



User Manual

Wireless AC750 Dual Band Cloud Router

DIR-810L

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	January 31, 2013	• Initial release for Revision A1

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 © 2013 by D-Link Systems, Inc.

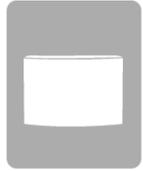
All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Table of Contents

Preface	i	PPTP	33
Manual Revisions	i	L2TP	35
Trademarks	i	DS-Lite	37
Product Overview	1	Wireless Connection Setup Wizard	38
Package Contents	1	Wi-Fi Protected Setup Wizard	41
System Requirements	2	Manual wireless network setup	42
Introduction	3	Manual Setup - 2.4Ghz Band	43
Features	4	Manual Setup - 5Ghz Band	48
Hardware Overview	5	Wireless Security	53
Connections	5	What is WPA?	53
LEDs	6	Network Settings	54
Installation	7	Router Settings	54
Before you Begin	7	DHCP Server Settings	55
Wireless Installation Considerations	8	DHCP Reservation	57
Manual Setup	9	IPv6	58
Configuration	11	IPv6 Internet Connection Setup Wizard	59
Quick Setup Wizard	12	IPv6 Local Connectivity Settings	64
QRS Mobile App (iOS, Android)	19	IPv6 Manual Setup	65
Web-based Configuration Utility	20	mydlink™ Settings	74
Internet Connection Setup	21	Advanced	77
Internet Connection Setup Wizard	22	Virtual Server	77
Internet (Manual Setup)	28	Port Forwarding	78
Static (assigned by ISP)	30	Application Rules	79
PPPoE (DSL)	31	QoS Engine	80
		Network Filters	82
		Access Control	83

Website Filters.....	86	IPv6	113
Inbound Filters.....	87	IPv6 Routing.....	114
Firewall Settings.....	88	Support	115
Routing.....	90	Connect a Wireless Client to your Router	116
Advanced Wireless	91	WPS Button.....	116
Wi-Fi Protected Setup (WPS)	92	Windows® 8.....	117
Advanced Network Settings.....	94	WPA/WPA2	117
Guest Zone.....	95	Windows® 7.....	119
IPv6 Firewall.....	96	WPA/WPA2	119
IPv6 Routing	97	WPS.....	122
Tools	98	Windows Vista®	126
Admin.....	98	WPA/WPA2	127
Time.....	99	WPS/WCN 2.0	129
SysLog.....	100	Windows® XP.....	130
Email Settings.....	101	WPA/WPA2	131
System	102	Troubleshooting	133
Firmware	103	Wireless Basics	137
Language Pack.....	103	What is Wireless?.....	138
Dynamic DNS	104	Tips.....	140
System Check.....	105	Wireless Modes.....	141
Schedules	106	Networking Basics	142
Status	107	Check your IP address.....	142
Device Info	107	Statically Assign an IP address.....	143
Logs.....	108	Technical Specifications	144
Statistics	109	Warranty.....	145
Internet Sessions.....	110		
Routing.....	111		
Wireless.....	112		

Package Contents



DIR-810L Wireless AC750 Dual Band Cloud Router



Ethernet Cable



Power Adapter



WI-FI Configuration Note

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-810L will cause damage and void the warranty for this product.

System Requirements

<p>Network Requirements</p>	<ul style="list-style-type: none"> • An Ethernet-based Cable or DSL modem • 802.11a, 802.11g, 802.11n, or 802.11ac wireless clients • 10/100 Ethernet
<p>Web-based Configuration Utility Requirements</p>	<p>Computer with the following:</p> <ul style="list-style-type: none"> • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter <p>Browser Requirements:</p> <ul style="list-style-type: none"> • Internet Explorer 7 or higher • Firefox 3.5 or higher • Safari 4 or higher • Chrome 8 or higher <p>Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.</p>
<p>mydlink Requirements</p>	<ul style="list-style-type: none"> • iPhone/iPad/iPod Touch (iOS 3.0 or higher) • Android device (1.6 or higher) • Computer with the following browser requirements: <ul style="list-style-type: none"> • Internet Explorer 7 or higher • Firefox 3 or higher • Safari 5 or higher • Chrome 5 or higher <p><small>iPhone, iPad, and iPod touch are registered trademarks of Apple Inc. Android is a trademark of Google, Inc.</small></p>

Introduction

Now you can monitor and manage your home network right from your laptop, iOS, or Android™ device. This cloud-enabled router can be configured to notify you whenever new devices are connected to your network or unwanted access is detected. Monitor in realtime websites that are being visited, with recent browser history displayed on the mydlink™ Lite app – which is great for parents keeping an eye on children using the internet at home. The D-Link Cloud Service can help you to detect and block unwelcome guests who attempt to access your wireless network, and any suspicious activities will be displayed right on your mydlink Lite app or browser.

The D-Link DIR-810L is a draft IEEE 802.11ac compliant device that delivers speeds up to 3 times faster than 802.11n, while staying backward compatible with older 802.11b/g/n devices. Connect the DIR-810L to a Cable or DSL modem and provide high-speed Internet access to multiple wireless clients. Powered by the latest draft 802.11ac technology, this router provides superior wireless coverage for small to medium sized homes. The DIR-810L also includes a 4-port 10/100 Fast Ethernet switch that connects Ethernet wired devices for high-speed wired connectivity.

With some routers, all wired and wireless traffic, including VoIP, Video Streaming, Online Gaming, and Web browsing are mixed together into a single data stream. By handling data this way, applications like video streaming could experience lags or delays. With D-Link Intelligent QoS Technology, wired and wireless traffic are analyzed and separated into multiple data streams. You can also assign priorities to different data streams to ensure that the traffic most important to you receives optimum bandwidth.

The DIR-810L supports the latest wireless security features to help prevent unauthorized access, be it from inside your wireless network or from the Internet. Support for the WPA and WPA2 standards gives you a range of security and encryption choices, based on the capabilities of your wireless clients. In addition, this router utilizes Dual Active Firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

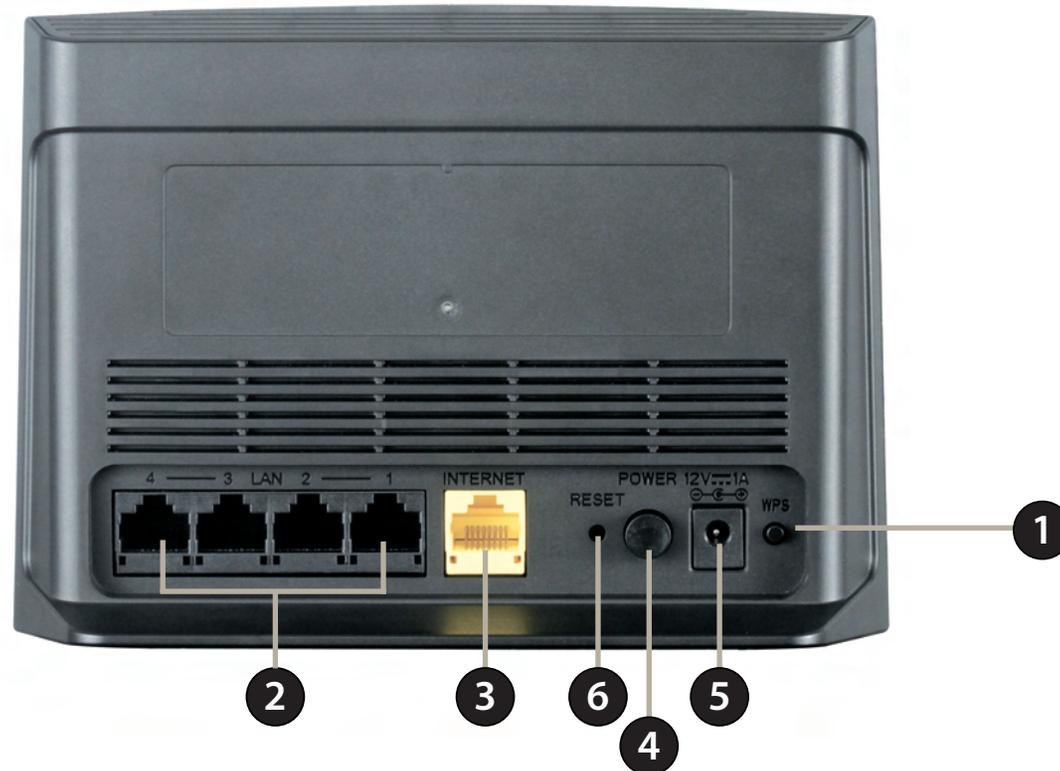
Features

- **Ultimate Fast Wireless Networking** - The DIR-810L provides a wireless connection up to 300Mbps on the 2.4GHz band, and up to 433Mbps on the 5GHz band. 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 802.11ac wireless router gives you the freedom of wireless networking at speeds up to three times faster than 802.11n.
- **Compatible with 802.11a/g/n Devices** - The DIR-810L remains fully compatible with the IEEE 802.11b, 802.11g and 802.11n standards, so it can connect your existing wireless clients, providing backwards compatibility for older devices.
- **Advanced Security 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-810L can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-810L can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-810L guides you through the process of setting up a customized, secure wireless network, allowing you to configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11b, 802.11g, 802.11n and draft 802.11ac 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	WPS Button	Press to start the WPS process. The Power LED will start to blink.
2	LAN Ports (1-4)	Connect 10/100 Ethernet devices such as computers, switches, storage (NAS) devices and game consoles.
3	Internet Port	Using an Ethernet cable, connect your broadband modem to this port.
4	Power Button	Press the power button to power on and off.
5	Power Receptor	Receptor for the supplied power adapter.
6	Reset Button (Hole)	Use a paperclip to depress the reset button and restore the router to its original factory settings.

Hardware Overview

LEDs



1	Power LED	A solid green light indicates a proper connection to the power supply. The light will blink green during the WPS process. The light will be solid orange during boot up.
2	Internet LED	A solid light indicates connection on the Internet port. If the LED is orange, a connection is present but the router cannot connect to the Internet.

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 an 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 this router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer, or you will not be able to connect to the Internet.

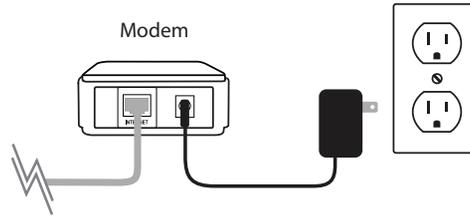
Wireless Installation Considerations

The DIR-810L Wireless AC750 Dual Band Cloud 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 used and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

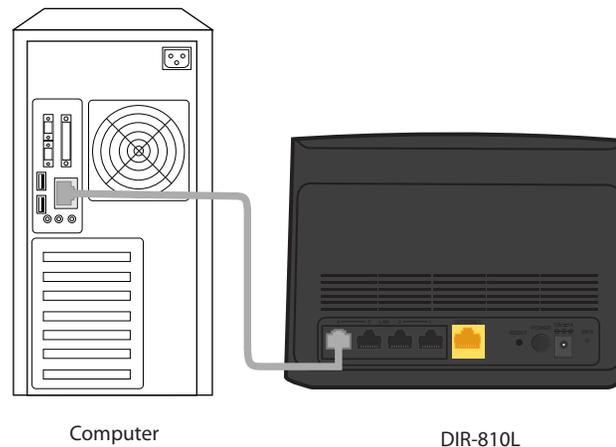
1. Keep the number of walls and ceilings between the router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range by 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 0.5 meters thick (1.5 feet), at a 45-degree angle appears to be almost 1 meter (3 feet) thick. At a 2-degree angle it can appear over 14 meters (42 feet) 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 can affect your wireless signal. 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 be degraded dramatically or even 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.

Manual Setup

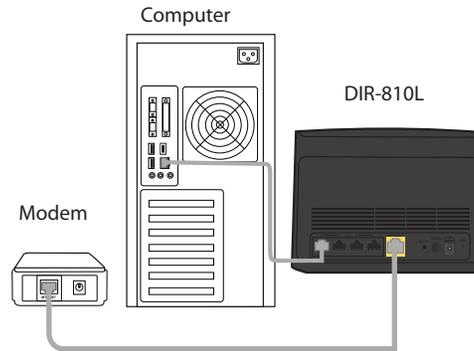
1. Turn off and unplug your cable or DSL broadband modem. This is required.



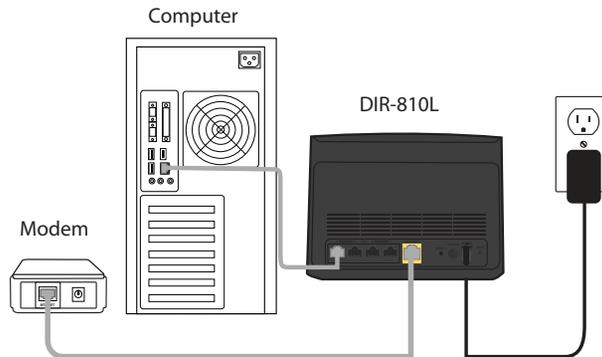
2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.
3. Unplug the Ethernet cable from your modem (or existing router if upgrading) that is connected to your computer. Plug it into the LAN port labeled **1** on the back of your router. The router is now connected to your computer.



4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.



5. Reconnect the power adapter to your cable or DSL broadband modem and wait for two minutes.
6. Connect the supplied power adaptor into the power port on the back of the router and then plug it into a power outlet or surge protector. Press the power button and verify that the power LED is lit. Allow 1 minute for the router to boot up.



7. If you are connecting to a Broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser and enter a web site. A solid light on the **Internet LED** indicates connection on the Internet port and the router can connect to the Internet. If the LED is orange, a connection is present but the router cannot connect to the Internet.

Configuration

There are several different ways you can configure your router to connect to the Internet and connect to your clients:

- **D-Link Setup Wizard** - This wizard will launch when you log into the router for the first time. Refer to “Quick Setup Wizard” on page 12.
- **QRS Mobile App** - Use your iOS or Android device to configure your router. Refer to “QRS Mobile App (iOS, Android)” on page 19.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to “Internet (Manual Setup)” on page 28.

Quick Setup Wizard

If this is your first time installing the router, open your web browser. You will automatically be directed to the **Wizard Setup Screen**. If not, enter “http://dlinkrouter.local”. Then, press **Enter**.

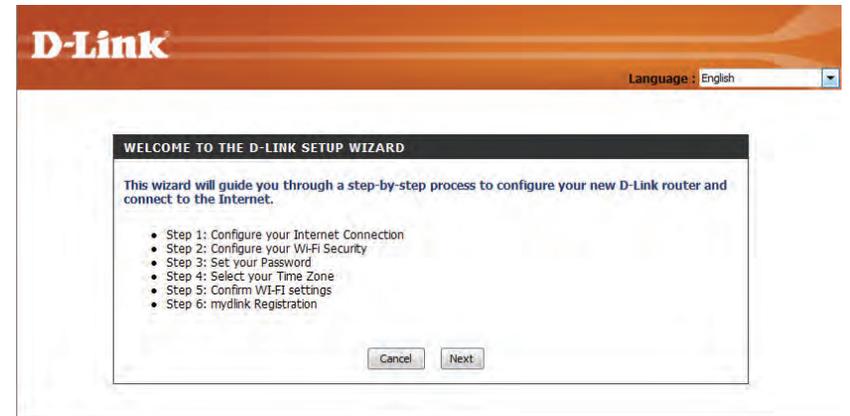


If you have already configured your settings and you would like to access the configuration utility, please refer to “Internet (Manual Setup)” on page 28.

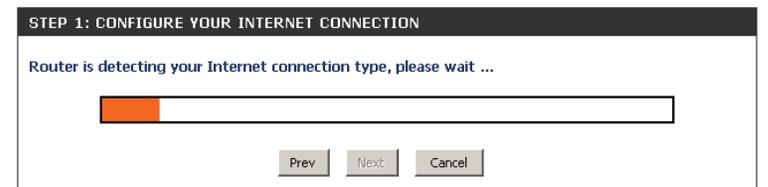
If this is your first time logging into the router, this wizard will start automatically.

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.

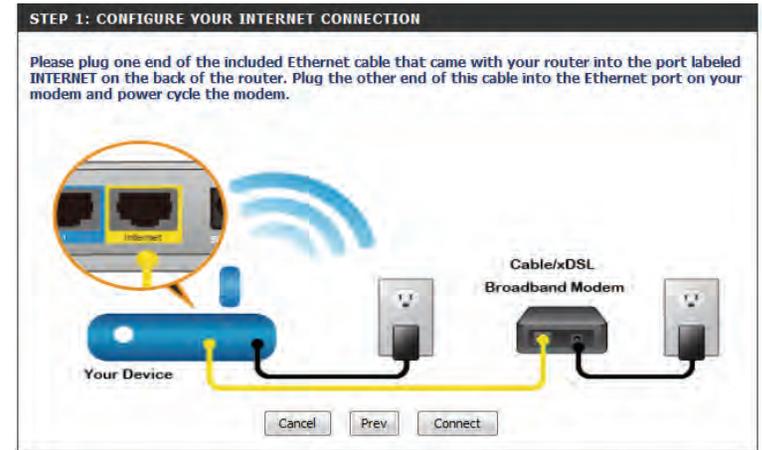
Click **Next** to continue.



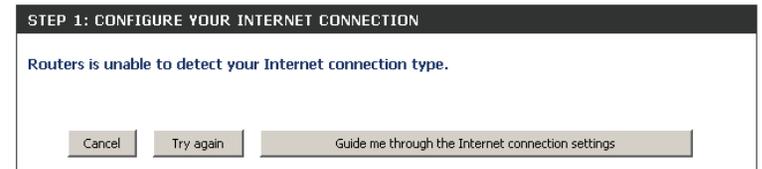
Please wait while your router detects your internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password.



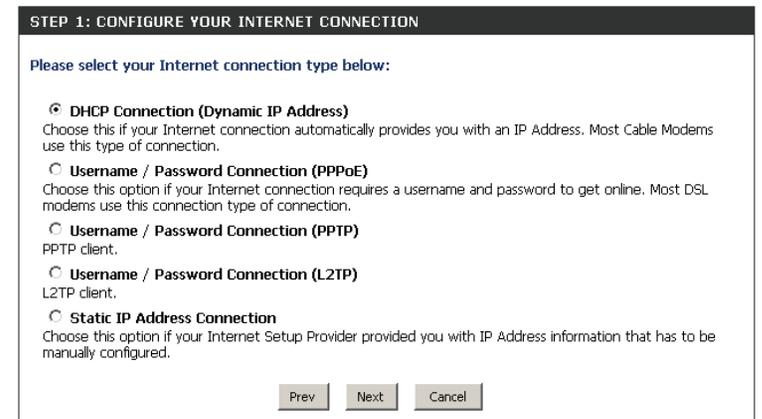
If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Check the connection between your broadband modem to the Internet port and then click **Try Again**.



If the router detects an Ethernet connection but does not detect the type of Internet connection you have, this screen will appear. Click **Guide me through the Internet Connection Settings** to display a list of connection types to choose from.



Select your Internet connection type and click **Next** to continue.



If the router detected or you selected **PPPoE**, enter your PPPoE username and password and click **Next** to continue.

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

If the router detected or you selected **PPTP**, enter your PPTP username, password, and other information supplied by your ISP. Click **Next** to continue.

If the router detected or you selected **L2TP**, enter your L2TP username, password, and other information supplied by your ISP. Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (PPPoE)

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

User Name :

Password :

Prev Next Cancel

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 :

Prev Next Cancel

SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

Prev Next Cancel

If the router detected or you selected **Static**, enter the IP and DNS settings supplied by your ISP. Click **Next** to continue.

SET STATIC IP ADDRESS CONNECTION

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

IP Address :

Subnet Mask :

Gateway Address :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

For both the 2.4GHz and 5GHz bands, create a Wi-Fi network name (SSID) using up to 32 characters. These names will identify your wireless network.

Create a Wi-Fi password (Network Key) (between 8-63 characters). Your wireless clients will need to have this password or key entered to be able to connect to your wireless network. It is recommended that you make a record of this information for future reference.

Click **Next** to continue.

STEP 2: CONFIGURE YOUR WI-FI SECURITY

Give your Wi-Fi network a name and a password. (2.4GHz Band)

Wi-Fi Network Name (SSID) : (Using up to 32 characters)

Wi-Fi Password : (Between 8 and 63 characters)

Give your Wi-Fi network a name and a password. (5GHz Band)

Wi-Fi Network Name (SSID) : (Using up to 32 characters)

Wi-Fi Password : (Between 8 and 63 characters)

In order to secure your router, please enter a new password, which will be used to access the web-based configuration utility. Check the Enable Graphical Authentication box to enable CAPTCHA authentication for added security. Click **Next** to continue.

STEP 3: SET YOUR PASSWORD

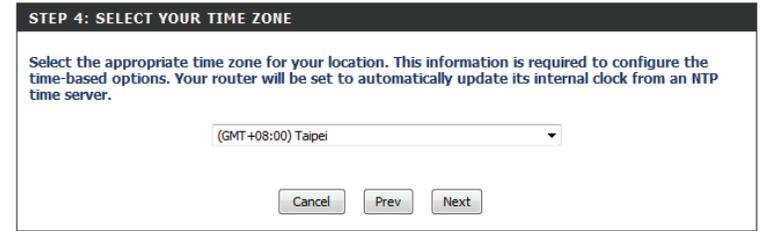
By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below, and enabling CAPTCHA Graphical Authentication provides added security protection to prevent unauthorized online users and hacker software from accessing your network settings.

Password:

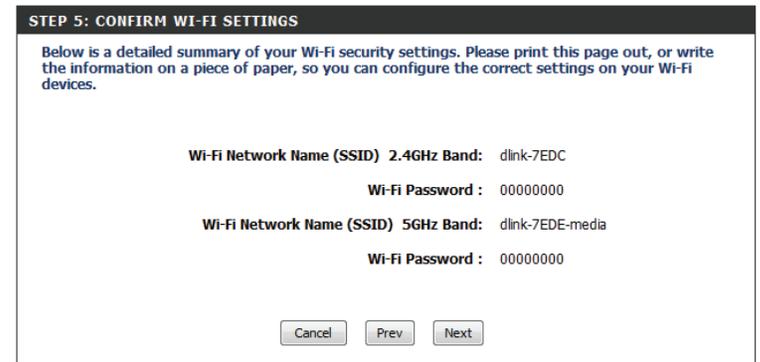
Verify Password :

Enable Graphical Authentication :

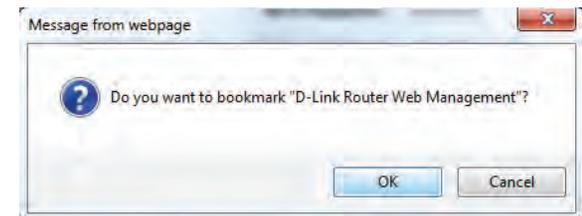
Select your time zone from the drop-down menu and click **Next** to continue.



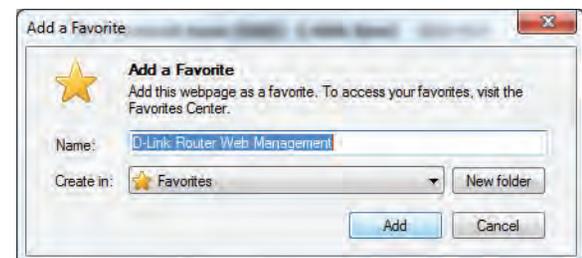
The Setup Complete window will display your Wi-Fi settings. Click **Next** to continue.



If you want to create a bookmark for the router's web-based configuration utility, click **OK**. Click **Cancel** if you do not want to create a bookmark.



If you clicked **Yes**, a window may appear (depending on which web browser you are using) to create a bookmark.



To use the mydlink service (mydlink.com or the mydlink Lite app), you must have an account. Select whether you do have a mydlink account or if you need to create one. Click **Next** to continue.

If you do not want to register at this time, click **Cancel**.

If you clicked **Yes**, enter your mydlink account name (email address) and password. Click **Login** to register your router.

If you clicked **No**, fill out the requested information and click **Sign Up** to create your mydlink account.

MYDLINK REGISTRATION

To use the features of mydlink.com and the mydlink Lite app, you will need an account with mydlink.com. If you already have an account, select **Yes, I have a mydlink account** and click **Next** to register the router with mydlink.com. If you do not have an account, select **No, I want to register and login with a new mydlink account** and click **Next** to create an account. If you do not wish to sign up for the mydlink service, please click **Cancel**.

Do you have mydlink account?

Yes, I have a mydlink account.

No, I want to register and login with a new mydlink account.

STEP 6: MYDLINK REGISTRATION

E-mail Address (Account Name):

Password:

STEP 6: MYDLINK REGISTRATION

Please fulfill the options to complete the registration.

E-mail Address (Account Name) :

Password :

Confirm Password :

First Name :

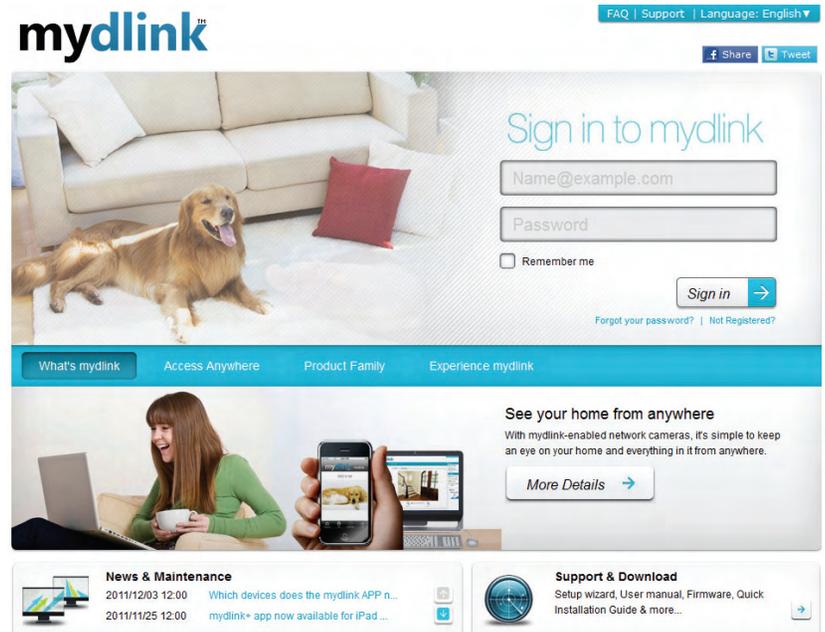
Last name :

[I Accept the mydlink terms and conditions.](#)

The mydlink App will allow you to receive notifications, browse network usage, and configure your router from an iOS (3.0 or higher), Android (1.6 or higher) device.

To download the "mydlink lite" app, visit the iOS App Store, Google Play Store, or <http://mydlink.com/Lite>.

PC and Mac users can use the mydlink portal at <http://mydlink.com>.



QRS Mobile App (iOS, Android)

D-Link offers an app for your iOS or Android device which will assist you to install and configure your router.

Step 1

From an iOS device, go to the iOS App Store. From an Android device go to the Google Play Store. Search for 'D-Link', select **QRS Mobile**, and download the app to your device. You may also scan the appropriate code on the right to locate the app download page.



iOS



Android

Step 2

Once your app is installed, you may now configure your router. Connect to the router wirelessly by going to your wireless utility on your device. Scan for the Wi-Fi name (SSID) as listed on the supplied info card. Select and then enter your Wi-Fi password.



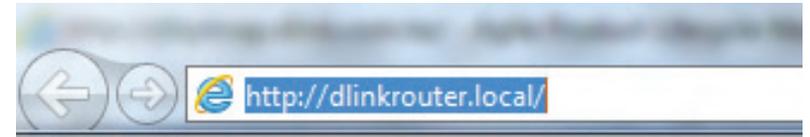
Step 3

Once you connect to the router, launch the QRS mobile app and it will guide you through the installation of your router.



Web-based Configuration Utility

To access the configuration utility, open a web-browser such as Internet Explorer and enter address of the router (**http://dlinkrouter.local** or **http://192.168.0.1**).



Non-Windows and Non-Mac users may also connect by typing **http://192.168.0.1** in the address bar.

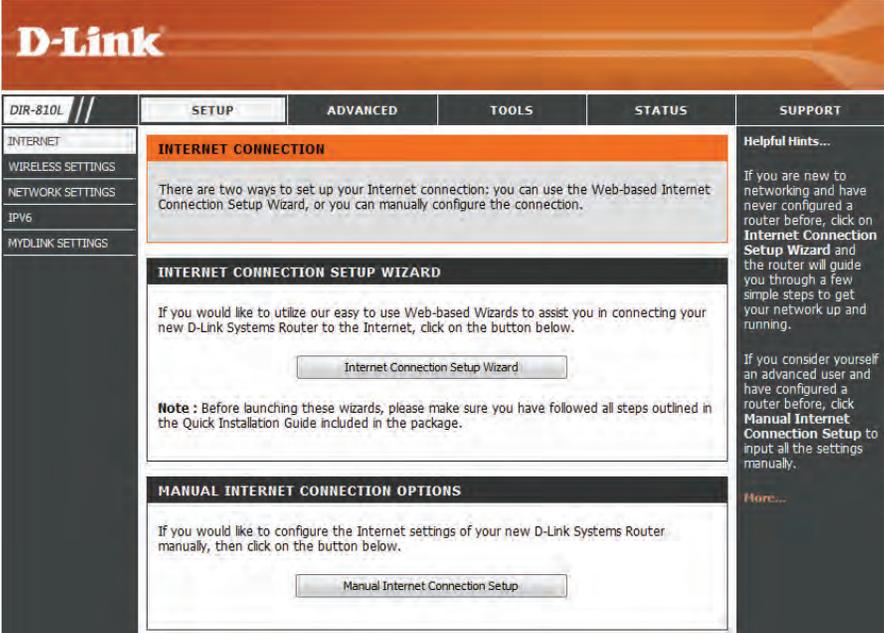
Leave the password blank by default.

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, the text "Login to the router :" is displayed. There are two input fields: "User Name :" with the text "Admin" entered, and "Password :". To the right of the password field is a "Login" button.

Internet Connection Setup

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.

Click **Manual Internet Connection Setup** to configure your connection manually and continue to the next page.



The screenshot displays the D-Link DIR-810L web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists menu items: INTERNET, WIRELESS SETTINGS, NETWORK SETTINGS, IPV6, and MYDLINK SETTINGS. The main content area is titled "INTERNET CONNECTION" and contains the following sections:

- INTERNET CONNECTION**: A header section with a sub-header "INTERNET CONNECTION" and a text box stating: "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 SETUP WIZARD**: A section with a sub-header "INTERNET CONNECTION SETUP WIZARD" and a text box: "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".
- MANUAL INTERNET CONNECTION OPTIONS**: A section with a sub-header "MANUAL INTERNET CONNECTION OPTIONS" and a text box: "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".

On the right side of the interface, there is a "Helpful Hints..." section with two paragraphs of text and a "More..." link.

Internet Connection Setup Wizard

When configuring the router for the first time, we recommend that you use the **Internet Connection Setup Wizard**, and follow the instructions on the screen. This wizard is designed to provide users with a quick and easy method to configure the Internet Connectivity of this router.

At any time during the Internet Connection Setup Wizard, users can click on the **Cancel** button to discard any changes made and return to the main Internet page. Also users can click on the **Prev** button, to return to the previous window for re-configuration.

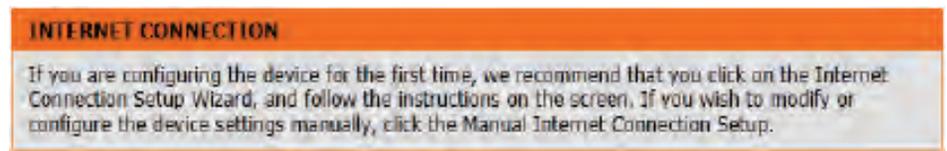
Welcome:

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

Step 1: Set Your Password

By default, the D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please enter and verify a password in the spaces provided. The two passwords must match. You should also make a record of this password for future reference.

Click **Next** to continue.



Step 2: Select Your Time Zone

Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

Click **Next** to continue.

Step 3: Internet Connection

Here the user will be able to configure the Internet connectivity used by this device. If your ISP connection is listed in the drop-down menu, select it and click **Next**. If your ISP connection is not listed then you can proceed to select any of the other manual Internet connection methods listed below.

The following internet connection types will be available for configuration:

Dynamic IP Address: Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

PPPoE: Choose this option if your Internet connection requires a PPPoE username and password to access the internet. Most DSL modems use this type of connection.

PPTP: Choose this option if your Internet connection requires a PPTP username and password to access the internet.

L2TP: Choose this option if your Internet connection requires an L2TP username and password to access the internet.

Static IP Address: Choose this option if your Internet Service Provider provided you with IP Address information that has to be manually configured.

The screenshot shows a configuration window titled "STEP 2: SELECT YOUR TIME ZONE". The text inside reads: "Select the appropriate time zone for your location. This information is required to configure the time-based options for the router." Below this text is a dropdown menu labeled "Time Zone" with the value "(GMT+08:00) Taipei" selected. At the bottom of the window are four buttons: "Prev", "Next", "Cancel", and "Connect".

The screenshot shows a configuration window titled "STEP 3: CONFIGURE YOUR INTERNET CONNECTION". The text inside reads: "Your Internet Connection could not be detected, please select your Internet Service Provider (ISP) from the list below. If your ISP is not listed; select the 'Not Listed or Don't Know' option to manually configure your connection." Below this text is a dropdown menu with "Not Listed or Don't Know" selected. Further down, it says: "If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:". There are five radio button options, each with a description: "DHCP Connection (Dynamic IP Address)", "Username / Password Connection (PPPoE)", "Username / Password Connection (PPTP)", "Username / Password Connection (L2TP)", and "Static IP Address Connection". At the bottom of the window are four buttons: "Prev", "Next", "Cancel", and "Connect".

Step 3: Internet Connection (Dynamic IP Address)

After selecting the Dynamic IP Address Internet connection method, the following page will appear.

The following parameters will be available for configuration:

- MAC Address:** Enter the MAC address of the Internet gateway (plugged into the Internet port of this device) here.
- Copy Button:** If the configuration PC also acts as the Internet gateway, then click on the **Copy Your PC's MAC Address** button to copy the PC's MAC address into the space provided. If you're not sure, leave the MAC Address field blank.
- Host Name:** Enter the host name used here. You may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

Click **Next** to continue.

Step 3: Internet Connection (PPPoE)

After selecting the PPPoE Internet connection method, the following page will appear:

The following parameters will be available for configuration:

- Address Mode:** Choose the IP address mode for your PPPoE connection.
- IP Address:** If you are using **Static PPPoE**, enter the IP address provided by your ISP.
- User Name:** Enter the PPPoE account user name used here. This information is given by the ISP.
- Password:** Enter the PPPoE account password used here. This information is given by the ISP.
- Name:** You may be required to enter a Service Name by your ISP.

DHCP CONNECTION (DYNAMIC IP ADDRESS)

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

MAC Address : 00:18:E7:95:7E:DD (optional)
Copy Your PC's MAC Address

Host Name : DIR-810L

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

Prev Next Cancel Connect

SET USERNAME AND PASSWORD CONNECTION (PPPOE)

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

Address Mode : Dynamic PPPoE Static IP

IP Address : 0.0.0.0

User Name :

Password :

Verify Password :

Service Name : (optional)

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

Prev Next Cancel Connect

Step 3: Internet Connection (PPTP)

After selecting the PPTP Internet connection method, the following page will appear:

The following parameters will be available for configuration:

Address Mode: Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPTP usually requires a Dynamic IP configuration.

PPTP IP Address: Enter the PPTP IP address used here. This option is only available if **Static IP** is selected.

PPTP Subnet Mask: Enter the PPTP Subnet Mask used here.

PPTP Gateway IP Address: Enter the PPTP Gateway IP address used here.

PPTP Server IP Address: Enter the PPTP Server IP address used here. This is normally the same as the PPTP Gateway IP address.

User Name: Enter the PPTP username used here.

Password: Enter the PPTP password used here.

Verify Password: Re-enter the PPTP password used here.

SET USERNAME AND PASSWORD CONNECTION (PPTP)

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

Address Mode : Dynamic IP Static IP

PPTP IP Address : 0.0.0.0

PPTP Subnet Mask : 0.0.0.0

PPTP Gateway IP Address : 0.0.0.0

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

User Name :

Password :

Verify Password :

Prev Next Cancel Connect

Click **Next** to continue.

Step 3: Internet Connection (L2TP)

After selecting the L2TP Internet connection method, the following page will appear:

The following parameters will be available for configuration:

Address Mode: Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. L2TP usual requires a Dynamic IP configuration.

L2TP IP Address: Enter the L2TP IP address used here. This option is only available if **Static IP** is selected.

L2TP Subnet Mask: Enter the L2TP Subnet Mask used here.

L2TP Gateway IP Address: Enter the L2TP Gateway IP address used here.

L2TP Server IP Address: Enter the L2TP Server IP address used here. This is normally the same as the L2TP Gateway IP address.

User Name: Enter the L2TP username used here.

Password: Enter the L2TP password used here.

Verify Password: Re-enter the L2TP password used here.

Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.

Address Mode : Dynamic IP Static IP

L2TP IP Address : 0.0.0.0

L2TP Subnet Mask : 0.0.0.0

L2TP Gateway IP Address : 0.0.0.0

L2TP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify Password :

Prev Next Cancel Connect

Step 3: Internet Connection (Static IP Address)

After selecting the Static IP Address Internet connection method, the following page will appear:

The following parameters will be available for configuration:

IP Address: Enter the Static IP address provided by the ISP here.

Subnet Mask: Enter the Subnet Mask provided by the ISP here.

Gateway Address: Enter the Gateway IP address provided by the ISP here.

Primary DNS Address: Enter the Primary DNS IP address used here.

Secondary DNS Address: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

Setup Complete!

This is the last page of the Internet Connection Setup Wizard.

Click the **Connect** button to save your settings.

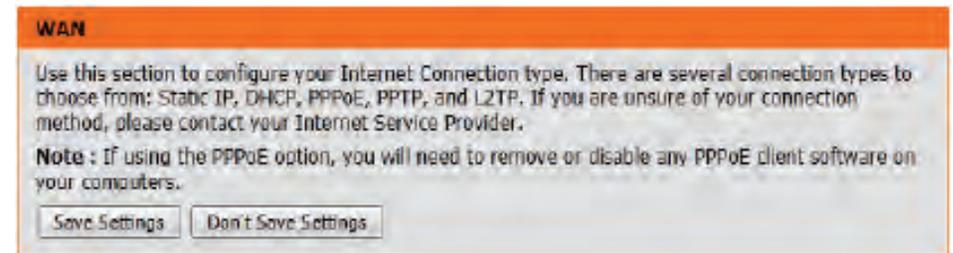
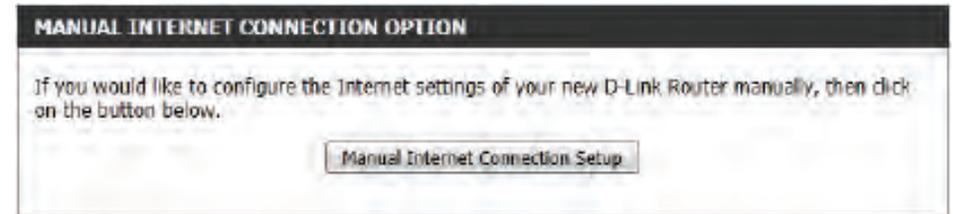
The screenshot shows a window titled "SET STATIC IP ADDRESS CONNECTION". Below the title bar, there is a warning message: "To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP." Below the warning, there are five input fields, each with a label and a value of "0.0.0.0": "IP Address", "Subnet Mask", "Gateway Address", "Primary DNS Address", and "Secondary DNS Address". At the bottom of the window, there are four buttons: "Prev", "Next", "Cancel", and "Connect".

The screenshot shows a window titled "SETUP COMPLETE!". Below the title bar, there is a message: "The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings." At the bottom of the window, there are four buttons: "Prev", "Next", "Cancel", and "Connect".

Internet (Manual Setup)

On this page the user can configure the Internet connection settings manually. To access the Manual Internet Connection Setup page, click on the **Manual Internet Connection Setup** button. On this page there are multiple parameters that can be configured regarding the Internet Connection setup.

At any stage throughout the wizard, users can save the current configuration by clicking on the **Save Settings** button. If you wish to discard the changes made, click on the **Don't Save Settings** button.



Internet Connection Type

In this section, the user can select from a list of Internet connection types that can be configured and used on this router. Options to choose from are **Static IP, Dynamic IP, PPPoE, PPTP, L2TP, and DS-Lite**.

After selecting a specific Internet connection type, this page will automatically refresh and provide unique fields to configure related to the specified Internet connection type.

My Internet Connection is: Dynamic IP (DHCP)

The default WAN configuration for this router is Dynamic IP (DHCP). This option allows the router to obtain an IP address automatically from the device that is connected to the Internet port.

Note: If you're not sure about the type of Internet Connection you have, please contact your Internet Service Provider (ISP) for assistance.

After selecting Dynamic IP, the following parameters will be available for configuration:

Advanced DNS Service: Check the box to enable Advanced DNS Service

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

Use Unicasting: Tick this option if your ISP uses the unicast method to provide IP addresses.

Primary DNS: Enter the Primary DNS IP address used here.

Secondary DNS: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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

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 **Copy 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 :

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 :

Manual 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.

My Internet Connection: Select **Static IP** to manually enter the IP settings supplied by your ISP.

Advanced DNS Service: Check the box to enable Advanced DNS Service.

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

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 **Copy 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 :

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 :

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 in this case. This option is typically used for DSL services. Make sure to remove any existing 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.

Advanced DNS Service: Check the box to enable Advanced DNS Service.

Address Mode: Here the user can specify whether this Internet connection requires the use of a **Dynamic** or **Static IP** address. PPPoE usually requires a Dynamic IP configuration.

IP Address: Enter the PPPoE IP address used here. This option is only available if **Static IP** is selected.

Username: Enter the PPPoE account user name used here. This information is given by the ISP.

Password: Enter the PPPoE account password used here. This information is given by the ISP.

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

Service Name: This optional field enables the user to enter a service name to identify this Internet connection here.

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page.

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 :

PPPOE INTERNET CONNECTION TYPE

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

Address Mode Dynamic IP Static IP

IP Address :

Username :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : Always on On demand Manual

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity.

Primary DNS Server: Enter the Primary DNS IP address used here.

Secondary DNS Server: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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

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 **Copy Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Maximum Idle Time :	<input type="text" value="5"/>	(minutes, 0=infinite)
Primary DNS Server :	<input type="text" value="0.0.0.0"/>	(optional)
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>	(optional)
MTU :	<input type="text" value="1492"/>	(bytes) MTU default = 1492
MAC Address :	<input type="text" value="00:18:E7:95:7E:DD"/>	
	<input type="button" value="Copy Your PC's 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.

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

Advanced DNS Service: Check the box to enable Advanced DNS Service.

Address Mode: Here the user can specify whether this Internet connection requires the use of a **Dynamic** or **Static IP** address. PPTP usually requires a Dynamic IP configuration.

PPTP IP Address: Enter the PPTP IP address used here. This option is only available if Static IP is selected.

PPTP Subnet Mask: Enter the PPTP Subnet Mask used here.

PPTP Gateway IP Address: Enter the PPTP Gateway IP address used here.

PPTP Server IP Address: Enter the PPTP Server IP address used here. This is normally the same as the PPTP Gateway IP address.

Username: Enter the PPTP username used here.

Password: Enter the PPTP password used here.

Verify Password: Re-enter the PPTP password used here.

Reconnect Mode: Use the radio buttons to specify the reconnect mode.

The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the New Schedule button to open the Schedules page. Schedules will be discussed later.

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

INTERNET CONNECTION TYPE

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

My Internet Connection is : PPTP (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 :

PPTP INTERNET CONNECTION TYPE

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

Address Mode Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server: Enter the Primary DNS IP address used here.

Secondary DNS Server: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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.

The screenshot shows a network configuration interface with the following fields and controls:

- Primary DNS Server :** A text input field containing the value "0.0.0.0".
- Secondary DNS Server :** A text input field containing the value "0.0.0.0".
- MTU :** A text input field containing the value "1400", followed by the text "(bytes) MTU default = 1400".
- MAC Address :** A text input field containing the value "00:18:E7:95:7E:DD".
- Copy Your PC's MAC Address**: A button located below the MAC Address field.

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.

My Internet Connection: Select **L2TP (Username/Password)** from the drop-down menu.

Advanced DNS Service: Check the box to enable Advanced DNS Service.

Address Mode: Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. L2TP usual requires a Dynamic IP configuration.

L2TP IP Address: Enter the L2TP IP address used here. This option is only available if Static IP is selected.

L2TP Subnet Mask: Enter the L2TP Subnet Mask used here.

L2TP Gateway IP Address: Enter the L2TP Gateway IP address used here.

L2TP Server IP Address: Enter the L2TP Server IP address used here. This is normally the same as the L2TP Gateway IP address.

Username: Enter the L2TP username used here.

Password: Enter the L2TP password used here.

Verify Password: Re-enter the L2TP password used here.

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the New Schedule button to open the Schedules page. Schedules will be discussed later.

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 INTERNET CONNECTION TYPE

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

Address Mode Dynamic IP Static IP

L2TP IP Address :

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

Primary DNS Server: Enter the Primary DNS IP address used here.

Secondary DNS Server: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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.

Maximum Idle Time :	<input type="text" value="5"/>	(minutes, 0=infinite)
Primary DNS Server :	<input type="text" value="0.0.0.0"/>	
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>	
MTU :	<input type="text" value="1400"/>	(bytes) MTU default = 1400
MAC Address :	<input type="text" value="00:18:E7:95:7E:DD"/>	
<input type="button" value="Copy Your PC's MAC Address"/>		

Internet Setup

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, the user can 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.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

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 : 192.168.0. (optional)

WAN IPv6 Address :

IPv6 WAN Default Gateway :

Wireless Connection Setup Wizard

On this page the user can configure the Wireless settings for this device. There are three ways to configure Wireless using this router. Firstly, the user can use of the quick and easy **Wireless Connection Setup Wizard**. Secondly, the user can choose Wi-Fi Protected Setup. Lastly, the user can configure the Wireless settings manually.

Wireless Settings: Wireless Connection Setup Wizard

The Wireless Connection Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to configure the wireless settings of this router. It is highly recommended to customize the wireless network settings to fit into your environment and to add higher security.

To initiate the **Wireless Connection Setup Wizard** click on the Wireless Connection Setup Wizard button.

Step 1: In this step, the user must enter a custom Wireless Network Name or SSID. Enter the new **Network Name (SSID)** in the appropriate space provided.

By default, the SSID selected for the **2.4GHz** Network Name will be the same for the **5GHz** Network Name. Users can check the **Manually set 5GHz band Network Name(SSID)** checkbox to specify a different SSID for the **5GHz** band.

Users can choose between two wireless security wizard configurations. The user can select **Automatically assign a network key**, by which the router will automatically generate a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods; or the user can select **Manually assign a network key** by which the user will be prompted to manually enter a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods.

At any stage during this wizard, you can click on the **Prev** button to return to the previous page, click on the **Next** button to continue to the next page, or click on the **Cancel** button to discard the changes made and return to the main wireless 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.

STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Give your network a name, using up to 32 characters.

Network Name (SSID) 2.4GHz Band:

Manully set 5GHz band Network Name(SSID)

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 (also called WEP or WPA key) to your network.

Manually assign a network key
Use this options if you prefer to create our own key.

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

Prev Next Cancel

Step 2: This step will only be available if the user selected **Manually assign a network key** in the previous step. Here the user can manually enter the WPA/WPA2 pre-shared key in the **Wireless Security Password** space provided. The key entered must be between 8 and 63 characters long. Remember, this key will be used when wireless clients connect to this device, so it is important to make a record of this key to prevent trouble accessing your wireless network in the future. If you wish to use the same Wireless Security Password for both 2.4GHz and 5GHz bands, **tick** the option provided. If not selected, you need to input two separate Wireless Security Passwords for each individual Wireless band.

Click on the **Next** button to advance to the next step.

Setup Complete: The wireless configuration information will be summarized on this page. It is recommended that you check the correctness of these settings and make a record of the information listed on this page for future reference.

Click on the **Save** button to advance to complete the setup wizard and save the changes made.

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 following guidelines

- Between 8 and 63 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 :

5GHz 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.

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.

Wireless Band : 2.4GHz Band

Wireless Network Name (SSID) : dlink-ecb8

Security Mode : Auto (WPA or WPA2) - Personal

Cipher Type : TKIP and AES

Pre-Shared Key : 2c2dbdbe54

Wireless Band : 5GHz Band

Wireless Network Name (SSID) : dlink-media-ecba

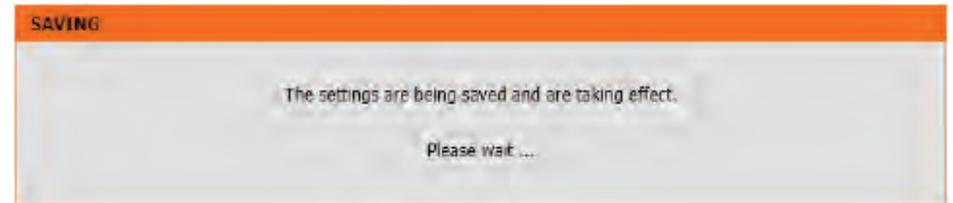
Security Mode : Auto (WPA or WPA2) - Personal

Cipher Type : TKIP and AES

Pre-Shared Key : 2c2dbdbe54

After clicking the **Save** button, the device will save the settings made and return to the main wireless page.

End of Wizard.



Wi-Fi Protected Setup Wizard

Wireless Settings: Wi-Fi Protected Setup Wizard

If your Wireless Clients support the W-Fi Protected Setup (WPS) connection method, this WPS Wizard can be used to initiate a secure wireless connection between this device and wireless clients with a simple click of the WPS button. The Wi-Fi Protected Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to connect wireless clients to this router securely using the WPS method.

To initiate the Wi-Fi Protected Setup Wizard click on the **Add Wireless Device with WPS** button.

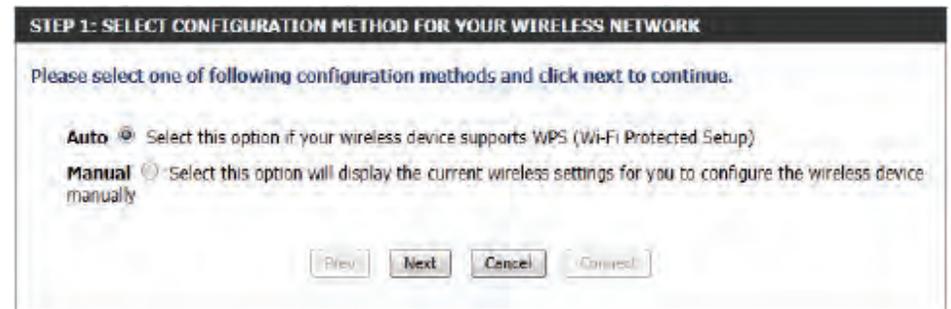
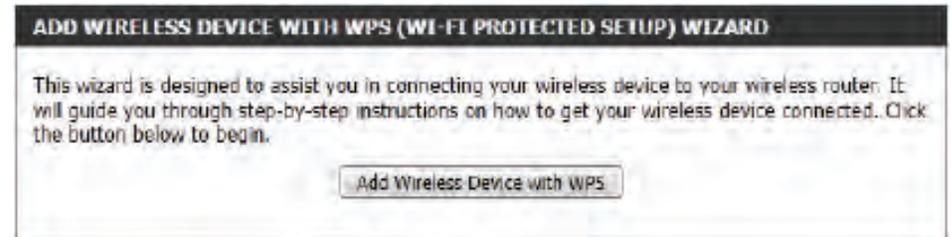
Step 1: In this step there are two options to choose from. You can choose **Auto** if the wireless client supports WPS, or **Manual** if the wireless client does not support WPS.

At any stage during this wizard, you can click on the **Prev** button to return to the previous page, click on the **Next** button to continue to the next page, or click on the **Cancel** button to discard the changes made and return to the main wireless page.

Step 2 - Auto: After selecting **Auto**, the following page will appear.

There are two ways to add a wireless device which supports WPS. Firstly, the Personal Identification Number (**PIN**) method will prompt you to enter the PIN code which was provided with your wireless device. This PIN code should be identical on the wireless client. Secondly, the Push Button Configuration (**PBC**) method will allow the wireless client to connect to your router by pressing the WPS button on the client device.

Choose the preferred method of WPS and click on the **Connect** button to establish a connection.



Step 2 - Manual: After selecting **Manual**, the following page will appear. On this page users can view the wireless configuration of this router. The wireless clients should configure their wireless settings to be identical to the settings displayed on this page for a successful connection. This option is for wireless clients that do not support the WPS Push Button method to connect to this router.

It is recommended that you make a record of this information for future reference. Click on the **OK** button to the Wireless Settings page.

End of Wizard.

STEP 2: CONNECT YOUR WIRELESS DEVICE

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.

2.4GHz Band SSID: **dlink-7EDC**
Security Mode: **Auto (WPA or WPA2) - Personal**
Cipher Type : **TKIP/AES**
Pre-shared Key: **00000000**

5GHz Band SSID: **dlink-7EDE-media**
Security Mode: **Auto (WPA or WPA2) - Personal**
Cipher Type : **TKIP/AES**
Pre-shared Key: **00000000**

Manual wireless network setup

Wireless Settings: Manual Wireless Network Setup

The Manual Wireless Network Setup option allows users to configure the wireless settings of this device manually. This option is for advanced users and includes all parameters that can be configured for wireless connectivity.

To initiate the Manual Wireless Setup page, click on the **Manual Wireless Connection Setup** button.

At any stage during setup, you can click on the **Save Settings** button to save the current configuration, or click on the **Don't Save Settings** button to discard any changes made and return to the main wireless setup page.

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.

WIRELESS NETWORK

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

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Manual Setup - 2.4Ghz Band

The following parameters will be available for configuration:

Wireless Band: Displays the wireless band being configured. The following configuration relates to the **2.4GHz** band.

Enable Wireless: Check the box to enable the wireless function at all times. If you do not want to use wireless, uncheck the box to disable all wireless functions. To set a schedule for the times when you want the wireless network to be available, click on the **Add New** button to specify a new schedule.

Wireless Network Name: The 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: Here the user can manually select the preferred wireless standard to use for this wireless network. You should select the 802.11 mode according to the capabilities of the wireless clients/devices which will be accessing this network. If only 802.11n devices will be accessing your network, it is recommended to set the 802.11 mode to **802.11n only**.

Enable Auto Channel Scan: The auto channel selection setting can be selected to allow this device to choose the wireless channel with the least amount of interference.

Wireless Channel: If Auto Channel Scan had been disabled, you can select your preferred wireless channel. By default the channel is set to 1. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Transmission Rate: Select the transmission rate. It is strongly suggested that **Best (Automatic)** is selected for best performance.

Channel Width: When using the 802.11n frequency band, users have an option to choose between a 20MHz or 20/40MHz bandwidth.

Visibility Status: This option allows you to adjust the visibility of your SSID. If **Visible** is selected, the SSID of your wireless network will be visible to any wireless clients within range of the signal. If **Invisible** mode is selected, clients must search for the SSID of your wireless network manually in order to connect to the network.

WIRELESS NETWORK SETTINGS

Wireless Band : 2.4GHz Band

Enable Wireless: Always

Wireless Network Name: dlink-7EDC (Also called the SSID)

802.11 Mode: Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan:

Wireless Channel: 2.437 GHz - CH 6

Transmission Rate : Best (automatic)

Channel Width: Auto 20/40 MHz

Visibility Status: Visible Invisible

By default the wireless security of this router will be disabled. In this option the user can enable or disable wireless security for the frequency band 2.4GHz. There are two types of encryption that can be used: WEP or WPA/WPA2. For further information on these security types, please refer to “Wireless Security” on page 53

Wireless Security Mode: WEP

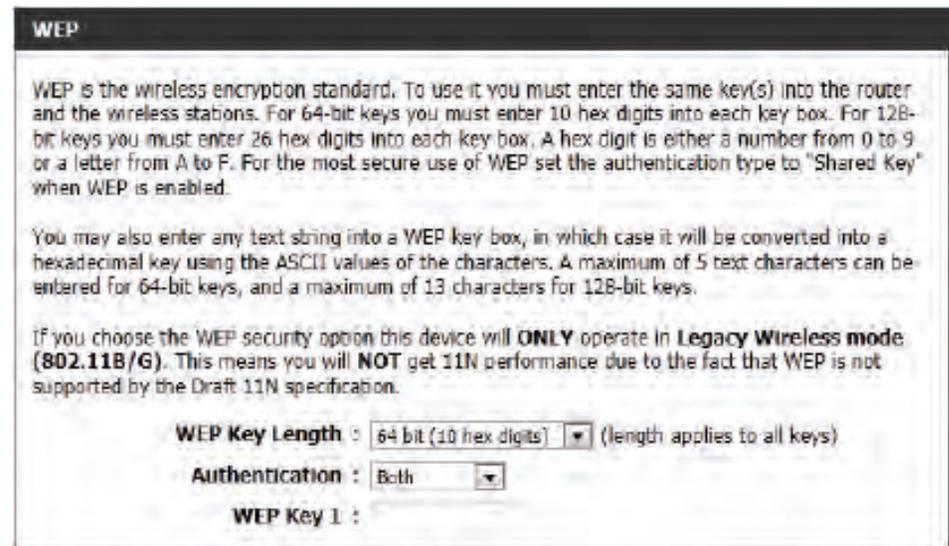
Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. WEP is considered to be a relatively weak security method, however it provides more protection than an unsecured network. Older wireless adapters may only support WEP encryption. It is recommended that this method is used only if your wireless clients do not support WPA.

The following parameters are available for configuration:

WEP Key Length: Here the user can specify to either use a 64Bit or a 128Bit encrypted key.

Authentication: Authentication is a process by which the router verifies the identity of a network device that is attempting to join the wireless network. There are two types authentication for this device when using WEP. **Open System** allows all wireless devices to communicate with the router before they are required to provide the encryption key needed to gain access to the network. **Shared Key** requires any wireless device attempting to communicate with the router to provide the encryption key needed to access the network before they are allowed to communicate with the router.

WEP Key 1: Enter the WEP key used here. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.



Wireless Security Mode: WPA-Personal

Wi-Fi Protected Access (WPA) is the most advanced wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a passphrase (Pre-Shared Key) for security.

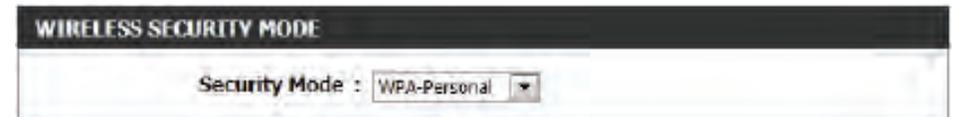
The following parameters will be available for configuration:

WPA Mode: WPA is an older standard; select this option if the clients that will be used with the router only support this older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), or Both (TKIP and AES).

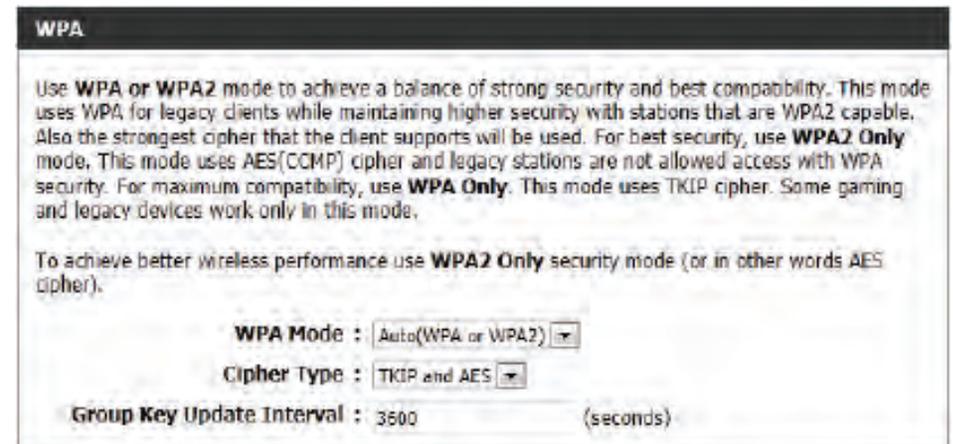
Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Pre-Shared Key: Enter the password to be used for the wireless network here. This password is required by wireless clients for them to be able to connect to the wireless network successfully.



WIRELESS SECURITY MODE

Security Mode : WPA-Personal



WPA

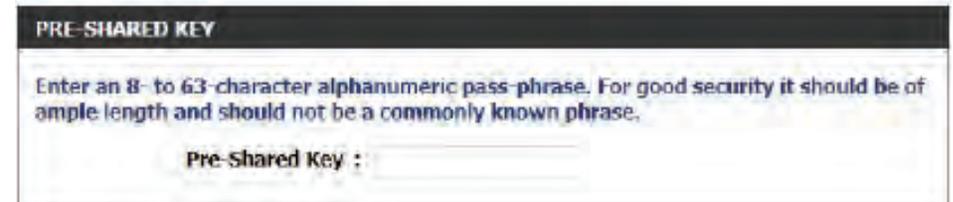
Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode.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

Wireless Security Mode: WPA-Enterprise

WPA-Enterprise is a more sophisticated level of wireless security which requires a RADIUS Authentication Server. This form of security is used primarily in medium to large-scale network environments.

The following parameters will be available for configuration:

WPA Mode: WPA is an older standard; select this option if the clients that will be used with the router only support this standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES).

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Authentication Timeout: Specifies the amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: When the user chooses to use the EAP authentication framework, the RADIUS server's IP address can be entered here.

RADIUS Server Port: When the user chooses to use the EAP authentication framework, the RADIUS server's port number can be entered here.

RADIUS Server Shared Secret: Enter the shared secret (password) used here. This password needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

MAC Address Authentication: Select this option to include authentication of clients according to their MAC address.

The screenshot shows the configuration page for WPA-Enterprise. At the top, there are three settings: **WPA Mode** set to 'Auto(WPA or WPA2)', **Cipher Type** set to 'TKIP and AES', and **Group Key Update Interval** set to '3600 (seconds)'. Below this is a section titled **EAP (802.1X)** with a note: 'When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.' The settings in this section include: **Authentication Timeout** (60 minutes), **RADIUS server IP Address** (0.0.0.0), **RADIUS server Port** (1812), **RADIUS server Shared Secret** (empty field), **MAC Address Authentication** (checked), and **Optional backup RADIUS server** settings: **Second RADIUS server IP Address** (0.0.0.0), **Second RADIUS server Port** (1812), **Second RADIUS server Shared Secret** (empty field), and **Second MAC Address Authentication** (checked). A '<<Advanced' button is visible below the MAC Address Authentication checkbox.

Optional backup RADIUS This option allows users to specify a secondary server: RADIUS server to be used in the event that the primary RADIUS server fails. Enter the information for the secondary server in the same manner as the primary server described in the steps on the previous page

<<Advanced

Optional backup RADIUS server:

Second RADIUS server IP Address:

Second RADIUS server Port:

Second RADIUS server Shared Secret:

Second MAC Address Authentication:

Manual Setup - 5Ghz Band

The following parameters will be available for configuration:

Wireless Band: Displays the wireless band being configured. The following configuration relates to the **5GHz** band.

Enable Wireless: Check the box to enable the wireless function at all times. If you do not want to use wireless, uncheck the box to disable all wireless functions. To set a schedule for the times when you want the wireless network to be available, click on the **Add New** button to specify a new schedule.

The screenshot shows the 'WIRELESS NETWORK SETTINGS' interface. The 'Wireless Band' is set to '5GHz Band'. The 'Enable Wireless' checkbox is checked, and the schedule is set to 'Always'. The 'Wireless Network Name' is 'dlink-media-ecba'. The '802.11 Mode' is 'Mixed 802.11ac'. The 'Enable Auto Channel Scan' checkbox is checked. The 'Wireless Channel' is set to '36'. The 'Transmission Rate' is 'Best (automatic)'. The 'Channel Width' is '20/40/80 MHz (Auto)'. The 'Visibility Status' is 'Visible'.

Wireless Network Name: The 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: Here the user can manually select the preferred frequency band to use for this wireless network.

Enable Auto Channel Scan: The auto channel selection setting can be selected to allow this device to choose the channel with the least amount of interference.

Wireless Channel: If Auto Channel Scan is not enabled, users can manually select a wireless channel. By default the channel is set to 36. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Transmission Rate: Select the transmission rate. It is strongly suggested to select Best (Automatic) for best performance.

Channel Width: When using the 802.11n frequency band, user have an option to choose between a 20 MHz, 20/40 MHz, or 20/40/80 MHz bandwidth for 802.11ac.

Visibility Status: This option allows you to adjust the visibility of your SSID. If **Visible** is selected, the SSID of your wireless network will be visible to any wireless clients within range of the signal. If **Invisible** mode is selected, clients must search for the SSID of your wireless network manually in order to connect to the network.

By default the wireless security of this router will be disabled. In this option the user can enable or disable wireless security for the frequency band 2.4GHz. There are two types of encryption that can be used: WEP or WPA/WPA2. For further information on these security types, please refer to “Wireless Security” on page 53

Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. WEP is considered to be a relatively weak security method, however it provides more protection than an unsecured network. Older wireless adapters may only support WEP encryption. It is recommended that this method is used only if your wireless clients do not support WPA.

The following parameters will be available for configuration:

WEP Key Length: Here the user can specify to either use a 64Bit or a 128Bit encrypted key.

Authentication: Authentication is a process by which the router verifies the identity of a network device that is attempting to join the wireless network. There are two types authentication for this device when using WEP. **Open System** allows all wireless devices to communicate with the router before they are required to provide the encryption key needed to gain access to the network. **Shared Key** requires any wireless device attempting to communicate with the router to provide the encryption key needed to access the network before they are allowed to communicate with the router.

WEP Key 1: Enter the WEP key used here. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)

Authentication : Both

WEP Key 1 :

Wireless Security Mode: WPA-Personal

Wi-Fi Protected Access (WPA) is the most advanced wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a passphrase (Pre-Shared Key) for security.

The following parameters will be available for configuration:

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES).

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Pre-Shared Key: Enter the password to be used for the wireless network here. This password is required by wireless clients for them to be able to connect to the wireless network successfully.

The screenshot shows the 'WIRELESS SECURITY MODE' configuration page. At the top, 'Security Mode' is set to 'WPA-Personal'. Below this is the 'WPA' section, which contains explanatory text about WPA and WPA2 modes. It includes a 'WPA Mode' dropdown set to 'Auto(WPA or WPA2)', a 'Cipher Type' dropdown set to 'TKIP and AES', and a 'Group Key Update Interval' field set to '3600' seconds. The bottom section is 'PRE-SHARED KEY', which contains instructions to enter an 8- to 63-character alphanumeric passphrase and a corresponding text input field.

Wireless Security Mode: WPA-Enterprise

WPA-Enterprise is a more sophisticated level of wireless security which requires a RADIUS Authentication Server. This form of security is used primarily in medium to large-scale network environments.

The following parameters will be available for configuration:

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support this older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES).

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Authentication Timeout: Specifies the amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: When the user chooses to use the EAP authentication framework, the RADIUS server's IP address can be entered here.

RADIUS Server Port: When the user chooses to use the EAP authentication framework, the RADIUS server's port number can be entered here.

RADIUS Server Shared Secret: Enter the shared secret (password) used here. This password needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

MAC Address Authentication: Select this option to include authentication of clients according to their MAC address.

Authentication:

The screenshot shows the configuration page for WPA-Enterprise. At the top, there are three settings: **WPA Mode** set to 'Auto(WPA or WPA2)', **Cipher Type** set to 'TKIP and AES', and **Group Key Update Interval** set to '3600 (seconds)'. Below this is a section titled **EAP (802.1X)** with a sub-header: 'When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.' The settings in this section include: **Authentication Timeout** (60 minutes), **RADIUS server IP Address** (0.0.0.0), **RADIUS server Port** (1812), **RADIUS server Shared Secret** (empty field), **MAC Address Authentication** (checked), and a '<<Advanced' button. Below the button is an **Optional backup RADIUS server** section with: **Second RADIUS server IP Address** (0.0.0.0), **Second RADIUS server Port** (1812), **Second RADIUS server Shared Secret** (empty field), and **Second MAC Address Authentication** (checked).

Optional backup RADIUS server: This option allows users to specify a secondary RADIUS server to be used in the event that the primary RADIUS server fails. Enter the information for the secondary server in the same manner as the primary server described in the steps on the previous page

<<Advanced

Optional backup RADIUS server:

Second RADIUS server IP Address:

Second RADIUS server Port:

Second RADIUS server Shared Secret:

Second MAC Address Authentication:

Wireless Security

This section discusses the different levels of security you can use to protect your data from intruders. The DIR-810L 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)
- Wired Equivalent Privacy (WEP)

What is WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP.

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.

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 in order to return to the configuration utility.

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

Device Name: Enter a name for the router.

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.

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-810L has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. If using DHCP, be sure to set your computers to be DHCP clients by setting their TCP/IP settings to **Obtain an IP Address Automatically**. When your wireless devices connect to the router, they will automatically load the TCP/IP settings provided by the DIR-810L. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting device. You must specify the starting and ending address of the IP address pool.

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

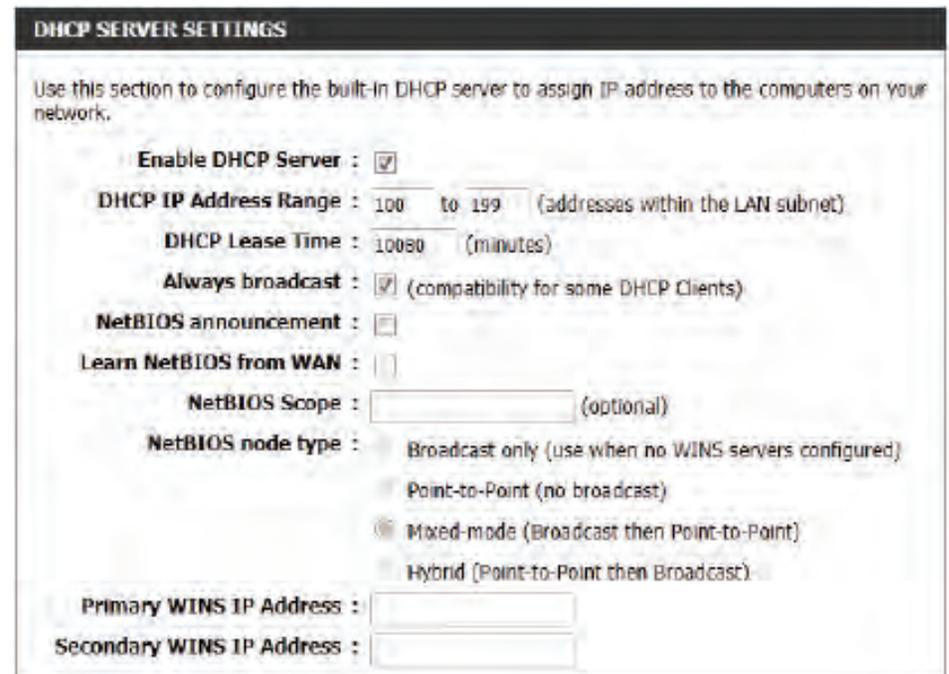
DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

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: If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

NetBIOS Announcement: Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts. NetBIOS allows LAN hosts to discover all other computers within the network, e.g. within Network Neighborhood.



DHCP SERVER SETTINGS

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

Enable DHCP Server :

DHCP IP Address Range : 100 to 199 (addresses within the LAN subnet)

DHCP Lease Time : 10080 (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 :

Learn NetBIOS from WAN: If NetBIOS announcement is switched on, it will cause WINS information to be learned from the WAN side, if available. Turn this setting off to configure manually.

NetBIOS Scope: This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS domain name under which network hosts operate. This setting has no effect if **Learn NetBIOS information from WAN** is activated.

NetBIOS Node: This field indicates how network hosts are to perform NetBIOS name registration and discovery. H-Node indicates a Hybrid-State of operation. First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers. M-Node (default), this indicates a Mixed-Mode of operation. First Broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favours broadcast operations which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN. P-Node indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operations to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server. B-Node indicates to use local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is preferred that you try M-Node operation first. This setting has no effect if the **Learn NetBIOS information from WAN** option is activated.

WINS IP Address: Enter your WINS Server IP address(es).

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 specified 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.

DHCP Reservations List

DHCP Reservations List: Displays any reservation entries. Displays the host name (name of your computer or device), MAC Address, and IP address.

Enable: Check to enable the reservation.

Edit: Click the edit icon to make changes to the reservation entry.

Delete: Click on the trash can icon to remove the reservation from the list.

ADD DHCP RESERVATION

Enable :

Computer Name : << Computer Name ▾

IP Address :

MAC Address :

DHCP RESERVATIONS LIST

Enable	Host Name	MAC Address	IP Address	Edit	Delete
<input checked="" type="checkbox"/>	PM_test01	00:04:23:2c:51:a3	192.168.0.112		

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Hardware Address	Assigned IP	Hostname	Expires	Actions
00:04:23:2c:51:a3	192.168.0.112	PM_test01	Thu Sep 1 19:49:06 2011	Revoke Reserve

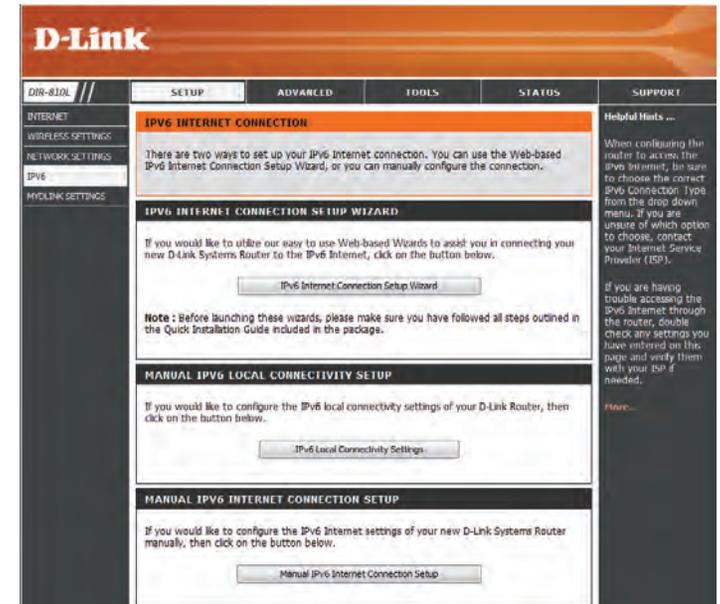
IPv6

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 Web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

For beginner users that have 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.

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.

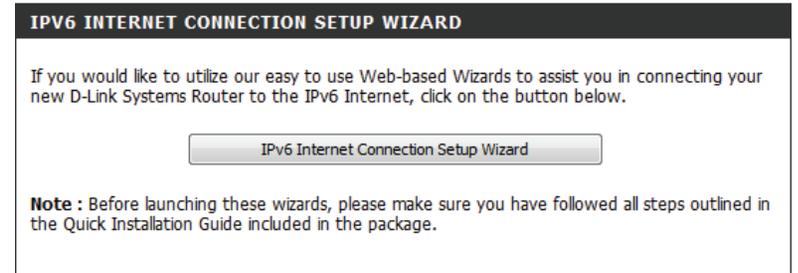
To configure the IPv6 local settings, click on the **IPv6 Local Connectivity Setup** button.



IPv6 Internet Connection Setup Wizard

On this page, the user can configure the IPv6 Connection type using the IPv6 Internet Connection Setup Wizard.

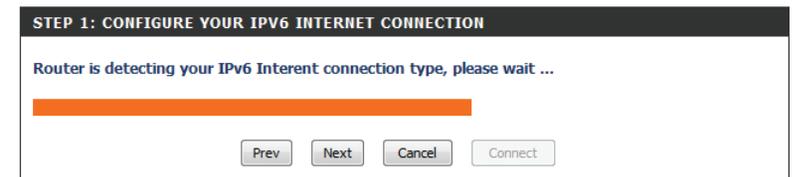
Click the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.



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



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.



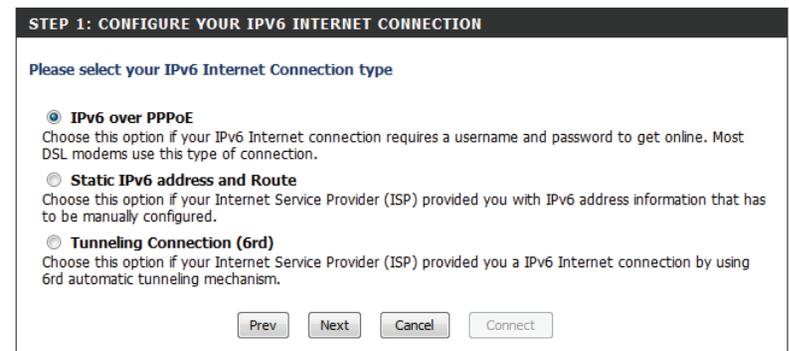
However, if the automatic detection fails, the user will be prompt to either **Try again** or to click on the **Guide me through the IPv6 settings** button to initiate the manual continual of the wizard.



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.



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 access the Internet. 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 its 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.

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

Username :

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 : FE80:0:0:0:218:E7FF:FE95:7EDD

Subnet Prefix Length : 64

Default Gateway :

Primary IPv6 DNS Server :

Secondary IPv6 DNS Server :

LAN IPv6 Address : /64

Prev Next Cancel Connect

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.

The screenshot shows a configuration window titled "SET UP 6RD TUNNELING CONNECTION". Below the title is a message: "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." The form contains several fields: "6rd IPv6 Prefix" with a text input and "/ 32" to its right; "IPv4 Address" with the value "0.0.0.0" and "Mask Length" with the value "0"; "Assigned IPv6 Prefix" with the value "None"; "6rd Border Relay IPv4 Address" with the value "0.0.0.0"; and "IPv6 DNS Server" with an empty text input. At the bottom right are four buttons: "Prev", "Next", "Cancel", and "Connect".

The IPv6 Internet Connection Setup Wizard is complete.

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.

The screenshot shows a confirmation window titled "SETUP COMPLETE!". Below the title is a message: "The IPv6 Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router." At the bottom are four buttons: "Prev", "Next", "Cancel", and "Connect".

IPv6 Local Connectivity Settings

This option can be used to manually configure IPv6 settings for local connectivity. These settings are used only on the local network, and will not be used to access the internet.

MANUAL IPV6 LOCAL CONNECTIVITY SETUP

If you would like to configure the IPv6 local connectivity settings of your D-Link Router, then click on the button below.

[IPv6 Local Connectivity Settings](#)

Enable ULA: Click here to enable Unique Local IPv6 Unicast Addresses settings.

Use Default ULA Prefix: Checking this box will automatically configure the ULA prefix for the default setting.

ULA Prefix: If you wish to choose your own ULA prefix, enter it here.

Current IPv6 ULA Settings: This section will display the current settings for your IPv6 ULA.

IPv6 ULA Settings

Enable ULA :

Use default ULA prefix :

ULA Prefix : /64

Current IPv6 ULA Settings

Current ULA Prefix :

LAN IPv6 ULA :

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</p> <p><input type="radio"/> Use the following DNS address</p> <p>Primary DNS Server : <input type="text"/></p> <p>Secondary 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:FE95:689E/64</p>
ADDRESS AUTOCONFIGURATION SETTINGS
<p>Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.</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:FE95:689F
Subnet Prefix Length :	64
Default Gateway :	
Primary DNS Server :	
Secondary DNS Server :	
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:FE95:689E/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 :	SLAAC + Stateless DHCPv6
Router Advertisement 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 (SLAAC/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 Server :	<input type="text"/>
Secondary DNS Server :	<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:FE95:689E/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.	
Enable automatic IPv6 address assignment :	<input checked="" type="checkbox"/>
Enable Automatic DHCP-PD in LAN :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	SLAAC + Stateless DHCPv6 ▾
Router Advertisement Lifetime:	1440 <input type="text"/> (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
PPPOE	
Enter the information provided by your Internet Service Provider (ISP).	
PPPoE Session:	<input checked="" type="radio"/> Share with IPv4 <input type="radio"/> Create a new session
Address Mode :	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
IP Address :	<input type="text"/>
Username :	<input type="text"/>
Password :	<input type="text"/>
Verify Password :	<input type="text"/>
Service Name :	<input type="text"/> (Optional)
Reconnect Mode :	<input checked="" type="radio"/> Always on <input type="radio"/> On demand <input type="radio"/> Manual
Maximum Idle Time :	5 (minutes, 0=infinite)
MTU :	1492 (bytes)MTU default = 1492
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 Server :	<input type="text"/>
Secondary DNS Server :	<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:FE95:689E/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.You can also enable DHCP-PD to delegate prefixes for router in your LAN.	
Enable automatic IPv6 address assignment :	<input checked="" type="checkbox"/>
Enable Automatic DHCP-PD in LAN :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	SLAAC + Stateless DHCPv6
Router Advertisement Lifetime:	1440 (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 :	
Remote IPv6 Address :	
Local IPv4 Address :	192.168.1.2
Local IPv6 Address :	
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 Server :	
Secondary DNS Server :	
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 :	/64
LAN IPv6 Link-Local Address :	FE80::218:E7FF:FE95:689E/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.	
Enable automatic IPv6 address assignment :	<input checked="" type="checkbox"/>
Enable Automatic DHCP-PD in LAN :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	SLAAC + Stateless DHCPv6
Router Advertisement Lifetime:	1440 (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 :	6to4
6to4 SETTINGS	
Enter the IPv6 address information provided by your Internet Service Provider (ISP).	
6to4 Address :	2002:COA8:0102::COA8:0102
6to4 Relay :	192.88.99.1
Primary DNS Server :	
Secondary DNS Server :	
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 :	2002:COA8:0102:0001::1/64
LAN IPv6 Link-Local Address :	FE80::218:E7FF:FE95:689E/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 :	SLAAC + Stateless DHCPv6
Router Advertisement Lifetime :	60 (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
<p>Choose the mode to be used by the router to the IPv6 Internet.</p> <p>My IPv6 Connection is : <input type="text" value="6rd"/></p>
6RD SETTINGS
<p>Enter the IPv6 address information provided by your Internet Service Provider (ISP).</p> <p>Enable Hub and Spoke Mode : <input checked="" type="checkbox"/></p> <p>6rd Configuration : <input checked="" type="radio"/> 6rd DHCPv4 Option <input type="radio"/> Manual Configuration</p> <p>6rd IPv6 Prefix : <input type="text"/> / <input type="text" value="0"/></p> <p>IPv4 Address: 0.0.0.0 Mask Length: <input type="text" value="0"/></p> <p>Assigned IPv6 Prefix : None</p> <p>6rd Border Relay IPv4 Address : <input type="text" value="0.0.0.0"/></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>LAN IPv6 Address : None</p> <p>LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:7EDC/64</p>
ADDRESS AUTOCONFIGURATION SETTINGS
<p>Use this section to setup IPv6 Autoconfiguration to assign IPv6 addresses to the computers in your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.</p> <p>Enable automatic IPv6 address assignment : <input checked="" type="checkbox"/></p> <p>Autoconfiguration Type : <input type="text" value="SLAAC + Stateless DHCPv6"/></p> <p>Router Advertisement Lifetime : <input type="text" value="10080"/> (minutes)</p>

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.

IPv6 CONNECTION TYPE
Choose the mode to be used by the router to the IPv6 Internet.
My IPv6 Connection is : <input type="text" value="Local Connectivity Only"/>

LAN IPv6 ADDRESS SETTINGS
LAN IPv6 address for local IPv6 communications.
LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64

mydlink™ Settings

The DIR-810L features a new cloud service that pushes information such as firmware upgrade notifications, user activity, and intrusion alerts to the mydlink app on your Android or iOS mobile device. To ensure that your router is up-to-date with the latest features, mydlink will notify you when an update is available for your router. You can also monitor users' online activity with real-time website browsing history, maintaining a safe and secure environment, especially useful for monitoring your children's Internet usage at home.

On this page the user can configure the mydlink settings for this router. This feature will allow you to use the mydlink cloud services, which include online access and management of this router through the mydlink portal website or the mydlink Lite app for iOS and Android mobile devices.

In the **mydlink** section, you can view the registration status of the mydlink account service. The **mydlink Service** field will either display **Registered** or **Non-Registered**.

In the **Register mydlink Service** section, we can register or modify a mydlink account. Click on the **Register mydlink Service** button to initiate this procedure.

After clicking the **Register mydlink Service** button, this window will appear.

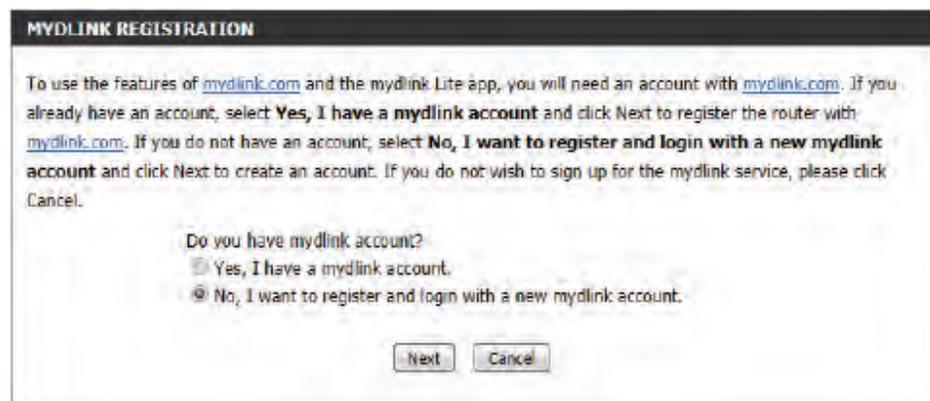
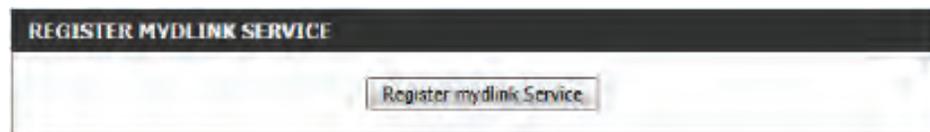
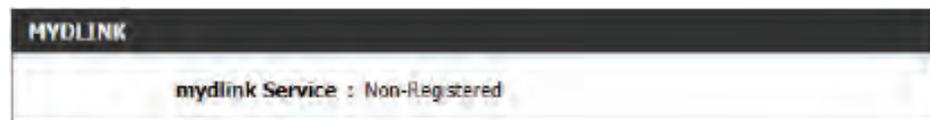
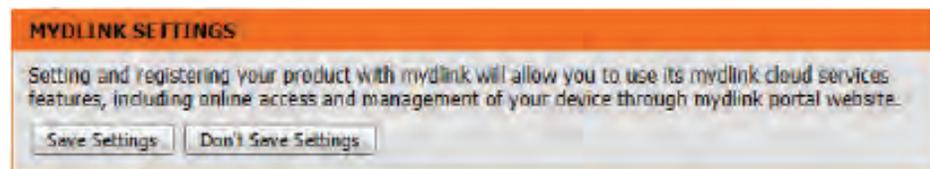
Register mydlink Service Wizard: Step 1

In this section we can select one of two options.

- Select the **'Yes, I have a mydlink account'** option if you already have a mydlink account that you want to use on this router.
- Select the **'No, I want to register and login with a new mydlink account'** option to register a new account and use it on this router.

Click the **Next** button to proceed to the next step.

Click the **Cancel** button to discard the changes made and return to the main page.



Register mydlink Service Wizard: Step 2

When registering a **new account**, the following page appears. The following parameters will be available for configuration:

E-mail Address (Account Name): Enter your e-mail address here. This e-mail address will also become your account name.

Password: Enter your preferred password choice here.

Confirm Password: Re-enter your preferred password choice here.

Last Name: Enter your last name here.

First Name: Enter your first name here.

Accept terms and conditions: Tick this option to accept the mydlink terms and conditions.

Click the **Next** button to proceed to the next step.

Click the **Prev** button to return to the previous step.

Click the **Cancel** button to discard the changes made and return to the main page.



The screenshot shows a web form titled "MYDLINK REGISTRATION" with a dark header. Below the header, it says "Please fulfill the options to complete the registration." The form contains several input fields: "E-mail Address (Account Name)", "Password", "Confirm Password", "Last name", and "First Name". There is a checkbox labeled "I Accept the mydlink terms and conditions." with a blue link. At the bottom, there are three buttons: "Next", "Prev", and "Cancel". A red 'X' icon is visible over the "Confirm Password" field.

When logging in with an **existing account**, the following page appears. The following parameters will be available for configuration:

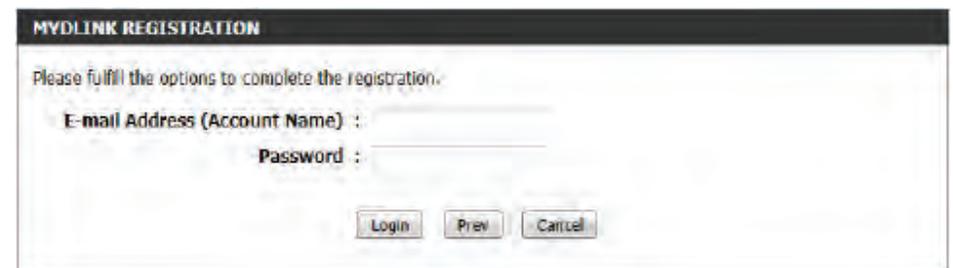
E-mail Address (Account Name): Enter your e-mail address here. This e-mail address will also be your account name.

Password: Enter your preferred password choice here.

Click the **Login** button to login using these account details.

Click the **Prev** button to return to the previous step.

Click the **Cancel** button to discard the changes made and return to the main page.



The screenshot shows a web form titled "MYDLINK REGISTRATION" with a dark header. Below the header, it says "Please fulfill the options to complete the registration." The form contains two input fields: "E-mail Address (Account Name)" and "Password". At the bottom, there are three buttons: "Login", "Prev", and "Cancel".

At any point during this wizard, you can change the preferred language. To change the language, select the desired language option from the **Language** drop-down menu, found on the top right of this page.

End of Wizard



Advanced Virtual Server

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.

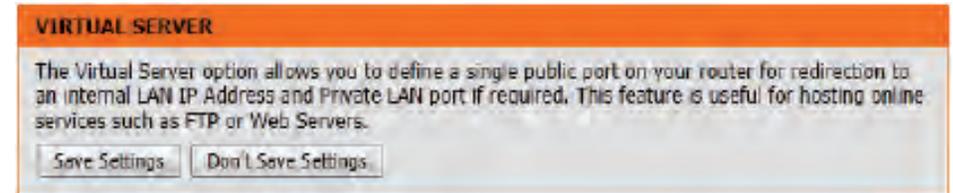
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the "Computer Name" drop-down menu. Select your computer and click 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

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

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

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.



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.

PORT FORWARDING

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

24 — PORT FORWARDING RULES

Remaining number of rules that can be created: 24

	Name	Ports to Open	Schedule
<input type="checkbox"/>	<input type="text"/> <input type="button" value="<<"/> Application Name ▼	TCP <input type="text"/>	Always ▼
<input type="checkbox"/>	<input type="text"/> <input type="button" value="<<"/> Computer Name ▼	UDP <input type="text"/>	Inbound Filter Allow All ▼
<input type="checkbox"/>	<input type="text"/> <input type="button" value="<<"/> Application Name ▼	TCP <input type="text"/>	Always ▼
<input type="checkbox"/>	<input type="text"/> <input type="button" value="<<"/> Computer Name ▼	UDP <input type="text"/>	Inbound Filter Allow All ▼

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-810L. 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-810L 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.

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.

24 — APPLICATION RULES

Remaining number of rules that can be created: 24

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

QoS Engine

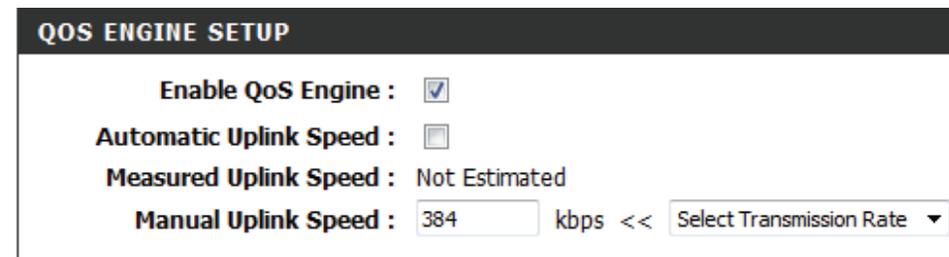
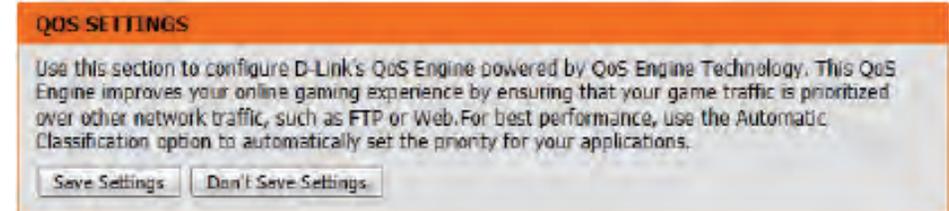
The QoS Engine option helps improve your network performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically. The QoS section contains a queuing mechanism, traffic shaping, and classification. It supports two kinds of queuing mechanisms: Strict Priority Queue (SPQ) and Weighted Fair Queue (WFQ). SPQ will process traffic based on traffic priority. Queue1 has the highest priority and Queue4 has the lowest priority. WFQ will process traffic based on the queue weight. Users can configure each queue's weight. The sum of all the queue's weights must be 100. When surfing the Internet, the system will do traffic shaping based on the uplink and downlink speed. The classification rules can be used to classify traffic to different queues, then SPQ or WFQ will do QoS based on the queue's priority or weight.

The following parameters will be available for configuration:

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

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 define speed as a download/upload pair. For example, 1.5Mbps/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.

Downlink Speed: The speed at which data can be transferred from the ISP to the router. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5Mbps/284Kbits. Using this example, you would enter 1500. Alternatively you can test your downlink speed with a service such as www.dslreports.com.



After specifying the QoS framework used, in the QoS setup section, the user can now create individual rules for scenarios that require the use of traffic control and data priority manipulation.

The following parameters will be available for configuration:

Checkbox: Tick this option to enable the rule specified.

Name: Enter a custom name for the rule being created here. This name is used for identification.

Queue ID: Select the appropriate priority requirement from the drop-down menu that will be applied to this rule. Option to choose from are Highest, Higher, Normal, and Best Effort.

Protocol: Select the protocol used for the application for in the drop-down menu and it will automatically place it in the Protocol field.

Local IP Range: Enter the local IP range used here. This is the IP range of you Local Area Network. The Router's IP cannot be included in this range.

Remote IP Range: Enter the remote IP range used here. This is the IP range of the public network from the Internet Port side. To apply this rule to any IP addresses from the public side, enter the range 0.0.0.1 to 255.255.255.254.

Application Port: Enter the application port number used here.

Click on the **Save Settings** button to accept the changes made. Click on the **Don't Save Settings** button to discard the changes made.

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

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.

24 — MAC FILTERING RULES

Configure MAC Filtering below:
 Turn MAC Filtering ON and ALLOW computers listed to access the network ▾

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

Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as a parental control 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.

The screenshot shows the 'ACCESS CONTROL' configuration page. At the top, there is an orange header with the text 'ACCESS CONTROL'. Below this, a grey box contains the following text: 'The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.' Below the text are two buttons: 'Save Settings' and 'Don't Save Settings'. Below this is another section with a black header 'ACCESS CONTROL'. It contains the text 'Enable Access Control:' followed by a checked checkbox and an 'Add Policy' button. Below this is a 'POLICY TABLE' section with a black header. The table has five columns: 'Enable', 'Policy', 'Machine', 'Filtering', and 'Logged', and a 'Schedule' column with three empty cells.

Access Control Wizard

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

The screenshot shows the 'ADD NEW POLICY' wizard screen. It has a black header with the text 'ADD NEW POLICY'. Below the header, the text reads: 'This wizard will guide you through the following steps to add a new policy for Access Control.' Below this, there is a list of six steps: 'Step 1 - Choose a unique name for your policy', 'Step 2 - Select a schedule', 'Step 3 - Select the machine to which this policy applies', 'Step 4 - Select filtering method', 'Step 5 - Select filters', and 'Step 6 - Configure Web Access Logging'. At the bottom of the screen, there are four buttons: 'Prev', 'Next', 'Save', and 'Cancel'.

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

STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name:

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

STEP 2: SELECT SCHEDULE

Choose a schedule to apply to this policy.

Details:

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

- **Address Type** - Select IP address, MAC address, or Other Machines.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.
- **Machine Address** - Enter the PC MAC address (i.e. 00:00.00.00.00).

STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

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

Address Type: IP MAC Other Machines

IP Address: <<

Machine Address: <<

Machine

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

STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

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

Apply Web Filter:

Apply Advanced Port Filters:

Enter the rule:

Enable - Check to enable the rule.

Name - Enter a name for your rule.

Dest IP Start - Enter the starting IP address.

Dest IP End - Enter the ending IP address.

Protocol - Select the protocol.

Dest Port Start - Enter the starting port number.

Dest Port End - Enter the ending port number.

STEP 5: PORT FILTER

Add Port Filters Rules.

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

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

Prev Next Save Cancel

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

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

STEP 6: CONFIGURE WEB ACCESS LOGGING

Web Access Logging: Disabled
 Enabled

Prev Next Save Cancel

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

ACCESS CONTROL

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

Save Settings Don't Save Settings

ACCESS CONTROL

Enable Access Control:

Add Policy

POLICY TABLE

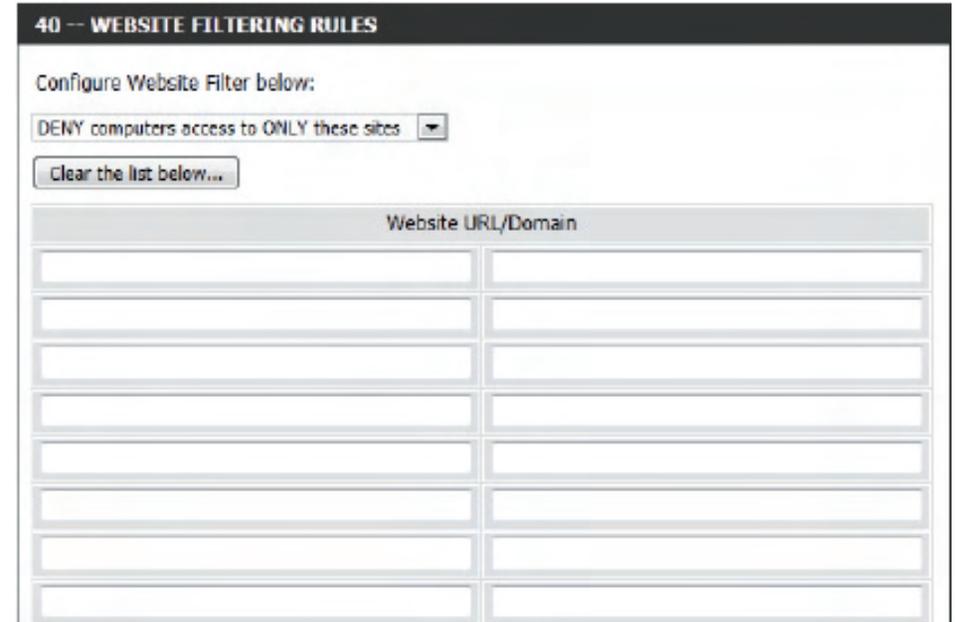
Enable Policy	Machine	Filtering	Logged	Schedule		
<input checked="" type="checkbox"/>	D-link 1	192.168.1.1	Block Some Access	No	Always	

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.

Add Website Select either **DENY** computers access to **ONLY** Filtering Rule: **these sites** or **ALLOW** computers access to **ONLY** these sites.

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



40 -- WEBSITE FILTERING RULES

Configure Website Filter below:

DENY computers access to ONLY these sites ▼

Clear the list below...

Website URL/Domain	

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 an 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.

INBOUND FILTER

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

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

ADD INBOUND FILTER RULE

Name : _____

Action : **Allow** ▼

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

Add **Cancel**

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range	
Inbound1	allow	192.168.1.0-192.168.1.254	 

Firewall Settings

A firewall protects your network from the outside world. The DIR-810L 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. The firewall setup also features a Demilitarized Zone (DMZ) option, which will expose the selected clients 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.

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

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.

FIREWALL SETTINGS

The Firewall Settings allows you to set a single computer on your network outside of the router.

ENABLE SPI

Enable SPI:

ANTI-SPOOF CHECKING

Enable anti-spoof checking:

DMZ HOST

DMZ means "Demilitarized Zone." 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: Putting 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.

Enable DMZ :

DMZ IP Address : <<

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP :

IPSec (VPN) :

RTSP :

SIP :

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.

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

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

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

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

The screenshot shows a configuration interface with two main sections. The first section is titled "DMZ HOST" and contains a descriptive paragraph about DMZ, a note about security risks, and a form with an "Enable DMZ" checkbox (unchecked), a "DMZ IP Address" field (containing "0.0.0.0"), and a "Computer Name" dropdown menu. The second section is titled "APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION" and contains four checked checkboxes: "PPTP", "IPSec (VPN)", "RTSP", and "SIP".

Routing

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

Name: Enter a name for your route.

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.

ROUTING

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

32 --ROUTE LIST

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

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, this is less reliable and may lead to higher data loss.

HT20/40 Coexistence: Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40MHz and there is another wireless network's channel over-lapping and causing interference, the router will automatically change to 20MHz.

ADVANCED WIRELESS

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz
Transmit Power : High
WLAN Partition :
WMM Enable :
HT 20/40 MHz Coexistence : Enable Disable

ADVANCED WIRELESS SETTINGS

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

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 has certified WPS across different products as well as manufacturers. The process as simple as pressing a button for the Push-Button Method or correctly entering an 8-digit code for the Pin Code Method. WPS significantly reduces the amount of time required to set up a secure wireless network, while maintaining the highest level of wireless security provided by the WPA2 standard.

Enable: Enable the Wi-Fi Protected Setup feature.

Note: *if this option is unchecked, the WPS button on the side of the router will be disabled.*

Lock Wireless Security Settings: Tick this option to lock the configured wireless security settings.

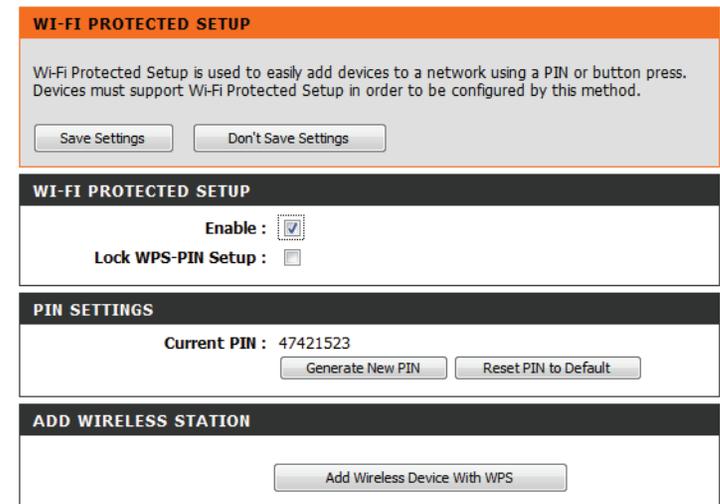
PIN Settings: A PIN is a unique number that can be used to add the router to an existing network or to create a new network. Only the Administrator (“admin” account) can change or reset the PIN.

Current PIN: Shows the current PIN.

Reset PIN to Default: Restore the default PIN of the router.

Default:

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 wireless client.



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

Save Settings Don't Save Settings

WI-FI PROTECTED SETUP

Enable :

Lock WPS-PIN Setup :

PIN SETTINGS

Current PIN : 47421523

Generate New PIN Reset PIN to Default

ADD WIRELESS STATION

Add Wireless Device With WPS

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 120 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: Click to start the wizard and refer to “Wi-Fi Protected Setup Wizard” on page 41.

WPS Button

You can also simply press the WPS button on the side of the router, and then press the WPS button on your wireless client to automatically connect without logging into the router.

Refer to “Connect a Wireless Client to your Router” on page 116 for more information.



WPS Button

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: Checking the box will allow the DIR-810L to respond to pings. Unchecking the box may provide some extra security from hackers.

WAN Port Speed: You may set the port speed of the Internet port to 10Mbps, 100Mbps, or Auto (recommended).

Enable IPV4 Multicast Streams: Check the box to allow multicast traffic to pass through the router from the Internet (IPv4).

Enable IPV6 Multicast Streams: Check the box to allow multicast traffic to pass through the router from the Internet (IPv6).

ADVANCED NETWORK

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP :

WAN PING

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.

Enable WAN Ping Respond :

WAN Ping **Inbound Filter** : Deny All

Details : Deny All

WAN PORT SPEED

WAN Port Speed : Auto 10/100Mbps

IPV4 MULTICAST STREAMS

Enable IPv4 Multicast Streams :

IPV6 MULTICAST STREAMS

Enable IPv6 Multicast Streams :

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 5GHz 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 or click **Add New**.

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.

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

GUEST ZONE SELECTION

Enable Guest Zone : Always Add New

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 Add New

Wireless Band : 5GHz Band

Wireless Network Name : dlink_media_guest (Also called the SSID)

Enable Routing Between Zones :

Security Mode : None

IPv6 Firewall

The DIR-810L's IPv6 Firewall feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-810L'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.

Configure IPv6 Firewall: Select an action from the drop-down menu.

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

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.

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.

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 first box and enter the last port in the field in the second box.

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.

IPv6 SIMPLE SECURITY

Enable IPv6 Ingress Filtering:

Enable IPv6 Simple Security :

IPv6 FIREWALL

Configure IPv6 Firewall below:

Remaining number of firewall rules that can be configured:

	Name	Schedule	
	<input type="text"/>	Always	
<input type="checkbox"/>	Source	Interface	IP Address Range
		*	<input type="text"/>
			Protocol
			TCP
	Dest	Interface	IP Address Range
		*	<input type="text"/>
			Port Range
			1 ~ 65535

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/Prefix Length: This is the IP address of the router used to reach the specified destination or enter the IPv6 address prefix length of the packets that will take this route.

Metric: Enter the metric value for this rule here.

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.

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

10 --ROUTE LIST			
<input type="checkbox"/>	Name	Destination IPv6/Prefix Length	
			/ 64
	Metric	Interface	Gateway
	0	NULL	

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).

Gateway name: Enter a name for your 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. This means to connect to the router, you must enter **https://192.168.0.1** (for example) instead of **http://192.168.0.1**.

Enable Remote Management: Remote management allows the DIR-810L to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

Remote Admin Port: The port number used to access the DIR-810L is used in the URL. Example: **http://x.x.x.x:8080** whereas x.x.x.x is the Internet IP address of the DIR-810L and 8080 is the port used for the Web Management interface.

If you have enabled **HTTPS Server**, you must enter **https://** as part of the URL to access the router remotely.

Remote Admin Inbound Filter: 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. **Details** will display the current status.

ADMINISTRATOR SETTINGS

The 'admin' account can access the management interface. The admin has read/write access and can change passwords.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
 Verify Password :

SYSTEM NAME

Gateway Name :

ADMINISTRATION

Enable Graphical Authentication :
 Enable HTTPS Server :
 Enable Remote Management :
 Remote Admin Port : Use HTTPS
 Remote Admin **Inbound Filter** : ▼
 Details :

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: Displays the current date and time of the router.

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

Enable 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. A NTP server will synch the time and date with your router. This will only connect to a server on the Internet, not a local server. Check the box to enable this feature.

NTP Server Used: Enter the IP address of a 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** to synch the date and time with the computer you are currently on.

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 NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME CONFIGURATION

Current Router Time : Sat Jan, 1, 2011 00:43:04

Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana

Enable Daylight Saving :

	Month	Week	Day of Week	TIME
Daylight Saving Dates : DST Start	Jan	1st	Sun	12:00 AM
DST End	Jan	1st	Sun	12:00 AM

AUTOMATIC TIME CONFIGURATION

Enable NTP Server :

NTP Server Used : <<

SET THE DATE AND TIME MANUALLY

Date And Time : Year Month Day

Hour Minute Second

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).

SYSLOG

The SysLog options allow you to send log information to a SysLog Server.

Save Settings Don't Save Settings

SYSLOG SETTINGS

Enable Logging To Syslog Server:

Syslog Server IP Address: 0.0.0.0 << Computer Name ▼