Version 1.1 | 10/30/2012

# User Manual

# Wireless N300 Cloud VPN Router

DIR-640L

# 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 |
|---|---|---|
| 1.1 | October 30, 2012 | • Initial release |

## Trademarks

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

# Table of Contents

**Preface** ........ **i**
Manual Revisions ........ i
Trademarks ........ i

**Product Overview** ........ **1**
Package Contents ........ 1
System Requirements ........ 2
Introduction ........ 3
Features ........ 4
Hardware Overview ........ 5
Back ........ 5
Front ........ 6

**Installation** ........ **7**
Before you Begin ........ 7
Wireless Installation Considerations ........ 8
Wall-Mount Kit Installation ........ 9
Hardware Setup ........ 10

**Configuration** ........ **12**
Web Setup Wizard ........ 12
Web-based Configuration Utility ........ 16
Internet Connection Setup ........ 17
Internet Connection Wizard ........ 17
Manual Internet Connection ........ 19
Static (assigned by ISP) ........ 20
Dynamic (Cable) ........ 21
PPPoE (DSL) ........ 22
PPTP ........ 23
L2TP ........ 24
Dial-Up ........ 25
3G ........ 26
Russian PPPoE ........ 27
Russian L2TP ........ 28
Russian PPTP ........ 29
Wireless Settings ........ 30
Wireless Setup Wizard ........ 31
WPS Connection Wizard ........ 33
Manual Wireless Settings ........ 35
Network Settings ........ 38
VPN Settings ........ 39
VPN Setup Wizard ........ 39
Dynamic IPSec VPN ........ 40
IPSec VPN ........ 41
PPTP VPN ........ 42
L2TP VPN ........ 43
VPN Manual Settings ........ 44
IPSec Settings ........ 45
PPTP/L2TP Settings ........ 47
GRE Settings ........ 48

**Advanced** ........ **49**
Virtual Server ........ 49
Application Rules ........ 50
QoS Engine ........ 51

Network Filter ........................................................................53
Web Filter...............................................................................54
Firewall Setting........................................................................55
Routing....................................................................................57
Advanced Network Settings.......................................................58
IPv6 ........................................................................................59
Static IPv6 ..............................................................................60
DHCP ......................................................................................61
PPPoE .....................................................................................62
IPv6 over IPv4 Tunneling..........................................................63
6 to 4 Tunneling........................................................................64
6rd .........................................................................................65
Link-Local Connectivity .............................................................66
IPv6 Firewall............................................................................67
User Group ..............................................................................68

**Maintenance ..........................................................................69**
Admin ......................................................................................69
SNMP.......................................................................................70
Time.........................................................................................71
SysLog.....................................................................................72
Email Settings ..........................................................................73
System ....................................................................................74
Firmware..................................................................................75
Dynamic DNS ...........................................................................76
System Check...........................................................................77
Schedule .................................................................................78

**Status.....................................................................................79**
Device Info ..............................................................................79
Log .........................................................................................80
Statistics .................................................................................81
Active Session ..........................................................................82
LAN Clients...............................................................................83
Routing....................................................................................84
VPN .........................................................................................85
IPv6 ........................................................................................86

**Support ..................................................................................87**

**Troubleshooting .....................................................................88**

**Wireless Basics .....................................................................92**
Tips.........................................................................................95
Wireless Modes.........................................................................96

**Networking Basics .................................................................97**
Check your IP address ...............................................................97
Statically Assign an IP address ...................................................98

**Technical Specifications .......................................................99**

**GPL Code Statement...............................................................100**

**Safety Statements ................................................................112**

# Package Contents

DIR-640L Wireless N300 Cloud VPN Router

Two Detachable Antennas

Ethernet Cable

Power Adapter

Optional Wall-Mount Kit

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-640L will cause damage and void the warranty for this product.*

# System Requirements

| | |
|---|---|
| **Network Requirements** | • An Ethernet-based Cable or DSL modem<br>• IEEE 802.11n or 802.11g wireless clients<br>• 10/100 Ethernet |
| **Web-based Configuration Utility Requirements** | **Computer with the following:**<br>• Windows®, Macintosh, or Linux-based operating system<br>• An installed Ethernet adapter<br><br>**Browser Requirements:**<br>• Internet Explorer 7 or higher<br>• Firefox 12 or higher<br>• Safari 4 or higher<br>• Chrome 20 or higher<br><br>**Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version. |

# Introduction

## ULTIMATE PERFORMANCE

The D-Link Wireless N300 Cloud VPN Router (DIR-640L) is a 802.11n compliant device that delivers real world performance of up to 14x faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the DIR-640L router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this Router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

## EXTENDED WIRELESS COVERAGE

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

## TOTAL NETWORK SECURITY

The Wireless N router supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA/WPA2 standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

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

# Features

- **Faster Wireless Networking** - The DIR-640L provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11n wireless router gives you the freedom of wireless networking at speeds 14x faster than 802.11g.

- **Compatible with 802.11b/g/n Devices** - The DIR-640L is still fully compatible with the IEEE 802.11b, 802.11g, and 802.11n standards, so it can connect with existing 802.11b, 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:

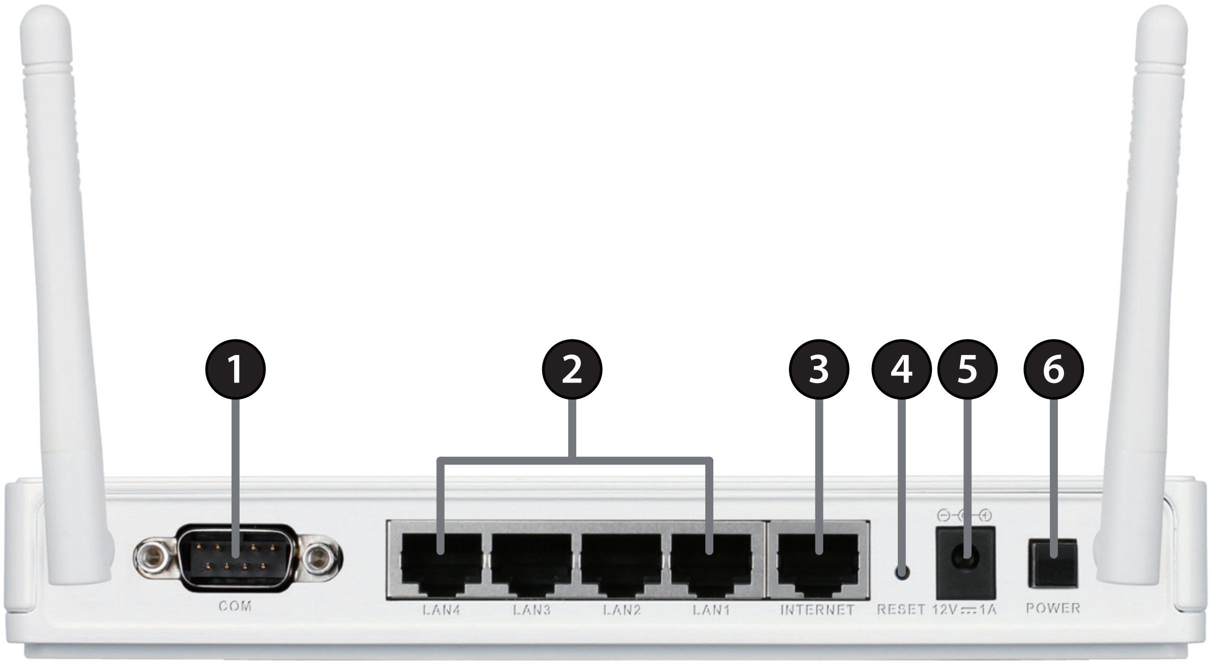
    - **Secure Multiple/Concurrent Sessions** - The DIR-640L can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-640L can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-640L lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

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

# Hardware Overview

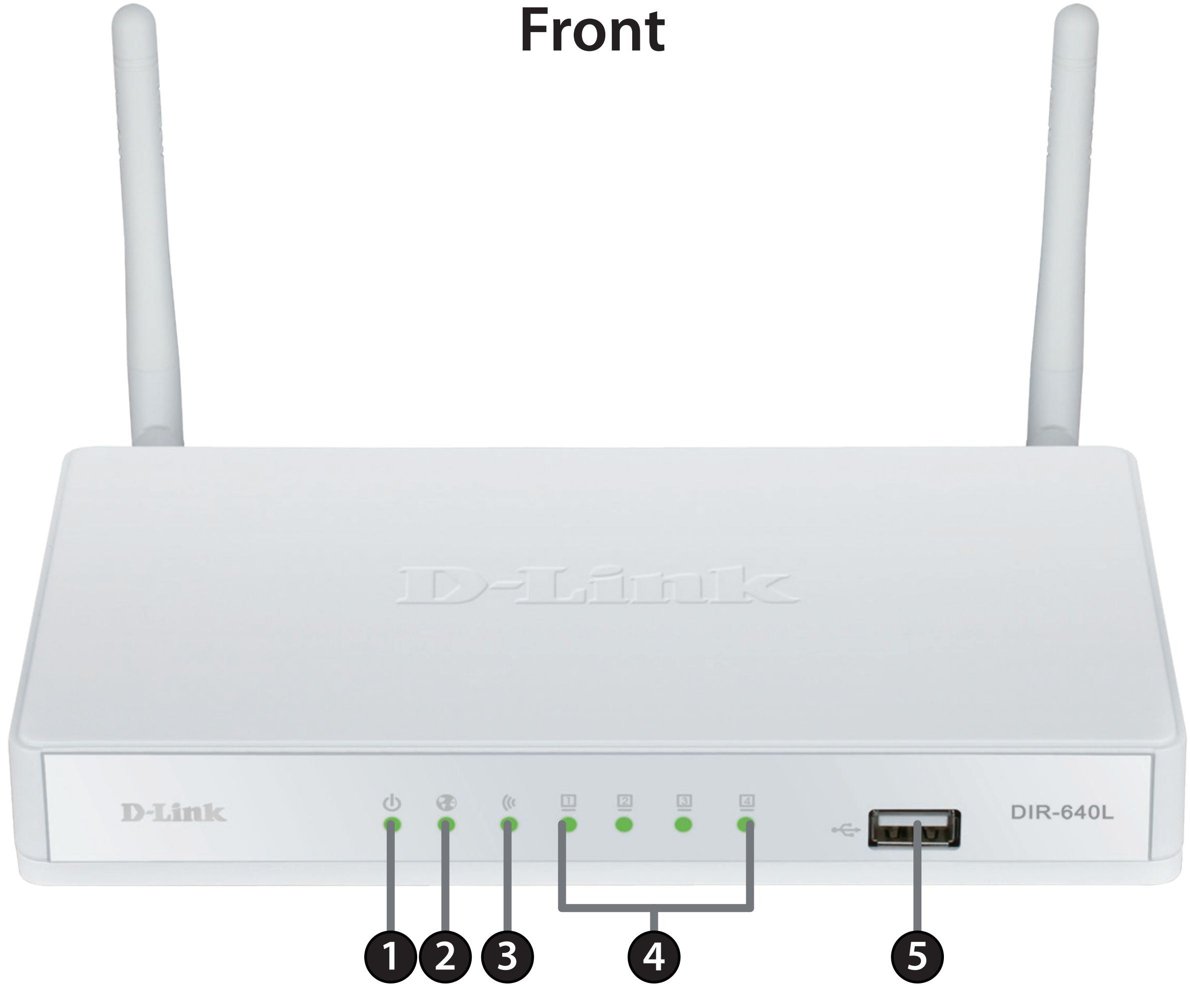
## Back



| | | |
|---|---|---|
| **1** | COM Port | RS-232 COM port for serial port communication and legacy device connectivity. |
| **2** | LAN Ports (1-4) | Connect 10/100 Ethernet devices such as computers, switches, and NAS. |
| **3** | Internet Port | The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem. |
| **4** | Reset Button | Pressing the Reset button restores the router to its original factory default settings. |
| **5** | Power Receptor | Receptor for the supplied power adapter. |
| **6** | Power Button | Turns the device On/Off. |

# Hardware Overview

## Front



| | | |
|---|---|---|
| **1** | Power LED | A solid light indicates a proper connection to the power supply. |
| **2** | Internet LED | A solid light indicates connection on the Internet port. This LED blinks during data transmission. |
| **3** | WLAN LED | A solid light indicates that the 2.4GHz wireless segment is ready. This LED blinks during wireless data transmission. |
| **4** | LAN LEDs (1-4) | A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission. |
| **5** | USB 2.0 port | Allows you to connect 3G modems. |

# 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.

# Wall-Mount Kit Installation

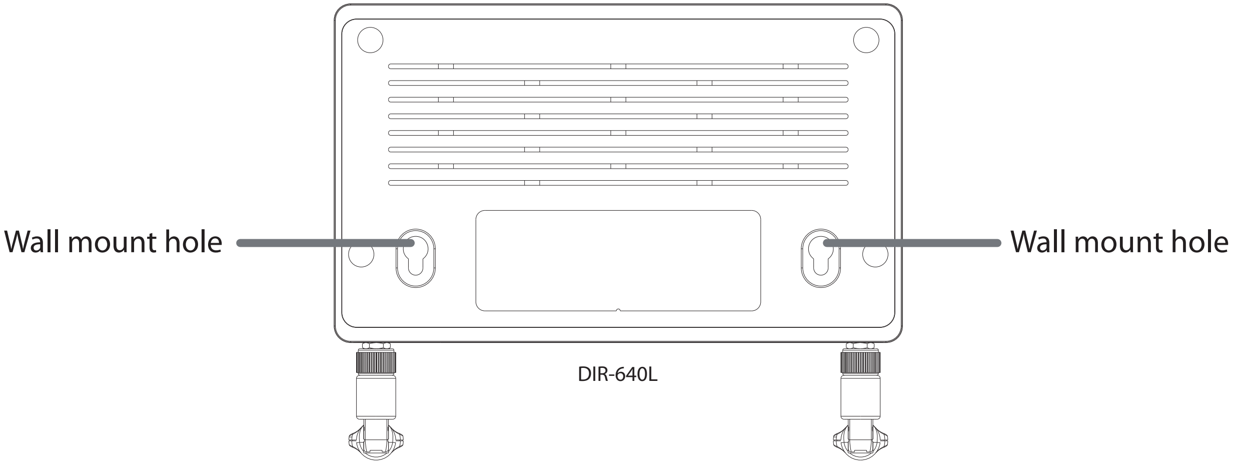
The wall-mount kit includes the following items:

- Two 2 cm screws
- Two screw anchors
- One attachment plate

Step 1. Align the attachment plate to your preferred position, and mark the hole positions on the wall, preferably after you locate one of the studs in the wall.

Step 2. Poke holes into the wall and insert the screw anchors where there is no stud. Check the screw anchors are securely in place.

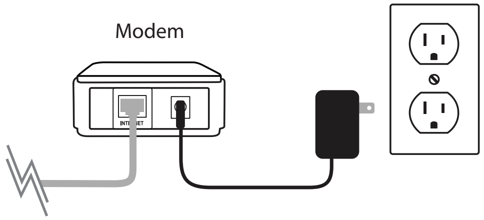
Step 3. Securely screw down the attachment plate on the wall.



Step 4. Hang the router on the wall by sliding the tops of the screws through the holes on the bottom of the router and then slide to lock into position. Confirm the the router is firmly in place.

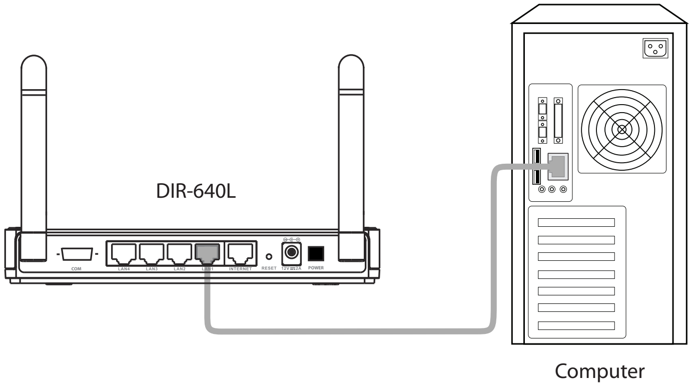
# Hardware Setup

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

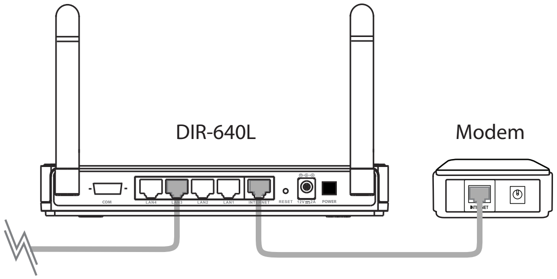


2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.

3. Unplug the Ethernet cable from your modem (or existing router if upgrading) that is connected to your computer. Plug it into the blue port labeled 1 on the back of your router. The router is now connected to your computer.

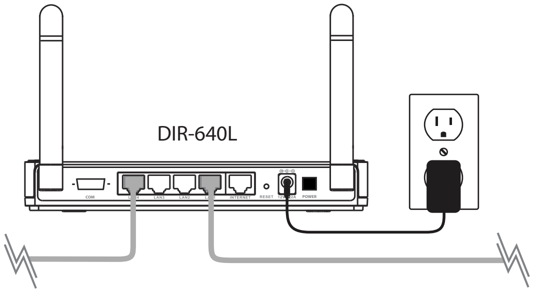


4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.



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.



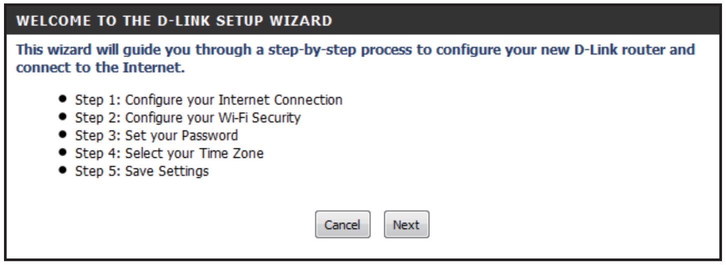
7. If you are connecting to a Broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser and enter a web site. If you connect, you are finished with your Internet setup. Please skip to page 13 to configure your router and use the manual setup procedure to configure your network and wireless settings. If you did not connect to the Internet, use the D-Link Setup Wizard (refer to page 15).

# Configuration

## Web Setup Wizard

Open your web browser and the setup wizard will automatically launch.

**Step 1:** The Welcome screen will appear. Click **Next** to continue.

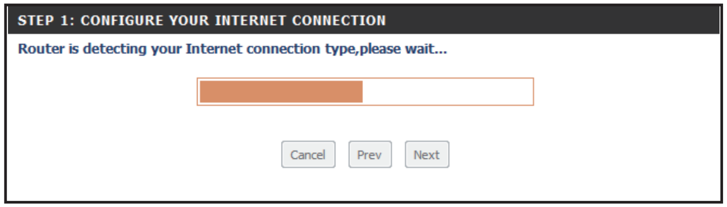


WELCOME TO THE D-LINK SETUP WIZARD

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: Save Settings

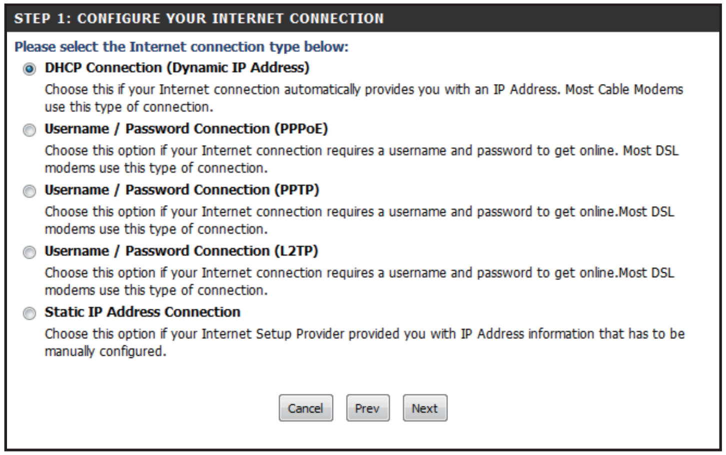
**Step 2:** The router will automatically detect your Internet connection type.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

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

**Step 3:** If the router could not automatically detect your connection type, select your connection type and click **Next** to continue.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

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)**

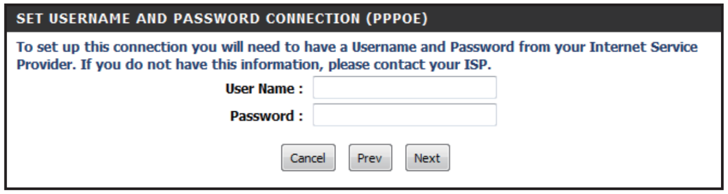
Choose this option if your Internet connection requires a username and password to get online.Most DSL modems use this type of connection.

○ **Static IP Address Connection**

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

If you selected PPPoE, enter your PPPoE username and password. 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.*



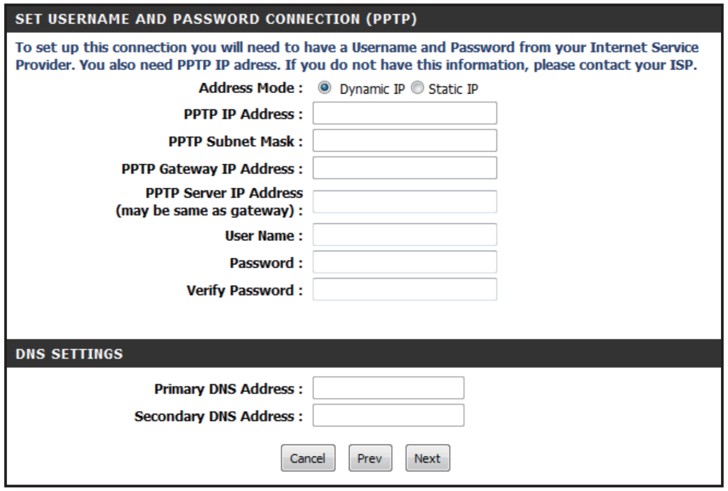
SET USERNAME AND PASSWORD CONNECTION (PPPOE)

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 you selected PPTP, enter your PPTP settings supplied by your ISP and your PPTP username and password. 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 :

PPTP Subnet Mask :

PPTP Gateway IP Address :

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

User Name :

Password :

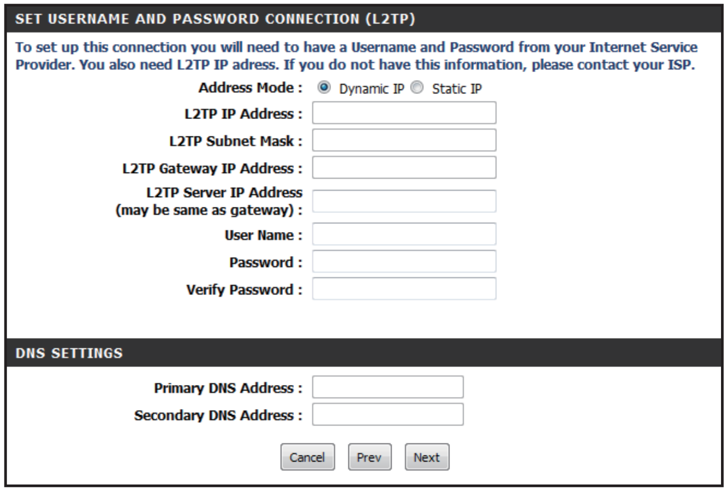
Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

If you selected L2TP, enter your L2TP settings supplied by your ISP and your L2TP username and password. 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 :

L2TP Subnet Mask :

L2TP Gateway IP Address :

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

User Name :

Password :

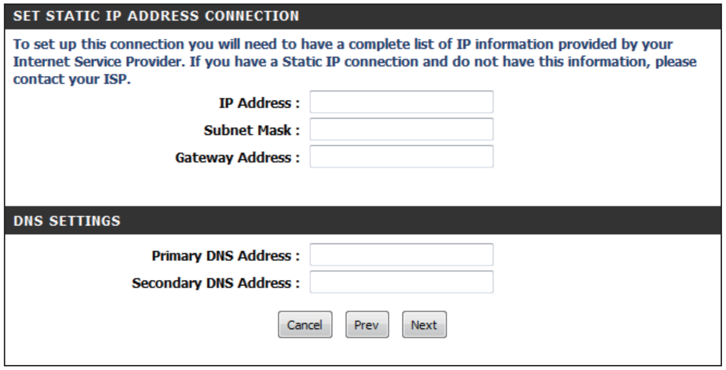
Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

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



SET STATIC IP ADDRESS CONNECTION

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

IP Address :

Subnet Mask :

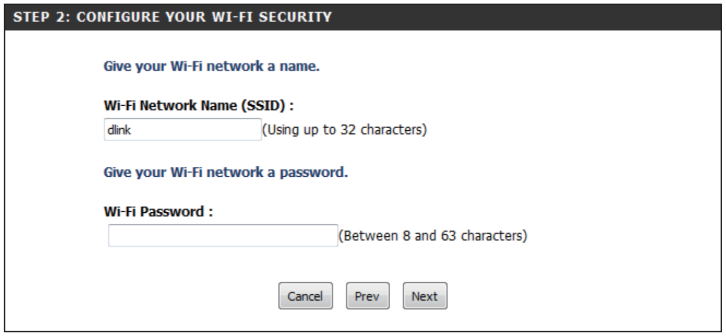
Gateway Address :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

**Step 4:** Create a name for your wireless network (SSID), create a password for your wireless network (Wi-Fi password), and then click **Next** to continue.



STEP 2: CONFIGURE YOUR WI-FI SECURITY

Give your Wi-Fi network a name.

Wi-Fi Network Name (SSID) :

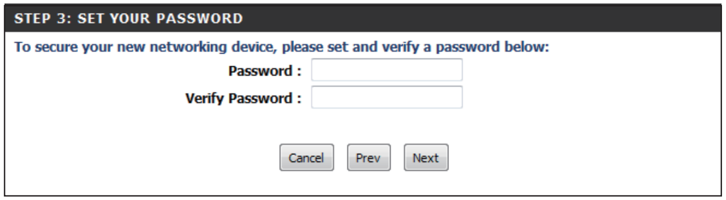
dlink (Using up to 32 characters)

Give your Wi-Fi network a password.

Wi-Fi Password :

(Between 8 and 63 characters)

**Step 5:** Create a new password and then click **Next** to continue.



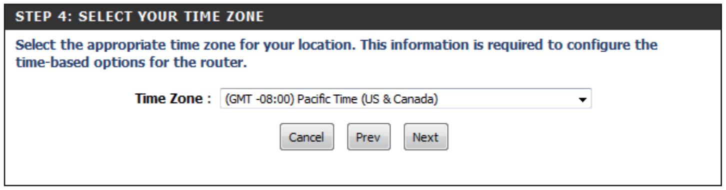
STEP 3: SET YOUR PASSWORD

To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

**Step 6:** Select your time zone from the drop-down menu and then click **Next** to continue.

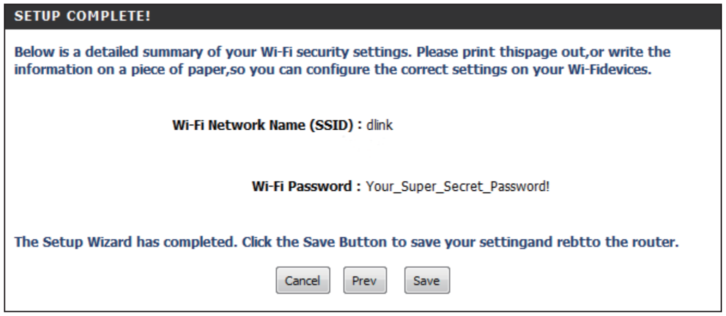


STEP 4: SELECT YOUR TIME ZONE

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

Time Zone : (GMT -08:00) Pacific Time (US & Canada)

**Step 7:** Your setup is complete. Click **Save** to continue.



SETUP COMPLETE!

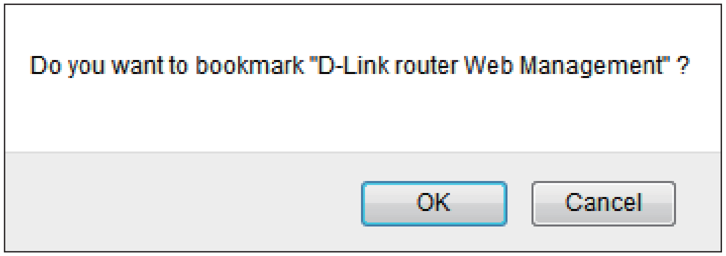
Below is a detailed summary of your Wi-Fi security settings. Please print thispage out,or write the information on a piece of paper,so you can configure the correct settings on your Wi-Fidevices.

Wi-Fi Network Name (SSID) : dlink

Wi-Fi Password : Your_Super_Secret_Password!

The Setup Wizard has completed. Click the Save Button to save your settingand rebtto the router.

**Step 8:** You may bookmark the router's web UI by clicking **OK**. If you do not want to bookmark the link, click **Cancel**.



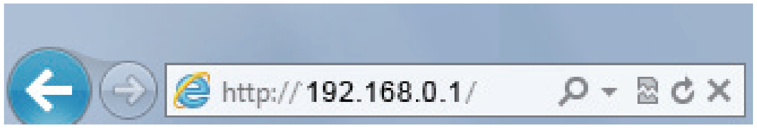
Do you want to bookmark "D-Link router Web Management" ?

The router will reboot. Please allow 1-2 minutes.

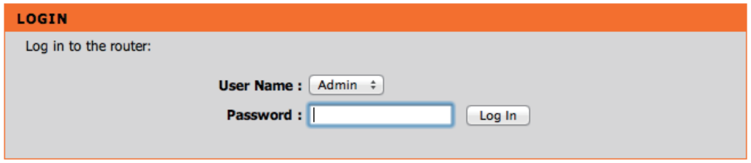
Close your browser window and reopen it to test your Internet connection. It may take a few tries to initially connect to the Internet.

# Web-based Configuration Utility

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


http://192.168.0.1/

Select **Admin** from the drop-down menu and the password **should be left empty**.


LOGIN

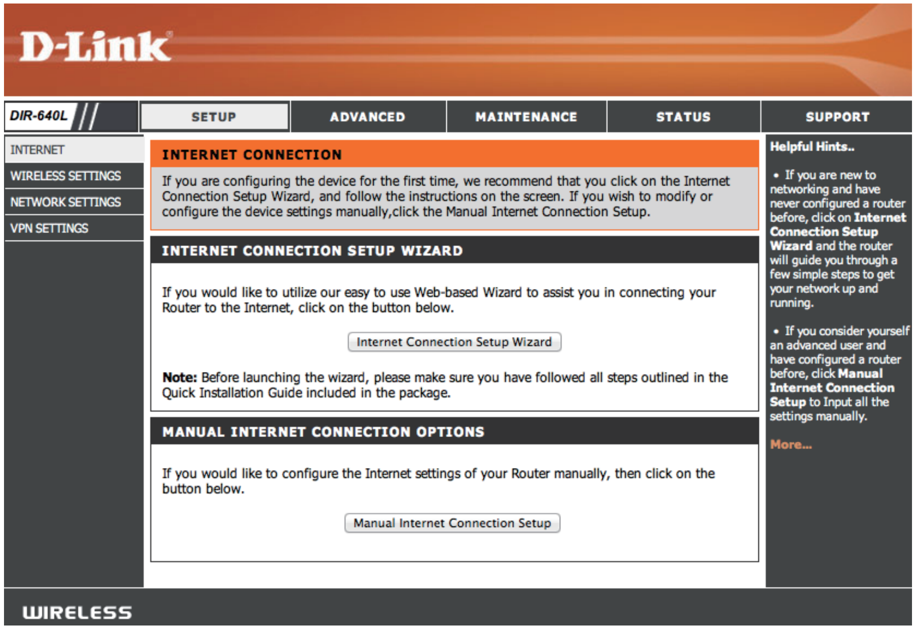
Log in to the router:

User Name : Admin

Password :

# Internet Connection Setup

Use this tab to choose if you want to follow the simple steps of the Connection Setup Wizard, or if you want to set up your Internet connection manually.



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 utilize our easy to use Web-based Wizard to assist you in connecting your 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 OPTIONS

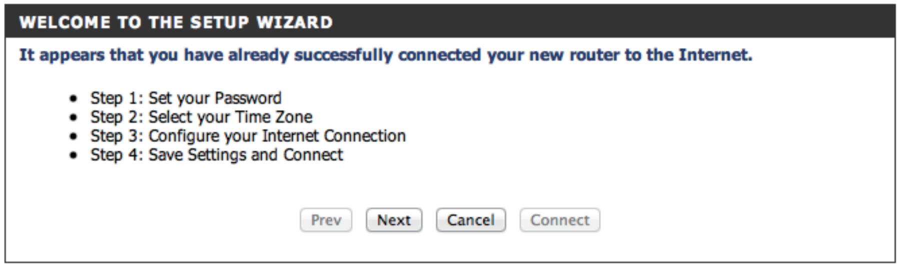
If you would like to configure the Internet settings of your Router manually, then click on the button below.

**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 Wizard

Click **Next** to begin the Setup Wizard.

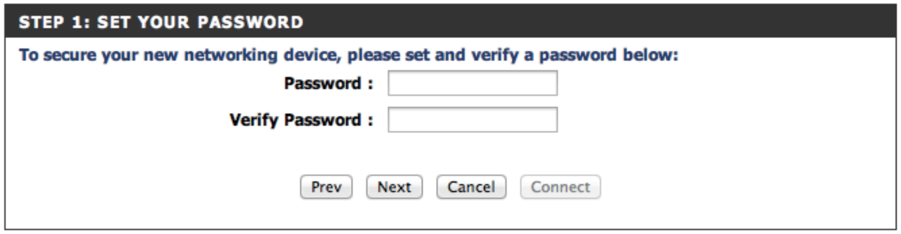


WELCOME TO THE SETUP WIZARD

It appears that you have already successfully connected your new router 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:** Choose a password for your device.



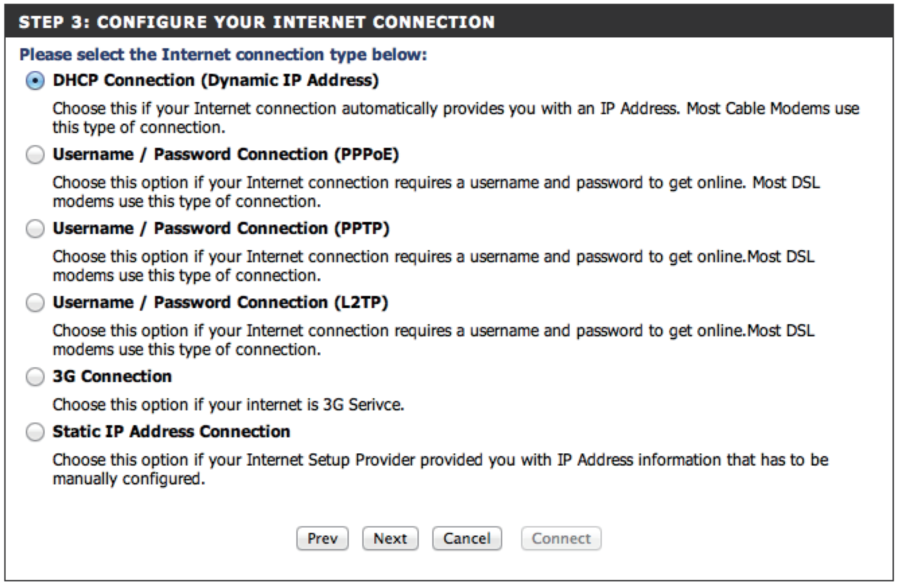
STEP 1: SET YOUR PASSWORD

To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

**STEP 2:** Choose the method you use to connect to the Internet, and follow the step-by-step instructions.



STEP 3: CONFIGURE YOUR INTERNET CONNECTION

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.

○ **3G Connection**

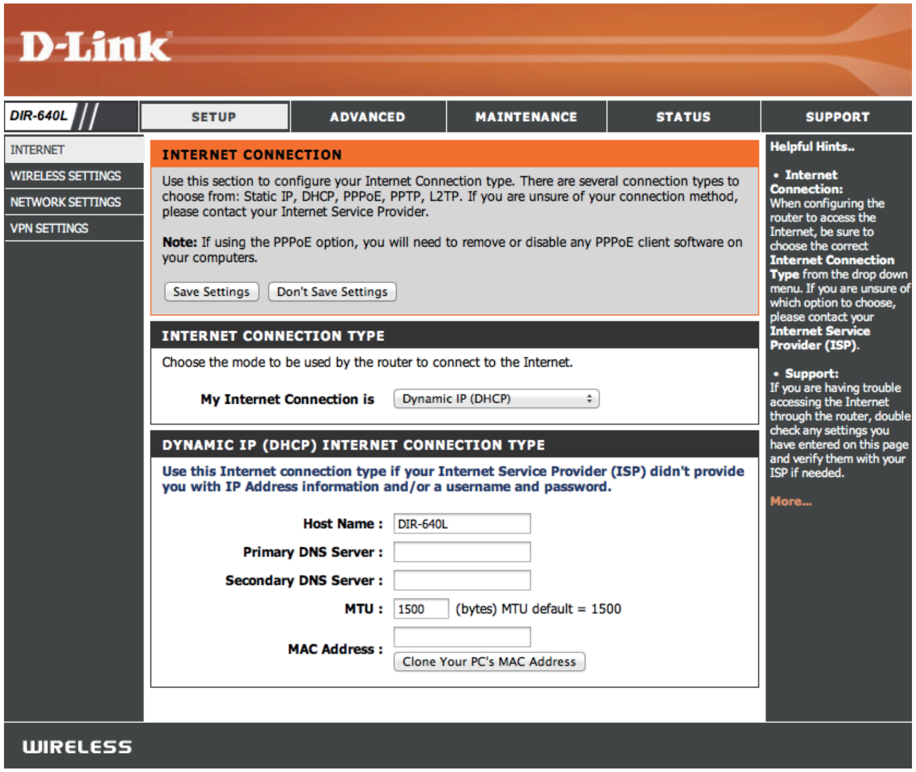
Choose this option if your internet is 3G Serivce.

○ **Static IP Address Connection**

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

# Manual Internet Connection

Use this tab to choose either Static IP, DHCP, PPPoE, PPTP, L2TP, Dial-Up, 3G, Russian PPPoE, Russian PPTP, or Russian L2TP to configure your Internet connection. You may need to get this information from your ISP (Internet Service Provider).



**INTERNET CONNECTION**

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP. 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**

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

**My Internet Connection is** Dynamic IP (DHCP)

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

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

**Host Name :** DIR-640L

**Primary DNS Server :**

**Secondary DNS Server :**

**MTU :** 1500 (bytes) MTU default = 1500

**MAC Address :**

**Helpful Hints..**

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

# Static (assigned by ISP)

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

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

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

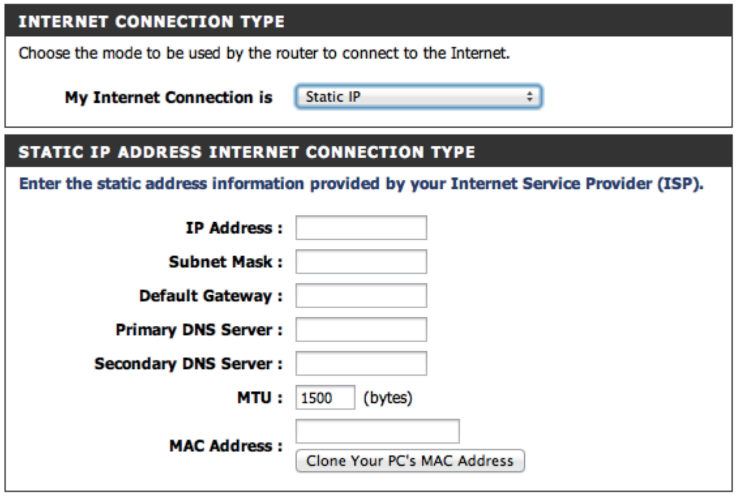
**Subnet Mask:** Enter the Subnet Mask assigned by your ISP.

**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 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 :

Subnet Mask :

Default Gateway :

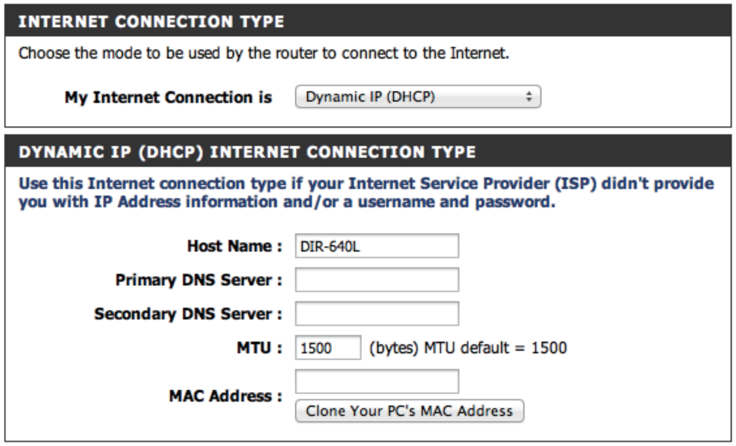
Primary DNS Server :

Secondary DNS Server :

MTU : 1500 (bytes)

MAC Address :

# Dynamic (Cable)



INTERNET CONNECTION TYPE

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

My Internet Connection is: Dynamic IP (DHCP)

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE

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

Host Name : DIR-640L

Primary DNS Server :

Secondary DNS Server :

MTU : 1500 (bytes) MTU default = 1500

MAC Address :

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

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

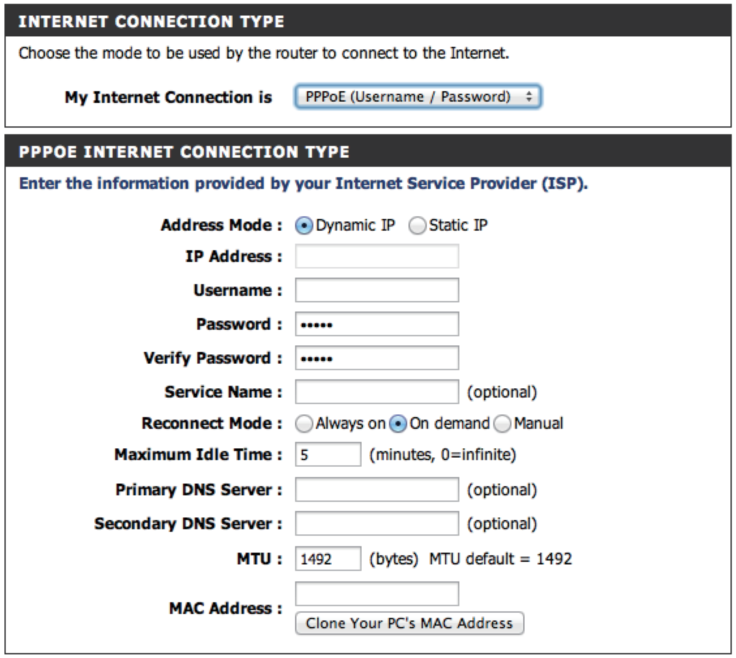
**Primary/Secondary DNS Server:** Enter the Primary and secondary DNS server IP addresses assigned by your ISP. These addresses are usually obtained automatically from your ISP. Leave at 0.0.0.0 if you did not specifically receive these from your ISP.

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

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

# 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.



**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 on ● On demand ○ Manual

Maximum Idle Time : 5 (minutes, 0=infinite)

Primary DNS Server : (optional)

Secondary DNS Server : (optional)

MTU : 1492 (bytes) MTU default = 1492

MAC Address :

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

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

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

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

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

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

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

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

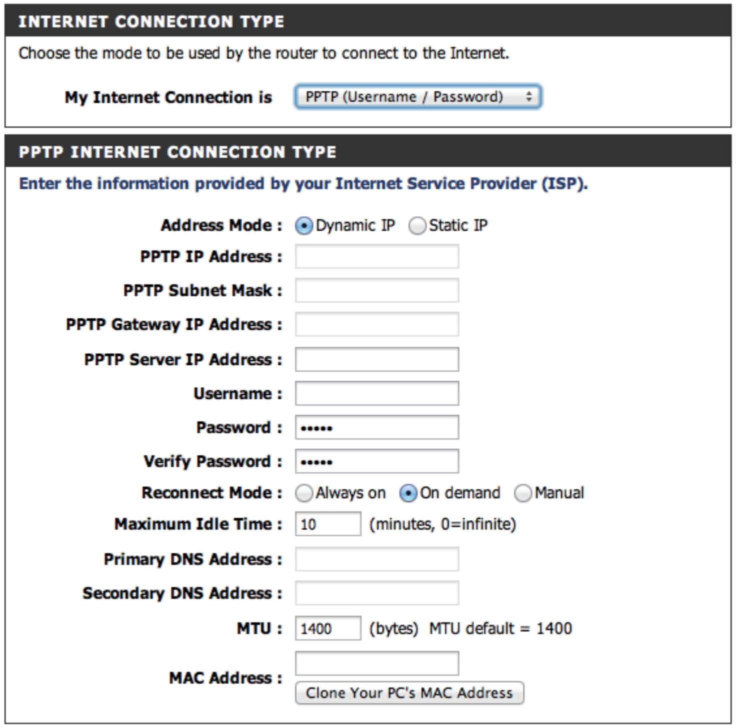
**DNS Addresses:** Enter the Primary and Secondary DNS Server Addresses (Static PPPoE only).

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

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

# PPTP

Choose PPTP if your ISP uses a PPTP connection. Your ISP will provide you with a username and password.



**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 ● On demand ○ Manual |
| **Maximum Idle Time :** | 10 (minutes, 0=infinite) |
| **Primary DNS Address :** | |
| **Secondary DNS Address :** | |
| **MTU :** | 1400 (bytes) MTU default = 1400 |
| **MAC Address :** | <br>Clone Your PC's MAC Address |

**My Internet Connection Is:** Select **PPTP** from the drop-down menu.

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

**PPTP IP Address:** Enter the IP address for your PPTP connection.

**PPTP Subnet Mask:** Enter your PPTP subnet mask.

**PPTP Gateway IP Address:** Enter the Gateway IP address for your PPTP connection.

**PPTP Server IP Address:** Enter the Server IP address for your PPTP connection.

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

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

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

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

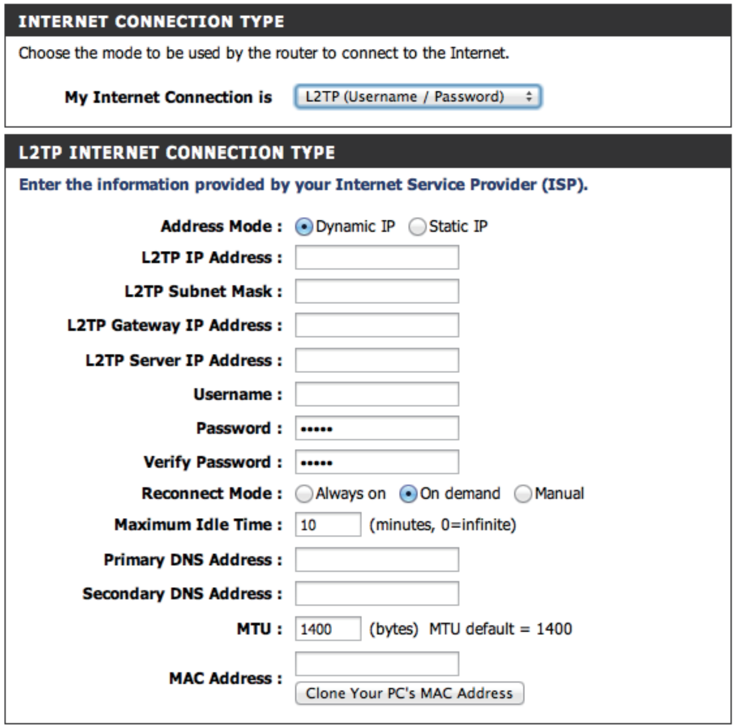
**DNS Addresses:** Enter the Primary and Secondary DNS Server Addresses (Static PPTP only).

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

**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

# L2TP

Choose L2TP if your ISP uses a L2TP connection. Your ISP will provide you with a username and password.



**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 on ● On demand ○ Manual |
| Maximum Idle Time : | 10 (minutes, 0=infinite) |
| Primary DNS Address : | |
| Secondary DNS Address : | |
| MTU : | 1400 (bytes) MTU default = 1400 |
| MAC Address : | Clone Your PC's MAC Address |

**My Internet Connection Is:** Select **L2TP** from the drop-down menu.

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

**PPTP IP Address:** Enter the IP address for your L2TP connection.

**PPTP Subnet Mask:** Enter your L2TP subnet mask.

**PPTP Gateway IP Address:** Enter the Gateway IP address for your L2TP connection.

**PPTP Server IP Address:** Enter the Server IP address for your L2TP connection.

**User Name:** Enter your L2TP user name.

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

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

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

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

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

**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

# Dial-Up

Choose Dial-Up if you use a dial-up connection with your ISP to connect to the Internet.

**My Internet Connection Is:** Select **Dial-up Network** from the drop-down menu.

**Dial-up Telephone:** Enter the telephone number you use to reach your dial-up provider.

**Dial-up Account:** Enter the account name for your dial-up service.

**Dial-up Password:** Enter your password and then retype the password in the next box.

**Maximum Idle Time:** Choose the amount of minutes of inactivity before the connection is dropped. Choose '0" if you want to never drop the connection.

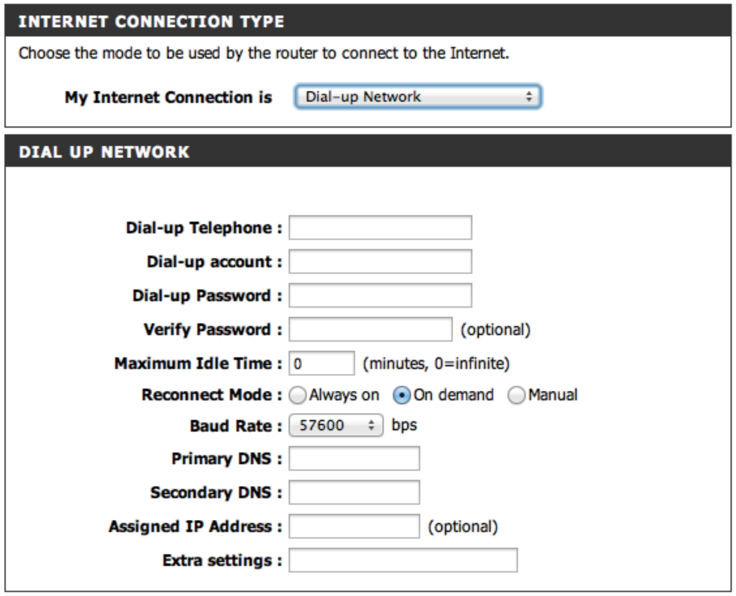
**Reconnect Mode:** Select either **Always-on**, **On-Demand**, or **Manual**.

**Baud Rate:** Choose the speed of your modem connection from the drop-down menu.

**DNS Addresses:** Enter the Primary and Secondary DNS Server Addresses.

**Assigned IP Address:** If your ISP gave you a static IP address for your connections, enter it here.

**Extra Settings:** Add any additional settings provided by your ISP here.



**INTERNET CONNECTION TYPE**

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

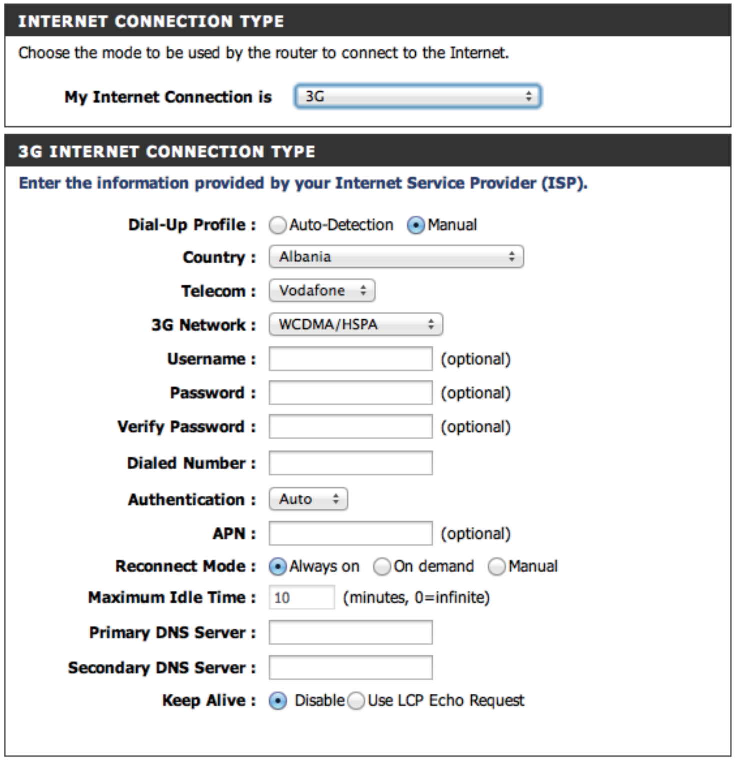
| | |
|---|---|
| My Internet Connection is | Dial-up Network |

**DIAL UP NETWORK**

| | |
|---|---|
| Dial-up Telephone : | |
| Dial-up account : | |
| Dial-up Password : | |
| Verify Password : | (optional) |
| Maximum Idle Time : | 0 (minutes, 0=infinite) |
| Reconnect Mode : | ○ Always on ● On demand ○ Manual |
| Baud Rate : | 57600 bps |
| Primary DNS : | |
| Secondary DNS : | |
| Assigned IP Address : | (optional) |
| Extra settings : | |

# 3G

Choose 3G if you are connection from a mobile wireless network with an ISP that uses a 3G connection.



**INTERNET CONNECTION TYPE**

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

My Internet Connection is: 3G

**3G INTERNET CONNECTION TYPE**

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

| | |
|---|---|
| Dial-Up Profile : | ○ Auto-Detection ● Manual |
| Country : | Albania |
| Telecom : | Vodafone |
| 3G Network : | WCDMA/HSPA |
| Username : | (optional) |
| Password : | (optional) |
| Verify Password : | (optional) |
| Dialed Number : | |
| Authentication : | Auto |
| APN : | (optional) |
| Reconnect Mode : | ● Always on ○ On demand ○ Manual |
| Maximum Idle Time : | 10 (minutes, 0=infinite) |
| Primary DNS Server : | |
| Secondary DNS Server : | |
| Keep Alive : | ● Disable ○ Use LCP Echo Request |

**My Internet Connection Is:** Select **3G** from the drop-down menu.

**Dial-Up Profile:** In most cases you can choose **Auto-Detection** to get a connection. Otherwise choose **Manual** and personalize the settings below.

**Country:** Choose the country where you get 3G service from the drop-down menu.

**Telecom** Choose the telecom that provides your service from the drop-down menu.

**3G Network:** Choose the type of 3G network you have from the drop-down menu.

**User Name:** Enter your 3G network user name, this is not always required by your ISP.

**Password:** Enter your 3G network password and then retype the password in the next box. This is also not always required by your ISP.

**Dialed Number:** Enter the number your ISP gave you to dial for a connection.

**Authentication:** Choose the type of authentification need to connect or use auto detection.

**APN:** If your ISP has given you an Access Point Name to use for your connectivity, you may enter it here.

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

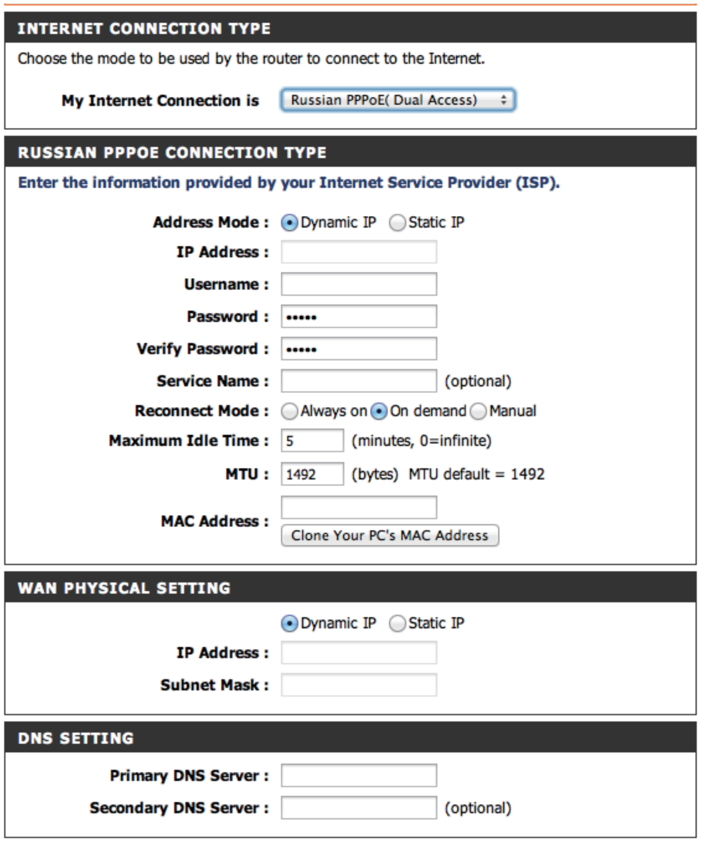
**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

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

**Keep Alive:** To keep prevent inactivity from assuming a dropped connection you can Use LCP Echo Request to request frequent pings to maintain communication. This is disabled by default.

# Russian PPPoE

Choose Russian PPPoE (Dual Access) if your ISP uses a PPPoE connection in Russia with WAN physical access.



**INTERNET CONNECTION TYPE**

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

My Internet Connection is: Russian PPPoE( Dual Access)

**RUSSIAN PPPOE CONNECTION TYPE**

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

Address Mode : ● Dynamic IP ○ Static IP
IP Address :
Username :
Password : •••••
Verify Password : •••••
Service Name : (optional)
Reconnect Mode : ○ Always on ● On demand ○ Manual
Maximum Idle Time : 5 (minutes, 0=infinite)
MTU : 1492 (bytes) MTU default = 1492
MAC Address :
Clone Your PC's MAC Address

**WAN PHYSICAL SETTING**

● Dynamic IP ○ Static IP
IP Address :
Subnet Mask :

**DNS SETTING**

Primary DNS Server :
Secondary DNS Server : (optional)

**My Internet Connection Is:** Select **Russian PPPoE (Dual Access)** from the drop-down menu.

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

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

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

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

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

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

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

**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.

**WAN Physical Setting:** Select a **Dynamic IP** or **Static IP** if your WAN physical setting.

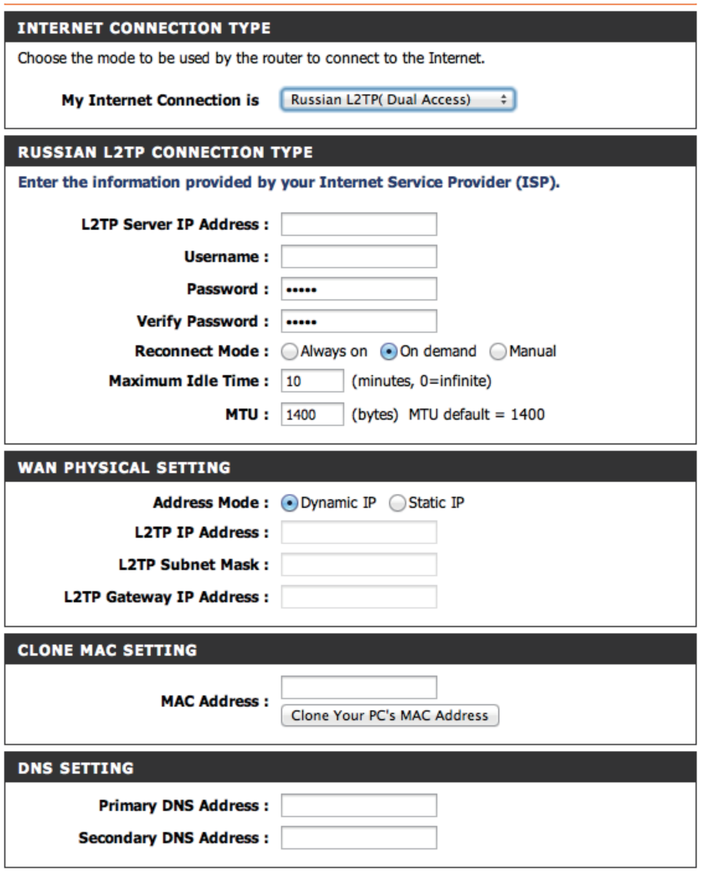
**IP Address** Enter the IP address for your PPTP connection.

**Subnet Mask:** Enter your PPTP subnet mask.

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

# Russian L2TP

Choose Russian L2TP (Dual Access) if your ISP uses an L2TP connection in Russia with WAN physical access.



**INTERNET CONNECTION TYPE**

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

My Internet Connection is: Russian L2TP( Dual Access)

**RUSSIAN L2TP CONNECTION TYPE**

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

| | |
|---|---|
| L2TP Server IP Address : | |
| Username : | |
| Password : | ••••• |
| Verify Password : | ••••• |
| Reconnect Mode : | ○ Always on ● On demand ○ Manual |
| Maximum Idle Time : | 10 (minutes, 0=infinite) |
| MTU : | 1400 (bytes) MTU default = 1400 |

**WAN PHYSICAL SETTING**

| | |
|---|---|
| Address Mode : | ● Dynamic IP ○ Static IP |
| L2TP IP Address : | |
| L2TP Subnet Mask : | |
| L2TP Gateway IP Address : | |

**CLONE MAC SETTING**

| | |
|---|---|
| MAC Address : | |

**DNS SETTING**

| | |
|---|---|
| Primary DNS Address : | |
| Secondary DNS Address : | |

**My Internet Connection:** Select **Russian L2TP (Dual Access)** from the drop-down menu.

**LT2P Server IP Address:** Enter the IP address provided by your ISP.

**User Name:** Enter your L2TP user name.

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

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

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

**MTU:** Enter the desired Maximum Transmission Unit.

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

**L2TP IP Address:** Enter the L2TP IP address.

**L2TP Subnet Mask:** Enter your L2TP subnet mask.

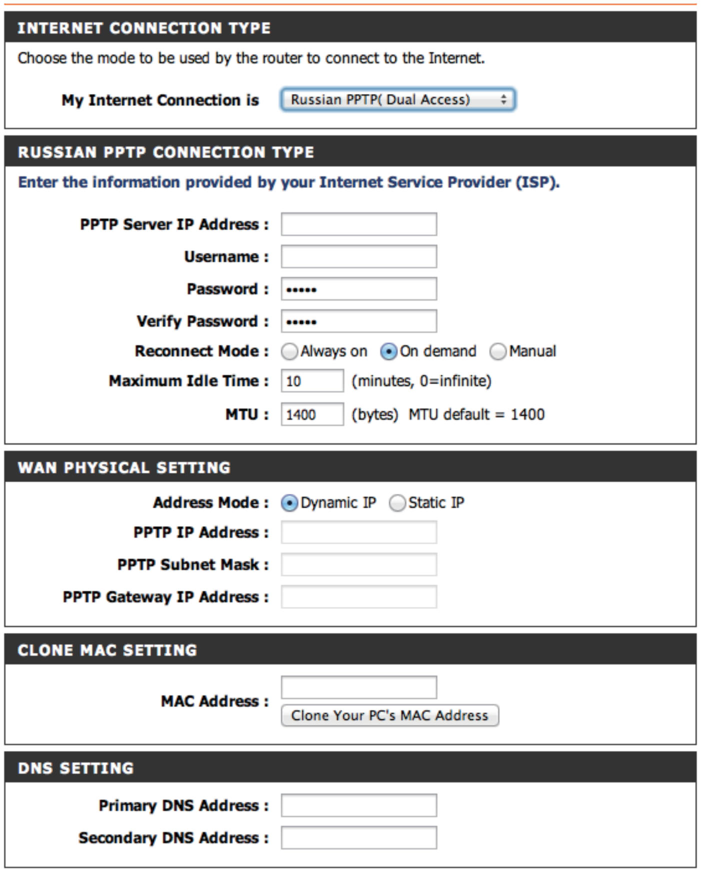
**L2TP Gateway IP Address:** Enter the L2TP Gateway IP address.

**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.

**DNS Addresses:** Enter the Primary and Secondary DNS Server Addresses.

# Russian PPTP

Choose Russian PPTP (Dual Access) if your ISP uses an PPTP connection in Russia with WAN physical access.



INTERNET CONNECTION TYPE

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

My Internet Connection is: Russian PPTP( Dual Access)

RUSSIAN PPTP CONNECTION TYPE

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

PPTP Server IP Address :

Username :

Password : •••••

Verify Password : •••••

Reconnect Mode : ○ Always on ● On demand ○ Manual

Maximum Idle Time : 10 (minutes, 0=infinite)

MTU : 1400 (bytes) MTU default = 1400

WAN PHYSICAL SETTING

Address Mode : ● Dynamic IP ○ Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

CLONE MAC SETTING

MAC Address :

DNS SETTING

Primary DNS Address :

Secondary DNS Address :

**My Internet Connection:** Select **Russian PPTP (Dual Access)** from the drop-down menu.

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

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

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

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

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

**MTU:** Enter the desired Maximum Transmission Unit.

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

**PPTP IP Address:** Enter the PPTP IP address.

**PPTP Subnet Mask:** Enter your PPTP subnet mask.

**PPTP Gateway IP Address:** Enter the PPTP Gateway IP address.

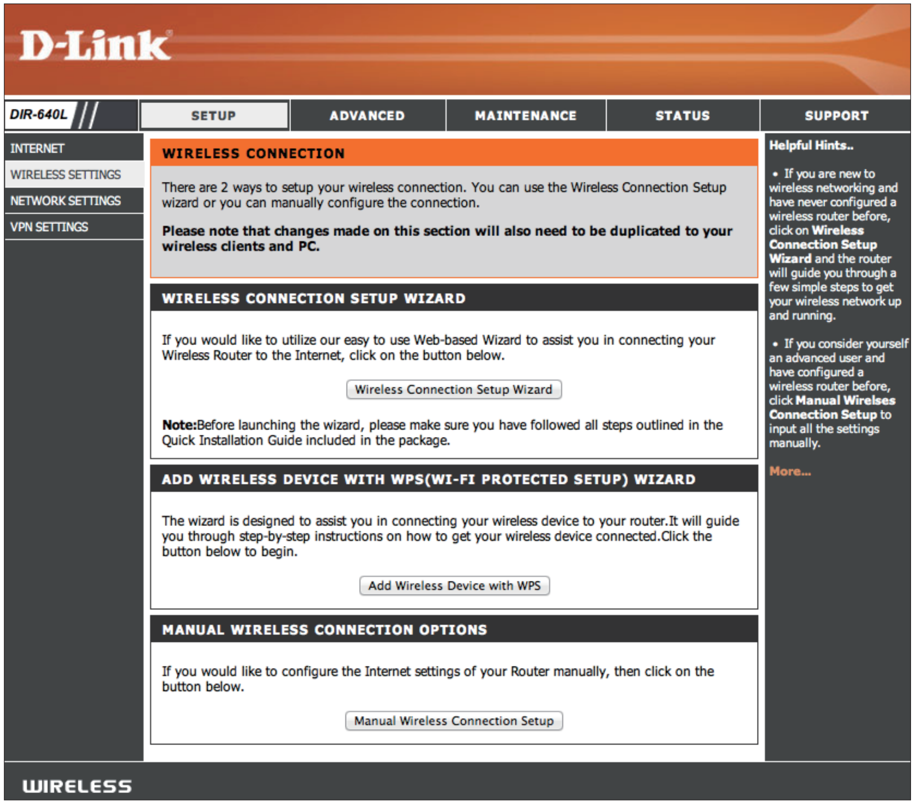
**MAC Address:** The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

**DNS Addresses:** Enter the Primary and Secondary DNS Server Addresses.

# Wireless Settings

On this page you can set up advanced options for your the wireless settings of your DIR-640L.

Use this page you can choose if you want to follow the simple steps of the Wireless Setup Wizard, add a device using WPS, or if you want to set up your wireless connection options manually.



**WIRELESS CONNECTION**

There are 2 ways to setup your wireless connection. You can use the Wireless Connection Setup wizard or you can manually configure the connection.

**Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.**

**WIRELESS CONNECTION SETUP WIZARD**

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your Wireless 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.

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

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

**MANUAL WIRELESS CONNECTION OPTIONS**

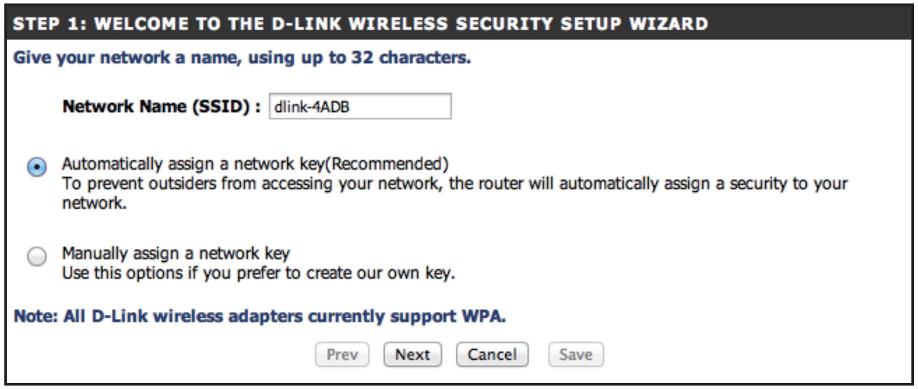
If you would like to configure the Internet settings of your Router manually, then click on the button below.

**Helpful Hints..**

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

# Wireless Setup Wizard

**STEP 1:** If you choose **Automatically assign a network key** click next to immediately complete the process.



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

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

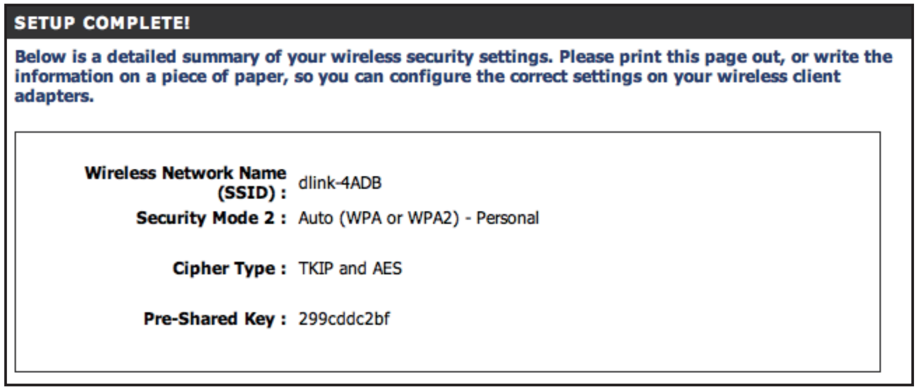
Network Name (SSID) : dlink-4ADB

● Automatically assign a network key(Recommended)
To prevent outsiders from accessing your network, the router will automatically assign a security to your network.

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

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

**STEP 2:** Setup is completed, you should take note of your settings, especially your network name and pre-shared key.

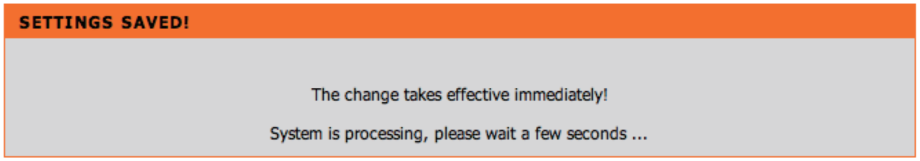


SETUP COMPLETE!

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 Network Name (SSID) : | dlink-4ADB |
| Security Mode 2 : | Auto (WPA or WPA2) - Personal |
| Cipher Type : | TKIP and AES |
| Pre-Shared Key : | 299cddc2bf |

**STEP 3:** The router must now reboot.

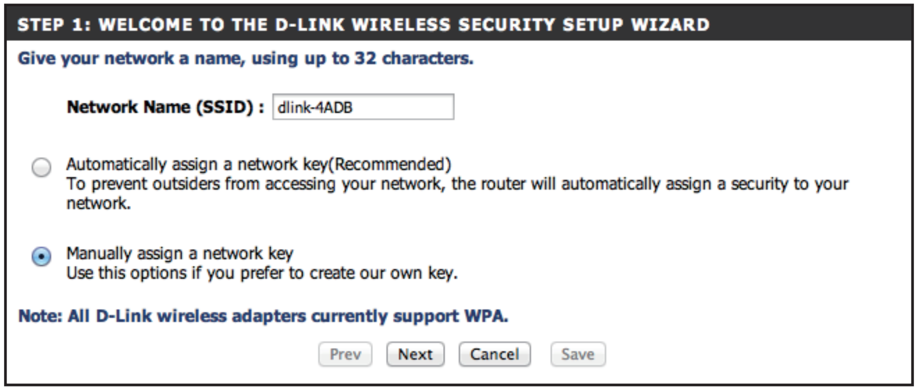


SETTINGS SAVED!

The change takes effective immediately!

System is processing, please wait a few seconds ...

**STEP 1:** If you choose **Manually assign a network key** click next to go to the next step.



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

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

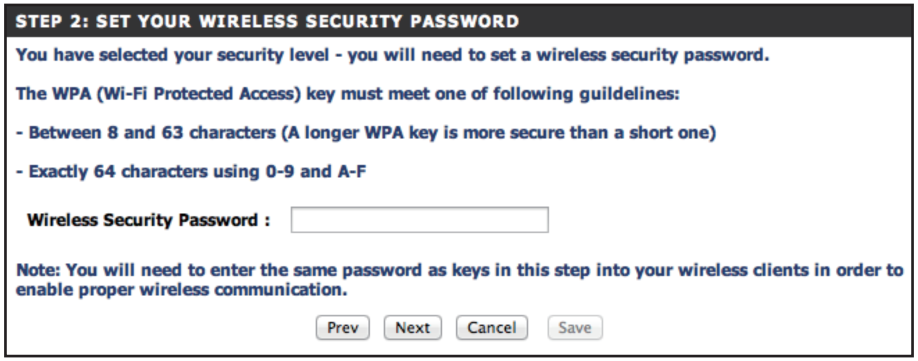
**Network Name (SSID) :** dlink-4ADB

○ Automatically assign a network key(Recommended)
To prevent outsiders from accessing your network, the router will automatically assign a security to your network.

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

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

**STEP 2:** Choose your wireless password. You will need this when connecting to the router from now on.



**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 guildelines:

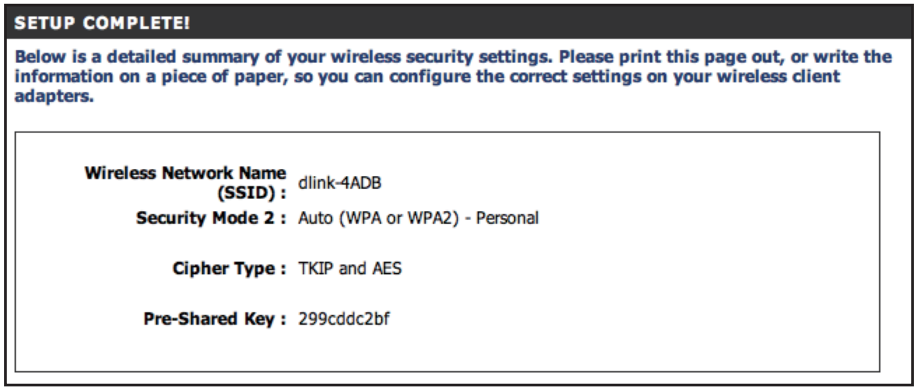
- Between 8 and 63 characters (A longer WPA key is more secure than a short one)

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

**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.

**STEP 3:** Setup is completed, you should take note of your settings, especially your network name and pre-shared key.

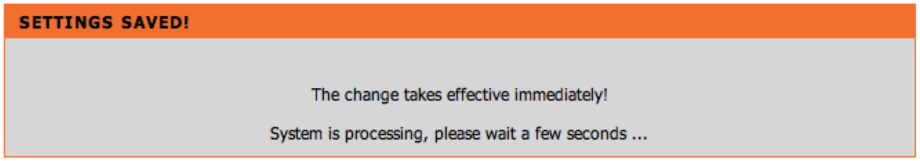


**SETUP COMPLETE!**

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 Network Name (SSID) :** | dlink-4ADB |
| **Security Mode 2 :** | Auto (WPA or WPA2) - Personal |
| **Cipher Type :** | TKIP and AES |
| **Pre-Shared Key :** | 299cddc2bf |

**STEP 4:** The router must now reboot.



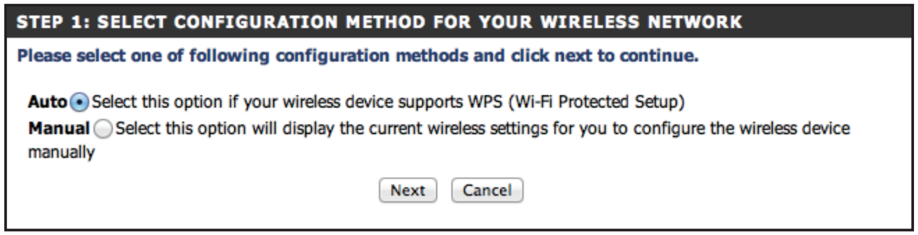
**SETTINGS SAVED!**

The change takes effective immediately!

System is processing, please wait a few seconds ...

# WPS Connection Wizard

**STEP 1:** Choose **Auto** to connect a device that already has support for WPS connections.



STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

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

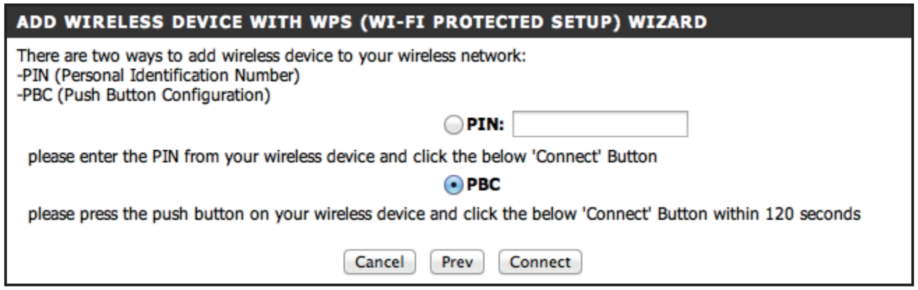
**Auto** ● Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

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

**STEP 2:** Choose whether you want to connect via **PIN** or **PBC**.

If you want to use the PIN method, simply enter your PIN and click **Connect**.

If you want to use the **PBC** method click **Connect** and go to the next step.



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

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

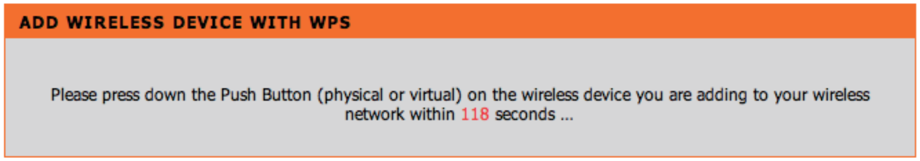
○ **PIN:**

please enter the PIN from your wireless device and click the below 'Connect' Button

● **PBC**

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

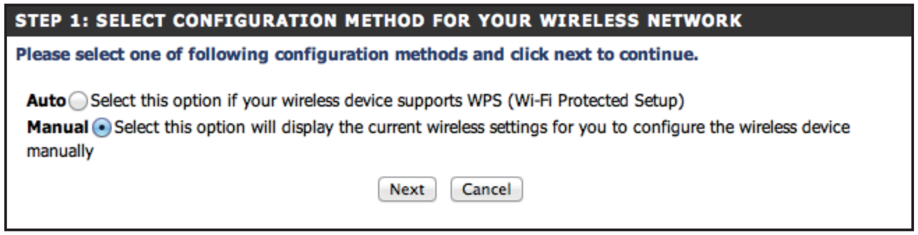
**STEP 3:** Press the button on your device and wait for the connection to be established.



ADD WIRELESS DEVICE WITH WPS

Please press down the Push Button (physical or virtual) on the wireless device you are adding to your wireless network within 118 seconds ...

**STEP 1:** Choose **Manual** to configure a device manually.



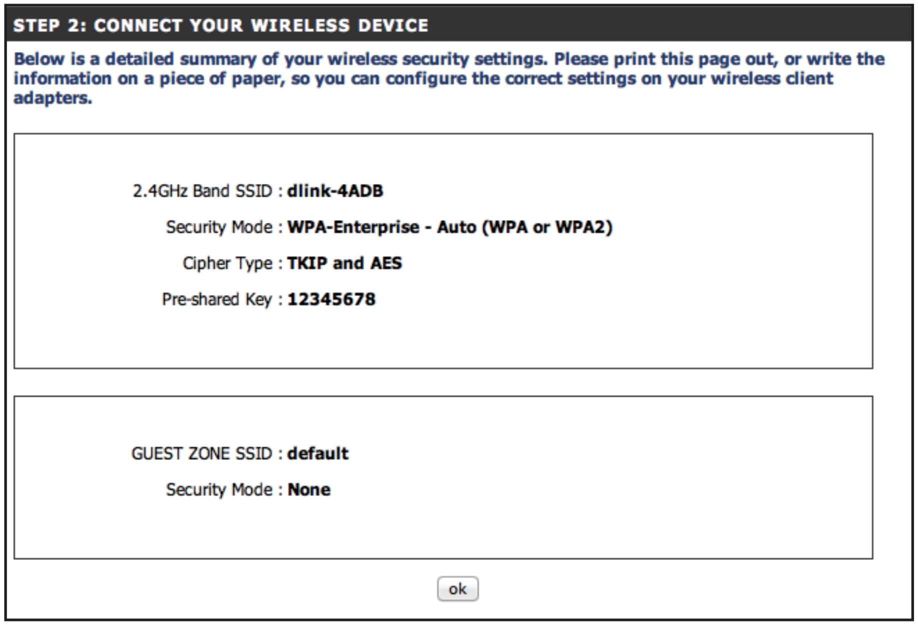
**STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK**

**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:** Use the information in this window to configure your device. When your device is prepared, click ok.



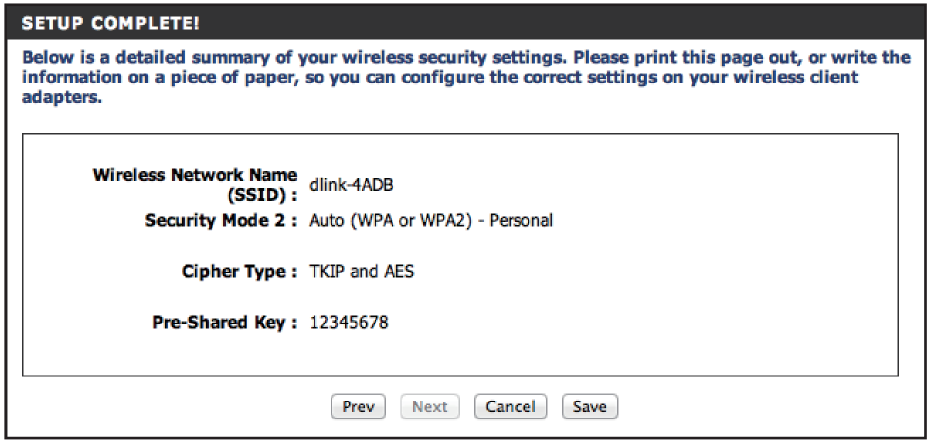
**STEP 2: CONNECT YOUR WIRELESS DEVICE**

**Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.**

| | |
|---|---|
| 2.4GHz Band SSID : | **dlink-4ADB** |
| Security Mode : | **WPA-Enterprise - Auto (WPA or WPA2)** |
| Cipher Type : | **TKIP and AES** |
| Pre-shared Key : | **12345678** |

| | |
|---|---|
| GUEST ZONE SSID : | **default** |
| Security Mode : | **None** |

**STEP 3:** Your device is now ready. Save your settings..



**SETUP COMPLETE!**

**Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.**

| | |
|---|---|
| **Wireless Network Name (SSID) :** | dlink-4ADB |
| **Security Mode 2 :** | Auto (WPA or WPA2) - Personal |
| **Cipher Type :** | TKIP and AES |
| **Pre-Shared Key :** | 12345678 |

# Manual Wireless Settings

The Wireless Settings feature will allow you to create temporary zones that can be used by guests to access the Internet.

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

**IP Address:** Input the IP Address of the router. (The default is 192.169.0.1)

**802.11 Mode:** Select the wireless mode from the drop-down menu.

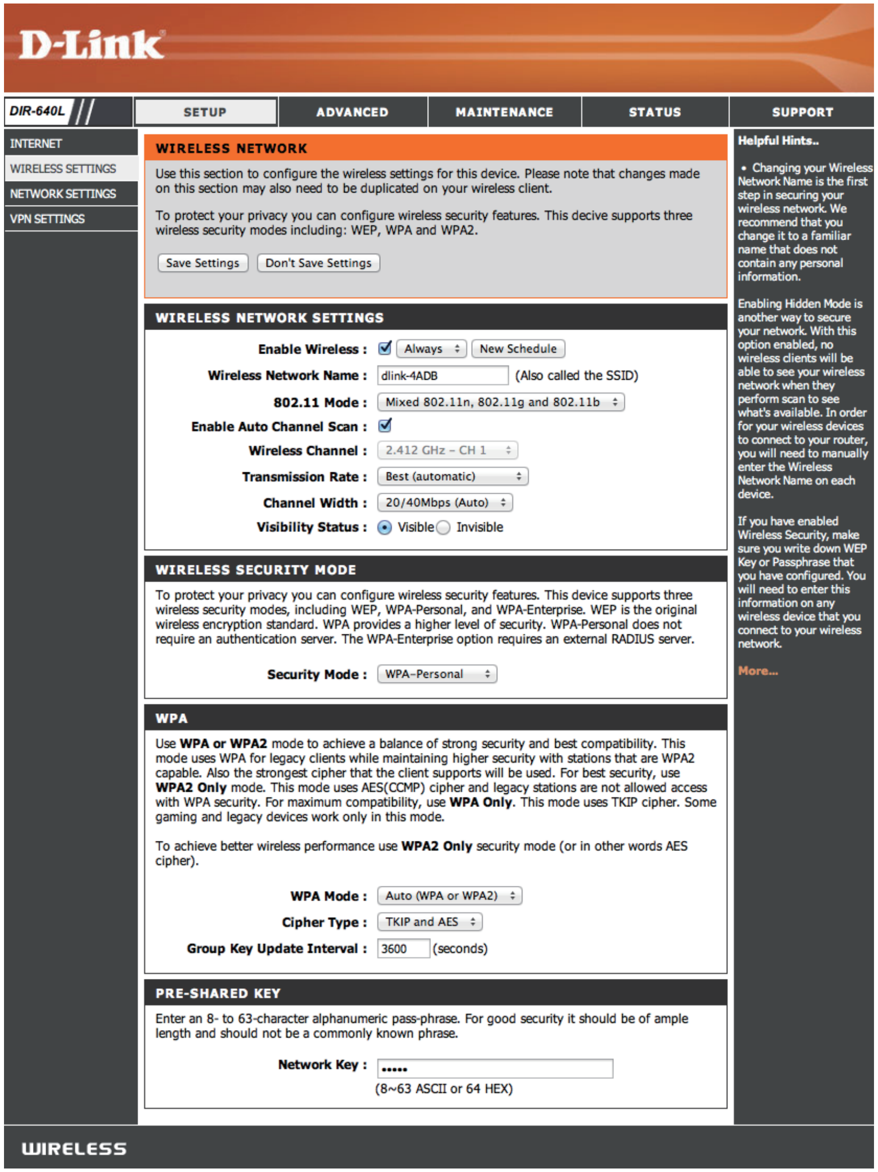
**Enable Auto Channel Scan:** This setting can be selected to allow the DIR-640L to choose the channel with the least amount of interference.

**Wireless Channel:** Indicates the channel setting for the DIR-640L. If you enable Auto Channel Scan, this option will be greyed out.

**Transmission Rate:** Select the transmission rate or let the router automatically choose for you.

**Channel Width:** Select the Channel Width:
Auto 20/40 - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.
20MHz - Select if you are not using any 802.11n wireless clients.
40MHz - Select if using only 802.11n wireless clients.

**Visibility Status:** Select Invisible if you do not want the SSID of your wireless network to be broadcasted by the DIR-640L. If Invisible is selected, the SSID will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of the DIR-640L.



**WIRELESS NETWORK**

Use this section to configure the wireless settings for this device. Please note that changes made on this section may also need to be duplicated on your wireless client.

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

**WIRELESS NETWORK SETTINGS**

Enable Wireless : ☑ Always

Wireless Network Name : dlink-4ADB (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)

Channel Width : 20/40Mbps (Auto)

Visibility Status : ● Visible ○ Invisible

**WIRELESS SECURITY MODE**

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : 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.

Network Key : •••••
(8~63 ASCII or 64 HEX)

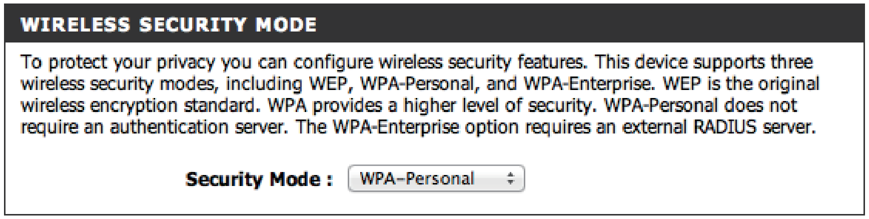
**Helpful Hints..**

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.

Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.

If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

**Security Mode:** Select the type of security or encryption you would like to enable for the guest zone. You can choose from **WPA**, **WEP**, or **WPA Enterprise** from the drop-down menu.



**WIRELESS SECURITY MODE**

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

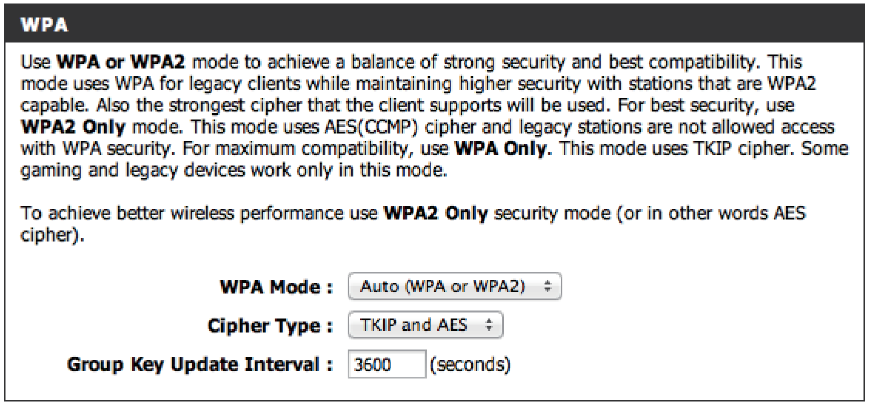
**Security Mode :** WPA-Personal

**WPA Mode (WPA):** If you selected WPA security, choose the type of WPA security to use from the drop-down menu: **WPA**, **WPA2**, or **Auto (WPA or WPA2)**.

**Cipher Type:** Choose the cipher type from the drop-down menu.

**Group Key Update Interval:** Set the length of time before the group key is updated.

**Network Key:** Enter the network pass key phrase to use.



**WPA**

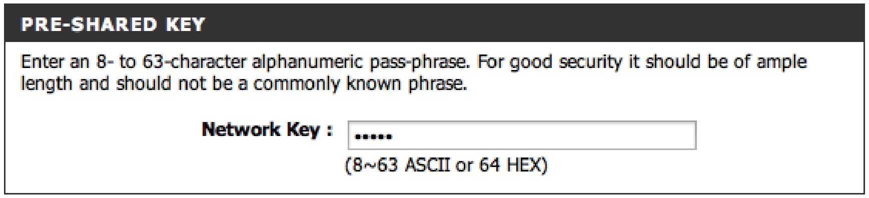
Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode.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

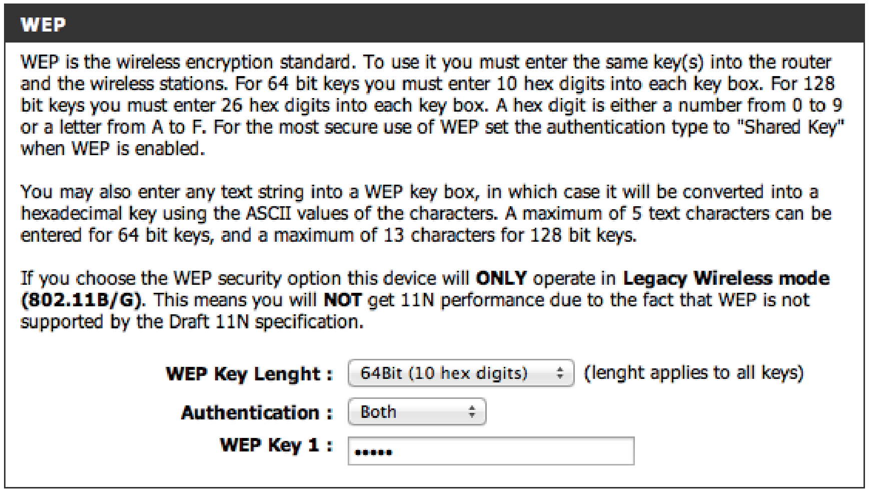
**Network Key :** •••••

(8~63 ASCII or 64 HEX)

**WEP Key Length (WEP):** If you selected WEP security, select the length you would like to set for your key.

**Authentification:** Choose your authentification method from the drop-down menu.

**WEP Key 1:** Enter your pass key.



**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 Lenght :** 64Bit (10 hex digits) (lenght applies to all keys)

**Authentication :** Both

**WEP Key 1 :** •••••

**WPA Mode (WPA Enterprise):** If you selected WPA Enterprise security, choose the WPA mode you would like to use from the drop-down menu: **WPA**, **WPA2**, or **Auto (WPA or WPA2)**.

**Cipher Type:** Choose the cipher type from the drop-down menu.

**Group Key Update Interval:** Set the length of time before the group key is updated.

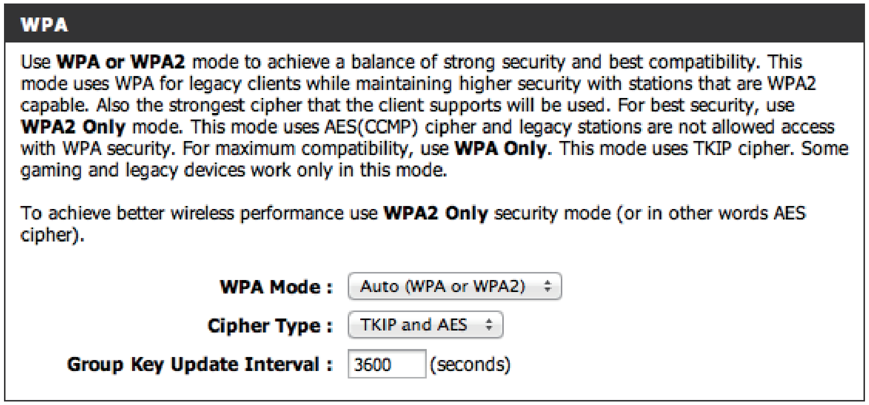
**Authentification Timeout:** Enter the amount of time in minutes before EAP authentification is abandoned.

**RADIUS Server IP Address:** Enter the IP address of the RADIUS server to connect to for authentification.

**RADIUS Server Port:** Enter the port used for contacting the RADIUS server.

**RADIUS Server Shared Secret:** Enter the shared secret of the RADIUS server.

**MAC Address Authentification:** Click to allow the RADIUS server to verify the devices MAC address for connection.



**WPA**

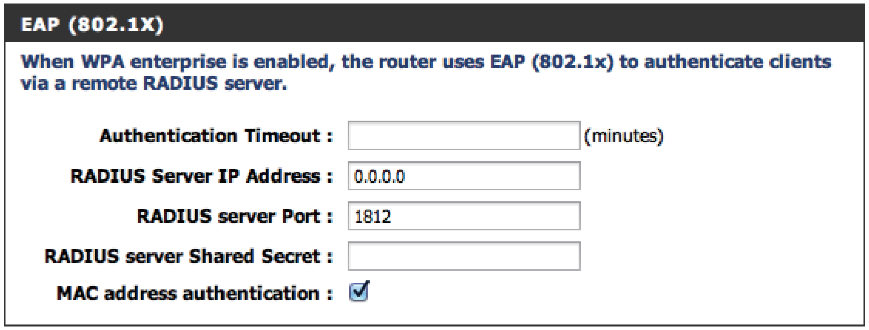
Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode.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

**Authentication Timeout :** (minutes)

**RADIUS Server IP Address :** 0.0.0.0

**RADIUS server Port :** 1812

**RADIUS server Shared Secret :**

**MAC address authentication :** ☑

# Network Settings

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

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

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

**Device Name:** Choose a name for the router.

**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.

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

**Primary WINS IP Address:** Enter your primary WINS Server IP address.

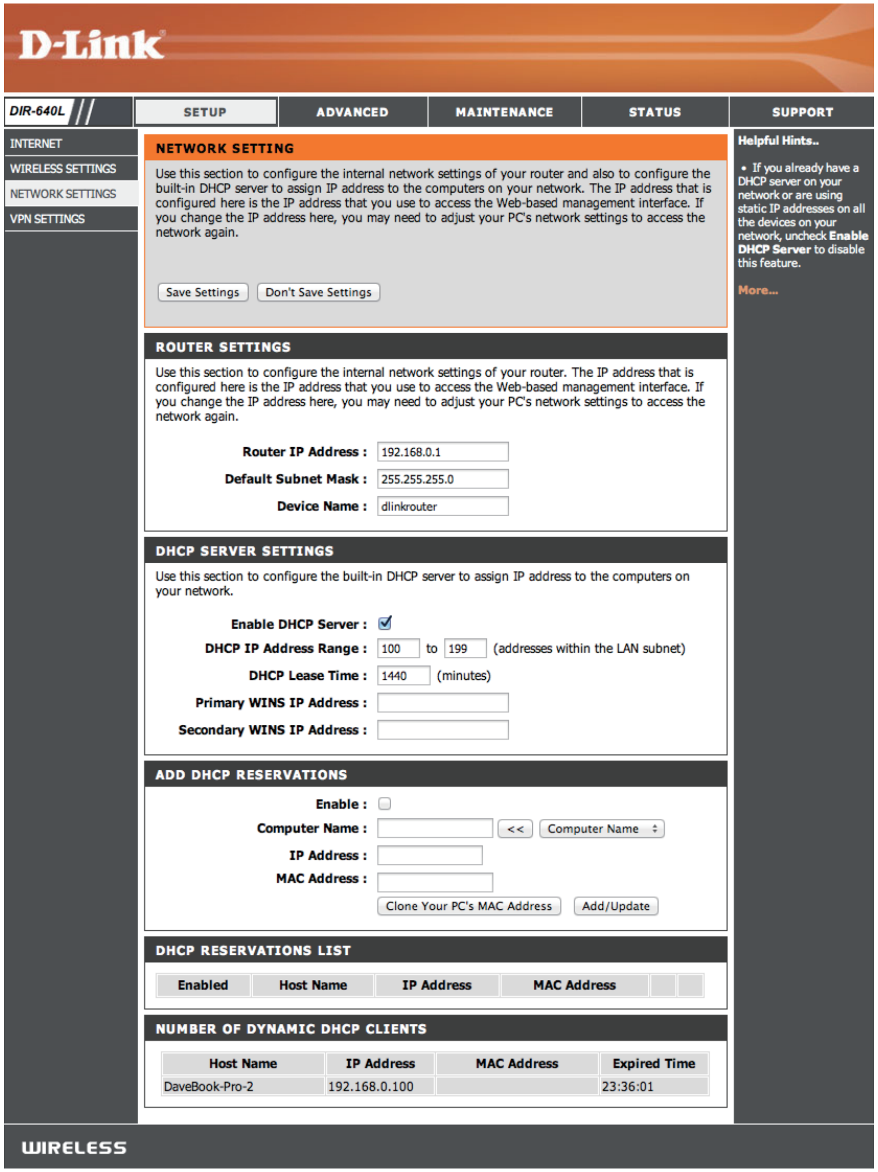
**Secondary WINS IP Address:** Enter your secondary WINS Server IP address.

**Enable DHCP Reservations:** Check this box to add a DHCP reservations list.

**Computer Name:** Give an identity to the computer.

**IP Address:** Enter the computer's IP address.

**MAC Address:** Enter the MAC address or Clone your PC's address.



NETWORK SETTING

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

Helpful Hints..

- If you already have a DHCP server on your network or are using static IP addresses on all the devices on your network, uncheck **Enable DHCP Server** to disable this feature.

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
Default Subnet Mask : 255.255.255.0
Device Name : dlinkrouter

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 : 1440 (minutes)
Primary WINS IP Address :
Secondary WINS IP Address :

ADD DHCP RESERVATIONS

Enable : □
Computer Name : Computer Name
IP Address :
MAC Address :

DHCP RESERVATIONS LIST

| Enabled | Host Name | IP Address | MAC Address | | |
|---|---|---|---|---|---|

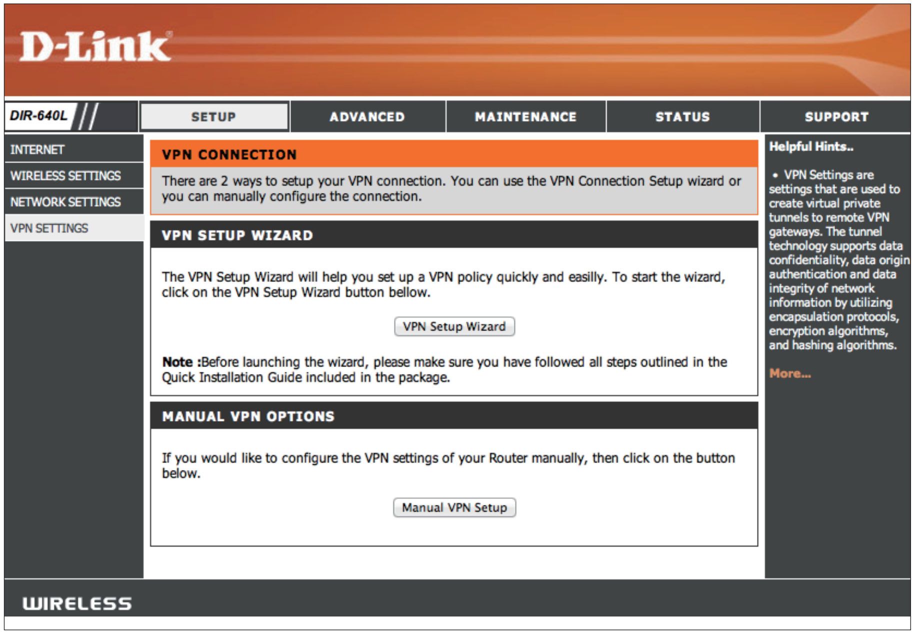
NUMBER OF DYNAMIC DHCP CLIENTS

| Host Name | IP Address | MAC Address | Expired Time |
|---|---|---|---|
| DaveBook-Pro-2 | 192.168.0.100 | | 23:36:01 |

# VPN Settings

On this page you can set up advanced options for a Virtual Private Network (VPN). The DIR-640L supports both IPSec and L2TP as the Server Endpoint. IPSec (Internet Protocol Security) is a set of protocols that can provide IP security at the network layer.

Use this page you can choose if you want to follow the simple steps of the VPN Setup Wizard, or if you want to set up VPN options manually.



VPN CONNECTION

There are 2 ways to setup your VPN connection. You can use the VPN Connection Setup wizard or you can manually configure the connection.

VPN SETUP WIZARD

The VPN Setup Wizard will help you set up a VPN policy quickly and easilly. To start the wizard, click on the VPN Setup Wizard button bellow.

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

MANUAL VPN OPTIONS

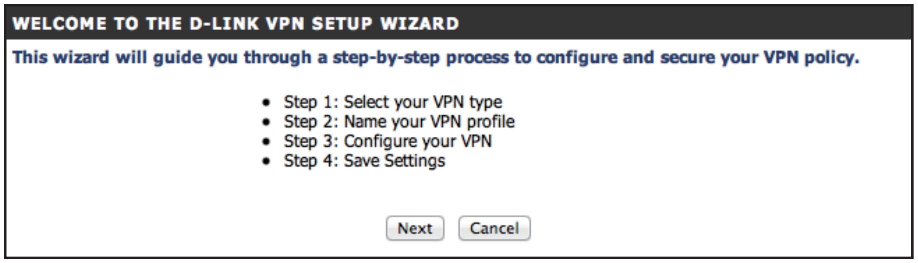
If you would like to configure the VPN settings of your Router manually, then click on the button below.

Helpful Hints..

- VPN Settings are settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

# VPN Setup Wizard

This tells you was to expect when you go through the wizard. To get to Step 1 (Selecting Your VPN Type), click **Next**.



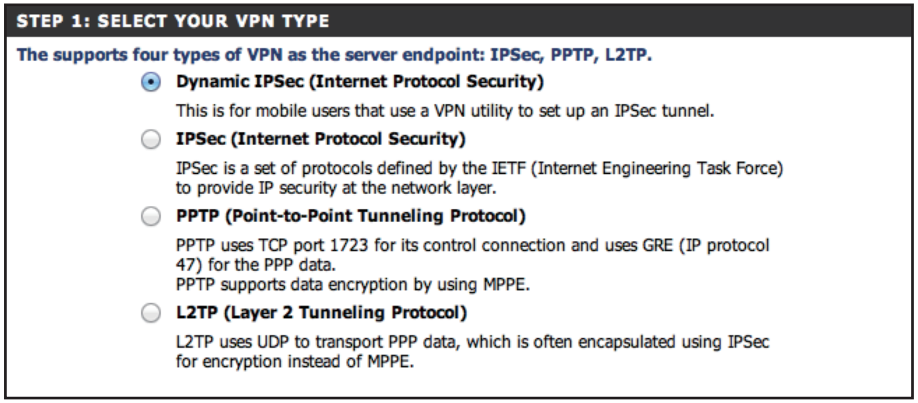
WELCOME TO THE D-LINK VPN SETUP WIZARD

This wizard will guide you through a step-by-step process to configure and secure your VPN policy.

- Step 1: Select your VPN type
- Step 2: Name your VPN profile
- Step 3: Configure your VPN
- Step 4: Save Settings

# Dynamic IPSec VPN

**STEP 1:** Choose **Dynamic IPSec** (Internet Protocol Security) then click **Next**.



**STEP 1: SELECT YOUR VPN TYPE**

The supports four types of VPN as the server endpoint: IPSec, PPTP, L2TP.

● **Dynamic IPSec (Internet Protocol Security)**

This is for mobile users that use a VPN utility to set up an IPSec tunnel.

○ **IPSec (Internet Protocol Security)**

IPSec is a set of protocols defined by the IETF (Internet Engineering Task Force) to provide IP security at the network layer.

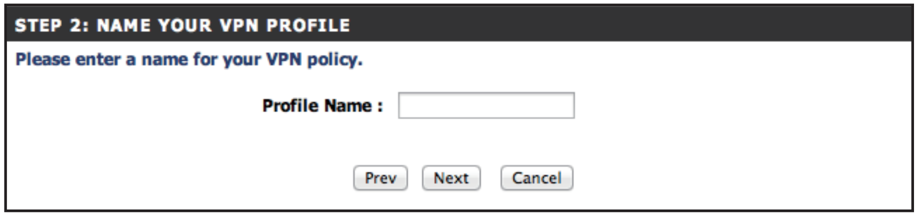
○ **PPTP (Point-to-Point Tunneling Protocol)**

PPTP uses TCP port 1723 for its control connection and uses GRE (IP protocol 47) for the PPP data.
PPTP supports data encryption by using MPPE.

○ **L2TP (Layer 2 Tunneling Protocol)**

L2TP uses UDP to transport PPP data, which is often encapsulated using IPSec for encryption instead of MPPE.

**STEP 2:** Give your VPN profile a name, and click **Next**.

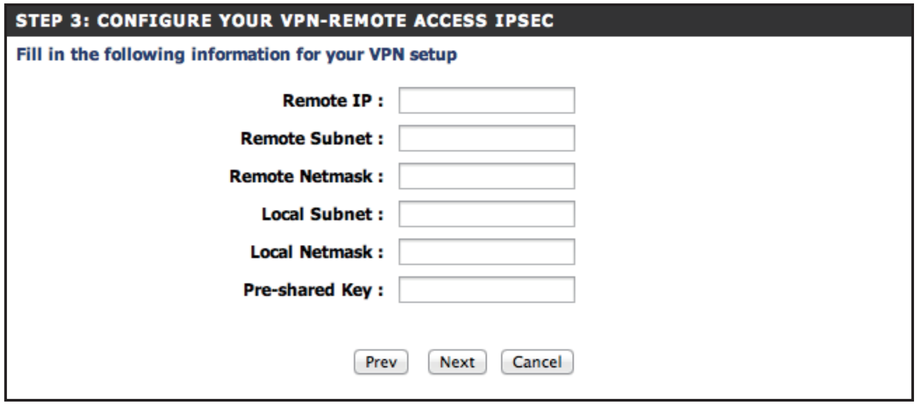


**STEP 2: NAME YOUR VPN PROFILE**

Please enter a name for your VPN policy.

Profile Name :

**STEP 3:** Enter the Local Subnet/Mask and the pre-shared key for your VPN, and click **Next**.



**STEP 3: CONFIGURE YOUR VPN-REMOTE ACCESS IPSEC**

Fill in the following information for your VPN setup

Remote IP :

Remote Subnet :

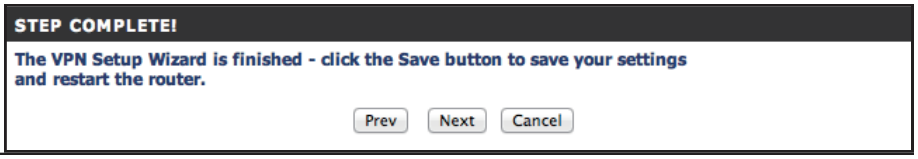
Remote Netmask :

Local Subnet :

Local Netmask :

Pre-shared Key :

**STEP 4:** Click **Next** to restart the router. You have now completed the VPN Wizard Setup.

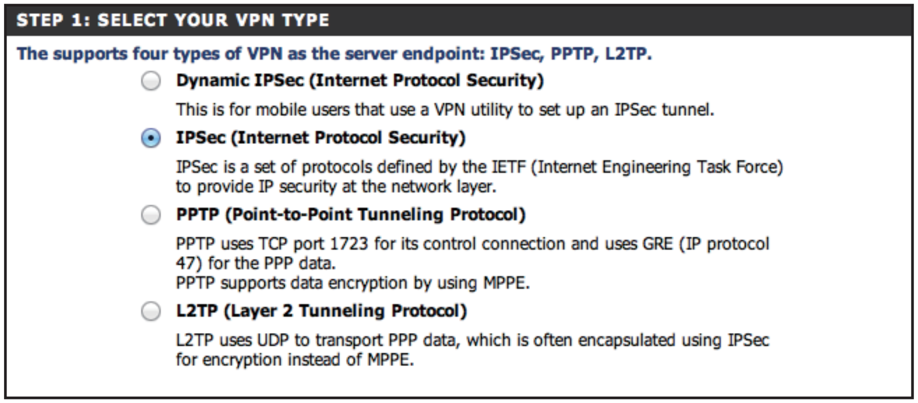


**STEP COMPLETE!**

The VPN Setup Wizard is finished - click the Save button to save your settings and restart the router.

# IPSec VPN

**STEP 1:** Choose **Dynamic IPSec** (Internet Protocol Security) then click **Next**.



STEP 1: SELECT YOUR VPN TYPE

The supports four types of VPN as the server endpoint: IPSec, PPTP, L2TP.

○ **Dynamic IPSec (Internet Protocol Security)**

This is for mobile users that use a VPN utility to set up an IPSec tunnel.

● **IPSec (Internet Protocol Security)**

IPSec is a set of protocols defined by the IETF (Internet Engineering Task Force) to provide IP security at the network layer.

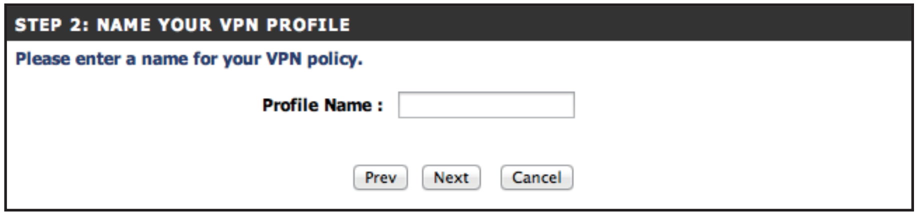
○ **PPTP (Point-to-Point Tunneling Protocol)**

PPTP uses TCP port 1723 for its control connection and uses GRE (IP protocol 47) for the PPP data.
PPTP supports data encryption by using MPPE.

○ **L2TP (Layer 2 Tunneling Protocol)**

L2TP uses UDP to transport PPP data, which is often encapsulated using IPSec for encryption instead of MPPE.

**STEP 2:** Give your VPN profile a name, and click **Next**.

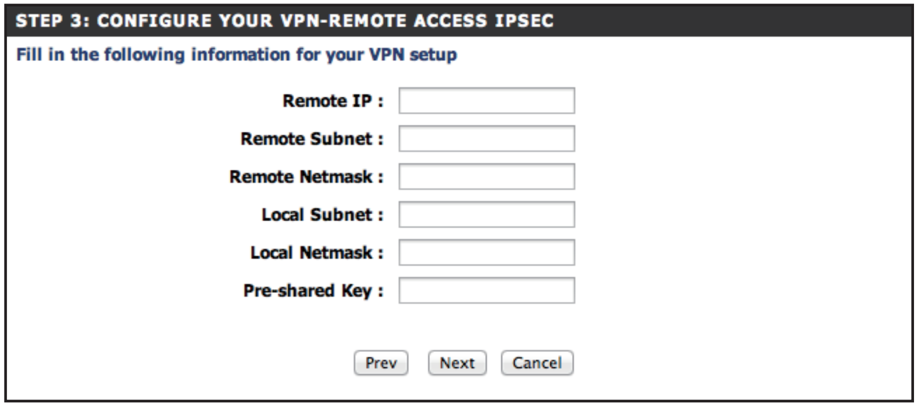


STEP 2: NAME YOUR VPN PROFILE

Please enter a name for your VPN policy.

Profile Name :

**STEP 3:** Enter the Local Subnet/Mask and the pre-shared key for your VPN, and click **Next**.



STEP 3: CONFIGURE YOUR VPN-REMOTE ACCESS IPSEC

Fill in the following information for your VPN setup

Remote IP :

Remote Subnet :

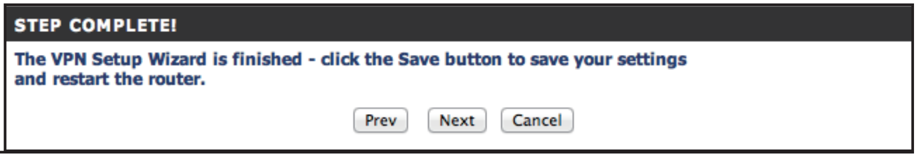
Remote Netmask :

Local Subnet :

Local Netmask :

Pre-shared Key :

**STEP 4:** Click **Next** to restart the router. You have now completed the VPN Wizard Setup.

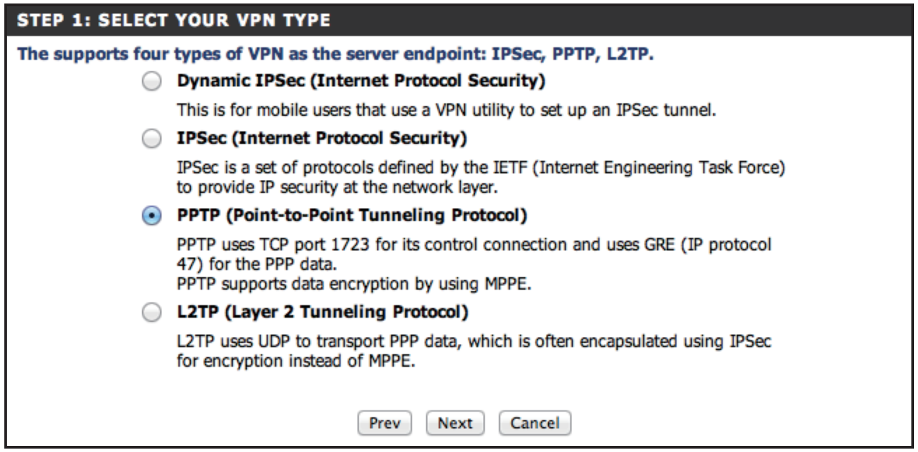


STEP COMPLETE!

The VPN Setup Wizard is finished - click the Save button to save your settings and restart the router.

# PPTP VPN

**STEP 1:** Choose **PPTP** (Point-to-Point Tunneling Protocol) then click on **Next**.



STEP 1: SELECT YOUR VPN TYPE

The supports four types of VPN as the server endpoint: IPSec, PPTP, L2TP.

○ **Dynamic IPSec (Internet Protocol Security)**

This is for mobile users that use a VPN utility to set up an IPSec tunnel.

○ **IPSec (Internet Protocol Security)**

IPSec is a set of protocols defined by the IETF (Internet Engineering Task Force) to provide IP security at the network layer.

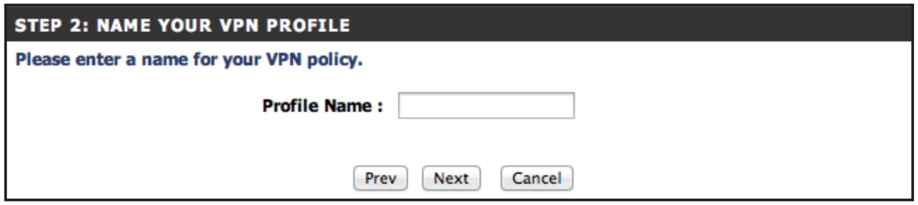
● **PPTP (Point-to-Point Tunneling Protocol)**

PPTP uses TCP port 1723 for its control connection and uses GRE (IP protocol 47) for the PPP data.
PPTP supports data encryption by using MPPE.

○ **L2TP (Layer 2 Tunneling Protocol)**

L2TP uses UDP to transport PPP data, which is often encapsulated using IPSec for encryption instead of MPPE.

**STEP 2:** Give your VPN profile a name, and click  **Next**.

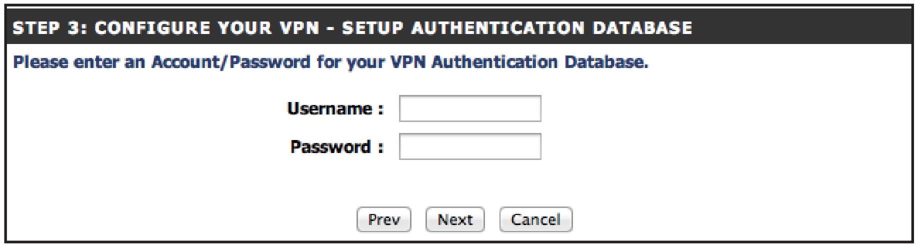


STEP 2: NAME YOUR VPN PROFILE

Please enter a name for your VPN policy.

Profile Name :

**STEP 3:** Choose and username and password for your VPN, and click  **Next**.



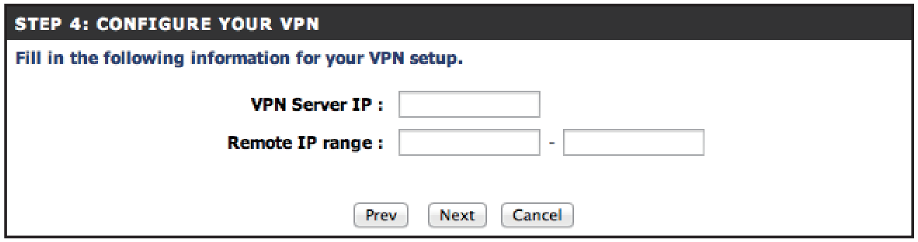
STEP 3: CONFIGURE YOUR VPN - SETUP AUTHENTICATION DATABASE

Please enter an Account/Password for your VPN Authentication Database.

Username :

Password :

**STEP 4:** Enter a VPN server IP and remote IP range, and click **Next**.



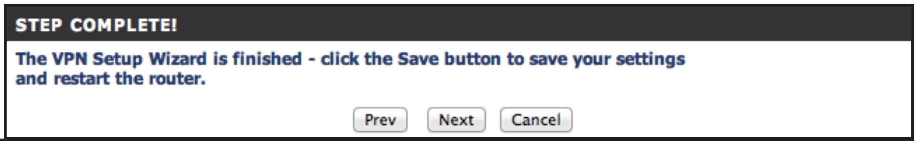
STEP 4: CONFIGURE YOUR VPN

Fill in the following information for your VPN setup.

VPN Server IP :

Remote IP range : -

**STEP 4:** Click **Next** to restart the router. You have now completed the VPN Wizard Setup.

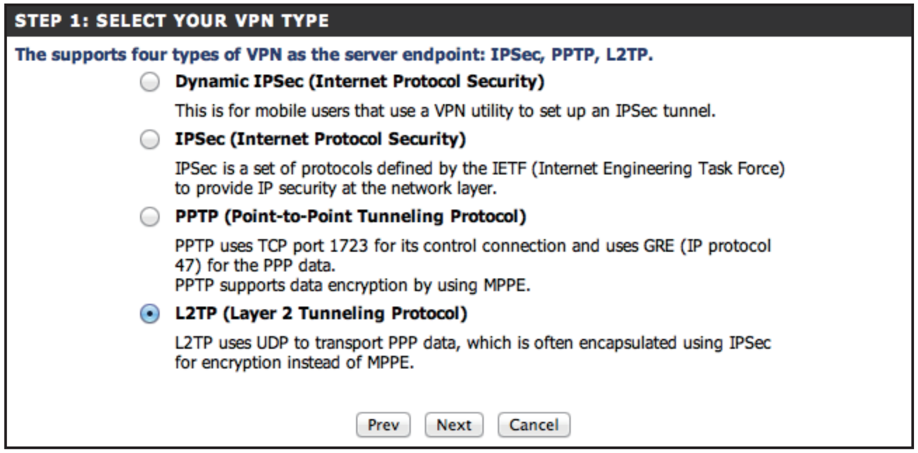


STEP COMPLETE!

The VPN Setup Wizard is finished - click the Save button to save your settings and restart the router.

# L2TP VPN

**STEP 1:** Choose **L2TP** (Layer 2 Tunneling Protocol) then click on **Next**.



**STEP 1: SELECT YOUR VPN TYPE**

The supports four types of VPN as the server endpoint: IPSec, PPTP, L2TP.

○ **Dynamic IPSec (Internet Protocol Security)**

This is for mobile users that use a VPN utility to set up an IPSec tunnel.

○ **IPSec (Internet Protocol Security)**

IPSec is a set of protocols defined by the IETF (Internet Engineering Task Force) to provide IP security at the network layer.

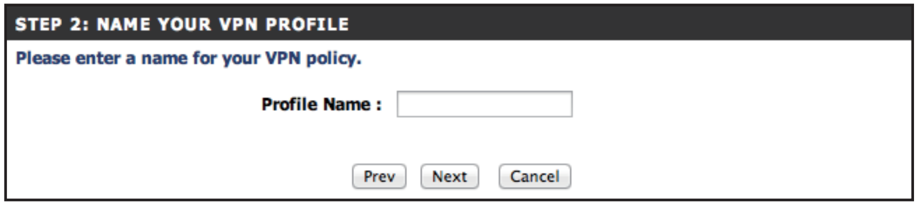
○ **PPTP (Point-to-Point Tunneling Protocol)**

PPTP uses TCP port 1723 for its control connection and uses GRE (IP protocol 47) for the PPP data.
PPTP supports data encryption by using MPPE.

● **L2TP (Layer 2 Tunneling Protocol)**

L2TP uses UDP to transport PPP data, which is often encapsulated using IPSec for encryption instead of MPPE.

**STEP 2:** Give your VPN profile a name, and click **Next**.

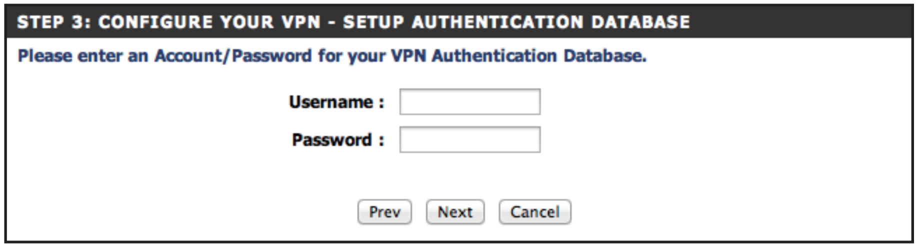


**STEP 2: NAME YOUR VPN PROFILE**

Please enter a name for your VPN policy.

Profile Name :

**STEP 3:** Choose and username and password for your VPN, and click **Next**.



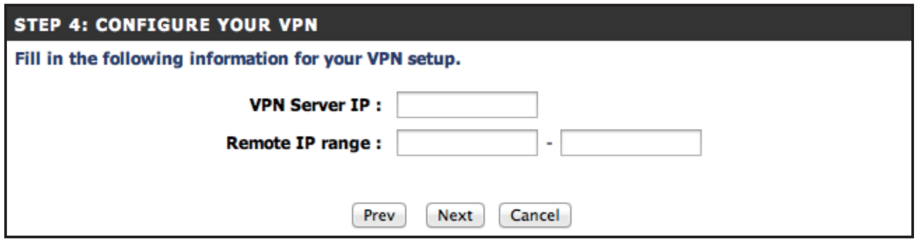
**STEP 3: CONFIGURE YOUR VPN - SETUP AUTHENTICATION DATABASE**

Please enter an Account/Password for your VPN Authentication Database.

Username :

Password :

**STEP 4:** Enter a VPN server IP and remote IP range, and click **Next**.



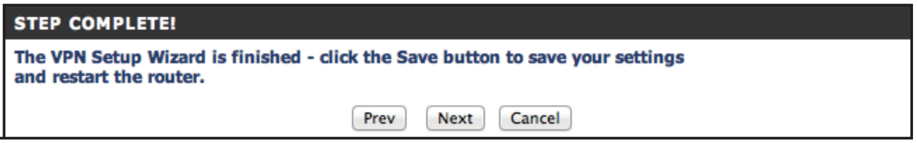
**STEP 4: CONFIGURE YOUR VPN**

Fill in the following information for your VPN setup.

VPN Server IP :

Remote IP range : -

**STEP 4:** Click **Next** to restart the router. You have now completed the VPN Wizard Setup.



**STEP COMPLETE!**

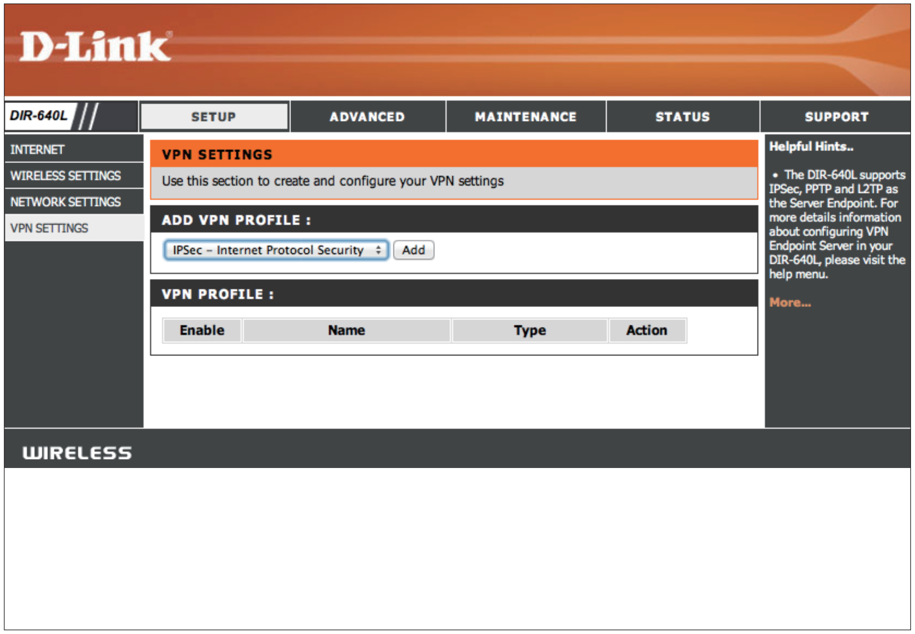
The VPN Setup Wizard is finished - click the Save button to save your settings and restart the router.

# VPN Manual Settings

On this page you can set up advanced options for a Virtual Private Network (VPN). The DIR-640L supports both IPSec and L2TP as the Server Endpoint. IPSec (Internet Protocol Security) is a set of protocols that can provide IP security at the network layer.

**Add VPN Profile:** Choose either **IPSec** or **PPTP/L2TP** and **GRE Tunnel** from the drop-down menu and click **Add** to begin configuring a VPN profile.

**VPN Profile:** This list allows you to **Enable** established VPN profiles as well as **Edit** and **Delete** them.



VPN SETTINGS

Use this section to create and configure your VPN settings

ADD VPN PROFILE :

IPSec – Internet Protocol Security

VPN PROFILE :

| Enable | Name | Type | Action |
|---|---|---|---|

Helpful Hints..

- The DIR-640L supports IPSec, PPTP and L2TP as the Server Endpoint. For more details information about configuring VPN Endpoint Server in your DIR-640L, please visit the help menu.

# IPSec Settings

The DIR-640L supports IPSec as the Server Endpoint. IPSec (Internet Protocol Security) protocols can provide IP security at the network layer.

**IPSec:** Check this box to enable IPSec.

**Name:** Enter a name for your VPN tunnel.

**Local Subnet/ Netmask:** Enter the local (LAN) subnet and mask. (ex. 192.168.0.0/24)

**Remote IP:** Select if you will be connecting as a remote user or on a site to site basis.

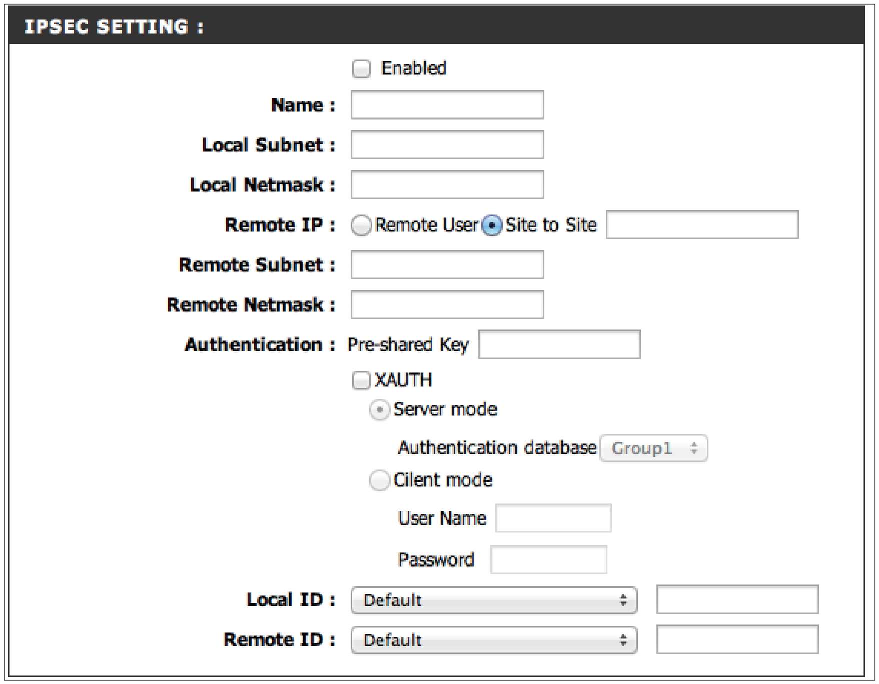
**Remote Subnet/ Netmask:** Enter the remote subnet and mask.

**Authentification Pre-Shared Key:** Enter the key for authentification.

**Authentification XAUTH:** If you choose to enable **XAUTH** you need to choose between Server mode with an Authetification database, or Client mode with a user name and password.

**Local ID:** Enter the local identification for how you appear on the network VPN when connected locally.

**Remote ID:** Enter the local identification for how you appear on the network VPN when connected remotely.



IPSEC SETTING :

□ Enabled

Name :

Local Subnet :

Local Netmask :

Remote IP : ○ Remote User ● Site to Site

Remote Subnet :

Remote Netmask :

Authentication : Pre-shared Key

□ XAUTH

● Server mode

Authentication database Group1

○ Cilent mode

User Name

Password

Local ID : Default

Remote ID : Default

**Phase1 Mode:** Choose if you want to use a main or aggressive mode.

**NAT-T Enable:** **Enable** or **Disable** the NAT-T option.

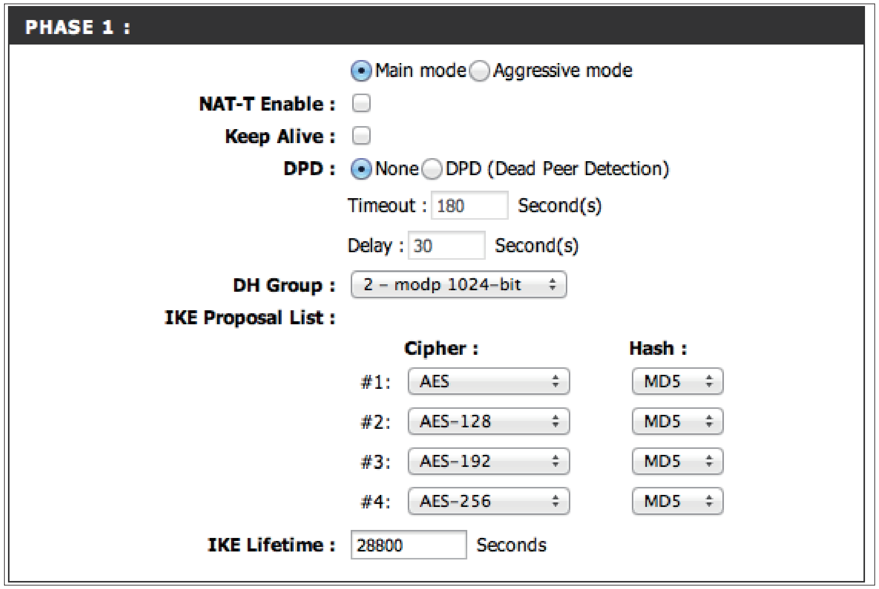
**Keep Alive:** **Enable** or **Disable** Keep Alive protocols.

**DPD:** Choose whether or not to detect dead peers, then set the amount of time in seconds before disconnect of dead peers. You can also set a delay time in second before release.

**DH Group:** **Enable** or **Disable** the DH Group option using the drop-down menu.

**IKE Proposal Settings:** Use this area to **Enable** IKE Proposals. Then determine encryption and authentification types from the drop-down menus.

**IKE Lifetime:** Enter the amount of time in seconds that the Phase 1 keys should last.



**PHASE 1 :**

● Main mode ○ Aggressive mode

NAT-T Enable : □

Keep Alive : □

DPD : ● None ○ DPD (Dead Peer Detection)

Timeout : 180 Second(s)

Delay : 30 Second(s)

DH Group : 2 - modp 1024-bit

IKE Proposal List :

| | Cipher : | Hash : |
|---|---|---|
| #1: | AES | MD5 |
| #2: | AES-128 | MD5 |
| #3: | AES-192 | MD5 |
| #4: | AES-256 | MD5 |

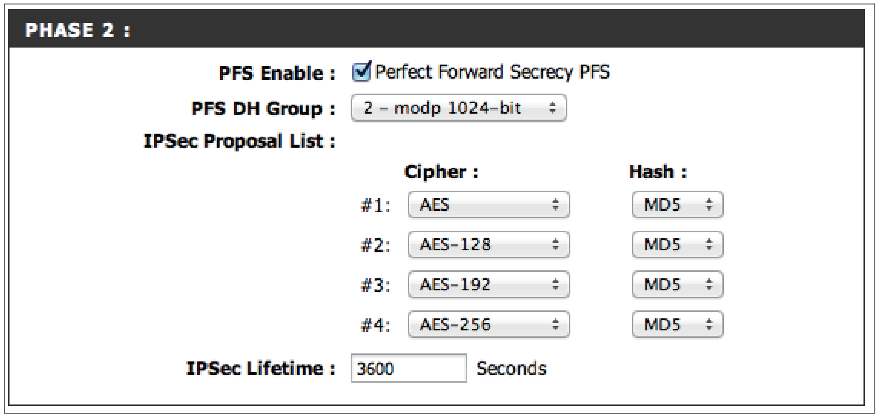
IKE Lifetime : 28800 Seconds

**PFS Enable:** Choose if you want to use Perfect Forward Secrecy. PFS is an additional security protocol.

**PFS DH Group:** Choose a PFS DH Group from the drop-down menu.

**IPSEC Proposal List:** Use this area to choose the encryption and authentification methods for IPSec proposals by choosing from the drop-down menus.

**IPSec Lifetime:** Enter the amount of time in seconds that the Phase 2 keys should last.



**PHASE 2 :**

PFS Enable : ☑ Perfect Forward Secrecy PFS

PFS DH Group : 2 - modp 1024-bit

IPSec Proposal List :

| | Cipher : | Hash : |
|---|---|---|
| #1: | AES | MD5 |
| #2: | AES-128 | MD5 |
| #3: | AES-192 | MD5 |
| #4: | AES-256 | MD5 |

IPSec Lifetime : 3600 Seconds

# PPTP/L2TP Settings

This page allows you to set up a VPN using either PPTP or L2TP.

**PPTP/L2TP:** Check this box to enable PPTP/L2TP settings.

**Name:** Enter a name for your VPN.

**Connection Type:** Select **PPTP** or **L2TP**.

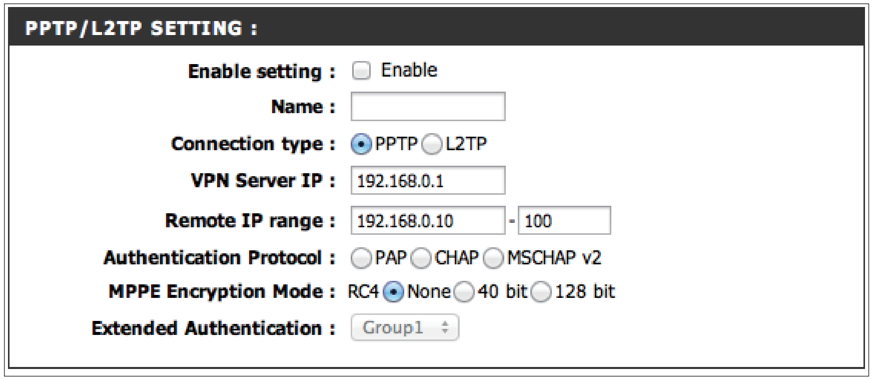
**VPN Server IP:** Enter the IP address of the VPN server.

**Remote IP Range:** Enter the remote IP range in the boxes.

**Authentification Protocol:** Choose **PAP**, **CHAP**, or **MSCHAP v2** for your authentification.

**MPPE Encryption Mode:** Choose either **RC4**, **None**, **40 bit**, or **128 bit** to determine the strength level of your authentification.

**Extended Authentification:** If you wish to use extended authentification, choose a group from the drop-down menu.



PPTP/L2TP SETTING :

Enable setting : □ Enable

Name :

Connection type : ● PPTP ○ L2TP

VPN Server IP : 192.168.0.1

Remote IP range : 192.168.0.10 - 100

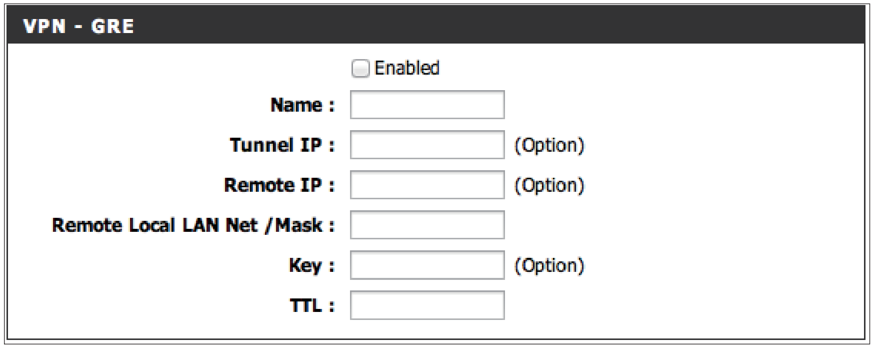
Authentication Protocol : ○ PAP ○ CHAP ○ MSCHAP v2

MPPE Encryption Mode : RC4 ● None ○ 40 bit ○ 128 bit

Extended Authentication : Group1

# GRE Settings

This page shows you the options for setting up a VPN tunnel using Generic Routing Encapsulation (GRE), which is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol.



**VPN - GRE Enable:** Check this box to enable GRE VPN settings.

**Name:** Enter a name for your VPN.

**Tunnel IP:** Select an IP address for the tunnel.

**Remote IP:** Select an IP address to access the tunnel remotely.

**Remote Local LAN Net/Mask:** Enter the remote local (LAN) subnet and mask. (ex. 192.168.0.0/24)

**Key:** Enter the key for the tunnel.

**TTL:** Enter the time to live for packets delivered.

# 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.

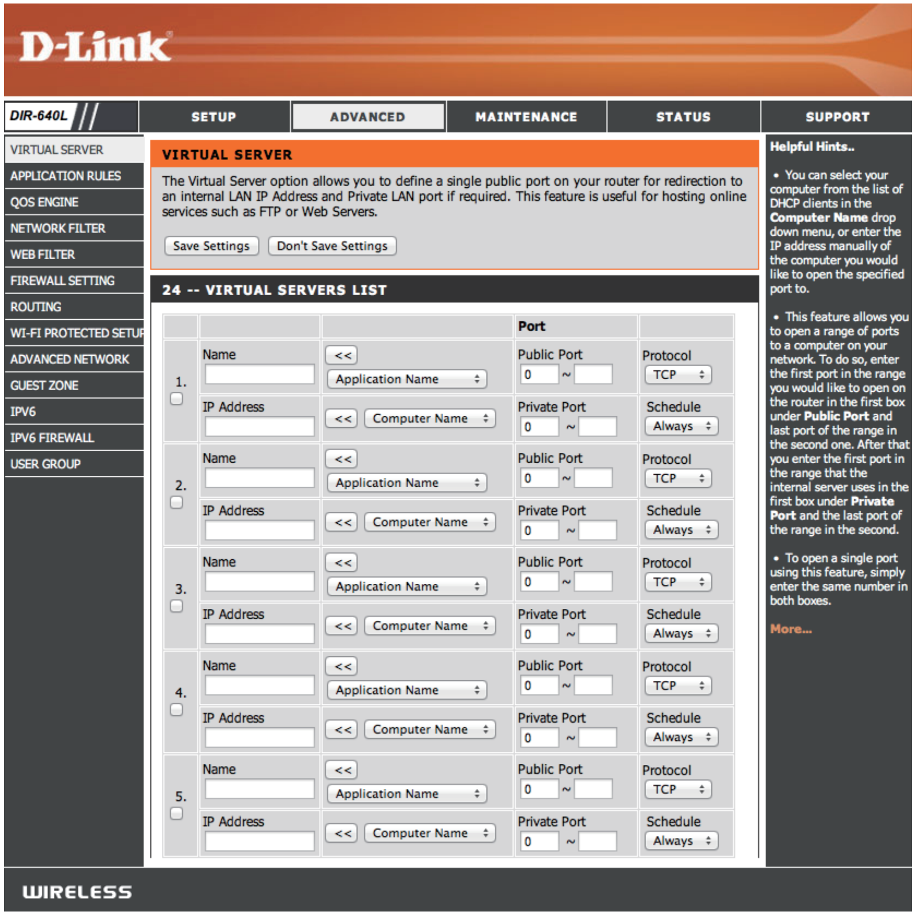
**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click **<<** to populate the fields.

**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 **Maintenance** > **Schedules** section.



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

| | | | Port | |
|---|---|---|---|---|
| 1. □ | Name | << Application Name | Public Port 0 ~ | Protocol TCP |
| | IP Address | << Computer Name | Private Port 0 ~ | Schedule Always |
| 2. □ | Name | << Application Name | Public Port 0 ~ | Protocol TCP |
| | IP Address | << Computer Name | Private Port 0 ~ | Schedule Always |
| 3. □ | Name | << Application Name | Public Port 0 ~ | Protocol TCP |
| | IP Address | << Computer Name | Private Port 0 ~ | Schedule Always |
| 4. □ | Name | << Application Name | Public Port 0 ~ | Protocol TCP |
| | IP Address | << Computer Name | Private Port 0 ~ | Schedule Always |
| 5. □ | Name | << Application Name | Public Port 0 ~ | Protocol TCP |
| | IP Address | << Computer Name | Private Port 0 ~ | Schedule Always |

Helpful Hints..

- You can select your computer from the list of DHCP clients in the **Computer Name** drop down menu, or enter the IP address manually of the computer you would like to open the specified port to.
- This feature allows you to open a range of ports to a computer on your network. To do so, enter the first port in the range you would like to open on the router in the first box under **Public Port** and last port of the range in the second one. After that you enter the first port in the range that the internal server uses in the first box under **Private Port** and the last port of the range in the second.
- To open a single port using this feature, simply enter the same number in both boxes.

More...

# Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DIR-640L. 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.

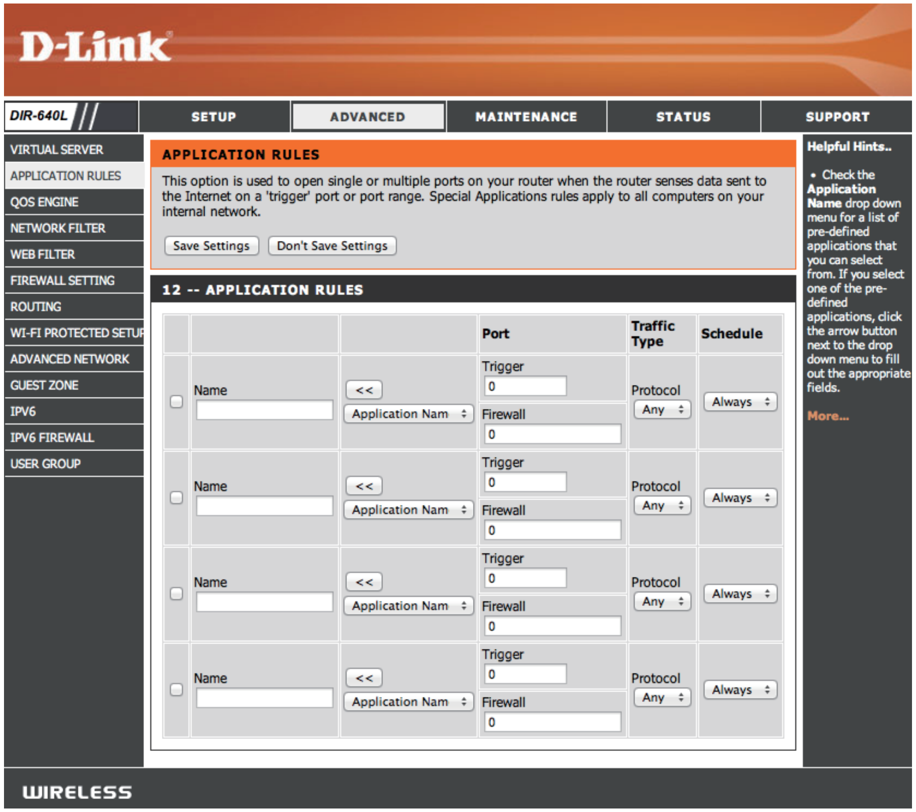
**Name:** Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click.

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

**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 **Maintenance** > **Schedules** section.



APPLICATION RULES

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

12 -- APPLICATION RULES

| | | | Port | Traffic Type | Schedule |
|---|---|---|---|---|---|
| □ | Name | << <br> Application Nam | Trigger 0 <br> Firewall 0 | Protocol <br> Any | Always |
| □ | Name | << <br> Application Nam | Trigger 0 <br> Firewall 0 | Protocol <br> Any | Always |
| □ | Name | << <br> Application Nam | Trigger 0 <br> Firewall 0 | Protocol <br> Any | Always |
| □ | Name | << <br> Application Nam | Trigger 0 <br> Firewall 0 | Protocol <br> Any | Always |

Helpful Hints..

- Check the **Application Name** drop down menu for a list of pre-defined applications that you can select from. If you select one of the pre-defined applications, click the arrow button next to the drop down menu to fill out the appropriate fields.

More...

# QoS Engine

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

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

**Upstream Bandwidth:** The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as speedtest.net.

**QoS Engine Rules:** A QoS Engine Rule identifies a specific message flow and assigns a priority to that flow. For most applications, automatic classification will be adequate, and specific QoS Engine Rules will not be required.

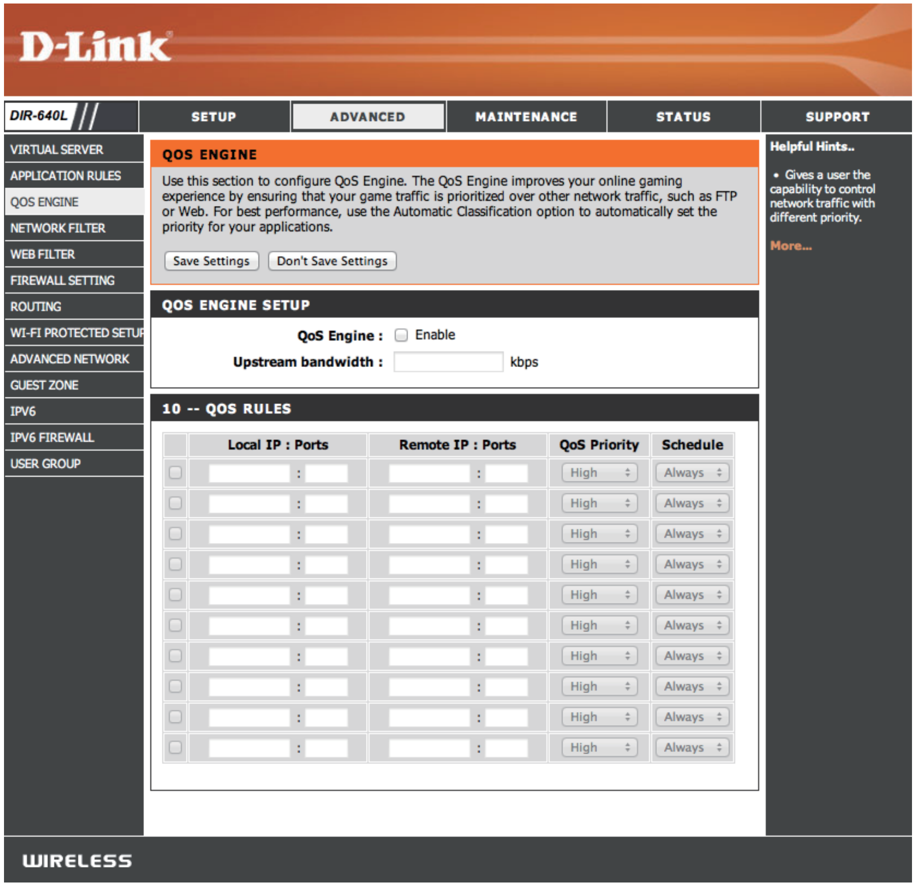
The QoS Engine supports overlaps between rules, where more than one rule can match for a specific message flow. If more than one rule is found to match the rule with the highest priority will be used.

**Local IP:** The rule applies to a flow of messages whose LAN-side IP address falls within the range set here.

**Local Port:** The rule applies to a flow of messages whose LAN-side port number is within the range set here.

**Remote IP:** The rule applies to a flow of messages whose WAN-side IP address falls within the range set here.

**Remote Port:** The rule applies to a flow of messages whose WAN-side port number is within the range set here.



QOS ENGINE

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

Helpful Hints..

- Gives a user the capability to control network traffic with different priority.

QOS ENGINE SETUP

QoS Engine : ☐ Enable

Upstream bandwidth : kbps

10 -- QOS RULES

| | Local IP : Ports | Remote IP : Ports | QoS Priority | Schedule |
|---|---|---|---|---|
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |
| ☐ | : | : | High | Always |

**Priority:** The priority of the message flow is entered here -- 1 receives the highest priority (most urgent) and 255 receives the lowest priority (least urgent).

**Schedule:** Choose a schedule for the QoS rule.

# 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.

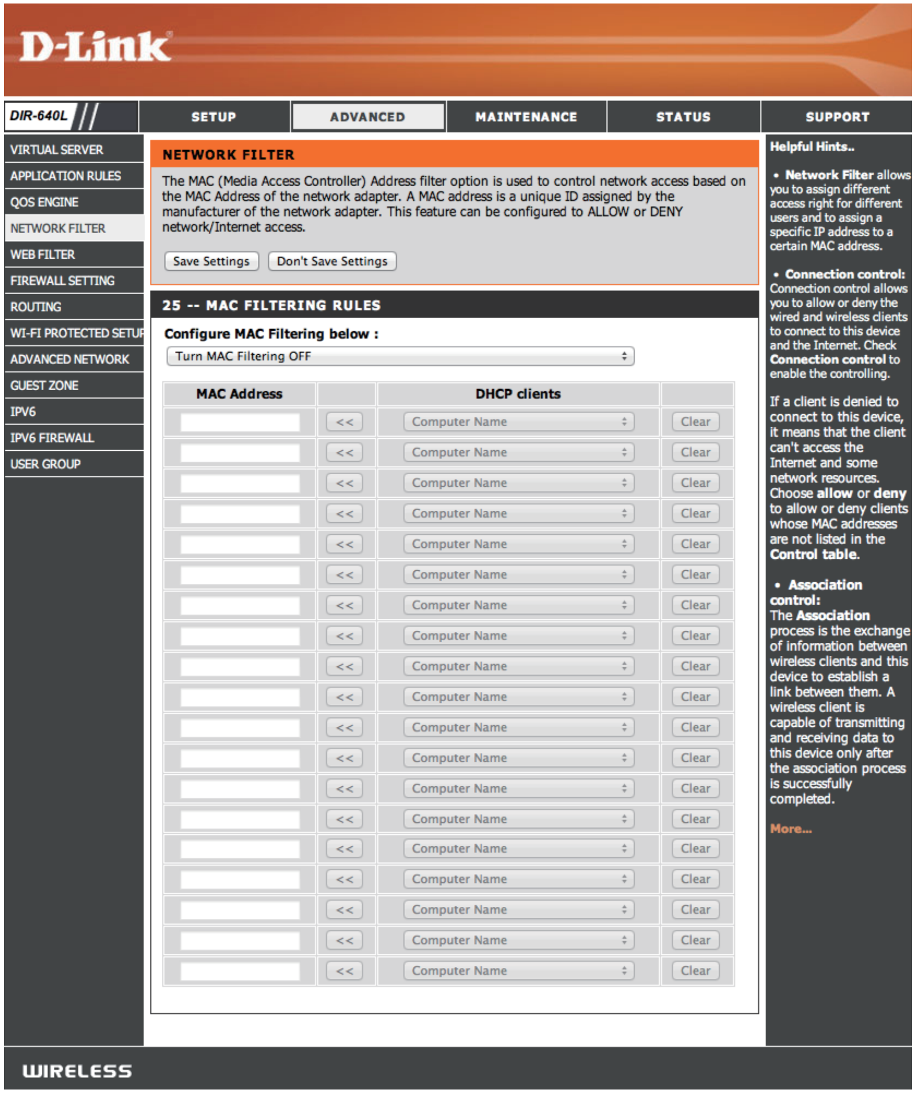
**Configure MAC Filtering:** Select **Turn MAC Filtering Off**, **Allow MAC addresses listed below**, or **Deny MAC addresses listed below** from the drop-down menu.

**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.

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



NETWORK FILTER

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

25 -- MAC FILTERING RULES

Configure MAC Filtering below :

Turn MAC Filtering OFF

| MAC Address | | DHCP clients | |
|---|---|---|---|
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |
| | << | Computer Name | Clear |

Helpful Hints..

- **Network Filter** allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- **Connection control:** Connection control allows you to allow or deny the wired and wireless clients to connect to this device and the Internet. Check **Connection control** to enable the controlling.

If a client is denied to connect to this device, it means that the client can't access the Internet and some network resources. Choose **allow** or **deny** to allow or deny clients whose MAC addresses are not listed in the **Control table.**

- **Association control:** The **Association** process is the exchange of information between wireless clients and this device to establish a link between them. A wireless client is capable of transmitting and receiving data to this device only after the association process is successfully completed.

More...

# Web Filter

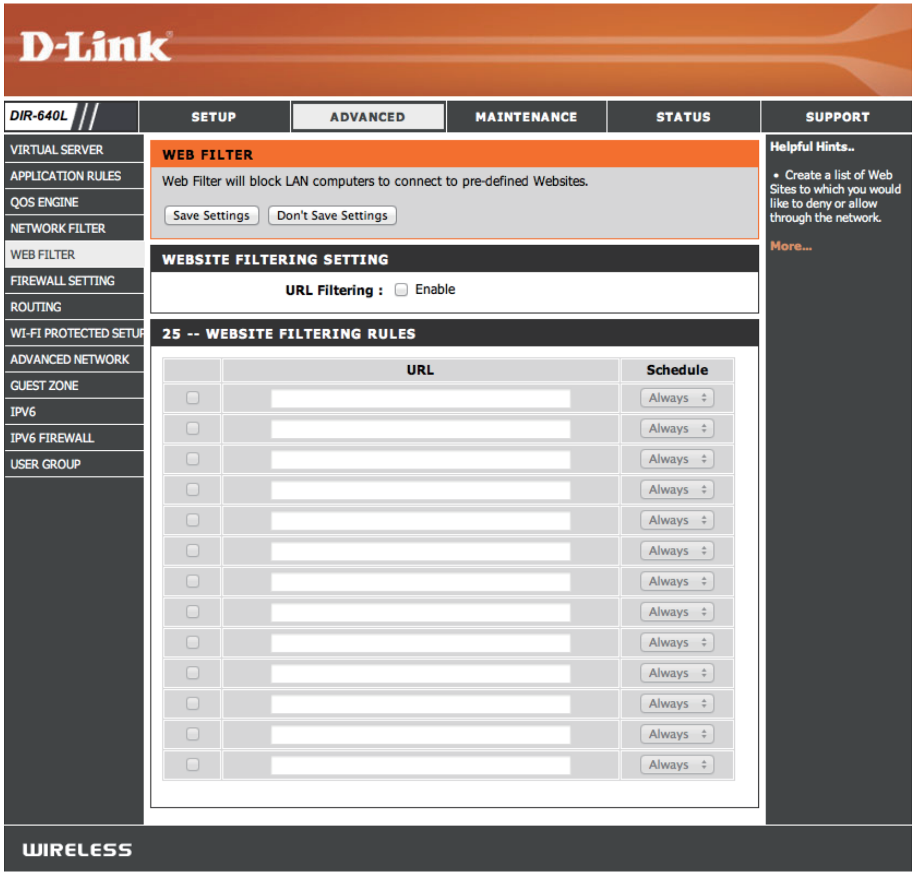
Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control*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

**URL Filtering:** Enable URL filtering by checking this box.

**Enable Rule:** Click to enable or disable a rule.

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

**Schedule:** Choose a schedule for the rule.



WEB FILTER

Web Filter will block LAN computers to connect to pre-defined Websites.

WEBSITE FILTERING SETTING

URL Filtering : □ Enable

25 -- WEBSITE FILTERING RULES

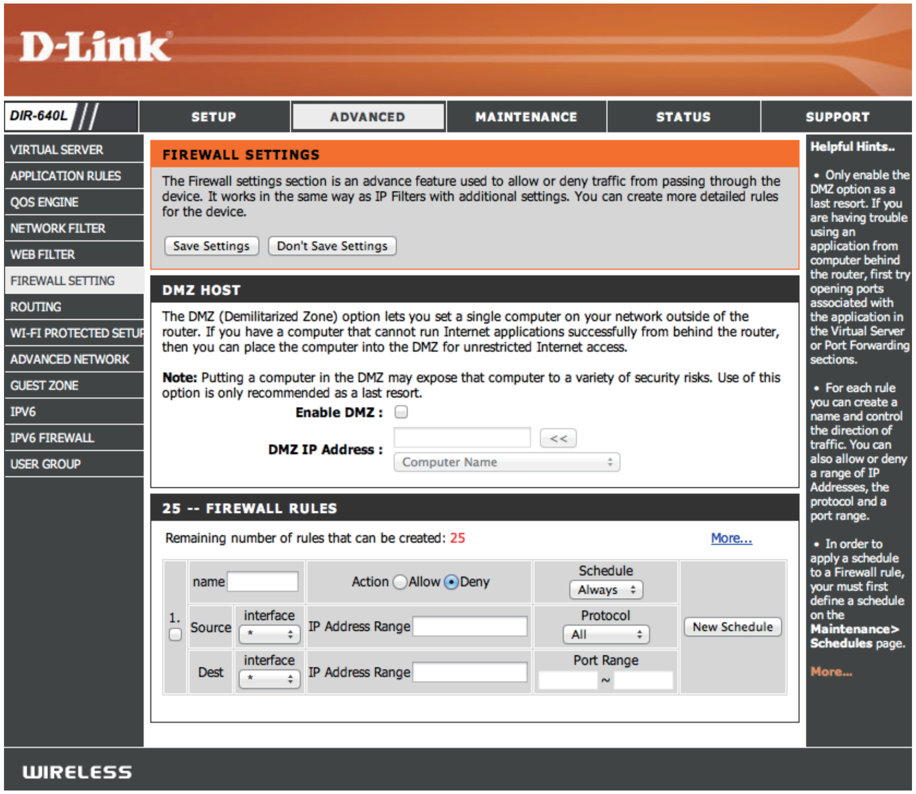
| | URL | Schedule |
|---|---|---|
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |
| □ | | Always |

Helpful Hints..

- Create a list of Web Sites to which you would like to deny or allow through the network.

# Firewall Setting

A firewall protects your network from the outside world. The DIR-640L 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.



**FIREWALL SETTINGS**

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

Save Settings | Don't Save Settings

**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

**25 -- FIREWALL RULES**

Remaining number of rules that can be created: 25 More...

| | | | | |
|---|---|---|---|---|
| 1. □ | name | Action ○ Allow ● Deny | Schedule<br>Always | |
| | Source interface * | IP Address Range | Protocol<br>All | New Schedule |
| | Dest interface * | IP Address Range | Port Range<br>~ | |

**Helpful Hints..**

- Only enable the DMZ option as a last resort. If you are having trouble using an application from computer behind the router, first try opening ports associated with the application in the Virtual Server or Port Forwarding sections.
- For each rule you can create a name and control the direction of traffic. You can also allow or deny a range of IP Addresses, the protocol and a port range.
- In order to apply a schedule to a Firewall rule, your must first define a schedule on the **Maintenance> Schedules** page.

More...

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

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

**DMZ IP Address:** Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains 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.

**Firewall Rules:** Choose whether to Allow or Deny the addresses you list below.

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

**Action:** Choose whether to Allow or Deny all of the rules listed below.

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

**Schedule:** Use the drop-down menu to select the time schedule that the IPv6 Firewall Rule will be enabled on. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.

**IP Address Range:** Enter the source **IP Address** range.

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

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

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

**New Schedule:** Click this button to create a new schedule.

# Routing

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

**Name:** Enter a name for your route.

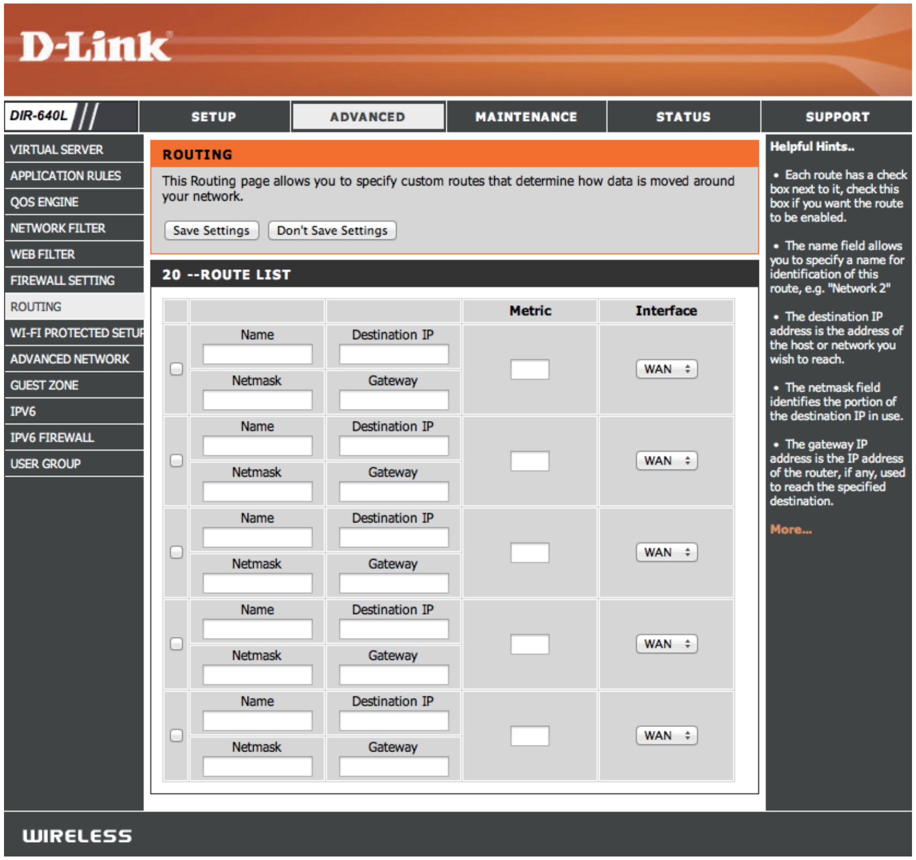
**Destination IP:** Enter the IP address of packets that will take this route.

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

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

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

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



ROUTING

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

20 --ROUTE LIST

| | | | Metric | Interface |
|---|---|---|---|---|
| □ | Name<br>Netmask | Destination IP<br>Gateway | | WAN |
| □ | Name<br>Netmask | Destination IP<br>Gateway | | WAN |
| □ | Name<br>Netmask | Destination IP<br>Gateway | | WAN |
| □ | Name<br>Netmask | Destination IP<br>Gateway | | WAN |
| □ | Name<br>Netmask | Destination IP<br>Gateway | | WAN |

Helpful Hints..

- Each route has a check box next to it, check this box if you want the route to be enabled.
- The name field allows you to specify a name for identification of this route, e.g. "Network 2"
- The destination IP address is the address of the host or network you wish to reach.
- The netmask field identifies the portion of the destination IP in use.
- The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

More...

# Advanced Network Settings

The Advanced Network Settings page offers additional feature options for power users.

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

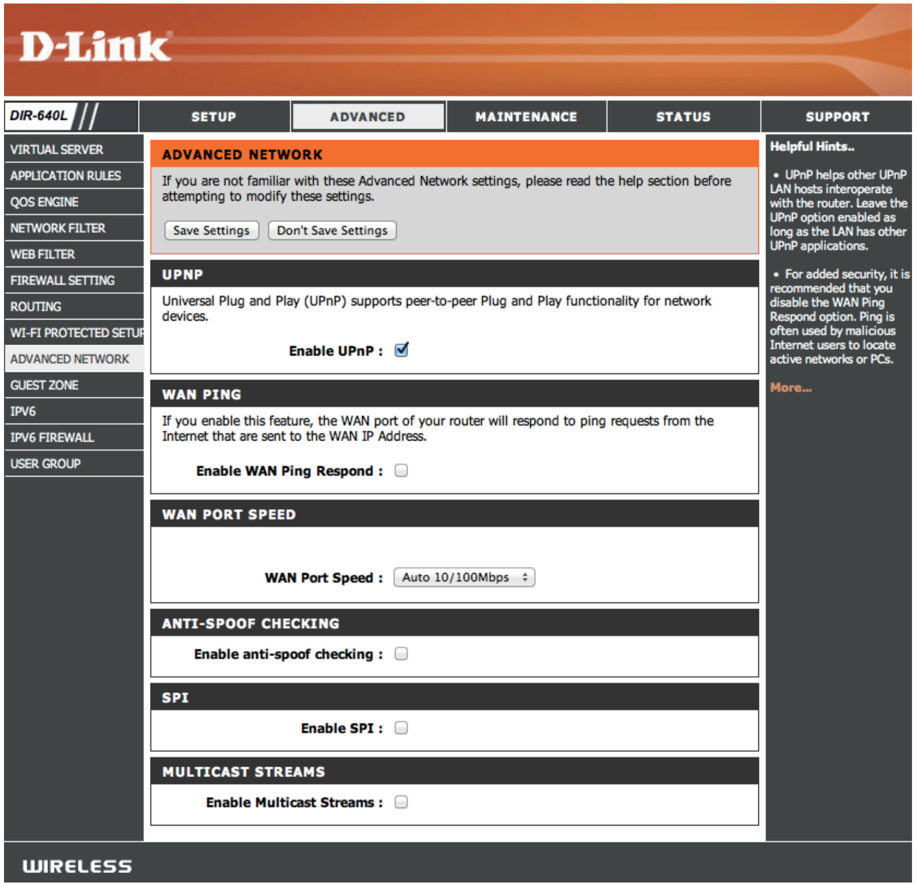
**Enable WAN Ping Respond:** Checking the box will allow the DIR-640L to respond to pings. Unchecking the box may provide some extra security from hackers.

**WAN Port Speed:** Choose your WAN port speed from the drop-down menu.

**Enable Anti-Spoof Checking:** Check this box to automatically check the origins of packets against a blacklist of known spoofers.

**Enable SPI:** Check this box to enable Stateful Packet Inspection which will only allow packets from known active connections and reject all others.

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



ADVANCED NETWORK

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

UPNP

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

Enable UPnP : ☑

WAN PING

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Respond : □

WAN PORT SPEED

WAN Port Speed : Auto 10/100Mbps

ANTI-SPOOF CHECKING

Enable anti-spoof checking : □

SPI

Enable SPI : □

MULTICAST STREAMS

Enable Multicast Streams : □

Helpful Hints..

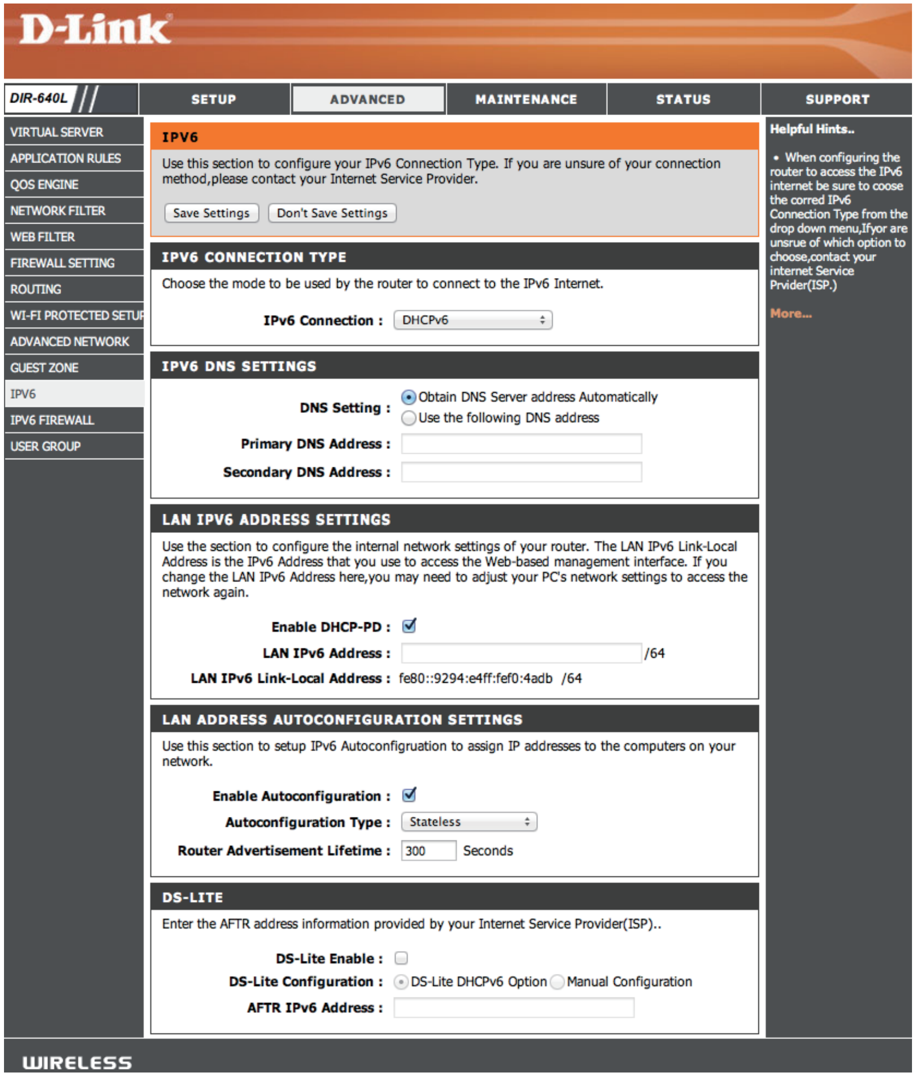
- UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.
- For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

# IPv6

There are several connection types to choose from: Static IPv6, DHCPv6, PPPoE, IPv6 in IPv4 Tunnel, 6to4, 6rd, and Link-local. If you are unsure of your connection method, please contact your IPv6 ISP.

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

Choose your IPv6 connection method from the drop-down menu under the IPv6 Connection Type.



**IPV6**

Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method,please contact your Internet Service Provider.

**IPV6 CONNECTION TYPE**

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

**IPv6 Connection :** DHCPv6

**IPV6 DNS SETTINGS**

**DNS Setting :** ● Obtain DNS Server address Automatically ○ Use the following DNS address

**Primary DNS Address :**

**Secondary DNS Address :**

**LAN IPV6 ADDRESS SETTINGS**

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

**Enable DHCP-PD :** ☑

**LAN IPv6 Address :** /64

**LAN IPv6 Link-Local Address :** fe80::9294:e4ff:fef0:4adb /64

**LAN ADDRESS AUTOCONFIGURATION SETTINGS**

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

**Enable Autoconfiguration :** ☑

**Autoconfiguration Type :** Stateless

**Router Advertisement Lifetime :** 300 Seconds

**DS-LITE**

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

**DS-Lite Enable :** □

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

**AFTR IPv6 Address :**

**Helpful Hints..**

- When configuring the router to access the IPv6 internet be sure to coose the corred IPv6 Connection Type from the drop down menu,Ifyor are unsrue of which option to choose,contact your internet Service Prvider(ISP.)

# 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).

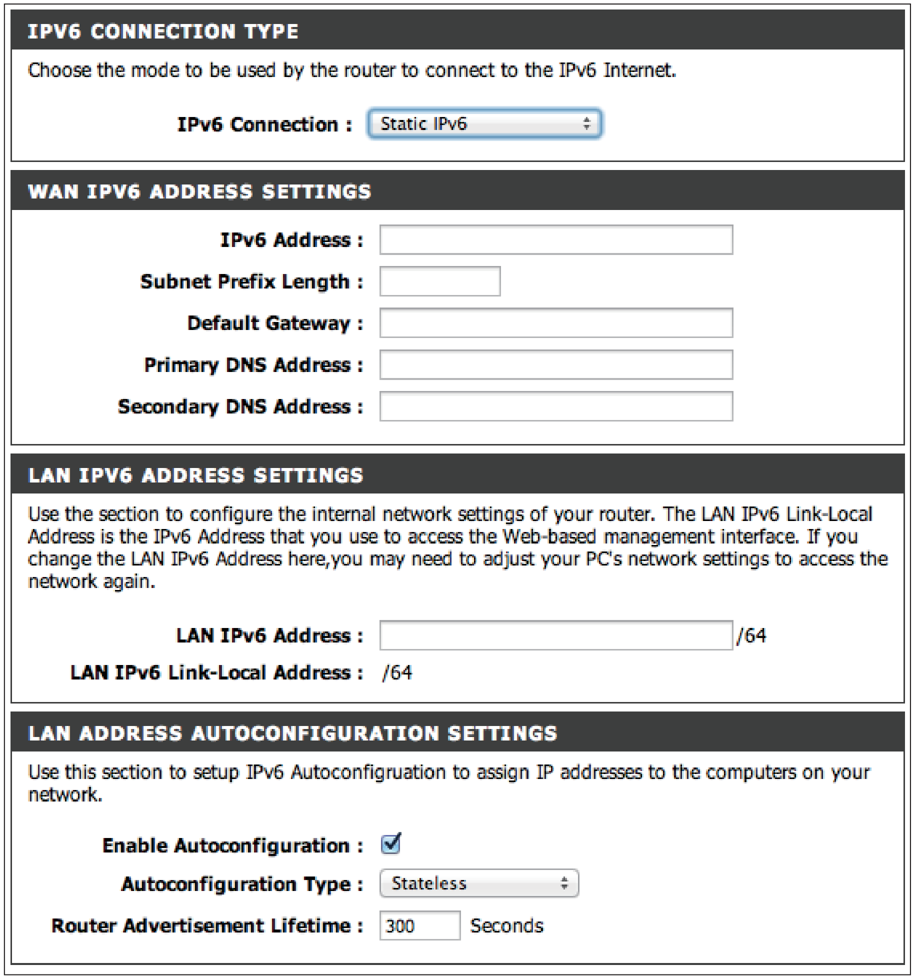
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

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

**Autoconfiguration Type:** Select **Stateful** or **Stateless** autoconfiguration.

**Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).



IPV6 CONNECTION TYPE

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

IPv6 Connection : Static IPv6

WAN IPV6 ADDRESS SETTINGS

IPv6 Address :

Subnet Prefix Length :

Default Gateway :

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration : ☑

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : 300 Seconds

# DHCP

**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.

**Enable DHCP-PD** Check to enable DHCP-PD.

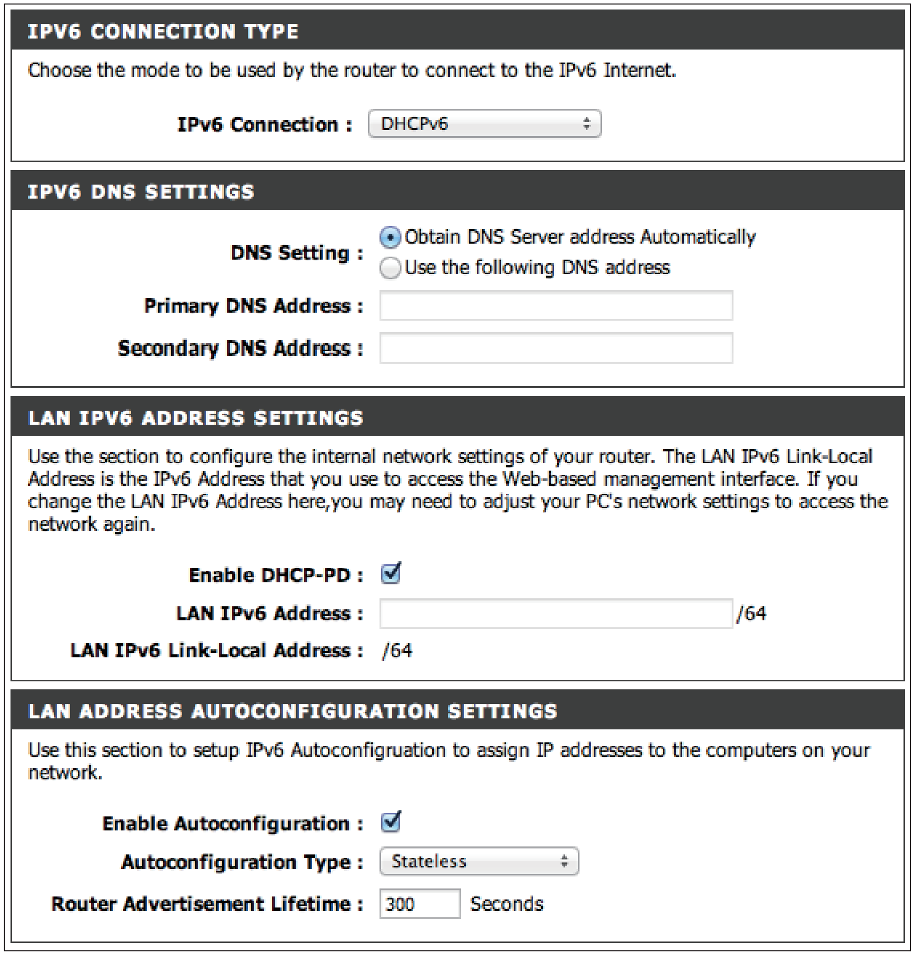
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

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

**Autoconfiguration Type:** Select **Stateful** or **Stateless** autoconfiguration.

**Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).



IPV6 CONNECTION TYPE

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

IPv6 Connection : DHCPv6

IPV6 DNS SETTINGS

DNS Setting : ● Obtain DNS Server address Automatically ○ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration : ☑

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : 300 Seconds

# PPPoE

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

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

**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).

**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.

**Enable DHCP-PD** Check to enable DHCP-PD.

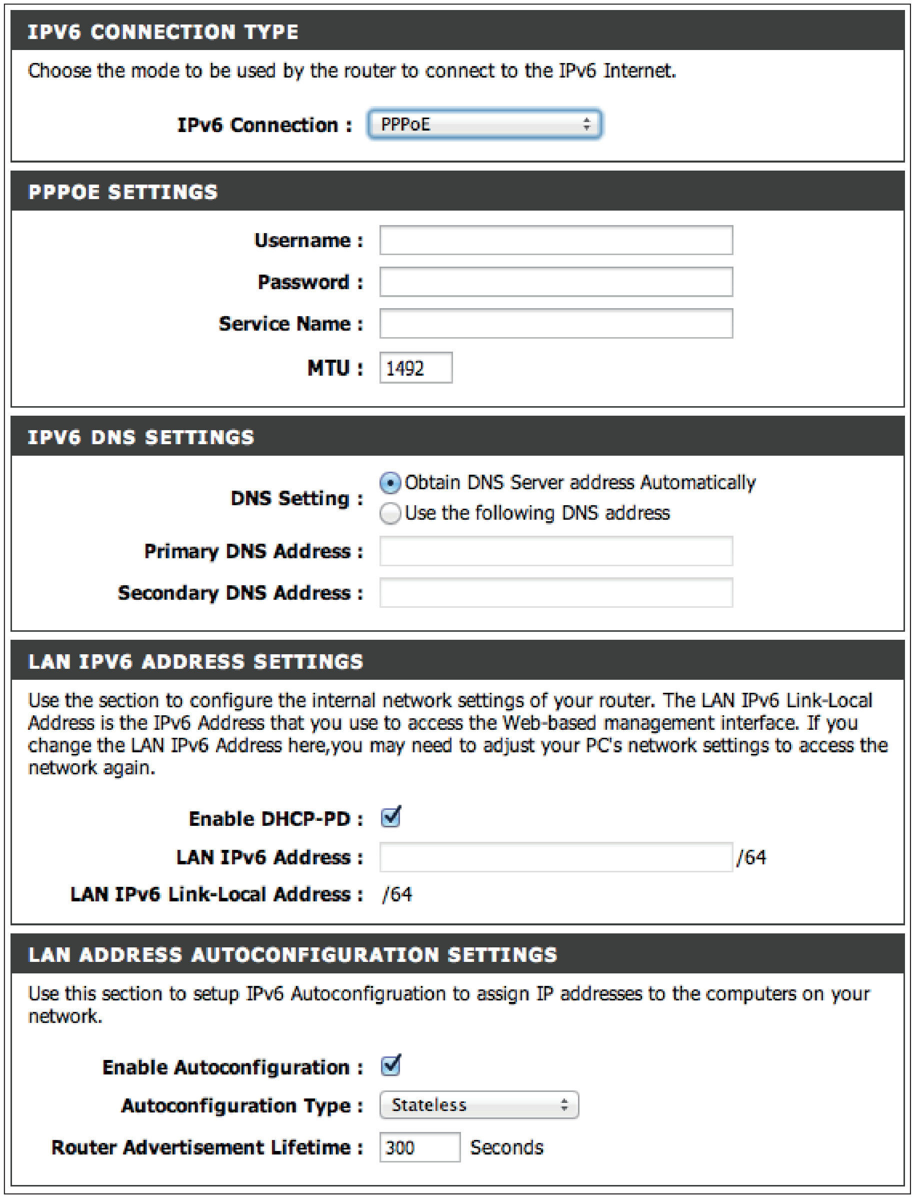
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

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

**Autoconfiguration Type:** Select **Stateful** or **Stateless** autoconfiguration.

**Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).



IPV6 CONNECTION TYPE

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

IPv6 Connection : PPPoE

PPPOE SETTINGS

Username :

Password :

Service Name :

MTU : 1492

IPV6 DNS SETTINGS

DNS Setting : ● Obtain DNS Server address Automatically
○ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration : ☑

Autoconfiguration Type : Stateless

Router Advertisement Lifetime : 300 Seconds

# IPv6 over IPv4 Tunneling

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

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

**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.

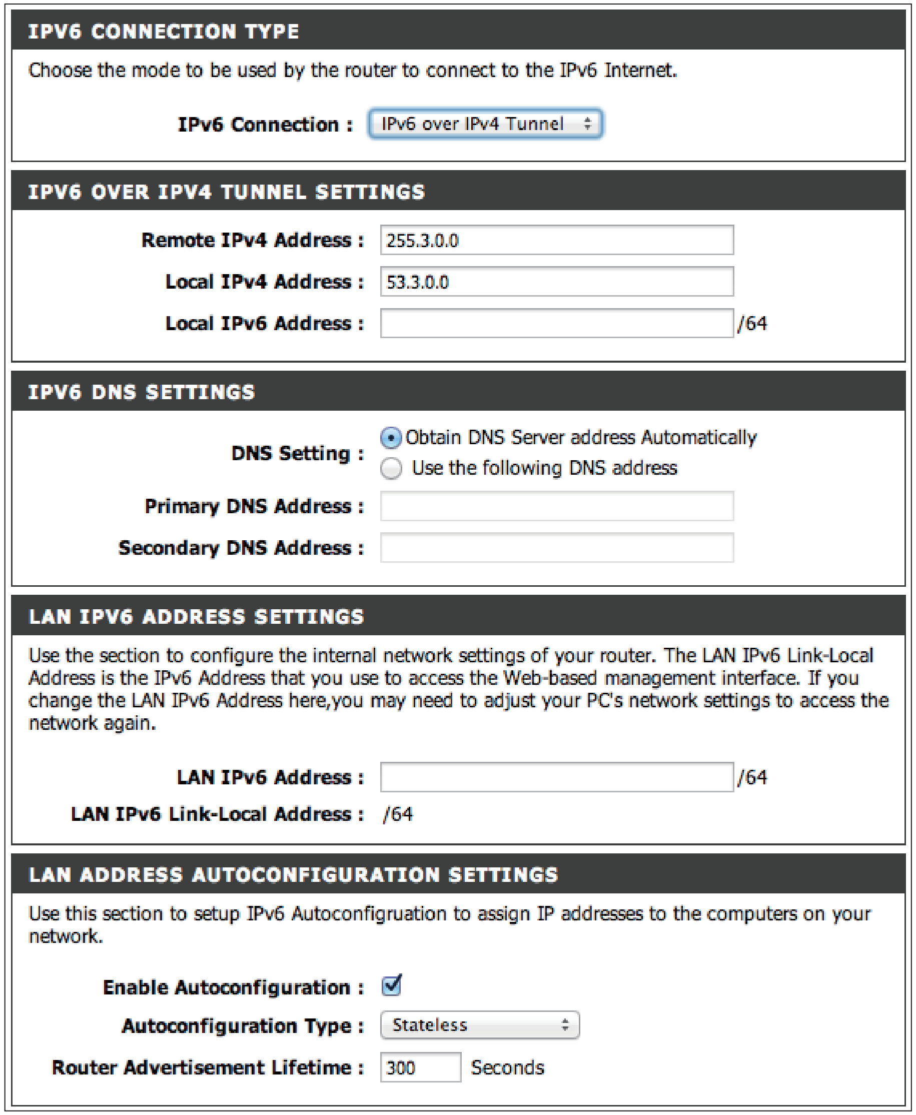
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

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

**Autoconfiguration Type:** Select **Stateful** or **Stateless** autoconfiguration.

**Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).



**IPV6 CONNECTION TYPE**

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

**IPv6 Connection :** IPv6 over IPv4 Tunnel

**IPV6 OVER IPV4 TUNNEL SETTINGS**

**Remote IPv4 Address :** 255.3.0.0

**Local IPv4 Address :** 53.3.0.0

**Local IPv6 Address :** /64

**IPV6 DNS SETTINGS**

**DNS Setting :** ● Obtain DNS Server address Automatically ○ Use the following DNS address

**Primary DNS Address :**

**Secondary DNS Address :**

**LAN IPV6 ADDRESS SETTINGS**

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

**LAN IPv6 Address :** /64

**LAN IPv6 Link-Local Address :** /64

**LAN ADDRESS AUTOCONFIGURATION SETTINGS**

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

**Enable Autoconfiguration :** ☑

**Autoconfiguration Type :** Stateless

**Router Advertisement Lifetime :** 300 Seconds

# 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.

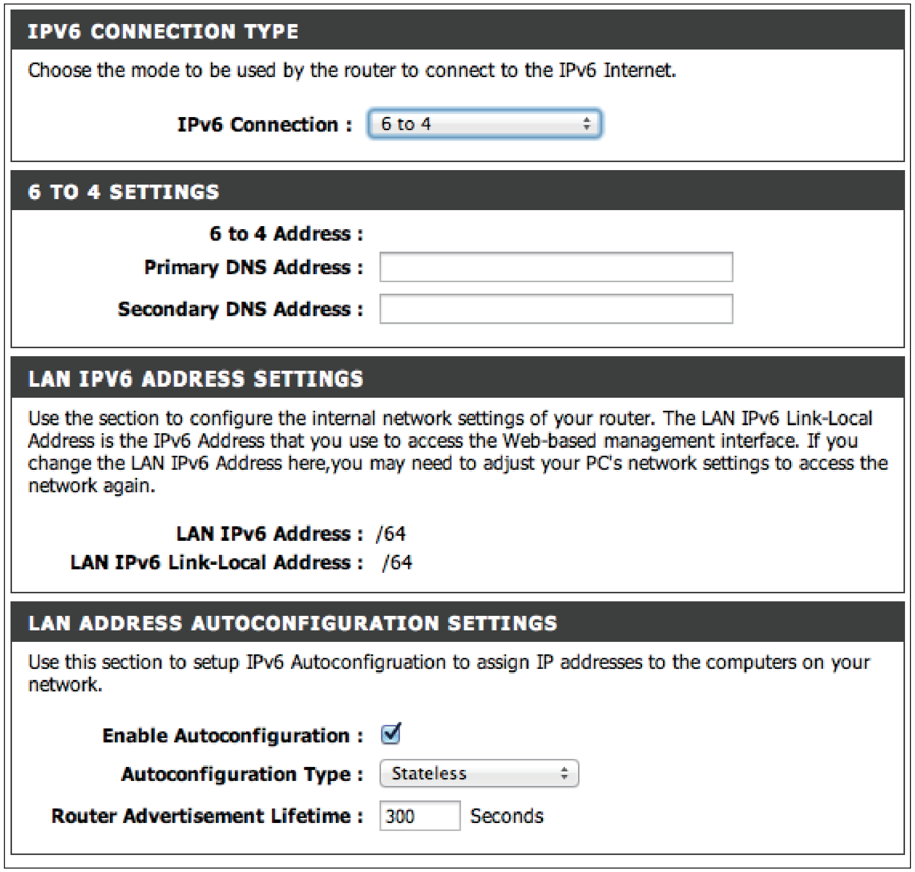
**LAN IPv6 Address:** Displays the LAN (local) IPv6 address for the router.

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

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

**Autoconfiguration Type:** Select **Stateful** or **Stateless** autoconfiguration.

**Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).



**IPV6 CONNECTION TYPE**

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

**IPv6 Connection :** 6 to 4

**6 TO 4 SETTINGS**

**6 to 4 Address :**
**Primary DNS Address :**
**Secondary DNS Address :**

**LAN IPV6 ADDRESS SETTINGS**

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

**LAN IPv6 Address :** /64
**LAN IPv6 Link-Local Address :** /64

**LAN ADDRESS AUTOCONFIGURATION SETTINGS**

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

**Enable Autoconfiguration :** ☑
**Autoconfiguration Type :** Stateless
**Router Advertisement Lifetime :** 300 Seconds

# 6rd

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

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

**Remote IPv4 Address:** Enter the IPv4 (remote) address here.

**IPv4 Mask Length:** Enter the mask length of the IPv4 address.

**Remote Prefix:** Enter the remote prefix of the IPv4 address.

**Prefix Length:** Enter the length of the remote prefix.

**Primary/Secondary DNS Addresses:** Enter the DNS server addresses.

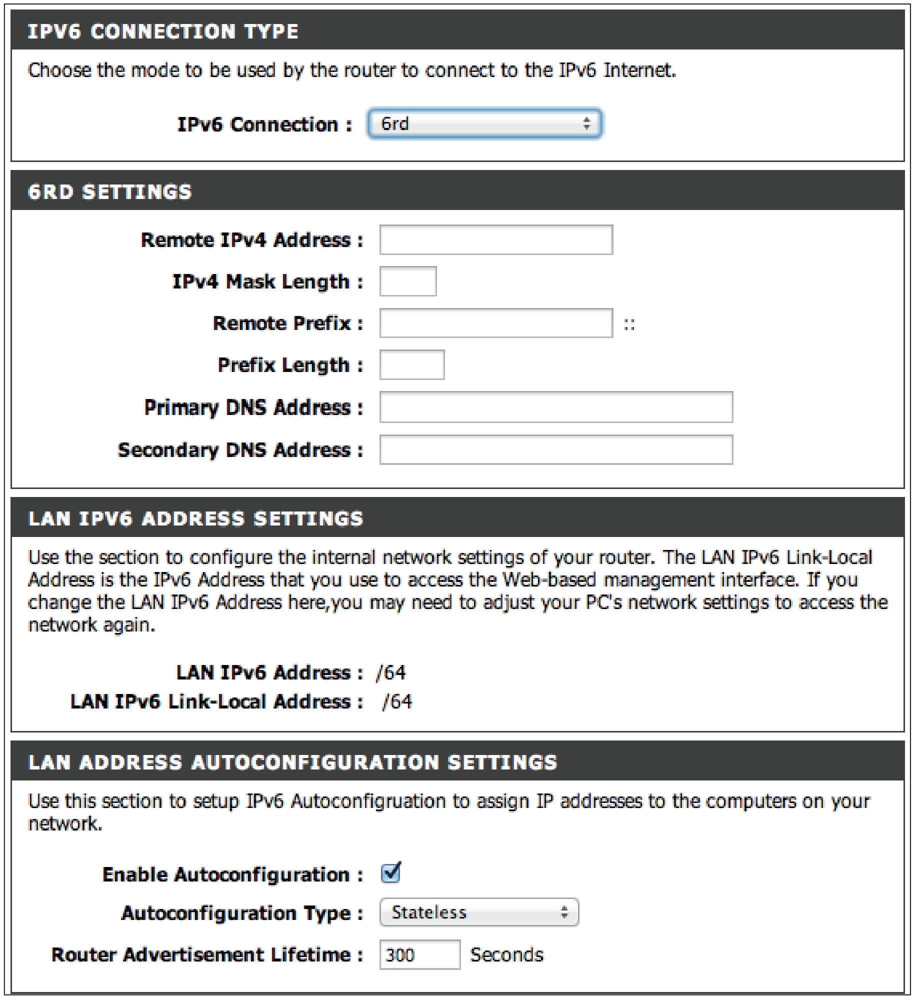
**LAN IPv6 Address:** Displays the LAN (local) IPv6 address for the router.

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

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

**Autoconfiguration Type:** Select **Stateful** or **Stateless** autoconfiguration.

**Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).



IPV6 CONNECTION TYPE

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

IPv6 Connection : 6rd

6RD SETTINGS

Remote IPv4 Address :

IPv4 Mask Length :

Remote Prefix : ::

Prefix Length :

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration : ☑

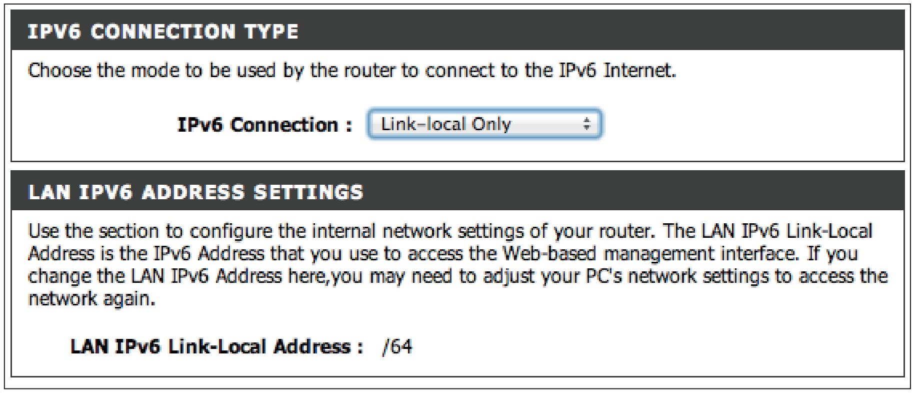
Autoconfiguration Type : Stateless

Router Advertisement Lifetime : 300 Seconds

# 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 connect to the IPv6 Internet.

IPv6 Connection : Link-local Only

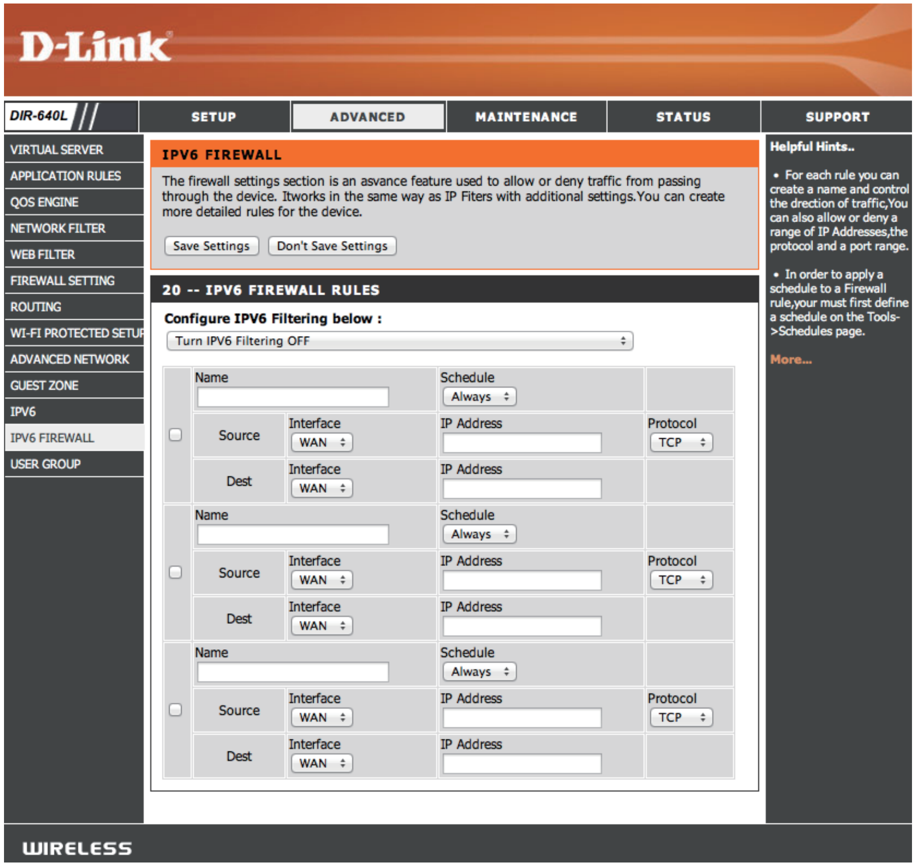
LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Link-Local Address : /64

# IPv6 Firewall

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



**IPV6 FIREWALL**

The firewall settings section is an asvance feature used to allow or deny traffic from passing through the device. Itworks in the same way as IP Fiters with additional settings.You can create more detailed rules for the device.

**20 -- IPV6 FIREWALL RULES**

**Configure IPV6 Filtering below :**

Turn IPV6 Filtering OFF

| | | | | |
|---|---|---|---|---|
| ☐ | Name | | Schedule: Always | |
| | Source | Interface: WAN | IP Address | Protocol: TCP |
| | Dest | Interface: WAN | IP Address | |
| ☐ | Name | | Schedule: Always | |
| | Source | Interface: WAN | IP Address | Protocol: TCP |
| | Dest | Interface: WAN | IP Address | |
| ☐ | Name | | Schedule: Always | |
| | Source | Interface: WAN | IP Address | Protocol: TCP |
| | Dest | Interface: WAN | IP Address | |

**Helpful Hints..**

- For each rule you can create a name and control the drection of traffic,You can also allow or deny a range of IP Addresses,the protocol and a port range.
- In order to apply a schedule to a Firewall rule,your must first define a schedule on the Tools->Schedules page.

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

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

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

**Schedule:** Use the drop-down menu to select the time schedule that the IPv6 Firewall Rule will be enabled on. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.

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

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

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

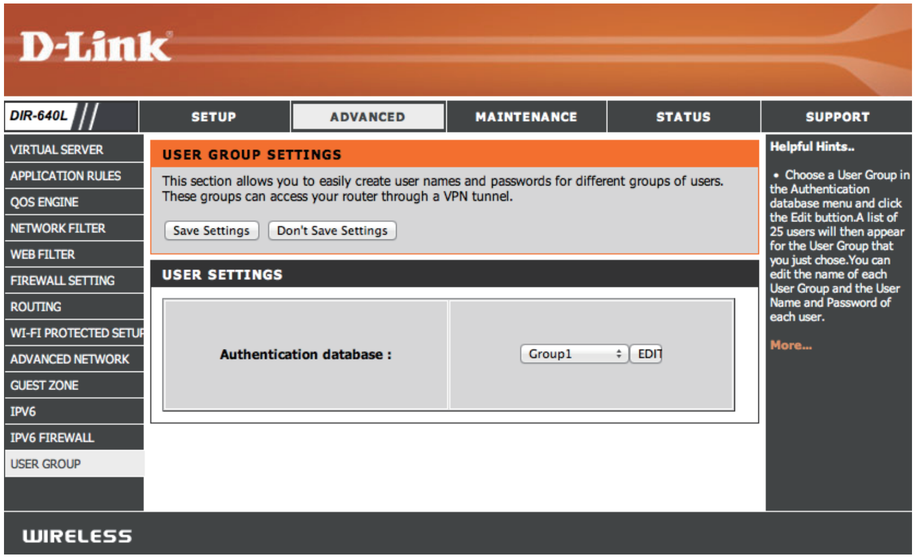
**Protocol:** Select the protocol of the firewall port (**All**, **TCP**, **UDP**, or **ICMP**). Enter the first port of the range that will be used for the firewall rule in the first box and enter the last port in the field in the second box.

# User Group

The User Group feature allows you to select an authentification database to store a group of user settings

**User Settings:** Here you will find a list of Authetification databases you have created.

**Authentification database:** Choose a database from the drop-down menu and choose Edit to make changes.



USER GROUP SETTINGS

This section allows you to easily create user names and passwords for different groups of users. These groups can access your router through a VPN tunnel.

USER SETTINGS

Authentication database : Group1

Helpful Hints..

- Choose a User Group in the Authentication database menu and click the Edit buttion.A list of 25 users will then appear for the User Group that you just chose.You can edit the name of each User Group and the User Name and Password of each user.

# Maintenance

## Admin

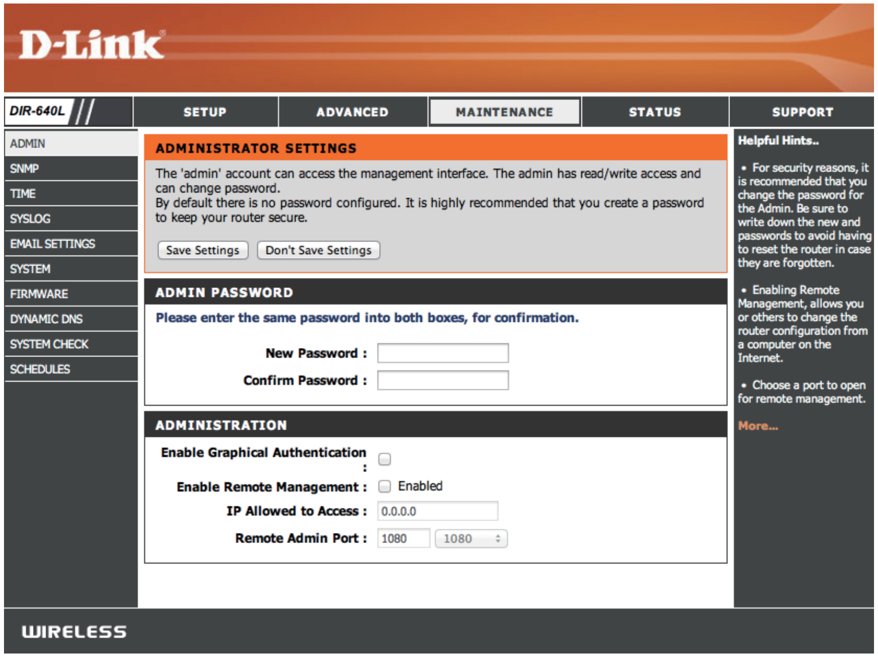
This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can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

**Admin Password:** Enter a new password for the Administrator Login Name. And type it again in the next box.

**Enable Remote Management:** Remote management allows the DIR-640L to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

**IP Allowed to Access:** Enter the IP address used to access the DIR-640L.

**Remote Admin Port:** Enter the port number used to access the DIR-640L is used in the URL. Example: **http://x.x.x.x:8080** whereas x.x.x.x is the Internet IP address of the DIR-640L and 8080 is the port used for the Web Management interface.



ADMINISTRATOR SETTINGS

The 'admin' account can access the management interface. The admin has read/write access and can change password.
By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

ADMIN PASSWORD

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

New Password :
Confirm Password :

ADMINISTRATION

Enable Graphical Authentication : □
Enable Remote Management : □ Enabled
IP Allowed to Access : 0.0.0.0
Remote Admin Port : 1080 1080

Helpful Hints..

- For security reasons, it is recommended that you change the password for the Admin. Be sure to write down the new and passwords to avoid having to reset the router in case they are forgotten.
- Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet.
- Choose a port to open for remote management.

# SNMP

The DIR-640L allows you to use the Simple Network Management Protocol for easy management of your network.

**SNMPLocal:** Enable this option to allow local SNMP management.

**SNMPLocal:** Enable this option to allow remote SNMP management.

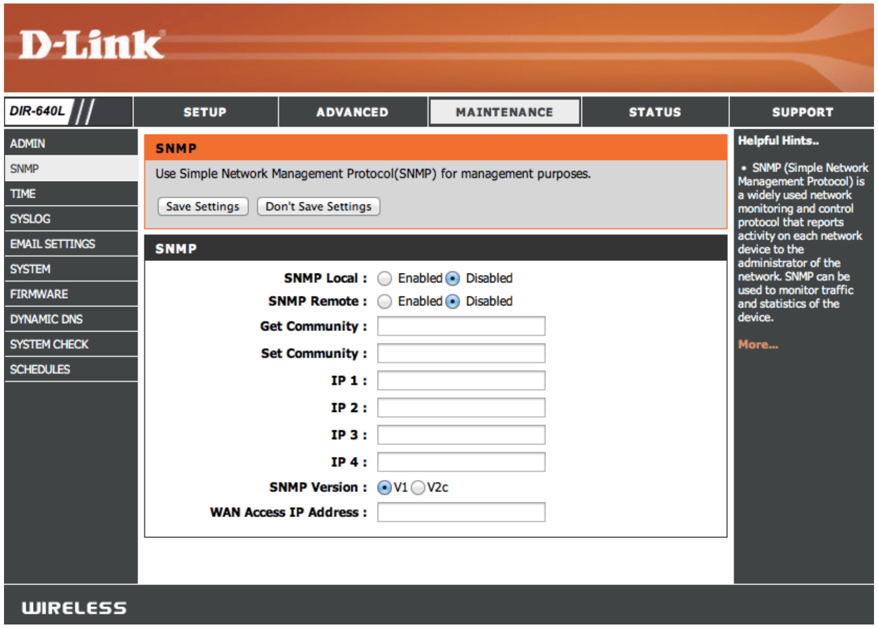
**Get Community:** Enter a name for the read community of your SNMP server.

**Set Community:** Enter a name for the write community of your SNMP server.

**IP1-4:** Set up to four IP addresses to be managed here.

**SNMP Variation:** Choose the version of SNMP to be used by your server V1 or V2c..

**WAN Access IP Address:** Enter the IP address used for WAN access here.



**SNMP**

Use Simple Network Management Protocol(SNMP) for management purposes.

**SNMP**

**SNMP Local :** ○ Enabled ● Disabled
**SNMP Remote :** ○ Enabled ● Disabled
**Get Community :**
**Set Community :**
**IP 1 :**
**IP 2 :**
**IP 3 :**
**IP 4 :**
**SNMP Version :** ● V1 ○ V2c
**WAN Access IP Address :**

**Helpful Hints..**

- SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the device.

# Time

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

**Current Router Time:** Displays the current date and time of the router.

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

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

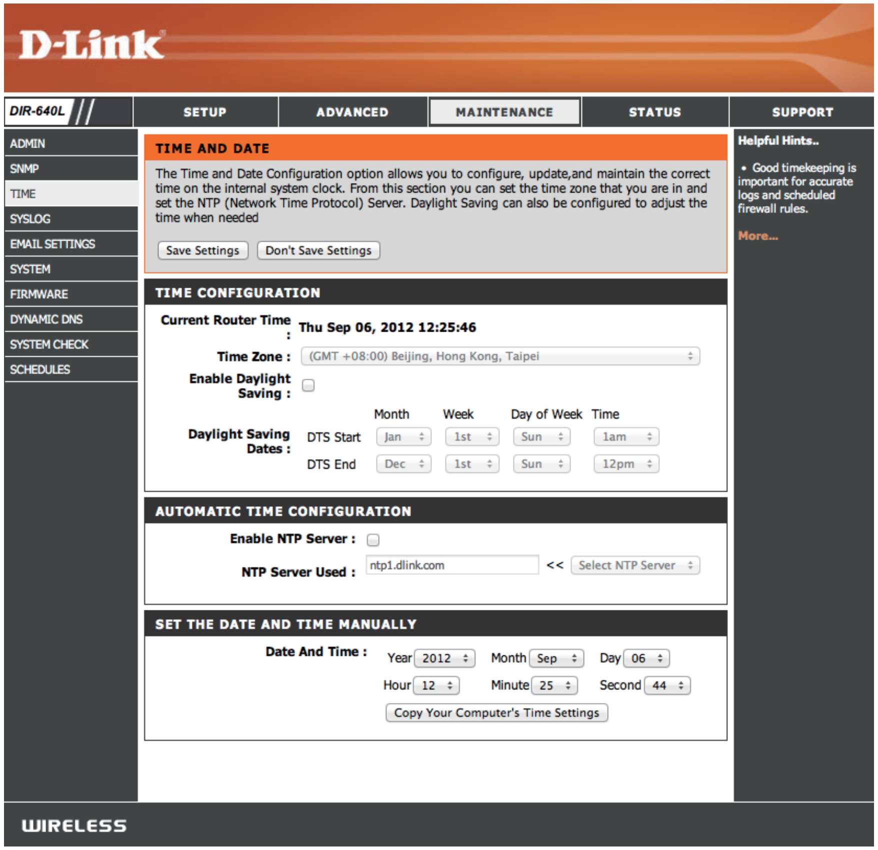
**Daylight Saving Dates:** If Daylight Saving is enabled, you may specify the date it begins and ends.

**Enable NTP Server:** NTP is short for Network Time Protocol. A NTP server will synch the time and date with your router. This will only connect to a server on the Internet, not a local server. Check the box to enable this feature.

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

**Date And Time:** To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Set Time**.

You can also click **Copy Your Computer's Time Settings** to synch the date and time with the computer you are currently on.



TIME AND DATE

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

TIME CONFIGURATION

Current Router Time : Thu Sep 06, 2012 12:25:46

Time Zone : (GMT +08:00) Beijing, Hong Kong, Taipei

Enable Daylight Saving : □

Daylight Saving Dates :

|  | Month | Week | Day of Week | Time |
|---|---|---|---|---|
| DTS Start | Jan | 1st | Sun | 1am |
| DTS End | Dec | 1st | Sun | 12pm |

AUTOMATIC TIME CONFIGURATION

Enable NTP Server : □

NTP Server Used : ntp1.dlink.com << Select NTP Server

SET THE DATE AND TIME MANUALLY

Date And Time : Year 2012 Month Sep Day 06 Hour 12 Minute 25 Second 44

Helpful Hints..

- Good timekeeping is important for accurate logs and scheduled firewall rules.

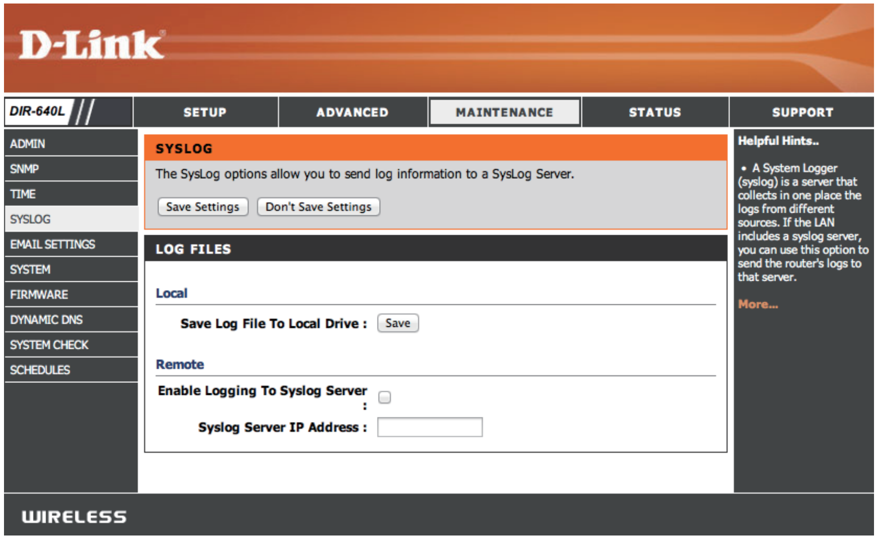
# SysLog

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

**Save Log File To Local Drive:** Click the **Save** button to save a local copy of the Log file on your PC.

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

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



SYSLOG

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

LOG FILES

Local

Save Log File To Local Drive :

Remote

Enable Logging To Syslog Server : □

Syslog Server IP Address :

Helpful Hints..

- A System Logger (syslog) is a server that collects in one place the logs from different sources. If the LAN includes a syslog server, you can use this option to send the router's logs to that server.

# Email Settings

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

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

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

**SMTP Server Address:** Enter the SMTP server address for sending email.

**SMTP Server Port:** Enter the SMTP port used on the server.

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

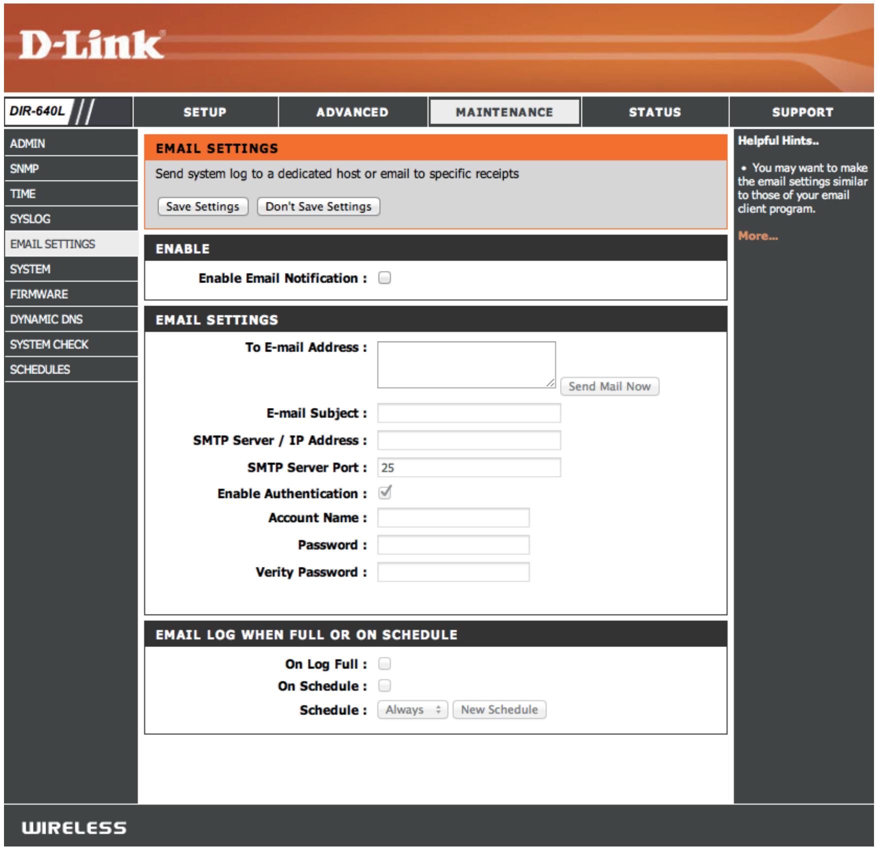
**Account Name:** Enter your account for sending email.

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

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

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

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



EMAIL SETTINGS

Send system log to a dedicated host or email to specific receipts

ENABLE

Enable Email Notification : □

EMAIL SETTINGS

To E-mail Address :

E-mail Subject :

SMTP Server / IP Address :

SMTP Server Port : 25

Enable Authentication : ☑

Account Name :

Password :

Verity Password :

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full : □

On Schedule : □

Schedule : Always

Helpful Hints..

- You may want to make the email settings similar to those of your email client program.

# System

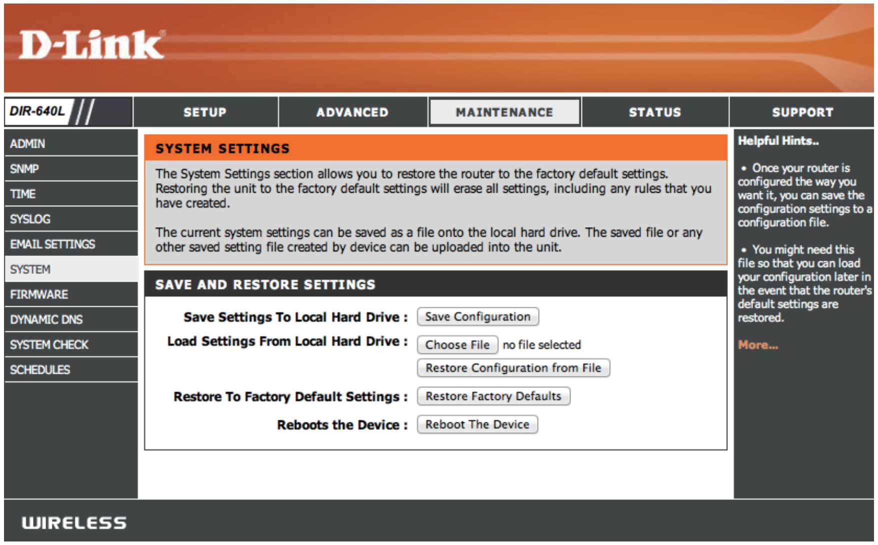
This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

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

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

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

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



SYSTEM SETTINGS

The System Settings section allows you to restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

SAVE AND RESTORE SETTINGS

Save Settings To Local Hard Drive : Save Configuration

Load Settings From Local Hard Drive : Choose File no file selected

Restore Configuration from File

Restore To Factory Default Settings : Restore Factory Defaults

Reboots the Device : Reboot The Device

Helpful Hints..

- Once your router is configured the way you want it, you can save the configuration settings to a configuration file.
- You might need this file so that you can load your configuration later in the event that the router's default settings are restored.

More...

# Firmware

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

**Check Now:** Click **Check Now** to check for new firmware and language pack versions online.

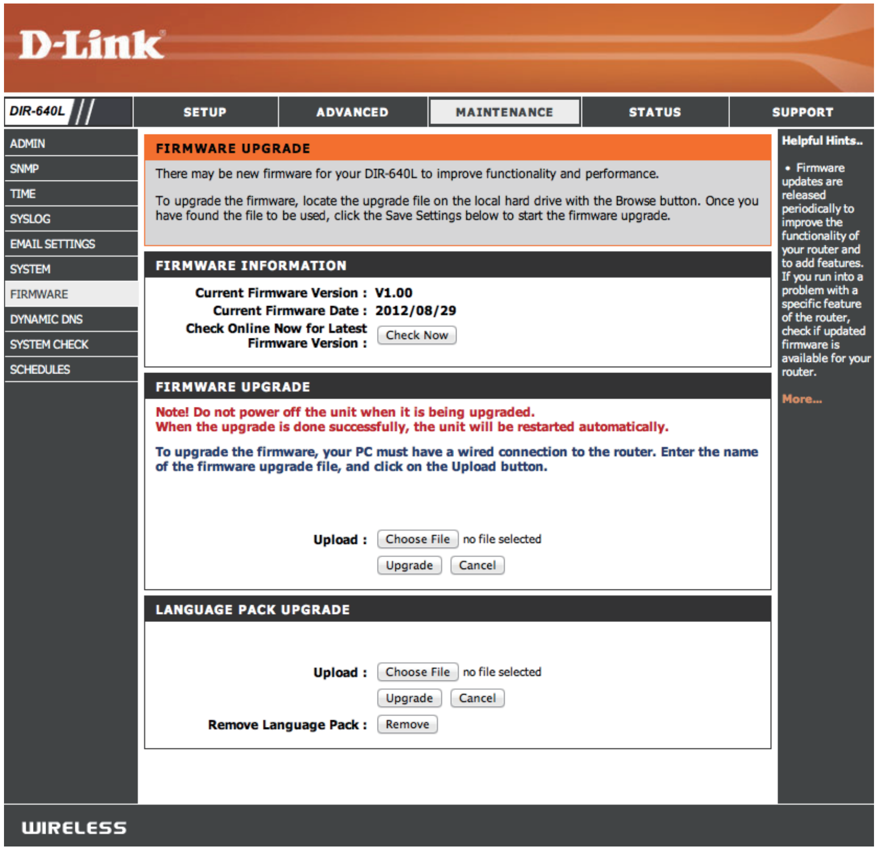
**Choose File:** After you have downloaded the new firmware, click **Choose File** to locate the firmware update on your hard drive.

**Upgrade:** Click **Upgrade** to complete the firmware upgrade.

**Choose File:** After you have downloaded the new language pack, click **Choose File** to locate the language pack file on your hard drive.

**Upgrade:** Click **Upgrade** to complete the language pack upgrade.

**Remove:** Click **Remove** to delete an installed Language Pack.



FIRMWARE UPGRADE

There may be new firmware for your DIR-640L to improve functionality and performance.

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

FIRMWARE INFORMATION

Current Firmware Version : V1.00
Current Firmware Date : 2012/08/29
Check Online Now for Latest Firmware Version :

FIRMWARE UPGRADE

Note! Do not power off the unit when it is being upgraded.
When the upgrade is done successfully, the unit will be restarted automatically.

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

Upload : no file selected

LANGUAGE PACK UPGRADE

Upload : no file selected

Remove Language Pack :

Helpful Hints..

- Firmware updates are released periodically to improve the functionality of your router and to add features. If you run into a problem with a specific feature of the router, check if updated firmware is available for your router.

# Dynamic DNS

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

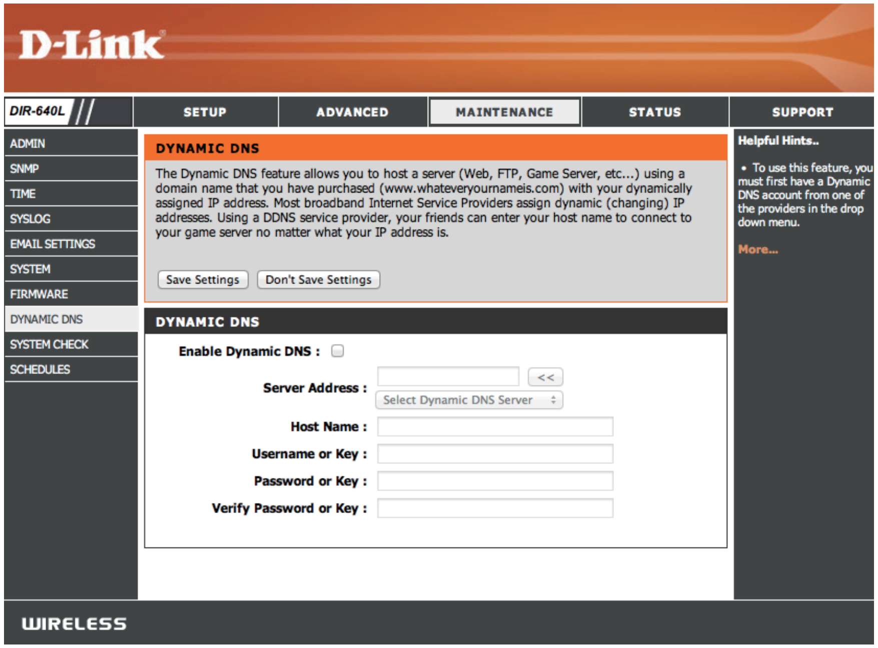
**Enable Dynamic DNS:** Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.

**Server Address:** Select your DDNS provider from the drop-down menu or enter the DDNS server address.

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

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

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



DYNAMIC DNS

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

DYNAMIC DNS

Enable Dynamic DNS : □

Server Address : Select Dynamic DNS Server

Host Name :

Username or Key :

Password or Key :

Verify Password or Key :

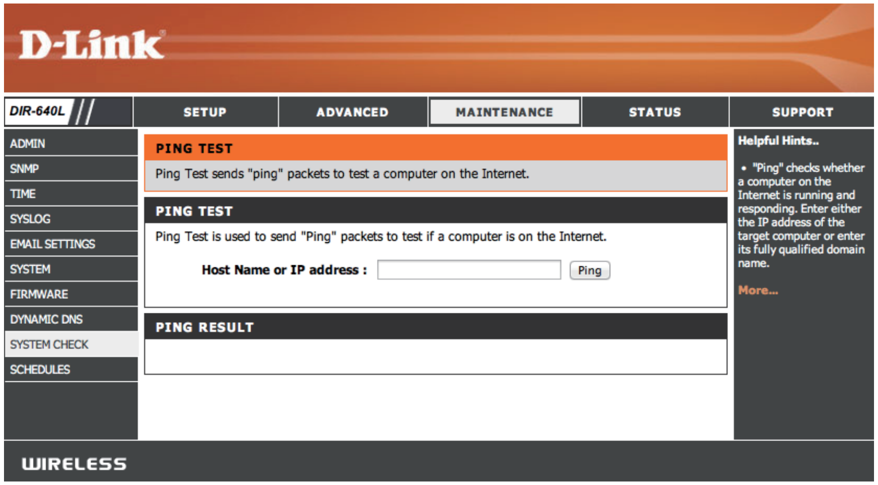
Helpful Hints..

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

# System Check

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

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



PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Ping Test is used to send "Ping" packets to test if a computer is on the Internet.

Host Name or IP address :

PING RESULT

Helpful Hints..

- "Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.

# Schedule

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

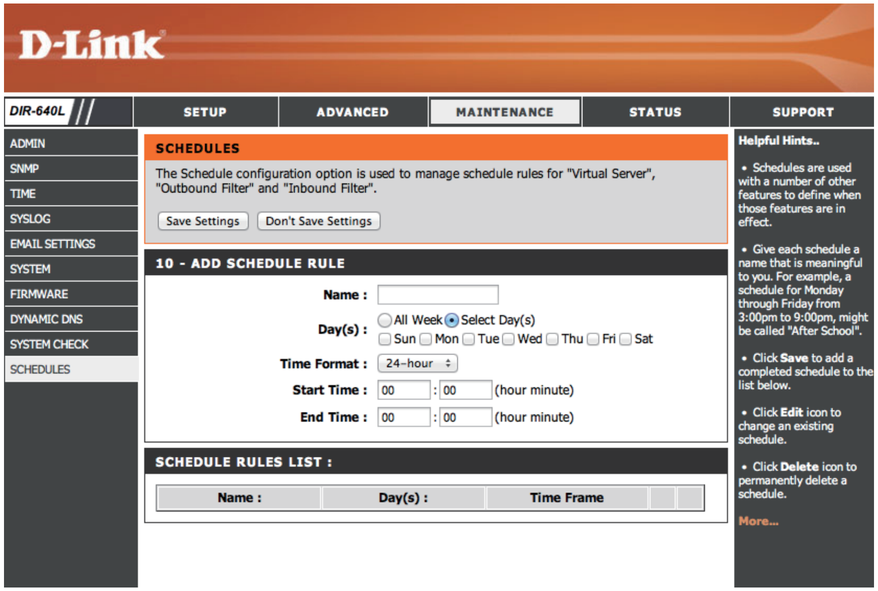
**Days:** Select a day, a range of days, or All Week to include every day.

**Time Format:** Choose a 24 hour or 12 hour clock-style.

**Start Time:** Enter a start time for your schedule.

**End Time:** Enter an end time for your schedule.

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



SCHEDULES

The Schedule configuration option is used to manage schedule rules for "Virtual Server", "Outbound Filter" and "Inbound Filter".

10 - ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time Format : 24-hour

Start Time : 00 : 00 (hour minute)

End Time : 00 : 00 (hour minute)

SCHEDULE RULES LIST :

| Name : | Day(s) : | Time Frame | | |
|---|---|---|---|---|

Helpful Hints..

- Schedules are used with a number of other features to define when those features are in effect.
- Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".
- Click **Save** to add a completed schedule to the list below.
- Click **Edit** icon to change an existing schedule.
- Click **Delete** icon to permanently delete a schedule.

# Status

## Device Info

This page displays the current information for the DIR-640L. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

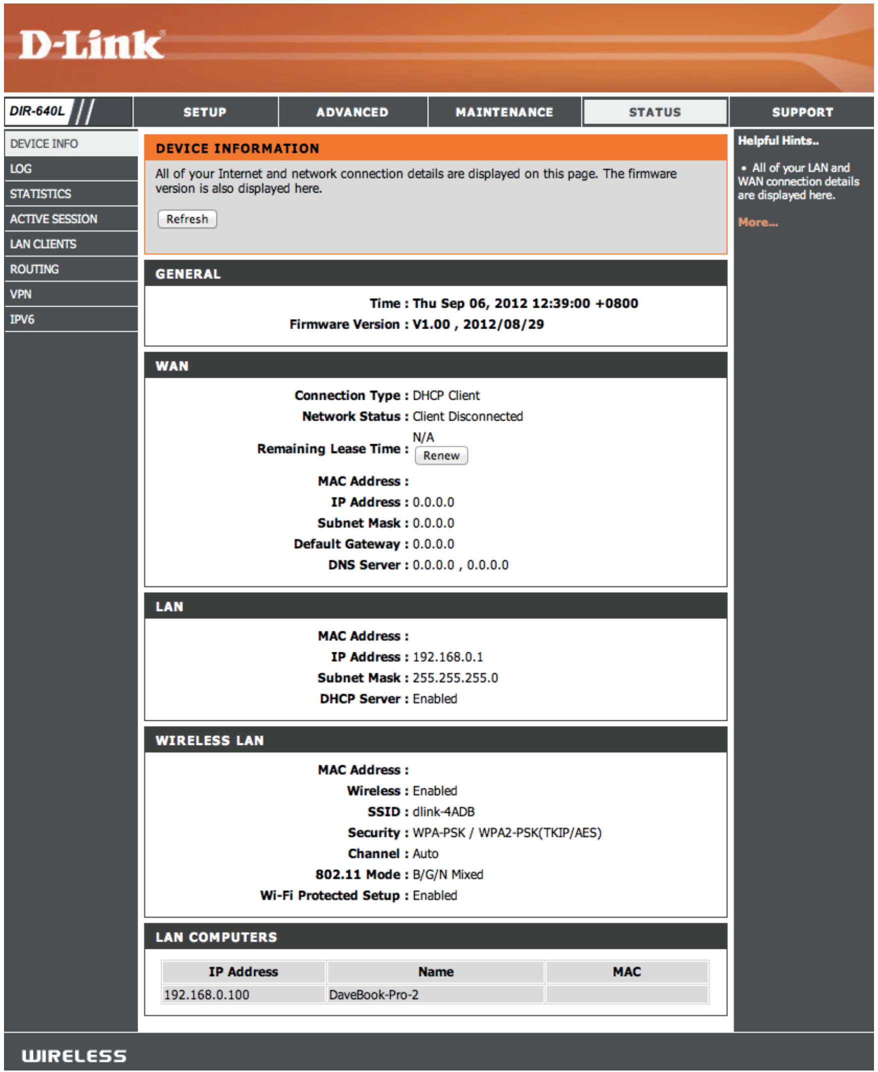
If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

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

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

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

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



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

Helpful Hints..

- All of your LAN and WAN connection details are displayed here.

GENERAL

Time : Thu Sep 06, 2012 12:39:00 +0800
Firmware Version : V1.00 , 2012/08/29

WAN

Connection Type : DHCP Client
Network Status : Client Disconnected
Remaining Lease Time : N/A
MAC Address :
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS Server : 0.0.0.0 , 0.0.0.0

LAN

MAC Address :
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

MAC Address :
Wireless : Enabled
SSID : dlink-4ADB
Security : WPA-PSK / WPA2-PSK(TKIP/AES)
Channel : Auto
802.11 Mode : B/G/N Mixed
Wi-Fi Protected Setup : Enabled

LAN COMPUTERS

| IP Address | Name | MAC |
|---|---|---|
| 192.168.0.100 | DaveBook-Pro-2 | |

# Log

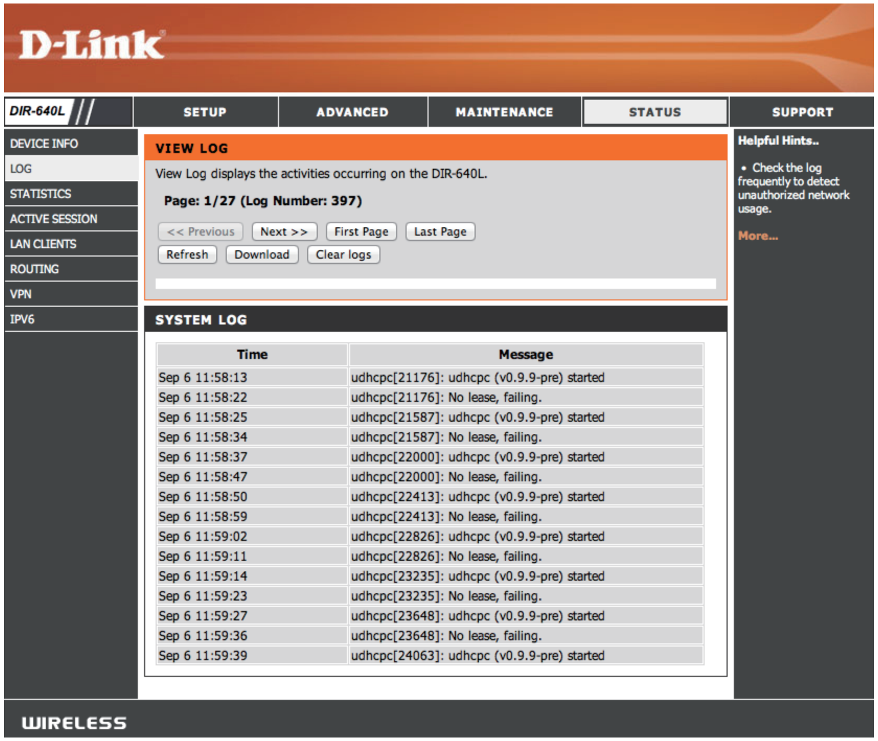
The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types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

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

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

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

**Link To Log Settings:** This option will jump to **Tools** > **Syslog** settings.



VIEW LOG

View Log displays the activities occurring on the DIR-640L.

**Page: 1/27 (Log Number: 397)**

SYSTEM LOG

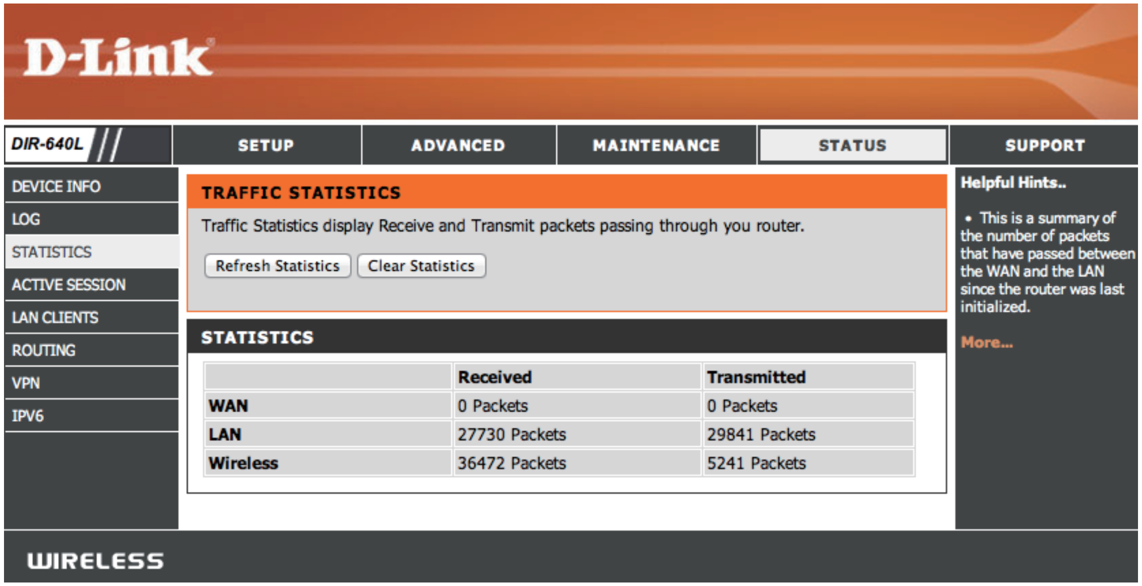
| Time | Message |
|---|---|
| Sep 6 11:58:13 | udhcpc[21176]: udhcpc (v0.9.9-pre) started |
| Sep 6 11:58:22 | udhcpc[21176]: No lease, failing. |
| Sep 6 11:58:25 | udhcpc[21587]: udhcpc (v0.9.9-pre) started |
| Sep 6 11:58:34 | udhcpc[21587]: No lease, failing. |
| Sep 6 11:58:37 | udhcpc[22000]: udhcpc (v0.9.9-pre) started |
| Sep 6 11:58:47 | udhcpc[22000]: No lease, failing. |
| Sep 6 11:58:50 | udhcpc[22413]: udhcpc (v0.9.9-pre) started |
| Sep 6 11:58:59 | udhcpc[22413]: No lease, failing. |
| Sep 6 11:59:02 | udhcpc[22826]: udhcpc (v0.9.9-pre) started |
| Sep 6 11:59:11 | udhcpc[22826]: No lease, failing. |
| Sep 6 11:59:14 | udhcpc[23235]: udhcpc (v0.9.9-pre) started |
| Sep 6 11:59:23 | udhcpc[23235]: No lease, failing. |
| Sep 6 11:59:27 | udhcpc[23648]: udhcpc (v0.9.9-pre) started |
| Sep 6 11:59:36 | udhcpc[23648]: No lease, failing. |
| Sep 6 11:59:39 | udhcpc[24063]: udhcpc (v0.9.9-pre) started |

Helpful Hints..

- Check the log frequently to detect unauthorized network usage.

# Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-640L on both the WAN, LAN ports and both the 802.11n/g and 802.11n/a wireless bands. The traffic counter will reset if the device is rebooted.



TRAFFIC STATISTICS

Traffic Statistics display Receive and Transmit packets passing through you router.

STATISTICS

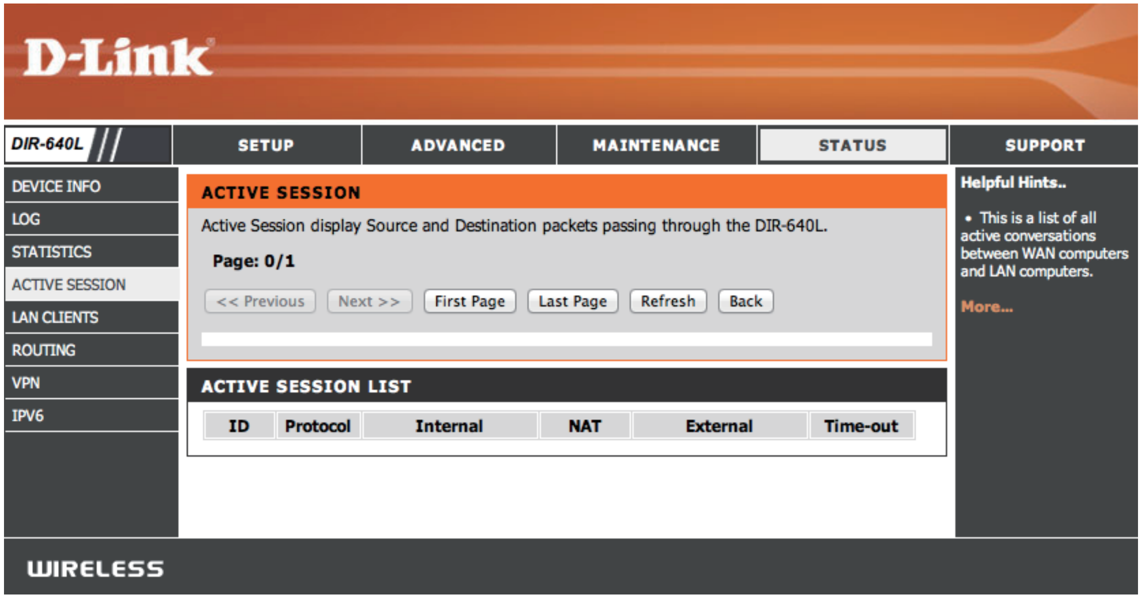
| | Received | Transmitted |
|---|---|---|
| WAN | 0 Packets | 0 Packets |
| LAN | 27730 Packets | 29841 Packets |
| Wireless | 36472 Packets | 5241 Packets |

Helpful Hints..

- This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized.

# Active Session

The Active Session page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.



ACTIVE SESSION

Active Session display Source and Destination packets passing through the DIR-640L.

Page: 0/1

ACTIVE SESSION LIST

| ID | Protocol | Internal | NAT | External | Time-out |
|---|---|---|---|---|---|

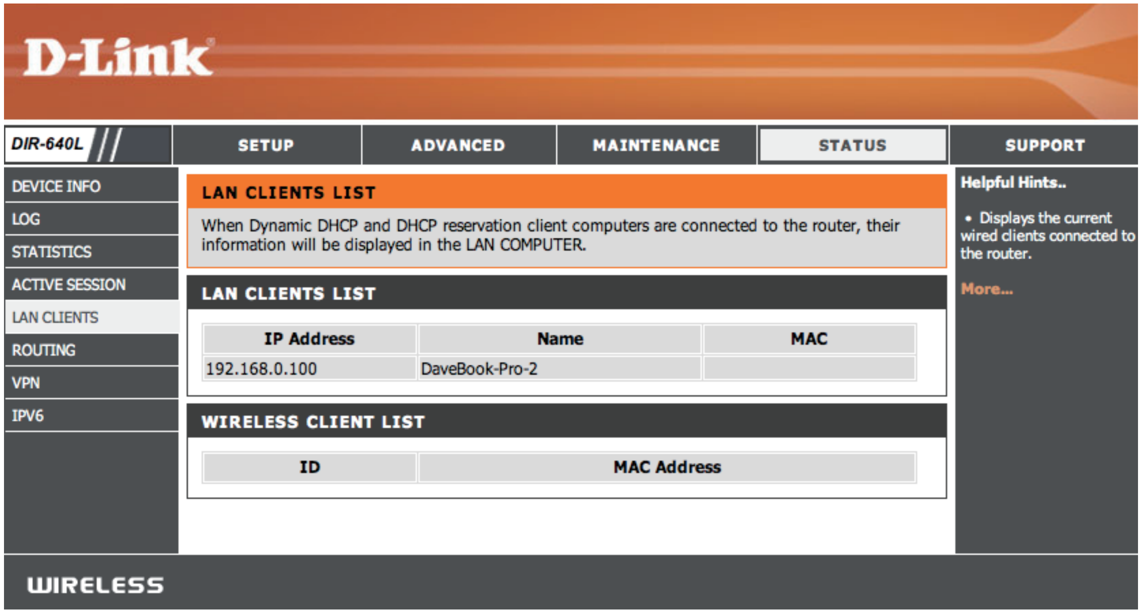
Helpful Hints..

- This is a list of all active conversations between WAN computers and LAN computers.

More...

# LAN Clients

This page will list the LAN clients currently connected to your network.



LAN CLIENTS LIST

When Dynamic DHCP and DHCP reservation client computers are connected to the router, their information will be displayed in the LAN COMPUTER.

LAN CLIENTS LIST

| IP Address | Name | MAC |
|---|---|---|
| 192.168.0.100 | DaveBook-Pro-2 | |

WIRELESS CLIENT LIST

| ID | MAC Address |
|---|---|

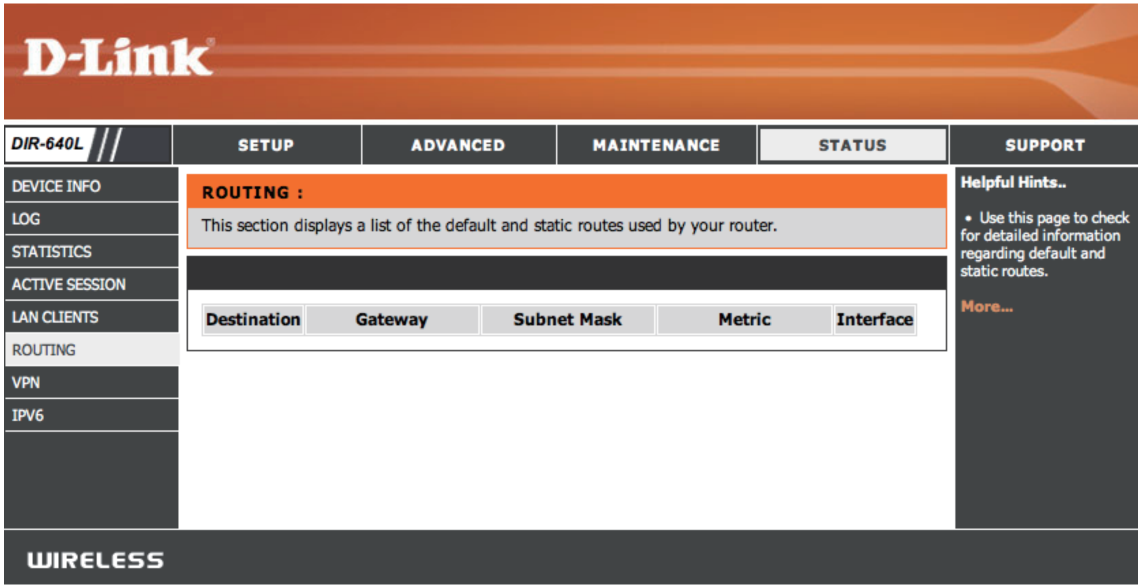
Helpful Hints..

- Displays the current wired clients connected to the router.

More...

# Routing

This page will display your current routing table.



ROUTING :

This section displays a list of the default and static routes used by your router.

| Destination | Gateway | Subnet Mask | Metric | Interface |
|---|---|---|---|---|

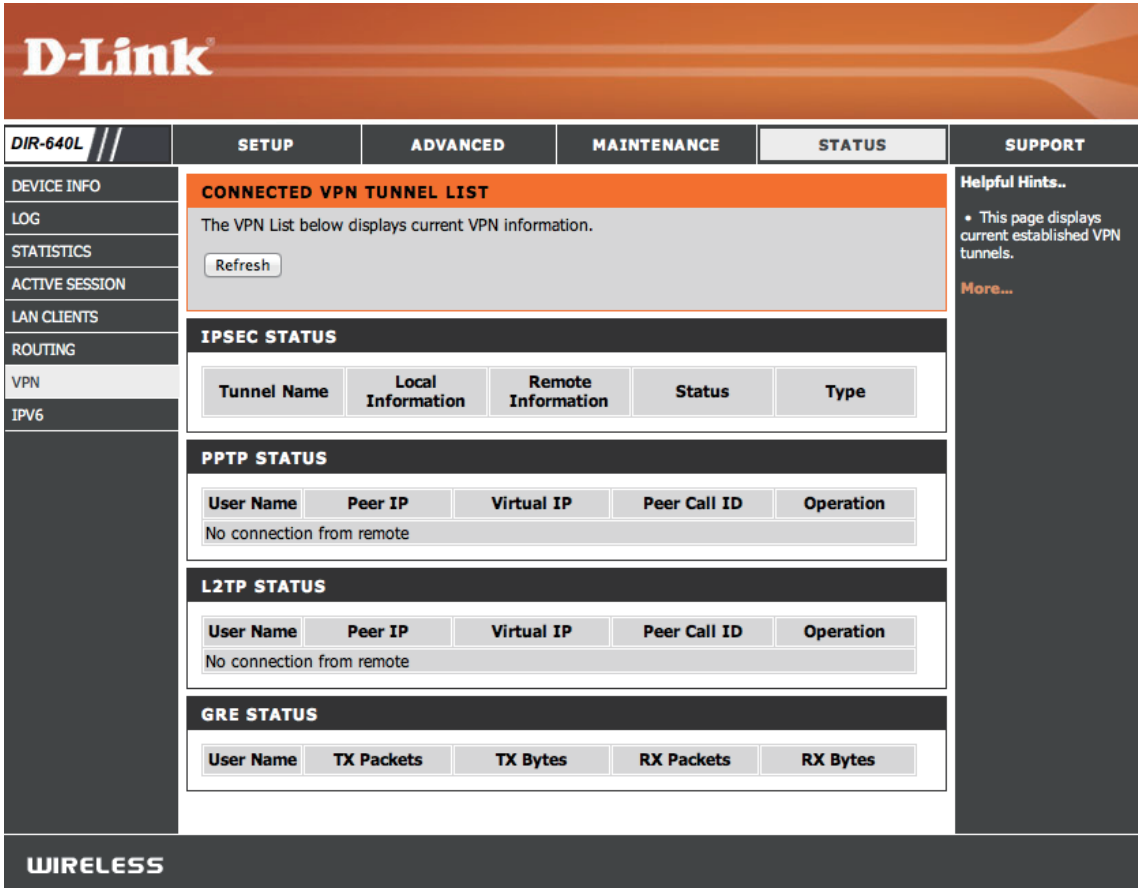
Helpful Hints..

- Use this page to check for detailed information regarding default and static routes.

More...

# VPN

This page is where the router displays information on the the current VPN tunnels.



**CONNECTED VPN TUNNEL LIST**

The VPN List below displays current VPN information.

**IPSEC STATUS**

| Tunnel Name | Local Information | Remote Information | Status | Type |
|---|---|---|---|---|

**PPTP STATUS**

| User Name | Peer IP | Virtual IP | Peer Call ID | Operation |
|---|---|---|---|---|
| No connection from remote | | | | |

**L2TP STATUS**

| User Name | Peer IP | Virtual IP | Peer Call ID | Operation |
|---|---|---|---|---|
| No connection from remote | | | | |

**GRE STATUS**

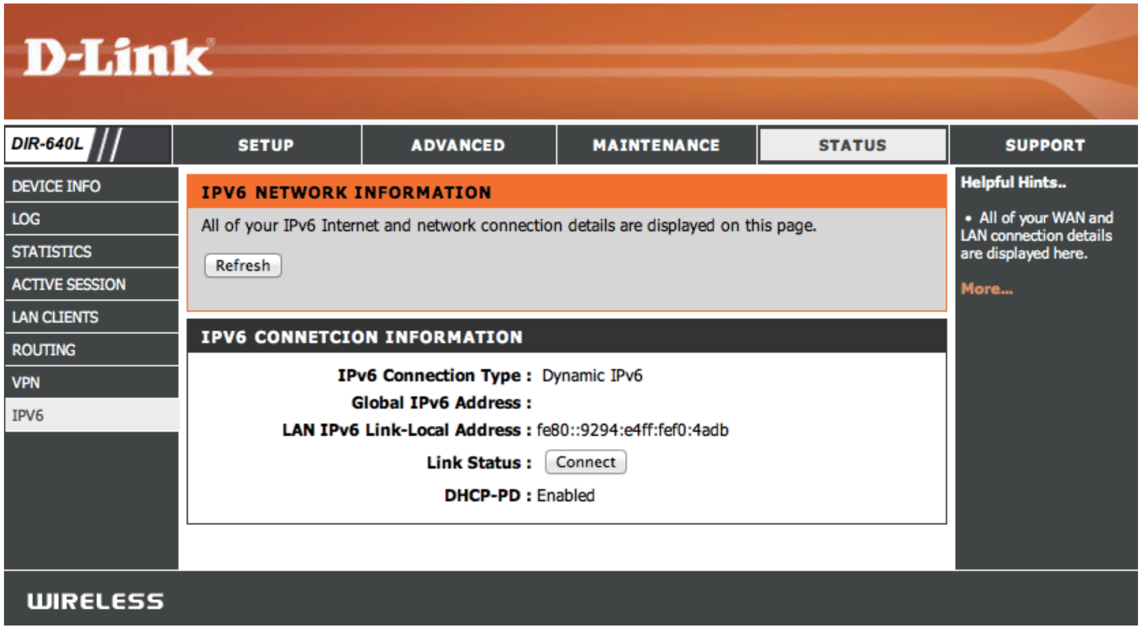
| User Name | TX Packets | TX Bytes | RX Packets | RX Bytes |
|---|---|---|---|---|

**Helpful Hints..**

- This page displays current established VPN tunnels.

# IPv6

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



IPV6 NETWORK INFORMATION

All of your IPv6 Internet and network connection details are displayed on this page.

IPV6 CONNETCION INFORMATION

IPv6 Connection Type : Dynamic IPv6
Global IPv6 Address :
LAN IPv6 Link-Local Address : fe80::9294:e4ff:fef0:4adb
Link Status : Connect
DHCP-PD : Enabled

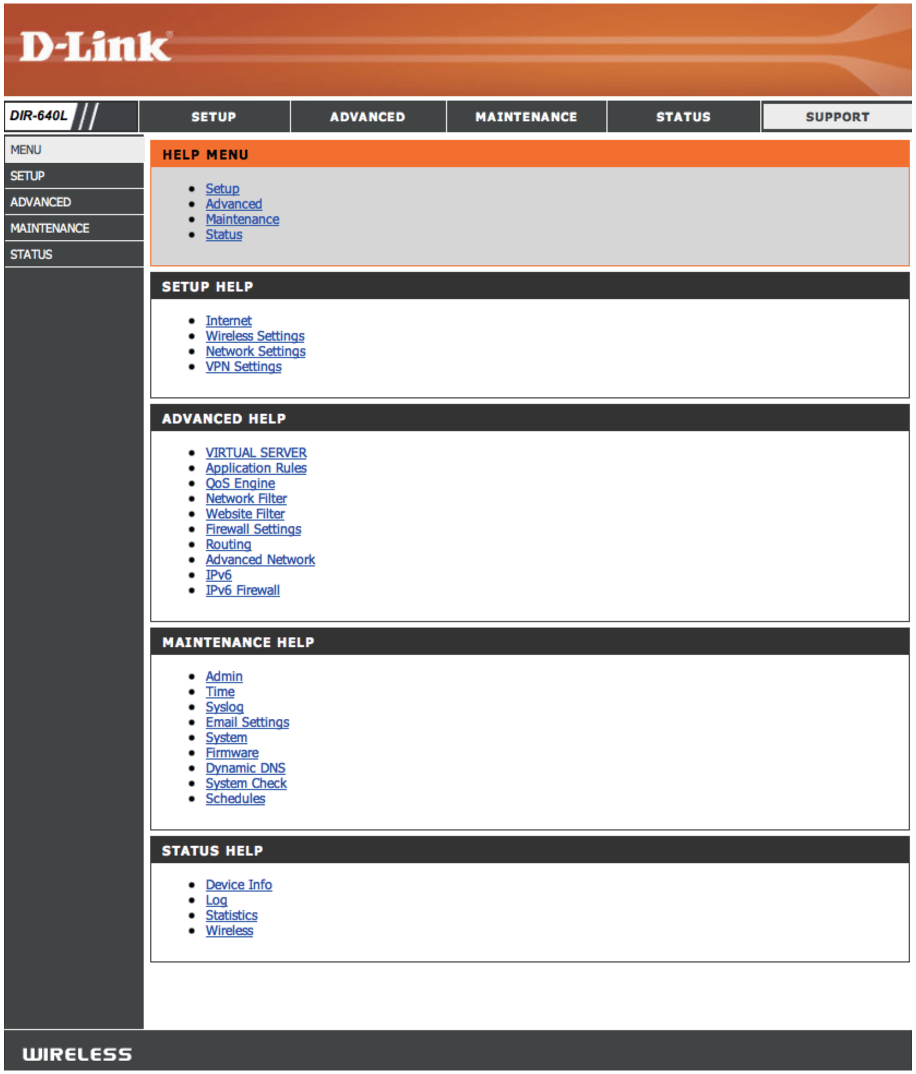
Helpful Hints..

- All of your WAN and LAN connection details are displayed here.

More...

# Support

Click these links to get further instruction when configuring your DIR-640L Wireless N300 Cloud VPN Router.



HELP MENU

- Setup
- Advanced
- Maintenance
- Status

SETUP HELP

- Internet
- Wireless Settings
- Network Settings
- VPN Settings

ADVANCED HELP

- VIRTUAL SERVER
- Application Rules
- QoS Engine
- Network Filter
- Website Filter
- Firewall Settings
- Routing
- Advanced Network
- IPv6
- IPv6 Firewall

MAINTENANCE HELP

- Admin
- Time
- Syslog
- Email Settings
- System
- Firmware
- Dynamic DNS
- System Check
- Schedules

STATUS HELP

- Device Info
- Log
- Statistics
- Wireless

# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-640L. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:

  - Microsoft Internet Explorer® 6.0 and higher
  - Mozilla Firefox 3.0 and higher
  - Google™ Chrome 2.0 and higher
  - Apple Safari 3.0 and higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

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

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

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

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

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

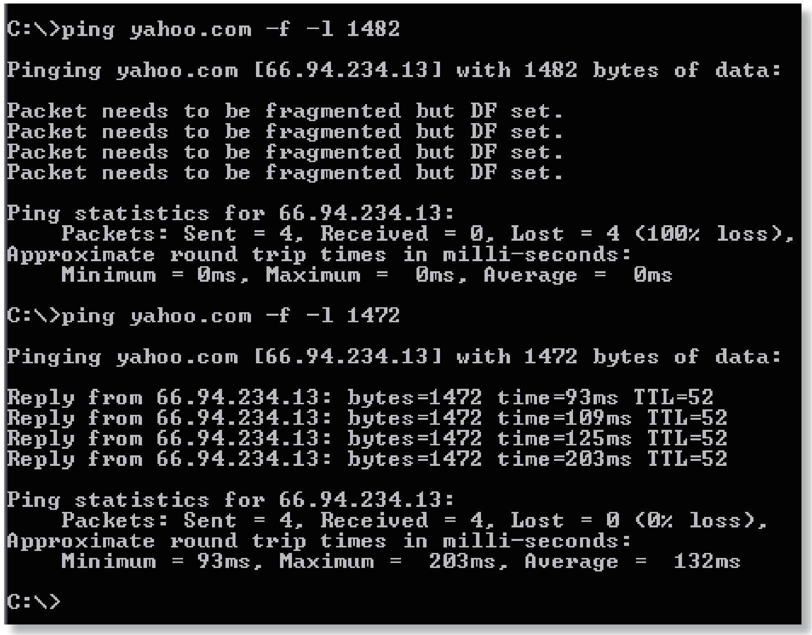
If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

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

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

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

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



```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

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

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

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

C:\>
```

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

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

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

- Open your browser, enter the IP address of your router (http://192.168.0.1) and click **OK**.
- Enter your username (admin) and password (should be left empty). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.

# Wireless Basics

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

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

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

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

## What is Wireless?

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

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

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

## How does wireless work?

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

### Wireless Local Area Network (WLAN)

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

### Wireless Personal Area Network (WPAN)

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

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

## Who uses wireless?

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

**Home**

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

**Small Office and Home Office**

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

## Where is wireless used?

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

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

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

## Tips

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

### Centralize your router or Access Point

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

### Eliminate Interference

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

### Security

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

# Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-640L wireless network Cardbus adapters.

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

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

# Networking Basics

## Check your IP address

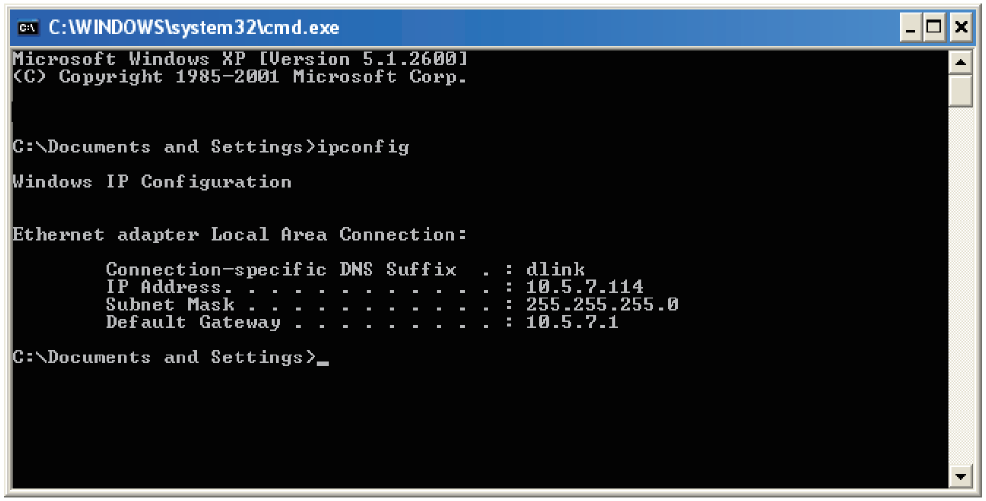
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.


C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

# Statically Assign an IP address

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

**Step 1**

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

**Step 2**

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

**Step 3**

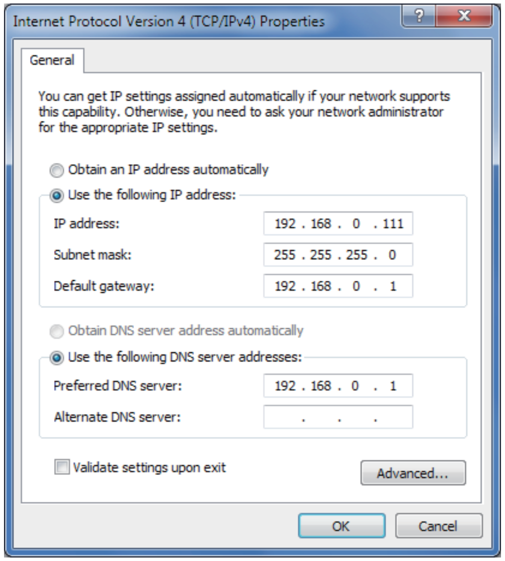
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

**Step 4**

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

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 111
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

**Step 5**

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

# Technical Specifications

## Standards

- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

## Security

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

## Wireless Signal Rates[1]

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

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

### IEEE 802.11g:

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

## Frequency Range[2] (North America)

- 2.412 GHz to 2.462 GHz (802.11g/n)

## External Antenna Type

- Two (2) detachable Antennas

## Operating Temperature

- 32°F to 104°F ( 0°C to 40°C)

## Humidity

- 95% maximum (non-condensing)

## Safety & Emissions

- FCC
- CE

## Dimensions

- L = 7.4 inches
- W = 4.4 inches
- H = 1.1 inches

## Warranty

- 1 Year

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

[2] Frequency Range varies depending on country's regulation

[3] The DIR-640L does not include 5.25-5.35 GHz & 5.47-5.725 GHz in some regions.

# GPL Code Statement

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License (“GPL”) or GNU Lesser General Public License (“LGPL”). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

http://tsd.dlink.com.tw/GPL.asp

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

## WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPLsource code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Please direct all inquiries to:
Email: GPLCODE@DLink.com
Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Corporation.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

**GNU GENERAL PUBLIC LICENSE**
**Version 3, 29 June 2007**

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

**Preamble**

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

## TERMS AND CONDITIONS

### 0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License.  Each licensee is addressed as “you”.  “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy.  The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy.  Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies.  Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License.  If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

### 1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it.  “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

**2. Basic Permissions.**

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

**3. Protecting Users' Legal Rights From Anti-Circumvention Law.**

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

**4. Conveying Verbatim Copies.**
You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

**5. Conveying Modified Source Versions.**
You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

**6. Conveying Non-Source Forms.**

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

**7. Additional Terms.**

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work). You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

**8. Termination.**

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

**9. Acceptance Not Required for Having Copies.**

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

**10. Automatic Licensing of Downstream Recipients.**

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

**11. Patents.**

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

**12. No Surrender of Others' Freedom.**

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

**13. Use with the GNU Affero General Public License.**

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

**14. Revised Versions of this License.**

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation. If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

**15. Disclaimer of Warranty.**

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

**16. Limitation of Liability.**
IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**17. Interpretation of Sections 15 and 16.**

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

# Safety Statements

## CE Mark Warning:

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

## FCC Statement:

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

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

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

## IMPORTANT NOTICE:

**FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

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