# USER MANUAL

## DIR-130

VERSION 1.2

D-Link®

WIRED

# Manual Overview

This manual contains the following sections:

**Section 1 -** “Product Overview” describes what is included with the DIR-130 router, and things to consider before installing (page 1).

**Section 2 -** “Installation” describes how to install the router on your network (page 6).

**Section 3 -** “Configuration” describes how to configure the settings on your DIR-130 router (page 10).

**Section 4 -** “Troubleshooting” explains how to resolve common issues (page 58).

**Section 5 -** “Appendix” contains networking basics, technical specifications, technical support information, warranty, GNU general public license, and registration information (page 62).

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 | February 8, 2007 | • DIR-130 Revision A1 with firmware version 1.00 |
| 1.1 | September 5, 2007 | • Updated for firmware version 1.10<br>• Added Windows Vista™ support |
| 1.2 | October 23, 2008 | • Updated for firmware version 1.20<br>• Added SSL VPN<br>• Added Bandwidth Control |

# Trademarks

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

Copyright © 2008 by D-Link Systems, Inc.

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

# Table of Contents

**Manual Overview ..... i**
Manual Revisions ..... ii
Trademarks ..... ii

**Product Overview ..... 1**
Package Contents ..... 1
System Requirements ..... 2
Features ..... 3
Hardware Overview ..... 4
Connections ..... 4
LEDs ..... 5

**Installation ..... 6**
Before you Begin ..... 6
Connect to Cable/DSL/Satellite Modem ..... 7
Connect to Another Router ..... 8

**Configuration ..... 10**
Web-based Configuration Utility ..... 10
Setup Wizard ..... 11
Manual Configuration ..... 16
Dynamic (Cable) ..... 16
PPPoE (DSL) ..... 17
PPTP ..... 18
L2TP ..... 19
Static (assigned by ISP) ..... 20
Russian PPPoE (DSL) ..... 21
Russian PPTP ..... 22
Network Settings ..... 23
Router Settings ..... 23
DHCP Server Settings ..... 24
DHCP Reservation ..... 25
VPN Settings ..... 26
IPSec Settings ..... 27
PPTP/L2TP Settings ..... 30
SSL VPN Settings ..... 31
Port Forwarding ..... 32
Application Rules ..... 33
MAC Filters ..... 34
Website Filters ..... 35
Firewall Settings ..... 36
DMZ ..... 36
Firewall Rules ..... 37
Advanced Network Settings ..... 38
UPnP ..... 38
WAN Ping Respond ..... 38
WAN Port Speed ..... 38
Routing ..... 39
Certificates ..... 40
User Groups ..... 41
Bandwidth Control ..... 42
Administrator Settings ..... 43
Administrator ..... 43
Change Password ..... 43
Remote Management ..... 43

Remote Management / SSL Remote Management ..... 44
Time and Date ..... 45
System Settings ..... 46
Update Firmware ..... 47
DDNS ..... 48
System Check ..... 49
Schedules ..... 50
Log Settings ..... 51
Device Information ..... 52
Log ..... 53
Statistics ..... 54
Active Session ..... 55
LAN Clients ..... 56
Routing ..... 56
VPN ..... 57
Help ..... 57

**Troubleshooting ..... 58**

**Networking Basics ..... 62**
Check your IP address ..... 62
Statically Assign an IP address ..... 63

**Technical Specifications ..... 65**

**Default Factory Settings ..... 66**

**Contacting Technical Support ..... 67**

**Warranty ..... 68**

**GNU/Linux GPL ..... 73**
GNU General Public License ..... 74

**Registration ..... 80**

# Package Contents

| | |
|---|---|
| **D-Link DIR-130 8-port VPN Router** | |
| **Power Adapter** | |
| **Ethernet Cable** | |
| **CD-ROM** | |

**Note:** Using a power supply with a different voltage rating than the one included with the DIR-130 will cause damage and void the warranty for this product.

# System Requirements

| | |
|---|---|
| **Network Requirements** | • An Ethernet-based Cable or DSL modem<br>• 10/100 Ethernet devices |
| **Web-based Configuration Utility Requirements** | **Computer with the following:**<br>• Windows®, Macintosh, or Linux-based operating system<br>• An installed Ethernet adapter<br><br>**Browser Requirements:**<br>• Internet Explorer 6.0 or higher<br>• Mozilla 1.7.12 or higher<br>• Firefox 1.5 or higher<br>• Safari 1.0 or higher (with Java 1.3.1 or higher)<br>• Flock 0.7.14 or higher<br>• Opera 6.0 or higher<br><br>**Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version. |
| **CD Installation Wizard Requirements** | **Computer with the following:**<br>• Windows® XP with Service Pack 2 or Vista™<br>• An installed Ethernet adapter<br>• CD-ROM drive |

# Features

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

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

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

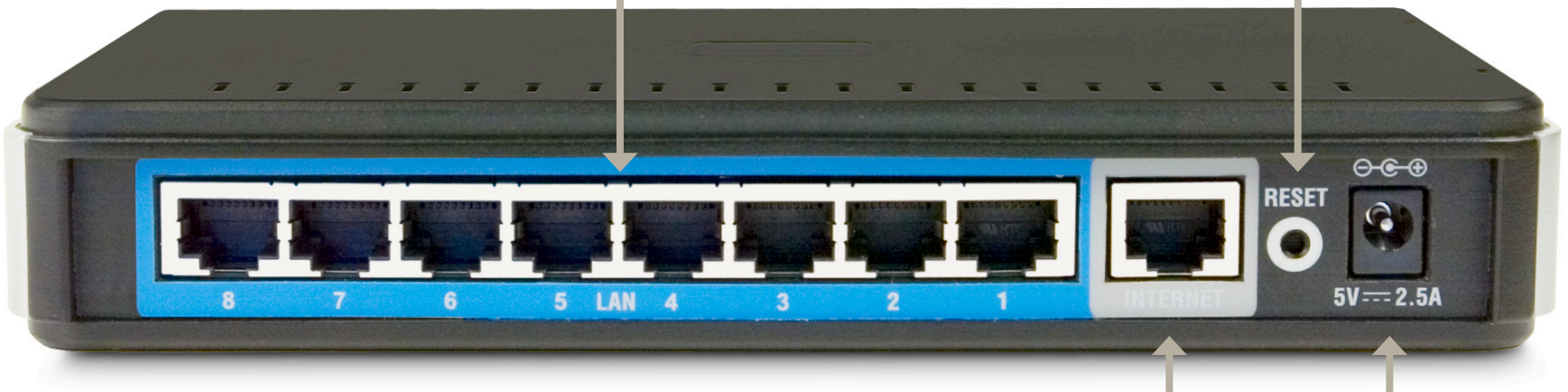
    - **Secure Multiple/Concurrent Sessions** - The DIR-130 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-130 can securely access corporate networks.

- **User-friendly Setup Wizard** - Through the easy-to-use web-based user interface, the DIR-130 allows you to 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.

# Hardware Overview
## Connections

**LAN Ports (1-8)**
Connect Ethernet devices such as computers, switches, and hubs.

**Reset**
Pressing the Reset button restores the router to its original factory default settings.




**Internet Port**
The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.

**Power Receptor**
Receptor for the supplied power adapter.

# Hardware Overview

## LEDs

**Status LED**
A blinking light indicates that the DIR-130 is ready.

**Local Network LEDs**
A solid light indicates a connection to an Ethernet-enabled computer on ports 1-8. This LED blinks during data transmission.

**Power LED**
A solid light indicates a proper connection to the power supply.

**Internet LED**
A solid light indicates connection on the Internet port. This LED blinks during data transmission.

# Installation

This section will walk you through the installation process.

# Before you Begin

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

# Connect to Cable/DSL/Satellite Modem

If you are connecting the router to a cable/DSL/satellite modem, please follow the steps below:

1. Place the router in an open and central location. Do not plug the power adapter into the router.

2. Turn the power off on your modem. If there is no on/off switch, then unplug the modem's power adapter. Shut down your computer.

3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.

4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.

5. Turn on or plug in your modem.  Wait for the modem to boot (about 30 seconds).

6. Plug the power adapter to the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot.

7. Turn on your computer.

8. Verify the link lights on the router. The power light, Internet light, and the LAN light (the port that your computer is plugged into) should be lit. If not, make sure your computer, modem, and router are powered on and verify the cable connections are correct.

9. Refer to page 10 to configure your router.

# Connect to Another Router

If you are connecting the D-Link router to another router to use as a switch, you will have to do the following before connecting the router to your network:

- Disable UPnP™
- Disable DHCP
- Change the LAN IP address to an available address on your network. The LAN ports on the router cannot accept a DHCP address from your other router.

To connect to another router, please follow the steps below:

1. Plug the power into the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). Please see the **Networking Basics** section for more information. If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.

2. Open a web browser and enter **http://192.168.0.1** and press **Enter**. When the login window appears, set the user name to **Admin** and leave the password box empty. Click **Log In** to continue.

3. Click on **Advanced** and then click **Advanced Network**. Uncheck the Enable UPnP checkbox. Click **Save Settings** to continue.

4. Click **Setup** and then click **Network Settings**. Uncheck the Enable DHCP Server server checkbox. Click **Save Settings** to continue.

5. Under Router Settings, enter an available IP address and the subnet mask of your network. Click **Save Settings** to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 1.

6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.

7. Connect an Ethernet cable in one of the LAN ports of the router and connect it to your other router. Do not plug anything into the Internet port of the D-Link router.

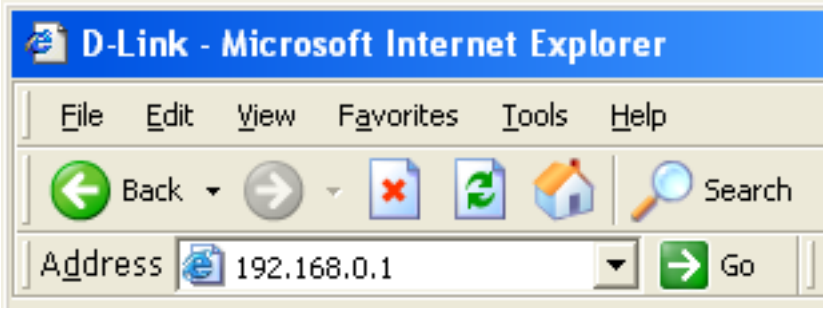
8. You may now use the other 7 LAN ports to connect other Ethernet devices and computers.

# Configuration

This section will show you how to configure your new D-Link router using the web-based configuration utility.

## Web-based Configuration Utility

To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.0.1).



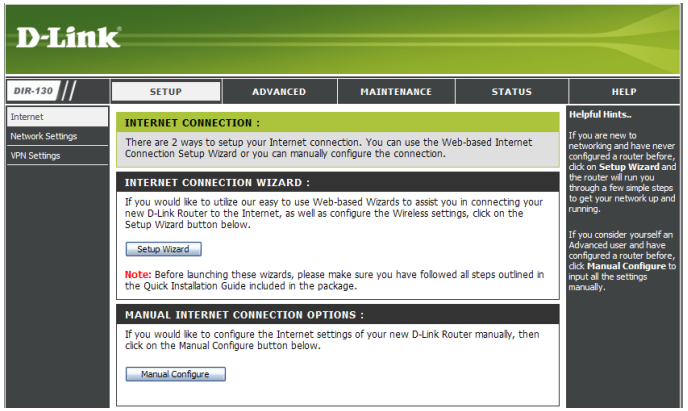

Enter **admin** as the User name field and enter the password in the Password field. Leave the password blank by default.

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

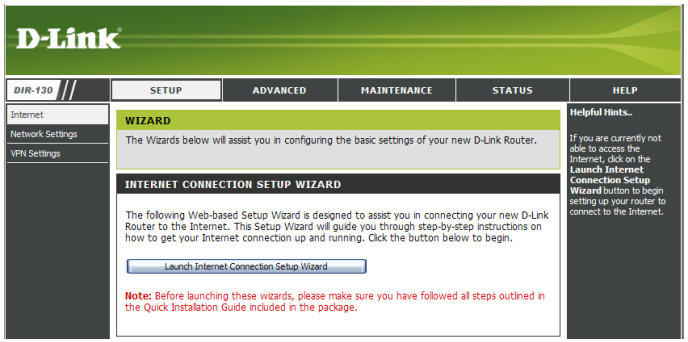
# Setup Wizard

You may click **Setup Wizard** to quickly configure your router.

If you want to enter your settings without running the wizard, click **Manual Configure** and skip to page 16.

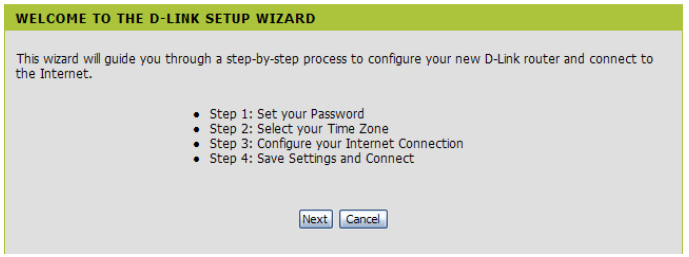



Click **Launch Internet Connection Setup Wizard** to begin.



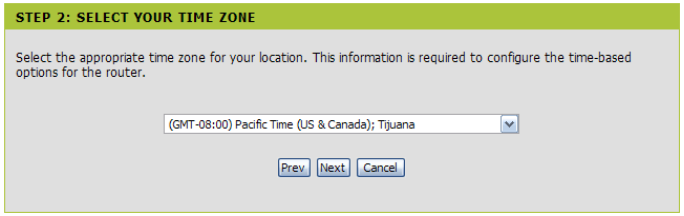

*PPTP, L2TP, Russian PPPoE, and Russian PPTP Internet configurations referenced in this section do not apply in North America.

Click **Next** to continue.

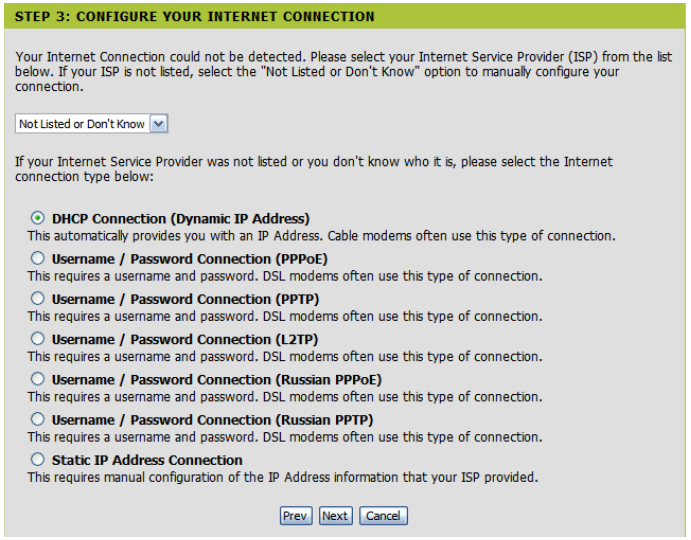



Create a new password and then click **Next** to continue.

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

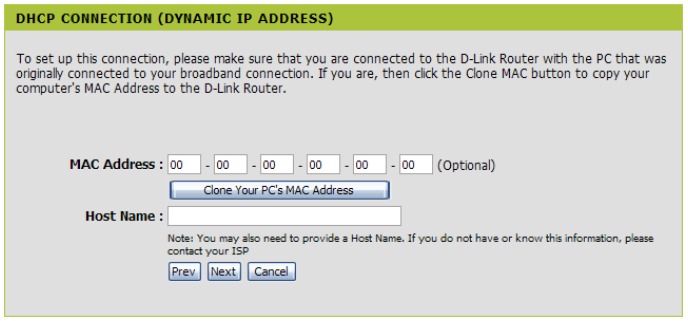



Select the type of Internet connection you use and then click **Next** to continue.



If you selected Dynamic, you may need to enter the MAC address of the computer that was last connected directly to your modem. If you are currently using that computer, click **Clone Your PC's MAC Address** and then click **Next** to continue.

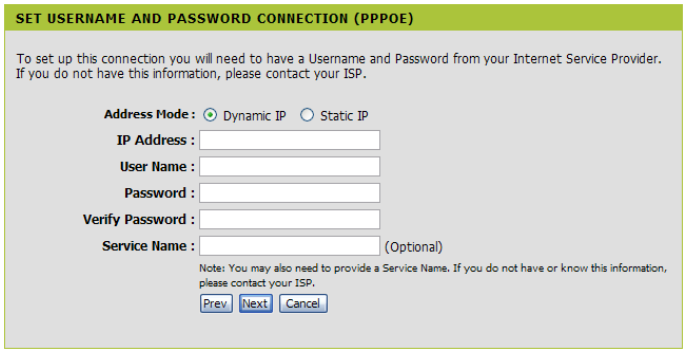
The Host Name is optional but may be required by some ISPs. The default host name is the device name of the Router and may be changed.



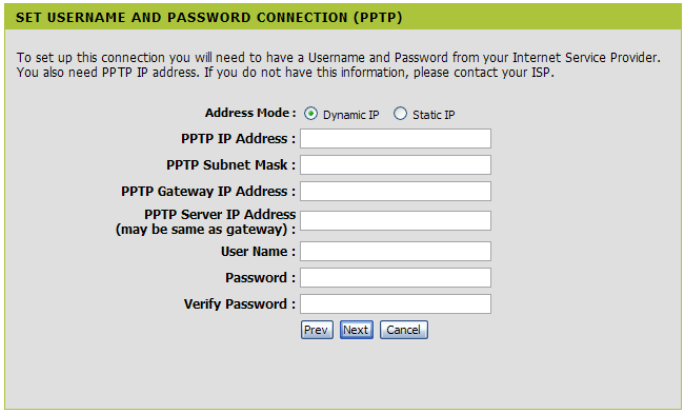

If you selected PPPoE, enter your PPPoE username and password. Click **Next** to continue.

Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

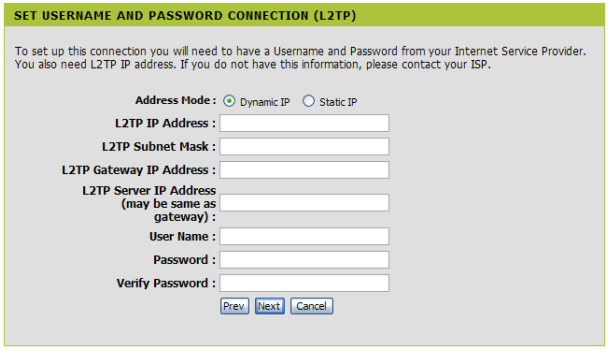
**Note:** Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.



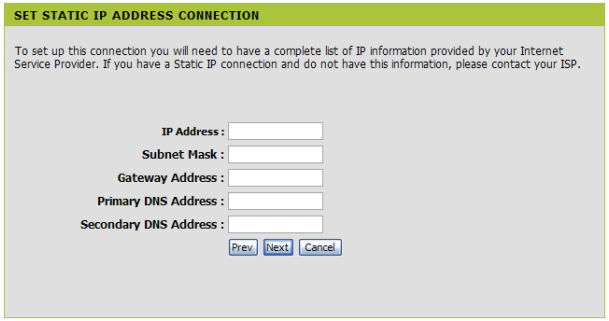

If you selected PPTP, enter your PPTP username and password. Click **Next** to continue.



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



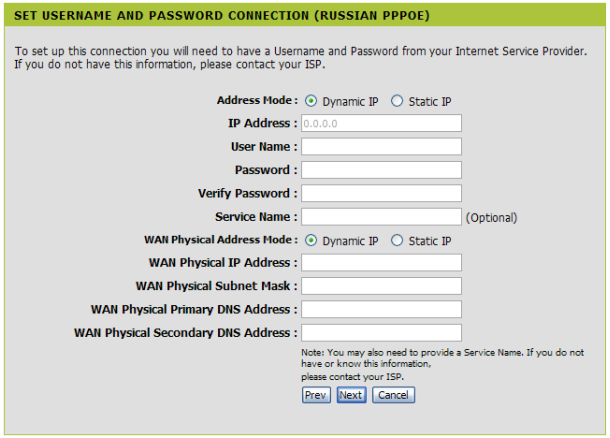

If you selected Static, enter your network settings supplied by your Internet provider. Click **Next** to continue.



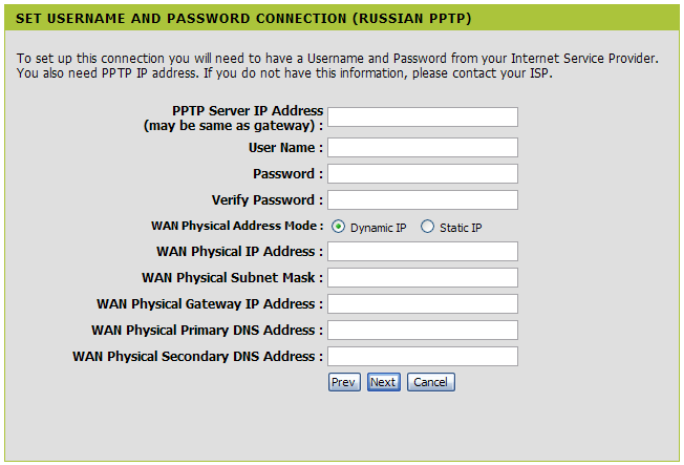

If you selected Russian PPPoE, enter your PPPoE username and password. Click **Next** to continue.

Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

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

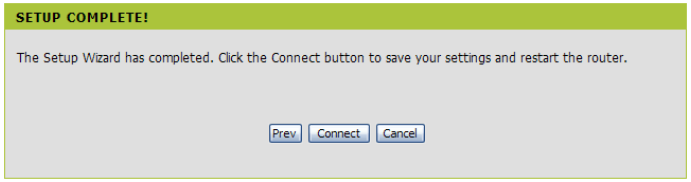


If you selected Russian PPTP, enter your PPTP username and password. Click **Next** to continue.




Click **Connect** to save your settings. Once the router is finished rebooting, click **Continue**. Please allow 1-2 minutes to connect.

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



# Manual Configuration
## Dynamic (Cable)

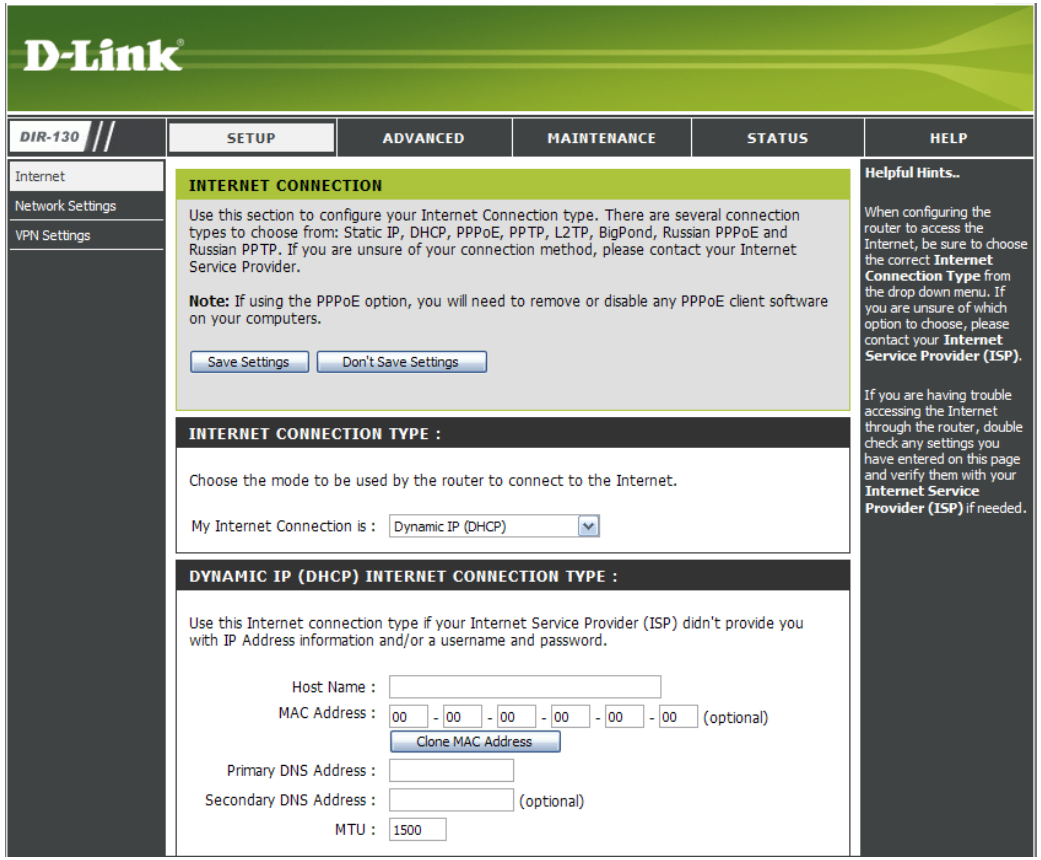
**My Internet Connection:** Select **Dynamic IP (DHCP)** to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services.

**Host Name:** The Host Name is optional but may be required by some ISPs.

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

**DNS Addresses:** Enter the Primary and Secondary DNS server IP address(es) assigned by your ISP.

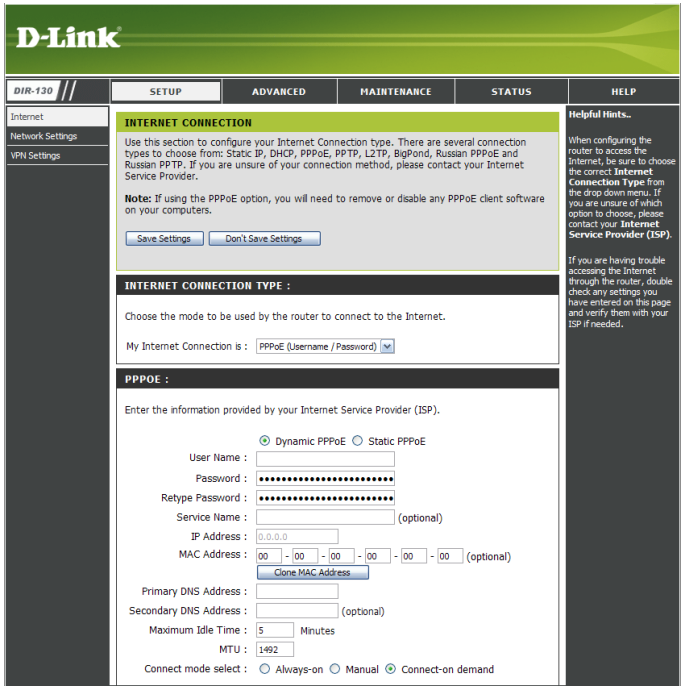
**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.




*PPTP, L2TP, Russian PPPoE, and Russian PPTP Internet configurations referenced in this section do not apply in North America.

# Internet Setup
## PPPoE (DSL)

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




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

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

**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).

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

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

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

**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.

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

# Internet Setup
## PPTP

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

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

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

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

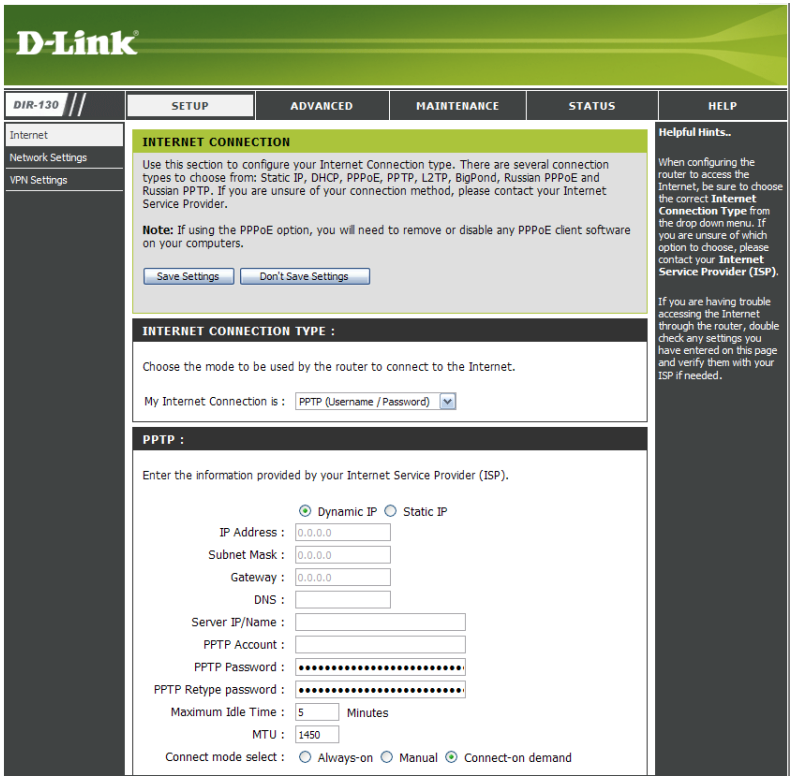
**Gateway:** Enter the Gateway IP Address provided by your ISP.

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

**Server IP/Name:** Enter the Server IP provided by your ISP (optional).

**PPTP Account:** Enter your PPTP account (username).

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



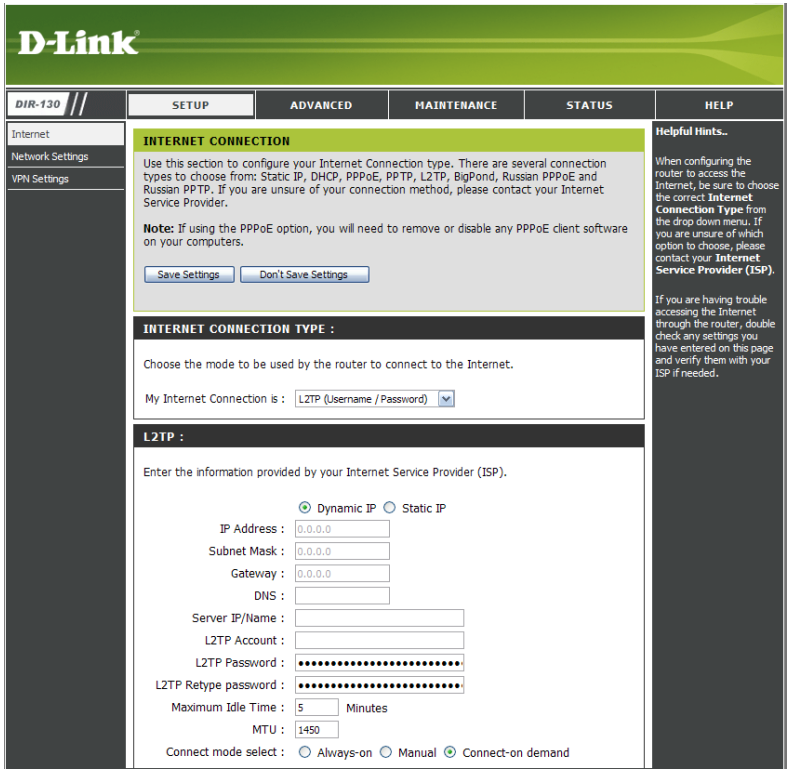

**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1450 is the default MTU.

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

# Internet Setup
## L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.




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

**IP Address:** Enter the L2TP IP address supplied by your ISP (Static only).

**Subnet Mask:** Enter the Subnet Mask supplied by your ISP (Static only).

**Gateway:** Enter the Gateway IP Address provided by your ISP.

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

**Server IP/Name:** Enter the Server IP provided by your ISP (optional).

**L2TP Account:** Enter your L2TP account (username).

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

**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. 1450 is the default MTU.

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

# Internet Setup
## Static (assigned by ISP)

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

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

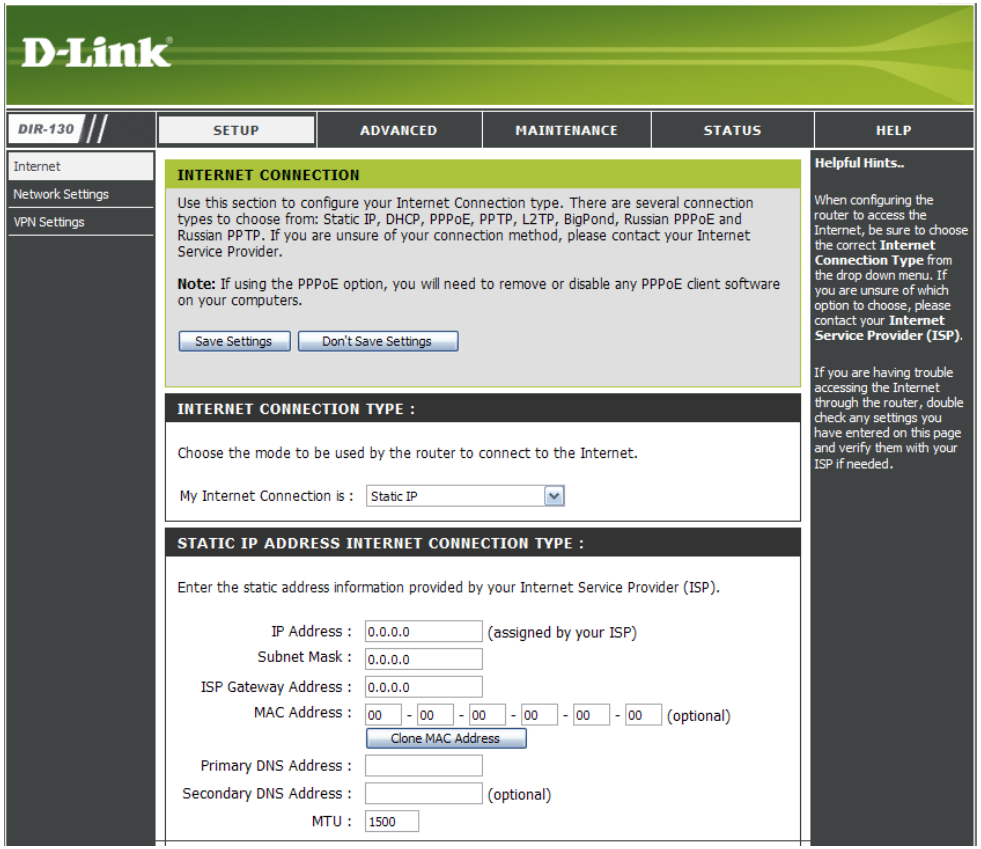
**Subnet Mask:** Enter the Subnet Mask assigned by your ISP.

**ISP Gateway:** Enter the Gateway assigned by your ISP.

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

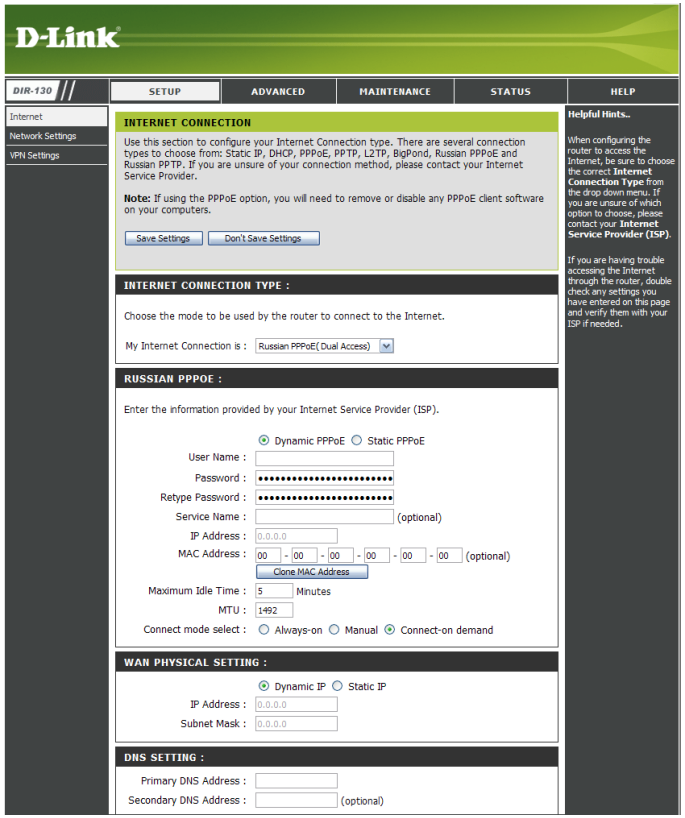
**DNS Servers:** The DNS server information will be supplied by your ISP (Internet Service Provider.)

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



# Internet Setup
## Russian PPPoE (DSL)

Choose **Russian 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.




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

**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).

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

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

**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.

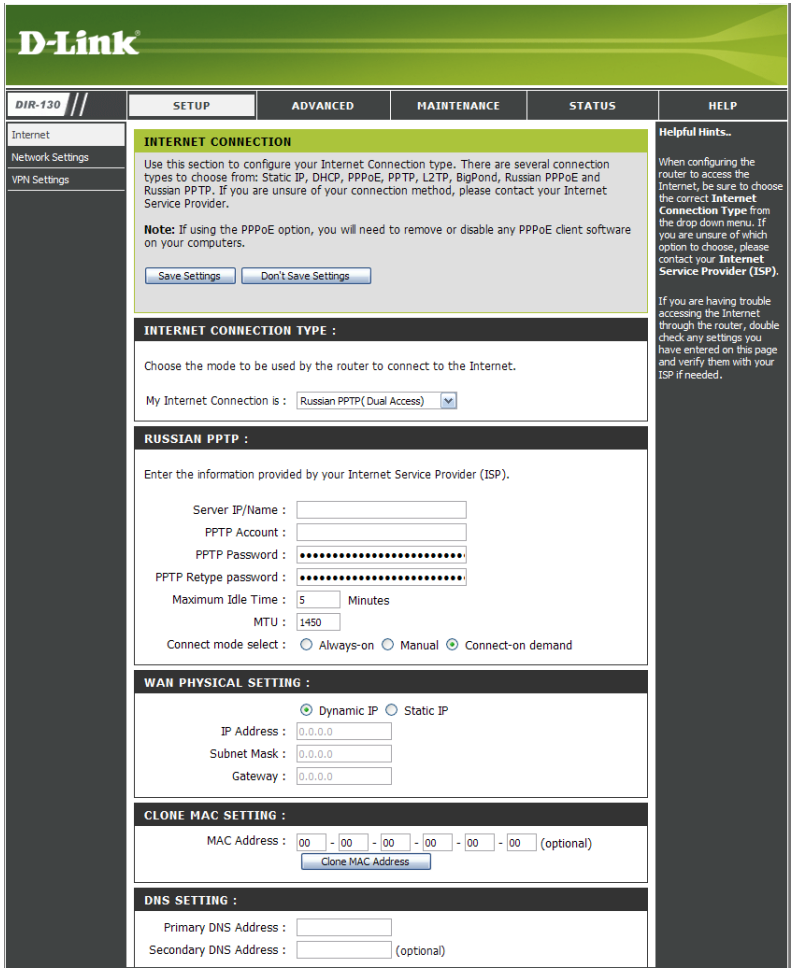
**Connect Mode:** Select either **Always-on**, **On-Demand**, or **Manual**.

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

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

# Internet Setup
## Russian PPTP

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




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

**Server IP/Name:** Enter the Server IP provided with your ISP.

**PPTP Account:** Enter your PPTP account (username).

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

**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.

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

**WAN Physical Setting:** Select Static IP if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

**IP Address:** Enter the Server IP provided by your ISP (optional).

**Subnet Mask:** Enter the Subnet Mask supplied by your ISP (Static IP only).

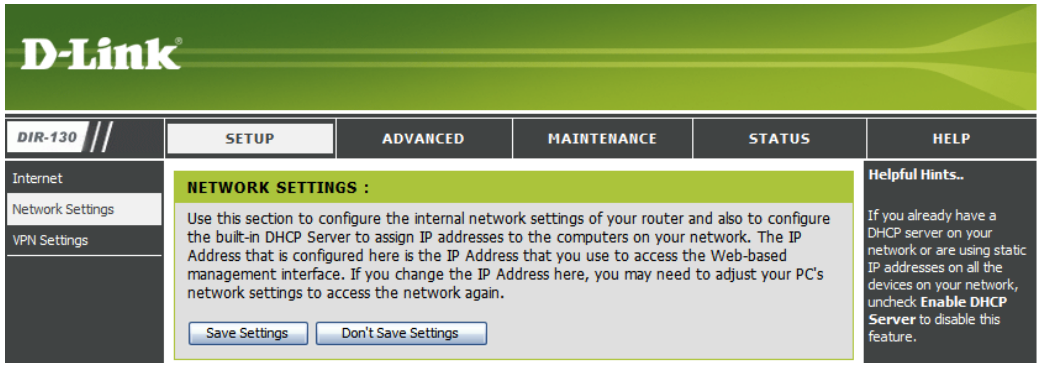
**Gateway:** Enter the Gateway Address provided by your ISP (Static IP only)

**Clone MAC Setting:** Click the Clone MAC Address button to copy the MAC Address from your PC.

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

# Network Settings

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




# Router Settings

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

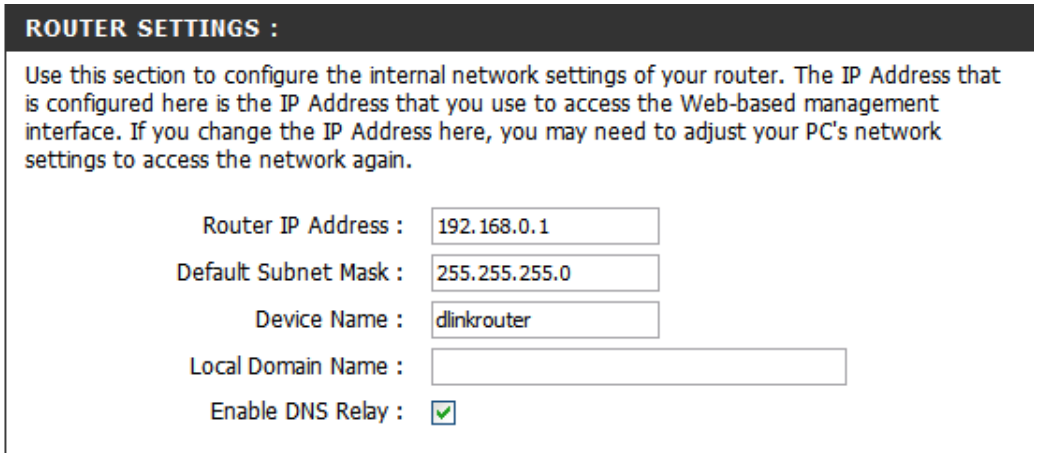
If you change the IP address, once you click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

**Device Name:** Enter a name for your router.

**Local Domain Name:** Enter the Domain name (optional).

**Enable DNS Relay:** Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.



# DHCP Server Settings

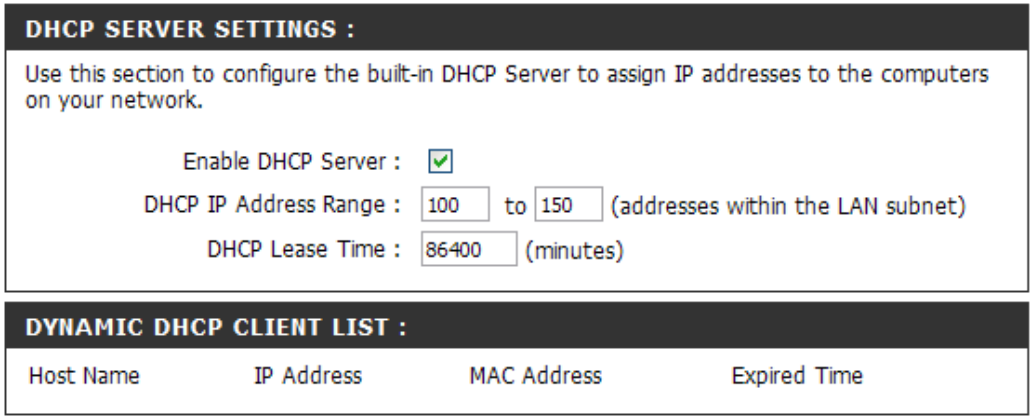
The router has a built-in DHCP (Dynamic Host Control Protocol) server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.” When you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

**Enable DHCP 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.



# DHCP Reservation

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

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

**DHCP Reservations List:** Check the box under the first column to enable the reservation.

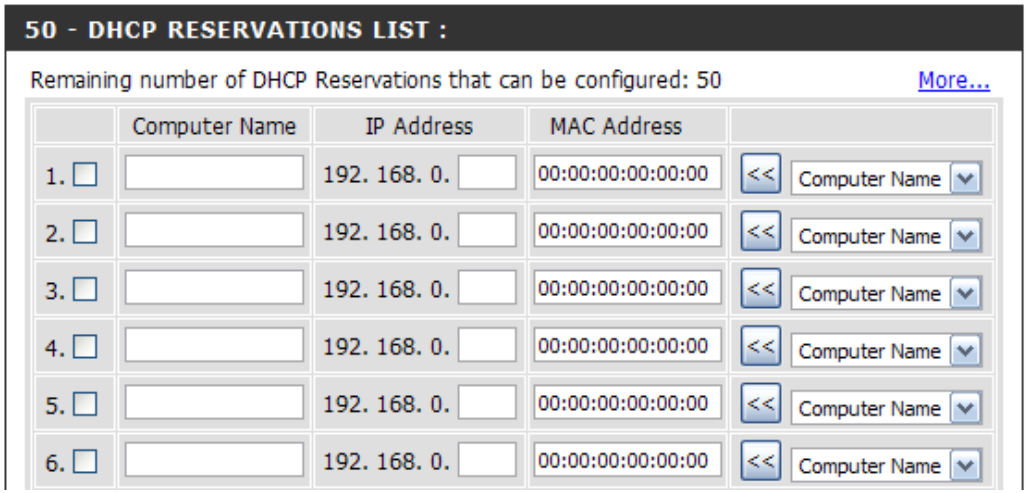
**Computer Name:** Enter the computer name or select from the drop-down menu (last column) and click **<<**.

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

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

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

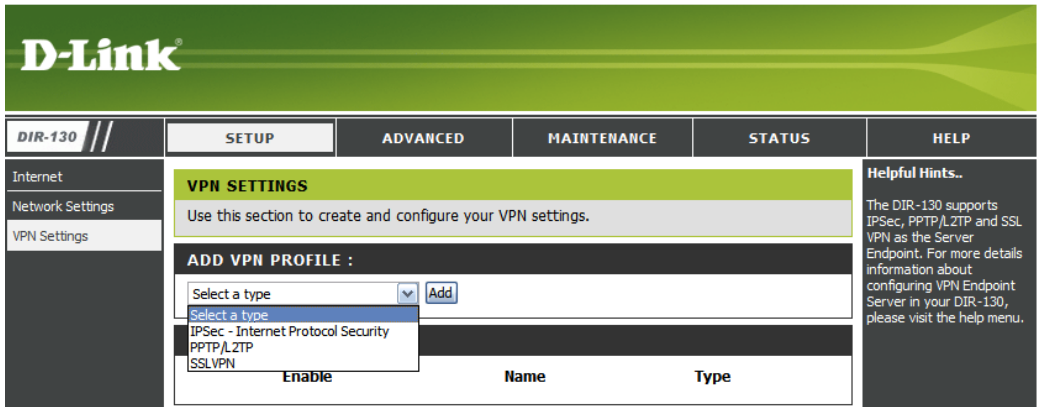
**Save:** Click **Save** to save your entry. You must click **Save Settings** at the top to activate your reservations.



# VPN Settings

The DIR-130 supports IPSec, PPTP, L2TP VPN, and SSL VPN as the Server Endpoint.

**Add VPN Profile:** Select **IPSec**, **PPTP/L2TP**, or **SSL VPN** from the drop-down menu and then click **Add**.



# IPSec Settings

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

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

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

**Remote IP:** Select Site to Site or Remote User for the required VPN configuration.

- **Site to Site** - Network-to-network VPN in which two entire LAN networks are virtually connected across the Internet. If selected, enter the destination gateway IP address in the box which is the public WAN IP or host address of the remote VPN server endpoint.
- **Remote User** – Client-to-server VPN in which remote VPN clients can to connect to the router from the Internet and access Local Network resources.

**Remote Local LAN Net/ Mask:** If **Site to Site** is selected, enter the Destination subnet and mask of the remote network. (ex. 192.168.1.0/24)

**Authentication:** Select Pre-shared Key or X.509 Certificate Authentication. One of these two authentication methods must be selected.

- **Pre-shared Key** - Manually enter ASCII passphrase in box.
- **X.509 Certificate** - For certificate authentication, certificates must be manually uploaded to the router. See the “Certificates” section for details.

• Additional Authentication Methods (Optional)

**XAUTH** - Check this box to include additional username and password authentication requirements for the VPN. Select **Server Mode** or **Client Mode**.

- **Server Mode** - Select a group from the Authentication database drop-down menu containing the list of user credentials permitted.
- **Client Mode** - Enter the user name and password if required by the remote VPN server endpoint configured in xAuth Server Mode.

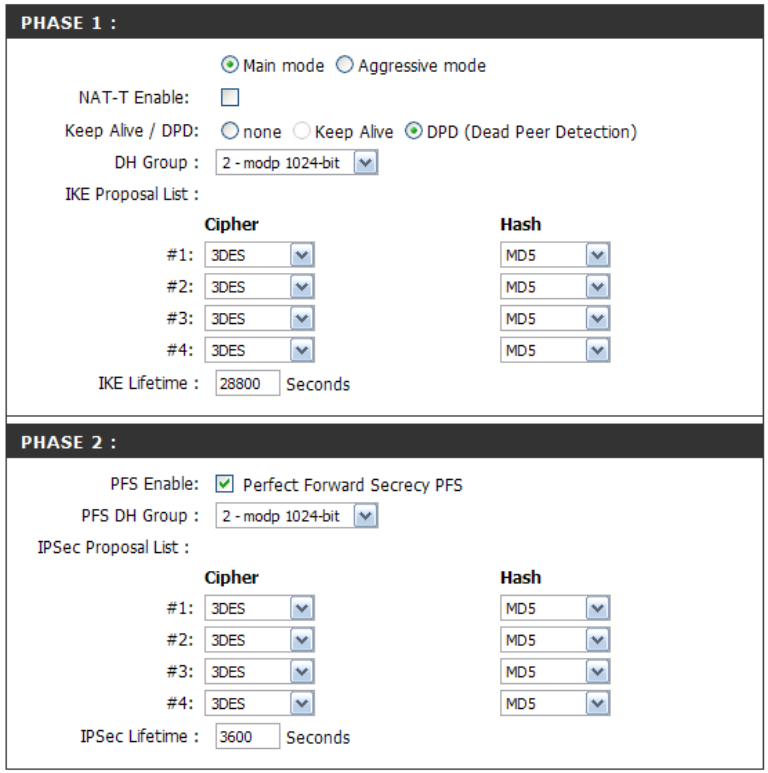
**Local/Remote ID** - Check this box to include additional ID authentication requirements for the VPN using a specific IP Address, FQDN, ASN1, or a Custom String.

- **Local ID** - Select one of the options from the drop-down menu. Enter an ID to identify and authenticate the local VPN endpoint.
- **Remote ID** - Select one of the options from the drop-down menu. Enter an ID to identify and authenticate the remote VPN endpoint.

**Main / Aggressive Mode:** Select Main Mode or Aggressive Mode for IKE Phase 1 negotiation.

- **Main Mode** - Select this option to configure the standard negotiation parameters for IKE Phase 1 of the VPN Tunnel. (Recommended Setting)
- **Aggressive Mode** - Select this option to configure IKE Phase 1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended - Less Secure)

**NAT-T Enable:** Check this box to enable NAT Traversal. Enabling this option will allow IPSec traffic from this endpoint to traverse through the translation process during NAT. The remote VPN endpoint must also support this feature and it must be enabled to function properly over the VPN.




**Keep Alive / DPD:** Select **None**, **Keep Alive**, or **DPD** (Dead Peer Connection).

- **None** - Select this option to disable Keep Alive.
- **Keep Alive** - Select this option to send random ping requests from this endpoint to the remote endpoint keeping the tunnel established during long idle periods of inactivity.
- **DPD** - Select this option to delete the VPN tunnel if there is no traffic detected. The VPN will re-establish once traffic is again sent through the tunnel.

**DH Group:** Select a DH Group from the drop-down menu. As the DH Group number increases, the higher the level of encryption implemented for Phase 1.

**IKE Proposal List:** Select the Cipher and Hash from the drop-down menus. The proposal listing is evaluated in order with #1 being the first proposal to attempt in IKE negotiation.

**IKE Lifetime:** Enter the number of seconds for the IKE Lifetime. The period of time to pass before establishing a new IKE security association (SA) with the remote endpoint. The default value is 28800.

**PFS Enable:** Check to enable or uncheck to disable. PFS is an additional security protocol.

**PFS DH Group:** Select a PFS DH Group from the drop-down menu. As the DH Group number increases, the higher the level of encryption implemented for PFS.

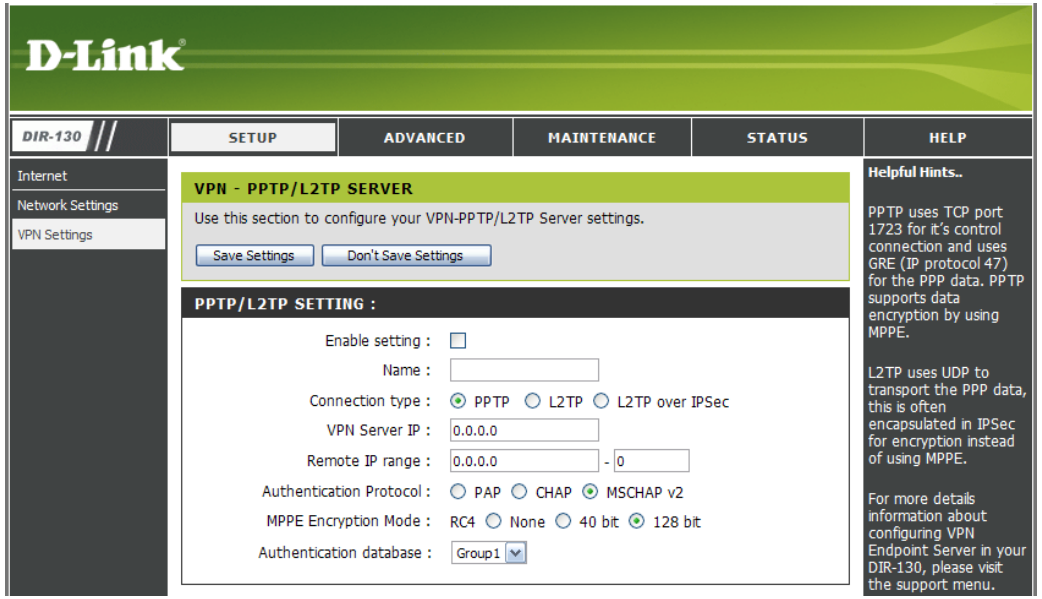
**IPSec Proposal List:** Select the Cipher and Hash from the drop-down menus. The proposal listing is evaluated in order with #1 being the first proposal to attempt in IPSec negotiation.

**IPSec Lifetime:** Enter the number of seconds for the IPSec Lifetime. The period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint. The default value is 3600.

# PPTP/L2TP Settings

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

L2TP uses UDP protocol to transport the PPP data. This is often encapsulated in IPSec encryption instead of MPPE.




**Enable Setting:** Check this box to enable.

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

**Connection Type:** Select **PPTP**, **L2TP**, or **L2TP over IPSec**.

**VPN Server IP:** Enter the VPN Server IP address which is the LAN IP of the router. (i.e. 192.168.0.1).

**Remote IP Range:** Assign a range of IP addresses. The assigned IP range should be on the same IP network but not the in the same range as your DHCP IP range.
For example, if your network is 192.168.0.xxx and you set the DHCP range to 192.168.0.100-200, the remote IP range cannot be within 192.168.0.100-200.

**Authentication Protocol:** Select the desired authentication protocol (PAP/CHAP/MS-CHAP v2).

**MPPE Encryption Mode:** Select the level of encryption (None/40-bit/128-bit).

**Authentication Database:** Select a user group from the drop-down menu. You can create user groups in the **Advanced** > **User Group** section.

# SSL VPN Settings

**Certificate Select:** Select a certificate to use for SSL. You can add a new certificate by clicking **New**, which will take you to the **Advanced > Certificates** page.

**Enable SSLVPN:** Check this box to enable SSL VPN.

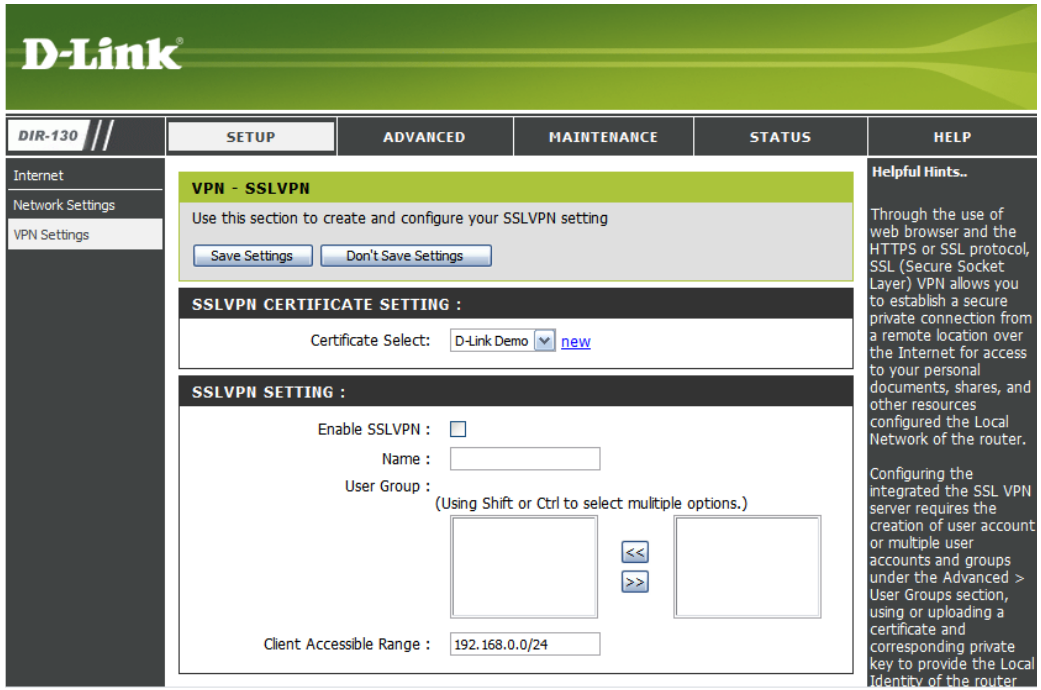
**Name:** Enter a name for your VPN.

**User Group:** Select a User Group to include in your SSL VPN.

**Client Accessible Range:** Enter the LAN IP network in which connected SSL VPN clients are allowed access.

Example:
If these are the current settings,
**Router IP Address: 192.168.0.1**
**Router Subnet Mask: 255.255.255.0**

Use the following configuration,
**Client Accessible Range: 192.168.0.0/24**



# Port Forwarding

This section allows you to open a single port or a range of ports.

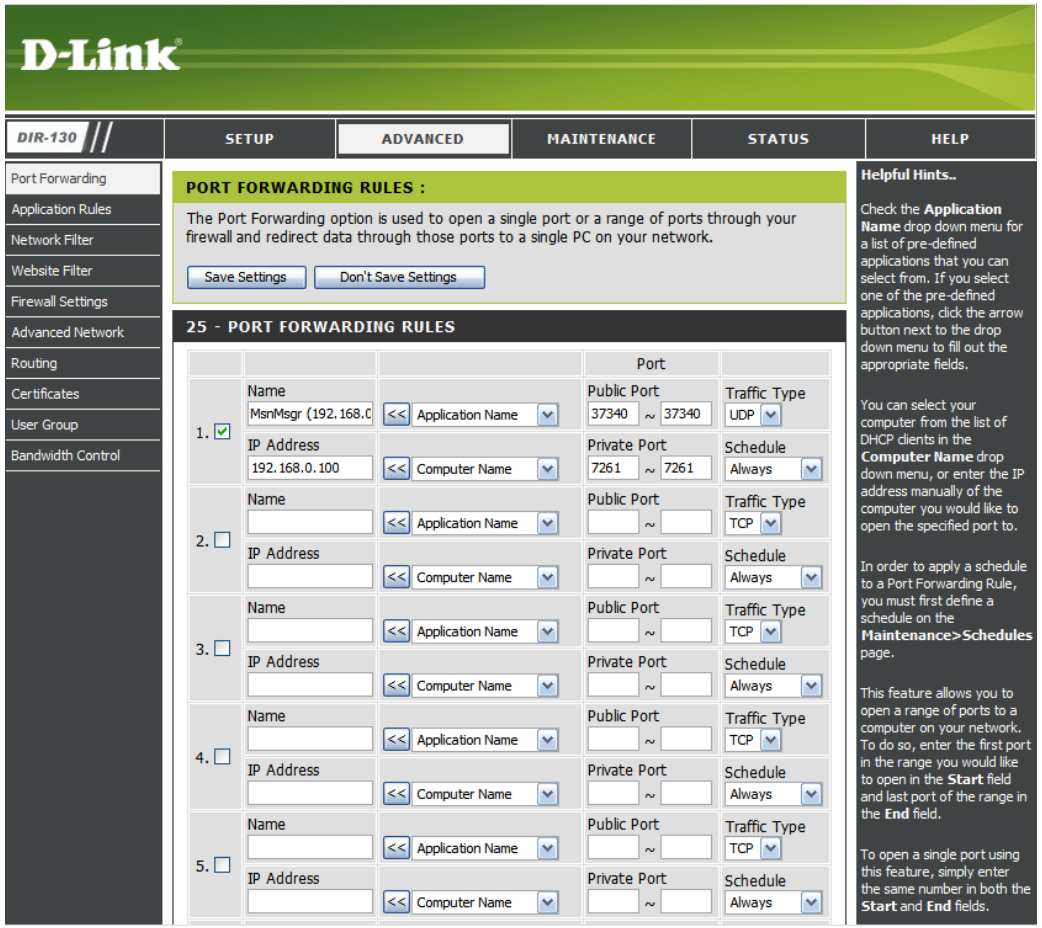
**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

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

**Port:** Enter a port or port range for the public and private port.

**Traffic Type:** Select the type of protocol you would like to assign to the rule.

**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-130. 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.

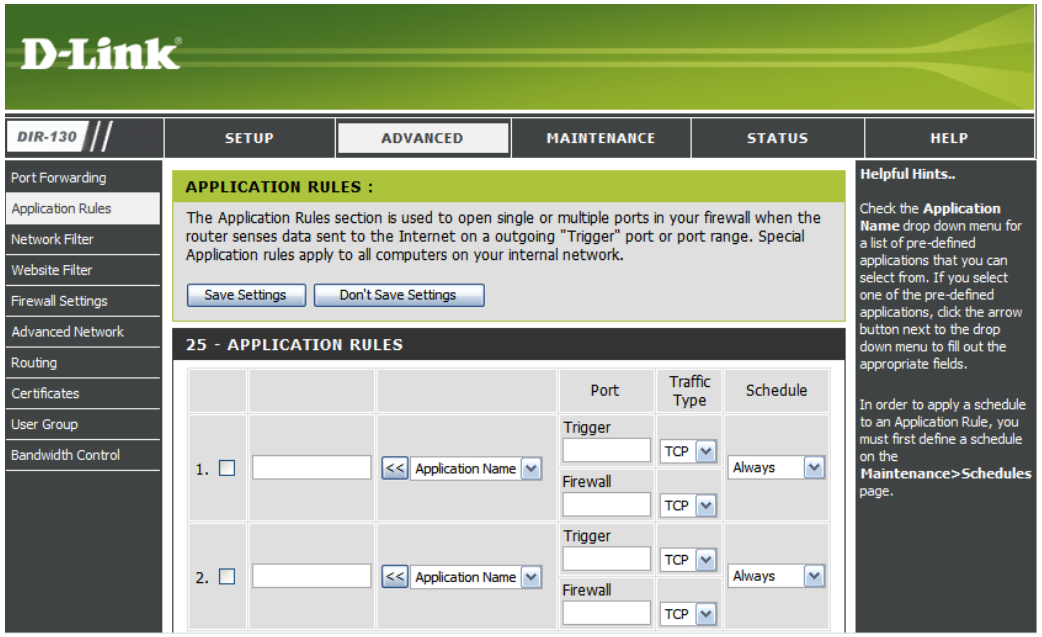
**Name:** Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click **<<**.

**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 **Any**).

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



# MAC Filters

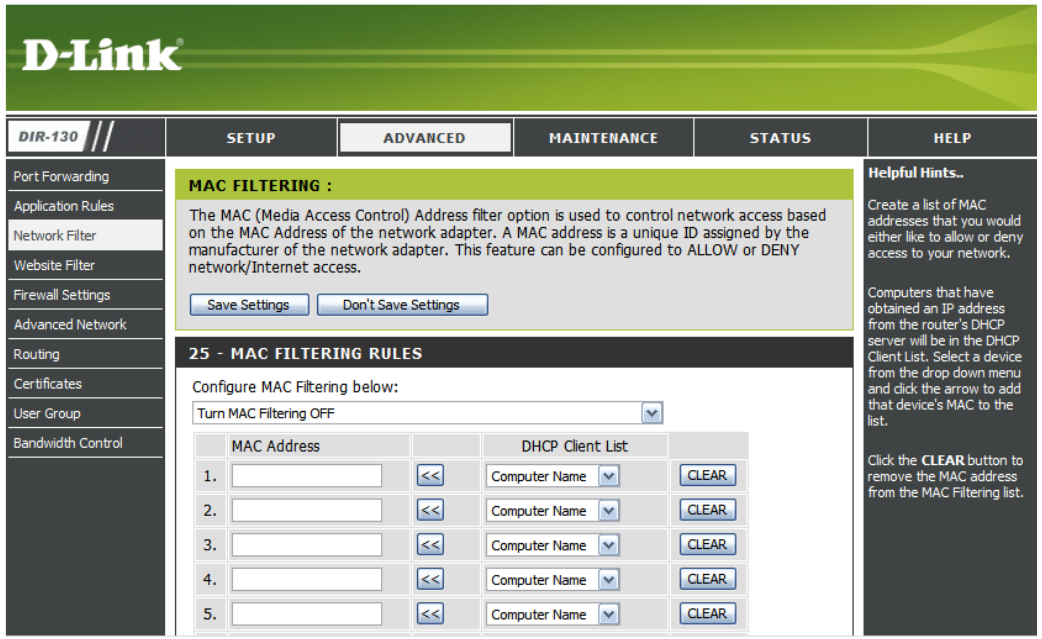
Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the router. You may enter up to 25 rules.

**Configure MAC Filtering:** Select **Turn MAC Filtering Off**, **Turn MAC filtering on and ALLOW computers listed to access the network**, or **Turn MAC filtering on and DENY computers listed to access the network** 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 delete the settings of the filter rule.



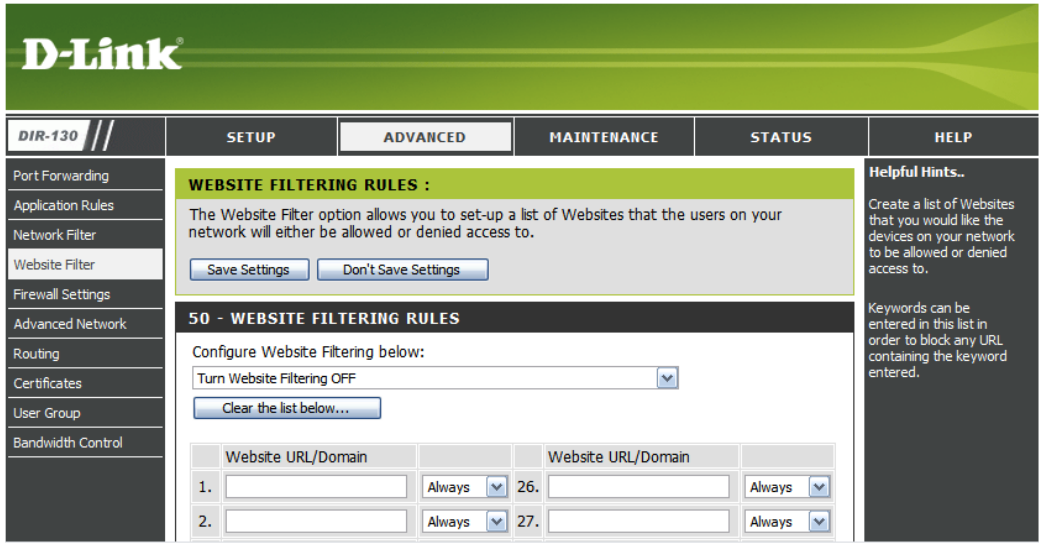
# Website Filters

Website Filters are used to deny LAN computers from accessing specific web sites by the URL or domain. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display. To use this feature, enter the text string to be blocked and click **Save Settings**. The text to be blocked will appear in the list. To delete the text, click the **Clear the List Below** button.

**Configure Website Filtering:** Select **Turn Website Filtering Off**, **Turn Website filtering on and ALLOW computers listed to access the network**, or **Turn Website filtering on and DENY computers listed to access the network** from the drop-down menu.

**Website URL/ Domain:** Enter the keywords or URLs that you want to block (or allow). Any URL with the keyword in it will be blocked or allowed.

**Schedule:** The schedule of time when the selected rule will be enabled. The schedule may be set to **Always**, which will allow the filter to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.



# Firewall Settings
## DMZ

A firewall protects your network from the outside work. The D-Link DIR-130 offers a firewall protection such as SPI (Stateful Packet Inspection) and NAT/PAT (Network Address Translation/Port Address Translation). 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 (Demilitarized Zone). This option will expose the chose computer completely to the outside world.

**Enable DMZ Host:** 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. This option is only recommended as a last resort.

**DMZ IP Address:** Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its IP address automatically using DHCP, be sure to make a static reservation on the **Internet** > **DHCP** page so that the IP address of the DMZ machine does not change.

**Schedule:** The schedule of time when the DMZ will be enabled. The schedule may be set to Always, which will allow the DMZ to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.

# Firewall Settings

## Firewall Rules

Up to 75 Firewall Rules can be created to control the incoming and outgoing traffic on your router. For each rule you can create a name and control the direction of traffic. You can also allow or deny a range of IP Addresses, protocol and a port range. In order to apply a schedule to a Firewall Rule, you must first define a schedule on the **Maintenance** > **Schedules** page. The first 2 Firewall Rules are default and cannot be changed.

**Name:** Enter a name for your Firewall Rule.

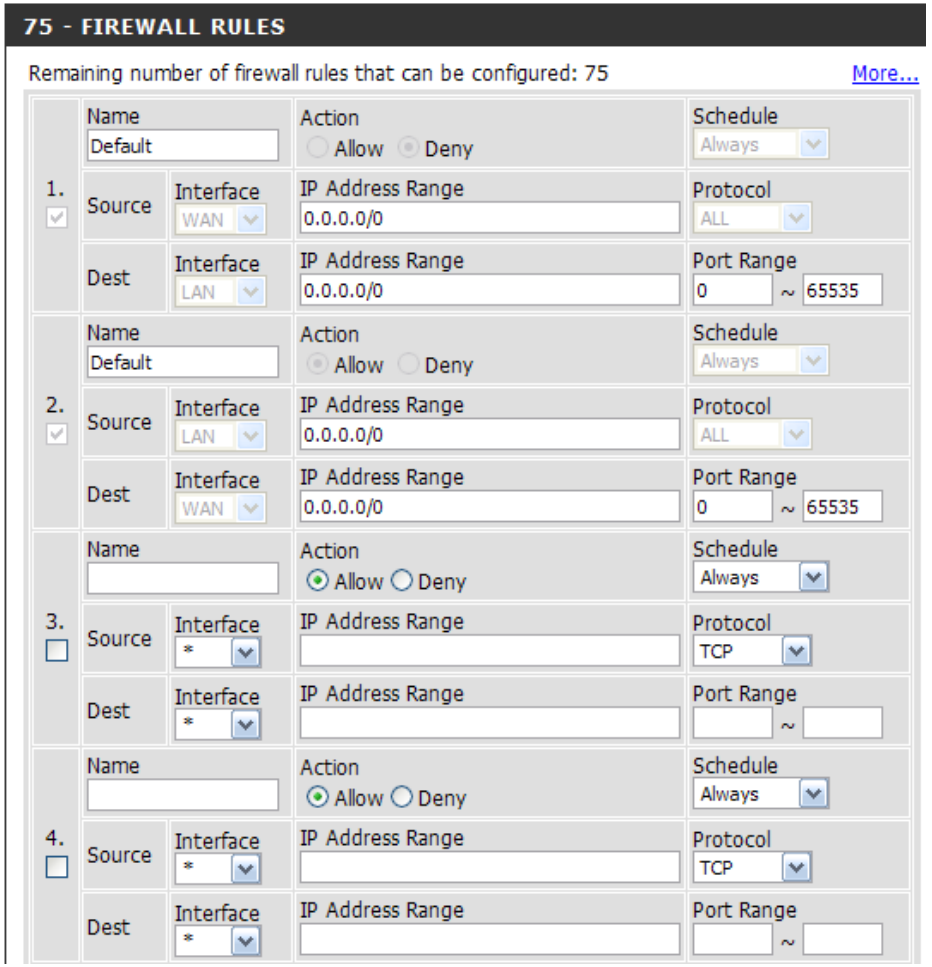
**Schedule:** Select a schedule from the drop-down menu. In order to apply a schedule to a Firewall Rule, you must first define a schedule on the **Maintenance** > **Schedules** page.

**Source/Dest:** This setting controls the direction of traffic. To control incoming traffic, set the Source Interface to WAN and the Dest Interface to LAN. To control outgoing traffic, set the Source Interface to LAN and the Dest Interface to WAN.

**IP Address Range:** Enter the IP Address Range for both the Source Interface and Dest Interface. These IP Address Ranges will be either allowed or denied, depending on the selected action.

**Protocol:** Select a protocol from the drop-down menu. The protocol that is selected will be either allowed or denied, depending on the selected action.

**Port Range:** Enter a Port Range. The Port Range that is entered will be either allowed, or denied, depending on the selected action.

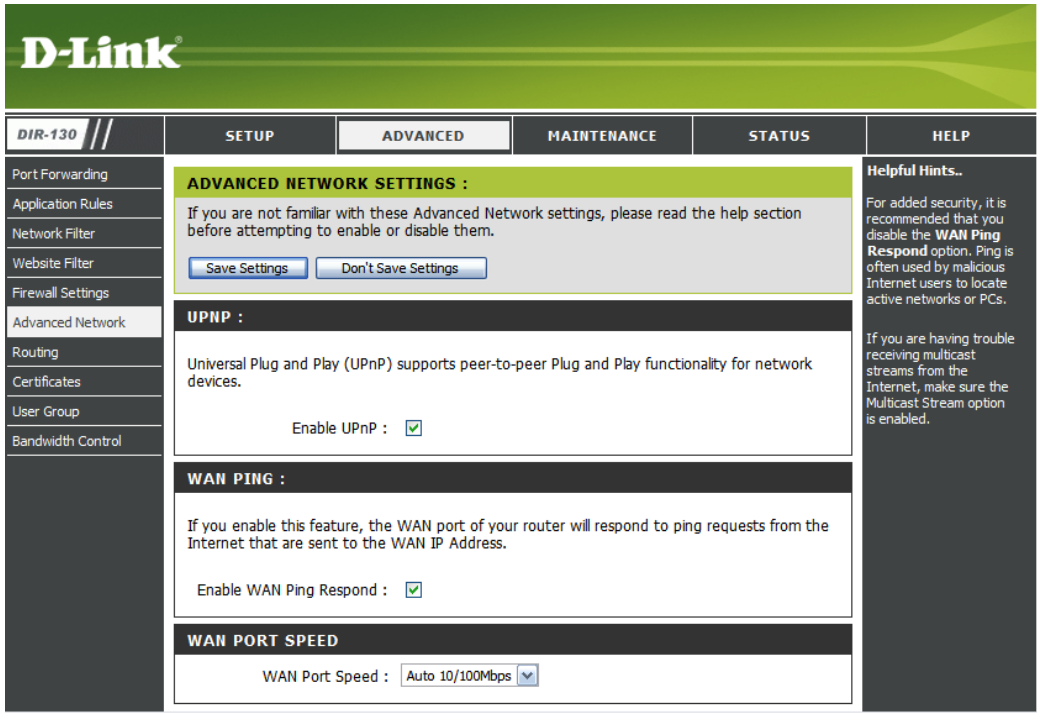


# Advanced Network Settings

**UPnP:** Click on the checkbox to enable Universal Plug and Play (UPnP™). UPnP provides compatibility with networking equipment, software and peripherals.

**Enable WAN Ping Respond:** Unchecking the box will not allow the DIR-130 to respond to pings. Blocking pings may provide some extra security from hackers. Check the box to allow the Internet port to be "pinged".

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



# Routing

This section allows you to define static routes for the WAN types of Static IP, Dynamic IP, Russian PPPoE, and Russian PPTP with ISPs that require these parameters. Up to 50 Static Routing Rules can be defined.

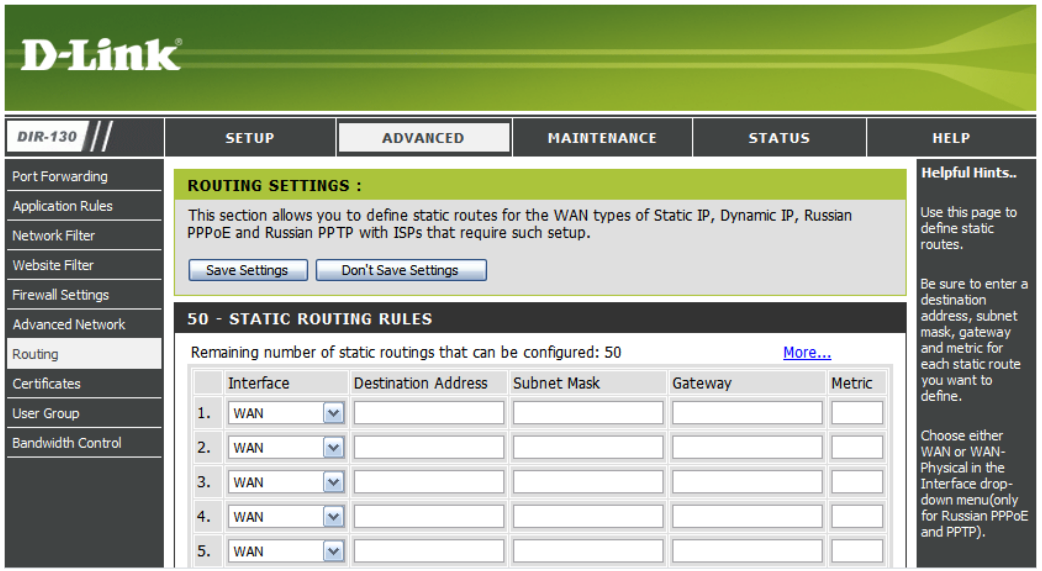
**Interface:** Select **WAN** or **WAN_Physical** from the drop down menu. Only select **WAN_Physical** if your Internet connection type is **Russian PPPoE** or **Russian PPTP**.

**Destination Address:** Enter the destination address for the static routing rule.

**Subnet Mask:** Enter the subnet mask for the static routing rule.

**Gateway:** Enter the gateway for the static routing rule.

**Metric:** Enter the metric for the static routing rule.




*PPTP, L2TP, Russian PPPoE, and Russian PPTP Internet configurations and the WAN_Physical parameter referenced in this section does not apply in North America.

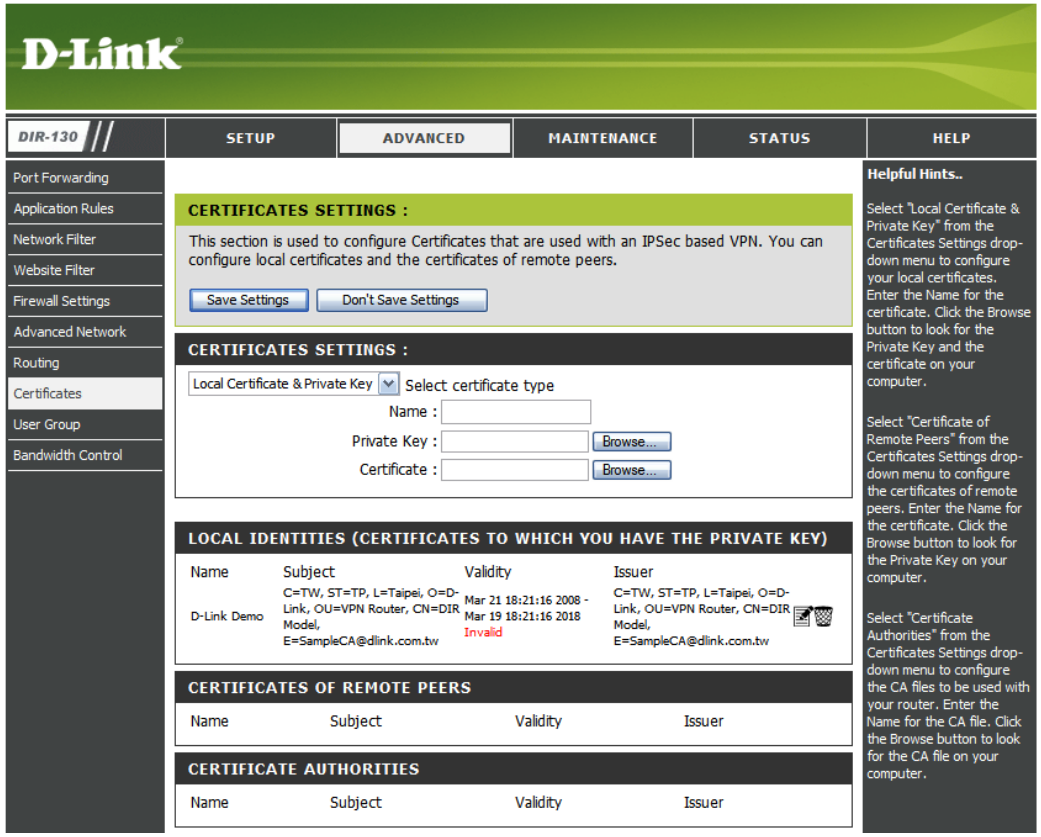
# Certificates

This section is used to configure Certificates that are used with an IPSec based VPN. You can configure local certificates and the certificates of remote peers. Select one of the three options from the drop-down menu: **Local Certificate & Private key**, **Certificate of Remote Peers**, or **Certificate Authorities**.

**Local Certificate & Private Key:** Select this option from the drop-down menu to configure your local certificates. Enter a name for the certificate. Click the browse button to look for the Private Key and the certificate on your computer.

**Certificate of Remote Peers:** Select this option from the drop-down menu to configure the certificates of remote peers. Enter a name for the certificate. Click the browse button on your computer to look the Private Key on your computer.

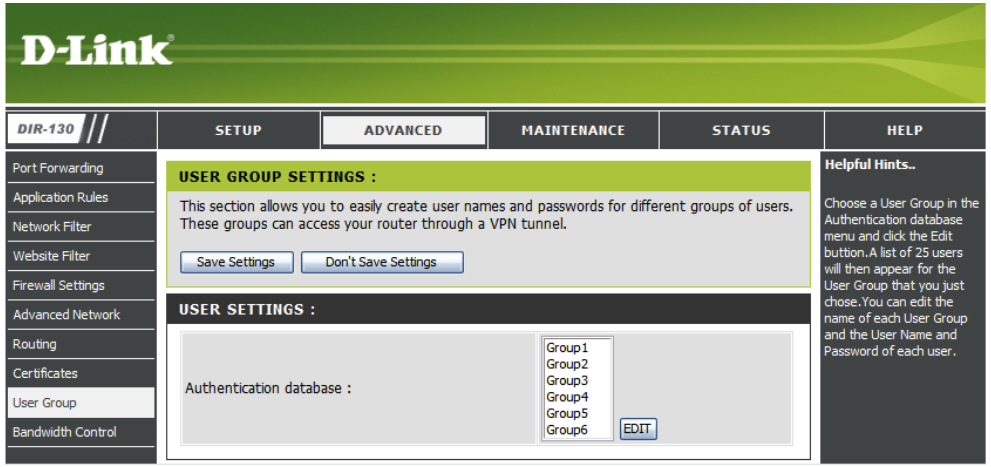
**Certificate Authorities:** Select this option from the drop-down menu to configure Certificate Authority (CA) files to be used with your router. Enter a name for the CA file. Click the browse button to look for the CA file on your computer.



# User Groups

This section is used to configure Certificates that are used with an IPSec based VPN. You can configure local certificates and the certificates of remote peers. Select one of the three options from the drop-down menu: **Local Certificate & Private key**, **Certificate of Remote Peers**, or **Certificate Authorities**.

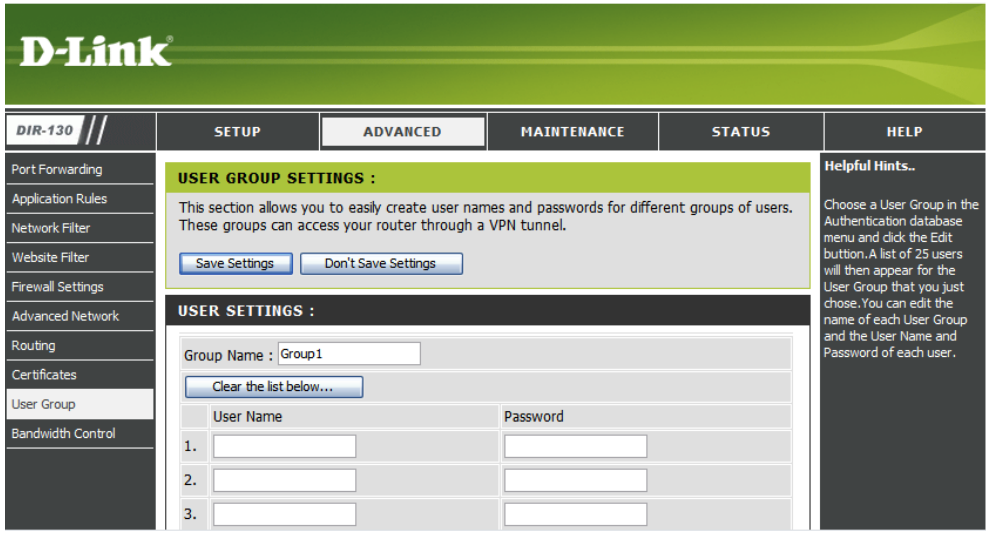
**Authentication Database:** Select a user group from the menu and click the EDIT button to configure that group.




**Group Name:** Enter a name for the user group. Click the **Clear the list below** button to erase all of the user names and passwords for the user group.

**User Name:** Enter a User Name.

**Password:** Enter a Password for your User Name.



# Bandwidth Control

This section allows you to set bandwidth limits for specific IP addresses and/or applications.

**Name:** Select a name for your bandwidth control rule.

**Application Name:** This dropdown box lets you select from a list of common applications and fills in some of the settings automatically for you after you select an application, then click the **< <** button.

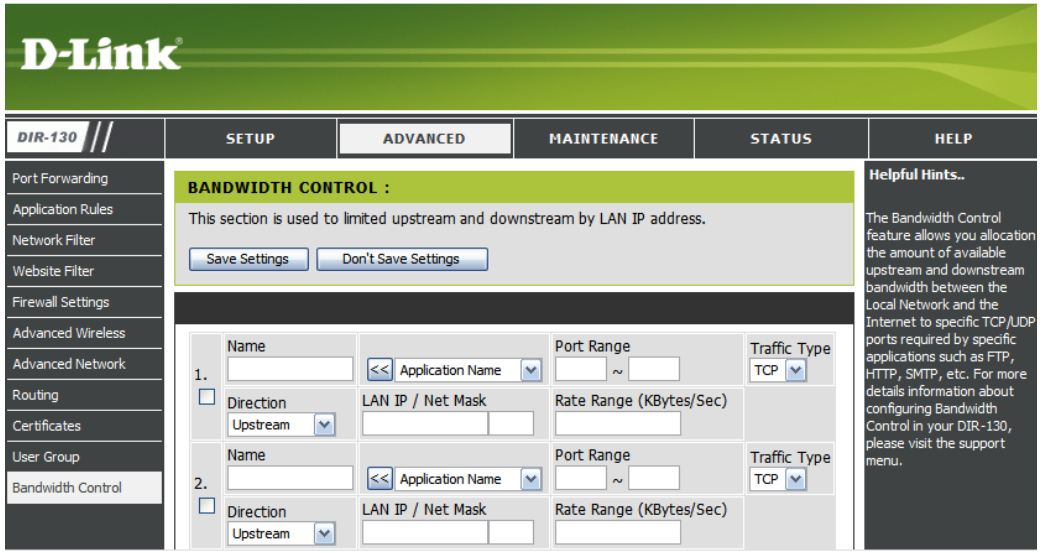
**Port Range:** Select the port range to apply bandwidth control to.

**Traffic Type:** Select what type of traffic to apply bandwidth control to: **UDP**, **TCP**, or **All**.

**Direction:** Specify whether you want to limit **Upstream**, **Downstream**, or **All** bandwidth.

**LAN IP / Net Mask:** Enter the IP or Net Mask of the computers you want to apply bandwidth control to.

**Rate Range (KBytes/Sec):** Enter a transfer speed range you want to use to control your bandwidth.



# Administrator Settings

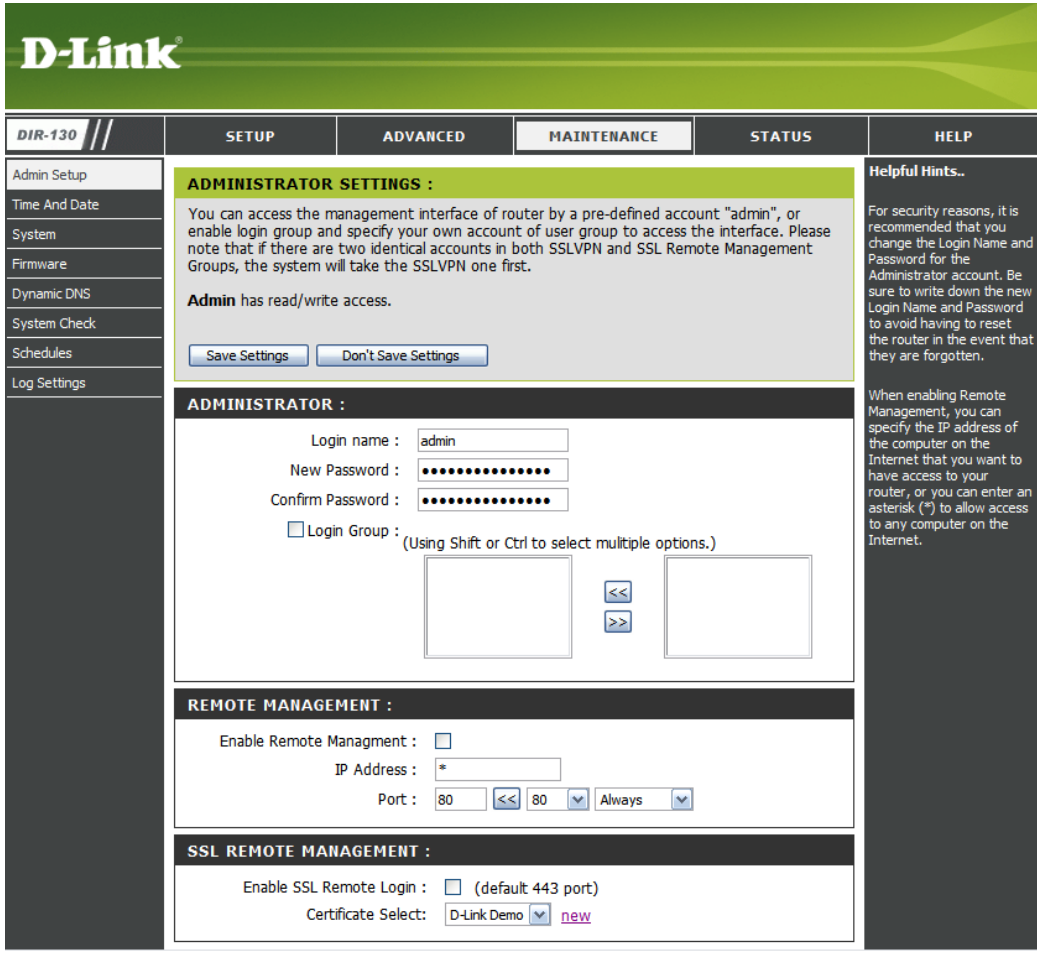
This page will allow you to manage administrative access to your router. You can also enable Remote Management here.

## Administrator

**Login name:** Enter a login name to use for administrative access to your router.

**New/Confirm Password:** Enter a **New Password** for the administrator login, and retype your password in **Confirm Password**. Only the administrator can make changes to the settings.

**Login Group:** You can also assign a User Group to have administrative access to your router. To do so, check the checkbox next to **Login Group**, select one or more User Groups, then click the **> >** button to allow access to the User Group, or use the **< <** button to remove access.



# Remote Management / SSL Remote Management

**Enable Remote Management:** Check this checkbox to enable remote management.

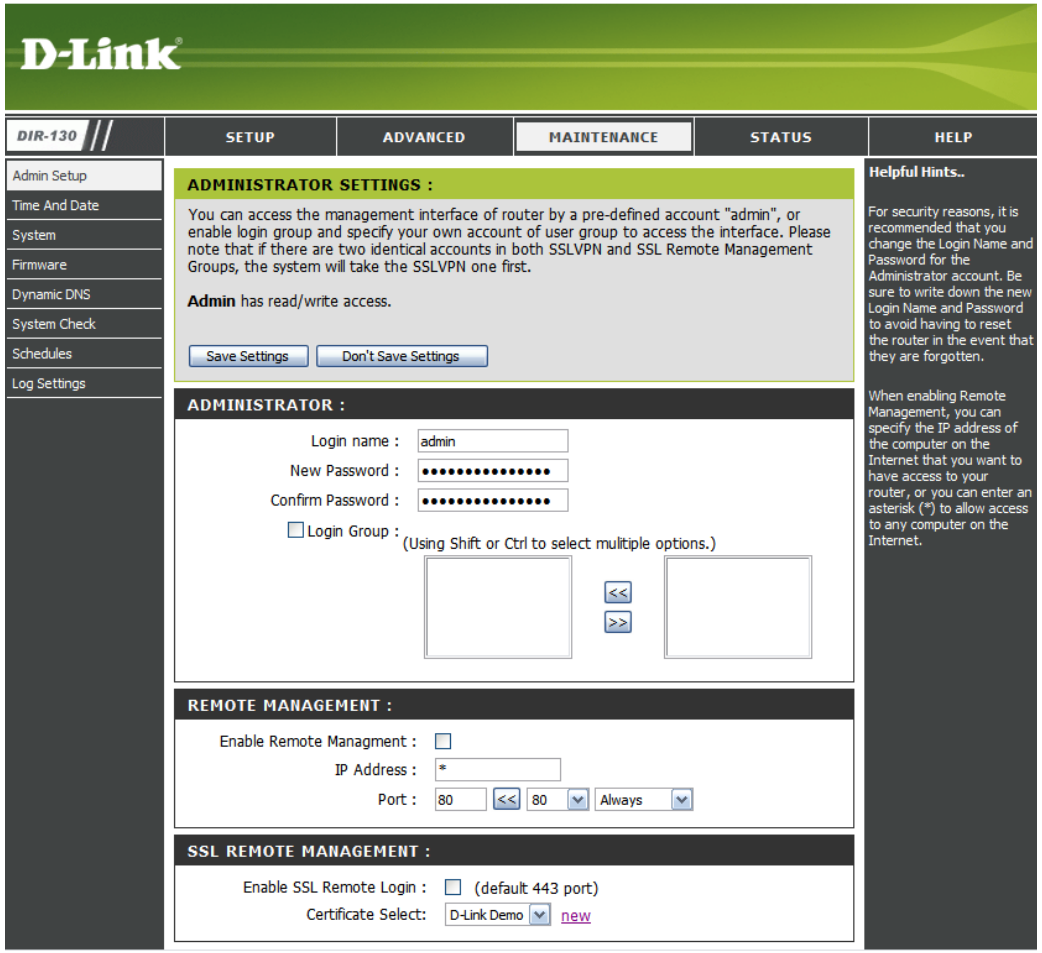
**IP Address:** Enter an IP address to allow remote access to. You can enter * to allow connection from any IP.

**Port:** The port number used to remotely access the DIR-130.

Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DIR-130 and 8080 is the port used for the Web Management interface. The schedule may be set to **Always**, which will allow the filter to always be enabled. You can create your own times in the **Maintenance** > **Schedules** section.

**Enable SSL Remote Login:** Check this checkbox to enable SSL remote login to your router.

**Certificate Select:** Select a certificate to use for SSL. You can add a new certificate by clicking **New**, which will take you to the **Advanced > Certificates** page.



# Time and Date

The Time and Date page allows you to configure, update, and maintain the correct time and date 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 configure to automatically adjust the time when needed.

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

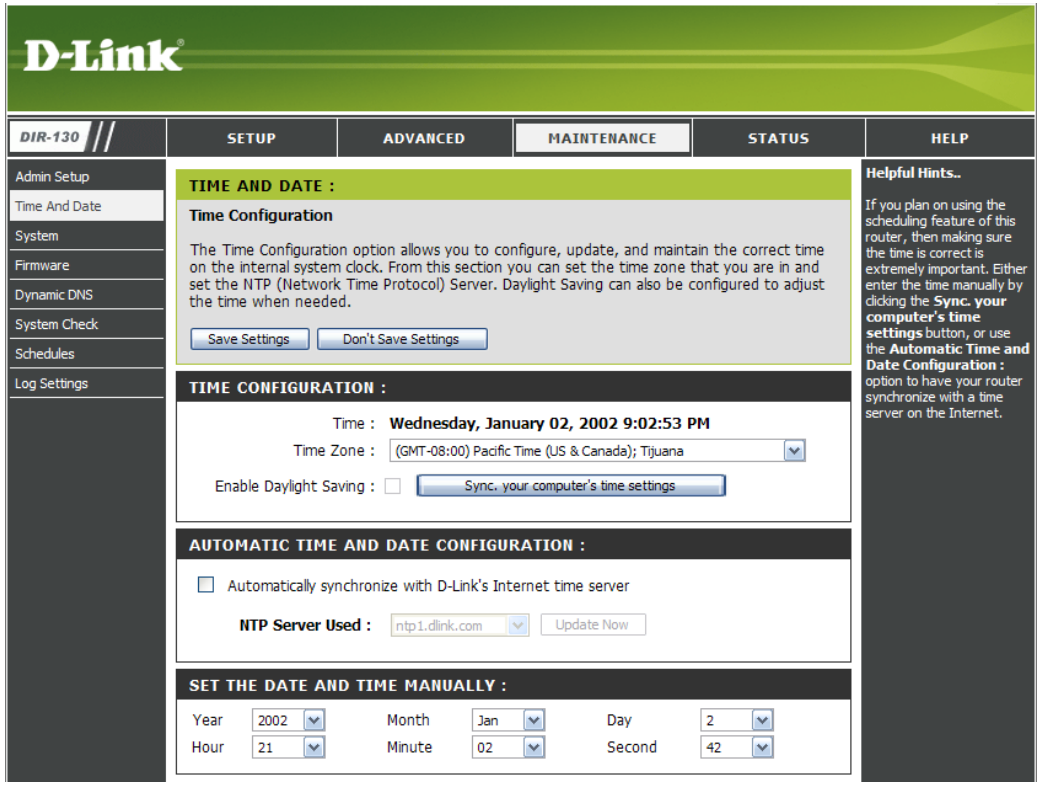
**Enable Daylight Saving:** Check the checkbox to enable daylight savings time.

**Sync. Your computer's time settings:** Click this button to copy the time settings from your computer.

**Automatic Time and Date Configuration:** Check the box to use NTP (Network Time Protocol) server. NTP synchronizes computer clock times in a network of computers. This will only connect to a server on the Internet, not a local server.

**NTP Server Used:** Select an NTP server from the drop-down menu.

**Manual:** To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Save Settings**.



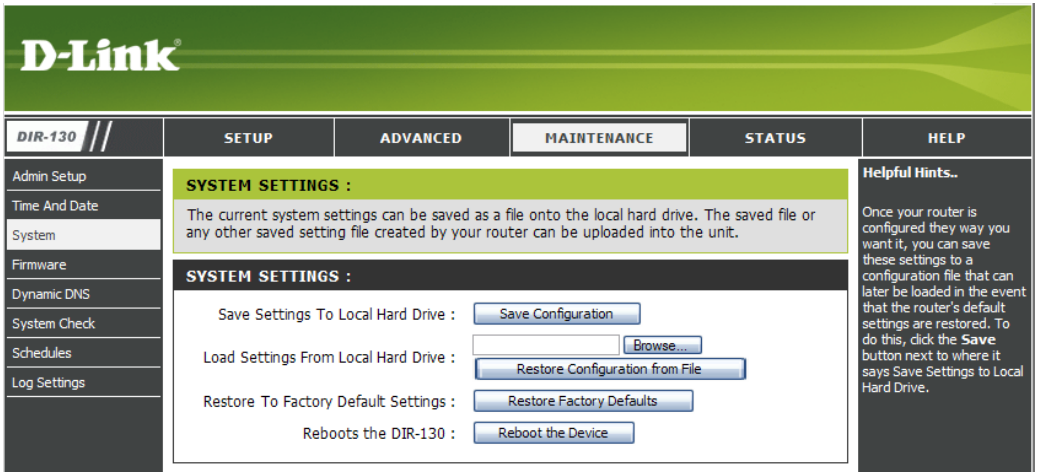
# System Settings

**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 Configuration** button. You will then see a file dialog, where you can 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, click the **Browse** button to find a previously save file of configuration settings. Then, click the **Restore Configuration from File** 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 Configuration** button above.

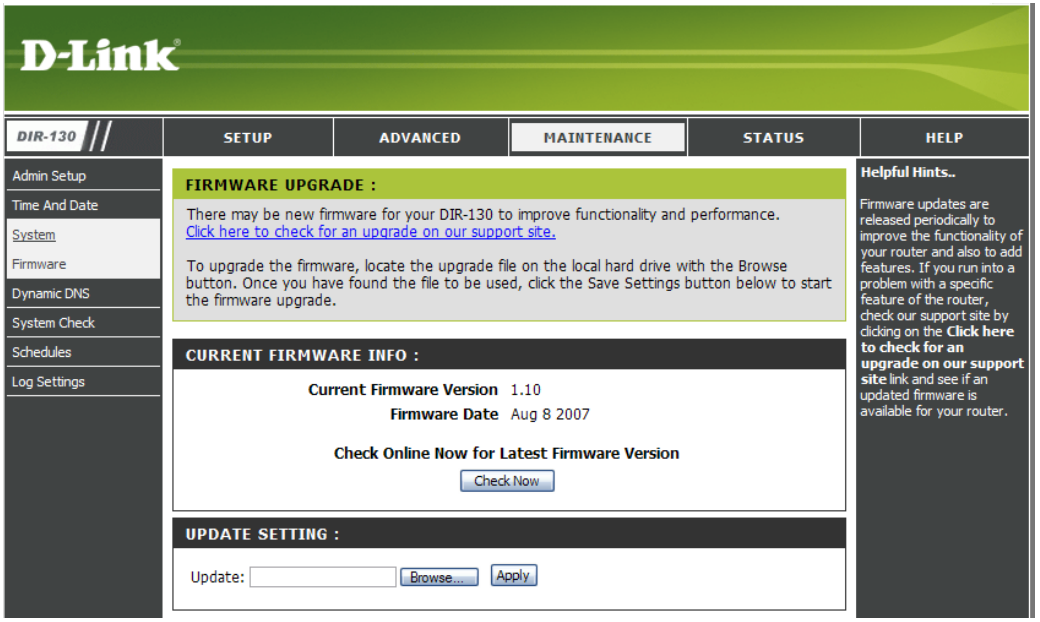
**Reboot the DIR-130:** Click to reboot the router.



# Update Firmware

You can upgrade the firmware of the router 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 site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

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



# DDNS

DDNS (Dynamic Domain Name System) is a method of keeping a domain name linked to a changing IP Address. 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 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.

**DDNS:** Check the box to enable DDNS.

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

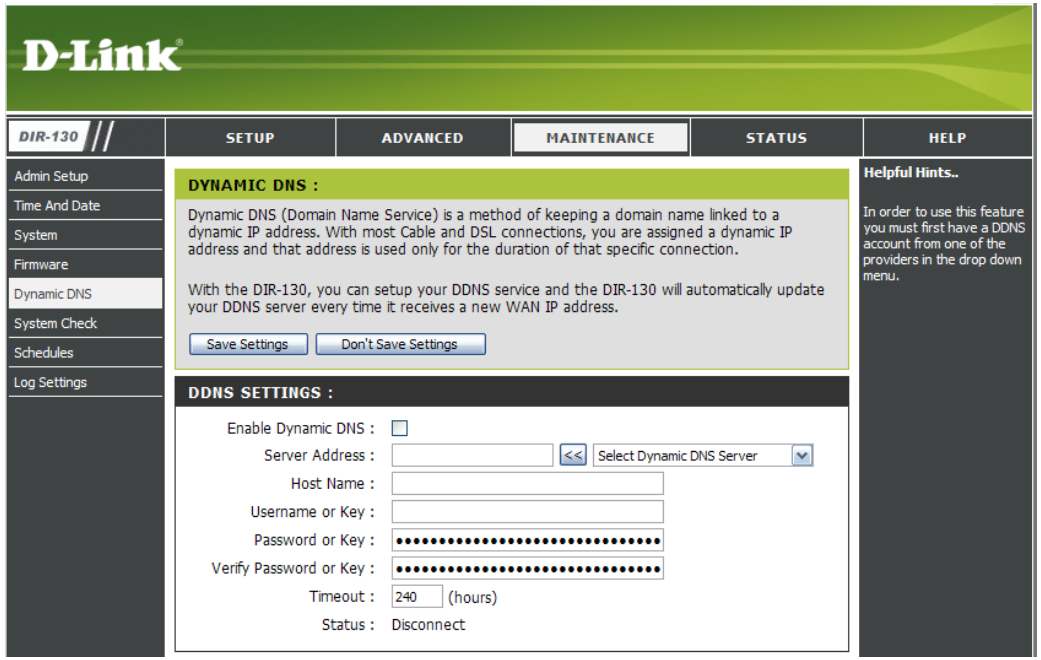
**Host Name:** Enter you Host Name that you registered with your DDNS service provider.

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

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

**Verify Password or Key:** Reenter the password or key for your DDNS account.

**Timeout:** The default value is 240 (hours). Do not change this value unless otherwise specified by you DDNS service provider.

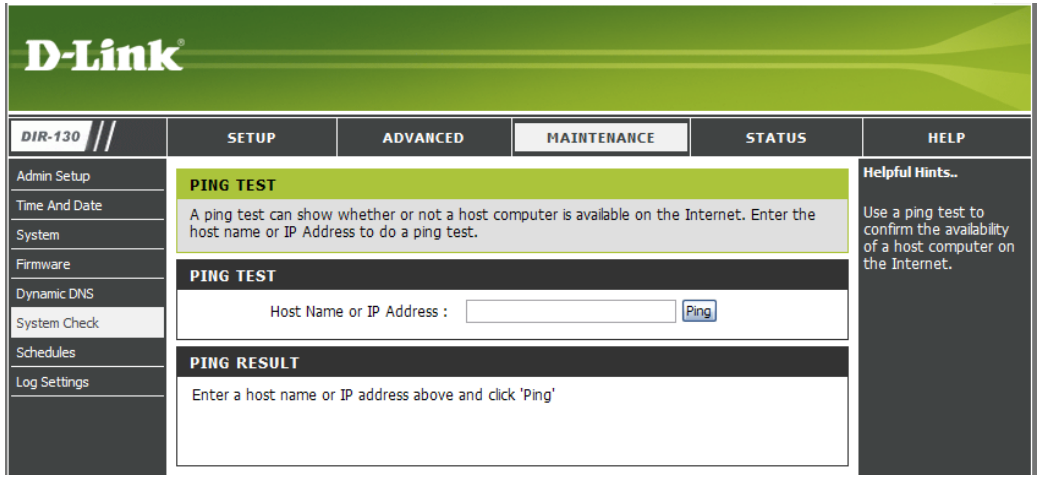


# System Check

The router System Check uses a ping test to send ping packets to test if a computer in on the Internet.

**Ping Test:** Enter the IP address that you wish to ping and click the **Ping** button.

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



# Schedules

This section is used to manage schedule rules for port forwarding, firewall rules, web filtering, and remote management.

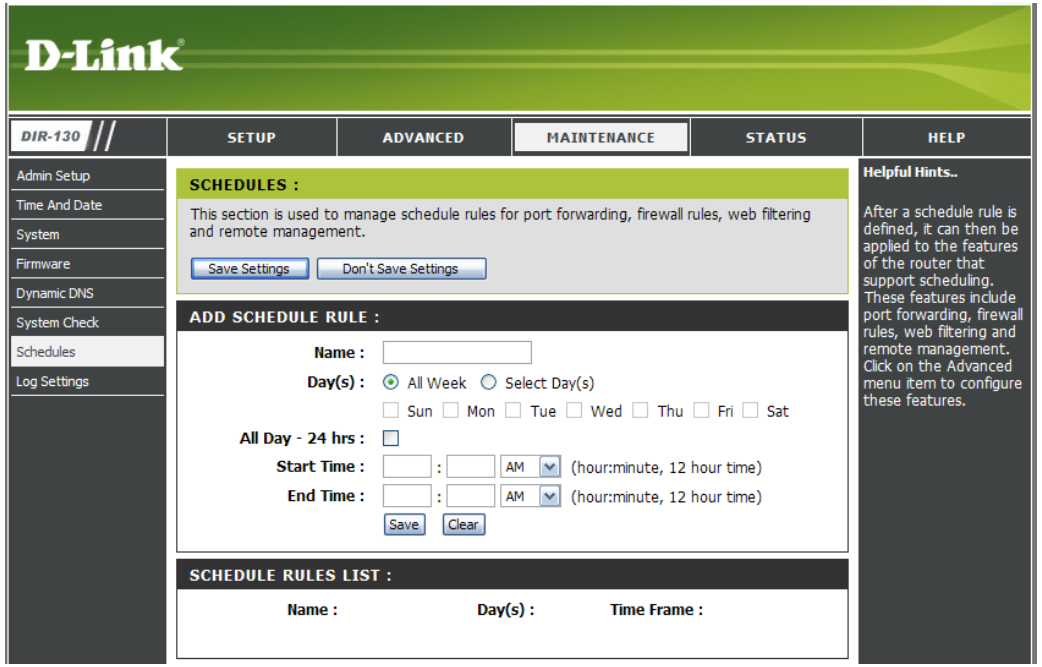
**Name:** Enter a name for your new schedule.

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

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

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

**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.



# Log Settings

The DIR-130 can send event logs to your e-mail address.

**From Email Address:** Enter what e-mail address you want the log e-mail to have in its From field.

**To Email Address:** Enter what e-mail address you want to send log e-mails to. Click on the **Send Mail Now** button to send the current log file to your e-mail address.

**SMTP Server/IP Address:** Enter the address of the SMTP server that will be used to send the logs.

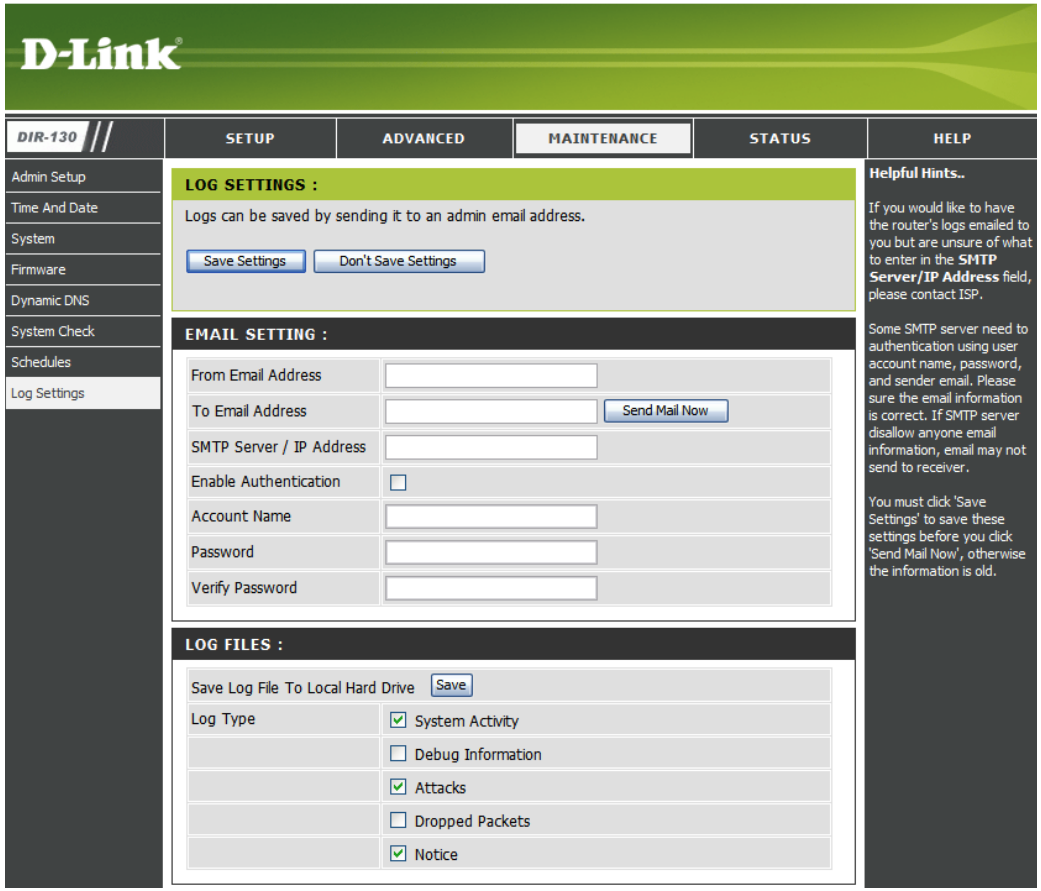
**Enable Authentication:** If your SMTP server requires authentication, check this box.

**Account Name:** If your SMTP server requires authentication, enter your account name for your SMTP server.

**Password/Verify Password:** If your SMTP server requires authentication, enter the password required to log in to your SMTP server, then retype the password in the **Verify Password** text box.

**Save Log File to Local Hard Drive:** Click the **Save** button to open a dialog box to save the log to your local hard drive.

**Log Type:** Here, check the different events you would like to be added to the router log.



# Device Information

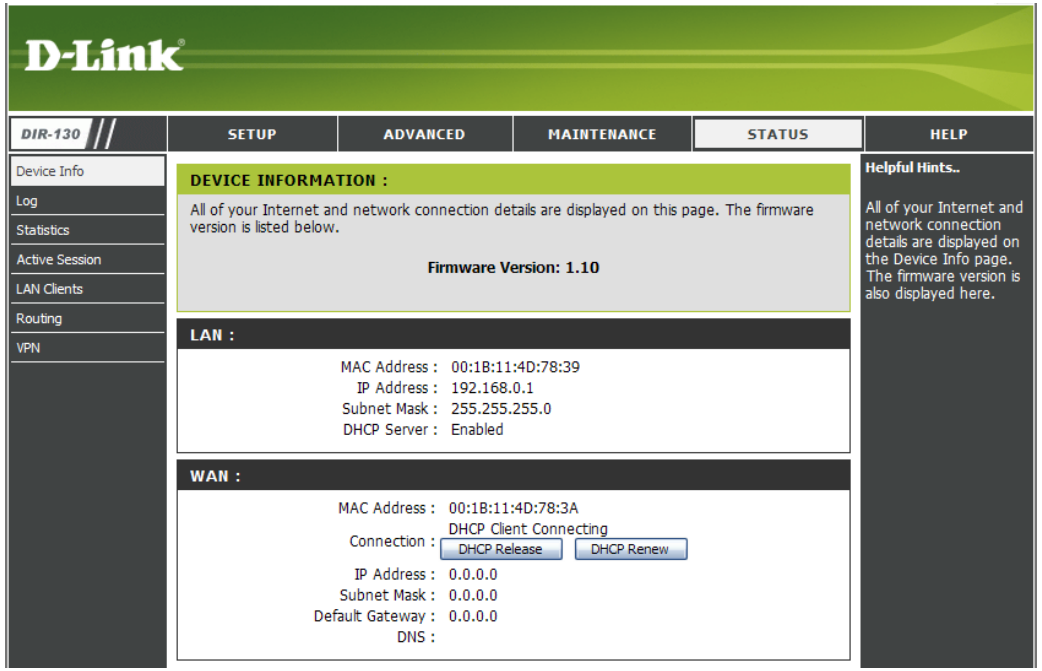
This page displays the current information for the DIR-130. It will display the LAN, WAN (Internet), and the firmware version of the router.

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.

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

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



# Log

This page displays the log events of the router. Here you can view the logs of the router.

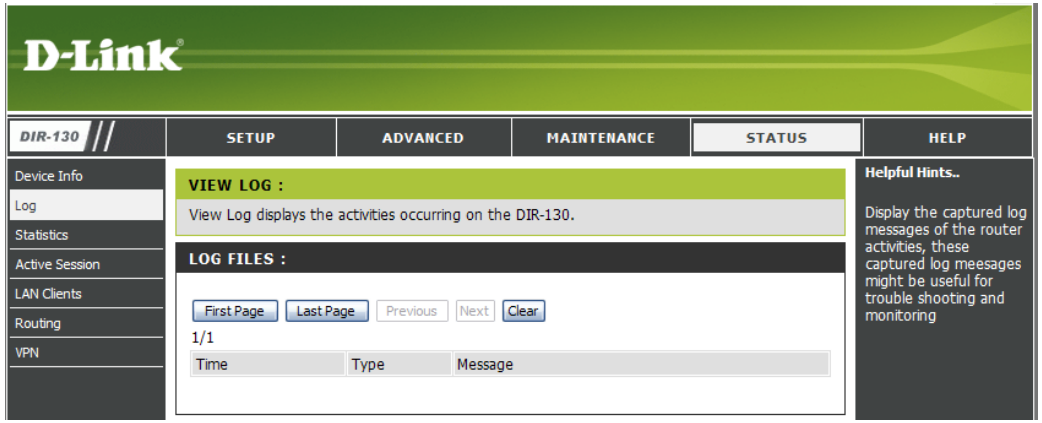
**First Page:** This button will direct you to the current first page of the log.

**Last Page:** This button will direct you to the current last page of the log.

**Previous:** Click to view the previous page of the log.

**Next:** Click to view the next page of the log.

**Clear:** Clears all current log content.



# Statistics

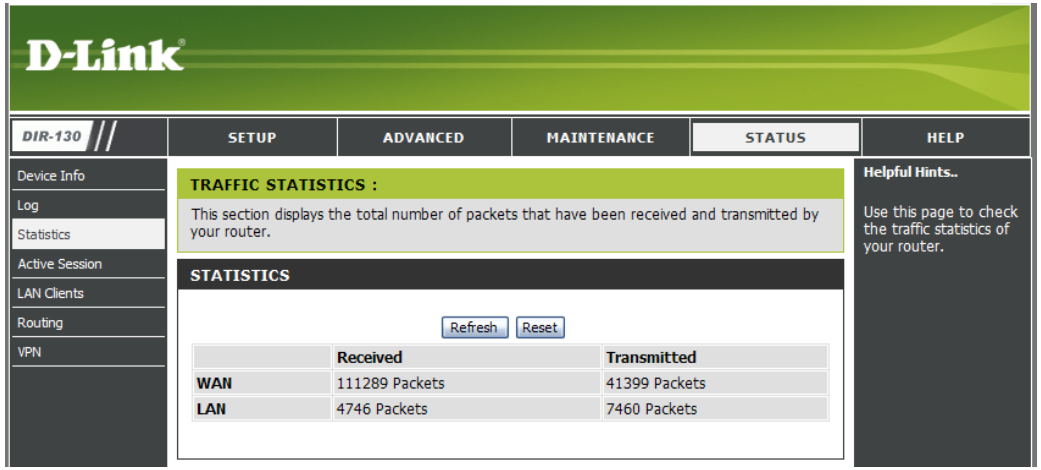
This page displays the current statistics of the router. Here you can view the amount of packets that pass through the router.

**Refresh:** This button will refresh the statistics to display updated information.

**Reset:** This button will reset the statistics packet count to zero for all interfaces listed.

**WAN:** Displays the amount of packets transmitted and received on the WAN interface.

**LAN:** Displays the amount of packets transmitted and received on the LAN interface.



# Active Session

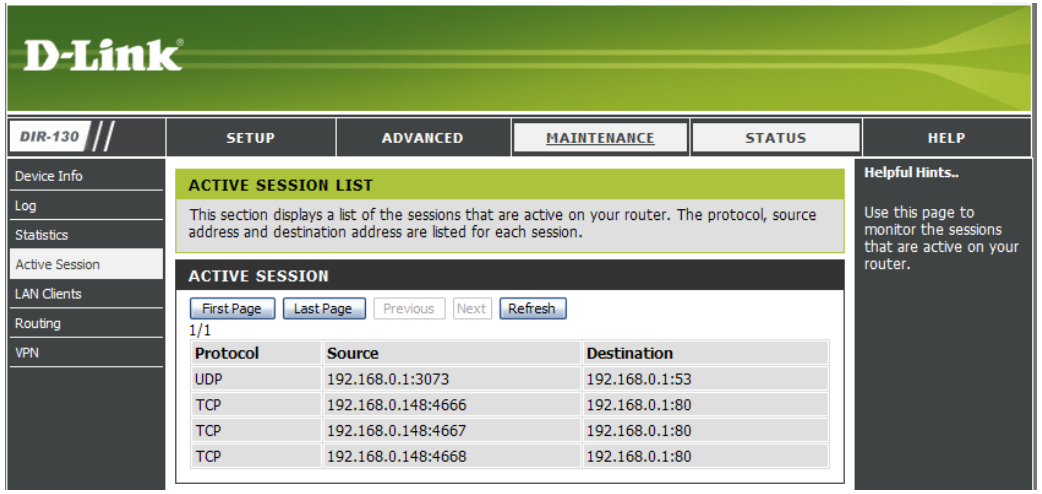
The Active Session Status menu shows the active sessions currently running on your router. The list will display the protocol, the source IP address and the destination IP address for each active session.

**First Page:** This button will direct you to the current first page of the active sessions.

**Last Page:** This button will direct you to the current last page of the active sessions.

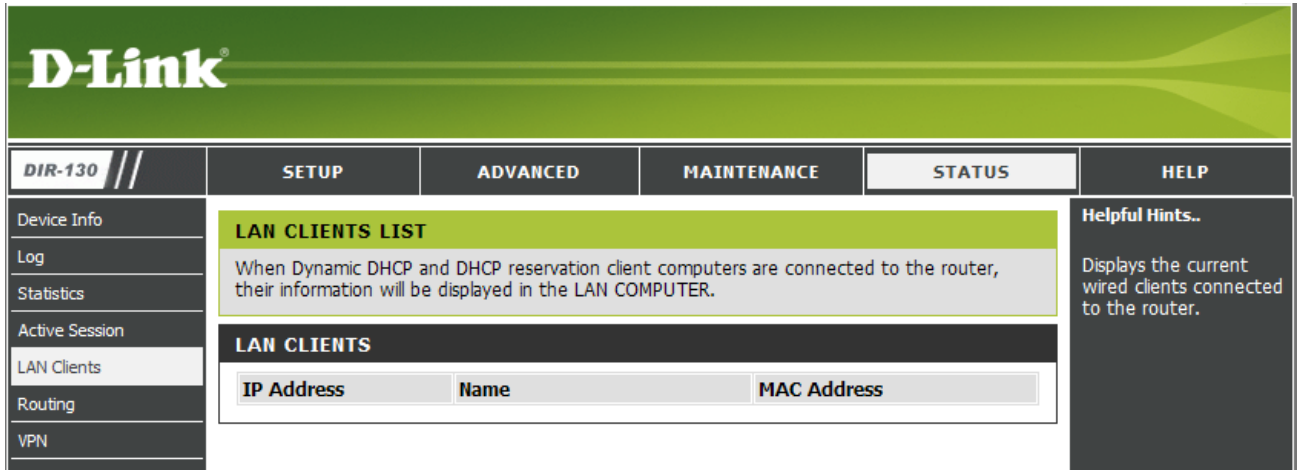
**Previous:** This button will direct you to the previous page of the active sessions.

**Next:** This button will direct you to the next page of the active sessions.



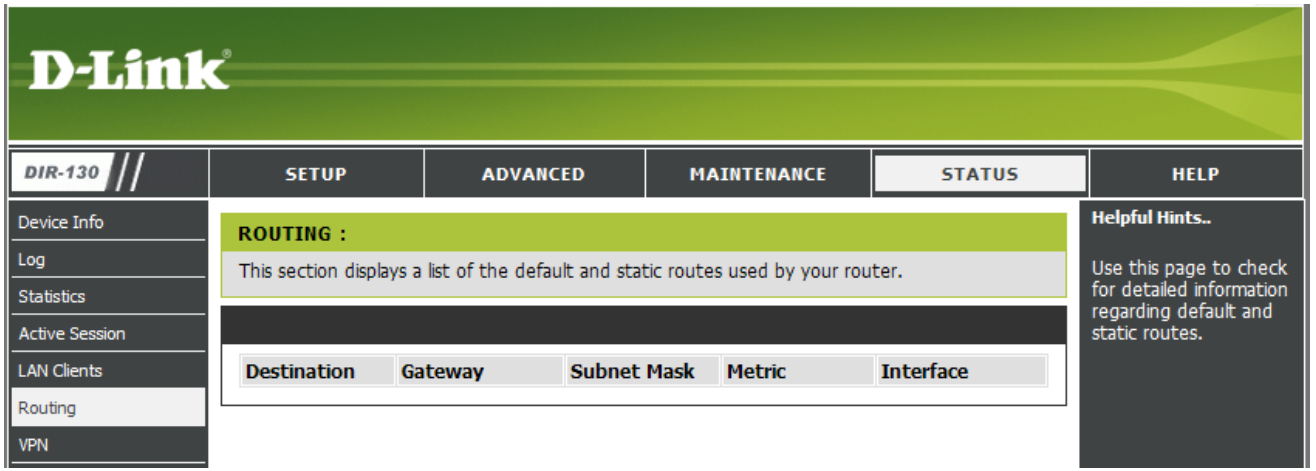
# LAN Clients

This page displays a list of currently connected wired clients. This table also displays the connection time and MAC address of the connected wired clients.



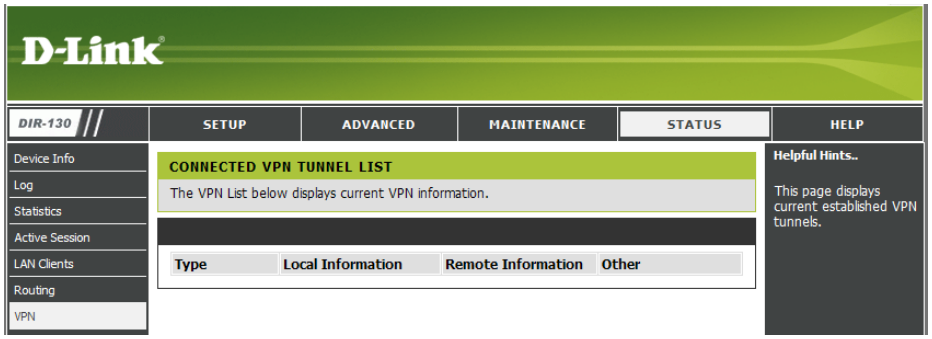

# Routing

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



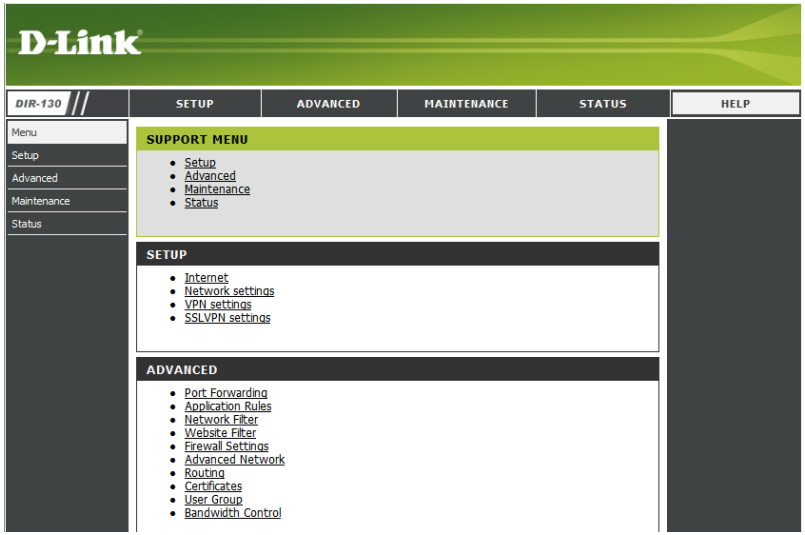
# VPN

The VPN table displays a list of current PPTP, L2TP, L2TP over IPsec, and SSL VPN sessions.




# Help

The support menu provides additional information regarding features included in the DIR-130 Web Management Interface.



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-130. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® Vista™ and 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 on the Internet or 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:
  - Internet Explorer 6.0 or higher
  - Firefox 1.5 or higher
  - Netscape 8 or higher
  - Mozilla 1.7.12 (5.0) or higher
  - Opera 8.5 or higher
  - Safari 1.2 or higher (with Java 1.3.1 or higher)
  - Camino 0.8.4 or 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® 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** > **Control Panel**. In Windows® XP or Windows Vista™, make sure you are in Classic View. 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 the 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. You will lose all your custom settings.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is **admin** and leave the password box empty. A list of the default settings can be found on page 64.

**3. Why can't I connect to certain sites or send and receive e-mails when connecting through my router?**

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

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

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

- Windows Vista™ users click on **Start** and type ***cmd*** in the **Start Search** box. Click **OK** or press **Enter**.
- Windows® NT, 2000 and XP users click on **Start,** click **Run**, and then type ***cmd*** in the box. Click **OK** or press **Enter**.
- Windows® 95, 98, and Me users click on **Start,** click **Run**, and then type ***command***. Click **OK** or press **Enter**.
- 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 (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your e-mail. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

**4. Why is the date on the logs incorrect?**

The router has not successfully connected to a Network Time (NTP) server. Check that your Internet connection settings are correct. If you have connected for the first time, allow up to 10 minutes to connect.

If the time is off by 1 hour, make sure you have selected the correct time zone and that Daylight Savings is selected.

Refer to **Section 3 - Configuration > Time and Date** for more information.

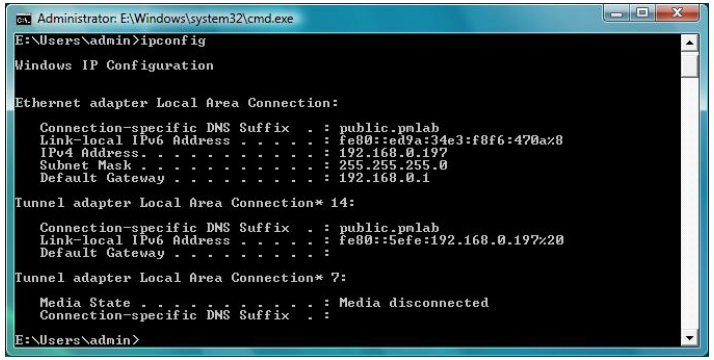
# Networking Basics

## Check your IP address

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

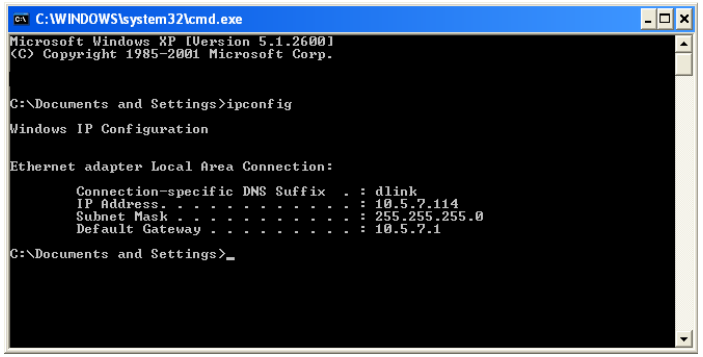
### Windows Vista™ Users:

- Click **Start** > **All Programs** > **Accessories** > **Command Prompt**. You may need administrative access to run this application.
- For all additional prompt windows inquiring of running the command prompt application, select **Yes**, **OK**, or **Continue**.
- At the prompt, type ***ipconfig*** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.




### Windows® 2000/XP Users:

- Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK**.
- 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.

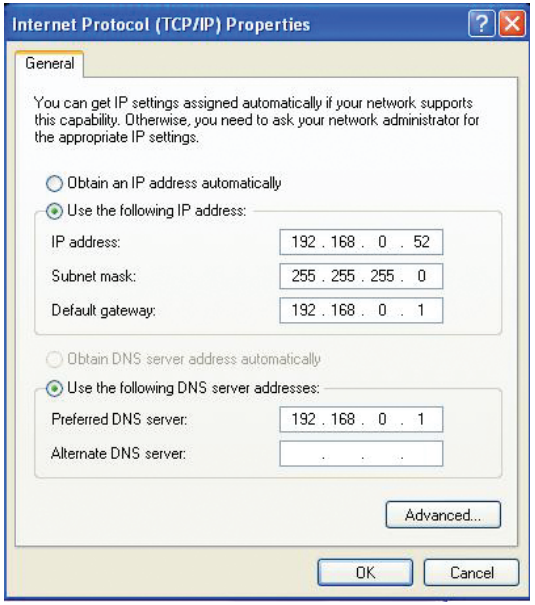
# Statically Assign an IP address

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

## Windows® XP/2000 Users

- **Windows® XP** - Click on **Start** > **Control Panel**. Make sure you are in Classic View. Double-click on the Network Connections icon.
  **Windows® 2000** – From the desktop, right-click **My Network Places** > **Properties**.
- Right-click on the **Local Area Connection** which represents your D-Link network adapter (or other adapter) which will be connected to your router.
- Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router.

  Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.
- Set **Default Gateway** the same as the LAN IP address of your router (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 optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.

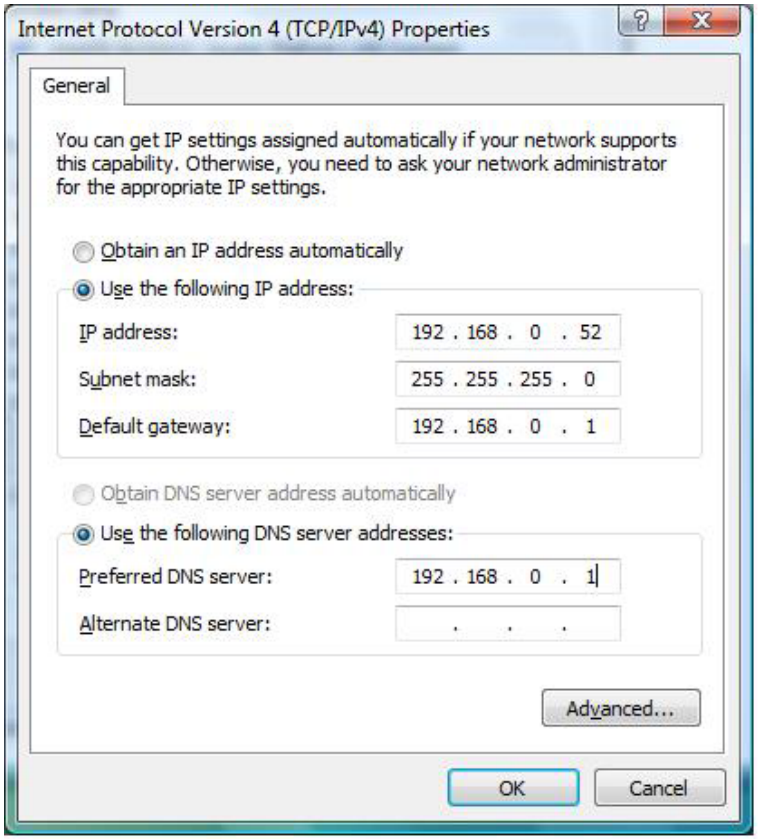


## Windows Vista™ Users

- Click on **Start** > **Control Panel**. Make sure you are in Classic View. Double-click on the **Network and Sharing Center** icon. Along the left panel in the window, click on **Manage network connections**.
- Right-click on the **Local Area Connection** which represents your D-Link network adapter (or other adapter) which will be connected to your router.
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router.

  Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.

- Set **Default Gateway** the same as the LAN IP address of your router (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 optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.



# Technical Specifications

**Standards**

- IEEE 802.3
- IEEE 802.3u

**LEDs**

- Power
- Status
- WAN
- LAN (1-8)

**Operating Temperature**

- 32°F to 104°F ( 0°C to 40°C)

**Humidity**

- 95% maximum (non-condensing)

**Safety & Emissions**

- FCC
- CE
- IC

**Dimensions**

- Length = 7.6 inches
- Width = 4.6 inches
- Height = 1.2inches

**Warranty**

- 1 Year

# Default Factory Settings

When you receive your router, the default factory settings are in effect as listed in the table below. You may change any of the network settings. If you perform a reset (hold the reset button on the back of the unit), the router will reset with the following settings:

| Setting | Default Value |
|---|---|
| Username | admin |
| Password | (leave blank) |
| LAN IP Address | 192.168.0.1 |
| DHCP Server | Enabled |
| DHCP IP Range | 192.168.0.100 - 192.168.0.150 |
| Filtering / Virtual Server / DMZ / Applications | Disabled |

# 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-130)
- 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:**
(877) 354-6560

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

# 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 DLink 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 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.

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

Copyright © 2007 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

## CE Mark Warning:

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

## 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.

## FCC Caution:

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

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

## IC statement

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

# GNU/Linux GPL

- “GPL Software” means GPL software licensed to you under the GNU General Public License as published by the Free Software Foundation (GPL). A copy of the GPL is included below.

- “Open Source Software” means various open source software components licensed under the terms of applicable open source license agreements included in the materials relating to such software. Open Source Software is composed of individual software components, each of which has its own copyright and its own applicable license conditions. The Open Source Software licenses can be found in the **gpl.pdf** file, other materials accompanying the software package, the documentation or corresponding source files available from http://support.dlink.com/GPL.asp.

# GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

**Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) 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 this service 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 make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. 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.

We protect your rights with two steps:

(1) copyright the software, and

(2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that hat they have is not the original,

so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

   Whether that is true depends on what the Program does.

1. You may copy and distribute 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 and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any

change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This

alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), 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 distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the 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 a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, 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.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE 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.

**END OF TERMS AND CONDITIONS**

# Registration

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

Version 1.2(WW)
December 10, 2008