D-Link®

Version 1.0 | 09/19/2012

User Manual

Broadband Cloud VPN Router

DIR-140L

Preface

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

Manual Revisions

Revision	Date	Description
1.0	September 19, 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
Wall-Mount Kit Installation 8
Hardware Setup 9

Configuration 11
Web Setup Wizard 11
Web-based Configuration Utility 15
Internet Connection Setup 16
Internet Connection Wizard 16
Manual Internet Connection 18
Static (assigned by ISP) 19
Dynamic (Cable) 20
PPPoE (DSL) 21
PPTP 22
L2TP 23
Dial-Up 24
3G 25
Russian PPPoE 26
Russian Dual Access L2TP 27
Russian Dual Access PPTP 28
Network Settings 29
VPN Settings 31
VPN Setup Wizard 31
Dynamic IPSec VPN 32
IPSec VPN 33
PPTP VPN 34
L2TP VPN 35
VPN Manual Settings 36
IPSec Settings 37
PPTP/L2TP Settings 39
GRE Settings 40

Advanced 41
Virtual Server 41
Application Rules 42
QoS Engine 43
Network Filters 45
Website Filters 46
Firewall Settings 47
Routing 49
Advanced Network Settings 50

IPv6 51
Static IPv6 52
DHCP 53
PPPoE 54
IPv6 over IPv4 Tunneling 55
6 to 4 Tunneling 56
6rd 57
Link-Local Connectivity 58
IPv6 Firewall 59
User Group 60

Maintenance 61
Admin 61
SNMP 62
Time 63
SysLog 64
Email Settings 65
System 66
Firmware 67
Dynamic DNS 68
System Check 69
Schedules 70

Status 71
Device Info 71
Log 72
Statistics 73
Active Session 74
LAN Clients 75
Routing 76
VPN 77
IPv6 78

Support 79

Troubleshooting 80

Networking Basics 84
Check your IP address 84
Statically Assign an IP address 85

Technical Specifications 86

GPL Code Statement 87

Contacting Technical Support 100

Warranty 101

Registration 106

Package Contents

DIR-140L Broadband Cloud VPN Router

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-140L will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6 or higher • Firefox 3.0 or higher • Safari 3.0 or higher • Chrome 2.0 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

TERRIFIC VPN PERFORMANCE

For optimal VPN configuration, the DIR-140L has an integrated VPN Client and Server to support almost any required VPN policy. This device has a hardware VPN engine to support and manage up to 25 VPN configurations. The DIR-140L can support IPSec, PPTP, L2TP, and GRE protocols in Server mode and can handle pass-through traffic as well. Advanced VPN configuration options include: DES, 3DES, and AES encryption, IKE/ISAKMP key management, Main/Aggressive Negotiation modes, and VPN authentication support using the internal 10-user database.

USER CONFIGURABLE INTERFACE

The DIR-140L features an intuitive user interface that can easily be configured and monitored via D-Link's web-based management interface. These configuration options can be managed through Admin or Read/Write administrator rights. With these access management levels, any authorized user can easily configure or access the management interface of the DIR-140L.

USE MYDLINK TO MONITOR YOUR NETWORK

The Broadband Cloud VPN Router is mydlink-enabled, so you can effortlessly access and view your network no matter where you are. See who is connected to your router, change settings, or block someone from using your network connection, all from any Internet connected PC, or an iOS or Android mobile device. Home users can check on their children's web browsing habits, and business users can manage employee Internet activity, all while staying informed and in control on the go.

ADVANCED HARDWARE FEATURES

The DIR-140L can be connected to a cable or DSL line to share high-speed Internet access. It also doubles as a 4-port full-duplex 10/100 switch to connect up to four Ethernet-enabled devices, and you can simply add more switches to expand your wired network. In addition, you can create a Virtual Private Network (VPN) with the DIR-140L and allow up to 25 off-site or traveling users to securely access your central network through the Internet simultaneously.

TOTAL NETWORK SECURITY

The DIR-140L has a host of security features to prevent unauthorized access and utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

Features

- **Versatile VPN Connectivity** - The DIR-140L can create secure connections easily with support for up to 25 VPN tunnels and standards including IPSec, PPTP, L2TP, and GRE tunneling

- **Built-In Security** - The DIR-140L features a dual-active firewall that works to protect against network attacks and keep your network safe from outside threats

- **Cloud Management** - The DIR-140L is mydlink-enabled, which helps you manage your router from anywhere.[1]

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

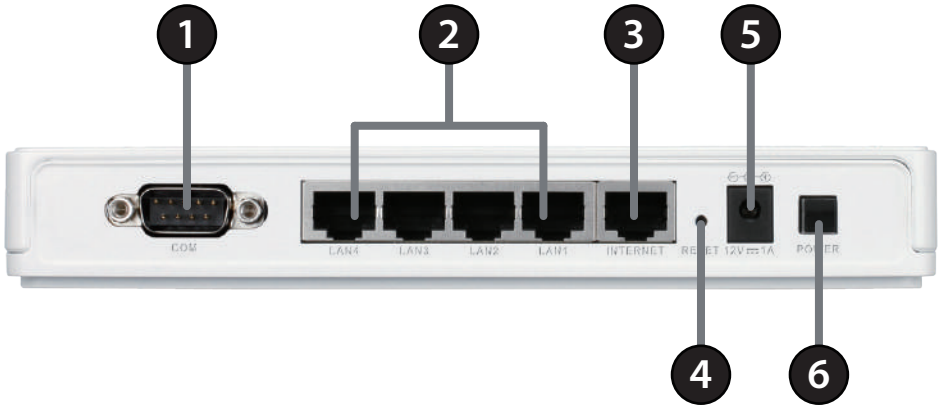
    - **Secure Multiple/Concurrent Sessions** - The DIR-140L can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-140L can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-140L lets you control what information is accessible to those on the network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

[1] mydlink support available soon through a future firmware update.

Hardware Overview

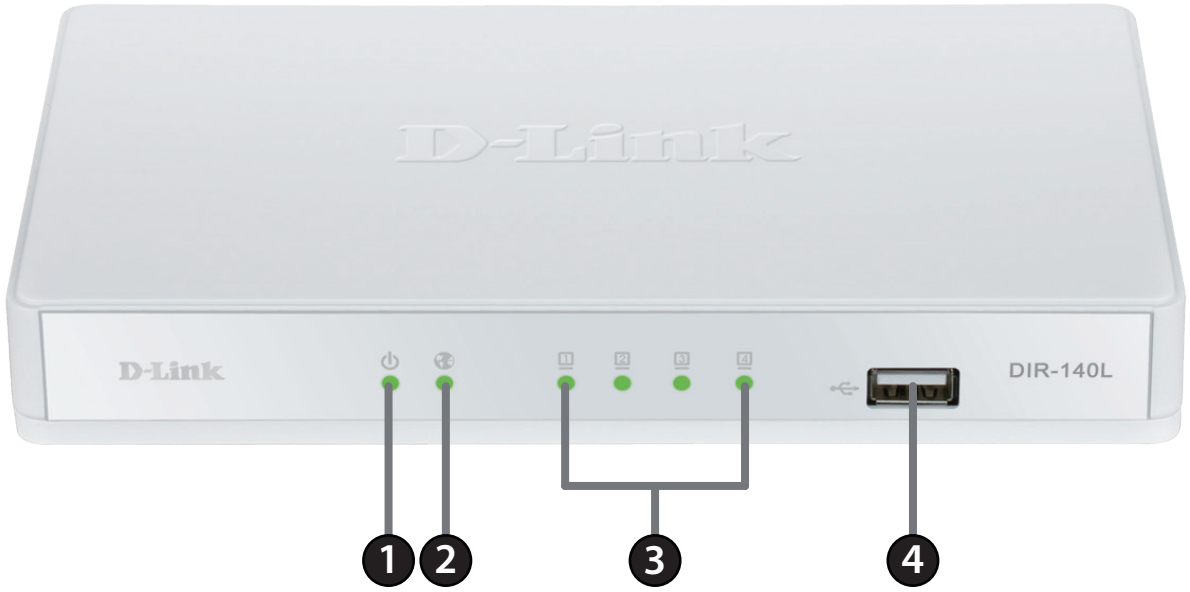
Back



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 Connector	Receptor for the supplied power adapter.
6	Power Switch	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	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.
4	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.

Wall-Mount Kit Installation

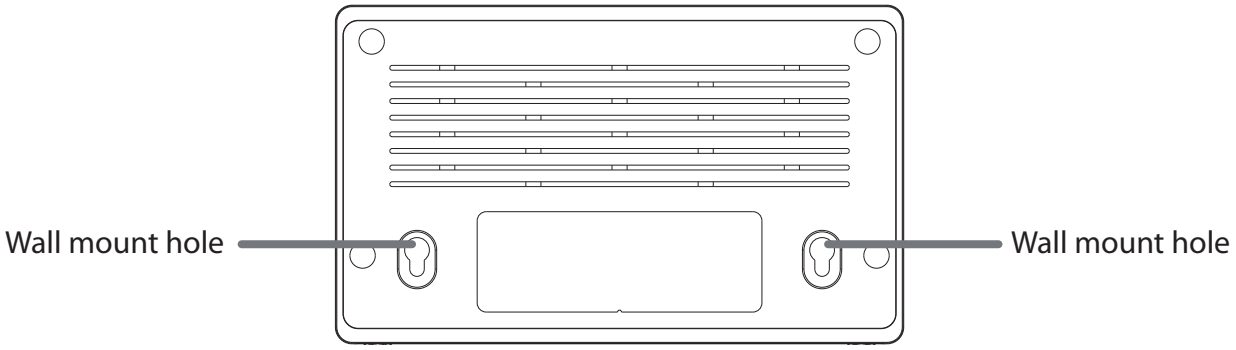
The wall-mount kit includes the following items:

- 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.

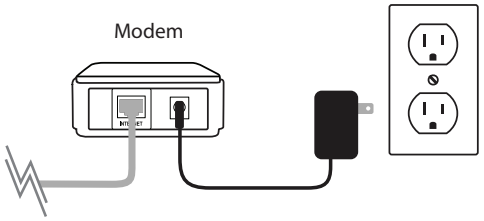


DIR-140L

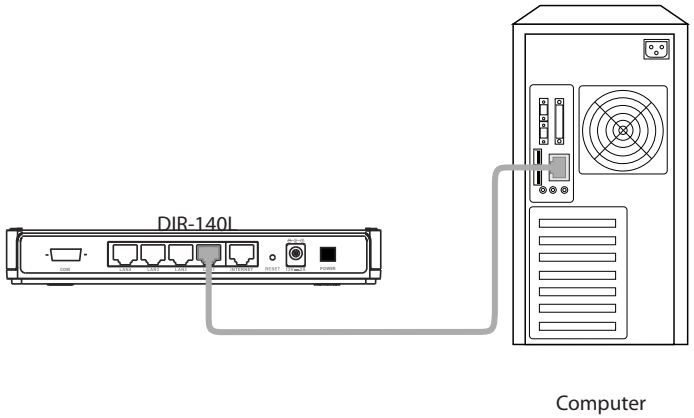
Step 4. Hang the router on the wall by sliding the tops of the screws through the holes on the bottom of the router and then slide to lock into position. Confirm the the router is firmly in place.

Hardware Setup

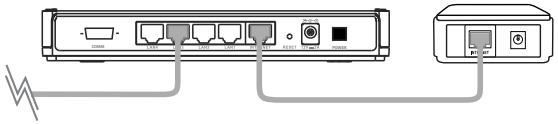
1. Turn off and unplug your cable or DSL broadband modem. This is required.



2. 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.



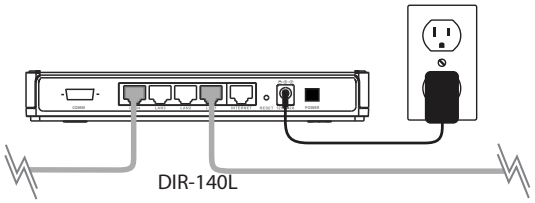
4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.



DIR-140L 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.



DIR-140L

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. If you did not connect to the Internet, use the D-Link Setup Wizard (refer to page 15).

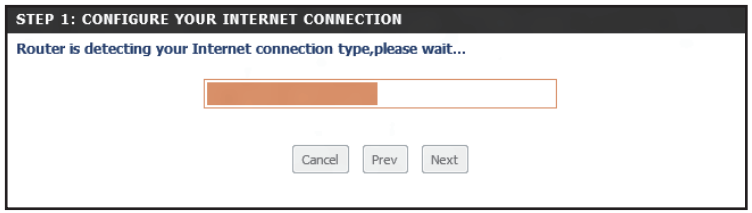
Configuration

Web Setup Wizard

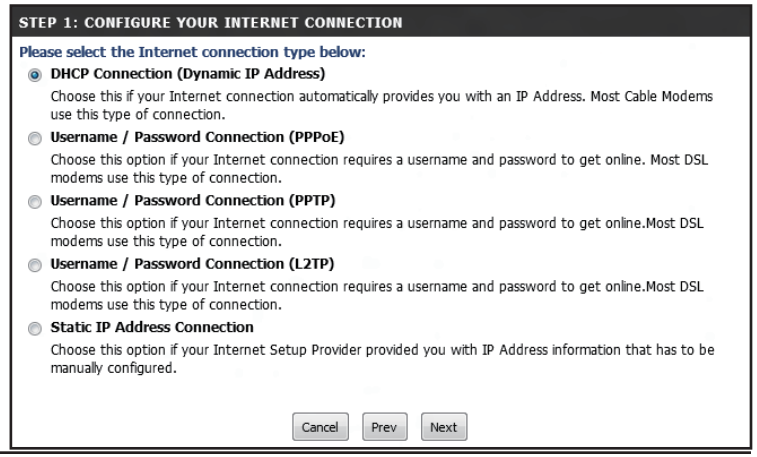
Step 1: The Welcome screen will appear. Click **Next** to continue.

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

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

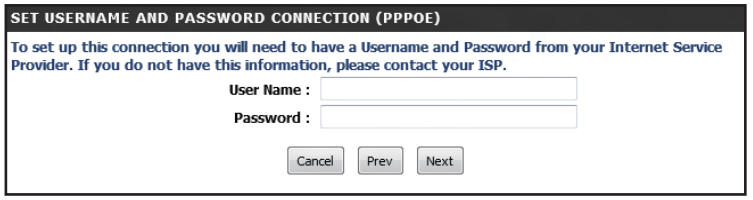


Step 3: If the router could not automatically detect your connection type, select your connection type and click **Next** to continue.

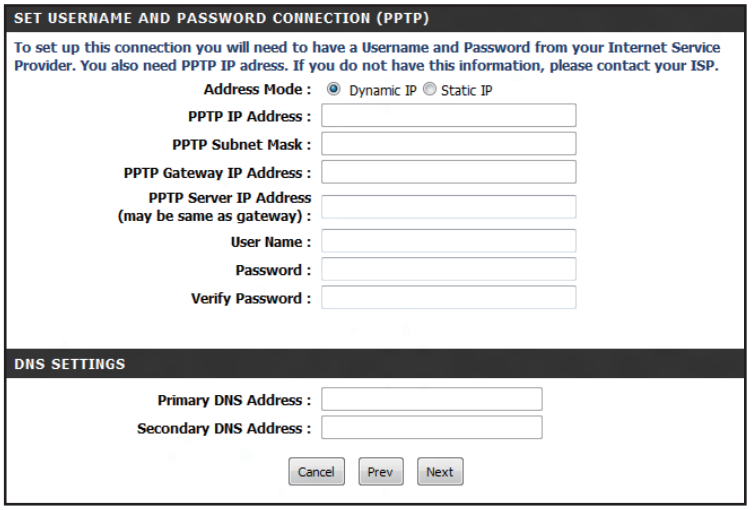


If you selected PPPoE, enter your PPPoE username and password. Click **Next** to continue.

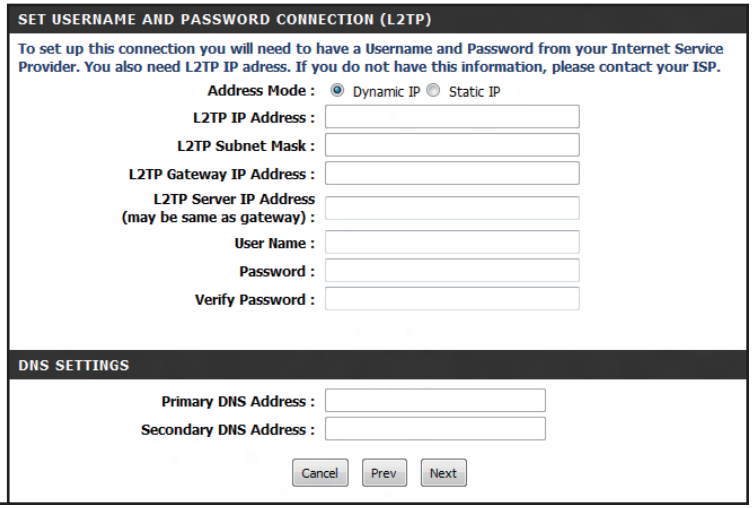
Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*



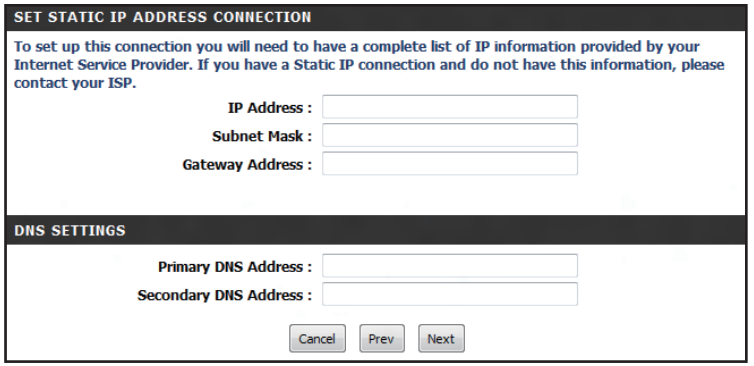
If you selected PPTP, enter your PPTP settings supplied by your ISP and your PPTP username and password. Click **Next** to continue.



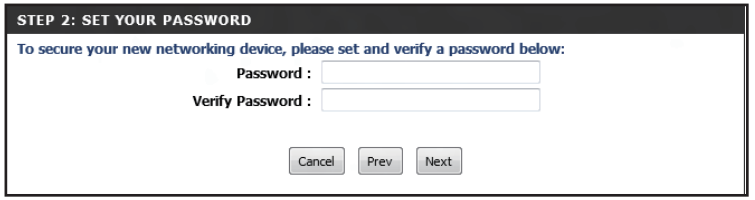
If you selected L2TP, enter your L2TP settings supplied by your ISP and your L2TP username and password. Click **Next** to continue.



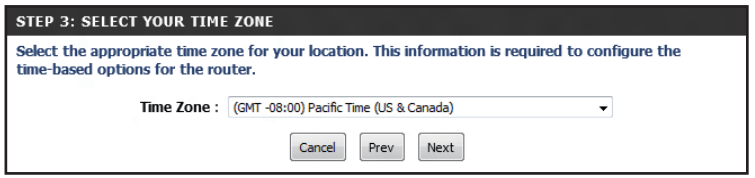
If you selected Static, enter your network settings supplied by your Internet provider. Click **Next** to continue.



Step 4: Create a new password and then click **Next** to continue.



Step 5: Select your time zone from the drop-down menu and then click **Next** to continue.



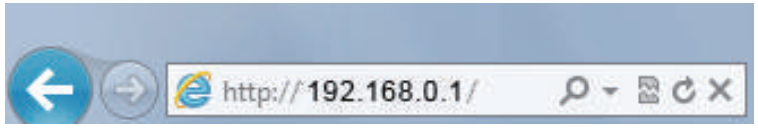
Step 6: Setup is complete. Click **Save** to continue.

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

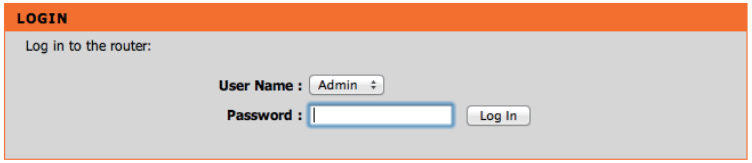
Close your browser window and reopen it to test your Internet connection.
It may take a few tries to initially connect to the Internet.

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 you can use **http://dlinkrouter.local.**).

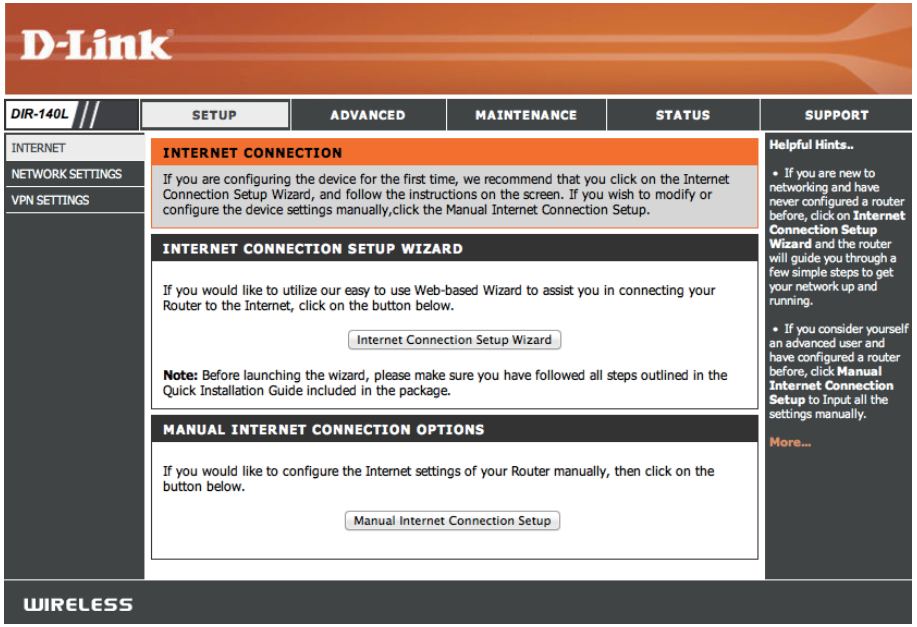


Select **Admin** from the drop-down menu and the password **should be left empty**.



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.

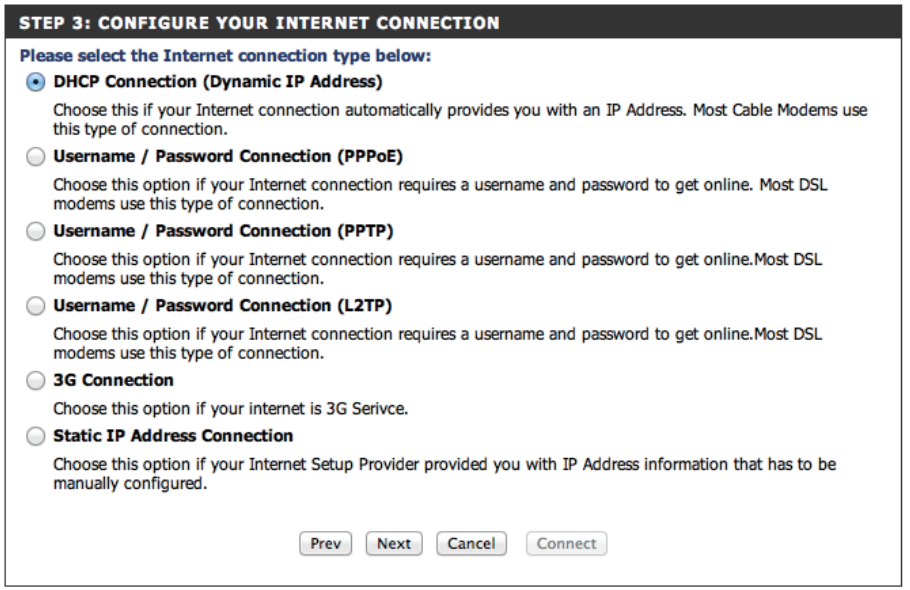


Internet Connection Wizard

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

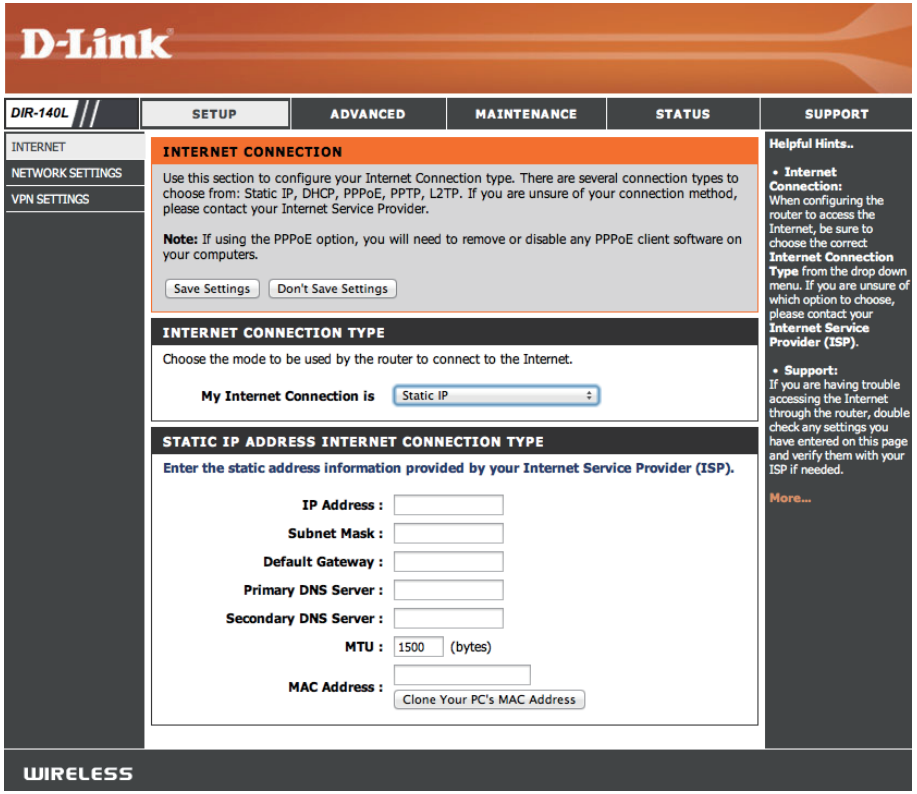
STEP 1: Choose a password for your device.

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



Manual Internet Connection

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



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.

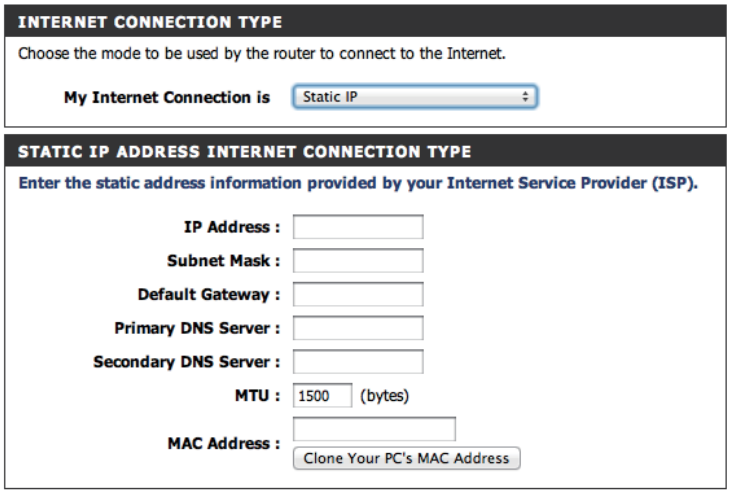
Subnet Mask: Enter the Subnet Mask assigned by your ISP.

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.



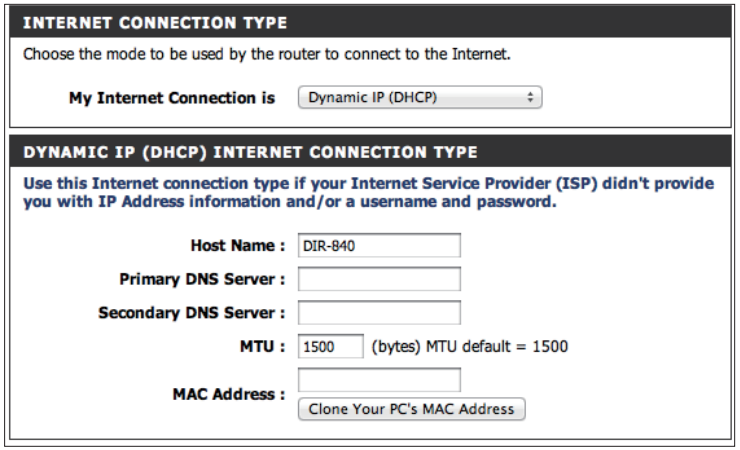
Dynamic (Cable)

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.

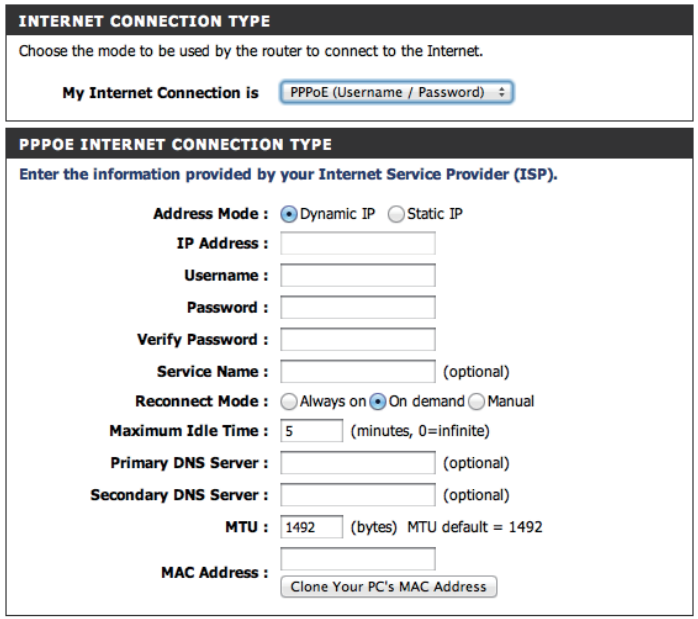
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.



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.



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.

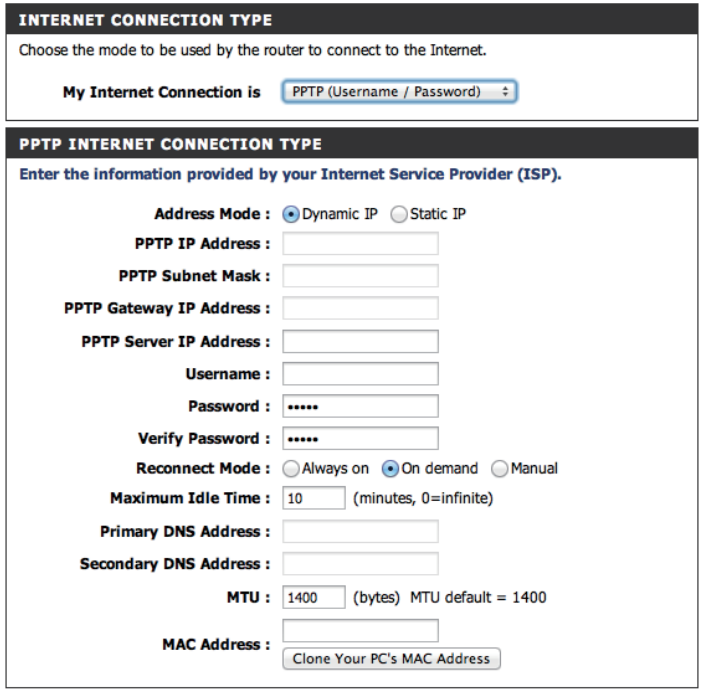
DNS Addresses: Enter the Primary and Secondary DNS Server Addresses (Static PPPoE only).

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.



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.

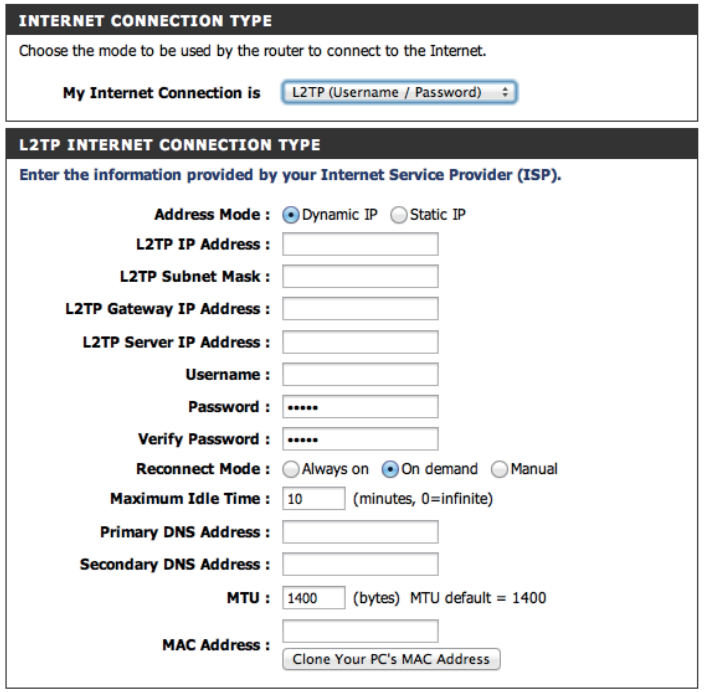
DNS Addresses: Enter the Primary and Secondary DNS Server Addresses (Static PPTP only).

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.



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.

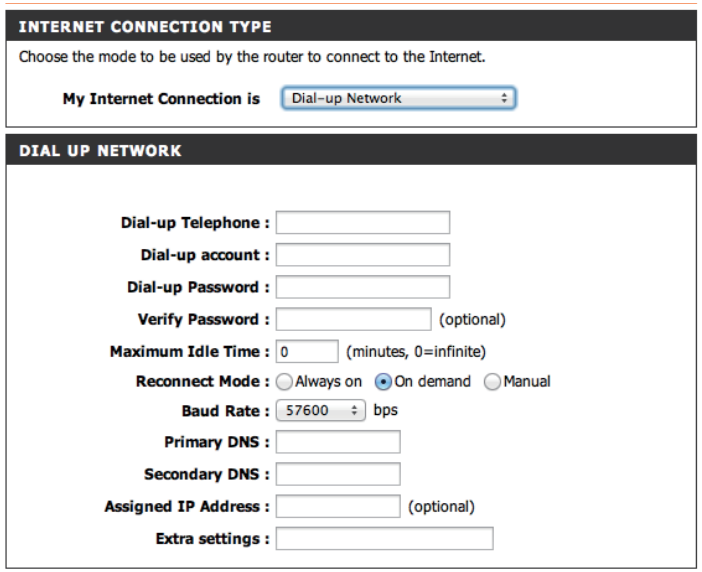
DNS Addresses: Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

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.

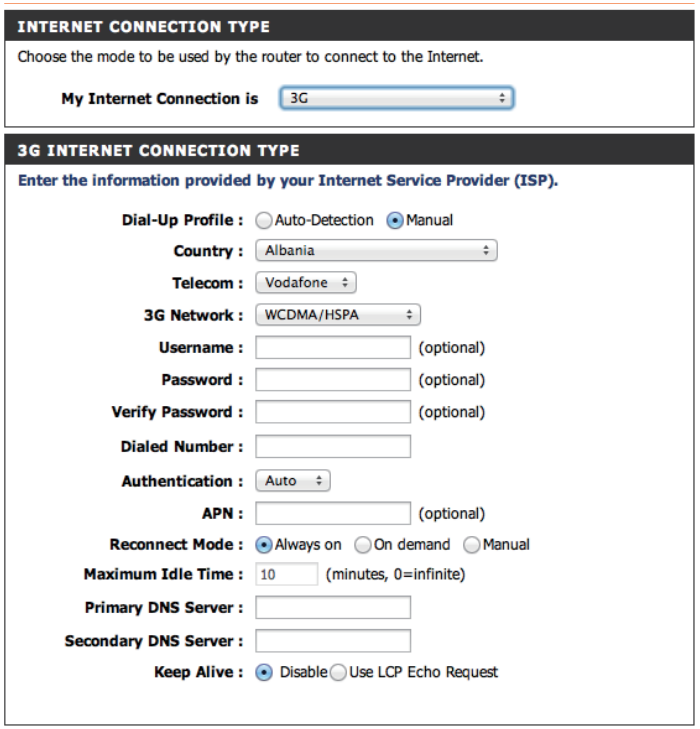
DNS Addresses: Enter the Primary and Secondary DNS Server Addresses.

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.

3G

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



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**.

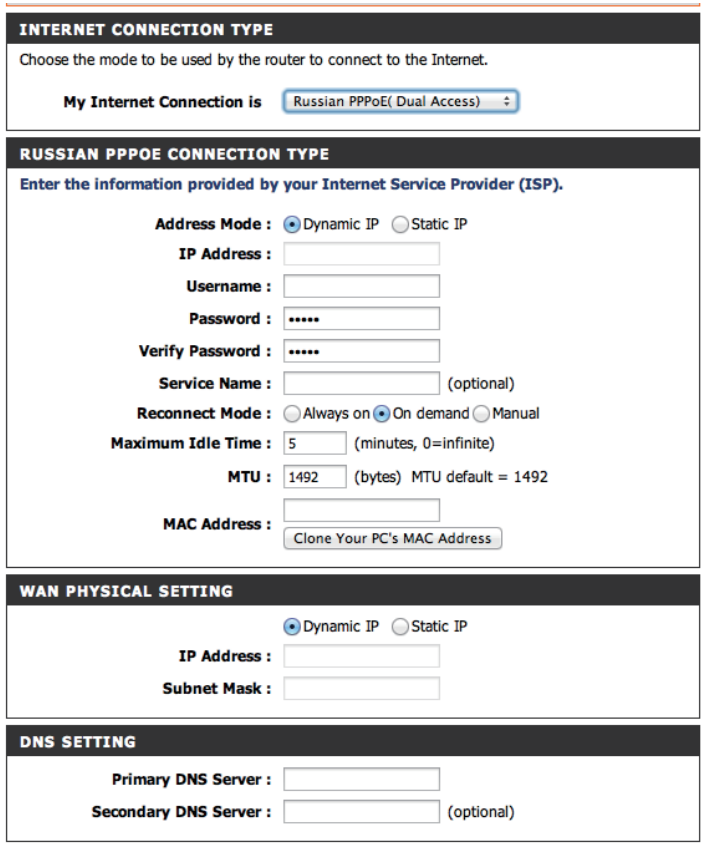
Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

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.



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.

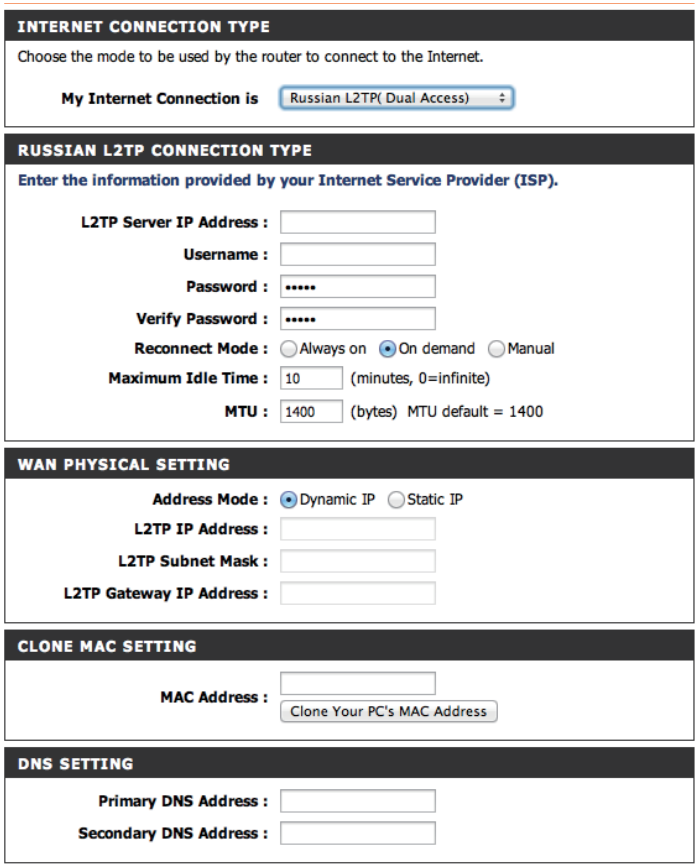
IP Address Enter the IP address for your PPTP connection.

Subnet Mask: Enter your PPTP subnet mask.

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

Russian Dual Access L2TP

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



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.

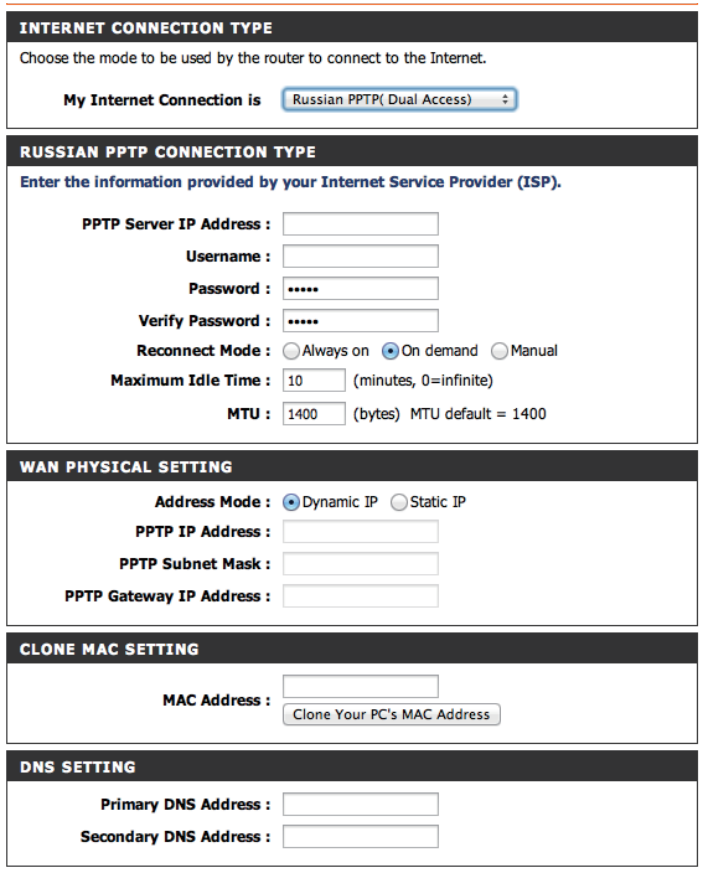
L2TP Gateway IP Address: Enter the L2TP Gateway IP address.

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 Dual Access PPTP

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



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.

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.

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

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

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

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

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

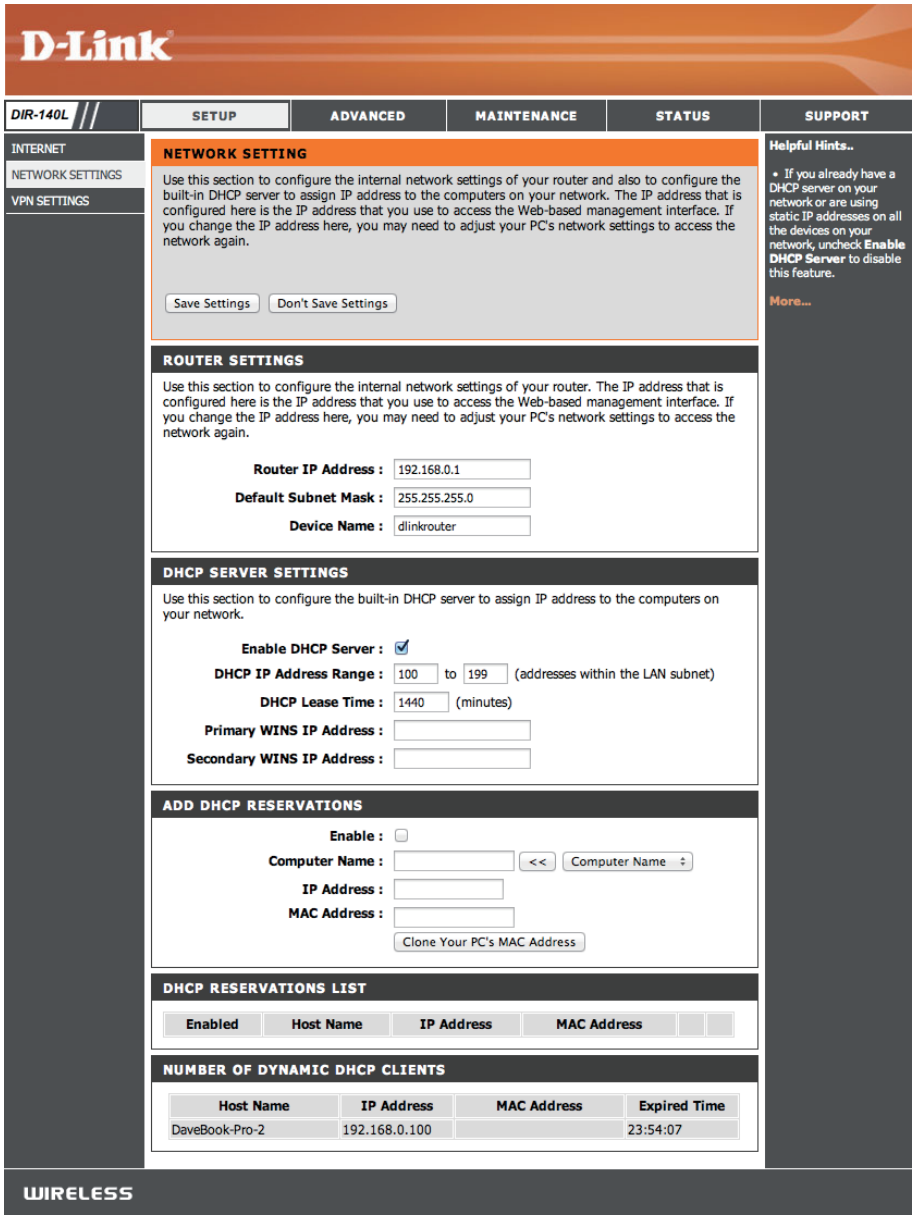
DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

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

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

Enable: Check this box to enable the DHCP reservations.

Computer Name: Enter the computer name or select from the drop-down menu.



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

Enter the MAC address of the computer or device.

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

Copy Your PC's MAC Address: Click **Save** to save your entry. You must click **Save Settings** at the top to activate your reservations.

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

Enable: Check to enable/disable the reservation from the existing DHCP reservation list.

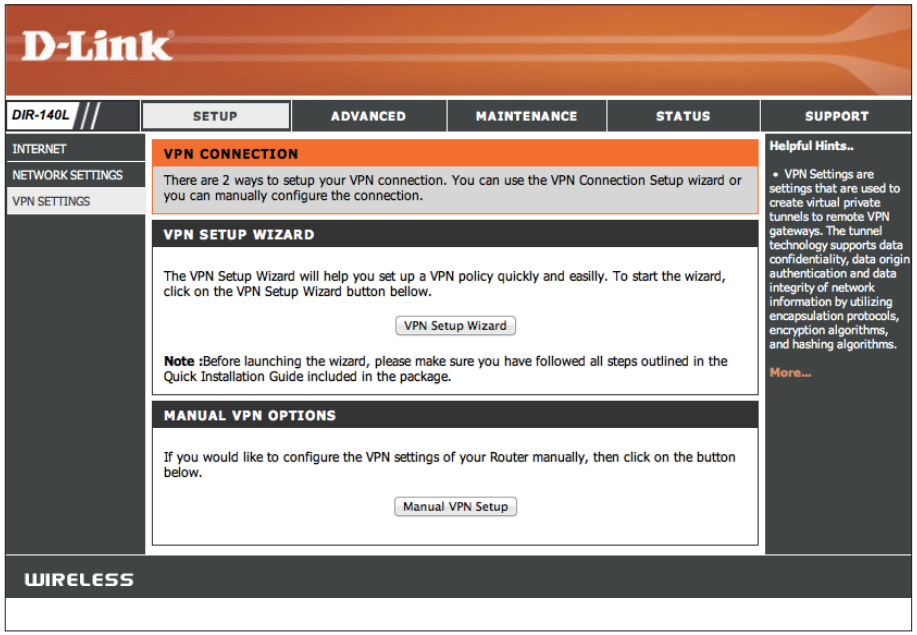
Edit: Click the edit icon to make changes to the reservation entry.

Delete: Click to remove the reservation from the list.

VPN Settings

On this page you can set up advanced options for a Virtual Private Network (VPN). The DIR-140L 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 tab to choose if you want to follow the simple steps of the VPN Setup Wizard, or if you want to set up VPN options manually.

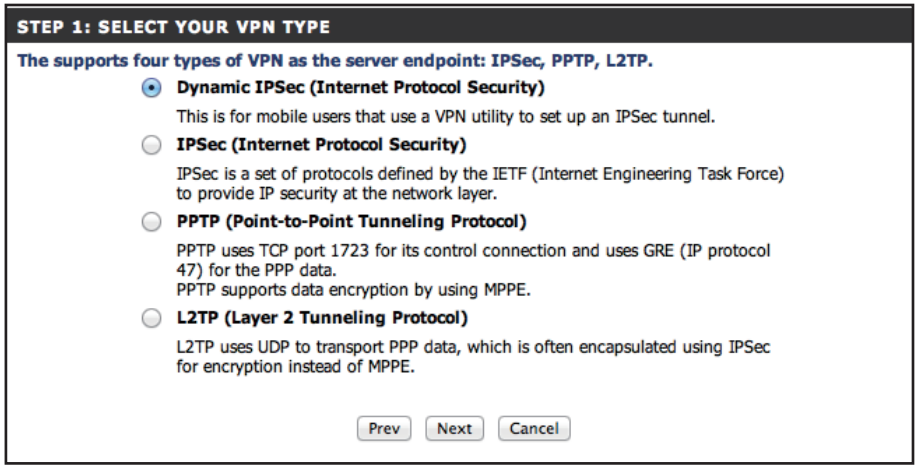


VPN Setup Wizard

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

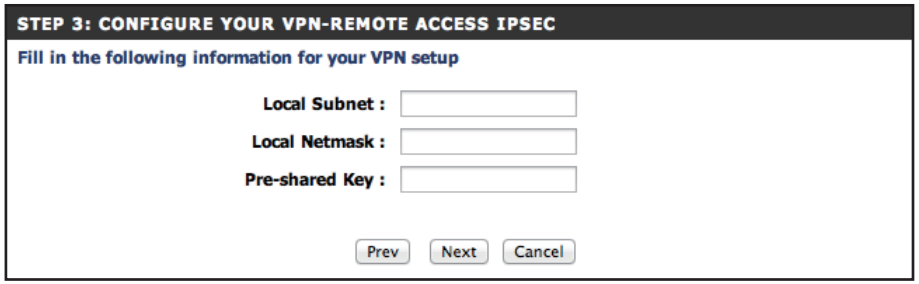
Dynamic IPSec VPN

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



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

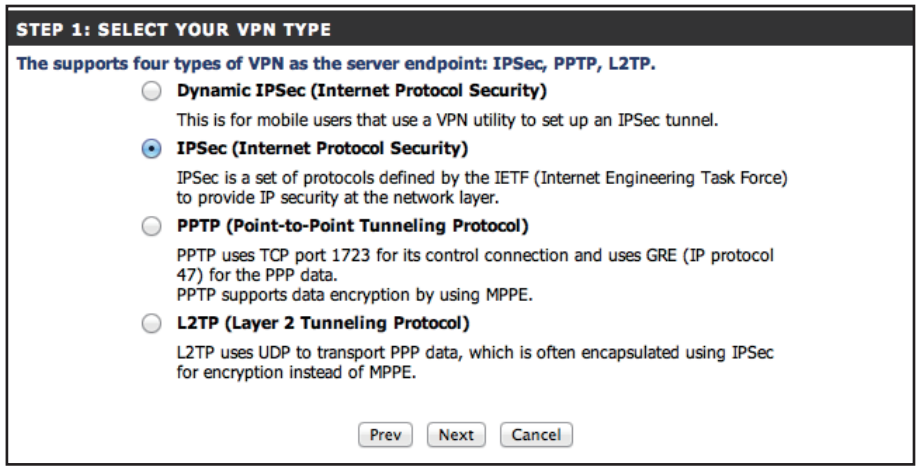
STEP 3: Enter the Local Subnet/Mask and the pre-shared key for your VPN, and click **Next**.



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

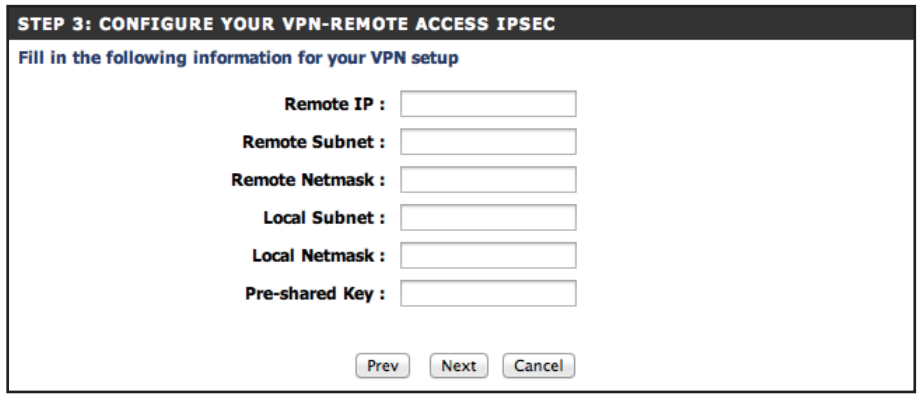
IPSec VPN

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



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

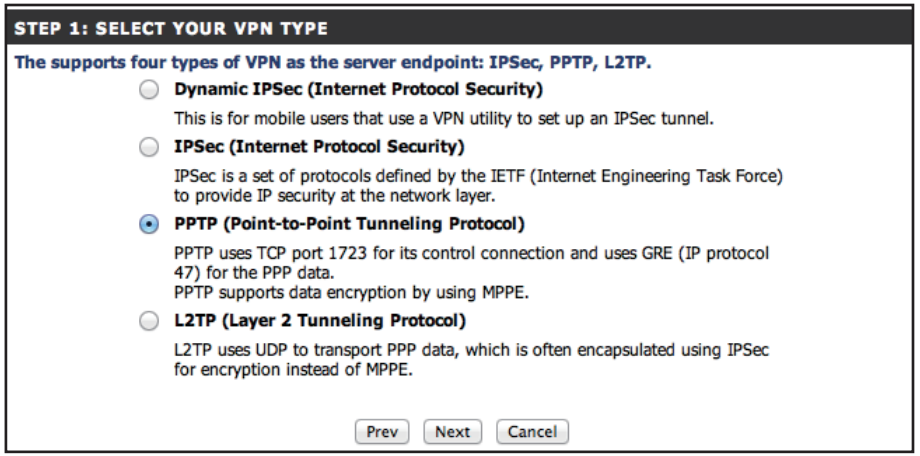
STEP 3: Enter the remote and local IP/subnet/masks and the pre-shared key for your VPN, and click **Next**.



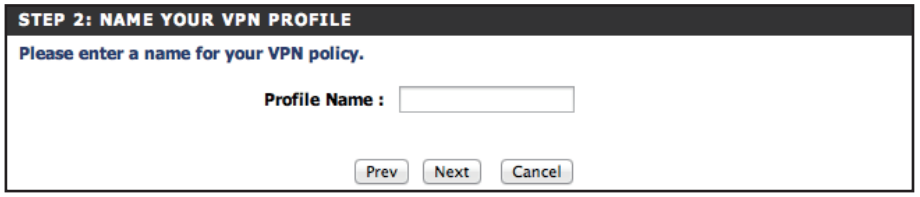
STEP 4: Click **Next** to restart the router. You have now completed the VPN Wizard Setup.

PPTP VPN

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

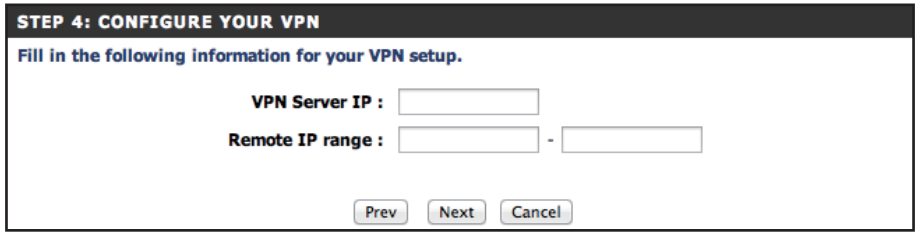


STEP 2: Give your VPN profile a name, and click **Next**.



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

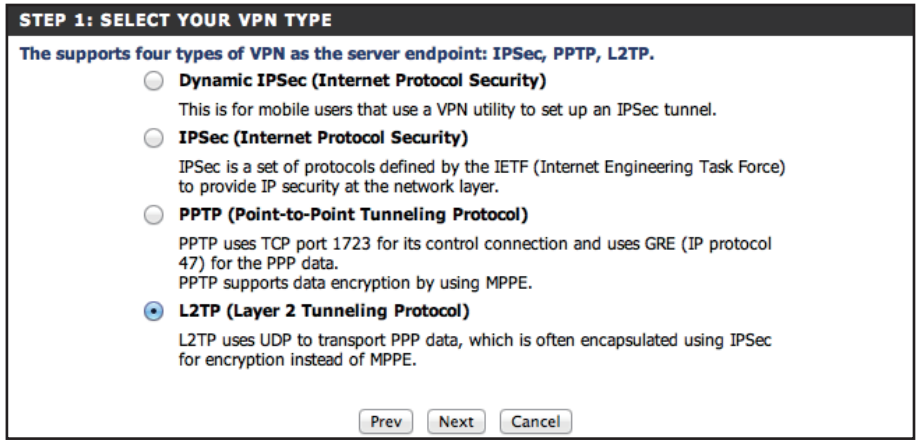
STEP 4: Enter a VPN server IP and remote IP range, and click **Next**.



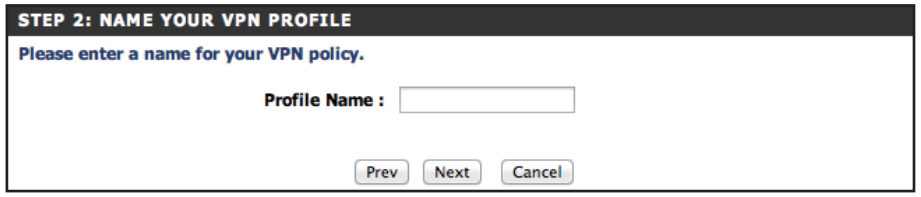
STEP 4: Click **Next** to restart the router. You have now completed the VPN Wizard Setup.

L2TP VPN

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

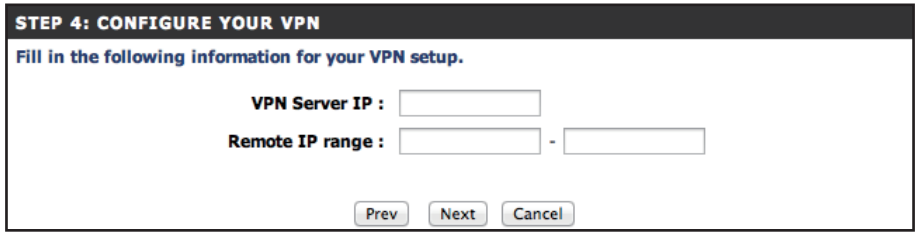


STEP 2: Give your VPN profile a name, and click **Next**.



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

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



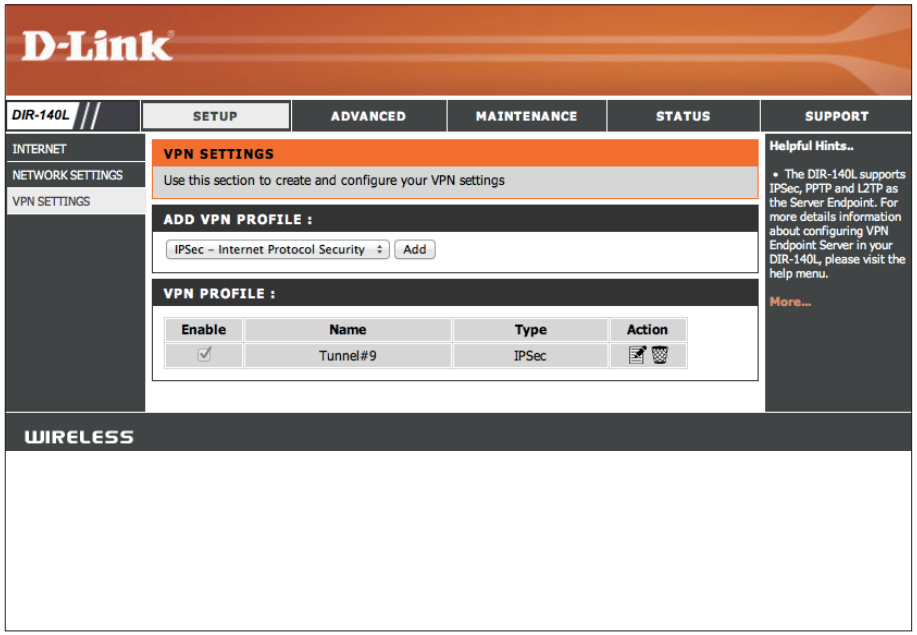
STEP 4: Click **Next** to restart the router. You have now completed the VPN Wizard Setup.

VPN Manual Settings

On this page you can set up advanced options for a Virtual Private Network (VPN). The DIR-140L 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**, **PPTP/L2TP**, or **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.



IPSec Settings

The DIR-140L 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.

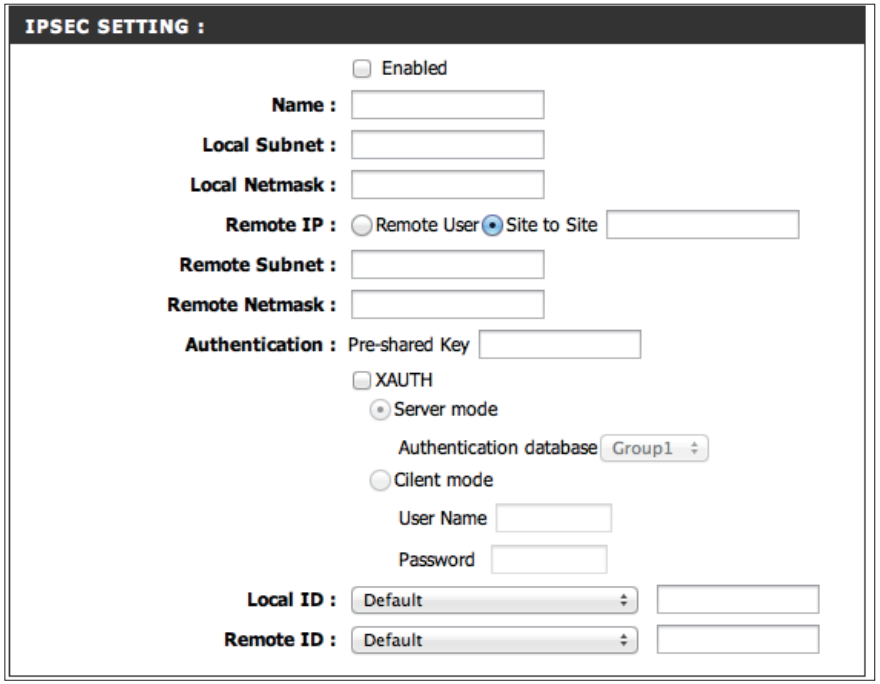
Remote Subnet/ Netmask: Enter the remote subnet and mask.

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.



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

Encapsulation Protocol: Enter the amount of time in seconds that the Phase 1 and Phase 2 keys should last.

PFS Group: Choose either **ESP**, **AH** or **ESP + AH** from the drop-down menu.

Aggressive Mode: **Enable** or **Disable** the PFS Group option using the drop-down menu. PFS is an additional security protocol.

Preshare Key: Select this option to configure IKE Phase 1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (This option is not recommended as it is less secure)

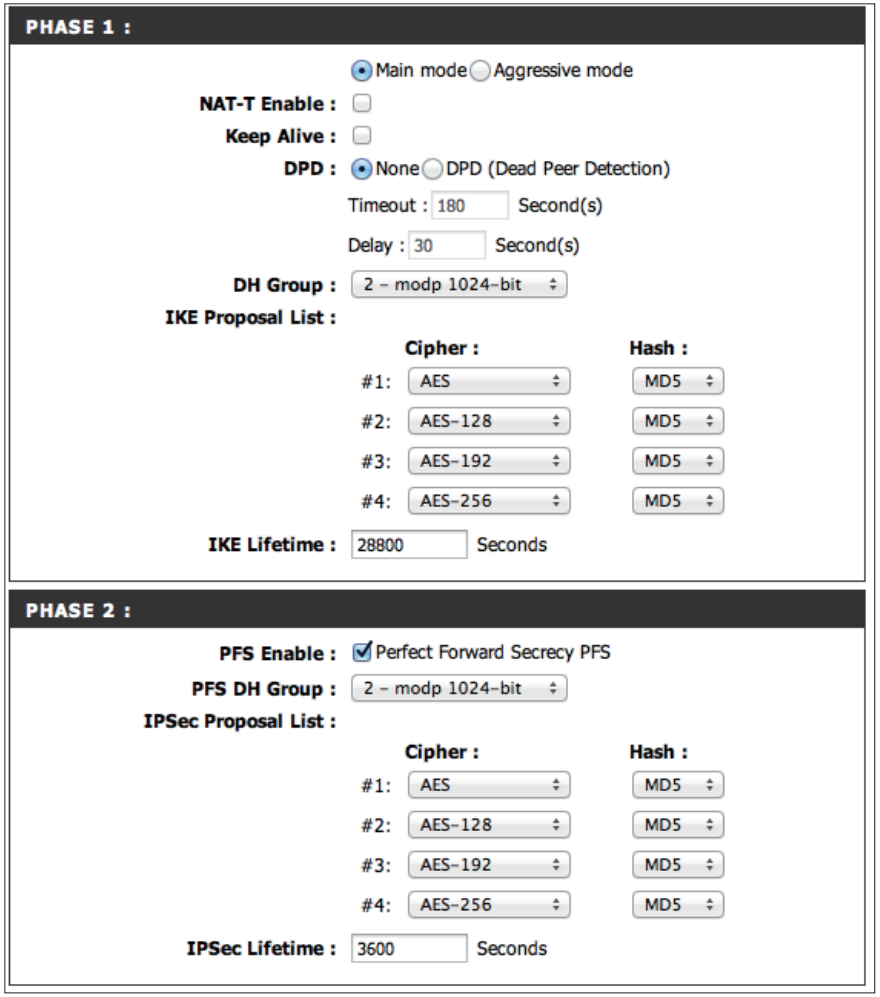
Connecting Type: Manually enter an ASCII passphrase in box.

Remote ID: Choose **Always on** or **Manual** from the drop-down menu.

IKE Proposal Settings: Choose from **Username**, **FQDN**, **User@FQDN**, or **Key ID** using the drop-down menu and then the ID in the box.

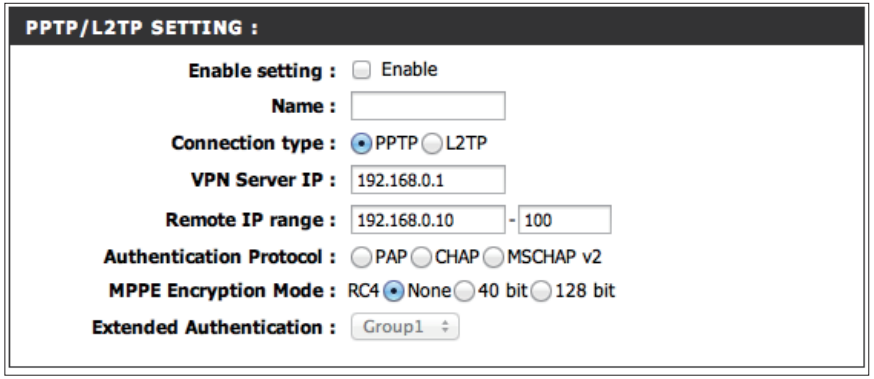
IPSEC Proposal Settings: Use this area to **Enable** IKE Proposals. Then determine the **Encryption** and **Authentification** types, as well as the **DH Group** from the drop-down menus.

Use this area to **Enable** IPSec Proposals. Then determine the **Encryption** and **Authentification** types from the drop-down menus.



PPTP/L2TP Settings

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



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.

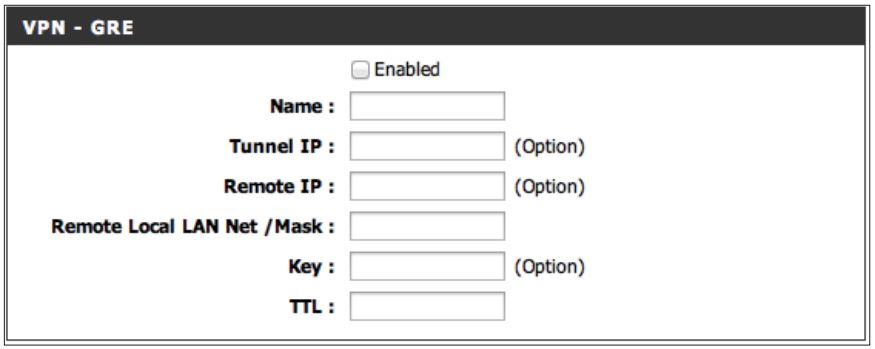
Authentification Protocol: Choose **PAP**, **CHAP**, or **MSCHAP v2** for your authentification.

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.

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.

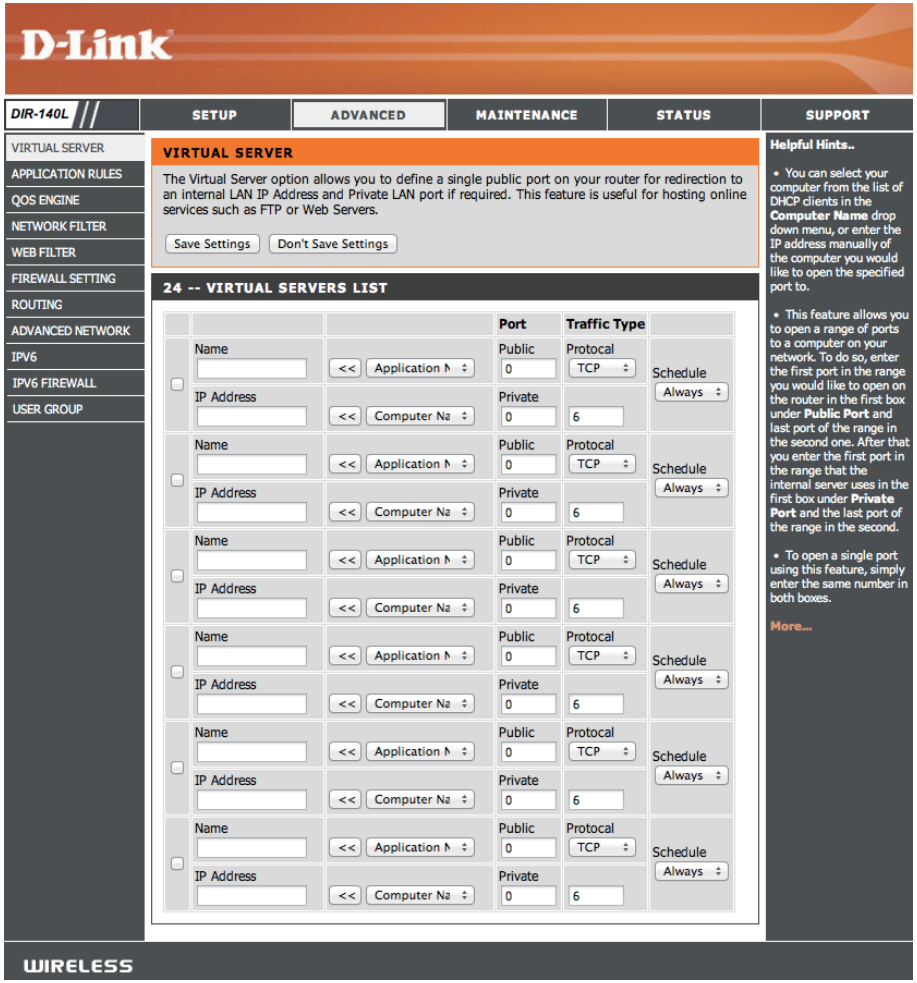
Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

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.



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-140L. 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.

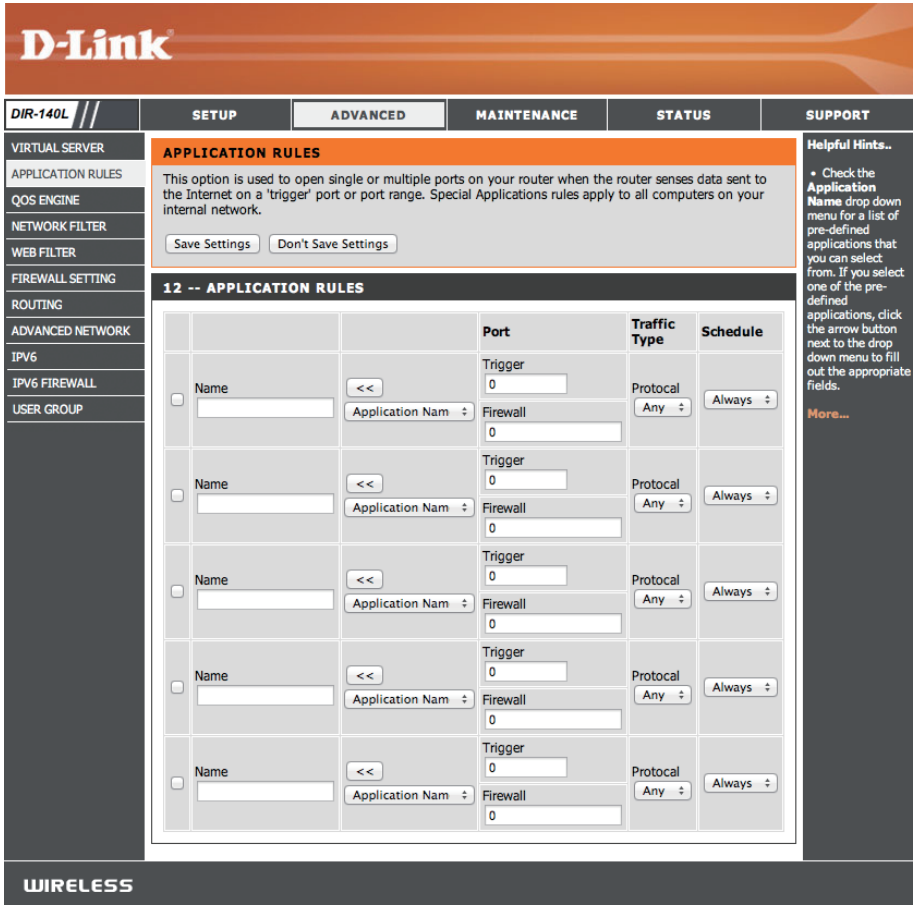
Name: Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click.

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: Schedule the time when Application Rules 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.



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.

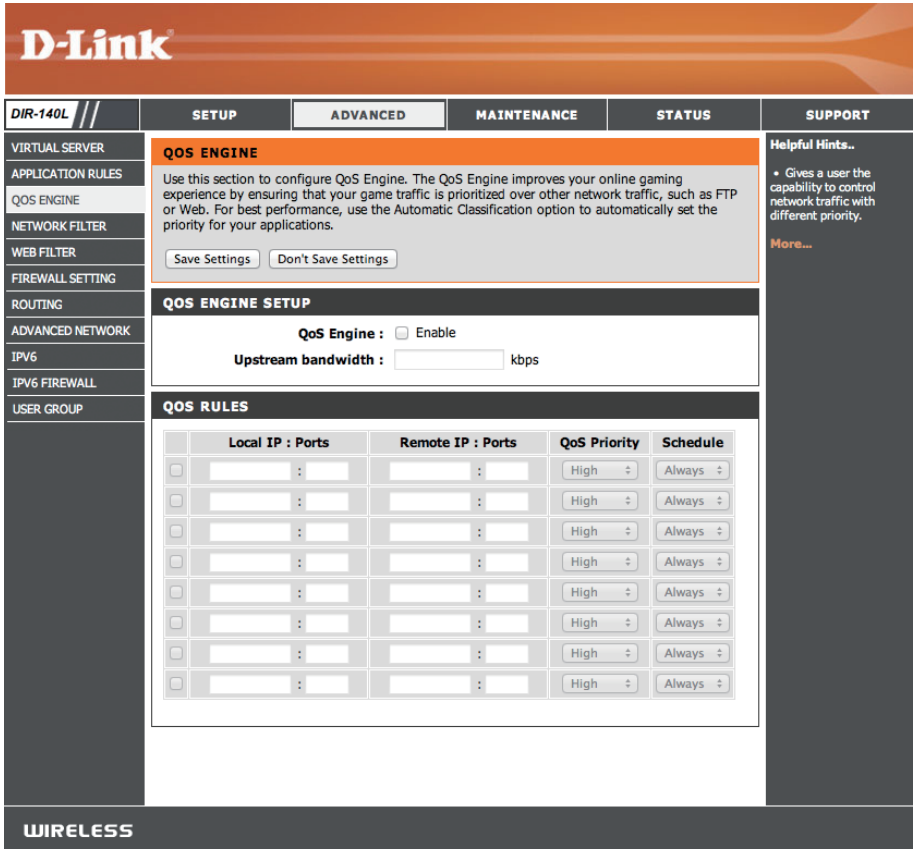
The QoS Engine supports overlaps between rules, where more than one rule can match for a specific message flow. If more than one rule is found to match the rule with the highest priority will be used.

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.



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 Filters

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

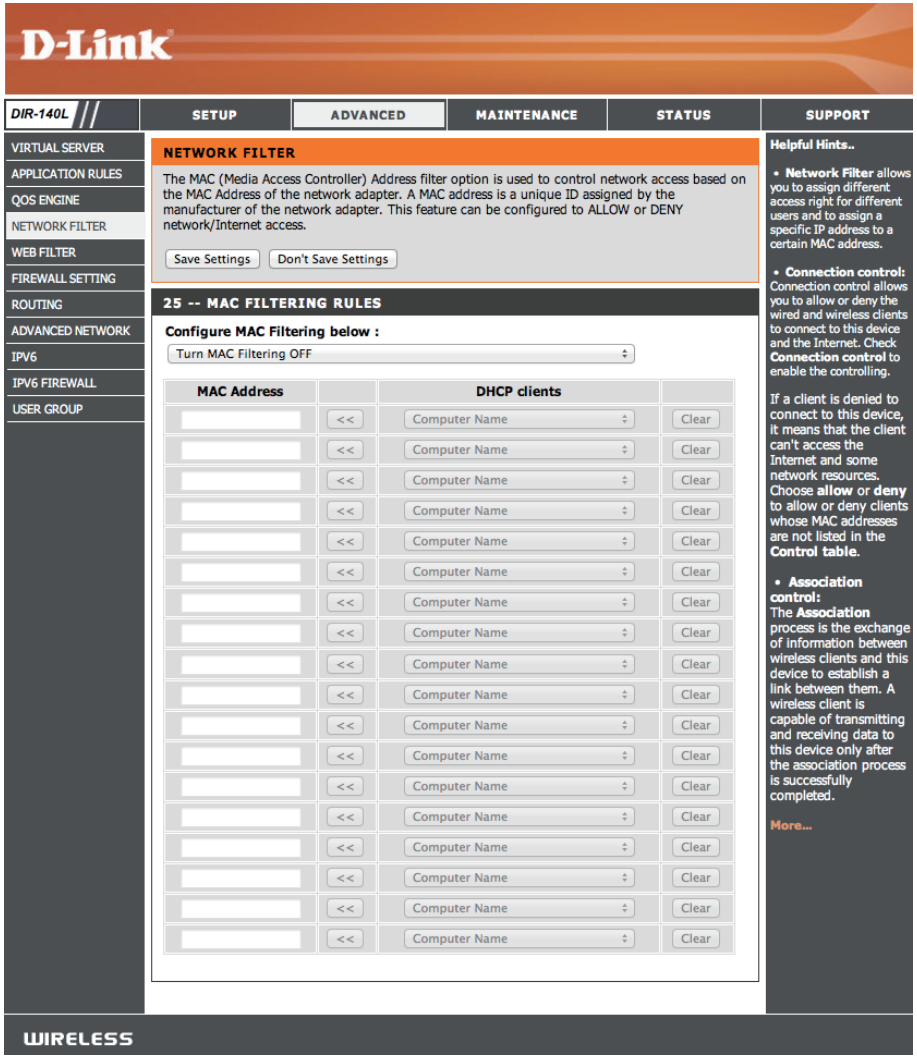
Configure MAC Filtering: Select **Turn MAC Filtering Off**, **Allow MAC addresses listed below**, or **Deny MAC addresses listed below** from the drop-down menu.

MAC Address: Enter the MAC address you would like to filter.

To find the MAC address on a computer, please refer to the *Networking Basics* section in this manual.

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

Clear: Click to remove the MAC address.



Website Filters

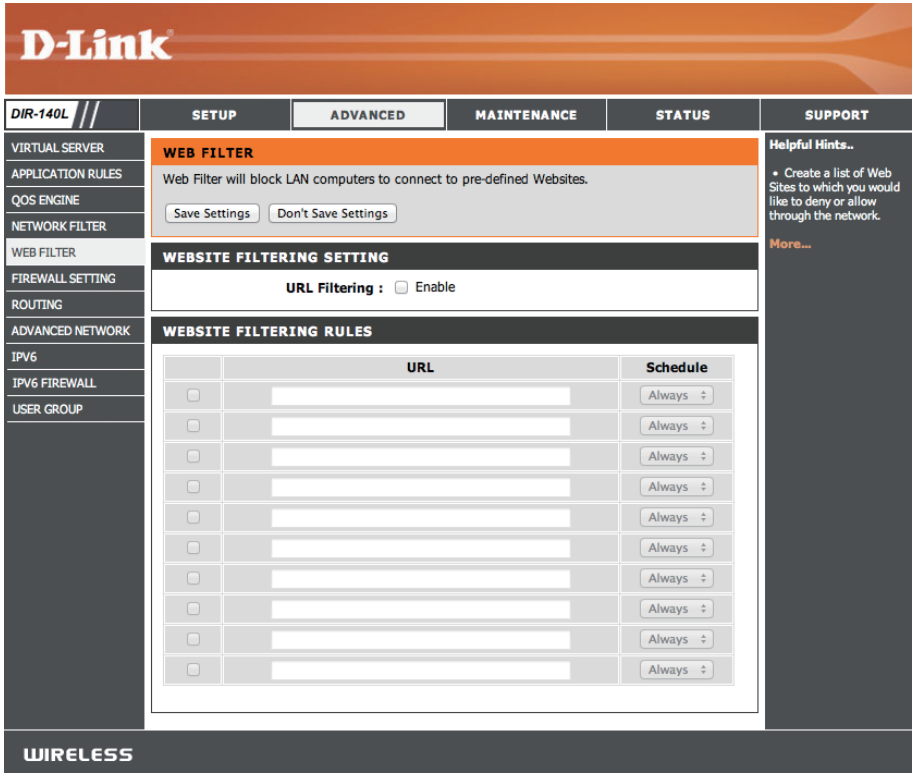
Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control*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

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.



Firewall Settings

A firewall protects your network from the outside world. The DIR-140L offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

Enable 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.

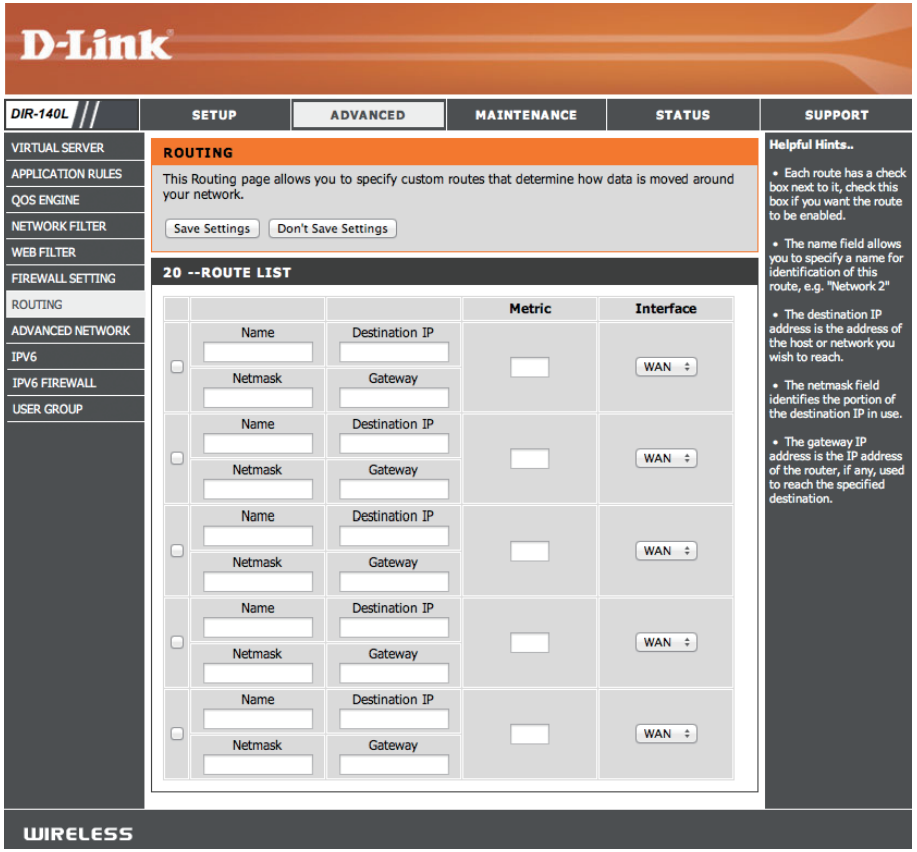
Destination IP: Enter the IP address of packets that will take this route.

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.



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.

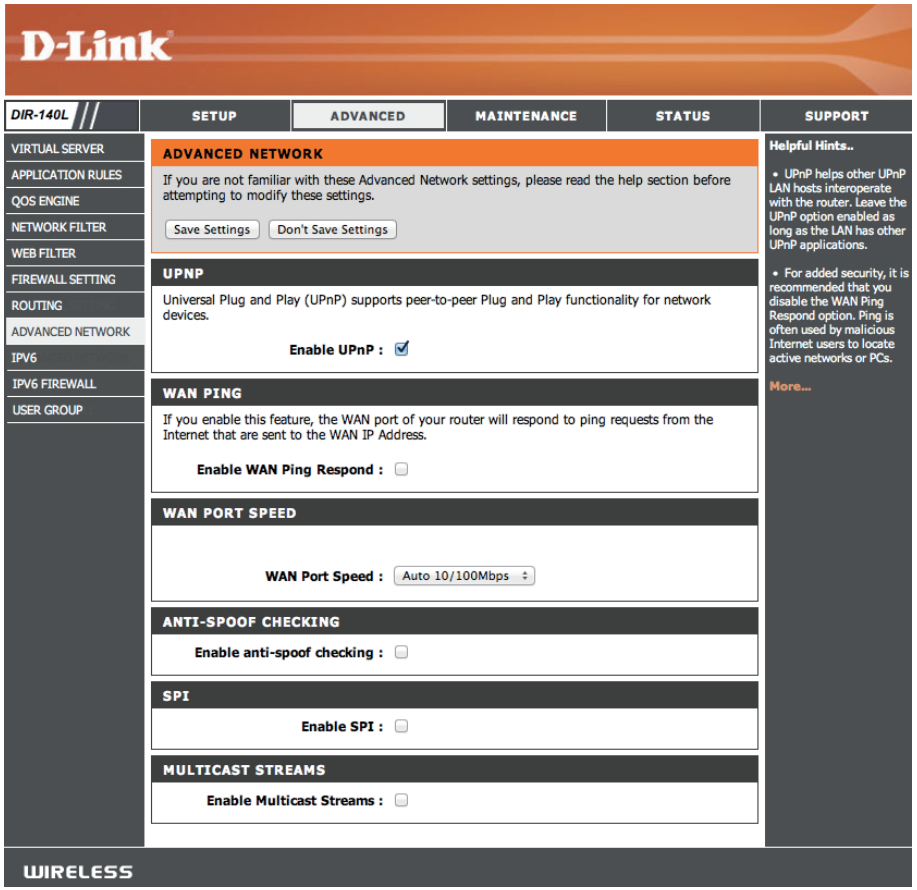
Enable WAN Ping Respond: Checking the box will allow the DIR-140L to respond to pings. Unchecking the box may provide some extra security from hackers.

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.



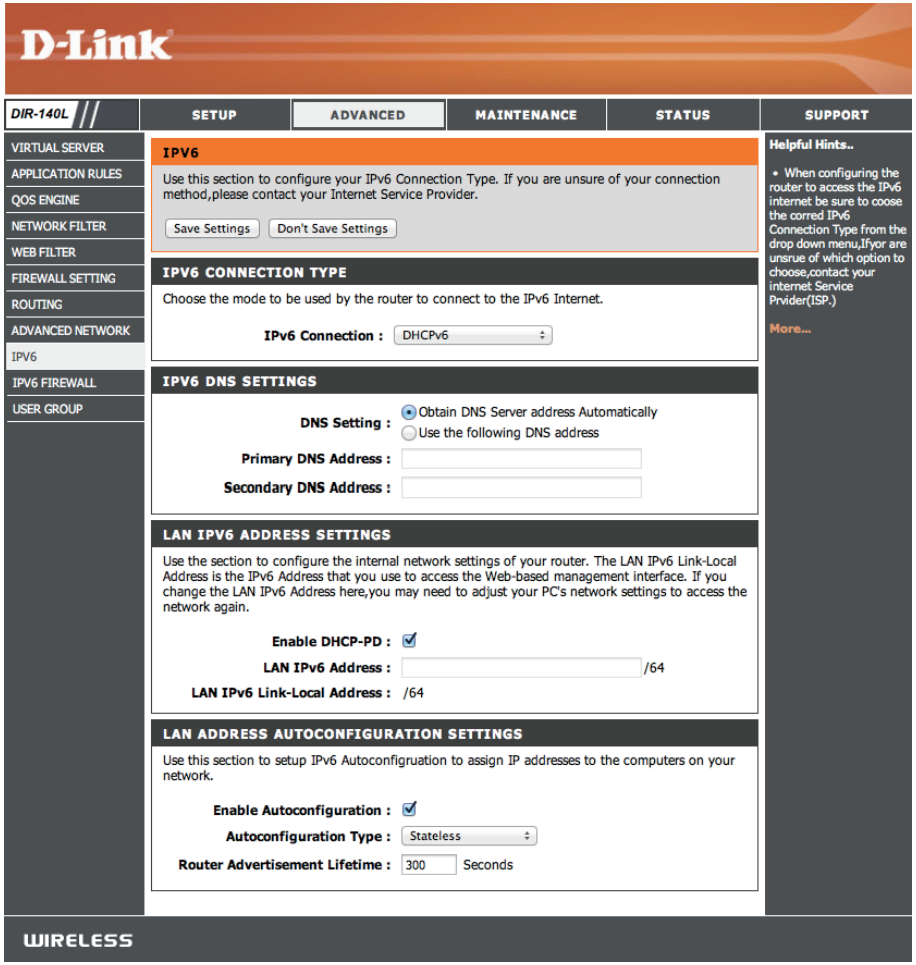
IPv6

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

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

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

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

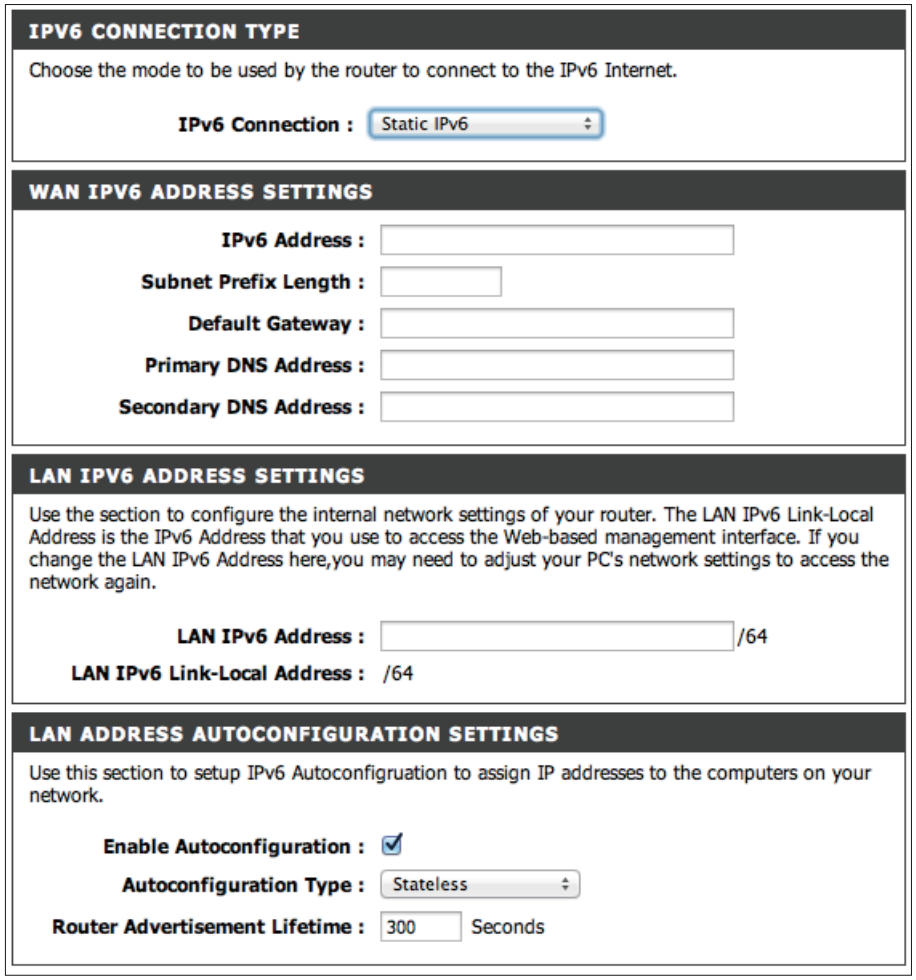
LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

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).



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.

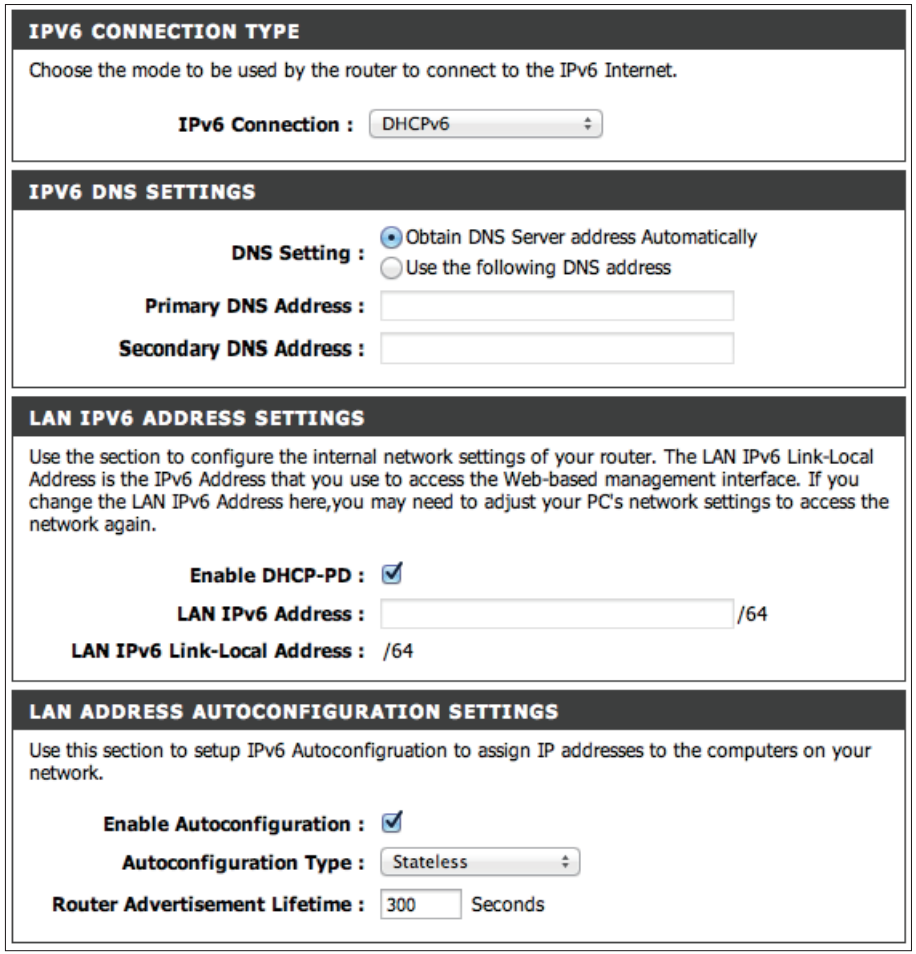
LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

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).



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.

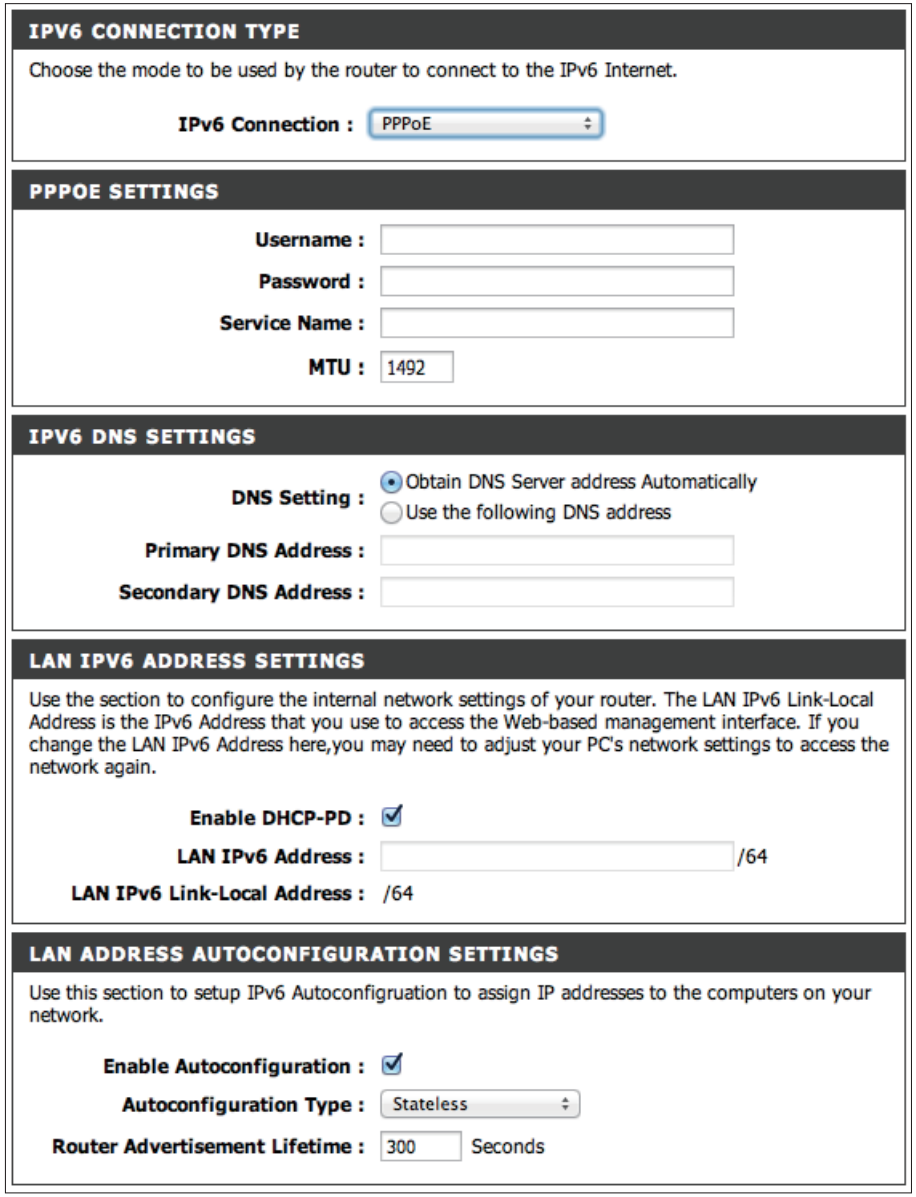
LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

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 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.

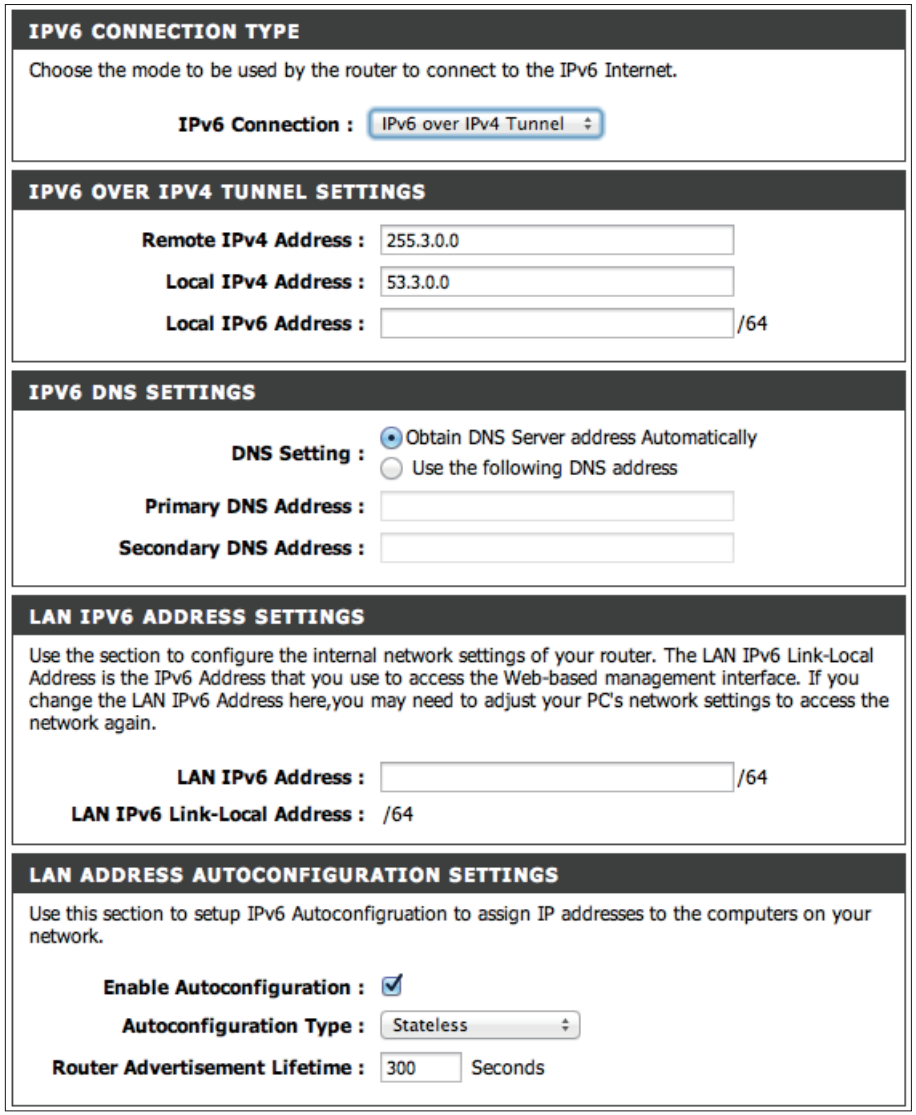
LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

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).



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.

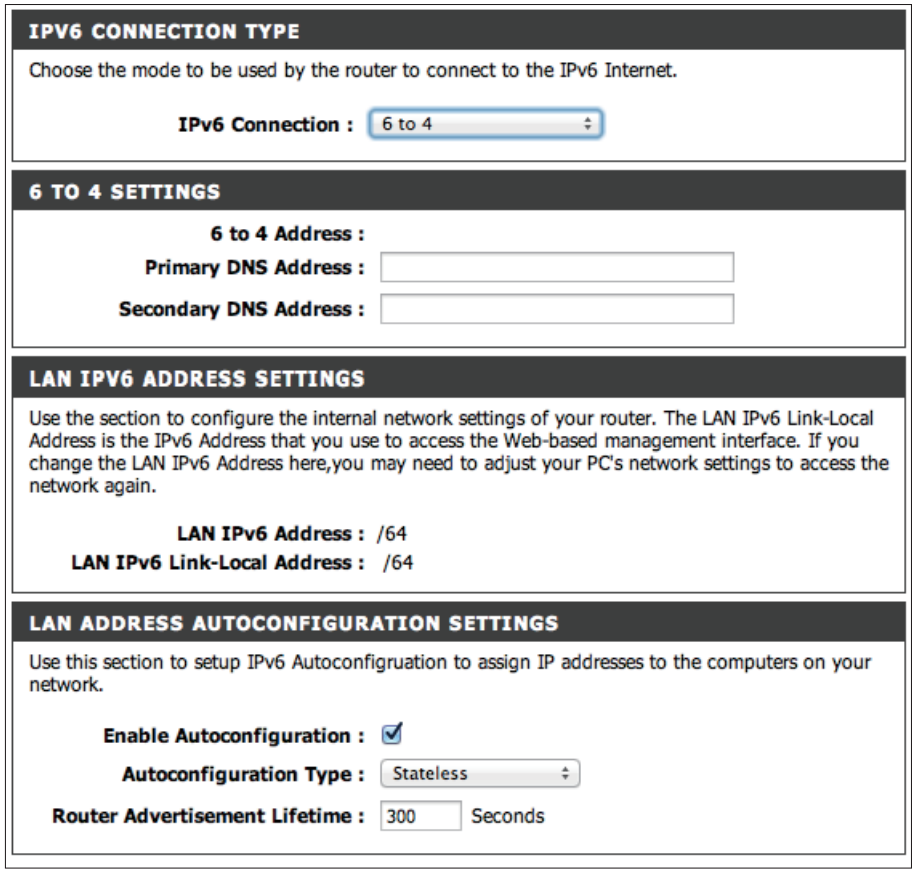
LAN IPv6 Address: Displays the LAN (local) IPv6 address for the router.

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).



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.

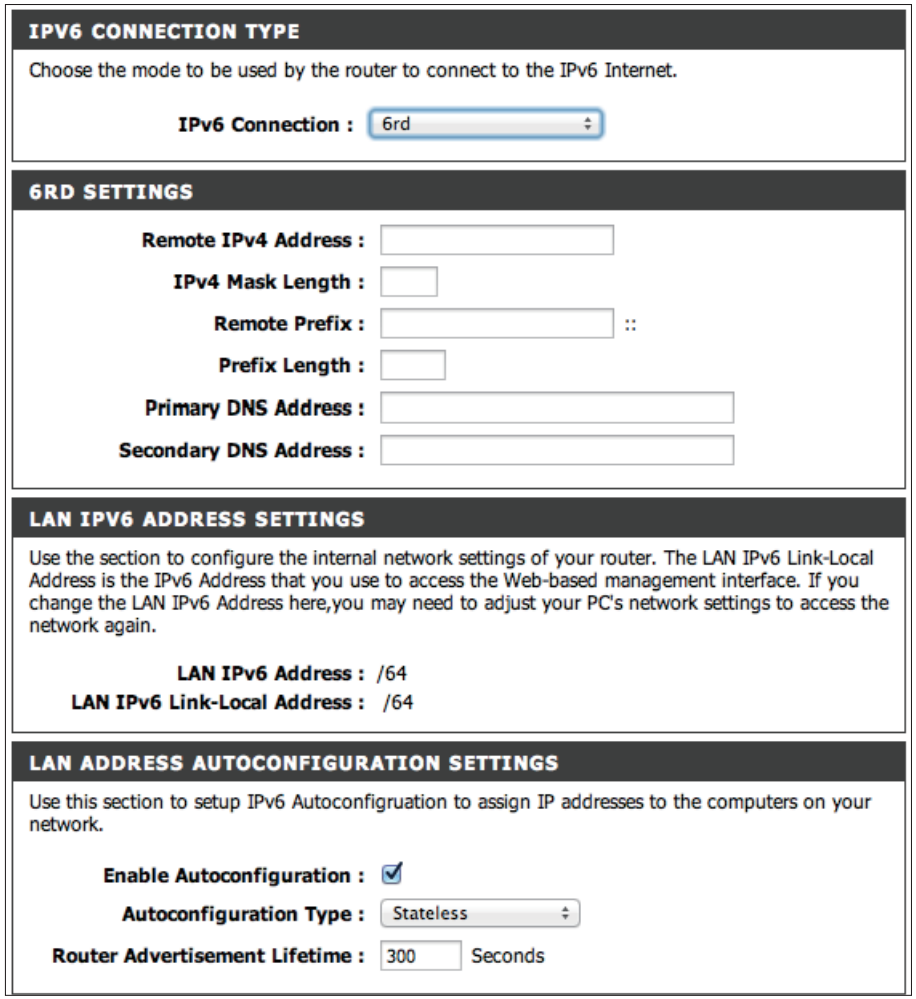
LAN IPv6 Address: Displays the LAN (local) IPv6 address for the router.

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.

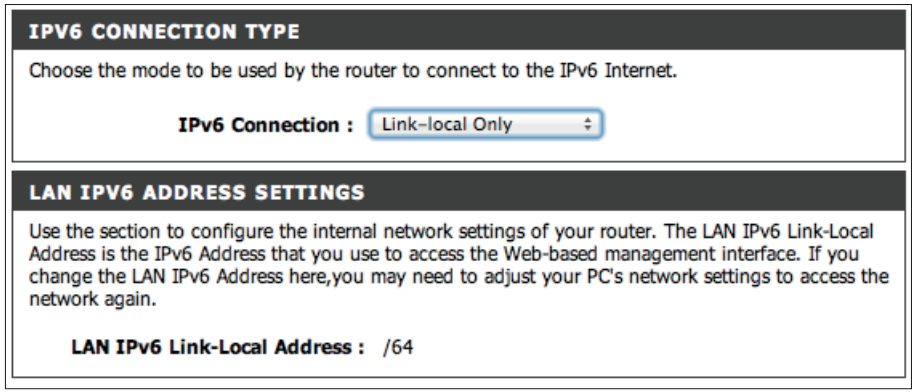
Router Advertisement Lifetime: Enter the IPv6 address lifetime (in seconds).



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 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.

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.

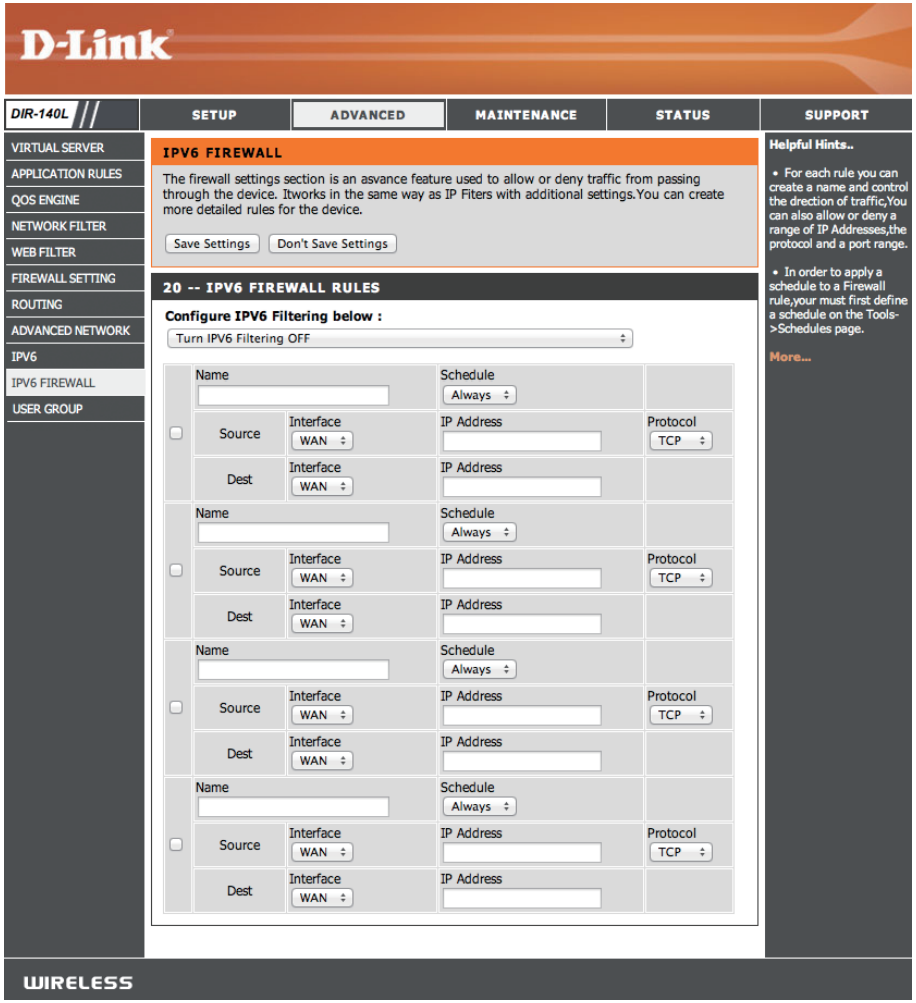
Schedule: Use the drop-down menu to select the time schedule that the IPv6 Firewall Rule will be enabled on. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.

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.

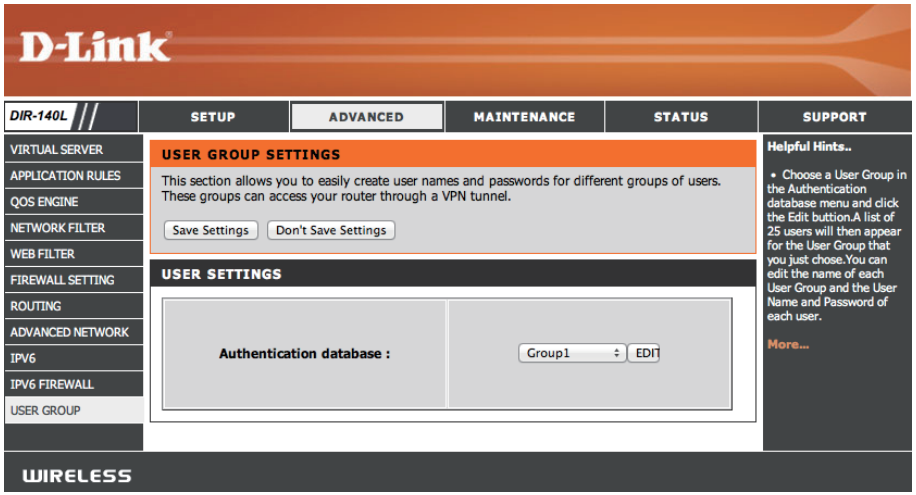


User Group

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.



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.

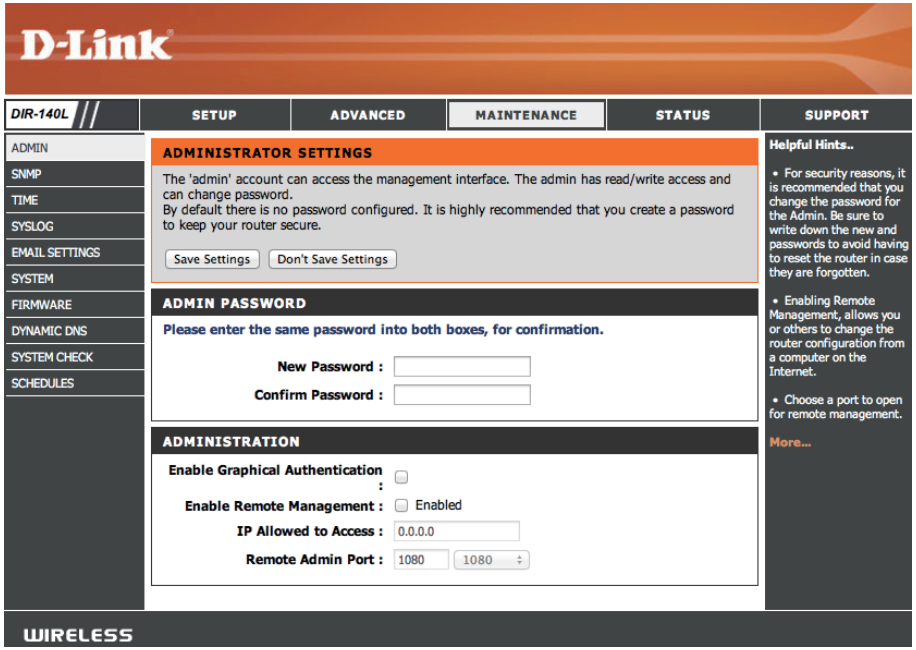
Admin Password: Enter a new password for the Administrator Login Name. And type it again in the next box.

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

Enable Remote Management: Remote management allows the DIR-140L 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-140L.

Remote Admin Port: Enter the port number used to access the DIR-140L 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-140L and 8080 is the port used for the Web Management interface.



SNMP

The DIR-140L 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.

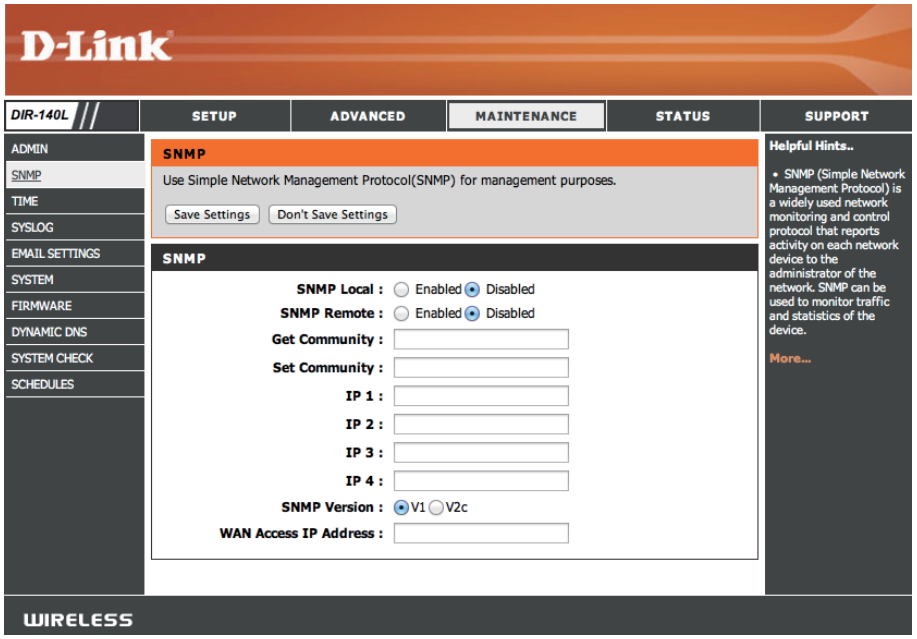
Get Community: Enter a name for the read community of your SNMP server.

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.



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.

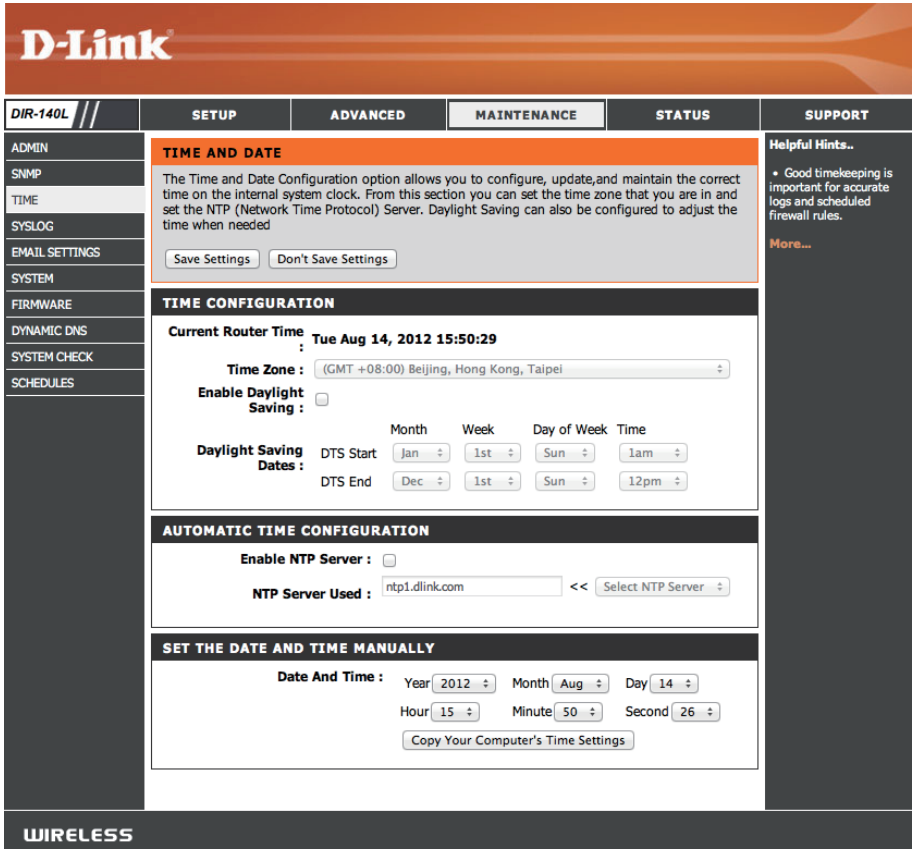
Daylight Saving Dates: If Daylight Saving is enabled, you may specify the date it begins and ends.

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.



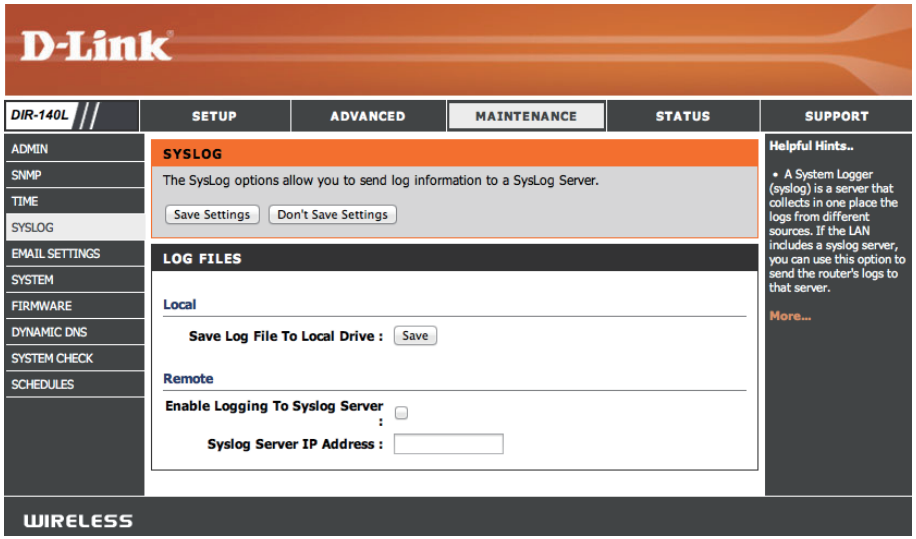
SysLog

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).



Email Settings

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

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

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.

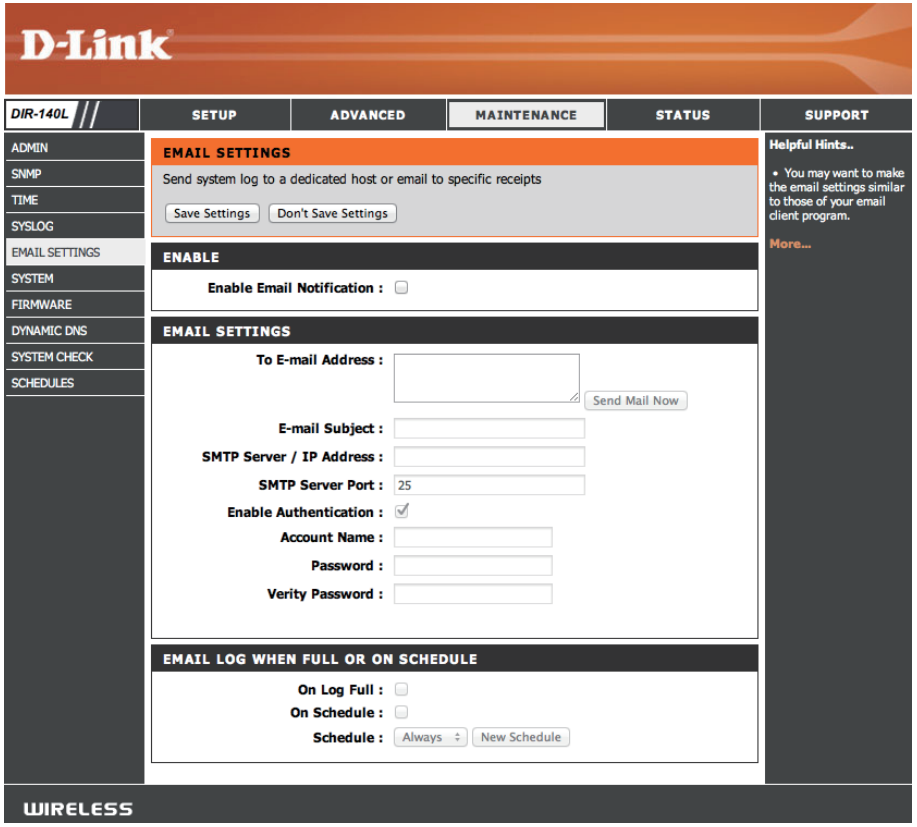
Enable Authentication: Check this box if your SMTP server requires authentication.

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**.

System

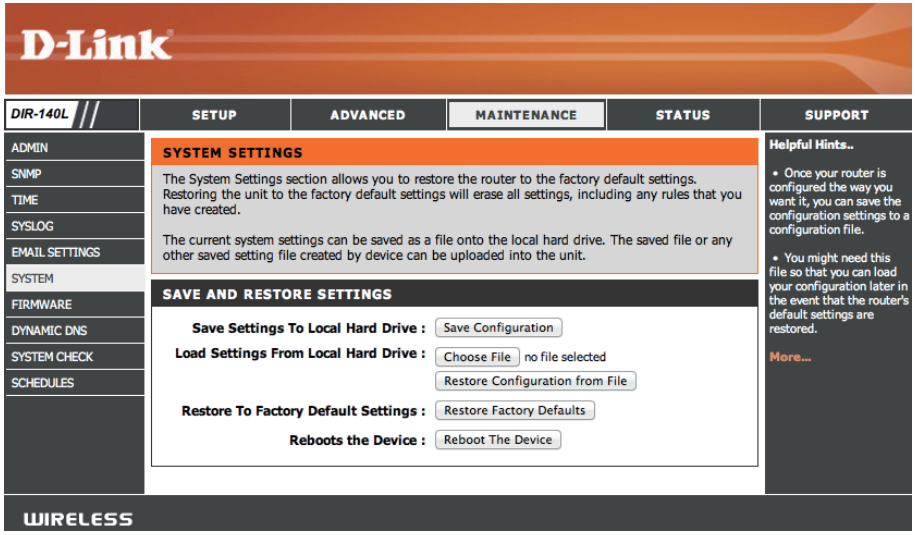
This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

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

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

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

Reboot Device: Click to reboot the router.



Firmware

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

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

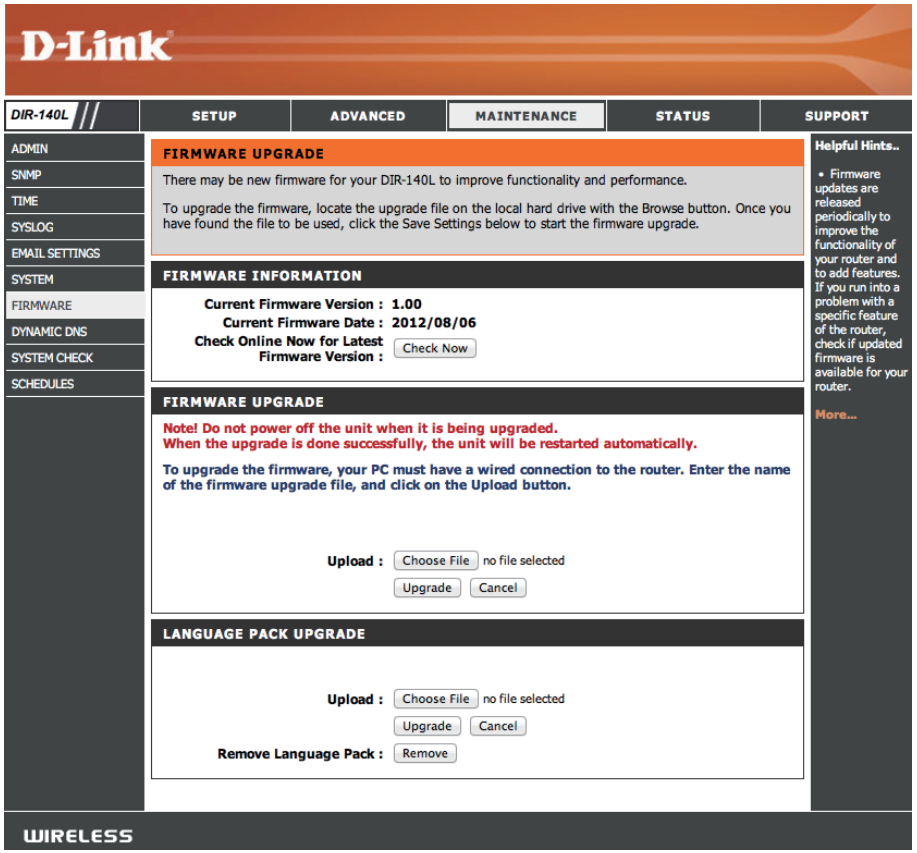
Choose File: After you have downloaded the new firmware, click **Choose File** to locate the firmware update on your hard drive.

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.



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.

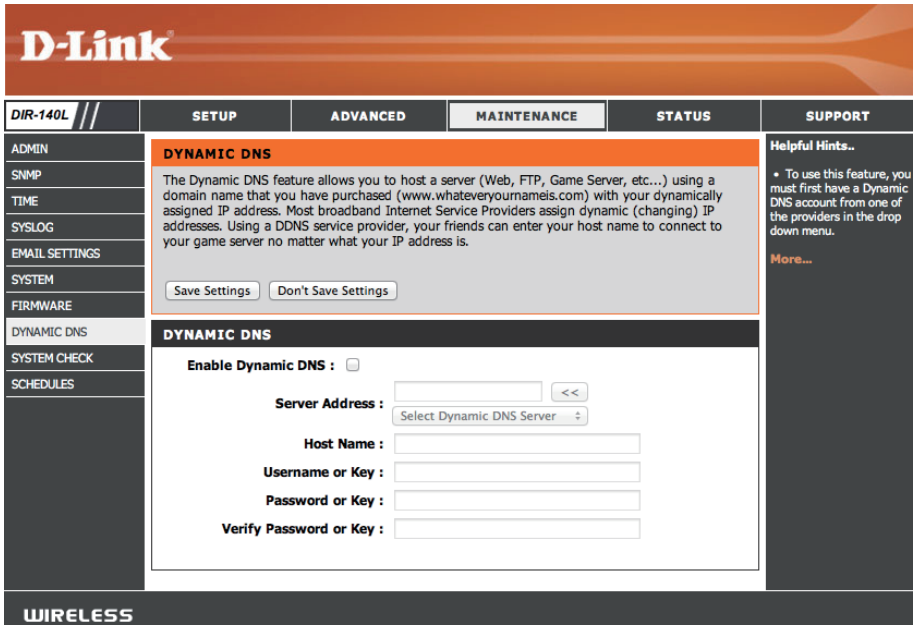
Enable Dynamic DNS: Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.

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.

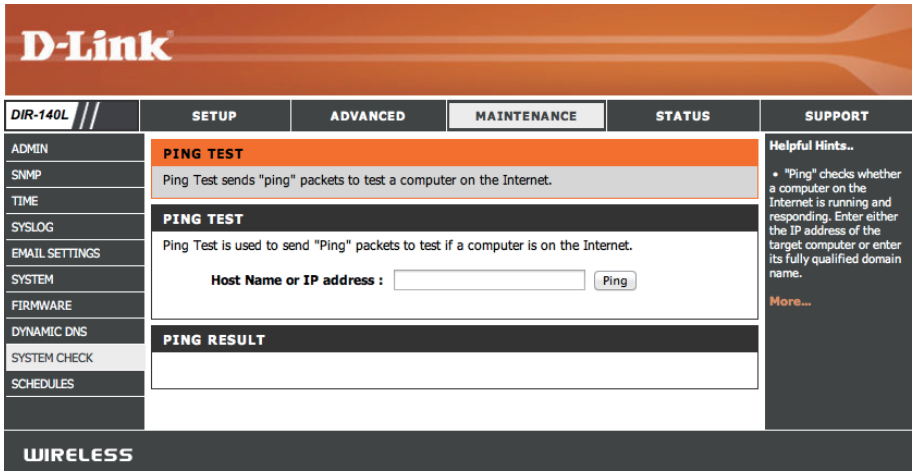
Password or Key: Enter the Password or key for your DDNS account.



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.



Schedules

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

Name: Enter a name for your new schedule.

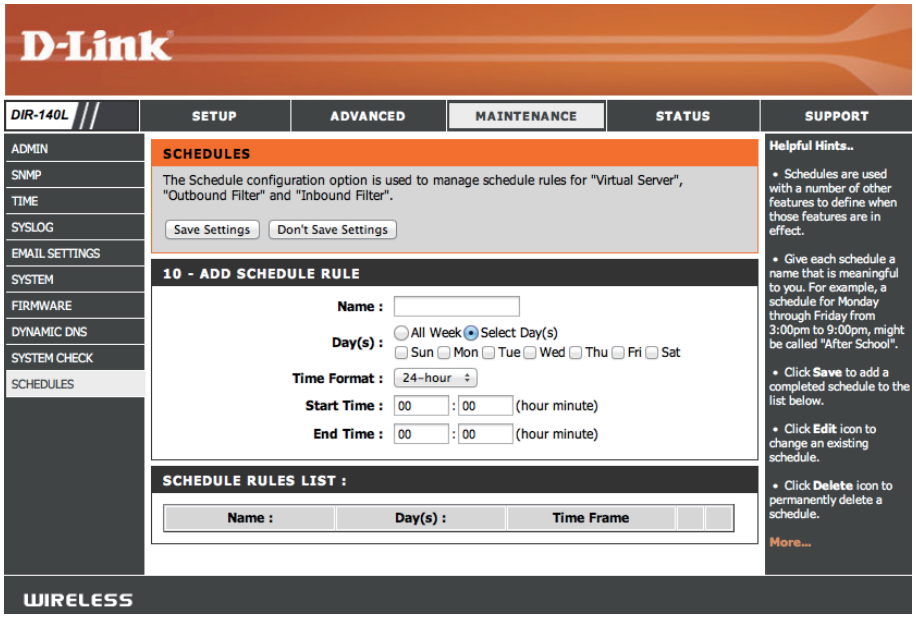
Days: Select a day, a range of days, or All Week to include every day.

Time 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.



Status
Device Info

This page displays the current information for the DIR-140L. It will display the LAN and WAN (Internet) 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.

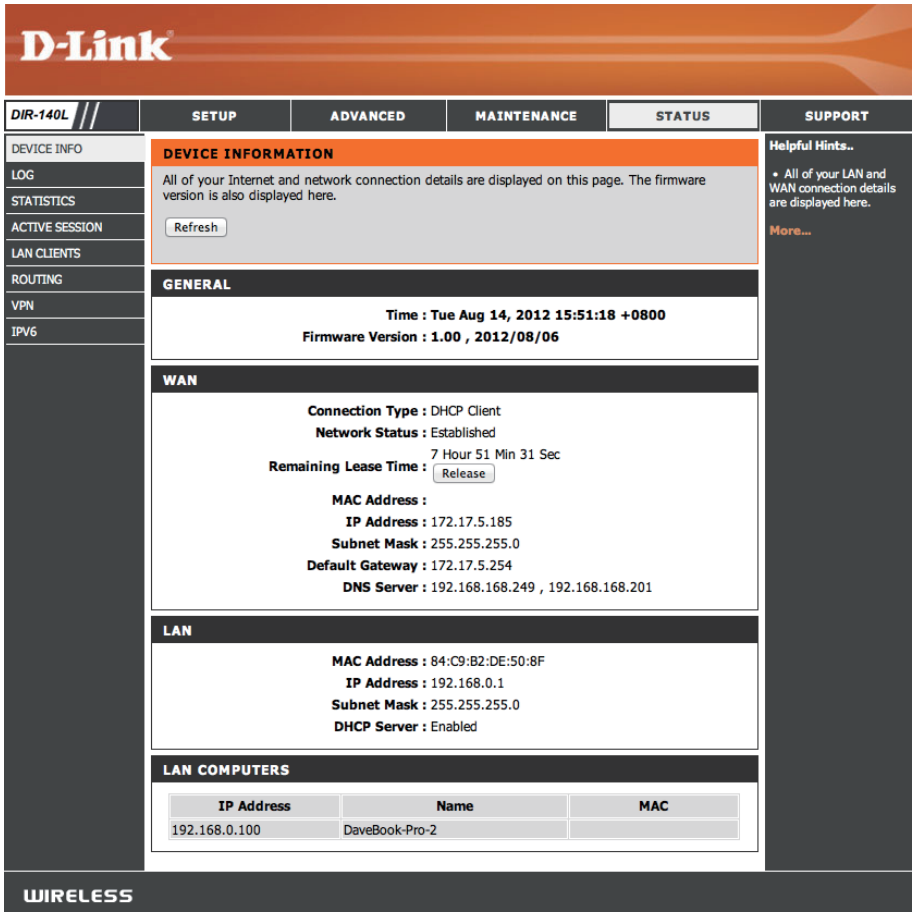
If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

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).



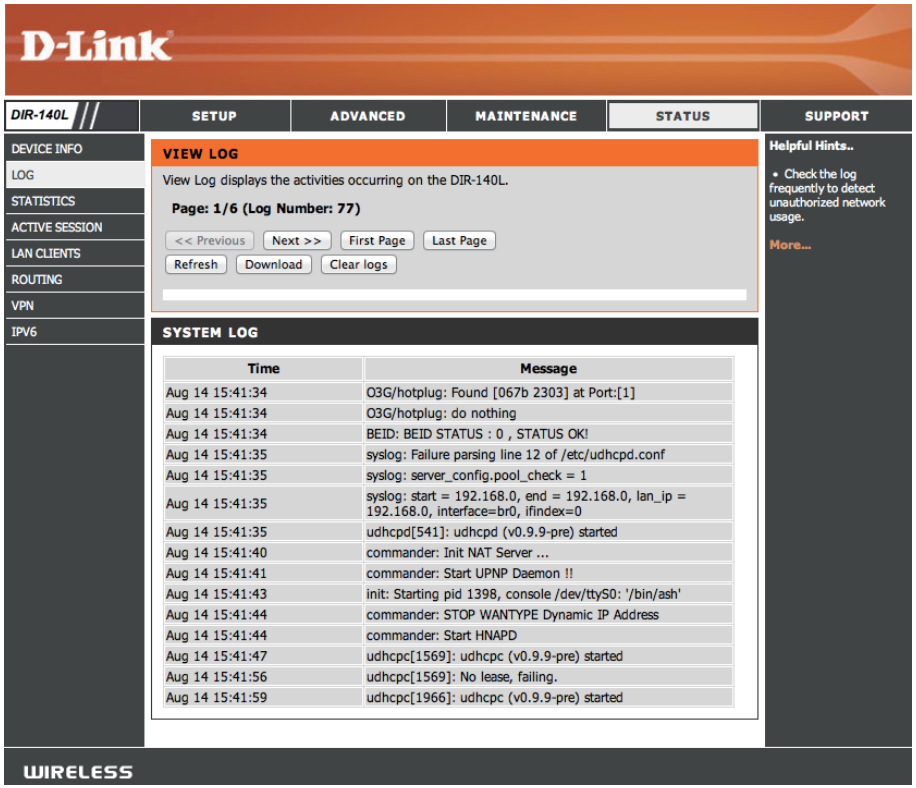
Log

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.

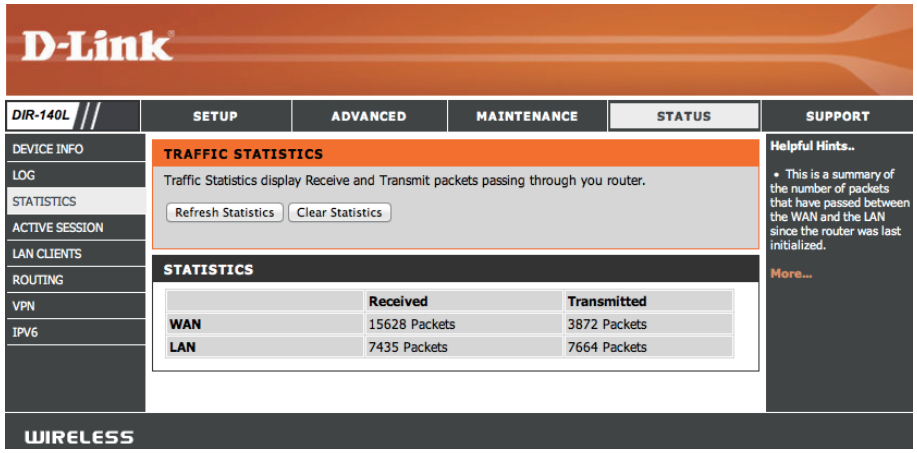
Download: This option will save the router log to a file on your computer.

Clear Logs: Clears all of the log contents.



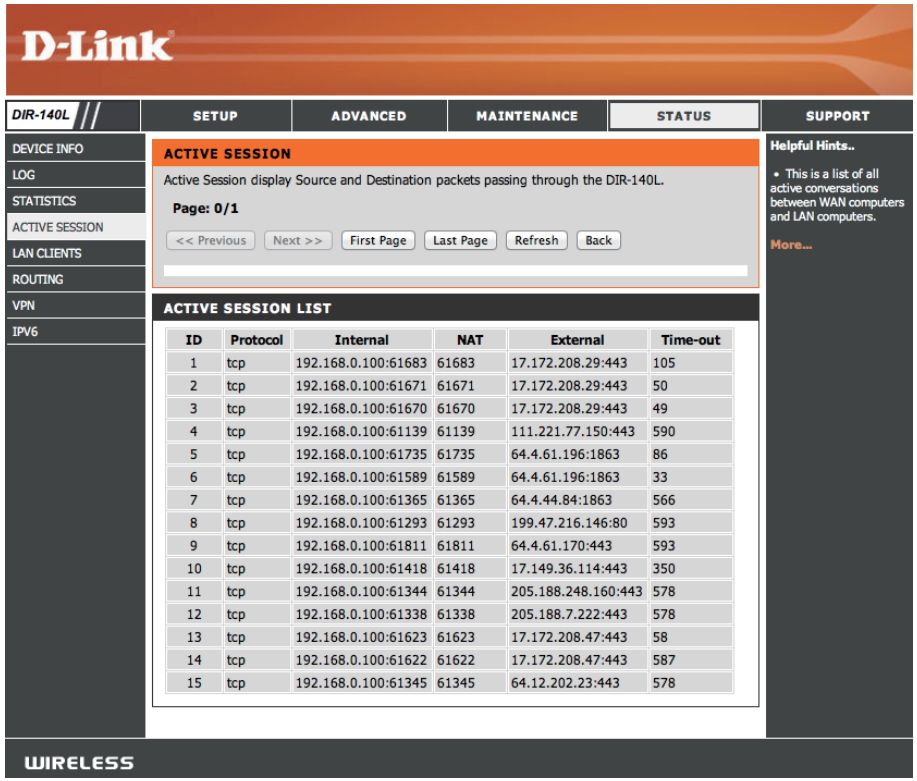
Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-140L on both the WAN and LAN ports. The traffic counter will reset if the device is rebooted.



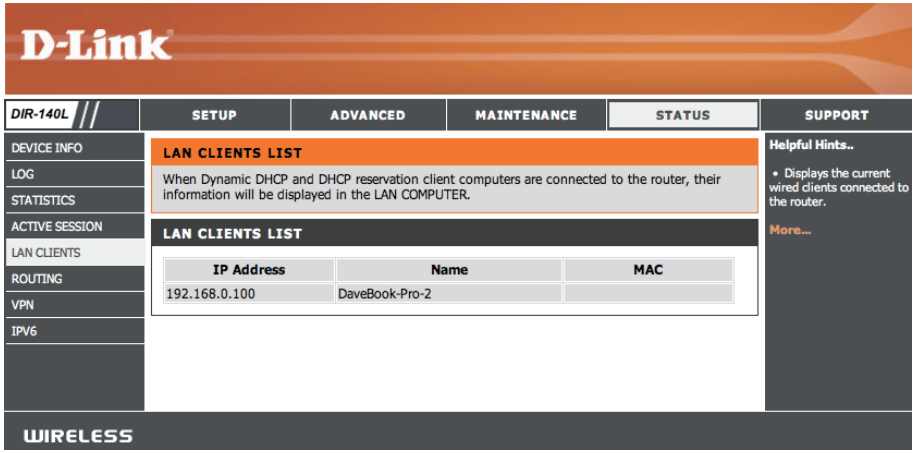
Active Session

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.



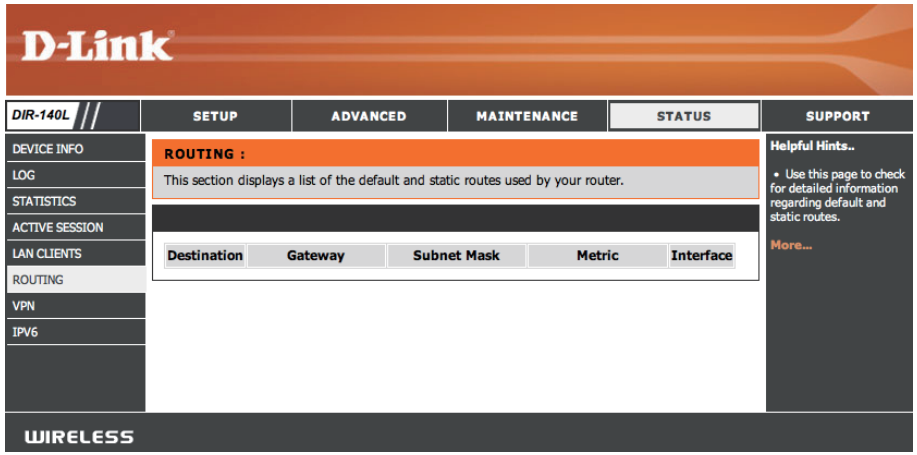
LAN Clients

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



Routing

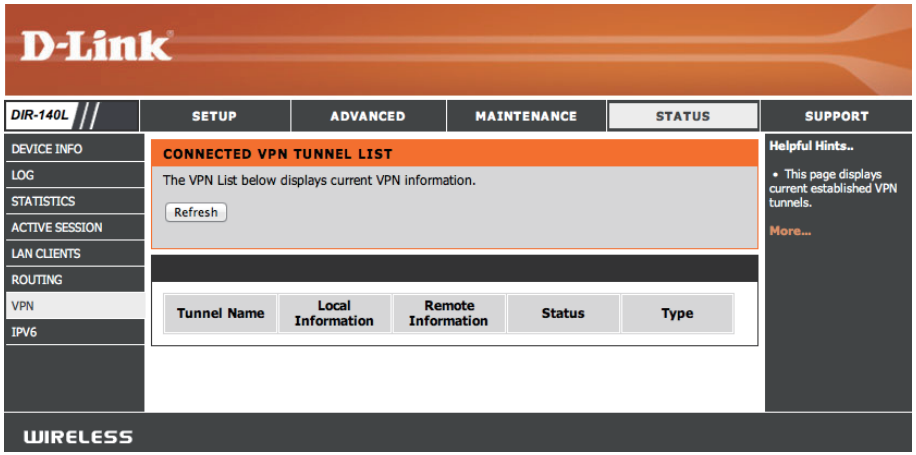
This page will display your current routing table.



VPN

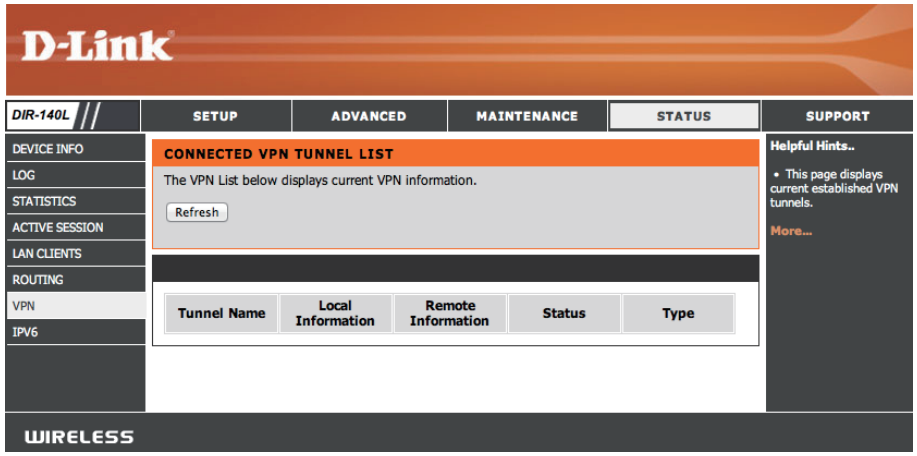
This page is where the router displays information on the the current VPN tunnels.

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

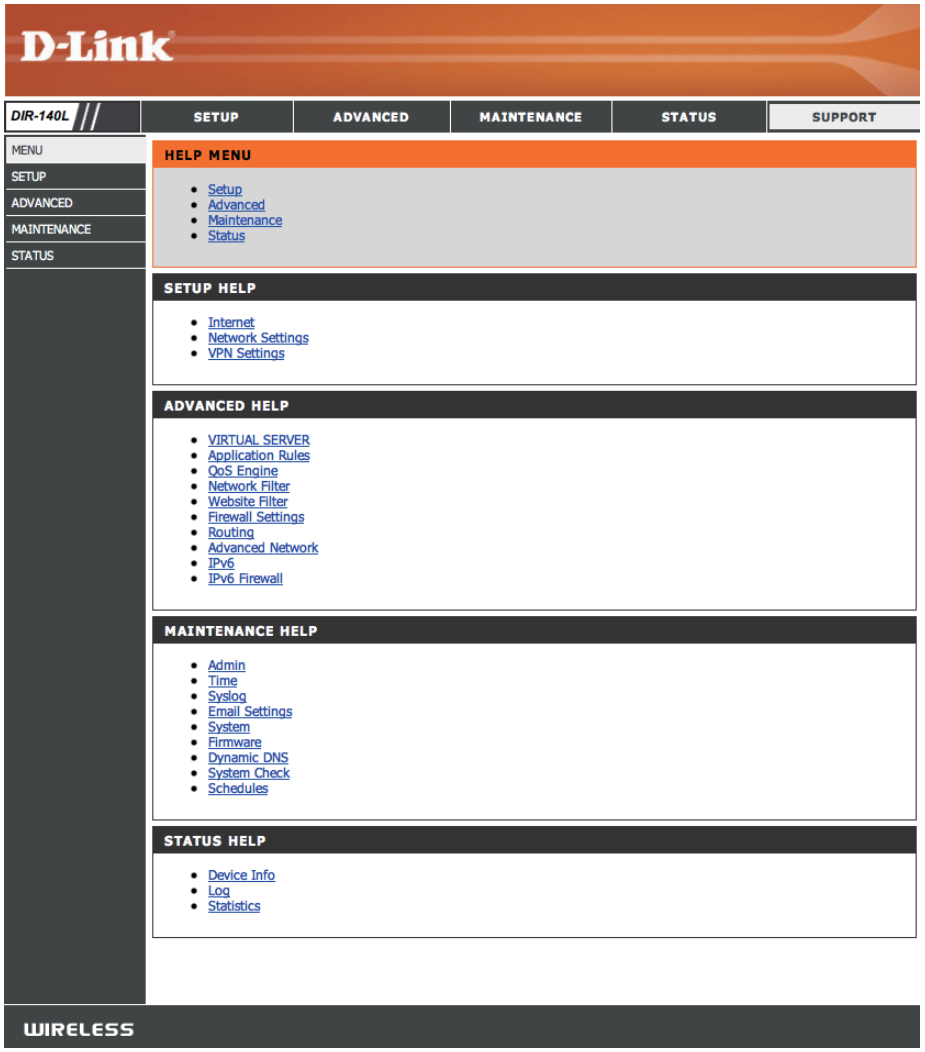


IPv6

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



Support


D-Link
DIR-140L
SETUP
ADVANCED
MAINTENANCE
STATUS
SUPPORT
MENU
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP MENU
Setup
Advanced
Maintenance
Status
SETUP HELP
Internet
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-140L. 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**.

Networking Basics

Check your IP address

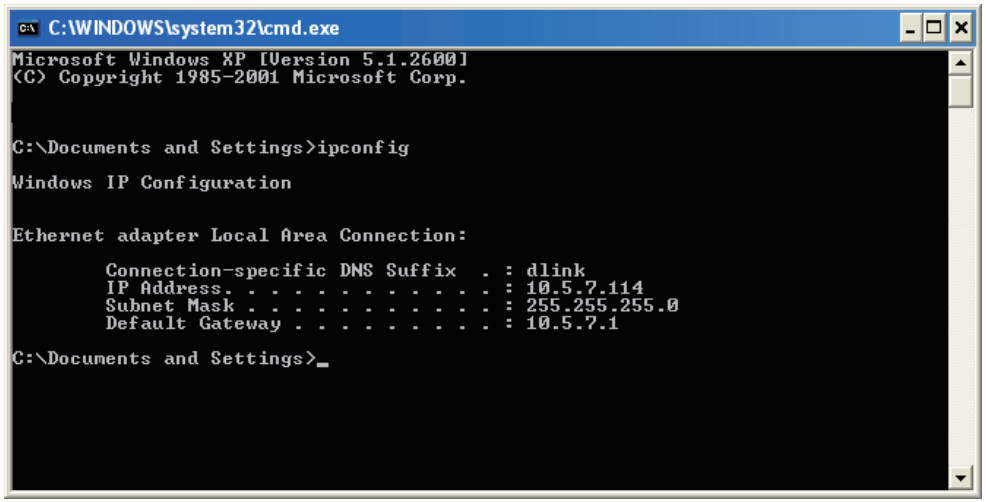
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server automatically. To verify your IP address, please follow the steps below.

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.



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**.

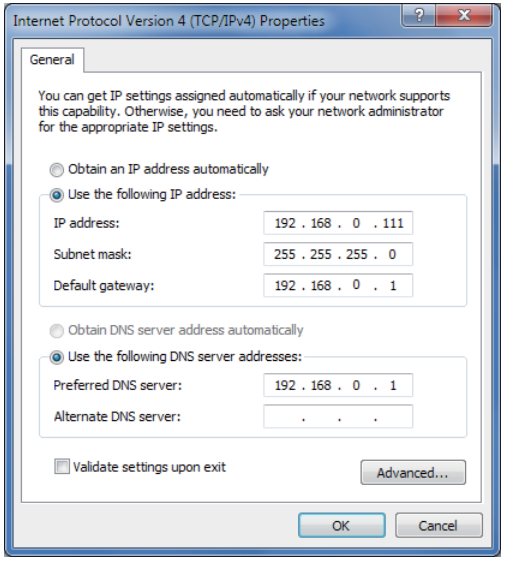
Step 2
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

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.



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

Technical Specifications

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

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 Maintenance 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.

Contacting Technical Support

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

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

- Model number of the product (e.g. DIR-140L)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the router).

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

For customers within the United States:

Phone Support:
(877) 354-6555

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(800) 361-5265

Internet Support:
http://support.dlink.ca

Warranty

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

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

Limited Warranty:

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

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

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

Limited Software Warranty:

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

Non-Applicability of Warranty:

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

Submitting A Claim:

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-354-6555, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

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

What Is Not Covered:

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

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

Disclaimer of Other Warranties:

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

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

Limitation of Liability:

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

Governing Law:

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

Trademarks:

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

Copyright Statement:

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

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.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Registration

Register your product online at registration.dlink.com

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