D-Link®

Version 1.0 | 2013/01/18

User Manual

Wireless AC1000 Dual Band Cloud Router

DIR-820L

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	November 21, 2012	• Initial release for Revision A1

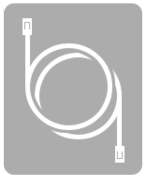
Trademarks

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.

Table of Contents

Package Contents

DIR-820L Wireless AC1000 Dual Band Cloud Router



Ethernet Cable

Power Adapter

WI-FI Configuration Card

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-820L will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11ac, 802.11a, 802.11n or 802.11g wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 7 or higher • Firefox 3.5 or higher • Safari 4 or higher • Chrome 8 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
mydlink Requirements	• iPhone/iPad/iPod Touch (iOS 3.0 or higher) • Android device (1.6 or higher) • Computer with th following browser requirements: • Internet Explorer 7 or higher • Firefox 3 or higher • Safari 5 or higher • Chrome 5 or higher iPhone, iPad, and iPod touch are registered trademarks of Apple Inc. Android is a trademark of Google, Inc.

Introduction

Now you can monitor and manage your home network right from your laptop, iPhone®, iPad®, or Android™ device. The cloud-enabled router can be configured to send an email to keep you informed anywhere, anytime when new devices are connecting 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. The D-Link Cloud Service can detect and block unwelcomed guests who try to get into your wireless network and suspicious activities will be displayed right on your mydlink™ Lite app or browser.

The D-Link DIR-820L is a IEEE 802.11ac compliant device that delivers up to 3 times faster speeds than 802.11n while staying backward compatible with 802.11a/g/b devices. Connect the DIR-820L to a Cable or DSL modem and provide high-speed Internet access to multiple computers, game consoles, and media players. Create a secure wireless network to share photos, files, music, videos, printers, and network storage. Powered by the 802.11ac technology and equipped with six internal antennas, this router provides superior wireless coverage for larger homes and offices, or for users running bandwidth-intensive applications. The DIR-820L also includes a 4-port 10/100 Fast Ethernet switch that connects wired devices for enjoying lag-free network gaming and faster file transfers.

D-Link has created SharePort™ technology to bring more flexibility to your network. With SharePort™ technology, you can connect a USB printer and share it throughout your network. You can also share a USB storage device, providing network storage for everyone to share.

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 pause or delay. With the D-Link Intelligent QoS Technology, wired and wireless traffic are analyzed and separated into multiple data streams.

The DIR-820L supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption regardless of your client devices. In addition, this router utilizes Dual Active Firewalls (SPI and NAT) to prevent potential attacks from across the Internet for the ideal centerpiece for your wireless network in the home or office.

Features

- **Ultimate Fast Wireless Networking** - The DIR-820L provides up to 300Mbps wireless connection in 2.4GHz band, 900Mbps wireless connection in 5GHz with other 802.11ac and draft 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11ac wireless router gives you the freedom of wireless networking at speeds 3x faster than 802.11n.

- **Compatible with 802.11a/g/n Devices** - The DIR-820L is still fully compatible with the IEEE 802.11a, 802.11g and 802.11n, so it can connect with existing 802.11a, 802.11g and 802.11n PCI, USB, and Cardbus adapters.

- **Advanced Firewall Features** - The Web-based user interface displays a number of advanced network management features including:

    - **Content Filtering** - Easily applied content filtering based on MAC Address, URL, and/or Domain Name.

    - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.

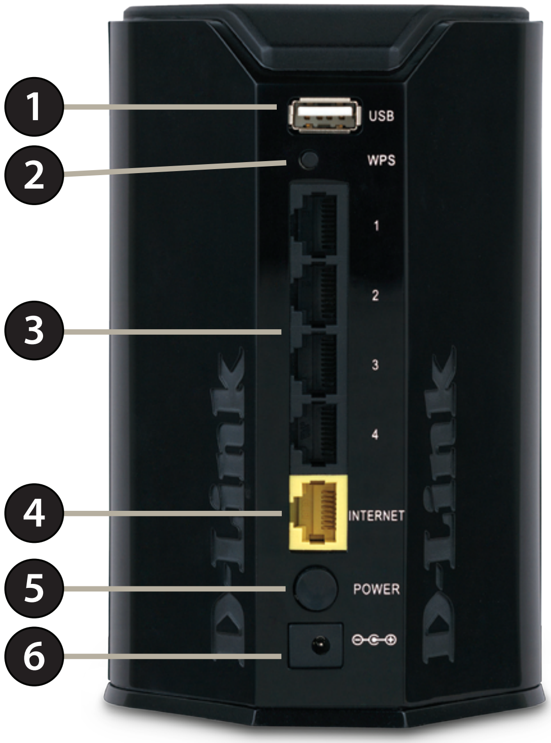
    - **Secure Multiple/Concurrent Sessions** - The DIR-820L can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-820L can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-820L lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 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

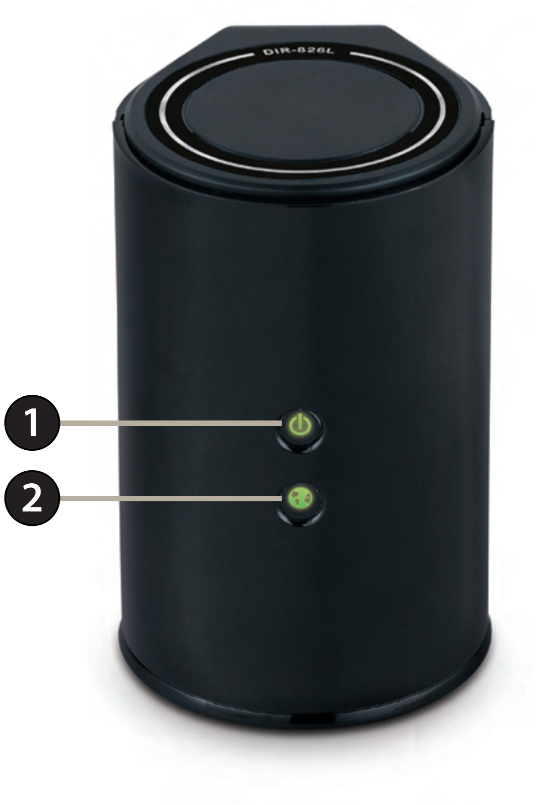
Connections



1	USB Port	Connect a USB flash drive to share content throughout your network.
2	WPS Button	Press to start the WPS process. The Internet LED will start to blink.
3	LAN Ports (1-4)	Connect 10/100 Ethernet devices such as computers, switches, storage (NAS) devices and game consoles.
4	Internet Port	Using an Ethernet cable, connect your broadband modem to this port.
5	Power Button	Press the power button to power on and off.
6	Power Receptor	Receptor for the supplied power adapter.

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 blink orange during boot up.
2	Internet LED	A solid green light indicates a connection to the Internet. If the LED is orange, a cable is connected but the router can not communicate with 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 the attic or garage.

Before you Begin

- Please configure the router with the computer that was last connected directly to your modem.

- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).

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

Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

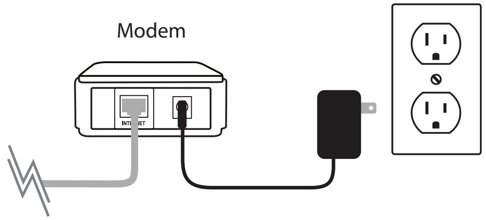
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

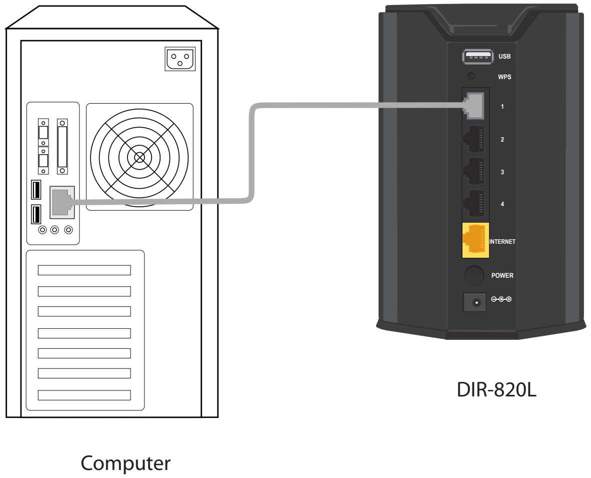
Hardware Setup

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

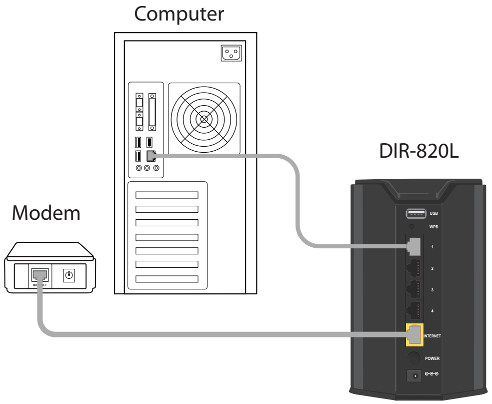


2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.

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.

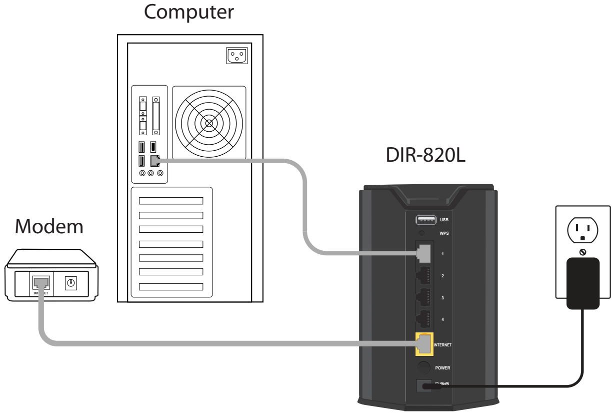


4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.



5. Reconnect the power adapter to your cable or DSL broadband modem and wait for two minutes.

6. Connect the supplied power adapter 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 green light indicates connection on the Internet port and the router can connect to the Internet. If the LED is orange, the connection is good but the router cannot connect to the Internet. It may need to be configured. See next page.

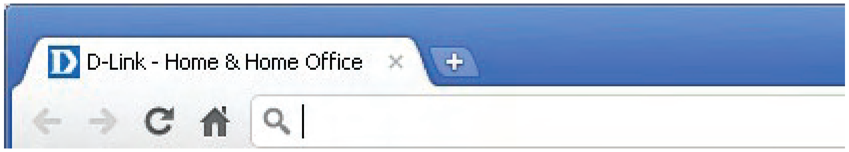
Configuration

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” on page 19.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to “Internet” on page 25.

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.

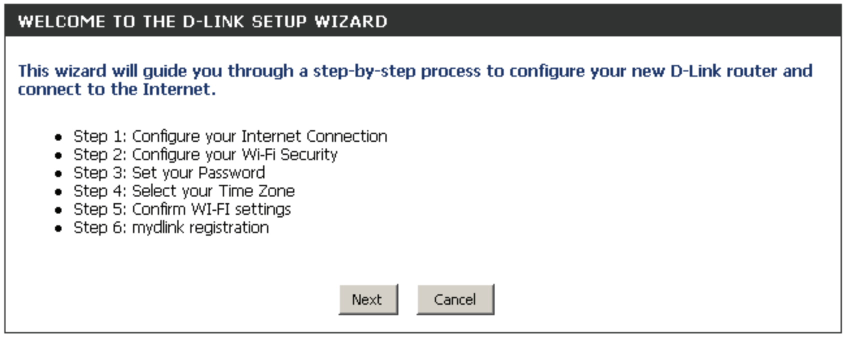


If you have already configured your settings and you would like to access the configuration utility, please refer to page 27.

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.

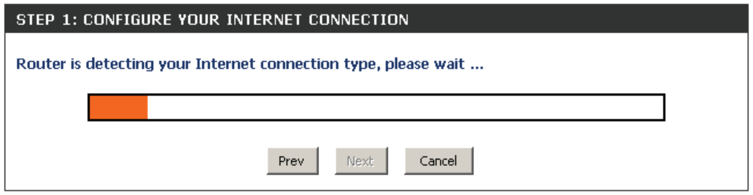
Click **Next** to continue.


WELCOME TO THE D-LINK SETUP WIZARD

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

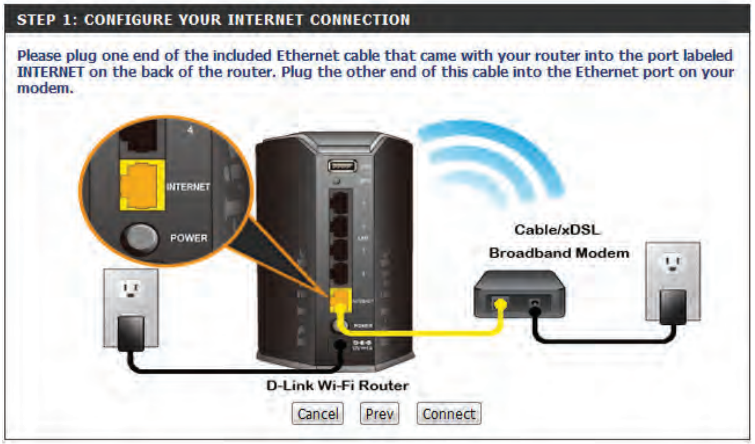
- Step 1: Configure your Internet Connection
- Step 2: Configure your Wi-Fi Security
- Step 3: Set your Password
- Step 4: Select your Time Zone
- Step 5: Confirm WI-FI settings
- Step 6: mydlink registration

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.


STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Router is detecting your Internet connection type, please wait ...

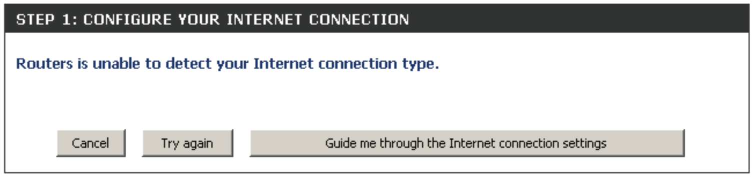
If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Connect your broadband modem to the Internet port and then click **Try Again**.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

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

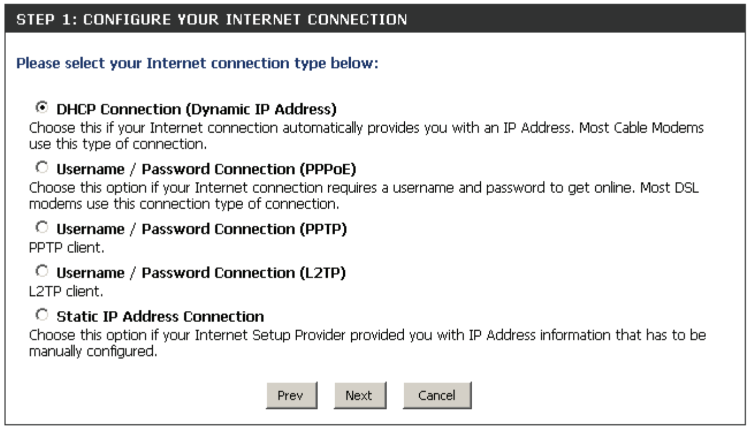
If the router detects an Ethernet connection but does not detect the type of Internet connection you have, this screen will appear. Click **Guide me through the Internet Connection Settings** to display a list of connection types to choose from.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Routers is unable to detect your Internet connection type.

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



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Please select your Internet connection type below:

● DHCP Connection (Dynamic IP Address)
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

○ Username / Password Connection (PPPoE)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this connection type of connection.

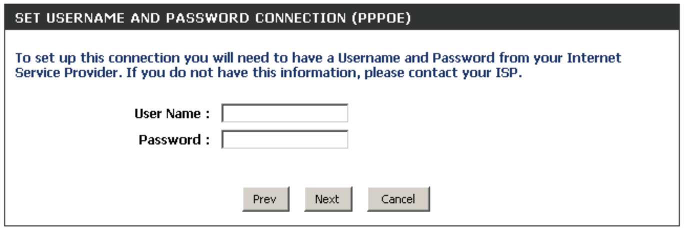
○ Username / Password Connection (PPTP)
PPTP client.

○ Username / Password Connection (L2TP)
L2TP client.

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

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

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



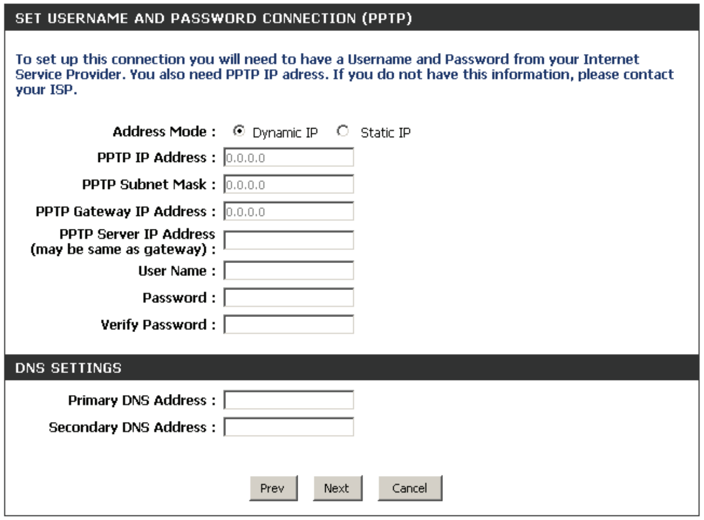
SET USERNAME AND PASSWORD CONNECTION (PPPOE)

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 :

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



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 adress. 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 :

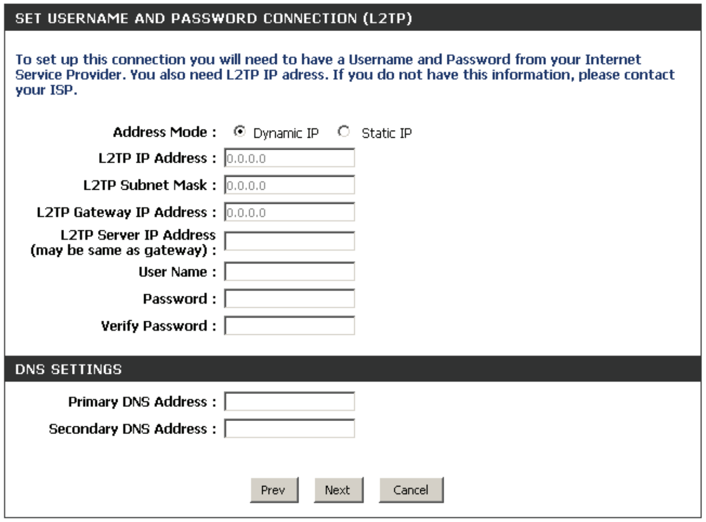
Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

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 (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 adress. 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 :

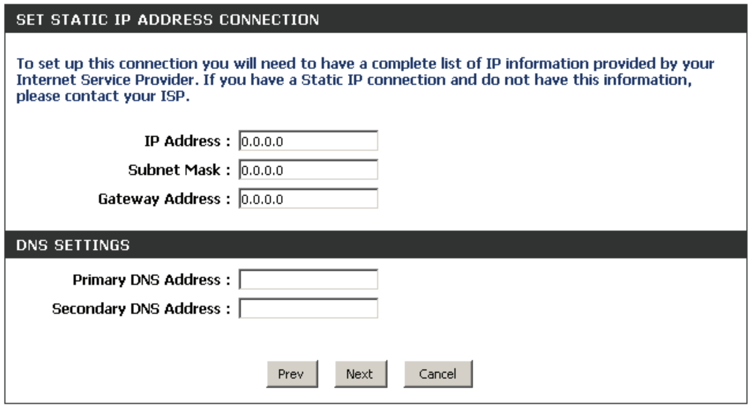
Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

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 :	0.0.0.0
Subnet Mask :	0.0.0.0
Gateway Address :	0.0.0.0

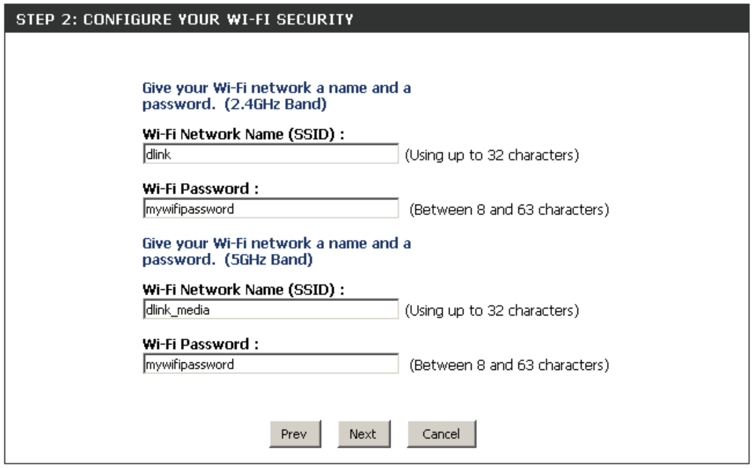
DNS SETTINGS

Primary DNS Address :	
Secondary DNS Address :	

For both the 2.4GHz and 5GHz segments, create a Wi-Fi network name (SSID) using up to 32 characters.

Create a Wi-Fi password (between 8-63 characters). Your wireless clients will need to have this passphrase entered to be able to connect to your wireless network.

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) : dlink (Using up to 32 characters)

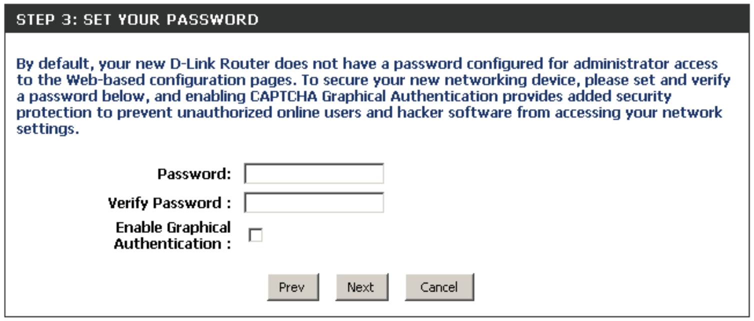
Wi-Fi Password : mywifipassword (Between 8 and 63 characters)

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

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

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

In order to secure your router, please enter a new password. Check the Enable Graphical Authentication box to enable CAPTCHA authentication for added security. Click **Next** to continue.

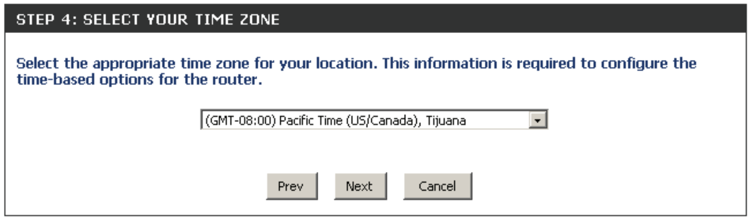


STEP 3: SET YOUR PASSWORD

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.

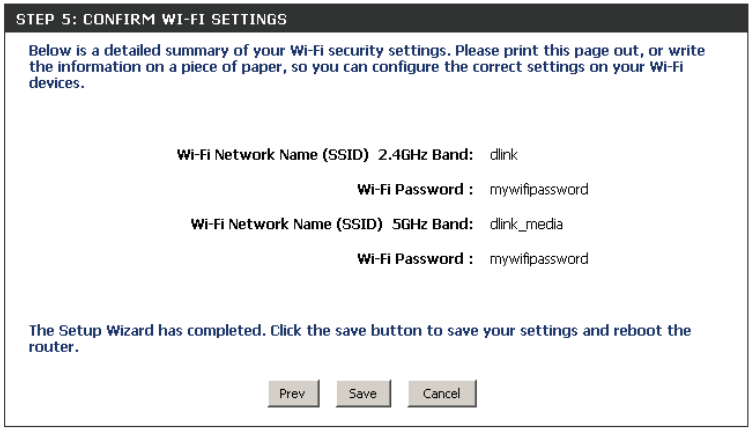


STEP 4: SELECT YOUR TIME ZONE

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

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

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



STEP 5: CONFIRM WI-FI SETTINGS

Below is a detailed summary of your Wi-Fi 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 Wi-Fi devices.

Wi-Fi Network Name (SSID) 2.4GHz Band: dlink

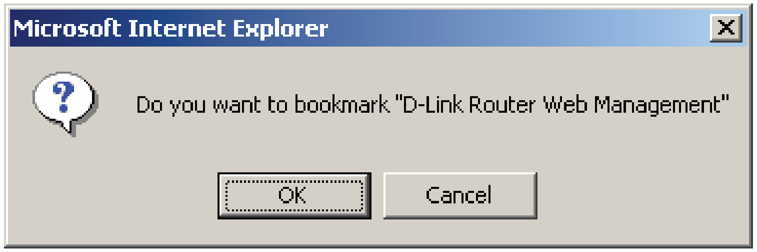
Wi-Fi Password : mywifipassword

Wi-Fi Network Name (SSID) 5GHz Band: dlink_media

Wi-Fi Password : mywifipassword

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

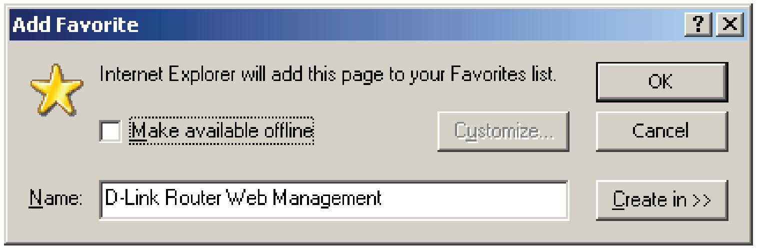
If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.



Microsoft Internet Explorer

Do you want to bookmark "D-Link Router Web Management"

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



Add Favorite

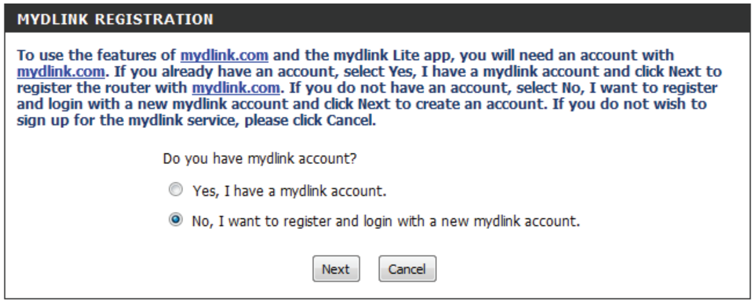
Internet Explorer will add this page to your Favorites list.

□ Make available offline

Name: D-Link Router Web Management

To use the mydlink service (mydlink.com or the mydlink Lite app), you must have an account. Select if 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**.



MYDLINK REGISTRATION

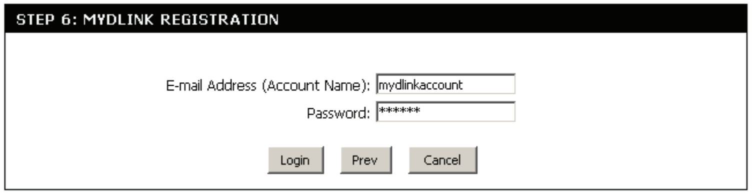
To use the features of mydlink.com and the mydlink Lite app, you will need an account with mydlink.com. If you already have an account, select Yes, I have a mydlink account and click Next to register the router with mydlink.com. If you do not have an account, select No, I want to register and login with 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.

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

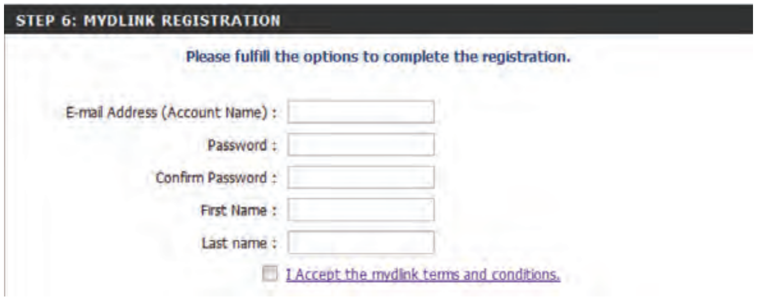


STEP 6: MYDLINK REGISTRATION

E-mail Address (Account Name): mydlinkaccount

Password: *******

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



STEP 6: MYDLINK REGISTRATION

Please fulfill the options to complete the registration.

E-mail Address (Account Name) :

Password :

Confirm Password :

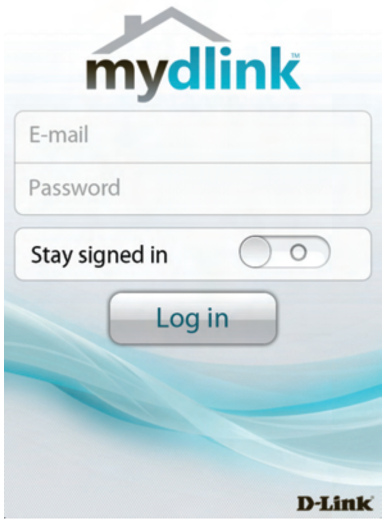
First Name :

Last name :

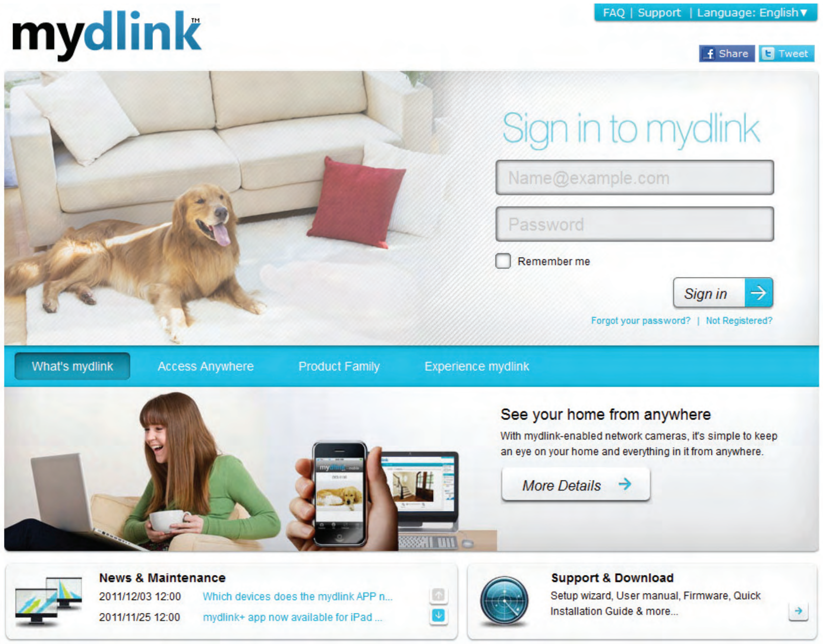
□ I Accept the mydlink terms and conditions.

The mydlink App will allow you to receive notices, browse network users, and configure your router from an iPhone/iPad/iPod Touch (iOS 3.0 or higher), Android device (1.6 or higher).

To download the "mydlink lite" app, visit the Apple Store, Android Market or **http://mydlink.com/Lite**.



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



See your home from anywhere

With mydlink-enabled network cameras, it's simple to keep an eye on your home and everything in it from anywhere.

News & Maintenance

2011/12/03 12:00 Which devices does the mydlink APP n...

2011/11/25 12:00 mydlink+ app now available for iPad ...

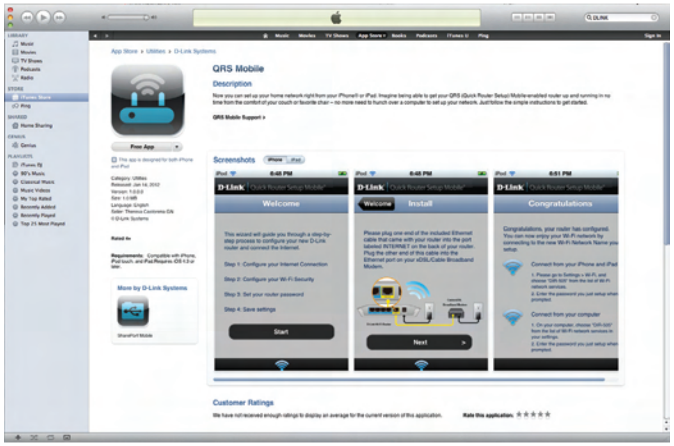
Support & Download

Setup wizard, User manual, Firmware, Quick Installation Guide & more...

QRS Mobile App

D-Link offers an app for your iOS/Android device to install and configure your router.

Step 1
From your iPad, Touch, or iPhone, go to the iTunes Store and search for 'D-Link'. Select **QRS Mobile** and then download it.



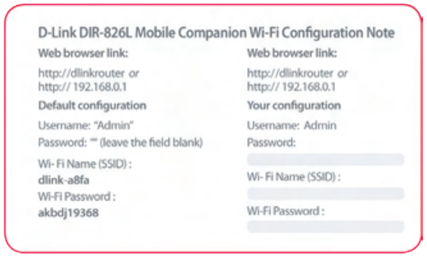
Now you can set up your home network right from your iPhone® or iPad. Imagine being able to get your QRS (Quick Router Setup) Mobile-enabled router up and running in no time from the comfort of your couch or favorite chair – no more need to hunch over a computer to set up your network. Just follow the simple instructions to get started.

You may also scan this code to download.

Available on the App Store

ANDROID APP ON Google play

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.



D-Link DIR-826L Mobile Companion Wi-Fi Configuration Note

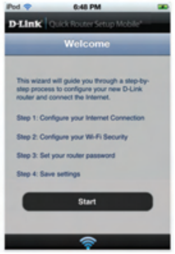
Web browser link:
http://dlinkrouter *or*
http:// 192.168.0.1

Default configuration
Username: "Admin"
Password: "" (leave the field blank)
Wi- Fi Name (SSID) :
dlink-a8fa
Wi-Fi Password :
akbdj19368

Web browser link:
http://dlinkrouter *or*
http:// 192.168.0.1

Your configuration
Username: Admin
Password:
Wi- Fi Name (SSID) :
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.



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

Step 1: Configure your Internet Connection

Step 2: Configure your Wi-Fi Security

Step 3: Set your router password

Step 4: Save settings

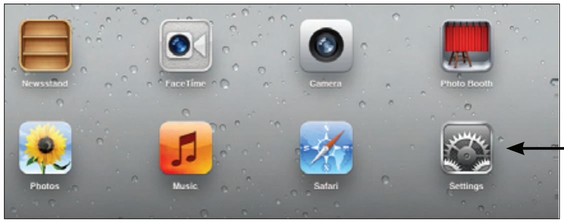
SharePort Mobile App

The SharePort Mobile app will allow you to access files from a USB thumb drive that is plugged into your router. You must enable file sharing from the **Setup** > **Storage** page (refer to page 68) for this app to work properly.

1. Insert your USB flash drive into DIR-820L.

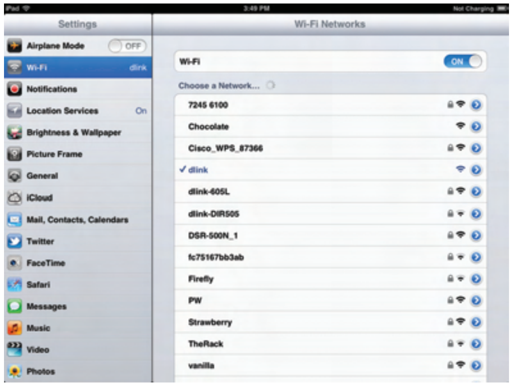
2. Scan the QR code to download the **SharePort Mobile** app to your iOS or Android device.

3. From your iOS mobile device, click **Settings.**

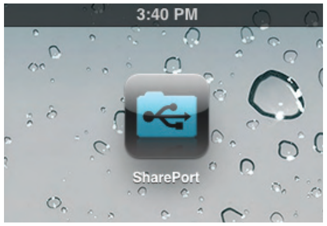


Settings

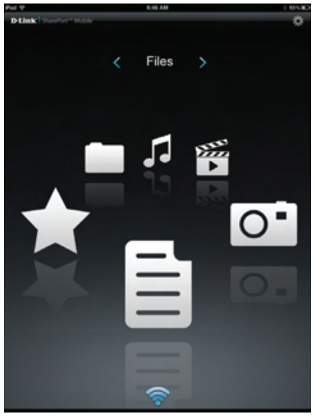
4. Click **Wi-Fi,** select the Wi-Fi Network Name (SSID) that you created in the setup and then enter your Wi-Fi password.



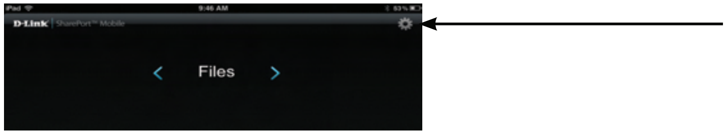
5. Once connected, click on the **SharePort Mobile** icon.



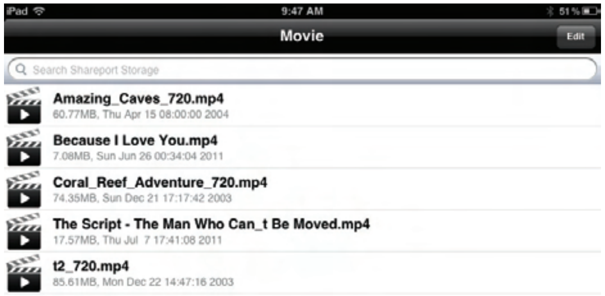
6. The following screen will appear.



7. Click on **Settings** icon located on the right top corner of the screen. Click **Edit** to enter your User Name and Password. Once you finish, click **Done** to continue.



8. For the Movie section, click the movie icon to play your movie from your USB flash drive. Supported video formats are mp4, mov, and m4v.



Amazing_Caves_720.mp4
60.77MB, Thu Apr 15 08:00:00 2004

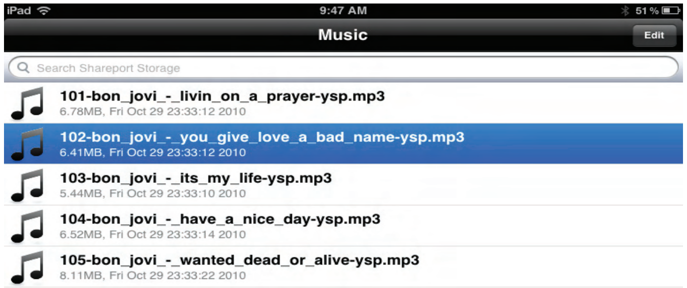
Because I Love You.mp4
7.08MB, Sun Jun 26 00:34:04 2011

Coral_Reef_Adventure_720.mp4
74.35MB, Sun Dec 21 17:17:42 2003

The Script - The Man Who Can_t Be Moved.mp4
17.57MB, Thu Jul 7 17:41:08 2011

t2_720.mp4
85.61MB, Mon Dec 22 14:47:16 2003

9. For the Music section, click the music icon to play your music from your USB flash drive. Supported audio formats are mp3, wav, and m4a



101-bon_jovi_-_livin_on_a_prayer-ysp.mp3
6.78MB, Fri Oct 29 23:33:12 2010

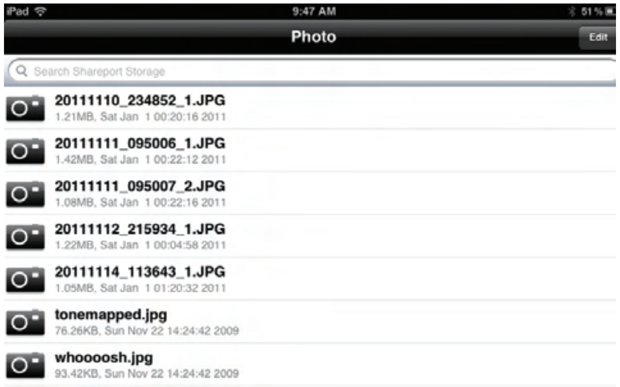
102-bon_jovi_-_you_give_love_a_bad_name-ysp.mp3
6.41MB, Fri Oct 29 23:33:12 2010

103-bon_jovi_-_its_my_life-ysp.mp3
5.44MB, Fri Oct 29 23:33:10 2010

104-bon_jovi_-_have_a_nice_day-ysp.mp3
6.52MB, Fri Oct 29 23:33:14 2010

105-bon_jovi_-_wanted_dead_or_alive-ysp.mp3
8.11MB, Fri Oct 29 23:33:22 2010

10. For the Photo section, click the Photo icon to view your photos from your USB flash drive. Supported image formats are bmp, jpg, and png.



20111110_234852_1.JPG
1.21MB, Sat Jan 1 00:20:16 2011

20111111_095006_1.JPG
1.42MB, Sat Jan 1 00:22:12 2011

20111111_095007_2.JPG
1.08MB, Sat Jan 1 00:22:16 2011

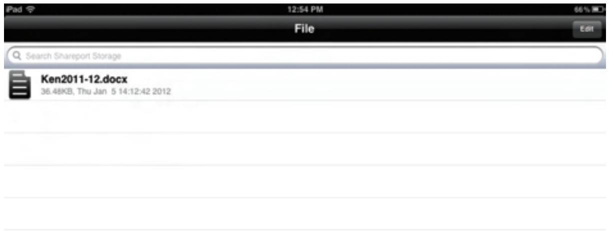
20111112_215934_1.JPG
1.22MB, Sat Jan 1 00:04:58 2011

20111114_113643_1.JPG
1.05MB, Sat Jan 1 01:20:32 2011

tonemapped.jpg
76.26KB, Sun Nov 22 14:24:42 2009

whoooosh.jpg
93.42KB, Sun Nov 22 14:24:42 2009

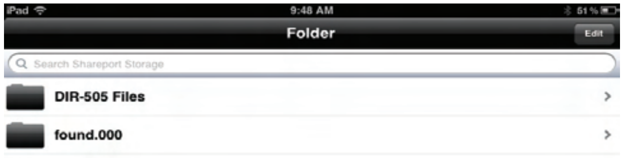
11. For the Files section, click on the Files icon to view your files from your USB flash drive. Supported formats for iOS are Microsoft Office and Adobe Acrobat. Supported formats for Android vary by device.



Ken2011-12.docx
36.48KB, Thu Jan 5 14:12:42 2012

12. To upload a file from your mobile device to your USB drive, go to the **Folder** section, select **Upload** from the menu, (Android users may need to press a "**...**" button to create the menu.) and then select the "**+**" at the top-right corner. This will give you a direct view of your device's files and folders. Browse for the file you want to upload, and select it. Your file will then be copied from your mobile device to your USB drive.

    In **Folder** you may also explore the various folders on the USB drive without separating the content by type of file.



iPad 9:48 AM 51 %

Folder

Edit

Search Shareport Storage

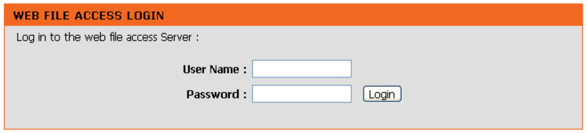
DIR-505 Files

found.000

13. To permanently download a file to your mobile device, select the **"Star"** icon next to it while browsing the categories (listed below). This will save it as a **Favorite** and make the file available to you even when not connected to the DIR-505. If a file is not added as a favorite, then it will not be saved to your mobile device.

14. You can access files on a USB hard drive that is plugged into the DIR-505 from a web browser: **http://shareport.local.**

    Note: *If you change your device/admin password, you will need to use the new password in the SharePort Mobile app.*



WEB FILE ACCESS LOGIN

Log in to the web file access Server :

User Name :

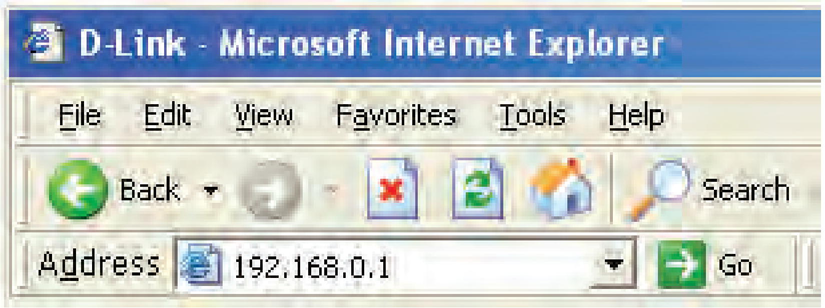
Password :

Login

Web-based Configuration Utility

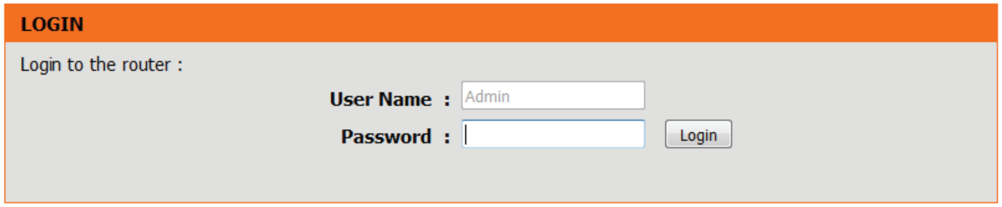
To access the configuration utility, open a web-browser such as Internet Explorer and enter address of the router (**http://dlinkrouter.local.**).

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



Address: 192.168.0.1

Leave the password blank by default.


LOGIN

Login to the router :

User Name : Admin

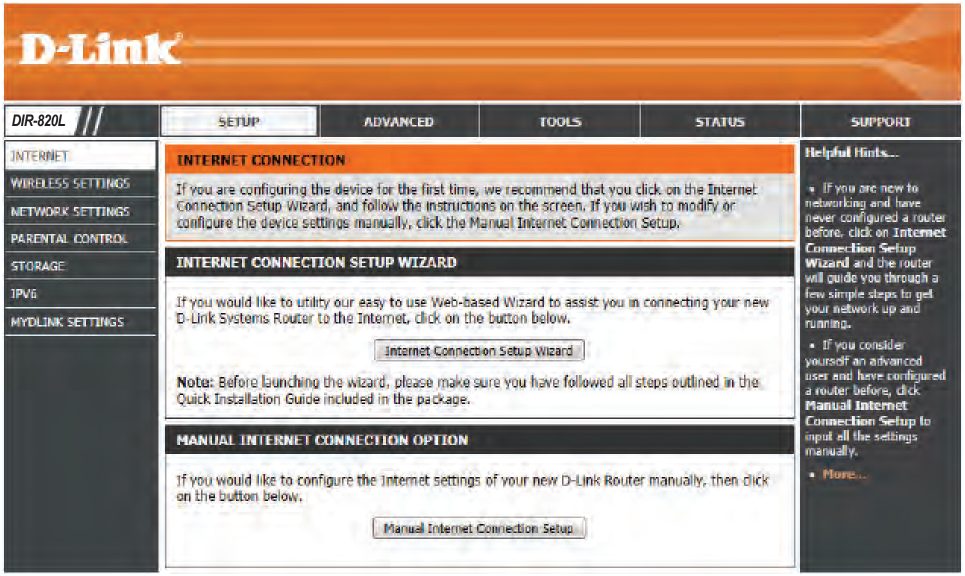
Password :

Setup

Internet

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

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.



INTERNET CONNECTION

If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

INTERNET CONNECTION SETUP WIZARD

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

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

MANUAL INTERNET CONNECTION OPTION

If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

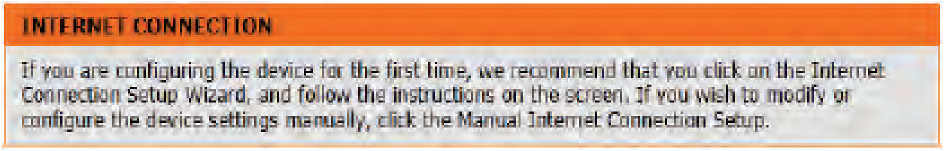
Helpful Hints...

- If you are new to networking and have never configured a router before, click on **Internet Connection Setup Wizard** and the router will guide you through a few simple steps to get your network up and running.
- If you consider yourself an advanced user and have configured a router before, click **Manual Internet Connection Setup** to input all the settings manually.

Internet Connection Setup Wizard

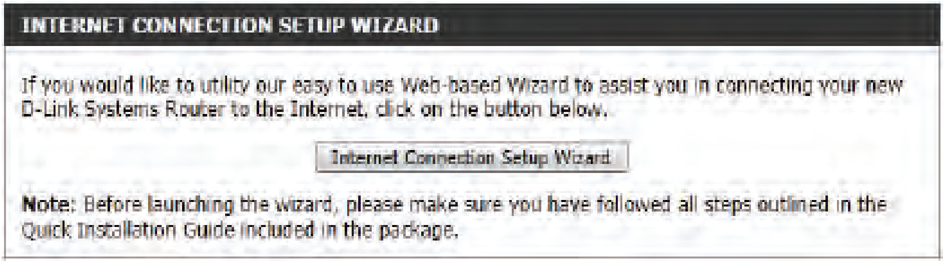
When configuring the router for the first time, we recommend that you click use the **Internet Connection Setup Wizard**, and follow the instructions on the screen. This wizard is designed to assist user with a quick and easy method to configure the Internet Connectivity of this router.

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



INTERNET CONNECTION

If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

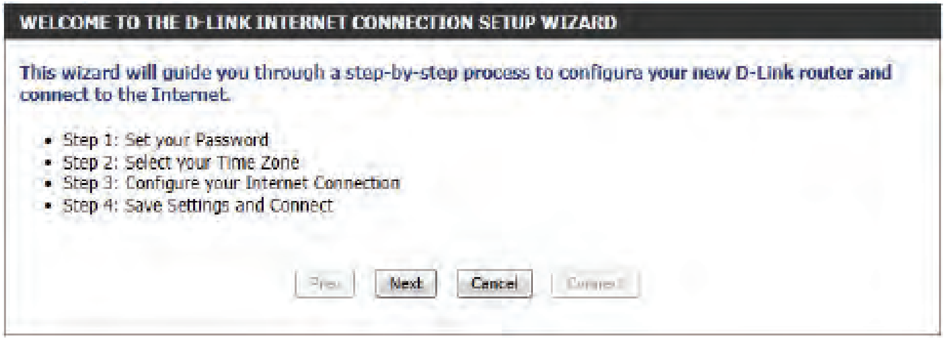


INTERNET CONNECTION SETUP WIZARD

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

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

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.



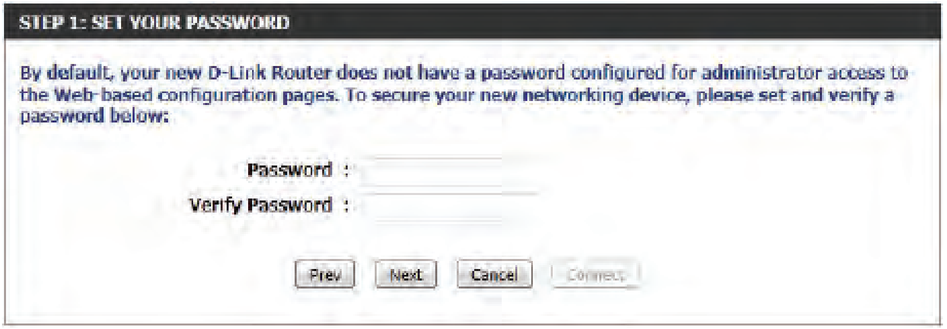
WELCOME TO THE D-LINK INTERNET CONNECTION SETUP WIZARD

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

- Step 1: Set your Password
- Step 2: Select your Time Zone
- Step 3: Configure your Internet Connection
- Step 4: Save Settings and Connect

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.

Click **Next** to continue.



STEP 1: SET YOUR PASSWORD

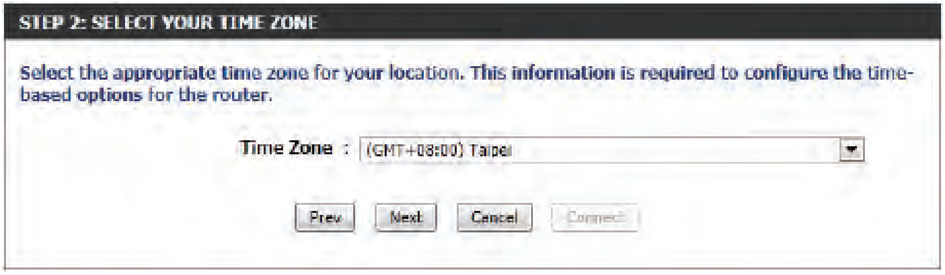
By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:

Password :
Verify Password :

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 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.

Time Zone : (GMT+08:00) Taipei

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 parameters will be available for configuration:

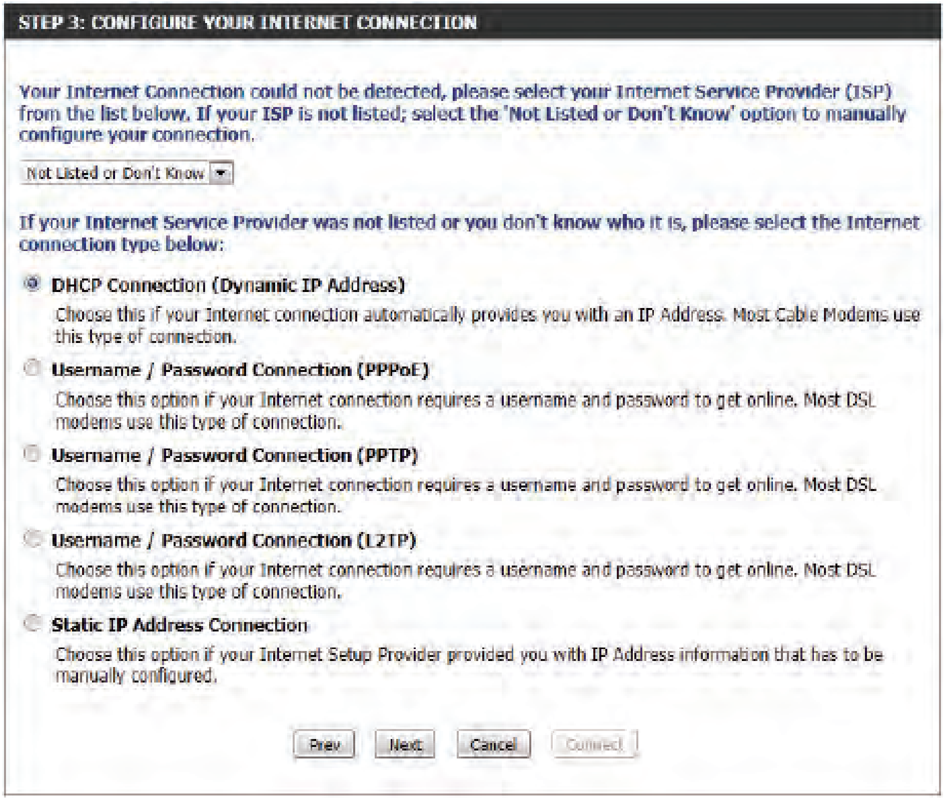
Dynamic IP Address: Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

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

PPTP: Choose this option if your Internet connection requires a PPTP username and password to get online.

L2TP: Choose this option if your Internet connection requires an L2TP username and password to get online.

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



STEP 3: CONFIGURE YOUR INTERNET CONNECTION

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.

Not Listed or Don't Know

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

● DHCP Connection (Dynamic IP Address)

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

○ Username / Password Connection (PPPoE)

Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

○ Username / Password Connection (PPTP)

Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

○ Username / Password Connection (L2TP)

Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

○ Static IP Address Connection

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

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:

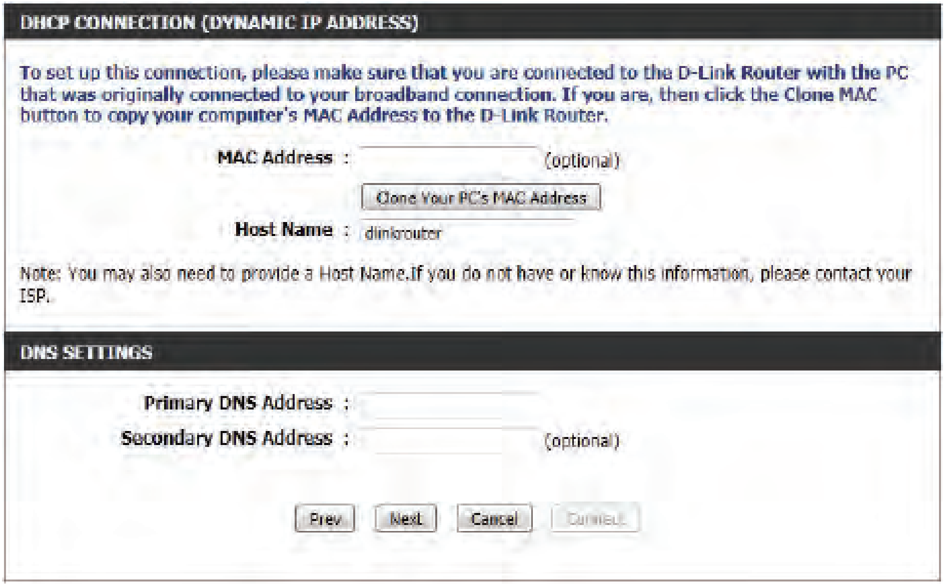
MAC Address: Enter the MAC address of the Internet gateway (plugged into the Internet port of this device) here.

Clone Button: If the configuration PC also acts as the Internet gateway, then click on the Clone 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.

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.



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 : (optional)

Host Name : dlinkrouter

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

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address : (optional)

Click **Next** to continue.

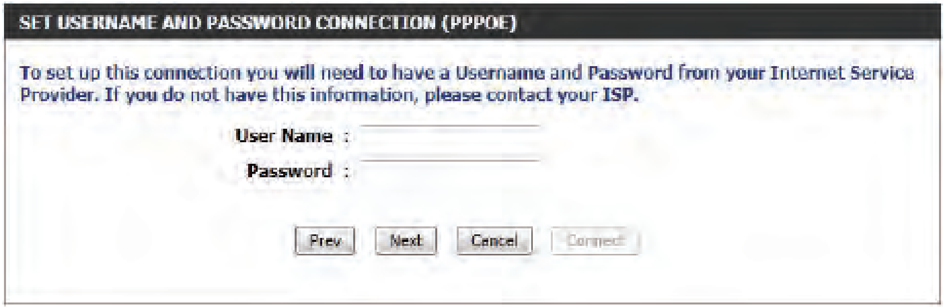
Step 3: Internet Connection (PPPoE)

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

The following parameters will be available for configuration:

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.



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.

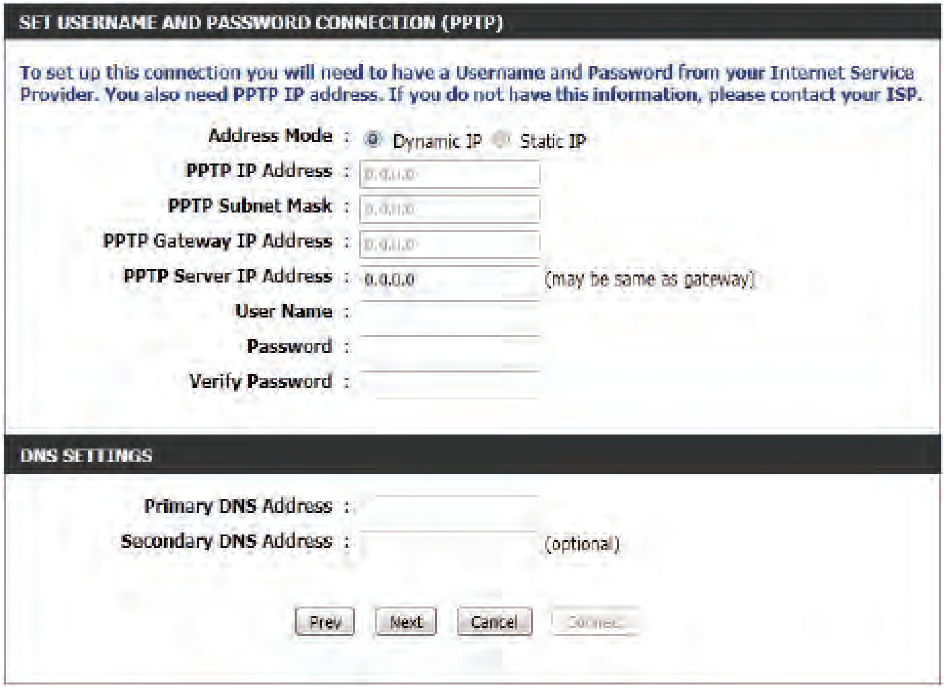
User Name :

Password :

Click **Next** to continue.

Step 3: Internet Connection (PPTP)

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



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 : 0.0.0.0 (may be same as gateway)
User Name :
Password :
Verify Password :

DNS SETTINGS

Primary DNS Address :
Secondary DNS Address : (optional)

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 usual 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 a 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.

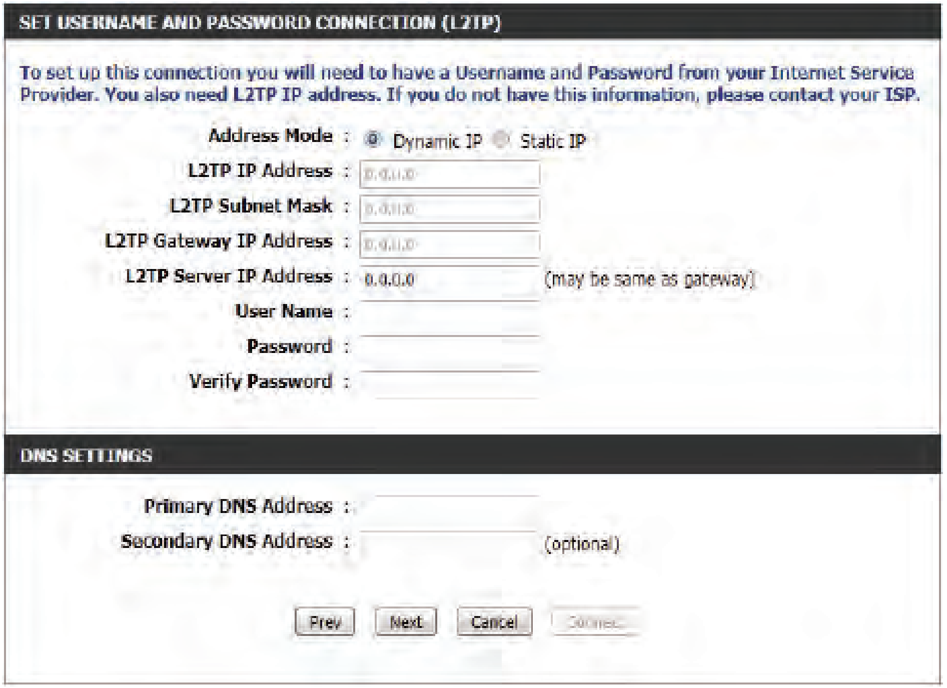
Primary DNS Address: Enter the Primary DNS IP address used here.

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.

Step 3: Internet Connection (L2TP)

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



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 : 0.0.0.0 (may be same as gateway)
User Name :
Password :
Verify Password :

DNS SETTINGS

Primary DNS Address :
Secondary DNS Address : (optional)

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 a 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.

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.

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:

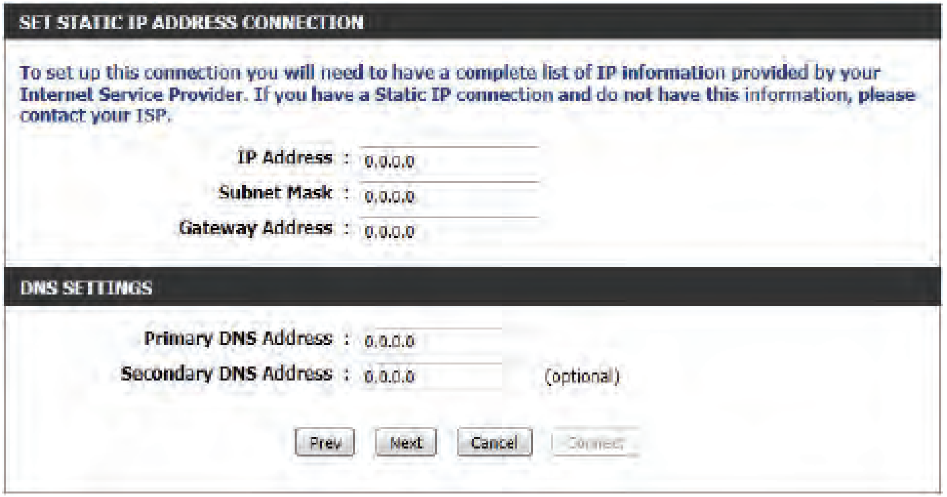
IP Address: Enter the Static IP address provided by the ISP here.

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.



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 : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway Address : 0.0.0.0

DNS SETTINGS

Primary DNS Address : 0.0.0.0

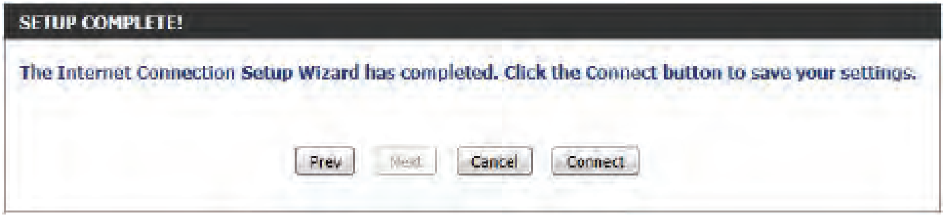
Secondary DNS Address : 0.0.0.0 (optional)

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.

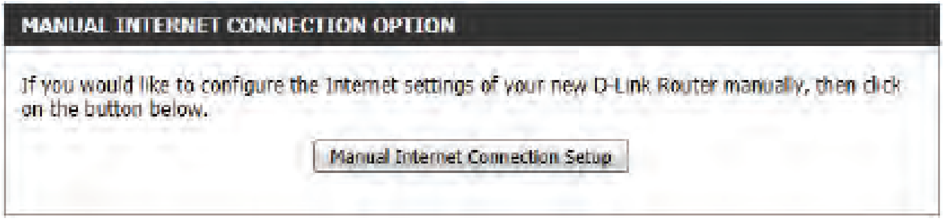


SETUP COMPLETE!

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

Internet (Manual)

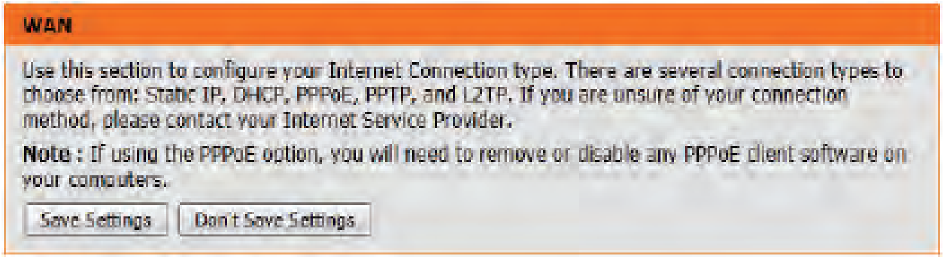
On this page the user can configure the Internet Connection settings manually. To access the Manual Internet Connection Setup page, click on the **Manual Internet Connection Setup** button. On this page there a multiple parameters that can be configured regarding the Internet Connection setup. We'll discuss them from top to bottom.



MANUAL INTERNET CONNECTION OPTION

If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

At any given point the user can save the configuration done, on this page, by clicking on the **Save Settings** button. If you choose to discard the changes made, click on the **Don't Save Settings** button.



WAN

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

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

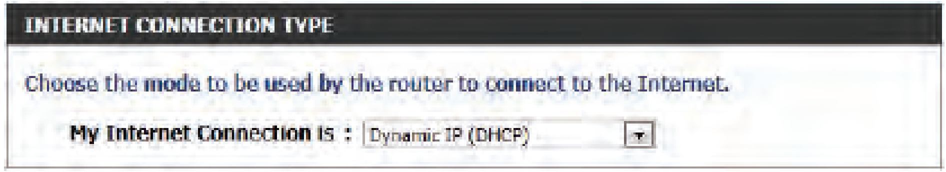
Internet Connection Type

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.

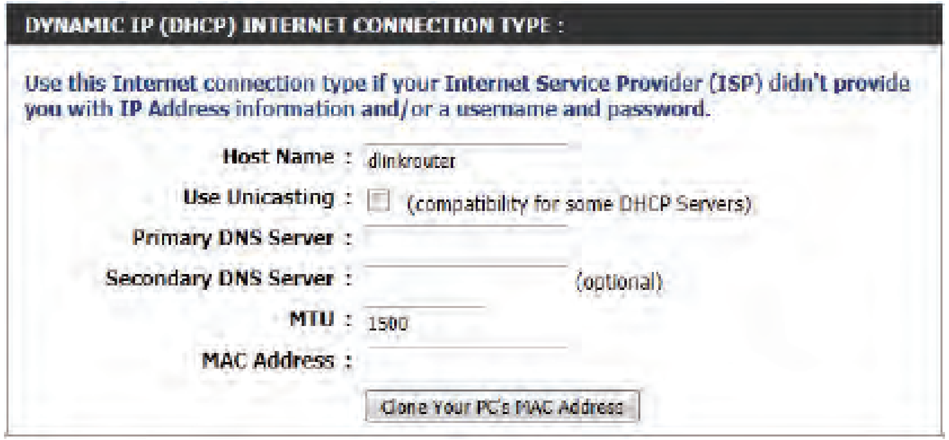


INTERNET CONNECTION TYPE

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

My Internet Connection is : Dynamic IP (DHCP)

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



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 :	dlinkrouter
Use Unicasting :	□ (compatibility for some DHCP Servers)
Primary DNS Server :	
Secondary DNS Server :	(optional)
MTU :	1500
MAC Address :	

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

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 you ISP uses the unicast method to provide IP addresses.

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

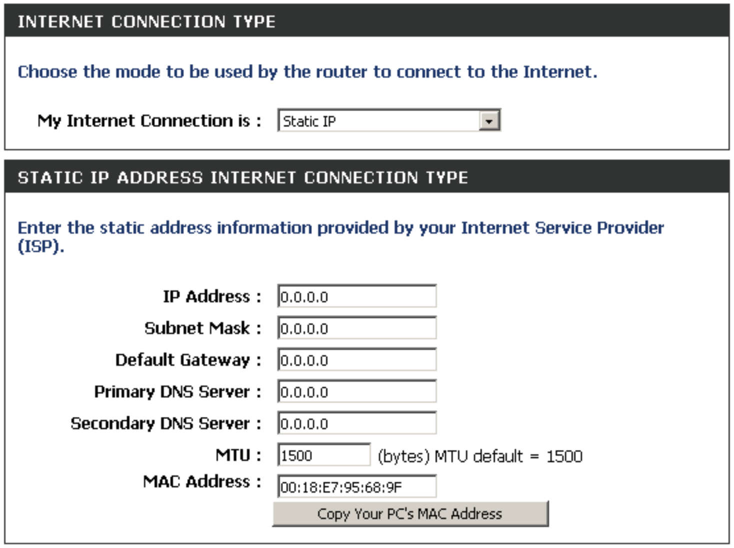
Secondary DNS: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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

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

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.



INTERNET CONNECTION TYPE

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

My Internet Connection is : Static IP

STATIC IP ADDRESS INTERNET CONNECTION TYPE

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

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Default Gateway : 0.0.0.0

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

MTU : 1500 (bytes) MTU default = 1500

MAC Address : 00:18:E7:95:68:9F

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

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

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

Default Gateway: Enter the Gateway assigned by your ISP.

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

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

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

Internet Setup
PPPoE (DSL)

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

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

Address Mode: 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.

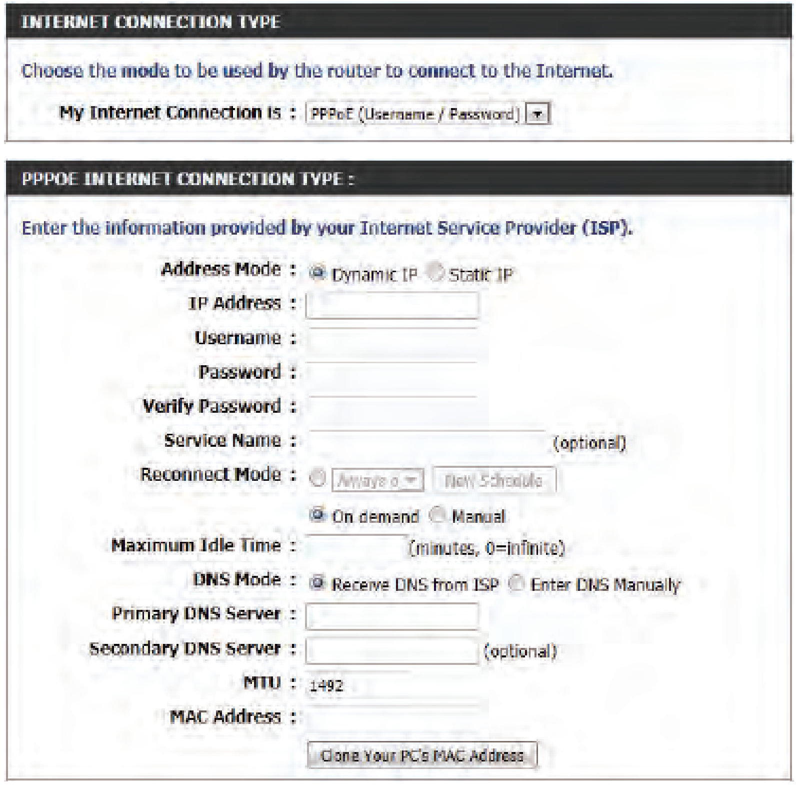
Username: Enter the PPPoE account user name used here. This information is given by the ISP.

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)

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 o New Schedule

● On demand ○ Manual

Maximum Idle Time : (minutes, 0=infinite)

DNS Mode : ● Receive DNS from ISP ○ Enter DNS Manually

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1492

MAC Address :

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.

DNS Mode: This option allow the router to obtain the DNS IP addresses from the ISP, when **Receive DNS from ISP** is selected, or allows the user to enter DNS IP address manually, when **Enter DNS Manually** is selected.

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

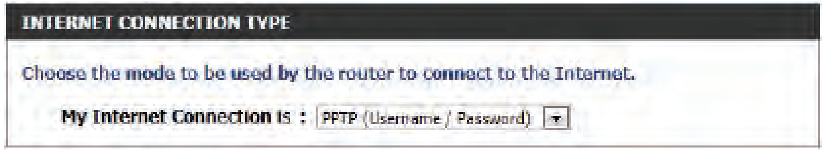
Secondary DNS Server: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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

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

Internet Setup
PPTP

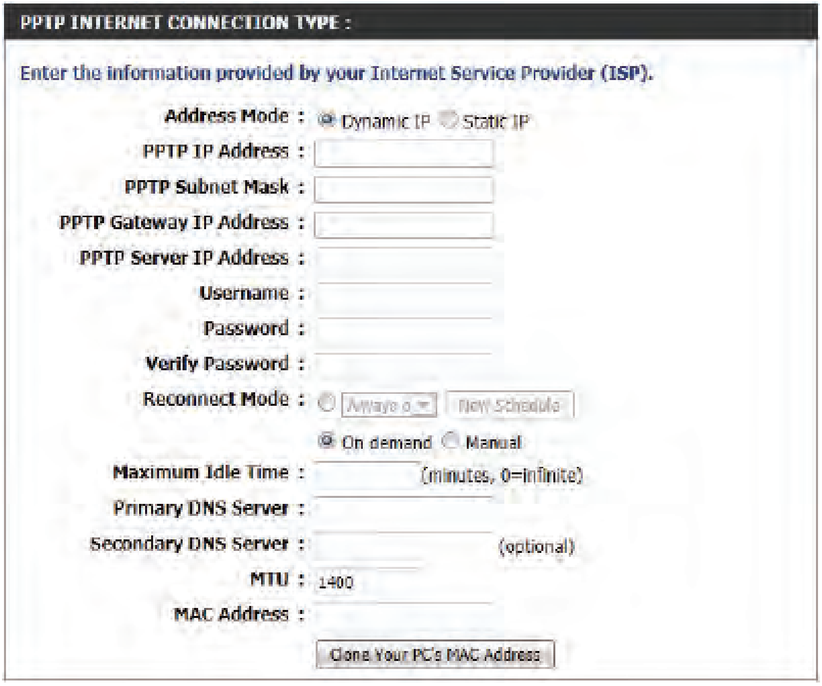
Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



INTERNET CONNECTION TYPE

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

My Internet Connection is : PPTP (Username / Password)



PPTP INTERNET CONNECTION TYPE :

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

Address Mode : ● Dynamic IP ○ Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : ○ Always on New Schedule

● On demand ○ Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1400

MAC Address :

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

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 a 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.

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.

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.

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.

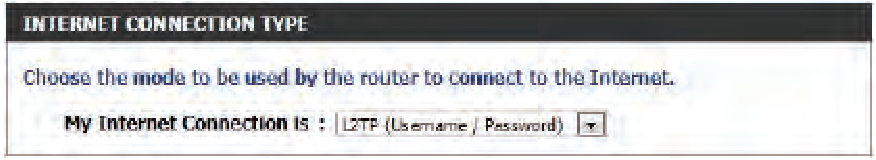
L2TP Server IP Address: Enter the L2TP Server IP address used here. This is normally the same a the L2TP Gateway IP address.

Username: Enter the L2TP username used here.

Password: Enter the L2TP password used here.

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

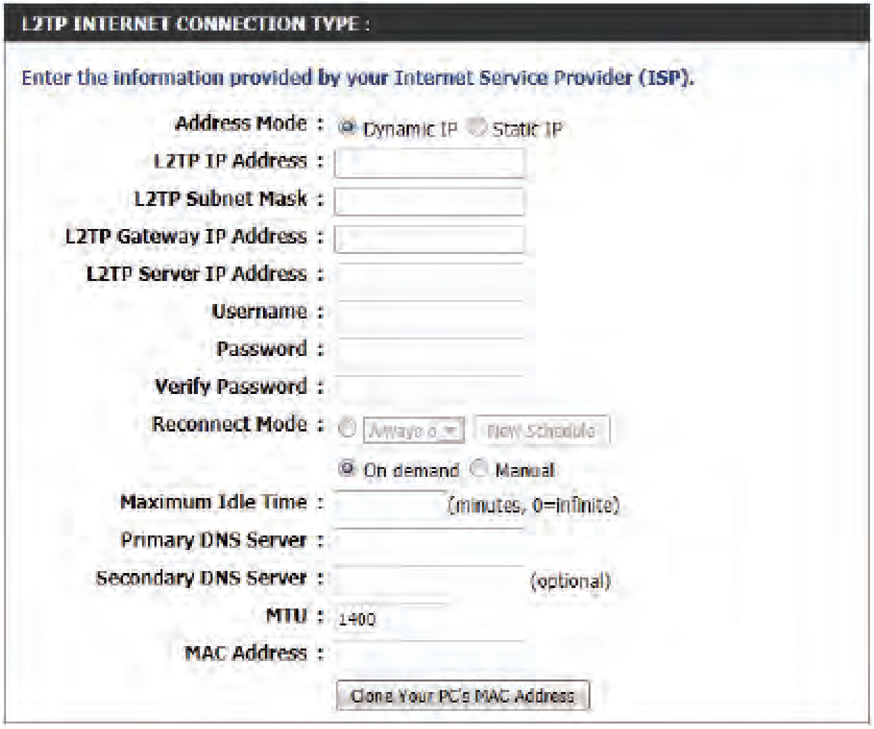
Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a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



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 o New Schedule
● On demand ○ Manual
Maximum Idle Time : (minutes, 0=infinite)
Primary DNS Server :
Secondary DNS Server : (optional)
MTU : 1400
MAC Address :

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.

Internet Setup

DS-Lite

Another Internet Connection type is DS-Lite.

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

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

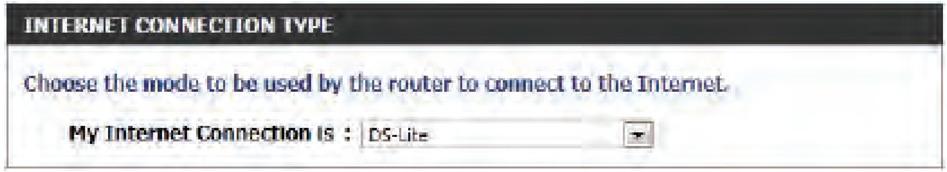
AFTR IPv6 Address: After selecting the Manual Configuration option above, the user can enter the AFTR IPv6 address used here.

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.

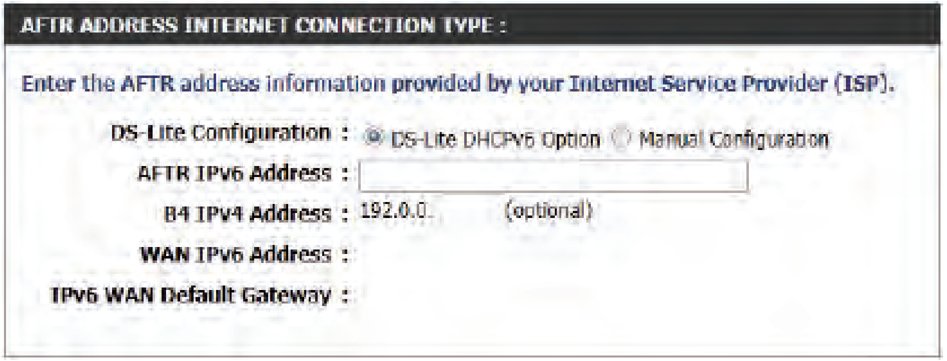
Click on the **Save Settings** button to accept the changes made.
Click on the **Don’t Save Settings** button to discard the changes made.



INTERNET CONNECTION TYPE

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

My Internet Connection is : DS-Lite



AFTR ADDRESS INTERNET CONNECTION TYPE :

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

DS-Lite Configuration : ● DS-Lite DHCPv6 Option ○ Manual Configuration

AFTR IPv6 Address :

B4 IPv4 Address : 192.0.0. (optional)

WAN IPv6 Address :

IPv6 WAN Default Gateway :

Wireless Settings

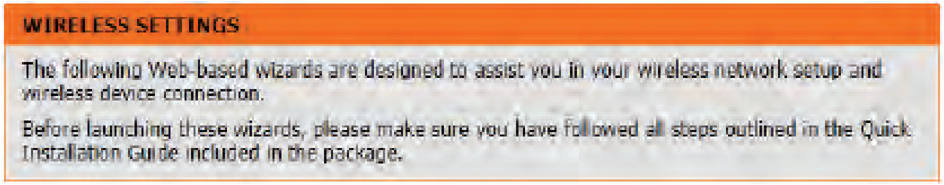
Wireless Connection Setup wizard

On this page the user can configure the Wireless settings for this device. There are 3 ways to configure Wireless using this router. Firstly, the user can choose to make use for the quick and easy **Wireless Connection Setup Wizard**. Secondly, the user can choose to make use 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 customized the wireless network settings to fit into your environment and to add higher security.

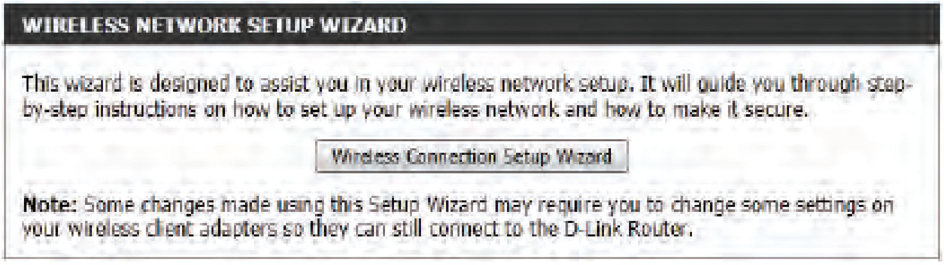
To initiate the **Wireless Connection Setup Wizard** click on the Wireless Connection Setup Wizard button.



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

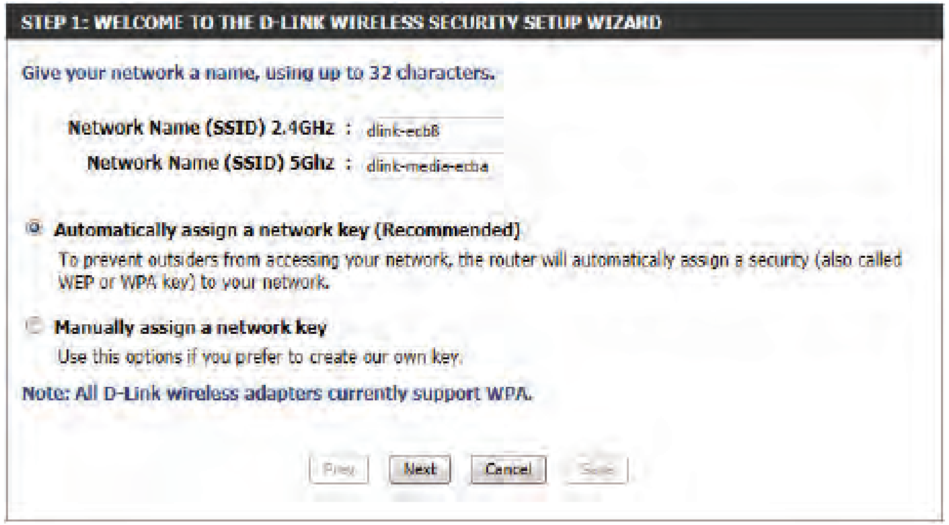
This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

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: 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.
There are seperate spaces provided for a **2.4GHz** Network Name and a **5GHz** Network Name.

Secondly the user 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 prompt to manually enter a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods.

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



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 : dlink-ecb8

Network Name (SSID) 5Ghz : dlink-media-ecba

● **Automatically assign a network key (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.

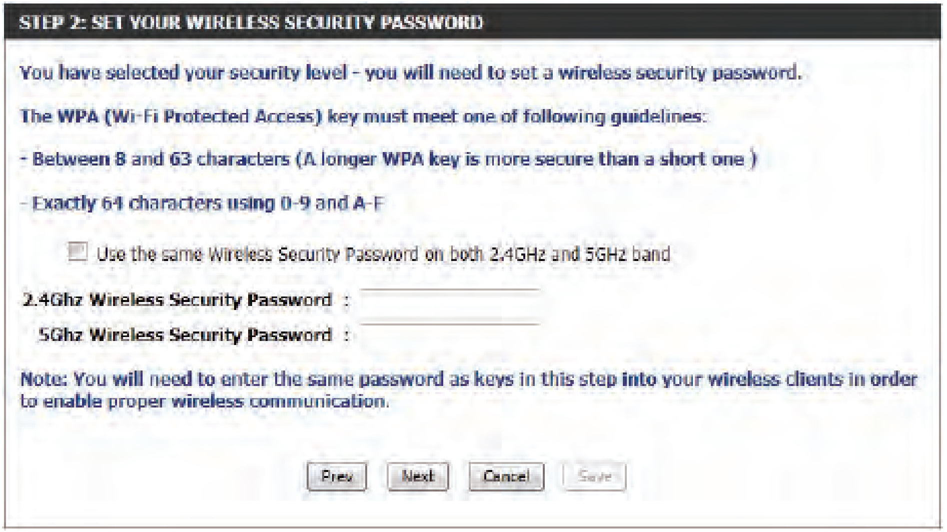
Note: All D-Link wireless adapters currently support WPA.

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 wants to connect to this device. So please remember this key to prevent future troubleshooting.
If you want 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 seperate Wireless Security Passwords for each individual Wireless band.

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

Setup Complete: On this page the user can view the configuration made and verify whether they are correct.

Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard the changes made and return to the main wireless page. Click on the **Save** button to accept 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 one of following guidelines:

- Between 8 and 63 characters (A longer WPA key is more secure than a short one)

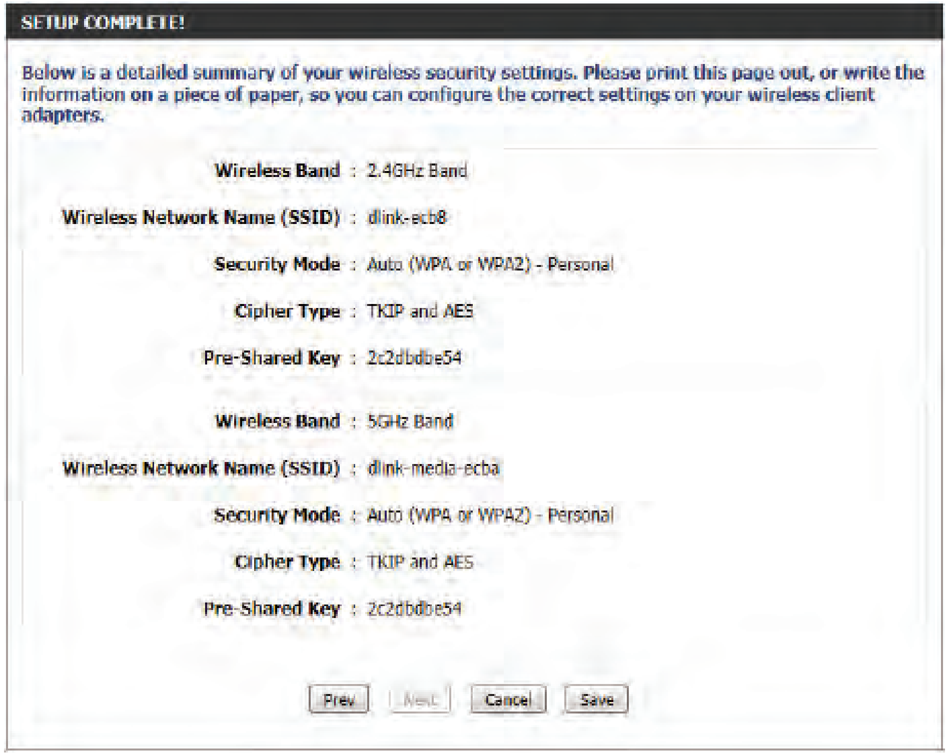
- Exactly 64 characters using 0-9 and A-F

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

2.4Ghz Wireless Security Password :

5Ghz 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.



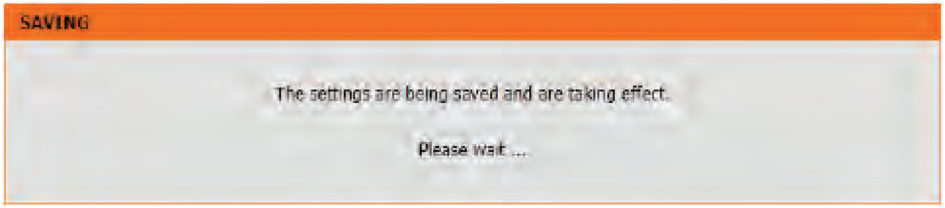
SETUP COMPLETE!

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



SAVING

The settings are being saved and are taking effect.

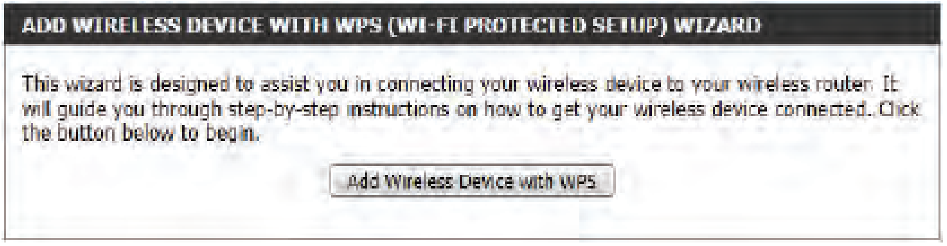
Please wait ...

End of Wizard.

Wi-Fi Protected Setup Wizard

Wireless Settings: Wi-Fi Protected Setup Wizard

If your Wireless Clients support the WPS connection method, this Wi-Fi Protected Setup Wizard can be used to initiate a 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 using the WPS method.



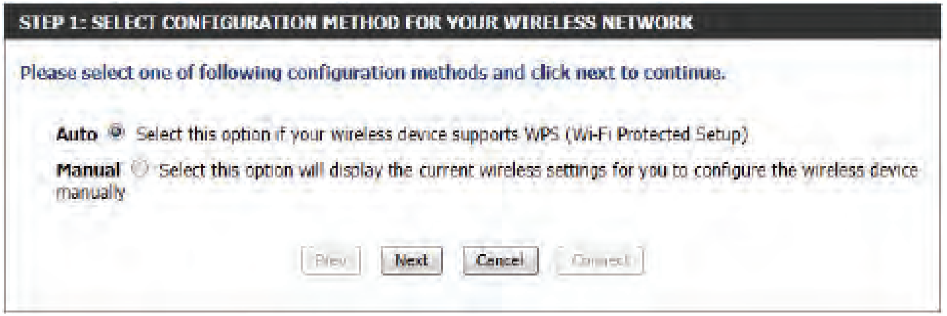
ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

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

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

Step 1: In this step the user have 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.

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



STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

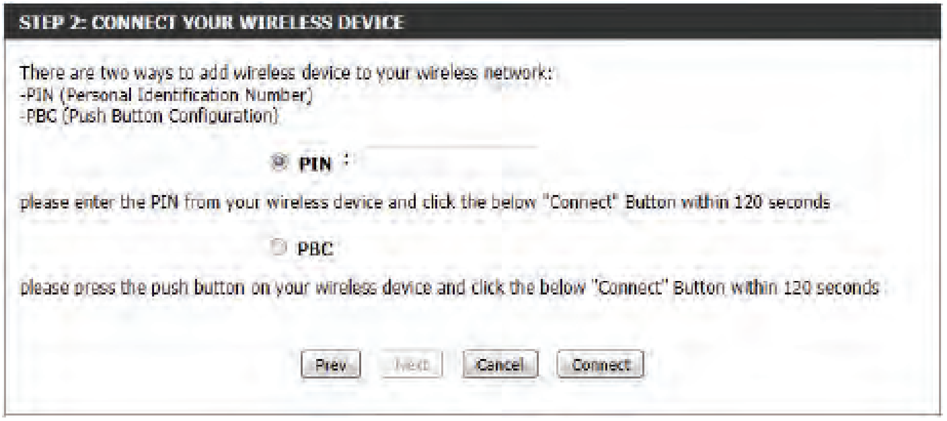
Please select one of following configuration methods and click next to continue.

Auto ● Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

Manual ○ Select this option will display the current wireless settings for you to configure the wireless device manually

Step 2: After selecting **Auto**, the following page will appear. There are two ways to add a wireless device, that supports WPS. Firstly, there is the Personal Identification Number (**PIN**) method. Using this method will prompt the user to enter a PIN code. This PIN code should be identical on the wireless client. Secondly, there is the Push Button Configuration (**PBC**) method. Using this method will allow the wireless client to connect to this device by similarly pressing the PBC button on it.

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



STEP 2: CONNECT YOUR WIRELESS DEVICE

There are two ways to add wireless device to your wireless network:
-PIN (Personal Identification Number)
-PBC (Push Button Configuration)

● **PIN** :

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

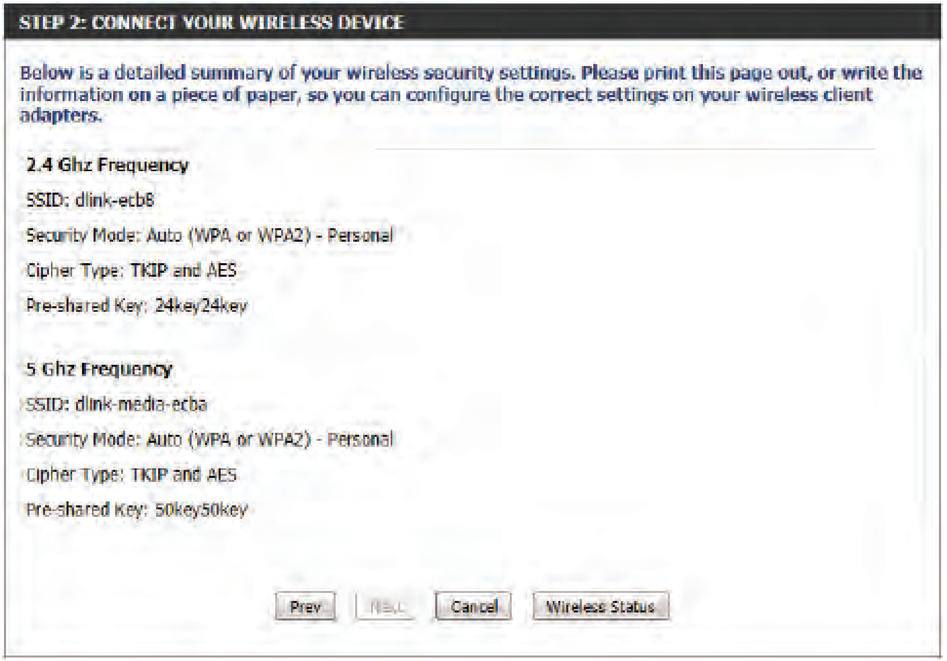
○ **PBC**

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

Step 2: After selecting Manual, the following page will appear. On this page to user 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 can't use the WPS method to connect to this device.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page. Click on the **Wireless Status** button to navigate to the Status > Wireless page to view what wireless client are connected to this device.

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.

2.4 Ghz Frequency

SSID: dlink-ecb8

Security Mode: Auto (WPA or WPA2) - Personal

Cipher Type: TKIP and AES

Pre-shared Key: 24key24key

5 Ghz Frequency

SSID: dlink-media-ecba

Security Mode: Auto (WPA or WPA2) - Personal

Cipher Type: TKIP and AES

Pre-shared Key: 50key50key

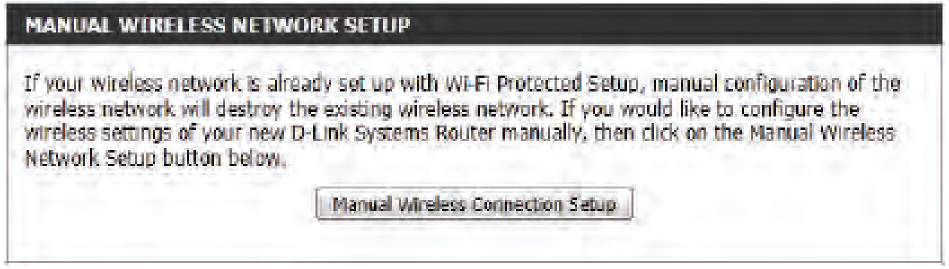
Manual Wireless Network Setup

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 the more advanced user and includes all parameters that can be configured for wireless connectivity.

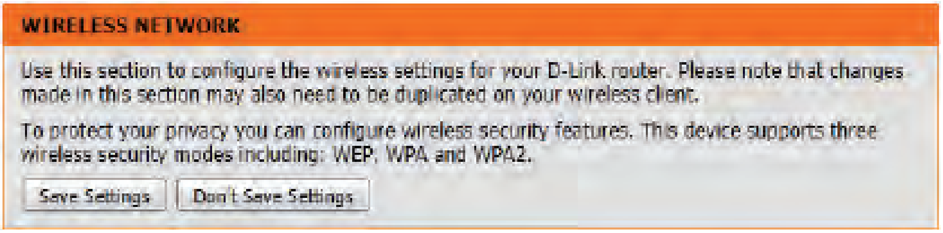
To initiate the Manual Wireless Setup page, click on the **Manual Wireless Connection Setup** button.

On this page the user can configure all the parameters related to the wireless connectivity of this router.



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

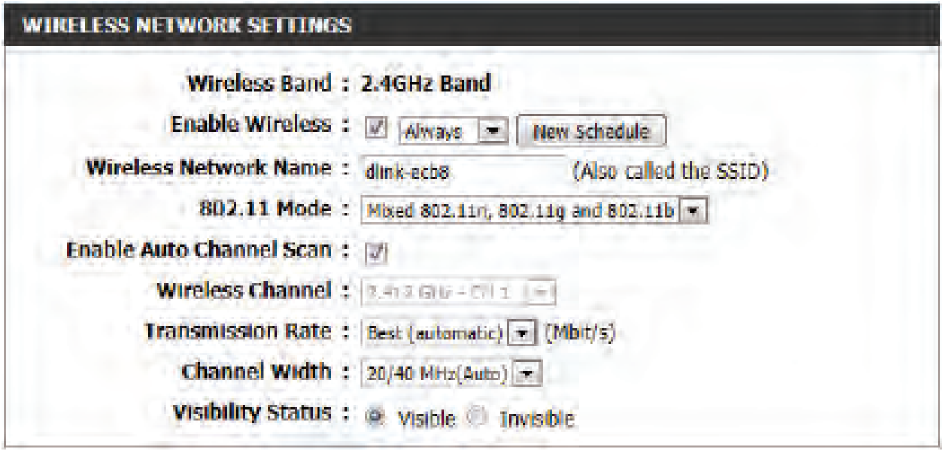
Use this section to configure the wireless settings for your D-Link router. Please note that changes made in this section may also need to be duplicated on your wireless client.

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

The following parameters will be available for configuration:

Wireless Band: Displays the wireless band being configured. In this option we find that the following parameters will be regarding the 2.4GHz band.

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click New Schedule to create a new schedule.



WIRELESS NETWORK SETTINGS

Wireless Band : 2.4GHz Band

Enable Wireless : ☑ Always ▾ New Schedule

Wireless Network Name : dlink-ecb8 (Also called the SSID)

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

Enable Auto Channel Scan : ☑

Wireless Channel : 2.412 GHz - CH 1 ▾

Transmission Rate : Best (automatic) ▾ (Mbit/s)

Channel Width : 20/40 MHz(Auto) ▾

Visibility Status : ● Visible ○ Invisible

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. Enable Auto Channel

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.

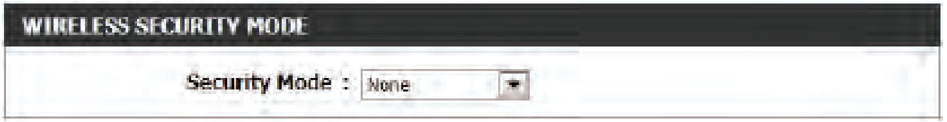
Wireless Channel: By default the channel is set to 1. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.

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

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

Visibility Status: The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcasted to anyone within the range of your signal. If you are not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

By default the wireless security of this router will be disabled. In this next option the user can enabled or disable wireless security for the frequency band 2.4GHz. There are two types of encryption that can be used. WEP or WPA/WPA2.

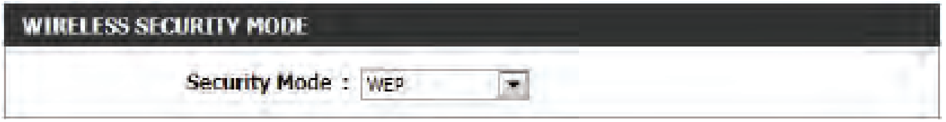


WIRELESS SECURITY MODE

Security Mode : None

Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. Even though it is known as a 'weak' security method, it is better than no security at all. Older wireless adapter sometimes only supports WEP encryption and thus we still find this encryption method used today.



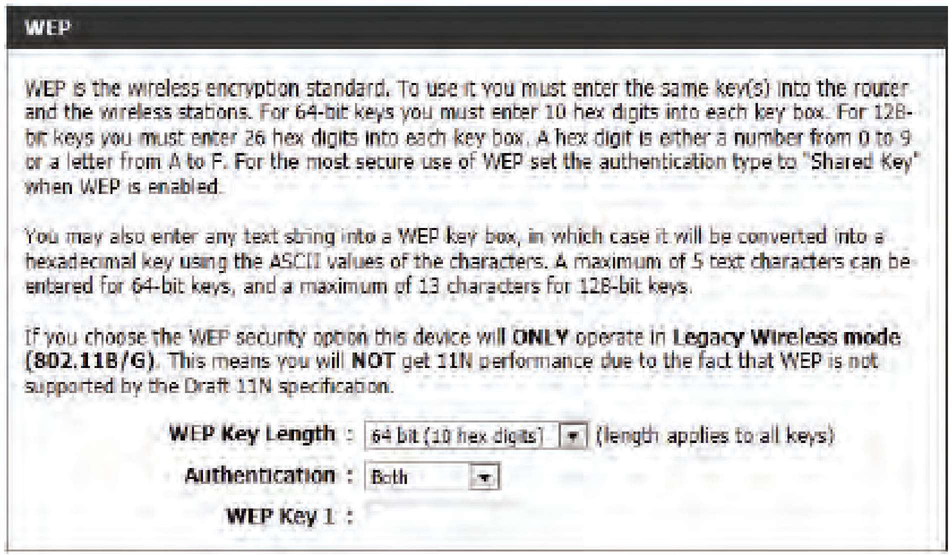
WIRELESS SECURITY MODE

Security Mode : WEP

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

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 :

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 and up to date 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 (Shared Secret) for security.

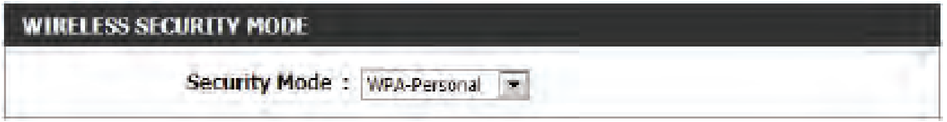
The following parameters will be available for configuration:

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**).

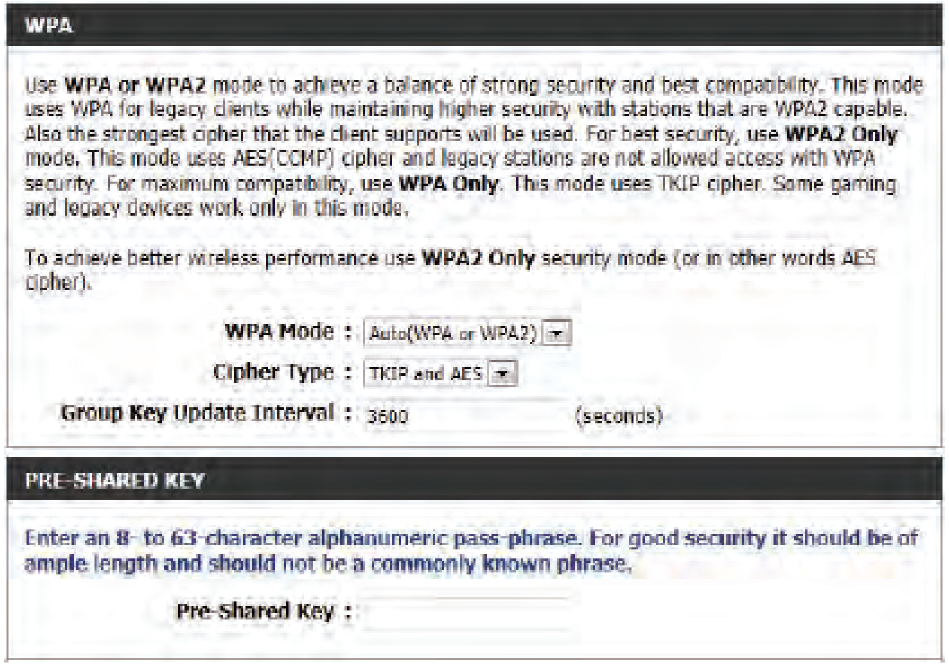
Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Pre-Shared Key: Enter the shared secret used here. This secret phrase needs to be the same on all of the 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-Personal

Wi-Fi Protected Access (WPA) is the most advanced and up to date 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 (Shared Secret) for security.

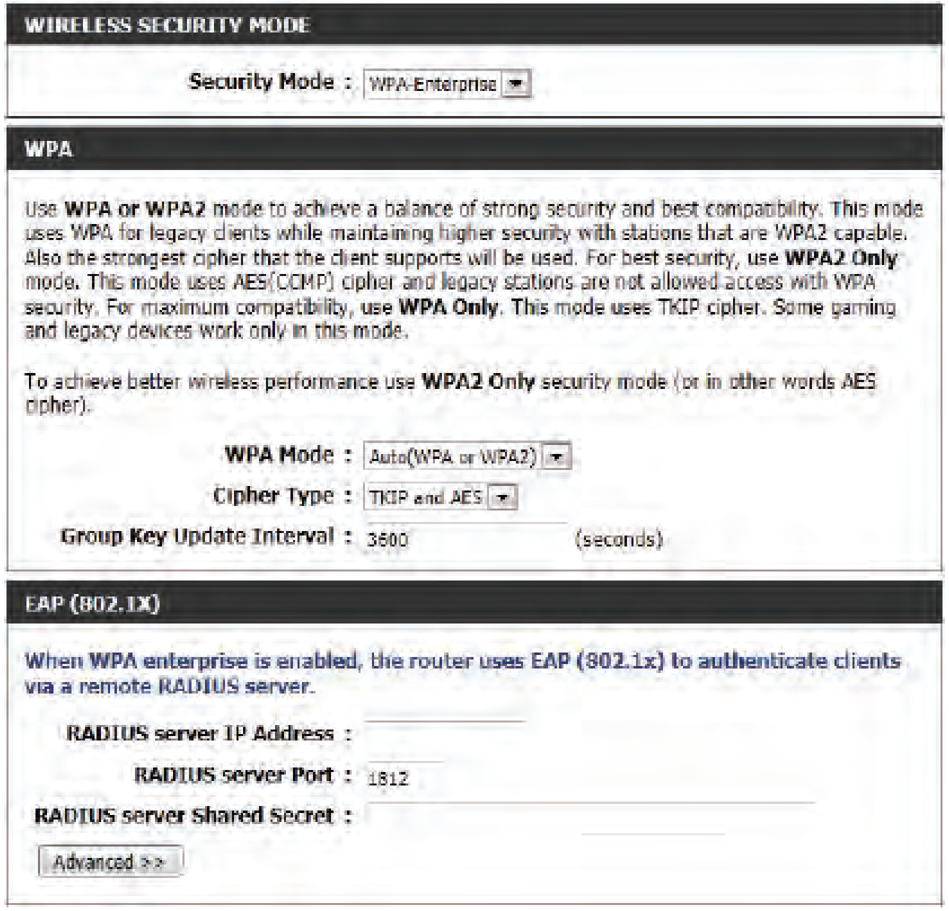
The following parameters will be available for configuration:

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.

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



WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

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)

EAP (802.1X)

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

RADIUS server IP Address :

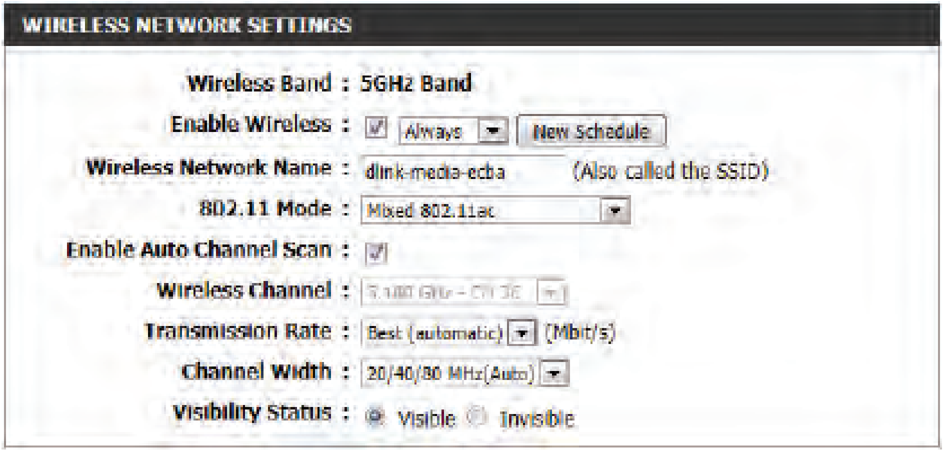
RADIUS server Port : 1812

RADIUS server Shared Secret :

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 used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

The following parameters will be available for configuration:



WIRELESS NETWORK SETTINGS

Wireless Band : 5GHz Band

Enable Wireless : ☑ Always ▾ New Schedule

Wireless Network Name : dlink-media-ecba (Also called the SSID)

802.11 Mode : Mixed 802.11ac ▾

Enable Auto Channel Scan : ☑

Wireless Channel : 5.180 GHz - CH 36 ▾

Transmission Rate : Best (automatic) ▾ (Mbit/s)

Channel Width : 20/40/80 MHz(Auto) ▾

Visibility Status : ● Visible ○ Invisible

Wireless Band: Displays the wireless band being configured. In this option we find that the following parameters will be regarding the 5GHz band.

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click New Schedule to create 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. Enable Auto Channel

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.

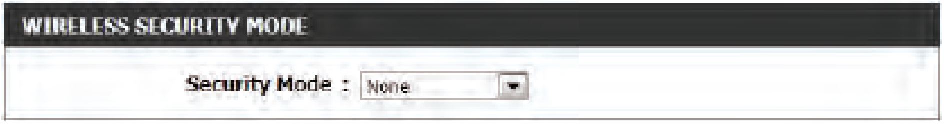
Wireless Channel: By default the channel is set to 36. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.

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

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

Visibility Status: The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcasted to anyone within the range of your signal. If you are not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

By default the wireless security of this router will be disabled. In this next option the user can enabled or disable wireless security for the frequency band 2.4GHz. There are two types of encryption that can be used. WEP or WPA/WPA2.

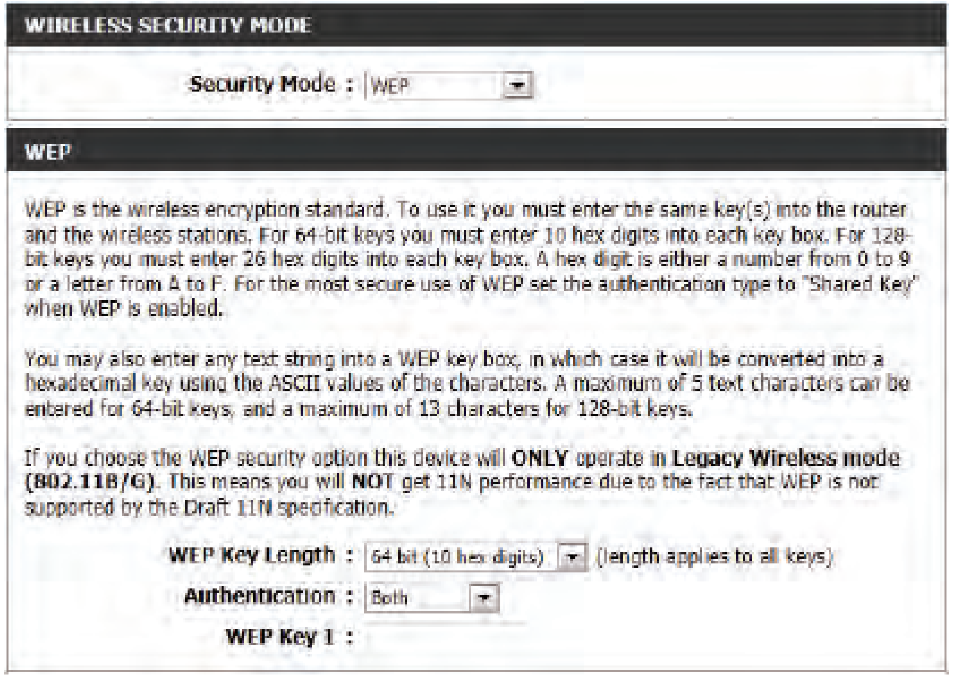


WIRELESS SECURITY MODE

Security Mode : None

Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. Even though it is known as a ‘weak’ security method, it is better than no security at all. Older wireless adapter sometimes only supports WEP encryption and thus we still find this encryption method used today.



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 :

The following parameters will be available for configuration:

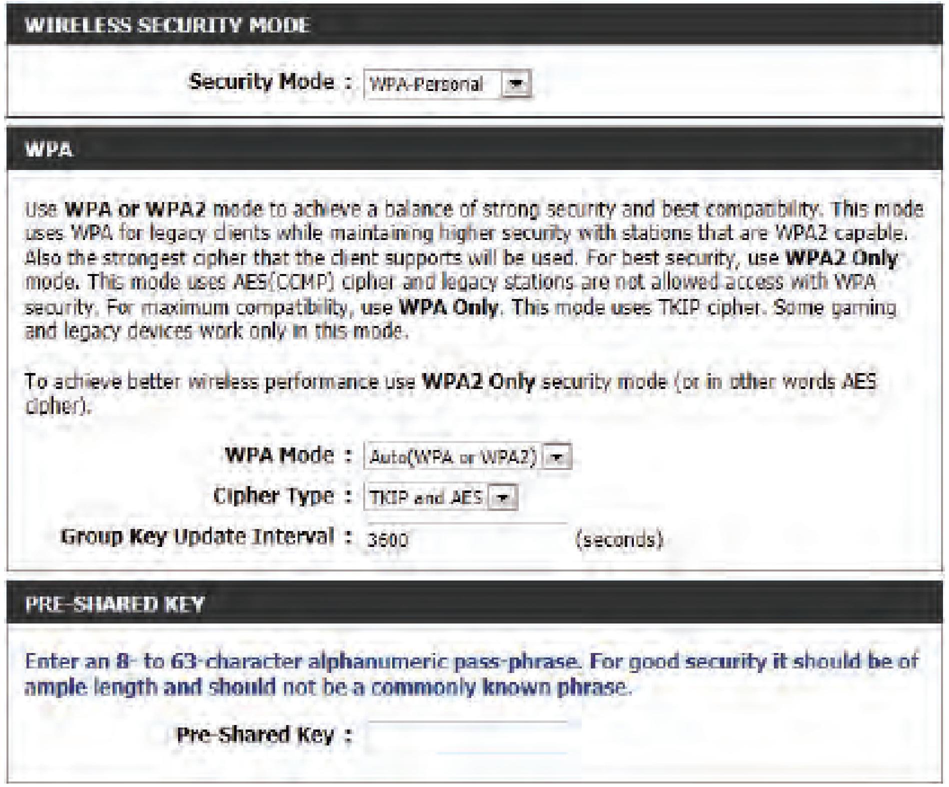
WEP Key Length: Here the user can specify to either use a 64Bit or a 128Bit encrypted key.

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: WPA-Personal

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP).



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 :

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.

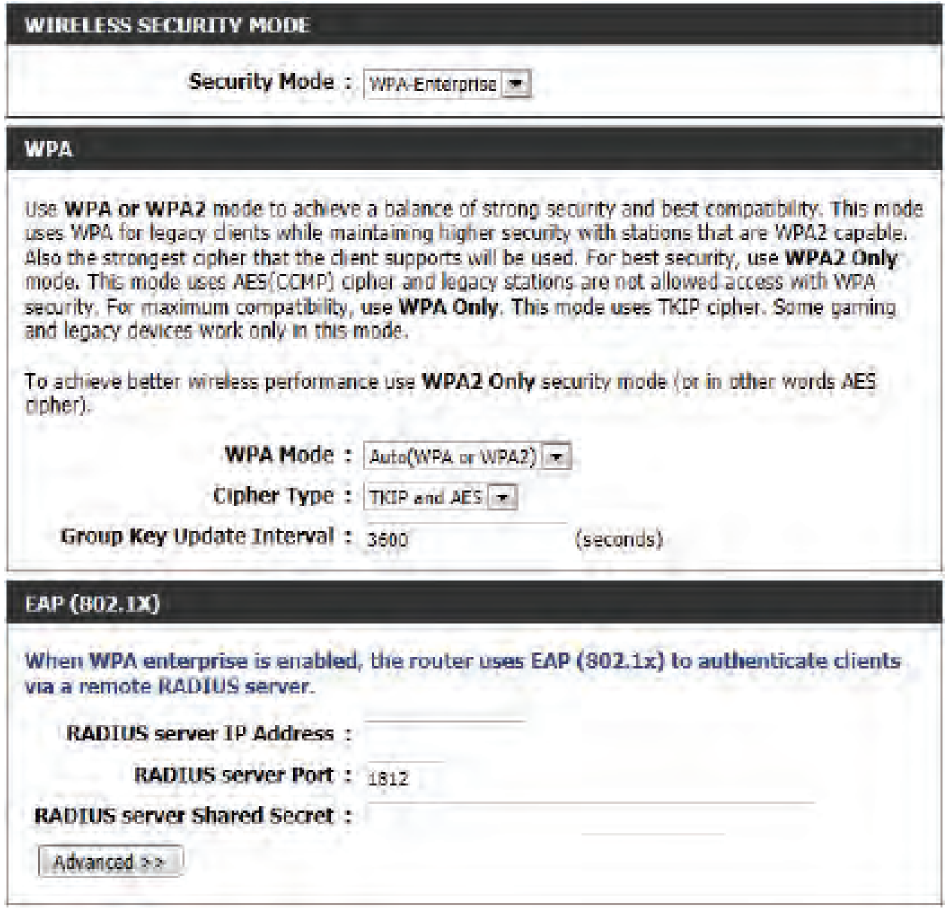
Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), and Both (**TKIP and AES**).

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 shared secret used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

Wireless Security Mode: WPA-Enterprise

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP).



WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

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)

EAP (802.1X)

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

RADIUS server IP Address :

RADIUS server Port : 1812

RADIUS server Shared Secret :

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.

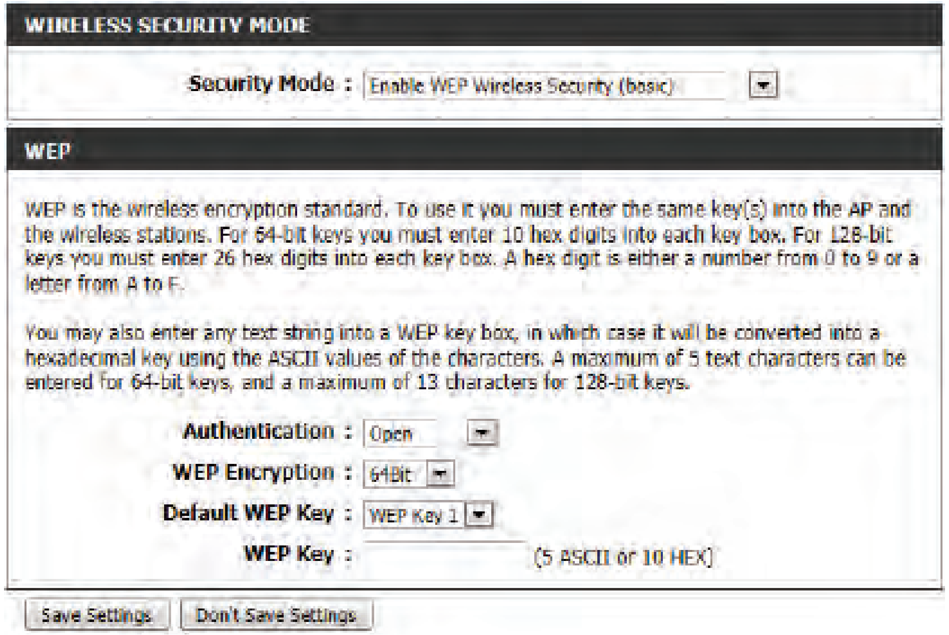
RADIUS Server IP Address: When the user chooses to use the EAP authentication framework, the RADIUS server's IP address can be entered here.

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 used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

Wireless Security Mode: Enable WEP Wireless Security (basic)

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. Even though it is known as a 'weak' security method, it is better than no security at all. Older wireless adapter sometimes only supports WEP encryption and thus we still find this encryption method used today.



WIRELESS SECURITY MODE

Security Mode : Enable WEP Wireless Security (basic)

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the AP 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.

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.

Authentication : Open

WEP Encryption : 64Bit

Default WEP Key : WEP Key 1

WEP Key : (5 ASCII or 10 HEX)

The following parameters will be available for configuration:

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

Default WEP Key: Select the default WEP key number that will be used for the encryption.

WEP Key: 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.

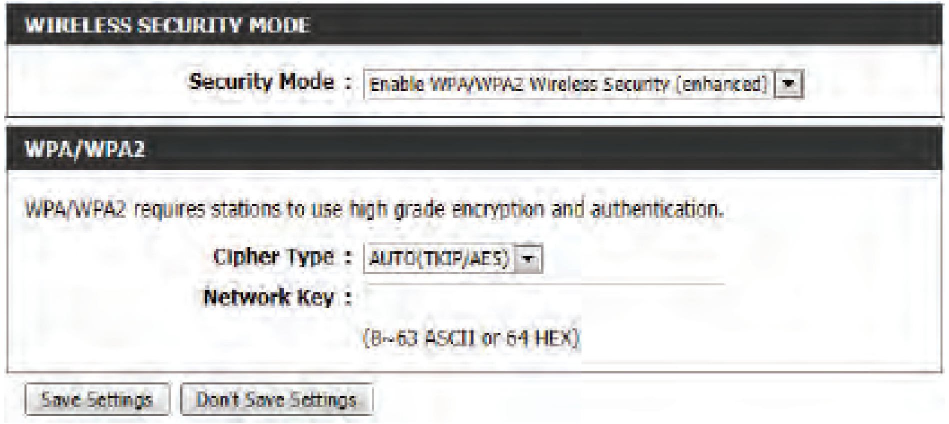
Wireless Security Mode: Enable WPA/WPA2 Wireless Security (enhanced)

Wi-Fi Protected Access (WPA) is a more advanced and up to date wireless encryption method used today. This is the recommended wireless security option.

The following parameters will be available for configuration:

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 (**Auto TKIP and AES**).

Network Key: Enter the shared secret used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.



WIRELESS SECURITY MODE

Security Mode : Enable WPA/WPA2 Wireless Security (enhanced)

WPA/WPA2

WPA/WPA2 requires stations to use high grade encryption and authentication.

Cipher Type : AUTO(TKIP/AES)

Network Key :

(8~63 ASCII or 64 HEX)

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

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-820L offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WPA?

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

The 2 major improvements over WEP:

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

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Network Settings

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

Router Settings

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

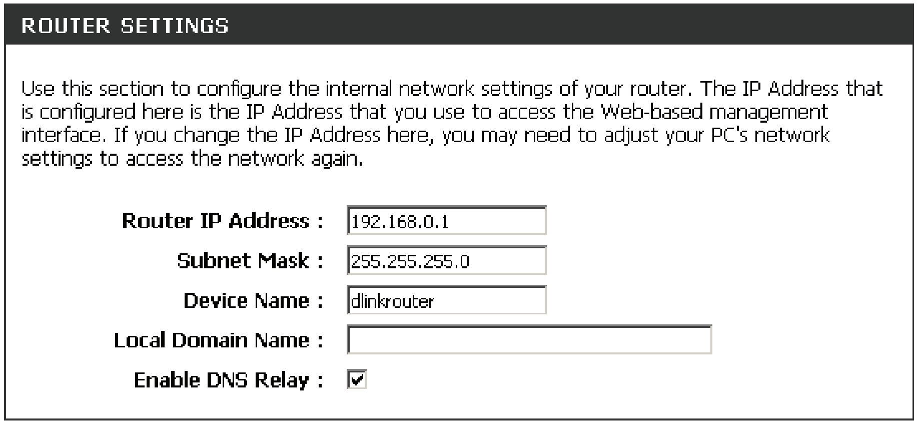
If you change the IP address, once you click **Save Settings**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

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 : 192.168.0.1

Subnet Mask : 255.255.255.0

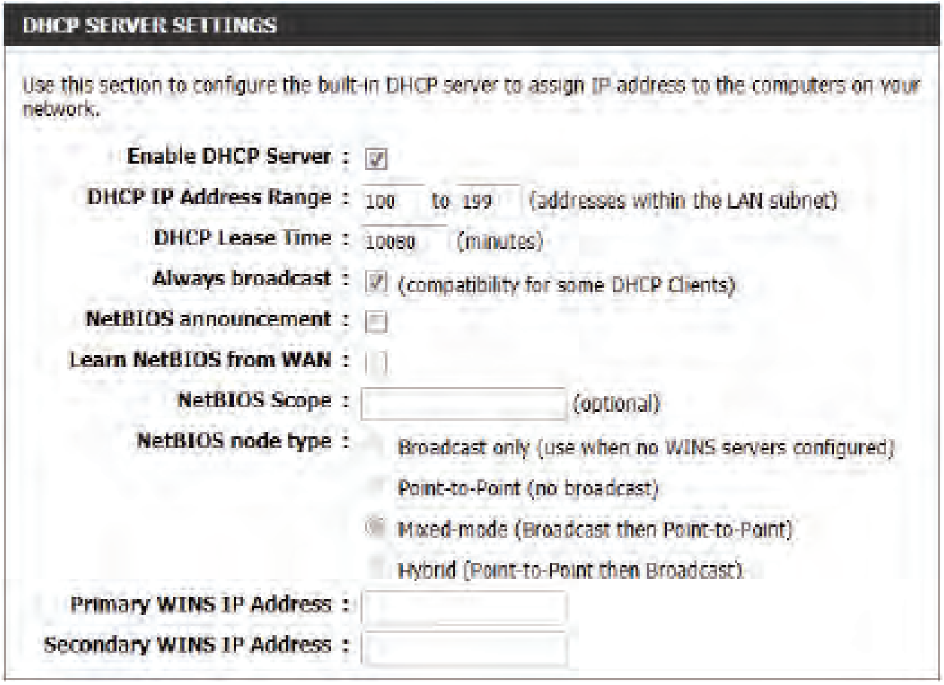
Device Name : dlinkrouter

Local Domain Name :

Enable DNS Relay : ☑

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-820L has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-820L. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.



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 :	

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

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

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

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 allow LAN hosts to discover all other computers within the network, e.g. within Network Neighborhood.

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 the '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, this 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 operation 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, this indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operation 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, this indicates to use local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is preferred you try M-Node operation first. This setting has no effect if the 'Learn NetBIOS information from WAN' 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 IP address only to that computer or device.

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

Enable: Check this box to enable the reservation.

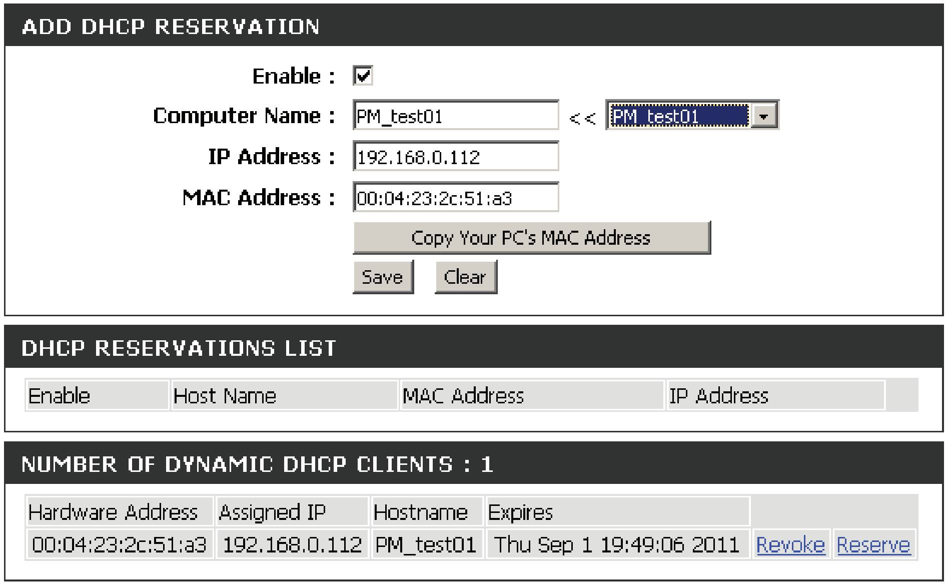
Computer Name: Enter the computer name or select from the drop-down menu and click **<<**.

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

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

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

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



ADD DHCP RESERVATION

Enable : ☑

Computer Name : PM_test01 << PM_test01

IP Address : 192.168.0.112

MAC Address : 00:04:23:2c:51:a3

DHCP RESERVATIONS LIST

Enable	Host Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS : 1

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

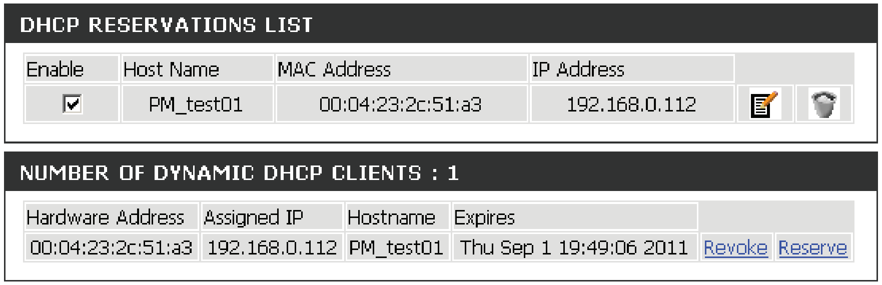
DHCP Reservations List

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 to remove the reservation from the list.



DHCP RESERVATIONS LIST

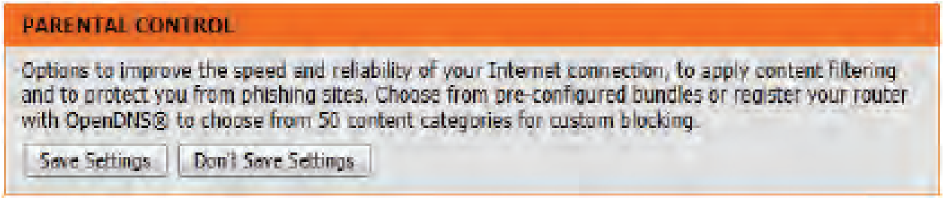
Enable	Host Name	MAC Address	IP Address		
☑	PM_test01	00:04:23:2c:51:a3	192.168.0.112		

NUMBER OF DYNAMIC DHCP CLIENTS : 1

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

Parental Control

Parental control 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 types.



PARENTAL CONTROL

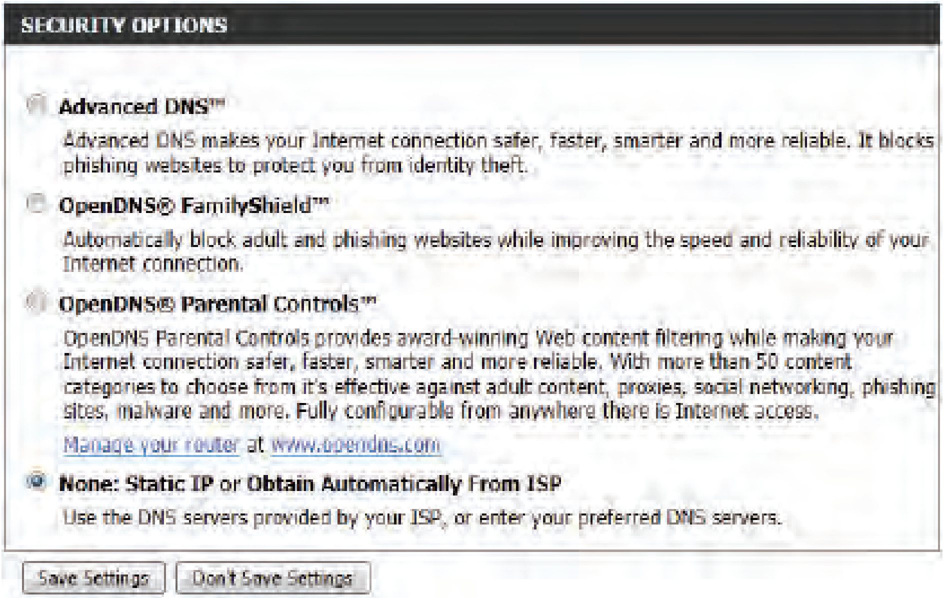
Options to improve the speed and reliability of your Internet connection, to apply content filtering and to protect you from phishing sites. Choose from pre-configured bundles or register your router with OpenDNS® to choose from 50 content categories for custom blocking.

The following parameters will be available for configuration:

Advanced DNS: Select this option to enable a fast and reliable DNS with minimal blocking of phishing sites only. No OpenDNS account required.

OpenDNS® FamilyShield: Select this option to enable a fast and reliable DNS with non-configurable blocking of sites that are inappropriate or risky for children. No OpenDNS account required.

OpenDNS® Parental Control: Select this option to enable a fast and reliable DNS with configurable content filtering and phishing protection. This option includes an OpenDNS account. Click on the 'Manage your router' link to navigate to the OpenDNS account website, where you can either login (if you have an existing account) or you can register a new OpenDNS account.



SECURITY OPTIONS

○ **Advanced DNS™**
Advanced DNS makes your Internet connection safer, faster, smarter and more reliable. It blocks phishing websites to protect you from identity theft.

○ **OpenDNS® FamilyShield™**
Automatically block adult and phishing websites while improving the speed and reliability of your Internet connection.

○ **OpenDNS® Parental Controls™**
OpenDNS Parental Controls provides award-winning Web content filtering while making your Internet connection safer, faster, smarter and more reliable. With more than 50 content categories to choose from it's effective against adult content, proxies, social networking, phishing sites, malware and more. Fully configurable from anywhere there is Internet access.
Manage your router at www.opendns.com

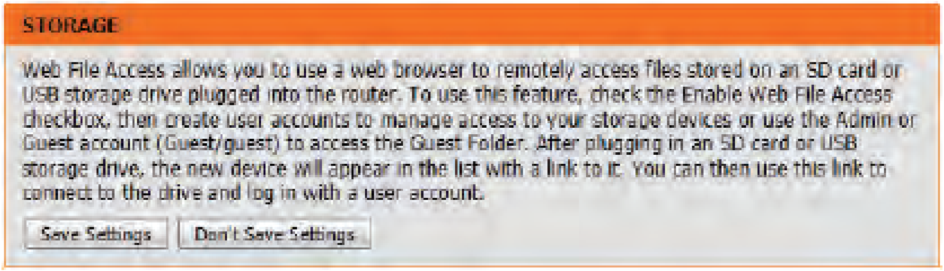
● **None: Static IP or Obtain Automatically From ISP**
Use the DNS servers provided by your ISP, or enter your preferred DNS servers.

None: Select this option to enable the option to specify the DNS servers provided via DHCP by their ISP or their own preferred DNS servers.

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

Storage

This page allows the user to use a web browser to remotely access files stored on an SD card or USB storage drive plugged into the router. You can access storage device by http://shareport.local when you enable SharePort Web Access



STORAGE

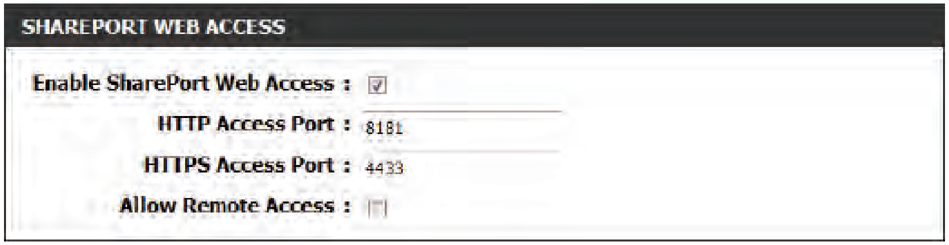
Web File Access allows you to use a web browser to remotely access files stored on an SD card or USB storage drive plugged into the router. To use this feature, check the Enable Web File Access checkbox, then create user accounts to manage access to your storage devices or use the Admin or Guest account (Guest/guest) to access the Guest Folder. After plugging in an SD card or USB storage drive, the new device will appear in the list with a link to it. You can then use this link to connect to the drive and log in with a user account.

The following parameters will be available for configuration:

Enable SharePort Web Access: Tick this option to enable the share port web access feature.

HTTP Access Port: Enter the HTTP Access Port number used here. By default, this value is 8181.

HTTPS Access Port: Enter the HTTPS Access Port number used here. By default, this value is 4433.



SHAREPORT WEB ACCESS

Enable SharePort Web Access : ☑

HTTP Access Port : 8181

HTTPS Access Port : 4433

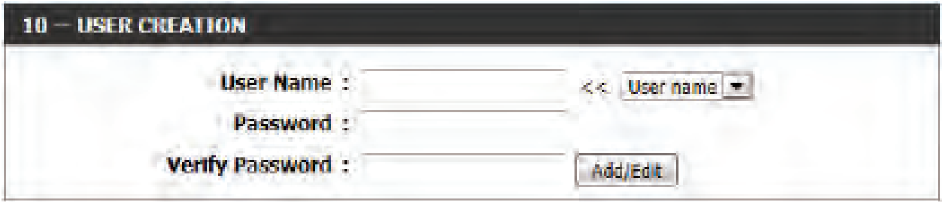
Allow Remote Access : □

Allow Remote Access: Tick this option the allow remote access to this router.

In the **User Creation** section, the user can create and modify usernames and passwords.

The following parameters will be available for configuration:

User Name: In the **User Name** field we can enter the new username that will be created. Alternatively, if we want to modify an existing user account, select a username from the **drop-down** menu. It will automatically be added to the User Name field for modification.



10 — USER CREATION

User Name : << User name ▾

Password :

Verify Password :

Password: In the **Password** field, the user can enter the password that will be associated with the user account.

Verify Password: In the **Verify Password** field, the user can re-enter the password that will be associated with the user account.

Click the **Add/Edit** button the add a new user account or modify an existing account.

In the **User List** section, the user can modify or delete different user settings for each account.

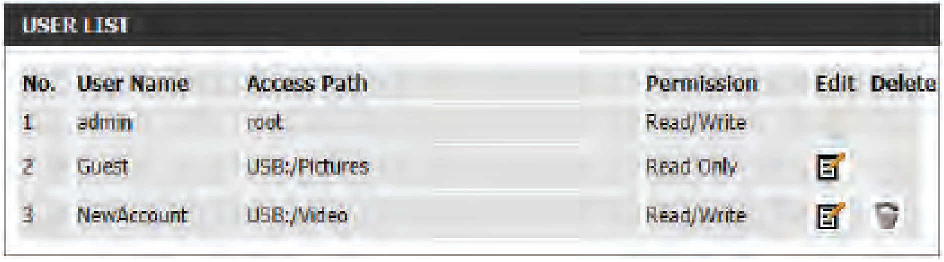
The following parameters will be available in the display.

No. Displays the number of the entry in the user list.

User Name: Displays the user name of the entry in the list.

Access Path: Displays the access path of the entry in the list.

Permission: Displays the permission settings of the entry in the list.



USER LIST

No.	User Name	Access Path	Permission	Edit	Delete
1	admin	root	Read/Write		
2	Guest	USB:/Pictures	Read Only	📝	
3	NewAccount	USB:/Video	Read/Write	📝	🗑

Click the **Edit** icon to edit the access path and permission, for each user.
Click the **Delete** icon to delete an account from the list.

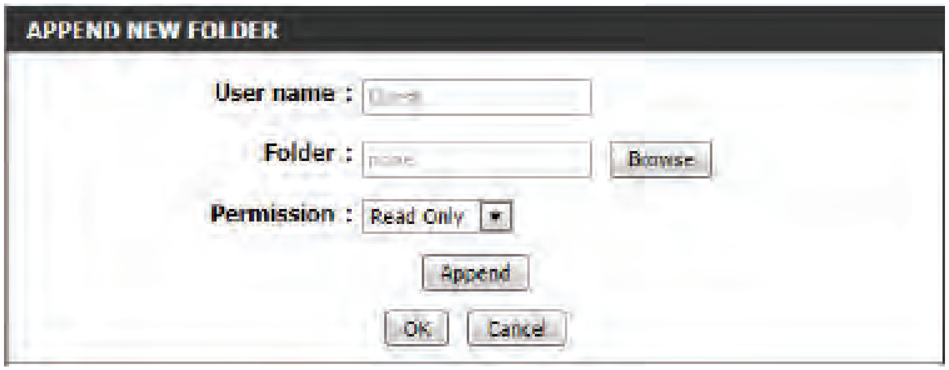
After click on the **Edit** button, this window will appear.

The following parameters will be available for configuration:

User Name: This field will display the current user name that will be modified.

Folder: This filed will display the access path that this user will have access to, after logging in. Click the Browse button to navigate to a folder, located on the USB storage device.

Permission: Here the user can select the appropriate permission setting for this user account. Permissions available for selection, from the drop-down menu are **Read Only** and **Read/Write**.



APPEND NEW FOLDER

User name : Guest

Folder : none

Permission : Read Only

Read Only permission will only allow this account to read data stored on the USB storage device within the constrains of the access path specified. **Read/Write** permission will allow this account to read and write data to and from the USB storage device within the constrains of the access path specified.

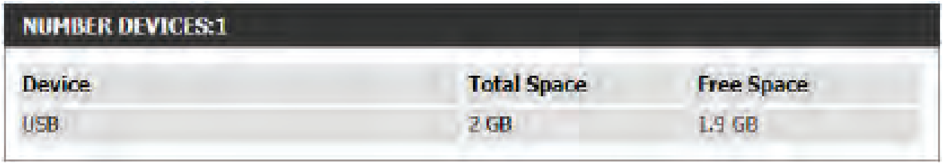
Click the **Append** button to add a blank account with the access path and permission specified.
Click the **OK** button to accept the changes made for the existing account.
Click the **Cancel** button to discard the changes made.

In the **Number Devices** section, the user can view information about the external USB storage devices inserted into the USB port of this router.

The following parameters will be available in the display

Number of Devices: This field will display the number of USB storage devices that are attached to the USB port of the router.

Device: This field will display the USB storage device's name.



NUMBER DEVICES:1

Device	Total Space	Free Space
USB	2 GB	1.9 GB

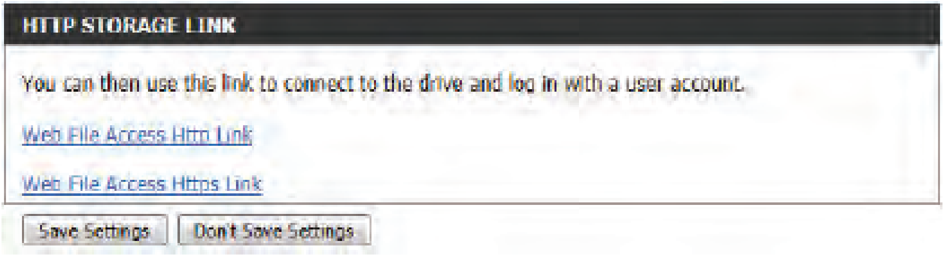
Total Space: This field will display the total space that is available on the USB storage device attached.

Free Space: This field will display the free space that is available on the USB storage device attached.

In the **HTTP Storage Link** section, the user can use this link to connect to the drive remotely after logging in with a user account.

Notice the path of the link(s) provided will point the external interface of this router. If no DDNS account is specified on the Dynamic DNS page, the WAN IP address will be used. If, however, a DDNS account is specified, then the domain name will be used.

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



HTTP STORAGE LINK

You can then use this link to connect to the drive and log in with a user account.

Web File Access Http Link

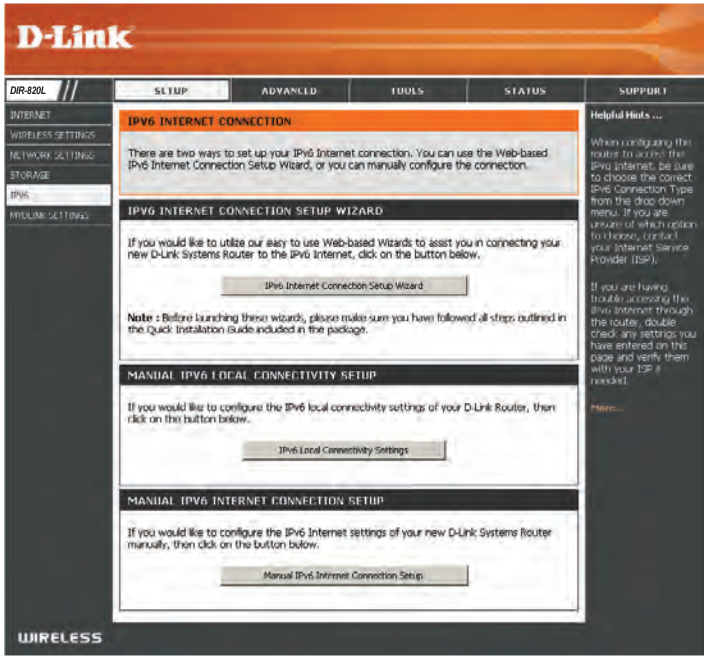
Web File Access Https Link

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

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.



IPV6 INTERNET CONNECTION

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

IPV6 INTERNET CONNECTION SETUP WIZARD

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

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

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.

MANUAL IPV6 INTERNET CONNECTION SETUP

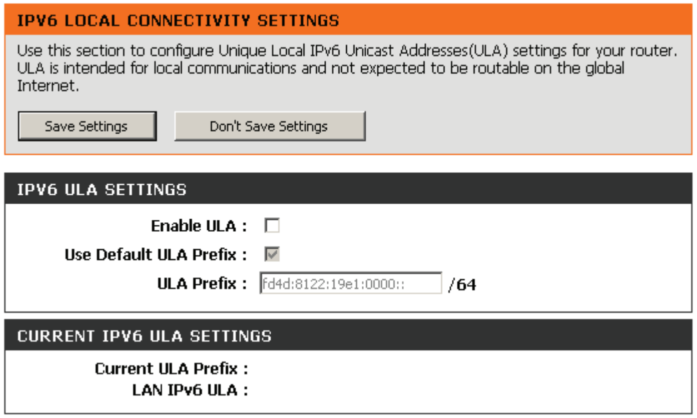
If you would like to configure the IPv6 Internet settings of your new D-Link Systems Router manually, then click on the button below.

Helpful Hints ...

When configuring the router to access the IPv6 Internet, be sure to choose the correct IPv6 Connection Type from the drop down menu. If you are unsure of which option to choose, contact your Internet Service Provider (ISP).

If you are having trouble accessing the IPv6 Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.

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



IPV6 LOCAL CONNECTIVITY SETTINGS

Use this section to configure Unique Local IPv6 Unicast Addresses(ULA) settings for your router. ULA is intended for local communications and not expected to be routable on the global Internet.

IPV6 ULA SETTINGS

Enable ULA : □

Use Default ULA Prefix : ☑

ULA Prefix : fd4d:8122:19e1:0000:: /64

CURRENT IPV6 ULA SETTINGS

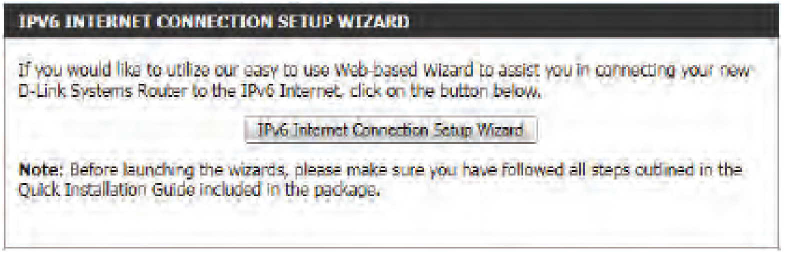
Current ULA Prefix :

LAN IPv6 ULA :

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.

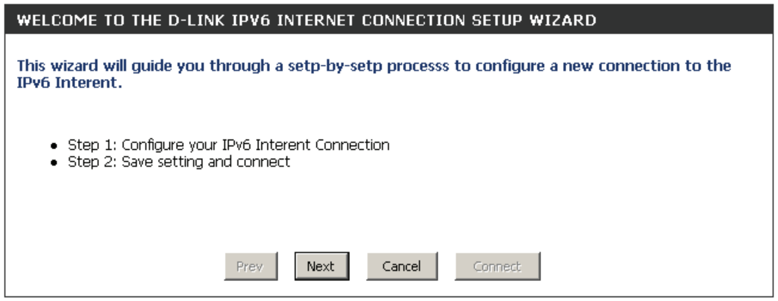


IPV6 INTERNET CONNECTION SETUP WIZARD

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

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

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

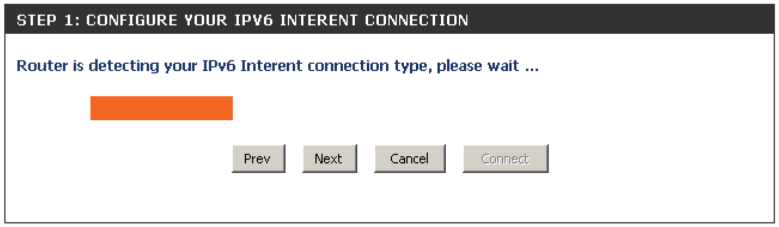


WELCOME TO THE D-LINK IPV6 INTERNET CONNECTION SETUP WIZARD

This wizard will guide you through a setp-by-setp processs to configure a new connection to the IPv6 Interent.

- Step 1: Configure your IPv6 Interent Connection
- Step 2: Save setting and connect

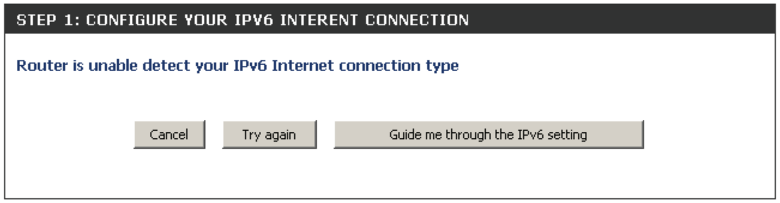
The router will try to detect whether its possible to obtain the IPv6 Internet connection type automatically. If this succeeds then the user will be guided through the input of the appropriate parameters for the connection type found.



STEP 1: CONFIGURE YOUR IPV6 INTERENT CONNECTION

Router is detecting your IPv6 Interent connection type, please wait ...

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.



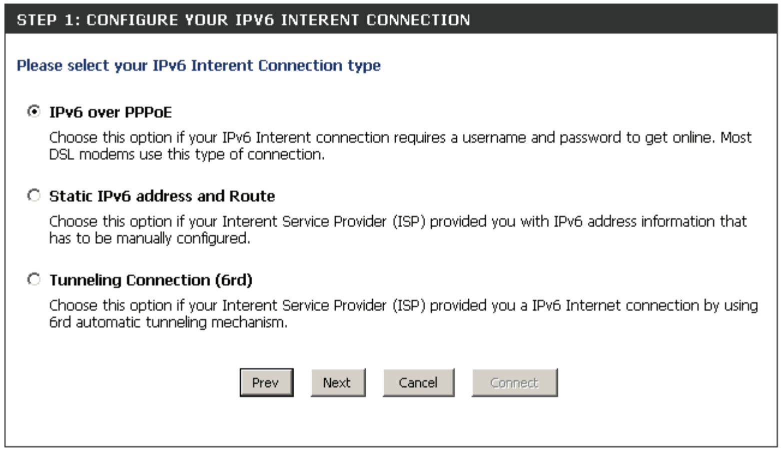
STEP 1: CONFIGURE YOUR IPV6 INTERENT CONNECTION

Router is unable detect your IPv6 Internet connection type

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.



STEP 1: CONFIGURE YOUR IPV6 INTERENT CONNECTION

Please select your IPv6 Interent Connection type

● **IPv6 over PPPoE**

Choose this option if your IPv6 Interent connection requires a username and password to get online. Most DSL modems use this type of connection.

○ **Static IPv6 address and Route**

Choose this option if your Interent Service Provider (ISP) provided you with IPv6 address information that has to be manually configured.

○ **Tunneling Connection (6rd)**

Choose this option if your Interent Service Provider (ISP) provided you a IPv6 Internet connection by using 6rd automatic tunneling mechanism.

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page.

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

IPv6 over PPPoE

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

The following parameters will be available for configuration:

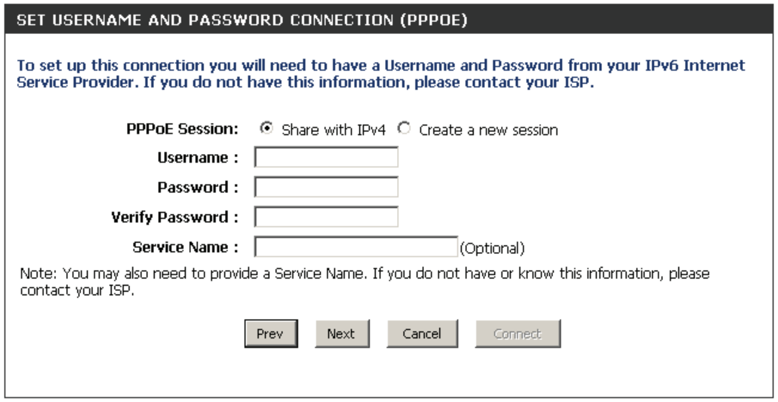
PPPoE Session: Select the PPPoE Session value used here. This option will state that this connection shares it’s information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.

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

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

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

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



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 :

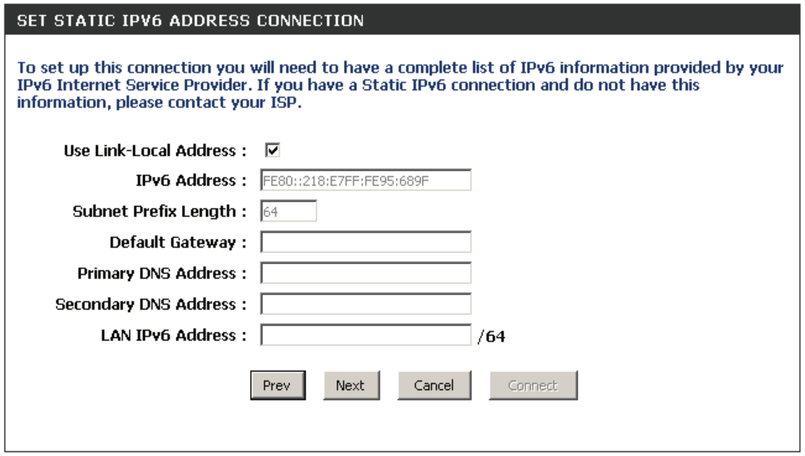
Verify Password :

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.



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::218:E7FF:FE95:689F

Subnet Prefix Length : 64

Default Gateway :

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 Address : /64

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.)

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.

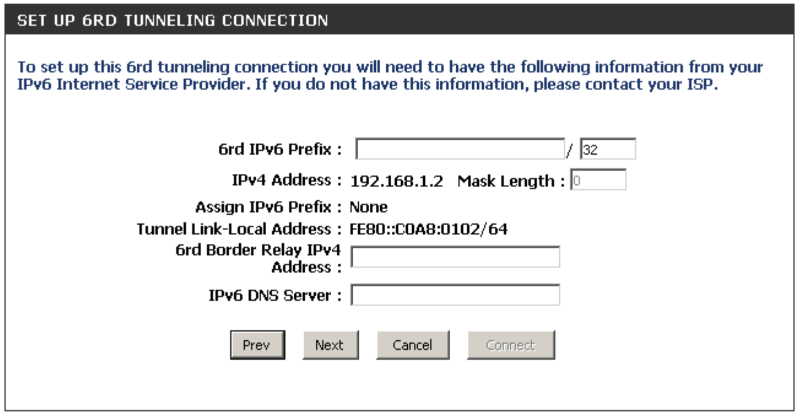
IPv4 Address: Enter the IPv4 address used here.

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.



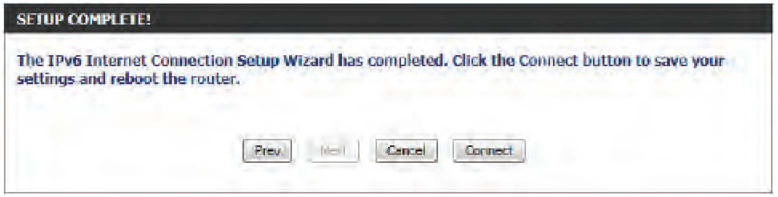
SET UP 6RD TUNNELING CONNECTION

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

6rd IPv6 Prefix : / 32
IPv4 Address : 192.168.1.2 Mask Length : 0
Assign IPv6 Prefix : None
Tunnel Link-Local Address : FE80::C0A8:0102/64
6rd Border Relay IPv4 Address :
IPv6 DNS Server :

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.



SETUP COMPLETE!

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

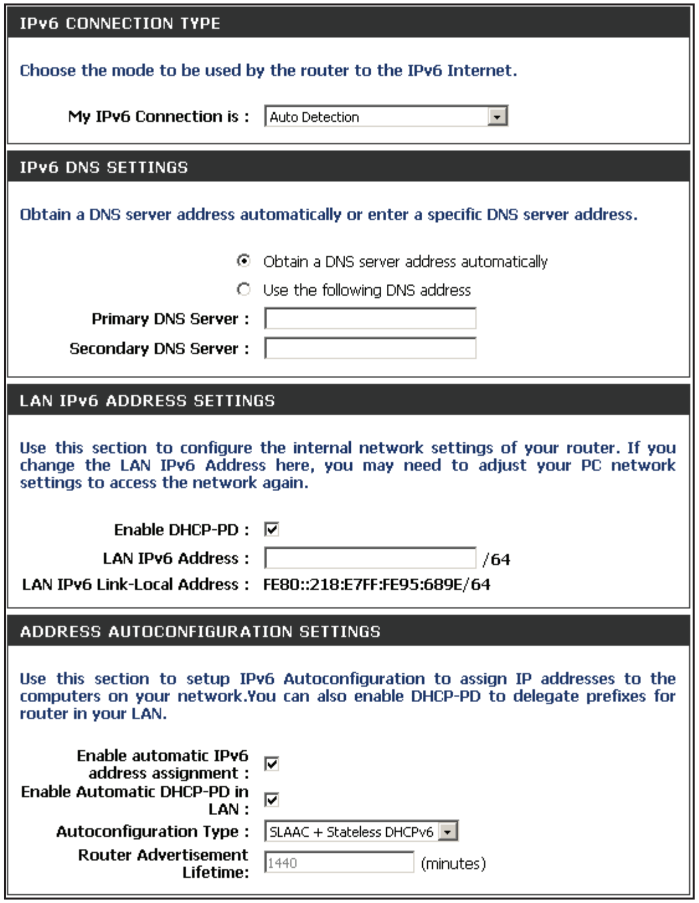
IPv6 Manual Setup

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

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

Auto Detection

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



IPv6 CONNECTION TYPE

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

My IPv6 Connection is : Auto Detection

IPv6 DNS SETTINGS

Obtain a DNS server address automatically or enter a specific DNS server address.

● Obtain a DNS server address automatically

○ 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 : ☑

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 : ☑

Enable Automatic DHCP-PD in LAN : ☑

Autoconfiguration Type : SLAAC + Stateless DHCPv6

Router Advertisement Lifetime: 1440 (minutes)

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.

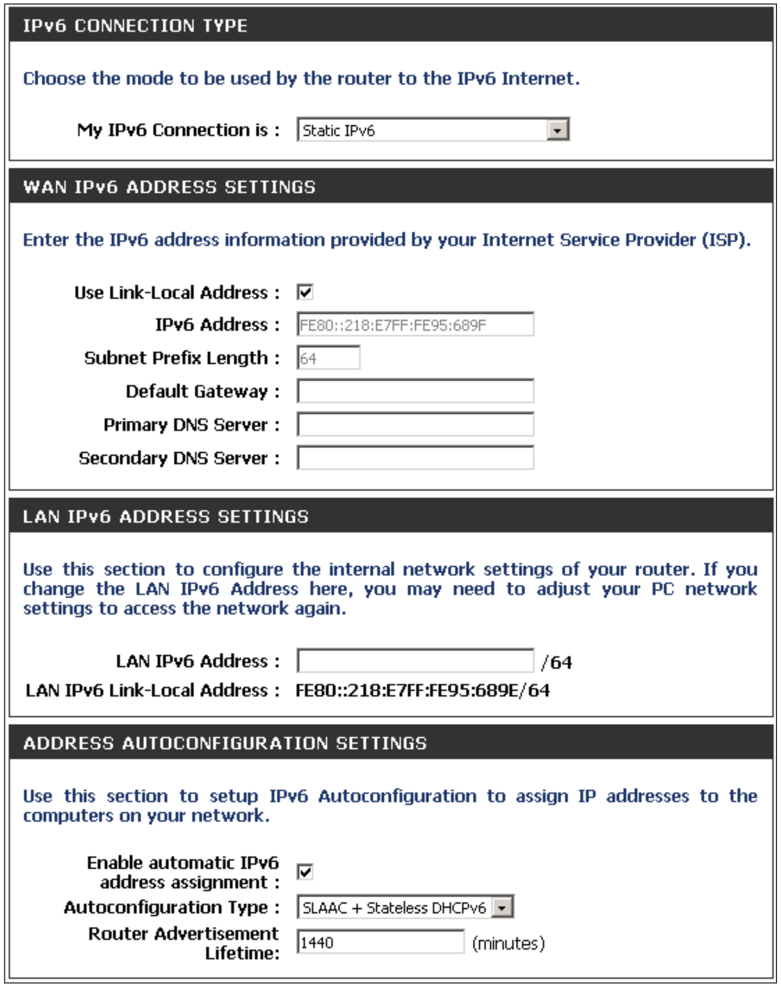
Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

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 : ☑

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 : ☑

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.

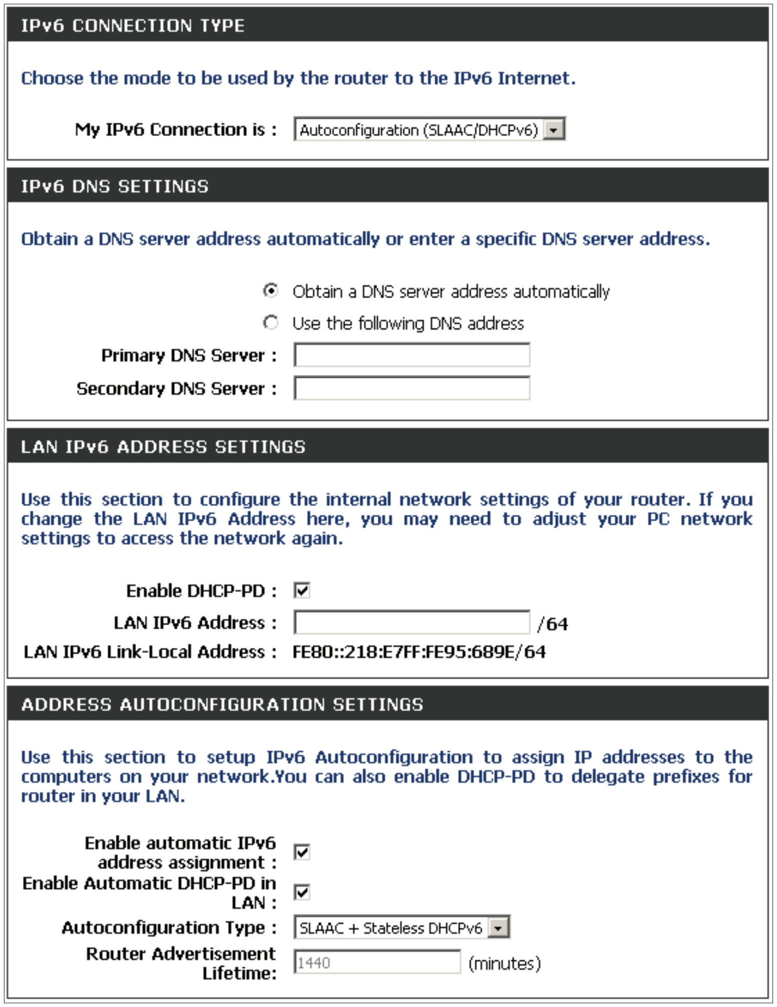
Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

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.

● Obtain a DNS server address automatically

○ 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 : ☑

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 : ☑

Enable Automatic DHCP-PD in LAN : ☑

Autoconfiguration Type : SLAAC + Stateless DHCPv6

Router Advertisement Lifetime: 1440 (minutes)

PPPoE

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

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

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

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

User Name: Enter your PPPoE user name.

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

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

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

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

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

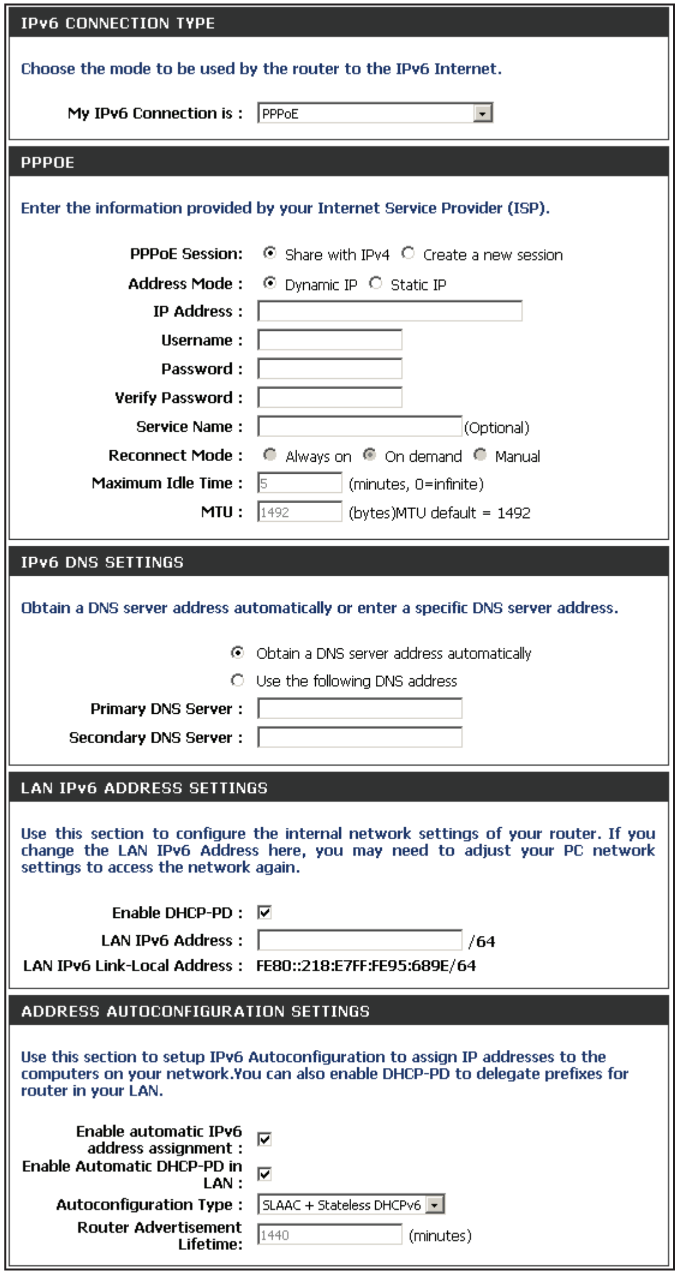
IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

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

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

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

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.



IPV6 CONNECTION TYPE

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

My IPv6 Connection is : PPPoE

PPPOE

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

PPPoE Session: ● Share with IPv4 ○ Create a new session
Address Mode : ● Dynamic IP ○ Static IP
IP Address :
Username :
Password :
Verify Password :
Service Name : (Optional)
Reconnect Mode : ○ Always on ● On demand ○ 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.

● Obtain a DNS server address automatically
○ 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 : ☑
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 : ☑
Enable Automatic DHCP-PD in LAN : ☑
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.

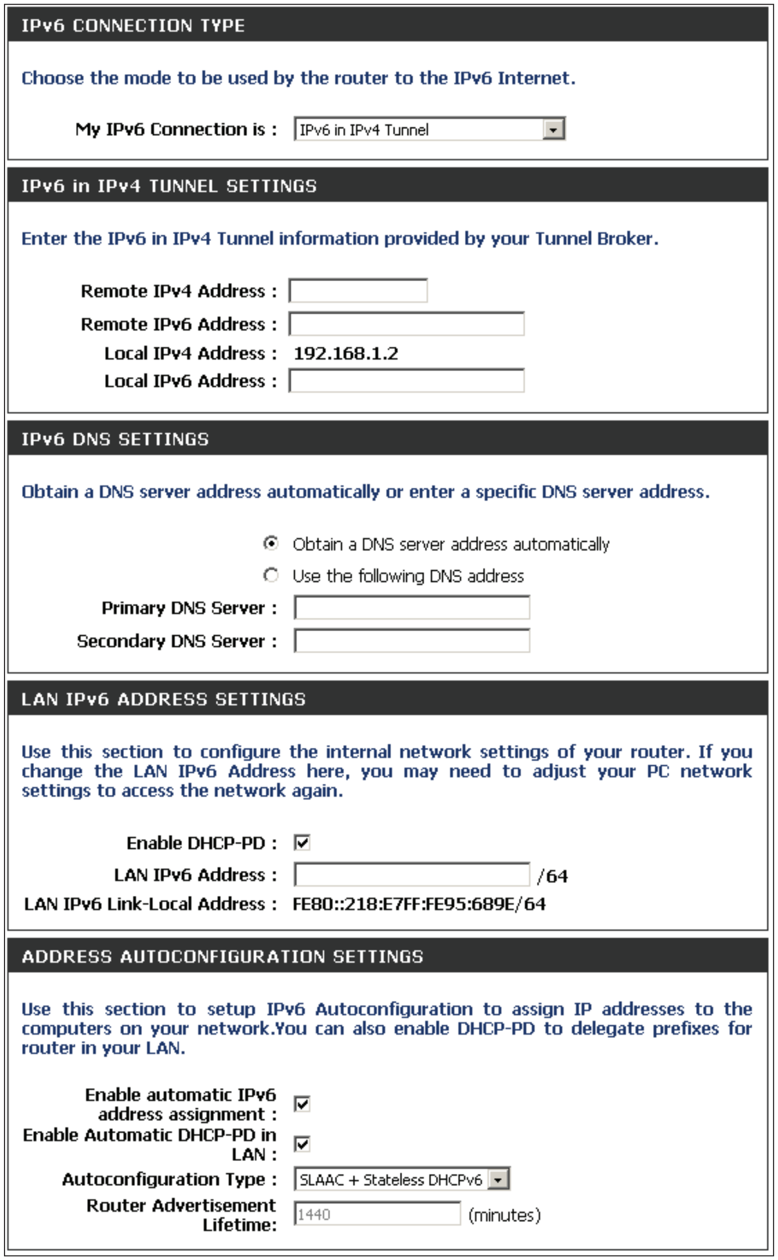
Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

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.

● Obtain a DNS server address automatically

○ 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 : ☑

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 : ☑

Enable Automatic DHCP-PD in LAN : ☑

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.

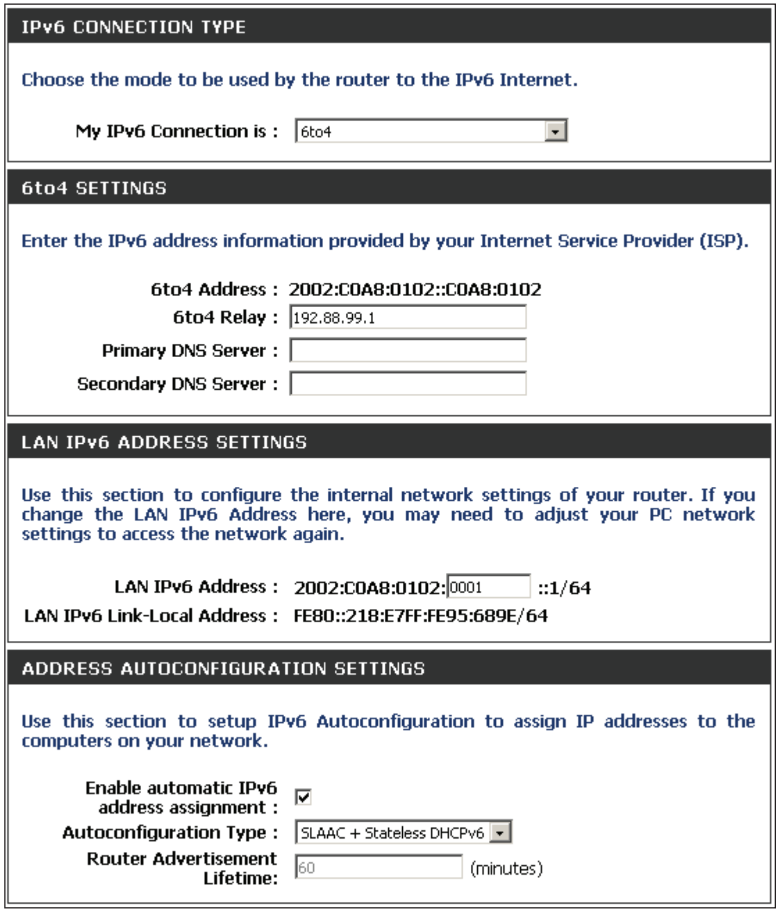
Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

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:C0A8:0102::C0A8:0102
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:C0A8:0102:0001 ::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 : ☑
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).

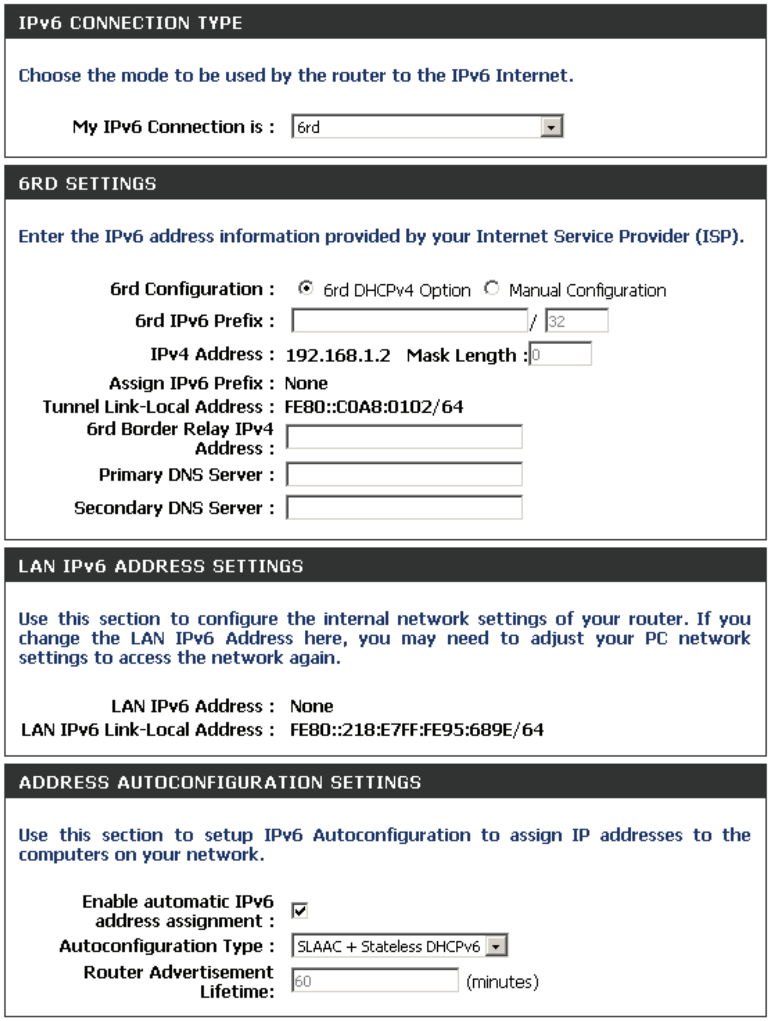
LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

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

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

My IPv6 Connection is : 6rd

6RD SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

6rd Configuration : ● 6rd DHCPv4 Option ○ Manual Configuration

6rd IPv6 Prefix : / 32

IPv4 Address : 192.168.1.2 Mask Length : 0

Assign IPv6 Prefix : None

Tunnel Link-Local Address : FE80::C0A8:0102/64

6rd Border Relay IPv4 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.

LAN IPv6 Address : None

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 : ☑

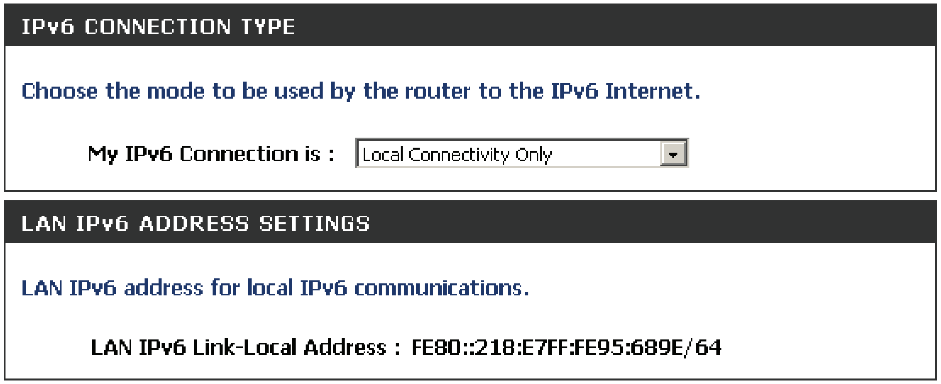
Autoconfiguration Type : SLAAC + Stateless DHCPv6

Router Advertisement Lifetime: 60 (minutes)

Link-Local Connectivity

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

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



IPV6 CONNECTION TYPE

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

My IPv6 Connection is : Local Connectivity Only

LAN IPV6 ADDRESS SETTINGS

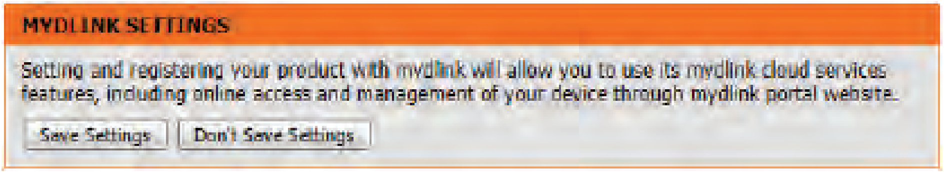
LAN IPv6 address for local IPv6 communications.

LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64

mydlink Settings

The DIR-820L features a new cloud service that pushes information such as firmware upgrade notifications, user activity, and intrusion alerts to the mydlink™ app on Android and Apple mobile devices. To insure 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 a user's online activity with real-time website browsing history, maintaining a safe and secure environment, especially for children at home.

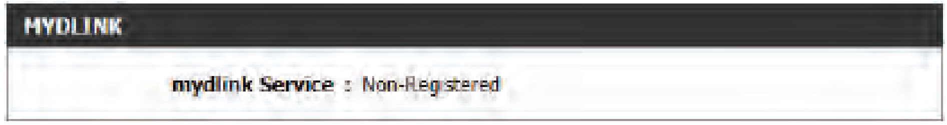
On this page the user can configure the mydlink™ settings for this router. This feature will allow us to use the mydlink cloud services that includes online access and management of this router through the mydlink portal website or portable device applications like iOS apps and Android applications.



MYDLINK SETTINGS

Setting and registering your product with mydlink will allow you to use its mydlink cloud services features, including online access and management of your device through mydlink portal website.

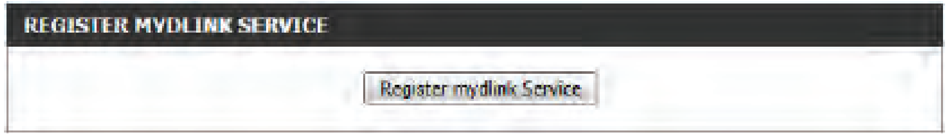
In the **mydlink** section, we can view the registration status of the mydlink account service. The **mydlink Service** field will either display **Registered** or **Non-Registered**.



MYDLINK

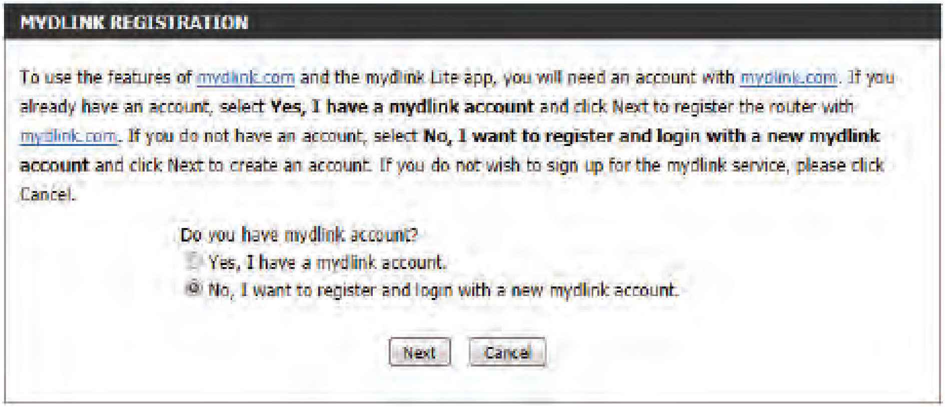
mydlink Service : Non-Registered

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.



REGISTER MYDLINK SERVICE

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



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.

__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.

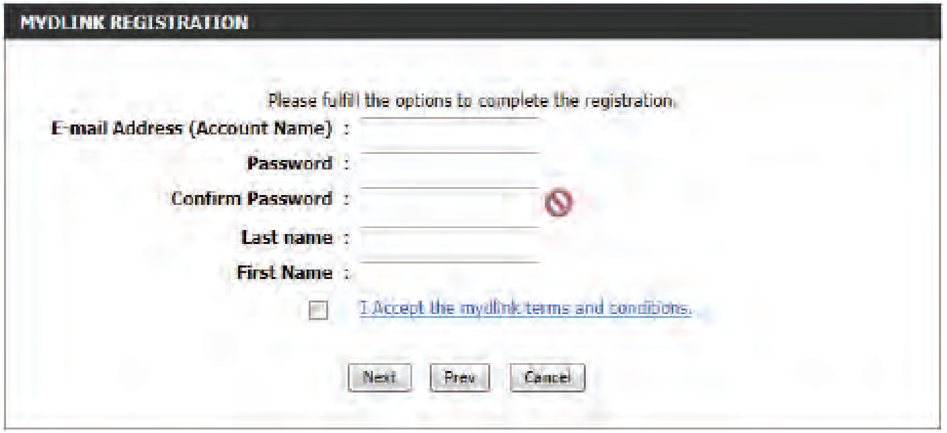
Password: Enter your preferred password choice here.

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.



MYDLINK REGISTRATION

Please fulfill the options to complete the registration.

E-mail Address (Account Name) :

Password :

Confirm Password :

Last name :

First Name :

□ I Accept the mydlink terms and conditions.

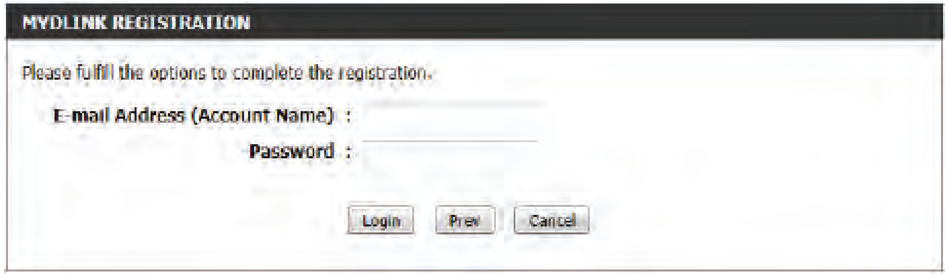
Next Prev Cancel

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.

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.



MYDLINK REGISTRATION

Please fulfill the options to complete the registration.

E-mail Address (Account Name) :

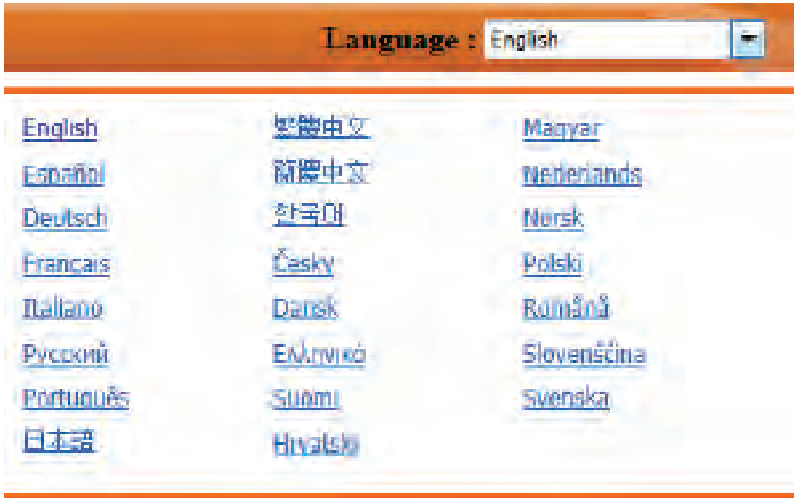
Password :

Login Prev Cancel

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.

At any point during this wizard, we can change the prefered language used. 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



Language : English

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.

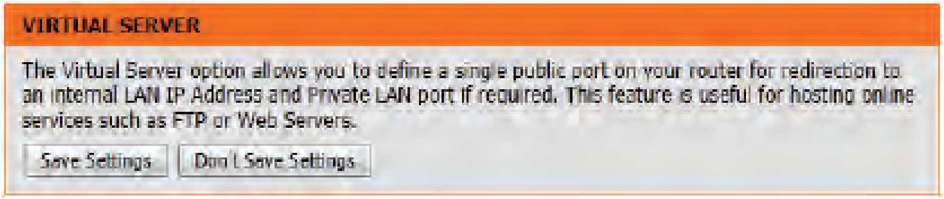
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the “Computer Name” drop-down menu. Select your computer and click **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

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

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

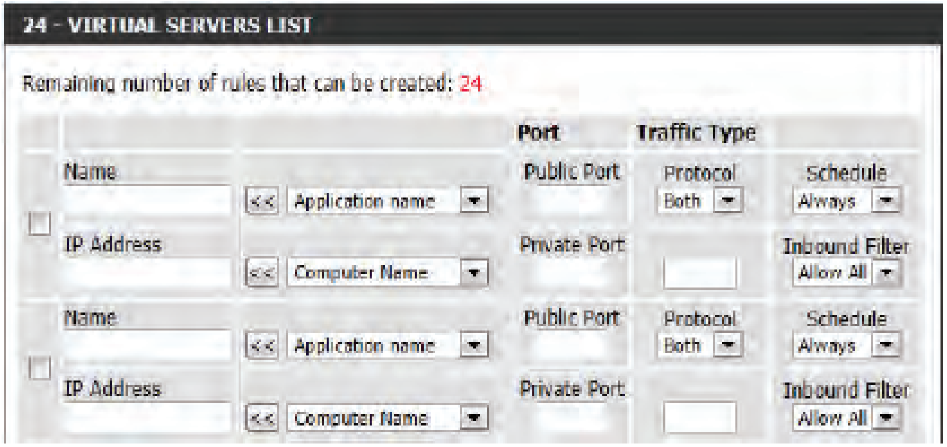
Schedule: The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools** > **Schedules** section.

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



VIRTUAL SERVER

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



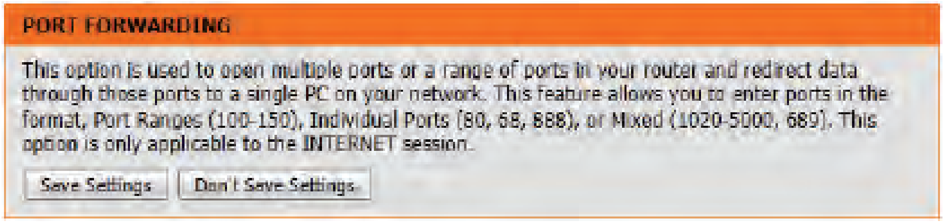
24 - VIRTUAL SERVERS LIST

Remaining number of rules that can be created: 24

			Port	Traffic Type	
	Name		Public Port	Protocol	Schedule
□		<< Application name ▾		Both ▾	Always ▾
	IP Address		Private Port		Inbound Filter
		<< Computer Name ▾			Allow All ▾
	Name		Public Port	Protocol	Schedule
□		<< Application name ▾		Both ▾	Always ▾
	IP Address		Private Port		Inbound Filter
		<< Computer Name ▾			Allow All ▾

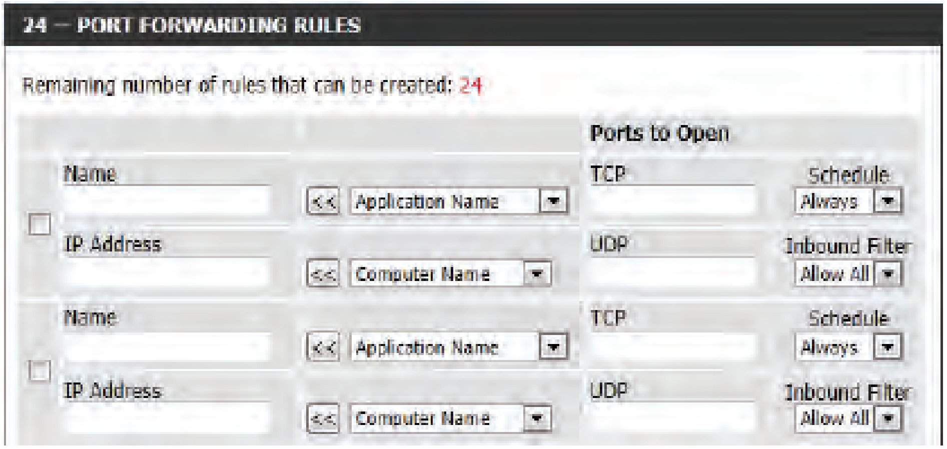
Port Forwarding

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



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 the format, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689). This option is only applicable to the INTERNET session.



24 — PORT FORWARDING RULES

Remaining number of rules that can be created: 24

			Ports to Open	
□	Name	<< Application Name ▾	TCP	Schedule Always ▾
	IP Address	<< Computer Name ▾	UDP	Inbound Filter Allow All ▾
□	Name	<< Application Name ▾	TCP	Schedule Always ▾
	IP Address	<< Computer Name ▾	UDP	Inbound Filter Allow All ▾

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

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

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

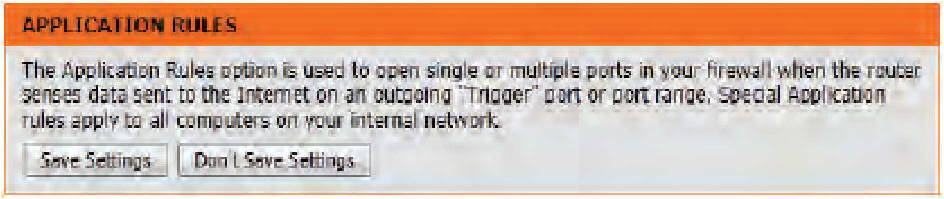
Schedule: The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools** > **Schedules** section.

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.

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-820L. 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-820L provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.



APPLICATION RULES

The Application Rules option is used to open single or multiple ports in your firewall when the router senses data sent to the Internet on an outgoing "Trigger" port or port range. Special Application rules apply to all computers on your internal network.

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

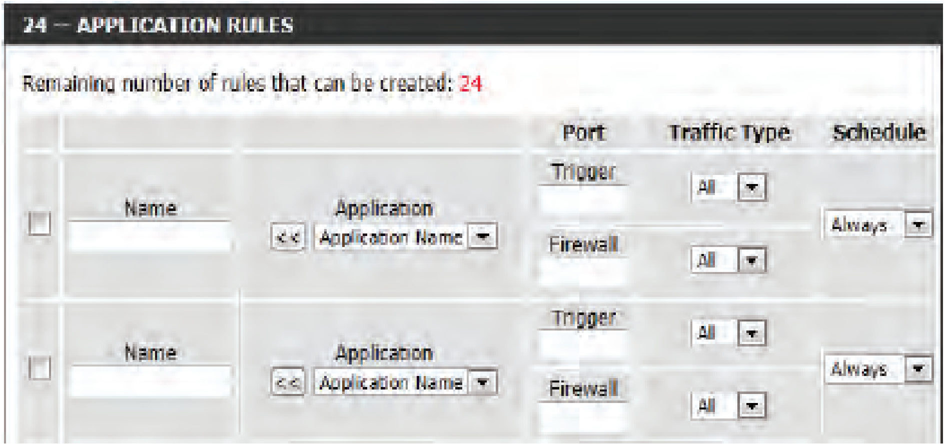
Trigger: This is the port used to trigger the application. It can be either a single port or a range of ports.

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.



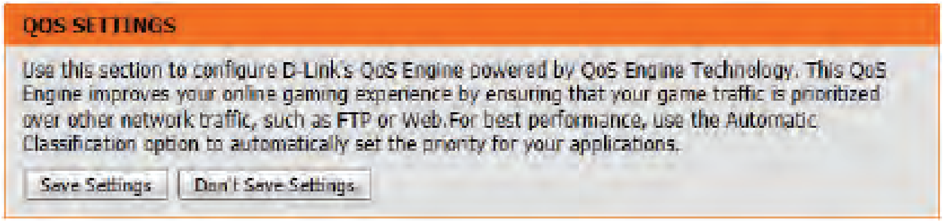
24 — APPLICATION RULES

Remaining number of rules that can be created: 24

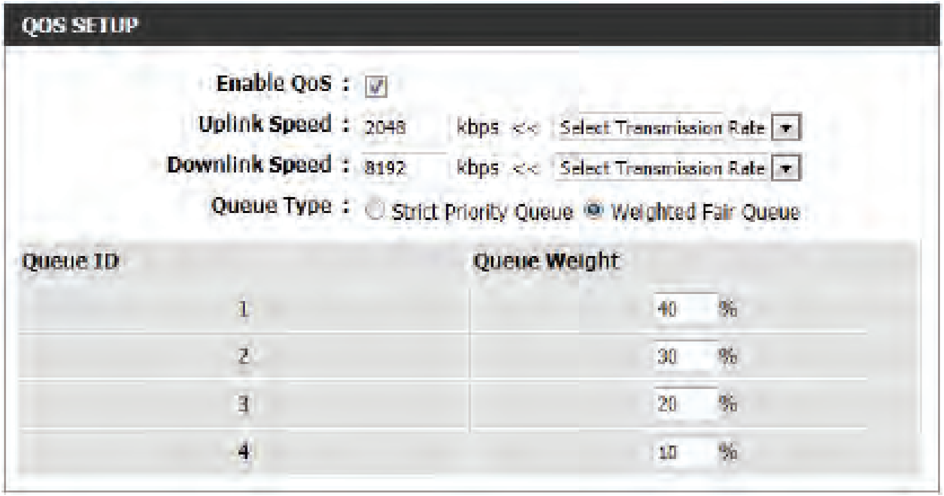
			Port	Traffic Type	Schedule
□	Name	Application << Application Name ▾	Trigger	All ▾	Always ▾
			Firewall	All ▾	
□	Name	Application << Application Name ▾	Trigger	All ▾	Always ▾
			Firewall	All ▾	

QoS Engine

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


QOS SETTINGS

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


QOS SETUP

Enable QoS : ☑

Uplink Speed : 2048 kbps << Select Transmission Rate

Downlink Speed : 8192 kbps << Select Transmission Rate

Queue Type : ○ Strict Priority Queue ● Weighted Fair Queue

Queue ID	Queue Weight
1	40 %
2	30 %
3	20 %
4	10 %

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, 1.5Mbits/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, 1.5Mbits/284Kbits.
Using this example, you would enter 1500. Alternatively you can test your downlink speed with a service such as www.dslreports.com.

Queue Type: Here the user can specify the queue type used. When choosing the option Strict Priority Queue, the router will apply QoS based on the internal specification for the queue ID's listed. When choosing the option Weight Fair Queue, the router will apply QoS based on the user defined percentage in the Queue Weight column.

Queue ID: In this column the Queue ID used will be displayed.

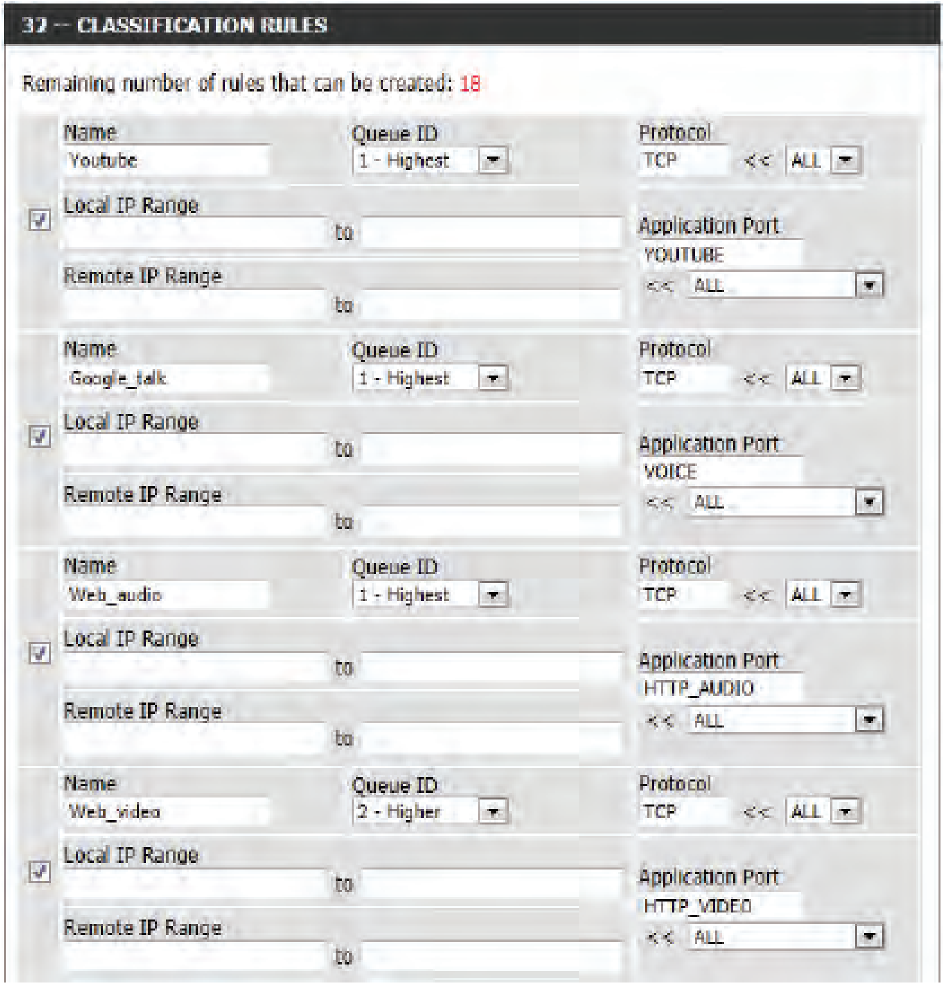
Queue Priority: In this column the Queue Priority used will be displayed.
Queue Weight: After choosing to use the Weight Fair Queue option, under Queue Type, the user will be able to manual enter the Queue Weight for each individual Queue ID.

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.



32 -- CLASSIFICATION RULES

Remaining number of rules that can be created: 18

☑ Name: Youtube — Queue ID: 1 - Highest — Protocol: TCP << ALL
Local IP Range: to — Application Port: YOUTUBE << ALL
Remote IP Range: to

☑ Name: Google_talk — Queue ID: 1 - Highest — Protocol: TCP << ALL
Local IP Range: to — Application Port: VOICE << ALL
Remote IP Range: to

☑ Name: Web_audio — Queue ID: 1 - Highest — Protocol: TCP << ALL
Local IP Range: to — Application Port: HTTP_AUDIO << ALL
Remote IP Range: to

☑ Name: Web_video — Queue ID: 2 - Higher — Protocol: TCP << ALL
Local IP Range: to — Application Port: HTTP_VIDEO << ALL
Remote IP Range: to

Network Filter

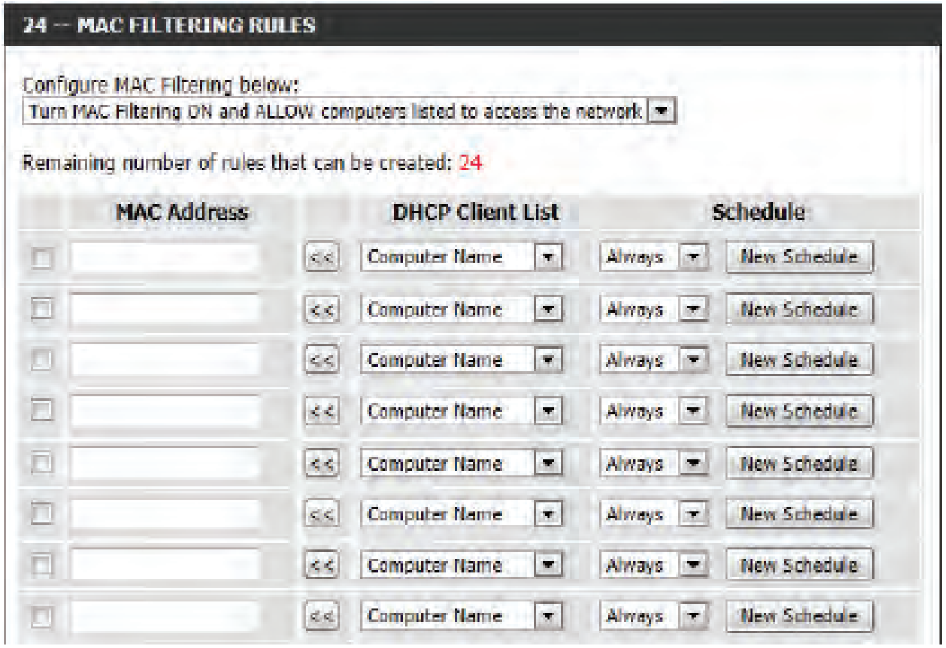
Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

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

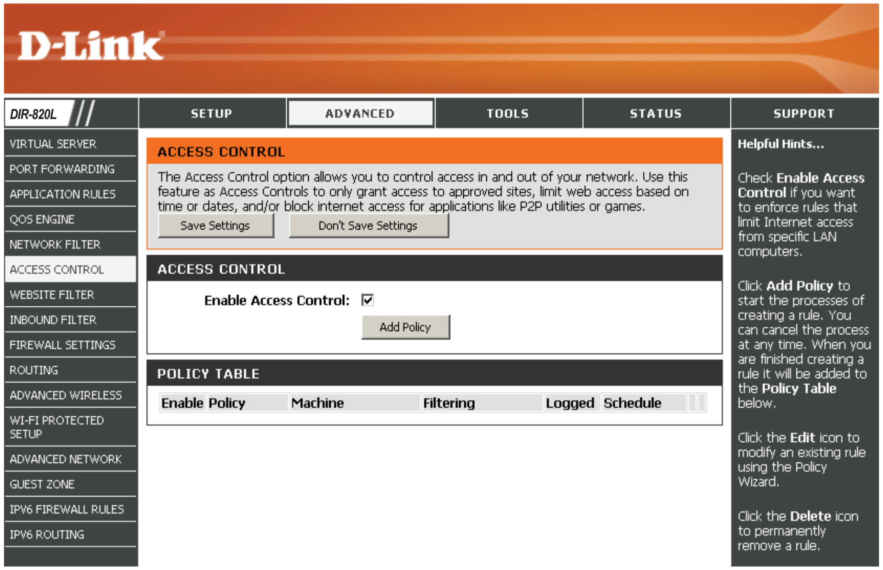
Remaining number of rules that can be created: 24

	MAC Address		DHCP Client List	Schedule	
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule

Access Control

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

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



ACCESS CONTROL

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.

ACCESS CONTROL

Enable Access Control: ☑

POLICY TABLE

Enable Policy	Machine	Filtering	Logged	Schedule

Helpful Hints...

Check **Enable Access Control** if you want to enforce rules that limit Internet access from specific LAN computers.

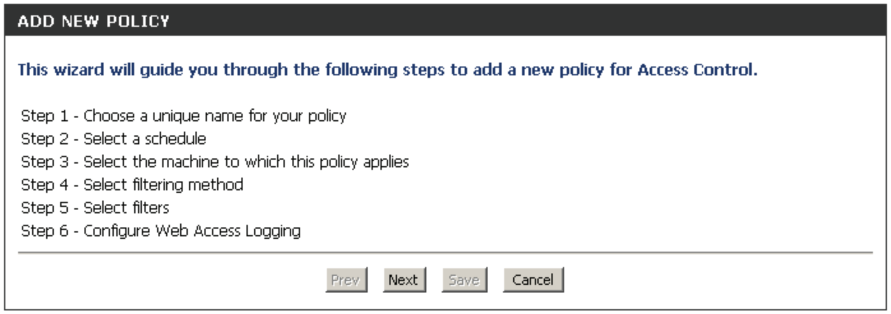
Click **Add Policy** to start the processes of creating a rule. You can cancel the process at any time. When you are finished creating a rule it will be added to the **Policy Table** below.

Click the **Edit** icon to modify an existing rule using the Policy Wizard.

Click the **Delete** icon to permanently remove a rule.

Access Control Wizard

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

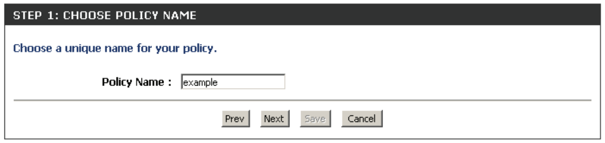


ADD NEW POLICY

This wizard will guide you through the following steps to add a new policy for Access Control.

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
Step 6 - Configure Web Access Logging

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

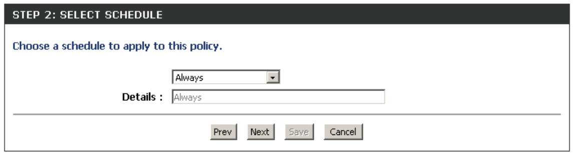


STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name : example

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



STEP 2: SELECT SCHEDULE

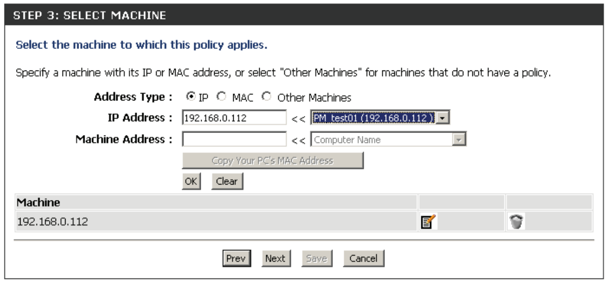
Choose a schedule to apply to this policy.

Always

Details : Always

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.

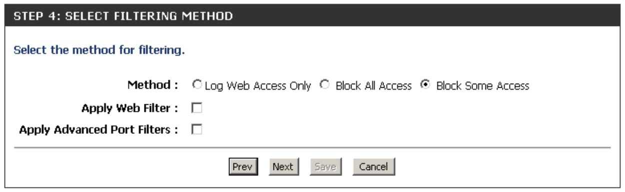
Address Type : ● IP ○ MAC ○ Other Machines

IP Address : 192.168.0.112 << PM_test01 (192.168.0.112)

Machine Address : << Computer Name

Machine		
192.168.0.112		

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



STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

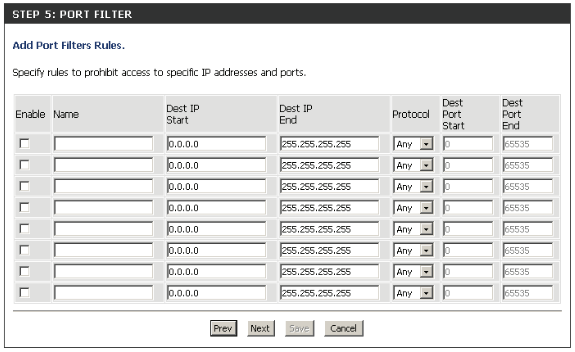
Method : ○ Log Web Access Only ○ Block All Access ● Block Some Access

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

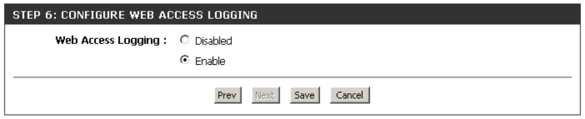
Add Port Filters Rules.

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
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535
☐		0.0.0.0	255.255.255.255	Any	0	65535

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

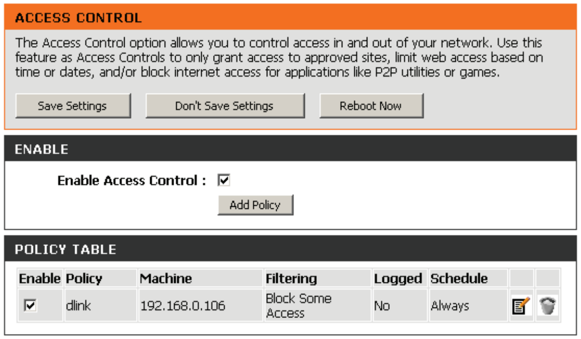
Click **Save** to save the access control rule.



STEP 6: CONFIGURE WEB ACCESS LOGGING

Web Access Logging : ○ Disabled ● Enable

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.

ENABLE

Enable Access Control : ☑

POLICY TABLE

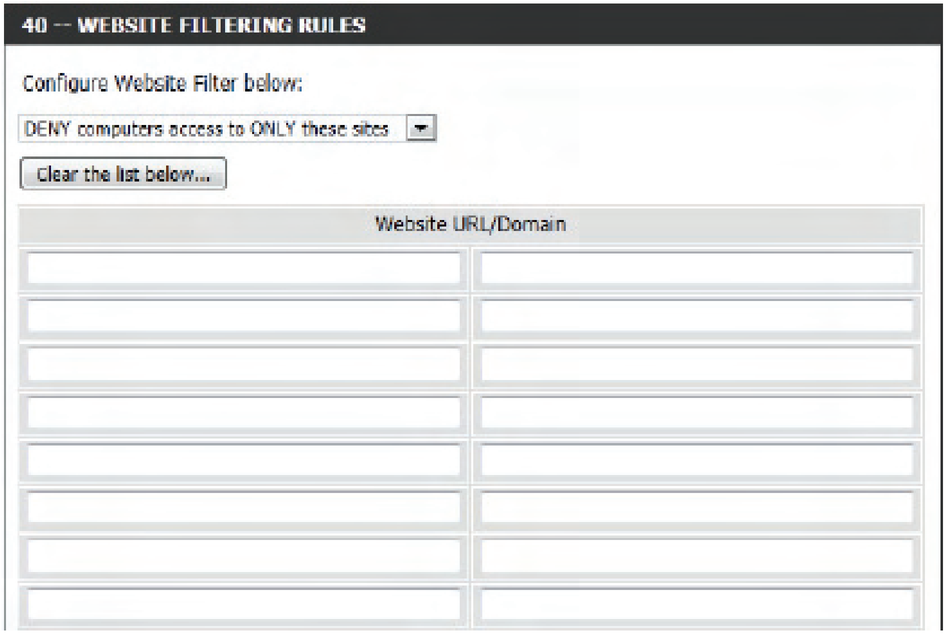
Enable	Policy	Machine	Filtering	Logged	Schedule		
☑	dlink	192.168.0.106	Block Some Access	No	Always	📝	🗑

Website Filters

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

Add Website Filtering Rule: Select either **DENY computers access to ONLY 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

Inbound Filters

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

Name: Enter a name for the inbound filter rule.

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

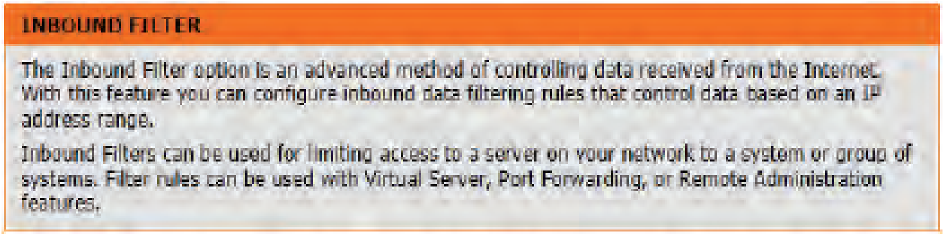
Enable: Check to enable rule.

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

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

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

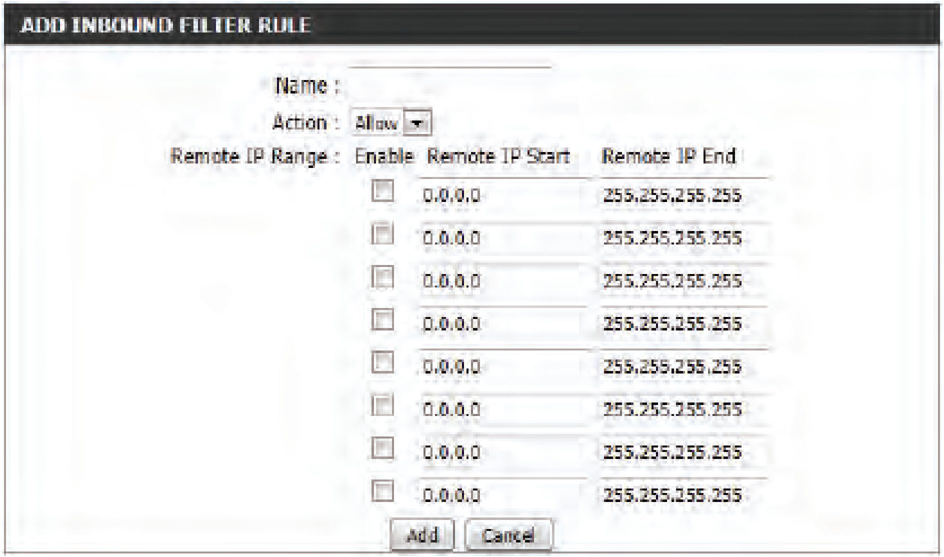
Inbound Filter Rules List: This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.



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.



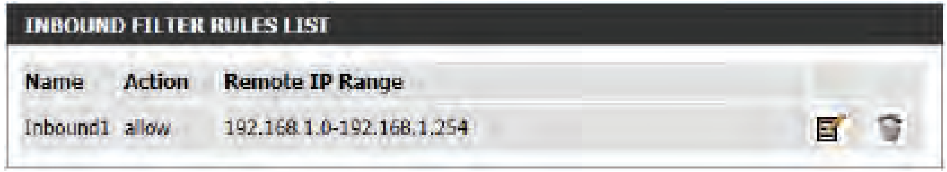
ADD INBOUND FILTER RULE

Name :

Action : Allow

Remote IP Range :

Enable	Remote IP Start	Remote IP End
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255



INBOUND FILTER RULES LIST

Name	Action	Remote IP Range
Inbound1	allow	192.168.1.0-192.168.1.254

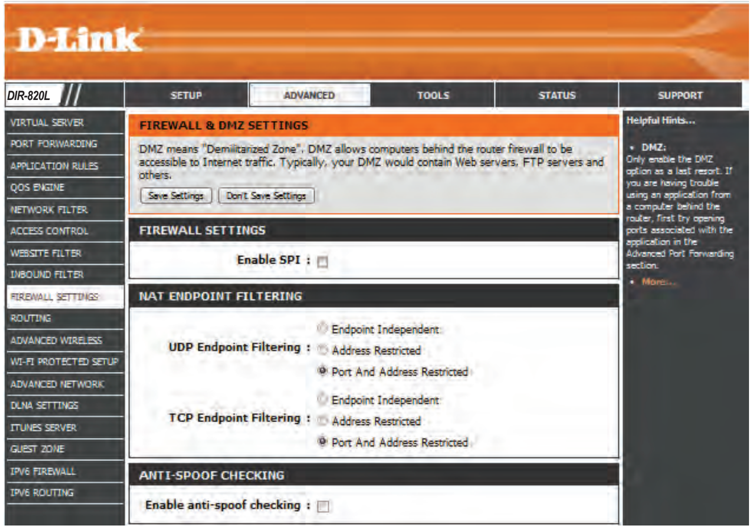
Firewall Settings

A firewall protects your network from the outside world. The DIR-820L offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

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

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 & DMZ SETTINGS

DMZ means "Demilitarized Zone". DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers and others.

FIREWALL SETTINGS

Enable SPI : □

NAT ENDPOINT FILTERING

UDP Endpoint Filtering : ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

TCP Endpoint Filtering : ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

ANTI-SPOOF CHECKING

Enable anti-spoof checking : □

Helpful Hints...

- DMZ: Only enable the DMZ option as a last resort. If you are having trouble using an application from a computer behind the router, first try opening ports associated with the application in the Advanced Port Forwarding section.

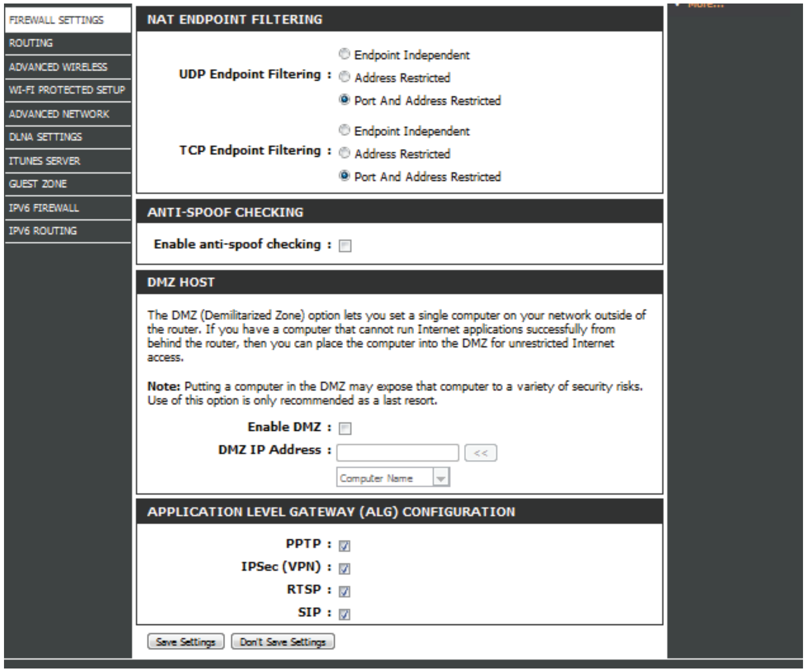
DMZ IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains it's IP address automatically using DHCP, be sure to make a static reservation on the **Setup** > **Network Settings** page so that the IP address of the 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.



NAT ENDPOINT FILTERING

UDP Endpoint Filtering : ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

TCP Endpoint Filtering : ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

ANTI-SPOOF CHECKING

Enable anti-spoof checking : □

DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

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 : << Computer Name

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP : ☑

IPSec (VPN) : ☑

RTSP : ☑

SIP : ☑