



# User Manual

## Wireless N750 Dual Band Router

---

# Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

## Manual Revisions

Revision	Date	Description
1.0	October 12, 2011	• Initial release

## Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2011 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

# Table of Contents

<b>Preface</b> .....	<b>i</b>	PPTP .....	21
Manual Revisions .....	i	L2TP .....	23
Trademarks .....	i	DS-Lite .....	25
<b>Product Overview</b> .....	<b>1</b>	Wireless Settings .....	26
Package Contents .....	1	Manual Wireless Settings .....	27
System Requirements .....	2	802.11n/g (2.4GHz) .....	27
Introduction .....	3	802.11n/a (5GHz) .....	29
Features .....	4	Network Settings .....	31
Hardware Overview .....	5	Router Settings .....	31
Connections .....	5	DHCP Server Settings .....	32
LEDs .....	6	DHCP Reservation .....	34
<b>Installation</b> .....	<b>7</b>	Media Server .....	35
Before you Begin .....	7	IPv6 .....	36
Wireless Installation Considerations .....	8	IPv6 Internet Connection Setup Wizard .....	37
Connect to Cable/DSL/Satellite Modem .....	9	IPv6 Manual Setup .....	42
Connect to Another Router .....	10	Auto Detection .....	42
Getting Started .....	12	Static IPv6 .....	43
<b>Configuration</b> .....	<b>13</b>	Autoconfiguration .....	44
Quick Setup Wizard .....	13	PPPoE .....	45
Web-based Configuration Utility .....	16	IPv6 in IPv4 Tunneling .....	47
Internet Connection Setup .....	17	6 to 4 Tunneling .....	48
Static (assigned by ISP) .....	18	6rd .....	49
Static IP .....	18	Link-Local Connectivity .....	50
Dynamic (Cable) .....	19	Advanced .....	51
PPPoE (DSL) .....	20	Virtual Server .....	51
		Port Forwarding .....	53

Application Rules.....	54	Firmware .....	79
QoS Engine.....	55	Dynamic DNS .....	80
Network Filters.....	57	System Check.....	82
Access Control .....	58	Schedules .....	83
Access Control Wizard .....	58	Status .....	84
Website Filters.....	61	Device Info .....	84
Inbound Filters.....	62	Logs .....	85
Firewall Settings.....	63	Statistics .....	86
Routing.....	64	Internet Sessions.....	87
Advanced Wireless .....	65	Routing.....	88
Advanced Wireless Settings.....	66	Wireless .....	89
802.11n/g (2.4GHz) .....	66	IPv6 .....	90
802.11n/a (5GHz) .....	67	IPV6 Routing.....	91
Wi-Fi Protected Setup (WPS) .....	68	Support .....	92
Advanced Network Settings.....	70	<b>Wireless Security .....</b>	<b>93</b>
UPnP .....	70	What is WPA? .....	93
Internet Ping Block.....	70	Wireless Security Setup Wizard .....	94
Internet Port Speed.....	70	Add Wireless Device with WPS Wizard.....	96
Multicast Streams .....	70	Configure WPA-Personal (PSK).....	97
Guest Zone.....	71	Configure WPA-Enterprise (RADIUS).....	98
IPv6 Firewall.....	72	<b>Connect to a Wireless Network.....</b>	<b>100</b>
IPv6 Routing .....	73	Using Windows® 7 .....	100
Tools .....	74	Configure WPS .....	103
Admin .....	74	Windows Vista® .....	107
Time.....	75	Configure Wireless Security .....	108
SysLog.....	76	Connect Using WCN 2.0 in Windows Vista® .....	110
Email Settings .....	77	Windows® XP.....	111
System .....	78	Configure WPA-PSK.....	112
Language Pack.....	79		

<b>Troubleshooting .....</b>	<b>114</b>
<b>Wireless Basics .....</b>	<b>118</b>
What is Wireless? .....	119
Tips.....	121
Wireless Modes.....	122
<b>Networking Basics .....</b>	<b>123</b>
Check your IP address.....	123
Statically Assign an IP address .....	124
<b>Technical Specifications .....</b>	<b>125</b>
<b>Contacting Technical Support .....</b>	<b>126</b>
<b>Warranty.....</b>	<b>127</b>
<b>Registration .....</b>	<b>135</b>

# Package Contents



DIR-835 Wireless N750 Dual Band Router



Ethernet Cable



Three Detachable Antennas



Power Adapter



CD-ROM with Manual and Setup Wizard

If any of the above items are missing, please contact your reseller.

**Note:** Using a power supply with a different voltage rating than the one included with the DIR-835 will cause damage and void the warranty for this product.

# System Requirements

<p><b>Network Requirements</b></p>	<ul style="list-style-type: none"> <li>• An Ethernet-based Cable or DSL modem</li> <li>• IEEE 802.11n or 802.11g wireless clients</li> <li>• IEEE 802.11a wireless clients</li> <li>• 10/100/1000 Ethernet</li> </ul>
<p><b>Web-based Configuration Utility Requirements</b></p>	<p><b>Computer with the following:</b></p> <ul style="list-style-type: none"> <li>• Windows®, Macintosh, or Linux-based operating system</li> <li>• An installed Ethernet adapter</li> </ul> <p><b>Browser Requirements:</b></p> <ul style="list-style-type: none"> <li>• Internet Explorer 6 or higher</li> <li>• Firefox 3.0 or higher</li> <li>• Safari 3.0 or higher</li> <li>• Chrome 2.0 or higher</li> </ul> <p><b>Windows® Users:</b> Make sure you have the latest version of Java installed. Visit <a href="http://www.java.com">www.java.com</a> to download the latest version.</p>
<p><b>CD Installation Wizard Requirements</b></p>	<p><b>Computer with the following:</b></p> <ul style="list-style-type: none"> <li>• Windows® 7, Vista®, or XP (Service Pack 2 or higher)</li> <li>• An installed Ethernet adapter</li> <li>• CD-ROM drive</li> </ul>

# Introduction

## **TOTAL PERFORMANCE**

Combines award winning router features and IEEE 802.11a/g/n wireless technology to provide the best wireless performance.

## **TOTAL SECURITY**

The most complete set of security features including Active Firewall and WPA/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 Wireless N750 Dual Band Router (DIR-835) is an 802.11n/802.11a compliant device that delivers real world performance of up to 13x faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the DIR-835 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 Wireless N technology, this high performance router provides superior Whole Home Coverage while reducing dead spots. The router is designed for use in bigger homes and for users who demand higher performance networking. Add a Wireless N notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

## **TOTAL NETWORK SECURITY**

The Wireless 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/WPA2 standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

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

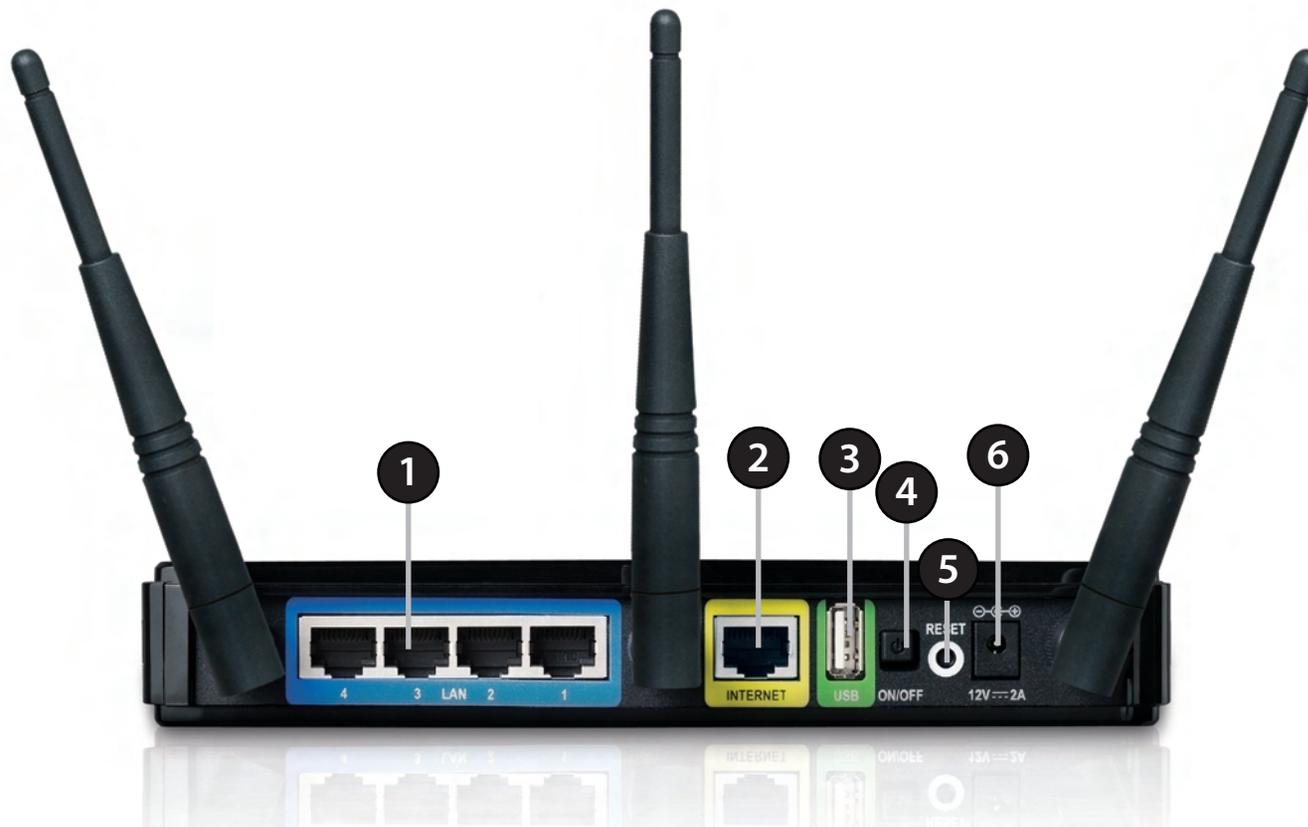
# Features

- **Faster Wireless Networking** - The DIR-835 provides up to 750Mbps\* combined wireless bandwidth 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 13x faster than 802.11g.
- **Compatible with 802.11a/g Devices** - The DIR-835 is still fully compatible with the IEEE 802.11g and 802.11a standards, so it can connect with existing 802.11g and 802.11a 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-835 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-835 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-835 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, 802.11a, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

# Hardware Overview

## Connections



1	LAN Ports (1-4)	Connect 10/100/1000 Ethernet devices such as computers, switches, and NAS.
2	Internet Port	The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.
3	USB Port	Connect a USB 1.1 or 2.0 flash drive to configure the wireless settings using WCN and SharePort.
4	Reset Button	Pressing the Reset button restores the router to its original factory default settings.
5	Power Button	Press the power button to power on and off.
6	Power Receptor	Receptor for the supplied power adapter.

# Hardware Overview

## LEDs



<b>1</b>	Power LED	A solid green light indicates a proper connection to the power supply.
<b>2</b>	Internet LED	A solid green light indicates connection on the Internet port. This LED blinks during data transmission.

# 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.
- 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.
- When running the Setup Wizard from the D-Link CD, make sure the computer you are running the CD from is connected to the Internet and online or the wizard will not work. If you have disconnected any hardware, re-connect your computer back to the modem and make sure you are online.

# 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. 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. 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. Refer to page 13 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** 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 (WAN) 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-835 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:\autorun.exe**" (where **D:** represents the drive letter of your CD-ROM drive).

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



**Note:** It is recommended to write down the SSID and Security Key, followed by 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.

## Quick Setup Wizard

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).

You may also connect using the NetBIOS name in the address bar (**http://dlinkrouter**).

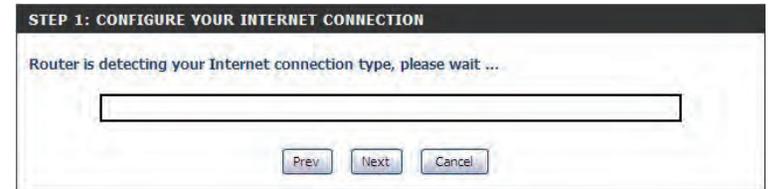


This wizard is designed to guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

Click **Next** to continue.

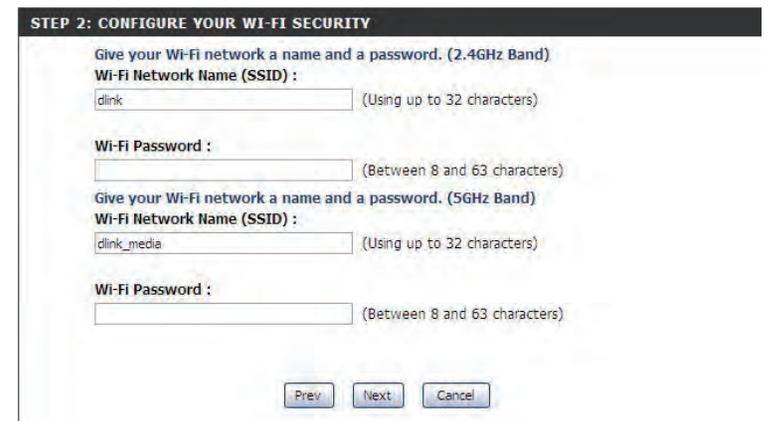


Please wait while your router detects your internet connection type.

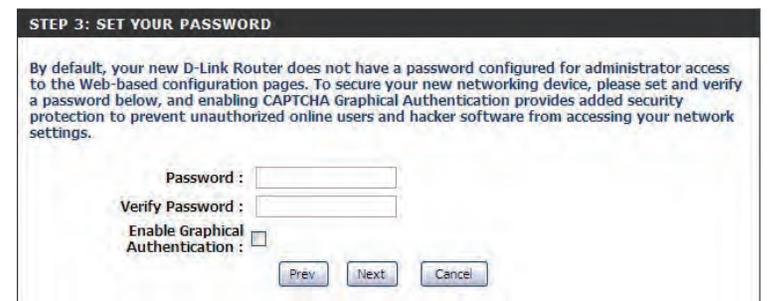


Please give your network a name using up to 32 characters.

Click **Next** to continue.



In order to secure your new networking device, please enter a password and click **Next**.



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



Once this screen appears, your setup is complete. Click **Save & Connect** to reboot the router.



# 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).



If you selected **Cancel Setup** on the Quick Setup Wizard page, you will be directed to this screen.

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

A screenshot of the "LOGIN" page for the router configuration utility. The page has an orange header with the word "LOGIN" in white. Below the header, it says "Log in to the router :". There are two input fields: "User Name" with a dropdown menu showing "Admin" and a blue arrow, and "Password" with an empty text box. Below these fields is a "Log In" button.

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

# Internet Connection Setup

Select the Internet Connection you would like to use.

Click **Manual Internet Connection Setup** to configure your connection manually and continue on pg 18.

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard**. You will be directed to the Quick Setup Wizard section on pg 13.

The screenshot displays a web-based configuration interface for an Internet connection. It is divided into three main sections:

- INTERNET CONNECTION**: An orange header section containing the text: "There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection."
- INTERNET CONNECTION WIZARD**: A dark grey header section containing the text: "If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below." Below this text is a button labeled "Internet Connection Setup Wizard". A **Note** follows: "Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package."
- MANUAL INTERNET CONNECTION OPTIONS**: A dark grey header section containing the text: "If you would like to configure the Internet settings of your new D-Link Systems Router manually, then click on the button below." Below this text is a button labeled "Manual Internet Connection Setup".

# 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.

**INTERNET CONNECTION TYPE**

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

My Internet Connection is :

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

---

**TRUE GIGABIT ROUTING CONNECTIVITY SETTING**

Enable True Gigabit Routing Connectivity :

---

**STATIC IP ADDRESS INTERNET CONNECTION TYPE :**

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

IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

Secondary DNS Server :

MTU :  (bytes) MTU default = 1500

MAC Address :

## 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 such as Comcast and Cox.

**Enable Advanced DNS Service:** Advanced Domain Name System (DNS) services enhances your Internet performance by getting you the information and web pages you are looking for faster and more reliably. In addition, it improves your overall Internet experience by correcting many common typo mistakes automatically, taking you where you intended to go and saving you valuable time.

**Disclaimer:** D-Link makes no warranty as to the availability, reliability, functionality and operation of the Advanced DNS service or its features.

**Host Name:** The Host Name is optional but may be required by some ISPs. Leave blank if you are not sure.

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

**Primary/Secondary DNS Server:** Enter the Primary and secondary DNS server IP addresses assigned by your ISP. These addresses are usually obtained automatically from your ISP. Leave at 0.0.0.0 if you did not specifically receive these from 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.

**INTERNET CONNECTION TYPE**

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

My Internet Connection is :

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

---

**TRUE GIGABIT ROUTING CONNECTIVITY SETTING**

Enable True Gigabit Routing Connectivity :

---

**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 :

# 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 IP** 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).

**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 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.

**INTERNET CONNECTION TYPE**

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

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

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

---

**TRUE GIGABIT ROUTING CONNECTIVITY SETTING**

Enable True Gigabit Routing Connectivity :

---

**PPPOE :**

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

**Address Mode**  Dynamic IP (DHCP)  Static IP

**IP Address :**

**Username**

**Password**

**Verify Password**

**Service Name**  (optional)

**Reconnect Mode :**  Always on  On demand  Manual

**Maximum Idle Time**  (minutes, 0=infinite)

**Primary DNS Address**  (Optional)

**Secondary DNS Address**  (Optional)

**MTU**  (bytes)MTU default =1492

**MAC Address**

# 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.)

**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 :**

**PPTP Subnet Mask :**

**PPTP Gateway IP Address :**

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

**User Name :**

**Password :**

**Verify Password :**

**DNS SETTINGS**

**Primary DNS Address :**

**Secondary DNS Address :**

**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).

**INTERNET CONNECTION TYPE**

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

My Internet Connection is : L2TP (Username / Password) ▾

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

---

**L2TP :**

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

**Address Mode**  Dynamic IP (DHCP)  Static IP

**L2TP :**

**L2TP Subnet Mask :**

**L2TP Gateway IP Address :**

**L2TP Server IP Address :**

**Username:**

**Password**

**Verify Password :**

**Reconnect Mode :**  Always on  On demand  Manual

**Maximum Idle Time**  (minutes, 0=infinite)

**Primary DNS Address**

**Secondary DNS Address**

**MTU**  (bytes)MTU default = 1400

**MAC Address**

[Clone Your PC's MAC Address](#)

**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

## DS-Lite

Another Internet Connection type is DS-Lite.

DS-Lite is an IPv6 connection type. After selecting DS-Lite, the following parameters will be available for configuration:

**DS-Lite Configuration:** Select the DS-Lite DHCPv6 option to let the router allocate the AFTR IPv6 address automatically. Select the Manual Configuration to enter the AFTR IPv6 address in manually.

**AFTR IPv6 Address:** After selecting the Manual Configuration option above, enter the AFTR IPv6 address used here.

**B4 IPv4 Address:** Enter the B4 IPv4 address value used here.

**WAN IPv6 Address:** Once connected, the WAN IPv6 address will be displayed here.

**IPv6 WAN Default Gateway:** Once connected, the IPv6 WAN Default Gateway address will be displayed here.

**INTERNET CONNECTION TYPE**

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

My Internet Connection is :

---

**AFTR ADDRESS INTERNET CONNECTION TYPE :**

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

**DS-Lite Configuration**  DS-Lite DHCPv6 Option  Manual Configuration

**AFTR IPv6 Address :**

**B4 IPv4 Address :** 192.0.0.1  (Optional)

**WAN IPv6 Address :**

**IPv6 WAN Default Gateway :**

# Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Security Setup Wizard** and refer to page 94.

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 96.

If you want to manually configure the wireless settings on your router click **Manual Wireless Network Setup** and refer to the next page.

**WIRELESS SETTINGS**

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

**WIRELESS NETWORK SETUP WIZARD**

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Wireless Network Setup Wizard

**Note :** Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

**ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD**

This wizard is designed to assist you in connecting your wireless device to your router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

Add Wireless Device with WPS

**MANUAL WIRELESS NETWORK SETUP**

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

Manual Wireless Network Setup

# Manual Wireless Settings

## 802.11n/g (2.4GHz)

**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.

**Schedule:** Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click **Add New** to create a new schedule.

**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.

**802.11 Mode:** Select one of the following:  
**802.11g Only** - Select if all of your wireless clients are 802.11g.  
**Mixed 802.11n and 802.11g** - Select if you are using both 802.11n and 802.11g wireless clients.  
**802.11n Only** - Select only if all of your wireless clients are 802.11n.

**Enable Auto Channel Scan:** The **Auto Channel Scan** setting can be selected to allow the DIR-835 to choose the channel with the least amount of interference.

**Wireless Channel:** Indicates the channel setting for the DIR-835. 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.

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

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.

The screenshot shows two sections of a configuration interface. The top section, titled "WIRELESS NETWORK SETTINGS", includes the following options: "Wireless Band" set to "2.4GHz Band"; "Enable Wireless" checked with a dropdown menu set to "Always" and a "New Schedule" button; "Wireless Network Name" set to "dlink" (with a note "(Also called the SSID)"); "802.11 Mode" set to "Mixed 802.11n, 802.11g and 802.11b"; "Enable Auto Channel Scan" checked; "Wireless Channel" set to "2.412 GHz - CH 1"; "Channel Width" set to "20 MHz"; and "Visibility Status" with "Visible" selected. The bottom section, titled "WIRELESS SECURITY MODE", contains a descriptive paragraph about security features and a "Security Mode" dropdown menu currently set to "None".

**Channel Width:** **20MHz** - Select if you are not using any 802.11n wireless clients.  
**40MHz** - Select if you are using 802.11n wireless clients only.

**Visibility Status:** Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-835. If Invisible is selected, the SSID of the DIR-835 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-835 in order to connect to it.

**Wireless Security:** Refer to page 93 for more information regarding wireless security.

## 802.11n/a (5GHz)

**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.

**Schedule:** Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click **Add New** to create a new schedule.

**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.

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

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

**Mixed 802.11n and 802.11a** - Select if you are using both 802.11n and 802.11a wireless clients.

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

**Enable Auto Channel Scan:** The **Auto Channel Scan** setting can be selected to allow the DIR-835 to choose the channel with the least amount of interference.

**Wireless Channel:** Indicates the channel setting for the DIR-835. 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.

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

**WIRELESS NETWORK SETTINGS**

**Wireless Band :** 5GHz Band

**Enable Wireless :**  Always  New Schedule

**Wireless Network Name :**  (Also called the SSID)

**802.11 Mode :**

**Enable Auto Channel Scan :**

**Wireless Channel :**

**Channel Width :**

**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 :**

**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.

**40MHz** - Select if you are using 802.11n wireless clients only.

**Visibility Status:** Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-835. If Invisible is selected, the SSID of the DIR-835 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-835 in order to connect to it.

**Wireless Security:** Refer to page 93 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.

## Router Settings

**Router 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 **Save Settings**, 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.

### NETWORK SETTINGS

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



### ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

**Router IP Address :**

**Subnet Mask :**

**Device Name :**

**Local Domain Name :**

**Enable DNS Relay :**

## DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-835 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-835. 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** Check this box to enable the DHCP server on your router.  
**Server:** 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.

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

**Always Broadcast:** Enable this feature to broadcast your networks DHCP server to LAN/WLAN clients.

**NetBIOS Announcement:** NetBIOS allows LAN hosts to discover all other computers within the network, enable this feature to allow the DHCP Server to offer NetBIOS configuration settings.

**Learn NetBIOS from WAN:** Enable this feature to allow WINS information to be learned from the WAN side, disable to allow manual configuration.

**NetBIOS Scope:** This feature allows the configuration of a NetBIOS 'domain' name under which network hosts operates. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

**DHCP SERVER SETTINGS**

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

**Enable DHCP Server :**

**DHCP IP Address Range :**  to

**DHCP Lease Time :**  (minutes)

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

**NetBIOS announcement :**

**Learn NetBIOS from WAN :**

**NetBIOS Scope :**  (Optional)

**NetBIOS node type :**  Broadcast only (use when no WINS servers configured)  
 Point-to-Point (no broadcast)  
 Mixed-mode (Broadcast then Point-to-Point)  
 Hybrid (Point-to-Point then Broadcast)

**Primary WINS IP Address :**

**Secondary WINS IP Address :**

**NetBIOS Node:** Select the different type of NetBIOS node; **Broadcast only, Point-to-Point, Mixed-mode,** and **Hybrid.**

**WINS IP** Enter your WINS IP address.

**Address:**

## 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.

**ADD DHCP RESERVATION**

**Enable :**

**Computer Name :**  << Computer Name ▾

**IP Address :**

**MAC Address :**

**DHCP RESERVATIONS LIST :**

Enable	Host Name	MAC Address	IP Address
<input type="checkbox"/>			

**NUMBER OF DYNAMIC DHCP CLIENTS : 2**

Hardware Address	Assigned IP	Hostname	Expires	
00:16:ea:61:54:76	192.168.0.106	Lifebook	Wed Aug 3 16:59:25 2011	<a href="#">Revoke</a> <a href="#">Reserve</a>
00:04:23:2c:51:a3	192.168.0.100	PM_test01	Wed Aug 3 16:10:13 2011	<a href="#">Revoke</a> <a href="#">Reserve</a>

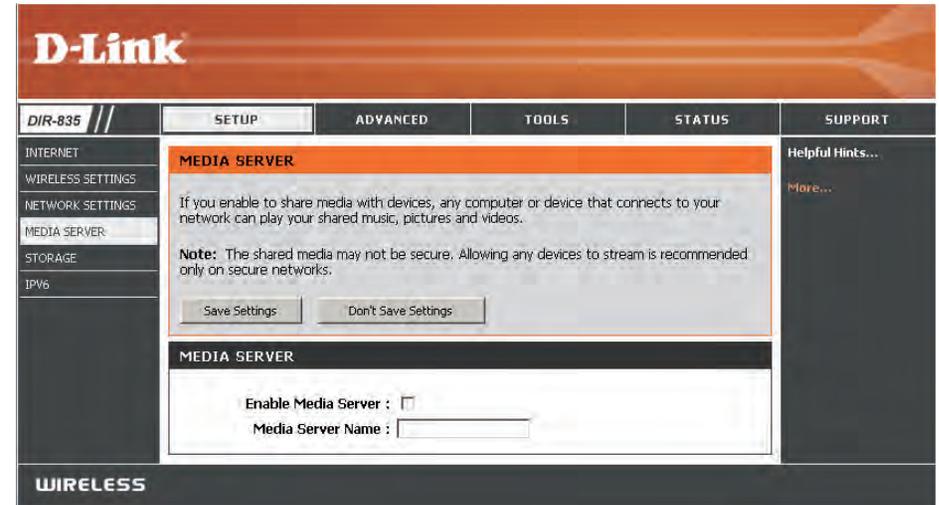
# Media Server

This feature allows you to share music, pictures and videos with any devices connected to your network.

**Enable Media Server:** Check this box to enable the media server feature.

**Computer Name:** Enter the media server's name.

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



The screenshot displays the D-Link DIR-835 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections: INTERNET, WIRELESS SETTINGS, NETWORK SETTINGS, MEDIA SERVER, STORAGE, and IPV6. The main content area is titled 'MEDIA SERVER' and contains the following text:

If you enable to share media with devices, any computer or device that connects to your network can play your shared music, pictures and videos.

**Note:** The shared media may not be secure. Allowing any devices to stream is recommended only on secure networks.

Below the text are two buttons: 'Save Settings' and 'Don't Save Settings'.

At the bottom of the main content area, there is a section titled 'MEDIA SERVER' with the following configuration options:

- Enable Media Server :
- Media Server Name :

The bottom of the interface features a 'WIRELESS' section.

# IPv6

On this page, the user can configure the IPv6 Connection type. There are two ways to set up the IPv6 Internet connection. You can use the Webbased IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

## IPv6 Internet Connection Setup Wizard

For the beginner user that has not configured a router before, click on the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.

## Manual IPv6 Internet Connection Option

For the advanced user that has configured a router before, click on the **Manual IPv6 Internet Connection Setup** button to input all the settings manually.

The screenshot displays the D-Link DIR-835 web interface. At the top, it shows 'Product Page: DIR-835', 'Hardware Version: XX', and 'Firmware Version: 1.00'. The D-Link logo is prominently displayed. Below the logo is a navigation menu with tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SETUP' tab is active, and the 'IPv6' sub-tab is selected in the left sidebar. The main content area is titled 'IPv6 INTERNET CONNECTION' and contains three sections:

- IPv6 INTERNET CONNECTION**: A text block stating, 'There are two ways to set up your IPv6 internet connection. You can use the Web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.'
- IPv6 INTERNET CONNECTION SETUP WIZARD**: A text block stating, 'If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the IPv6 Internet, click on the button below.' Below this text is a button labeled 'IPv6 Internet Connection Setup Wizard'.
- MANUAL IPv6 LOCAL CONNECTIVITY SETTINGS**: A text block stating, 'If you would like to configure IPv6 local connectivity setting of your D-Link Router, then click on the button below.' Below this text is a button labeled 'IPv6 Local Connectivity Settings'.
- MANUAL IPv6 INTERNET CONNECTION SETUP**: A text block stating, 'If you would like to configure the IPv6 Internet settings of your new D-Link Systems Router manually, then click on the button below.' Below this text is a button labeled 'Manual IPv6 Internet Connection Setup'.

On the right side of the interface, there is a 'Helpful Hints...' section with text: 'If you are new to networking and have never configured a router before, click on IPv6 Internet Connection Setup Wizard and the router will guide you through a few simple steps to get your network up and running.' Below this, it says: 'If you consider yourself an advanced user and have configured a router before, click IPv6 Local Connectivity Settings and Manual IPv6 Internet Connection Setup to input all the settings manually.' There is also a 'Hints...' link at the bottom of this section. The bottom of the page shows the 'WIRELESS' tab in the sidebar.

# IPv6 Internet Connection Setup Wizard

On this page, the user can configure the IPv6 Connection type. There are two ways to set up the IPv6 Internet connection. You can use the Web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

Click the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.

**IPv6 INTERNET CONNECTION**

There are two ways to set up your IPv6 Internet connection. You can use the Web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

**IPv6 INTERNET CONNECTION SETUP WIZARD**

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the IPv6 Internet, click on the button below.

**Note:** Before launching the wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

The wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the IPv6 Internet.

Click **Next** to continue to the next page. Click **Cancel** to discard the changes made and return to the main page.

**WELCOME TO THE D-LINK IPv6 INTERNET CONNECTION SETUP WIZARD**

This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the IPv6 Internet.

- Step 1: Configure your IPv6 Internet Connection
- Step 2: Save Settings and Connect

The router will try to detect whether its possible to obtain the IPv6 Internet connection type automatically. If this succeeds then the user will be guided through the input of the appropriate parameters for the connection type found.

However, if the automatic detection fails, the user will be prompt to either **Try again** or to click on the **Guide me through the IPv6 settings** button to initiate the manual continual of the wizard.



There are several connection types to choose from. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

**Note:** If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled. The 3 options available on this page are **IPv6 over PPPoE**, **Static IPv6 address and Route**, and **Tunneling Connection**.

Choose the required IPv6 Internet Connection type and click on the **Next** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

### IPv6 over PPPoE

After selecting the IPv6 over PPPoE option, the user will be able to configure the IPv6 Internet connection that requires a username and password to get online. Most DSL modems use this type of connection.

The following parameters will be available for configuration:

**PPPoE Session:** Select the PPPoE Session value used here. This option will state that this connection shares it's information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.

**User Name:** Enter the PPPoE username used here. If you do not know your user name, please contact your ISP.

**Password:** Enter the PPPoE password used here. If you do not know your password, please contact your ISP.

**Verify Password:** Re-enter the PPPoE password used here.

**Service Name:** Enter the service name for this connection here. This option is optional.

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

**STEP 1: CONFIGURE YOUR IPV6 INTERNET CONNECTION**

Please select your IPv6 Internet Connection type:

- IPv6 over PPPoE**  
Choose this option if your IPv6 Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Static IPv6 address and Route**  
Choose this option if your Internet Setup Provider (ISP) provided you with IPv6 Address information that has to be manually configured.
- Tunneling Connection (6rd)**  
Choose this option if your Internet Setup Provider (ISP) provided you a IPv6 Internet Connection by using 6rd automatic tunneling mechanism.

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

To set up this connection you will need to have a Username and Password from your IPv6 Internet Service Provider. If you do not have this information, please contact your ISP.

PPPoE Session :  Share with IPv4  Create a new session

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.

## Static IPv6 Address Connection

This mode is used when your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings. You must enter the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all this information.

**Use Link-Local Address:** The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.

**IPv6 Address:** Enter the WAN IPv6 address for the router here.

**Subnet Prefix Length:** Enter the WAN subnet prefix length value used here.

**Default Gateway:** Enter the WAN default gateway IPv6 address used here.

**Primary IPv6 DNS Address:** Enter the WAN primary DNS Server address used here.

**Secondary IPv6 DNS Address:** Enter the WAN secondary DNS Server address used here.

**LAN IPv6 Address:** These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

**SET STATIC IPV6 ADDRESS CONNECTION**

To set up this connection you will need to have a complete list of IPv6 information provided by your IPv6 Internet Service Provider. If you have a Static IPv6 connection and do not have this information, please contact your ISP.

Use Link-Local Address :

IPv6 Address :

Subnet Prefix Length :

Default Gateway :

Primary IPv6 DNS Address :

Secondary IPv6 DNS Address :

LAN IPv6 Address :  /64

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

### Tunneling Connection (6rd)

After selecting the Tunneling Connection (6rd) option, the user can configure the IPv6 6rd connection settings.

The following parameters will be available for configuration:

**6rd IPv6 Prefix:** Enter the 6rd IPv6 address and prefix value used here.

**IPv4 Address:** Enter the IPv4 address used here.

**Mask Length:** Enter the IPv4 mask length used here.

**Assigned IPv6 Prefix:** Displays the IPv6 assigned prefix value here.

**6rd Border Relay IPv4 Address:** Enter the 6rd border relay IPv4 address used here.

**IPv6 DNS Server:** Enter the primary DNS Server address used here.

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

The IPv6 Internet Connection Setup Wizard was completed.

Click on the **Connect** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

**SET UP 6RD TUNNELING CONNECTION**

To set up this 6rd tunneling connection you will need to have the following information from your IPv6 Internet Service Provider. If you do not have this information, please contact your ISP.

6rd IPv6 Prefix :  /

IPv4 Address :  Mask Length :

Assigned IPv6 Prefix :

6rd Border Relay IPv4 Address :

IPv6 DNS Server :

**SETUP COMPLETE!**

The IPv6 Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

# IPv6 Manual Setup

There are several connection types to choose from: Auto Detection, Static IPv6, Autoconfiguration (SLAAC/DHCPv6), PPPoE, IPv6 in IPv4 Tunnel, 6to4, 6rd, and Link-local. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

**Note:** If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.

## Auto Detection

Select **Auto Detection** to have the router detect and automatically configure your IPv6 setting from your ISP.

IPv6 CONNECTION TYPE
<p>Choose the mode to be used by the router to the IPv6 Internet.</p> <p>My IPv6 Connection is : <input type="text" value="Auto Detection"/></p>
IPv6 DNS SETTINGS
<p>Obtain a DNS server address automatically or enter a specific DNS server address.</p> <p> <input checked="" type="radio"/> Obtain a DNS server address automatically  <input type="radio"/> Use the following DNS address         </p> <p>Primary IPv6 DNS Server : <input type="text"/></p> <p>Secondary IPv6 DNS Server : <input type="text"/></p>
LAN IPv6 ADDRESS SETTINGS
<p>Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.</p> <p>Enable DHCP-PD : <input checked="" type="checkbox"/></p> <p>LAN IPv6 Address : <input type="text"/> /64</p> <p>LAN IPv6 Link-Local Address : FE80::218:E7FF:FE6A:3B54/64</p>
ADDRESS AUTOCONFIGURATION SETTINGS
<p>Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.</p> <p>Enable automatic IPv6 address assignment : <input checked="" type="checkbox"/></p> <p>Enable Automatic DHCP-PD in LAN : <input checked="" type="checkbox"/></p> <p>Autoconfiguration Type : <input type="text" value="SLAAC + Stateless DHCPv6"/></p> <p>Router Advertisement Lifetime: <input type="text" value="1440"/> (minutes)</p>

## Static IPv6

**My IPv6 Connection:** Select **Static IPv6** from the drop-down menu.

**WAN IPv6 Address Settings:** Enter the address settings supplied by your Internet provider (ISP).

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the Router's LAN Link-Local Address.

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Lifetime:** Enter the IPv6 Address Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	Static IPv6
WAN IPv6 ADDRESS SETTINGS :	
Enter the IPv6 address information provided by your Internet Service Provider (ISP).	
Use Link-Local Address :	<input checked="" type="checkbox"/>
IPv6 Address :	FE80::218:E7FF:FE6A:3847
Subnet Prefix Length :	64
Default Gateway :	
Primary DNS Address :	
Secondary DNS Address :	
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.	
LAN IPv6 Address :	/64
LAN IPv6 Link-Local Address :	FE80::218:E7FF:FE6A:3846/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable automatic IPv6 address assignment :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	Stateful DHCPv6
IPv6 Address Range (Start) :	:: /64
IPv6 Address Range (End) :	:: /64
IPv6 Address Lifetime :	1440 (minutes)

## Autoconfiguration

**My IPv6 Connection:** Select **Autoconfiguration (Stateless/DHCPv6)** from the drop-down menu.

**IPv6 DNS Settings:** Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

**Primary/Secondary DNS Address:** Enter the primary and secondary DNS server addresses.

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the Router's LAN Link-Local Address.

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Lifetime:** Enter the IPv6 Address Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	Autoconfiguration (Stateless/DHCPv6) ▾
IPv6 DNS SETTINGS :	
Obtain a DNS server address automatically or enter a specific DNS server address.	
<input checked="" type="radio"/> Obtain a DNS server address automatically <input type="radio"/> Use the following DNS address	
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.	
Enable DHCP-PD :	<input checked="" type="checkbox"/>
LAN IPv6 Address :	<input type="text"/> /64
LAN IPv6 Link-Local Address :	FE80::218:E7FF:FE6A:3846/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable automatic IPv6 address assignment :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	Stateful DHCPv6 ▾
IPv6 Address Range (Start):	<input type="text"/> :: <input type="text"/>
IPv6 Address Range (End):	<input type="text"/> :: <input type="text"/>
IPv6 Address Lifetime:	1440 (minutes)

## PPPoE

**My IPv6 Connection:** Select **PPPoE** from the drop-down menu.

**PPPoE:** Enter the PPPoE account settings supplied by your Internet provider (ISP).

**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.

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

**IPv6 DNS Settings:** Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

**Primary/Secondary DNS Address:** Enter the primary and secondary DNS server addresses.

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the Router's LAN Link-Local Address.

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**IPv6 CONNECTION TYPE**

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is :

---

**PPPOE :**

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

PPPoE Session:  Share with IPv4  Create a new session

Address Mode  Dynamic IP  Static IP

IP Address :

User Name :

Password :

Verify Password :

Service Name :  (optional)

Reconnect Mode :  Always on  On demand  Manual

Maximum Idle Time :  (minutes, 0=infinite)

MTU :  (bytes) MTU default = 1492

---

**IPv6 DNS SETTINGS :**

Enter a specific DNS server address.

Obtain a DNS server address automatically

Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

---

**LAN IPv6 ADDRESS SETTINGS :**

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

Enable DHCP-PD :

LAN IPv6 Address :  /64

LAN IPv6 Link-Local Address : FE80::218:E7FF:FE6A:3846/64

---

**ADDRESS AUTOCONFIGURATION SETTINGS**

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful (DHCPv6)

IPv6 Address Range(Start):  :

IPv6 Address Range(End):  :

IPv6 Address Lifetime:  (minutes)

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Lifetime:** Enter the IPv6 Address Lifetime (in minutes).

## IPv6 in IPv4 Tunneling

**My IPv6 Connection:** Select **IPv6 in IPv4 Tunnel** from the drop-down menu.

**IPv6 in IPv4 Tunnel Settings:** Enter the settings supplied by your Internet provider (ISP).

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the Router's LAN Link-Local Address.

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 Address for the DHCPv6 range for your local computers.

**Pv6 Address Lifetime:** Enter the Router Advertisement Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	IPv6 in IPv4 Tunnel ▾
IPv6 in IPv4 TUNNEL SETTINGS :	
Enter the IPv6 in IPv4 Tunnel information provided by your Tunnel Broker.	
Remote IPv4 Address :	<input type="text"/>
Remote IPv6 Address :	<input type="text"/>
Local IPv4 Address :	<input type="text"/>
Local IPv6 Address :	<input type="text"/>
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.	
LAN IPv6 Address :	<input type="text"/> /64
LAN IPv6 Link-Local Address :	FE80::240:F4FF:FE03:1A9C/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable Autoconfiguration :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	Stateful (DHCPv6) ▾
IPv6 Address Range(Start):	<input type="text"/> : <input type="text"/>
IPv6 Address Range(End):	<input type="text"/> : <input type="text"/>
IPv6 Address Lifetime:	30 <input type="text"/> (minutes)

## 6 to 4 Tunneling

**My IPv6 Connection:** Select **6 to 4** from the drop-down menu.

**6 to 4 Settings:** Enter the IPv6 settings supplied by your Internet provider (ISP).

**Primary/Secondary DNS Address:** Enter the primary and secondary DNS server addresses.

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the Router's LAN Link-Local Address.

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Lifetime:** Enter the IPv6 Address Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	6 to 4 Tunnel
IPv6 in IPv4 TUNNEL SETTINGS :	
Enter the IPv6 in IPv4 Tunnel information provided by your Tunnel Broker.	
Remote IPv4 Address :	<input type="text"/>
Remote IPv6 Address :	<input type="text"/>
Local IPv4 Address :	0.0.0.0
Local IPv6 Address :	<input type="text"/>
IPv6 DNS SETTINGS :	
Obtain a DNS server address automatically or enter a specific DNS server address.	
<input checked="" type="radio"/> Obtain a DNS server address automatically <input type="radio"/> Use the following DNS address	
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.	
Enable DHCP-PD :	<input checked="" type="checkbox"/>
LAN IPv6 Address :	<input type="text"/> /64
LAN IPv6 Link-Local Address :	FE80::218:E7FF:FE6A:3846/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable automatic IPv6 address assignment :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	Stateful DHCPv6
IPv6 Address Range (Start) :	<input type="text"/> :: <input type="text"/>
Stateful DHCPv6 :	<input type="text"/> :: <input type="text"/>
IPv6 Address Lifetime :	1440 (minutes)

## 6rd

**My IPv6 Connection:** Select **6rd** from the drop-down menu.

**6RD Settings:** Enter the address settings supplied by your Internet provider (ISP).

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the Router's LAN Link-Local Address.

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC+RDNSS** or **SLAAC + Stateless DHCPv6**.

**Router Advertisement Lifetime:** Enter the Router Advertisement Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	6rd
6RD SETTINGS :	
Enter the IPv6 address information provided by your Internet Service Provider (ISP).	
6rd IPv6 Prefix :	/ 32
IPv4 Address	0.0.0.0 Mask Length : 0
Assign IPv6 Prefix :	None
Tunnel Link-Local Address :	FE80::0000:0000/64
6rd Border Relay IPv4 Address :	
Primary DNS Address :	
Secondary DNS Address :	
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.	
LAN IPv6 Address :	None
LAN IPv6 Link-Local Address :	FE80::218:E7FF:FE6A:3846/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable automatic IPv6 address assignment :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	Stateless
Router Advertisement Lifetime:	1440 (minutes)

## Link-Local Connectivity

**My IPv6 Connection:** Select **Link-Local Only** from the drop-down menu.

**LAN IPv6 Address Settings:** Displays the IPv6 address of the router.

The screenshot shows a web-based configuration interface for IPv6 settings. It is divided into three main sections:

- IPv6:** An orange header section containing a grey box with instructions: "Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider." Below this are two buttons: "Save Settings" and "Don't Save Settings".
- IPv6 CONNECTION TYPE:** A dark grey header section containing the instruction "Choose the mode to be used by the router to the IPv6 Internet." Below this is a label "My IPv6 Connection is :" followed by a dropdown menu currently set to "Link-local only".
- LAN IPv6 ADDRESS SETTINGS :** A dark grey header section containing the instruction "Use this section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface." Below this is the text "LAN IPv6 Link-Local Address : FE80::218:E7FF:FE6A:3B46/64".

# Advanced Virtual Server

The DIR-835 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-835 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-835 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-835 redirects the external service request to the appropriate server within the LAN network.

The DIR-835 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 the next page.

**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), you 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.

**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.

**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.

**D-Link**

DIR-835 // 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	IP Address	Computer Name	Port	Traffic Type	Schedule	Inbound Filter
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Public Port 0	Protocol TCP	Schedule Always	Inbound Filter Allow All
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Private Port 0	Protocol TCP	Schedule Always	Inbound Filter Allow All
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Public Port 0	Protocol TCP	Schedule Always	Inbound Filter Allow All
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Private Port 0	Protocol TCP	Schedule Always	Inbound Filter Allow All
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Public Port 0	Protocol TCP	Schedule Always	Inbound Filter Allow All
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Private Port 0	Protocol TCP	Schedule Always	Inbound Filter Allow All
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Public Port 0	Protocol TCP	Schedule Always	Inbound Filter Allow All
<input type="checkbox"/>		<< Application Name	0.0.0.0	<< Computer Name	Private Port 0	Protocol TCP	Schedule Always	Inbound Filter 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

**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.

**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.

**D-Link**

DIR-835 // SETUP ADVANCED TOOLS STATUS SUPPORT

**PORT FORWARDING RULES :**

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 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	TCP 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	TCP 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP 0	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-835. 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-835 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.

**D-Link**

DIR-835 // 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"/>	<input type="text"/>	<< Application Name	Trigger <input type="text"/>	TCP	Always
			Firewall <input type="text"/>	TCP	
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger <input type="text"/>	TCP	Always
			Firewall <input type="text"/>	TCP	
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger <input type="text"/>	TCP	Always
			Firewall <input type="text"/>	TCP	
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger <input type="text"/>	TCP	Always
			Firewall <input type="text"/>	TCP	

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

**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, 1.5Mbits/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 Network Type:** When Connection Type is set to automatic, the automatically detected connection type is displayed here. This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

The screenshot shows the D-Link DIR-835 configuration interface. The 'QoS ENGINE' section is active, showing the following settings:

- QoS Engine:** Use this section to configure D-Link's QoS Engine powered by QoS Engine™ Technology. This 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** buttons.
- WAN TRAFFIC SHAPING:**
  - Enable Traffic Shaping:
  - Automatic Uplink Speed:
  - Measured Uplink Speed: Not Estimated
  - Manual Uplink Speed: 128 kbps << 128 kbps
  - Connection Type: Auto-detect
  - Detected Network type: Not detected
- QoS ENGINE SETUP:**
  - Enable QoS Engine:
  - Automatic Classification:
  - Dynamic Fragmentation:
- 10 -- QoS ENGINE RULES:**

Name	Priority	Protocol
	1 (1..255)	6 << TCP
<input type="checkbox"/> Local IP Range		Local Port Range
0.0.0.0 to 255.255.255.255		0 to 65535
Remote IP Range		Remote Port Range
0.0.0.0 to 255.255.255.255		0 to 65535

**Enable QoS Engine:** This option is enabled by default. This will allow your router to automatically determine the network priority of running programs.

**Automatic Classification:** 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.

# 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.

**Clear:** Click to remove the MAC address.

**D-Link**

DIR-835 // 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	
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	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

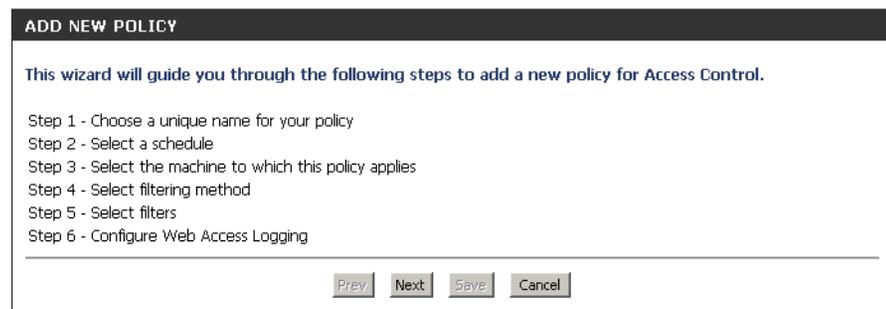
The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

**Add Policy:** Click the **Add Policy** button to start the Access Control Wizard.



## Access Control Wizard

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



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

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

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.
- **Machine Address** - Enter the PC MAC address (i.e. 00:00.00.00.00).

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

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.

To enable web logging, click **Enable**.

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

Your newly created policy will now show up under **Policy Table**.

Enable Policy	Machine	Filtering	Logged	Schedule			
<input checked="" type="checkbox"/>	dlink	192.168.0.106	Block Some Access	No	Always		

## Website Filters

Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section (page 45).

**Add Website** Select **Allow** or **Deny**.  
**Filtering Rule:**

**Website URL/** Enter the keywords or URLs that you want to allow  
**Domain:** or block. Click **Save Settings**.

The screenshot displays the D-Link DIR-835 web interface. The top navigation bar includes 'D-Link', 'DIR-835 //', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'WEBSITE FILTER' selected. The main content area is titled 'WEBSITE FILTER' and contains the following text: 'The Website Filter option allows you to set up a list of Web sites you would like to allow or deny through your network. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.' Below this text are three buttons: 'Save Settings', 'Don't Save Settings', and 'Reboot Now'. A section titled '40 - WEBSITE FILTERING RULES' contains the text 'Configure Website Filter below:' followed by a dropdown menu set to 'DENY computers access to ONLY these sites'. A 'Clear the list below...' button is also present. At the bottom, there is a table with the header 'Website URL/Domain' and four rows of input fields. The right sidebar contains 'Helpful Hints...' with instructions: 'Create a list of Web Sites to which you would like to deny or allow through the network. Use with 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.

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

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

**Add:** Click the **Add** 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.

**D-Link**

DIR-835 // 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. [Reboot Now](#)

**ADD INBOUND FILTER RULE**

Name :

Action :

Remote IP Range	Enable	Remote IP Start	Remote IP End
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>

[Add](#) [Clear](#)

**INBOUND FILTER RULES LIST**

Name	Action	Remote 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 DIR-835 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.

**Anti-Spoof Check:** Enable this feature to protect your network from certain kinds of "spoofing" attacks.

**Enable DMZ:** 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.

**DMZ 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 **Setup > Network Settings** page so that the IP address of the DMZ machine does not change.

The screenshot displays the D-Link DIR-835 web interface for Firewall Settings. The left sidebar contains a navigation menu with options like Virtual Server, Port Forwarding, Application Rules, QoS Engine, Network Filter, Access Control, Website Filter, Inbound Filter, Firewall Settings (selected), Routing, Advanced Wireless, Wi-Fi Protected Setup, Advanced Network, Guest Zone, IPv6 Firewall, and IPv6 Routing. The main content area is titled 'FIREWALL SETTINGS' and includes a 'Helpful Hints...' section on the right. The 'FIREWALL SETTINGS' section contains an 'Enable SPI' checkbox. The 'NAT ENDPOINT FILTERING' section has radio buttons for 'Endpoint Independent', 'Address Restricted', and 'Port And Address Restricted' for both UDP and TCP. The 'ANTI-SPOOF CHECKING' section has an 'Enable anti-spoof checking' checkbox. The 'DMZ HOST' section includes an 'Enable DMZ Host' checkbox and a 'DMZ IP Address' field with a dropdown for 'Computer Name'. The 'APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION' section has checkboxes for PPTP, IPsec (VPN), RTSP, and SIP, all of which are checked.

# Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

**Destination IP:** Enter the IP address of packets that will take this route.

**Netmask:** Enter the netmask of the route, please note that the octets must match your destination IP address.

**Gateway:** Enter your next hop gateway to be taken if this route is used.

**Metric:** The route metric is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

**Interface:** Select the interface that the IP packet must use to transit out of the router when this route is used.

**D-Link**

DIR-835 // SETUP **ADVANCED** TOOLS STATUS SUPPORT

**ROUTING :**

This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings Don't Save Settings Reboot Now

**32 --ROUTE LIST**

Name	Destination IP	Netmask	Gateway	Metric	Interface
<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>
<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>
<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>
<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>

**Helpful Hints..**

Each route has a check box next to it, check this box if you want the route to be enabled.

The name field allows you to specify a name for identification of this route, e.g. "Network 2"

The destination IP address is the address of the host or network you wish to reach.

The netmask field identifies the portion of the destination IP in use.

The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

More...

# Advanced Wireless

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

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

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

**HT20/40 Coexistence:** Select to Enable or Disable this feature.

**D-Link**

DIR-835 // 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**

Wireless Band : 2.4GHz  
 Transmit Power : High  
 WLAN Partition :   
 WMM Enable :   
 Short GI :   
 HT20/40 Coexistence :  Enable  Disable

**ADVANCED WIRELESS SETTINGS**

Wireless Band : 5GHz  
 Transmit Power : High  
 WLAN Partition :   
 WMM Enable :   
 Short GI :

**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**

# Advanced Wireless Settings

## 802.11n/g (2.4GHz)

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

**WLAN Partition:** Enable this option to prevent associated wireless clients from communicating with each other.

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

**ADVANCED WIRELESS SETTINGS**

Wireless Band : 2.4GHz

Transmit Power : High

WLAN Partition :

WMM Enable :

Short GI :

HT20/40 Coexistence :  Enable  Disable

**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.

**HT20/40 Coexistence:** Select to Enable or Disable this feature.

## Advanced Wireless Settings 802.11n/a (5GHz)

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

**WLAN Partition:** Enable this option to prevent associated wireless clients from communicating with each other.

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

**ADVANCED WIRELESS SETTINGS**

Wireless Band : 5GHz

Transmit Power : High ▼

WLAN Partition :

WMM Enable :

Short GI :

**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.

## Wi-Fi Protected Setup (WPS)

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 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 PIN becomes the router’s PIN. You can then copy this PIN to the user interface of the registrar.

The screenshot displays the D-Link DIR-835 router's web interface. The main content area is titled "WI-FI PROTECTED SETUP". It includes a "Save Settings" button and a "Don't Save Settings" button. Below this, there are two sections: "WI-FI PROTECTED SETUP" and "PIN SETTINGS". In the "WI-FI PROTECTED SETUP" section, the "Enable" checkbox is checked, and the "Lock Wireless Security Settings" checkbox is unchecked. A "Reset to Unconfigured" button is present. In the "PIN SETTINGS" section, the "Current PIN" is displayed as 56759518, with buttons for "Generate New PIN" and "Reset PIN to Default". Below this is the "ADD WIRELESS STATION" section, which contains a button labeled "Add Wireless Device with WPS". On the right side of the interface, there are "Helpful Hints" and a "More..." link.

**Add Wireless Station:** This Wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

**Add Wireless Device Wizard:** Start the wizard.

# Advanced Network Settings

**Enable UPnP:** To use the Universal Plug and Play (UPnP™) feature click on **Enabled**. UPnP provides compatibility with networking equipment, software and peripherals.

**WAN Ping:** Unchecking the box will not allow the DIR-835 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be “pinged”.

**WAN Ping Inbound Filter:** Select from the drop-down menu if you would like to apply the Inbound Filter to the WAN ping. Refer to page 47 for more information regarding Inbound Filter.

**WAN Port Speed:** You may set the port speed of the Internet port to 10Mbps, 100Mbps, or auto. Some older cable or DSL modems may require you to set the port speed to 10Mbps.

**Multicast streams:** Check the box to allow multicast traffic to pass through the router from the Internet.

**Enable IPV6** Check the box to allow IPv6 multicast traffic.

**Multicast Streams:**

The screenshot displays the 'Advanced Network' configuration page for a D-Link DIR-835 router. The page is organized into several sections:

- ADVANCED NETWORK:** A warning message states, "If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings." Below this are 'Save Settings' and 'Don't Save Settings' buttons.
- UPNP:** A section titled 'Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.' It includes a checked checkbox for 'Enable UPnP'.
- WAN PING:** A section titled 'If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.' It contains:
  - 'Enable WAN Ping Respond': unchecked checkbox.
  - 'WAN Ping Inbound Filter': a dropdown menu set to 'Allow All'.
  - 'Details': a text input field containing 'Allow\_All'.
- WAN PORT SPEED:** A section with a dropdown menu for 'WAN Port Speed' set to 'Auto'.
- IPv4 MULTICAST STREAMS:** A section with an unchecked checkbox for 'Enable IPv4 Multicast Streams'.
- IPv6 MULTICAST STREAMS:** A section with a checked checkbox for 'Enable IPv6 Multicast Streams'.

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

UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.

For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

The WAN speed is usually detected automatically. If you are having problems connecting to the WAN, try selecting the speed manually.

If you are having trouble receiving multicast streams from the Internet, make sure the Multicast Streams option is enabled.

At the bottom of the page, there is a 'Home...' link.

## Guest Zone

The Guest Zone feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network. You may configure different zones for the 2.4GHz and 5.0GHz wireless bands.

**Enable Guest Zone:** Check to enable the Guest Zone feature.

**Schedule:** The schedule of time when the Guest Zone will be active. 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.

**Wireless Network Name:** Enter a wireless network name (SSID) that is different from your main wireless network.

**Enable Routing Between Zones:** Check to allow network connectivity between the different zones created.

**Security Mode:** Select the type of security or encryption you would like to enable for the guest zone.

**D-Link**

DIR-835

SETUP ADVANCED TOOLS STATUS SUPPORT

**GUEST ZONE**

Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.

Save Settings Don't Save Settings Reboot Now

**GUEST ZONE SELECTION**

Enable Guest Zone :  Always

Wireless Band : 2.4GHz Band

Wireless Network Name : dlink\_guest (Also called the SSID)

Enable Routing Between Zones :

Security Mode : None

**GUEST ZONE SELECTION**

Enable Guest Zone :  Always

Wireless Band : 5GHz Band

Wireless Network Name : dlink\_media\_guest (Also called the SSID)

Enable Routing Between Zones :

Security Mode : None

Helpful Hints...  
Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.  
More...

# IPv6 Firewall

The DIR-835's IPv6 Firewall feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-835's IPv6 Firewall functions in a similar way to the IP Filters feature.

**Enable Checkbox:** Check the box to enable the IPv6 firewall simple security.

**Name:** Enter a name to identify the IPv6 firewall rule.

**Action:** Use the radio buttons to *Allow* or *Deny* transport of the IPv6 data packets according to the criteria defined in the firewall rule.

**Source:** Use the **Source** drop-down menu to specify the interface that connects to the source IPv6 addresses of the firewall rule.

**IP Address Range:** Enter the source IPv6 address range in the adjacent **IP Address Range** field.

**Dest:** Use the **Dest** drop-down menu to specify the interface that connects to the destination IP addresses of the firewall rule.

**Select Schedule:** Use the drop-down menu to select the time schedule that the IPv6 Firewall Rule will be enabled on. 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.

**Protocol:** Select the protocol of the firewall port (All, TCP, UDP, or ICMP).

**Port Range:** Enter the first port of the range that will be used for the firewall rule in the top port range field and enter the last port in the field underneath.

Click the **Save Settings** button to save any changes made.

**D-Link**

DIR-835 // SETUP ADVANCED TOOLS STATUS SUPPORT

**IPV6 FIREWALL**

The Firewall settings section is an advance feature used to allow or deny traffic from passing through the device. It works in the same way as IP Filters with additional settings. You can create more detailed rules for the device.

Save Settings Don't Save Settings Reboot Now

**IPV6 SIMPLE SECURITY**

Enable IPv6 Simple Security:

**IPV6 FIREWALL**

Configure IPv6 Firewall below:  
Turn IPv6 Firewall OFF

Remaining number of firewall rules that can be configured:

	Name	Schedule	Interface	IP Address Range	Protocol	Port Range
1.		Always	*		TCP	1 ~ 65535
			Source			
			Dest			
2.		Always	*		TCP	1 ~ 65535
			Source			
			Dest			
3.		Always	*		TCP	1 ~ 65535
			Source			
			Dest			

**Helpful Hints...**

For each rule you can create a name and control the direction of traffic. You can also allow or deny a range of IP Addresses, the protocol and a port range.

In order to apply a schedule to a firewall rule, you must first define a schedule on the [Tools → Schedules](#) page.

[More...](#)

# IPv6 Routing

This page allows you to specify custom routes that determine how data is moved around your network.

**Route List:** Check the box next to the route you wish to enable.

**Name:** Enter a specific name to identify this route.

**Destination IP:** Enter the host or network address you wish to reach.

**Gateway IP:** This is the IP address of the router used to reach the specified destination.

Product Page: DIR-835 Hardware Version: XX Firmware Version: 1.00

**D-Link**

DIR-835 // SETUP ADVANCED TOOLS STATUS SUPPORT

**IPV6 ROUTING**

This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings Don't Save Settings

ROUTE LIST			
<input type="checkbox"/>	Name	Destination IP/Prefix Length	/64
<input type="checkbox"/>	Metric	Interface	Gateway
1	NULL		
<input type="checkbox"/>	Name	Destination IP/Prefix Length	/64
<input type="checkbox"/>	Metric	Interface	Gateway
1	NULL		
<input type="checkbox"/>	Name	Destination IP/Prefix Length	/64
<input type="checkbox"/>	Metric	Interface	Gateway
1	NULL		

**Helpful Hints...**

Each route has a check box next to it, check this box if you want the route to be enabled.

The name field allows you to specify a name for identification of this route, e.g. "Network 2".

The destination IP address is the address of the host or network you wish to reach.

The netmask field identifies the portion of the destination IP in use.

The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

[More...](#)

# Tools Admin

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

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

**User Password:** Enter the new password for the User login. If you login as the User, you cannot change the settings (you can only view them). Enter a name for the DIR-835 router.

**Gateway Name:** Enter a name for the router.

**Enable Graphical Authentication:** Enables a challenge-response test to require users to type letters or numbers from a distorted image displayed on the screen to prevent online hackers and unauthorized users from gaining access to your router's network settings.

**Enable HTTPS Server:** Check to enable HTTPS to connect to the router securely.

**Enable Remote Management:** Remote management allows the DIR-835 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host. The port number used to access the DIR-835.

Example: `http://x.x.x.x:8080` whereas x.x.x.x is the Internet IP address of the DIR-835 and 8080 is the port used for the Web Management interface.

**Remote Admin Inbound Filter:** If you have enabled **HTTPS Server** and checked **Use HTTPS**, you must enter **https://** as part of the URL to access the router remotely.

**Details:** 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.

The screenshot shows the D-Link DIR-835 web management interface. The top navigation bar includes 'DIR-835', 'SETUP', 'ADVANCED', 'TOOLS' (selected), 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration categories like ADMIN, TIME, SYSLOG, etc. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains several sections:

- ADMINISTRATOR SETTINGS:** A text box explaining that the 'admin' account has read/write access and can change passwords, while the 'user' account has read-only access. Below this are 'Save Settings' and 'Don't Save Settings' buttons.
- ADMIN PASSWORD:** A section for setting the administrator password, with fields for 'Password' and 'Verify Password'.
- USER PASSWORD:** A section for setting the user password, with fields for 'Password' and 'Verify Password'.
- SYSTEM NAME:** A section for setting the 'Gateway Name', which is currently 'DIR-835'.
- ADMINISTRATION:** A section with several checkboxes and input fields:
  - Enable Graphical Authentication:
  - Enable HTTPS Server:
  - Enable Remote Management:
  - Remote Admin Port: 8080
  - Use HTTPS:
  - Remote Admin Inbound Filter: Allow All
  - Details: Allow All

On the right side, there are 'Helpful Hints...' and 'More...' sections providing additional information and instructions.

# Time

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

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

**Daylight Saving:** To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

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

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

**Manual:** To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Set Time**. You can also click **Copy Your Computer's Time Settings**.

The screenshot shows the D-Link DIR-835 web interface. The top navigation bar includes 'DIR-835', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists 'ADMIN', 'TIME', 'SYSLOG', 'EMAIL SETTINGS', 'SYSTEM', 'FIRMWARE', 'DYNAMIC DNS', 'SYSTEM CHECK', and 'SCHEDULES'. The main content area is titled 'TIME' and contains the following sections:

- TIME CONFIGURATION:**
  - Time: Tuesday, August 02, 2011 6:42:49 PM
  - Time Zone: [(GMT-08:00) Pacific Time (US/Canada), Tijuana]
  - Enable Daylight Saving:
  - Daylight Saving Dates: DST Start (Mar 3rd Sun 1 am), DST End (Nov 2nd Sun 1 am)
- AUTOMATIC TIME CONFIGURATION:**
  - Enable NTP Server:
  - NTP Server Used: [ ] << [ Select NTP Server ] >>
- SET THE DATE AND TIME MANUALLY:**
  - Date And Time: Year (2011), Month (Aug), Day (2), Hour (06), Minute (42), Second (45), PM
  - Copy Your Computer's Time Settings

The right sidebar contains 'Helpful Hints...' with the text: 'Good timekeeping is important for accurate logs and scheduled firewall rules. More...'

# SysLog

The Broadband Router keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network.

**Enable Logging to SysLog Server:** Check this box to send the router logs to a SysLog Server.

**SysLog Server IP Address:** The address of the SysLog server that will be used to send the logs. You may also select your computer from the drop-down menu (only if receiving an IP address from the router via DHCP).

The screenshot displays the D-Link DIR-835 web interface. The top navigation bar includes 'D-Link' and tabs for 'DIR-835', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists menu items: ADMIN, TIME, SYSLOG (selected), EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSLOG' and contains the following text: 'The SysLog options allow you to send log information to a SysLog Server.' Below this text are three buttons: 'Save Settings', 'Don't Save Settings', and 'Reboot Now'. Underneath is a section titled 'SYSLOG SETTINGS' with a checkbox labeled 'Enable Logging To Syslog Server' which is currently unchecked. A large empty text input field is positioned below the checkbox. On the right side of the interface, there is a 'Helpful Hints...' section with text explaining that a System Logger (syslog) is a server that collects logs from different sources and that the LAN includes a syslog server. A 'More...' link is located at the bottom of this section. The footer of the page features the 'WIRELESS' logo.

# Email Settings

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

**Enable Email Notification:** When this option is enabled, router activity logs are emailed to a designated email address.

**From Email Address:** This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

**To Email Address:** Enter the email address where you want the email sent.

**SMTP Server Address:** Enter the SMTP server address for sending email. If your SMTP server requires authentication, select this option.

**Enable Authentication:** Check this box if your SMTP server requires authentication.

**Account Name:** Enter your account for sending email.

**Password:** Enter the password associated with the account. Re-type the password associated with the account.

**On Log Full:** When this option is selected, logs will be sent via email to your account when the log is full.

**On Schedule:** Selecting this option will send the logs via email according to schedule.

**Schedule:** This option is enabled when **On Schedule** is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to **Tools > Schedules**.

The screenshot displays the D-Link DIR-835 web interface for configuring email settings. The main content area is titled "EMAIL SETTINGS" and contains the following sections:

- EMAIL NOTIFICATION:** A checkbox labeled "Enable Email Notification" is currently unchecked.
- EMAIL SETTINGS:** A series of input fields for configuring email parameters:
  - From Email Address: [Empty text box]
  - To Email Address: [Empty text box]
  - SMTP Server Address: [Empty text box]
  - SMTP Server Port: [25]
  - Enable Authentication: [Unchecked checkbox]
  - Account Name: [User]
  - Password: [Masked with asterisks]
  - Verify Password: [Masked with asterisks]
- EMAIL LOG WHEN FULL OR ON SCHEDULE:**
  - On Log Full: [Unchecked checkbox]
  - On Schedule: [Unchecked checkbox]
  - Schedule: [Never (dropdown menu)]
  - Details: [Never (dropdown menu)]

The interface also features a left-hand navigation menu with options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS (highlighted), SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The top navigation bar includes SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The bottom navigation bar includes WIRELESS. A "Helpful Hints..." section on the right provides additional information about email settings.

# System

This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

**Save Settings to Local Hard Drive:** Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. A file dialog will appear, allowing you to select a location and file name for the settings.

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

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

**Reboot Device:** Click to reboot the router.

# Firmware

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

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

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

## Language Pack

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

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

The screenshot displays the D-Link DIR-835 web management interface. The top navigation bar includes 'DIR-835 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. A left sidebar lists menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE (highlighted), DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'FIRMWARE UPDATE' and contains the following text:

There may be new firmware for your DIR-835 to improve functionality and performance.

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button below to start the firmware upgrade.

The language pack allows you to change the language of the user interface on the DIR-835. We suggest that you upgrade your current language pack if you upgrade the firmware. This ensures that any changes in the firmware are displayed correctly.

To upgrade the language pack, locate the upgrade file on the local hard drive with Browse button. Once you have found the file to be used, click the Upload button to start the language pack upgrade.

**FIRMWARE AND LANGUAGE PACK INFORMATION**

Current Firmware Version : 1.00    Date : 09 Sep 2011  
 Current Language Pack Version: No Language Pack  
 Check Online Now for Latest Firmware and Language pack version:

**FIRMWARE UPGRADE**

**Note:** Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the [Tools → System](#) screen.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

**LANGUAGE PACK UPGRADE**

Upload :

The bottom of the page features a 'WIRELESS' logo.

# Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.

**Enable Dynamic DNS:** Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.

**Server Address:** Choose your DDNS provider from the drop down menu.

**Host Name:** Enter the Host Name that you registered with your DDNS service provider.

**Username or Key:** Enter the Username for your DDNS account.

**Password or Key:** Enter the Password for your DDNS account.

**Timeout:** Enter a time (in hours).

**Status:** Displays the current connection status.

## DDNS for IPv6 Hosts

**Enable:** Check the box to enable DDNS for IPv6 Hosts.

**IPv6 Address:** Enter the IPv6 address of your computer/server in your local network. You can click the << button and select a computer/server from the drop-down list.

**D-Link**

DIR-835 // SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN  
TIME  
SYSLOG  
EMAIL SETTINGS  
SYSTEM  
FIRMWARE  
DYNAMIC DNS  
SYSTEM CHECK  
SCHEDULES

**DYNAMIC DNS**

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at [www.DLinkDDNS.com](http://www.DLinkDDNS.com).

Save Settings Don't Save Settings Reboot Now

**DYNAMIC DNS SETTINGS**

Enable Dynamic DNS :

Server Address :  << Select Dynamic DNS Server

Host Name :

Username or Key :

Password or Key :

Verify Password or Key :

Timeout : 576 (hours)

Status : Disconnected

**DYNAMIC DNS FOR IPV6 HOSTS**

Enable:

IPv6 Address:  << Computer Name

Host Name:  (e.g.: ipv6.mydomain.net)

Save Clear

**IPV6 DYNAMIC DNS LIST**

Enable	Host Name	IPv6 Address
<input type="checkbox"/>		

WIRELESS

Helpful Hints...  
To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu.  
More...

**Host Name:** Enter the IPv6 Host Name that you registered with your DDNS service provider.

**IPv6 DDNS List:** Once you save your entry, the IPv6 DDNS host information will be displayed here.

**Enable:** Check to enable the entry.

**Host Name:** Displays the name of your IPv6 DDNS host.

**IPv6 Address:** Displays the IPv6 address of your computer/server associated with the IPv6 DDNS host.

**Edit/Delete:** Click the edit icon to make changes to the entry or click the delete icon to remove the entry.

# System Check

**Ping Test:** The Ping Test is used to send Ping packets to test if a computer is on the Internet. Enter the IP Address that you wish to Ping, and click **Ping**.

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

The screenshot displays the D-Link DIR-835 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various system settings, with SYSTEM CHECK highlighted. The main content area is titled 'PING TEST' and contains the following sections:

- PING TEST**: A header section with a description: "Ping Test sends 'ping' packets to test a computer on the Internet."
- PING TEST**: A form with a text input field labeled "Host Name or IP Address :" and a "ping" button.
- IPV6 PING TEST**: A form with a text input field labeled "Host Name or IPV6 Address:" and a "ping" button.
- PING RESULT**: A section with a text input field and a "ping" button, with the instruction "Enter a host name or IP address above and click 'Ping'".

On the right side, there is a "Helpful Hints..." section with the text: "Ping checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name." and a "More..." link.

The bottom of the interface features a "WIRELESS" section.

# Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

**Name:** Enter a name for your new schedule.

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

**Time:** Check **All Day - 24hrs** or enter a start and end time for your schedule.

**Save:** You must click **Save Settings** at the top for your schedules to go into effect.

**Schedule Rules** The list of schedules will be listed here. Click the **List:** **Edit** icon to make changes or click the **Delete** icon to remove the schedule.

The screenshot shows the D-Link DIR-835 web interface. The top navigation bar includes 'DIR-835 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration categories: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SCHEDULES' and contains the following text: 'The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.' Below this text are three buttons: 'Save Settings', 'Don't Save Settings', and 'Reboot Now'. The '10 - ADD SCHEDULE RULE' section contains the following form fields:

- Name :** [Text input field]
- Day(s) :**  All Week  Select Day(s)
- Sun  Mon  Tue  Wed  Thu  Fri  Sat
- All Day - 24 hrs :**
- Time Format :** [24-hour dropdown menu]
- Start Time :** [00] : [00] [AM/PM dropdown] (hour minute)
- End Time :** [00] : [00] [AM/PM dropdown] (hour minute)

Below the form is the 'SCHEDULE RULES LIST' section, which is currently empty. The table has the following columns: Name, Day(s), and Schedule Rules List. On the right side of the interface, there is a 'Helpful Hints...' sidebar with the following text:

**Helpful Hints...**

Schedules are used with a number of other features to define when those features are in effect.

Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

Click **Save** to add a completed schedule to the list below.

Click the **Edit** icon to change an existing schedule.

Click the **Delete** icon to permanently delete a schedule.

[More...](#)

# Status

## Device Info

This page displays the current information for the DIR-835. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

**General:** Displays the router's time and firmware version.

**WAN:** Displays the MAC address and the public IP settings

**LAN:** Displays the MAC address and the private (local) IP settings for the router.

**Wireless LAN:** Displays the wireless MAC address and your wireless settings such as SSID and Channel.

**LAN Computers:** Displays computers and devices that are connected to the router via Ethernet and that are receiving an IP address assigned by the router (DHCP).

The screenshot shows the D-Link DIR-835 web interface. The top navigation bar includes 'Product Page: DIR-835', 'Hardware Version: X3', and 'Firmware Version: 1.00'. The main menu has tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'STATUS' tab is selected, and the 'DEVICE INFO' sub-tab is active. The page displays the following information:

- GENERAL:**
  - Time: Friday, August 12, 2011 7:29:58 PM
  - Firmware Version: 1.00, 12, Aug, 2011
- WAN:**
  - Connection Type: DHCP Client
  - Cable Status: Disconnected
  - Network Status: Disconnected
  - Connection Up Time: N/A
  - MAC Address: 00:01:23:45:67:89
  - IP Address: 0.0.0.0
  - Subnet Mask: 0.0.0.0
  - Default Gateway: 0.0.0.0
  - Primary DNS Server: 0.0.0.0
  - Secondary DNS Server: 0.0.0.0
  - Advanced DNS: Disabled
- LAN:**
  - MAC Address: 00:01:23:45:67:89
  - IP Address: 192.168.0.1
  - Subnet Mask: 255.255.255.0
  - DHCP Server: Enabled
- WIRELESS LAN:**
  - Wireless Band: 2.4GHz Band
  - Wireless Radio: Enabled
  - 802.11 Mode: Mixed 802.11n, 802.11g and 802.11b
  - Channel Width: Auto 20/40 Mhz
  - Channel: 11
  - Wi-Fi Protected Setup: Enabled/Not Configured
  - SSID List:
 

Network Name (SSID)	Guest	MAC Address	Security Mode
dir_835	No	00:01:23:45:67:89	Disabled
- WIRELESS LAN:**
  - Wireless Band: 5GHz Band
  - Wireless Radio: Enabled
  - 802.11 Mode: 11n
  - Channel Width: Auto 20/40 Mhz
  - Channel: 32
  - Wi-Fi Protected Setup: Enabled/Not Configured
  - SSID List:
 

Network Name (SSID)	Guest	MAC Address	Security Mode
dir_835a	No	00:01:23:45:67:89	Disabled
- LAN COMPUTERS:**

IP Address	Name (if any)	MAC
192.168.0.100	zen-4200a504	00:18:2D:95:4E:49
192.168.0.101	Hsiv-P9d	94:67:06:13:20:76
- IGMP MULTICAST MEMBERSHIPS:**

MULTICAST Group Address

# Logs

The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

**Log Options:** You can select the types of messages that you want to display from the log. System Activity, Debug Information, Attacks, Dropped Packets, and Notice messages can be selected. Click **Apply Log Settings Now** to activate your settings.

**Refresh:** Updates the log details on the screen so it displays any recent activity.

**Clear:** Clears all of the log contents.

**Email Now:** This option will send a copy of the router log to your email address configured in the Tools > Email Settings screen.

**Save Log:** This option will save the router log to a file on your computer.

**D-Link**

DIR-835 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO  
LOGS  
STATISTICS  
INTERNET SESSIONS  
ROUTING  
WIRELESS  
IPv6  
IPv6 ROUTING

**LOGS**

Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has internal syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

**LOG OPTIONS**

**Log Type :**  System Activity  
 Debug Information  
 Attacks  
 Dropped Packets  
 Notice

Apply Log Settings Now

**LOG DETAILS**

First Page Last Page Previous Next  
Refresh Clear Email Now Save Log

1/19

Time	Message
Aug 2 18:51:28	Sending discover...
Aug 2 18:51:26	Sending discover...
Aug 2 18:51:24	Sending discover...
Aug 2 18:50:20	Sending discover...
Aug 2 18:50:18	Sending discover...
Aug 2 18:50:16	Sending discover...
Aug 2 18:49:24	UDHCPD Inform: add_lease 192.168.0.106
Aug 2 18:49:20	ath0: STA 00:16:ea:61:54:76 RADIUS: starting accounting session 4E98193B-00000049
Aug 2 18:49:20	ath0: STA 00:16:ea:61:54:76 IEEE 802.11: associated
Aug 2 18:49:20	ath0: STA 00:16:ea:61:54:76 IEEE 802.11: disassociated

WIRELESS

Helpful Hints...  
Check the log frequently to detect unauthorized network usage.  
You can also have the log mailed to you periodically. Refer to Tools -> Email.  
More...

# Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-835 on both the WAN, 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.

**D-Link**

DIR-835 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICES INFO  
LOGS  
STATISTICS  
INTERNET SESSIONS  
ROUTING  
WIRELESS  
IPv6  
IPv6 ROUTING

**TRAFFIC STATISTICS**  
Traffic Statistics display Receive and Transmit packets passing through your router.  
Refresh Statistics Clear Statistics

**LAN STATISTICS**

Sent : 79673	Received : 41191
TX Packets Dropped : 0	RX Packets Dropped : 0
Collisions : 0	Errors : 0

**WAN STATISTICS**

Sent : 536	Received : 0
TX Packets Dropped : 0	RX Packets Dropped : 0
Collisions : 0	Errors : 0

**WIRELESS STATISTICS**

Sent : 30007	Received : 8354
TX Packets Dropped : 0	RX Packets Dropped : 0
	Errors : 0

Helpful Hints...  
This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized.  
[More...](#)

WIRELESS

# 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.

Product Page: DIR-835 Hardware Version: XX Firmware Version: 1.00

**D-Link**

DIR-835 // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO  
LOGS  
STATISTICS  
INTERNET SESSIONS  
ROUTING  
WIRELESS  
IPV6  
IPV6 ROUTING

**INTERNET SESSIONS**

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

**INTERNET SESSIONS**

Local	Net	Internet	Protocol	State	Dir	Timeout
-------	-----	----------	----------	-------	-----	---------

Helpful Hints...  
This is a list of all active conversations between WAN computers and LAN computers.  
[More...](#)

# Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

**Interface:** Use the drop-down menu to specify if the IP packet must use the *WAN* or *LAN* interface to transit out of the Router.

**Destination IP:** Enter the IP address of the packets that will take this route.

**Subnet Mask:** Enter the subnet mask to specify the subnet of the IP packets that will take this route.

**Gateway:** Enter the next hop that will be taken if this route is used.

Click the **Save Settings** button to save any changes made.



**D-Link**

DIR-835 // SETUP ADVANCED TOOLS STATUS SUPPORT

ROUTING

**Routing Table**

This page displays the routing details configured for your router.

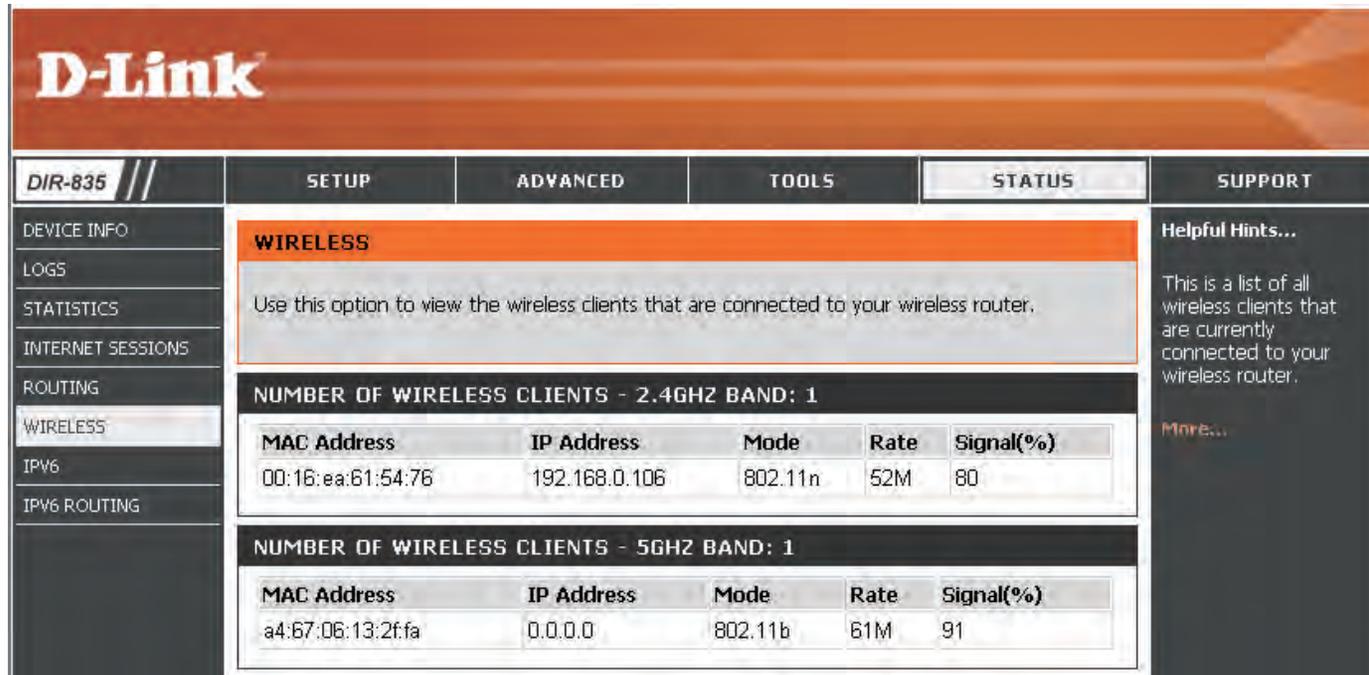
**ROUTING TABLE**

Destination IP	Netmask	Gateway	Metric	Interface	Type	Creator
192.168.0.0	255.255.255.0	0.0.0.0	0	LAN	Internal	System
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN	Internal	System
127.0.0.0	255.0.0.0	0.0.0.0	0	Local Loopback	Internal	System

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.



**D-Link**

DIR-835 // SETUP ADVANCED TOOLS **STATUS** SUPPORT

DEVICE INFO  
LOGS  
STATISTICS  
INTERNET SESSIONS  
ROUTING  
**WIRELESS**  
IPV6  
IPV6 ROUTING

**WIRELESS**

Use this option to view the wireless clients that are connected to your wireless router.

**NUMBER OF WIRELESS CLIENTS - 2.4GHZ BAND: 1**

MAC Address	IP Address	Mode	Rate	Signal(%)
00:16:ea:61:54:76	192.168.0.106	802.11n	52M	80

**NUMBER OF WIRELESS CLIENTS - 5GHZ BAND: 1**

MAC Address	IP Address	Mode	Rate	Signal(%)
a4:67:06:13:2f:fa	0.0.0.0	802.11b	61M	91

**Helpful Hints...**

This is a list of all wireless clients that are currently connected to your wireless router.

[More...](#)

# IPv6

The IPv6 page displays a summary of the Router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

The screenshot displays the D-Link DIR-835 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a menu with options: DEVICE INFO, LOGS, STATISTICS, INTERNET SESSIONS, ROUTING, WIRELESS, IPv6 (highlighted), and IPv6 ROUTING. The main content area is titled "IPv6 Network Information" and contains the following sections:

- IPv6 Network Information**: A summary box stating, "All of your IPv6 Internet and network connection details are displayed on this page."
- IPv6 Connection Information**: A box showing "IPv6 Connection Type : Local Connectivity Only" and "LAN IPv6 Link-Local Address : fe80::201:23ff:fe45:6789/64".
- LAN IPv6 Computers**: A table with two columns: "IPv6 Address" and "Name (if any)". The table is currently empty.

On the right side of the interface, there is a "Helpful Hints..." section with the text: "All of your WAN and LAN connection details are displayed here." and a "More..." link.

# IPv6 Routing

This page displays the IPv6 routing details configured for your router.

The screenshot shows the D-Link web interface for a DIR-835 router. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a menu with options: DEVICE INFO, LOGS, STATISTICS, INTERNET SESSIONS, ROUTING, WIRELESS, IPV6, and IPV6 ROUTING (which is currently selected). The main content area is titled 'IPv6 ROUTING' and contains the following text:

**IPv6 Routing Table**

This page displays the IPv6 routing details configured for your router.

**IPv6 ROUTING TABLE**

Destination IP	Gateway	Metric	Interface
----------------	---------	--------	-----------

# Support

Product Page: DIR-835 Hardware Version: XX Firmware Version: 1.00



<b>DIR-835</b> //	<b>SETUP</b>	<b>ADVANCED</b>	<b>TOOLS</b>	<b>STATUS</b>	<b>SUPPORT</b>
-------------------	--------------	-----------------	--------------	---------------	----------------

MENU

SETUP

ADVANCED

TOOLS

STATUS

**SUPPORT MENU**

- [Setup](#)
- [Advanced](#)
- [Tools](#)
- [Status](#)

**SETUP HELP**

- [Internet](#)
- [WAN](#)
- [Wireless Settings](#)
- [Network Settings](#)
- [IPv6](#)

**ADVANCED HELP**

- [Virtual Server](#)
- [Port Forwarding](#)
- [Application Rules](#)
- [QoS Engine](#)
- [Network Filter](#)
- [Access Control](#)
- [Website Filter](#)
- [Inbound Filter](#)
- [Firewall Settings](#)
- [Routing](#)
- [Advanced Wireless](#)
- [Wi-Fi Protected Setup](#)
- [Advanced Network](#)
- [GUEST ZONE](#)
- [IPv6Firewall](#)
- [IPv6 Routing](#)

**TOOLS HELP**

- [Admin](#)
- [Time](#)
- [Syslog](#)
- [Email Settings](#)
- [System](#)
- [Firmware](#)
- [Dynamic DNS](#)
- [System Check](#)
- [Schedules](#)

**STATUS**

- [Device Info](#)
- [Logs](#)
- [Statistics](#)
- [Internet Sessions](#)
- [Routing](#)
- [Wireless](#)
- [IPv6](#)
- [IPv6 Routing](#)

**WIRELESS**

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-835 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 (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:

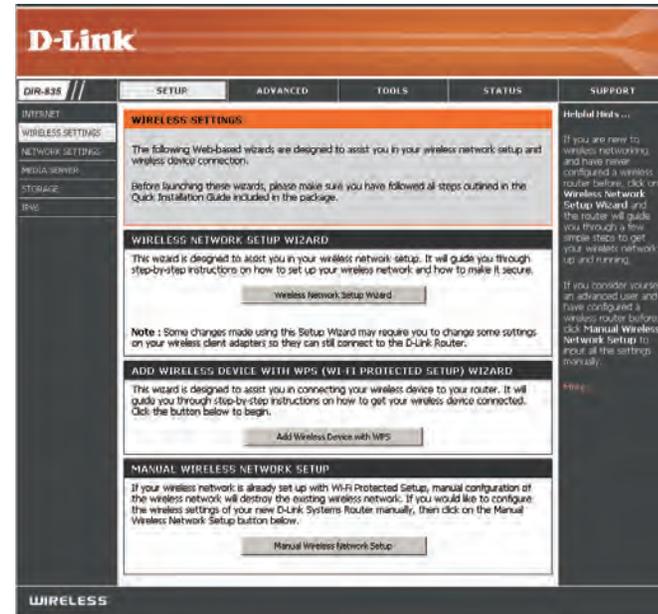
- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead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

 The screenshot shows the first step of the wizard: 'STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD'. The instruction is 'Give your network a name, using up to 32 characters.' There is a text input field for 'Network Name (SSID) 2.4GHz Band' containing 'dlink'. Below it is a checkbox for 'Manually set 5GHz band Network Name (SSID)'. There are two radio button options:
 

- Automatically assign a network key for both 2.4GHz and 5GHz band (Recommended). To prevent outsiders from accessing your network, the router will automatically assign a security to your network.
- Manually assign a network key. Use this options if you prefer to create our own key.

 A note states: 'Note: All D-Link wireless adapters currently support WPA.' At the bottom, there are four buttons: 'Prev', 'Next', 'Cancel', and 'Save'.

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> dlink</p> <p><b>Security Mode 2 :</b> Auto (WPA or WPA2) - Personal</p> <p><b>Cipher Type :</b> TKIP and AES</p> <p><b>Pre-Shared Key :</b> c47086bee2659742883d5bb36da53356e51407f1635855aa7cbef92b5598bf6c</p>
<p><b>Wireless Band :</b> 5GHz Band</p> <p><b>Wireless Network Name (SSID) :</b> dlink_media</p> <p><b>Security Mode 2 :</b> Auto (WPA or WPA2) - Personal</p> <p><b>Cipher Type :</b> TKIP and AES</p> <p><b>Pre-Shared Key :</b> c47086bee2659742883d5bb36da53356e51407f1635855aa7cbef92b5598bf6c</p>

Prev Next Cancel Save

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.

Prev Next Cancel Save

## Add Wireless Device with WPS Wizard

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



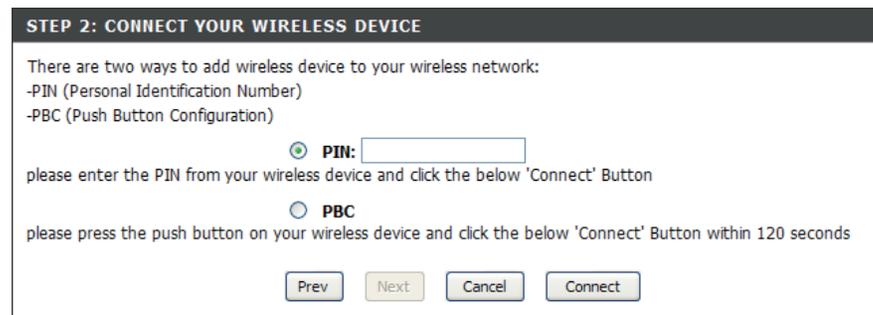
Select **Auto** to add a wireless client using WPS (Wi-Fi Protected Setup). Once you select **Auto** and click **Connect**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

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**.

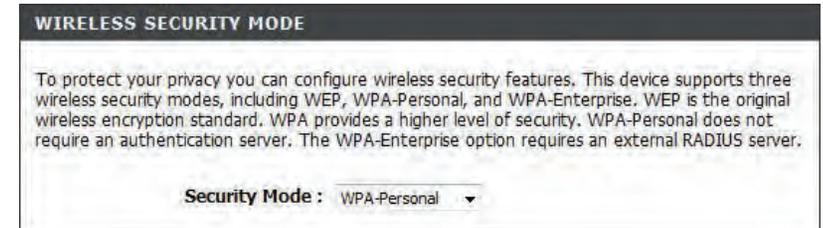
**PBC:** Select this option to use PBC (Push Button) method to add a wireless client. Click **Connect**.



# 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.

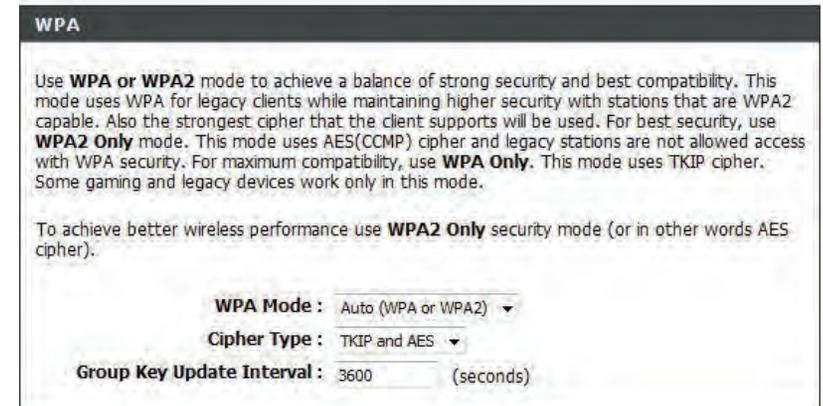
1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WPA-Personal**.
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, 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).
6. Next to *Pre-Shared Key*, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.
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.



**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**

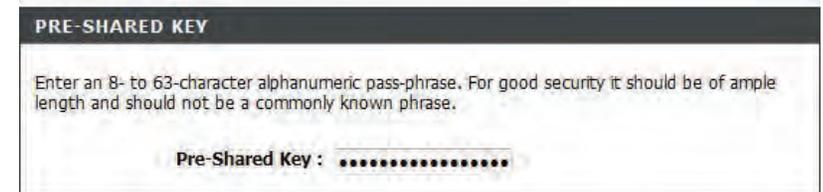
Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** 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 : .....

# 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**

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 strongest cipher that 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:**

**Cipher Type:**

**Group Key Update Interval:**  (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:**  (minutes)

**RADIUS server IP Address:**

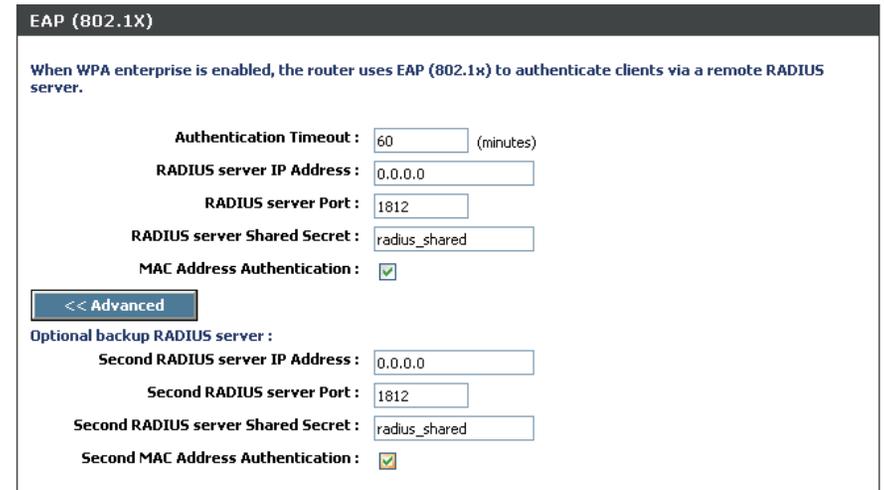
**RADIUS server Port:**

**RADIUS server Shared Secret:**

**MAC Address Authentication:**

[Advanced >>](#)

8. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
9. Next to *RADIUS Server Shared Secret*, enter the security key.
10. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.
11. Click **Advanced** to enter settings for a secondary RADIUS Server.
12. Click **Apply Settings** to save your settings.



**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 : 1812

RADIUS server Shared Secret : radius\_shared

MAC Address Authentication :

**<< Advanced**

Optional backup RADIUS server :

Second RADIUS server IP Address : 0.0.0.0

Second RADIUS server Port : 1812

Second RADIUS server Shared Secret : radius\_shared

Second MAC Address Authentication :

# Connect to a Wireless Network Using Windows® 7

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

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



Wireless Icon

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

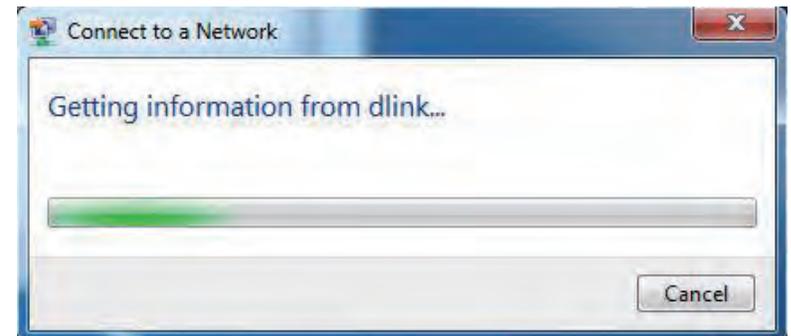


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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



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



5. Enter the same security key or passphrase that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

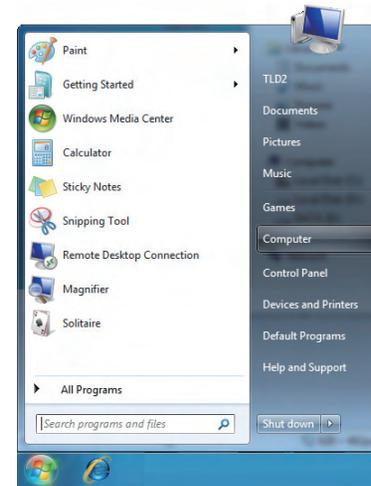
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



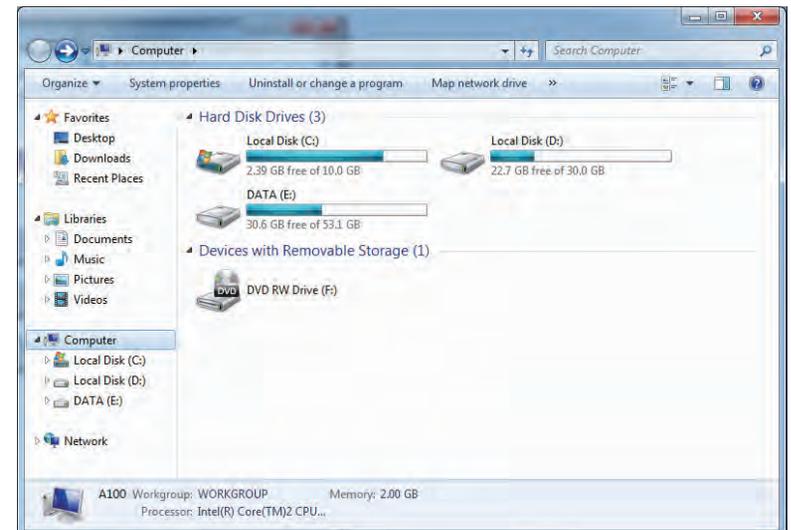
# Configure WPS

The WPS feature of the DIR-835 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

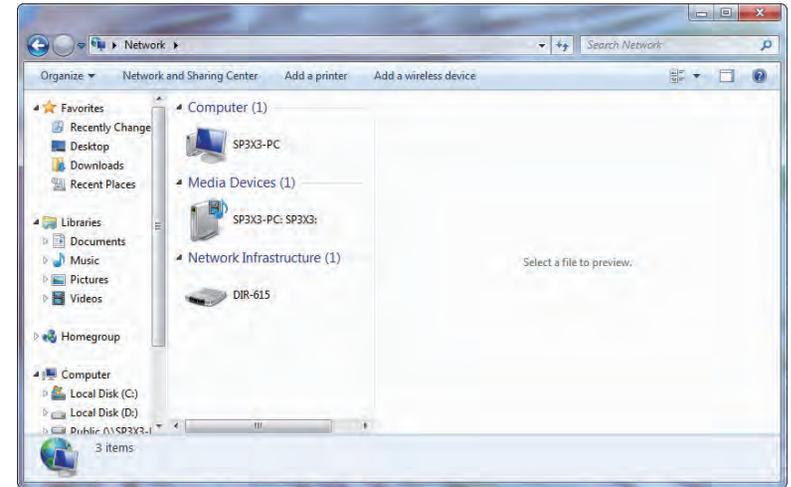
1. Click the **Start** button and select **Computer** from the Start menu.



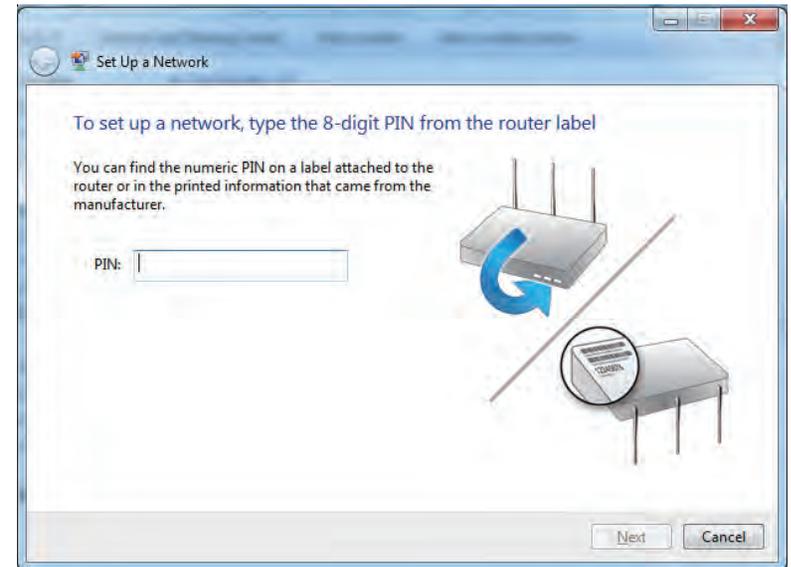
2. Click the **Network** option.



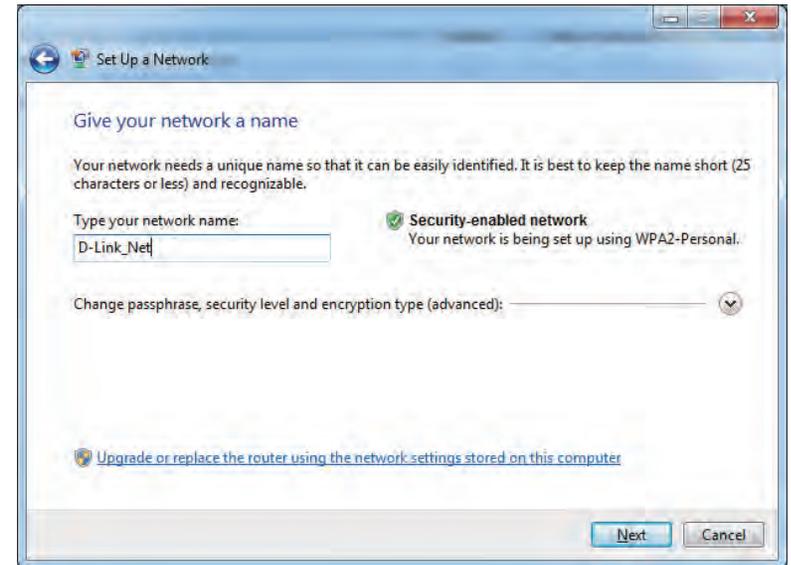
3. Double-click the DIR-835.



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

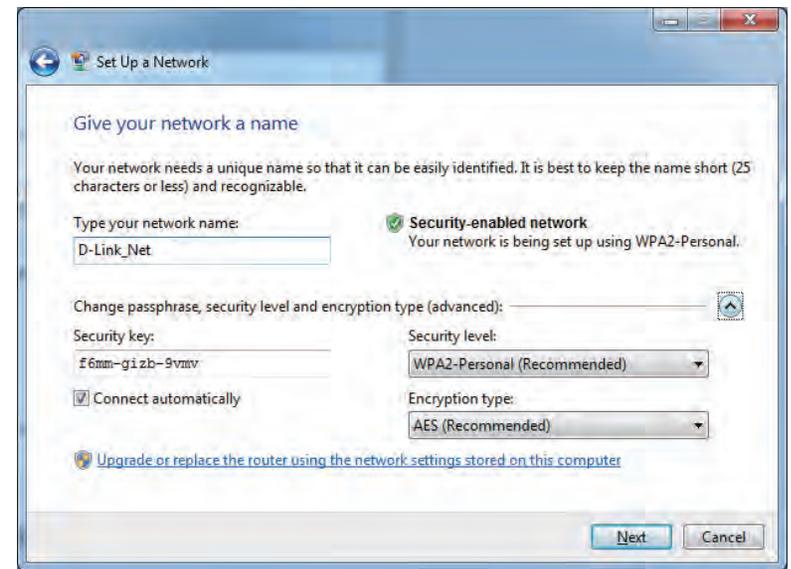


5. Type a name to identify the network.



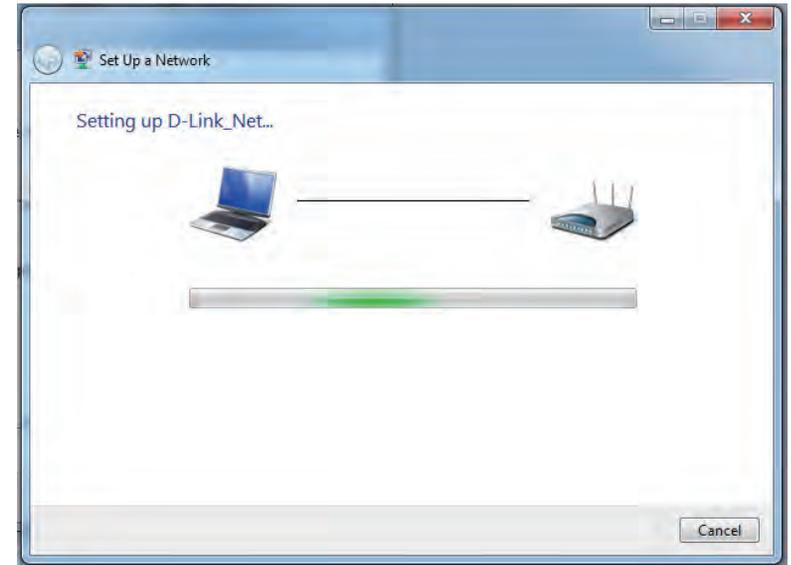
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



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

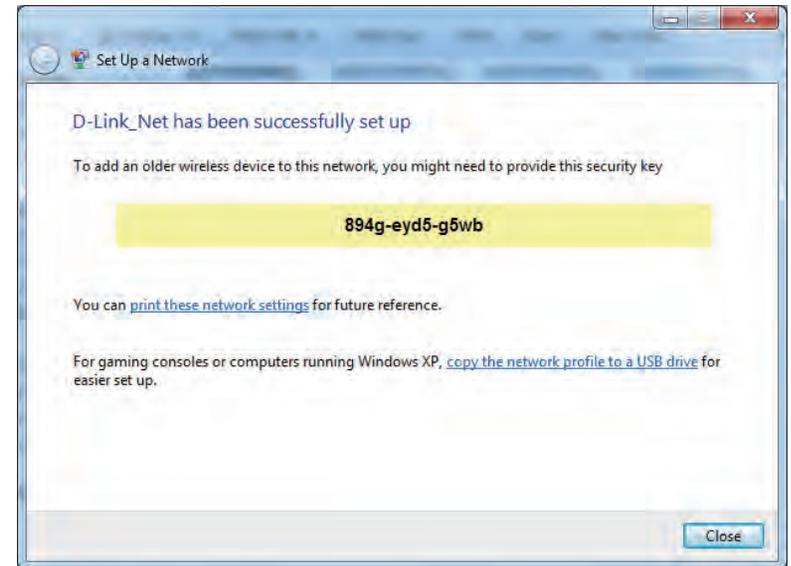
Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been setup successfully.

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

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



# Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

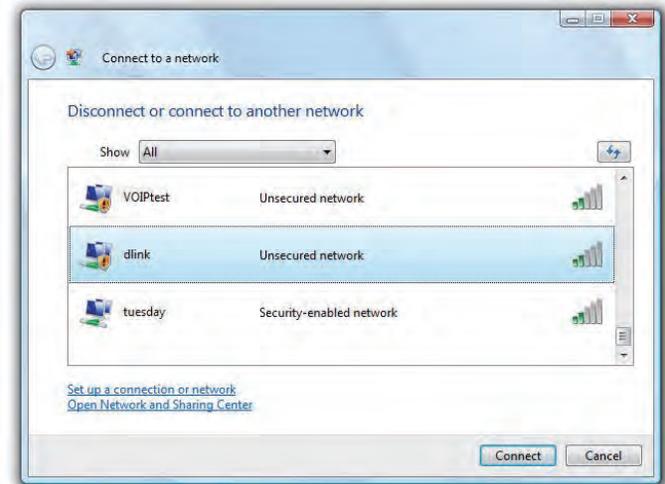
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.

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

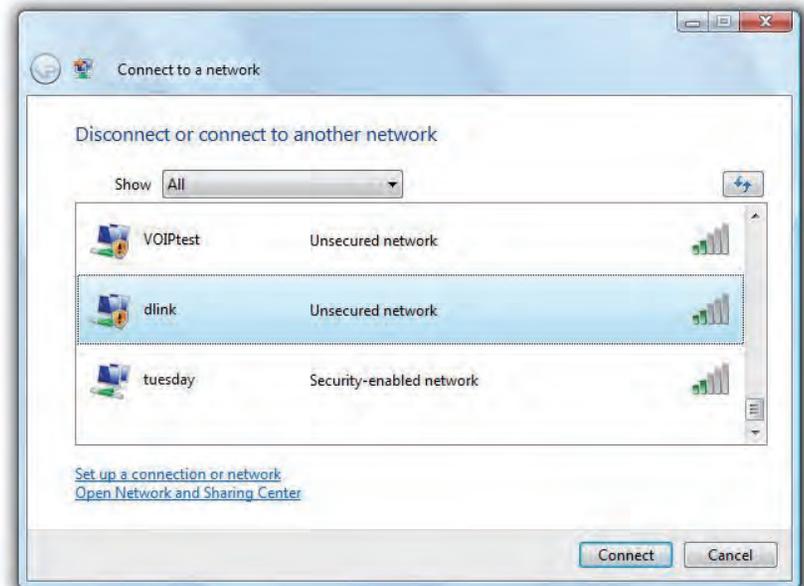
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



## Configure Wireless Security

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

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase that is on your router and click **Connect**.

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



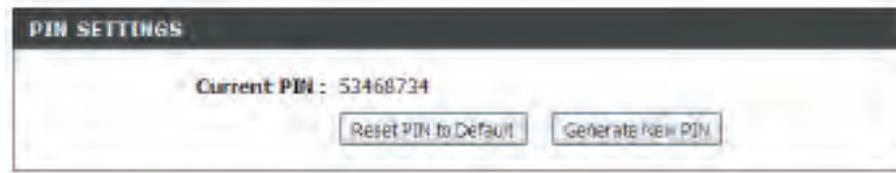
## Connect Using WCN 2.0 in Windows Vista®

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and unconfigured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the **Enable** checkbox in the **Basic > Wireless** section. Use the Current PIN that is displayed on the **Advanced > Wi-Fi Protected Setup** section or choose to click the **Generate New PIN** button or **Reset PIN to Default** button.

For additional information, please refer to page 85.



If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

# Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

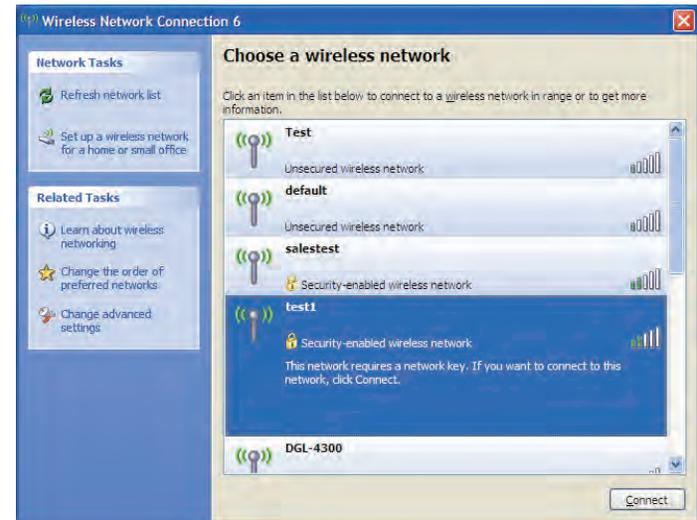
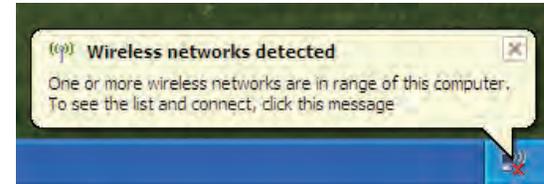
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.

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

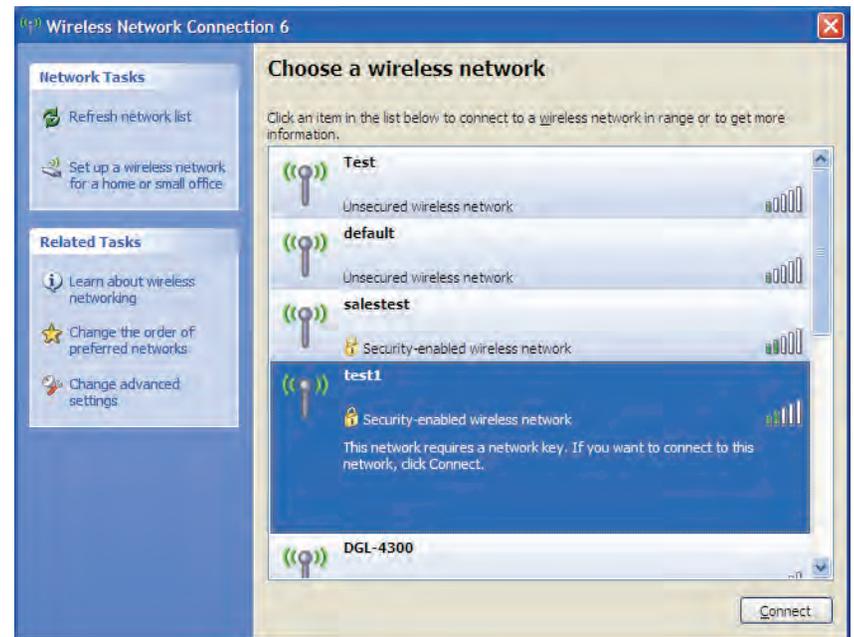
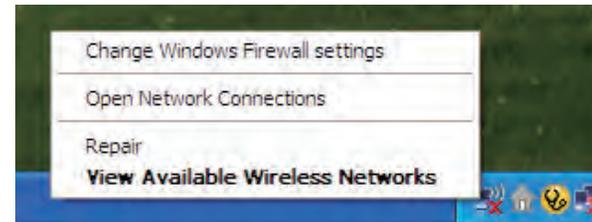
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



## Configure WPA-PSK

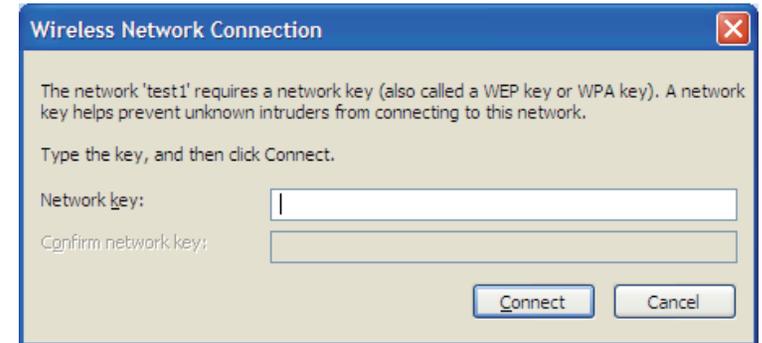
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-835. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Microsoft Internet Explorer® 6.0 and higher
  - Mozilla Firefox 3.0 and higher
  - Google™ Chrome 2.0 and higher
  - Apple Safari 3.0 and higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

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

## 2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is **admin** and leave the password box empty.

### 3. Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

**Note: AOL DSL+ users must use MTU of 1400.**

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

**ping [url] [-f] [-l] [MTU value]**

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, let's say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with ( $1452+28=1480$ ).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

# Wireless Basics

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

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

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

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

## **What is Wireless?**

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

## **Why D-Link Wireless?**

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

## **How does wireless work?**

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

### **Wireless Local Area Network (WLAN)**

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

## **Wireless Personal Area Network (WPAN)**

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

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

## **Who uses wireless?**

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

### **Home**

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

### **Small Office and Home Office**

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

## **Where is wireless used?**

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

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

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

## **Tips**

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

### **Centralize your router or Access Point**

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

### **Eliminate Interference**

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

## Security

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

# Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-835 wireless network Cardbus adapters.

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

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

# Networking Basics

## Check your IP address

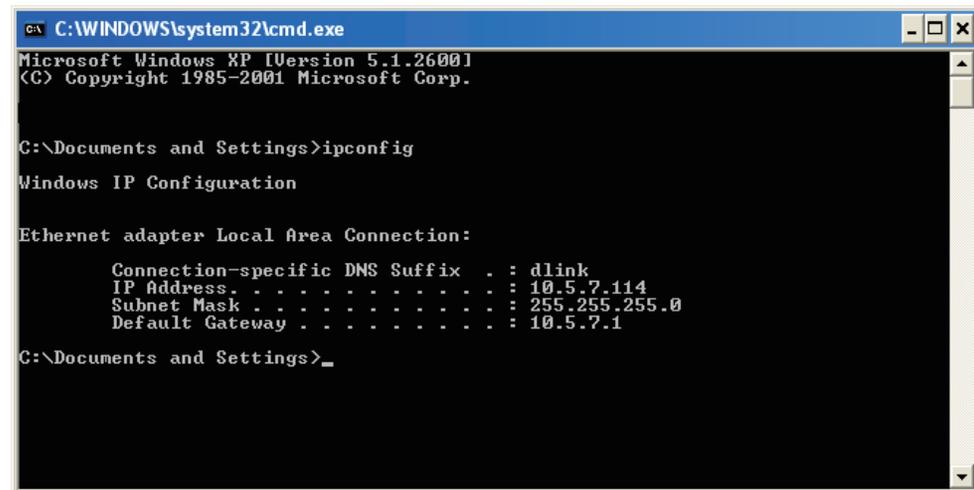
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

## Statically Assign an IP address

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

- Step 1**
- Windows® 7 - Click on Start > Control Panel > Network and Internet > Network and Sharing Center.
  - Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**
  - Windows® XP - Click on **Start > Control Panel > Network Connections.**
  - Windows® 2000 - From the desktop, right-click **My Network Places > Properties.**

**Step 2**  
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties.**

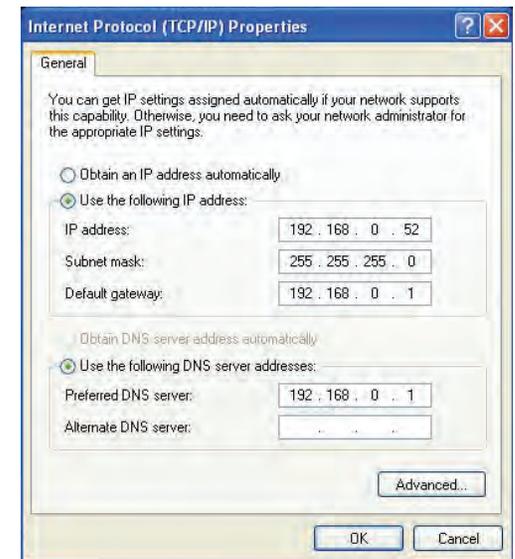
**Step 3**  
Highlight **Internet Protocol (TCP/IP)** and click **Properties.**

**Step 4**  
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

**Step 5**  
Click **OK** twice to save your settings.



# Technical Specifications

## Standards

- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab

## Security

- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise

## Wireless Signal Rates<sup>1</sup>

### IEEE 802.11n 2.4GHz(HT20/40):

- 144.4Mbps (300)
- 115.6Mbps (240)
- 72.2Mbps (150)
- 57.8Mbps (120)
- 28.9Mbps (60)
- 14.4Mbps (30)
- 130Mbps (270)
- 86.7Mbps (180)
- 65Mbps (135)
- 43.3Mbps (90)
- 21.7Mbps (45)
- 7.2Mbps (15)

### IEEE 802.11n 5GHz(HT20/40):

- 216Mbps (450)
- 173.3Mbps (360)
- 130.7Mbps (270)
- 115.6Mbps (240)
- 72.2Mbps (150)
- 57.8Mbps (120)
- 28.9Mbps (60)
- 14.4Mbps (30)
- 195Mbps (405)
- 144.4Mbps (300)
- 130Mbps (270)
- 86.7Mbps (180)
- 65Mbps (135)
- 43.3Mbps (90)
- 21.7Mbps (45)
- 7.2Mbps (15)

## IEEE 802.11g:

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

## Frequency Range<sup>2</sup> (North America)

- 2.412GHz to 2.462GHz (802.11g/n)
- 5.15GHz to 5.825GHz (802.11a/n)<sup>3</sup>

## External Antenna Type

- Three (3) detachable Antennas

## Operating Temperature

- 32°F to 131°F ( 0°C to 40°C)

## Humidity

- 95% maximum (non-condensing)

## Safety & Emissions

- FCC
- IC

## Dimensions

- L = 7.6 inches
- W = 4.6 inches
- H = 1.2inches

## Warranty

- 1 Year

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

<sup>2</sup> Frequency Range varies depending on country's regulation

<sup>3</sup> The DIR-835 does not include 5.25-5.35GHz & 5.47-5.725GHz in some regions.

# Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DIR-835)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the router).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

## For customers within the United States:

**Phone Support:**

(877) 453-5465

**Internet Support:**

<http://support.dlink.com>

## For customers within Canada:

**Phone Support:**

(800) 361-5265

**Internet Support:**

<http://support.dlink.ca>

# Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

## **Limited Warranty:**

D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

### **Limited Software Warranty:**

D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Software Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

### **Non-Applicability of Warranty:**

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link’s products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold “As-Is” without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

### **Submitting A Claim (USA):**

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization (“RMA”) number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

**Submitting A Claim (Canada):**

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.
- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-800-361-5265, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization (“RMA”) number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.ca/>.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.
- RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

### **What Is Not Covered:**

The Limited Warranty provided herein by D-Link does not cover:

Products that, in D-Link’s judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

### **Disclaimer of Other Warranties:**

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED “AS-IS” WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

**Limitation of Liability:**

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

**Governing Law:**

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

**Trademarks:**

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

**Copyright Statement:**

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

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

**CE Mark Warning:**

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

### **Federal Communication Commission Interference Statement**

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

### **IMPORTANT NOTICE: FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 22cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

**Industry Canada statement:**

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**IMPORTANT NOTE:**

**Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 22cm between the radiator & your body.

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

This device has been designed to operate with an antenna having a maximum gain of [2] dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (IC: 4216A-IR835A1/ Model: DIR-835A1) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

**NOTE IMPORTANTE:**

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 22cm de distance entre la source de rayonnement et votre corps.

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de dB [3x]. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteur radio (IC: 4216A-IR835A1 / Modèle: DIR-835A1) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Antenna information: dipole / 2dBi (Brand: D-Link / Manufacturer: Wha Yu)

# Registration

Register your product online at [registration.dlink.com](http://registration.dlink.com)



Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0  
October 12, 2011