

# Statistics

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-825 on both the Internet, LAN ports and both the 802.11n/g (2.4GHz) and 802.11n/a (5GHz) wireless bands. The traffic counter will reset if the device is rebooted.

The screenshot shows the D-Link DIR-825 web interface. At the top, there is a navigation bar with tabs for SETUP, ADVANCED, TOOLS, and STATUS. Below this is a header with the D-Link logo and the model number DIR-825. The main content area is titled 'TRAFFIC STATISTICS' and contains a sub-header 'Traffic Statistics display receive and transmit packets passing through your router.' Below this are two buttons: 'Refresh Statistics' and 'Clear Statistics'. The statistics are presented in three main sections: LAN, WAN, and WIRELESS. Each section has a sub-header and a table of statistics. The LAN section shows 3728 sent packets, 1 dropped, and 0 collisions. The WAN section shows 0 sent and 0 dropped packets. The WIRELESS section is split into two bands: 2.4GHz and 5GHz, both showing 0 sent and 0 dropped packets. A 'Helpful Hints...' section at the bottom provides a summary of packets and a link to 'More...'. The footer of the page contains the word 'WIRELESS'.

SECTION	TX Packets Dropped	TX Packets Sent	RX Packets Dropped	RX Packets Received	Collisions	Errors
LAN STATISTICS	1	3728	0	4707	0	0
WAN STATISTICS	0	0	0	0	0	0
WIRELESS STATISTICS — 2.4GHZ BAND	0	2025	0	0	0	0
WIRELESS STATISTICS — 5GHZ BAND	0	962	0	0	0	0

## Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

**D-Link**

**DIR-825** // **SETUP** **ADVANCED** **TOOLS** **STATUS** **SUPPORT**

**INTERNET SESSIONS**

This page displays the full details of active internet sessions to your router.

**Local** **NAT** **Internet** **Protocol** **State** **Dir** **Priority** **Time Out**

**Helpful Hints...**

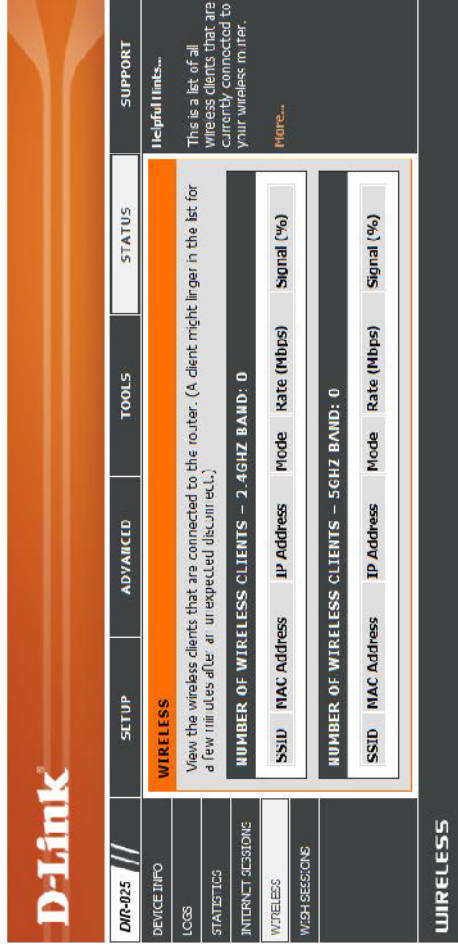
This is a list of all active conversations between WAN computers and LAN computers.

[More...](#)

**WIRELESS**

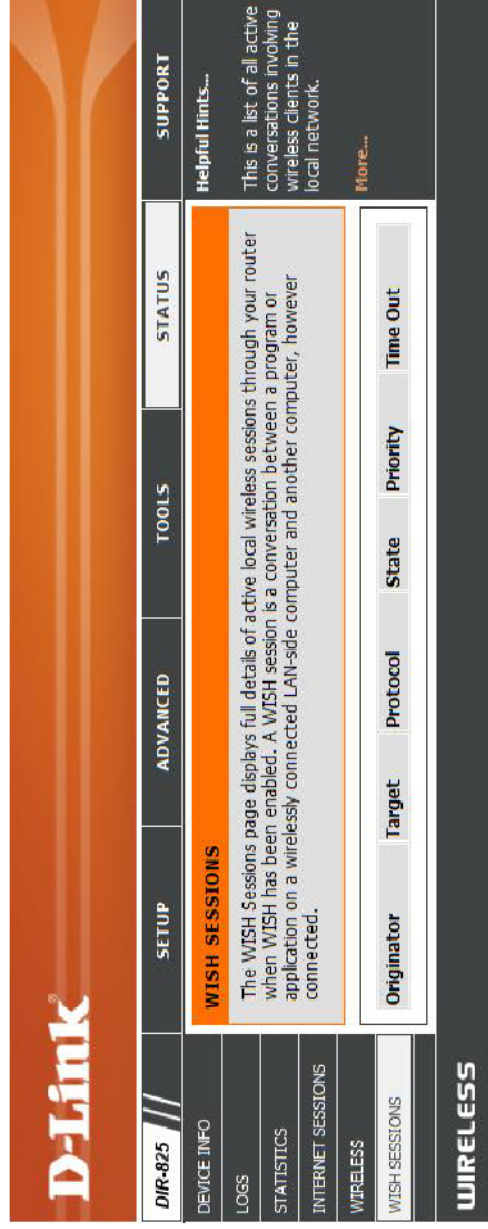
# Wireless

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.



# WISH

The WISH details page displays full details of wireless clients that are connected when WISH is enabled.



# Support

The screenshot displays the D-Link DIR-825 web interface. At the top left is the D-Link logo. Below it is a navigation bar with tabs for MENU, SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The SUPPORT tab is active. The main content area is titled 'SUPPORT MENU' and contains a list of links: Setup, Advanced, Tools, and Status. Below this is a 'SETUP HELP' section with links for Internet Connection, WAN, Wireless, and Network Settings. An 'ADVANCED HELP' section follows with a comprehensive list of links including Virtual Server, Port Forwarding, Application Rules, QoS Engine, Access Control, WebSite Filter, Network Filter, Firewall Settings, Routing, Inbound Filter, Advanced Wireless, WAN, WPA Protected Setup, Advanced Network, and Guest Zone. The 'TOOLS HELP' section includes Admin, Time, SPI, SRA, Email Alerts, System, Firmware, Dynamic DNS, and System Check. Finally, the 'STATUS HELP' section contains Device Info, Wireless, Routing, Logs, Statistics, and Active Sessions. A 'WIRELESS' section is visible at the bottom of the page.

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-825 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:

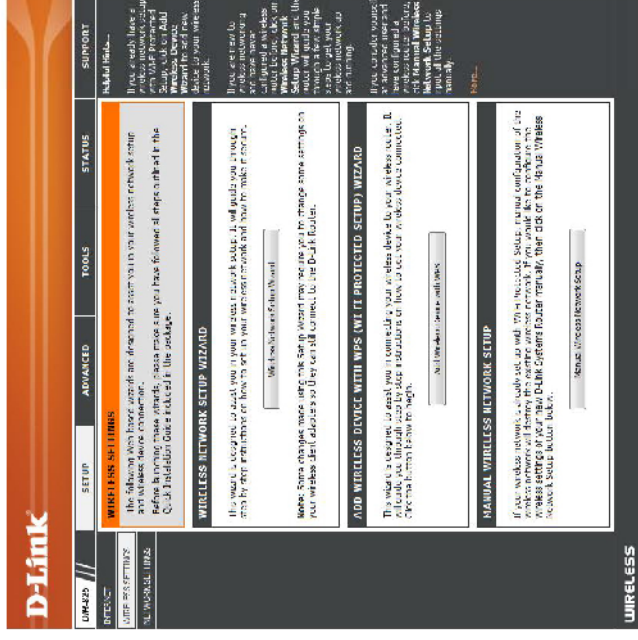
- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead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

# Wireless Security Setup Wizard

To run the security wizard, click on Setup at the top and then click **Launch Wireless Security Setup Wizard**.

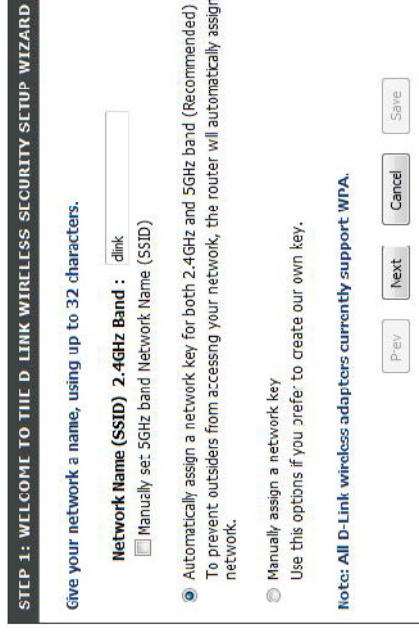


Check the **Manually set 5GHz band Network Name...** box to manually set your desired wireless network name for the 5GHz band.

Type your desired wireless network name (SSID).

**Automatically:** Select this option to automatically generate the router's network key and click **Next**.

**Manually:** Select this option to manually enter your network key and click **Next**.



If you selected **Automatically**, the summary window will display your settings. Write down the security key and enter this on your wireless clients. Click **Save** to save your settings.

**SETUP COMPLETE!**

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.

<p><b>Wireless Band :</b> 2.4GHz Band</p> <p><b>Wireless Network Name (SSID) :</b> <code>dhlink</code></p> <p><b>Security Mode 2 :</b> A-JT0 (WPA or WPA2) - Personal</p> <p><b>Cipher Type :</b> TKIP and AES</p> <p><b>Pre-Shared Key :</b> <code>6170664e26597e2688303d564535868514c771635855a470460215598d06c</code></p>
<p><b>Wireless Band :</b> 5GHz Band</p> <p><b>Wireless Network Name (SSID) :</b> <code>dhlink_meha</code></p> <p><b>Security Mode 2 :</b> A-JT0 (WPA or WPA2) - Personal</p> <p><b>Cipher Type :</b> TKIP and AES</p> <p><b>Pre-Shared Key :</b> <code>6170664e26597e2688303d564535868514c771635855a470460215598d06c</code></p>

If you selected **Manually**, the following screen will appear.

**STEP 2: SET YOUR WIRELESS SECURITY PASSWORD**

You have selected your security level - you will need to set a wireless security password.

The WPA (Wi-Fi Protected Access) key must meet one of following guidelines:

- Between 8 and 64 characters (A longer WPA key is more secure than a short one)
- Exactly 64 characters using 0-9 and A-F

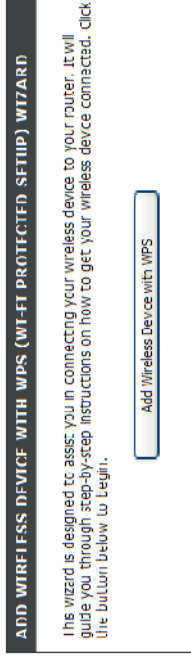
Use the same Wireless Security Password on both 2.4GHz and 5GHz band

**2-4GHz Band Wireless Security Password :**

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

## Add Wireless Device with WPS Wizard

From the **Setup** > **Wireless Settings** screen, click **Add Wireless Device with WPS**.



Select **Auto** to add a wireless client using WPS (Wi-Fi Protected Setup). Once you select **Auto** and click **Connect**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

If you select **Manual**, a settings summary screen will appear. Write down the security key and enter this on your wireless clients.



**PIN:** Select this option to use PIN method. In order to use this method you must know the wireless client's 8 digit PIN and click **Connect**.

**PBC:** Select this option to use PBC (Push Button) method to add a wireless client. Click **Connect**.





# Configure WPA-Personal (PSK)

It is recommended to enable encryption on your wireless router 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 router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to **Security Mode**, select **WPA-Personal**.
3. Next to **WPA Mode**, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to **Cypher Type**, select **TKIP and AES**, **TKIP**, or **AES**.
5. Next to **Group Key Update Interval**, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

**WIRELESS SECURITY MODE**

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal

**WPA**

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

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

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

**PRE-SHARED KEY**

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

Pre-Shared Key : .....

7. Click **Save Settings** to save your settings. If you are configuring the router 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 router.

# Configure WPA-Enterprise (RADIUS)

It is recommended to enable encryption on your wireless router 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 router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to **Security Mode**, select **WPA-Enterprise**.
3. Next to **WPA Mode**, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to **Cypher Type**, select **TKIP and AES**, **TKIP**, or **AES**.
5. Next to **Group Key Update Interval**, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
6. Next to **Authentication Timeout**, enter the amount of time before a client is required to re-authenticate (60 minutes is default).
7. Next to **RADIUS Server IP Address** enter the IP Address of your RADIUS server.

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. This device supports two wireless security modes including WPA-Personal and WPA-Enterprise. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Enterprise

---

WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA** or **WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The stronger higher than the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode : Auto (WPA or WPA2)

Cypher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

---

EAP (802.1X)

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

Authentication Timeout : 60 (minutes)

RADIUS server IP Address : 0.0.0.0

RADIUS server Port : 812

RADIUS server shared secret : radius\_shared

MAC Address Authentication :

[Advanced >>](#)