

# USER MANUAL

DIR-625

VERSION 3.0



**D-Link**<sup>®</sup>

**WIRELESS**

# Table of Contents

<b>Product Overview .....</b>	<b>4</b>	DHCP Server Settings .....	31
Package Contents.....	4	DHCP Reservation .....	32
System Requirements .....	4	Virtual Server .....	34
Introduction.....	5	Port Forwarding .....	36
Features.....	6	Application Rules .....	37
Hardware Overview .....	7	QoS Engine .....	38
Connections .....	7	Network Filters .....	39
LEDs .....	8	Access Control.....	40
<b>Installation.....</b>	<b>9</b>	Access Control Wizard .....	40
Before you Begin .....	9	Website Filters .....	43
Wireless Installation Considerations.....	10	Inbound Filters .....	44
Connect to Cable/DSL/Satellite Modem .....	11	Firewall Settings.....	45
Connect to Another Router .....	12	Application Level Gateway (ALG)	
Getting Started .....	14	Configuration.....	46
<b>Configuration .....</b>	<b>15</b>	VPN Passthrough.....	46
Web-based Configuration Utility .....	15	RTSP .....	46
Setup Wizard .....	16	H.323.....	46
Manual Configuration.....	20	SIP (VoIP).....	46
Dynamic (Cable).....	20	MMS.....	46
PPPoE (DSL) .....	21	Advanced Wireless Settings .....	47
PPTP .....	22	WISH .....	48
L2TP .....	24	Wi-Fi Protected Setup.....	50
Static (assigned by ISP) .....	26	Advanced Network Settings.....	52
Big Pond.....	27	UPnP .....	52
Wireless Settings .....	28	Internet Ping Block .....	52
Network Settings.....	30	Internet Port Speed.....	52

Multicast Streams.....	52	Configure WEP .....	80
Administrator Settings.....	53	Configure WPA-PSK .....	82
Change Password .....	53	<b>Troubleshooting.....</b>	<b>84</b>
Remote Management.....	53	<b>Wireless Basics .....</b>	<b>88</b>
Time Settings.....	54	What is Wireless? .....	89
SysLog.....	55	Tips.....	91
Email Settings.....	56	Wireless Modes .....	92
System Settings.....	57	<b>Networking Basics .....</b>	<b>93</b>
Update Firmware .....	58	Check your IP address .....	93
DDNS.....	59	Statically Assign an IP address .....	94
System Check.....	60	<b>Technical Specifications.....</b>	<b>95</b>
Schedules .....	61	<b>Contacting Technical Support.....</b>	<b>96</b>
Device Information.....	62	<b>Warranty .....</b>	<b>97</b>
Log.....	63	<b>Registration.....</b>	<b>103</b>
Stats.....	64		
Internet Sessions.....	65		
Wireless .....	67		
WISH Sessions.....	68		
Support.....	69		
<b>Wireless Security.....</b>	<b>70</b>		
What is WEP?.....	70		
What is WPA? .....	71		
Wireless Security Setup Wizard .....	72		
Configure WEP .....	75		
Configure WPA-Personal (PSK).....	76		
Configure WPA-Enterprise (RADIUS).....	77		
<b>Connect to a Wireless Network .....</b>	<b>79</b>		
Using Windows® XP .....	79		

# Package Contents

- D-Link DIR-625 RangeBooster N™ Router
- 2 Detachable Antennas
- Power Adapter
- CAT5 Ethernet Cable
- CD-ROM with Installation Wizard, User Manual, and Special Offers



**Note:** Using a power supply with a different voltage rating than the one included with the DIR-625 will cause damage and void the warranty for this product.

# System Requirements

- Ethernet-based Cable or DSL Modem
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0, Mozilla 1.7.12 (5.0), or Firefox 1.5 and above (for configuration)
- Installation Wizard requires Windows® XP with Service Pack 2

# Introduction

## **TOTAL PERFORMANCE**

Combines award winning router features and Draft 802.11n wireless technology to provide the best wireless performance

## **TOTAL SECURITY**

The most complete set of security features including Active Firewall and WPA2 to protect your network against outside intruders

## **TOTAL COVERAGE**

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

## **ULTIMATE PERFORMANCE**

The D-Link RangeBooster N™ Router (DIR-625) 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 throughout your home. Connect the RangeBooster N™ Router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this Router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

## **EXTENDED WHOLE HOME COVERAGE**

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

## **TOTAL NETWORK SECURITY**

The RangeBooster N™ Router supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA and WEP standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this RangeBooster N™ Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

\* 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.

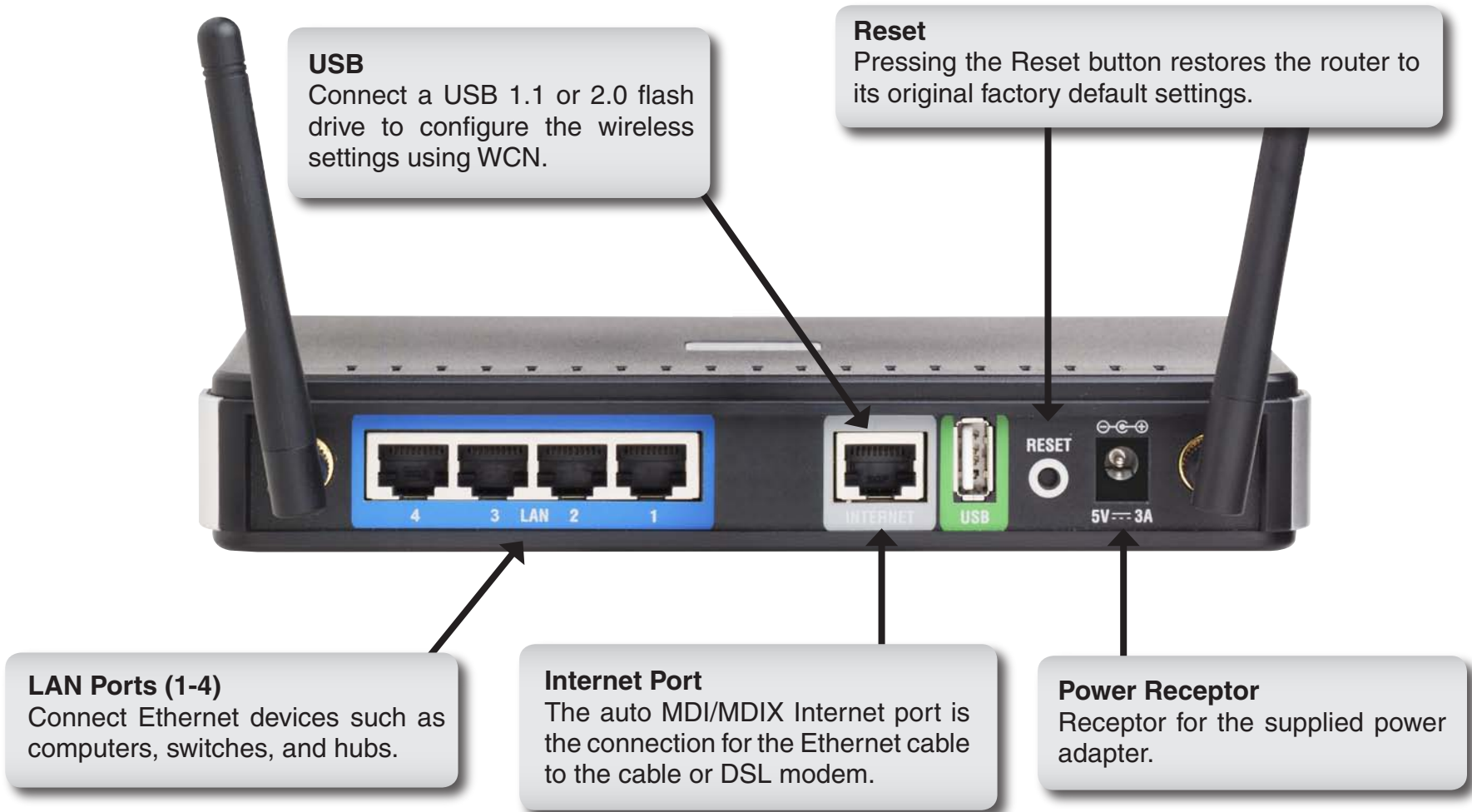
# Features

- **Faster Wireless Networking** - The DIR-625 provides up to 300Mbps\* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11n wireless router gives you the freedom of wireless networking at speeds 650% faster than 802.11g.
- **Compatible with 802.11b and 802.11g Devices** - The DIR-625 is still fully compatible with the IEEE 802.11b standard, so it can connect with existing 802.11b PCI, USB and Cardbus adapters.
- **Advanced Firewall Features** - The Web-based user interface displays a number of advanced network management features including:
  - **Content Filtering** - Easily applied content filtering based on MAC Address, URL, and/or Domain Name.
  - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.
  - **Secure Multiple/Concurrent Sessions** - The DIR-625 can pass through VPN sessions. It supports multiple and concurrent IPsec and PPTP sessions, so users behind the DIR-625 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-625 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 router 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.

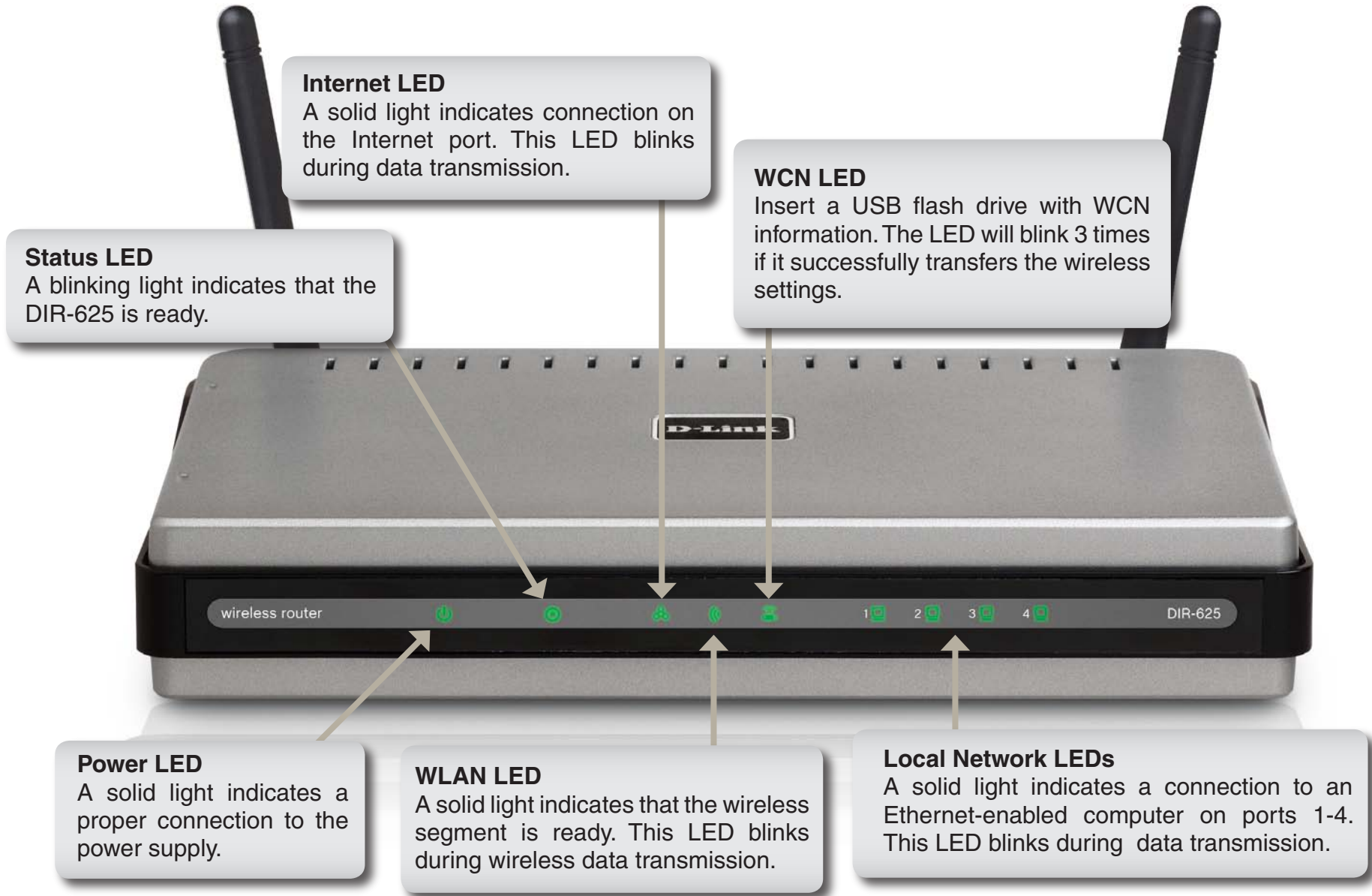
# Hardware Overview

## Connections



# Hardware Overview

## LEDs





# Installation

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

## Before you Begin

Please configure the router with the computer that was last connected directly to your modem. Also, you can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).

If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.

# Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link router 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.

# Connect to Cable/DSL/Satellite Modem

If you are connecting the router to a cable/DSL/satellite modem, please follow the steps below:

1. Place the router in an open and central location. Do not plug the power adapter into the router.
2. Turn the power off on your modem. If there is no on/off switch, then unplug the modem's power adapter. Shut down your computer.
3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.
4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.
5. Turn on or plug in your modem. Wait for the modem to boot (about 30 seconds).
6. Plug the power adapter to the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot.
7. Turn on your computer.
8. Verify the link lights on the router. The power light, Internet light, and the LAN light (the port that your computer is plugged into) should be lit. If not, make sure your computer, modem, and router are powered on and verify the cable connections are correct.
9. Skip to page 15 to configure your router.

# Connect to Another Router

If you are connecting the D-Link router to another router to use as a wireless access point and/or switch, you will have to do the following before connecting the router to your network:

- Disable UPnP™
- Disable DHCP
- Change the LAN IP address to an available address on your network. The LAN ports on the router cannot accept a DHCP address from your other router.

To connect to another router, please follow the steps below:

1. Plug the power into the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). Please see the **Networking Basics** section for more information. If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.
2. Open a web browser and enter **http://192.168.0.1** and press **Enter**. When the login window appears, set the user name to **Admin** and leave the password box empty. Click **Log In** to continue.
3. Click on **Advanced** and then click **Advanced Network**. Uncheck the Enable UPnP checkbox. Click **Save Settings** to continue.
4. Click **Setup** and then click **Network Settings**. Uncheck the Enable DHCP Server server checkbox. Click **Save Settings** to continue.
5. Under Router Settings, enter an available IP address and the subnet mask of your network. Click **Save Settings** to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 1.

6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.
7. Connect an Ethernet cable in one of the LAN ports of the router and connect it to your other router. Do not plug anything into the Internet port of the D-Link router.
8. You may now use the other 3 LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the **Configuration** and **Wireless Security** sections for more information on setting up your wireless network.

# Getting Started

The DIR-625 includes a Quick Router Setup Wizard CD. Follow the simple steps below to run the Setup Wizard to guide you quickly through the installation process.

Insert the **Quick Router Setup Wizard CD** in the CD-ROM drive. The step-by-step instructions that follow are shown in Windows XP. The steps and screens are similar for the other Windows operating systems.

If the CD Autorun function does not automatically start on your computer, go to **Start > Run**. In the run box type "**D:\DIR625.exe**" (where **D:** represents the drive letter of your CD-ROM drive).

When the autorun screen appears, click **Install Router**.

Click **Install Router**



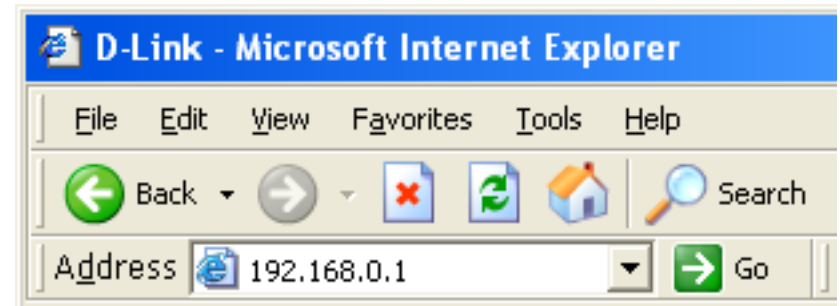
**Note:** It is recommended to write down the login password on the provided CD holder.

# Configuration

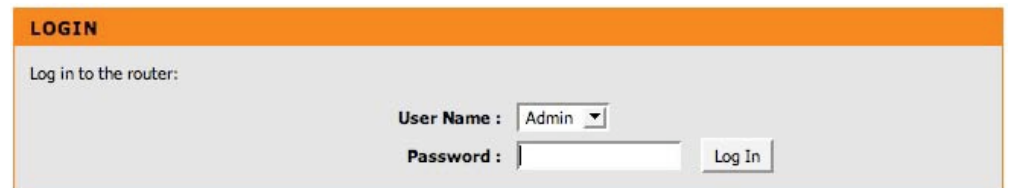
This section will show you how to configure your new D-Link wireless router using the web-based configuration utility.

## Web-based Configuration Utility

To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.0.1).



Select **Admin** from the drop-down menu and then enter your password. Leave the password blank by default.

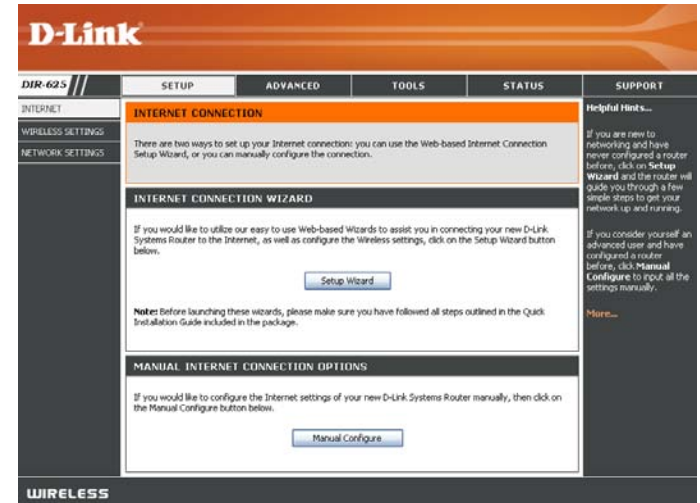


If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.

# Setup Wizard

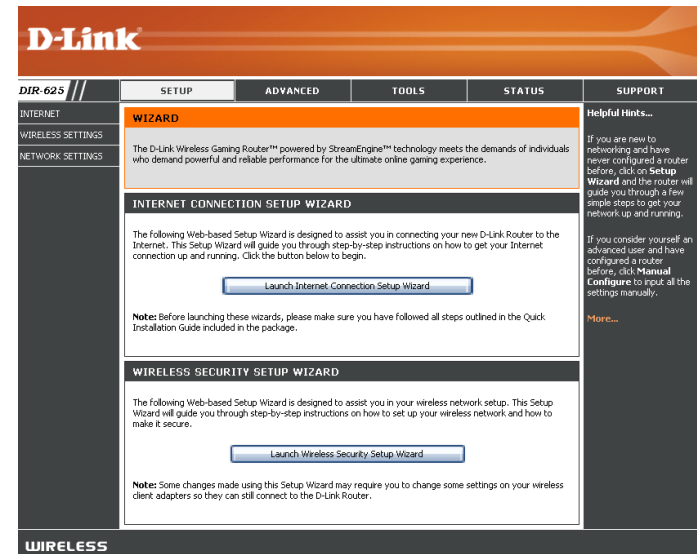
You may click **Setup Wizard** to quickly configure your router.

If you want to enter your settings without running the wizard, click **Manual Configuration** and skip to page 20.



Click **Launch Internet Connection Setup Wizard** to begin.

If you want to configure your wireless settings, click **Launch Wireless Security Setup Wizard** and skip to page 63.



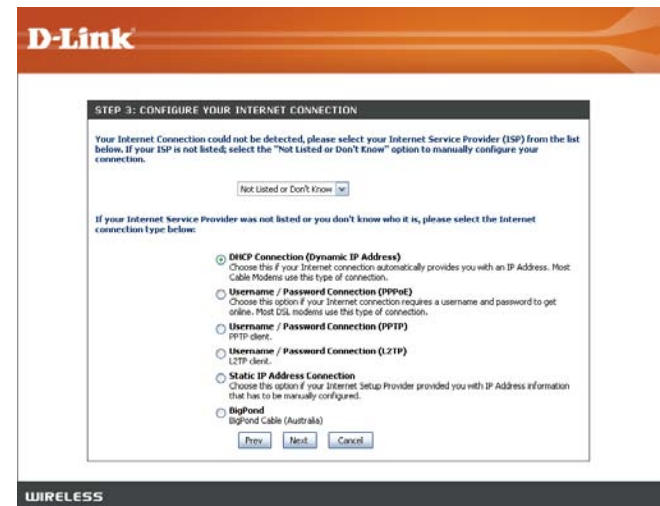
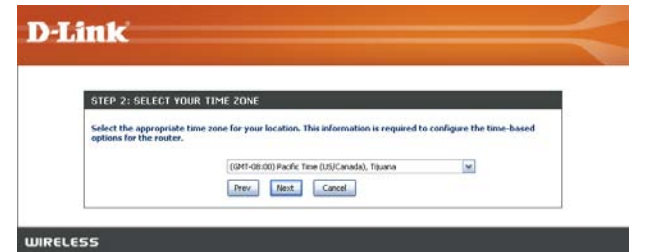
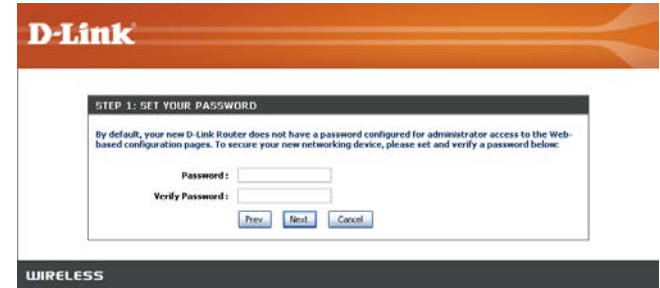
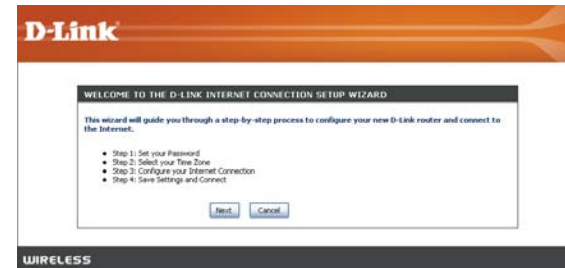


Click **Next** to continue.

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

Select your time zone from the drop-down menu and then click **Next** to continue.

Select the type of Internet connection you use and then click **Next** to continue.



If you selected Dynamic, you may need to enter the MAC address of the computer that was last connected directly to your modem. If you are currently using that computer, click **Clone Your PC's MAC Address** and then click **Next** to continue.

The Host Name is optional but may be required by some ISPs. The default host name is the device name of the Router and may be changed.

If you selected PPPoE, enter your PPPoE username and password. Click **Next** to continue.

Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

**Note:** Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.

If you selected PPTP, enter your PPTP username and password. Click **Next** to continue.

**D-Link**

**DHCP CONNECTION (DYNAMIC IP ADDRESS)**

To set up this connection, please make sure that you are connected to the D-Link Router with the PC that was originally connected to your broadband connection. If you are, then click the Clone MAC button to copy your computer's MAC Address to the D-Link Router.

MAC Address: 00:00:56:28:22:88 (optional)

Host Name:

Note: You may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

**WIRELESS**

**D-Link**

**SET USERNAME AND PASSWORD CONNECTION (PPPOE)**

To set up this connection you will need to have a Username and Password from your Internet Service Provider. If you do not have this information, please contact your ISP.

Address Mode:  Dynamic IP  Static IP

IP Address: 0.0.0.0

User Name:

Password: \*\*\*\*\*

Verify Password: \*\*\*\*\*

Service Name:  (optional)

Note: You may also need to provide a Service Name. If you do not have or know this information, please contact your ISP.

**WIRELESS**

**D-Link**

**SET USERNAME AND PASSWORD CONNECTION (PPTP)**

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.

Address Mode:  Dynamic IP  Static IP

PPTP IP Address: 0.0.0.0

PPTP Subnet Mask: 255.255.255.0

PPTP Gateway IP Address: 0.0.0.0

PPTP Server IP Address (may be same as gateway): 0.0.0.0

User Name:

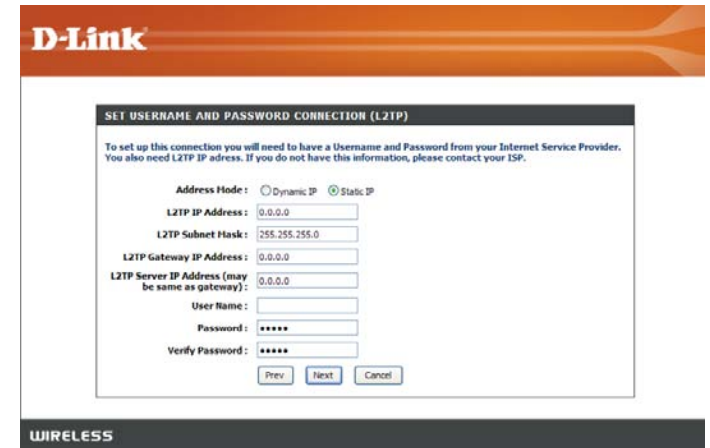
Password: \*\*\*\*\*

Verify Password: \*\*\*\*\*

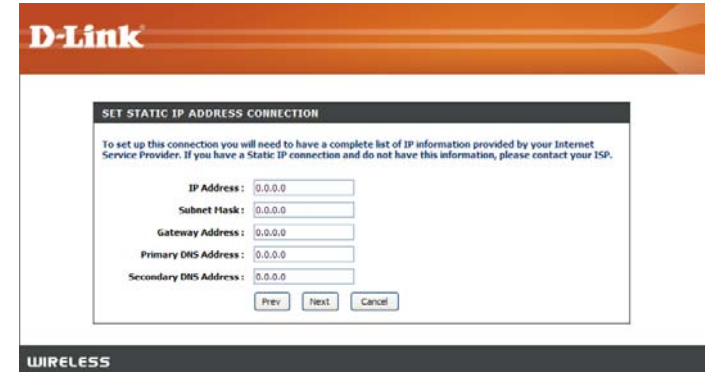
Note: You also need PPTP IP address. If you do not have this information, please contact your ISP.

**WIRELESS**

If you selected L2TP, enter your L2TP username and password. Click **Next** to continue.

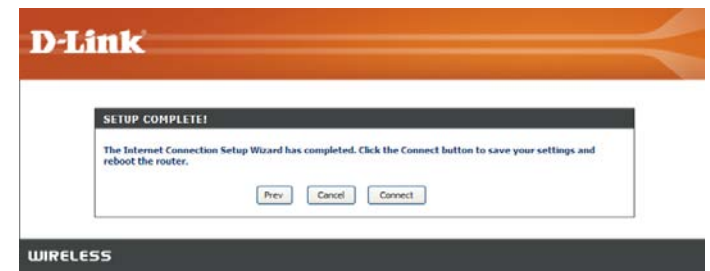


If you selected Static, enter your network settings supplied by your Internet provider. Click **Next** to continue.



Click **Connect** to save your settings. Once the router is finished rebooting, click **Continue**. Please allow 1-2 minutes to connect.

Close your browser window and reopen it to test your Internet connection. It may take a few tries to initially connect to the Internet.



# Manual Configuration

## Dynamic (Cable)

**My Internet Connection:** Select **Dynamic IP (DHCP)** to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services.

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

**Use Unicasting:** Check the box if you are having problems obtaining an IP address from your ISP.

**DNS Addresses:** Enter the Primary DNS server IP address assigned by your ISP.

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

**D-Link**

DIR-625 //

SETUP    ADVANCED    TOOLS    STATUS    SUPPORT

INTERNET  
WIRELESS SETTINGS  
NETWORK SETTINGS

**WAN**

**Internet Connection**

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are unsure of your connection method, please contact your Internet Service Provider.

**Note:** If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Save Settings    Don't Save Settings

**INTERNET CONNECTION TYPE**

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : Dynamic IP (DHCP)

**DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :**

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Use Unicasting :  (compatibility for some DHCP Servers)

Primary DNS Server :

Secondary DNS Server :

MTU :  (bytes)    MTU default = 1500

MAC Address :

Clone Your PC's MAC Address

**WIRELESS**

**Helpful Hints...**

When configuring the router to access the Internet, be sure to choose the correct **Internet Connection Type** from the drop down menu. If you are unsure of which option to choose, contact your **Internet Service Provider (ISP)**.

If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.

More...

# Internet Setup

## PPPoE (DSL)

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

**My Internet Connection:** Select **PPPoE (Username/Password)** from the drop-down menu.

**Address Mode:** Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

**IP Address:** Enter the IP address (Static PPPoE only).

**User Name:** Enter your PPPoE user name.

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

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

**Reconnection Mode:** Select either **Always-on**, **On-Demand**, or **Manual**.

**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

**DNS Addresses:** Enter the Primary and Secondary DNS Server Addresses (Static PPPoE only).

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

The screenshot shows the D-Link router's web interface for configuring the Internet connection. The page is titled "Internet Setup" and is for a "DIR-625" router. The "WAN" tab is selected, and the "Internet Connection" section is active. The "Internet Connection Type" is set to "PPPoE (Username / Password)". The "PPPoE INTERNET CONNECTION TYPE" section is expanded, showing fields for "Address Mode" (Dynamic IP selected), "IP Address", "Username", "Password", "Verify Password", "Service Name", "Reconnect Mode" (Always on selected), "Maximum Idle Time" (20 minutes), "Primary DNS Server", "Secondary DNS Server", "MTU" (1492 bytes), and "MAC Address". A "Clone Your PC's MAC Address" button is visible at the bottom of the form. The page also includes a "Helpful Hints" sidebar on the right and a "WIRELESS" section at the bottom.

# Internet Setup

## PPTP

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

**Address Mode:** Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

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

**PPTP Subnet Mask:** Enter the Primary and Secondary DNS Server Addresses (Static PPTP only).

**PPTP Gateway:** Enter the Gateway IP Address provided by your ISP.

**PPTP Server IP:** Enter the Server IP provided by your ISP (optional).

**Username:** Enter your PPTP username.

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

**Reconnect Mode:** Select either **Always-on**, **On-Demand**, or **Manual**.

**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

**DNS Servers:** The DNS server information will be supplied by your ISP (Internet Service Provider.)

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET WIRELESS SETTINGS NETWORK SETTINGS

**WAN**

**Internet Connection**

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are unsure of your connection method, please contact your Internet Service Provider.

**Note:** If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Save Settings Don't Save Settings

**INTERNET CONNECTION TYPE**

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is: PPTP (Username / Password)

**PPTP INTERNET CONNECTION TYPE :**

Enter the information provided by your Internet Service Provider (ISP).

Address Mode:  Dynamic IP  Static IP

PPTP IP Address: 0.0.0.0

PPTP Subnet Mask: 255.255.255.0

PPTP Gateway IP Address: 0.0.0.0

PPTP Server IP Address: 0.0.0.0

Username: \_\_\_\_\_

Password: •••••

Verify Password: •••••

Reconnect Mode:  Always on  On demand  Manual

Maximum Idle Time: 20 (minutes, 0=infinite)

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

MTU: 1400 (bytes) MTU default = 1400

MAC Address: 00:00:00:00:00:00

Clone Your PC's MAC Address

Helpful Hints...  
When configuring the router to access the Internet, be sure to choose the correct **Internet Connection Type** from the drop down menu. If you are unsure of which option to choose, contact your **Internet Service Provider (ISP)**.  
If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.  
More...

WIRELESS

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

# Internet Setup

## L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

**Address Mode:** Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

**L2TP IP Address:** Enter the L2TP IP address supplied by your ISP (Static only).

**L2TP Subnet Mask:** Enter the Subnet Mask supplied by your ISP (Static only).

**L2TP Gateway:** Enter the Gateway IP Address provided by your ISP.

**L2TP Server IP:** Enter the Server IP provided by your ISP (optional).

**Username:** Enter your L2TP username.

**Password:** Enter your L2TP password and then retype the password in the next box.

**Reconnect Mode:** Select either **Always-on**, **On-Demand**, or **Manual**.

**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

**DNS Servers:** Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

The screenshot shows the D-Link DIR-625 router's web interface for configuring L2TP. The main heading is "WAN" under "Internet Connection". Below this, there is a section for "INTERNET CONNECTION TYPE" where "L2TP (Username / Password)" is selected. The "L2TP INTERNET CONNECTION TYPE" section contains the following fields:

- Address Mode:** Radio buttons for "Dynamic IP" and "Static IP" (selected).
- L2TP IP Address:** Text input field.
- L2TP Subnet Mask:** Text input field.
- L2TP Gateway IP Address:** Text input field.
- L2TP Server IP Address:** Text input field.
- Username:** Text input field.
- Password:** Password input field.
- Verify Password:** Password input field.
- Reconnect Mode:** Radio buttons for "Always on", "On demand" (selected), and "Manual".
- Maximum Idle Time:** Text input field with "(minutes, 0=infinite)" below it.
- Primary DNS Server:** Text input field.
- Secondary DNS Server:** Text input field.
- MTU:** Text input field with "(bytes) MTU default = 1400" below it.
- MAC Address:** Text input field.

At the bottom of the form is a button labeled "Clone Your PC's MAC Address". The left sidebar shows navigation tabs for "SETUP", "ADVANCED", "TOOLS", "STATUS", and "SUPPORT". The right sidebar contains "Helpful Hints..." and "More..." sections.



**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

**Clone MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

# Internet Setup

## Static (assigned by ISP)

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

**IP Address:** Enter the IP address assigned by your ISP.

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

**Default Gateway:** Enter the Gateway assigned by your ISP.

**DNS Servers:** The DNS server information will be supplied by your ISP (Internet Service Provider.)

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

The screenshot shows the D-Link router's web interface for configuring the Internet connection. The page is titled "WAN" and "Internet Connection". It provides instructions on how to choose the connection type and includes a note about PPPoE. The "INTERNET CONNECTION TYPE" section shows "Static IP" selected. The "STATIC IP ADDRESS INTERNET CONNECTION TYPE" section contains input fields for IP Address, Subnet Mask, Default Gateway, Primary DNS Server, Secondary DNS Server, MTU (set to 1500), and MAC Address. A "Clone Your PC's MAC Address" button is also present. The page includes a "Helpful Hints..." section on the right and a "WIRELESS" section at the bottom.

# Internet Setup

## Big Pond

**BigPond Server:** Enter the IP address of the login server.

**BigPond Username:** Enter your BigPond username.

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

**DNS Servers:** The DNS server information will be supplied by your ISP (Internet Service Provider.)

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

**MAC Address:** The default MAC Address is set to the Internet's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

The screenshot shows the D-Link DIR-625 web interface for Internet Setup. The page is titled "WAN" and "Internet Connection". It provides instructions on how to configure the Internet Connection type, listing options like Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. A note specifies that if using PPPoE, PPPoE client software should be removed or disabled. The "My Internet Connection is:" dropdown menu is set to "BigPond (Australia)". Below this, the "BIG POND INTERNET CONNECTION TYPE" section prompts the user to enter information from their Internet Service Provider (ISP). Fields include BigPond Server, BigPond User Id, BigPond Password, Verify Password, Primary DNS Server (0.0.0.0), Secondary DNS Server (0.0.0.0), MTU (1500 bytes, default 1500), and MAC Address (00:00:00:00:00:00). A "Clone Your PC's MAC Address" button is provided. The page also features a "Helpful Hints..." section on the right side, which offers advice on configuring the router and checking settings.

# Wireless Settings

**Enable Wireless:** Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

**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.

**Enable Auto Channel Scan:** The **Auto Channel Scan** setting can be selected to allow the DIR-625 to choose the channel with the least amount of interference.

**Wireless Channel:** Indicates the channel setting for the DIR-625. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

**802.11 Mode:** Select one of the following:

**802.11g Only** - Select if all of your wireless clients are 802.11g.

**Mixed 802.11g and 802.11b** - Select if you are using both 802.11b and 802.11g wireless clients.

**802.11b Only** - Select if all of your wireless clients are 802.11b.

**802.11n Only** - Select only if all of your wireless clients are 802.11n.

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

**Channel Width:** Select the Channel Width:

**Auto 20/40** - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.

**20MHz** - Select if you are not using any 802.11n wireless clients.

**Transmission Rate:** Select the transmit rate. It is strongly suggested to select **Best (Auto)** for best performance.

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET WIRELESS SETTINGS NETWORK SETTINGS

**WIRELESS**

**Wireless Network Settings**

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

Save Settings Don't Save Settings

**WIRELESS NETWORK SETTINGS**

Enable Wireless:

Wireless Network Name:  (Also called the SSID)

Enable Auto Channel Scan:

Wireless Channel:

802.11 Mode:

Channel Width:

Transmission Rate:  (Mbps)

Visibility Status:  Visible  Invisible

**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:

**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.

If you are not utilizing Super G with Dynamic Turbo for it's speed improvements, enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on.

Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, 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 WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

More...

**WIRELESS**

**Visibility Status:** Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-625. If Invisible is selected, the SSID of the DIR-625 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-625 in order to connect to it.

**Wireless Security:** Refer to page 61 for more information regarding wireless security.

# Network Settings

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

**IP Address:** Enter the IP address of the router. The default IP address is 192.168.0.1.

If you change the IP address, once you click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

**Local Domain:** Enter the Domain name (Optional).

**Enable DNS Relay:** Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.

The screenshot shows the D-Link DIR-625 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists menu items: INTERNET, WIRELESS SETTINGS, and NETWORK SETTINGS. The main content area is titled 'NETWORK SETTINGS' and contains several sections:

- NETWORK SETTINGS:** A section with a description and two buttons: 'Save Settings' and 'Don't Save Settings'.
- ROUTER SETTINGS:** A section with a description and fields for 'Router IP Address' (192.168.0.1), 'Subnet Mask' (255.255.255.0), 'Local Domain Name' (optional), and 'Enable DNS Relay' (checked).
- DHCP SERVER SETTINGS:** A section with a description and fields for 'Enable DHCP Server' (checked), 'DHCP IP Address Range' (192.168.0.100 to 192.168.0.199), 'DHCP Lease Time' (1440 minutes), and 'Always broadcast' (checked).
- ADD DHCP RESERVATION:** A section with 'Enable' (checked), 'Computer Name' (dropdown), 'IP Address' (0.0.0.0), 'MAC Address' (00:00:00:00:00:00), a 'Copy Your PC's MAC Address' button, and 'Save'/'Clear' buttons.
- DHCP RESERVATIONS LIST:** A table with columns: Enable, Computer Name, MAC Address, IP Address.
- NUMBER OF DYNAMIC DHCP CLIENTS : 1:** A table with columns: Computer Name, IP Address, MAC Address, Expire Time, and buttons for Revoke and Reserve.

At the bottom of the interface, there is a 'WIRELESS' section. On the right side, there is a 'Helpful Hints...' section with text about DHCP server configuration and a 'More...' link.

## DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-625 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.” When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-625. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

**Enable DHCP Server:** Check this box to enable the DHCP server on your router. Uncheck to disable this function.

**DHCP IP Address Range:** Enter the starting and ending IP addresses for the DHCP server’s IP assignment.

**Note:** If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

**Lease Time:** The length of time for the IP address lease. Enter the Lease time in minutes.

**Add DHCP Reservation:** Refer to the next page for the DHCP Reservation function.

**DHCP SERVER SETTINGS**

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

**Enable DHCP Server :**

**DHCP IP Address Range :** 192.168.0.100 to 192.168.0.199

**DHCP Lease Time :** 1440 (minutes)

**Always broadcast :**  (compatibility for some DHCP Clients)

---

**ADD DHCP RESERVATION**

**Enable :**

**Computer Name :**  << Computer Name

**IP Address :** 0.0.0.0

**MAC Address :** 00:00:00:00:00:00

---

**DHCP RESERVATIONS LIST**

Enable	Computer Name	MAC Address	IP Address

---

**NUMBER OF DYNAMIC DHCP CLIENTS : 1**

Computer Name	IP Address	MAC Address	Expire Time		
prescott	192.168.0.156	00:11:09:2a:94:11	23 Hours 18 Minutes	<a href="#">Revoke</a>	<a href="#">Reserve</a>

## DHCP Reservation

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

**Note:** This IP address must be within the DHCP IP Address Range.

**Enable:** Check this box to enable the reservation.

**Computer Name:** Enter the computer name or select from the drop-down menu and click <<.

**IP Address:** Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.

**MAC Address:** Enter the MAC address of the computer or device.

**Copy Your PC's MAC Address:** If you want to assign an IP address to the computer you are currently on, click this button to populate the fields.

**Save:** Click **Save** to save your entry. You must click **Save Settings** at the top to activate your reservations.

**Number of Dynamic DHCP Clients:** In this section you can see what LAN devices are currently leasing IP addresses.

**Revoke:** Click **Revoke** to cancel the lease for a specific LAN device and free an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

ADD DHCP RESERVATION

**Enable :**

**Computer Name :**  << Computer Name

**IP Address :**

**MAC Address :**

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address	

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Computer Name	IP Address	MAC Address	Expire Time		
prescott	192.168.0.156	00:11:09:2a:94:11	23 Hours 18 Minutes	<a href="#">Revoke</a>	<a href="#">Reserve</a>



**Note:** The Revoke option will not disconnect a PC with a current network session from the network; you would need to use MAC Address Filter to do that. Revoke will only free up a DHCP Address for the very next requester. If the previous owner is still available, those two devices may both receive an IP Address Conflict error, or the second device may still not receive an IP Address; in that case, you may still need to extend the “DHCP IP Address Range” to address the issue, it is located in the DHCP Server section.

**Reserve:** The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

## Virtual Server

The DIR-625 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DIR-625 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-625 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-625 redirects the external service request to the appropriate server within the LAN network.

The DIR-625 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

For a list of ports for common applications, please visit [http://support.dlink.com/faq/view.asp?prod\\_id=1191](http://support.dlink.com/faq/view.asp?prod_id=1191).

This will allow you to open a single port. If you would like to open a range of ports, refer to page 35.

**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the “Computer Name” drop-down menu. Select your computer and click <<.

**Private Port/ Public Port:** Enter the port that you want to open next to Private Port and Public Port. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

**Protocol Type:** Select **TCP**, **UDP**, or **Both** from the drop-down menu.

**Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

**Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

Product Page: DIR-625 Hardware Version: C1 Firmware Version: 3.00

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

**VIRTUAL SERVER**

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

**24--VIRTUAL SERVERS LIST**

	Name	Application Name	Port	Protocol	Traffic Type	Schedule	Inbound Filter
<input type="checkbox"/>		<< Application Name	Public 0	TCP		Always	Allow All
	IP Address	<< Computer Name	Private 0	6			Allow All
<input type="checkbox"/>		<< Application Name	Public 0	TCP		Always	Allow All
	IP Address	<< Computer Name	Private 0	6			Allow All
<input type="checkbox"/>		<< Application Name	Public 0	TCP		Always	Allow All
	IP Address	<< Computer Name	Private 0	6			Allow All
<input type="checkbox"/>		<< Application Name	Public 0	TCP		Always	Allow All
	IP Address	<< Computer Name	Private 0	6			Allow All
<input type="checkbox"/>		<< Application Name	Public 0	TCP		Always	Allow All
	IP Address	<< Computer Name	Private 0	6			Allow All
<input type="checkbox"/>		<< Application Name	Public 0	TCP		Always	Allow All
	IP Address	<< Computer Name	Private 0	6			Allow All

**Helpful Hints...**

Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.

Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** screen and create a new schedule.

Select a filter that restricts the Internet hosts that can access this virtual server to hosts that you trust. If you do not see the filter you need in the list of filters, go to the **Advanced → Inbound Filter** screen and create a new filter.

[More...](#)

# Port Forwarding

This will allow you to open a single port or a range of ports.

**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the “Computer Name” drop-down menu. Select your computer and click <<.

**TCP/UDP:** Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.

Example: 24,1009,3000-4000

**Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

**Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

**PORT FORWARDING**

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

Save Settings Don't Save Settings

**24 -- PORT FORWARDING RULES**

	Name	IP Address	Application Name	Computer Name	Ports to Open	Schedule	Inbound Filter
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	TCP	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	TCP	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	TCP	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP	Always	Allow All

**Helpful Hints...**

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the LAN computer to which you would like to open the specified port.

Select a schedule for when the rule will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** screen and create a new schedule.

You can enter ports in various formats:

Range (50-100)  
Individual (80, 68, 888)  
Mixed (1020-5000, 689)

[More...](#)

# Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DIR-625. If you need to run applications that require multiple connections, specify the port normally associated with an application in the “Trigger Port” field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-625 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

**Name:** Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click <<.

**Trigger:** This is the port used to trigger the application. It can be either a single port or a range of ports.

**Traffic Type:** Select the protocol of the trigger port (TCP, UDP, or Both).

**Firewall:** This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

**Traffic Type:** Select the protocol of the firewall port (TCP, UDP, or Both).

**Schedule:** The schedule of time when the Application Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

Product Page: DIR-625 Hardware Version: C1 Firmware Version: 3.00

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

**APPLICATION RULES**

This option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

Save Settings Don't Save Settings

**24 -- APPLICATION RULES**

	Name	Application	Port	Traffic Type	Schedule
<input type="checkbox"/>		<< Application Name	Trigger	TCP	Always
<input type="checkbox"/>		<< Application Name	Firewall	TCP	Always
<input type="checkbox"/>		<< Application Name	Trigger	TCP	Always
<input type="checkbox"/>		<< Application Name	Firewall	TCP	Always
<input type="checkbox"/>		<< Application Name	Trigger	TCP	Always
<input type="checkbox"/>		<< Application Name	Firewall	TCP	Always

**Helpful Hints...**

Use this feature if you are trying to execute one of the listed network applications and it is not communicating as expected.

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools > Schedules** screen and create a new schedule.

**More...**

# QoS Engine

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.

**Enable StreamEngine:** This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

**Dynamic Fragmentation:** This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones.

**Automatic Uplink Speed:** This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

**Measured Uplink Speed:** This displays the detected uplink speed.

**Manual Uplink Speed:** The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbps/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as [www.dslreports.com](http://www.dslreports.com).

**Connection Type:** By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the Internet settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

**Detected xDSL:** When Connection Type is set to automatic, the automatically detected connection type is displayed here.

Product Page: DIR-625 Hardware Version: C1 Firmware Version: 3.00

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

**QOS ENGINE**

Use this section to configure D-Link's QoS Engine powered by StreamEngine™ Technology. The QoS Engine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

Save Settings Don't Save Settings

**QOS ENGINE SETUP**

Enable QoS Engine :

Automatic Classification :

Dynamic Fragmentation :

Automatic Uplink Speed :

Measured Uplink Speed : Not Estimated

Manual Uplink Speed : 128 kbps << Select Transmission Rate

Connection Type : Auto-detect

Detected xDSL or Other Frame Relay Network : Yes

Helpful Hints...  
If the **Measured Uplink Speed** is known to be incorrect (that is, it produces suboptimal performance), disable **Automatic Uplink Speed** and enter the **Manual Uplink Speed**. Some experimentation and performance measurement may be required to converge on the optimal value.  
[More...](#)

# Network Filters

Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

**Configure MAC Filtering:** Select Turn MAC Filtering Off, allow MAC addresses listed below, or deny MAC addresses listed below from the drop-down menu.

**MAC Address:** Enter the MAC address you would like to filter. To find the MAC address on a computer, please refer to the Networking Basics section in this manual.

**DHCP Client:** Select a DHCP client from the drop-down menu and click << to copy that MAC Address.

Product Page: DIR-625 Hardware Version: C1 Firmware Version: 3.00

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

**MAC ADDRESS FILTER**

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

Save Settings Don't Save Settings

**24 -- MAC FILTERING RULES**

Configure MAC Filtering below:  
Turn MAC Filtering OFF

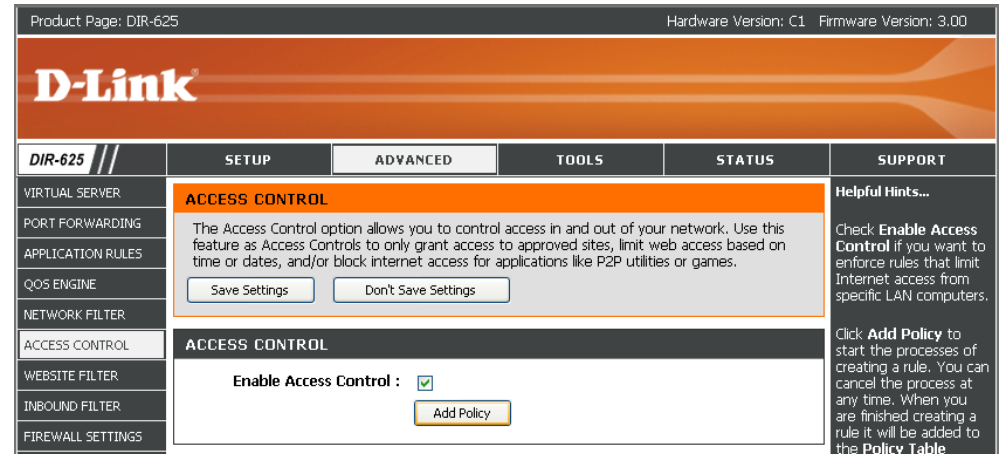
MAC Address		DHCP Client List	
<input type="text"/>	<<	Computer Name	Clear
<input type="text"/>	<<	Computer Name	Clear
<input type="text"/>	<<	Computer Name	Clear
<input type="text"/>	<<	Computer Name	Clear
<input type="text"/>	<<	Computer Name	Clear

Helpful Hints...  
Create a list of MAC addresses that you would either like to allow or deny access to your network.  
Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu, then click the arrow to add that device's MAC address to the list.  
Click the **Clear** button to remove the MAC address from the MAC Filtering list.  
More...

# Access Control

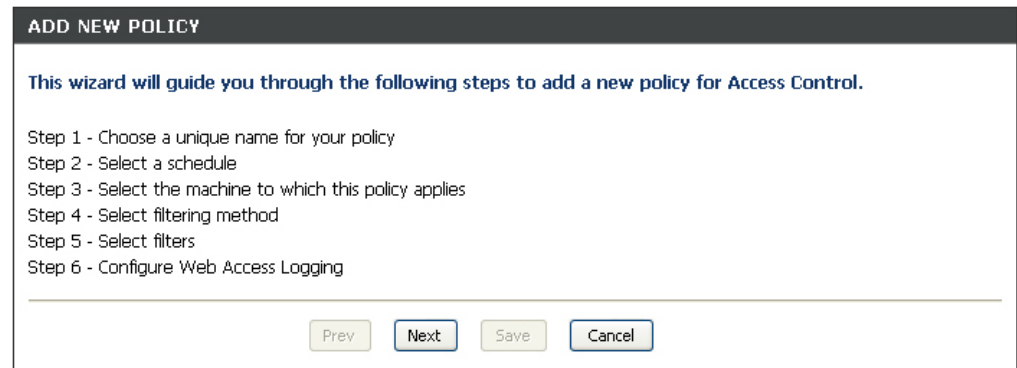
The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

**Add Policy:** Check the **Enable Access Control** check box and click the **Add Policy** button to start the **Access Control Wizard**.



## Access Control Wizard

Click **Next** to continue with the wizard.





## Access Control Wizard (continued)

Enter a name for the policy and then click **Next** to continue.

**STEP 1: CHOOSE POLICY NAME**

Choose a unique name for your policy.

Policy Name :

Select a schedule (I.E. Always) from the drop-down menu and then click **Next** to continue.

**STEP 2: SELECT SCHEDULE**

Choose a schedule to apply to this policy.

Details :

Enter the following information and then click **Next** to continue.

- Address Type - Select IP address, MAC address, or Other Machines.
- IP Address - Enter the IP address of the computer you want to apply the rule to.

**STEP 3: SELECT MACHINE**



Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type :  IP  MAC  Other Machines

IP Address :  <<

Machine Address :  <<

Machine		
192.168.0.100		

## Access Control Wizard (continued)

Select the filtering method and then click **Next** to continue.

**STEP 4: SELECT FILTERING METHOD**

Select the method for filtering.

Method :  Log Web Access Only  Block All Access  Block Some Access

Apply Web Filter :

Apply Advanced Port Filters :

Prev Next Save Cancel

Enter the rule:

**Enable** - Check to enable the rule.

**Name** - Enter a name for your rule.

**Dest IP Start** - Enter the starting IP address.

**Dest IP End** - Enter the ending IP address.

**Protocol** - Select the protocol.

**Dest Port Start** - Enter the starting port number.

**Dest Port End** - Enter the ending port number.

**STEP 5: PORT FILTER**

Add Port Filters Rules.

Specify rules to prohibit access to specific IP addresses and ports.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535

Prev Next Save Cancel

To enable web logging, click Enable.

Click **Save** to save the access control rule.

**STEP 6: CONFIGURE WEB ACCESS LOGGING**

Web Access Logging :  Disabled  Enabled

Prev Next Save Cancel

## Website Filters

Website Filters are used to deny LAN computers from accessing specific web sites by the URL or domain. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display. To use this feature, enter the text string to be blocked and click **Save Settings**. The text to be blocked will appear in the list. To delete the text, click **Clear the List Below**.

**Website URL/ Domain:** Enter the keywords or URLs that you want to block (or allow). Any URL with the keyword in it will be blocked.

The screenshot displays the D-Link DIR-625 web interface. At the top, it shows 'Product Page: DIR-625' and 'Hardware Version: C1 Firmware Version: 3.00'. The D-Link logo is prominently displayed. Below the logo is a navigation menu with tabs for 'DIR-625', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'WEBSITE FILTER' option is highlighted in the left sidebar. The main content area is titled 'WEBSITE FILTER' and contains the following text: 'The Web Filter option allows you to set up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. Underneath, there is a section titled '40 -- WEBSITE FILTERING RULES' with a 'Clear the list below...' button. A table with the header 'Website URL/Domain' is shown, containing four rows of empty input fields for URLs and domains. On the right side of the interface, there is a 'Helpful Hints...' section with instructions: 'Create a list of Web sites to which you would like to allow access from the devices on your network.' and 'Use with **Advanced** → **Access Control**. More...'

# Inbound Filters

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound Filters can be used with Virtual Server, Port Forwarding, or Remote Administration features.

**Name:** Enter a name for the inbound filter rule.

**Action:** Select **Allow** or **Deny**.

**Enable:** Check to enable rule.

**Source IP Start:** Enter the starting IP address. Enter 0.0.0.0 if you do not want to specify an IP range.

**Source IP End:** Enter the ending IP address. Enter 255.255.255.255 if you do not want to specify and IP range.

**Save:** Click the **Save** button to apply your settings. You must click Save Settings at the top to save the settings.

**Inbound Filter Rules List:** This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.

Product Page: DIR-625 Hardware Version: C1 Firmware Version: 3.00

**D-Link**

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

**INBOUND FILTER**

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.

**ADD INBOUND FILTER RULE**

Name :

Action :

Source IP Range	Enable	Source IP Start	Source IP End
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255

**INBOUND FILTER RULES LIST**

Name	Action	Source IP Range

**Helpful Hints...**

Give each rule a **Name** that is meaningful to you.

Each rule can either **Allow** or **Deny** access from the WAN.

Up to eight ranges of WAN IP addresses can be controlled by each rule. The checkbox by each IP range can be used to disable ranges already defined.

The starting and ending IP addresses are WAN-side address.

Click the **Add** or **Update** button to store a finished rule in the Rules List below.

Click the **Edit** icon in the Rules List to change a rule.

Click the **Delete** icon in the Rules List to permanently remove a rule.

[More...](#)

**WIRELESS**

# Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-625 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

**Enable SPI:** SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

**NAT Endpoint Filtering:** Select one of the following for TCP and UDP ports:  
**Endpoint Independent** - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

**Address Restricted** - Incoming traffic must match the IP address of the outgoing connection.

**Address + Port Restriction** - Incoming traffic must match the IP address and port of the outgoing connection.

**Enable DMZ Host:** If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

**Note:** Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

**IP Address:** Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its IP address automatically using DHCP, be sure to make a static reservation on the Basic > DHCP page so that the IP address of the DMZ machine does not change.

The screenshot displays the D-Link DIR-625 web interface. The top navigation bar includes 'DIR-625', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The main content area is titled 'FIREWALL SETTINGS' and contains the following sections:

- FIREWALL SETTINGS:** A text box explains that these settings allow setting a single computer on the network outside the router. Below it are 'Save Settings' and 'Don't Save Settings' buttons. The 'Enable SPI' checkbox is checked.
- NAT ENDPOINT FILTERING:** This section has two sub-sections:
  - UDP Endpoint Filtering:** Three radio buttons are present: 'Endpoint Independent' (unchecked), 'Address Restricted' (checked), and 'Port And Address Restricted' (unchecked).
  - TCP Endpoint Filtering:** Three radio buttons are present: 'Endpoint Independent' (unchecked), 'Address Restricted' (unchecked), and 'Port And Address Restricted' (checked).
- DMZ HOST:** A text box explains the DMZ (Demilitarized Zone) option. Below it, the 'Enable DMZ' checkbox is unchecked. The 'DMZ IP Address' is set to '0.0.0.0' with a dropdown menu for 'Computer Name'.
- NON-UDP/TCP/ICMP LAN SESSIONS:** The 'Enable' checkbox is checked.
- APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION:** A list of protocols with checkboxes:
  - PPTP:
  - IPSec (VPN):
  - RTSP:
  - Windows/MSN Messenger:  (automatically disabled if UPnP is enabled)
  - FTP:
  - H.323 (NetMeeting):
  - SIP:
  - Wake-On-LAN:
  - MMS:

A 'Helpful Hints...' sidebar on the right provides additional information, including a note about enabling DMZ as a last resort and a warning about security risks associated with the DMZ option.

## Application Level Gateway (ALG) Configuration

Here you can enable or disable ALG's. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

**PPTP:** Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

**IPSEC (VPN):** Allows multiple VPN clients to connect to their corporate network using IPsec. Some VPN clients support traversal of IPsec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

**RTSP:** Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

**MSN Messenger:** Allows all of the Windows/MSN Messenger functions to work properly through the router.

**FTP:** Allows FTP clients and servers to transfer data across NAT. Refer to the Advanced > Virtual Server page if you want to host an FTP server.

**H.323 (Netmeeting):** Allows Microsoft NetMeeting clients to communicate across NAT. Note that if you want your buddies to call you, you should also set up a virtual server for NetMeeting. Refer to the Advanced > Virtual Server page for information on how to set up a virtual server.

**SIP:** Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

**Wake-On-LAN:** Allows Ethernet network adapters with Wake-On-LAN (WOL) to function.

**MMS:** Allows Windows Media Player, using MMS protocol, to receive streaming media from the Internet.

# Advanced Wireless Settings

**Transmit Power:** Set the transmit power of the antennas.

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

**RTS Threshold:** This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

**Fragmentation Threshold:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

**DTIM Interval:** (Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

**802.11d:** This enables 802.11d operation. 802.11d is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it.

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

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

Product Page: DIR-625 Hardware Version: C1 Firmware Version: 3.0

DIR-625 // SETUP ADVANCED TOOLS STATUS SUPPORT

**ADVANCED WIRELESS**

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 : High

Beacon Period : 100 (20..1000)

RTS Threshold : 2346 (0..2347)

Fragmentation Threshold : 2346 (256..2346)

DTIM Interval : 1 (1..255)

802.11d Enable :

WMM Enable :

Aggregation Limit : 8 Kbytes

TPC Max Gain : 20 (0..50)

Aggregation Max Size : 64000 (2000..65535)

Aggregation Num Packets : 32 (1..64)

Force Short Slot for 11N Clients :

Short GI :

Extra Wireless Protection :

**Helpful Hints...**

It is recommended that you leave these parameters at their default values. Adjusting them could limit the performance of your wireless network.

Use **802.11d** only for countries where it is required.

Enabling **WMM** can help control latency and jitter when transmitting multimedia content over a wireless connection.

More...

**WIRELESS**

# WISH

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications. The WISH configuration has a max of 24 Rules that can be defined.

**Enable WISH:** Enable this option if you want to allow WISH to prioritize your traffic.

**HTTP:** Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

**Windows Media Center:** Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

**Automatic:** When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

**WISH Rules:** A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required. WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

The screenshot shows the D-Link DIR-625 Advanced Setup page. The top navigation bar includes 'DIR-625', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'WISH' section is highlighted in orange. The 'WISH' section contains the following options:

- WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications.** (Save Settings / Don't Save Settings)
- Enable WISH :**
- PRIORITY CLASSIFIERS**
  - HTTP :**
  - Windows Media Center :**
  - Automatic :**  (default if not matched by anything else)
- 24 -- WISH RULES**

Name	Priority	Protocol
<input type="text"/>	Best Effort (BE)	6 << TCP
Host 1 IP Range: 0.0.0.0 to 255.255.255.255		Host 1 Port Range: 0 to 65535
Host 2 IP Range: 0.0.0.0 to 255.255.255.255		Host 2 Port Range: 0 to 65535
<input type="text"/>	Best Effort (BE)	6 << TCP

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

Enable this option if you want to allow WISH to prioritize wireless traffic.

For most applications, the priority classifiers ensure the right priorities, and specific WISH Rules are not required.

[More...](#)



**Name:** Create a name for the rule that is meaningful to you.

**Priority:** The priority of the message flow is entered here. Four priorities are defined:

- BK: Background (least urgent).
- BE: Best Effort
- VI: Video
- VO: Voice (most urgent)

**Protocol:** The protocol used by the messages.

**Host 1 IP Range:** The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

**Host 1 Port Range:** The rule applies to a flow of messages for which host 1's port number is within the range set here.

**Host 2 IP Range:** The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.

**Host 2 IP Range:** The rule applies to a flow of messages for which host 2's port number is within the range set here.

# Wi-Fi Protected Setup

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

**Enable:** Enable the Wi-Fi Protected Setup feature.

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

**PIN Settings:** A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.

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

### Reset PIN to Default:

Restore the default PIN of the router.

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

The screenshot shows the D-Link DIR-625 router's web interface. At the top, it displays 'Product Page: DIR-625' and 'Hardware Version: C1 Firmware Version: 3.00'. The D-Link logo is prominent. Below the logo is a navigation menu with tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'WI-FI PROTECTED SETUP' page is displayed. The page is divided into several sections:

- WI-FI PROTECTED SETUP:** A section with a title bar and a description: 'Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.' It contains two buttons: 'Save Settings' and 'Don't Save Settings'.
- WI-FI PROTECTED SETUP:** A section with a title bar and two checkboxes: 'Enable : ' and 'Lock Wireless Security Settings : '. The 'Enable' checkbox is checked.
- PIN SETTINGS (ADMINISTRATOR ACCESS ONLY):** A section with a title bar and a 'Current PIN : 24681353'. It contains two buttons: 'Reset PIN to Default' and 'Generate New PIN'.
- ADD WIRELESS STATION (ADMINISTRATOR ACCESS ONLY):** A section with a title bar and one button: 'Add Wireless Device Wizard'.

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

- Enable if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup.**
- Only "Admin" account can change security settings.**
- Lock Wireless Security Settings after all wireless network devices have been configured.**
- Click Add Wireless Device Wizard to use Wi-Fi Protected Setup to add wireless devices to the wireless network.**
- More...**

At the bottom of the interface, there is a 'WIRELESS' section.