

USER MANUAL

DAP-1353

VERSION 2.10



Table of Contents

Product Overview	4	DHCP SERVER.....	27
Package Contents	4	DHCP Server Settings	28
System Requirements	4	Multi-SSID	29
Introduction	5	Multi-SSID Settings	30
Features	6	User Limit	31
Hardware Overview	7	User Limit Setting	32
Connections	7	Maintenance	33
LEDs	8	Device Administration	34
Installation.....	9	System	35
Wireless Installation Considerations.....	10	Firmware	36
Configuration	11	MISC.....	37
Web-based Configuration Utility	11	Time.....	38
Setup Wizard	13	Status	39
Wireless Setup.....	18	Device Info.....	40
Wireless Settings	19	Statistics	41
LAN Setup	20	Log.....	42
LAN Settings	21	Client Info.....	44
Advanced.....	22	Support	45
Performance	22	Wireless Security.....	46
Advanced Wireless Settings	23	What is WEP?	46
Filter.....	24	Configure WEP.....	47
Wireless Access Settings.....	25	What is WPA?	49
WLAN Partition	26	Configure WPA-Personal	50
		Configure WPA (Enterprise)	51

Connect to a Wireless Network.....	52
Using Windows® XP.....	52
Configure WEP	53
Configure WPA-Personal	55
Troubleshooting	57
Wireless Basics	59
What is Wireless?	60
Tips	62
Wireless Modes	63
Networking Basics	64
Check your IP address	64
Statically Assign an IP address	65
Technical Specifications.....	66

Package Contents

- D-Link DAP-1353 RangeBooster N 650 Access Point
- 3 Detachable Antennas
- Power Adapter
- CAT5 Ethernet Cable
- CD-ROM with Product Documentation
- Quick Install Guide

Note:1. Using a power supply with a different voltage rating than the one included with the DAP-1353 will cause damage and void the warranty for this product.
2. The power supply shall instruct the user not to remove the plug and plug into a wall outlet by itself; always attach the plug to the power supply first before insert.



System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet Adapter
- Internet Explorer Version 6.0 and Firefox 1.5 or above (for configuration)

Introduction

TOTAL PERFORMANCE

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

TOTAL COVERAGE

Provides greater wireless signal rates even at further distances for best-in-class coverage.

ULTIMATE PERFORMANCE

The D-Link RangeBooster N 650 Access Point (DAP-1353) is a draft 802.11n compliant device that delivers real world performance of up to 650% 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.

EXTENDED WHOLE HOME COVERAGE

Powered by RangeBooster N 650 technology, this high performance access point provides superior Whole Home Coverage while reducing wireless dead spots. The RangeBooster N 650 Access Point is designed for use in bigger homes and for users who demand higher performance networking. Add a RangeBooster N 650 notebook or desktop wireless adapter and stay connected to your network from virtually anywhere in your home.

TOTAL NETWORK SECURITY

The RangeBooster N 650 Access Point supports all of the latest wireless security features to prevent unauthorized access. Support for WPA and WEP encryption standards ensure that you'll be able to use the best possible encryption method, regardless of your wireless client devices.

* Maximum wireless signal rate derived from IEEE Standard 802.11g and draft 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.

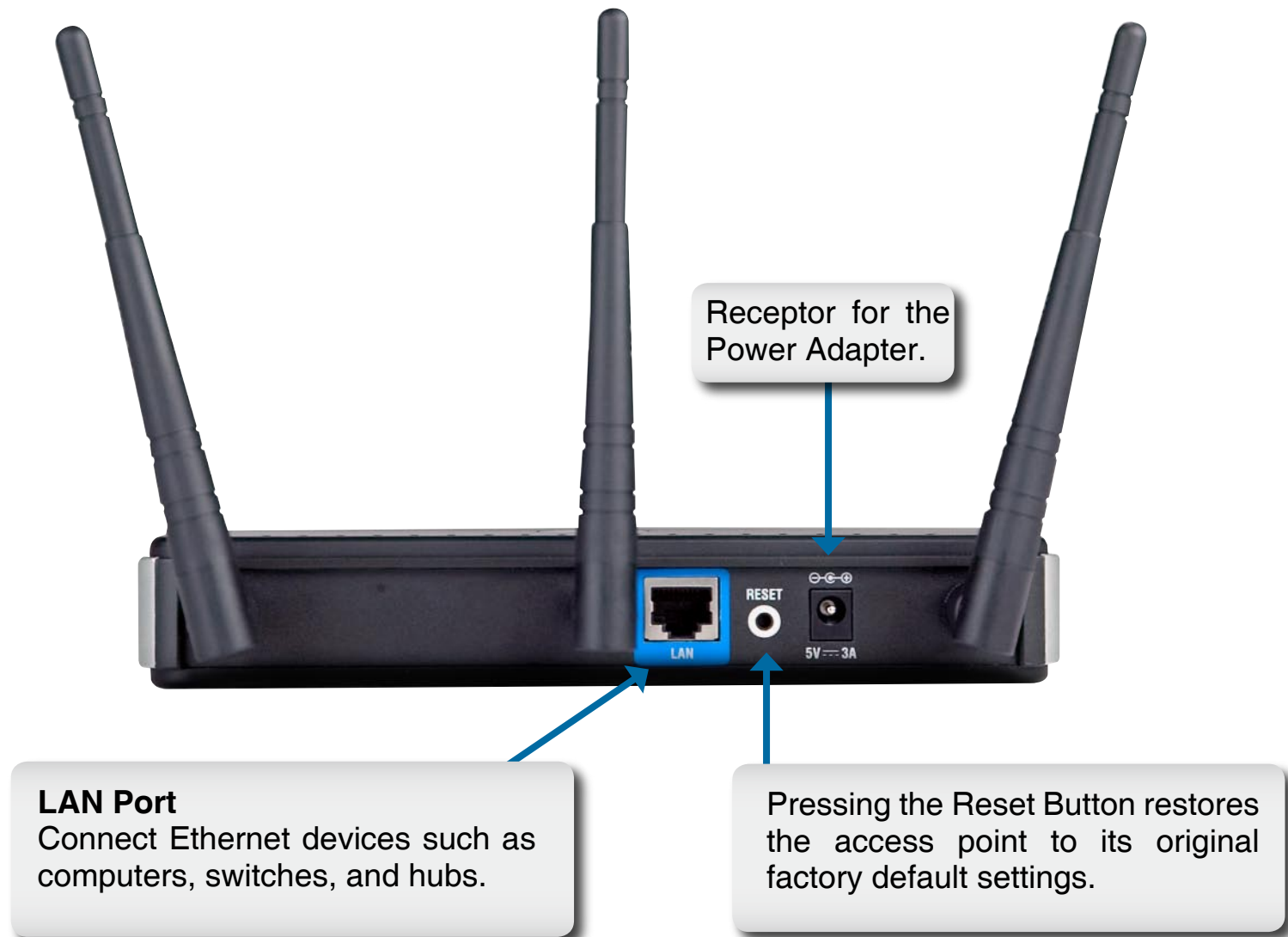
Features

- **Faster Wireless Networking** - The DAP-1353 provides up to 300Mbps* wireless connection with other draft 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. The performance of this draft 802.11n wireless access point gives you the freedom of wireless networking at speeds 650% faster than 802.11g.
- **Compatible with 802.11b and 802.11g Devices** - The DAP-1353 is still fully compatible with the IEEE 802.11b standard, so it can connect with existing 802.11b PCI, USB and Cardbus adapters.
- **MAC Address Filtering** - Allow or deny wireless clients access to the network based on their MAC address.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DAP-1353 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.

* Maximum wireless signal rate derived from IEEE Standard 802.11g and draft 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.

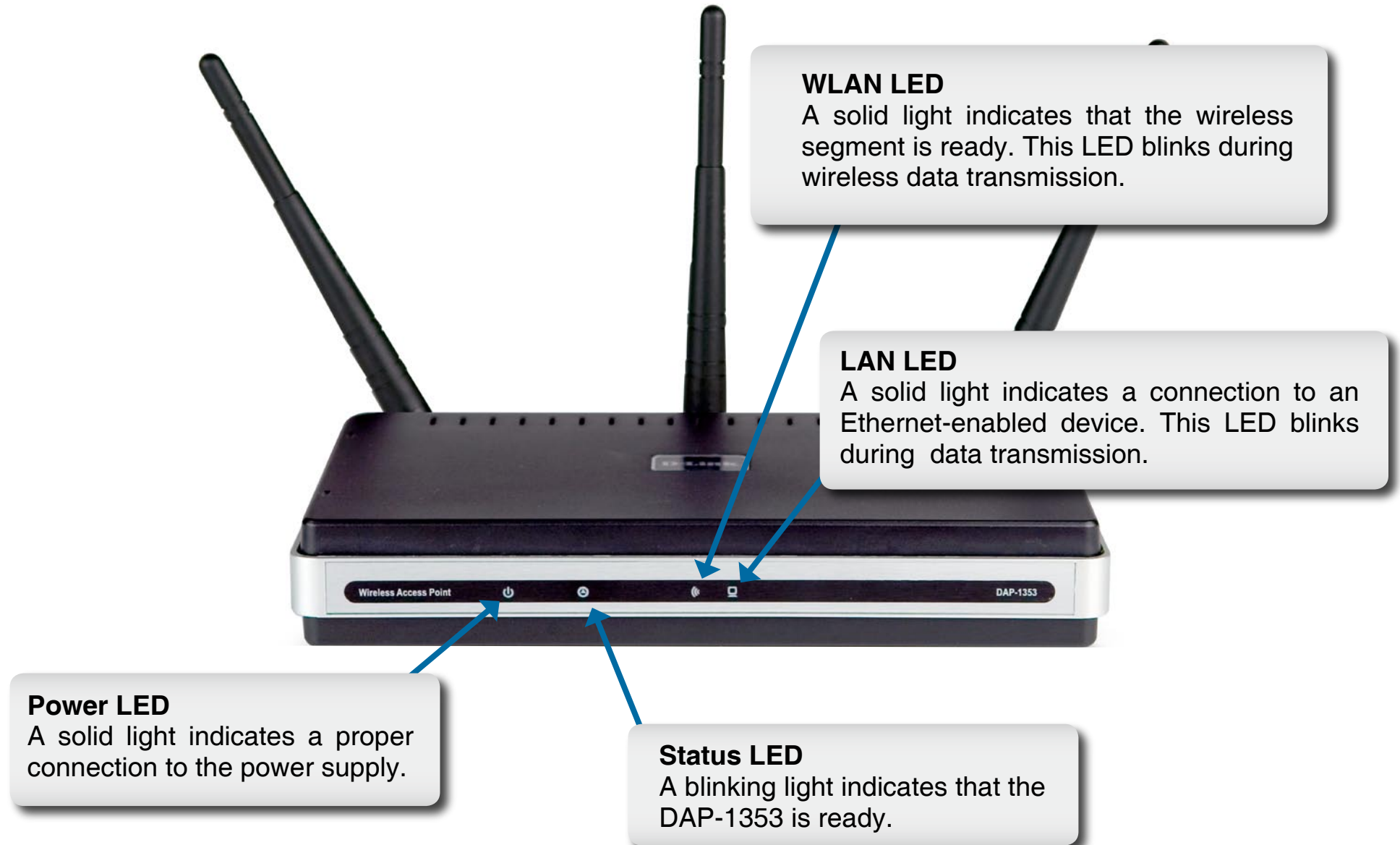
Hardware Overview

Connections



Hardware Overview

LEDs



Installation

This section will walk you through the installation process. Placement of the access point is very important. Do not place the access point in an enclosed area such as a closet, cabinet, or in the attic or garage.

Wireless Installation Considerations

The D-Link RangeBooster N 650 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:

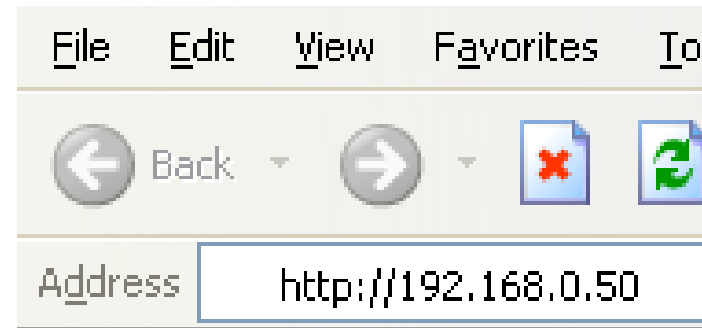
1. Keep the number of walls and ceilings between the access point and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between 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 routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4GHz 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.

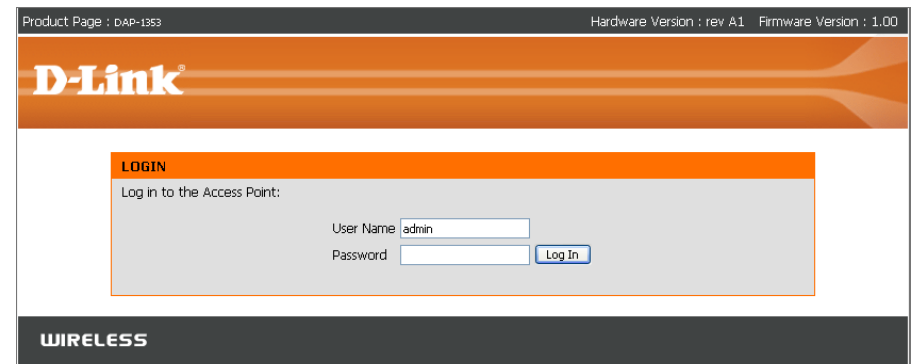
Web-based Configuration Utility

To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the access point (192.168.0.50).

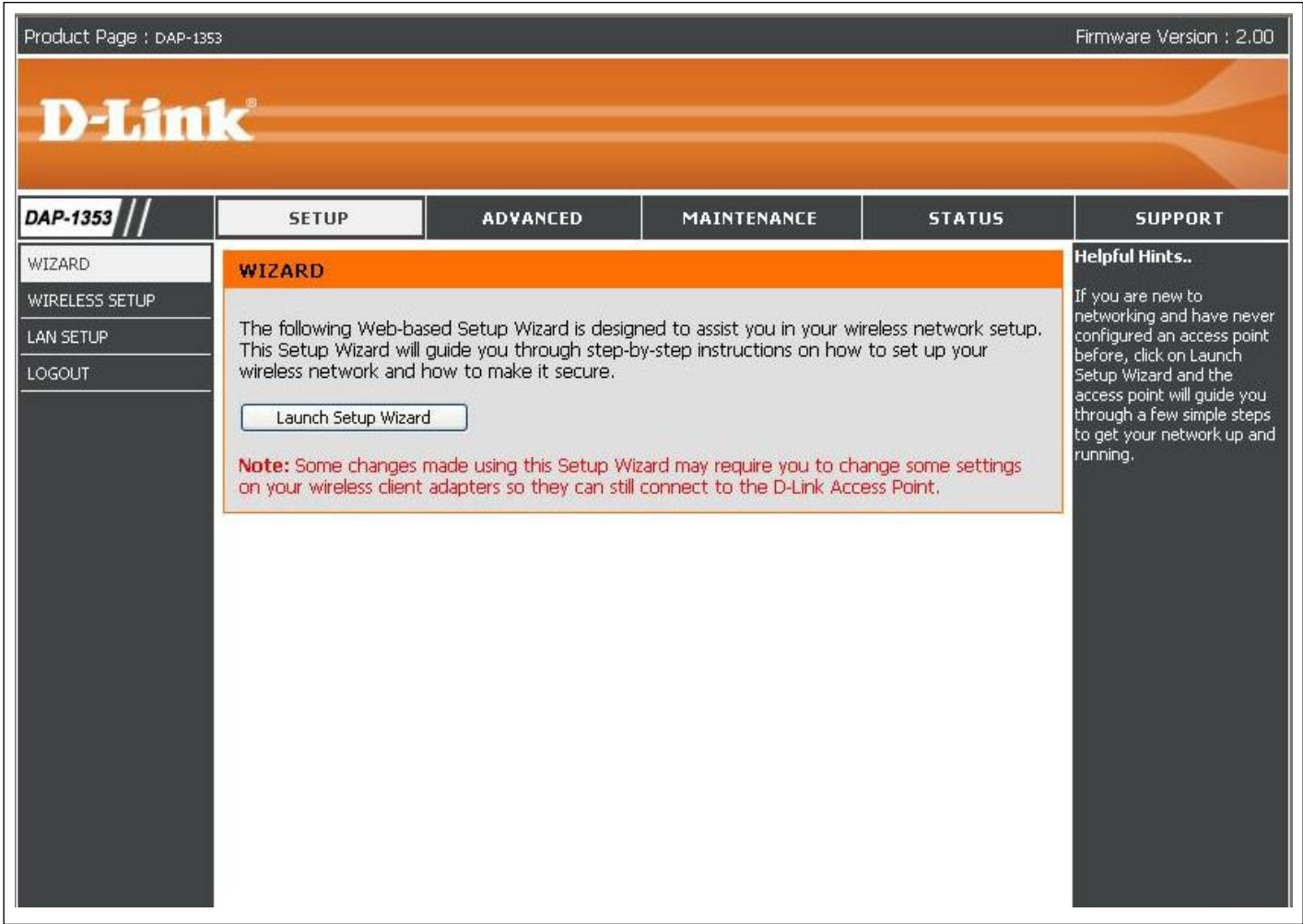


Enter the user name (admin) and your password. Leave the password blank by default.

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



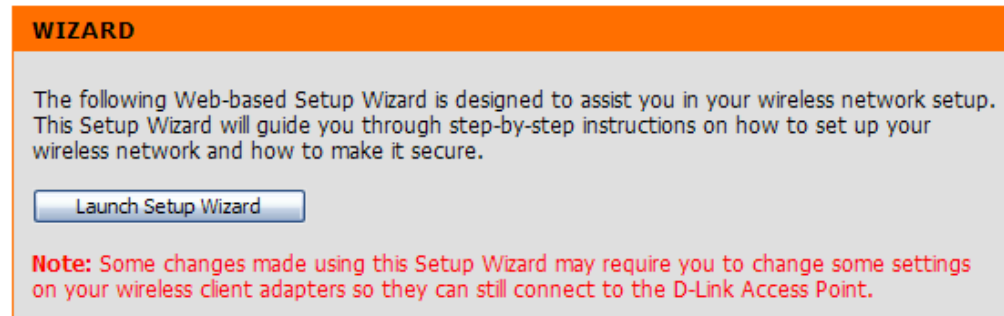
After logging in the **Setup > Wizard** page will be displayed:



Setup Wizard

A Setup Wizard is available to quickly and easily configure access point wireless security settings.

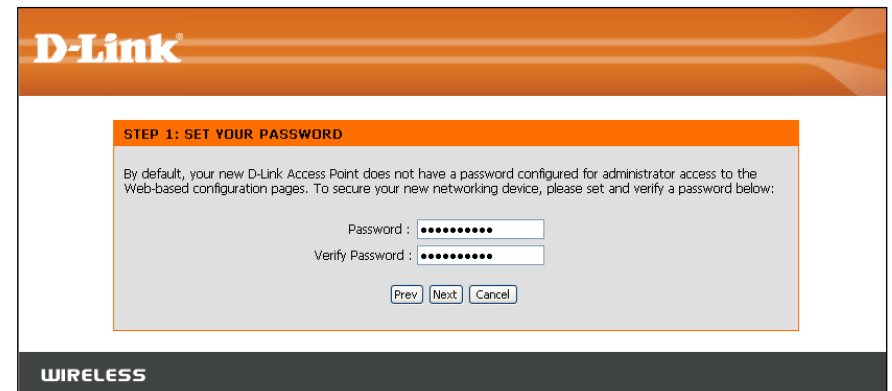
Click **Launch Setup Wizard**.



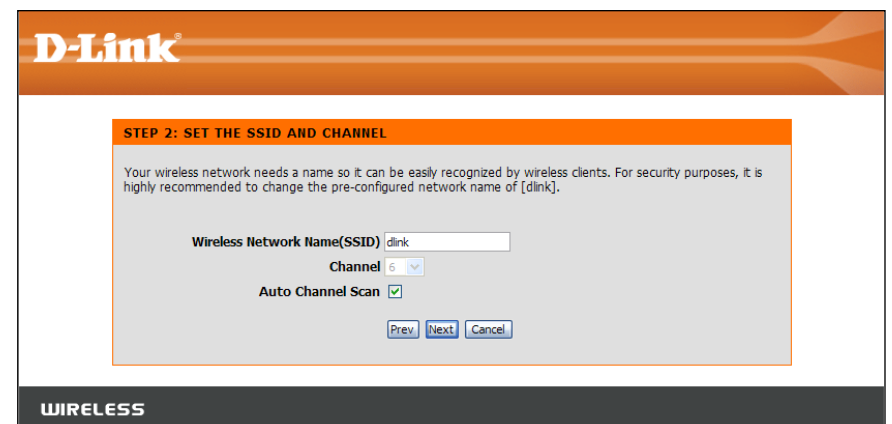
The wizard welcome screen will appear. Click **Next** to continue.



Create a new password and then click **Next** to continue.



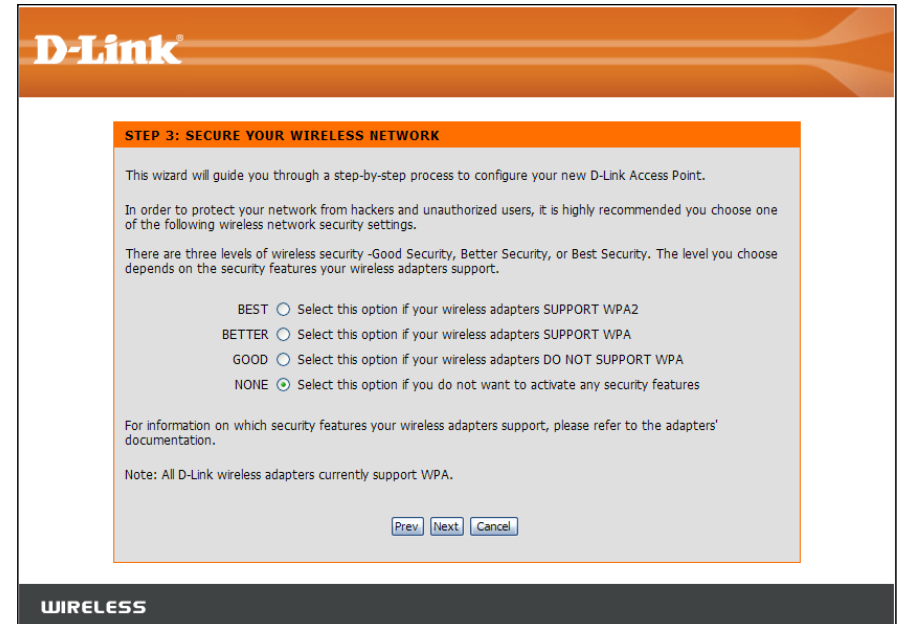
Enter your wireless network name (SSID). Auto Channel Scan is enabled by default. Uncheck the option to select a channel. Click **Next** to continue.



Select the type of wireless security you want to use:

- Best - WPA2 Authentication
- Better - WPA Authentication
- Good - WEP Encryption
- None - No Security

Click **Next** to continue.



The screenshot shows the D-Link configuration interface for Step 3: SECURE YOUR WIRELESS NETWORK. The page has an orange header with the D-Link logo. The main content area is white with an orange border. It contains instructions about selecting a security level and four radio button options: BEST (WPA2), BETTER (WPA), GOOD (WEP), and NONE (No Security). The 'NONE' option is selected. At the bottom, there are 'Prev', 'Next', and 'Cancel' buttons. A dark grey footer bar contains the word 'WIRELESS' in white.

D-Link

STEP 3: SECURE YOUR WIRELESS NETWORK

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

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are three levels of wireless security -Good Security, Better Security, or Best Security. The level you choose depends on the security features your wireless adapters support.

BEST ☐ Select this option if your wireless adapters SUPPORT WPA2

BETTER ☐ Select this option if your wireless adapters SUPPORT WPA

GOOD ☐ Select this option if your wireless adapters DO NOT SUPPORT WPA

NONE ☒ Select this option if you do not want to activate any security features

For information on which security features your wireless adapters support, please refer to the adapters' documentation.

Note: All D-Link wireless adapters currently support WPA.

Prev Next Cancel

WIRELESS

If you selected Good (WEP) security, select a **Key Type**, **Key Size**, and enter a **Wireless Security Password**:

Click **Next** to continue.



The screenshot shows the D-Link configuration interface for Step 3: SET YOUR WIRELESS SECURITY PASSWORD. The page has an orange header with the D-Link logo. The main content area is white with an orange border. It contains instructions about entering encryption key values and fields for Key Type (set to HEX), Key Size (64 selected), and Wireless Security Password. At the bottom, there are 'Prev', 'Next', and 'Cancel' buttons. A dark grey footer bar contains the word 'WIRELESS' in white.

D-Link

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

Once you have selected your security level - enter the encryption Key Values.

Key Type: HEX

Key Size: ☒ 64 ☐ 128

Wireless Security Password: 0000000000

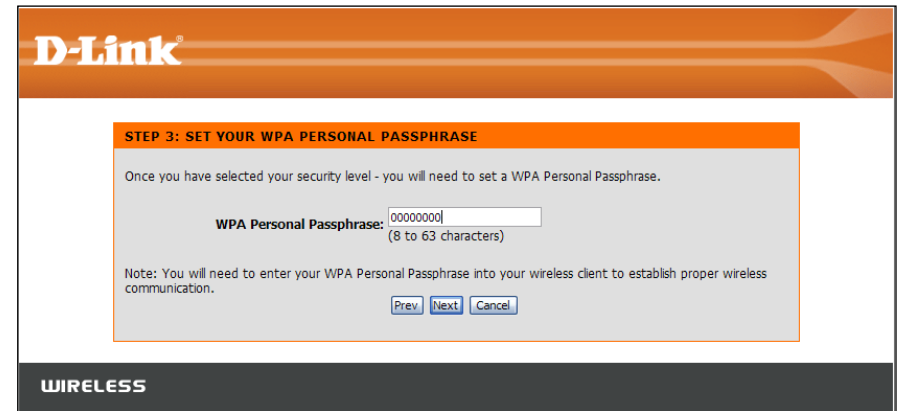
Note: You will need to enter your Wireless Security Password into your wireless client to establish proper wireless communication.

Prev Next Cancel

WIRELESS

If you selected Better/Best security, enter a **Wireless Security Password** between 8-63 characters:

Click **Next** to continue.



The screenshot shows the D-Link wireless setup interface. At the top is the D-Link logo. Below it, a section titled "STEP 3: SET YOUR WPA PERSONAL PASSPHRASE" contains instructions: "Once you have selected your security level - you will need to set a WPA Personal Passphrase." There is a text input field for the "WPA Personal Passphrase:" with a placeholder "00000000" and a note "(8 to 63 characters)". Below the field is a note: "Note: You will need to enter your WPA Personal Passphrase into your wireless client to establish proper wireless communication." At the bottom of the section are three buttons: "Prev", "Next", and "Cancel". The bottom of the screen features a dark grey bar with the word "WIRELESS" in white.

At the **Setup Complete** screen, if you selected Good security, the following screen will show your WEP key. This key should be used by wireless clients connecting to the wireless network:

Click **Save**.



The screenshot shows the D-Link wireless setup interface at the "SETUP COMPLETE!" stage. The D-Link logo is at the top. Below it, a section titled "SETUP COMPLETE!" contains a message: "Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters." The settings listed are: "Wireless Network Name (SSID) : dlink", "Channel : 6", "Wep Key Type : HEX", "Wep Key Length : 64bits", "Default WEP Key to Use : 1", "Authentication : Open", and "Wep Key : 0000000000". At the bottom of the section are three buttons: "Prev", "Save", and "Cancel". The bottom of the screen features a dark grey bar with the word "WIRELESS" in white.

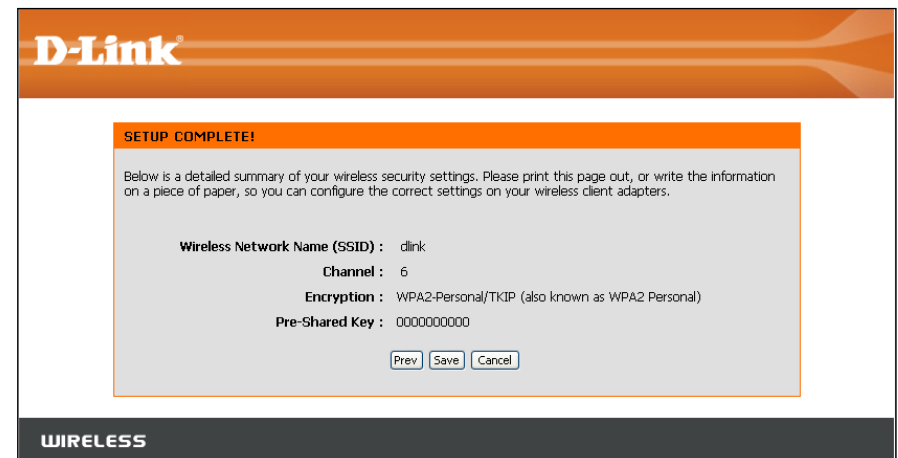
If you selected Better security, the following screen will show your Pre-Shared Key. This key should be used by wireless clients connecting to the wireless network.

Click **Save**.



If you selected Best security, the following screen will show your Pre-Shared Key. This key should be used by wireless clients connecting to the wireless network:

Click **Save**.



Wireless Setup

The Wireless Setup page is used to configure the wireless settings for the access point. Wireless security settings are also configured on this page.

DAP-1353

WIZARD

WIRELESS SETUP

LAN SETUP

LOGOUT

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

WIRELESS NETWORK

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

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

Save Settings

Don't Save Settings

WIRELESS NETWORK SETTINGS

Wireless Network Name : (Also called the SSID)

Operation Mode :

Access Point

Wireless Channel :

6

Enable Auto Channel Scan : ☒

802.11 Mode :

Mixed 802.11n, 802.11g and 802.11b

Channel Width :

20 MHz

Transmission Rate :

Best(Up to 300)

SSID Broadcast :

Enable

WIRELESS SECURITY MODE

Security Mode :

Disable Wireless Security (not recommended)

Disable Wireless Security (not recommended)

Enable WEP Wireless Security (basic)

Enable WPA Wireless Security (enhanced)

Enable WPA2 Wireless Security (enhanced)

Enable WPA2-Auto Wireless Security (enhanced)

Helpful Hints..

- Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.
- Enable Auto Channel Scan so that the access point can select the best possible channel for your wireless network to operate on.
- Setting SSID Broadcast to Disable is another way to secure your network. With SSID Broadcast disabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your access point, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down the Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Wireless Settings

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive, and set to **dlink** by default.

Operation Mode : Select Access Point mode, WDS mode, WDS with AP mode, AP Repeater mode or AP Client mode.

Wireless Channel: Indicates the channel setting for the DAP-1353. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Enable Auto Channel Scan: Enabled by default, allows the DAP-1353 to select the channel with the least amount of interference.

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

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

Transmission Rate: Select the transmission rate. It is strongly suggested to use the **Best** setting for optimal performance.

SSID Broadcast: Select Disable if you do not want the SSID to be broadcast by the DAP-1353. 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-1353 in order to connect to it.

Wireless Security Mode: Select a wireless security setting. Options are None, WEP, WPA, WPA2 or WPA2-Auto. See p. 46 for a detailed explanation of the wireless security options.

The screenshot displays two configuration sections. The top section, titled 'WIRELESS NETWORK SETTINGS', includes fields for 'Wireless Network Name' (set to 'dlink'), 'Operation Mode' (set to 'Access Point'), 'Wireless Channel' (set to '6'), 'Enable Auto Channel Scan' (checked), '802.11 Mode' (set to 'Mixed 802.11n, 802.11g and 802.11b'), 'Channel Width' (set to '20 MHz'), 'Transmission Rate' (set to 'Best (Up to 300)'), and 'SSID Broadcast' (set to 'Enable'). The bottom section, titled 'WIRELESS SECURITY MODE', shows a 'Security Mode' dropdown menu with the following options: 'Disable Wireless Security (not recommended)', 'Enable WEP Wireless Security (basic)', 'Enable WPA Wireless Security (enhanced)', 'Enable WPA2 Wireless Security (enhanced)', and 'Enable WPA2-Auto Wireless Security (enhanced)'. The first option is currently selected.

LAN Setup

The LAN, or Local Area Network, is your private, internal network. This page allows you to configure the IP settings of the LAN interface for the DAP-1353. The IP address can be changed to your current network IP range. This IP address cannot be seen from the Internet.

Product Page : DAP-1353

Firmware Version : 2.00

DAP-1353 //

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

WIZARD
WIRELESS SETUP
LAN SETUP
LOGOUT

LAN CONNECTION

Use this section to configure your LAN Connection type. There are two connection types to choose from: Static IP, DHCP.

Save Settings

Don't Save Settings

LAN CONNECTION TYPE

Choose the mode to be used by the Access Point.

My LAN Connection is :

Static IP

STATIC IP ADDRESS LAN CONNECTION TYPE

Enter the static address information.

IP Address : 192.168.0.50

Subnet Mask : 255.255.255.0

Gateway Address :

Helpful Hints..

LAN Settings

Also referred as private settings, LAN settings allow you to configure LAN interface of DAP-1353. LAN IP address is private to your internal network and is not visible to Internet. The default IP address 192.168.0.50 with subnet mask as 255.255.255.0.

- My LAN Connection is - The factory default setting is "Static IP" which allows the IP address of the DAP-1353 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

LAN Settings

My LAN Connection Is:

The DAP-1353 is set to Static by default. Select this option if you do not have a DHCP server on your network, or if you wish to assign a static IP address to the DAP-1353.

IP Address:

If you change the IP address and save the settings, you will need to log back into the DAP-1353 using the new IP address.

Subnet Mask:

Enter the subnet mask. Default setting is 255.255.255.0.

Gateway Address:

Enter the IP address of the your network gateway.

LAN CONNECTION TYPE

Choose the mode to be used by the Access Point.

My LAN Connection is :

Static IP

Static IP

Dynamic IP (DHCP)

STATIC IP ADDRESS LAN CONNECTION TYPE

Enter the static address information.

IP Address :

192.168.0.50

Subnet Mask :

255.255.255.0

Gateway Address :

Advanced Performance

This section contains advanced wireless configuration options. It is recommended that these options remain at their default values, as improperly adjusting them can have a negative effect on your wireless network performance. If you want to modify these settings and are unfamiliar with them, refer to the explanations below or the Support menu of the access point.

Product Page : DAP-1353

Firmware Version : 2.10

D-Link

DAP-1353

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

PERFORMANCE

FILTER

WLAN PARTITION

DHCP SERVER

MULTI-SSID

USER LIMIT

LOGOUT

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%

Beacon interval : 100 (msec, range:25~500, default:100)

DTIM interval : 1 (range: 1~15, default:1)

WMM : ☒ Enable ☐ Disable

Helpful Hints..

- If 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.


Advanced Wireless Settings

Transmit Power: Set the transmit power of the antennas.

Beacon Interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

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

WMM Function: WMM is QoS for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.

ADVANCED WIRELESS SETTINGS	
Transmit Power :	100% 
Beacon interval :	100 (msec, range:25~500, default:100)
DTIM interval :	1 (range: 1~15, default:1)
WMM :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Filter

Use MAC address filters to allow or deny wireless clients network access based on their MAC address.

Product Page : DAP-1353

Firmware Version : 2.10

D-Link

DAP-1353

PERFORMANCE

FILTER

WLAN PARTITION

DHCP SERVER

MULTI-SSID

USER LIMIT

LOGOUT

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

NETWORK SETTING

The DAP-1353 can be setup to deny or only allow access to wireless clients with the listed MAC addresses.

Save Settings

Don't Save Settings

WIRELESS ACCESS SETTINGS

Use the client's **MAC Address** to authorise network access through the Access Point.

Access Control :

Disable

MAC Address : : : : :

MAC ADDRESS LIST

MAC Address	Del	MAC Address	Del
-------------	-----	-------------	-----

Helpful Hints..

Access Control

- Use the client's **MAC Address** to authorise network access through the Access Point.
- Select **Accept** to enable communication between the Access Point and only other wireless devices with MAC addresses listed in the Authorization table.
- Select **Reject** to disable communication between the Access Point and other wireless devices with MAC addresses listed in the Authorization table.

Wireless Access Settings

- Access Control:** Disabled by default, select **Accept** or **Reject** to filter wireless access to the MAC addresses listed in the MAC Address List.
- MAC Address:** Enter MAC addresses to be associated with the selected Access Control option.
- MAC Address List:** Displays list of currently filtered MAC addresses.

WIRELESS ACCESS SETTINGS

Use the client's **MAC Address** to authorize network access through the Access Point.

Access Control :

Disable

MAC Address : : : : : :

MAC ADDRESS LIST

MAC Address	Del	MAC Address	Del
-------------	-----	-------------	-----

WLAN Partition

Internal Station Connection

The default value is "allow" which allows stations to inter-communicate by connecting to target AP. By disabling this function, wireless stations cannot exchange data through AP.

Ethernet to WLAN Access

The default value is "allow" which allows data flow from the Ethernet to wireless stations connected to the AP. By disabling this function, all data from the Ethernet to associated wireless devices is blocked while wireless stations can still send data to the Ethernet through the AP.

The screenshot shows the D-Link DAP-1353 Advanced Setup page. The top header bar is orange with the D-Link logo. Below it, a navigation bar contains tabs for SETUP, ADVANCED (selected), MAINTENANCE, STATUS, and SUPPORT. On the left, a sidebar lists various configuration categories: PERFORMANCE, FILTER, WLAN PARTITION (selected), DHCP SERVER, MULTI-SSID, USER LIMIT, and LOGOUT. The main content area is titled 'WLAN PARTITION SETTINGS' and contains two settings: 'Internal Station Connection' and 'Ethernet to WLAN Access', both set to 'Allow'. There are 'Save Settings' and 'Don't Save Settings' buttons at the top of the settings area. A 'Helpful Hints..' link is visible on the right side of the page.

Product Page : DAP-1353		Firmware Version : 2.10	
D-Link			
DAP-1353 //	SETUP	ADVANCED	MAINTENANCE
PERFORMANCE	WLAN PARTITION SETTINGS		Helpful Hints..
FILTER	<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>		
WLAN PARTITION			
DHCP SERVER	WLAN PARTITION SETTINGS		
MULTI-SSID	Internal Station Connection : <input type="button" value="Allow"/>		
USER LIMIT	Ethernet to WLAN Access : <input type="button" value="Allow"/>		
LOGOUT			

DHCP SERVER

Dynamic Host Configuration Protocol assigns IP addresses to wireless devices on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign IP addresses.

Product Page : DAP-1353

Firmware Version : 2.10

D-Link

DAP-1353

PERFORMANCE

FILTER

WLAN PARTITION

DHCF SERVER

MULTI-SSID

USER LIMIT

LOGOUT

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

NETWORK SETTING

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP address to the computers on your network. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.

Save Settings

Don't Save Settings

DHCP SERVER SETTINGS

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

Enable DHCP Server :

☐

IP Assigned From :

192.168.0.20

to

254

Default Subnet Mask :

255.255.255.0

Default Gateway :

Default Wins :

Default DNS :

Lccal Domain Name :

dlink-ap

Helpful Hints..

• 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.

DHCP Server Settings

Enable DHCP Server: Check the box to enable the DHCP server on your DAP-1353. Uncheck to disable this function.

IP Assigned From: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

Default Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

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

Default WINS: Windows Internet Naming Service is a system that determines the IP address of a network computer with a dynamically assigned IP address, if applicable.

Default DNS: Enter the IP address of the Domain Name Server, if applicable. The DNS translates domain names such as www.dlink.com into IP addresses.

Local Domain Name: Enter the domain name of the DAP-1353, if applicable.

DHCP Lease Time: The length of time in minutes for the IP lease.

DHCP SERVER SETTINGS

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


Enable DHCP Server :	<input type="checkbox"/>	
IP Assigned From :	<input type="text" value="192.168.0.20"/>	to <input type="text" value="254"/>
Default Subnet Mask :	<input type="text" value="255.255.255.0"/>	
Default Gateway :	<input type="text"/>	
Default Wins :	<input type="text"/>	
Default DNS :	<input type="text"/>	
Local Domain Name :	<input type="text" value="dlink-ap"/>	
DHCP Lease Time :	<input type="text" value="10080"/> (minutes)	

Multi-SSID

If you want to configure the Guest and Internal networks on Virtual LAN (VLANs), the switch and DHCP server you are using must support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard.

Product Page : DAP-1353

Firmware Version : 2.10



DAP-1353 //

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

PERFORMANCE

FILTER

WLAN PARTITION

DHCP SERVER

MULTI-SSID

USER LIMIT

LOGOUT

MULTI-SSID SETTINGS

Save Settings Don't Save Settings

MULTI-SSID SETTINGS

☐ Enable Multi-SSID ☐ Enable VLAN State

Index Primary SSID

SSID dlink

SSID Broadcast Disable

Security Open System

VLAN ID 1

KEY SETTINGS

Key Type HEX

WEP Encryption 64Bit

Key 1

Helpful Hints..

Multi-SSID Settings



The screenshot shows a web interface titled "MULTI-SSID SETTINGS". At the top, there are two checkboxes: "Enable Multi-SSID" and "Enable VLAN State", both of which are currently unchecked. Below these, there is a table-like structure with labels on the left and input fields on the right. The labels are "Index", "SSID", "SSID Broadcast", "Security", and "VLAN ID". The corresponding input fields are: "Primary SSID" (a dropdown menu), "dlink" (a text input field), "Enable" (a dropdown menu), "None" (a dropdown menu), and "1" (a text input field).

MULTI-SSID SETTINGS	
<input type="checkbox"/> Enable Multi-SSID <input type="checkbox"/> Enable VLAN State	
Index	Primary SSID ▼
SSID	dlink
SSID Broadcast	Enable ▼
Security	None ▼
VLAN ID	1

Index: The Primary SSID and Security cannot be changed here. Those values follow the setting in SETUP>WIRELESS.

SSID: When you Enable Multi-SSID you can name each Multi-SSID.

SSID Broadcast: Enable or Disable SSID Broadcast. Enabling this feature broadcasts the SSID across the network.

Security: The Security option for these seven Multi-SSIDs are None, Open System or Shared Key, WPA-EAP, WPA-PSK, WPA2-EAP, WPA2-PSK, WPA-Auto-EAP, WPA-Auto-PSK.

VLAN ID: When you Enable VLAN State and configure internal and Multi-SSID networks on VLANs, this field will be enable.

Provide a number between 1 and 4094 for internal VLAN. This will cause the access point to send DHCP request with the VLAN tags. The switch and the DHCP server must support VLAN IEEE802.1Q frames. The access point must be able to reach the DHCP Server. Check with the Administrator regarding the VLAN and DHCP configurations.

User Limit

The D-Link DAP-1353 can set limit of wireless client. Using user limit, you can prevent scenarios where the DAP-1353 in your network shows performance degradation because it is handling a heavy wireless traffic.



User Limit Settings

User Limit: When user limit is enabled, select the user limit.

User Limit Select user limit in this field , range cover from 0~64. You can specify the limit only when user limit is enabled.
(0 - 64):


Maintenance

Device Administration

This page will allow you to change the Administrator and User passwords. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

Product Page : DAP-1353

Firmware Version : 2.00



DAP-1353

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

DEVICE ADMINISTRATION

SYSTEM

FIRMWARE

MISC

TIME

LOGOUT

ADMINISTRATOR SETTINGS

There are two accounts that can access the Access Point's management interface. These accounts are **admin** and **user**.
Admin has read/write access while **user** has read-only access.
User can only view the settings but cannot make any changes.
Only the **admin** account has the ability to change both **admin** and **user** account passwords.

ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "admin")

Login Name:

New Password:

Confirm Password:

USER (THE DEFAULT LOGIN NAME IS "user")

Login Name:

New Password:

Confirm Password:

Helpful Hints..

- For security reasons, it is recommended that you change the Login Name and Password for the Administrator and User accounts. Be sure to write down the new Login Names and Passwords to avoid having to reset the Access Point in the event that they are forgotten.

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

User Password: Enter the new password for the User login. If you login as the User, you can only see the settings, but cannot change them.

ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "admin")	
Login Name:	<input type="text" value="admin"/>
New Password:	<input type="password" value="••••••••"/>
Confirm Password:	<input type="password" value="••••••••"/>

USER (THE DEFAULT LOGIN NAME IS "user")	
Login Name:	<input type="text" value="user"/>
New Password:	<input type="password" value="••••••••"/>
Confirm Password:	<input type="password" value="••••~•••"/>

System

Save Settings 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. First, click the **Save** button. You will then see a file dialog, where you can select a location and file name for the settings.

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

Restore to Factory Default Settings: 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, click the **Save** button above.

Reboot: Reboots the DAP-1353.


The screenshot shows the D-Link DAP-1353 web interface. At the top, it says 'Product Page : DAP-1353' and 'Firmware Version : 2.00'. Below this is a large orange banner with the 'D-Link' logo. A navigation bar contains tabs for 'DAP-1353 //', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'SUPPORT'. On the left, a sidebar lists 'DEVICE ADMINISTRATION' with sub-items: 'SYSTEM', 'FIRMWARE', 'MISC', 'TIME', and 'LOGOUT'. The main content area is titled 'SYSTEM SETTINGS' and contains the following text: 'The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.' Below this, there are four sections with buttons: 'Save Settings To Local Hard Drive : [Save]', 'Load Settings From Local Hard Drive : [Browse...] [Upload Settings]', 'Restore To Factory Default Settings : [Restore Device]', and 'Reboots the device : [Reboot]'. On the right, a 'Helpful Hints..' section contains a bullet point: 'Once your Access Point is configured the way you want it, you can save these settings to a configuration file that can later be loaded in the event that the Access Point's default settings are restored. To do this, click the **Save** button next to where it says Save Settings to Local Hard Drive.'

Firmware

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 the this site.

Firmware Upgrade: Click on the link in this screen to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Browse: After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive. Click **Save Settings** to complete the firmware upgrade.

Product Page : DAP-1353		Firmware Version : 2.00							
									
DAP-1353 // DEVICE ADMINISTRATION SYSTEM FIRMWARE MISC TIME LOGOUT		SETUP ADVANCED MAINTENANCE STATUS SUPPORT	Helpful Hints.. <ul style="list-style-type: none"> Firmware updates are released periodically to improve the functionality of your Access Point and also to add features. If you run into a problem with a specific feature of the Access Point, check our support site by clicking on the Click here to check for an upgrade on our support site link and see if an updated firmware is available for your Access Point. 						
		FIRMWARE UPGRADE There may be new firmware for your DAP-1353 to improve functionality and performance. Click here to check for an upgrade on our support site. To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Save Settings below to start the firmware upgrade. <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>							
		CURRENT FIRMWARE INFO <table> <tr> <td>Current Firmware Version</td> <td>2.00</td> </tr> <tr> <td>Firmware Date</td> <td>20:02:13 05/07/2007</td> </tr> <tr> <td></td> <td> <input type="button" value="Browse..."/> </td> </tr> </table>		Current Firmware Version	2.00	Firmware Date	20:02:13 05/07/2007		<input type="button" value="Browse..."/>
Current Firmware Version	2.00								
Firmware Date	20:02:13 05/07/2007								
	<input type="button" value="Browse..."/>								

MISC

Product Page : DAP-1353 Firmware Version : 2.00

D-Link

DAP-1353 // SETUP ADVANCED MAINTENANCE STATUS SUPPORT

DEVICE ADMINISTRATION
SYSTEM
FIRMWARE
MISC
TIME
LOGOUT

MISC SETTINGS

Save Settings Don't Save Settings

CONSOLE SETTINGS

Console Protocol ☐ None ☒ Telnet ☐ SSH

Timeout 3 Mins

SNMP SETTINGS

Status ☐ Enabled

Public Community String public

Private Community String private

Helpful Hints..

Console Protocol: Choose None, Telnet or SSH.

Time Out: Select a time period after which a session timeout will occur.

Status: Check the check box to enable SNMP.

Community String: Enter the Public/Private Community string as the password to access the SNMP service.

Trap Sever IP: Enter the trap server IP when you enable User status notification.

Time

The Time Configuration settings are used by the Access Point for synchronizing scheduled services and system logging activities. You will need to set the time zone corresponding to your location. The time can be set manually or the device can connect to a NTP (Network Time Protocol) server to retrieve the time. You may also set Daylight Saving dates and the system time will automatically adjust on those dates.

DAP-1353	SETUP	ADVANCED	MAINTENANCE	STATUS	SUPPORT
DEVICE ADMINISTRATION SYSTEM FIRMWARE MISC TIME LOGOUT	<div> TIME </div> <div> Time Configuration <p>The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.</p> <p> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p> </div> <div> TIME CONFIGURATION <p>Time : 01/01/1970 00:22:00</p> <p>Time Zone : (GMT-08:00) Pacific Time (US & Canada); Tijuana</p> <p>Enable Daylight Saving : <input type="checkbox"/></p> </div> <div> AUTOMATIC TIME CONFIGURATION <p>Enable NTP server : <input type="checkbox"/></p> <p>Interval : 7 Days</p> <p>NTP Server Used : << Select NTP Server</p> </div> <div> SET THE DATE AND TIME MANUALLY <p>Current Gateway Time :</p> <p> Year 2007 Month May Day 22 Hour 14 Minute 49 Second 40 </p> <p><input type="button" value="Copy Your Computer's Time Settings"/></p> </div>				Helpful Hints.. <ul style="list-style-type: none"> • Either enter the time manually by clicking the Copy Your Computers Time Settings button, or use the Automatic Time Configuration option to have your router synchronize with a time server on the Internet.

Time Zone: Select the Time Zone for the region you are in.

Daylight Saving: If the region you are in observes Daylight Savings Time, enable this option and specify the Starting and Ending Month, Week, Day, and Time for this time of the year.

Automatic Time Configuration: Check the check box to enable SNMP.

Set the Date and Time Manually: Enter the NTP server which you would like the DAP-1353 to synchronize its time with. Also, select the interval at which the DAP-1353 will communicate with the specified NTP server.

Trap Sever IP: Select this option if you would like to specify the time manually. You must specify the Year, Month, Day, Hour, Minute, and Second, or you can click the Copy Your Computer's Time Settings button to copy the system time from the computer being used to access the management interface.

Status

Device Info

This page displays the current information for the DAP-1353. It will display the LAN and Wireless information.

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, Channel and Security Type.

Product Page : DAP-1353

Firmware Version : 2.00

DAP-1353

SETUP

ADVANCED

MAINTENANCE

STATUS

SUPPORT

DEVICE INFO

STATISTICS

LOG

CLIENT INFO

LOGOUT

DEVICE INFORMATION

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

Firmware Version : 2.00 , 20:02:13 05/07/2007

LAN

MAC Address : 00:19:5b:ec:cf:48
Connection : Static IP
IP Address : 192.168.0.50
Subnet Mask : 255.255.255.0
Default Gateway :

WIRELESS LAN

MAC Address : 00:19:5b:ec:cf:48
Network Name(SSID) : dlink
Channel : 11
Security Type : Open / Disabled

Helpful Hints..

This page displays the current information of the DAP-1353. The page will show the firmware currently loaded, wired and wireless settings applied on the unit.

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.

WIRELESS LAN

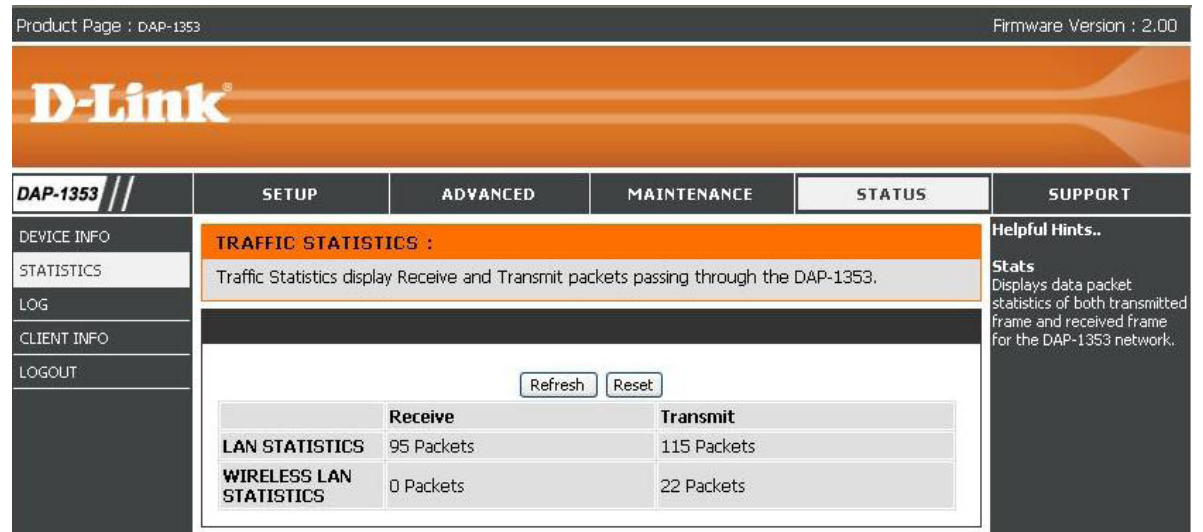
The Wireless MAC address, Wireless Network Name (SSID), Wireless Channel and Wireless Security Type are displayed in this section.

Statistics

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DAP-1353 on the LAN and Wireless network. The traffic counter will reset if the device is rebooted.

Refresh Click Refresh to refresh the Traffic Statistics display.

Reset Click Reset to reset the Traffic Statistics.



Product Page : DAP-1353 Firmware Version : 2.00

D-Link

DAP-1353 // SETUP ADVANCED MAINTENANCE STATUS SUPPORT

TRAFFIC STATISTICS :

Traffic Statistics display Receive and Transmit packets passing through the DAP-1353.

Refresh Reset

	Receive	Transmit
LAN STATISTICS	95 Packets	115 Packets
WIRELESS LAN STATISTICS	0 Packets	22 Packets

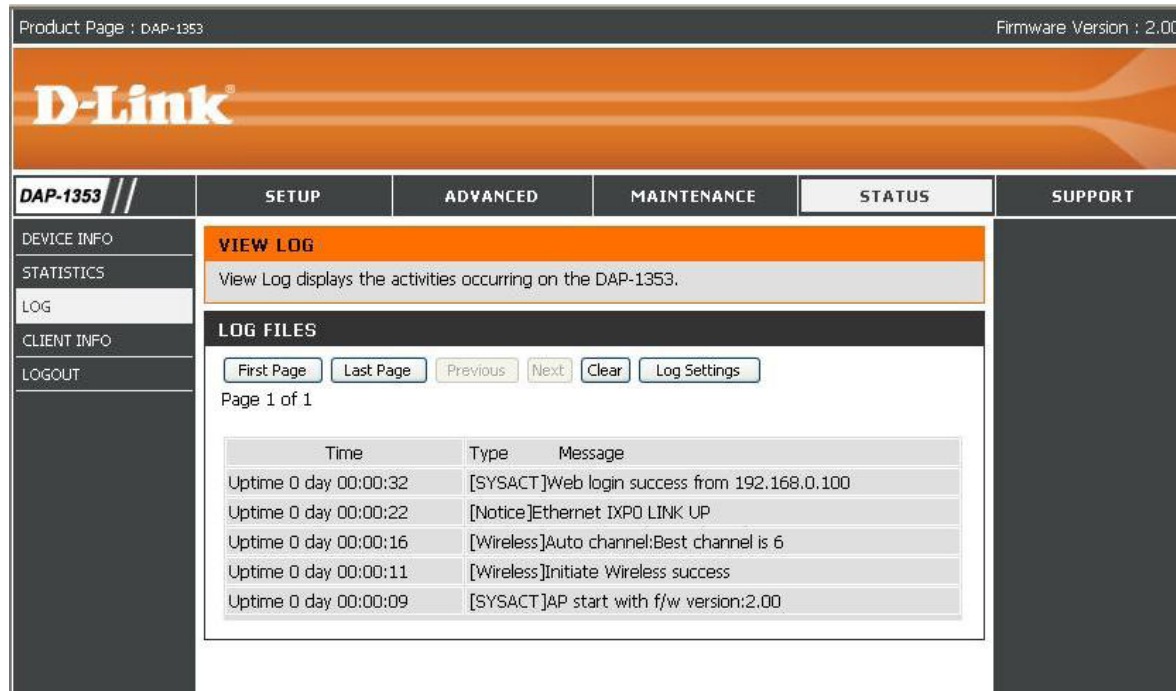
Helpful Hints..

Stats
Displays data packet statistics of both transmitted frame and received frame for the DAP-1353 network.

Log

The log information will include, but not limited to, the following items:

- Upgrade Firmware
- Client associate and disassociate with AP
- Web login If you require



Product Page : DAP-1353 Firmware Version : 2.00

D-Link

DAP-1353 // SETUP ADVANCED MAINTENANCE STATUS SUPPORT

DEVICE INFO
STATISTICS
LOG
CLIENT INFO
LOGOUT

VIEW LOG

View Log displays the activities occurring on the DAP-1353.

LOG FILES

First Page Last Page Previous Next Clear Log Settings

Page 1 of 1

Time	Type	Message
Uptime 0 day 00:00:32	[SYSACT]	Web login success from 192.168.0.100
Uptime 0 day 00:00:22	[Notice]	Ethernet XP0 LINK UP
Uptime 0 day 00:00:16	[Wireless]	Auto channel:Best channel is 6
Uptime 0 day 00:00:11	[Wireless]	Initiate Wireless success
Uptime 0 day 00:00:09	[SYSACT]	AP start with f/w version:2.00

Log Sever: If you require more space to hold your logs, please provide the IP address of the Server that will store your logs. The embedded memory can only have up to 300 logs.

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

Log Type: Check the box for the type of activity you want to log. There are three types: System Activity, Wireless Activity, and Notice.

Mail Server/IP Address: Enter the IP address of the mail server.

Email: Enter mail address that you want send to.

Client Info

The Connected Wireless Client list shows the currently connected wireless clients. This table also displays the MAC address and wireless mode of the connected wireless clients.

Product Page : DAP-1353Firmware Version : 2.00

D-Link

DAP-1353

SETUPADVANCEDMAINTENANCESTATUSSUPPORT

DEVICE INFO

STATISTICS

LOG

CLIENT INFO

LOGOUT

CONNECTED WIRELESS CLIENT LIST

The Wireless Client table below displays Wireless clients Connected to the AP (Access Point).

SSID

Connect Time

MAC Address

Signal

Mode

Helpful Hints..

Client Info

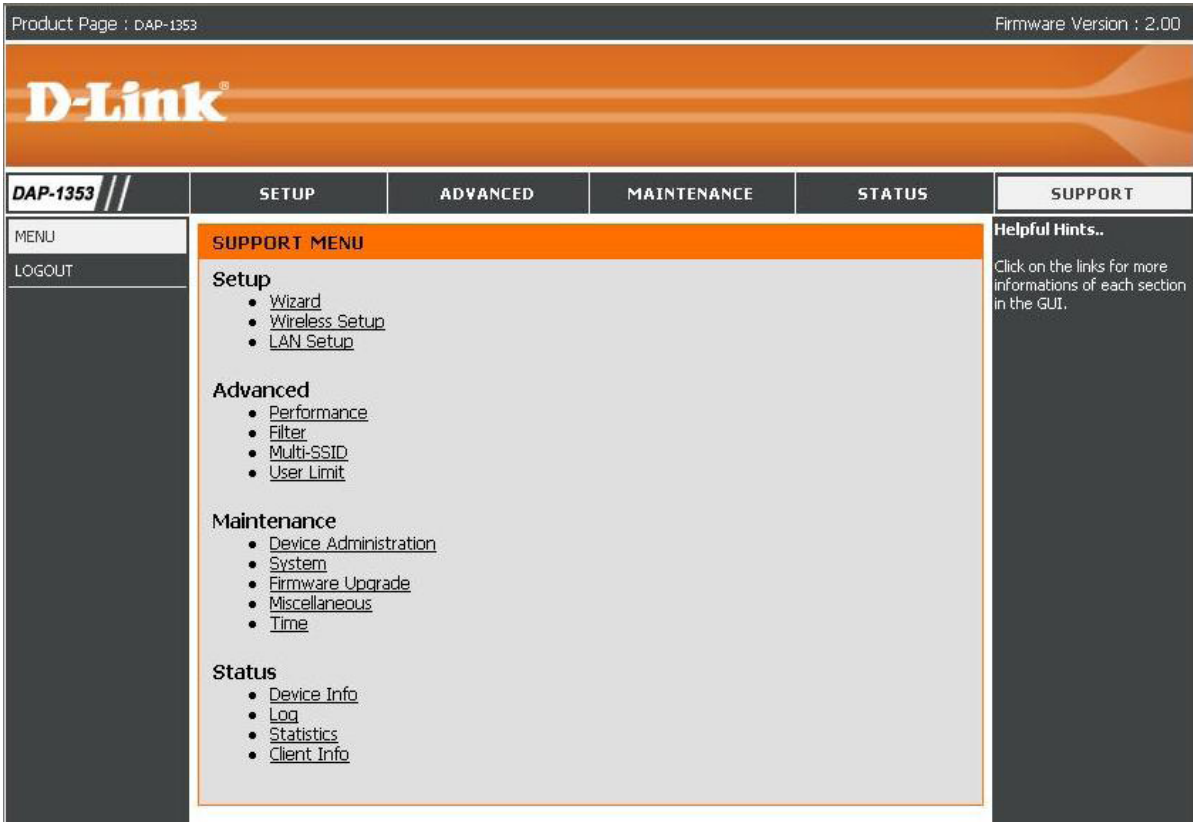
Displays connected client station main parameters, such as Connect Time, station MAC address, signal quality and wireless mode status for better management and monitoring.

D-Link DAP-1353 User Manual

44

Support

The Support page contains an index of links to help topics for each function of the DAP-1353.



Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-1353 offers the following types of security:

- WPA-Personal (Pre-Shared Key)
- WPA2-Personal (Pre-Shared Key 2)
- WPA2-Auto-Personal
- WEP (Wired Equivalent Privacy)
- WPA-Enterprise (Extensible Authentication Protocol)
- WPA2-Enterprise (Extensible Authentication Protocol 2)
- WPA2-Auto-Enterprise (Extensible Authentication Protocol 2 Auto)

What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

Configure WEP

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 (192.168.0.50). Click on **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WEP Security**.
3. Next to *Authentication*, select **Shared Key** or **Open**.
4. Select either **64-bit** or **128-bit** encryption from the drop-down menu next to *WEP Encryption*.
5. Next to *Key Type*, select either **Hex** or **ASCII**.
 Hex (recommended) - Letters A-F and numbers 0-9 are valid.

 ASCII - All numbers and letters are valid.

WIRELESS SECURITY MODE :

Security Mode : Enable WEP Wireless Security (basic)

WEP :

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

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

Authentication : Open

WEP Encryption : 64Bit

Key Type : HEX

Default WEP Key : WEP Key 1

WEP Key 1 : 0000000000

WEP Key 2 : 0000000000

WEP Key 3 : 0000000000

WEP Key 4 : 0000000000

6. Next to *Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.
7. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the access point.

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 router 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-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 (192.168.0.50). Click on **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 **Personal**.
5. Next to *Passphrase*, enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.
6. Enter the passphrase again next to *Confirmed Passphrase*.
7. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-Personal, WPA2-Personal, or WPA2-Auto-Personal 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 has two main sections: 'WIRELESS SECURITY MODE' and 'WPA'. In the 'WIRELESS SECURITY MODE' section, there is a 'Security Mode' dropdown menu currently set to 'Enable WPA Wireless Security (enhanced)'. The 'WPA' section contains a text box stating 'WPA requires stations to use high grade encryption and authentication.' Below this, there are four configuration fields: 'Cipher Type' with a dropdown set to 'Auto', 'Personal / Enterprise' with a dropdown set to 'Personal', 'Passphrase' with an empty text input field, and 'Confirmed Passphrase' with another empty text input field.

Configure WPA (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 (192.168.0.50). Click on **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 **Apply Settings** to save your settings.

The screenshot shows a web-based configuration interface for WPA settings. The top section is titled "WIRELESS SECURITY MODE" and contains a "Security Mode" dropdown menu set to "Enable WPA Wireless Security (enhanced)". Below this is a section titled "WPA" which includes a note: "WPA requires stations to use high grade encryption and authentication." Under the "WPA" section, there are two dropdown menus: "Cipher Type" set to "Auto" and "Personal / Enterprise" set to "Enterprise". Below these are three input fields: "802.1X RADIUS Server IP Address" (empty), "Port" (empty), and "Shared Secret" (empty).

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.

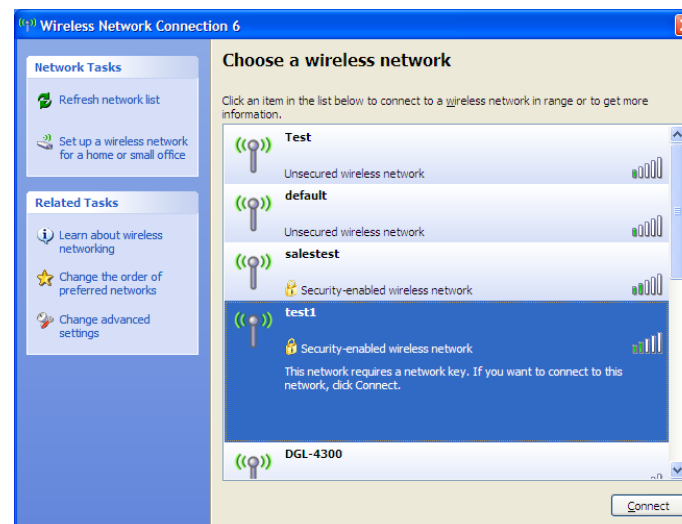
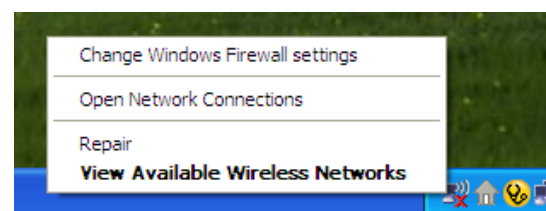
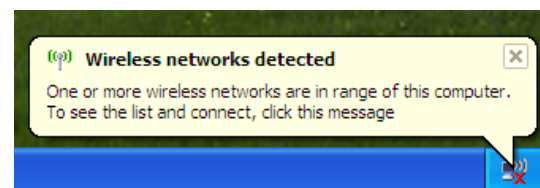
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

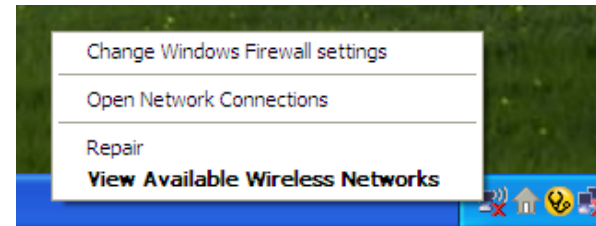
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



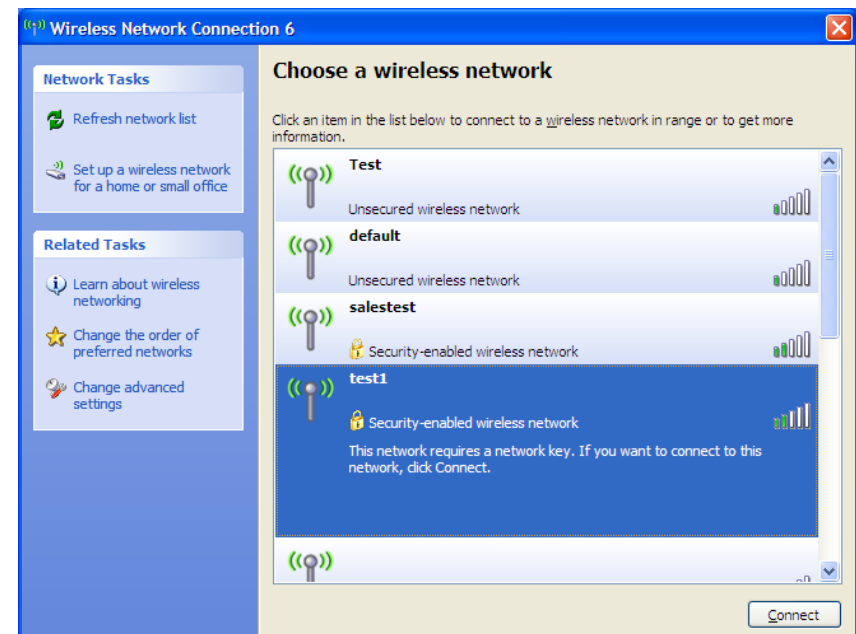
Configure WEP

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

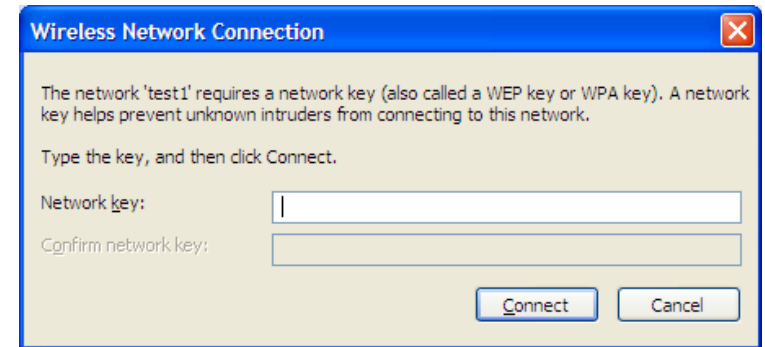


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection box will appear. Enter the same WEP key that is on your access point and click **Connect**.**

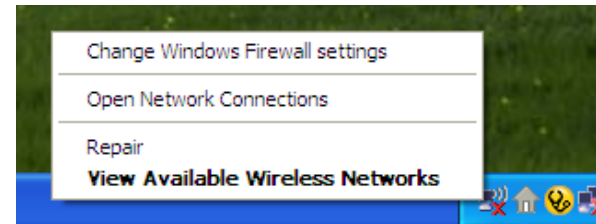
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless access point.



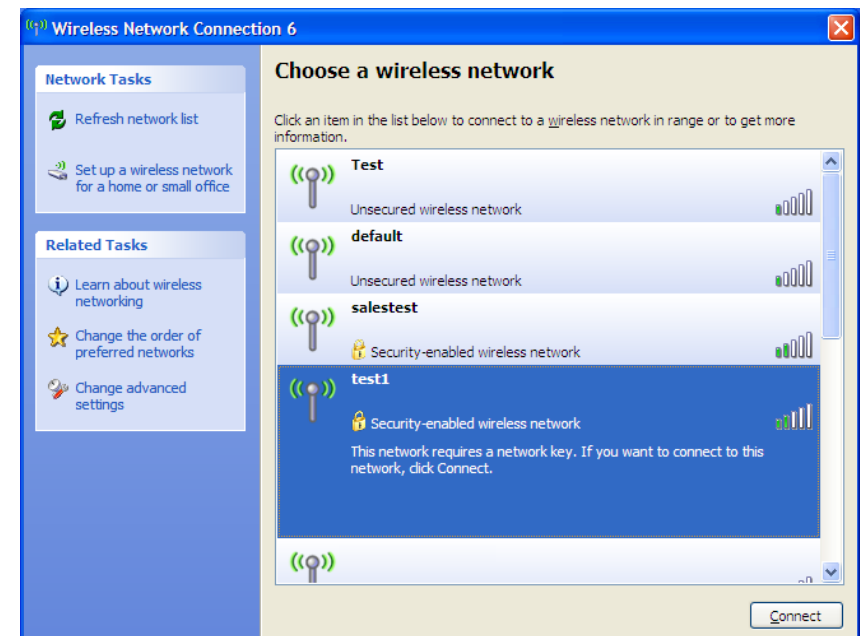
Configure WPA-Personal

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

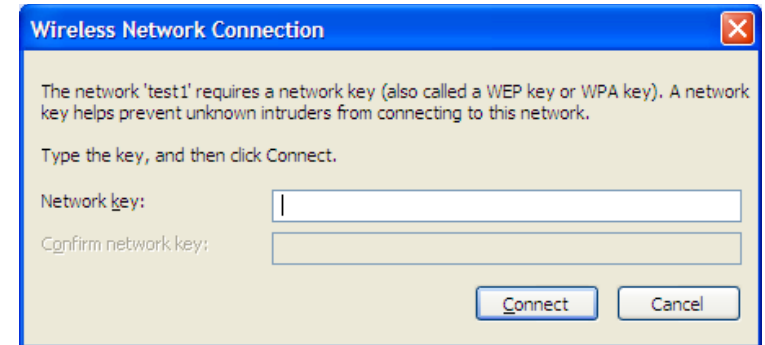


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-Personal 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-Personal settings are correct. The WPA-Personal passphrase must be exactly the same as on the wireless access point.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-1353. 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 (192.168.0.50 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 6.0 or higher
 - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® 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.

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point, 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, at home and in the office.

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your Access Point

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

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This will significantly reduce any interference that the appliances might cause if operating 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 router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer.

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

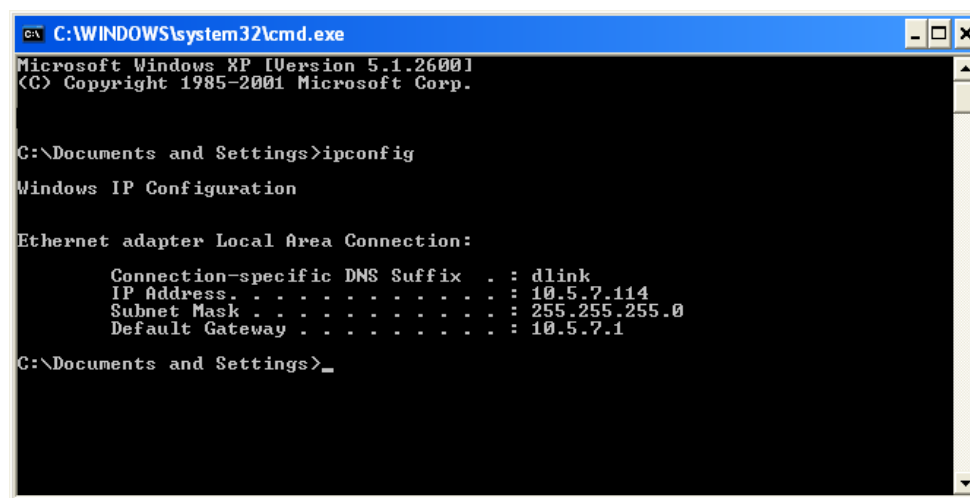
After you install your network adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>
```

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

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® 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

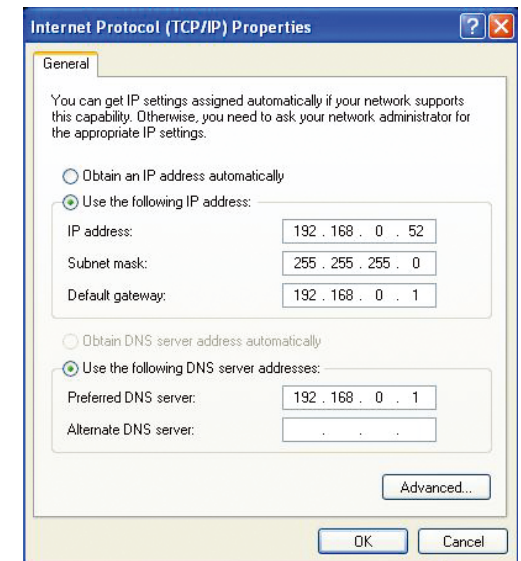
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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 (draft)
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

- 104Mbps (216)
- 66Mbps (135)
- 52Mbps (108)
- 26Mbps (54)
- 12Mbps (27)
- 78Mbps (162)
- 58.5Mbps (121.5)
- 39Mbps (81)
- 19.5Mbps (40.5)
- 6.5Mbps (13.5)

Operation Modes

- Access Point
- WDS with AP
- WDS
- AP Repeater
- AP Client

Frequency Range

2.4GHz to 2.483GHz

Transmitter Output Power

15dBm \pm 2dB

External Antenna Type

Three (3) detachable reverse SMA Antennas

Security

- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise
- 64/128-bit WEP
- MAC address filtering
- 8 SSID for network segmentation
- SSID broadcast disable function
- 802.1Q VLAN Tagging

LEDs

- Power
- WLAN
- Status
- LAN (10/100)

Operating Temperature

32°F to 131°F (0°C to 55°C)

Humidity

95% maximum (non-condensing)

QoS & Performance Enhancement

- WMM (Wi-Fi Multimedia) certified
- User Limit

Safety & Emissions

- FCC
- CE
- C-Tick
- IC
- CSA

Wireless Signal Rates*

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

Dimensions

- L = 7.8 inches
- W = 4.72 inches
- H = 1.26 inches

MSC (0-15)

- 130Mbps (270)
- 117Mbps (243)

Warranty

1 Year

* Maximum wireless signal rate derived from IEEE Standard 802.11g and Draft 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 factors will adversely affect wireless signal range.



Version 2.1
Sep. 19, 2008