D-Link®
Building Networks for People
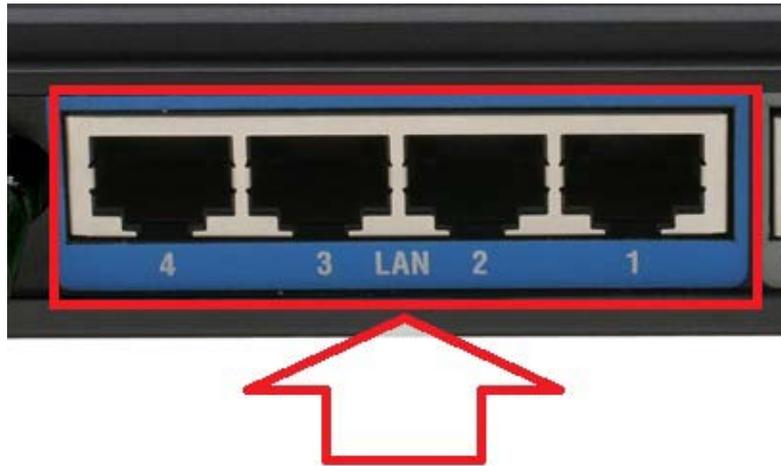
WIRELESS G

Applying WPA-PSK Encryption

This document will detail how to setup WPA-PSK Encryption on the DIR-600.

WPA-PSK is now considered to be the standard with encrypting a wireless network, it is far more secure then WEP and is therefore recommended.

1. First you will need a computer/laptop to be connected to one of the LAN Ethernet ports.

NOTE: If you are going to change your Wireless Encryption, DO NOT perform this over a Wireless connection, connect your computer/laptop to a LAN Port.

2. Proceed to open an Internet Browser and login to the DIR-600 Web Configuration.

NOTE: Instructions are on the Technical Support Knowledge Base if you are unsure on how to login to the Web Configuration.

3. Click on SETUP > Wireless Setup > Manual Wireless Connection Setup button.

4. Once you have access to the Wireless Setup page, there are only a couple of adjustments needed to be made, please see below:

It is recommended to change the Wireless Network Name (SSID) to a name of your liking, in this example it is called "home_network". Enable Auto Channel Selection can be enabled however it is not mandatory. The Wireless Channel can be changed, Channel's 1, 6 and 11 are non overlapping and are recommended.

Under the WIRELESS SECURITY MODE heading select from the dropdown "Enable WPA Only Wireless Security (enhanced)".

Under the WPA ONLY heading the Cipher Type and PSK/EAP settings are recommended on their default setting. The Network Key is where you type in a password for your Wireless, it can be alphanumeric and a minimum of 8 characters. The Network Key is considered to be your Wireless Password. REMEMBER IT!

5. Now proceed to click on the Save Settings button.

6. WPA-PSK Encryption is now configured.

IMPORTANT:

If you decide to change your Wireless Encryption password, you will need to remove your existing Wireless Profile or edit it to reflect the new changes.

Please remember to ensure your DIR-600 has the most current firmware version applied. To apply this firmware please refer to the Technical Support Knowledge Base.