

USER MANUAL

DIR-330

VERSION 1.2



D-Link[®]

WIRELESS

Manual Overview

This manual contains the following sections:

Section 1 - “Product Overview” describes what is included with the DIR-330 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-330 router (page 11).

Section 4 - “Wireless Security” explains how to setup wireless encryption on your wireless router (page 64).

Section 5 - “Connect to a Wireless Network” explains how to configure your wireless clients to connect to your router (page 73).

Section 6 - “Troubleshooting” explains how to resolve common issues (page 81).

Appendix - “Appendix” contains wireless and networking basics, technical specifications, technical support information, warranty, GNU general public license, and registration information (page 85).

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

Manual Revisions

Revision	Date	Description
1.0	January 15, 2007	<ul style="list-style-type: none">• DIR-330 Revision A1 with firmware version 1.00
1.1	September 13, 2007	<ul style="list-style-type: none">• Updated for firmware version 1.10• Added Windows Vista™ support
1.2	October 28, 2008	<ul style="list-style-type: none">• Updated for firmware version 1.20• Added SSL VPN• 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	Russian PPTP	24
Manual Revisions	ii	Wireless Settings	25
Trademarks	ii	Wi-Fi Protected Setup (WCN 2.0)	25
Product Overview	1	Wireless Network Settings	26
Package Contents	1	Network Settings	27
System Requirements	2	DHCP Server Settings	28
Features	3	DHCP Reservation	29
Hardware Overview	4	VPN Settings	30
Connections	4	IPSec Settings	31
LEDs	5	PPTP/L2TP Settings	34
Installation	6	SSL VPN Settings	35
Before you Begin	6	Port Forwarding	36
Wireless Installation Considerations	7	Application Rules	37
Connect to Cable/DSL/Satellite Modem	8	MAC Filters	38
Connect to Another Router	9	Website Filters	39
Configuration	11	Firewall Settings	40
Web-based Configuration Utility	11	DMZ	40
Setup Wizard	12	Firewall Rules	41
Manual Configuration	17	Advanced Wireless Settings	42
Dynamic (DHCP)	17	Tx Rate	42
PPPoE (DSL)	18	DTIM Interval	42
PPTP	19	Preamble	42
L2TP	20	WMM Function	42
Static IP	21	Advanced Network Settings	43
Russian PPPoE	22	UPnP	43
		WAN Ping Respond	43
		WAN Port Speed	43

Routing	44	Configure WPA/WPA2-PSK	71
Certificates	45	Configure WPA/WPA2-EAP (RADIUS)	72
User Groups	46	Connect to a Wireless Network.....	73
Bandwidth Control	47	Using Windows Vista™	73
Administrator Settings.....	48	Configure WEP/WPA/WPA2.....	74
Change Password.....	48	Using Windows® XP.....	76
Remote Management.....	48	Configure WEP	77
Time and Date Settings	50	Configure WPA-PSK.....	79
System Settings.....	51	Troubleshooting	81
Update Firmware	52	Wireless Basics	85
DDNS.....	53	What is Wireless?	86
System Check.....	54	Tips.....	88
Schedules	55	Wireless Modes	89
Log Settings.....	56	Networking Basics	90
Device Information.....	57	Check your IP address	90
Log.....	58	Statically Assign an IP address	91
Statistics	59	Technical Specifications.....	93
Active Session	60	Default Factory Settings	94
Wireless Clients	61	Contacting Technical Support	95
LAN Clients.....	61	Warranty.....	96
Routing	62	GNU/Linux GPL.....	102
VPN	62	GNU General Public License.....	103
Help	63	Registration.....	109
Wireless Security.....	64		
What is WEP?	64		
What is WPA?	65		
Wireless Security Setup Wizard	66		
Configure WEP.....	70		

Package Contents

<p>D-Link DIR-330 Wireless VPN Router</p>	
<p>Power Adapter</p>	
<p>Ethernet Cable</p>	
<p>CD-ROM</p>	

Note: Using a power supply with a different voltage rating than the one included with the DIR-330 will cause damage and void the warranty for this product.

System Requirements

<p>Network Requirements</p>	<ul style="list-style-type: none"> • An Ethernet-based Cable or DSL modem • 802.11g/b wireless clients • 10/100 Ethernet devices
<p>Web-based Configuration Utility Requirements</p>	<p>Computer with the following:</p> <ul style="list-style-type: none"> • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter <p>Browser Requirements:</p> <ul style="list-style-type: none"> • Internet Explorer 6.0 or higher • Mozilla 1.7.12 or higher • Firefox 1.5 or higher • Safari 1.0 or higher (with Java 1.3.1 or higher) • Flock 0.7.14 or higher • Opera 6.0 or higher <p>Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.</p>
<p>CD Installation Wizard Requirements</p>	<p>Computer with the following:</p> <ul style="list-style-type: none"> • Windows® XP with Service Pack 2 or Vista™ • An installed Ethernet adapter • CD-ROM drive

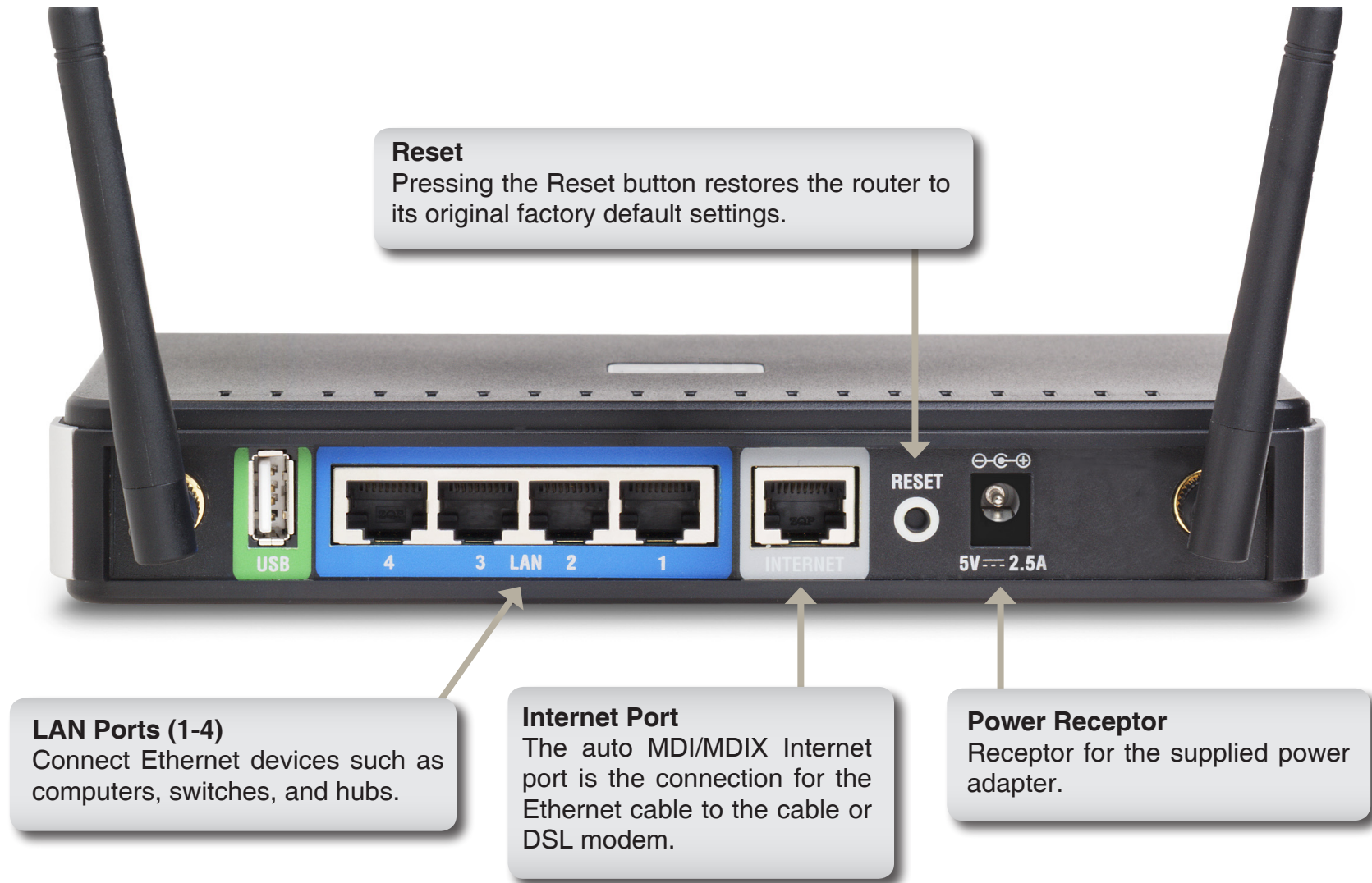
Features

- **Faster Wireless Networking** - The DIR-330 provides up to 54Mbps* wireless connection with other 802.11g wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.
- **Compatible with 802.11b Devices** - The DIR-330 is still fully compatible with the IEEE 802.11b standard, so it can connect with existing 802.11b PCI, USB and Cardbus adapters.
- **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-330 can pass through VPN sessions. It supports multiple and concurrent IPsec and PPTP sessions, so users behind the DIR-330 can securely access corporate networks.

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

Hardware Overview

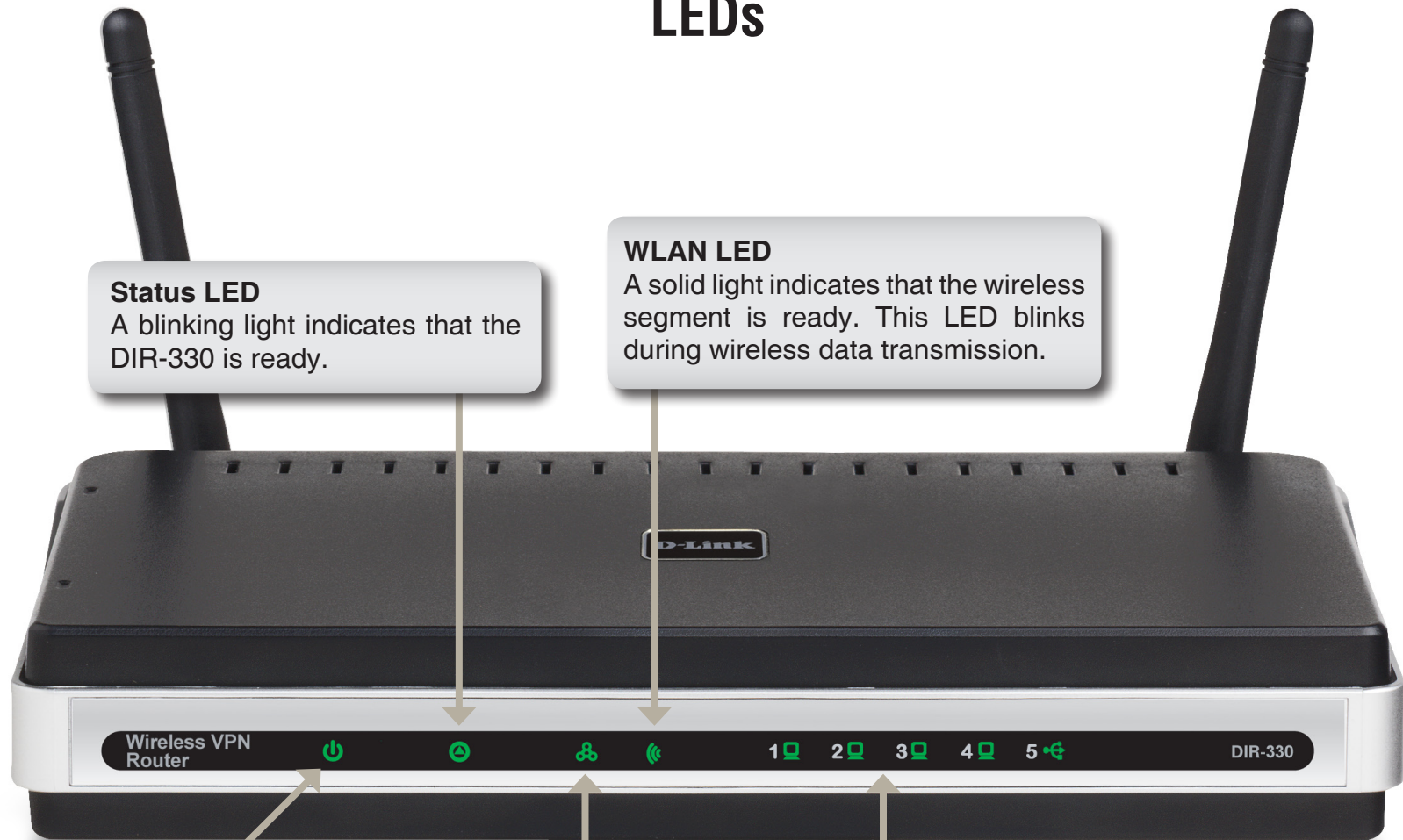
Connections



* The USB port is currently inactive.

Hardware Overview

LEDs



Status LED

A blinking light indicates that the DIR-330 is ready.

WLAN LED

A solid light indicates that the wireless segment is ready. This LED blinks during wireless 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.

Local Network LEDs

A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

Installation

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, or in the attic or garage.

Before you Begin

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

Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

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 11 to configure your router.

Connect to Another Router

If you are connecting the D-Link router to another router to use as a wireless access point and/or 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** 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.

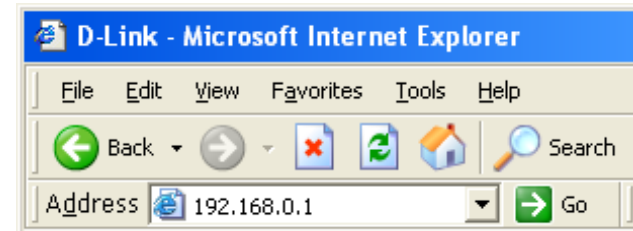
6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.
7. Connect an Ethernet cable in one of the LAN ports of the router and connect it to your other router. Do not plug anything into the Internet port of the D-Link router.
8. You may now use the other 3 LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the **Configuration** and **Wireless Security** sections for more information on setting up your wireless network.

Configuration

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

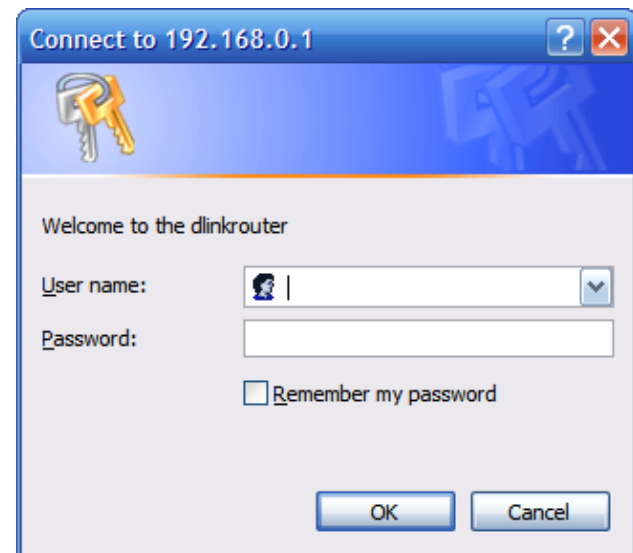
Web-based Configuration Utility

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

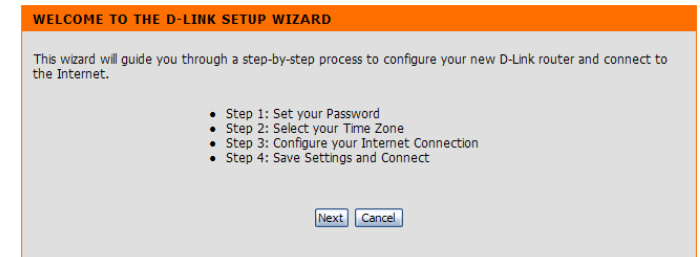
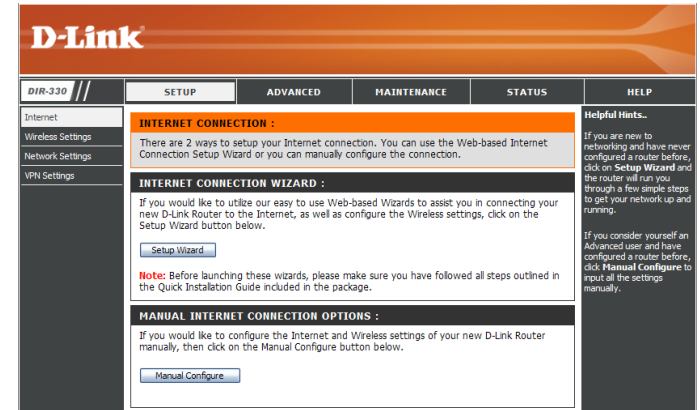
You may click **Setup Wizard** to quickly configure your router.

If you want to enter your settings without running the wizard, click **Manual Configure** and skip to page 17.

If you want to configure your wireless settings using the **Wireless Security Setup Wizard**, skip to page 64.

Click **Next** to continue.

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



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

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

STEP 2: SELECT YOUR TIME ZONE

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

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

Prev Next Cancel

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

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Your Internet Connection could not be detected. Please select your Internet Service Provider (ISP) from the list below. If your ISP is not listed, select the "Not Listed or Don't Know" option to manually configure your connection.

Not Listed or Don't Know

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

- DHCP Connection (Dynamic IP Address)**
This automatically provides you with an IP Address. Cable modems often use this type of connection.
- Username / Password Connection (PPPoE)**
This requires a username and password. DSL modems often use this type of connection.
- Username / Password Connection (PPTP)**
This requires a username and password. DSL modems often use this type of connection.
- Username / Password Connection (L2TP)**
This requires a username and password. DSL modems often use this type of connection.
- Username / Password Connection (Russian PPPoE)**
This requires a username and password. DSL modems often use this type of connection.
- Username / Password Connection (Russian PPTP)**
This requires a username and password. DSL modems often use this type of connection.
- Static IP Address Connection**
This requires manual configuration of the IP Address information that your ISP provided.

Prev Next Cancel

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.

DHCP CONNECTION (DYNAMIC IP ADDRESS)

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

MAC Address : 00 - 00 - 00 - 00 - 00 - 00 (Optional)

Clone Your PC's MAC Address

Host Name :

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

Prev Next Cancel

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.

SET USERNAME AND PASSWORD CONNECTION (PPPOE)

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

Address Mode: Dynamic IP Static IP

IP Address:

User Name:

Password:

Verify Password:

Service Name: (Optional)

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

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

SET USERNAME AND PASSWORD CONNECTION (PPTP)

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

Address Mode: Dynamic IP Static IP

PPTP IP Address:

PPTP Subnet Mask:

PPTP Gateway IP Address:

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

User Name:

Password:

Verify Password:

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

SET USERNAME AND PASSWORD CONNECTION (L2TP)

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

Address Mode: Dynamic IP Static IP

L2TP IP Address:

L2TP Subnet Mask:

L2TP Gateway IP Address:

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

User Name:

Password:

Verify Password:

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

SET STATIC IP ADDRESS CONNECTION

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

IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Gateway Address : 0.0.0.0
Primary DNS Address :
Secondary DNS Address :

Prev Next Cancel

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.

SET USERNAME AND PASSWORD CONNECTION (RUSSIAN PPPOE)

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

Address Mode : Dynamic IP Static IP
IP Address : 0.0.0.0
User Name :
Password :
Verify Password :
Service Name : (Optional)
WAN Physical Address Mode : Dynamic IP Static IP
WAN Physical IP Address : 0.0.0.0
WAN Physical Subnet Mask : 0.0.0.0
WAN Physical Primary DNS Address :
WAN Physical Secondary DNS Address :

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

Prev Next Cancel

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

SET USERNAME AND PASSWORD CONNECTION (RUSSIAN PPTP)

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

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

User Name :

Password :

Verify Password :

WAN Physical Address Mode : Dynamic IP Static IP

WAN Physical IP Address :

WAN Physical Subnet Mask :

WAN Physical Gateway IP Address :

WAN Physical Primary DNS Address :

WAN Physical Secondary DNS Address :

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.

SETUP COMPLETE!

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

Manual Configuration

Dynamic (DHCP)

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 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 assigned by your ISP.

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

D-Link

DIR-330 //

SETUP ADVANCED MAINTENANCE STATUS HELP

Internet
Wireless Settings
Network Settings
VPN Settings

INTERNET CONNECTION

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

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

Save Settings Don't Save Settings

INTERNET CONNECTION TYPE :

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

My Internet Connection is :

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

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

Host Name :

MAC Address : - - - - - (optional)

Primary DNS Address :

Secondary DNS Address : (optional)

MTU :

Helpful Hints...

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

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

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

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 **Always-on** (Connect Mode option below).

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

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

The screenshot shows the D-Link DIR-330 web interface for Internet Setup. The page is titled "INTERNET CONNECTION" and includes a "Helpful Hints" section on the right. The main content area is divided into sections for "INTERNET CONNECTION TYPE" and "PPPOE".

INTERNET CONNECTION TYPE: The "My Internet Connection is:" dropdown menu is set to "PPPoE (Username / Password)".

PPPOE: The "Dynamic PPPoE" radio button is selected. The form includes fields for:

- User Name: []
- Password: []
- Retype Password: []
- Service Name: [] (optional)
- IP Address: 0.0.0.0
- MAC Address: 00 - 00 - 00 - 00 - 00 - 00 (optional)
- Primary DNS Address: []
- Secondary DNS Address: [] (optional)
- Maximum Idle Time: 5 Minutes
- MTU: 1492
- Connect mode select: Always-on Manual Connect on demand

Buttons for "Save Settings" and "Don't Save Settings" are visible at the top of the form.

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

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 **Always-on** (Connect Mode option below).

MTU: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. 1450 is the default MTU.

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

D-Link

DIR-330

SETUP ADVANCED MAINTENANCE STATUS HELP

Internet

INTERNET CONNECTION

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

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

Save Settings Don't Save Settings

INTERNET CONNECTION TYPE :

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

My Internet Connection is : PPTP (Username / Password)

PPTP :

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

Dynamic IP Static IP

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway : 0.0.0.0

DNS :

Server IP/Name :

PPTP Account :

PPTP Password :

PPTP Retype password :

Maximum Idle Time : 5 Minutes

MTU : 1450

Connect mode select : Always-on Manual Connect-on demand

Helpful Hints..

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

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

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 **Always-on** (Connect Mode option below).

MTU: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. 1450 is the default MTU.

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

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes 'DIR-330', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'Internet' section is selected in the left sidebar. The main content area is titled 'INTERNET CONNECTION' and contains the following sections:

- INTERNET CONNECTION:** A text block explaining the connection types and a 'Note' about PPPoE. Below it are 'Save Settings' and 'Don't Save Settings' buttons.
- INTERNET CONNECTION TYPE:** A section with the instruction 'Choose the mode to be used by the router to connect to the Internet.' and a dropdown menu set to 'L2TP (Username / Password)'.
- L2TP:** A section with the instruction 'Enter the information provided by your Internet Service Provider (ISP)'. It includes radio buttons for 'Dynamic IP' (selected) and 'Static IP'. Below are input fields for:
 - IP Address: 0.0.0.0
 - Subnet Mask: 0.0.0.0
 - Gateway: 0.0.0.0
 - DNS: (empty)
 - Server IP/Name: (empty)
 - L2TP Account: (empty)
 - L2TP Password: (masked with dots)
 - L2TP Retype password: (masked with dots)
 - Maximum Idle Time: 5 Minutes
 - MTU: 1450
- Connect mode select:** Radio buttons for 'Always-on', 'Manual', and 'Connect-on demand' (selected).

On the right side, there is a 'Helpful Hints...' section with text: 'When configuring the router to access the Internet, be sure to choose the correct Internet Connection Type from the drop down menu. If you are unsure of which option to choose, please contact your Internet Service Provider (ISP). If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.'

Internet Setup

Static IP

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

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes 'DIR-330 //', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar lists 'Internet', 'Wireless Settings', 'Network Settings', and 'VPN Settings'. The main content area is titled 'INTERNET CONNECTION' and contains the following text: 'Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, BigPond, Russian PPPoE and Russian PPTP. If you are unsure of your connection method, please contact your Internet Service Provider.' Below this is a 'Note' about PPPoE and two buttons: 'Save Settings' and 'Don't Save Settings'. The 'INTERNET CONNECTION TYPE' section has a dropdown menu set to 'Static IP'. The 'STATIC IP ADDRESS INTERNET CONNECTION TYPE' section includes fields for IP Address (0.0.0.0), Subnet Mask (0.0.0.0), ISP Gateway Address (0.0.0.0), MAC Address (00-00-00-00-00-00) with a 'Clone MAC Address' button, Primary DNS Address, Secondary DNS Address, and MTU (1500). A 'Helpful Hints...' sidebar on the right provides additional guidance.

Internet Setup

Russian PPPoE

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.

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

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

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 **Always-on** (Connect Mode option below).

The screenshot shows the D-Link DIR-330 web interface for Internet Setup. The main heading is "INTERNET CONNECTION". Below this, there is a "Note" stating that PPPoE client software should be removed from computers. There are "Save Settings" and "Don't Save Settings" buttons. The "INTERNET CONNECTION TYPE" section shows "My Internet Connection is:" set to "Russian PPPoE(Dual Access)". The "RUSSIAN PPPoE" section includes radio buttons for "Dynamic PPPoE" (selected) and "Static PPPoE". Fields for "User Name", "Password", "Retype Password", "Service Name (optional)", "IP Address" (0.0.0.0), and "MAC Address" (00-00-00-00-00-00) are present, along with a "Clone MAC Address" button. "Maximum Idle Time" is set to 5 minutes and "MTU" is 1492. The "Connect mode select" options are "Always-on", "Manual", and "Connect-on demand" (selected).

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

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

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

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.

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

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

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

RUSSIAN PPPoE :

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

Dynamic PPPoE Static PPPoE

User Name :

Password :

Retype Password :

Service Name : (optional)

IP Address :

MAC Address : - - - - (optional)

Maximum Idle Time : Minutes

MTU :

Connect mode select : Always-on Manual Connect-on demand

WAN PHYSICAL SETTING :

Dynamic IP Static IP

IP Address :

Subnet Mask :

DNS SETTING :

Primary DNS Address :

Secondary DNS Address : (optional)

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.

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 **Always-on** (Connect Mode option below).

MTU: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. 1450 is the default MTU.

Connect Mode: Click either Always-on, Manual, or Connect-on demand.

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

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

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

Gateway: Enter the Gateway 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).

The screenshot shows the D-Link DIR-330 web interface for Internet Setup. The page is titled "INTERNET CONNECTION" and includes a "Helpful Hints" sidebar. The main content area is divided into several sections:

- INTERNET CONNECTION TYPE :** A dropdown menu is set to "Russian PPTP (Dual Access)".
- RUSSIAN PPTP :** This section contains input fields for "Server IP/Name", "PPTP Account", "PPTP Password", and "PPTP Retype password". It also has a "Maximum Idle Time" field set to 5 minutes and an "MTU" field set to 1450. The "Connect mode select" options are "Always-on", "Manual", and "Connect-on demand", with "Connect-on demand" selected.
- WAN PHYSICAL SETTING :** This section has radio buttons for "Dynamic IP" (selected) and "Static IP". Below are input fields for "IP Address", "Subnet Mask", and "Gateway", all set to 0.0.0.0.
- CLONE MAC SETTING :** This section has a "MAC Address" field with a "Clone MAC Address" button.
- DNS SETTING :** This section has input fields for "Primary DNS Address" and "Secondary DNS Address" (optional).

The sidebar on the right contains "Helpful Hints" regarding the Internet Connection Type and troubleshooting advice for accessing the Internet through the router.

Wireless Settings

Wi-Fi Protected Setup (WPN 2.0)

Enable: Check the box to enable WPS.

Current PIN: WPS uses this PIN (Personal Identification Number) to establish the wireless network. You can generate a new PIN or reset the PIN to its default setting.

Reset to Unconfigured: Click this button if you don't want to further configure the settings of WPS and only need to use one PIN.

Add Wireless Device With WPS: Click this button if you want to add a wireless device with WPS. In the screen that follows, you can enter the wireless device's PIN or click a virtual push button to add a wireless device.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar lists menu items: Internet, Wireless Settings, Network Settings, and VPN Settings. The main content area is titled "WIRELESS NETWORK :" and contains the following text: "Use this section to configure the wireless settings for your D-Link router. Please note that changes made on this section may also need to be duplicated on your wireless client." Below this, it states: "To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2." There are two buttons: "Save Settings" and "Don't Save Settings".

The second section is titled "WI-FI PROTECTED SETUP (ALSO CALLED WPN 2.0 IN WINDOWS VISTA) :". It shows:

- Enable :
- Current PIN : 12345670
- Buttons: "Generate New PIN" and "Reset PIN to Default"
- Wi-Fi Protected Setup Status: Disabled / Configured
- Buttons: "Reset to Unconfigured" and "Add Wireless Device With WPS"

On the right side, there is a "Helpful Hints..." section with the following text: "Wi-Fi Protected Setup provides a more intuitive way of setting up wireless security between the router and the wireless client. Make sure the wireless card supports such feature or uses a certified Windows Vista driver in order to take advantage of this feature." Below this, it says: "Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information." At the bottom right, there is a partially visible link: "Enabling Hidden Mode is".

Wireless Network Settings

Enable Wireless: Check the box to enable the wireless connection. If you do not want to use wireless, uncheck the box to disable the wireless connection.

Wireless Network Name: The name of your wireless network is also called the Service Set Identifier (SSID). Create a name using up to 32 characters. The SSID is case-sensitive.

Wireless Channel: Indicates the channel setting for the router. The channel can be changed to fit the channel setting of an existing wireless network or to customize the wireless network. If you enable Auto Channel Scan, this option will be grayed out.

Enable Auto Channel Selection: The Enable Auto Channel Scan setting can be selected to allow the router to choose the channel with least amount of interference. This feature is enabled by default.

802.11 Mode: Select one of the following:

- **802.11b only** – Select if all of your wireless clients are 802.11b.
- **802.11b/g mixed** – Select if you are using both 802.11b and 802.11g wireless clients.
- **802.11g only** – Select if all of your wireless clients are 802.11g.

Enable Hidden Wireless: Check the box if you do not want the SSID of your wireless network to be broadcasted by the router. If the box is checked, the SSID will not be seen by site survey utilities so your wireless clients must manually enter the SSID to connect to the router.

Wireless Security Mode: Refer to page 62 for more information regarding wireless security.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

Internet
Wireless Settings
Network Settings
VPN Settings

WIRELESS NETWORK :

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

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

Save Settings Don't Save Settings

WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA) :

Enable :

Current PIN : 12345670

Generate New PIN Reset PIN to Default

Wi-Fi Protected Setup Status: Disabled / Configured

Reset to Unconfigured Add Wireless Device With WPS

WIRELESS NETWORK SETTINGS :

Enable Wireless :

Wireless Network Name : dlink (Also called the SSID)

Wireless Channel : 6

Enable Auto Channel Selection :

802.11 Mode : 802.11 b/g mixed

Enable Hidden Wireless : (Also called the SSID Broadcast)

WIRELESS SECURITY MODE :

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

Security Mode : Disable Wireless Security (not recommended)

Helpful Hints..

Wi-Fi Protected Setup provides a more intuitive way of setting up wireless security between the router and the wireless client. Make sure the wireless card supports such feature or uses a certified Windows Vista driver in order to take advantage of this feature.

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

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

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

The DIR-330 only supports mandatory cipher type in

Network Settings

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

Router IP Address: Enter the IP address of the router. The default IP address is 192.168.0.1. If you change the IP address, once you click **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.

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.

D-Link

DIR-330 //

SETUP ADVANCED MAINTENANCE STATUS HELP

Internet
Wireless Settings
Network Settings
VPN Settings

NETWORK SETTINGS :

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

Save Settings Don't Save Settings

ROUTER SETTINGS :

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

Router IP Address : 192.168.0.1
Default Subnet Mask : 255.255.255.0
Local Domain Name :
Enable DNS Relay :

Helpful Hints..

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

In order to ensure that devices on your network are always assigned the same IP address, add a **DHCP Reservation** for each device.

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 DIR-330. 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.

Add DHCP Reservation: Refer to the next page for the DHCP Reservation function.

DHCP SERVER SETTINGS :			
Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.			
Enable DHCP Server :	<input checked="" type="checkbox"/>		
DHCP IP Address Range :	<input type="text" value="100"/>	to	<input type="text" value="150"/> (addresses within the LAN subnet)
DHCP Lease Time :	<input type="text" value="86400"/>	(minutes)	
DYNAMIC DHCP CLIENT LIST :			
Host Name	IP Address	MAC Address	Expired Time
msimaster	192.168.0.106	00:15:e9:46:17:50	Sun Oct 28 18:14:53 2007

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. You may assign up to 50 reservations.

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

Enable: Check this box to enable the reservation.

Computer Name: Enter the computer name.

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.

<< Button: If you want to assign an IP address to the computer you are currently on, select a computer from the last column and click the << button to populate the fields.

Save Settings: Click **Save Settings** to save your entry and activate the reservations.

50 - DHCP RESERVATIONS LIST :

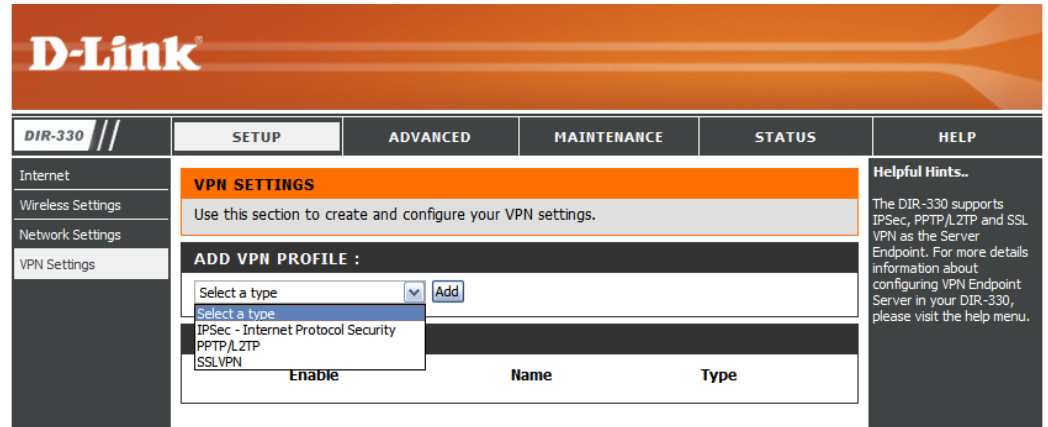
Remaining number of DHCP Reservations that can be configured: 50 [More...](#)

	Computer Name	IP Address	MAC Address	
1. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
2. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
3. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
4. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
5. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
6. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
7. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
8. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
9. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>
10. <input type="checkbox"/>	<input type="text"/>	192. 168. 0. <input type="text"/>	00:00:00:00:00:00	<< Computer Name <input type="button" value="v"/>

VPN Settings

The DIR-330 supports **IPSec**, **PPTP/L2TP**, and **SSL VPN** as the Server Endpoint.

Add VPN Profile: Select **IPSec**, **PPTP/L2TP**, or **SSLVPN** 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 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.

The screenshot shows the D-Link DIR-330 web interface for configuring VPN-IPSEC. The page is titled "VPN - IPSEC" and includes a "Helpful Hints..." section on the right. The main configuration area is titled "IPSEC SETTING :" and contains the following fields and options:

- Enable
- Name :
- Local Net /Mask :
- Remote IP : Remote User Site to Site
- Remote Local LAN Net /Mask :
- Authentication : Pre-shared Key
 X.509 Certificate
 Local Identity
 Certificates
- XAUTH
 Server mode
 Authentication database
- Client mode
 User Name
 Password
- Local ID :
- Remote ID :

The "Helpful Hints..." section on the right provides additional information: "The DIR-330 supports IPSec as the Server Endpoint. IPSec (Internet Protocol Security) is a set of protocols defined by the IETF (Internet Engineering Task Force) to provide IP security at the network layer." It also states: "An IPSec based VPN, such as that of the DIR-330, is made up of two basic parts: - Internet Key Exchange security protocol (IKE) - IPSec protocol (AH/ESP/both). The first part, IKE, is the initial negotiation phase, where the two endpoints agree on which methods will be used to provide security for the underlying IP traffic. Furthermore, IKE is used to manage connections. Each SA is unidirectional, so there will be at least two SA per IPSec connection."

- 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.

PHASE 1 :

Main mode Aggressive mode

NAT-T Enable:

Keep Alive / DPD: none Keep Alive DPD (Dead Peer Detection)

DH Group : 2 - modp 1024-bit ▼

IKE Proposal List :

Cipher	Hash
#1: 3DES ▼	MD5 ▼
#2: 3DES ▼	MD5 ▼
#3: 3DES ▼	MD5 ▼
#4: 3DES ▼	MD5 ▼

IKE Lifetime : 28800 Seconds

PHASE 2 :

PFS Enable: Perfect Forward Secrecy PFS

PFS DH Group : 2 - modp 1024-bit ▼

IPSec Proposal List :

Cipher	Hash
#1: 3DES ▼	MD5 ▼
#2: 3DES ▼	MD5 ▼
#3: 3DES ▼	MD5 ▼
#4: 3DES ▼	MD5 ▼

IPSec Lifetime : 3600 Seconds

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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

Internet
Wireless Settings
Network Settings
VPN Settings

VPN - PPTP/L2TP SERVER
Use this section to configure your VPN-PPTP/L2TP Server settings.
Save Settings Don't Save Settings

PPTP/L2TP SETTING :

Enable setting :

Name :

Connection type : PPTP L2TP L2TP over IPsec

VPN Server IP :

Remote IP range : -

Authentication Protocol : PAP CHAP MSCHAP v2

MPPE Encryption Mode : RC4 None 40 bit 128 bit

Authentication database :

Helpful Hints..
PPTP uses TCP port 1723 for its control connection and uses GRE (IP protocol 47) for the PPP data. PPTP supports data encryption by using MPPE.
L2TP uses UDP to transport the PPP data, this is often encapsulated in IPsec for encryption instead of using MPPE.
For more details information about configuring VPN Endpoint Server in your DIR-330, please visit the support menu.

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

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

VPN - SSLVPN

Use this section to create and configure your SSLVPN setting

Save Settings Don't Save Settings

SSLVPN CERTIFICATE SETTING :

Certificate Select: D-Link Demo [new](#)

SSLVPN SETTING :

Enable SSLVPN :

Name :

User Group : (Using Shift or Ctrl to select multiple options.)

Client Accessible Range : 192.168.0.0/24

Helpful Hints..

Through the use of web browser and the HTTPS or SSL protocol, SSL (Secure Socket Layer) VPN allows you to establish a secure private connection from a remote location over the Internet for access to your personal documents, shares, and other resources configured the Local Network of the router.

Configuring the integrated the SSL VPN server requires the creation of user account or multiple user accounts and groups under the Advanced > User Groups section, using or uploading a certificate and corresponding private key to provide the Local Identity of the router to remote VPN clients.

Port Forwarding

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

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

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

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

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

Schedule: The schedule of time when the Port Forward 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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

Port Forwarding

Application Rules

Network Filter

Website Filter

Firewall Settings

Advanced Wireless

Advanced Network

Routing

Certificates

User Group

Bandwidth Control

PORT FORWARDING RULES :

The Port Forwarding option is used to open a single port or a range of ports through your firewall and redirect data through those ports to a single PC on your network.

Save Settings Don't Save Settings

25 - PORT FORWARDING RULES

	Name	IP Address	Port	Traffic Type	Schedule
1. <input checked="" type="checkbox"/>	MsnMsgr (192.168.0.100) << Application Name	192.168.0.100 << Computer Name	Public Port: 37854 ~ 37854 Private Port: 7775 ~ 7775	UDP	Always
2. <input type="checkbox"/>	<< Application Name	<< Computer Name	Public Port: ~ Private Port: ~	TCP	Always
3. <input type="checkbox"/>	<< Application Name	<< Computer Name	Public Port: ~ Private Port: ~	TCP	Always

Helpful Hints..

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

You can select your computer from the list of DHCP clients in the **Computer Name** drop down menu, or enter the IP address manually of the computer you would like to open the specified port to.

In order to apply a schedule to a Port Forwarding Rule, you must first define a schedule on the **Maintenance>Schedules** page.

This feature allows you to

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-330. 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.

APPLICATION RULES :

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

Save Settings Don't Save Settings

25 - APPLICATION RULES

			Port	Traffic Type	Schedule
1.	<input type="checkbox"/>	<input type="text"/>	Trigger <input type="text"/>	TCP	Always
		<< Application Name	Firewall <input type="text"/>	TCP	
2.	<input type="checkbox"/>	<input type="text"/>	Trigger <input type="text"/>	TCP	Always
		<< Application Name	Firewall <input type="text"/>	TCP	
3.	<input type="checkbox"/>	<input type="text"/>	Trigger <input type="text"/>	TCP	Always
		<< Application Name	Firewall <input type="text"/>	TCP	

Helpful Hints..

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

In order to apply a schedule to an Application Rule, you must first define a schedule on the **Maintenance>Schedules** page.

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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

MAC FILTERING :

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

Save Settings Don't Save Settings

25 - MAC FILTERING RULES

Configure MAC Filtering below:

Turn MAC Filtering OFF

	MAC Address		DHCP Client List	
1.	<input type="text"/>	<<	Computer Name	CLEAR
2.	<input type="text"/>	<<	Computer Name	CLEAR
3.	<input type="text"/>	<<	Computer Name	CLEAR

Helpful Hints..

Create a list of MAC addresses that you would either like to allow or deny access to your network.

Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu and click the arrow to add that device's MAC to the list.

Click the **CLEAR** button to remove the MAC address from the MAC Filtering list.

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.

The screenshot shows the D-Link DIR-330 Advanced Setup page. The 'ADVANCED' tab is selected. The 'WEBSITE FILTERING RULES' section is highlighted in orange. Below this, there is a description: 'The Website Filter option allows you to set-up a list of Websites that the users on your network will either be allowed or denied access to.' There are two buttons: 'Save Settings' and 'Don't Save Settings'. Below this is a section titled '50 - WEBSITE FILTERING RULES'. It contains a dropdown menu set to 'Turn Website Filtering OFF' and a 'Clear the list below...' button. At the bottom, there is a table with columns for 'Website URL/Domain' and 'Website URL/Domain', and rows for '1.', '2.', and '3.'. Each row has a text input field and a dropdown menu set to 'Always'.

Website URL/Domain		Website URL/Domain	
1. <input type="text"/>	Always	26. <input type="text"/>	Always
2. <input type="text"/>	Always	27. <input type="text"/>	Always
3. <input type="text"/>	Always	28. <input type="text"/>	Always

Firewall Settings

DMZ

A firewall protects your network from the outside world. The router 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 chosen 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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

FIREWALL SETTINGS :
The Firewall settings section is an advance feature used to allow or deny traffic from passing through the device. It works in the same way as IP Filters with additional settings. You can create more detailed rules for the device.
Save Settings Don't Save Settings

DMZ HOST :
The DMZ (Demilitarized Zone) option provides you with an option to set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.
Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.
Enable DMZ Host :
DMZ IP Address : 0.0.0.0 << Computer Name >>
Schedule : Always

75 - FIREWALL RULES
Remaining number of firewall rules that can be configured: 75 [More...](#)

Name	Action	Schedule
Default	Allow Deny	Always
1.		
Source	Interface IP Address Range	Protocol
	WAN 0.0.0.0/0	ALL
Dest	Interface IP Address Range	Port Range
	LAN 0.0.0.0/0	0 ~ 65535

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

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.

75 - FIREWALL RULES

Remaining number of firewall rules that can be configured: 75 [More...](#)

1.	<input checked="" type="checkbox"/>	Name	Default	Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny	Schedule	Always
		Source	Interface: WAN	IP Address Range	0.0.0.0/0	Protocol	ALL
		Dest	Interface: LAN	IP Address Range	0.0.0.0/0	Port Range	0 ~ 65535
2.	<input checked="" type="checkbox"/>	Name	Default	Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	Schedule	Always
		Source	Interface: LAN	IP Address Range	0.0.0.0/0	Protocol	ALL
		Dest	Interface: WAN	IP Address Range	0.0.0.0/0	Port Range	0 ~ 65535
3.	<input type="checkbox"/>	Name		Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	Schedule	Always
		Source	Interface: *	IP Address Range		Protocol	TCP
		Dest	Interface: *	IP Address Range		Port Range	~
4.	<input type="checkbox"/>	Name		Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	Schedule	Always
		Source	Interface: *	IP Address Range		Protocol	TCP
		Dest	Interface: *	IP Address Range		Port Range	~

Advanced Wireless Settings

Tx Rate: Select the basic transfer rates based on the speed of wireless adapters on your wireless network. It is strongly recommended to keep this setting to **Auto**.

Beacon Interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of 2436. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

DTIM Interval: A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast and multicast messages. 1 is the default setting.

Preamble Type: Select **Short** or **Long** Preamble. The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless router and the roaming wireless network adapters. Long is the default setting. **Note:** High network traffic areas should use the shorter preamble type.

WMM Function: WMM (Wi-Fi Multimedia) provides QoS (Quality of Service) for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'ADVANCED' tab is active, and the 'Advanced Wireless' sub-tab is selected in the left sidebar. The main content area is titled 'ADVANCED WIRELESS SETTINGS' and contains the following settings:

- TX Rates:** Auto (dropdown menu)
- Beacon interval:** 100 (text input, range: 20~1000, default: 100)
- RTS Threshold:** 2346 (text input, range: 256~2346, default: 2346)
- Fragmentation:** 2346 (text input, range: 1500~2346, default: 2346, even number only)
- DTIM interval:** 1 (text input, range: 1~5, default: 1)
- Preamble Type:** Short Preamble Long Preamble
- WMM Function:** Enable Disable

There are 'Save Settings' and 'Don't Save Settings' buttons at the top of the settings area. A 'Helpful Hints' section on the right side of the page provides additional information: 'It is recommended that you leave these options at their default values. Adjusting them could negatively impact the performance of your wireless network.'

Advanced Network Settings

UPnP: To use the Universal Plug and Play (UPnP™) feature click on the checkbox to enable. UPNP provides compatibility with networking equipment, software and peripherals.

Enable WAN Ping Respond: Unchecking the box will not allow the DIR-330 to respond to pings. Blocking the Ping 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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

ADVANCED NETWORK SETTINGS :
If you are not familiar with these Advanced Network settings, please read the help section before attempting to enable or disable them.
Save Settings Don't Save Settings

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

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

WAN PORT SPEED
WAN Port Speed : Auto 10/100Mbps

Helpful Hints..
For added security, it is recommended that you disable the **WAN Ping Respond** option. Ping is often used by malicious Internet users to locate active networks or PCs.
If you are having trouble receiving multicast streams from the Internet, make sure the Multicast Stream option is enabled.

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.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes 'DIR-330', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'ADVANCED' tab is selected, and the 'ROUTING SETTINGS' page is displayed. The page contains a 'ROUTING SETTINGS' section with a description and 'Save Settings' and 'Don't Save Settings' buttons. Below this is a '50 - STATIC ROUTING RULES' section with a table for defining static routes. The table has 5 rows and 5 columns: Interface, Destination Address, Subnet Mask, Gateway, and Metric. The 'Interface' column has a dropdown menu with 'WAN' selected. To the right of the table is a 'Helpful Hints...' section with instructions on how to use the interface.

	Interface	Destination Address	Subnet Mask	Gateway	Metric
1.	WAN				
2.	WAN				
3.	WAN				
4.	WAN				
5.	WAN				

*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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

Port Forwarding
Application Rules
Network Filter
Website Filter
Firewall Settings
Advanced Wireless
Advanced Network
Routing
Certificates
User Group
Bandwidth Control

CERTIFICATES SETTINGS :

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.

Save Settings Don't Save Settings

CERTIFICATES SETTINGS :

Local Certificate & Private Key Select certificate type

Name :

Private Key : Browse...

Certificate : Browse...

LOCAL IDENTITIES (CERTIFICATES TO WHICH YOU HAVE THE PRIVATE KEY)

Name	Subject	Validity	Issuer
D-Link Demo	C=TW, ST=TP, L=Taipei, O=D-Link, OU=Wireless VPN Router, CN=DIR Model, E=dir330@dlink.com	Mar 21 16:26:02 2008 - Mar 19 16:26:02 2018 Invalid	C=TW, ST=TP, L=Taipei, O=D-Link, OU=Wireless VPN Router, CN=DIR Model, E=dir330@dlink.com

CERTIFICATES OF REMOTE PEERS

Name	Subject	Validity	Issuer
------	---------	----------	--------

CERTIFICATE AUTHORITIES

Name	Subject	Validity	Issuer
------	---------	----------	--------

Helpful Hints..

Select "Local Certificate & Private Key" from the Certificates Settings drop-down menu to configure your local certificates. Enter the Name for the certificate. Click the Browse button to look for the Private Key and the certificate on your computer.

Select "Certificate of Remote Peers" from the Certificates Settings drop-down menu to configure the certificates of remote peers. Enter the Name for the certificate. Click the Browse button to look for the Private Key on your computer.

Select "Certificate Authorities" from the Certificates Settings drop-down menu to configure the CA files to be used with your router. Enter the 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 the User Name.

Password: Enter the Password.

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.

D-Link

DIR-330 //

SETUP **ADVANCED** MAINTENANCE STATUS HELP

Port Forwarding
Application Rules
Network Filter
Website Filter
Firewall Settings
Advanced Wireless
Advanced Network
Routing
Certificates
User Group
Bandwidth Control

BANDWIDTH CONTROL :

This section is used to limited upstream and downstream by LAN IP address.

Save Settings Don't Save Settings

	Name	Application Name	Port Range	Traffic Type
1. <input type="checkbox"/>	<input type="text"/>	<< Application Name	<input type="text"/> ~ <input type="text"/>	TCP
<input type="checkbox"/>	Direction	LAN IP / Net Mask	Rate Range (KBytes/Sec)	
	Upstream	<input type="text"/> <input type="text"/>	<input type="text"/>	
2. <input type="checkbox"/>	<input type="text"/>	<< Application Name	<input type="text"/> ~ <input type="text"/>	TCP
<input type="checkbox"/>	Direction	LAN IP / Net Mask	Rate Range (KBytes/Sec)	
	Upstream	<input type="text"/> <input type="text"/>	<input type="text"/>	
3. <input type="checkbox"/>	<input type="text"/>	<< Application Name	<input type="text"/> ~ <input type="text"/>	TCP
<input type="checkbox"/>	Direction	LAN IP / Net Mask	Rate Range (KBytes/Sec)	
	Upstream	<input type="text"/> <input type="text"/>	<input type="text"/>	

Helpful Hints...
The Bandwidth Control feature allows you allocation the amount of available upstream and downstream bandwidth between the Local Network and the Internet to specific TCP/UDP ports required by specific applications such as FTP, HTTP, SMTP, etc. For more details information about configuring Bandwidth Control in your DIR-330, please visit the support menu.

Administrator Settings

This page will allow you to change the Administrator password. You can also enable Remote Management.

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.

D-Link

DIR-330 //

SETUP ADVANCED MAINTENANCE STATUS HELP

ADMINISTRATOR SETTINGS :

You can access the management interface of router by a pre-defined account "admin", or enable login group and specify your own account of user group to access the interface. Please note that if there are two identical accounts in both SSLVPN and SSL Remote Management Groups, the system will take the SSLVPN one first.

Admin has read/write access.

Save Settings Don't Save Settings

ADMINISTRATOR :

Login name : admin

New Password :

Confirm Password :

Login Group : (Using Shift or Ctrl to select multiple options.)

REMOTE MANAGEMENT :

Enable Remote Management :

IP Address : *

Port : 80 << 80 >> Always

SSL REMOTE MANAGEMENT :

Enable SSL Remote Login : (default 443 port)

Certificate Select: D-Link Demo new

Helpful Hints..

For security reasons, it is recommended that you change the Login Name and Password for the Administrator account. Be sure to write down the new Login Name and Password to avoid having to reset the router in the event that they are forgotten.

When enabling Remote Management, you can specify the IP address of the computer on the Internet that you want to have access to your router, or you can enter an asterisk (*) to allow access to any computer on the Internet.

Administrator Settings

This page will allow you to change the Administrator password. You can also enable Remote Management.

Enable Remote Management: Remote management allows the router to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

IP Address: Enter the IP address of the remote computer. You may enter * to allow a connection from any Internet address.

Port: The port number used to access the DIR-330. Example: `http://x.x.x.x:8080` whereas `x.x.x.x` is the Internet IP address of the DIR-330 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.

REMOTE MANAGEMENT :

Enable Remote Management :

IP Address : *

Port : 80 << 80 >> Always >>

SSL REMOTE MANAGEMENT :

Enable SSL Remote Login : (default 443 port)

Certificate Select: D-Link Demo >> [new](#)

Time and Date Settings

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 configured 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**.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes 'DIR-330', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar lists 'Admin Setup', 'Time And Date', 'System', 'Firmware', 'Dynamic DNS', 'System Check', 'Schedules', and 'Log Settings'. The main content area is titled 'TIME AND DATE : Time Configuration' and contains the following sections:

- Time Configuration:** A text block explaining the purpose of the section, followed by 'Save Settings' and 'Don't Save Settings' buttons.
- TIME CONFIGURATION :** A section showing the current time as 'Tuesday, January 01, 2002 12:10:47 AM', a dropdown menu for 'Time Zone' set to '(GMT-08:00) Pacific Time (US & Canada); Tijuana', and an 'Enable Daylight Saving' checkbox with a 'Sync. your computer's time settings' button.
- AUTOMATIC TIME AND DATE CONFIGURATION :** A section with an unchecked checkbox for 'Automatically synchronize with D-Link's Internet time server' and an 'NTP Server Used' dropdown set to 'ntp1.dlink.com' with an 'Update Now' button.
- SET THE DATE AND TIME MANUALLY :** A section with input fields for Year (2002), Month (Jan), Day (1), Hour (00), Minute (10), and Second (39).

On the right side of the interface, there is a 'Helpful Hints..' section with text: 'If you plan on using the scheduling feature of this router, then making sure the time is correct is extremely important. Either enter the time manually by clicking the Sync. your computer's time settings button, or use the Automatic Time and Date Configuration option to have your router synchronize with a time server on the Internet.'

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-330: Click to reboot the router.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE (selected), STATUS, and HELP. The left sidebar lists menu items: Admin Setup, Time And Date, System, Firmware, Dynamic DNS, System Check, Schedules, and Log Settings. The main content area is titled "SYSTEM SETTINGS" and contains the following text and buttons:

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

SYSTEM SETTINGS :

- Save Settings To Local Hard Drive :
- Load Settings From Local Hard Drive :
- Restore To Factory Default Settings :
- Reboots the DIR-330 :

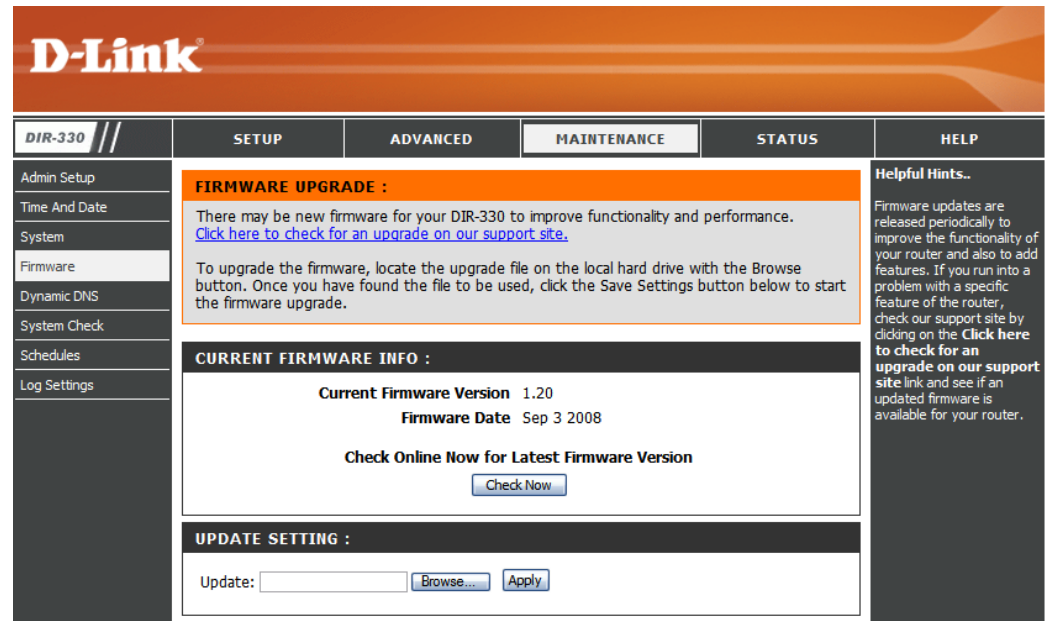
On the right side, there is a "Helpful Hints.." section with the following text:

Once your router is configured the way you want it, you can save these settings to a configuration file that can later be loaded in the event that the router's default settings are restored. To do this, click the **Save** button next to where it says Save Settings to Local Hard Drive.

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 **Save Settings** to complete the firmware upgrade.



The screenshot displays the D-Link DIR-330 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar lists various configuration options, with 'Firmware' selected. The main content area is titled 'FIRMWARE UPGRADE' and contains the following information:

- FIRMWARE UPGRADE :** There may be new firmware for your DIR-330 to improve functionality and performance. [Click here to check for an upgrade on our support site.](#)
- To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Save Settings button below to start the firmware upgrade.
- CURRENT FIRMWARE INFO :**
 - Current Firmware Version 1.20
 - Firmware Date Sep 3 2008
 - Check Online Now for Latest Firmware Version
 -
- UPDATE SETTING :**
 - Update:

On the right side, there is a 'Helpful Hints..' section with text: 'Firmware updates are released periodically to improve the functionality of your router and also to add features. If you run into a problem with a specific feature of the router, check our support site by clicking on the [Click here to check for an upgrade on our support site](#) link and see if an updated firmware is available for your router.'

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.

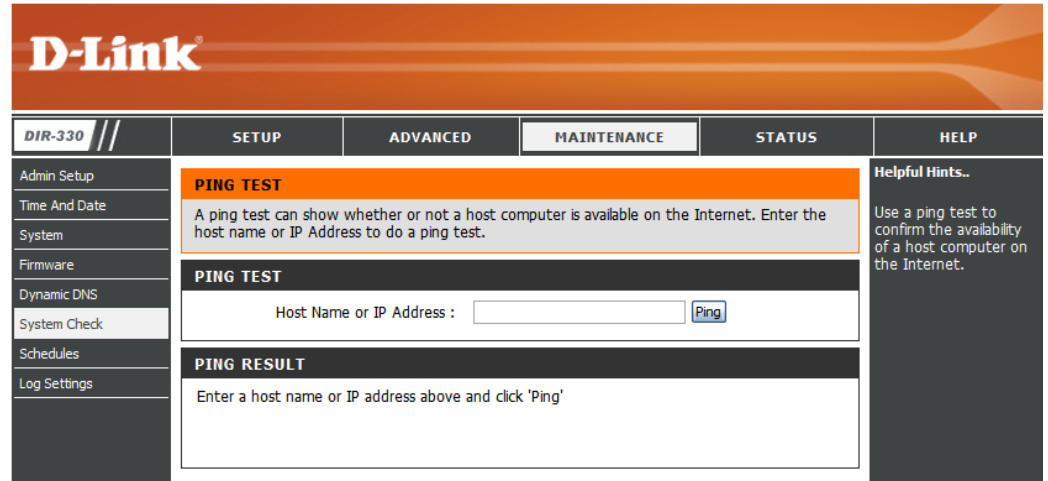
The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes 'DIR-330 //', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar lists menu items: Admin Setup, Time And Date, System, Firmware, Dynamic DNS (selected), System Check, Schedules, and Log Settings. The main content area is titled 'DYNAMIC DNS' and contains the following text: 'Dynamic DNS (Domain Name Service) is a method of keeping a domain name linked to a dynamic IP address. With most Cable and DSL connections, you are assigned a dynamic IP address and that address is used only for the duration of that specific connection. With the DIR-330, you can setup your DDNS service and the DIR-330 will automatically update your DDNS server every time it receives a new WAN IP address.' Below this text are 'Save Settings' and 'Don't Save Settings' buttons. The 'DDNS SETTINGS' section includes: 'Enable Dynamic DNS' (checkbox), 'Server Address' (text input with a '<<' button and a 'Select Dynamic DNS Server' dropdown), 'Host Name' (text input), 'Username or Key' (text input), 'Password or Key' (password input), 'Verify Password or Key' (password input), 'Timeout' (240 hours), and 'Status' (Disconnected). The right sidebar contains 'Helpful Hints..' text: 'In order to use this feature you must first have a DDNS account from one of the providers in the drop down menu.'

System Check

The router System Check uses a ping test to send ping packets to test if a computer is 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.



D-Link

DIR-330 //

SETUP ADVANCED MAINTENANCE STATUS HELP

Admin Setup
Time And Date
System
Firmware
Dynamic DNS
System Check
Schedules
Log Settings

PING TEST

A ping test can show whether or not a host computer is available on the Internet. Enter the host name or IP Address to do a ping test.

PING TEST

Host Name or IP Address :

PING RESULT

Enter a host name or IP address above and click 'Ping'

Helpful Hints..

Use a ping test to confirm the availability of a host computer on the Internet.

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.

D-Link

DIR-330 //

SETUP ADVANCED MAINTENANCE STATUS HELP

SCHEDULES :

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

Save Settings Don't Save Settings

ADD SCHEDULE RULE :

Name :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed Thu Fri Sat

All Day - 24 hrs :

Start Time : : AM (hour:minute, 12 hour time)

End Time : : AM (hour:minute, 12 hour time)

Save Clear

SCHEDULE RULES LIST :

Name :	Day(s) :	Time Frame :

Helpful Hints..

After a schedule rule is defined, it can then be applied to the features of the router that support scheduling. These features include port forwarding, firewall rules, web filtering and remote management. Click on the Advanced menu item to configure these features.

Log Settings

The DIR-330 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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

LOG SETTINGS :
Logs can be saved by sending it to an admin email address.
Save Settings Don't Save Settings

EMAIL SETTING :

From Email Address

To Email Address Send Mail Now

SMTP Server / IP Address

Enable Authentication

Account Name

Password

Verify Password

LOG FILES :

Save Log File To Local Hard Drive

Log Type System Activity
 Debug Information
 Attacks
 Dropped Packets
 Notice

Helpful Hints..
If you would like to have the router's logs emailed to you but are unsure of what to enter in the **SMTP Server/IP Address** field, please contact ISP.
Some SMTP server need to authentication using user account name, password, and sender email. Please sure the email information is correct. If SMTP server disallow anyone email information, email may not send to receiver.
You must click 'Save Settings' to save these settings before you click 'Send Mail Now', otherwise the information is old.

Device Information

This page displays the current information for the router. 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.

Wireless: Displays the SSID, Channel, and Encryption information of your wireless network.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar lists various configuration options: Device Info, Log, Statistics, Active Session, Wireless Clients, LAN Clients, Routing, and VPN. The main content area is titled "DEVICE INFORMATION" and contains the following details:

DEVICE INFORMATION :
All of your Internet and network connection details are displayed on this page. The firmware version is listed below.
Firmware Version: 1.20

LAN :
MAC Address : 00:1E:58:39:1A:BD
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WAN :
MAC Address : 00:1E:58:39:1A:BE
Connection : DHCP Client Connecting
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS :
Buttons:

WIRELESS :
SSID : dlink
Channel : 6
Encryption : Disabled

Helpful Hints..
All of your Internet and network connection details are displayed on the Device Info page. The firmware version is also displayed here.

Log

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

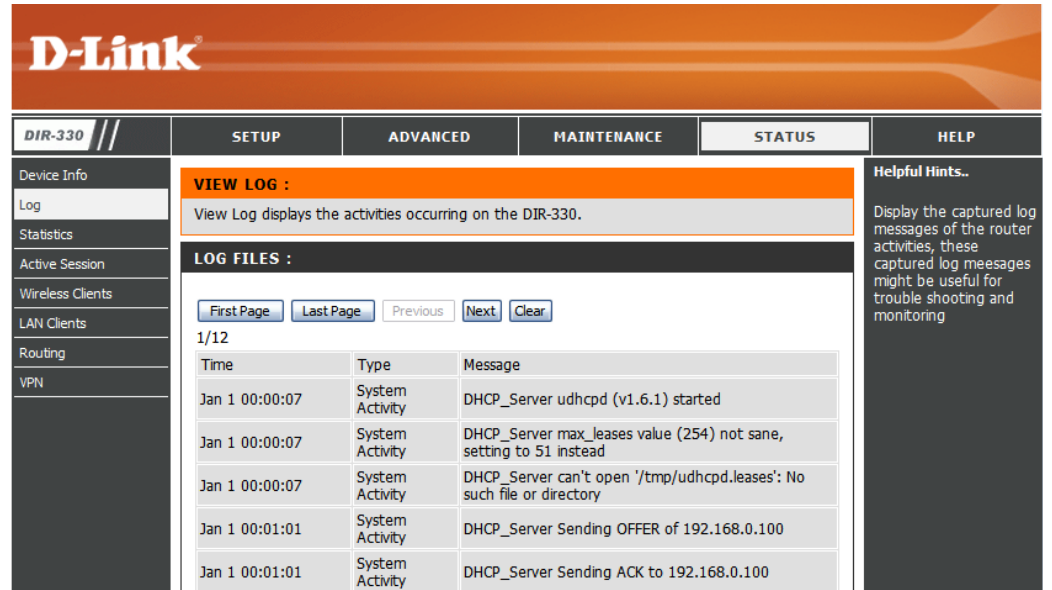
First Page: This button will direct you to the current first page of the log.

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.



D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

Device Info
Log
Statistics
Active Session
Wireless Clients
LAN Clients
Routing
VPN

VIEW LOG :
View Log displays the activities occurring on the DIR-330.

LOG FILES :
First Page Last Page Previous Next Clear

1/12

Time	Type	Message
Jan 1 00:00:07	System Activity	DHCP_Server udhcpd (v1.6.1) started
Jan 1 00:00:07	System Activity	DHCP_Server max_leases value (254) not sane, setting to 51 instead
Jan 1 00:00:07	System Activity	DHCP_Server can't open '/tmp/udhcpd.leases': No such file or directory
Jan 1 00:01:01	System Activity	DHCP_Server Sending OFFER of 192.168.0.100
Jan 1 00:01:01	System Activity	DHCP_Server Sending ACK to 192.168.0.100

Helpful Hints..
Display the captured log messages of the router activities, these captured log messages might be useful for trouble shooting and monitoring

Statistics

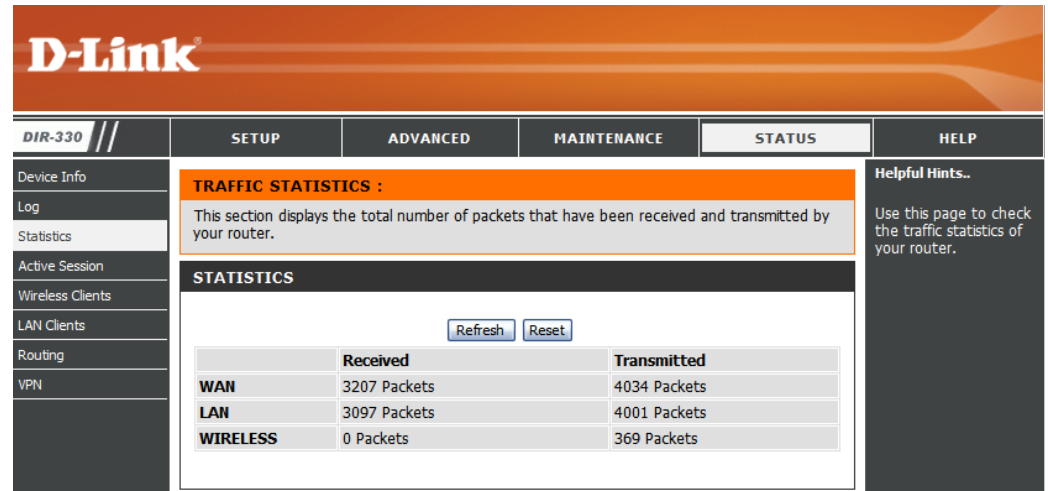
This page displays the current statistics of the router. Here you can view the amount of packets that pass through the router.

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.



The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar lists various system information sections. The main content area is titled 'TRAFFIC STATISTICS' and contains a table of statistics. The table has three columns: Interface, Received, and Transmitted. The data is as follows:

	Received	Transmitted
WAN	3207 Packets	4034 Packets
LAN	3097 Packets	4001 Packets
WIRELESS	0 Packets	369 Packets

Buttons for 'Refresh' and 'Reset' are located above the table. A 'Helpful Hints..' section on the right side of the page provides instructions on how to use the statistics page.

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.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar contains a menu with options: Device Info, Log, Statistics, Active Session (highlighted), Wireless Clients, LAN Clients, Routing, and VPN. The main content area is titled "ACTIVE SESSION LIST" and contains a descriptive text box: "This section displays a list of the sessions that are active on your router. The protocol, source address and destination address are listed for each session." Below this is a table with the following data:

Protocol	Source	Destination
UDP	192.168.0.1:54961	192.168.0.1:53
UDP	192.168.0.1:59623	192.168.0.1:53
UDP	192.168.0.1:60392	192.168.0.1:53

Navigation buttons include First Page, Last Page, Previous, Next, and Refresh. A "Helpful Hints.." section on the right side of the interface provides instructions: "Use this page to monitor the sessions that are active on your router."

Wireless Clients

This page displays a list of current connected wireless clients. This page also displays the connection time and MAC address of the connected wireless clients

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

Device Info
Log
Statistics
Active Session
Wireless Clients
LAN Clients
Routing
VPN

CONNECTED WIRELESS CLIENT LIST

The Wireless Client table below displays Wireless clients connected to the AP (Access Point).

WIRELESS CLIENTS

IP Address	Hostname	MAC Address	Connected Time	Idle Time
------------	----------	-------------	----------------	-----------

Helpful Hints..
Displays the current wireless clients connected to the AP (Access Point).

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.

D-Link

DIR-330 // SETUP ADVANCED MAINTENANCE STATUS HELP

Device Info
Log
Statistics
Active Session
Wireless Clients
LAN Clients
Routing
VPN

LAN CLIENTS LIST

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

LAN CLIENTS

IP Address	Name	MAC Address
192.168.0.100	06955PCWINXP2	00:19:b9:43:71:1e

Helpful Hints..
Displays the current wired clients connected to the router.

Routing

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

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes the D-Link logo and the model number DIR-330. Below this is a menu with tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar contains a list of navigation options: Device Info, Log, Statistics, Active Session, Wireless Clients, LAN Clients, Routing (highlighted), and VPN. The main content area is titled "ROUTING :" and contains the text: "This section displays a list of the default and static routes used by your router." Below this text is a table with the following headers: Destination, Gateway, Subnet Mask, Metric, and Interface. To the right of the main content area is a "Helpful Hints.." section with the text: "Use this page to check for detailed information regarding default and static routes."

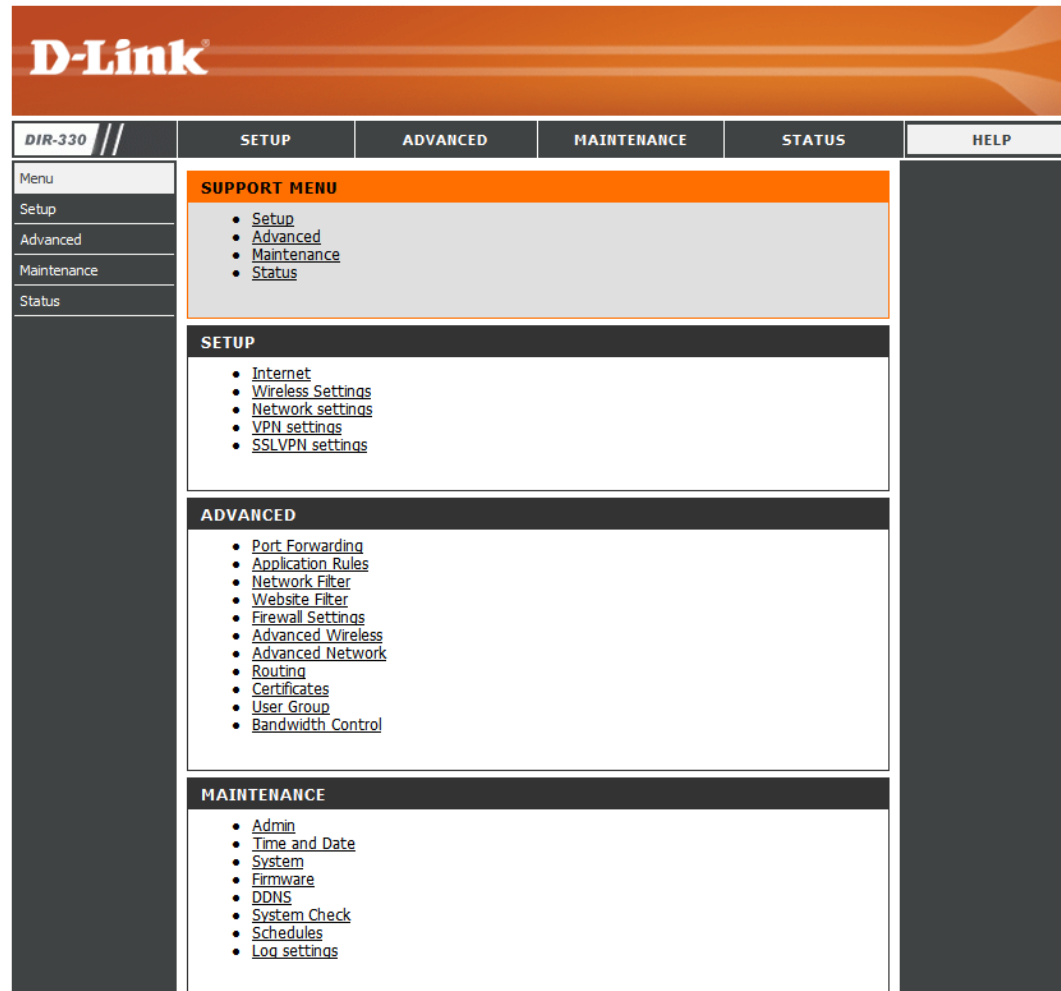
VPN

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

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes the D-Link logo and the model number DIR-330. Below this is a menu with tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar contains a list of navigation options: Device Info, Log, Statistics, Active Session, Wireless Clients, LAN Clients, Routing, and VPN (highlighted). The main content area is titled "CONNECTED VPN TUNNEL LIST" and contains the text: "The VPN List below displays current VPN information." Below this text is a table with the following headers: Type, Local Information, Remote Information, and Other. To the right of the main content area is a "Helpful Hints.." section with the text: "This page displays current established VPN tunnels."

Help

The support menu provides additional information regarding features included in the DIR-330 Web Management Interface.



The screenshot displays the D-Link DIR-330 Web Management Interface. At the top, the D-Link logo is visible on an orange background. Below the logo is a navigation bar with tabs for **DIR-330**, **SETUP**, **ADVANCED**, **MAINTENANCE**, **STATUS**, and **HELP**. The **HELP** tab is currently selected. On the left side, there is a vertical menu with options: **Menu**, **Setup**, **Advanced**, **Maintenance**, and **Status**. The main content area is titled **SUPPORT MENU** and contains three sections:

- SUPPORT MENU**
 - [Setup](#)
 - [Advanced](#)
 - [Maintenance](#)
 - [Status](#)
- SETUP**
 - [Internet](#)
 - [Wireless Settings](#)
 - [Network settings](#)
 - [VPN settings](#)
 - [SSLVPN settings](#)
- ADVANCED**
 - [Port Forwarding](#)
 - [Application Rules](#)
 - [Network Filter](#)
 - [Website Filter](#)
 - [Firewall Settings](#)
 - [Advanced Wireless](#)
 - [Advanced Network](#)
 - [Routing](#)
 - [Certificates](#)
 - [User Group](#)
 - [Bandwidth Control](#)
- MAINTENANCE**
 - [Admin](#)
 - [Time and Date](#)
 - [System](#)
 - [Firmware](#)
 - [DDNS](#)
 - [System Check](#)
 - [Schedules](#)
 - [Log settings](#)

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-330 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WEP?

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

What is WPA?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

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

Wireless Security Setup Wizard

To run the security wizard, click on **Setup** at the top and then click **Launch Wireless Security Setup Wizard**.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar shows a menu with Internet, Wireless Settings, Network Settings, and VPN Settings. The main content area is titled "WIRELESS CONNECTION :" and contains the following text:

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

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

WIRELESS CONNECTION SETUP WIZARD :

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

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

MANUAL WIRELESS CONNECTION OPTIONS :

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

On the right side, there is a "Helpful Hints.." section with the following text:

If you are new to wireless networking and have never configured a wireless router before, click on **Wireless Connection Setup Wizard** and the router will guide you through a few simple steps to get your wireless network up and running.

If you consider yourself an advanced user and have configured a wireless router before, click **Manual Wireless Connection Setup** to input all the settings manually.

Click **Next** to continue.

The screenshot shows the "WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD" screen. The text reads:

This wizard will guide you through a step-by-step process to setup your wireless network and make it secure.

- Step 1: Name your Wireless Network
- Step 2: Secure your Wireless Network
- Step 3: Set your Wireless Security Password

At the bottom, there are two buttons: and .

Enter the SSID (Service Set Identifier). The SSID is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

Click **Next** to continue.

Select the level of security for your wireless network:

- **Best** – WPA2 Authentication
- **Better** – WPA Authentication
- **Good** – WEP 128-bit Authentication
- **None** – No Security

Click **Next** to continue.

If you selected Best or Better, enter a password between 8-63 characters.

Click **Next** to continue.

STEP 1: NAME YOUR WIRELESS NETWORK

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name of [dlink].

Wireless Network Name (SSID)

STEP 2: SECURE YOUR WIRELESS NETWORK

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

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are three levels of wireless security - Good Security, Better Security or Best Security. The level you choose depends on the security features your wireless adapters support.

BEST Select this option if your wireless adapters SUPPORT WPA2

BETTER Select this option if your wireless adapters SUPPORT WPA

GOOD Select this option if your wireless adapters DO NOT SUPPORT WPA

NONE Select this option if you do not want to activate any security features

For information on which security features your wireless adapters support, please refer to the adapters' documentation.

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

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password :

(8~63 ASCII or 64 HEX)

You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

If you selected Good, enter a WEP encryption key (13 characters or 26 Hex (A-F, 0-9) characters).

Click **Next** to continue.



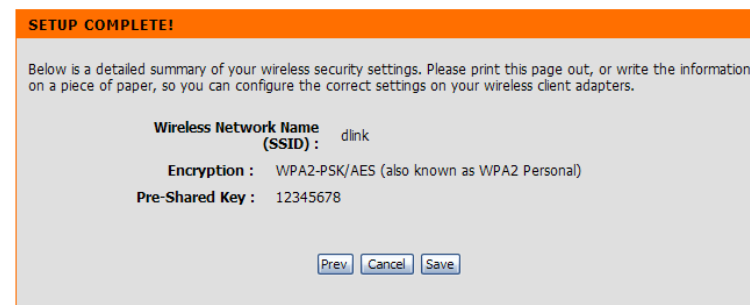
If you did not enable encryption, the following screen will appear.

Click **Save** to finish the Security Wizard.



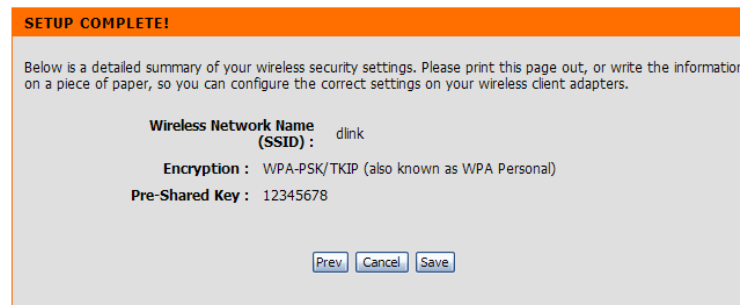
If you selected Best, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

Click **Save** to finish the Security Wizard.



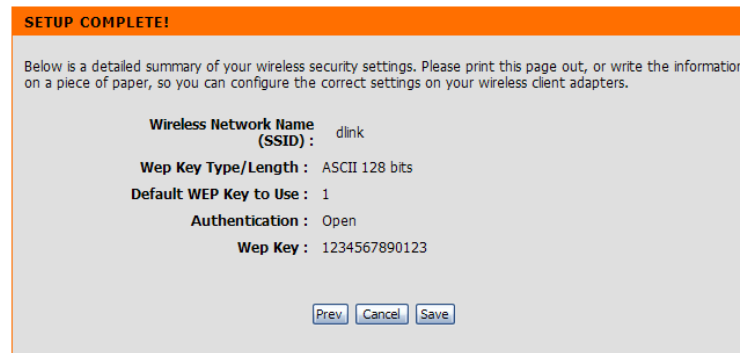
If you selected Better, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

Click **Save** to finish the Security Wizard.



If you selected Good, the following screen will show you your WEP Key to enter on your wireless clients.

Click **Save** to finish the Security Wizard.



Configure WEP

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Click the **Manual Wireless Connection Setup** button.
3. Next to Security Mode, select **Enable WEP**.
4. Next to Authentication, select **Shared Key** or **Open**.
5. Next to WEP Encryption, select the level of encryption (64 or 128-bit).
6. Next to Default WEP Key, select the key to modify. You may enter up to 4 different keys.
7. Next to WEP Key, enter a WEP key you create. Make sure you enter this key exactly on all your wireless devices.
8. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.

WIRELESS SECURITY MODE :

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

Security Mode :

WEP :

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

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

Authentication :

WEP Encryption :

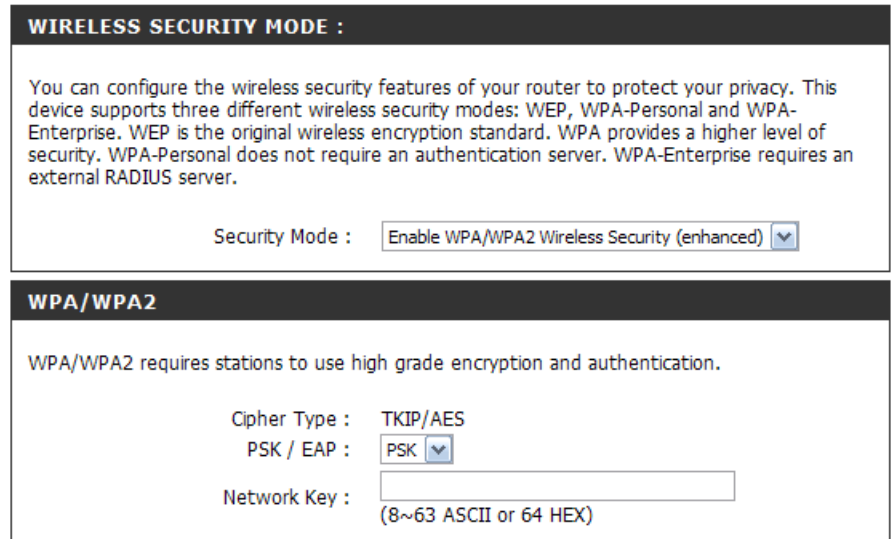
Default WEP Key :

WEP Key : (5 ASCII or 10 HEX)

Configure WPA/WPA2-PSK

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead. The configuration of WPA, WPA2, and WPA/WPA2 uses the same options.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Click the **Manual Wireless Connection Setup** button.
3. Next to Security Mode, select **Enable WPA, Enable WPA2, or Enable WPA/WPA2**.
4. Next to PSK/EAP, select **PSK**.
5. Next to Network Key, enter a passphrase.. The passphrase must be between 8-63 characters. This passphrase must be entered on your wireless clients to connect.
6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable encryption on your adapter and enter the same passphrase as you did on the router.



WIRELESS SECURITY MODE :

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

Security Mode :

WPA/WPA2

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

Cipher Type : TKIP/AES
PSK / EAP :
Network Key :
(8~63 ASCII or 64 HEX)

Configure WPA/WPA2-EAP (RADIUS)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Click the **Manual Wireless Connection Setup** button.
3. Next to Security Mode, select **Enable WPA**, **Enable WPA2**, or **Enable WPA/WPA2**.
4. Next to PSK/EAP, select **EAP**.
5. Next to RADIUS Server IP Address enter the IP Address of your RADIUS server.
6. Next to RADIUS Server Port, enter the port you are using with your RADIUS server. 1812 is the default port.
7. Next to RADIUS Server Shared Secret, enter the security key.
8. Click **Save Settings** to save your settings.

WIRELESS SECURITY MODE :

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

Security Mode :

WPA/WPA2

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

Cipher Type : TKIP/AES
PSK / EAP :

802.1X

RADIUS Server IP Address :

RADIUS Server Port :

RADIUS Server Shared Secret :

Connect to a Wireless Network Using Windows Vista™

Windows Vista™ users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista™ utility as seen below.

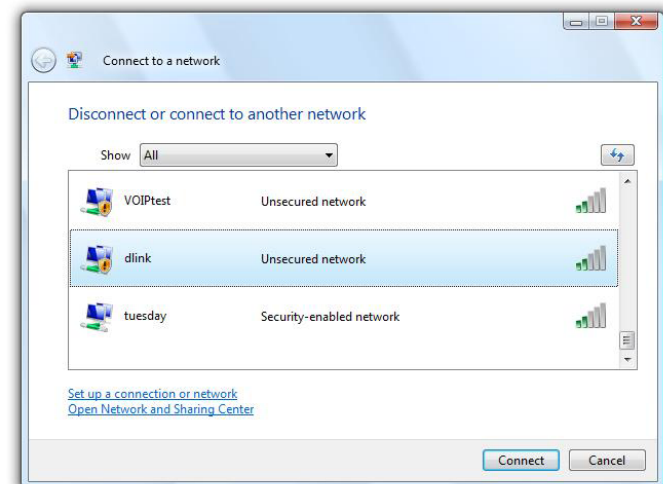
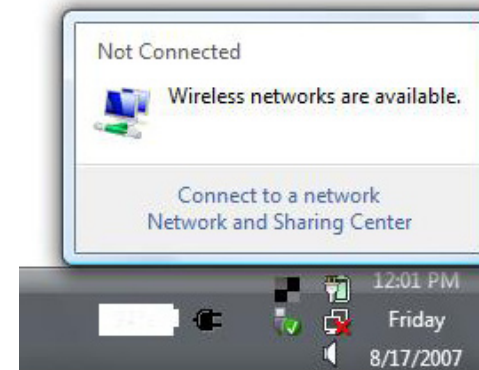
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

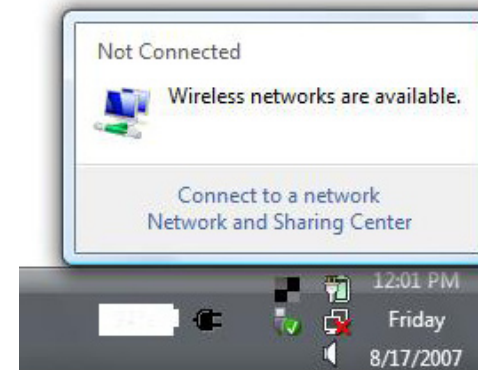
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



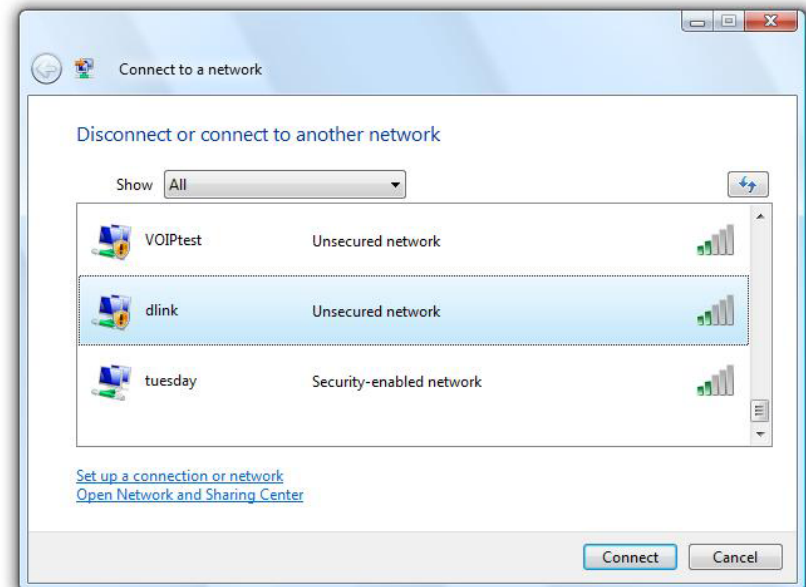
Configure WEP/WPA/WPA2

It is recommended to enable wireless security (WEP/WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista™ Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

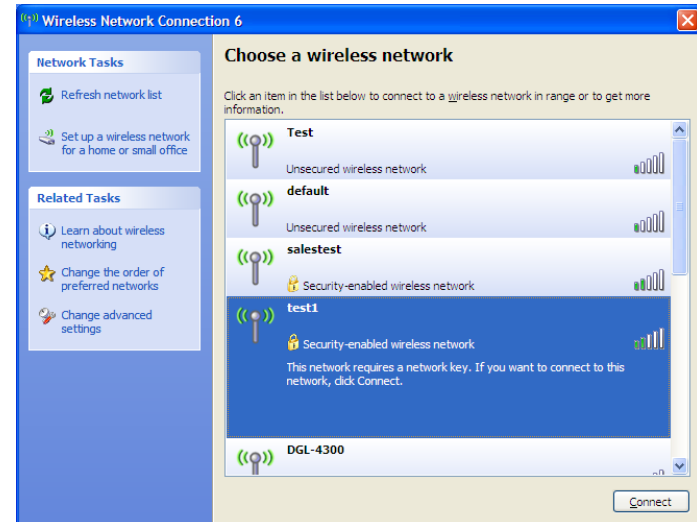
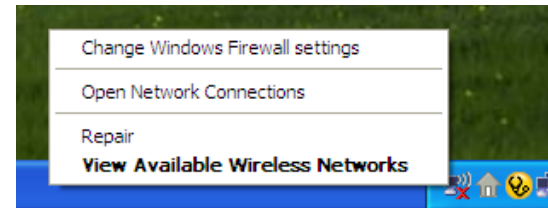
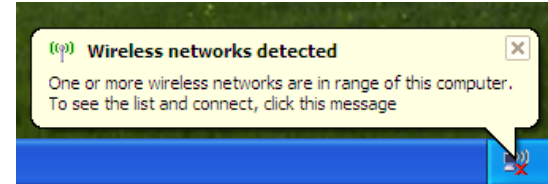
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

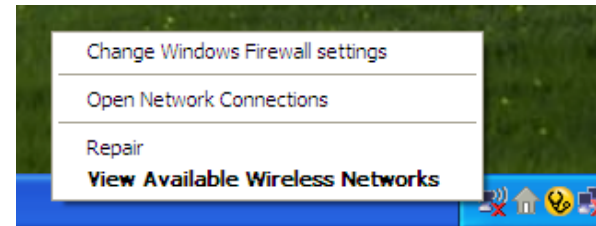
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



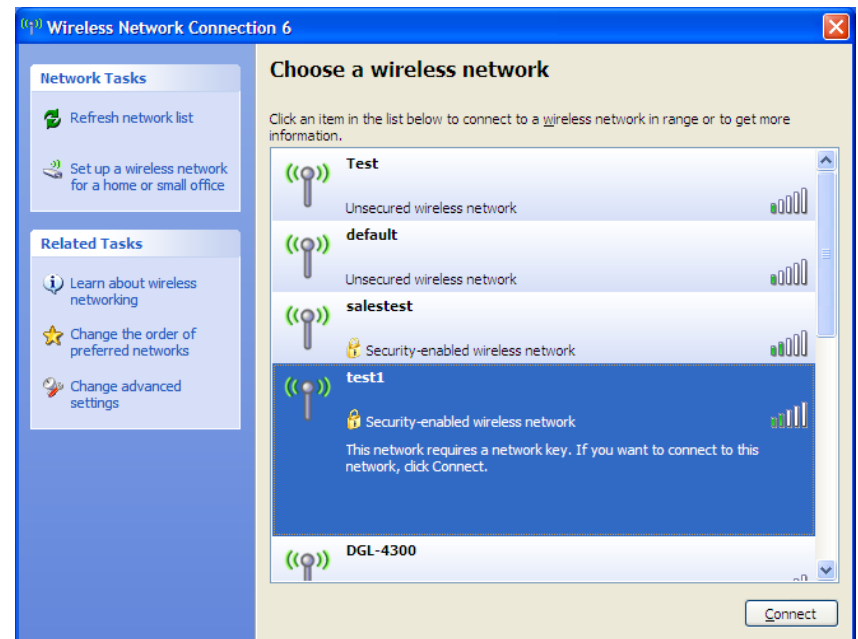
Configure WEP

It is recommended to enable WEP on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.

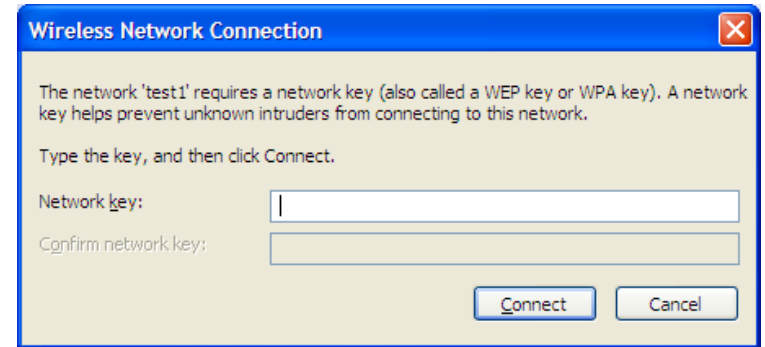


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the same WEP key that is on your router and click **Connect**.

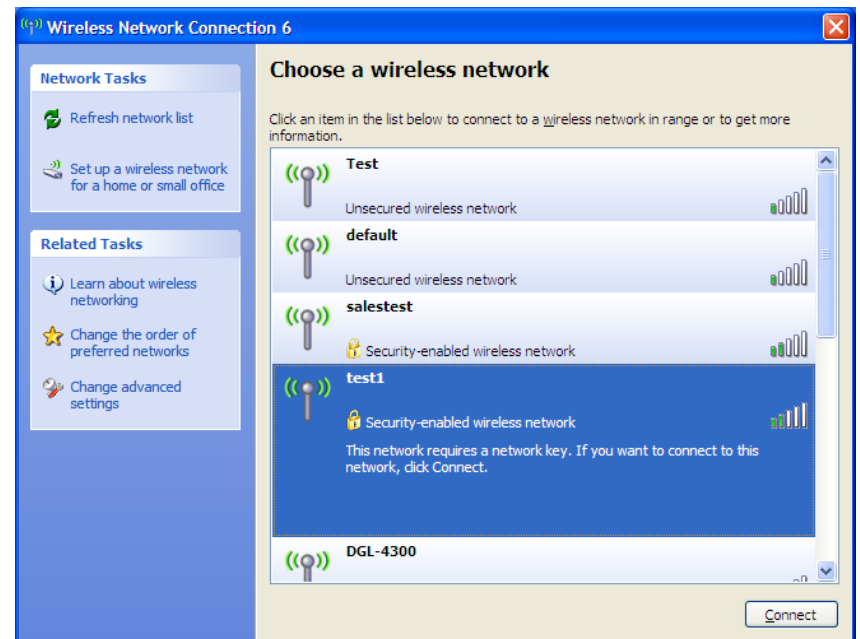
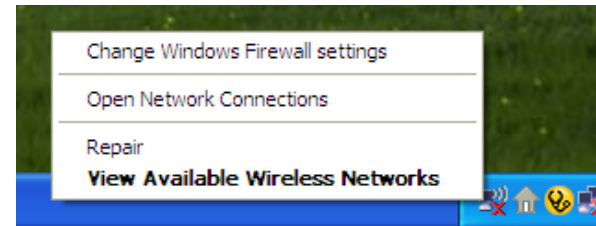
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



Configure WPA-PSK

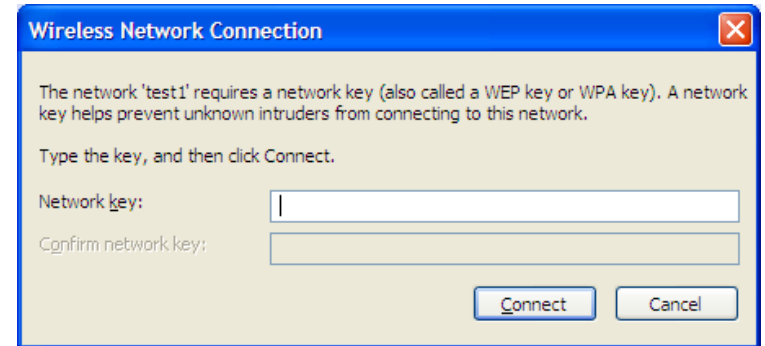
It is recommended to enable WEP on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.



Troubleshooting

This section provides solutions to problems that can occur during the installation and operation of the DIR-330. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP and Vista™. If you have a different operating system, the screenshots on your computer may 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® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your 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 91.

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

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 email. 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.

Wireless Basics

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

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, and etc
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let your next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-330 wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

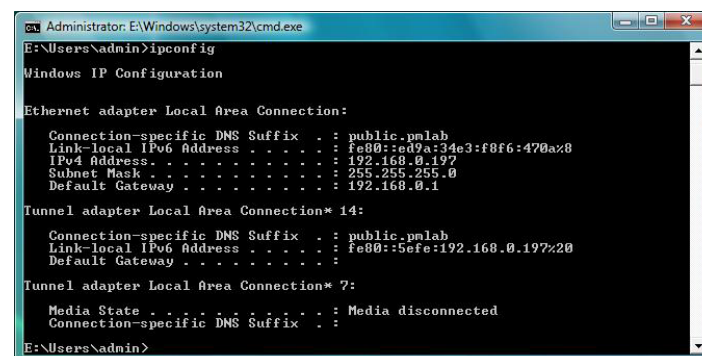
Networking Basics

Check your IP address

After you install your new D-Link adapter 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.



```
Administrator: E:\Windows\system32\cmd.exe
E:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : public.pmlab
    Link-local IPv6 Address . . . . . : fe80::ed9a:3463:f8f6:470az8
    IPv4 Address. . . . . : 192.168.0.197
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter Local Area Connection* 14:

    Connection-specific DNS Suffix  . : public.pmlab
    Link-local IPv6 Address . . . . . : fe80::5efe:192.168.0.197%20
    Default Gateway . . . . . :

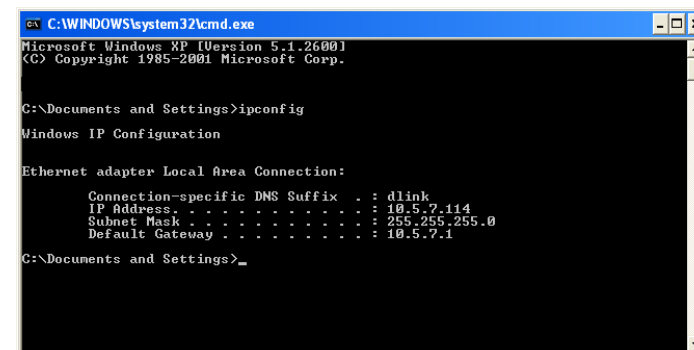
Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

E:\Users\admin>
```

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.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . . : 10.5.7.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>
```

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

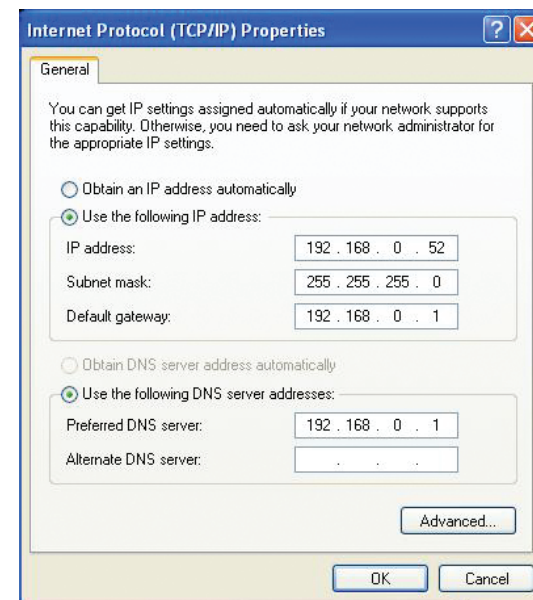
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

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.

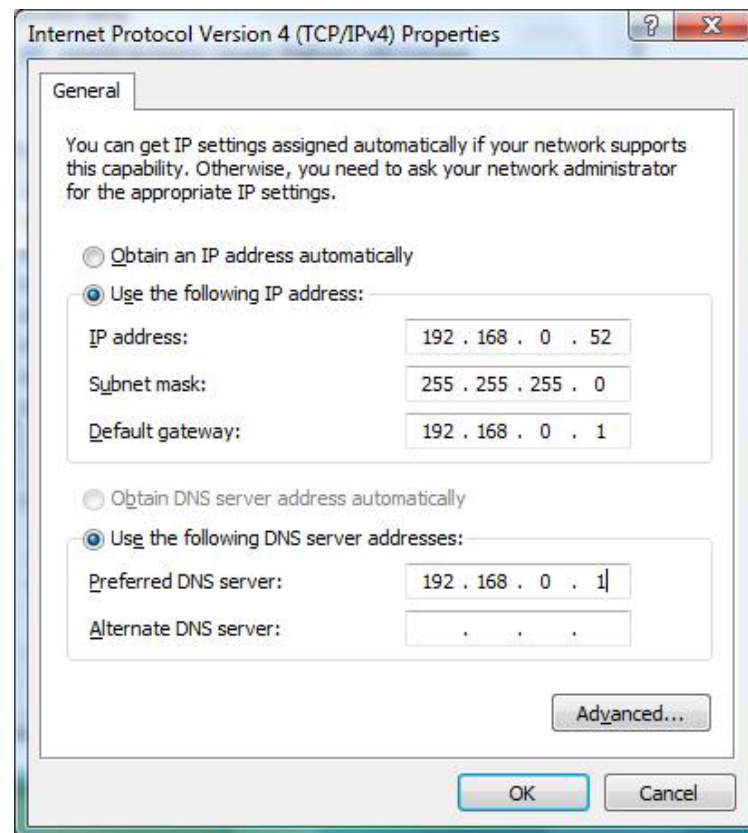


Windows Vista™ Users

- 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 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Security

- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise
- 64/128-bit WEP

Wireless Signal Rates*

- 54Mbps
- 48Mbps
- 36Mbps
- 24Mbps
- 18Mbps
- 12Mbps
- 11Mbps
- 9Mbps
- 6Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

Frequency Range

- 2.4GHz to 2.483GHz

Transmitter Output Power

- 16dBm \pm 2dB (max.)

External Antenna Type

- Two (2) detachable reverse SMA Antennas

LEDs

- Power
- WAN
- Status
- WLAN
- LAN (10/100)

Operating Temperature

- 32°F to 104°F (0°C to 40°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- CE
- IC

Dimensions

- L = 7.6 inches
- W = 4.6 inches
- H = 1.2inches

Warranty

- 1 Year

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

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 and wireless 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
Wireless Broadcast	Enabled
SSID	dlink
WEP / WPA / WPA2	Disabled
Wireless Channel	6

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-330)
- 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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

IC statement

Operation is subject to the following two conditions:

- 1) This device may not cause interference and
- 2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

- 1) Ce périphérique ne doit pas causer d'interférence et.
- 2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

The Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.

Cet appareil numérique de la class [B] respecte toutes les exigences du Règlement sur le matériel brouilleur 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 what 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 15, 2008