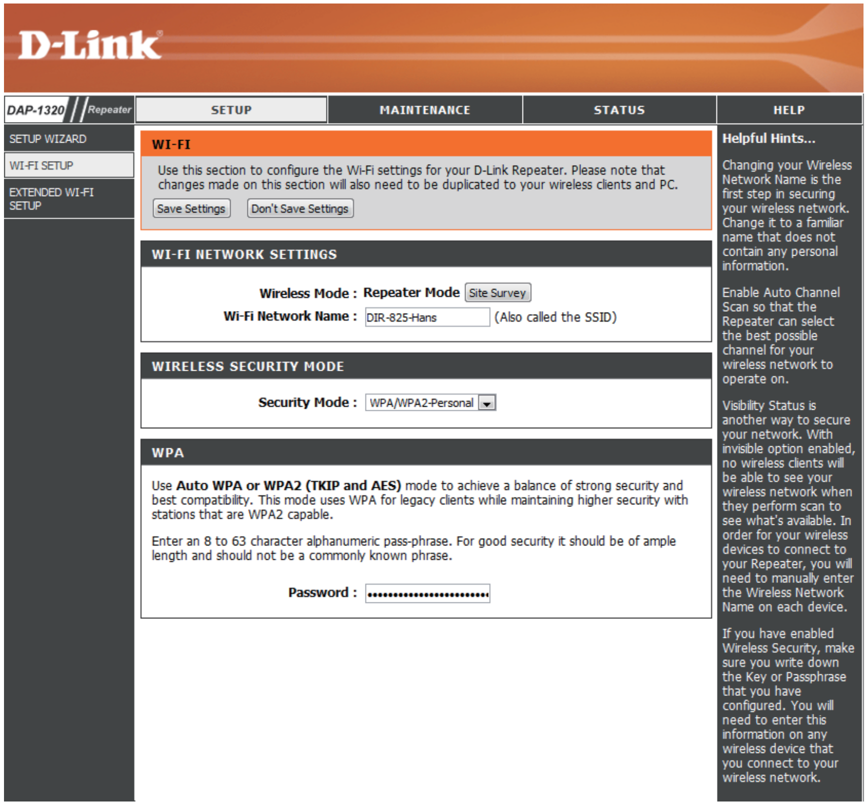
Wi-Fi Setup

This page lets you configure the Wi-Fi settings to connect your DAP-1320 to another wireless network. After making your changes, click the **Save Settings** button.

Wireless Mode: This is set to Repeater mode and cannot be changed.

Wi-Fi Network Name: Click **Site Survey** to scan for available wireless networks and select the one you want to use the DAP-1320 to extend. You can also type in the name (SSID) for your wireless network.

Wireless Security Mode: Select the security method that is being used by the wireless network that you have selected: **WEP, WPA/WPA2, or none**. Refer to the next page for details on configuring the different security modes.



WI-FI

Use this section to configure the Wi-Fi settings for your D-Link Repeater. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WI-FI NETWORK SETTINGS

Wireless Mode : Repeater Mode

Wi-Fi Network Name : DIR-825-Hans (Also called the SSID)

WIRELESS SECURITY MODE

Security Mode : WPA/WPA2-Personal

WPA

Use **Auto WPA or WPA2 (TKIP and AES)** 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.

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.

Password : ••••••••••••••••••••••••

Helpful Hints...

Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

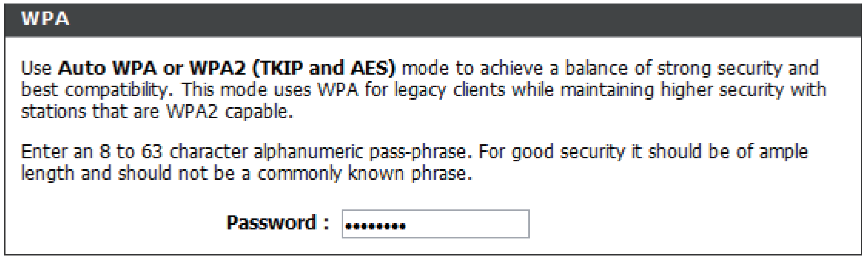
Enable Auto Channel Scan so that the Repeater can select the best possible channel for your wireless network to operate on.

Visibility Status is another way to secure your network. With invisible option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your Repeater, 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 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.

If you selected **WPA/WPA2-Personal**, you will see the following settings.

Password: Enter a password between 8 to 63 characters.



WPA

Use **Auto WPA or WPA2 (TKIP and AES)** 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.

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.

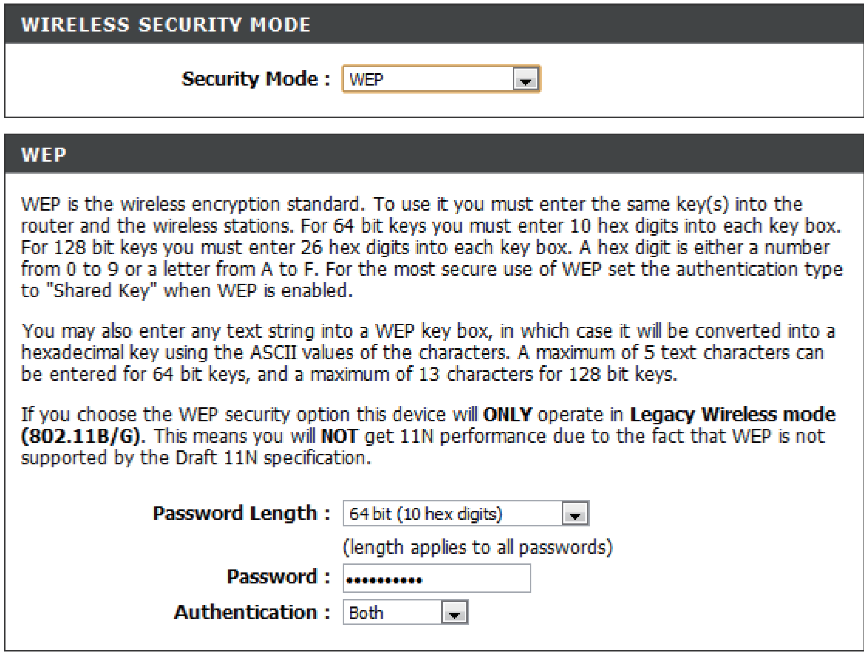
Password : ••••••••

If you selected **WEP**, you will see the following settings.

Password Length: Select the length of the password for your wireless network.

Password: Enter the password for your wireless network. It will need to meet the length requirement that you selected above.

Authentication: Choose what authentication type to use.



WIRELESS SECURITY MODE

Security Mode : WEP

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

Password Length : 64 bit (10 hex digits)

(length applies to all passwords)

Password : ••••••••••

Authentication : Both

Extended Wi-Fi Setup

This page lets you configure a wireless LAN for your DAP-1320. After making your changes, click **Save Settings**.

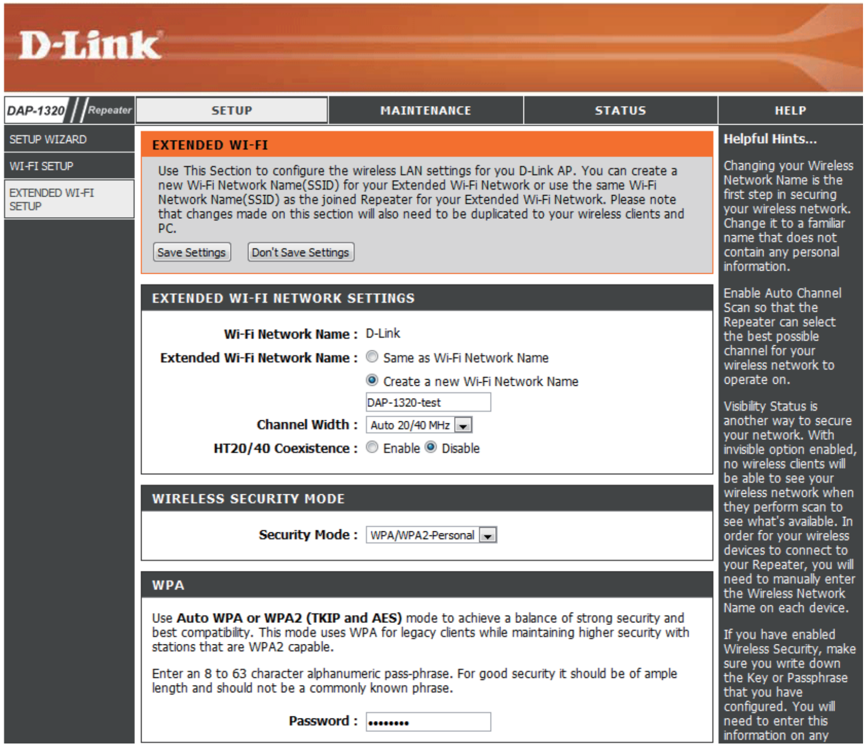
Wi-Fi Network Name: This is set in Wi-Fi Setup and cannot be changed here. Please go to Wi-Fi Setup if you wish to change it.

Extended Wi-Fi Network Name: Leave it as the same as the current Wi-Fi network name (SSID) or type in a new name.

Channel Width: Select the Wi-Fi channel width to use for your wireless network.

HT20/40 Coexistence: Enable or disable this feature.

Wireless Security Mode: Select the security method to use for your wireless network: **WEP, WPA/WPA2**. Refer to the next page for details on configuring the different security modes.



EXTENDED WI-FI

Use This Section to configure the wireless LAN settings for you D-Link AP. You can create a new Wi-Fi Network Name(SSID) for your Extended Wi-Fi Network or use the same Wi-Fi Network Name(SSID) as the joined Repeater for your Extended Wi-Fi Network. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

EXTENDED WI-FI NETWORK SETTINGS

Wi-Fi Network Name : D-Link

Extended Wi-Fi Network Name : ○ Same as Wi-Fi Network Name ● Create a new Wi-Fi Network Name

DAP-1320-test

Channel Width : Auto 20/40 MHz

HT20/40 Coexistence : ○ Enable ● Disable

WIRELESS SECURITY MODE

Security Mode : WPA/WPA2-Personal

WPA

Use **Auto WPA or WPA2 (TKIP and AES)** 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.

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.

Password : ••••••••

Helpful Hints...

Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

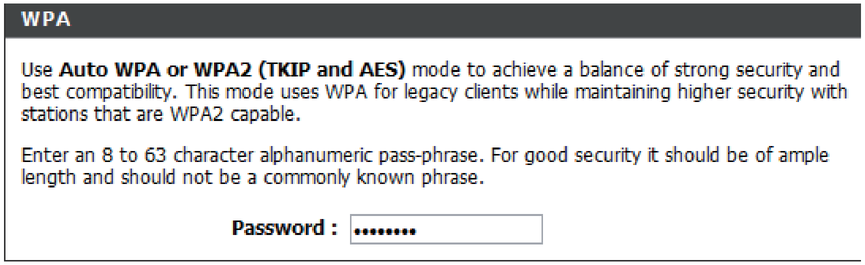
Enable Auto Channel Scan so that the Repeater can select the best possible channel for your wireless network to operate on.

Visibility Status is another way to secure your network. With invisible option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your Repeater, 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 Key or Passphrase that you have configured. You will need to enter this information on any

If you selected **WPA/WPA2-Personal**, you will see the following settings.

Password: Enter a password between 8 to 63 characters.



WPA

Use **Auto WPA or WPA2 (TKIP and AES)** 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.

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.

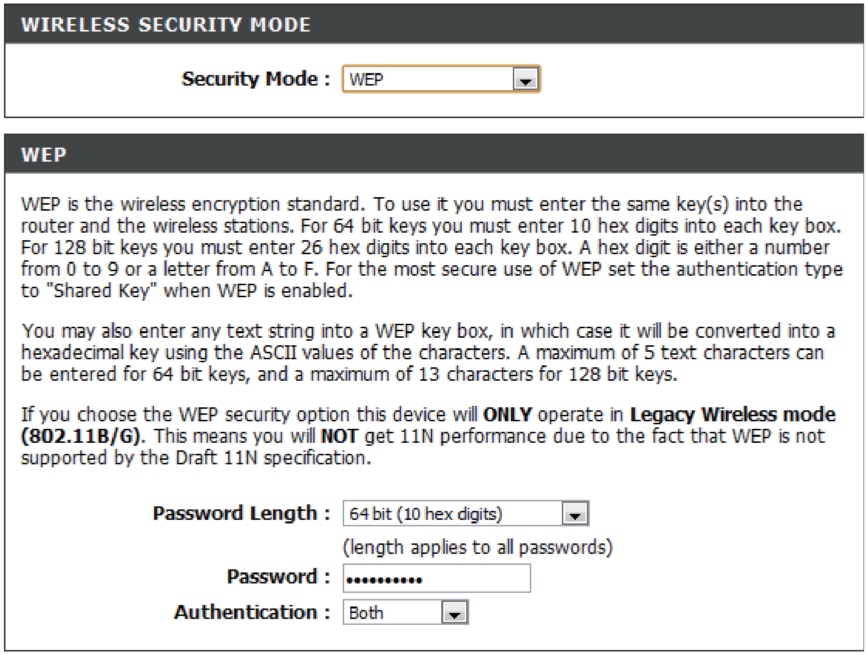
Password : ••••••••

If you selected **WEP**, you will see the following settings.

Password Length: Select the length of the password for your wireless network.

Password: Enter the password for your wireless network. It will need to meet the length requirement that you selected above.

Authentication: Choose what authentication type to use.



WIRELESS SECURITY MODE

Security Mode : WEP

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

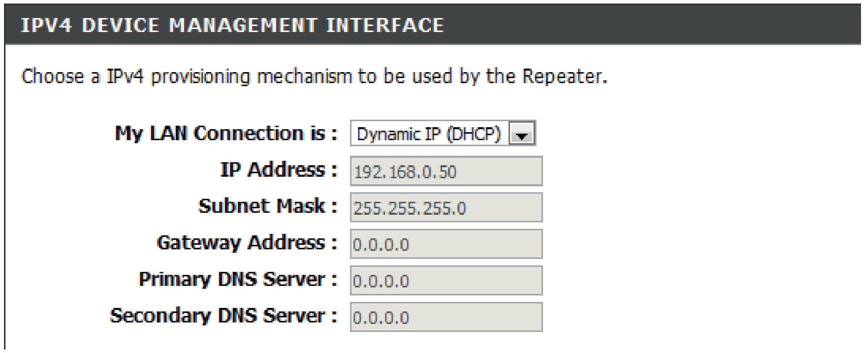
Password Length : 64 bit (10 hex digits)

(length applies to all passwords)

Password : ••••••••••

Authentication : Both

If you need to use a IPv4 provisioning mechanism for the Repeater, configure the settings below.



IPV4 DEVICE MANAGEMENT INTERFACE

Choose a IPv4 provisioning mechanism to be used by the Repeater.

My LAN Connection is : Dynamic IP (DHCP)

IP Address : 192.168.0.50

Subnet Mask : 255.255.255.0

Gateway Address : 0.0.0.0

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

My LAN Connection is: Select the type of LAN connection. If you select Dynamic IP, all the values below will already be set. If you select Static IP, you need to enter the below values.

IP Address: Enter the IP address.

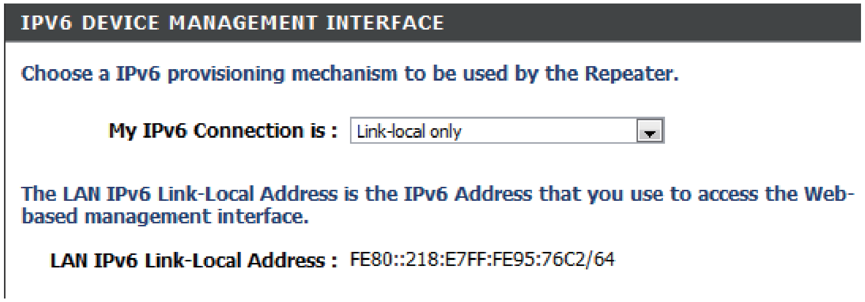
Subnet Mask: Enter the subnet mask.

Gateway Address: Enter the gateway address.

Primary DNS Server: Enter the IP address of the primary DNS server.

Secondary DNS Server: Enter the IP address of the secondary DNS server.

If you need to use a IPv6 provisioning mechanism for the Repeater, select the mechanism to use: **Link-local only, Static IPv6, and Autoconfiguration**. Refer to below and the next page for details on configuring the different security modes.



IPV6 DEVICE MANAGEMENT INTERFACE

Choose a IPv6 provisioning mechanism to be used by the Repeater.

My IPv6 Connection is : Link-local only

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::218:E7FF:FE95:76C2/64

If you selected **Link-Local only**, you will see the following settings:

LAN IPv6 Link-Local Address: The IPv6 Link-Local Address is the IPv6 Address that you use tto access the Web-based management interface.

If you selected **Static IPv6**, you will see the following settings. You must enter values for all the settings.

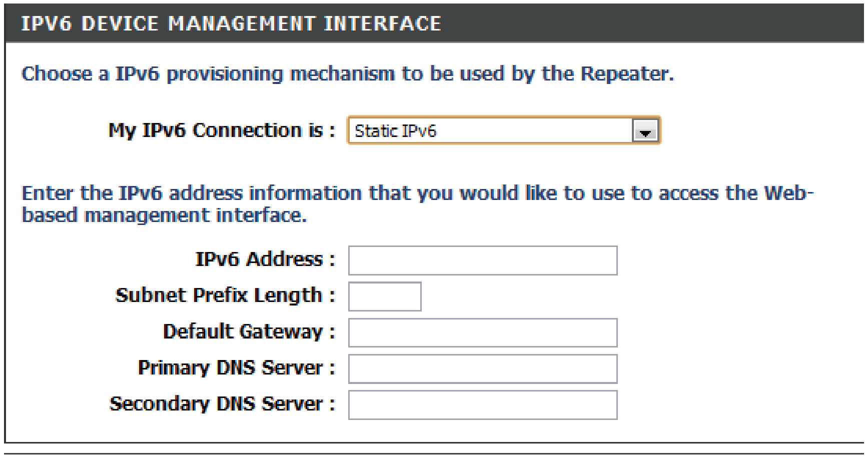
IPv6 Address: Enter the IPv6 address.

Subnet Prefix Length: Enter the length of the subnet prefix.

Default Gateway: Enter the default gateway.

Primary DNS Server: Enter the IP address of the primary DNS Server.

Secondary DNS Server: Enter the IP address of the secondary DNS Server.



IPV6 DEVICE MANAGEMENT INTERFACE

Choose a IPv6 provisioning mechanism to be used by the Repeater.

My IPv6 Connection is : Static IPv6

Enter the IPv6 address information that you would like to use to access the Web-based management interface.

IPv6 Address :

Subnet Prefix Length :

Default Gateway :

Primary DNS Server :

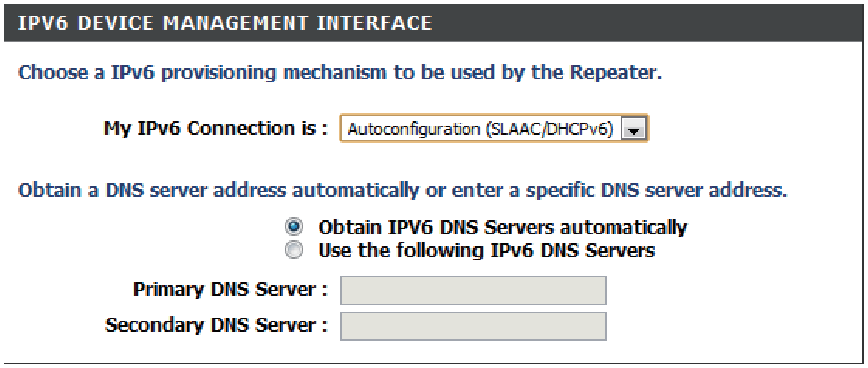
Secondary DNS Server :

If you selected **Autoconfiguration (SLAAC/DHCPv6)**, you will see the following settings.

You can either choose to obtain IPv6 DNS Servers automatically, or enter the servers you wish to use.

Primary DNS Server: Enter the primary DNS Server address.

Secondary DNS Server: Enter the secondary DNS Server address.



IPV6 DEVICE MANAGEMENT INTERFACE

Choose a IPv6 provisioning mechanism to be used by the Repeater.

My IPv6 Connection is : Autoconfiguration (SLAAC/DHCPv6)

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

● Obtain IPV6 DNS Servers automatically

○ Use the following IPv6 DNS Servers

Primary DNS Server :

Secondary DNS Server :

Maintenance

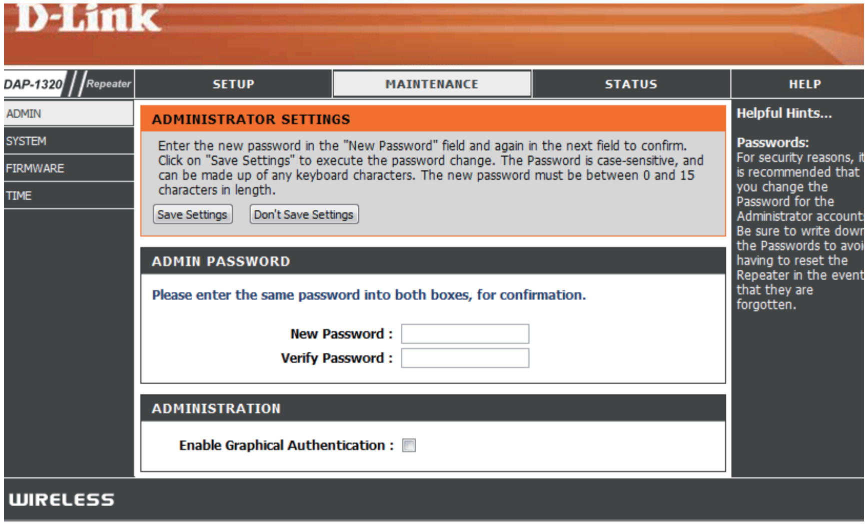
Admin

This page will allow you to set a new password for the administrator account for configuring the DAP-1320. You can also turn on graphical authentication (CAPTCHA) on this page. After making your changes, click the **Save Settings** button.

New Password: Enter the new password.

Verify Password: Enter the new password again.

Enable Graphical Authentication: Check this to enable graphical authentication, or CAPTCHAs. This provides an extra layer of security by requiring you to enter a code that is displayed onscreen.



ADMINISTRATOR SETTINGS

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.

ADMIN PASSWORD

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

New Password :	
Verify Password :	

ADMINISTRATION

Enable Graphical Authentication : □

Helpful Hints...

Passwords:
For security reasons, i
is recommended that
you change the
Password for the
Administrator account
Be sure to write dowr
the Passwords to avoi
having to reset the
Repeater in the event
that they are
forgotten.

System

This page allows you to save or restore your system configuration, reset or reboot the DAP-1320. After making your changes, click the **Save Settings** button.

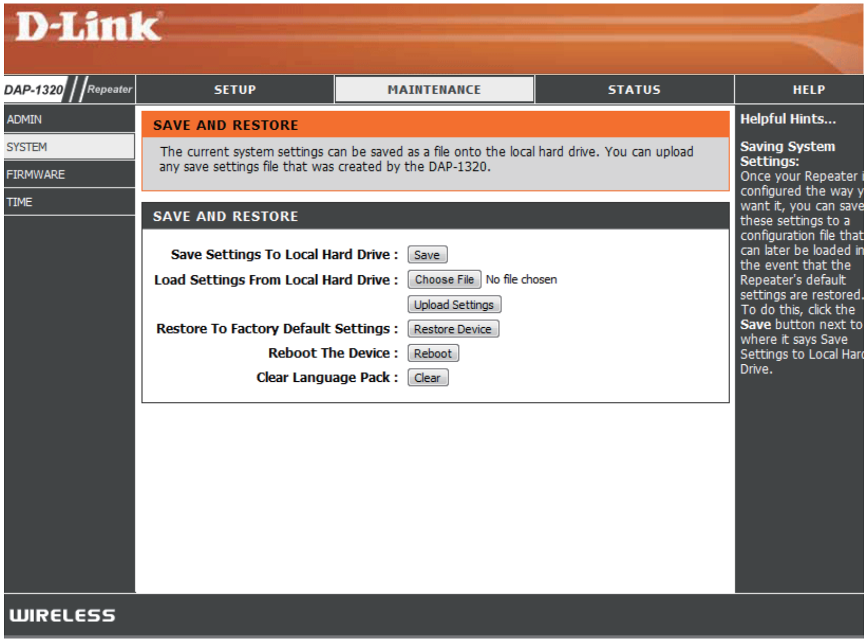
Save Settings To Local Hard Drive: Save the system settings onto a file to the local hard drive. You will then see a file dialog where you can select a location and file name for the settings.

Load Settings From Local Hard Drive: Load the system settings from a file on the local hard drive.

Restore to Factory Default Settings: Restore the system settings to factory default settings.

Reboot the Device: Click **Reboot** to reboot the DAP-1320.

Clear Language Pack: If you have previously installed a Language Pack, you can remove it by clicking **Remove**.



SAVE AND RESTORE

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-1320.

SAVE AND RESTORE

Save Settings To Local Hard Drive : Save

Load Settings From Local Hard Drive : Choose File No file chosen

Upload Settings

Restore To Factory Default Settings : Restore Device

Reboot The Device : Reboot

Clear Language Pack : Clear

Helpful Hints...

Saving System Settings:
Once your Repeater i
configured the way y
want it, you can save
these settings to a
configuration file that
can later be loaded in
the event that the
Repeater's default
settings are restored.
To do this, click the
Save button next to
where it says Save
Settings to Local Hard
Drive.

Firmware

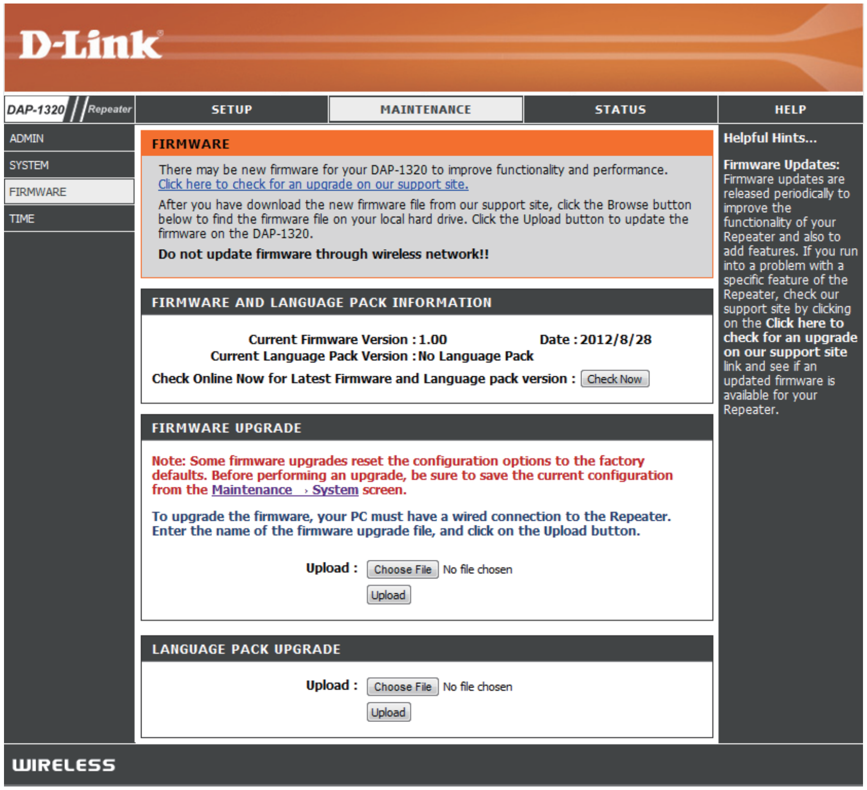
Firmware and language upgrades might be provided for the DAP-1320 in future. You can check and upgrade your firmware and language pack on this page. Please check the D-Link support website for firmware updates at **http://support.dlink.com**. You can download firmware upgrades to your hard drive from this site.

Click **Check Now** to find out if there is new updated firmware. If there is, you can download it to your hard drive.

Firmware Upgrade: After you have downloaded the new firmware, click **Choose File** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade. Do not disconnect from the DAP-1320 or power your computer or DAP-1320 off during the upgrade process.

You can change the language of the web UI by uploading available language packs.

Language Pack Upgrade: First, download a language pack from the D-Link website onto your hard drive. After you have downloaded the new language pack, click **Choose File** to locate the language pack file on your hard drive. Click **Upload** to complete the language pack upgrade.



FIRMWARE

There may be new firmware for your DAP-1320 to improve functionality and performance.
Click here to check for an upgrade on our support site.

After you have download the new firmware file from our support site, click the Browse button below to find the firmware file on your local hard drive. Click the Upload button to update the firmware on the DAP-1320.

Do not update firmware through wireless network!!

FIRMWARE AND LANGUAGE PACK INFORMATION

Current Firmware Version : 1.00 **Date : 2012/8/28**
Current Language Pack Version : No Language Pack
Check Online Now for Latest Firmware and Language pack 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 from the Maintenance › System screen.

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

Upload : [Choose File] No file chosen
[Upload]

LANGUAGE PACK UPGRADE

Upload : [Choose File] No file chosen
[Upload]

Helpful Hints...

Firmware Updates: Firmware updates are released periodically to improve the functionality of your Repeater and also to add features. If you run into a problem with a specific feature of the Repeater, check our support site by clicking on the **Click here to check for an upgrade on our support site** link and see if an updated firmware is available for your Repeater.

Time

This page allows you to configure, update, and maintain the correct time on the internal system clock. After making your changes, click the **Save Settings** button.

Time Zone: Select the time zone.

Enable Daylight Saving: Click to enable Daylight Saving Time.

Daylight Saving Offset: Select how many hours to offset the time if Daylight Saving Time is enabled.

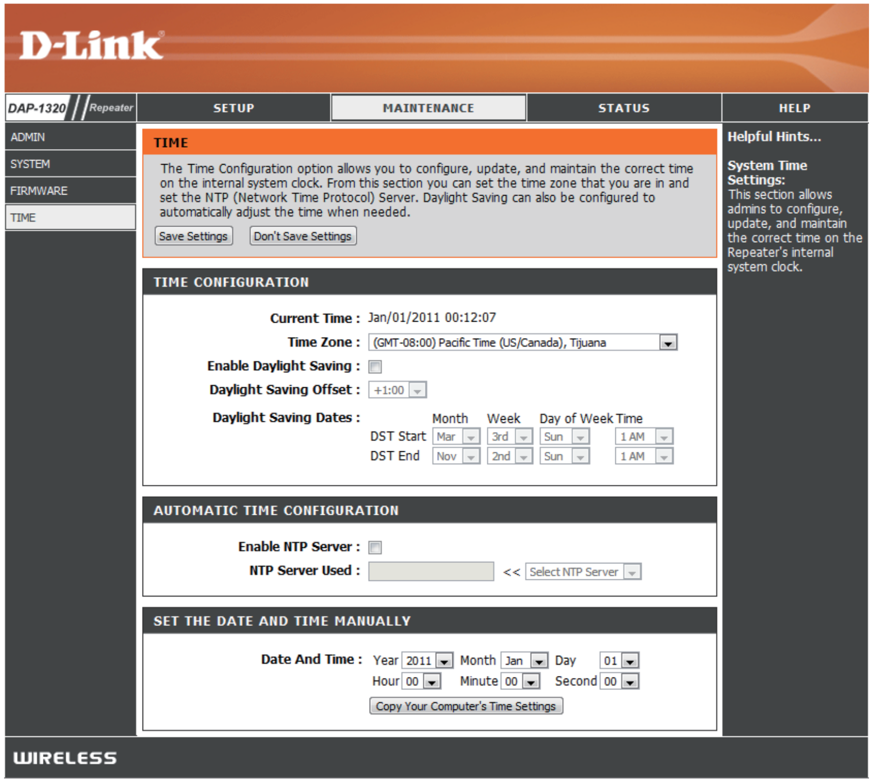
Daylight Saving Dates: Select the start and end dates for Daylight Savings Time to take effect.

Enable NTP Server: Click if you want to use a Network Time Protocol (NTP) server to synchronize the system time.

NTP Server Used: Select the NTP Server you wish to use.

Date and Time: Set the date and time manually.

Copy your Computer's Time Settings: Click to use your computer's time settings.



TIME

The Time 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 that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME CONFIGURATION

Current Time : Jan/01/2011 00:12:07

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

Enable Daylight Saving : □

Daylight Saving Offset : +1:00

Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Mar	3rd	Sun	1 AM
DST End	Nov	2nd	Sun	1 AM

AUTOMATIC TIME CONFIGURATION

Enable NTP Server : □

NTP Server Used : <<

SET THE DATE AND TIME MANUALLY

Date And Time : Year 2011 Month Jan Day 01
Hour 00 Minute 00 Second 00

Helpful Hints...

System Time Settings:
This section allows admins to configure, update, and maintain the correct time on the Repeater's internal system clock.

Status

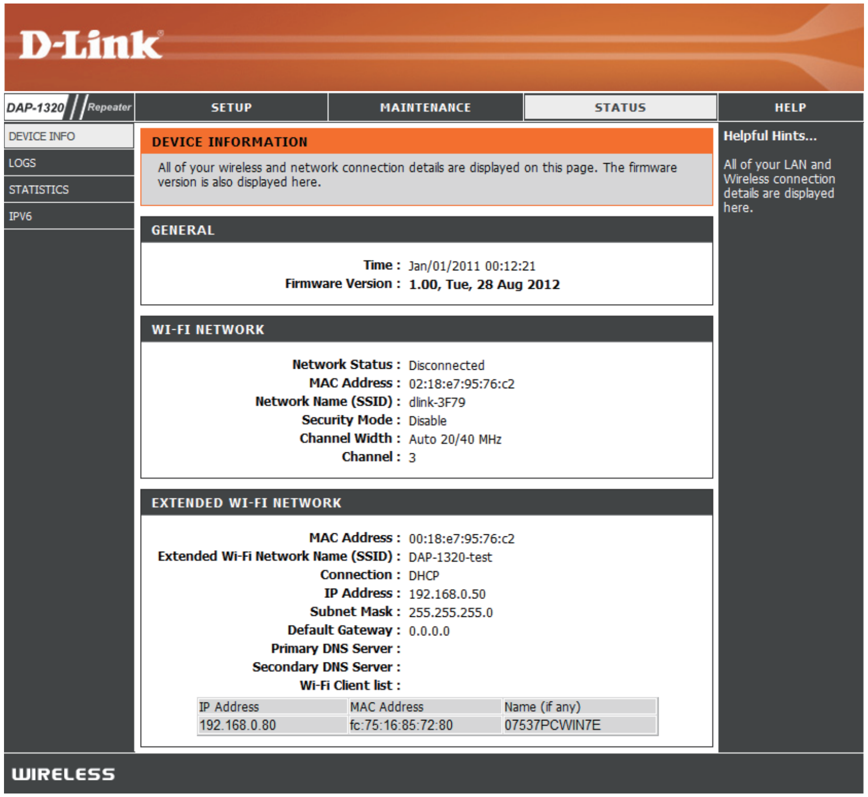
Device Info

This page displays details about your wireless and network connection, and the firmware version.

General: Displays the time and firmware version.

Wi-Fi Network: Displays information about the Wi-Fi network.

Extended Wi-Fi Network: Displays information about the extended Wi-Fi network.



DEVICE INFORMATION

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

GENERAL

Time : Jan/01/2011 00:12:21
Firmware Version : 1.00, Tue, 28 Aug 2012

WI-FI NETWORK

Network Status : Disconnected
MAC Address : 02:18:e7:95:76:c2
Network Name (SSID) : dlink-3F79
Security Mode : Disable
Channel Width : Auto 20/40 MHz
Channel : 3

EXTENDED WI-FI NETWORK

MAC Address : 00:18:e7:95:76:c2
Extended Wi-Fi Network Name (SSID) : DAP-1320-test
Connection : DHCP
IP Address : 192.168.0.50
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
Primary DNS Server :
Secondary DNS Server :
Wi-Fi Client list :

IP Address	MAC Address	Name (if any)
192.168.0.80	fc:75:16:85:72:80	07537PCWIN7E

Helpful Hints...

All of your LAN and Wireless connection details are displayed here.

Logs

The DAP-1320 keeps a running log of events and activities occurring on the DAP-1320. If the DAP-1320 is rebooted, the logs are automatically cleared.

Log Options: There are several types of logs that can be viewed: **System Activity, Debug Information, Attacks, Dropped Packets** and **Notice**.

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

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

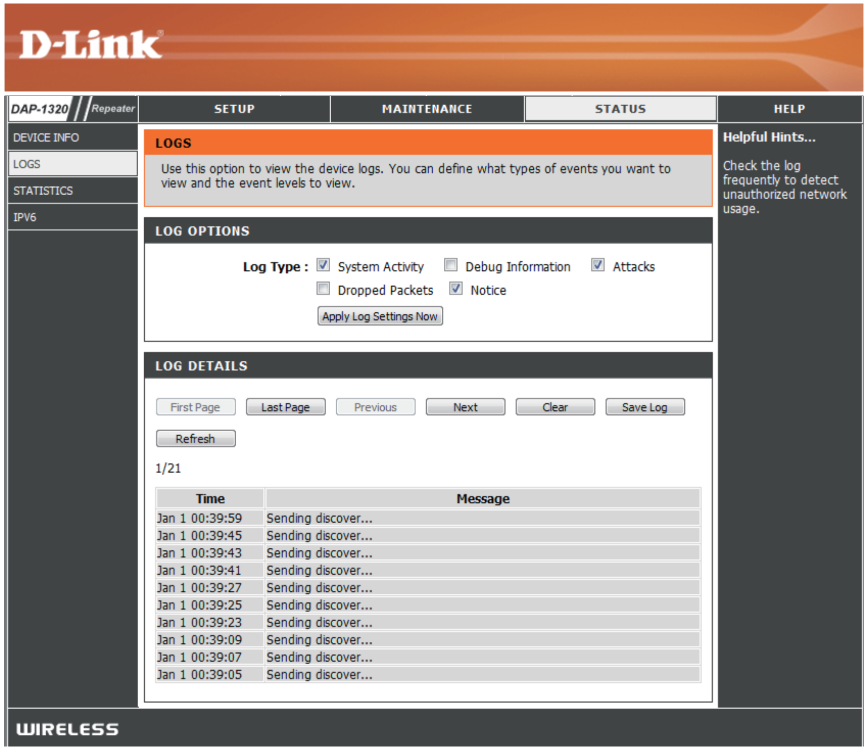
Previous: This directs you to the previous page of the log.

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

Clear: This clears all current log content.

Save Log: This opens dialog where you can save the current log to your hard drive.

Refresh: This 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 OPTIONS

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

Apply Log Settings Now

LOG DETAILS

First Page | Last Page | Previous | Next | Clear | Save Log

Refresh

1/21

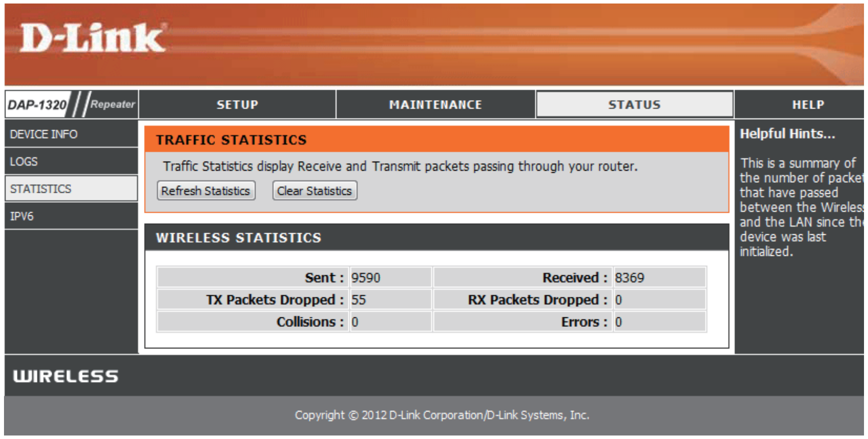
Time	Message
Jan 1 00:39:59	Sending discover...
Jan 1 00:39:45	Sending discover...
Jan 1 00:39:43	Sending discover...
Jan 1 00:39:41	Sending discover...
Jan 1 00:39:27	Sending discover...
Jan 1 00:39:25	Sending discover...
Jan 1 00:39:23	Sending discover...
Jan 1 00:39:09	Sending discover...
Jan 1 00:39:07	Sending discover...
Jan 1 00:39:05	Sending discover...

Helpful Hints...

Check the log frequently to detect unauthorized network usage.

Statistics

The DAP-1320 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. Click **Refresh Statistics** to update the information, or click **Clear Statistics** to reset all statistics. The traffic counter will reset if the DAP-1320 is rebooted.



TRAFFIC STATISTICS

Traffic Statistics display Receive and Transmit packets passing through your router.

WIRELESS STATISTICS

Sent :	9590	Received :	8369
TX Packets Dropped :	55	RX Packets Dropped :	0
Collisions :	0	Errors :	0

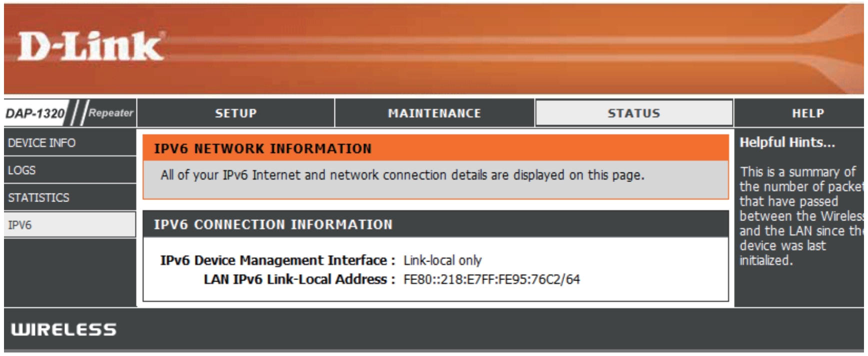
Helpful Hints...

This is a summary of the number of packe that have passed between the Wireles and the LAN since th device was last initialized.

Copyright © 2012 D-Link Corporation/D-Link Systems, Inc.

IPv6

This page displays all the IPv6 Internet and network connection information.



IPV6 NETWORK INFORMATION

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

IPV6 CONNECTION INFORMATION

IPv6 Device Management Interface : Link-local only

LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:76C2/64

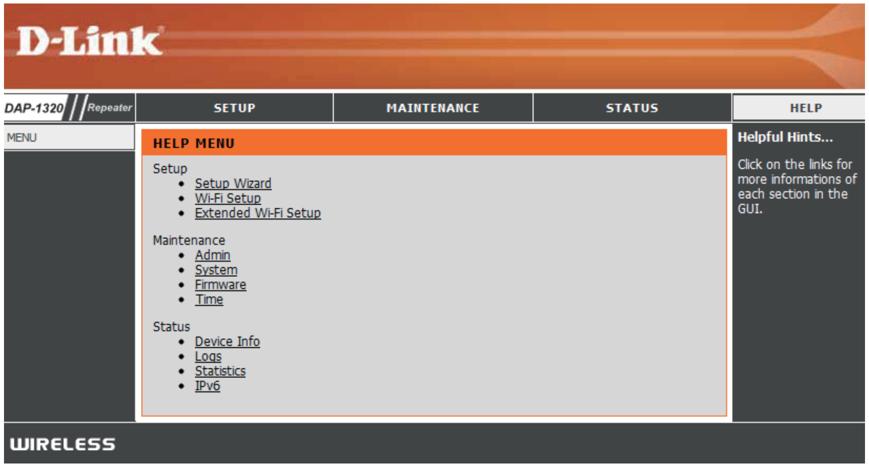
Helpful Hints...

This is a summary of the number of packet that have passed between the Wireles and the LAN since th device was last initialized.

Help

Menu

This page provides helpful information on the Setup, Maintenance, and Status sections in this Web GUI. Click on a link to learn more about that topic.



HELP MENU

Setup
- Setup Wizard
- Wi-Fi Setup
- Extended Wi-Fi Setup

Maintenance
- Admin
- System
- Firmware
- Time

Status
- Device Info
- Logs
- Statistics
- IPv6

Helpful Hints...

Click on the links for more informations of each section in the GUI.

Connecting a Wireless Client

WPS Button

The easiest and most secure way to connect your wireless devices to the repeater is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DAP-1320. Please refer to your 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-1320 for about 1 second. The WPS button will start to blink.

Step 2 - Within 2 minutes, press the WPS button on your wireless client.

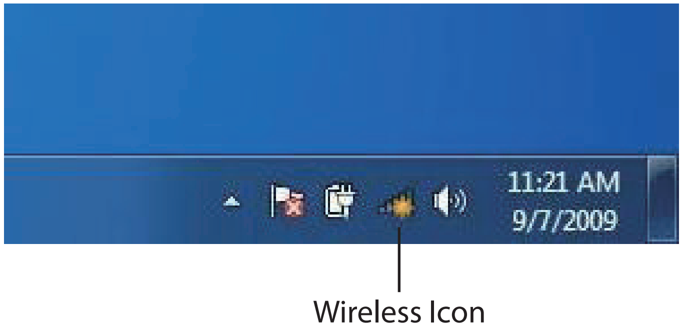
Step 3 - Allow up to 1 minute to configure. Once the WPS light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

Windows® 7

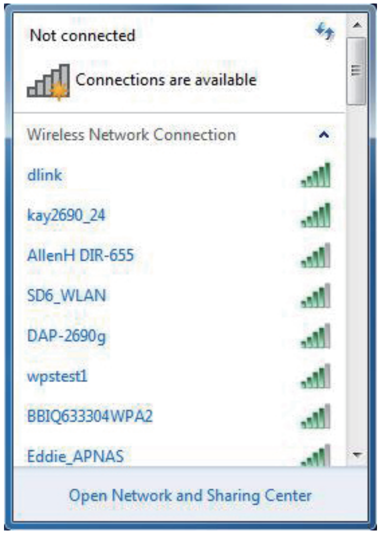
WPA/WPA2

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



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



Not connected

Connections are available

Wireless Network Connection

dlink

kay2690_24

AllenH DIR-655

SD6_WLAN

DAP-2690g

wpstest1

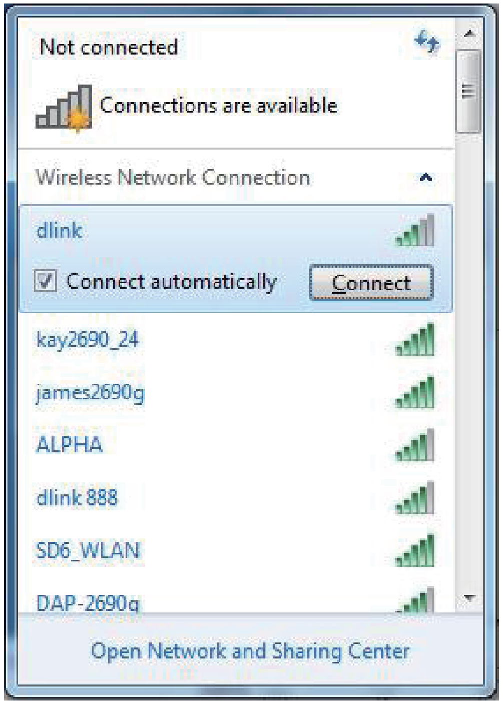
BBIQ633304WPA2

Eddie_APNAS

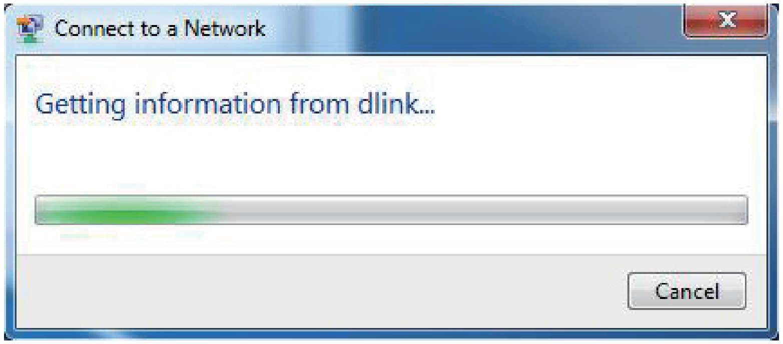
Open Network and Sharing Center

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.



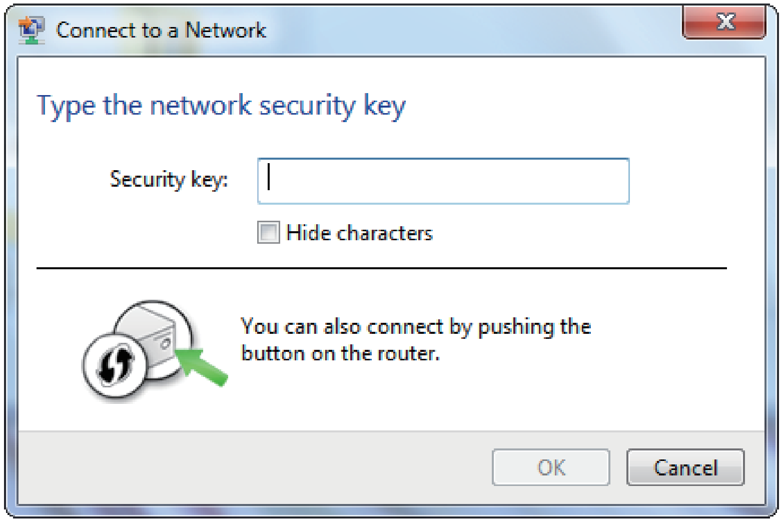
4. The following window appears while your computer tries to connect to the router.



Getting information from dlink...

5. Enter the same security key or passphrase that is on your router and click **Connect**.

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.



Connect to a Network

Type the network security key

Security key:

□ Hide characters

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

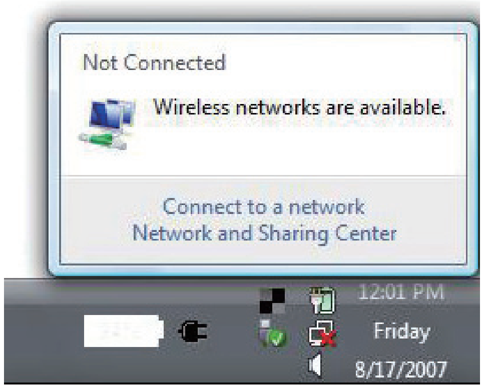
Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, 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**.

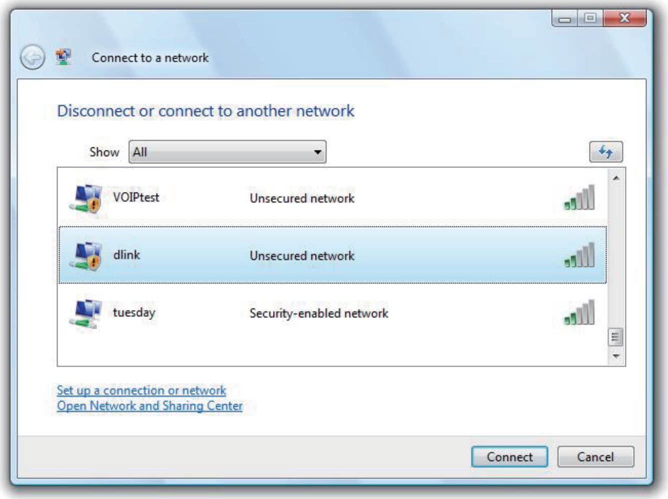


Not Connected

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 **Connect**.

If you get a good signal but cannot access the Internet, check you TCP/IP settings for 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

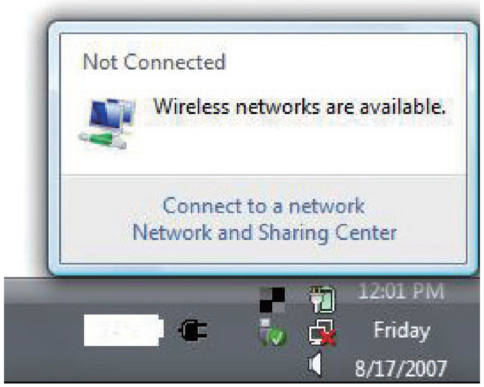
VOIPtest	Unsecured network
dlink	Unsecured network
tuesday	Security-enabled network

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.

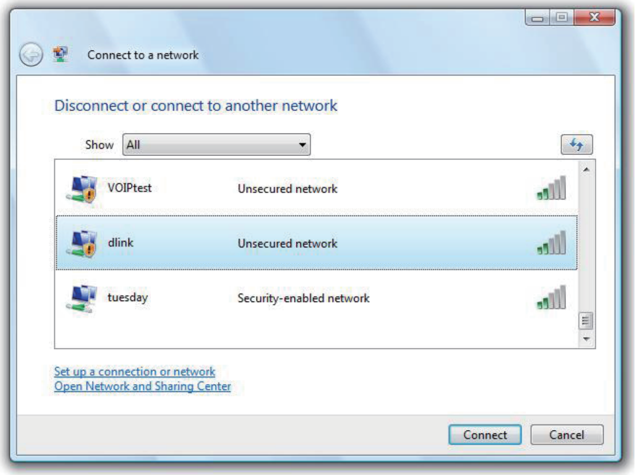
1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



Not Connected

Wireless networks are available.

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



Connect to a network

Disconnect or connect to another network

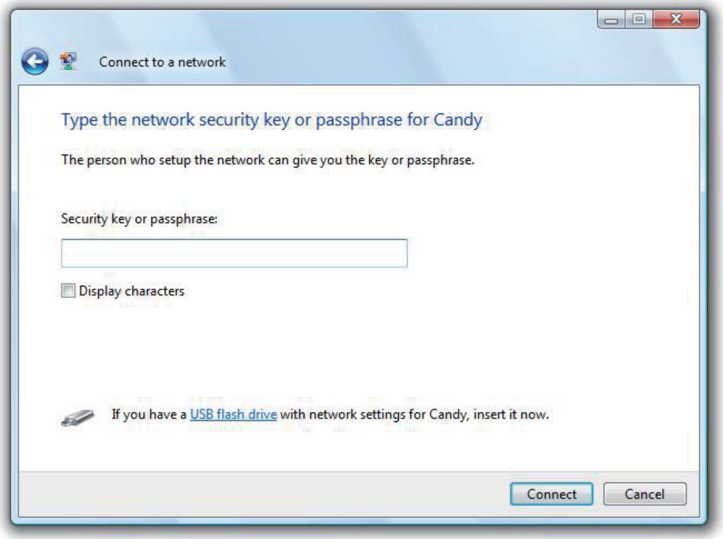
Show All

VOIPtest	Unsecured network
dlink	Unsecured network
tuesday	Security-enabled network

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

3. Enter the same security key or passphrase that is on your router and click **Connect**.

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.



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:

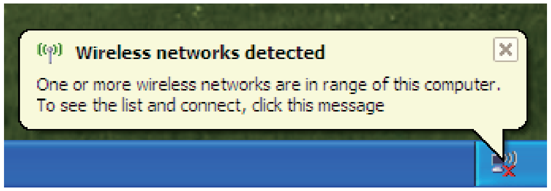
□ Display characters

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

Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. 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® XP utility as seen below.

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

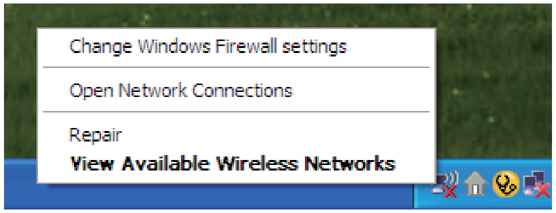


Wireless networks detected

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

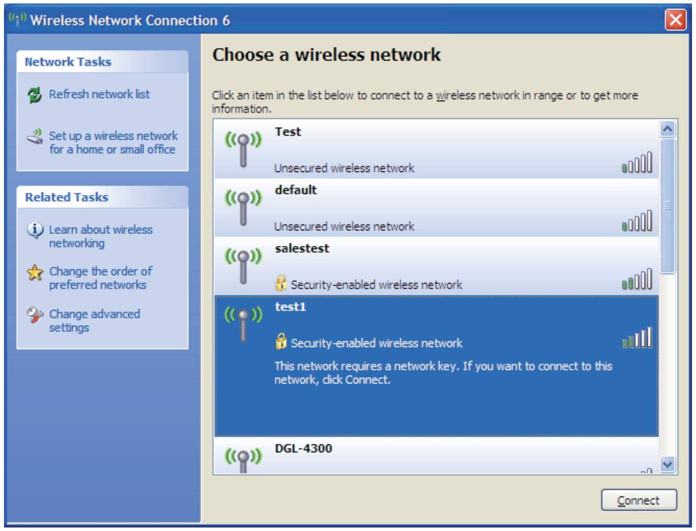
or

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 you TCP/IP settings for 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

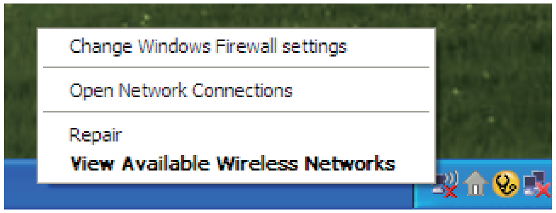
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

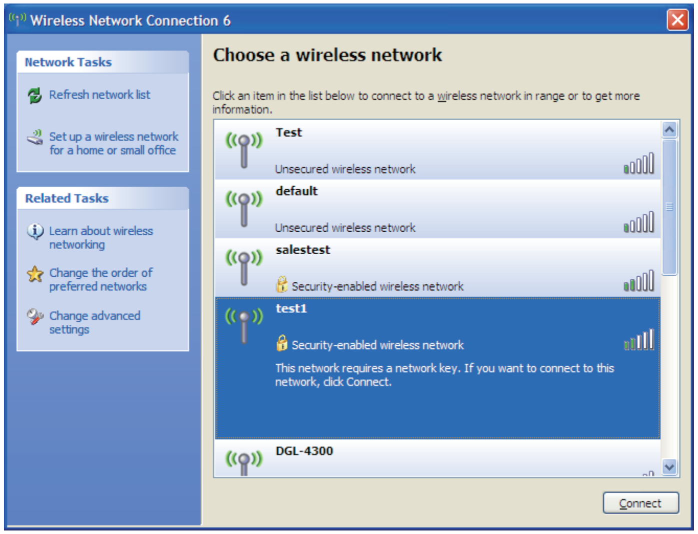
WPA/WPA2

It is recommended to enable WPA 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 WPA 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

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

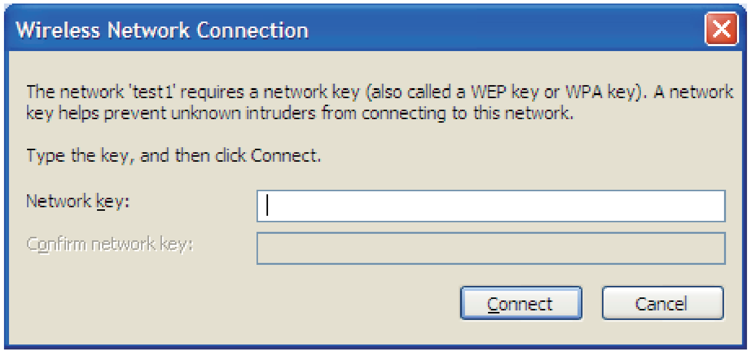
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

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

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-1320. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

When entering the IP address of the D-Link repeater (dlinkap.local for example), you are not connecting to a website nor do you 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® 6.0 and higher
  - Mozilla Firefox 3.0 and higher
  - Google™ Chrome 2.0 and higher
  - Apple Safari 3.0 and higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® 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 repeater in the address bar. This should open the login page for your web management.

- If you still cannot access the configuration, unplug the power to the repeater 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 repeater. Unfortunately this process will change all your settings back to the factory defaults.

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

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 access the data you want, when and where you want it. 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 adapter cards 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.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology as become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your Router or Access Point
Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference
Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security
Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

Technical Specifications

Standards
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11b

Wireless Frequency Range [1]
- 2.4 GHz to 2.4835 GHz

Antennas
- Internal Antenna

Security
- Wi-Fi Protected Access (WPA/WPA2)
- WPS™ (PBC)
- 64/128-bit WEP

Advanced Features
- QRS Mobile setup app for iOS and Android devices

Device Management
- Web UI

Diagnostic LEDs
- Status/WPS

Operating Temperature
- 0 to 40 ˚C (32 to 104 ˚F)

Operating Humidity
- 0% to 90% non-condensing

Power Input
- AC 110-240 V

Maximum Power Consumption
- 5.5 W

Certifications
- EMI/EMC
- FCC
- CE
- IC
- C-Tick
- UL
- Wi-Fi Certified

Dimensions
- 48 x 42 x 53.5 mm (1.89 x 1.65 x 2.11 inches)

Weight
- 69 grams (0.152 lb)

Warranty
- 2 Years

[1] Frequency range varies depending on local regulations

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

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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 noncommercially, 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.

Safety Statements

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

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

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

FCC Caution:

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

Operations in the 5.15-5.25GHz / 5.470 ~ 5.725GHz band are restricted to indoor usage 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 maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

ICC Notice:

Operation is subject to the following two conditions:

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

IMPORTANT NOTE:
IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

(i) The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems;
(ii) The maximum antenna gain (2dBi) permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

In addition, users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

(1) Ce périphérique ne doit pas causer d'interférence et.
(2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.