D-Link

Version 1.0 | 1/3/2014

User Manual

Wireless AC1200
Dual Band Access Point

DAP-1665

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	January 3, 2014	• Initial release for Revision A1

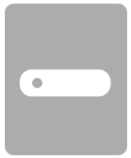
Trademarks

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.

Table of Contents

Product Overview

Package Contents



DAP-1665 Wireless AC1200 Dual Band Access Point

Ethernet Cable

Two Detachable Antennas[1]

Power Adapter

Wi-Fi Configuration Card

Quick Install Guide

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

Note: *Using a power supply with a different voltage rating than the one included with the DAP-1665 will cause damage and void the warranty for this product.*

[1] The appearance of the external antennas may vary depending on the region.

Minimum Requirements

Network Requirements	• An Ethernet-based Network • IEEE 802.11ac/n/g/a wireless clients (AP/Repeater Mode) • IEEE 802.11ac/n/g/a wireless network (Client/Bridge/Repeater Mode) • 10/100/1000 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter or wireless adapter **Browser Requirements:** • Internet Explorer® 8.0 or higher • Firefox®20.0 or higher • Chrome™ 20.0 or higher • Safari® 4.0 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

The DAP-1665 Wireless AC1200 Dual Band Access Point gives you with the ability to transfer files with a maximum combined wireless signal rate of up to 1200 Mbps[1], delivering high-speed wireless network access for your home or office.

The DAP-1665 is compliant with the latest draft IEEE 802.11ac standard, meaning that it can connect with other 802.11ac compatible wireless client devices. It is also backward compatible with 802.11g and 802.11n devices. The AP (access point) can be configured to operate in five different modes: *Access Point, Wireless Client, Repeater, Bridge,* and *Bridge with AP Mode*.

The DAP-1665 features Wi-Fi Protected Access (WPA-PSK/WPA2-PSK), providing an enhanced level of security for wireless data communications. The AP also supports Wi-Fi Protected Setup (WPS), using either the PIN or Push Button method, for both *Repeater* and *Wireless Client Mode*.

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

Features

- **Faster Wireless Networking -** The DAP-1665 provides combined wireless speeds of up to 1200 Mbps[1] . This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Flexible Operation Modes -** The DAP-1665 can operate as an Access Point, Repeater, Wireless Client, Bridge and Bridge with AP, meaning that you can customize its operation to suit your specific networking requirements.

- **Gigabit Ethernet Port** - The built-in Gigabit Ethernet port facilitates a wired connection of up to 1 Gbps, meaning that wired devices can also take advantage of the DAP-1665's high-speed wireless capabilities.

- **Compatible with IEEE 802.11n, 802.11g, or 802.11a Devices -** The DAP-1665 is still fully compatible with the 802.11n/g/a standards, so it can connect with existing wireless adapters found on older devices.

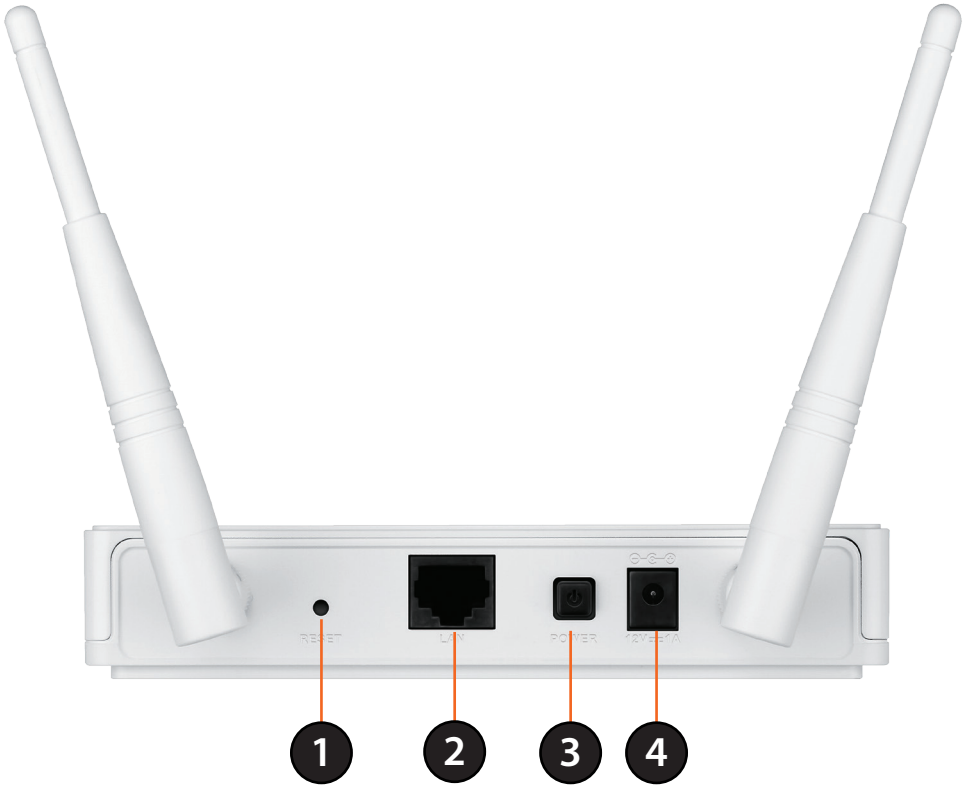
- **Robust Security -** For *Repeater Mode* and *Wireless Client Mode,* use WPS (Wi-Fi Protected Setup™) to create a secure connection to new devices in a matter of seconds by simply pushing a button or entering a PIN. There's also WPA/WPA2 security encryption, allowing you to customize your network's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

- **User-friendly Setup Wizard -** Through its easy-to-use web-based user interface, the DAP-1665 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server.

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

Hardware Overview

Connections



1	**Reset Button**	Use an unfolded paper clip to press and hold the reset button for 10 seconds. This will reset the DAP-1665 to its original factory default settings.
2	**LAN Port**	Connect an Ethernet-based device such as a computer, video game console, Network Attached Storage (NAS) device, or media player.
3	**Power Button**	Press the power button to power the device on and off.
4	**Power Receptor**	Plug the supplied power adapter into the power receptor.

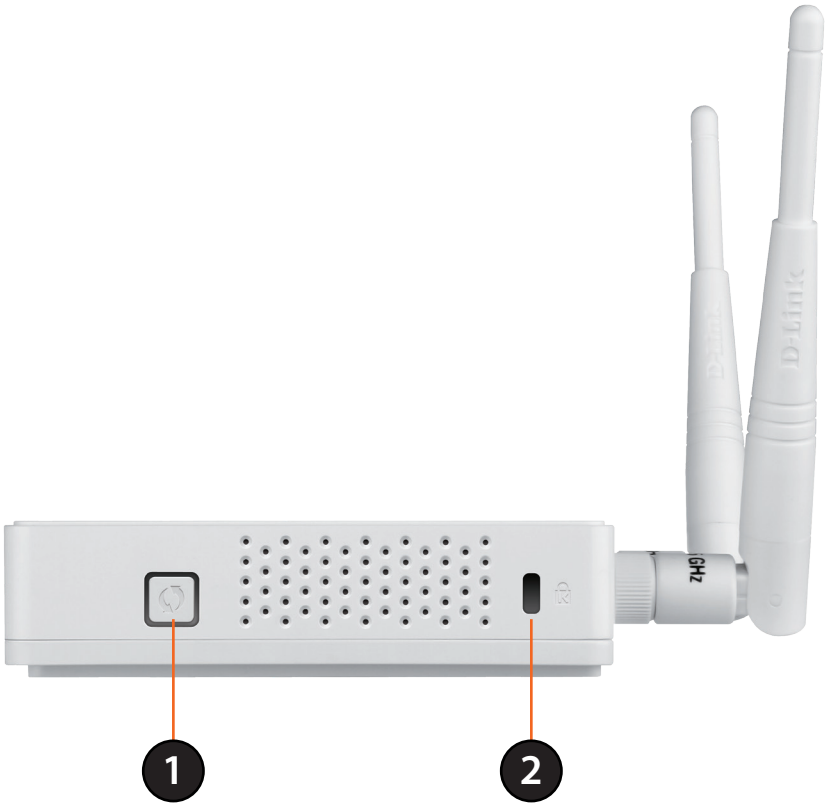
Hardware Overview

LEDs

1	**Power LED**	A solid green light indicates a proper connection to the power supply.
2	**2.4GHz Wireless LED**	A solid green light indicates that the 2.4 GHz wireless band is active. The light will be off during device reboot or if the wireless radio is disabled.
3	**5GHz Wireless LED**	A solid green light indicates that the 5 GHz wireless band is active. The light will be off during device reboot or if the wireless radio is disabled.
4	**LAN LED**	A solid green light indicates a connection to an Ethernet-enabled device.

Hardware Overview

WPS Button



1	**WPS Button**	Press this button to use WPS (Wi-Fi Protected Setup) to establish a secure connection with other wireless devices.
2	**Kensington Slot**	Connect a Kensington® lock device to protect your access point against theft.

Installation

You can simply connect a computer directly to the DAP-1665 with an Ethernet cable and then begin the configuration process. For *Access Point Mode*, you may use an Ethernet cable to connect the DAP-1665 to your wireless router. (Refer to "Access Point Mode Installation" on page 18.) You can also use WPS (Wi-Fi Protected Setup) for both the *Wireless Client Mode* and *Repeater Mode* if your router has WPS. (Refer to "Repeater or Wireless Client Mode Installation" on page 18.)

The next section describes the five function modes, and should help you decide which wireless mode to use. Then you can proceed with installation and configuration.

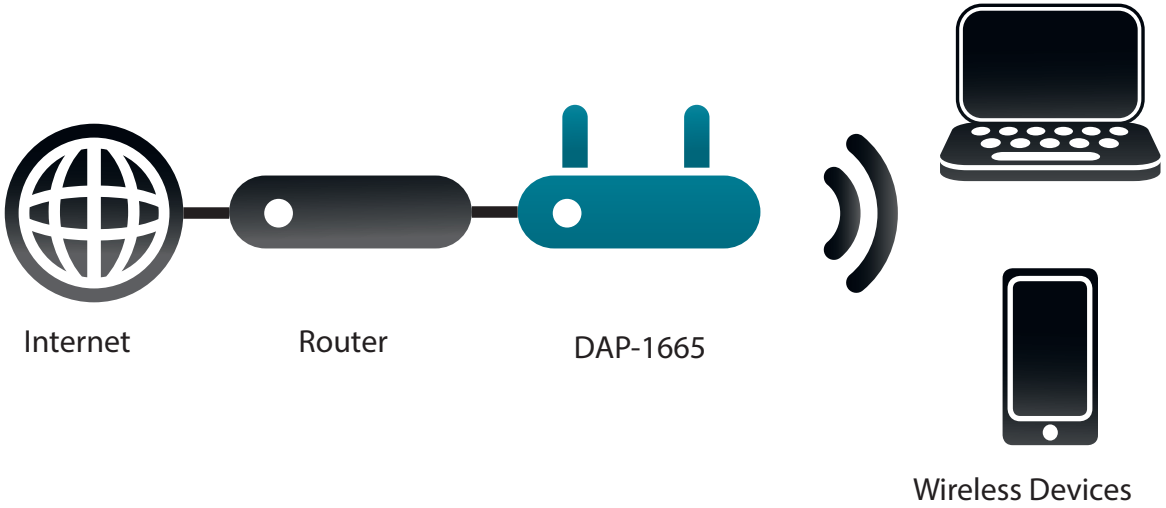
What Mode Should I Use?

The DAP-1665 gives you a choice of five operation modes, allowing you to customize the device to your networking requirements. Refer to the following sections to determine which mode is best for you.

Access Point Mode

Use *Access Point Mode* (default mode) if you want to connect wireless clients (such as laptops, tablets and smartphones) to your existing wired network. The DAP-1665 acts as a central connection point for any wireless client that has an 802.11ac or backward compatible 802.11n, g, or a wireless network interface and is within range of the AP (access point). From your wireless device, go to the **Wireless Utility**, and select the **Wi-Fi Network Name** (SSID) broadcast by the access point to wirelessly access the network. If wireless security is enabled on the AP, you must enter a password in order to connect to the Wi-Fi Network.

AP Mode

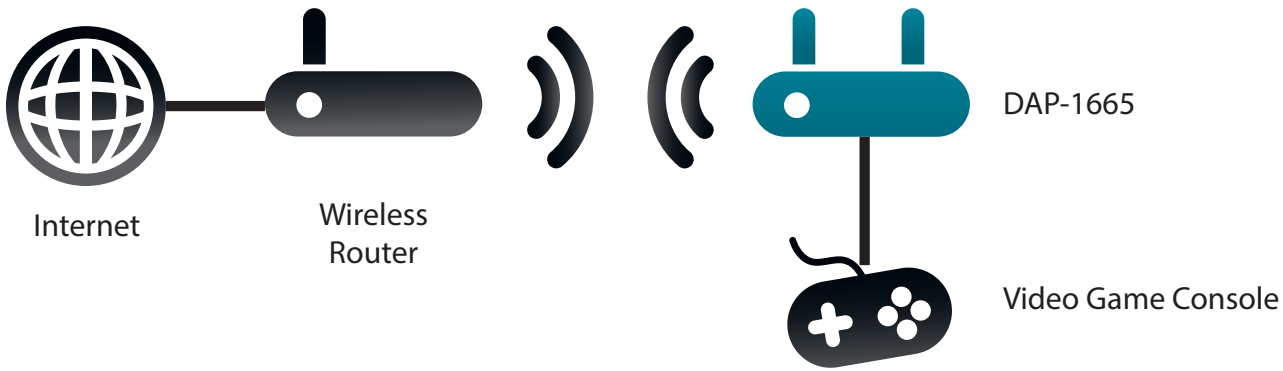


Wireless Client Mode

In *Wireless Client Mode*, the DAP-1665 acts as a wireless network adapter for an Ethernet-enabled device (such as a video game console, Network Attached Storage (NAS) device, or media player). Connect one Ethernet-enabled device to the AP using an Ethernet cable, and enjoy wired speeds of up to 1000 Mbps.

Example: Connect a video game console to the DAP-1665 using an Ethernet cable. Set the DAP-1665 to *Wireless Client Mode,* which will wirelessly connect to a wireless router on your network, providing Internet access to the video game console.

Client Mode

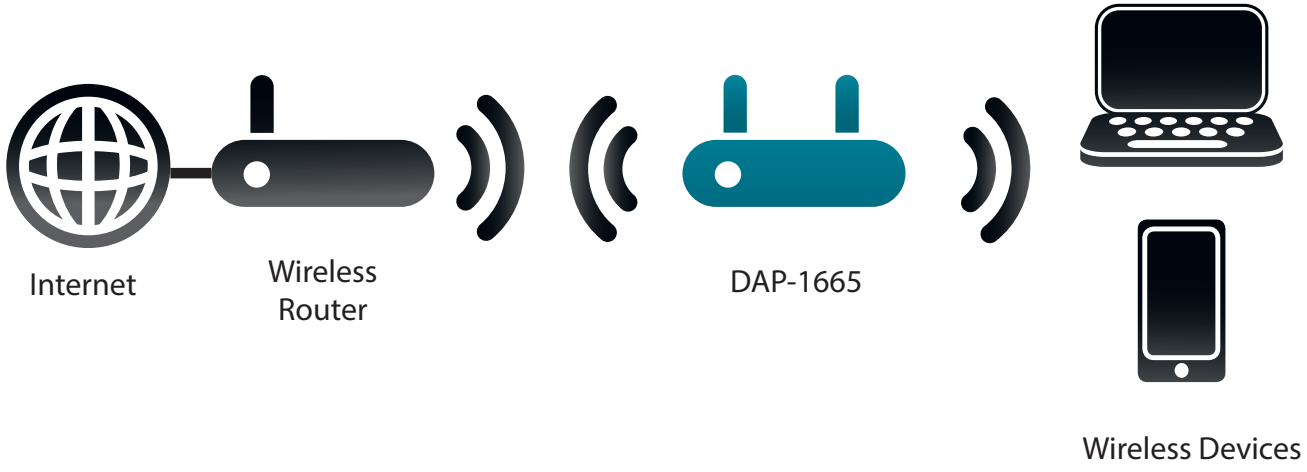


Note: *If you would like to connect multiple Ethernet-enabled devices to your DAP-1665, connect the LAN port of the DAP-1665 to an Ethernet switch, then connect your devices to this switch.*

Repeater Mode

Use the *Repeater Mode* to extend the wireless signal of your wireless router, increasing the range of your existing wireless network. The DAP-1665 will connect wirelessly to your wireless router or access point and will broadcast its signal to your wireless clients. The extended wireless network can use the same Wi-Fi Network Name (SSID) and security settings as the existing network, or you can choose to specify a new network name and security method.

Repeater Mode



Note: *For best performance, place your DAP-1665 in between your router and your dead zone, making sure it's placed in a location where the signal is still strong.*

Bridge Mode

In *Bridge Mode*, the DAP-1665 creates a wireless link between two separate existing networks, enabling data to be shared between the two networks without the need for a physical connection. The two networks must be within wireless range of one another in order for bridge mode to be effective.

Note: *Bridge mode is not specified in the Wi-Fi or IEEE standards. This mode will only work using two DAP-1665 units. Compatibility with other APs (even other D-Link APs) is not guaranteed.*

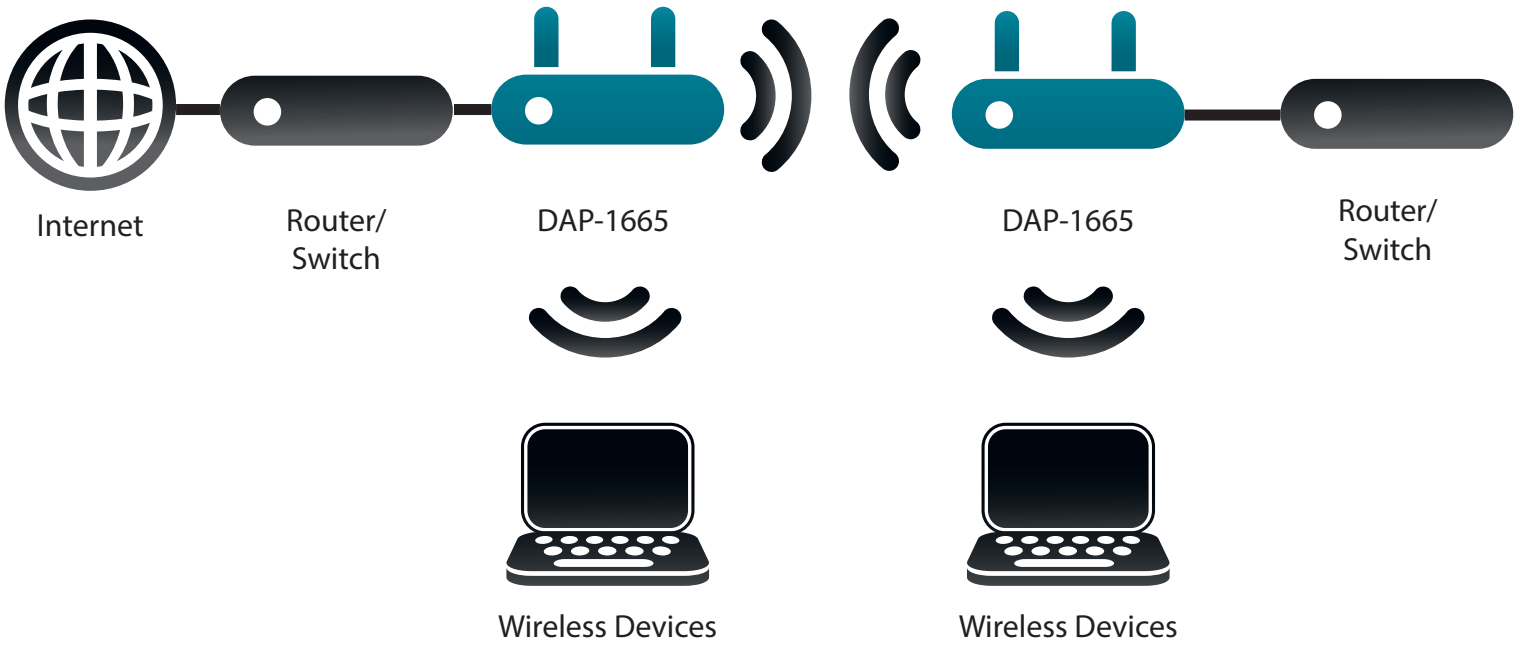
Bridge Mode

Bridge with AP Mode

Bridge with AP Mode is very similar to *Bridge Mode*, with the added functionality of *Access Point Mode*, meaning that wireless clients can connect to one of the DAP-1665s and have access to both networks via the wireless bridge.

Note: *The Bridge with AP mode is not specified in the Wi-Fi or IEEE standards. This mode will only work using two DAP-1665 units. Compatibility with other APs (even other D-Link APs) is not guaranteed.*

Bridge with AP Mode



Wireless Installation Considerations

The DAP-1665 wireless access point lets you access your network using a wireless connection from virtually anywhere within the operating range of the device. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

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

2. Be aware of the direct line between network devices. At a 45-degree angle, a wall that is 1.5 feet thick (0.5 meters), appears to be almost three feet (1 meter) thick. At a 2-degree angle, that wall appears to be over 42 feet (14 meters) thick! For better reception, always position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle).

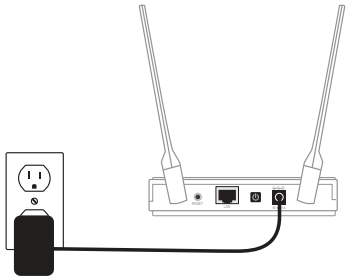
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, 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.

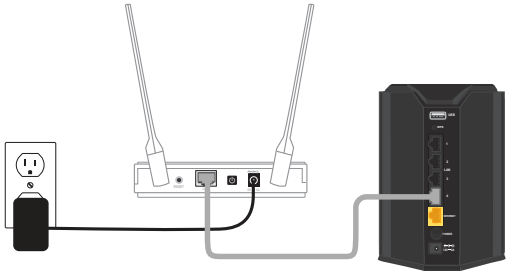
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may also be affected. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if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

Access Point Mode Installation

1. Plug the supplied power adapter into your DAP-1665 and connect it to the outlet or surge protector. Press the **Power** button on the back of the device. Verify that the Power LED is lit.

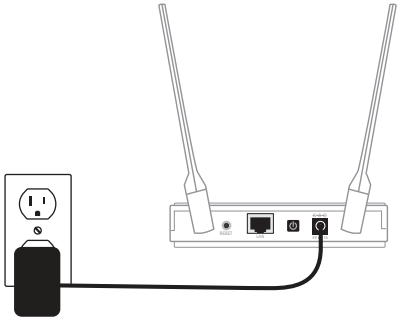


2. Attach one end of the included Ethernet cable to the LAN port on the back of the DAP-1665, and the other end into the Ethernet port on your wireless router.



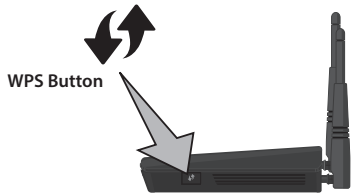
Repeater or Wireless Client Mode Installation

1. Find an available power outlet near your wireless router. Plug the supplied power adapter into your DAP-1665 and connect it to the outlet or to a surge protector. Press the **Power** button on the back of the device. Verify that the Power LED is lit.



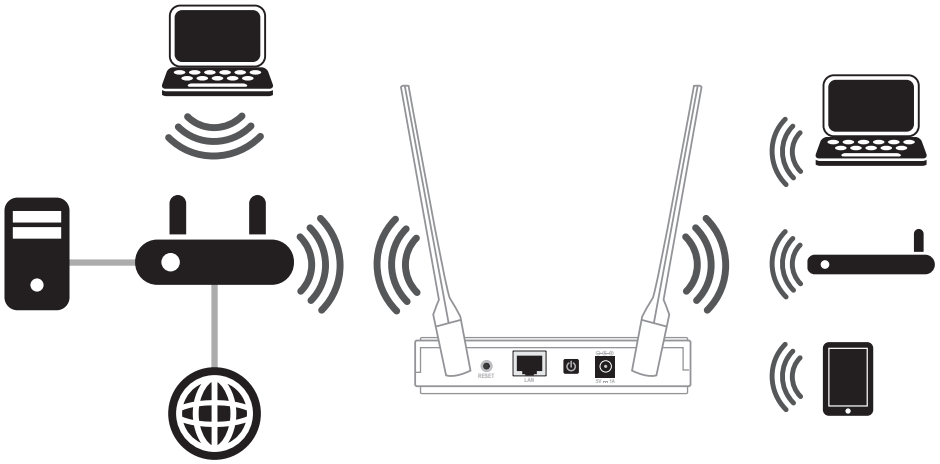
2 Press the **WPS** button on your existing wireless router or AP.

Note: Usually *the WPS LED on your router will start to blink. If necessary, check your router's user manual for more information.*

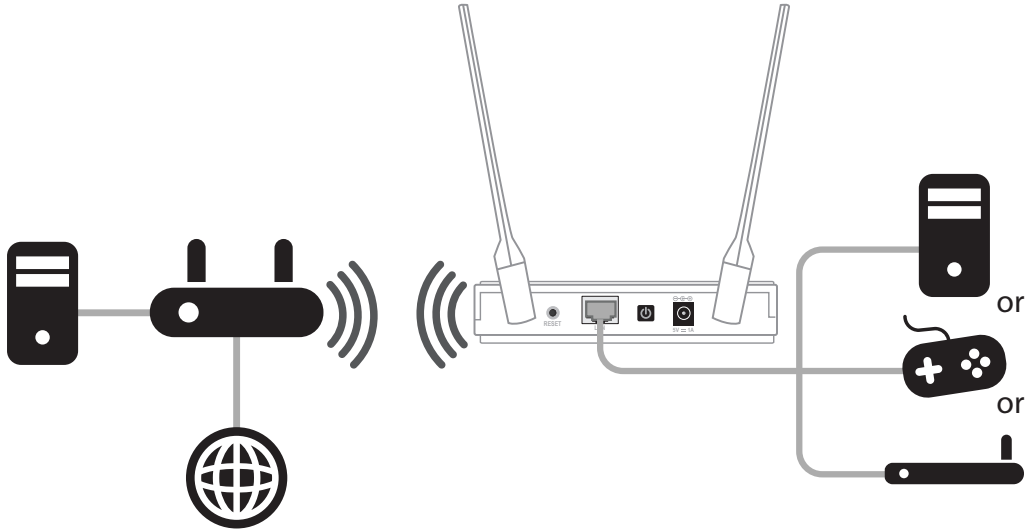


3 Within one minute, press and hold the **WPS** button on the side of the DAP-1665 for a minimum of one second. The WPS LED will blink. When the Security LED becomes a solid green, it means wireless security is enabled. Allow up to two minutes for the WPS process to complete.

Note: *For optimal performance using* ***Repeater Mode****, place your DAP-1665 in between your router and your dead zone, making sure it's placed in a location where the signal is still strong.*



Note: *Final installation step for* ***Wireless Client Mode*** *-- You can connect one Ethernet-enabled device to the AP using an Ethernet cable.*



Configuration

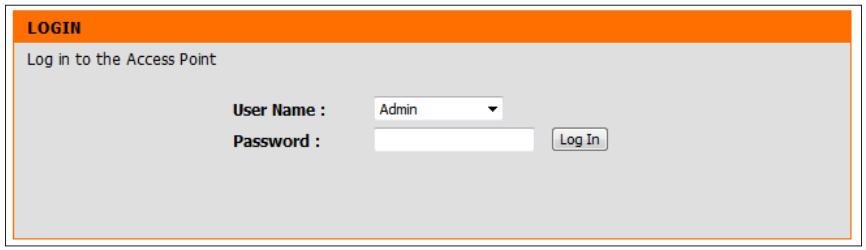
This section explains how to configure your D-Link wireless access point using the web-based configuration utility. The *Wireless Setup Wizard* will allow you to select either **Access Point**, **Wireless Client**, or **Repeater** for your preferred *Wireless Mode*. (Refer to "Wireless Setup Wizard" on page 22.) You must use Manual Configuration to set up your DAP-1665 in **Bridge Mode** or **Bridge with AP Mode**. Go to **Setup** > **Wireless Settings**. (Refer to "Manual Configuration" on page 33.)

Web-based Configuration Utility

From the computer connected to your router, open a web browser such as Internet Explorer, Firefox, Safari, or Chrome, and enter **http://dlinkap.local./**. Windows XP users can enter **http://dlinkap** in the address field.*

Select **Admin** for the **User Name** from the drop-down menu. Leave the password blank by default. Click **Log In**.

If you see an error message, *Page Cannot be Displayed*, refer to "Troubleshooting" on page 91.

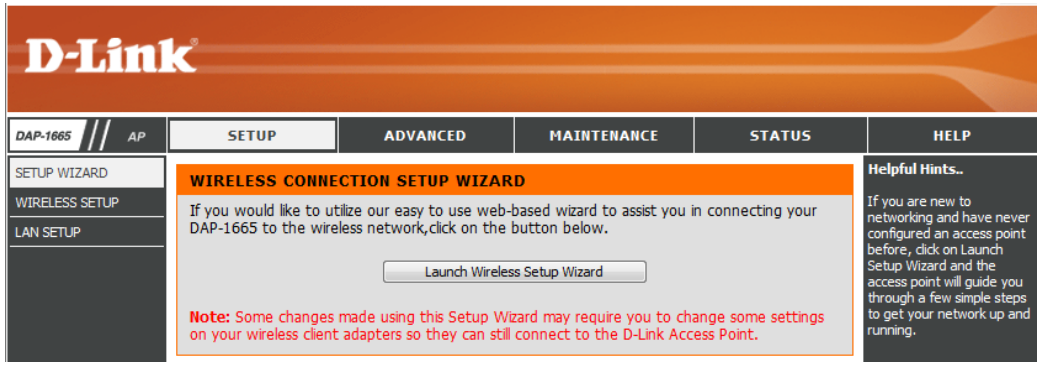


** **Note:** The default IP address is 192.168.0.50. Once the DAP-1665 (in Repeater or Client mode) connects to your router, it will get assigned a new IP address based on your router/network's DHCP settings. You will need to log in to your router and view the DHCP table to see what IP address was assigned to the DAP-1665. The MAC address is printed on the label on the bottom of the AP.*

Wireless Setup Wizard

Click **Launch Wireless Setup Wizard** to configure your DAP-1665 in *Access Point*, *Wireless Client*, or *Repeater* mode.

If you would like to configure the device in *Bridge* or *Bridge with AP* mode, skip to "Manual Configuration" on page 33.

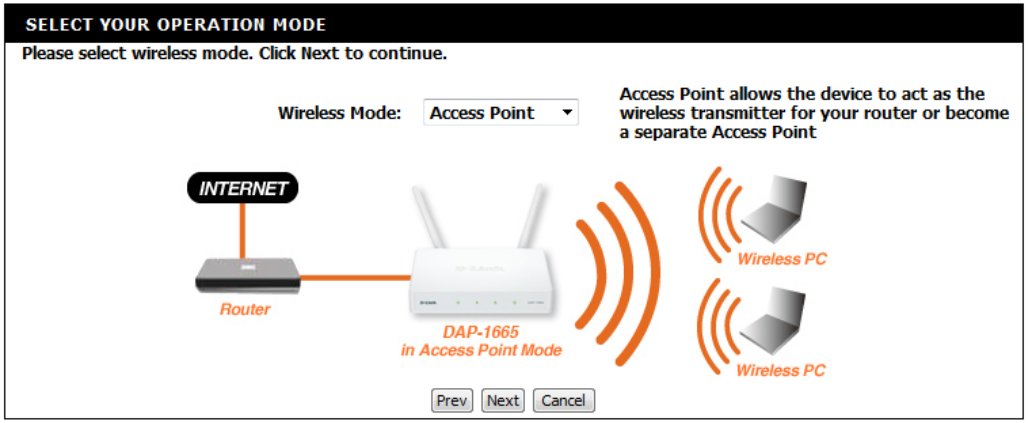


You will see the *Wi-Fi Connection Setup Wizard* screen. Click **Next** to continue.

Access Point Mode

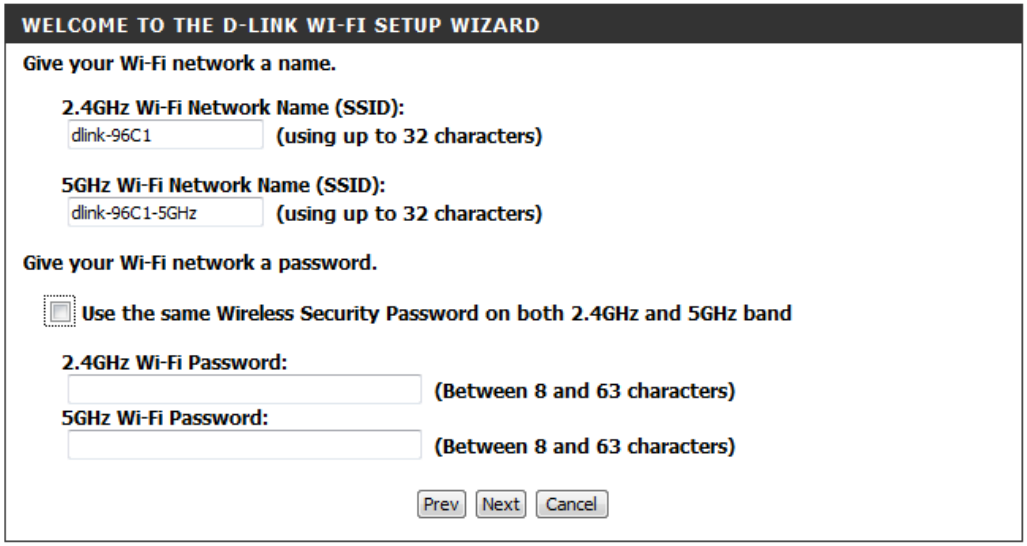
The *Wi-Fi Connection Setup Wizard* will assist you in configuring your DAP-1665 as an access point, allowing you to connect wireless clients to your wired network. The DAP-1665 can act as the wireless transmitter for your router or become a separate access point to expand your network.

Select **Access Point** from the drop-down menu. Click **Next** to continue.



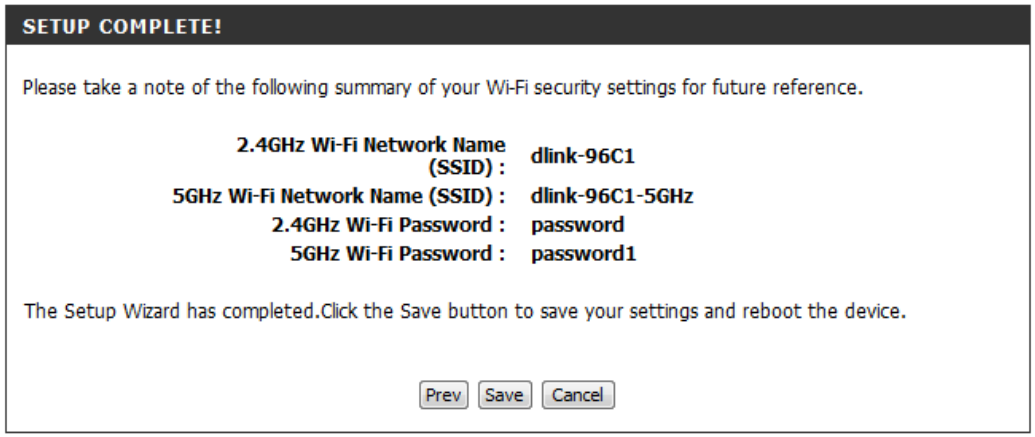
This screen will allow you to set a **Wi-Fi Network Name** (SSID) and **Wi-Fi Password** for your wireless network. Specify an SSID for both the 2.4GHz and 5GHz bands. If you wish to use the same wireless security password for both networks, check the box by the words, **Use the same Wireless Security Password on both**...and enter a single password in the field provided. If you wish to use a different password for each network, leave the box unchecked and enter passwords in the **2.4GHz Wi-Fi Password** and **5GHz Wi-Fi Password** fields.

Click **Next** to continue.



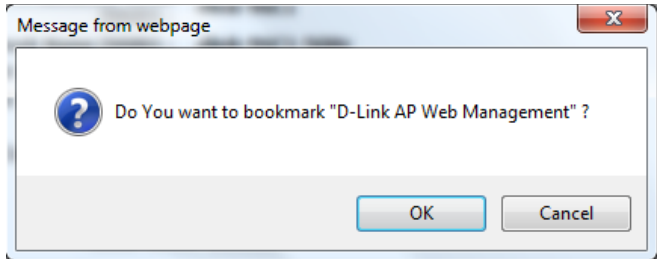
You will see a summary page, showing the current settings for your 2.4GHz and 5GHz wireless networks. Make a note of this information for future reference.

Click **Save** to save your network settings and reboot the AP.



A dialog box will appear, offering you the opportunity to save the address for the web-based configuration utility in your browser's bookmarks. Click **OK** to save or click **Cancel** to continue without saving a bookmark.

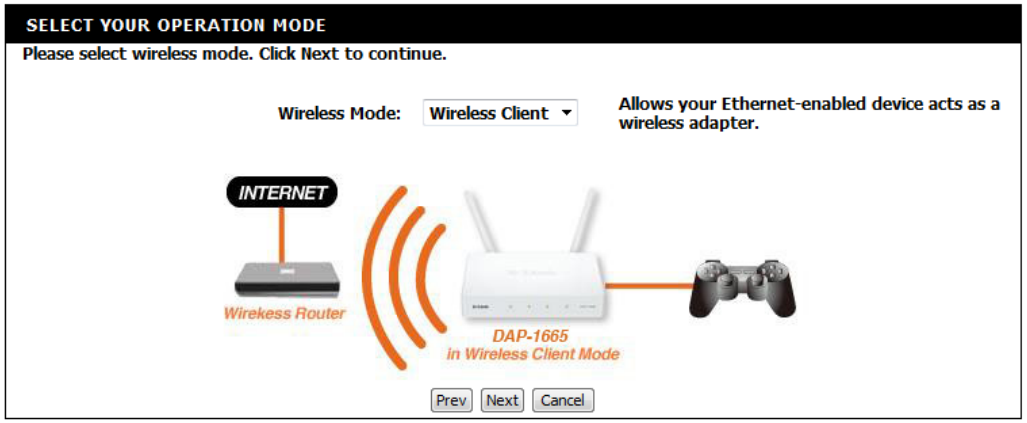
In order for your network settings to take effect AP will reboot automatically.



Wireless Client Mode

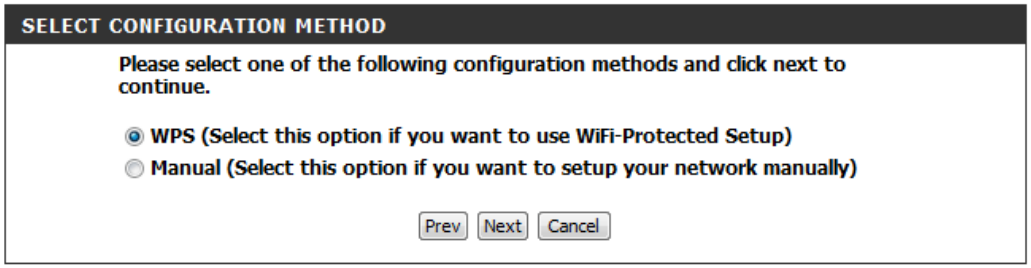
The *Wi-Fi Setup Wizard* will assist you in configuring your DAP-1665 as a wireless client. Then you will be able to connect an Ethernet-based device to your existing wireless network.

Select **Wireless Client** from the drop-down menu.

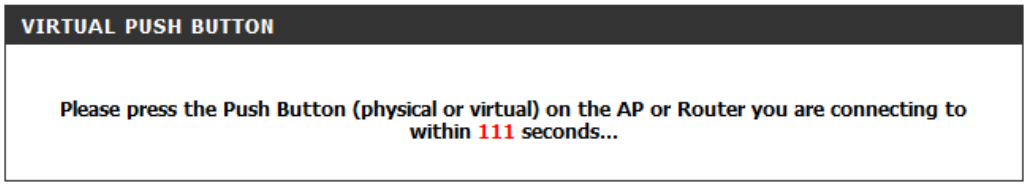


Select **WPS** as the configuration method only if your wireless device supports Wi-Fi Protected Setup (WPS). Otherwise, select **Manual** and, skip to page 27 for instructions.

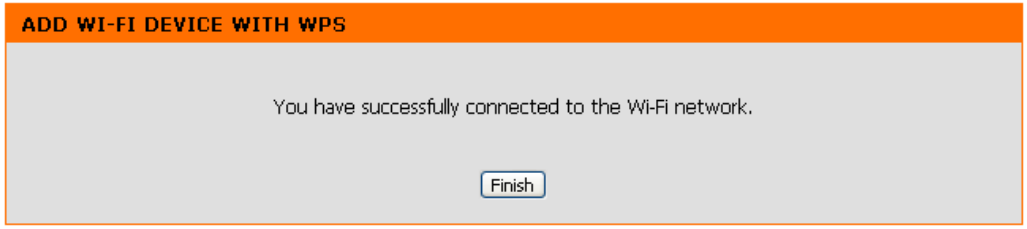
Click **Next** to continue.



Press the **WPS** button on your wireless router with 120 seconds to complete the WPS setup process.



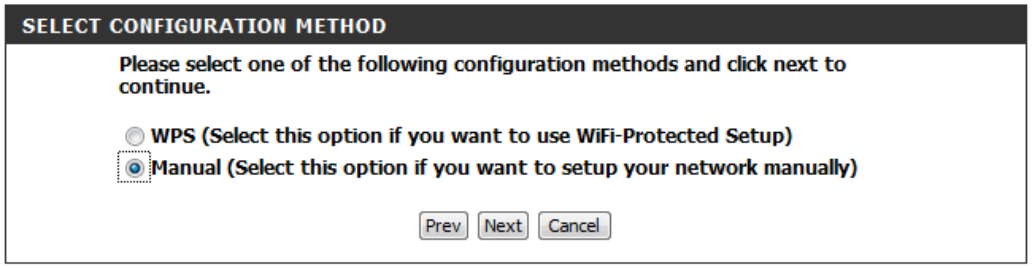
You will see a message that says a connection has been successfully made. Click **Finish** to complete the setup process.



Note: *If the connection was not successful, you will see a message that says the connection failed. Click* ***Retry*** *to try again, or* ***Cancel*** *to discontinue.*

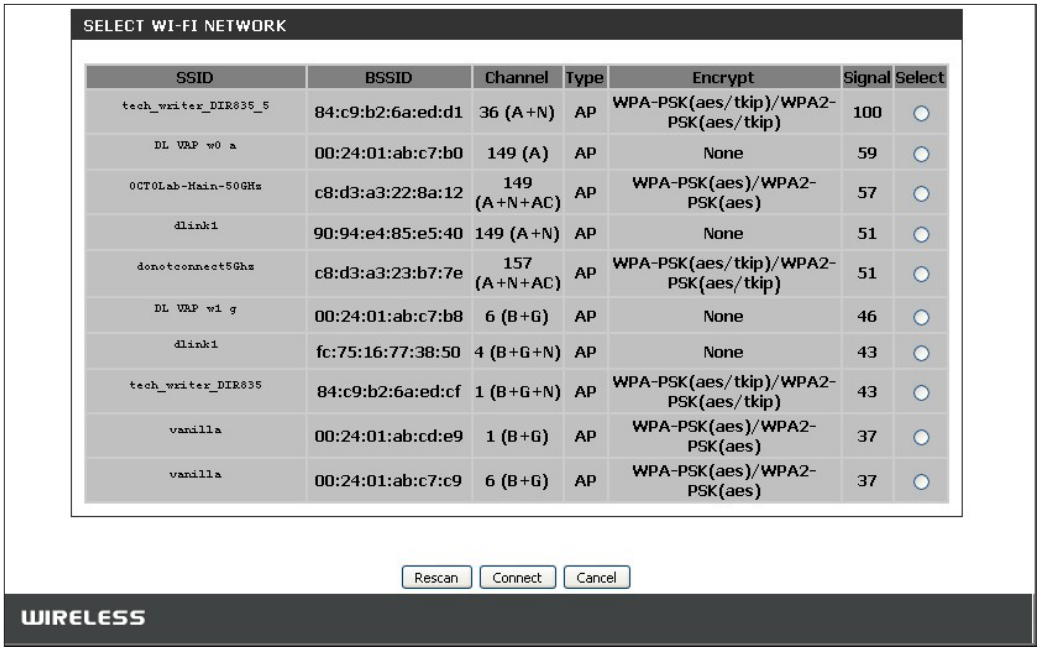
Select **Manual** configuration to setup your network manually.

Click **Next** to continue. The DAP-1665 will scan for available wireless networks in your area.



You will see a list of available wireless networks. Locate the **SSID** of the wireless network that you wish to connect to from the list. Select it by clicking on the corresponding radio button in the **Select** column.

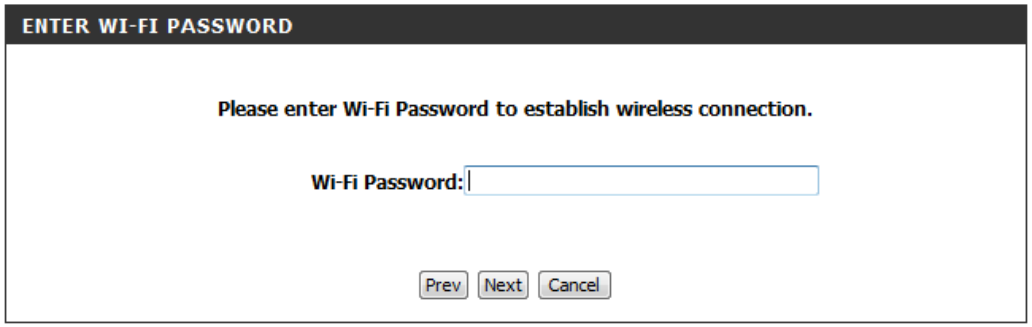
Click **Connect** at the bottom of the page to continue. If you do not see your network in the list, click **Rescan** to search again.



SSID	BSSID	Channel	Type	Encrypt	Signal	Select
tech_writer_DIR835_5	84:c9:b2:6a:ed:d1	36 (A+N)	AP	WPA-PSK(aes/tkip)/WPA2-PSK(aes/tkip)	100	
DL VAP w0 a	00:24:01:ab:c7:b0	149 (A)	AP	None	59	
OCTOLab-Main-50GHz	c8:d3:a3:22:8a:12	149 (A+N+AC)	AP	WPA-PSK(aes)/WPA2-PSK(aes)	57	
dlink1	90:94:e4:85:e5:40	149 (A+N)	AP	None	51	
donotconnect5Ghz	c8:d3:a3:23:b7:7e	157 (A+N+AC)	AP	WPA-PSK(aes/tkip)/WPA2-PSK(aes/tkip)	51	
DL VAP w1 g	00:24:01:ab:c7:b8	6 (B+G)	AP	None	46	
dlink1	fc:75:16:77:38:50	4 (B+G+N)	AP	None	43	
tech_writer_DIR835	84:c9:b2:6a:ed:cf	1 (B+G+N)	AP	WPA-PSK(aes/tkip)/WPA2-PSK(aes/tkip)	43	
vanilla	00:24:01:ab:cd:e9	1 (B+G)	AP	WPA-PSK(aes)/WPA2-PSK(aes)	37	
vanilla	00:24:01:ab:c7:c9	6 (B+G)	AP	WPA-PSK(aes)/WPA2-PSK(aes)	37	

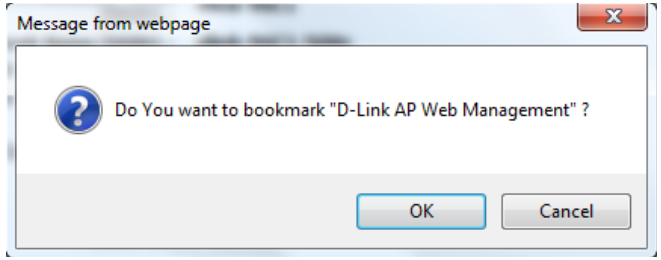
If the existing wireless network is password-protected, enter the **Wi-Fi Password**.

Click **Next** to continue.



A dialog box will appear offering you the opportunity to save the address for the web-based configuration utility in your browser's bookmarks. Click **OK** to save or click **Cancel** to continue without saving a bookmark.

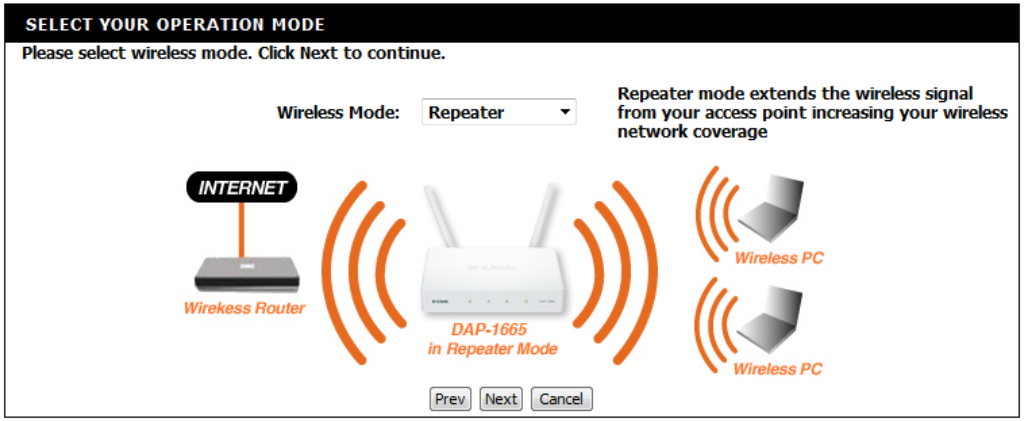
In order for your network settings to take effect AP will reboot automatically.



Repeater Mode

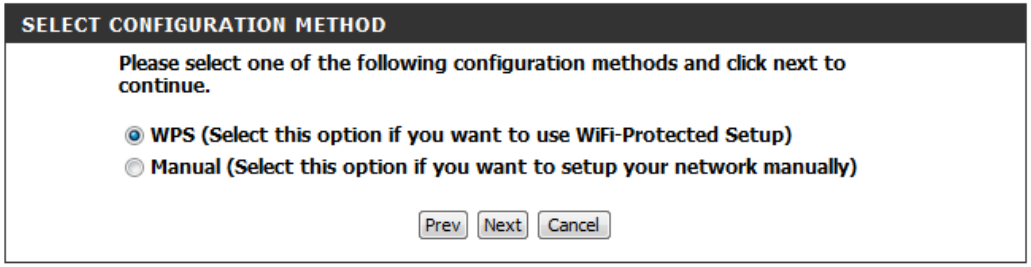
The *Wi-Fi Setup Wizard* will assist you in configuring your DAP-1665 as a repeater to extend the range of your existing wireless network.

Select **Repeater** from the drop-down menu.

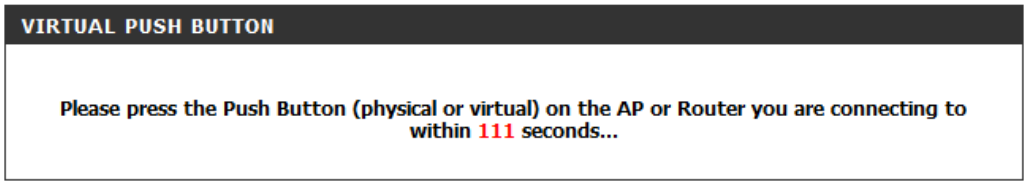


Select **WPS** as the configuration method only if your wireless device supports Wi-Fi Protected Setup (WPS). Otherwise, for **Manual** setup, skip to page 31.

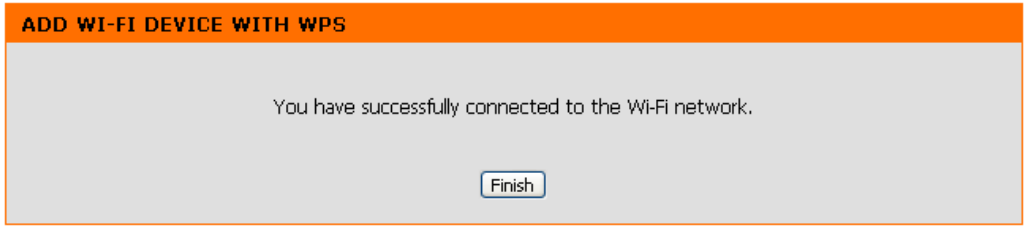
Click **Next** to continue.



Press the **WPS** Button on your existing wireless router with 120 seconds to complete the WPS setup process.



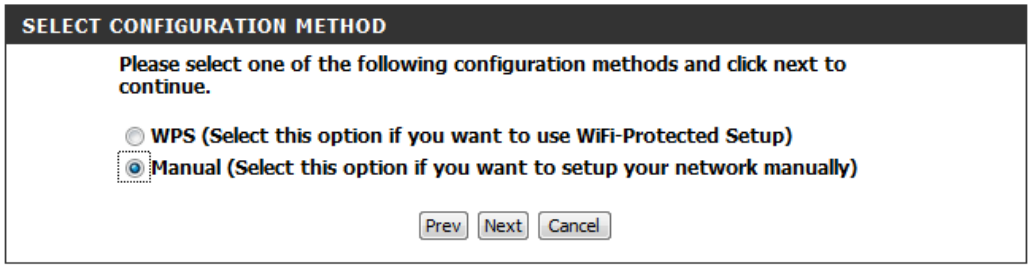
You will see a message that says a connection has been successfully made. Click **Finish** to complete the setup process.



Note: *If the connection was not successful, you will see a message that says the connection failed. Click* ***Retry*** *to try again, or* ***Cancel*** *to discontinue.*

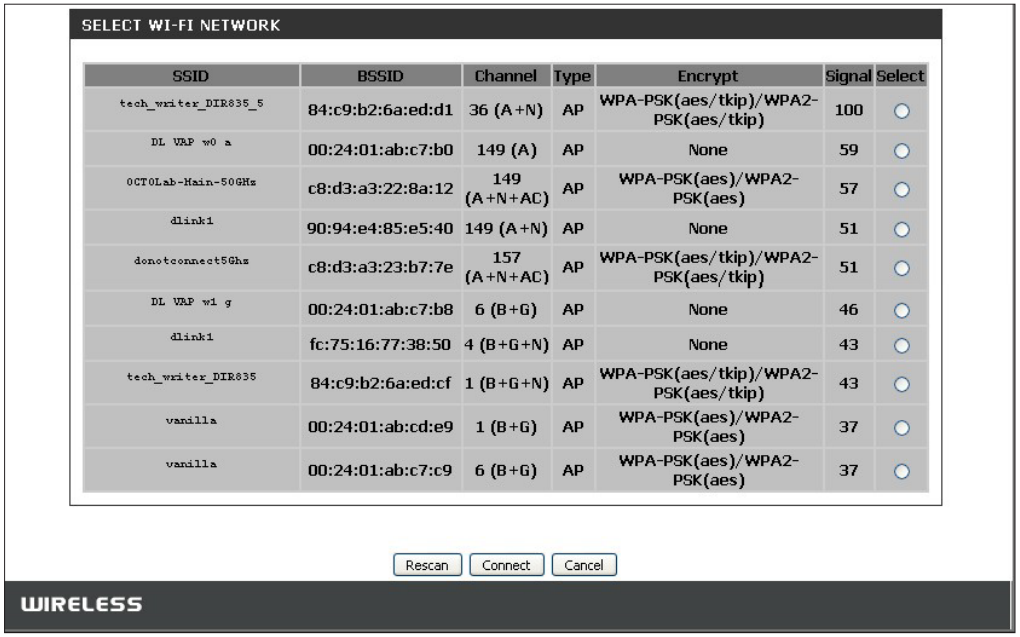
Select **Manual** configuration to setup your network manually.

Click **Next** to continue. The DAP-1665 will scan for available wireless networks in your area.



You will see a list of available wireless networks. Find the **SSID** of the wireless network that you wish to connect to from the list. Select it by clicking on the corresponding radio button in the **Select** column.

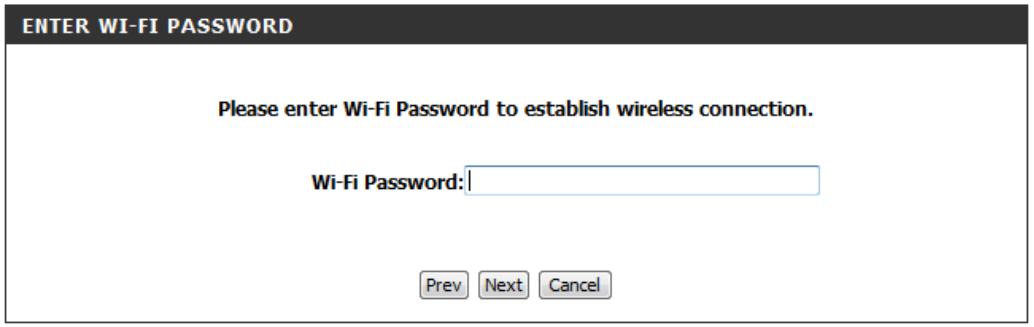
Click **Connect** at the bottom of the page to continue. If you do not see your network in the list, click **Rescan** to search again.



SSID	BSSID	Channel	Type	Encrypt	Signal	Select
tech_writer_DIR835_5	84:c9:b2:6a:ed:d1	36 (A+N)	AP	WPA-PSK(aes/tkip)/WPA2-PSK(aes/tkip)	100	
DL VAP w0 a	00:24:01:ab:c7:b0	149 (A)	AP	None	59	
OCTOLab-Main-50GHz	c8:d3:a3:22:8a:12	149 (A+N+AC)	AP	WPA-PSK(aes)/WPA2-PSK(aes)	57	
dlink1	90:94:e4:85:e5:40	149 (A+N)	AP	None	51	
donotconnect5Ghz	c8:d3:a3:23:b7:7e	157 (A+N+AC)	AP	WPA-PSK(aes/tkip)/WPA2-PSK(aes/tkip)	51	
DL VAP w1 g	00:24:01:ab:c7:b8	6 (B+G)	AP	None	46	
dlink1	fc:75:16:77:38:50	4 (B+G+N)	AP	None	43	
tech_writer_DIR835	84:c9:b2:6a:ed:cf	1 (B+G+N)	AP	WPA-PSK(aes/tkip)/WPA2-PSK(aes/tkip)	43	
vanilla	00:24:01:ab:cd:e9	1 (B+G)	AP	WPA-PSK(aes)/WPA2-PSK(aes)	37	
vanilla	00:24:01:ab:c7:c9	6 (B+G)	AP	WPA-PSK(aes)/WPA2-PSK(aes)	37	

If the existing wireless network is password-protected, enter the **Wi-Fi Password** in the field provided.

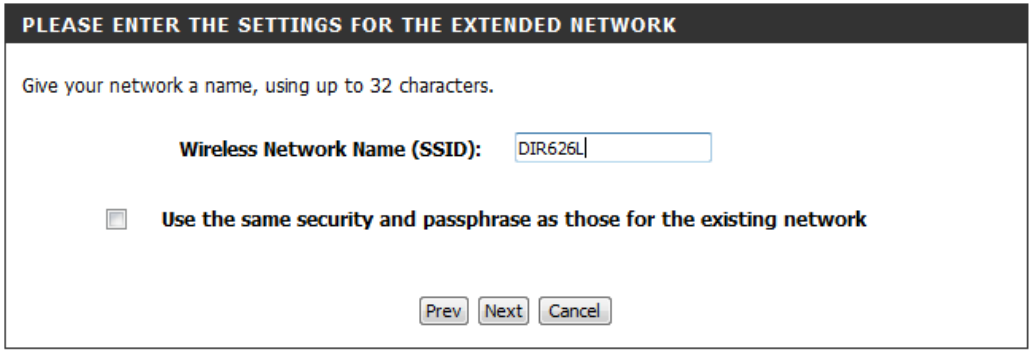
Click **Next** to continue.



By default, the **Wireless Network Name (SSID)** field will display the same network name as the source network. If you wish to specify a different name for the extended network, enter it in the field provided.

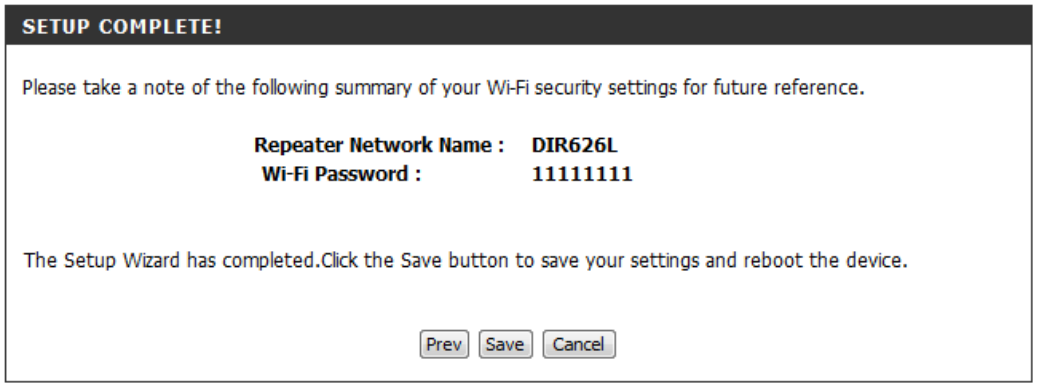
If you wish to use the same network name, check the box below. The security password will be the same as that of the source network, regardless of whether or not the network name is the same.

Click **Next** to continue.



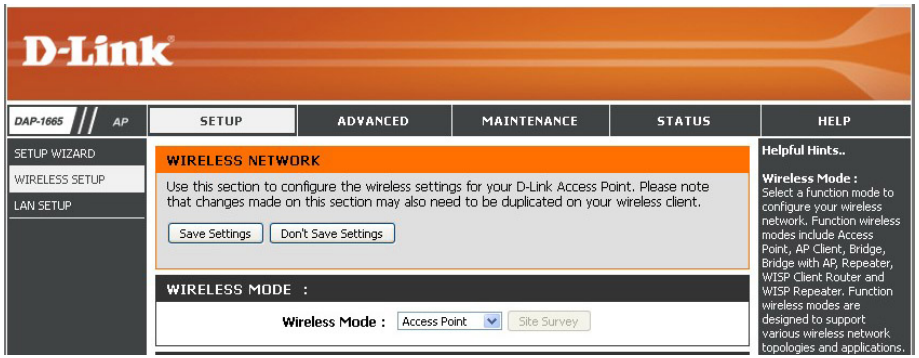
A summary page will be displayed showing the **Repeater Network Name** and **Wi-Fi Password** for the extended network. Make a note of this information for future reference.

Click **Save** to save the configuration.



Manual Configuration
Wireless Settings

Configure your DAP-1665 manually from the web-based configuration utility by navigating to **Setup** > **Wireless Setup**. Refer to the following pages for detailed instructions on how to manually configure the DAP-1665 after selecting the **Wireless Mode** that you prefer.



Access Point Mode

2.4GHz Band

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

Enable Wireless: Check the box to **Enable** the wireless function for the **2.4GHz** band. You may uncheck the box to disable all wireless functions. If wireless is enabled, you may also set up a specific schedule. Select a schedule from the drop-down menu or click **Add New** to create a new schedule. The schedule is set to **Always** by default.

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

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

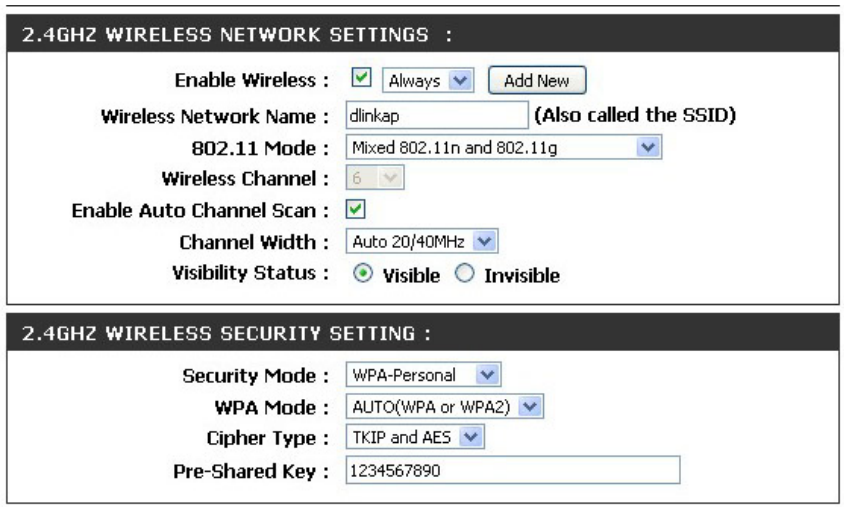
Wireless Channel: Indicates the channel setting for the DAP-1665. The Channel can be changed to the channel setting for an existing wireless network or to reduce interference in congested areas. If **Auto Channel Scan** is enabled, this option will not be available.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan.** This will allow the DAP-1665 to automatically choose the channel with the least amount of interference.

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

Visibility Status: Select whether you would like the network name (SSID) of your wireless network to be **Visible** or **Invisible**. If **Invisible**, the SSID of the DAP-1665 will not be shown by Site Survey utilities. Therefore, the SSID will have to be manually entered so wireless clients can connect.

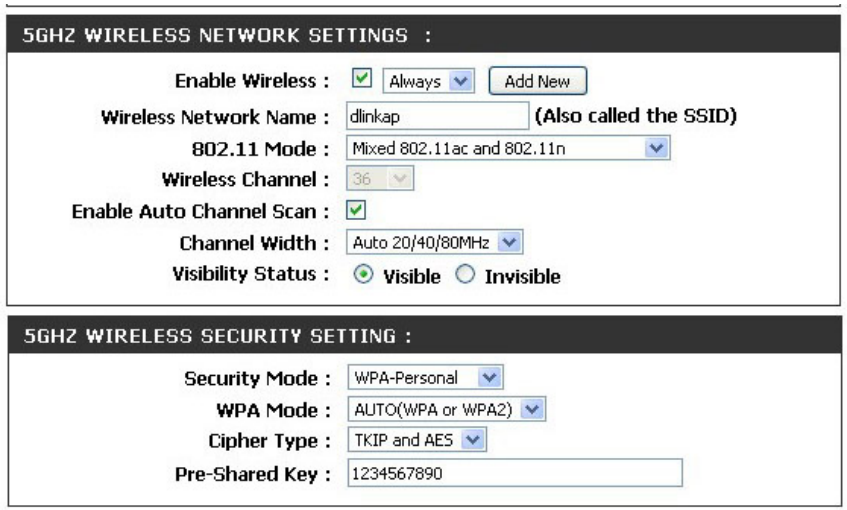
Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 46.



5GHz Band

Enable Wireless: Check the box to **Enable** the wireless function for the **5GHz** band. You may uncheck the box to disable all wireless functions. If wireless is enabled, you may also set up a specific schedule. Select a schedule from the drop-down menu or click **Add New** to create a new schedule. The schedule is set to **Always** by default.

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



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

Wireless Channel: Indicates the channel setting for the DAP-1665. The channel can be changed to the channel setting for an existing wireless network or to reduce interference in congested areas. If **Auto Channel Scan** is enabled, this option will not be available.

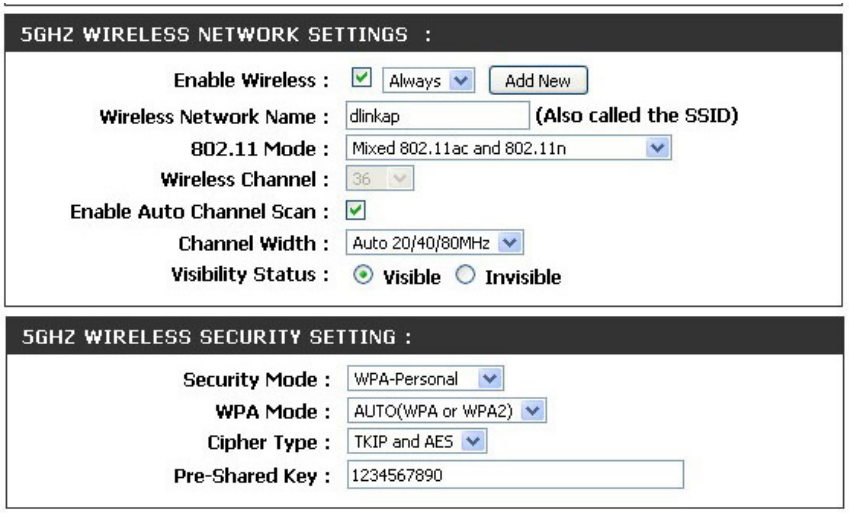
Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan.** This will allow the DAP-1665 to automatically choose the channel with the least amount of interference.

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

Visibility Status: Select whether you would like the network name (SSID) of your wireless network to be **Visible** or **Invisible**. If **Invisible**, the SSID of the DAP-1665 will not be shown by Site Survey utilities. Therefore, the SSID will have to be manually entered so wireless clients can connect.

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 46.

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



Wireless Client Mode

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

Site Survey: Click **Site Survey** to display a list of available wireless networks in your area. To select a wireless network, click the radio button in the far right column of the scan page. Click **Connect** at the bottom of the scan page to confirm the selection. The wireless network name will automatically appear in the *Wireless Network Name* field below.

Wireless Network Name: If you did not use the **Site Survey** option described above, enter the **Network Name** (SSID) of the wireless network that you wish to connect to. You can also click **Site Survey** and select an available **Network Name** from the list.

802.11 Band: Select **2.4GHz** or **5GHz** for the wireless band corresponding to the wireless network that you wish to connect to. You can only be connected to one wireless band at any time.

Channel Width: Select the **Channel Width** that you wish to use when connecting to the wireless network.

Security Mode: Select the wireless security mode used by the network you are connecting to. For more information regarding wireless security, please refer to "Configuring Wireless Security" on page 46.

Wireless MAC Clone: Check the box to **Enable** the cloning of another device's MAC address by the DAP-1665.

Wi-Fi Protected Setup: Check the box to **Enable** the use of *Wi-Fi Protected Setup* (WPS) for *Wireless Client Mode*.

Current PIN: Displays the *Current PIN* which can be used to connect to the router using the WPS-PIN method.

Click **Reset PIN to Default** to reset the PIN number to the factory default settings. Click **Generate New PIN** to randomly generate a new PIN for WPS connection. Click **Process WPS** to begin the WPS Push-Button setup process.

Click **Save Settings** to save the current configuration.

Bridge Mode

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

Bridge Band: Select the **Bridge Band** that you would like to use for the wireless bridge:
2.4GHz - The bridge can function using 802.11n or 802.11g.
5GHz - The bridge can function using 802.11ac, 802.11n, or 802.11a.

802.11 Mode: Select the **802.11 Mode** from the drop-down menu, based on which 802.11 standard you want the bridge to use.

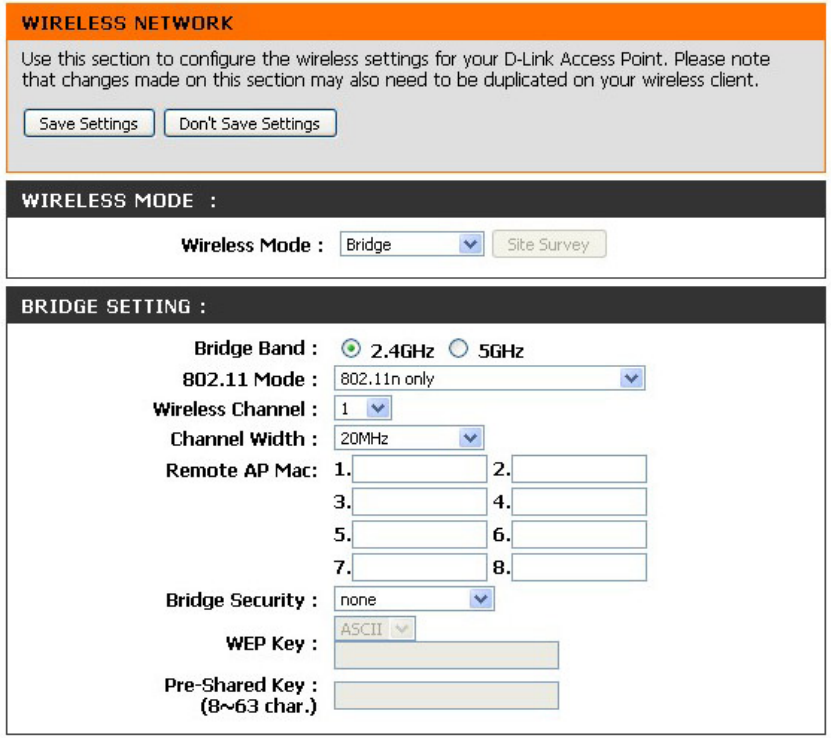
Wireless Channel: Select the **Wireless Channel** that you want the bridge to use. All access points (APs) on the bridge must be using the same wireless channel.

Channel Width: Select the appropriate **Channel Width**, either **20MHz** or **Auto 20/40MHz** from the drop-down menu. When you are using the 5GHz band, the **Auto 20/40/80MHz** option will also be available.

Remote AP MAC: Enter the MAC address for each of the APs in your network that will serve as bridges in order to wirelessly connect multiple networks.

Bridge Security: Select the desired security method from the drop-down menu. If you select **WEP**, you should also select the type of characters to be used for the WEP key, **ASCII** or **Hex**, from the drop-down menu. Then enter the **WEP Key** in the field provided. If you select **WPA**, you should enter a **Pre-Shared Key** (password) in the field below. Regardless of the security mode selected, the settings should be the same on all APs within the bridge. For further information regarding wireless security, please refer to "Configuring Wireless Security" on page 46.

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



Note: *The Bridge Mode is not completely specified in the Wi-Fi or IEEE standards. This mode will work with other DAP-1665 units. Communication with other APs (even other D-Link APs) is not guaranteed.*

Bridge with AP Mode

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

Bridge Band: Select the **Bridge Band** that you would like to use for the wireless bridge:
2.4GHz - The bridge can function using 802.11n or 802.11g.
5GHz - The bridge can function using 802.11ac, 802.11n, or 802.11a.

802.11 Mode: Select the appropriate **802.11 Mode** from the drop-down menu, depending on which 802.11 standard you want the bridge to use.

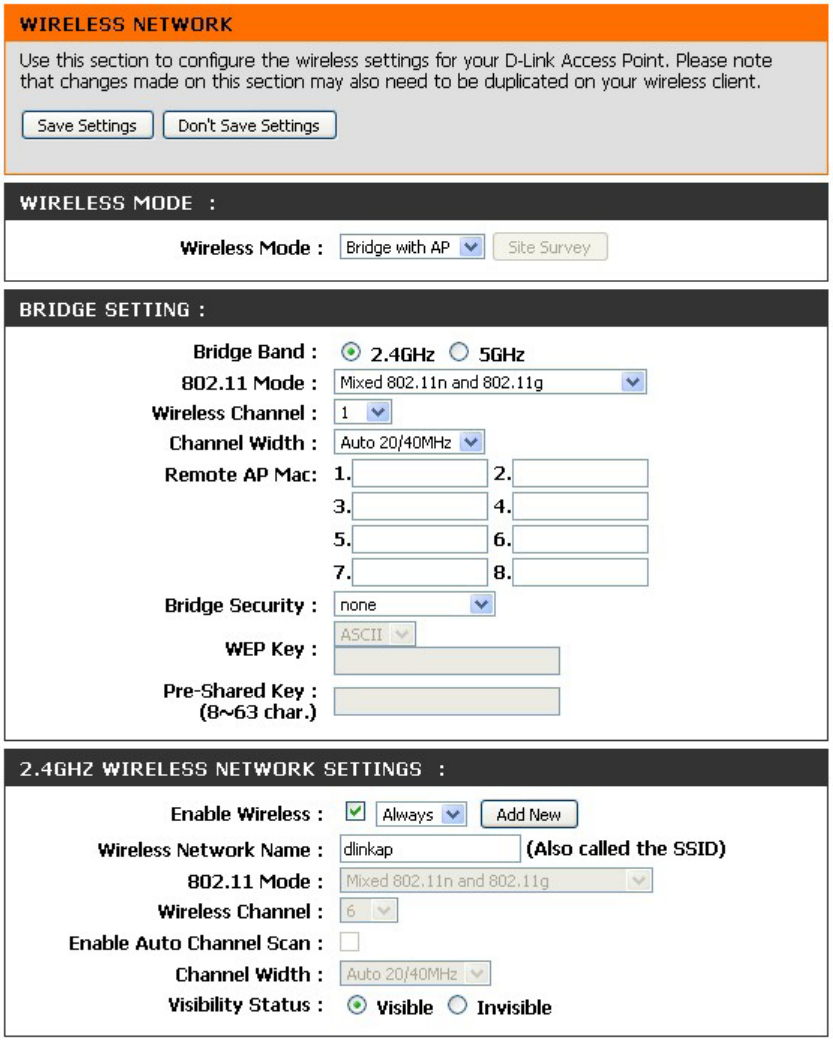
Wireless Channel: Select the **Wireless Channel** that you want the bridge to use. All access points (APs) on the bridge must be using the same wireless channel.

Channel Width: Select the appropriate **Channel Width**, either **20MHz** or **Auto 20/40MHz**, from the drop-down menu. When you are using the 5GHz band, the **Auto 20/40/80MHz** option will also be available.

Remote AP MAC: Enter the MAC address for each of the APs in your network that will serve as bridges in order to wirelessly connect multiple networks.

Bridge Security: Select the desired security method from the drop-down menu. If you select **WEP**, you should also select the type of characters to be used for the WEP key, **ASCII** or **Hex**, from the drop-down menu. Then enter the **WEP Key** in the field provided. If you select **WPA**, you should enter a **Pre-Shared Key** (password) in the field below. Regardless of the security mode selected, the settings should be the same on all APs within the bridge. For further information regarding wireless security, please refer to "Configuring Wireless Security" on page 46.

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



Note: *The Bridge with AP Mode is not completely specified in the Wi-Fi or IEEE standards. This mode will work with other DAP-1665 units. Communication with other APs (even other D-Link APs) is not guaranteed.*

2.4 GHz Band

Note: *If the Bridge Band is set to* ***2.4GHz****, the settings for the AP's 2.4GHz band will be the same as those for the bridge, so only the* ***Network Name*** *(SSID) and* ***Visibility*** *of the 2.4GHz band can be changed. However, you can configure all settings for the 5GHz AP, if you* ***check the box to Enable Wireless****.*

Enable Wireless: Check the box to **Enable** the wireless function for the **2.4GHz** band. When the box is unchecked, all wireless functions are disabled. With wireless enabled, you may set up a specific schedule. Select a schedule from the drop-down menu or click **Add New** to create a new schedule.

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

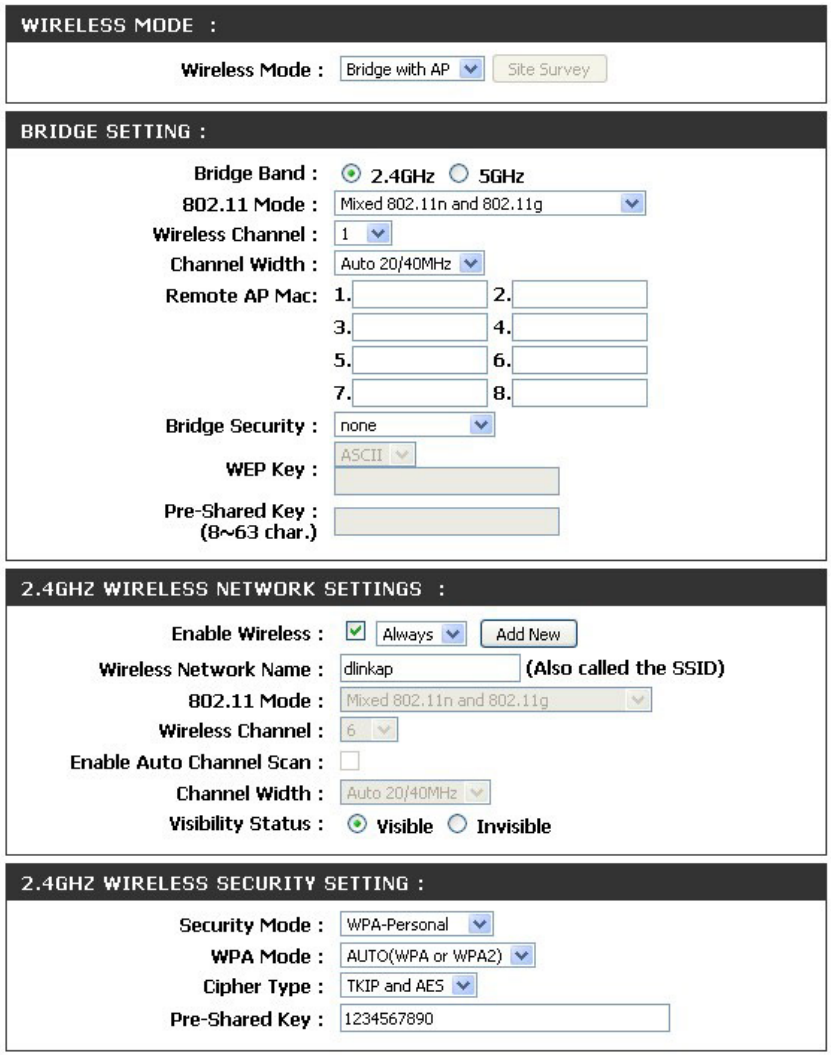
802.11 Mode: When the *Bridge Band* selected above is *2.4GHz*, the contents of this field will reflect the *802.11 Mode* selected above. Selecting an *802.11 Mode* is only possible when *Bridge Band* is 5GHz:
802.11n Only - Select if you are only using 802.11n wireless clients.
Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 802.11g wireless clients.
Mixed 802.11n, 802.11g and 802.11b - Select if you are using a mix of 802.11n, 802.11g, and 802.11b wireless clien

Wireless Channel: Indicates the channel setting. Do not check the box to **Enable Auto Channel Scan** if you would like to change the channel to match the channel setting of an existing wireless network.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan,** if you would like the DAP-1665 to automatically choose the channel with the least amount of interference.

Channel Width: When the *Bridge Band* selected above is *2.4GHz*, the contents of this field will reflect the *Channel Width* selected above. Selecting a different *Channel Width* here is only possible when *Bridge Band* is set to 5 GHz.

Visibility Status: Select whether you would like the network name (SSID) of your 2.4GHz wireless network to be **Visible** or **Invisible**. If **Invisible** is selected, the SSID of the DAP-1665 will not be shown by Site Survey utilities. Therefore, the SSID will have to be manually entered so wireless clients can connect.



Security Mode: For information on how to set up wireless security, refer to "Configuring Wireless Security" on page 46.

5 GHz Band

Enable Wireless: Check the box to **Enable** the wireless function for the **5GHz** band. When the box is unchecked, all wireless functions are disabled. With wireless enabled, you may set up a specific schedule. Select a schedule from the drop-down menu or click **Add New** to create a new schedule.

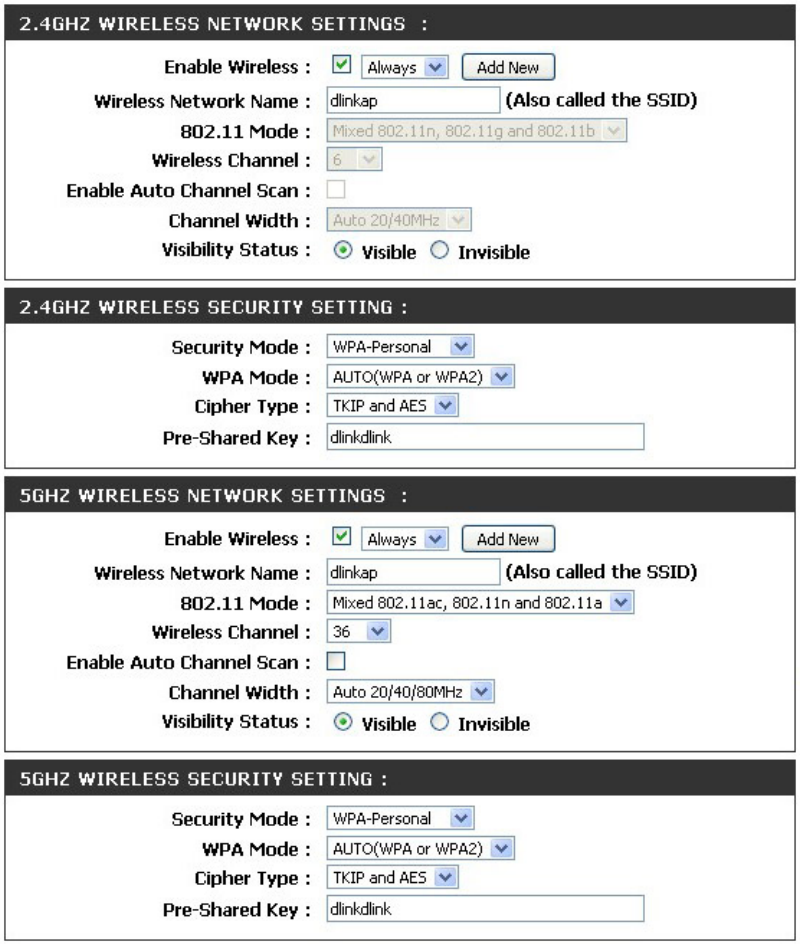
Wireless Network Name: Specify a **Network Name** (SSID) to identify the 5GHz network. This is the SSID that wireless clients will search for when connecting to your wireless network. This name should be different from that of the 2.4GHz network configured above.

802.11 Mode: When the *Bridge Band* selected above is *5GHz*, the contents of this field will reflect the *802.11 Mode* selected above. Selecting an *802.11 Mode* is only possible when *Bridge Band* is 2.4GHz:
802.11a Only - Select if you are only using 802.11a wireless clients.
802.11n Only - Select if you are only using 802.11n wireless clients.
Mixed 802.11n and 802.11a - Select if you are using a mix of 802.11n and 802.11a wireless clients.
802.11ac Only - Select if you are only using 802.11ac wireless clients.
Mixed 802.11ac and 802.11n - Select if you are using a mix of 802.11ac and 802.11n wireless clients.
Mixed 802.11ac, 802.11n and 802.11a - Select if you are using a mix of 802.11ac, 802.11n, and 802.11a wireless clients.

Wireless Channel: Indicates the channel setting. Do not check the box to **Enable Auto Channel Scan** if you would like to change the channel to match the channel setting of an existing wireless network.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan,** if you would like DAP-1665 to automatically choose the channel with the least amount of interference.

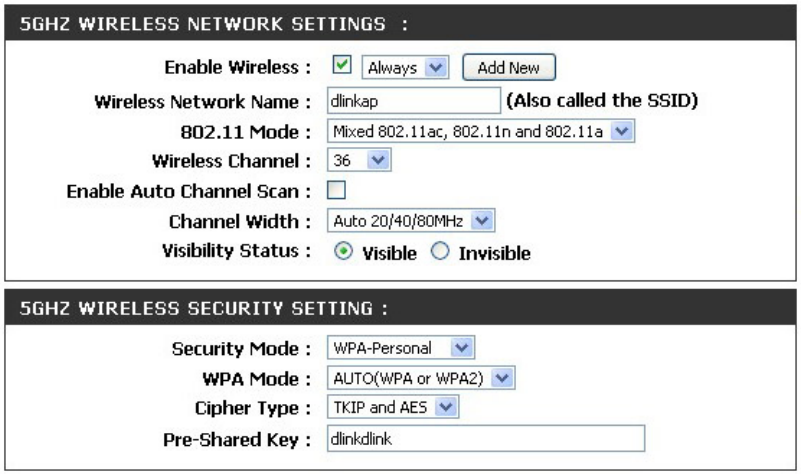
Channel Width: When the *Bridge Band* selected above is *5GHz*, the contents of this field will reflect the *Channel Width* selected above. Selecting a different *Channel Width* here is only possible when *Bridge Band* is set to 2.4GHz.



Visibility Status: Select whether you would like the network name (SSID) of your 5GHz wireless network to be **Visible** or **Invisible**. If **Invisible** is selected, the SSID of the DAP-1665 will not be shown by Site Survey utilities. Therefore, the SSID will have to be manually entered so wireless clients can connect.

Security Mode: For information on how to set up wireless security, refer to "Configuring Wireless Security" on page 46.

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



Repeater Mode

Repeater mode re-broadcasts the wireless signal of an existing network to increase coverage. The signal can be repeated using both the 2.4GHz and 5GHz bands.

2.4GHz Band

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

Site Survey: Click **Site Survey** to display a list of available wireless networks in your area. To select a wireless network, click on the radio button in the far right column, and click **Connect** at the bottom of the page to continue. The fields below for the *Repeater Network Name*, *Repeater Network Band,* and *Channel Width* will automatically be filled.

Repeater Network Name: If you did not use the **Site Survey** option described above, enter the **SSID** of the access point for which you would like to repeat the signal .

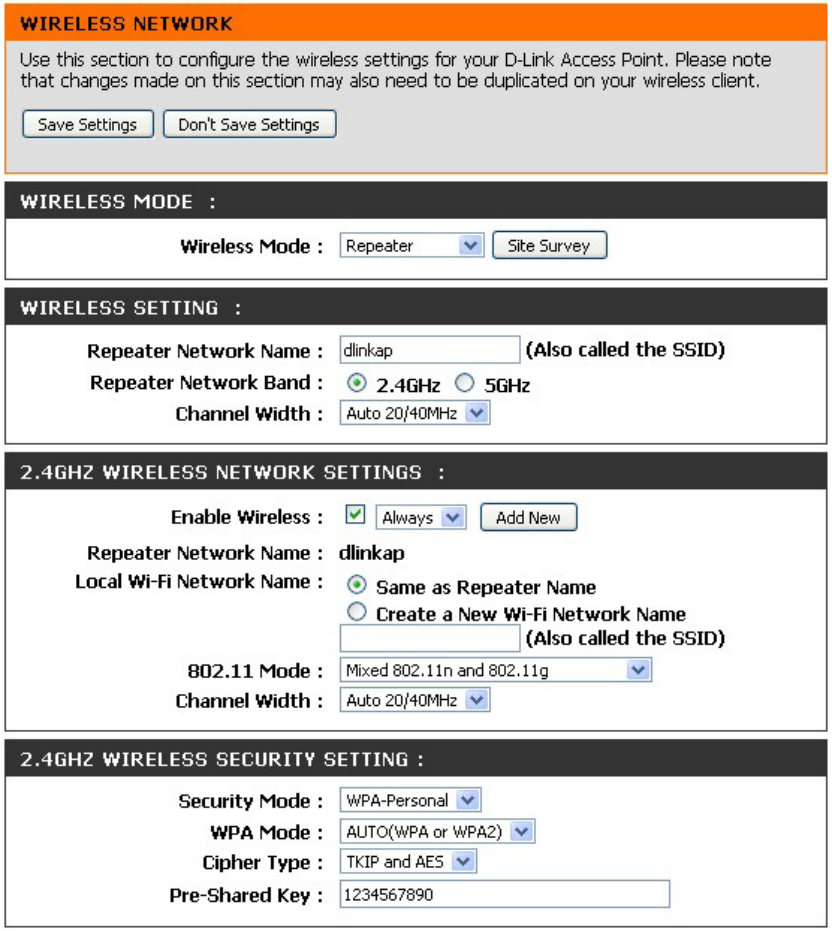
Repeater Network Band: If you did not use the **Site Survey** option described above, select the wireless band of the repeater network.

Channel Width: If you did not use the **Site Survey** option described above, select the **Channel Width** to be used for communication with the repeater network.

Enable Wireless: Check the box to enable the **2.4GHz** wireless band. If you do not want to use wireless, uncheck the box to disable all wireless functions. With wireless enabled, you may set up a specific schedule. By default, the schedule is set to **Always**. You can select a schedule from the drop-down menu, or click **Add New** to create a new schedule.

Repeater Network Name: Displays the name of the network to be repeated.

Local Wi-Fi Network Name: Select a method for naming the DAP-1665's extended network:
Same as Repeater Name - The extended network will have the same name (SSID) as the repeater network.
Create a New Wi-Fi Network Name - Enter a new **Network Name** (SSID) for the extended network in the field below.



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

Channel Width: Select the appropriate channel width from the drop-down menu, either **20MHz** or **Auto 20/40MHz**.

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 46.

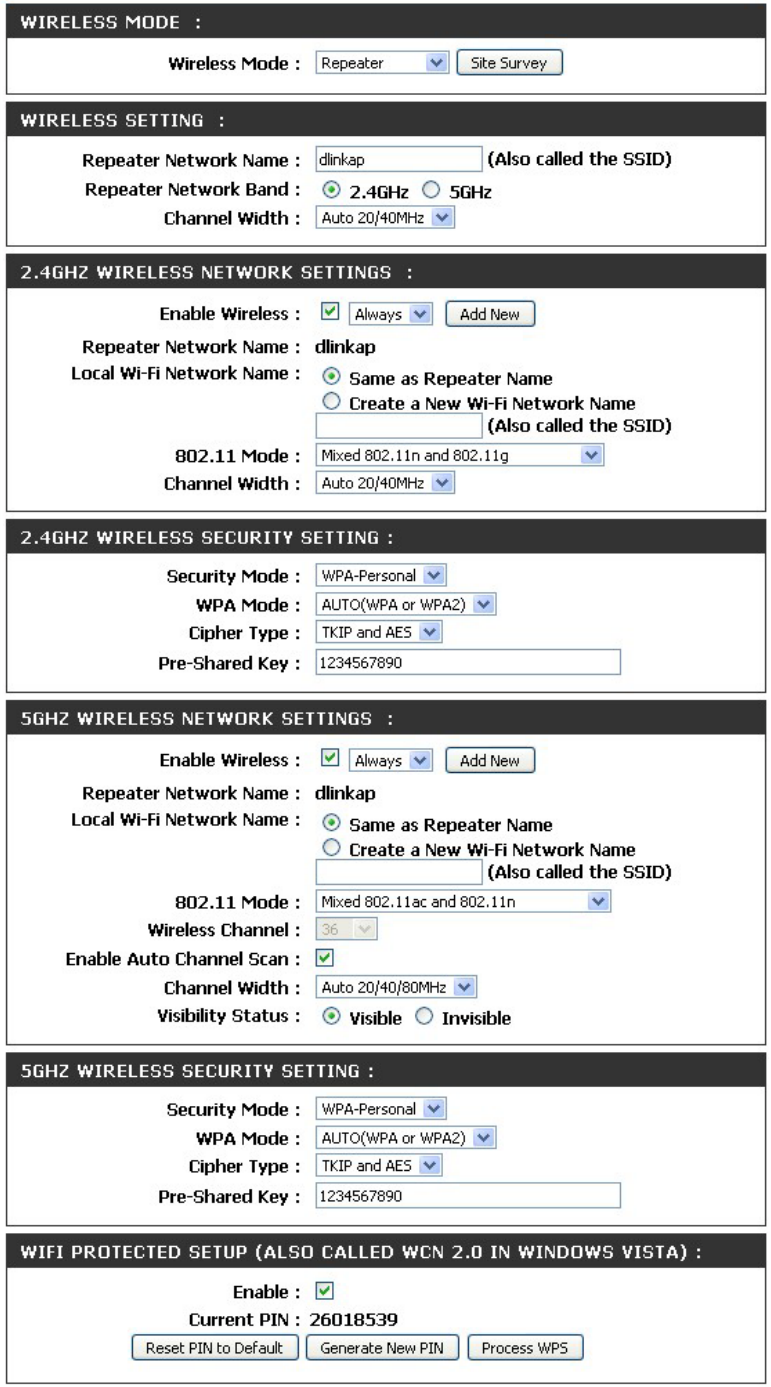
5GHz Band

Enable Wireless: Check the box to enable the **5GHz** wireless band. If you do not want to use wireless, uncheck the box to disable all wireless functions. With wireless enabled, you may also set up a specific schedule. You can select a schedule from the drop-down menu or click **Add New** to create a new schedule.

Repeater Network Name: Displays the name of the network which is to be repeated.

Local Wi-Fi Network Name: Select a method for naming the DAP-1665's extended network:
Same as Repeater Name - The extended network will have the same name (SSID) as the repeater network.
Create a New Wi-Fi Network Name - Enter a new name (SSID) for the extended network in the field below.

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



Wireless Channel: Indicates the channel setting. Do not check the box to **Enable Auto Channel Scan** if you would like to change the channel to match the channel setting of an existing wireless network.

Enable Auto Channel Scan: Check the box to **Enable Auto Channel Scan.** This will allow the DAP-1665 to automatically choose the channel with the least amount of interference.

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

Visibility Status: Select whether you want the wireless network name (SSID) of the 5GHz band to be **Visible** or **Invisible**. If **Invisible**, the SSID of the DAP-1665 will not be shown by Site Survey utilities. Therefore, the SSID will have to be manually entered so wireless clients can connect.

Security Mode: For information on how to set up wireless security, please refer to "Configuring Wireless Security" on page 46.

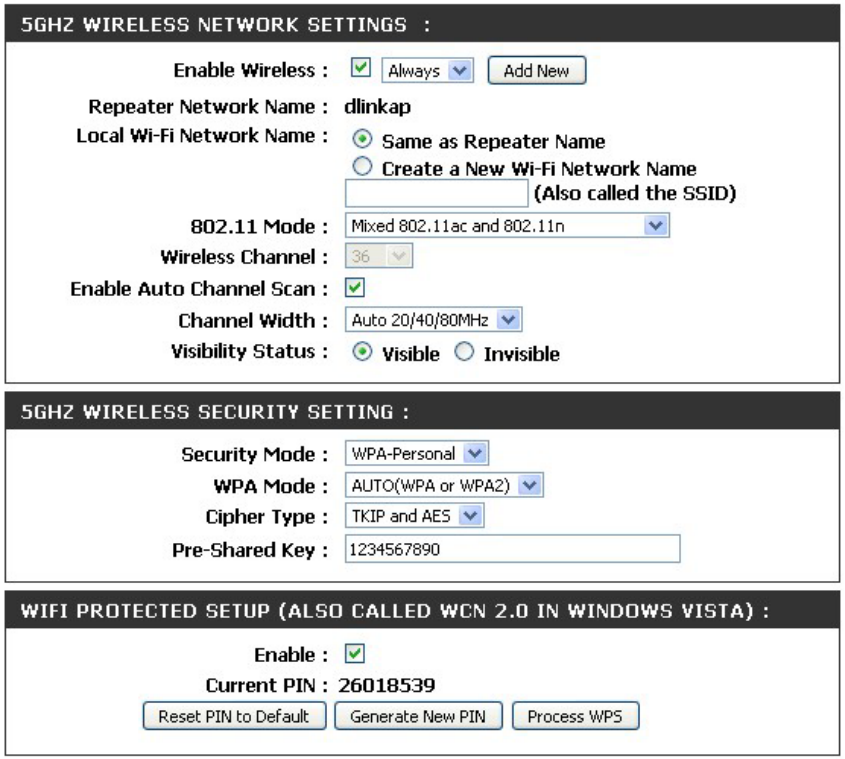
Wi-Fi Protected Setup: Check the box to **Enable** the use of *Wi-Fi Protected Setup* (WPS) for *Repeater Mode*.

Current PIN: Displays the *Current PIN* which can be used to connect to the router using the WPS-PIN method.

Click **Reset PIN to Default** to reset the PIN number to the factory default settings. Click **Generate New PIN** to randomly generate a new PIN for WPS connection. Click **Process WPS** to begin the WPS Push-Button setup process.

Note: *If you want to connect using WPS and the* ***Process WPS*** *button is greyed out, click on the* **Save Settings** *button at the top of the screen to save current settings. The button will be enabled after the DAP-1665 reboots.*

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

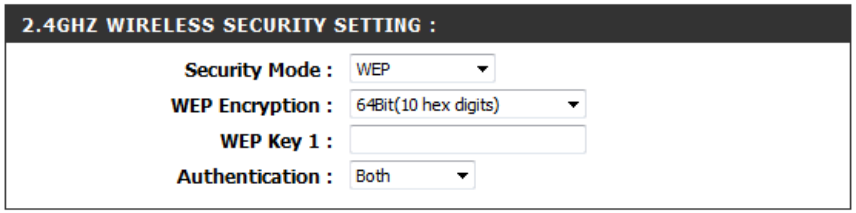


Configuring Wireless Security

Wireless security encryption prevents unauthorized users from accessing your wireless network. The DAP-1665 provides two methods of wireless security encryption from which to choose: **Wired Equivalent Privacy** (WEP), and **Wi-Fi Protected Access** (WPA). It is recommended that you use WPA security if your wireless devices support this standard, as it is more secure than the older WEP standard. Skip to the next page for WPA instructions. For details about wireless security, refer to "Wireless Security" on page 76.

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

WEP



Security Mode: Select **WEP** from the drop-down menu ONLY IF your wireless devices do not support the more secure WPA standard.

WEP Encryption: The WEP standard offers two levels of encryption: 64-bit and 128-bit. Each level has the option of a key (password) consisting of either HEX digits or ASCII characters:
64Bit (10 hex digits) - Uses a key consisting of 10 hex digits (0-9, A-F).
64Bit (5 ASCII characters) - Uses a key consisting of 5 ASCII characters (0-9, A-Z, plus symbols).
128Bit (26 hex digits) - Uses a key consisting of 26 hex digits (0-9, A-F).
128bit (13 ASCII characters) - Uses a key consisting of 13 ASCII characters (0-9, A-Z, plus symbols).

WEP Key 1: Enter the desired **WEP Key** (password) for your wireless network. The key should adhere to the requirements of WEP Encryption method specified above.

Authentication: Select an **Authentication** method from the drop-down menu

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

WPA-Personal

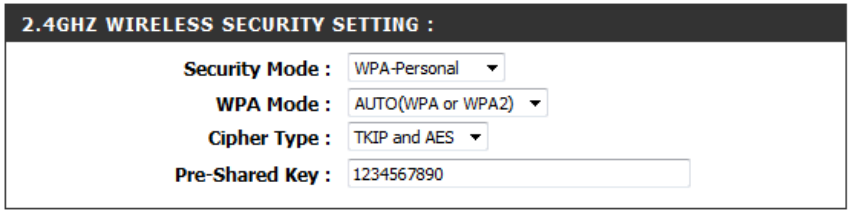
Security Mode: Select **WPA-Personal** from the drop-down menu.

WPA Mode: There are two versions of WPA supported by the DAP-1665, **WPA** and **WPA2**. We recommended that you use **AUTO(WPA or WPA2)** so that WPA2 will be used whenever the connecting wireless clients support it.

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

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

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



WPA-Enterprise

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

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

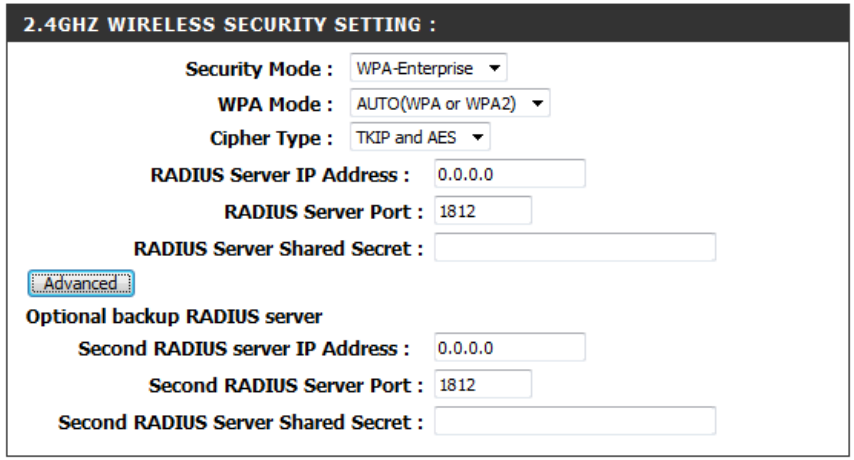
WPA Mode: There are two versions of WPA supported by the DAP-1665, **WPA** and **WPA2**. It is recommended that you use **AUTO(WPA or WPA2)** so that the WPA2 version will be used whenever the connecting wireless clients support it.

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

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

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

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



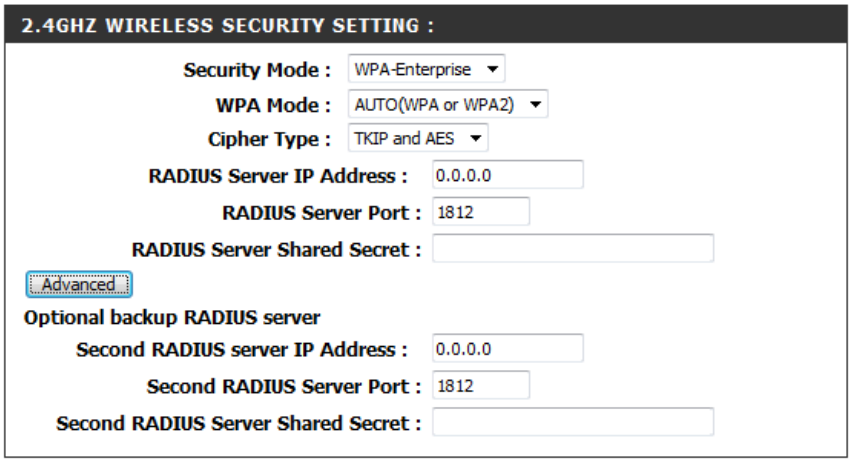
Advanced: Click on the **Advanced** button to display the additional fields for an optional backup RADIUS server configuration.

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

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

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

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



LAN Setup

The LAN Setup page enables you to configure the Local Area Network (LAN) settings for the access point. From this page you can adjust your local network's IP address settings. If you are connecting the access point to a network which is using IPv6, the DAP-1665 can be configured to operate using the IPv6 protocol.

Dynamic/Static IP

Device Name: You can change the name of your access point to make it easier to identify. Enter a name for the access point in the **Device Name** field. You can use this name in your web browser address field to access the web-based configuration utility.
Example: http://devicename

My LAN Connection is: Select how you would like to configure the access point's IP address settings from the drop-down menu:
Dynamic IP(DHCP) - The access point will request an IP address from the DHCP server that it is connected to. The *IP Address*, *Subnet Mask*, etc. will automatically be assigned.
Static IP - You can manually specify the IP address settings for the access point.

IP Address: Enter the **IP Address** for the access point (for *Static IP* only).

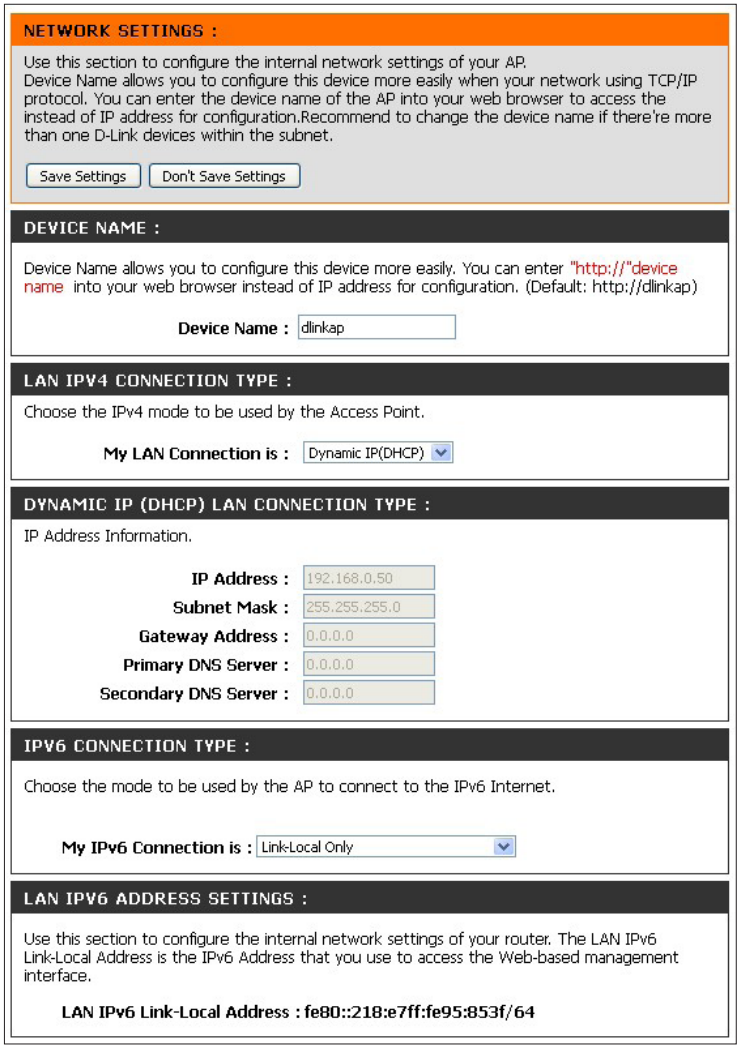
Subnet Mask: Enter the **Subnet Mask** to be used by the access point (for *Static IP* only).

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

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

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

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



DHCP Server

The access point has a built-in Dynamic Host Control Protocol (DHCP) server, which can automatically assign IP addresses to connected clients that request them. You can only enable this built-in DHCP server when **Static IP** Address mode is selected.

Enable DHCP Server: Check the box to **Enable** the built-in DHCP server function. If you already have a DHCP server on your network, do not check the box to enable this function on the DAP-1665.

DHCP IP Address Range: Enter the **Address Range** of the DHCP address pool from which requesting clients can be assigned addresses. You should ensure that the access point's static IP address is outside of this range in order to avoid any IP address conflicts.

Always Broadcast: Check the box to have the DHCP server **Always Broadcast** its response to clients. This can help to avoid problems when clients fail to obtain an IP address from the DHCP server.

Gateway: Enter the **Gateway Address** which will be sent to requesting clients.

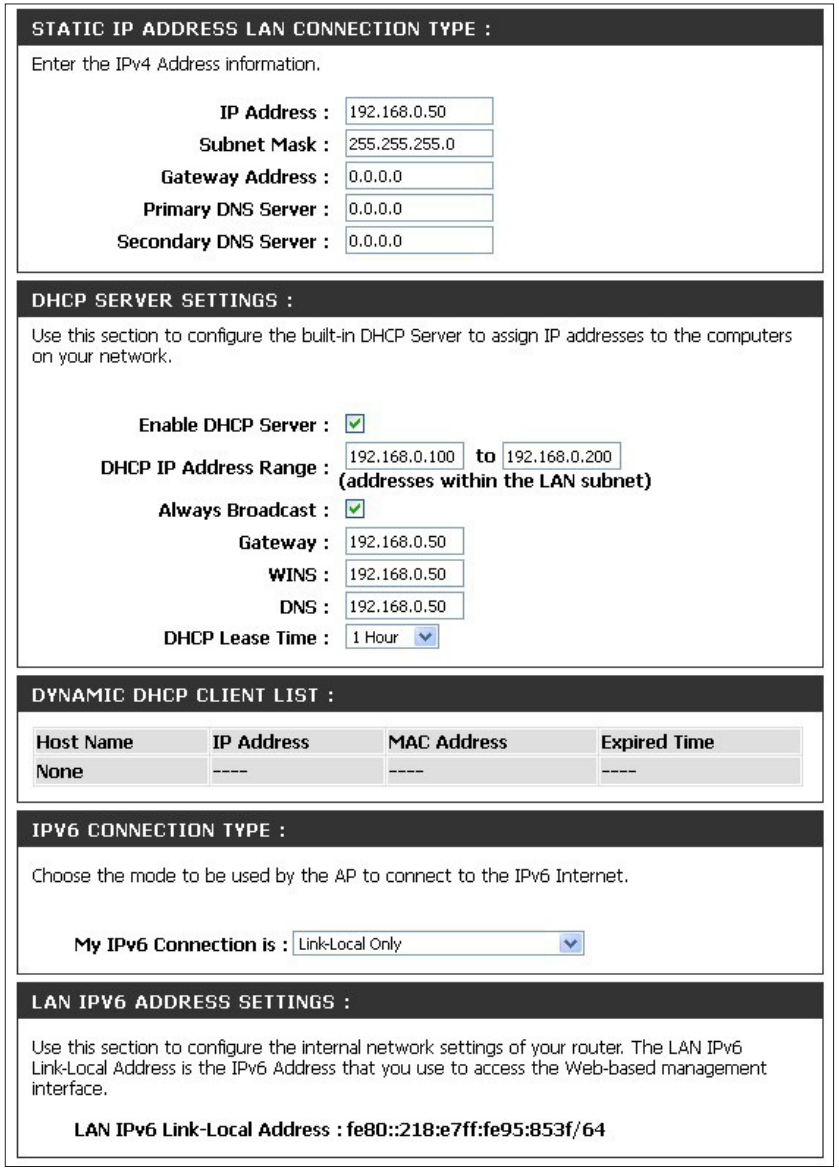
WINS: Enter the **WINS** server address which will be sent to requesting clients.

DNS: Enter the **DNS** server address which will be sent to requesting clients.

DHCP Lease Time: From the drop-down menu, select the desired length of time the **DHCP** address is leased for.

Dynamic DHCP Client List: This table will display details for the clients which are currently receiving a DHCP address from the DHCP server.

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



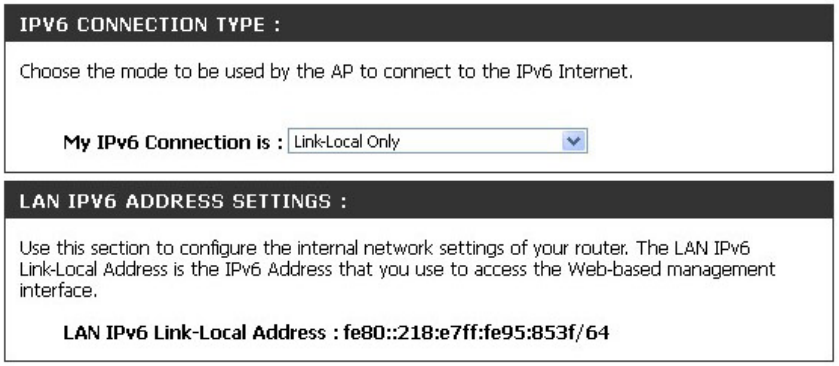
IPv6

If you are connecting the access point to a network which is using IPv6, the DAP-1665 can be configured to operate using the IPv6 protocol.

My IPv6 Connection is: When **Link-Local Only** is selected, this will set the access point's local IPv6 address.

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

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



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

LAN IPv6 Address: Enter the **LAN IPv6 Address** here. This address should be supplied by your Internet Service Provider (ISP).

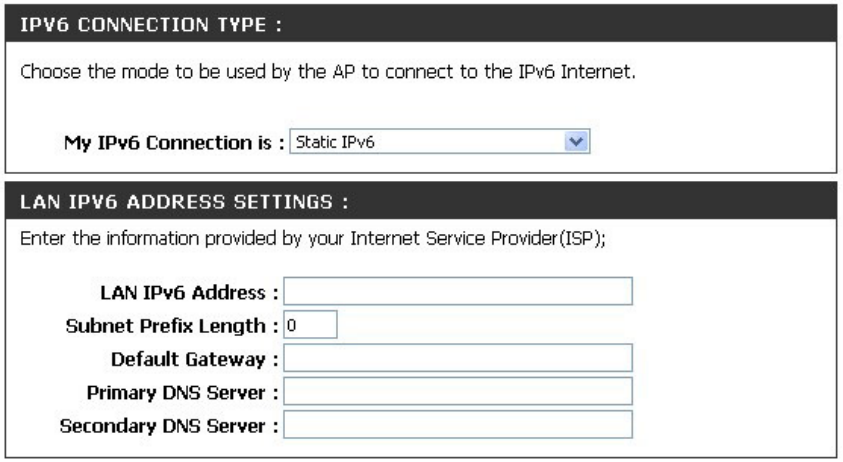
Subnet Prefix Length: Enter the **Prefix Length** for IPv6 IP addresses on your network.

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

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

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

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



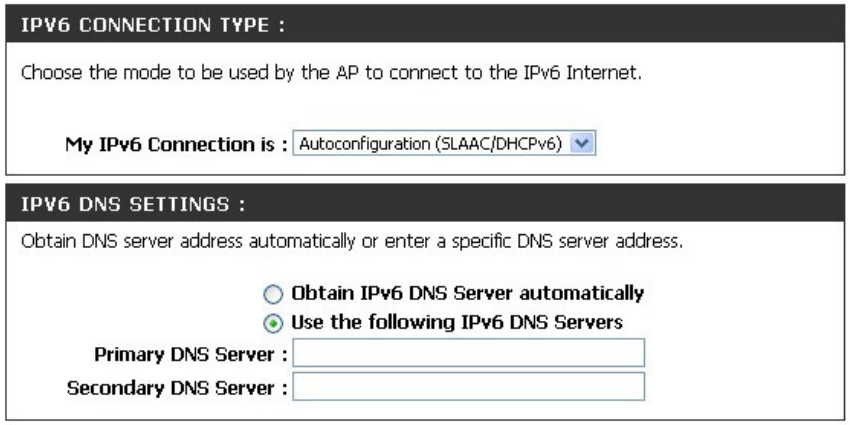
My IPv6 Connection is: Select **Autoconfiguration (SLAAC/DHCPv6)** from the drop-down menu. The access point will request IPv6 settings from a DHCPv6 server on your network.

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

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

Secondary DNS Server: Enter the Secondary IPv6 DNS server address to be used.

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



Advanced

This section allows you to configure the advanced parameters of your DAP-1665. There will be different advanced features available for configuration based on the mode in which your device is operating. The instructions below are listed according to operation mode.

Access Point Mode

Access Settings

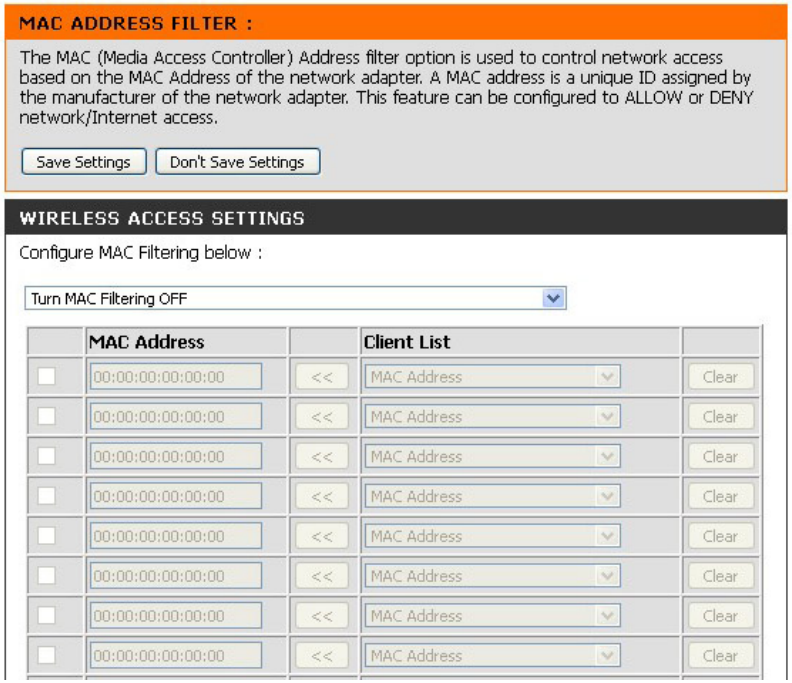
Mac (Media Access Controller) filtering allows you to control wireless access to your network according to clients' MAC addresses.

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

Checkbox: Check the box to indicate this *MAC Address* should be included in the MAC filtering rules.

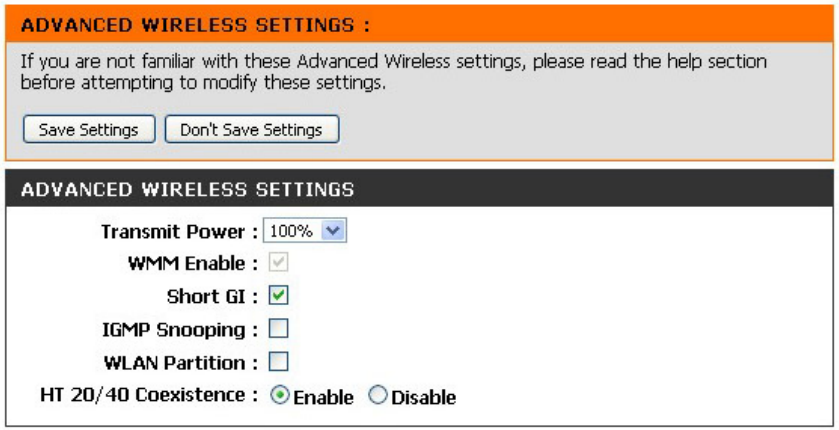
MAC Address: Enter the **MAC Address** of the client that you wish to filter. If the client is currently connected to the access point, you can select it from the **Client List** drop-down menu, and click **<<** to automatically populate the field.

Click **Clear** to clear all fields. Click **Save Settings** at the top of the page to save the current configuration.



Advanced Wireless

From this page, you can adjust the *Advanced Wireless Settings*. We recommend that you leave these settings at default values.



Transmit Power: You can select the transmission power of the wireless radio from the drop-down menu.

WMM Enable: Check the box to enable Wireless Multimedia (WMM), a QoS engine which can help to reduce lag and latency when transmitting multimedia over your wireless connection.

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

IGMP Snooping: Enabling this option allows the access point to listen for Internet Group Management Protocol (IGMP) traffic, which can help to detect clients that require multicast streams.

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

HT 20/40 Coexistance: Enabling this option will reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel overlapping and causing interference, the router will automatically change to 20 MHz.

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

Wi-Fi Protected Setup

This section allows you to select the method to be used for Wi-Fi Protected Setup (WPS) to create a secure wireless connection.
Note: *Clients must support WPS in order for this method to be used.*

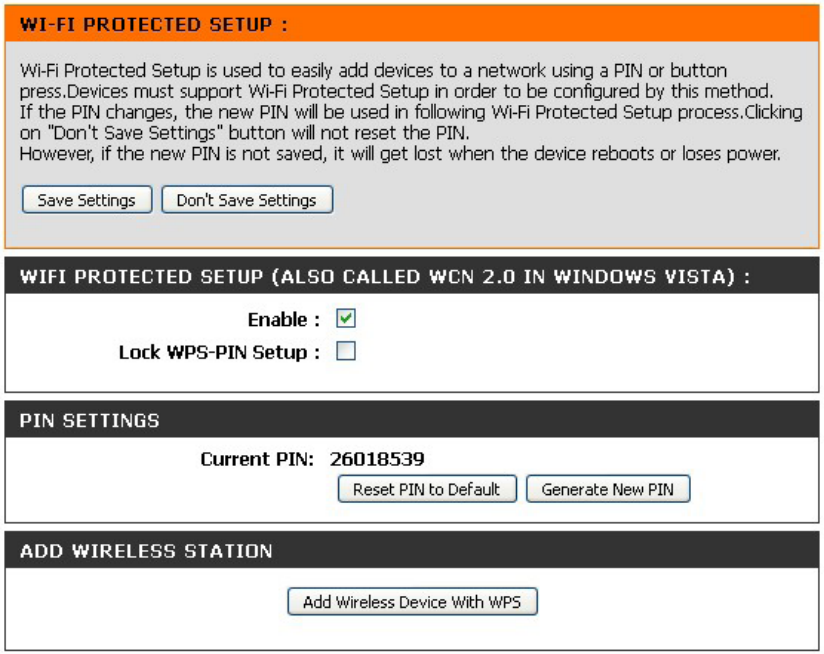
Enable: Check the box to **Enable** WPS.

Lock WPS-PIN Method: Check the box to lock WPS using the PIN method. If this option is selected, wireless clients will only be able to use the WPS-PBC (Push-button Connection) method.

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

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

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



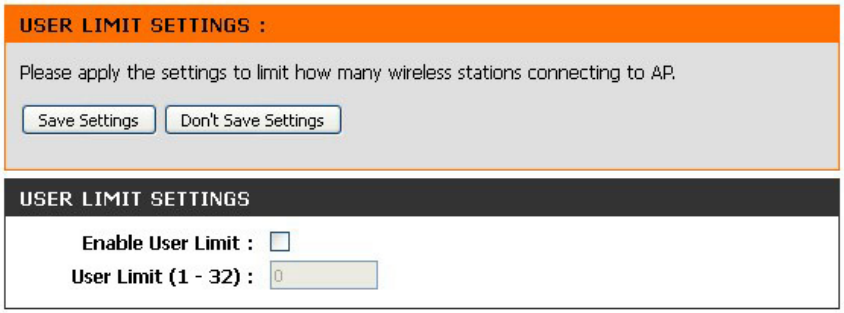
User Limit

From this page, you can set a maximum number of wireless clients that can be connected to the access point at any one time.

Enable User Limit: Check the box to **Enable** the user limit function.

User Limit: Enter a number of wireless clients (between 1-32).

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



Wireless Client Mode

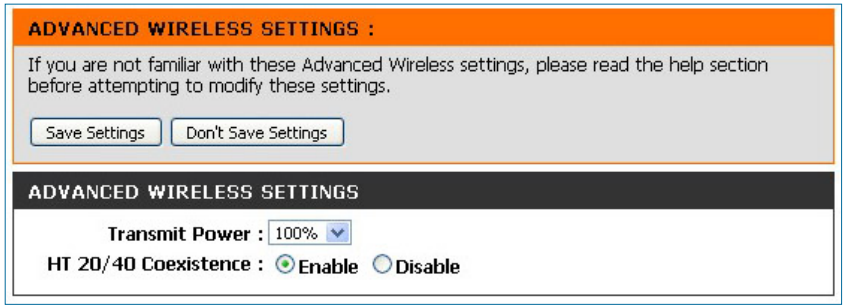
Advanced Wireless

From this page, you can adjust the *Advanced Wireless Settings*. We recommend that you leave these settings at default values.

Transmit Power: You can select the transmission power of the wireless radio from the drop-down menu.

HT 20/40 Coexistance: Click to **Enable** this option. It will reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel overlapping and causing interference, the router will automatically change to 20 MHz.

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



Bridge Mode

Advanced Wireless

From this page, you can adjust the *Advanced Wireless Settings*. We recommend that you leave these settings at default values.

Transmit Power: You can select the transmission power of the wireless radio from the drop-down menu.

WMM Enable: Check the box to enable Wireless Multimedia (WMM), a QoS engine which can help to reduce lag and latency when transmitting multimedia over your wireless connection.

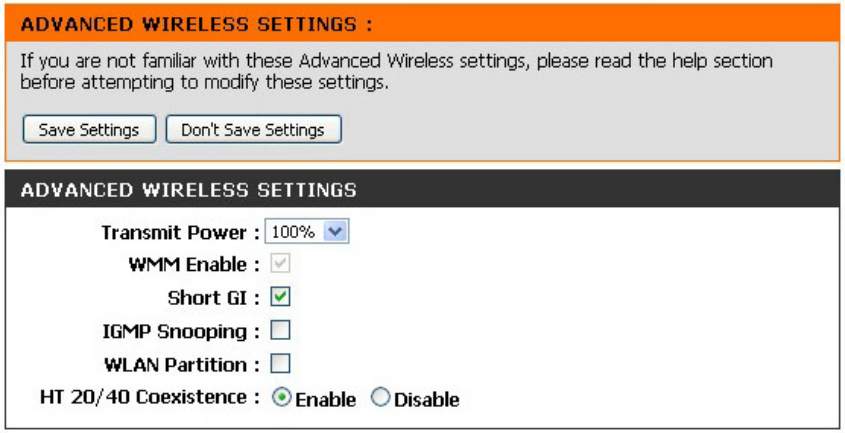
Short GI: Enabling a short Guard Interval (GI) can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

IGMP Snooping: Enabling this option allows the access point to listen for Internet Group Management Protocol (IGMP) traffic, which can help to detect clients which require multicast streams.

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

HT 20/40 Coexistance: Enabling this option will reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel overlapping and causing interference, the router will automatically change to 20 MHz.

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



Bridge with AP Mode

Advanced Wireless

From this page, you can adjust the *Advanced Wireless Settings*. We recommend that you leave these settings at default values.

Transmit Power: You can select the desired transmission power of the wireless radio from the drop-down menu.

WMM Enable: Check the box to enable Wireless Multimedia (WMM), a QoS engine which can help to reduce lag and latency when transmitting multimedia over your wireless connection.

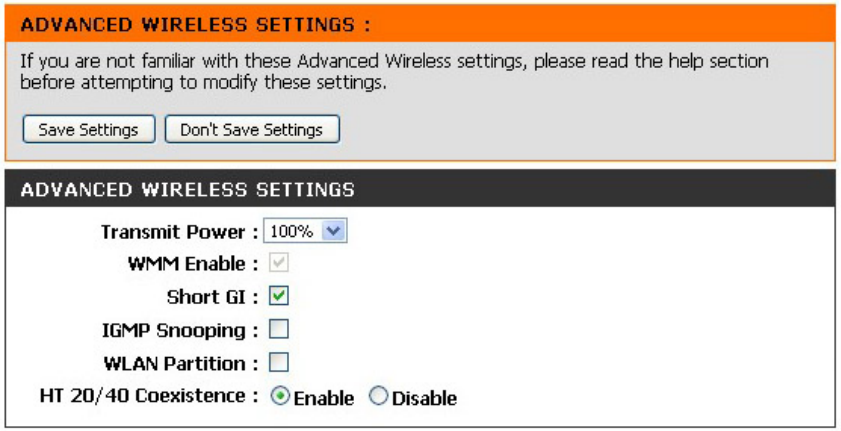
Short GI: Enabling a short Guard Interval (GI) can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

IGMP Snooping: Enabling this option allows the access point to listen for Internet Group Management Protocol (IGMP) traffic, which can help to detect clients which require multicast streams.

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

HT 20/40 Coexistance: Enabling this option will reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel overlapping and causing interference, the router will automatically change to 20 MHz.

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



Repeater Mode

Access Settings

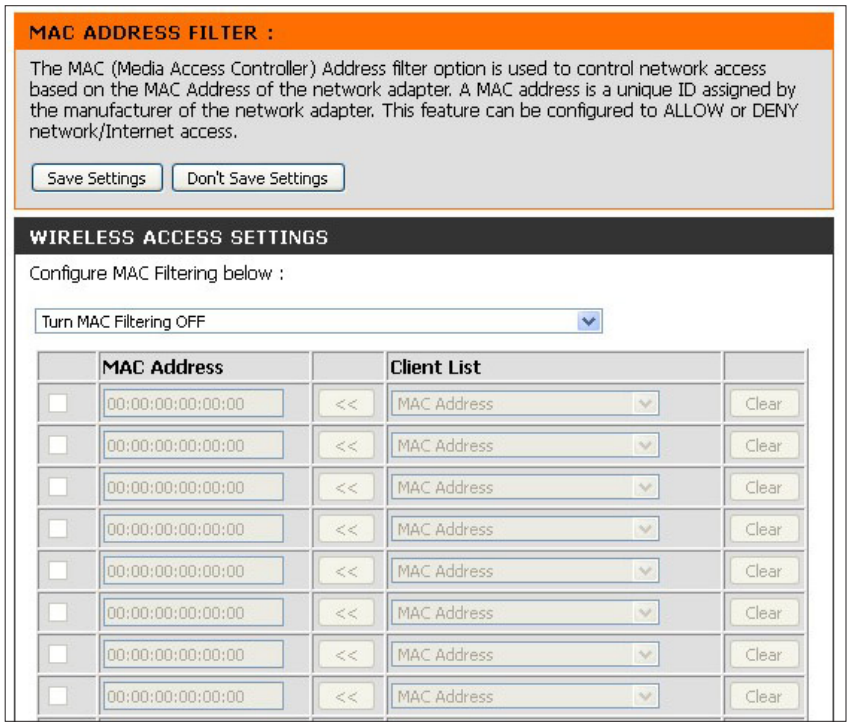
Mac (Media Access Controller) filtering allows you to control wireless access to your network according to clients' MAC addresses.

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

Checkbox: Check the box to indicate this *MAC Address* should be included in the MAC filtering rules.

MAC Address: Enter the **MAC Address** of the client that you wish to filter. If the client is currently connected to the access point, you can select it from the **Client List** drop-down menu, and click **<<** to automatically populate the field.

Click **Clear** to clear all fields. Click **Save Settings** at the top of the page to save the current configuration.



Advanced Wireless

From this page, you can adjust the *Advanced Wireless Settings*. We recommend that you leave these settings at default values.

Transmit Power: You can select the transmission power of the wireless radio from the drop-down menu.

WMM Enable: Check the box to enable Wireless Multimedia (WMM), a QoS engine which can help to reduce lag and latency when transmitting multimedia over your wireless connection.

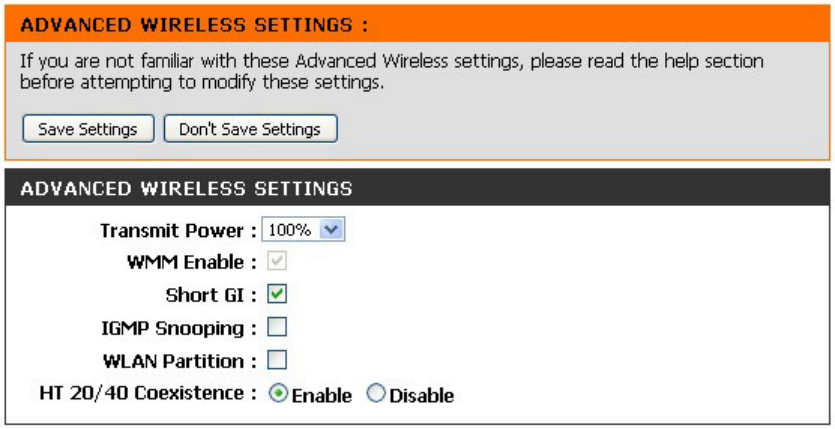
Short GI: Enabling a short Guard Interval (GI) can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

IGMP Snooping: Enabling this option allows the access point to listen for Internet Group Management Protocol (IGMP) traffic, which can help to detect clients which require multicast streams.

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

HT 20/40 Coexistance: Enabling this option will reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel overlapping and causing interference, the router will automatically change to 20 MHz.

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



Wi-Fi Protected Setup

This section allows you to select the method to be used for Wi-Fi Protected Setup (WPS) to create a secure wireless connection.
Note: *Clients must support WPS in order for this method to be used.*

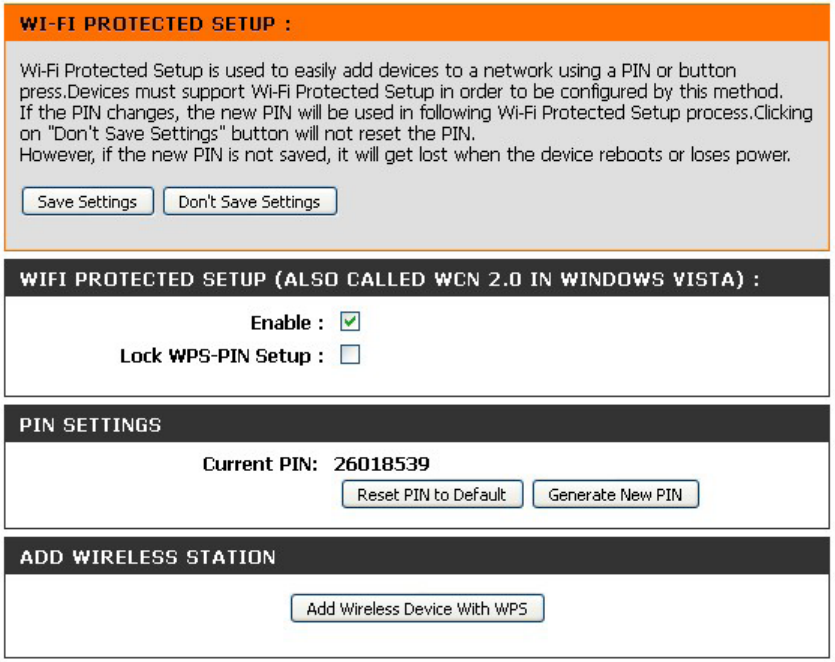
Enable: Check the box to **Enable** WPS.

Lock WPS-PIN Method: Check the box to lock WPS using the PIN method. If this option is selected, wireless clients will only be able to use the WPS-PBC (Push-button Connection) method.

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

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

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



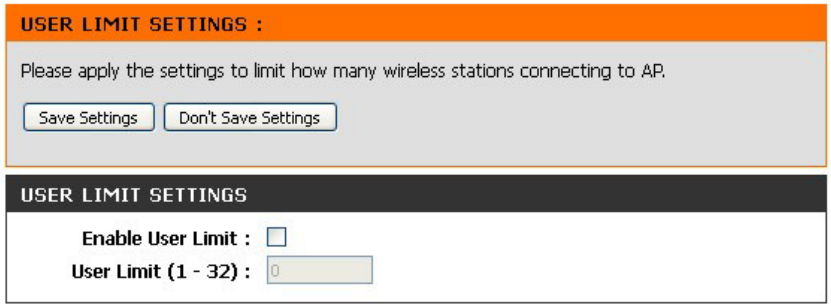
User Limit

From here, you can set a maximum number of wireless clients that can be connected to the access point at any one time.

Enable User Limit: Check the box to **Enable** the user limit function.

User Limit: Enter a number of wireless clients (between 1-32).

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



Maintenance

The Maintenance section allows you to adjust the administrative settings of the router such as time and date, and administrator password. You can update the device's firmware, and add or remove language packs.

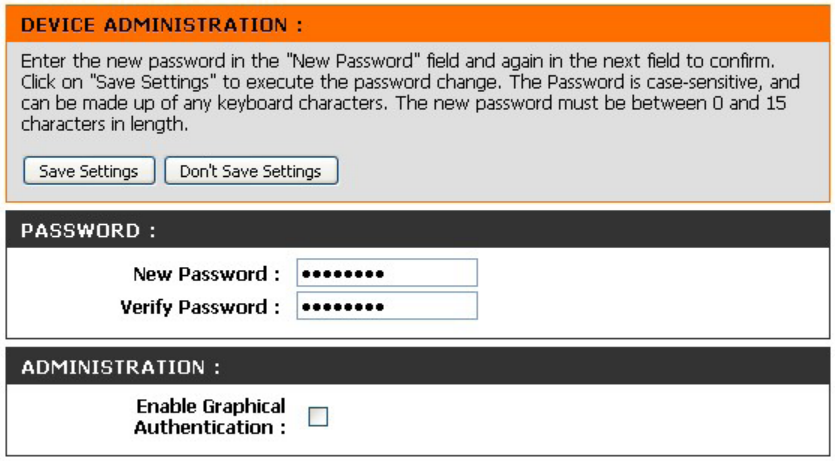
Admin

New Password: To change the password for the web-based configuration utility's Admin account, enter a new password in the field provided.

Verify Password: Re-enter the new password in this field.

Enable Graphical Authentication: Check the box to enable graphical authentication. Graphical authentication uses a challenge-response test to prevent unauthorized users from gaining access to the configuration utility through automated means.

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



System

The System page can be used to save and restore the device's configuration, as well as restore the AP's factory default settings.

Save Settings to Local Hard Drive: Click **Save** to save the access point's current configuration to a file on your local computer. After clicking, a *Save File* dialog box will appear, prompting you to save the configuration file on your computer.

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

Note: *This will overwrite any current configuration.*

Restore to Factory Default Settings: Click **Restore Device** to reset the DAP-1665's settings to the factory defaults.

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

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

Firmware

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

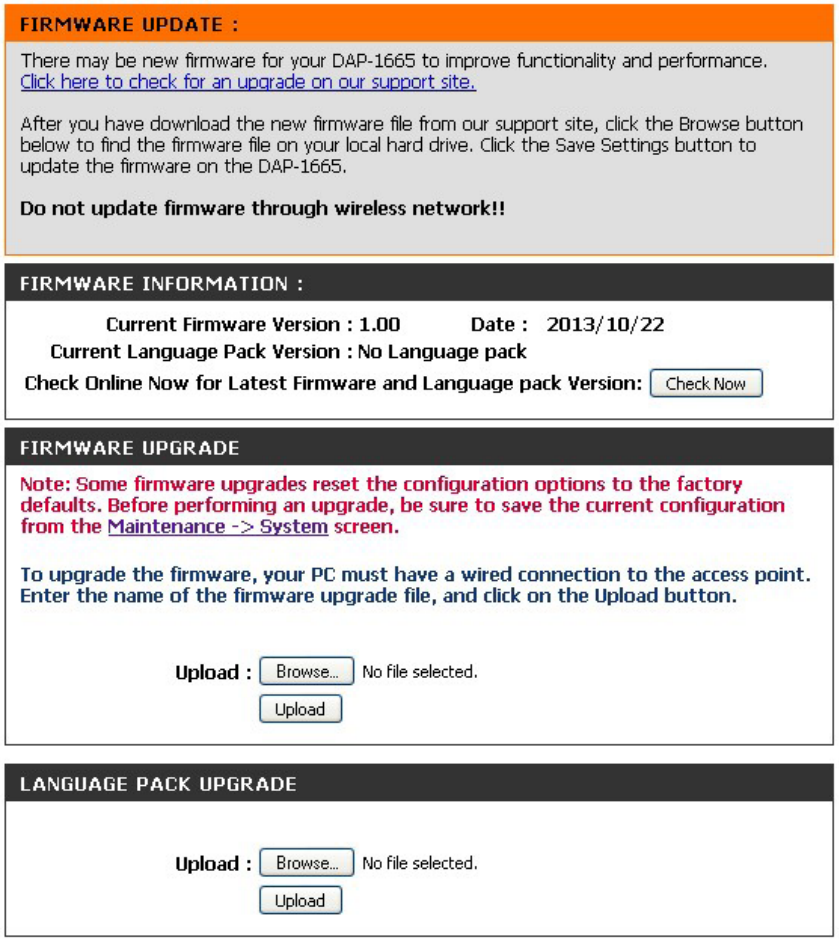
Firmware Information: This section displays information about the device's current firmware and language pack. Click **Check Now** to check for latest firmware or language pack versions.

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

Firmware Upgrade: After you have downloaded the new firmware, click **Browse** to locate a firmware file on your computer. Once located, click **Upload** to commence the firmware upgrade process. It is recommended that you save your current router configuration using the System page before you begin a firmware upgrade.

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

Language Pack Upgrade: After you have downloaded the new language pack, click **Browse** to locate a language pack file on your computer. Once located, click **Upload** to commence the language pack upgrade process.



Time

Use the Time page to configure the time and date settings of the access point. You can also configure daylight saving adjustments and synchronize the access point's clock and calendar with an Internet-based Network Time Protocol (NTP) server.

Time: Displays the access point's current date and time.

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

Enable Daylight Saving: Check the box to **Enable Daylight Saving** if you want the access point automatically adjust the clock for daylight saving.

Daylight Saving Offset: Select the offset for beginning daylight saving from the drop-down menu.

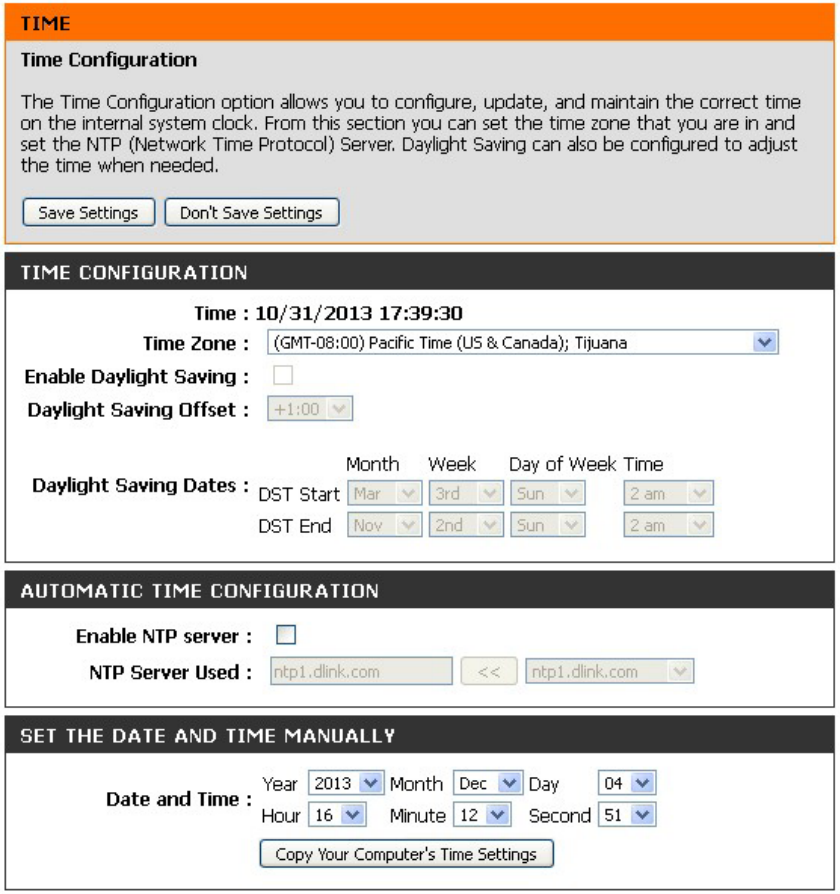
Daylight Saving Dates: Use the drop-down menus to set the **Start** and **End** dates for daylight saving time.

Enable NTP Server: Check the box to have the access point automatically synchronize its clock and calendar with an online NTP server.

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

Date and Time: Use the drop-down menus to manually configure the time and date. This option will not be available if the *Enable NTP Server* option is checked above.

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

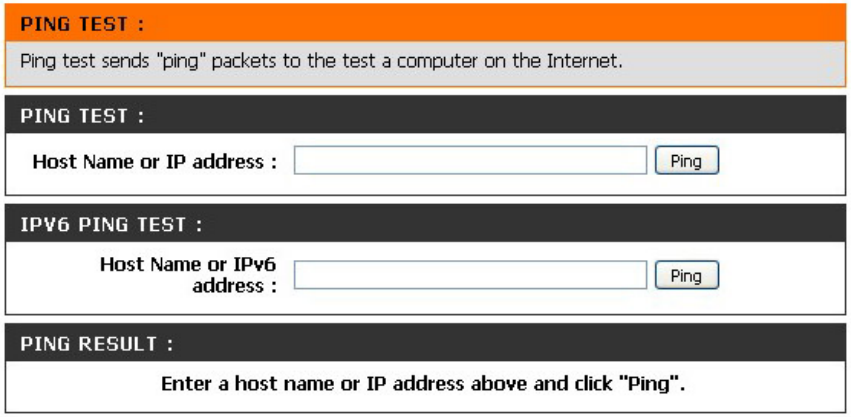


System Check

Host Name or IP Address: Enter the **Host Name** or **IP Address** and click **Ping** if you wish to conduct a ping test.

Host Name or IPv6 Address: Enter the **Host Name** or **IPv6 Address** and click **Ping** if you wish to conduct an IPv6 ping test.

Ping Result: Displays results of the ping test above.



Schedules

Use the Schedules page to create new schedule rules for various access point functions. Schedules created here will be available for selection from schedule selection drop-down menus throughout the configuration utility.

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

Day(s): Click**All Week** to make the rule active for every day of the week. Click **Select Day(s)** to specify days on which to activate the rule. Days of the week can be selected by checking the boxes below.

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

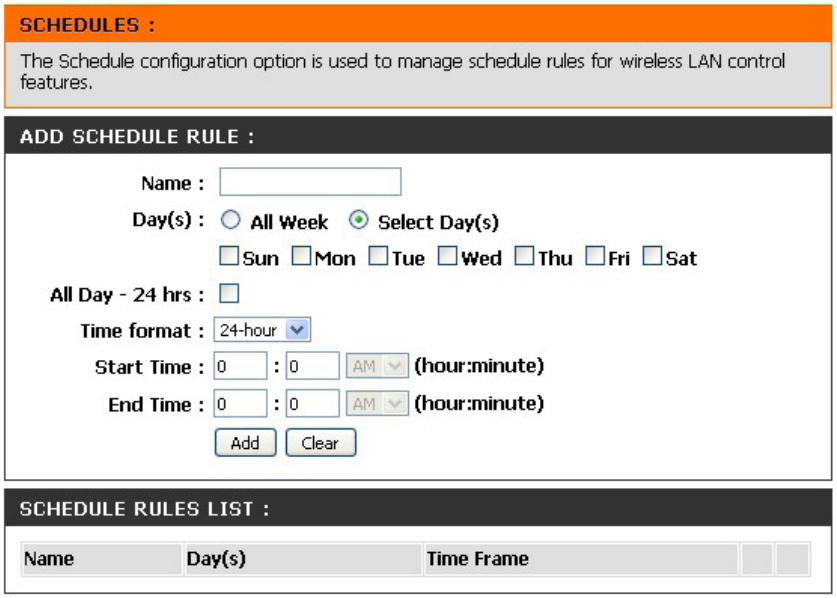
Time format: Select either **24-hour** or **12-hour** format for time display.

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

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

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

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



Status

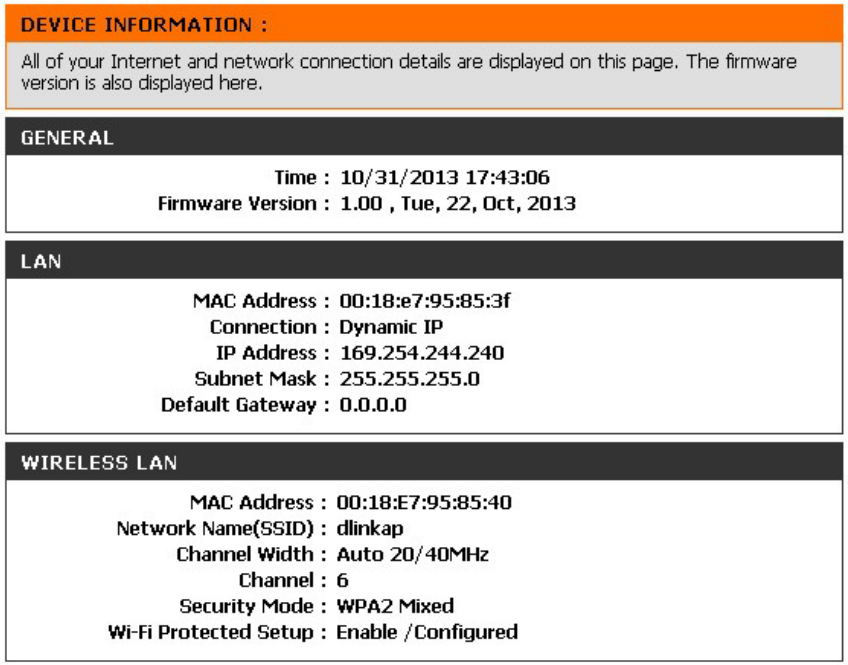
Device Info

This page displays the current information for the DAP-1665, such as *LAN* and *Wireless LAN* information and statistics.

General: Displays the access point's *Time (*as current date and time) and *Firmware Version*.

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

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



Logs

TheDAP-1665 keeps a running log of events and activities occurring on the access point. If the device is rebooted, the logs will automatically be cleared.

Log Options: You can select the types of logs that can be viewed: **System Activity, Debug Information, Attacks, Dropped Packets,** and **Notice**. Check the boxes to display log items of each type. Click **Apply Log Settings Now** to update the log options.

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

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

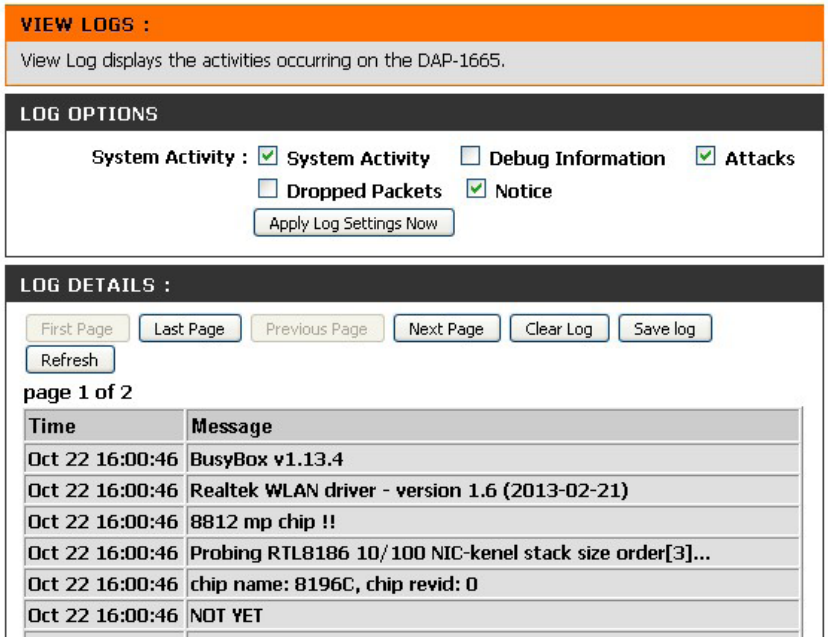
Previous Page: This button directs you to the previous page of the log.

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

Clear Log: This button clears all current log content.

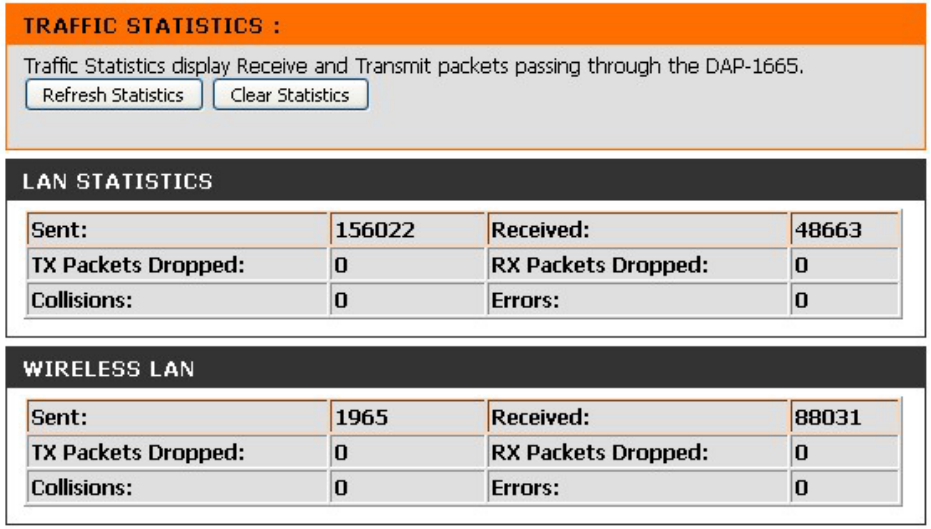
Save Log: This button allows you to save the current log to a file on your local computer.

Refresh: This button refreshes the log.



Statistics

The DAP-1665 keeps statistics of the traffic that passes through it. You can view the number of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the access point is rebooted. Use the buttons at the top of the page to **Refresh** or **Clear** the statistics.

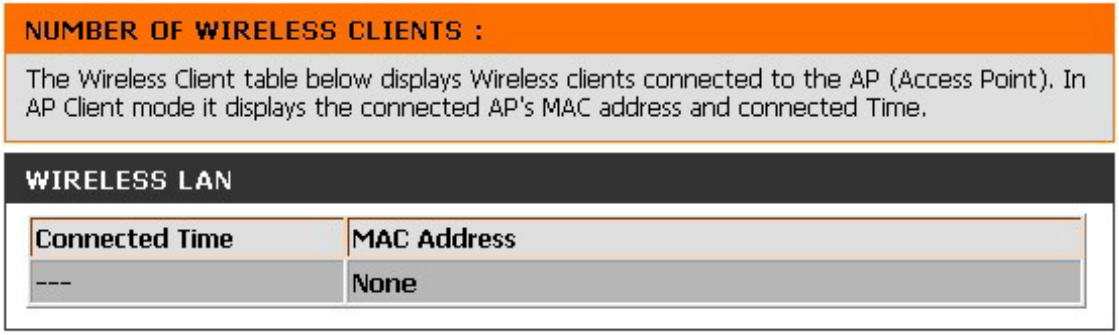


Wireless

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

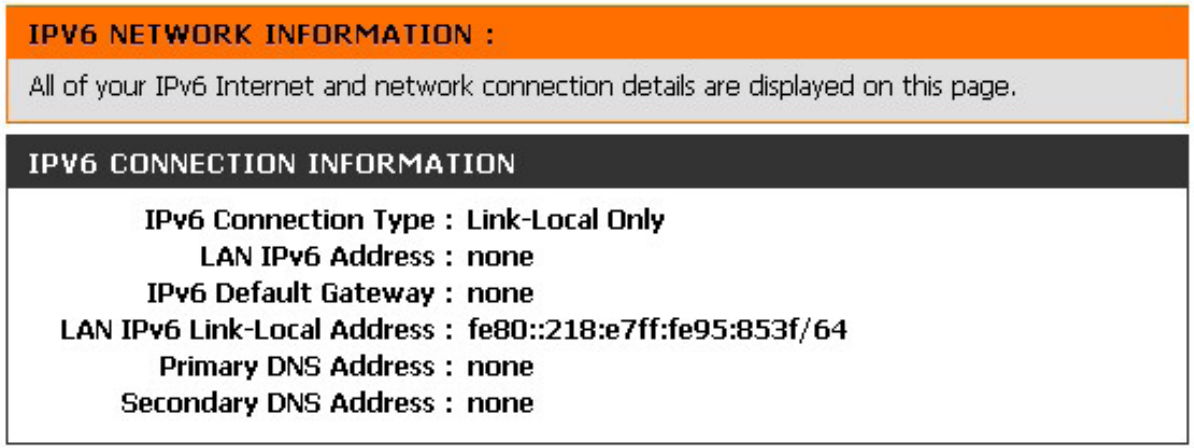
Connected Time: Displays the amount of time the wireless client has been connected to the access point.

MAC Address: The Ethernet ID (MAC address) of the wireless client.



IPv6

This page displays IPv6 Internet and network connection details.



Help Menu


HELP MENU
Setup
Wizard
Wireless Setup
LAN Setup
Advanced
MAC Address Filter
Advanced Wireless
Wi-Fi Protected Setup
User Limit
Maintenance
Device Administration
Save and Restore
Firmware Update
Time
Schedules
Status
Device Info
Log
Statistics
Wireless

Wireless Security

This section will explain the different types of security you can use to protect your wireless network from intruders. Please note that some security methods may not be available for all operation modes. The DAP-1665 offers the following types of security:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA/WPA2)
  - WPA - Personal
  - WPA - Enterprise

What is WEP?

Wired Equivalent Privacy (WEP) is an older form of wireless encryption which operates only in 802.11g legacy mode. WEP uses hex digits to create an authentication key, and is considered to be less secure than the newer WPA/WPA2 security standards. It is recommended that you only use this security mode if your wireless clients do not support WPA/WPA2.

What is WPS?

Wi-Fi Protected Setup (WPS) allows you to quickly and easily create a secure wireless connection between devices using a push-button or a PIN code. This method alleviates the need for users to change settings on their wireless devices, or remember security passwords. Many wireless devices have a physical push-button located somewhere on the exterior casing, while others may have a software button located within the device's configuration software. Please refer to your wireless device's documentation for further information on how to connect to the DAP-1665 using WPS.

What is WPA?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

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

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

Connecting to a Wireless Client

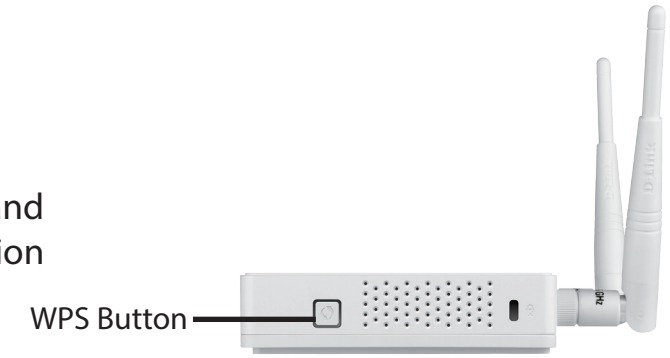
WPS Button

WPS (Wi-Fi Protected Setup) is a simple and secure way to connect your wireless devices with the DAP-1665 when using *Repeater* or *Wireless Client* mode. Most wireless devices such as wireless routers, media players, printers, and cameras will have a WPS button (or a software utility with WPS). Refer to the user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the **WPS** button on the DAP-1665 for a minimum of one second. The LED on the device will start to blink. (You can also use the WPS option in the *Wi-Fi Setup Wizard* as described in the *Configuration* section.)

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

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



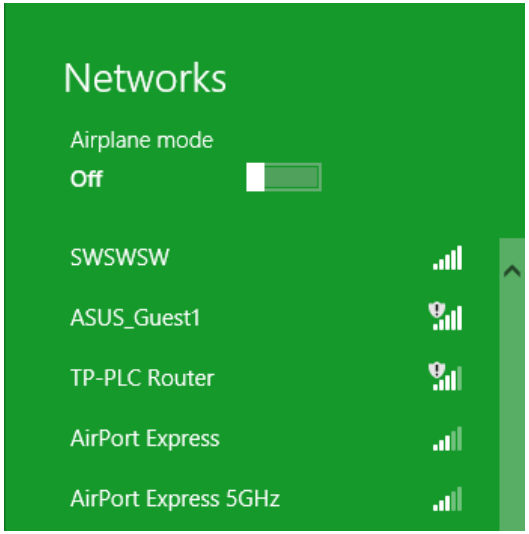
Connect to a Wireless Network
Windows® 8

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

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

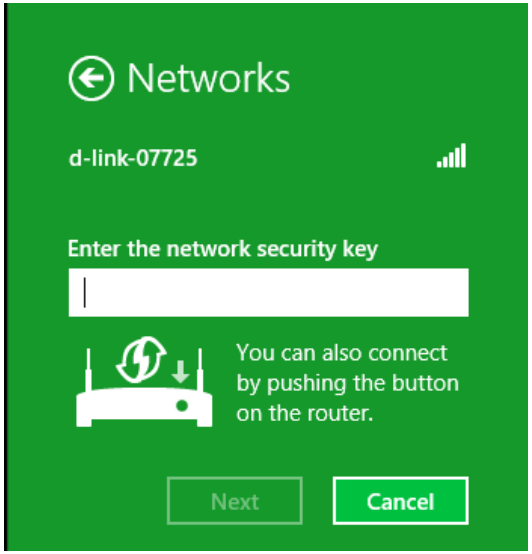
Wireless Icon

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

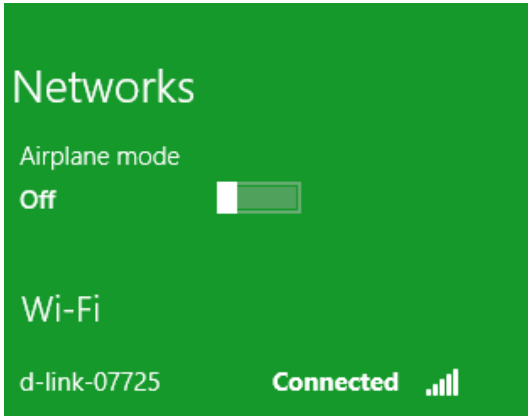


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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



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



Windows® 7

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

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

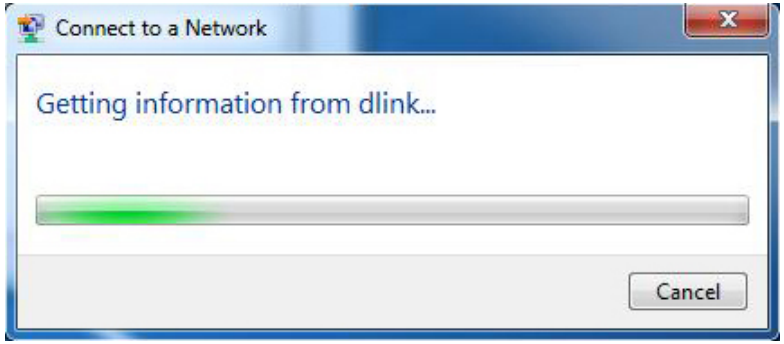
Wireless Icon

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

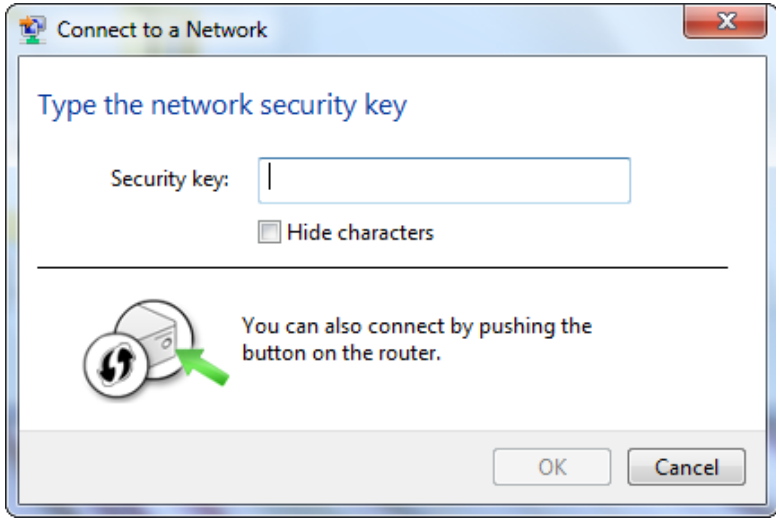
3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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

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



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



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

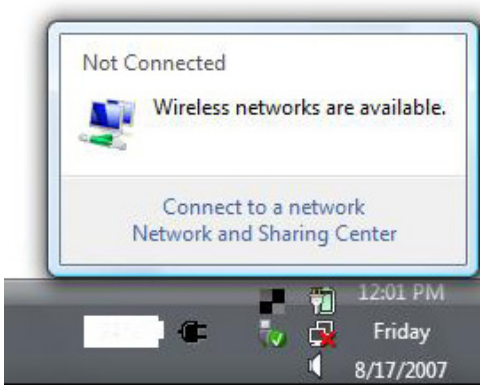
Windows Vista®

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

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

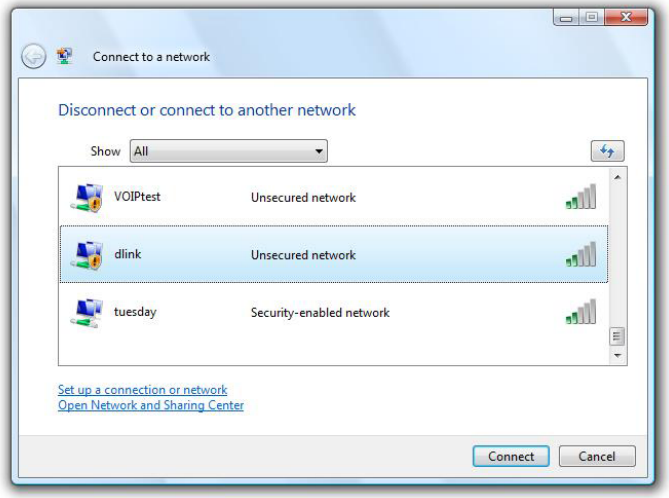
or

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



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

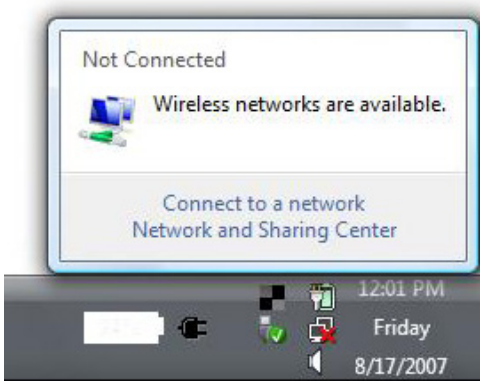
If you get a good signal but cannot access the Internet, check your TCP/IP settings of your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



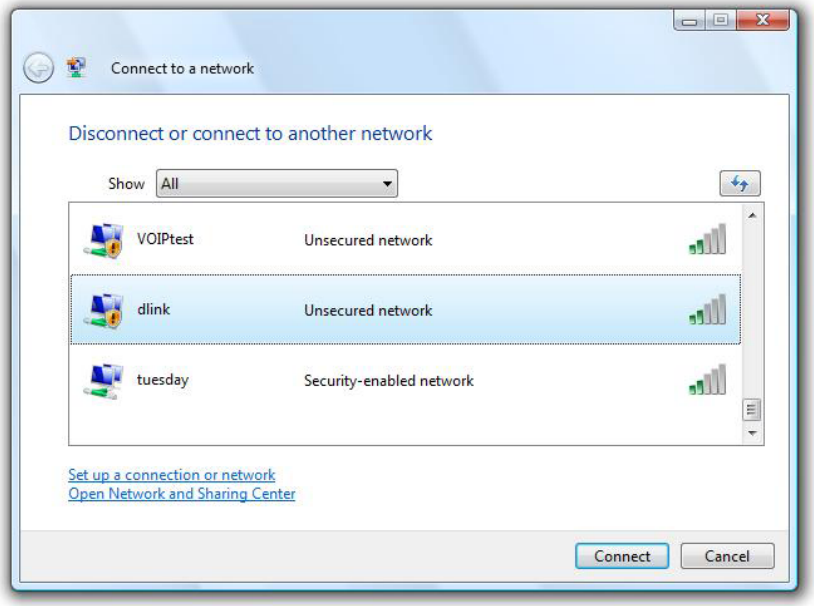
WPA/WPA2

It is recommended that you 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**.



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



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

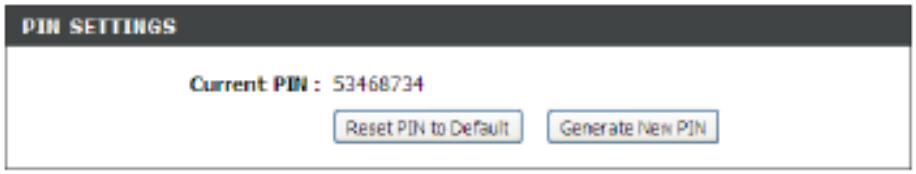
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

WPS/WCN 2.0

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

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

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

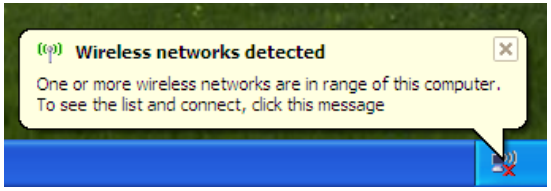


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Using Windows® XP

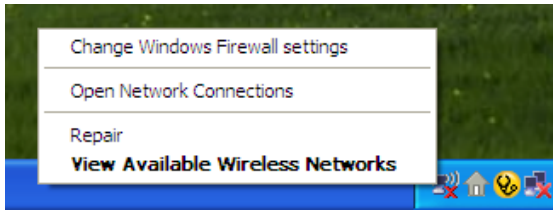
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

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



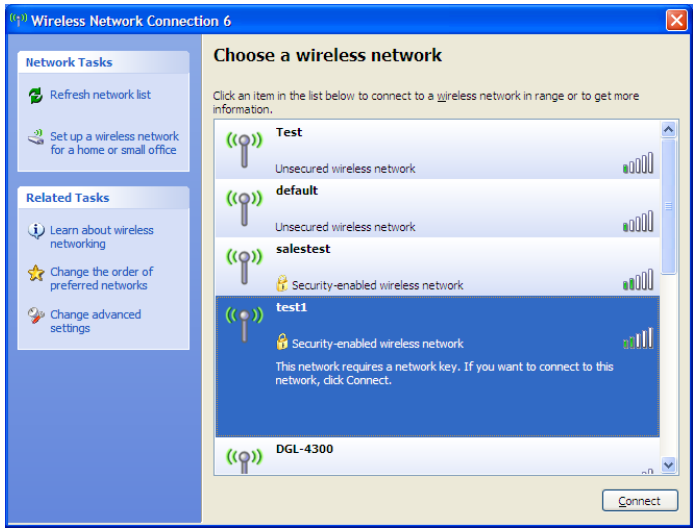
or

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



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

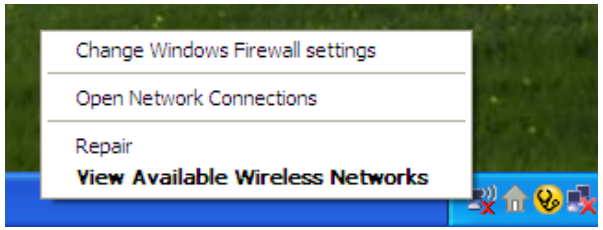
If you get a good signal but cannot access the Internet, check the TCP/IP settings of your wireless adapter. Refer to the Networking Basics section in this manual for more information.



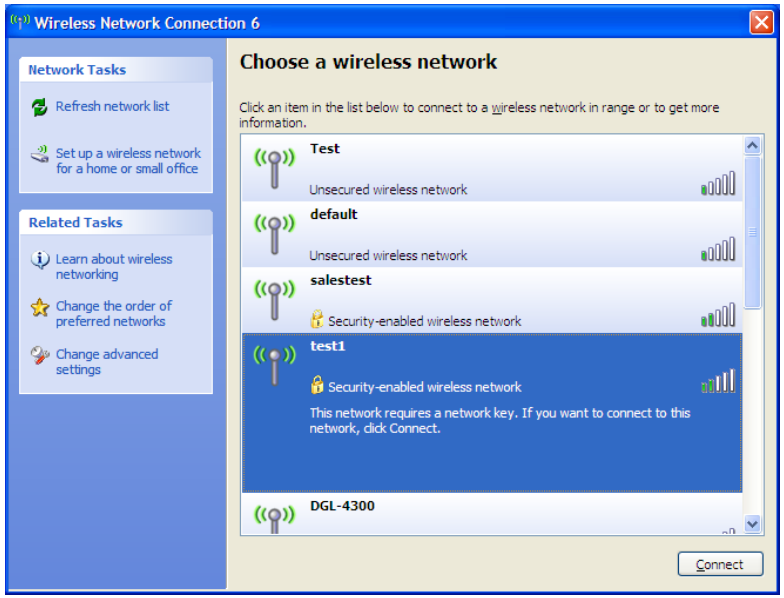
Configure WPA-PSK

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

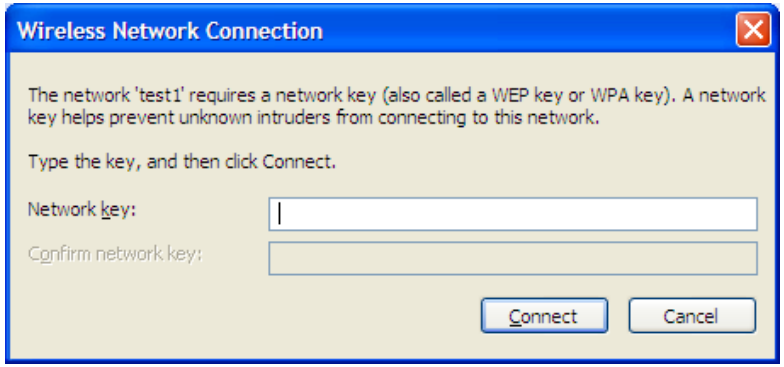
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-1665. Read the following descriptions if you are having problems.

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
    - Microsoft Internet Explorer® 8.0 or higher
    - Mozilla Firefox® 20.0 or higher
    - Google Chrome™ 20.0 or higher
    - Apple Safari® 4.0 or higher
- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
- Configure your Internet settings on your web browser:
    - 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.

- To access the web management interface, open your web browser and enter the IP address* of your D-Link access point in the address bar. This should open the login page for your the web management.

****Note:** The default IP address is **http://192.168.0.50**. Once the DAP-1665 connects to your router, it will be assigned a new IP address based on your router/network's DHCP settings. You will have to log in to your router and view the DHCP table to see what IP address was assigned to the DAP-1665. If you are using a D-Link router, follow these instructions to find the IP address that was assigned: Using the router's Web-based configuration utility, go to **Setup** > **Network Settings**. Scroll down to the bottom of the page, below the heading that says **Number of Dynamic DHCP Clients**, to view the list of connected devices. Refer to the MAC address that is printed on the label that is attached to the bottom of the DAP-1665 to find the corresponding IP address.*

- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug it 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 access point. Unfortunately this process will change all your settings back to the factory default settings.

To reset the access point, locate the reset button (hole) on the rear panel of the unit. With the access point powered on, use an unfolded paper clip to hold the button down for 10 seconds. Release the button and the access point will go through its reboot process.

Wait about 30 seconds to access the access point. The default IP address is **192.168.0.50**. When logging in, the username is Admin and leave the password field empty.

3. Why can't I connect to certain sites or send and receive emails when connecting through my access point?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and ME users type in *command* (Windows® NT, 2000, and XP users type in cmd) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

  ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your access point with the proper MTU size.

To change the MTU rate on your access point follow the steps below:

- Open your browser, enter the IP address of your access point (**192.168.0.50**) and click **OK.**
- Enter your username (Admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure.**
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely and conveniently access your network. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapters used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A wireless router is a device used to provide this link.

Tips

Here are a few things to keep in mind when you are installing your Wireless AC1200 Dual Band Access Point.

Centralize the extender's location

For best performance, make sure you place the extender in a centralized location within your desired usage area. Try to place the extender so that there are minimal obstructions between it and the uplink router. If possible, use an elevated power outlet, so the signal can be dispersed more easily. If you have a large home or usage area, you may need several extenders in order to achieve optimal coverage.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the extender. This can significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let your neighbors or intruders connect to your wireless network. Secure your wireless network by utilizing the WPA or WEP security feature on the extender and uplink router. Refer to "Wireless Security" on page 76 for more information.

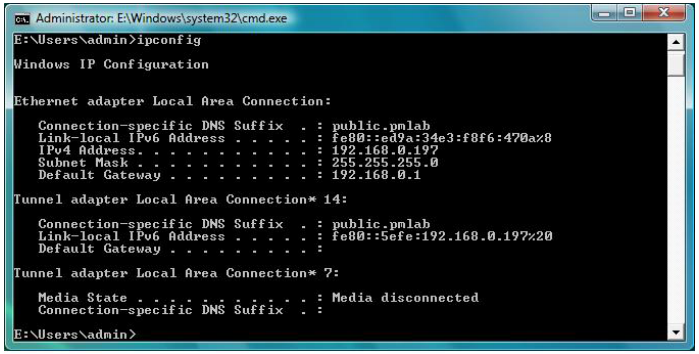
Networking Basics

Check your IP address

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

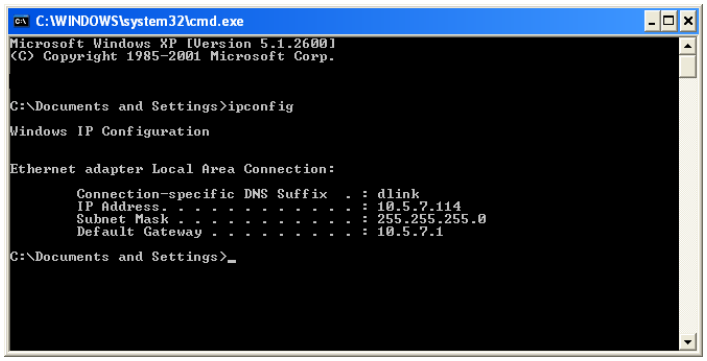
Windows® 8 Users

- Press the **Windows key** and **R** together. Type **cmd** in the box and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.



Windows® 7/Vista® Users

- Click **Start**, type **cmd** in the search box and then click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.



Windows® XP Users

- Click on **Start** > **Run**. In the run box type **cmd** and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and the default gateway of your adapter.

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

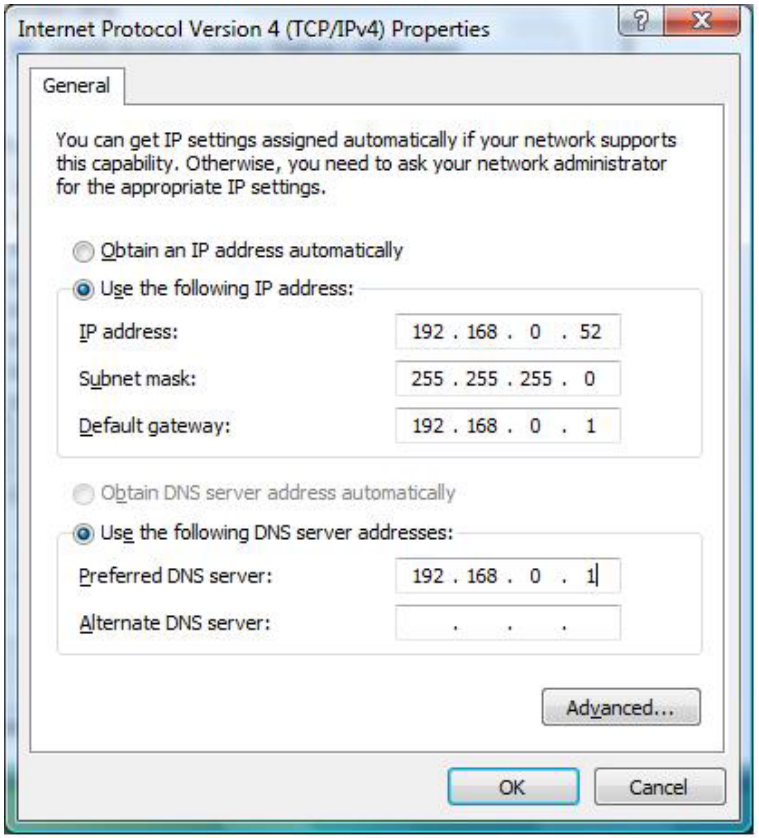
Statically Assign an IP Address

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

Windows® 8 Users

- Press the **Windows** key and then type **IP**. Click **Settings** on the right side and then click **View Network Connections**.
- Right-click on the adapter which represents your D-Link wireless network adapter.
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router or network.

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



Windows® 7/ Vista® Users

- Click on **Start** > **Control Panel** (make sure you are in Classic View). Double-click on the **Network and Sharing Center** icon. If you are using Windows Vista, click on **Manage network connections** along the left panel in the window. For Windows® 7, click on **Change adapter settings**.

- Right-click on the **Local Area Connection** which represents your D-Link wireless network adapter which will be connected to your network.

- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.

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

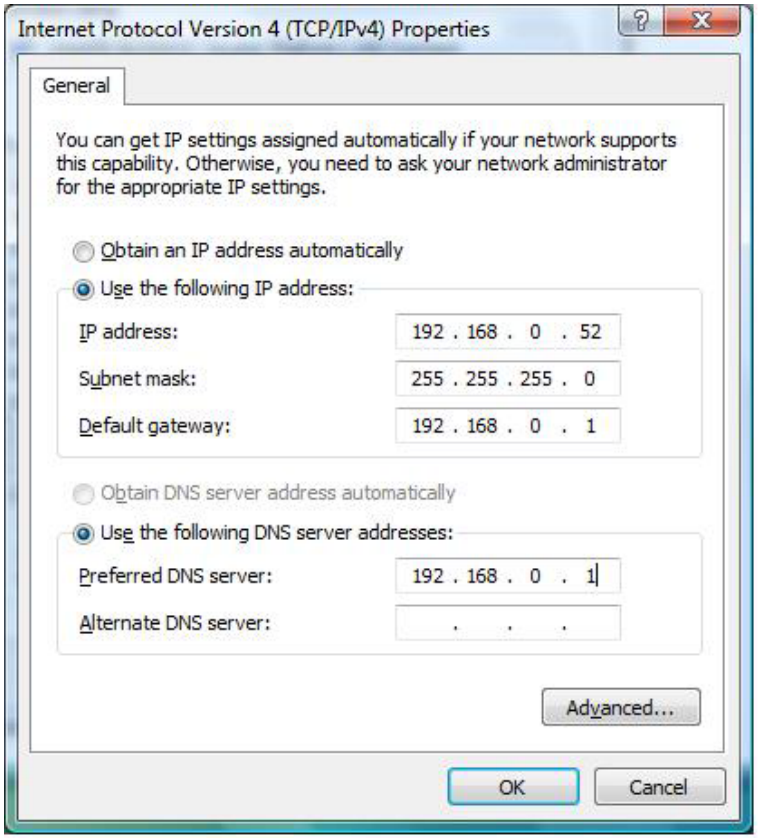
  Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.

- Set **Default Gateway** the same as the LAN IP address of your router or gateway.

- Set **Primary DNS** the same as the LAN IP address of your router or gateway.

- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).

- Click **OK** to save your settings.



Technical Specifications

Standards
- IEEE 802.11ac draft
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Security
- WPA/WPA2
  - Personal
  - Enterprise
- WPS
- WEP

Wireless Signal Rate
- Up to 1200 Mbps

Maximum Transmission Power[2]
- 2.4 GHz
  - 11n: 22dBm
  - 11g: 22dBm
  - 11b: 25dBm
- 5 GHz
  - 11ac: 21dBm
  - 11a: 21dBm
  - 11n: 20dBm

Maximum Operating Voltage
- 12 V 1A

Power Consumption
- 5.18 W

Frequency Range[3]
- 2.4 GHz Band:
  - 2.4 - 2.4835 GHz
- 5 GHz Band:
  - 5.15 GHz to 5.35 GHz
  - 5.47 GHz to 5.85 GHz

Antennas
- Two 2 dBi external antennas or, two 3/5 dBi external antennas[2]

LEDs
- Power
- 2.4 GHz wireless
- 5 GHz wireless
- LAN

Temperature
- Operating
  - 32°F to 131°F (0°C to 55°C)
- Storage
  - -4 to 149 °F (-20 to 65 °C)

Humidity
- Operating
  - 10 - 90% (non-condensing)
- Storage
  - 5 - 95% (non-condensing)

Safety & Emissions
- CE
- FCC
- TELEC
- IC
- Wi-Fi Certified
- VCCI

Dimensions
- 5.79 x 4.25 x 1.1 in (47 x 108 x 27.8 mm)

Weight
- 0.489 lbs (222 grams)

[1] Maximum wireless signal rate derived from IEEE Standard draft 802.11ac, 802.11n and 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.
[2] All Maximum transmission power values expressed are for dual-chain mode. Maximum transmission power and included antennas may vary depending on regional regulations.
[3] Frequency Range may vary depending on regional regulations.

Contacting Technical Support

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

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

- Model number of the product (e.g. DAP-1665)
- Hardware Revision (located on the label on the device (e.g. rev A1))
- Serial Number (s/n number located on the label on the device).

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

For customers within the United States:

Phone Support:
(877) 453-5465

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(800) 361-5265

Internet Support:
http://support.dlink.ca

GPL Code Statement

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

http://tsd.dlink.com.tw/GPL.asp

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPLsource code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Please direct all inquiries to:
Email: GPLCODE@DLink.com
Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Systems, Inc.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

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 non-commercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work). You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.
A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.
The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation. If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.
THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

Warranty

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

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

Limited Warranty:

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

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

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

Limited Software Warranty:

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

Non-Applicability of Warranty:

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

Submitting A Claim (USA):

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

Submitting A Claim (Canada):

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

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-800-361-5265, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.ca/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

- RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

What Is Not Covered:

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

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

Disclaimer of Other Warranties:

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

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

Limitation of Liability:

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

Governing Law:

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

Trademarks:

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

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

CE Mark Warning:

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

FCC Statement:

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

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

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

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

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

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:
This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

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

Declaration d'exposition aux radiations:
Cet equipement est conforme aux limites d'exposition aux rayonnements IC etablies pour un environnement non controle. Cet equipement doit etre installe et utilise avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Registration

Register your product online at registration.dlink.com

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

Version 1.0
January 3, 2014