



User Manual

Wireless N300 Access Point

Table of Contents

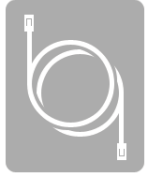
Package Contents.....	4	Access Point Mode	30
System Requirements	5	Repeater Mode	32
Introduction	6	Wireless Client Mode	33
Features.....	8	Bridge Mode	34
Hardware Overview	9	Bridge with AP Mode.....	35
Connections	9	WISP Client Router/WISP Repeater Modes.....	36
LEDs	10	WAN Settings	37
WPS LED/WPS Button	11	Dynamic IP (DHCP).....	37
Installation	12	Static IP	38
Operation Modes.....	12	PPPoE	39
Access Point Mode	13	PPTP	40
Wireless Client Mode	14	LAN Settings	41
Repeater Mode	15	Static IP	42
Bridge Mode	16	DHCP Server	43
Bridge with AP Mode	17	Advanced	44
WISP Client Router Mode.....	18	Advanced Wireless	44
WISP Repeater Mode.....	19	MAC Address Filter	45
Wireless Installation Considerations.....	20	Wi-Fi Protected Setup	46
Configuration	21	User Limits.....	47
Web-based Configuration Utility	21	Port Forwarding (WISP modes only)	48
Wireless Setup Wizard.....	22	Port Filter (WISP modes only)	49
Access Point Mode	23	DMZ (WISP modes only)	50
Repeater Mode	25	Parental Control (WISP modes only).....	51
Wireless Client Mode	27	Advanced Network (WISP modes only)	52
Manual Configuration.....	29	Maintenance	53
Wireless Settings.....	29	Admin	53
		System	54

Language Pack.....	55	Troubleshooting	82
Firmware	55	Wireless Basics	86
Watchdog	56	What is Wireless?.....	87
Time	57	Tips.....	89
System Check.....	58	Wireless Modes.....	90
Schedules	59	Networking Basics	91
Status	60	Check your IP address.....	91
Device Info	60	Statically Assign an IP address	92
Logs	61	Technical Specifications	93
Statistics	62		
Wireless	63		
Help	64		
Wireless Security	65		
What is WPA?	66		
Configure WPA/WPA2 Personal	67		
Configure WPA/WPA2 Enterprise	68		
Connect to a Wireless Network.....	69		
Using Windows® XP	69		
Configure WPA-PSK.....	70		
Using Windows Vista®	72		
Configure WPA-PSK.....	74		
Using Windows® 7	75		
Configure WPS	78		

Package Contents



DAP-2020 Wireless N300 Access Point



Ethernet Cable



Two Detachable Antennas



Power Adapter

Note: Using a power supply with a different voltage rating than the one included with the DAP-2020 will cause damage and void the warranty for this product.

System Requirements

Network Requirements	<ul style="list-style-type: none">• An Ethernet-based Network• IEEE 802.11n/g wireless clients (AP/Repeater Mode)• IEEE 802.11n/g wireless network (Client/Bridge/Repeater Mode)• 10/100 Ethernet
Web-based Configuration Utility Requirements	<p>Computer with the following:</p> <ul style="list-style-type: none">• Windows®, Macintosh, or Linux-based operating system• An installed Ethernet adapter <p>Browser Requirements:</p> <ul style="list-style-type: none">• Microsoft Internet Explorer® 11 and higher• Mozilla Firefox 28 and higher• Google™ Chrome 33 and higher• Apple Safari 7 and higher <p>Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.</p>

Introduction

D-Link, an industry leader in networking, introduces the new D-Link DAP-2020 Wireless N300 Access Point. With the ability to transfer files with a maximum wireless signal rate of up to 300Mbps*, the DAP-2020 gives you high-speed wireless network access for your home or office.

The DAP-2020 is Wi-Fi IEEE 802.11n compliant, meaning that it can connect and interoperate with other 802.11n compatible wireless client devices. The DAP-2020 is also backwards compatible with 802.11b/g. It can be flexibly configured to operate in 7 different modes **Access Point, Wireless Client, Bridge, Bridge with AP, Repeater, WISP Client Router** or **WISP Repeater**. With its Setup Wizard, the DAP-2020 ensures that you will be up and running on a wireless network in just a matter of minutes.

The DAP-2020 features Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) to provide an enhanced level of security for wireless data communications. The DAP-2020 also includes additional security features to keep your wireless connection safe from unauthorized access.

The DAP-2020 supports WPS on the AP, repeater and wireless client operation modes, with each capable of being conveniently set up by using the PIN method or Push Button.

• 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.

TOTAL PERFORMANCE

Combines award winning access point features and 802.11n wireless technology to provide the best wireless performance.

TOTAL SECURITY

The most complete set of security features including WPA/WPA2 encryption to protect your network against outside intruders.

TOTAL COVERAGE

Provides greater wireless signal rates even at farther distances for best-in-class Whole Home Coverage.

ULTIMATE PERFORMANCE

The D-Link Wireless N300 Access Point (DAP-2020) is an 802.11n compliant device that delivers real world performance of up to 13X faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the DAP-2020 to router and share your high-speed Internet access with everyone on the network. In addition, this Range Extender includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

EXTENDED WHOLE HOME COVERAGE

This high performance Wireless Bridge provides superior Whole Home Coverage while reducing dead spots. The DAP-2020 is designed for use in bigger homes and for users who demand higher performance networking.

TOTAL NETWORK SECURITY

The DAP-2020 supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA and WPA2 standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices.

POWER USAGE

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed.

Network Standby: 2.30 watts

Switched Off: 0.19 watts

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

Features

- **Faster Wireless Networking** - The DAP-2020 provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.
- **Compatible with IEEE802.11g Devices** - The DAP-2020 is still fully compatible with the 802.11g standards, so it can connect with existing 802.11g PCI, USB, and Cardbus adapters.
- **Advanced Firewall Features** - The Web-based user interface displays advanced network management features including Content Filtering, which allows easily applied content filtering based on MAC Address.
- **WPS PBC**- (Wi-Fi Protected Setup Push Button Configuration) Push Button Configuration is a button that can be pressed to add the device to an existing network or to create a new network. A virtual button can be used on the utility while a physical button is placed on the side of the device.
This easy setup method allows you to form a secured wireless link between the DAP-2020 and another WPS enabled device. A PC is no longer needed to log into the Web-based interface.
- **WPS PIN** - (Wi-Fi Protected Setup Personal Identification Number) A PIN is a unique number that can be used to add the access point to an existing network or to create a new network. The default PIN may be printed on the bottom of the access point. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DAP-2020 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company’s server. Configure your access point to your specific settings within minutes.

Hardware Overview

Connections



1	Reset Button	Pressing the Reset Button restores the access point to its original factory default settings.
2	LAN Port	Connect 10/100 Ethernet devices such as computers, switches, and hubs.
3	Power Button	Push the Power Button to switch power on/off.
4	Power Receptor	Receptor for the supplied power adapter.

Hardware Overview

LEDs



1	Power LED	A solid green light indicates a proper connection to the power supply.
2	Wireless LED	A solid green light indicates the wireless function is working. The light will be off during device reboot or if the wireless radio is disabled.
3	Security LED	A solid green light indicates that wireless security (WEP, WPA, WPA2) is enabled. It also indicates WPS status when using WPS button. A solid light indicates a successful WPS connection. A blinking light indicates the device is trying to establish a connection.
4	LAN LED	A solid green light indicates the LAN port connection is OK.

Hardware Overview

WPS LED/WPS Button



1	WPS Button	Push the WPS Button to use WPS function
----------	-------------------	---

Installation

Please configure the DAP-2020 with a computer connected directly to the AP. The next few pages will explain the different operational modes you can use.

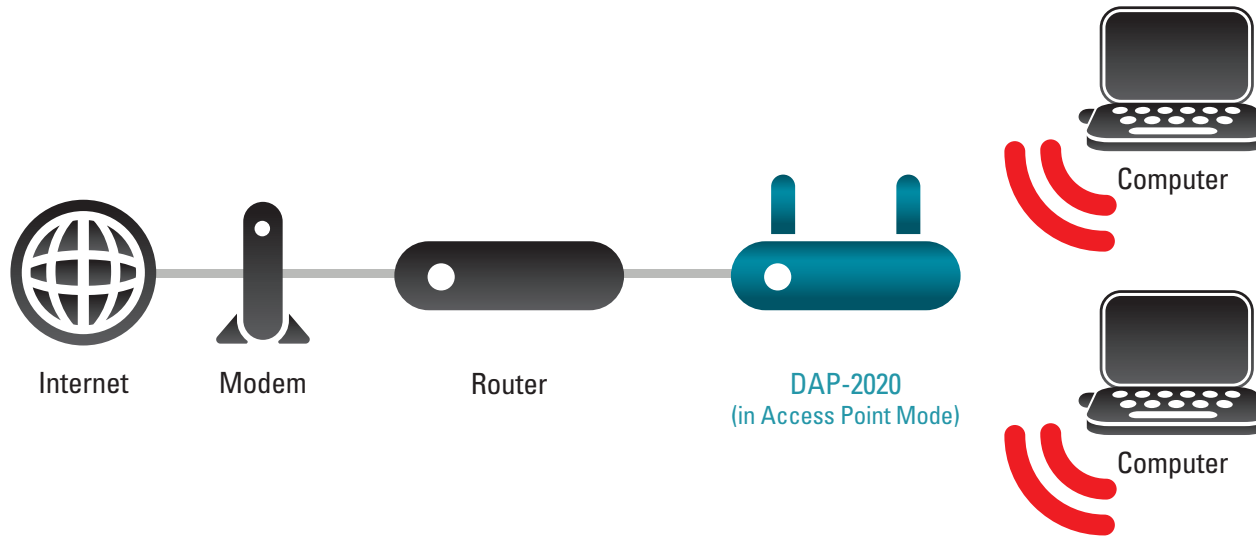
Operation Modes

Depending on how you want to use your DAP-2020 will determine which mode you use. This section will help you figure out which setting works with your setup.

- Access Point mode - page 13
- Wireless Client mode - page 14
- Repeater mode - page 15
- Bridge mode - page 16
- Bridge with AP mode - page 17
- WISP Client Router mode - page 18
- WISP Repeater mode - page 19

Access Point Mode

In the Access Point mode, the DAP-2020 acts as a central connection point for any computer (client) that has a 802.11n or backward-compatible 802.11g wireless network interface and is within range of the AP. Clients must use the same SSID (wireless network name) and channel as the AP in order to connect. If wireless security is enabled on the AP, the client will need to enter a password to connect to the AP. In Access Point mode, multiple clients can connect to the AP at the same time.

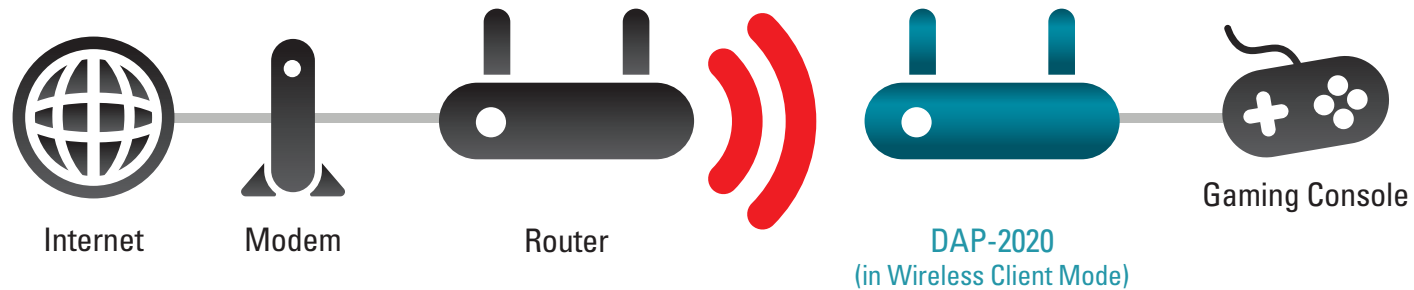


Wireless Client Mode

In the Wireless Client mode, the DAP-2020 acts as a wireless network adapter for your Ethernet-enabled device (such as a game console or a TV set-top box). Connect your Ethernet-enabled device to the AP using an Ethernet cable. The AP Client mode can support multiple wired clients.

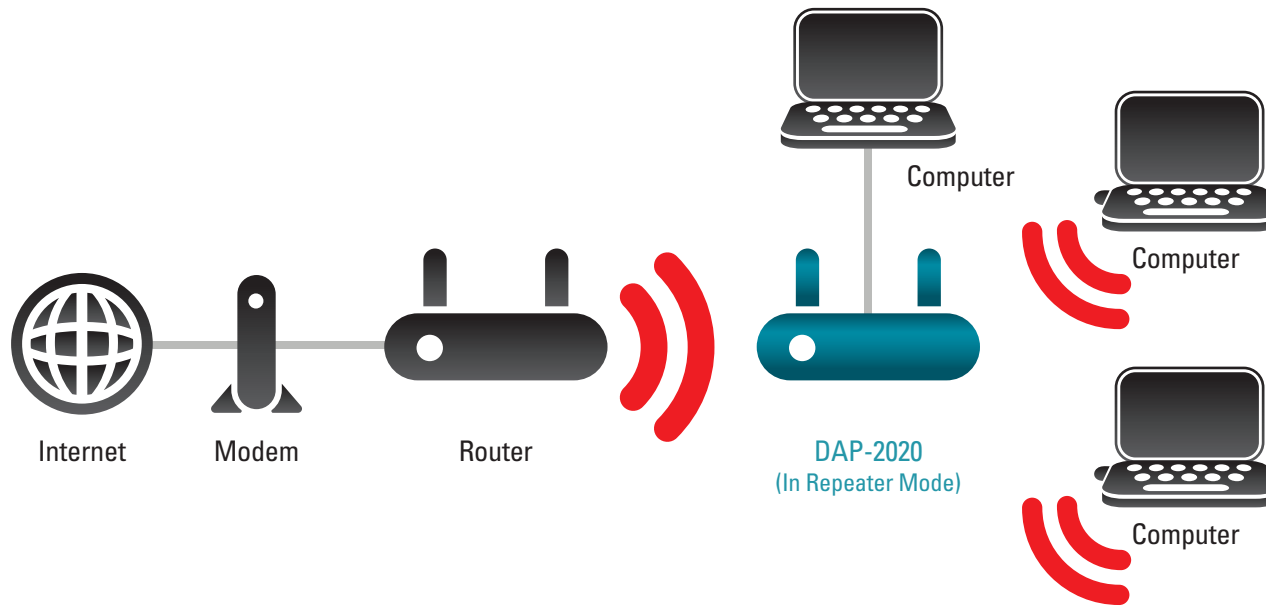
If you are going to connect several Ethernet-enabled devices to your DAP-2020, connect the LAN port of the DAP-2020 to an Ethernet switch, then connect your devices to this switch.

Example: Connect a gaming console using an ethernet cable to the DAP-2020. The unit is set to Wireless Client mode which will wirelessly connect to a wireless router on your network.



Repeater Mode

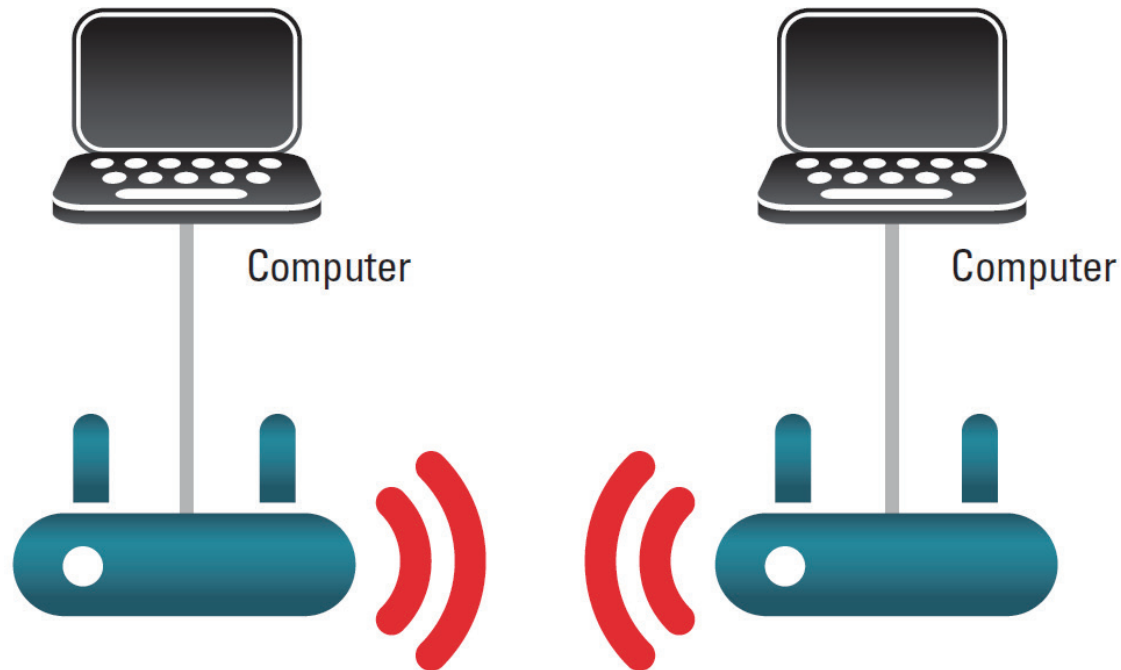
In Repeater mode, the DAP-2020 increases the range of your wireless network by extending the wireless coverage of another AP or wireless router. The APs and wireless router (if used) must be within range of each other. Make sure that all clients, APs, and the wireless router all use the same SSID (wireless network name), channel, and security settings.



Bridge Mode

In the Bridge mode, the DAP-2020 wirelessly connects separate local area networks (LANs) that can't easily be connected together with a cable. For example, if there are two wired LANs separated by a small courtyard, it would be expensive to bury cables to connect between the two sides together. A better solution is to use two DAP-2020 units to wirelessly connect the two LANs. In the Bridge mode, both DAP-2020 units do not act as APs.

Note: *The Bridge mode is not specified in the Wi-Fi or IEEE standards. This mode will only work using two DAP-2020 units. Communication with other APs (even other D-Link APs) is not guaranteed.*

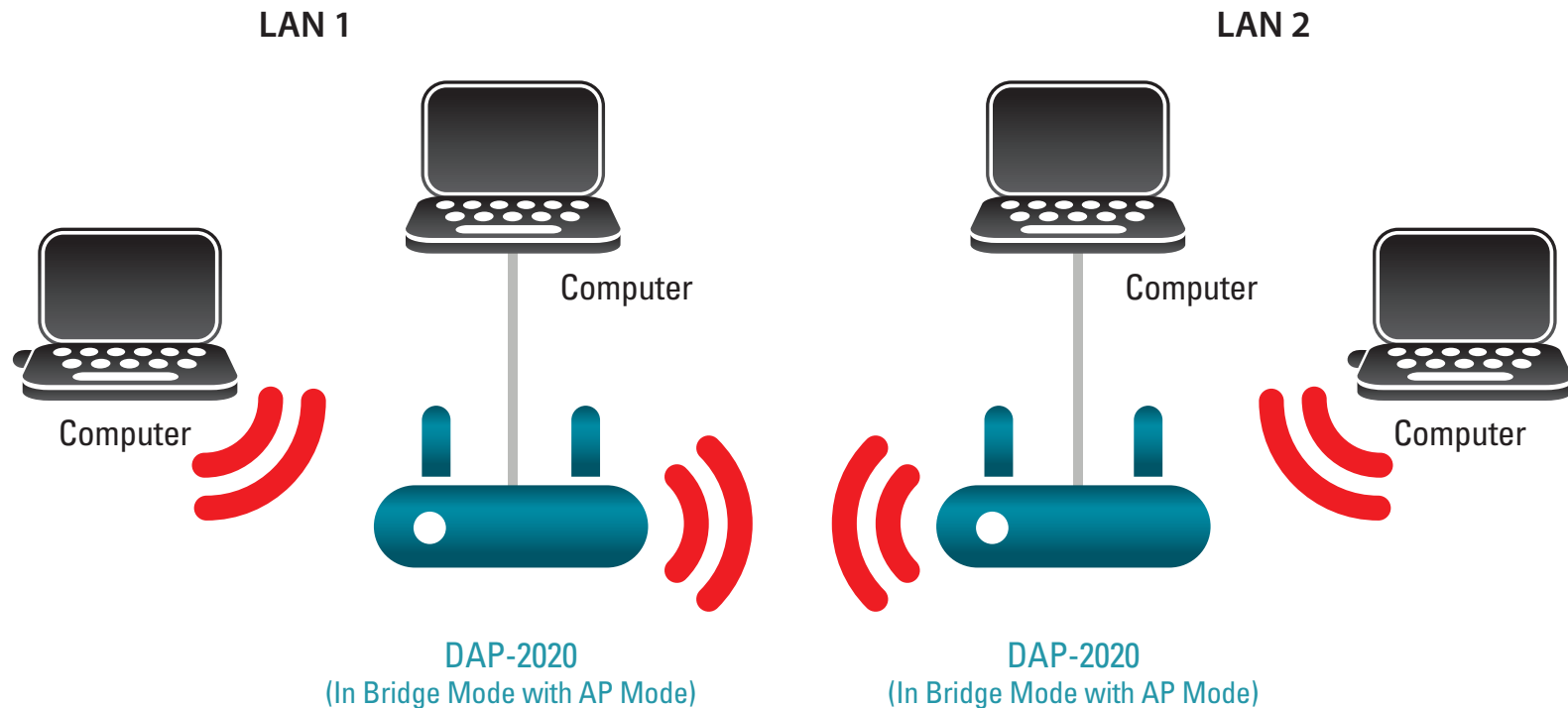


Connecting Two Separate LANs Together Through Two DAP-2020 Units

Bridge with AP Mode

The Bridge with AP mode is the same as the Bridge mode, but in this case, the DAP-2020 also acts as an AP. Clients with wireless interfaces can wirelessly connect to the DAP-2020 and then connect to the other LAN that the DAP-2020 bridges to.

Note: The Bridge with AP mode is not specified in the Wi-Fi or IEEE standards. This mode will only work using two DAP-2020 units. Communication with other APs (even other D-Link APs) is not guaranteed.

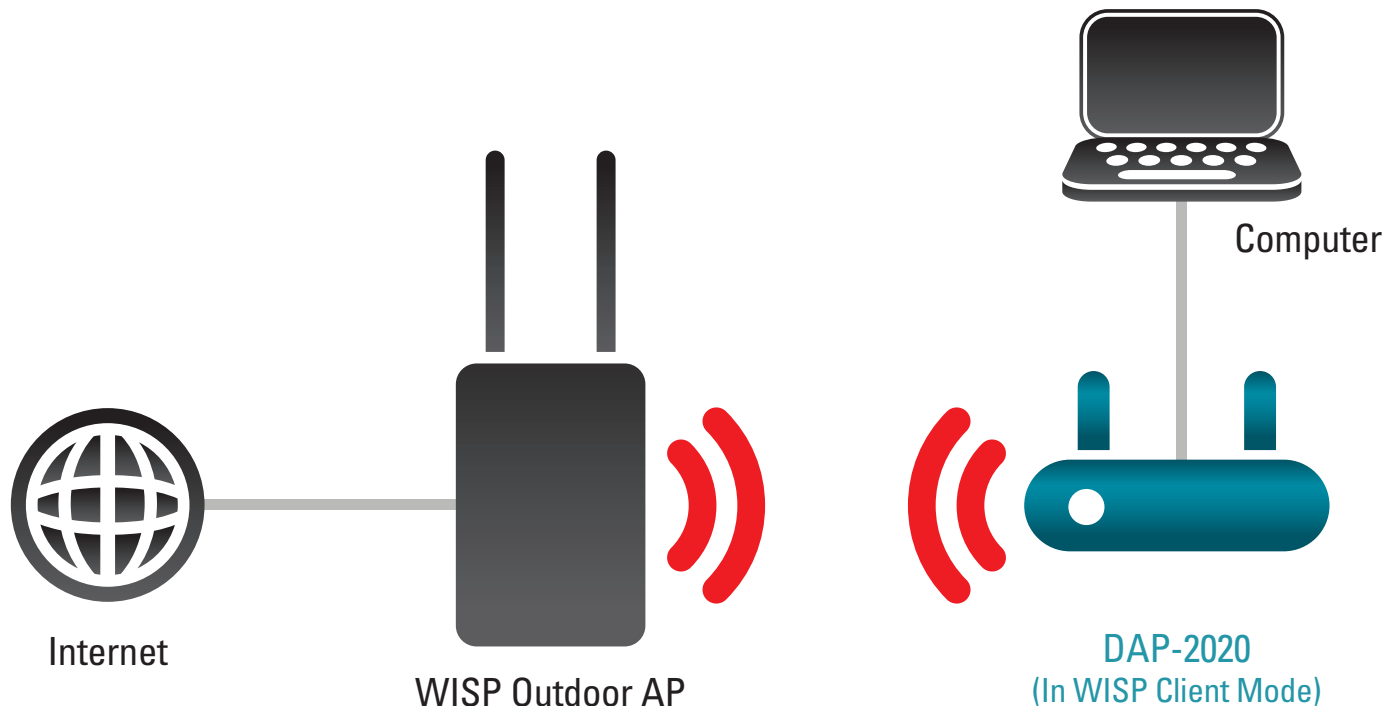


**Connecting Two Separate LANs Together Through Two DAP-2020 Units
(Wireless PCs Can Access the DAP-2020 Units)**

WISP Client Router Mode

In the WISP Client Router mode, the DAP-2020 wirelessly connects to a WISP (Wireless Internet Service Provider) AP. In this mode, the DAP-2020 also acts as a router for wired clients on your LAN and provides NAT (Network Address Translation) and a DHCP server to generate IP addresses for wired clients only. NAT and the DHCP server allow many computers to share the same wireless Internet connection.

If you are a WISP subscriber and want to access your WISP account using wired computers, connect your computers to the DAP-2020 to get NAT, and then connect them to the WISP AP.

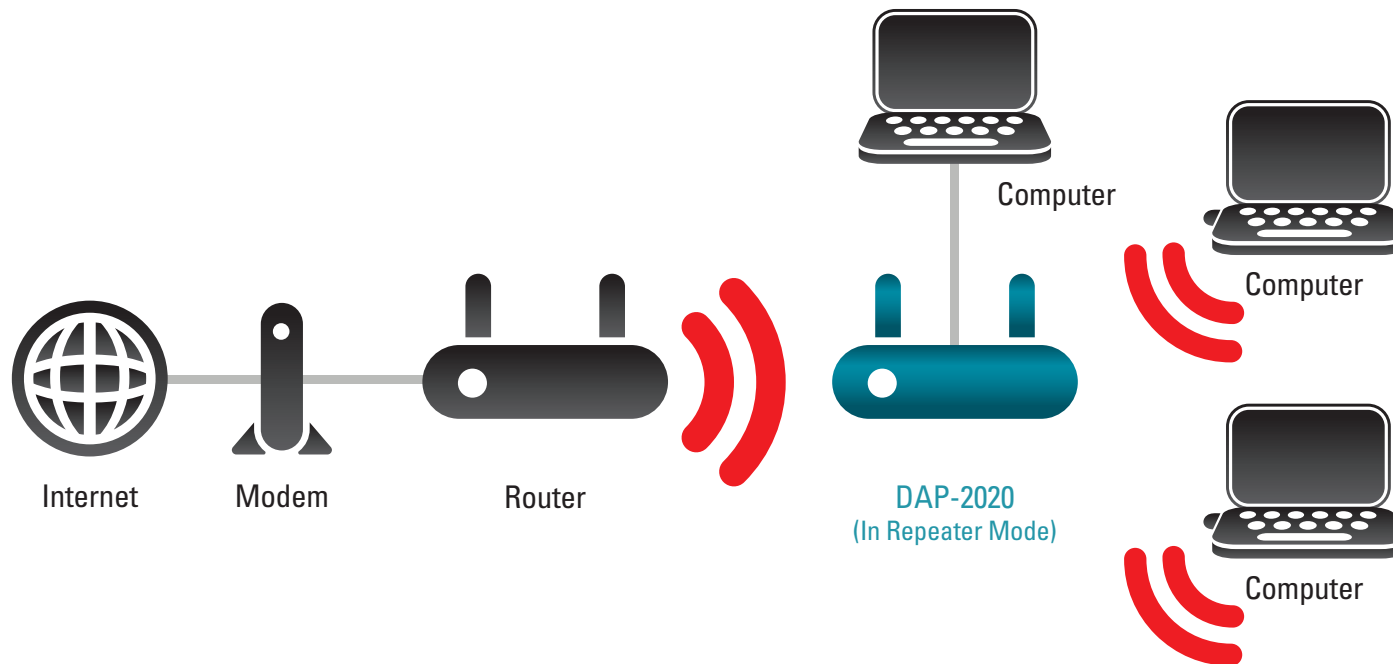


Connecting Wired PCs to the Internet Using the DAP-2020

WISP Repeater Mode

In the WISP Repeater mode, the DAP-2020 wirelessly connects to a WISP (Wireless Internet Service Provider) AP. In this mode, the DAP-2020 also acts as a router for both wireless and wired clients on your LAN. The WISP Repeater mode provides NAT (Network Address Translation) and a DHCP server to generate IP addresses for both wireless and wired clients. NAT and the DHCP server allow many computers to share the same wireless Internet connection.

If you are a WISP subscriber and want to use your WISP account in your house, but the signals from the outdoor WISP AP are not strong enough to reach all of the areas in the house, use the DAP-2020 to extend the signals from the outdoor WISP AP and provide access to wireless clients in your house. Using this mode, wireless as well as wired clients can connect to the outdoor WISP AP through the DAP-2020.



Connecting Wired and Wireless PCs to the Internet Using the DAP-2020

Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the 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. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless access points, 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 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Configuration

This section will show you how to configure your new D-Link wireless access point using the web-based configuration utility.

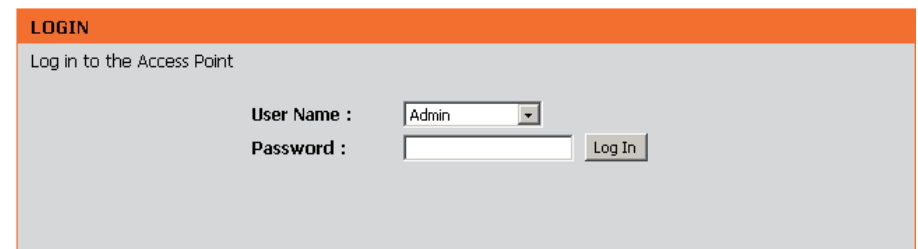
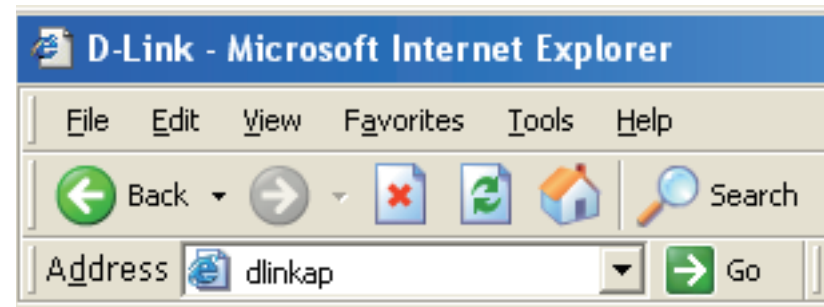
Web-based Configuration Utility

If you wish to change the default settings or optimize the performance of the DAP-2020, you may use the web-based configuration utility.

To access the configuration utility, open a web browser such as Internet Explorer and enter **http://dlinkap** in the address field.

Select **Admin** and then enter your password. Leave the password blank by default.

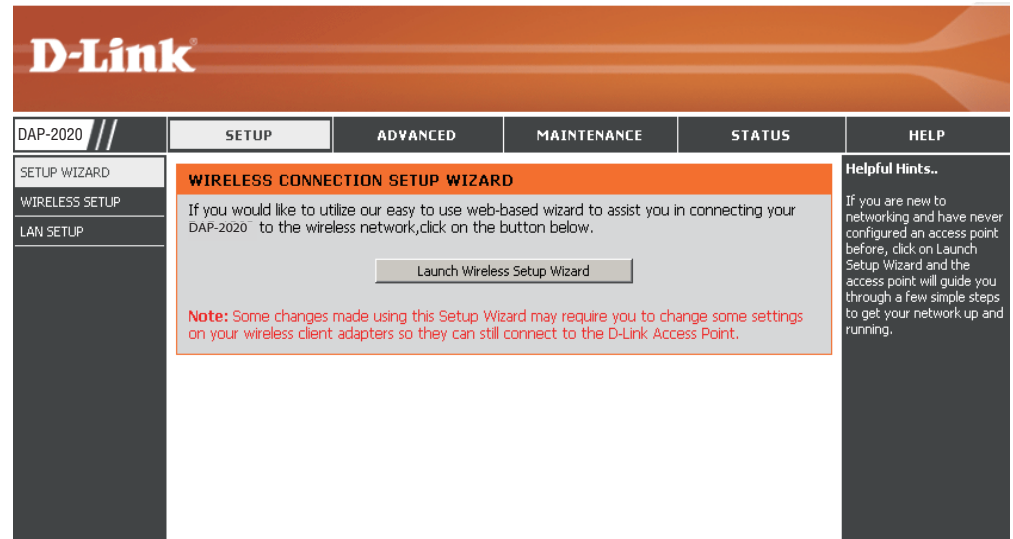
If you get a Page Cannot be Displayed error, please refer to the **Troubleshooting** section for assistance.



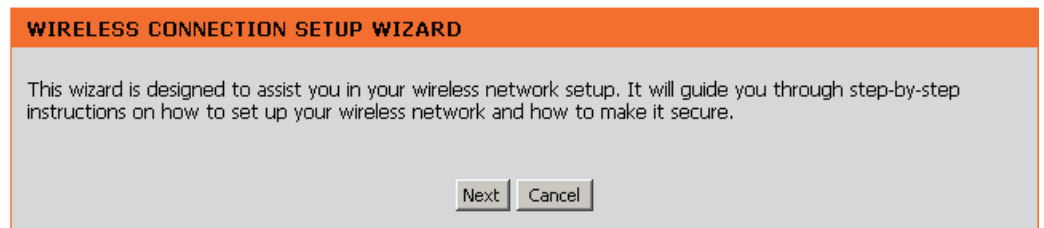
Wireless Setup Wizard

Click **Launch Wireless Setup Wizard** to configure your access point.

If you want to enter your settings without running the wizard, skip to page 34.



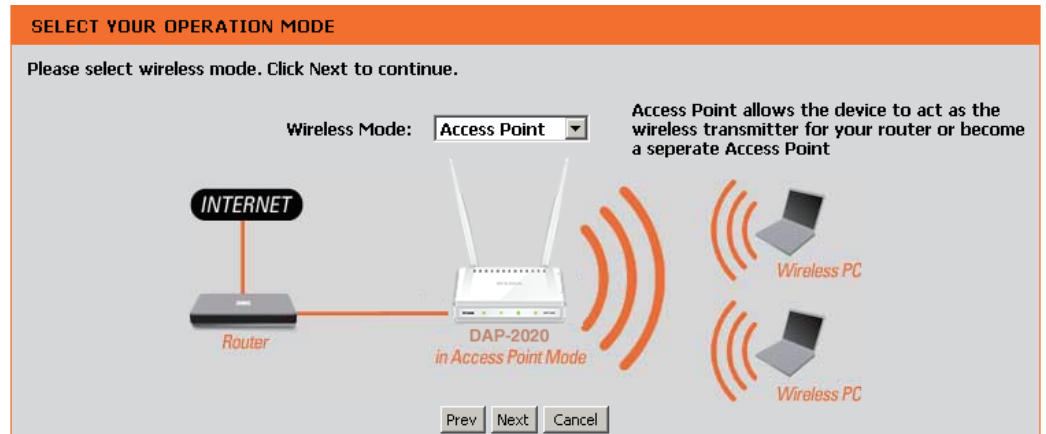
Click **Next** to continue.



Access Point Mode

This Wizard is designed to assist you in configuring your DAP-2020 as an access point.

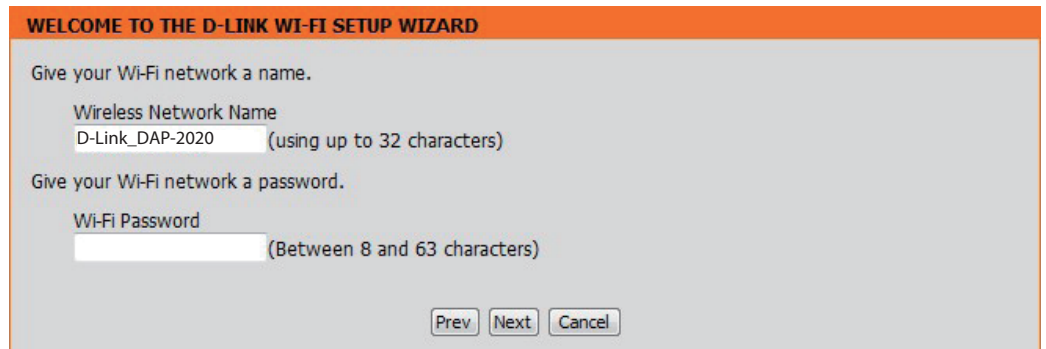
Select **Access Point** from the drop-down menu. Then, click **Next** to continue.



Enter a name for your wireless network (SSID).

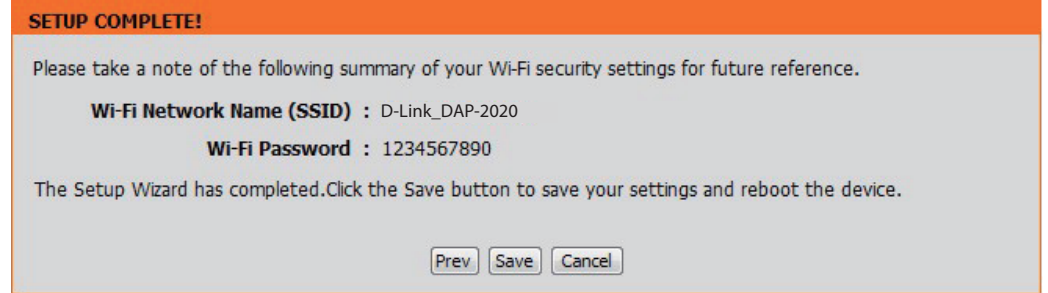
Enter your Wi-Fi Password. This Password must be entered on your wireless clients.

Click **Next** to continue.



The following screen will show you your network key to enter on your wireless clients.

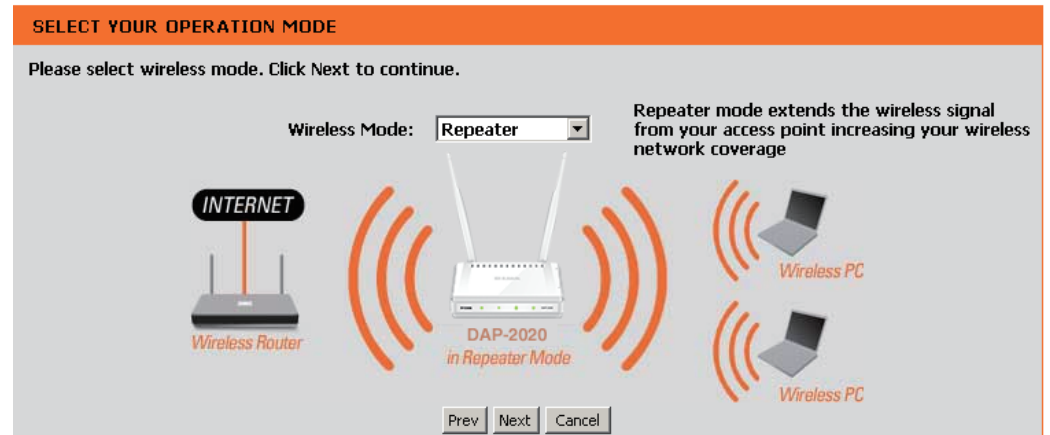
Click **Save** to finish the Setup Wizard.



Repeater Mode

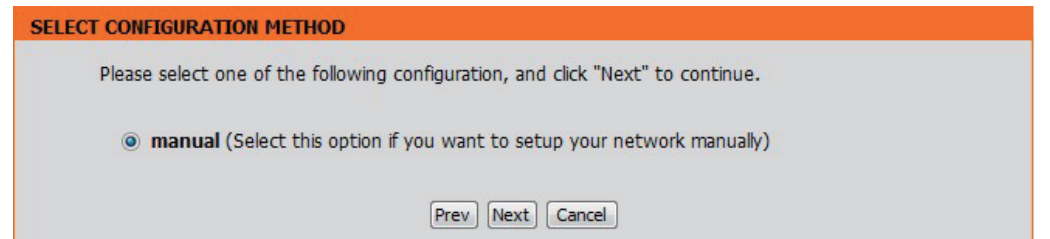
This Wizard is designed to assist you in configuring your DAP-2020 as a repeater.

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



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

Click **Next** to continue.



Section 3 - Configuration

Find your router or access point from the list, click the radio button in the right column, and click **Connect**.

SELECT WI-FI NETWORK

ID	Wi-Fi Network Name	Encrypt	Channel	Signal (%)	Select
1	CX468	WPA-PSK/WPA2-PSK(aes)	4	91	<input type="radio"/>
2	Apple Martini	WPA-PSK(auto)/WPA2-PSK(auto)	11	39	<input type="radio"/>
3	dlink-guest	no	4	29	<input type="radio"/>
4	Dlink_NewUI_24G	WPA-PSK(auto)/WPA2-PSK(auto)	4	29	<input type="radio"/>
5	wireless123	WPA2-PSK(aes)	11	20	<input type="radio"/>
6	dlink-andy	WPA-PSK(auto)/WPA2-PSK(auto)	9	20	<input type="radio"/>
7	845neutrino	WPA-PSK(auto)/WPA2-PSK(auto)	11	20	<input type="radio"/>
8	AirPort Express	WPA2-PSK(aes)	11	20	<input type="radio"/>
9	ray845-24g	WPA-PSK(auto)/WPA2-PSK(auto)	11	10	<input type="radio"/>
10	dlink-8575	WPA-PSK(auto)/WPA2-PSK(auto)	1	10	<input type="radio"/>
11	dlink_645L_Betty	WPA-PSK(auto)/WPA2-PSK(auto)	10	10	<input type="radio"/>
12	DIR508L_DESK	WPA-PSK(auto)/WPA2-PSK(auto)	3	10	<input type="radio"/>
13	Shareplay_Timmy	WPA-PSK(auto)/WPA2-PSK(auto)	8	10	<input type="radio"/>

Enter the Wi-Fi password. Click **Next** to complete the Setup Wizard.

ENTER WI-FI PASSWORD

Please enter Wi-Fi Password to establish wireless connection.

Wi-Fi Password:

The Wireless Setup Wizard is complete. Click **Save** to reboot the device.

SETUP COMPLETE!

Please take a note of the following summary of your Wi-Fi security settings for future reference.

Wi-Fi Network Name (SSID) : CX468

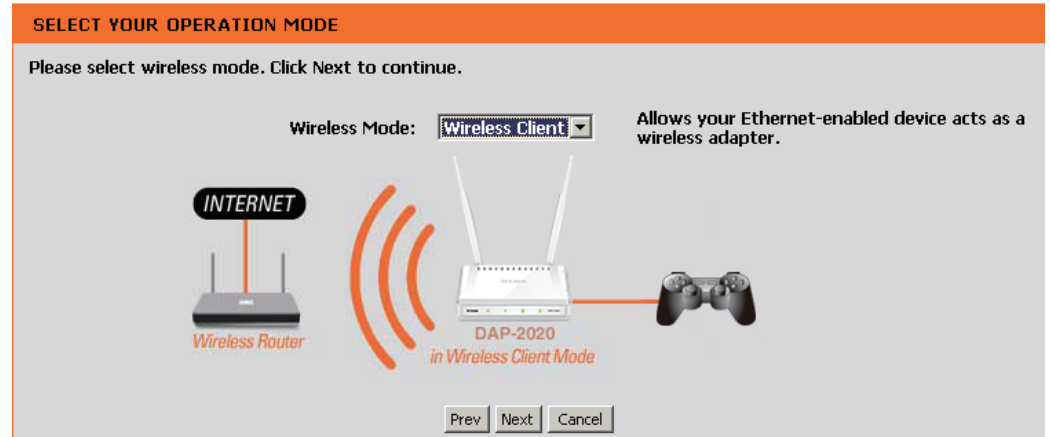
Wi-Fi Password : 1234567890

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

Wireless Client Mode

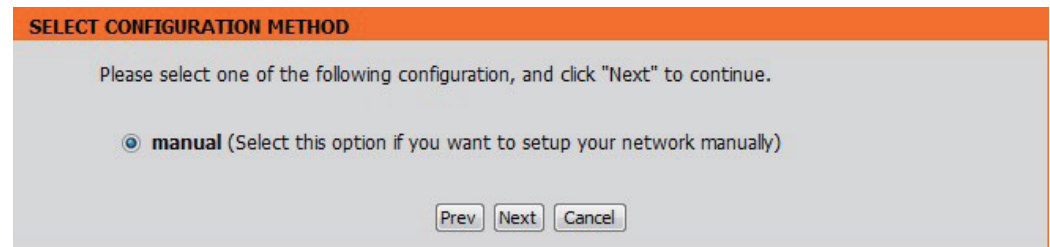
This Wizard is designed to assist you in configuring your DAP-2020 as a wireless client.

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



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

Click **Next** to continue.



Section 3 - Configuration

Find your access point from the list, click the radio button in the right column, and click **Connect**.

SELECT WI-FI NETWORK

ID	Wi-Fi Network Name	Encrypt	Channel	Signal (%)	Select
1	CX468	WPA-PSK/WPA2-PSK(aes)	4	70	<input type="radio"/>
2	Dlink_NewUI_24G	WPA-PSK(auto)/WPA2-PSK(auto)	4	29	<input type="radio"/>
3	Shareplay_Timmy	WPA-PSK(auto)/WPA2-PSK(auto)	8	29	<input type="radio"/>
4	Apple Martini	WPA-PSK(auto)/WPA2-PSK(auto)	11	29	<input type="radio"/>
5	dlink-guest	no	4	29	<input type="radio"/>
6	D-Link	no	6	26	<input type="radio"/>
7	AirPort Express	WPA2-PSK(aes)	11	20	<input type="radio"/>
8	dlink-andy	WPA-PSK(auto)/WPA2-PSK(auto)	9	20	<input type="radio"/>
9	845neutrino	WPA-PSK(auto)/WPA2-PSK(auto)	11	20	<input type="radio"/>
10	D-Link	no	1	13	<input type="radio"/>
11	dlink-8575	WPA-PSK(auto)/WPA2-PSK(auto)	1	10	<input type="radio"/>
12	dlink-435D	WPA-PSK(auto)/WPA2-PSK(auto)	3	10	<input type="radio"/>
13	ray845-24g	WPA-PSK(auto)/WPA2-PSK(auto)	11	10	<input type="radio"/>
14	DIR508L_DESK	WPA-PSK(auto)/WPA2-PSK(auto)	3	10	<input type="radio"/>
15	dlink_645L_Betty	WPA-PSK(auto)/WPA2-PSK(auto)	10	10	<input type="radio"/>
16	wireless123	WPA2-PSK(aes)	11	10	<input type="radio"/>
17	Shai-Hulud	WPA-PSK/WPA2-PSK(aes)	8	10	<input type="radio"/>

Enter the Wi-Fi password. Click **Next** to complete the Setup Wizard.

ENTER WI-FI PASSWORD

Please enter Wi-Fi Password to establish wireless connection.

Wi-Fi Password:

The Wi-Fi Setup Wizard is complete. Click **Save** to reboot the device.

CONNECT TO WIRELESS DEVICE

The Wi-Fi setup wizard has completed

Manual Configuration

Wireless Settings

You may manually configure your DAP-2020 instead of running the setup wizard.

- Access Point mode - page 30
- Repeater mode - page 32
- Wireless Client mode - page 33
- Bridge mode - page 34
- Bridge with AP mode - page 35
- WISP Client Router mode - page 36
- WISP Repeater mode - page 36

Access Point Mode

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. You may also set up a specific time range (schedule). Select a schedule from the drop-down menu or click **Add New** to create a new schedule.

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

Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the default network name.

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 11g wireless clients.
- Mixed 802.11n, 802.11g and 802.11b** - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

Wireless Channel: Indicates the channel setting for the DAP-2020. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Scan, this option will be grayed out.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DAP-2020 to choose the channel with the least amount of interference.

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

SETUP WIZARD
WIRELESS SETUP
LAN SETUP

WIRELESS NETWORK

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

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS :

Enable Wireless : Always Add New

Wireless Mode : Access Point See Survey

Wireless Network Name : Dlink (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Wireless Channel : 6

Enable Auto Channel Scan :

Channel Width : 20MHz

Visibility Status : (Also called Disable SSID Broadcast)

WIRELESS SECURITY MODE :

Security Mode : None

Helpful Hints..

Wireless Mode :
Select a function mode to configure your wireless network. Function wireless modes include Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router and WISP Repeater. Function wireless modes are designed to support various wireless network topologies and applications.

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

Hidden Wireless :
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.

Security Keys :
If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this

Channel Width: Select the Channel Width:

Auto 20/40 - 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: Check the box if you do not want the SSID of your wireless network to be broadcasted by the DAP-2020. If checked, the SSID of the DAP-2020 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DAP-2020 in order to connect to it.

Security Mode: Refer to page 65 for more information regarding the wireless security.

Repeater Mode

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. You may also set up a specific time range (schedule). Select a schedule from the drop-down menu or click **Add New** to create a new schedule.

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

Site Survey: Click **Site Survey** to display a list of wireless networks in your area. You may select the wireless access point to connect to.

Wireless Network Name: Enter the SSID of the access point you want to repeat the signal of. If you do not know for sure, click **Site Survey** and select it from the list, if available.

802.11 Mode: Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are **802.11n Only**, **Mixed 802.11n and 802.11g**, or **Mixed 802.11n, 802.11g and 802.11b**.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DAP-2020 to choose the channel with the least amount of interference.

Wireless Channel: The channel will automatically change to the channel of the AP you are connected to.

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

Visibility Status: Check the box if you do not want the SSID to be broadcast by the DAP-2020. This prevents the SSID from being seen by site survey utilities, so any wireless clients will have to be pre-configured with the SSID of the DAP-2020 in order to connect to it.

Wireless Security Mode: Select a wireless security setting. Options are **None**, **WEP**, **WPA**, or **WPA2**. See the Wireless Security section in this manual for a detailed explanation of the wireless security options.

The screenshot shows the D-Link configuration web interface for a DAP-2020 device. The main navigation bar includes 'DAP-2020 //', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar contains 'SETUP WIZARD', 'WIRELESS SETUP', and 'LAN SETUP'. The main content area is titled 'WIRELESS NETWORK' and contains the following settings:

- WIRELESS NETWORK SETTINGS :**
 - Enable Wireless :** Always
 - Wireless Mode :** Repeater
 - Wireless Network Name :** Dlink (Also called the SSID)
 - 802.11 Mode :** Mixed 802.11n, 802.11g and 802.11b
 - Wireless Channel :** 6
 - Enable Auto Channel Scan :**
 - Channel Width :** 20MHz
 - Visibility Status :** (Also called Disable SSID Broadcast)
- WIRELESS SECURITY MODE :**
 - Security Mode :** None

On the right side, there are two help sections:

- Helpful Hints..**
 - Wireless Mode :** Select a function mode to configure your wireless network. Function wireless modes include Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router and WISP Repeater. Function wireless modes are designed to support various wireless network topologies and applications.
 - Wireless Network Name :** Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
 - Hidden Wireless :** Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.

Wireless Client Mode

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

Wireless Type: Click **Site Survey** to display a list of wireless networks in your area. You may select the wireless access point to connect to. Select **Infrastructure** if connecting to an access point or wireless router, or select **Ad-Hoc** if connecting to another wireless client.

Wireless Network Name: Enter the SSID of the access point you want to repeat the signal of. If you do not know for sure, click **Site Survey** and select it from the list, if available.

802.11 Mode: Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are **802.11n Only**, **Mixed 802.11n and 802.11g**, or **Mixed 802.11n, 802.11g and 802.11b**.

Wireless Channel: The channel will automatically change to the channel of the AP you are connected to.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DAP-2020 to choose the channel with the least amount of interference.

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

Visibility Status: Check the box if you do not want the SSID to be broadcast by the DAP-2020. This prevents the SSID from being seen by site survey utilities, so any wireless clients will have to be pre-configured with the SSID of the DAP-2020 in order to connect to it.

Wireless MAC Clone: You can clone the wireless MAC address to connect the device.

Wireless Security Mode: Select a wireless security setting. Options are **None**, **WEP**, **WPA**, or **WPA2**. See the Wireless Security section in this manual for a detailed explanation of the wireless security options.

WPS: Select enable if you want to configure the DAP-2020 with Wi-Fi Protection setup.

The screenshot shows the D-Link web interface for the DAP-2020. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The main content area is titled "WIRELESS NETWORK" and contains the following sections:

- WIRELESS NETWORK:** A header section with a note: "Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made on this section may also need to be duplicated on your wireless client." Below this are "Save Settings" and "Don't Save Settings" buttons.
- WIRELESS NETWORK SETTINGS:** A section with several configuration options:
 - Wireless Mode:** A dropdown menu set to "Wireless Client" and a "Site Survey" button.
 - Wireless Type:** A dropdown menu set to "Infrastructure".
 - Wireless Network Name:** A text input field containing "Dlink" with a note "(Also called the SSID)".
 - 802.11 Mode:** A dropdown menu set to "Mixed 802.11n, 802.11g and 802.11b".
 - Wireless Channel:** A dropdown menu set to "6".
 - Enable Auto Channel Scan:** A checkbox that is currently unchecked.
 - Channel Width:** A dropdown menu set to "20MHz".
 - Visibility Status:** A checkbox labeled "(Also called Disable SSID Broadcast)" that is currently unchecked.
- WIRELESS MAC CLONE:** A section with:
 - Enable:** An unchecked checkbox.
 - MAC Source:** A dropdown menu set to "Auto".
 - MAC Address:** An empty text input field.
 - A "Scan" button.
 - A "MAC Address" label above another empty text input field.
- WIRELESS SECURITY MODE:** A section with:
 - Security Mode:** A dropdown menu set to "None".
- WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA):** A section with:
 - Enable:** A checked checkbox.
 - Current PIN:** A text input field containing "16343160".
 - "Generate New PIN" and "Reset PIN to Default" buttons.

On the right side of the interface, there is a "Helpful Hints..." section with several sub-sections: "Wireless Mode", "Wireless Network Name", "Hidden Wireless", "Security Keys", and "Bridge setting", each providing additional context and instructions for the user.

Bridge Mode

Enable Wireless: Select this to turn the Wi-Fi module on and off. Use the drop-down box to select if you want to use a schedule. Click **Add New** to add or change a schedule.

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

Wireless Network Name: The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your own wireless network name in this field.

802.11 Mode: Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are **802.11n Only, Mixed 802.11n and 802.11g, or Mixed 802.11n, 802.11g and 802.11b.**

Wireless Channel: All devices on the network must share the same channel.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DAP-2020 to choose the channel with the least amount of interference.

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

Visibility Status: Select the transmission rate. It is strongly suggested to use the Auto setting for optimal performance.

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

Bridge Security: Select None to disable encryption to across the network. Select WEP 64-bit or WEP 128-bit to limit communication to only those devices that share the same WEP settings. Select **WPA-PSK** or **WPA2-PSK** to secure your network using a password and dynamic key changes (No RADIUS server required).

Note: The Bridge mode is not completely specified in the Wi-Fi or IEEE standards. This mode can work with other DAP-2020 units. Communication with other APs (even other D-Link APs) is not guaranteed.

The screenshot shows the D-Link web interface for the DAP-2020. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar shows a menu with options: SETUP WIZARD, WIRELESS SETUP, and LAN SETUP. The main content area is divided into two sections:

- WIRELESS NETWORK:** This section contains instructions and configuration options. It includes a "Save Settings" button and a "Don't Save Settings" button. The "WIRELESS NETWORK SETTINGS" section includes:
 - Enable Wireless:** A checked checkbox with a dropdown menu set to "Always" and an "Add New" button.
 - Wireless Mode:** A dropdown menu set to "Bridge" and a "Site Survey" button.
 - Wireless Network Name:** A text field containing "Dlink" with a note "(Also called the SSID)".
 - 802.11 Mode:** A dropdown menu set to "Mixed 802.11n, 802.11g and 802.11b".
 - Wireless Channel:** A dropdown menu set to "6".
 - Enable Auto Channel Scan:** An unchecked checkbox.
 - Channel Width:** A dropdown menu set to "20MHz".
 - Visibility Status:** An unchecked checkbox with a note "(Also called Disable SSID Broadcast)".
- BRIDGE SETTING:** This section includes:
 - Remote AP Mac:** Eight numbered text input fields (1-8) for entering MAC addresses.
 - Bridge Security:** A dropdown menu set to "none".
 - WEP Key:** A text input field with a dropdown menu set to "ASCII".
 - Pre-Shared Key:** A text input field with a note "(8~63 char.)".

On the right side of the interface, there are "Helpful Hints..":

- Wireless Mode:** Select a Function mode to configure your wireless network. Function wireless modes include Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router and WISP Repeater. Function wireless modes are designed to support various wireless network topologies and applications.
- Wireless Network Name:** Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a Familiar name that does not contain any personal information.
- Hidden Wireless:** Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.
- Security Keys:** If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Bridge with AP Mode

Enable Wireless: Select this to turn the Wi-Fi module on and off. Use the drop-down box to select if you want to use a schedule. Click **Add New** to add or change a schedule.

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

Wireless Network Name: The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

802.11 Mode: Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are **802.11n Only, Mixed 802.11n and 802.11g, or Mixed 802.11n, 802.11g and 802.11b.**

Wireless Channel: All devices on the network must share the same channel.

Enable Auto Scan: The **Auto Channel Scan** setting can be selected to allow the DAP-2020 to choose the channel with the least amount of interference.

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

Visibility Status: Check the box if you do not want the SSID to be broadcast by the DAP-2020. This prevents the SSID from being seen by site survey utilities, so any wireless clients will have to be pre-configured with the SSID of the DAP-2020 in order to connect to it.

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

Bridge Security: Select None to disable encryption to across the network. Select WEP 64-bits or WEP 128-bits to limit communication to only those devices that share the same WEP settings. Select **WPA-PSK** or **WPA2-PSK** to secure your network using a password and dynamic key changes (No RADIUS server required).

The screenshot shows the D-Link configuration web interface for a DAP-2020 device. The main navigation tabs are SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The current page is WIRELESS NETWORK, which is part of the WIRELESS SETUP section. The interface includes the following settings:

- WIRELESS NETWORK:**
 - Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made on this section may also need to be duplicated on your wireless client.
 - Buttons: Save Settings, Don't Save Settings
- WIRELESS NETWORK SETTINGS:**
 - Enable Wireless: Always (Add New)
 - Wireless Mode: Bridge with AP (Site Survey)
 - Wireless Network Name: Dlink (Also called the SSID)
 - 802.11 Mode: Mixed 802.11n, 802.11g and 802.11b
 - Wireless Channel: 6
 - Enable Auto Channel Scan:
 - Channel Width: 20MHz
 - Visibility Status: (Also called Disable SSID Broadcast)
- WIRELESS SECURITY MODE:**
 - Security Mode: None
- BRIDGE SETTING:**
 - Remote AP Mac: 8 input fields (1-8)
 - Bridge Security: none
 - WEP Key: ASCII (input field)
 - Pre-Shared Key: (8~63 char.) (input field)

Helpful Hints..

- Wireless Mode:** Select a Function mode to configure your wireless network. Function wireless modes include Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router and WISP Repeater. Function wireless modes are designed to support various wireless network topologies and applications.
- Wireless Network Name:** Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a Familiar name that does not contain any personal information.
- Hidden Wireless:** Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.
- Security Keys:** If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this

Note: The Bridge with AP mode is not completely specified in the Wi-Fi or IEEE standards. This mode can work with other DAP-2020 units. Communication with other APs (even other D-Link APs) is not guaranteed.

WISP Client Router/WISP Repeater Modes

Enable Wireless: Select this to turn the Wi-Fi module on and off. Use the drop-down box to select if you want to use a schedule. Click **Add New** to add or change a schedule.

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

Site Survey: Click this button to choose the root AP from an available connection list. If the root AP has wireless encryption, you have to use the same wireless security mode to connect the root AP.

Wireless Network Name: You can input the wireless network name of the root AP or click the **Site Survey** button to find the root AP.

802.11 Mode: Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are **802.11n Only**, **Mixed 802.11n and 802.11g**, or **Mixed 802.11n, 802.11g and 802.11b**.

Wireless Channel: The channel used will be displayed. The channel will follow the root AP.

Enable Auto Scan: The **Auto Channel Scan** setting can be selected to allow the DAP-2020 to choose the channel with the least amount of interference.

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

Visibility Status: Check the box if you do not want the SSID to be broadcast by the DAP-2020. This prevents the SSID from being seen by site survey utilities, so any wireless clients will have to be pre-configured with the SSID of the DAP-2020 in order to connect to it.

Wireless Security Mode: Select a wireless security setting. Options are None, WEP, WPA, or WPA2. Refer to the **Wireless Security** section of this manual for a detailed explanation of the wireless security options.

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

SETUP WIZARD
WIRELESS SETUP
LAN SETUP

WIRELESS NETWORK

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

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS :

Enable Wireless : Always Add New

Wireless Mode : WISP Client Router Site Survey

Wireless Network Name : Dlink (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Wireless Channel : 6

Enable Auto Channel Scan :

Channel Width : 20MHz

Visibility Status : (Also called Disable SSID Broadcast)

WIRELESS SECURITY MODE :

Security Mode : None

WAN SETTINGS :

This page is used to configure the parameters for Internet network which connects to the WAN part of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

My Internet Connection is : Dynamic IP(DHCP)

Host Name : dlinkap

MTU Size : 1500 (bytes) MTU default= 1500

Attain DNS Automatically

Set DNS Manually

Clone MAC Address : 000000000000

Clone Your PC's MAC Address

Helpful Hints..

Wireless Mode :
Select a function mode to configure your wireless network. Function wireless modes include Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router and WISP Repeater. Function wireless modes are designed to support various wireless network topologies and applications.

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

Hidden Wireless :
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.

Security Keys :
If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

WAN Settings

Dynamic IP (DHCP)

WAN settings are only used in the WISP Client Router wireless mode and the WISP Repeater wireless mode. Choose Dynamic IP(DHCP) to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP number to use. This option is commonly used for Cable modem services.

Host Name: The Host Name is optional but may be required by some ISPs.

MTU Size: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The default MTU size is 1500.

Attain DNS Automatically: Select this option if you want the DAP-2020 to get the DNS (Domain Name System) server IP address automatically.

Set DNS manually: Select this option if you want to manually enter the DNS Server IP address(es). The fields to enter the Primary and Secondary DNS server IP addresses will appear after you have selected this option.

DNS Server: Enter the Primary and Secondary DNS server IP address assigned by your ISP.

Clone MAC Address: The default MAC address is set to the Ethernet MAC address your DAP-2020. You can click the Clone Your PC's MAC Address button to replace the AP's MAC address with the MAC address of the PC that you used to register with your ISP. It is not recommended that you change the default MAC address unless required by your ISP.

WAN SETTINGS :

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

My Internet Connection is :

Host Name :

MTU Size : (bytes) MTU default= 1500

Attain DNS Automatically

Set DNS Manually

Clone MAC Address :

Static IP

Select Static IP if all WAN IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP.

IP Address: 192.168.1.1 is the default WAN IP Address of the DAP-2020.

Subnet Mask: 255.255.255.0 is the default subnet mask. All devices on the network must have the same subnet mask to communicate on the network.

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

MTU Size: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The default MTU size is 1500.

Primary DNS Server: Enter the Primary DNS (Domain Name System) server IP address assigned by your ISP.

Secondary DNS Server: Enter the Secondary DNS (optional) server IP address assigned by your ISP.

Clone MAC Address: The default MAC address is set to the MAC address on the AP (Access Point). You can click the Clone Your PC's MAC Address button to replace the AP's MAC address with the MAC address of your Ethernet card. It is not recommended that you change the default MAC address unless required by your ISP.

WAN SETTINGS :

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

My Internet Connection is : Static IP

IP Address :

IP Subnet Mask :

Gateway IP Address :

MTU Size : 1500 (bytes) MTU default= 1500

Primary DNS :

Secondary DNS :

Clone MAC Address : 000000000000

PPPoE

Select PPPoE (Point-to-Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through the DAP-2020.

Login: Enter your PPPoE user name.

Password: Enter your PPPoE password and then retype the password in the next box.

Service Name: Enter the ISP Service Name (optional).

Reconnection Mode: Select **Always on**, **On demand**, or **Manual**.

Idle Timeout: Enter a maximum idle time during which the Internet connection is maintained during inactivity.

MTU Size: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The maximum/default MTU size is 1492.

Attain DNS Automatically: Select this option if you want the DAP-2020 to get the DNS (Domain Name System) server IP address automatically.

Set DNS Manually: Select this option if you want to manually enter the DNS Server IP address(es). Fields to enter the Primary and Secondary DNS server IP addresses will appear after you select this option.

DNS Servers: Enter the Primary and Secondary DNS server IP address assigned by your ISP.

Clone MAC Address: The default MAC address is set to the MAC address on the AP (Access Point). You can click the **Clone Your PC's MAC Address** button to replace the AP's MAC address with the MAC address of your Ethernet card. It is not recommended that you change the default MAC address unless required by your ISP.

WAN SETTINGS :

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

My Internet Connection is : PPPoE(Username / Password) ▼

Login :

Password :

Password Confirm :

Service Name (If Required) : (optional)

Connection Mode : Always On ▼

Idle Timeout (In minutes) : (1-1000 minutes)

MTU Size : (bytes) MTU default= 1480

Attain DNS Automatically

Set DNS Manually

Primary DNS :

Secondary DNS :

Clone MAC Address :

PPTP

Choose PPTP (Point-to-Point Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

My IP Address: Enter the IP address (Static PPTP only).

Subnet Mask: Enter the subnet mask.

Gateway IP address: Enter the Gateway IP address.

Server IP Address: Enter the Server IP Address provided by your ISP.

Login: Enter your PPTP username.

Password: Enter your PPTP password and then retype the password in the next box.

MTU Size: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The default MTU size is 1400.

Attain DNS Automarically: Select this option if you want the DAP-2020 get DNS server IP address automatically.

Set DNS Automatically: Select this option if you want to manually enter the DNS Server IP address(es). Fields to enter the Primary and Secondary DNS server IP addresses will appear after you select this option.

Enter the Primary and Secondary DNS (Domain Name System) server IP address assigned by your ISP.

DNS Servers: The default MAC address is set to the MAC address on the AP (Access Point). You can click the **Clone Your PC's MAC Address** button to replace the AP's MAC address with the MAC address of your Ethernet card. It is not recommended that you change

Clone MAC Address: the default MAC address unless required by your ISP.

WAN SETTINGS :

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

My Internet Connection is : PPTP(Username / Password) ▾

My IP Address :

Subnet Mask :

Gateway IP Address :

Server Address :

Login :

Password :

Password Confirm :

MTU Size : (bytes) MTU default= 1400

Attain DNS Automatically

Set DNS Manually

Primary DNS :

Secondary DNS :

Clone MAC Address :

LAN Settings

This section will allow you to change the local network settings of the access point and to configure the DHCP settings.

Device Name: Enter the Device Name of the AP. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.

LAN Connection Type: Use the drop-down menu to select Dynamic IP (DHCP) to automatically obtain an IP address on the LAN/private network.

My IPv6 Connection Type: Select from the drop-down menu the type of IPv6 connection you would like to use.

D-Link

DAP-2020 //

SETUP ADVANCED MAINTENANCE STATUS HELP

SETUP WIZARD
WIRELESS SETUP
LAN SETUP

NETWORK SETTINGS :

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

Save Settings Don't Save Settings

DEVICE NAME :

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

Device Name :

LAN IPV4 CONNECTION TYPE :

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

My LAN Connection is :

DYNAMIC IP (DHCP) LAN CONNECTION TYPE :

IP Address Information.

IP Address :

Subnet Mask :

Gateway Address :

Primary DNS Server :

Secondary DNS Server :

IPV6 CONNECTION TYPE :

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

My IPv6 Connection is :

LAN IPV6 ADDRESS SETTINGS :

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

LAN IPv6 Link-Local Address : fe80::218:e7ff:fe95:6561/64

Helpful Hints...

LAN Settings :

LAN Connection type :
The factory default setting is "Static IP" which allows the IP address of the DAP-1360 to be manually configured in accordance to the applied local area network. Enable Dynamic (DHCP) to allow the DHCP host to automatically assign the Access Point an IP address that conforms to the applied local area network.

IP Address :
The default IP address is 192.168.0.50. It can be modified to conform to an existing local area network. Please note that the IP address of each device in the wireless local area network must be within the same IP address range and subnet mask. Take default DAP-1360 IP address as an example, each station associated to the AP must be configured with a unique IP address falling in the range of 192.168.0.*. ** ranges from 1 to 254 but 50 in this case.

Subnet Mask :
A mask used to determine what subnet an IP address belongs to. The default subnet setting is 255.255.255.0.

Gateway :
Specify the gateway IP address of the local network.

DHCP Server :
If you already have a DHCP server on your network or are using static IP addresses on all the devices on your network, uncheck **Enable DHCP Server** to disable this feature.

WIRELESS

Static IP

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Access point will not accept the IP address if it is not in this format.

Device Name: Enter the Device Name of the AP. It is recommended to change the Device Name if there is more than one D-Link device within the subnet. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. If you are using the device name to connect, ensure that your PC and your DAP-2020 are on the same network.

LAN Connection Type: Select Static IP from the drop-down menu.

IP Address: Enter the IP address of the access point. The default IP address is 192.168.0.50. If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

The screenshot shows the D-Link DAP-2020 web interface. The top navigation bar includes 'DAP-2020', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar contains 'SETUP WIZARD', 'WIRELESS SETUP', and 'LAN SETUP'. The main content area is titled 'NETWORK SETTINGS' and contains the following sections:

- NETWORK SETTINGS :** A text box with instructions: "Use this section to configure the internal network settings of your AP. Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. Recommend to change the device name if there're more than one D-Link devices within the subnet." Below this are 'Save Settings' and 'Don't Save Settings' buttons.
- DEVICE NAME :** A text input field labeled 'Device Name' with the value 'dlinkap'.
- LAN IPV4 CONNECTION TYPE :** A section titled 'Choose the IPv4 mode to be used by the Access Point.' with a dropdown menu labeled 'My LAN Connection is' set to 'Static IP'.
- STATIC IP ADDRESS LAN CONNECTION TYPE :** A section titled 'Enter the IPv4 Address information.' with the following fields:
 - IP Address: 192.168.0.50
 - Subnet Mask: 255.255.255.0
 - Gateway Address: 0.0.0.0
 - Primary DNS Server: 0.0.0.0
 - Secondary DNS Server: 0.0.0.0

On the right side, there is a 'Helpful Hints..' section with the following text:

LAN Connection type :
The Factory default setting is "Static IP" which allows the IP address of the DAP-1360 to be manually configured in accordance to the applied local area network. Enable Dynamic (DHCP) to allow the DHCP host to automatically assign the Access Point an IP address that conforms to the applied local area network.

IP Address :
The default IP address is 192.168.0.50. It can be modified to conform to an existing local area network. Please note that the IP address of each device in the wireless local area network must be within the same IP address range and subnet mask. Take default DAP-1360 IP address as an example, each station associated to the AP must be configured with a unique IP address falling in the range of 192.168.0.*.*** ranges from 1 to 254 but 50 in this case.

Subnet Mask :
A mask used to determine what subnet an IP address belongs to. The default subnet setting is 255.255.255.0.

Gateway :
Specify the gateway IP address of the local network.

DHCP Server

The DHCP server settings defines the range of the IP address that can be assigned to stations in the network. If needed or required in the network, the DAP-2020 is capable of acting as a DHCP server.

Enable DHCP server : Check to allow the DAP-2020 to function as a DHCP server.

DHCP IP Address Range : Input the IP address available for assignment on your network.

Always Broadcast : Check to keep broadcast.

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

WINS : Enter the IP address of the WINS on the network.

DNS : Enter the IP address of the DNS on the network.

DHCP Lease Time : The lease time is the period of time before the DHCP server will assign new IP addresses.

DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range : to

Always Broadcast :

Gateway :

WINS :

DNS :

DHCP Lease Time :

Advanced Advanced Wireless

Transmit Power: Sets the transmit power of the antennas.

WMM Enable: WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

IGMP Snooping: This enables IGMP snooping for the wireless connection. We recommend enabling this if you often use multicast services such as video conferencing and streaming audio/video.

WLAN Partition: This feature enables client isolation. If enabling, all clients will not be able to view or access each other's information or within the network.

HT 20/40 Coexistence: Check to enable or disable this feature.

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

ADVANCED WIRELESS SETTINGS :

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

Save Settings Don't Save Settings

ADVANCED WIRELESS SETTINGS :

Transmit Power : 100% ▾

WMM Enable :

Short GI :

IGMP Snooping :

WLAN Partition :

HT 20/40 Coexistence : Enable Disbale

Helpful Hints..

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

Transmit Power:
You can lower the output power of the DAP-1360 by selecting lower percentage Transmit Power values from the drop down. Your choices are: 100%, 75%,

MAC Address Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

Configure MAC Filtering: When **Turn MAC Filtering OFF** is selected, MAC addresses are not used to control network access. When **Turn MAC Filtering ON and ALLOW computers listed to access the network** is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When **Turn MAC Filtering ON and DENY computers listed to access the network** is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.

Add MAC Filtering Rule: This parameter allows you to manually add a MAC filtering rule. Click the **Add** button to add the new MAC filtering rule to the MAC Filtering Rules list at the bottom of this screen.

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

ADVANCED WIRELESS
MAC ADDRESS FILTER

MAC ADDRESS FILTER :

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

Save Settings Don't Save Settings

WIRELESS ACCESS SETTINGS

Configure MAC Filtering below :

Turn MAC Filtering OFF

MAC Address	Wireless Client List	
00:00:00:00:00:00	<< MAC Address	Clear
00:00:00:00:00:00	<< MAC Address	Clear
00:00:00:00:00:00	<< MAC Address	Clear
00:00:00:00:00:00	<< MAC Address	Clear
00:00:00:00:00:00	<< MAC Address	Clear
00:00:00:00:00:00	<< MAC Address	Clear
00:00:00:00:00:00	<< MAC Address	Clear
00:00:00:00:00:00	<< MAC Address	Clear

Helpful Hints..

Wireless Access Settings:
Create a list of MAC addresses that you would either like to accept or reject access to your network.

Connected PCs:
Select a MAC address from the drop down menu, then click the arrow to add that MAC address to the list.

IP Filter:
Click the Clear button to remove the MAC Filtering list.

WIRELESS

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy, as depressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin-Code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

Enable: Check this box to enable the function

Disable WPS-PIN Method: Locking the wireless security settings prevents the settings from being changed by the Wi-Fi Protected Setup feature of the router. Devices can still be added to the network using Wi-Fi Protected Setup. However, the settings of the network will not change once this option is checked.

Pin Settings: Press the button to generate a new PIN or Reset to Default.

Current PIN: Shows the current value of the router’s PIN.

Reset PIN to Default: Restore the default PIN of the access point.

Generate New PIN: Create a random number that is a valid PIN. This PIN becomes the router’s PIN. You can then copy this PIN to the user interface of the registrar.

Add Wireless Station: Press the button to start with the wizard to setup the WPS.

D-Link

DAP-2000 // SETUP ADVANCED MAINTENANCE STATUS HELP

ADVANCED WIRELESS

MAC ADDRESS FILTER

WI-FI PROTECTED SETUP

USER LIMIT

WI-FI PROTECTED SETUP :

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method. If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN. However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

Save Settings Don't Save Settings

WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA) :

Enable :

Lock Wireless Security :

Reset to Unconfigured

PIN SETTINGS

Current PIN: 42700098

Reset PIN to Default Generate New PIN

ADD WIRELESS STATION

Add Wireless Device With WPS

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

WIRELESS

User Limits

Enter the maximum number of wireless clients that can connect at one time to your access point.

Enable User Limit: Check the **Enable User Limit** box to enable this feature.

User Limit: Enter the maximum number of clients, between 1 and 32.

Save Settings: Click **Save Settings** to save and activate the new changes.

The screenshot shows the D-Link configuration interface for the DAP-2020. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar lists menu items: ADVANCED WIRELESS, MAC ADDRESS FILTER, WI-FI PROTECTED SETUP, and USER LIMIT. The main content area is titled 'USER LIMIT SETTINGS' and contains the following text: 'Please apply the settings to limit how many wireless stations connecting to AP.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. A second section, also titled 'USER LIMIT SETTINGS', contains two settings: 'Enable User Limit' with an unchecked checkbox, and 'User Limit (1 - 32)' with an empty text input field. On the right side, there is a 'Helpful Hints..' section with the text: 'User Limit can set a limit upon the number of wireless clients. Using user limit, you can prevent scenarios where the DAP-1360 in your network shows performance degradation because it is handling heavy wireless traffic.'

Port Forwarding (WISP modes only)

This function is available if your DAP-2020 is in the WISP Client Router or WISP Repeater mode. This feature allows you to open a single port or a range of ports. Click **Save Settings** and the port forwarding rule will be put into the Port Forwarding List.

Port Forwarding Rules: Check the box to configure a port forwarding rule.

Name: Enter a name for the rule. You can select an application name from the Application Name drop-down menu. Click the << button to fill in the Name field with the application name that you selected.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to.

Start/End Ports: Enter the port or ports that you want to open. If you want to open one port, enter the same port in both boxes.

Traffic Type: Select **TCP**, **UDP**, or **Both**.

PORT FORWARDING RULES

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

			Port	Traffic Type
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	Start <input type="text"/>	Both ▼
	IP Address <input type="text"/>	<< Computer Name ▼	End <input type="text"/>	

PORT FORWARD LIST

Current Port Forwarding Table:

Name	IP Address	Protocol	Port Range	Select
<div style="display: flex; justify-content: space-around;"> Delete Selected Delete All Reset </div>				

Port Filter (WISP modes only)

This function is available if your DAP-2020 is in the WISP Client Router or WISP Repeater mode. This feature is used to secure or restrict your local network. It will deny the ports that you enter from the local network to the Internet. Click **Save Settings** and the port filter rule will be put into the Port Filter List.

Port Filter Rules: Check the box to configure a port filter rule.

Name: Enter a name for the rule. You can select an application name from the Application Name drop-down menu. Click the << button to fill in the Name field with the application name that you selected.

Start/End Ports: Enter the port or ports that you want to open. If you want to open one port, enter the same port in both boxes.

Traffic Type: Select **TCP**, **UDP**, or **Both**.

PORT FILTER RULES

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

			Port	Traffic Type	
<input type="checkbox"/>	Name <input style="width: 80%;" type="text"/>	<< Application Name ▾	Start <input style="width: 80%;" type="text"/>	End <input style="width: 80%;" type="text"/>	Both ▾

PORT FILTER LIST

Current Port Filter Table:

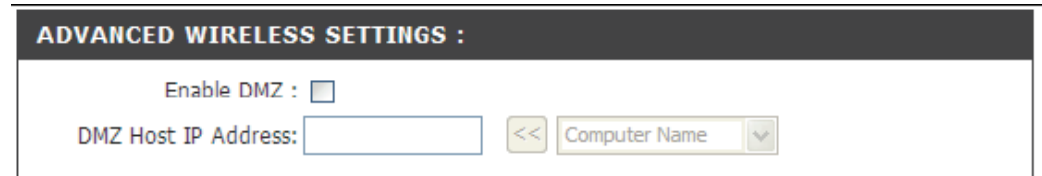
Name	Port Range	Protocol	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

DMZ (WISP modes only)

This function is available only if the DAP-2020 is in the WISP Client Router or WISP Repeater mode. This feature allows you to set up a DMZ (Demilitarized Zone) host. If you have a client PC that cannot run Internet applications properly from behind the DAP-2020, then you can set the client up for unrestricted Internet access. The DMZ allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP address of the computer that will be the DMZ host. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

Enable DMZ: Check this box to enable DMZ.

DMZ Host IP Address: Enter the IP address of the computer you would like to open all ports to. You can select a computer from the Computer Name drop-down menu and click << to enter the computer name into the DMZ Host IP Address field.



The screenshot shows a configuration window titled "ADVANCED WIRELESS SETTINGS :". Inside the window, there is a checkbox labeled "Enable DMZ :". Below it, there is a label "DMZ Host IP Address:" followed by a text input field. To the right of the input field is a button with two left-pointing arrows "<<". To the right of the button is a dropdown menu currently displaying "Computer Name".

Parental Control (WISP modes only)

This function is available only if the DAP-2020 is in the WISP Client Router or WISP Repeater mode. This feature allows you to create a list of websites that you want to deny users access.

Configure Website Filtering Below: Select **Turn Website Filtering OFF** or **Turn Website Filtering ON and DENY computers access to ONLY these sites.**

Website URL Address: Enter a keyword or URL that you want to block and click **Save Settings**. Any URL that contains the keyword will be blocked.

PARENTAL CONTROL :

The Parental Control allows you to set-up a list of Websites that the users on your network will either be allowed or denied access to.

WEBSITE FILTERING RULES

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Configure Website Filtering below:

▼
 Turn Website Filtering OFF

Website URL Address or keyword

WEB FILTER LIST

Current Filter Table:

URL Address or keyword	Select
	<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>

Advanced Network (WISP modes only)

This function is available if the DAP-2020 is in WISP Client Router or WISP Repeater mode. This feature allows you to change the LAN settings. Please be aware that any changes to the factory default settings may affect the behavior of your network.

Enable UPnP: Check this box to use the Universal Plug and Play (UPnP™) feature. UPnP provides compatibility with networking equipment, software and peripherals.

Enable WAN Ping Respond: Check this box to allow the WAN port of the DAP-2020 to be pinged. Unchecking the box will not allow the DAP-2020 to respond to pings. Blocking ping response may provide some extra security from intruders.

Remote Management: Remote management allows the DAP-2020 to be configured from the Internet by a web browser. A username and password are still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

UPNP : Universal plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices. Enable UPnP: <input type="checkbox"/>
WAN PING : If you enable this feature, the WAN port of your DAP-1360 will respond to ping requests from the Internet that are sent to the WAN IP Address. Enable WAN Ping Respond: <input type="checkbox"/>
REMOTE MANAGEMENT : If you enable this feature, you can manage the DAP-1360 from anywhere on the Internet. Enable Remote Management: <input type="checkbox"/>

Maintenance Admin

This page will allow you to change the Administrator password. The administrator password has read/write access.

Password: Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

Confirm Password: Enter the same password that you entered in the previous textbox in order to confirm its accuracy.

Enable Graphical Authentication: Check to enable this feature.

The screenshot displays the D-Link Maintenance Admin interface. At the top, the D-Link logo is visible. Below it, a navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE (selected), STATUS, and HELP. A sidebar on the left lists menu items: ADMIN, SYSTEM, FIRMWARE, WATCHDOG, TIME, and SYSTEM CHECK. The main content area is titled 'DEVICE ADMINISTRATION :'. It contains a text box with instructions: 'Enter the new password in the "New Password" field and again in the next field to confirm. Click on "Save Settings" to execute the password change. The Password is case-sensitive, and can be made up of any keyboard characters. The new password must be between 0 and 15 characters in length.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'PASSWORD :' section contains two input fields: 'New Password : *****' and 'Confirm Password : *****'. The 'ADMINISTRATION :' section includes a checkbox for 'Enable Graphical Authentication :'. On the right side, there is a 'Helpful Hints..' section with a 'Passwords:' note: 'For security reasons, it is recommended that you change the Password for the Administrator accounts. Be sure to write down the Passwords to avoid having to reset the AP in the event that they are forgotten.'

System

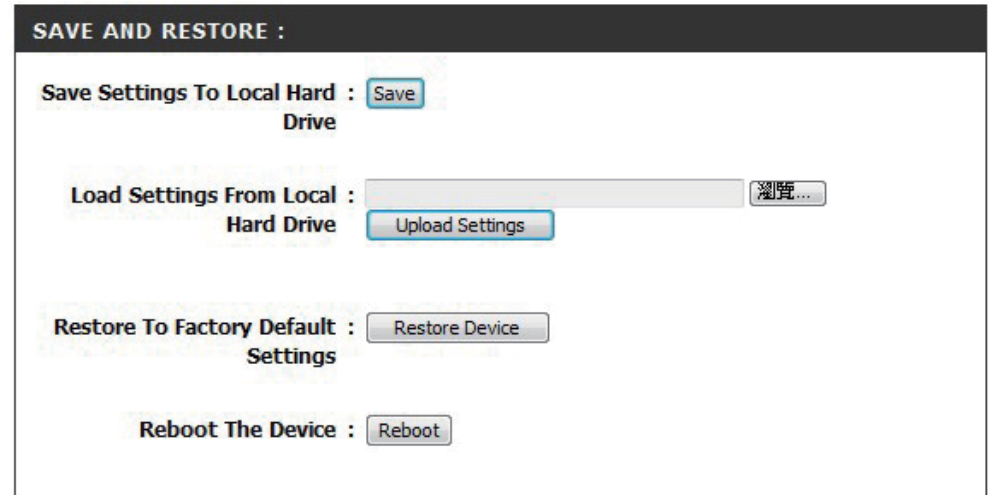
Save to Local Hard Drive: Use this option to save the current access point configuration settings to a file on the hard disk of the computer you are using. Click the **Save** button. You will then see a file dialog where you can select a location and file name for the settings.

Upload from Local Hard Drive: Use this option to load previously saved access point configuration settings. Click **Browse** to find a previously saved configuration file. Then, click the **Upload Settings** button to transfer those settings to the access point.

Restore to Factory Default: This option will restore all configuration settings back to the settings that were in effect at the time the access point was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current access point configuration settings, use the **Save** button above.

Note: Restoring the factory default settings will not reset the Wi-Fi Protected Status to Not Configured.

Reboot the Device: Click to reboot the access point.



Firmware

You can upgrade the firmware of the access point here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support website for firmware updates at <http://support.dlink.com>. You can download firmware upgrades to your hard drive from this site.

Browse: After you have downloaded the new firmware, click **Browse** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

Upload: Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the access point.

Language Pack

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

Browse: After you have downloaded the new language pack, click **Browse** to locate the language pack file on your hard drive. Click **Upload** to complete the language pack upgrade.

The screenshot displays the D-Link web interface for a DAP-2020 access point. The top navigation bar includes 'DAP-2020', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'MAINTENANCE' tab is active, showing the 'FIRMWARE UPGRADE' section. This section contains a notification about new firmware for the DAP-1360, a warning not to update wirelessly, and a 'FIRMWARE INFORMATION' box showing the current version (6.00) and date (2013-07-04). Below this is another 'FIRMWARE UPGRADE' section with a note that some updates reset configurations and instructions to upgrade via a wired connection. It features an 'Upload' button with a file selection field. A similar 'LANGUAGE PACK UPGRADE' section is visible at the bottom, also with an 'Upload' button and file selection field. A 'Helpful Hints...' sidebar on the right provides additional information about firmware updates.

Watchdog

The Watchdog feature pings a specified IP address. If the IP address stops responding to pings, your AP will be rebooted. You can also select an option to have the DAP-2020 send an e-mail alert if the specified IP address stops responding to pings.

Enable Watchdog (Ping of Life): Check this box to enable the Watchdog (Ping of Life) to check some host IP.

Update Time Interval: Enter the time interval of how often you would like the Watchdog to ping the response IP address.

Watchdog Response IP: Enter the IP address that the Watchdog will ping.

Enable Mail Alert: Check this box to enable e-mail notification for the Watchdog.

SMTP Server: Enter the SMTP server IP address.

Sender E-Mail: Enter the e-mail address from which the notification will be sent.

Receiver E-Mail: Enter the e-mail address which the notification will be sent to.

SMTP Server Port: Enter the SMTP server port.

Enable Authentication: Check the box to enable authentication that is used with the SMTP server.

Account Name: Enter your account name that is used with the SMTP server.

Password: Enter your password that is used with the SMTP server and re-enter it in the next box.

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

ADMIN
SYSTEM
FIRMWARE
WATCHDOG
TIME
SYSTEM CHECK

WATCHDOG (PING OF LIFE) :

The Watchdog feature pings a specified IP address. If the IP address stops responding to pings, your access point will be rebooted. You can also select an option to have the DAP-1360 send an e-mail alert if the specified IP address stops responding to pings.

Save Settings Don't Save Settings

WATCHDOG :

Enable Watchdog (Ping of Life) :

Update Time Interval : 1 (minutes, range:1-60, default:1)

Watchdog Response IP : 0.0.0.0

Enable Mail Alert :

SMTP Server :

Sender E-mail :

Receiver E-mail :

SMTP Server Port :

Enable Authentication :

Account Name :

Password :

Verify Password :

Helpful Hints..

Enable Watchdog (Ping of Life):
Enable the Watchdog (Ping of Life) to check some host IP.

Update Time Interval:
The interval to ping.

Watchdog Response IP:
Pair this DAP-1360 with a device that can respond back to the pings.

Enable Mail Alert:
If you want to enable Mail Alert, you must enable Syslog first. When DAP-1360 can't ping the host IP, the DAP-1360 will send mail to the user.

SMTP Server:
Please enter the mail server IP.

Mail Address:
Please enter the mail address of the user to be notified.

Time

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

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

Daylight Saving: To select Daylight Saving time manually, click the **Enable Daylight Saving** check box. Next use the drop-down menu to select a Daylight Saving Offset and then enter a start date and an end date for daylight saving time.

Enable NTP Server: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

NTP Server Used: Enter the NTP server or select one from the drop-down menu.

Date and Time: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Save Settings**. You can also click the **Copy Computer Time** button at the bottom of the screen.

The screenshot shows the D-Link DAP-2020 web interface for Time Configuration. The interface is divided into several sections:

- TIME Configuration:** This section contains a description of the Time Configuration option and two buttons: "Save Settings" and "Don't Save Settings".
- TIME CONFIGURATION:** This section displays the current time as "01/01/2011 20:19:01" and the selected time zone as "(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi". It includes a checkbox for "Enable Daylight Saving" (which is unchecked) and a "Daylight Saving Offset" dropdown menu set to "0:00". Below this, "Daylight Saving Dates" are configured with DST Start on "Apr 1st" at "2 am" and DST End on "Sep 1st" at "2 am".
- AUTOMATIC TIME CONFIGURATION:** This section has a checkbox for "Enable NTP server" (checked) and a text field for "NTP Server Used" containing "ntp1.dlink.com". A "Select NTP server" dropdown menu is also present.
- SET THE DATE AND TIME MANUALLY:** This section allows manual input of the date and time. The "Date and Time" fields are set to Year: 2011, Month: 1, Day: 1, Hour: 8 pm, Minute: 17, and second: 5. A "Copy computer time" button is located at the bottom of this section.

The interface also features a left sidebar with navigation options: ADMIN, SYSTEM, FIRMWARE, WATCHDOG, TIME (selected), SYSTEM CHECK, and SCHEDULES. A top navigation bar includes SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. A "D-Link" logo is at the top left, and "WIRELESS" is at the bottom left. A "Helpful Hints..." sidebar on the right provides additional information about System Time Settings.

System Check

This section Ping Tests by sending ping packets to test if a computer on the internet is running and responding.

Ping Test : The Ping Test / IPv6 Ping Test is used to send Ping.

Ping Result: The results of your ping attempts will be displayed here.

The screenshot displays the D-Link DAP-2020 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar contains a menu with options: ADMIN, SYSTEM, FIRMWARE, WATCHDOG, TIME, SYSTEM CHECK (which is currently selected), and SCHEDULES. The main content area is titled 'PING TEST :'. It contains a sub-section 'PING TEST :' with the text 'Ping test sends "ping" packets to the test a computer on the Internet.' Below this is a form with a text input field labeled 'Host Name or IP address :', a 'Ping' button, and a 'PING RESULT :' section with the instruction 'Enter a host name or IP address above and click "Ping".' On the right side, there is a 'Helpful Hints...' section with the text: 'Ping checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.'

Schedules

Name: Enter a name for your new schedule.

Days: Select a day, a range of days, or All Week to include every day.

Time: Enter a start and end time for your schedule.

Schedule Rules The list of schedules will be listed here. Click the

List: **Edit** icon to make changes or click the **Delete** icon to remove the schedule.

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

SCHEDULES :
The Schedule configuration option is used to manage schedule rules for wireless LAN control features.

ADD SCHEDULE RULE :

Name :

Day(s) : All Week Select Day(s)
 Sun Mon Tue Wed Thu Fri Sat

All Day - 24 hrs :

Time format : 24-hour

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

End Time : 0 : 0 AM (hour:minute)

SCHEDULE RULES LIST :

Name	Day(s)	Time Frame

Helpful Hints...
Schedules are used with a number of other features to define when those features are in effect.
Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".
Save to add a completed schedule to the list below.
Click the **Edit** icon to change an existing schedule.
Click the **Delete** icon to permanently delete a schedule.

WIRELESS

Status

Device Info

This page displays the current information for the DAP-2020. It will display the LAN and wireless LAN information.

General: Displays the access point's 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 your wireless settings such as SSID and Channel.

D-Link	
DAP-2020	SETUP ADVANCED MAINTENANCE STATUS HELP
DEVICE INFO	<p>DEVICE INFORMATION :</p> <p>All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.</p> <p>GENERAL</p> <p>Time : 2013-07-17 14:52:59 Firmware Version : 6.00</p> <p>LAN</p> <p>MAC Address : 00:1E:E3:13:05:10 Connection : Dynamic IP IP Address : 192.168.0.198 IP Subnet Mask : 255.255.0.0 Default Gateway : 192.168.0.254</p> <p>WIRELESS LAN</p> <p>MAC Address : 00:1E:E3:13:05:10 Wireless Network Name (SSID) : D-Link_DAP-1360 Channel Width : 20/40MHz Wireless Channel : 4 Wireless Security Mode : None Wi-Fi Protected Setup : ON</p>
LOGS	<p>Helpful Hints...</p> <p>Device Information: This page displays the current information of the DAP-1360. The page will show the firmware currently loaded, wired and wireless settings applied on the unit.</p> <p>LAN: The MAC address of the Ethernet LAN connection, Connection Type being used (DHCP or Static), Subnet Mask and Default Gateway are displayed in this section.</p> <p>WAN: The MAC address of the WAN connection, Connection Type being used (DHCP, Static, PPPoE or PPTP), Subnet Mask and Default Gateway are displayed in this section.</p> <p>WIRELESS LAN: The Wireless MAC address, Wireless Network Name (SSID), Wireless Channel and Wireless Security Type are displayed in this section.</p>
STATISTICS	
WIRELESS	
WIRELESS	

Logs

The DAP-2020 keeps a running log of events and activities occurring on the AP. If the AP is rebooted, the logs are automatically cleared. You can save the log files under Log Setting.

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

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.

Log Settings: This button opens a new menu where you can configure the log settings.

Refresh: This button refreshes the log.

The screenshot displays the D-Link web interface for the DAP-2020. The top navigation bar includes 'DAP-2020', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar lists 'DEVICE INFO', 'LOGS', 'STATISTICS', and 'WIRELESS'. The main content area is titled 'VIEW LOG' and contains the following sections:

- VIEW LOG :** A message stating 'View Log displays the activities occurring on the DAP-1360.'
- LOG OPTIONS:** A section with the heading 'System Activity :'. It contains five checkboxes: 'System Activity', 'Debug Information', 'Attacks', 'Dropped Packets', and 'Notice'. Below these is an 'Apply Log Settings Now' button.
- LOG DETAILS :** A section containing navigation buttons: 'First Page', 'Last Page', 'Previous Page', 'Next Page', 'Clear Log', and 'Save log'. Below these is a 'Refresh' button and the text 'page 1 of 1'. At the bottom, there is a table header with two columns: 'Time' and 'Message'.

On the right side, a 'Helpful Hints..' sidebar provides definitions for the navigation buttons:

- First Page:** The first page of the log.
- Last Page:** The last page of the log.
- Previous Page:** Moves back one log page.
- Next Page:** Moves forward one log page.
- Clear Log:** Clears the logs completely.

Statistics

The DAP-2020 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the access point is rebooted.

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

DEVICE INFO
LOGS
STATISTICS
WIRELESS

TRAFFIC STATISTICS :
Traffic Statistics display Receive and Transmit packets passing through the DAP-1360.
Refresh Statistics Clear Statistics

LAN STATISTICS

Sent:	1941	Received:	4547
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	0

WIRELESS STATISTICS

Sent:	1718	Received:	7356
TX Packets Dropped:	0	RX Packets Dropped:	0
Collisions:	0	Errors:	0

Helpful Hints..
Stats: Displays data packet statistics of both transmitted frame and received frame for the DAP-1360 network.

Wireless

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

Connection 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.

The screenshot shows the D-Link web interface for the DAP-2020 device. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar contains a menu with options: DAP-2020, DEVICE INFO, LOGS, STATISTICS, and WIRELESS. The main content area displays the 'CONNECTED WIRELESS CLIENT LIST' section, which includes a descriptive text box and a table. The table has two columns: 'Connected Time' and 'MAC Address'. The current row shows 'None' and '---' respectively. A 'Helpful Hints..' section on the right provides additional information about the 'Wireless' section.

Connected Time	MAC Address
None	---

Help

D-Link

DAP-2020 // SETUP ADVANCED MAINTENANCE STATUS HELP

MENU

HELP MENU

Setup

- [Wizard](#)
- [Wireless Setup](#)
- [WAN Setup](#)
- [LAN Setup](#)

Advanced

- [Port Forwarding](#)
- [Port Filter](#)
- [MAC Address Filter](#)
- [DMZ](#)
- [Parental Control](#)
- [Advanced Wireless](#)
- [Advanced Network](#)

Maintenance

- [Device Administration](#)
- [Save and Restore](#)
- [Firmware Update](#)
- [WatchDog](#)
- [Time](#)
- [Schedules](#)

Status

- [Device Info](#)
- [Log](#)
- [Statistics](#)
- [Wireless](#)

Helpful Hints..

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

WIRELESS

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-2020 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

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.

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point. Click on Setup and then click Wireless Settings on the left side.
2. Next to *Security Mode*, select **Enable WPA Wireless Security**, **Enable WPA2 Wireless Security**, or **Enable WPA2-Auto Wireless Security**.
3. Next to *Cipher Type*, select **TKIP**, **AES**, or **Auto**.
4. Next to *PSK / EAP*, select **Personal**.
5. Next to *Passphrase*, enter a key. The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The passphrase must be between 8-63 characters.
6. Click **Save Settings** at the top of the window to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the access point.

The screenshot shows a web-based configuration interface for wireless security. It is divided into two main sections: 'WIRELESS SECURITY MODE' and 'WPA'. In the 'WIRELESS SECURITY MODE' section, there is a dropdown menu for 'Security Mode' currently set to 'Enable WPA Wireless Security (enhanced)'. The 'WPA' section contains a note: 'WPA requires stations to use high grade encryption and authentication.' Below this note are four fields: 'Cipher Type' with a dropdown menu set to 'AUTO', 'PSK / EAP' with a dropdown menu set to 'Personal', 'Passphrase' with an empty text input field, and 'Confirmed Passphrase' with an empty text input field.

Configure WPA/WPA2 Enterprise

It is recommended to enable encryption on your wireless access point before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the access point. Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WPA Wireless Security, Enable WPA2 Wireless Security, or Enable WPA2-Auto Wireless Security**.
3. Next to *Cipher Mode*, select **TKIP, AES, or Auto**.
4. Next to *Personal / Enterprise*, select **Enterprise**.
5. Next to *RADIUS Server*, enter the IP Address of your RADIUS server.
6. Next to *Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
7. Next to *Shared Secret*, enter the security key.
8. Click **Save Settings** to save your settings.

The screenshot displays the configuration page for wireless security. At the top, under 'WIRELESS SECURITY MODE', the 'Security Mode' is set to 'Enable WPA Wireless Security (enhanced)'. Below this, the 'WPA' section is active, showing a note that WPA requires high-grade encryption and authentication. The 'Cipher Type' is set to 'AUTO' and 'PSK / EAP' is set to 'Enterprise'. Under the '802.1X' section, there are two RADIUS server configurations. 'RADIUS Server 1' has fields for IP, Port (1812), and Shared Secret. 'RADIUS Server 2' also has fields for IP, Port (1812), and Shared Secret.

Connect to a Wireless Network 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.

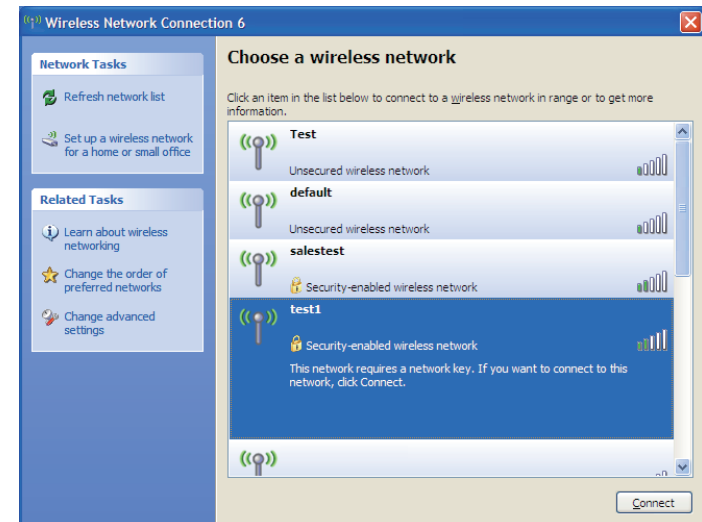
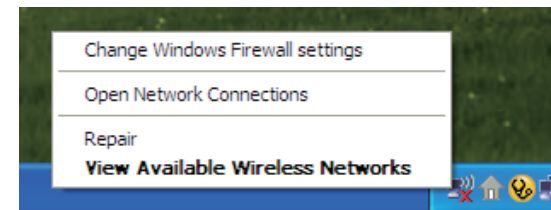
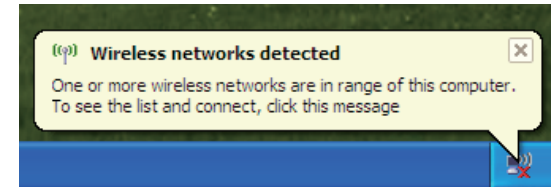
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

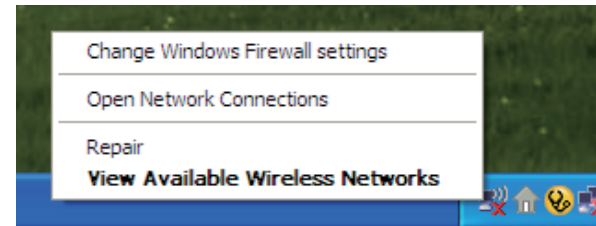
If you get a good signal, but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



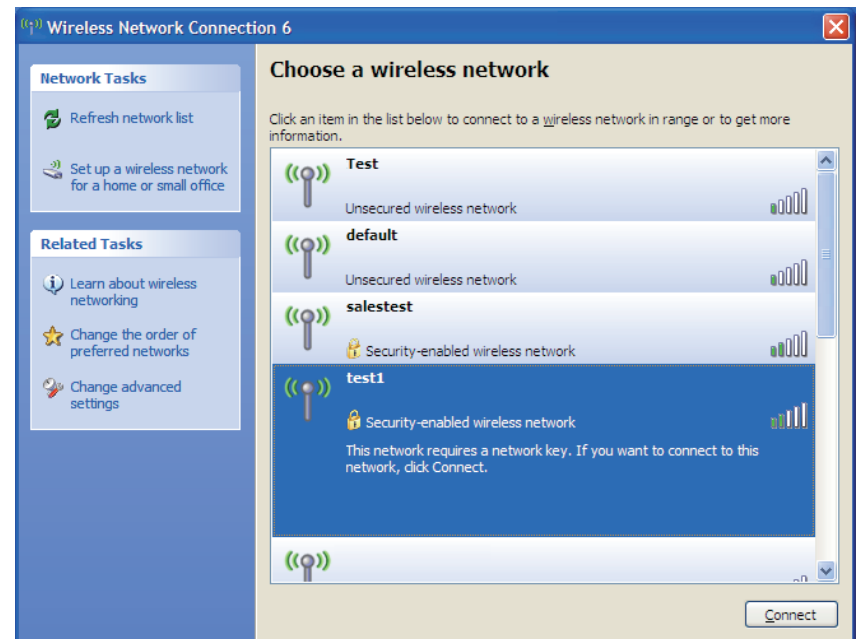
Configure WPA-PSK

It is recommended to enable WEP on your wireless bridge 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**.

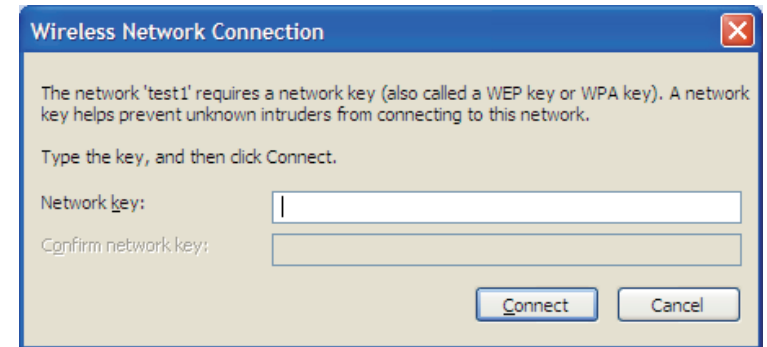


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

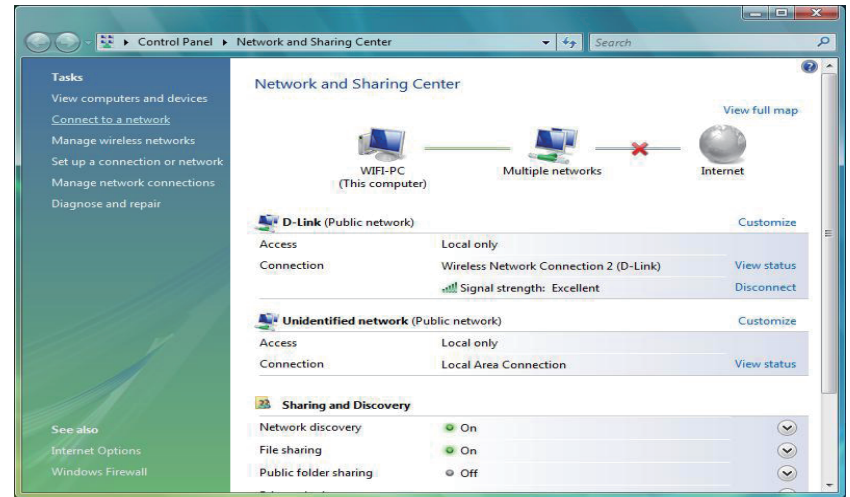
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless access point.



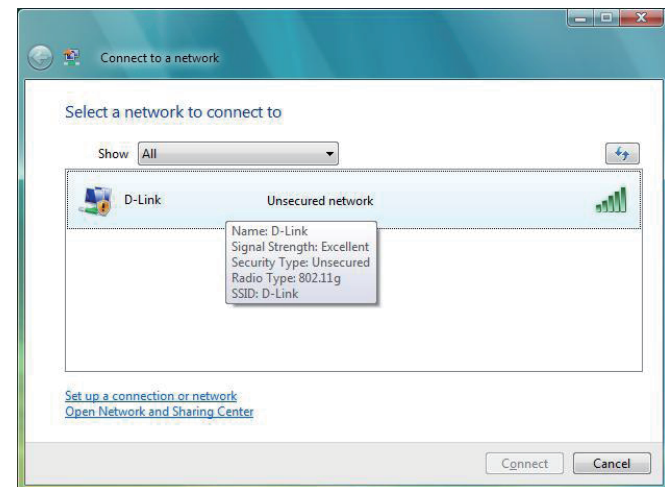
Using Windows Vista®

Windows Vista® users may use the convenient, built-in wireless utility. Follow these instructions:

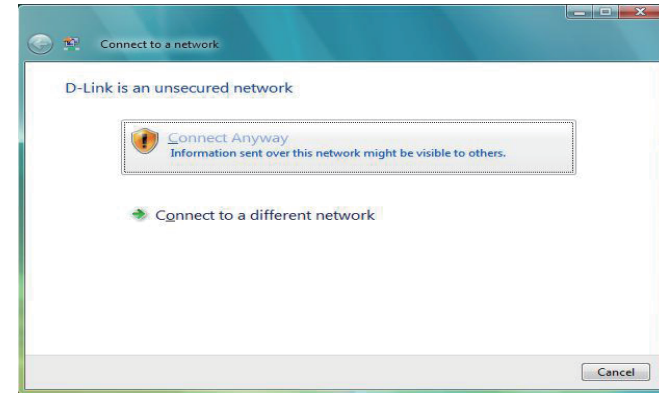
From the Start menu, go to Control Panel, and then click on **Network and Sharing Center**.



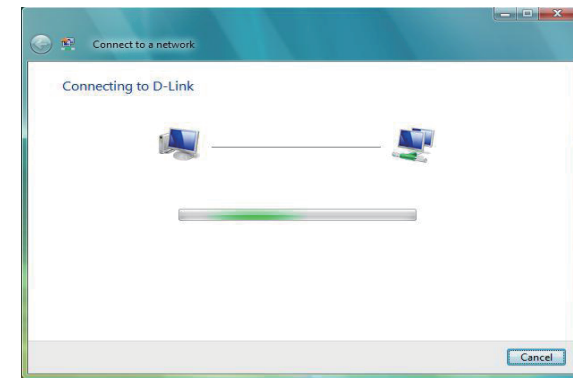
The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) under Select a network to connect to and then click the **Connect** button.



Click **Connect Anyway** to continue.

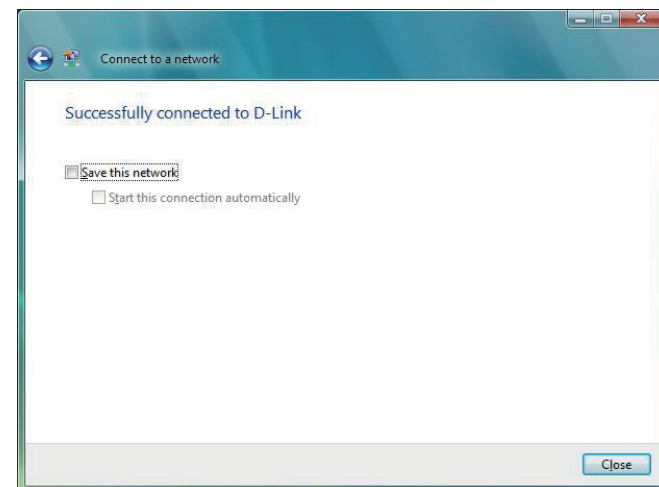


The utility will display the following window to indicate a connection is being made.



The final window indicates the establishment of a successful connection.

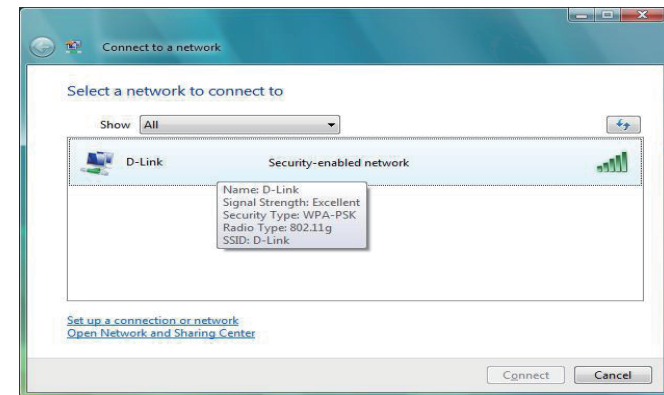
The next two pages display the windows used to connect to either a WEP or a WPA-PSK wireless network.



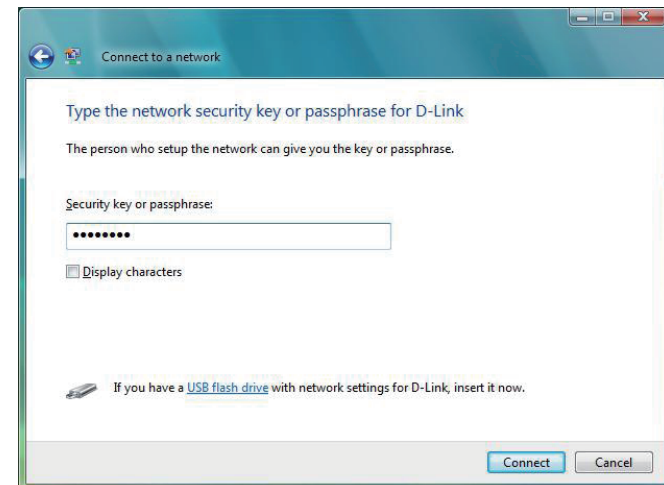
Configure WPA-PSK

It is recommended to enable WEP on your wireless bridge 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.

Click on a network (displayed using the SSID) using WPA-PSK under Select a network to connect to and then click the **Connect** button.



Enter the appropriate security key or passphrase in the field provided and then click the **Connect** button.



Using Windows® 7

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

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



Wireless Icon

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

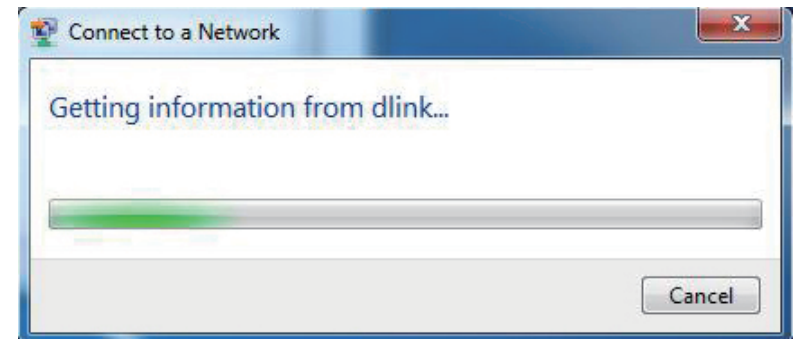


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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

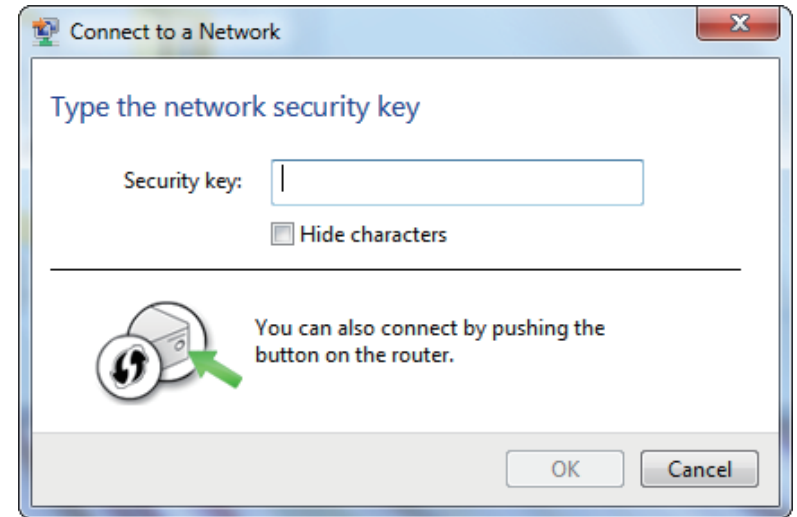


4. The following window appears while your computer tries to connect to the router.



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.

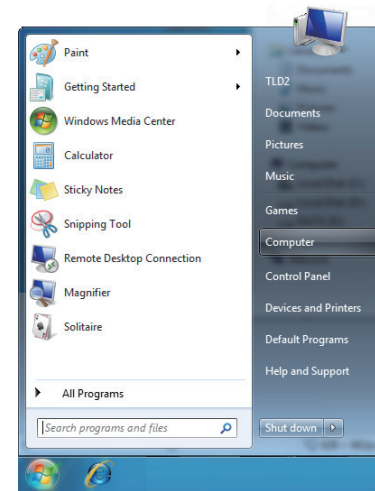
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



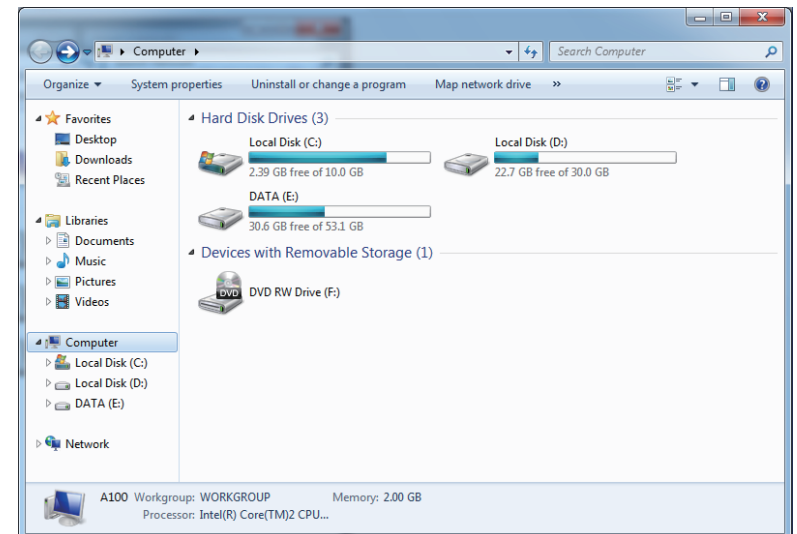
Configure WPS

The WPS feature of the DAP-2020 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature of the DAP-2020:

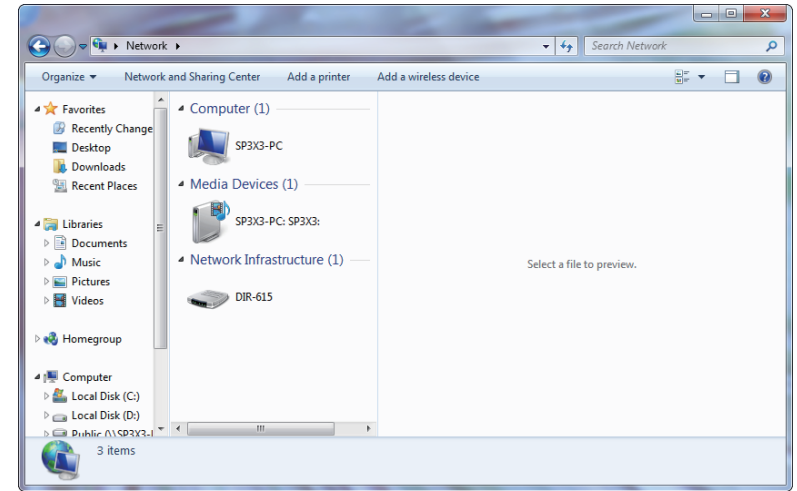
1. Click the **Start** button and select **Computer** from the Start menu.



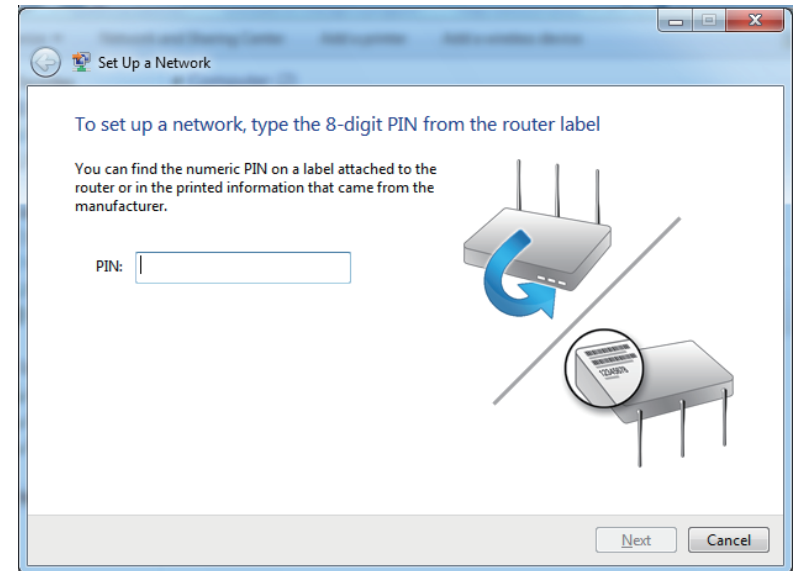
2. Click the **Network** option.



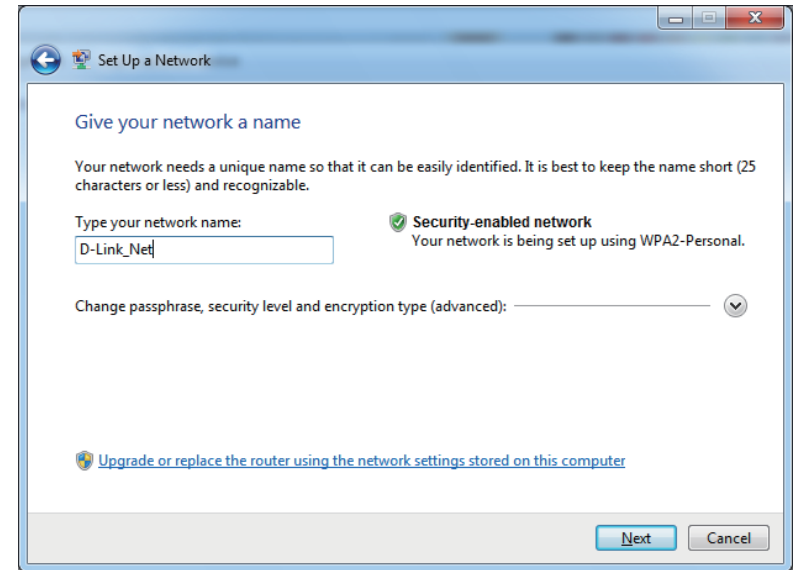
3. Double-click the DAP-2020.




4. Input the WPS PIN number (displayed in the WPS window on the Router's LCD screen or in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.

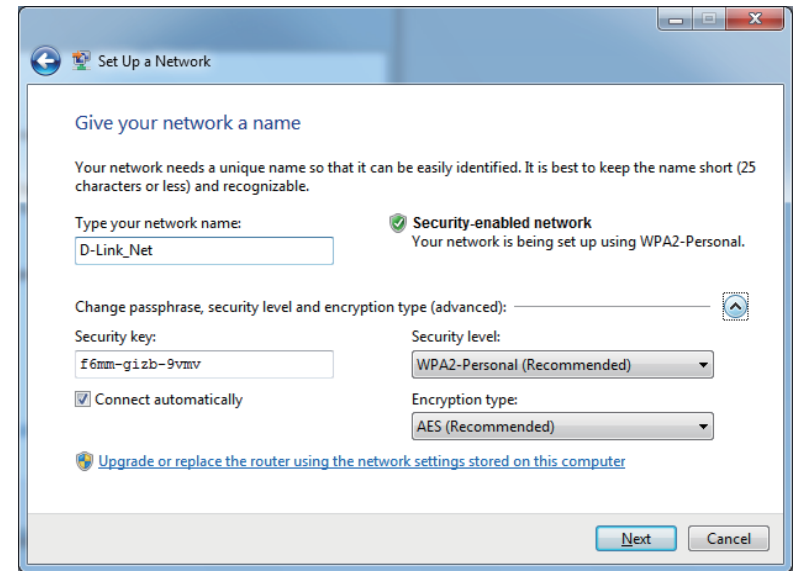


5. Type a name to identify the network.



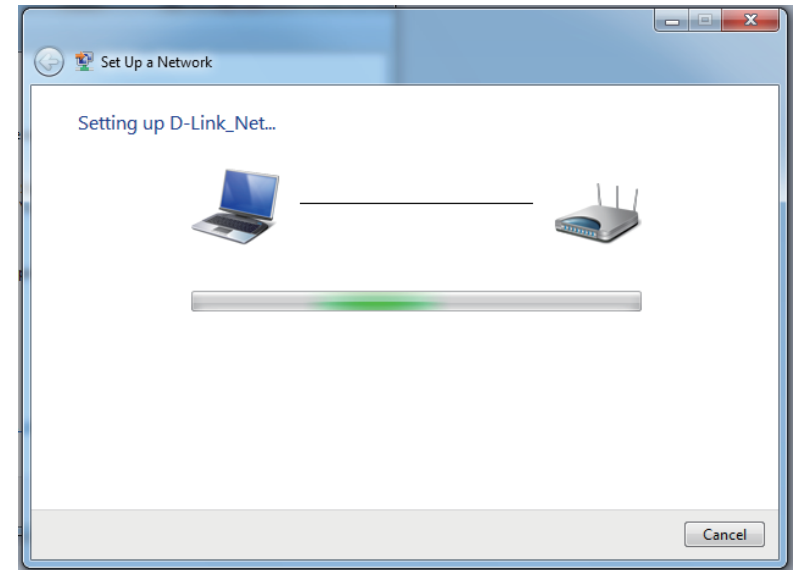
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



7. The following window appears while the Router is being configured.

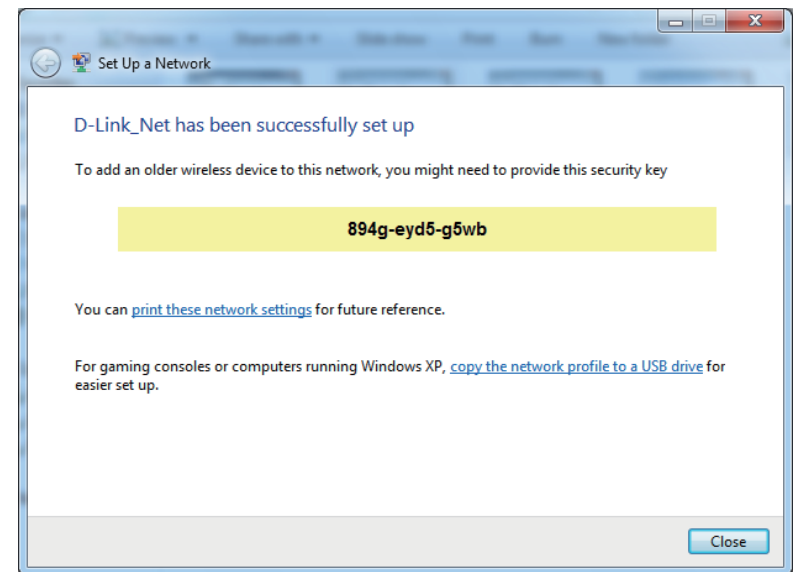
Wait for the configuration to complete.



8. The following window informs you that WPS on the DAP-2020 has been setup successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click **Close** to complete WPS setup.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-2020. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link access point, 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® 11 and higher
 - Mozilla Firefox 28 and higher
 - Google™ Chrome 33 and higher
 - Apple Safari 7 and higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the Security tab, click the button to restore the settings to their defaults.
 - Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.
 - Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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 defaults.

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

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, let's 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 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 access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

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

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

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

What is Wireless?

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

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your access point or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless bridge.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless bridge. All the wireless devices, or clients, will connect to the wireless bridge or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP address

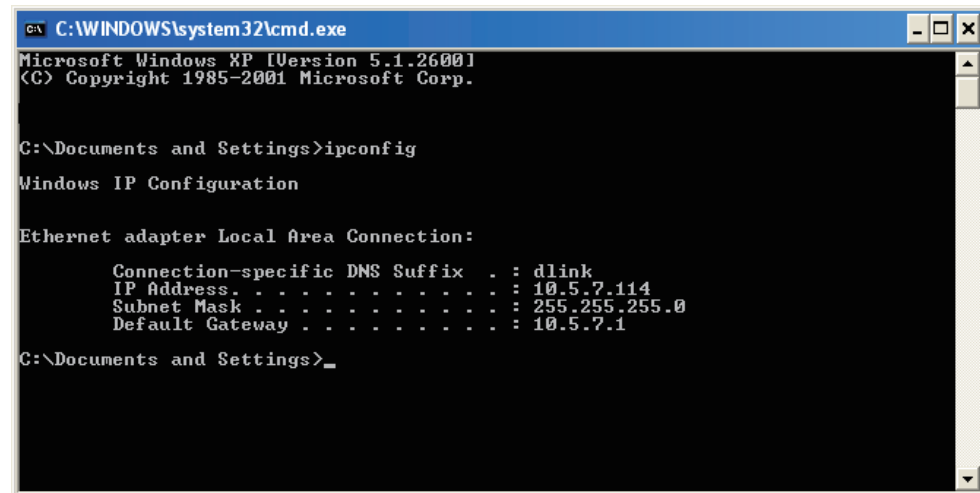
After you install your adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on Start > Run. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type cmd in the Start Search box.)

At the prompt, type **ipconfig** and press **Enter**.

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

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600.1
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

Statically Assign an IP address

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

Step 1

Windows® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Setting.**

Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**

Windows® XP - Click on **Start > Control Panel > Network Connections.**

Windows® 2000 - From the desktop, right-click **My Network Places > Properties.**

Step 2

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

Step 3

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

Step 4

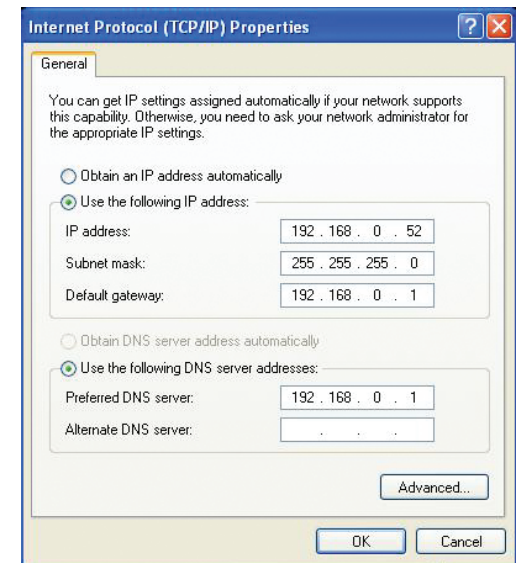
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

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



Technical Specifications

Standards

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

Security

- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise

Wireless Signal Rates¹

- 300Mbps
- 108Mbps
- 54Mbps
- 48Mbps
- 36Mbps
- 24Mbps
- 18Mbps
- 12Mbps
- 11Mbps
- 9Mbps
- 6Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

Maximum Operating Voltage

- 12V / 0.5A

Modulation

- DQPSK
- DBPSK
- CCK
- OFDM

Frequency Range²

- 2.4GHz to 2.483GHz

LEDs

- Power
- Wireless
- Security
- LAN

Operating Temperature

- 32°F to 131°F (0°C to 55°C)

Humidity

- 90% maximum (non-condensing)

Safety & Emissions

- FCC
- IC
- CE
- C-Tick

Dimensions

- 144 (W) x 109 (D) x 30 (H) mm (5.67 x 4.29 x 1.18 inches)

Warranty

- 2 years

¹Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

²Range varies depending on country's regulation.

Trademarks:

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

Copyright Statement:

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

Copyright ©2010-2011 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning:

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

Federal Communication Commission Interference Statement

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

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

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 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.