

USER MANUAL

DIR-330

VERSION 1.0



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.

Section 2 - “Installation” describes how to install the router on your network.

Section 3 - “Configuration” describes how to configure the settings on your DIR-330 router.

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

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

Section 6 - “Troubleshooting” explains how to resolve common issues.

Section 7 - “Appendix” contains wireless and networking basics, technical specifications, technical support information, warranty, GNU general public license, and registration information.

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	Jan. 15, 2007	DIR-330 rev. A1 with firmware 1.00.

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 © 2007 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	Wireless Settings	21
Manual Revisions	ii	Network Settings.....	22
Trademarks.....	ii	DHCP Server Settings	23
Product Overview	1	DHCP Reservation	24
Package Contents.....	1	VPN Settings	25
System Requirements	1	IPSec Settings.....	26
Features.....	2	PPTP/L2TP Settings	27
Hardware Overview	3	Virtual Server	28
Connections.....	3	Port Forwarding	30
LEDs	4	Application Rules	31
Installation.....	5	Network Filters.....	32
Before you Begin	5	Website Filters	33
Wireless Installation Considerations.....	6	Firewall Settings.....	34
Connect to Cable/DSL/Satellite Modem	7	DMZ	34
Connect to Another Router.....	8	VPN Passthrough.....	34
Configuration	10	Advanced Wireless Settings	35
Web-based Configuration Utility	10	Tx Rate.....	35
Setup Wizard	11	Preamble	35
Manual Configuration.....	15	WMM Function	35
Dynamic (Cable).....	15	Advanced Network Settings.....	36
PPPoE (DSL)	16	UPnP.....	36
PPTP	17	WAN Ping Respond	36
L2TP.....	18	WAN Port Speed	36
Big Pond.....	19	Administrator Settings.....	37
Static (assigned by ISP).....	20	Change Password	37
		Remote Management.....	37
		Time Settings.....	38

System Settings	39	Wireless Basics	67
Update Firmware	40	What is Wireless?	68
DDNS.....	41	Tips.....	70
System Check.....	42	Wireless Modes	71
Schedules	43	Networking Basics	72
Log Settings.....	44	Check your IP address	72
Device Information	45	Statically Assign an IP address	73
Log	46	Technical Specifications	74
Stats.....	47	Default Factory Settings	75
Wireless Computers	47	Contacting Technical Support.....	76
LAN Computers	48	Warranty	77
VPN	48	GNU/Linux GPL.....	83
Support	49	GNU General Public License	84
Wireless Security.....	50	Registration.....	90
What is WEP?.....	50		
What is WPA?	51		
Wireless Security Setup Wizard	52		
Configure WEP	55		
Configure WPA-Personal (PSK).....	56		
Configure WPA-Enterprise (RADIUS).....	57		
Connect to a Wireless Network	58		
Using Windows® XP	58		
Configure WEP	59		
Configure WPA-PSK	61		
Troubleshooting.....	63		

Package Contents

- D-Link DIR-330 Wireless G Broadband Router
- Power Adapter
- CAT5 Ethernet Cable
- CD-ROM with Installation Wizard, User Manual, and Special Offers



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

- Ethernet-based Cable or DSL Modem
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0, Mozilla 1.7.12 (5.0), or Firefox 1.5 and above (for configuration)
- Installation Wizard requires Windows® XP with Service Pack 2

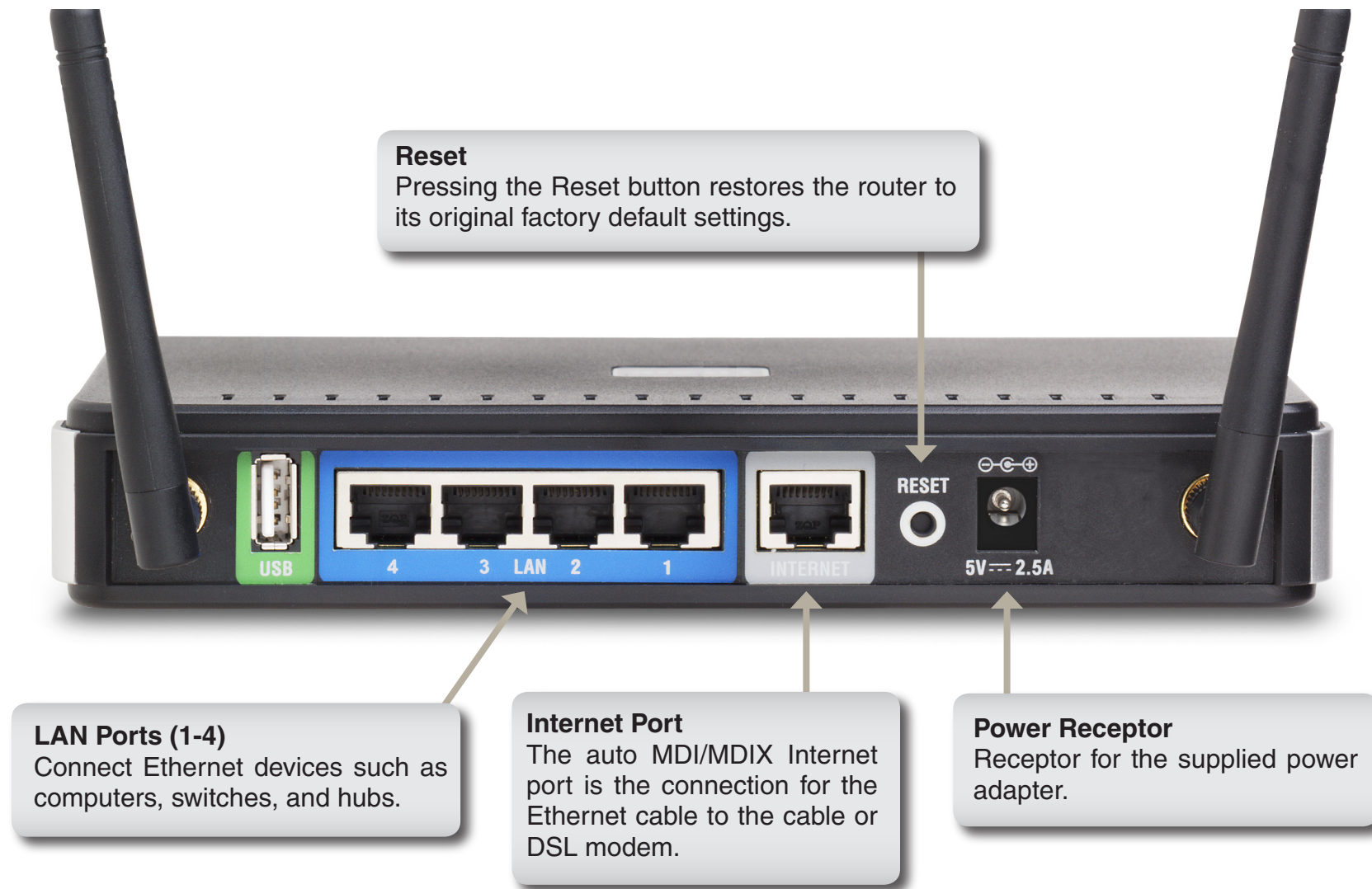
Features

- **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.
- **User-friendly Setup Wizard** - Through the easy-to-use Quick Router Setup on the included CD, the DIR-330 allows you to control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11g 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

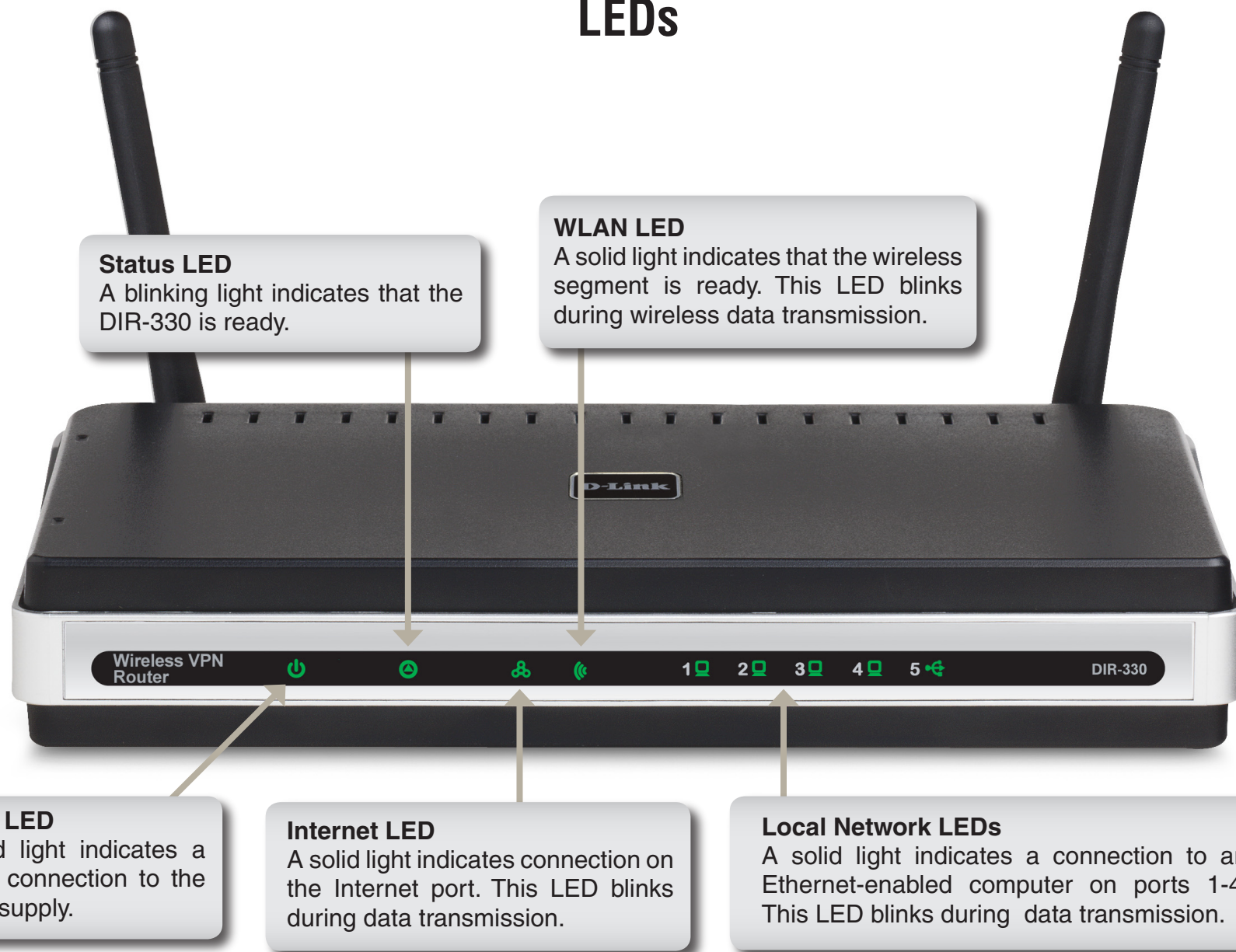
Connections



* The USB port is currently inactive.

Hardware Overview

LEDs



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 10 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 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.

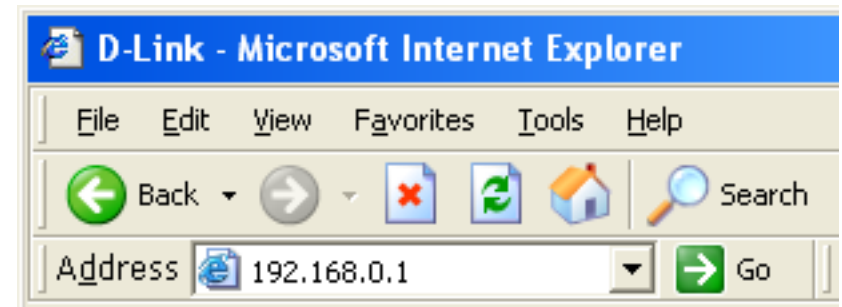
6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.
7. Connect an Ethernet cable in one of the LAN ports of the router and connect it to your other router. Do not plug anything into the Internet port of the D-Link router.
8. You may now use the other 3 LAN ports 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).



Select **Admin** from the drop-down menu and then enter your password. Leave the password blank by default.

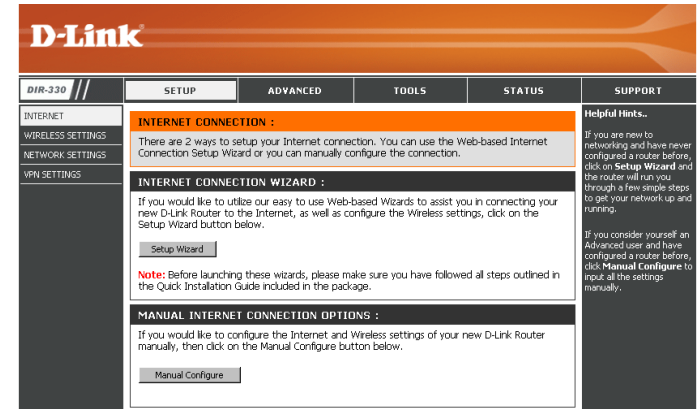
If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



Setup Wizard

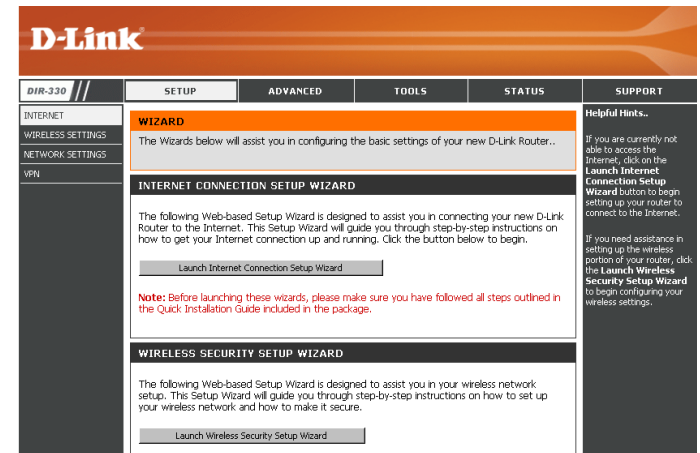
You may click **Setup Wizard** to quickly configure your router.

If you want to enter your settings without running the wizard, click **Manual Configure** and skip to page 15.



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

If you want to configure your wireless settings, click **Launch Wireless Security Setup Wizard** and skip to page 52.

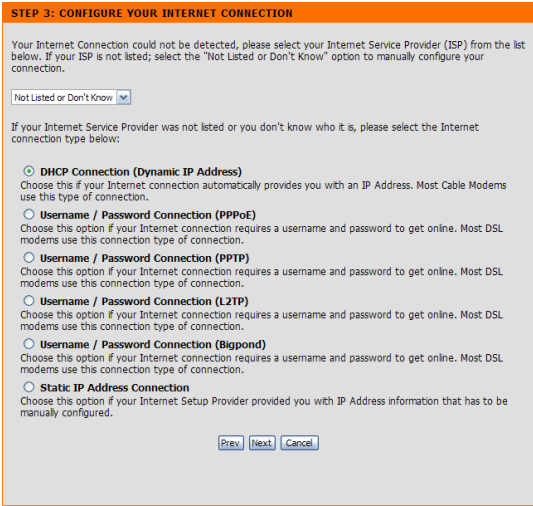
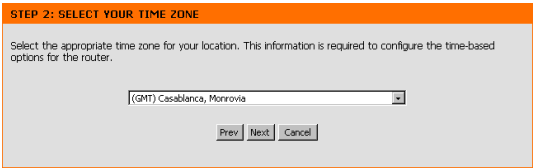
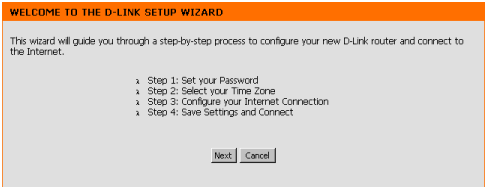


Click **Next** to continue.

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

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

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



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

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

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

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

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

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

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 - 90 - 4c - 4e - 00 - 0c (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

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.

Prev Next Cancel

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 :

Prev Next Cancel

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 :

Subnet Mask :

Gateway Address :

Primary DNS Address :

Secondary DNS Address :

If you selected Big Pond, select your authentication server from the drop down menu. You will also need to enter your Big Pond username and password. Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (BIGPOND)

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

Auth Server :

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

Bigpond User Name :

Bigpond Password :

Bigpond Verify Password :

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 (Cable)

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

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

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

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

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

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET WIRELESS SETTINGS NETWORK SETTINGS VPN

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, and BigPond. 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)

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 :

WIRELESS

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.

Internet Setup

PPPoE (DSL)

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

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

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

User Name: Enter your PPPoE user name.

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

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

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

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

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

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

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

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

The screenshot shows the D-Link DIR-330 web interface. The 'SETUP' tab is selected, and the 'INTERNET CONNECTION' section is active. The 'My Internet Connection is' dropdown is set to 'PPPoE (Username / Password)'. The 'INTERNET CONNECTION TYPE' section shows 'Dynamic PPPoE' selected. The 'PPPoe' section contains fields for User Name, Password, Retype Password, Service Name (optional), IP Address, MAC Address (with a 'Clone MAC Address' button), Primary DNS Address, Secondary DNS Address (optional), Maximum Idle Time (5 minutes), MTU (1492), and Connect mode select (Always-on, Manual, Connect-on demand).

Internet Setup

PPTP

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

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

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

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

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

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

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

PPTP Account: Enter your PPTP account (username).

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

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

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

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

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

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, and BigPond. 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 :

Subnet Mask :

Gateway :

DNS :

Server IP/Name :

PPTP Account :

PPTP Password :

PPTP Retype password :

Maximum Idle Time : Minutes

MTU :

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

WIRELESS

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 Auto-reconnect.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

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

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET WIRELESS SETTINGS NETWORK SETTINGS VPN

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, and BigPond. 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 :

L2TP :

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

☒ Dynamic IP ☐ Static IP

IP Address :

Subnet Mask :

Gateway :

DNS :

Server IP/Name :

L2TP Account :

L2TP Password :

L2TP Retype password :

Maximum Idle Time : Minutes

MTU :

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

Big Pond

My Internet Connection: Select BigPond (Australia) from the drop-down menu.

Username: Enter your BigPond username.

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

Auth Server: Select the type of authentication server being used from the drop-down menu.

Login Server IP: Enter the IP address of the login server.

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

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar shows a tree view with INTERNET, WIRELESS SETTINGS, and NETWORK SETTINGS. The main content area is titled 'WAN' and contains instructions for configuring the Internet Connection type. It lists options: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. A note specifies that PPPoE requires removing or disabling client software. Below this, there are 'Save Settings' and 'Don't Save Settings' buttons. The 'INTERNET CONNECTION TYPE' section prompts the user to choose a mode, with a dropdown menu currently set to 'BigPond (Australia)'. The 'BIGPOND' section prompts for ISP information, including fields for User Name, Password, Retype Password, Auth Server (set to 'sm-server'), Login Server IP/Name (optional), and MAC Address (with a 'Clone MAC Address' button). A 'Helpful Hints..' sidebar on the right provides additional guidance on selecting the correct connection type and verifying settings.

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
WIRELESS SETTINGS
NETWORK SETTINGS

WAN

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

BIGPOND :

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

User Name :

Password :

Retype Password :

Auth Server : sm-server

Login Server IP/Name : (optional)

MAC Address : - - - - - (optional)

Clone MAC Address

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.

WIRELESS

Internet Setup

Static (assigned by ISP)

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

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

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

ISP Gateway: Enter the Gateway assigned by your ISP.

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

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

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

The screenshot shows the D-Link DIR-330 Web UI. The top navigation bar includes 'DIR-330', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar has 'INTERNET', 'WIRELESS SETTINGS', and 'NETWORK SETTINGS'. The main content area is titled 'WAN' and contains instructions for configuring the Internet Connection type. It lists options: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. A note states that if using PPPoE, PPPoE client software must be removed. Below the instructions are 'Save Settings' and 'Don't Save Settings' buttons. The 'INTERNET CONNECTION TYPE' section shows 'Static IP' selected in a dropdown menu. The 'STATIC IP ADDRESS INTERNET CONNECTION TYPE' section prompts the user to enter static address information from their ISP. It includes fields for IP Address (with a note '(assigned by your ISP)'), Subnet Mask, ISP Gateway Address, MAC Address (with a 'Clone MAC Address' button), Primary DNS Address, Secondary DNS Address (marked as optional), and MTU (set to 1500). A 'Helpful Hints..' sidebar on the right provides additional guidance on selecting the correct Internet Connection Type and checking settings if there are access issues.

Wireless Settings

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

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

Wireless Channel: Indicates the channel setting for the DIR-330. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DIR-330 to choose the channel with the 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.

Visibility Status: Select Invisible if you do not want the SSID of your wireless network to be broadcasted by the router. If Invisible is selected the SSID will not be seen by site survey utilities so your wireless clients must have the SSID manually entered to connect to the router.

Wireless Security: Refer to page 50 for more information regarding wireless security.

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

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 or WPA-Personal.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS :

Enable Wireless : ☒

Wireless Network Name : dlink (Also called the SSID)

Wireless Channel : 6

Enable Auto Channel Scan : ☐

802.11 Mode : 802.11 b/g mixed

Visibility Status : ☒ Visible ☐ Invisible

WIRELESS SECURITY MODE :

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

Security Mode : None

WIRELESS

Helpful Hints..

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

We recommend that you Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on.

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.

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 TOOLS STATUS SUPPORT

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

DHCP stands for Dynamic Host Control Protocol. The DIR-330 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.” When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-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.

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 : ☒
 DHCP IP Address Range : to (addresses within the LAN subnet)
 DHCP Lease Time : (minutes)

ADD DHCP RESERVATION :

 Enable : ☐
 Computer Name : <<
 IP Address : 192 . 168 . 0 .
 MAC Address :

DHCP RESERVATIONS LIST :

Enable	Computer Name	MAC Address	IP Address

DYNAMIC DHCP CLIENT LIST :

Host Name	IP Address	MAC Address	Expired Time
192.168.0.130	192.168.0.130	00:13:ce:77:8d:45	Sun Jan 14 01:02:54 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.

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

Enable: Check this box to enable the reservation.

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

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

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

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

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

ADD DHCP RESERVATION :

Enable : ☐

Computer Name : << Computer Name ▼

IP Address : 192 . 168 . 0.

MAC Address :

Copy Your PC's MAC Address

Save Clear

DHCP RESERVATIONS LIST :

Enable	Computer Name	MAC Address	IP Address
--------	---------------	-------------	------------

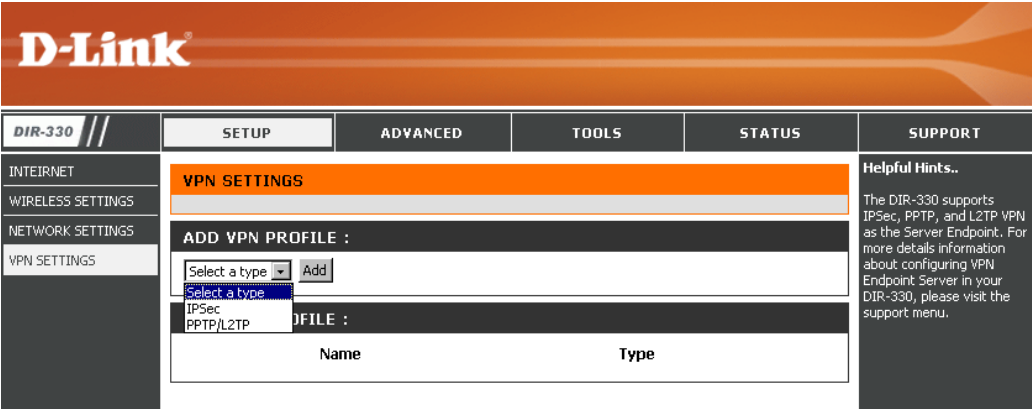
DYNAMIC DHCP CLIENT LIST :

Host Name	IP Address	MAC Address	Expired Time
192.168.0.130	192.168.0.130	00:13:ce:77:8d:45	Sun Jan 14 01:02:54 2007

VPN Settings

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

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

Encapsulation: Select **Tunnel**.

Remote IP: Select **Site to Site** for LAN-to-LAN configuration and enter the destination gateway IP address in the box.

Remote Local LAN Net/ Mask: For LAN-to-LAN configuration, enter the destination Subnet and Mask.

Authentication: Enter the pre-shared key. The VPN Servers Endpoint from both ends must use the same key.

Phase 1- Cipher #1-4 - Select **3DES** or **AES**.

IKE Proposal List: Hash #1-4 - Select **SHA1** or **MD5**.

Phase 2: Select PFS if both ends are supported.

IKE Proposal List: Cipher #1-4 - Select **3DES** or **AES**.

Hash #1-4 - Select **SHA1** or **MD5**.

D-Link

DIR-330 // SETUP ADVANCED TOOLS STATUS SUPPORT

VPN - IPSEC

Save Settings Don't Save Settings

IPSEC SETTING :

☐ Enable

Name :

Encapsulation Mode : ☒ Tunnel

Remote IP : ☒ Remote User ☐ Site to Site

Remote Local LAN Net / Mask : /

Authentication : Pre-shared / Shared Key

PHASE 1 :

IKE Proposal List :

	Cipher	Hash
#1:	3DES	SHA1
#2:	3DES	SHA1
#3:	3DES	SHA1
#4:	3DES	SHA1

PHASE 2 :

PFS : ☒ PFS

IPSec Proposal List :

	Cipher	Hash
#1:	3DES	SHA1
#2:	3DES	SHA1
#3:	3DES	SHA1
#4:	3DES	SHA1

Helpful Hints..

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.

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. The other part is the actual IP data being transferred, using the encryption and authentication methods agreed upon in the IKE negotiation. This can be accomplished in a

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 using MPPE.

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

Enable Settings: Check this box to enable.

Name: Enter a name for your VPN.

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

VPN Server IP: Enter the VPN Server IP address which is the LAN IP of the DIR-330 (I.E. 192.168.0.1).

Remote IP Range: Assign a range of IP addresses. The assigned IP range should be on the same network but not in the same range as your DHCP IP range. For example, if you 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/MSCHAP v2).

MPPE Encryption Mode: Select the level of encryption (40-bit/128-bit).

Authentication Sources: Select **Local**.

User Name: Enter your username.

Password: Enter your password.

D-Link

DIR-330 // SETUP ADVANCED TOOLS STATUS SUPPORT

VPN - PPTP/L2TP SERVER

Save Settings Don't Save Settings

PPTP/L2TP SETTING :

Enable setting : ☐

Name :

Connection type : ☒ PPTP ☐ L2TP

VPN Server IP :

Remote IP range : -

Authentication Protocol : ☐ PAP ☐ CHAP ☒ MSCHAP v2

MPPE Encryption Mode : ☐ RC4 ☒ 40 bit ☐ 128 bit

Authentication Sources : ☒ Local

User Name 1 :

Password 1 :

User Name 2 :

Password 2 :

User Name 3 :

Password 3 :

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.

Virtual Server

The DIR-330 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DIR-330 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-330 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-330 redirects the external service request to the appropriate server within the LAN network.

The DIR-330 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

For a list of ports for common applications, please visit http://support.dlink.com/faq/view.asp?prod_id=1191.

This will allow you to open a single port. If you would like to open a range of ports, refer to page 30.

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 <<.

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

Traffic Type: Select the type of protocol you would like to use for the selected rule.

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

The screenshot shows the D-Link DIR-330 Advanced Setup interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, NETWORK FILTER, WEBSITE FILTER, FIREWALL SETTINGS, ADVANCED WIRELESS, and ADVANCED NETWORK. The main content area is titled "VIRTUAL SERVER RULES" and contains a description of the feature, "Save Settings" and "Don't Save Settings" buttons, and a table for configuring rules.

24 - VIRTUAL SERVER RULES					
	Name	Application Name	Port	Traffic Type	Schedule
<input type="checkbox"/>	IP Address	<< Computer Name	Public	TCP	Always
<input type="checkbox"/>	IP Address	<< Computer Name	Private	TCP	Always
<input type="checkbox"/>	IP Address	<< Computer Name	Public	TCP	Always
<input type="checkbox"/>	IP Address	<< Computer Name	Private	TCP	Always
<input type="checkbox"/>	IP Address	<< Computer Name	Public	TCP	Always
<input type="checkbox"/>	IP Address	<< Computer Name	Private	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 Virtual Server Rule, you must first define a schedule on the **Tools>Schedules** page.

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 <<.

Start Port/End Port: Enter the port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.

Example: 24,1009,3000-4000

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

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

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

VIRTUAL SERVER
PORT FORWARDING
APPLICATION RULES
NETWORK FILTER
WEBSITE FILTER
FIREWALL SETTINGS
ADVANCED WIRELESS
ADVANCED NETWORK

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

24- PORT FORWARDING RULES

	Name	IP Address	Port	Traffic Type	Schedule
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	Start <input type="text"/> End <input type="text"/>	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	Start <input type="text"/> End <input type="text"/>	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	Start <input type="text"/> End <input type="text"/>	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 **Tools>Schedules** page.

This feature allows you to open a range of ports to a computer on your network.

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.

The DIR-330 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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

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

Firewall: This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Traffic Type: Select the protocol of the firewall port (TCP, UDP, or Both).

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

D-Link

DIR-330 // SETUP ADVANCED TOOLS STATUS SUPPORT

APPLICATION RULES :

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

Save Settings Don't Save Settings

24 - APPLICATION RULES

		Port	Traffic Type	Schedule
<input type="checkbox"/>	<< Application Name	Trigger	TCP	Always
	Battle.net	Firewall	TCP	
	Dialpad	Trigger	TCP	
	ICU II	Firewall	TCP	Always
	MSN Gaming Zone	Trigger	TCP	
	PC-to-Phone	Firewall	TCP	
	Quick Time 4			

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 **Tools > Schedules** page.

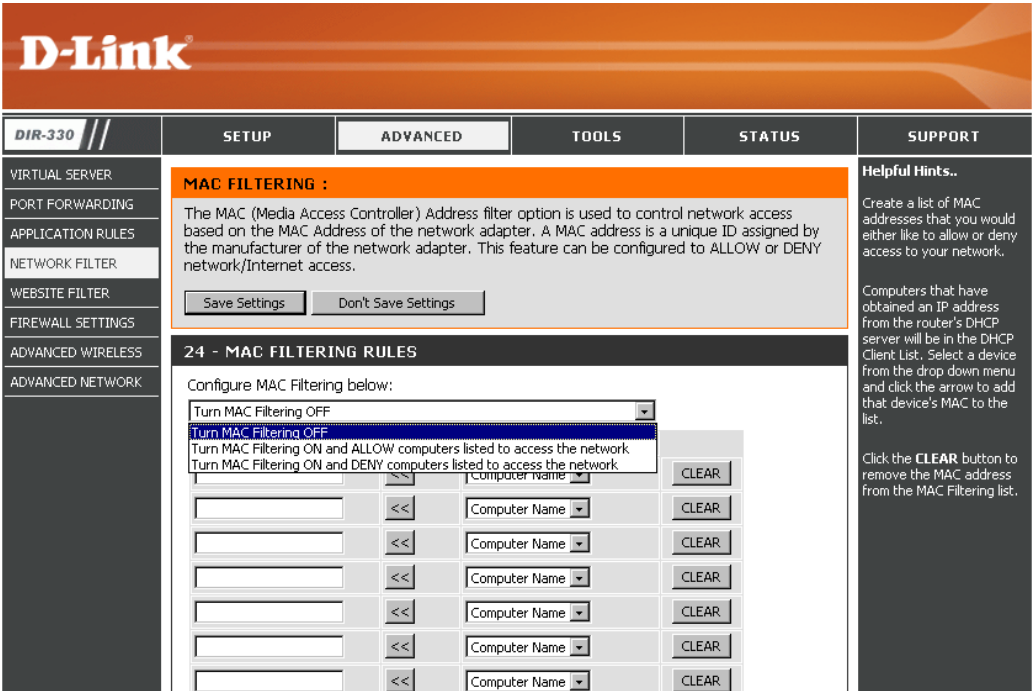
Network Filters

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

Configure MAC Filtering: Select **Turn MAC Filtering Off**, **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.



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 **Clear the List Below**.

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.

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 **Tools > Schedules** section.

The screenshot shows the D-Link DIR-330 Web Management Interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, NETWORK FILTER, WEBSITE FILTER (selected), FIREWALL SETTINGS, ADVANCED WIRELESS, and ADVANCED NETWORK.

The main content area is titled "WEBSITE FILTERING RULES :". It contains 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." Below this are two buttons: "Save Settings" and "Don't Save Settings".

Below the buttons is a section titled "40 - WEBSITE FILTERING RULES". It contains a "Configure Website Filtering below:" section with a dropdown menu. The dropdown menu is open, showing three options: "Turn Website Filtering OFF", "Turn Website Filtering ON and ALLOW computers access to ONLY these sites", and "Turn Website Filtering ON and DENY computers access to ONLY these sites".

Below the dropdown menu is a table with two columns: "Website URL/Domain" and "Website URL/Domain". Each column has a text input field and a dropdown menu set to "Always". There are six rows in total, each with a "Website URL/Domain" input field and an "Always" dropdown menu.

On the right side of the interface, there is a "Helpful Hints.." section. It contains two hints: "Create a list of Websites that you would like the devices on your network to be allowed or denied access to." and "Keywords can be entered in this list in order to block any URL containing the keyword entered."

Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-330 offers a firewall type functionality. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

Enable DMZ 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. Use of this option is only recommended as a last resort.

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 **Basic > DHCP** page so that the IP address of the DMZ machine does not change.

Enable PPTP Passthrough: Check this box to allow PPTP VPN traffic to pass through the router to your VPN client.

Enable L2TP Passthrough: Check this box to allow L2TP VPN traffic to pass through the router to your VPN client.

Enable IPSec Passthrough: Check this box to allow IPSec VPN traffic to pass through the router to your VPN client.

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

FIREWALL SETTINGS :

The Web Filter options allows you to set-up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all other Web sites not listed on this page will be blocked.

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

VPN PASSTHROUGH :

Enable PPTP Passthrough : ☐

Enable L2TP Passthrough : ☐

Enable IPSec Passthrough : ☐

Helpful Hints..

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

Make sure VPN passthrough is enabled if you are trying to use a VPN client from behind the router.

VPN Passthrough will only function if the VPN client being used runs on the standard ports associated with the VPN connection type. If you are having problems getting your VPN client connected from behind the router and these VPN passthrough options are enabled, please contact your network administrator to find out if any nonstandard ports or options are being used.

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 2432. 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: (Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

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. Auto is the default setting. Note: High network traffic areas should use the shorter preamble type.

WMM Function: WMM is QoS for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.

D-Link

DIR-330

SETUP ADVANCED TOOLS STATUS SUPPORT

ADVANCED WIRELESS SETTINGS :

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

Save Settings Don't Save Settings

ADVANCED WIRELESS SETTINGS :

TX Rates : Auto

Beacon interval : Auto (msec, range:20~1000, default:100)

RTS Threshold : 2 (range: 256~2346, default:2346)

Fragmentation : 5.5 (range: 1500~2346, default:2346, even number)

DTIM interval : 6 (range: 1~5, default:1)

Preamble Type : 12 Short Preamble Long Preamble

WMM Function: ☐ Enable ☒ Disable

Helpful Hints.

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 TOOLS STATUS SUPPORT

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 : 100Mbps
10Mbps
100Mbps
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.

Administrator Settings

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

Admin Password: Enter a new password for the administrator login. Only the administrator can make changes to the settings.

Enable Remote Management: Remote management allows the DIR-330 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 **Tools > Schedules** section.

The screenshot shows the D-Link DIR-330 web management interface. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES, and LOG SETTINGS. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains the following sections:

- ADMINISTRATOR SETTINGS :** A message states: 'There is one account that can access the router's management interface. This accounts is admin. Admin has read/write access.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.
- ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "ADMIN") :** This section contains two password fields: 'New Password' and 'Confirm Password', both masked with dots.
- REMOTE MANAGEMENT :** This section includes:
 - 'Enable Remote Management' with an unchecked checkbox.
 - 'IP Address' with a text field containing an asterisk (*).
 - 'Port' with a dropdown menu set to '80' and a schedule dropdown set to 'Always'.

On the right side of the interface, there is a 'Helpful Hints..' section with security advice: 'For security reasons, it is recommended that you change the Login Name and Password for the Administrator and User accounts. Be sure to write down the new Login Names and Passwords to avoid having to reset the router in the event that they are forgotten.' Below this, it states: '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.'

Time Settings

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

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

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

Enable NTP Server: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

NTP Server Used: Enter the NTP server or select one 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 **Set Time**. You can also click **Copy Your Computer's Time Settings**.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES, and LOG SETTINGS. The main content area is titled 'TIME : Time Configuration' and contains the following sections:

- TIME :** A sub-header for the Time Configuration section.
- Time Configuration:** A descriptive paragraph explaining the purpose of the section.
- Save Settings / Don't Save Settings:** Two buttons for saving or discarding changes.
- TIME CONFIGURATION :** A section containing:
 - Time :** A text field showing 'Nov/15/2006 01:15:55'.
 - Time Zone :** A dropdown menu currently set to '(GMT) Casablanca, Monrovia'.
 - Enable Daylight Saving :** A checkbox that is currently unchecked.
 - DST Start / DST End:** Fields for Daylight Saving Time, each with dropdowns for Month, Week, Day of Week, and Time.
- AUTOMATIC TIME CONFIGURATION :** A section containing:
 - Enable NTP server :** A checkbox that is currently unchecked.
 - NTP Server Used :** A text field showing 'ntp1.dlink.com' and a dropdown menu labeled 'Select NTP Server'.
- SET THE DATE AND TIME MANUALLY :** A section containing:
 - Current Gateway Time :** A heading for the manual time setting section.
 - Year, Month, Day, Hour, Minute, Second:** Individual dropdown menus for each time component.
 - AM/PM:** A dropdown menu for the time of day.
 - Copy Your Computer's Time Settings:** A button to copy the local computer's time.

On the right side of the interface, there is a 'Helpful Hints..' section with text about scheduling features and a 'Copy Your Computer's Time Settings' button.

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 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, use the Browse control 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 Device: Click to reboot the router.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists menu items: ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES, and LOG SETTINGS. The main content area is titled 'SYSTEM SETTINGS :'. It contains a text box stating: 'The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.' Below this, there are four sections with buttons: 'Save Settings To Local Hard Drive' with a 'Save Configuration' button; 'Load Settings From Local Hard Drive' with a text input field and a 'Browse...' button, followed by a 'Restore Configuration from File' button; 'Restore To Factory Default Settings' with a 'Restore Factory Defaults' button; and 'Reboots the DIR-330' with a 'Reboot the Device' button. On the right side, there is a 'Helpful Hints..' section with text explaining that settings can be saved to a file and restored later.

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 shows the D-Link DIR-330 web interface. The top navigation bar includes links for ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES, and LOG SETTINGS. The FIRMWARE section is active, displaying the 'FIRMWARE UPGRADE' page. This page contains instructions on how to upgrade the firmware, a 'Save Settings' button, and a 'Don't Save Settings' button. Below this, the 'CURRENT FIRMWARE INFO' section shows the current firmware version as 1.00 and the firmware date as Dec 21 2006, with a 'Browse...' button to select a new firmware file. A 'Helpful Hints..' section on the right provides additional information about firmware updates.

DIR-330 //	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
ADMIN					Helpful Hints.. 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.
TIME					
SYSTEM					
FIRMWARE	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. <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>				
DDNS					
SYSTEM CHECK					
SCHEDULES					
LOG SETTINGS					
CURRENT FIRMWARE INFO : Current Firmware Version 1.00 Firmware Date Dec 21 2006 <input type="text"/> <input type="button" value="Browse..."/>					

DDNS

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

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

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

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

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

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

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

Timeout: Enter the timeout time in hours*.

D-Link

DIR-330 //

SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSTEM
FIRMWARE
DDNS
SYSTEM CHECK
SCHEDULES
LOG SETTINGS

DYNAMIC DNS :

Dynamic DNS (Domain Name Service) is a method of keeping a domain name linked to a changing (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.

Save Settings Don't Save Settings

DDNS SETTINGS :

Enable Dynamic DNS : ☐

Server Address : << Select Dynamic DNS Server

Host Name : Select Dynamic DNS Server

Username or Key : www.dlinkddns.com (Free)

Password or Key : www.DynDns.org (Custom)

Verify Password or Key : www.DynDns.org (Static)

Timeout : 240 (hours)

Helpful Hints..

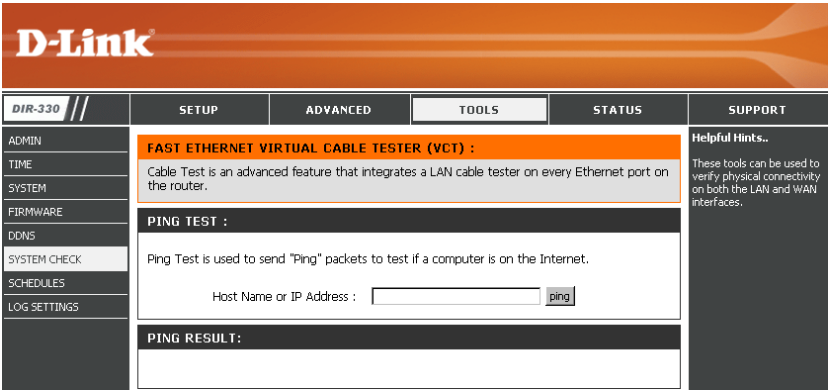
In order to use this feature you must first have a DDNS account from one of the providers in the drop down menu.

* The Timeout feature currently is not active. This feature will be available with a future firmware upgrade.

System Check

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

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



Schedules

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 **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSTEM
FIRMWARE
DDNS
SYSTEM CHECK
SCHEDULES
LOG SETTINGS

SCHEDULES :

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

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..

This page is used to configure global schedules for the router. Once defined, these schedules can later be applied to the features of the router that support scheduling.

Log Settings

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

Email Address: The email address to which the logs will be sent. Click on **Send Mail Now** to send the email.

Save Log File to Local Hard Drive: Click to save the log to your hard drive.

Log Type: Select the type of log you would like to view.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES, and LOG SETTINGS (which is currently selected). The main content area is titled 'LOG SETTINGS' and contains the following sections:

- LOG SETTINGS :** A message states 'Logs can be saved by sending it to an admin email address.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.
- LOG FILES :** This section contains several input fields and checkboxes:
 - 'SMTP Server / IP Address' with an empty text box.
 - 'Email Address' with an empty text box and a 'Send Mail Now' button to its right.
 - 'Save Log File To Local Hard Drive' with a 'Save' button.
 - 'Log Type' with a list of checkboxes:
 - ☒ System Activity
 - ☐ Debug Information
 - ☒ Attacks
 - ☐ Dropped Packets
 - ☒ Notice

On the right side of the interface, under the 'SUPPORT' tab, there is a 'Helpful Hints..' section. It contains a message: '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 your email provider or visit their support website to find out this information.'

Device Information

This page displays the current information for the DIR-330. It will display the LAN, WAN (Internet), Wireless information, 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 wireless MAC address and your wireless settings such as SSID and Channel.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: DEVICE INFO, LOG, STATS, WIRELESS COMPUTERS, LAN COMPUTERS, and VPN. The main content area is titled 'DEVICE INFORMATION' and displays the following details:

- DEVICE INFORMATION :** All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here. **Firmware Version: 1.00**
- LAN :**
 - MAC Address : 00:90:4C:4E:45:3A
 - IP Address : 192.168.0.1
 - Subnet Mask : 255.255.255.0
 - DHCP Server : Enabled
- WAN :**
 - MAC Address : 00:90:4c:4e:00:0c
 - Connection : DHCP Client Connecting
 - Buttons: DHCP Release, DHCP Renew
 - IP Address :
 - Subnt Mask :
 - Default Gateway :
 - DNS :
- WIRELESS :**
 - SSID : dlink
 - Channel : 6
 - Encryption : Disabled

A 'Helpful Hints..' section on the right side of the interface states: '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 DIR-330. Here you can view the logs of the router.

First Page: This option will direct you to the current first page of the logs.

Last Page: This option will direct you to the current last page of the logs.

Previous: Click to view the previous page.

Next: Click to view the next page.

Clear: Clears all current log content.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains links for DEVICE INFO, LOG, STATS, WIRELESS COMPUTERS, LAN COMPUTERS, and VPN. The main content area is titled 'VIEW LOG : View Log displays the activities occurring on the DIR-330.' Below this, there is a section for 'LOG FILES :'. It includes navigation buttons: First Page, Last Page, Previous, Next, and Clear. A table displays the log entries:

Time	Type	Message
Nov 15 01:28:18	System Activity	SSI parse Finished

On the right side of the interface, there is a 'Helpful Hints...' section with the text: 'Display the captured log messages of the router activities, these captured log messages might be useful for trouble shooting and monitoring.'

Stats

The screen below displays the current statistics of the DIR-330. Here you can view the amount of packets that pass through the router.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: DEVICE INFO, LOG, STATS, WIRELESS COMPUTERS, LAN COMPUTERS, and VPN. The main content area is titled "TRAFFIC STATISTICS :" and contains a sub-header "Traffic Statistics display Receive and Transmit packets passing through the DIR-330." Below this, there are "Refresh" and "Reset" buttons. A table displays the following data:

	Receive	Transmit
WAN	10843 Packets	17944 Packets
LAN	519 Packets	847 Packets
WIRELESS	290 Packets	1499 Packets

On the right side, there is a "Helpful Hints.." section with the text: "Show the traffic statistics receive and transmit packets passing through the router."

Wireless Computers

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

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: DEVICE INFO, LOG, STATS, WIRELESS COMPUTERS, LAN COMPUTERS, and VPN. The main content area is titled "CONNECTED WIRELESS CLIENT LIST" and contains a sub-header "The Wireless Client table below displays Wireless clients Connected to the AP (Access Point)." Below this, there is a section titled "WIRELESS COMPUTERS" with a table displaying the following data:

MAC Address	Connected Time	Idle Time

On the right side, there is a "Helpful Hints.." section with the text: "Display the current wireless clients connecting to the AP (Access Point)"

LAN Computers

The LAN computers table displays a list of current connected wired clients. This table also displays the connection time and MAC address of the connected wired clients.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options, with LAN COMPUTERS selected. The main content area displays the LAN COMPUTERS LIST, which includes a warning about Dynamic DHCP and DHCP reservation, a table of connected clients, and a helpful hint section.

LAN COMPUTERS LIST		
While Dynamic DHCP and DHCP reservation client computers connected to the unit will have their information display in the LAN COMPUTER.		
LAN COMPUTERS		
IP Address	Name	MAC Address
192.168.100.133	workhorse	00:0e:a6:39:e1:a1

Helpful Hints..
Display the current wire clients connecting to the router

VPN

The VPN table displays a list of current VPN sessions.

The screenshot shows the D-Link DIR-330 web interface. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options, with VPN selected. The main content area displays the CONNECTED VPN TUNNEL LIST, which includes a warning about the VPN List, a table of connected tunnels, and a helpful hint section.

CONNECTED VPN TUNNEL LIST			
The VPN List below displays VPN Connection.			
Type	Local Information	Remote Information	Other

Helpful Hints..
Display the current established VPN tunnel

Support

DIR-330

MENU

SETUP

ADVANCED

TOOLS

STATUS

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

SUPPORT MENU

Internet

Advanced

Tools

Status

SETUP

Internet

Wireless Settings

Network settings

ADVANCED

Virtual Server

Port Forwarding

Application Rules

Network Filter

Website Filter

Firewall Settings

Advanced Wireless

Advanced Network

TOOLS

Admin

Time

System

Firmware Upgrade

DDNS

System Check

Schedules

Log settings

STATUS

Device Info

Log

Stats

Wireless

WIRELESS

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 stands for Wired Equivalent Privacy. It 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, or 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:

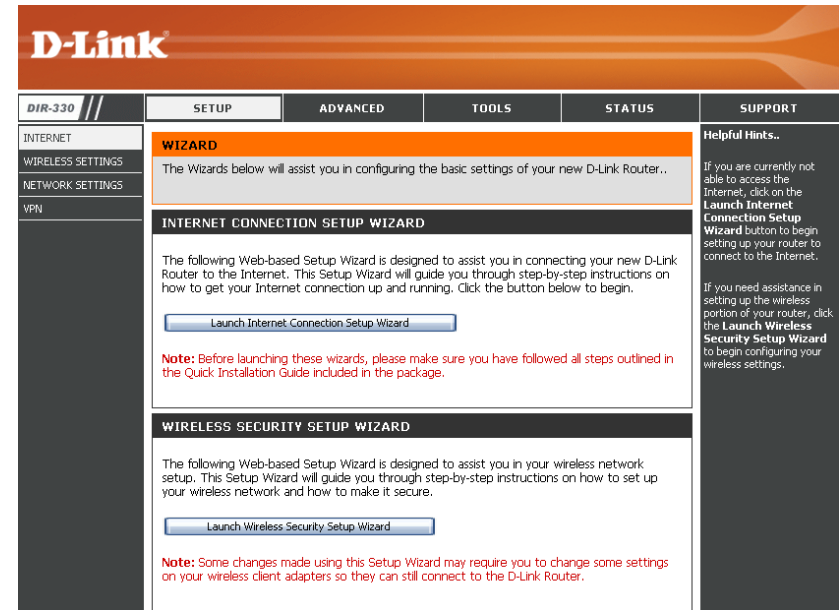
- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead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



Click **Next** to continue.



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.

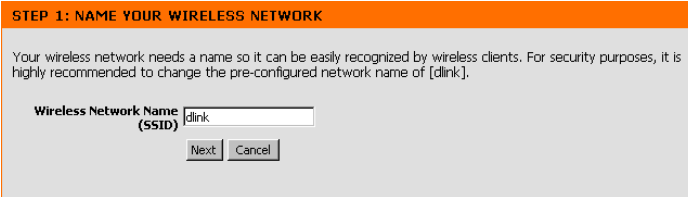
Select the level of security for your wireless network:

- Best - WPA2 Authentication
- Better - WPA Authentication
- None - No security

Click **Next** to continue.

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

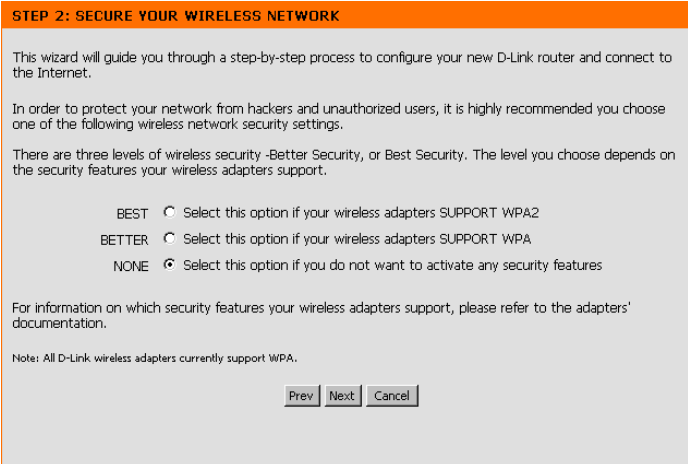
Click **Next** to continue.



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 -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
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.

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

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

SETUP COMPLETE!

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

Wireless Network Name (SSID) : dlink

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.

SETUP COMPLETE!

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

Wireless Network Name (SSID) : dlink

Encryption : WPA-PSK/TKIP (also known as WPA Personal)

Pre-Shared Key :

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.

SETUP COMPLETE!

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

Wireless Network Name (SSID) : dlink

Encryption : WPA2-PSK/AES (also known as WPA2 Personal)

Pre-Shared Key :

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. Next to *Security Mode*, select **WEP**.
3. Next to *Authentication*, select **Shared Key** or **Open**.
4. Next to *WEP Encryption*, select the level of encryption (64 or 128-bit).
5. Next to *Key Type*, select the type of WEP key (Hex or ASCII).
6. Next to *WEP Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.
7. 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 :

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

Security Mode :

WEP :

If you choose the WEP security option this device will ONLY operate in Legacy Wireless mode (802.11B/G). This means you will NOT get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

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

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

Authentication :

WEP Encryption :

Key Type :

Default WEP Key :

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Configure WPA-Personal (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.

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. Next to *Security Mode*, select **WPA-Personal**.
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Pre-Shared Key*, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.
5. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

WIRELESS SECURITY MODE :

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

Security Mode :

WPA :

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode :

PRE-SHARED KEY :

Pre-Shared Key :

Configure WPA-Enterprise (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. Next to *Security Mode*, select **WPA-Enterprise**.
3. Next to *WPA Mode*, select **WPA2 Only** or **WPA Only**.
4. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).
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. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.
9. Click **Save Settings** to save your settings.

WIRELESS SECURITY MODE :

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

Security Mode :

WPA :

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode :

EAP (802.1X) :

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

RADIUS server IP Address:

RADIUS server Port:

RADIUS server Shared Secret:

Connect to a Wireless Network 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.

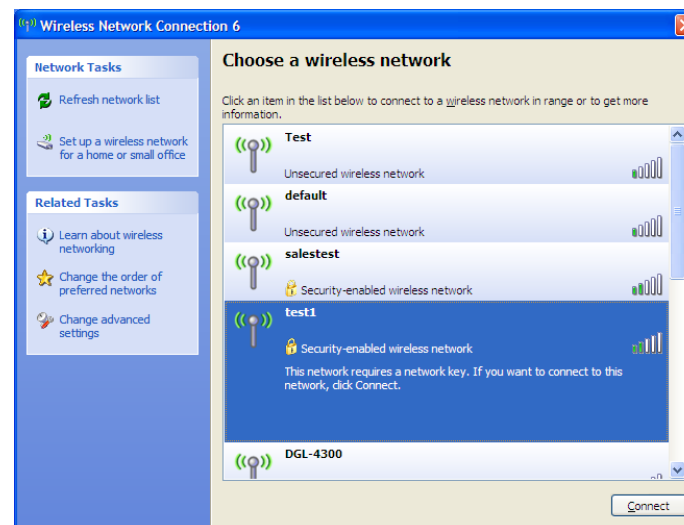
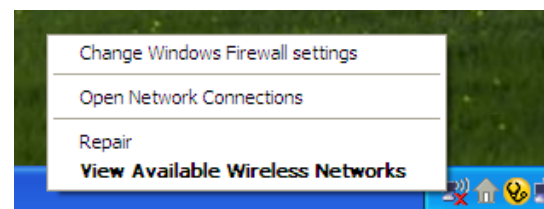
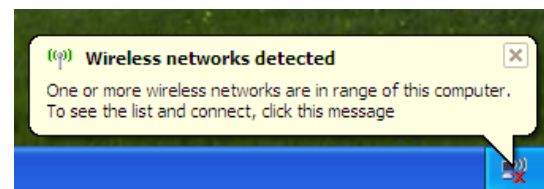
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

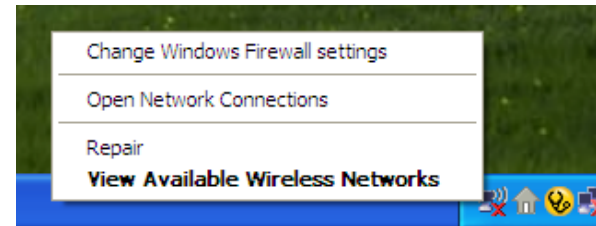
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



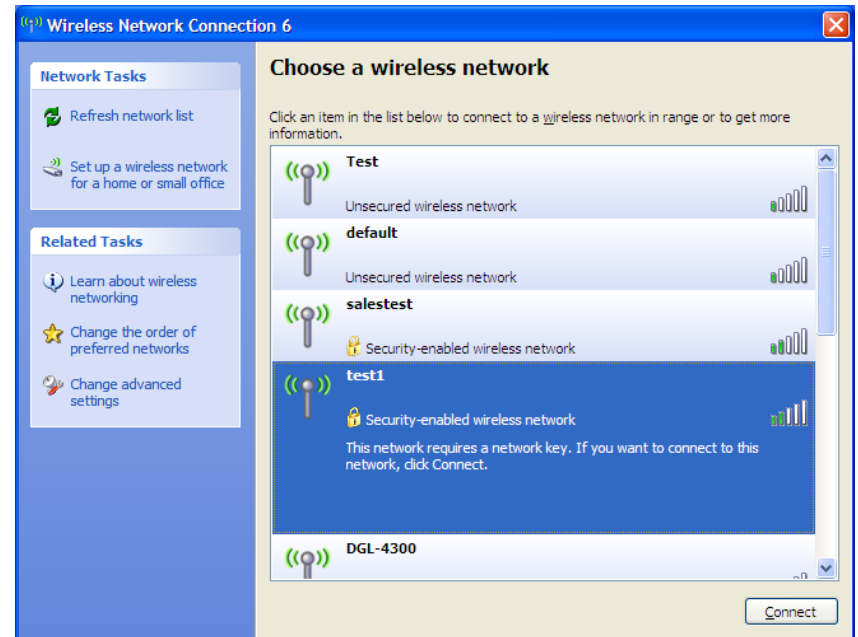
Configure WEP

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**.

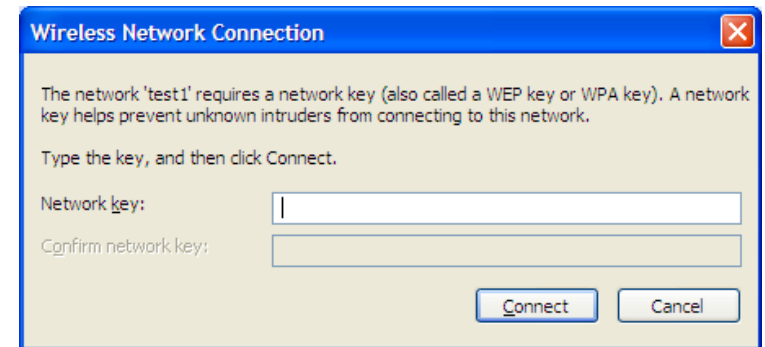


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

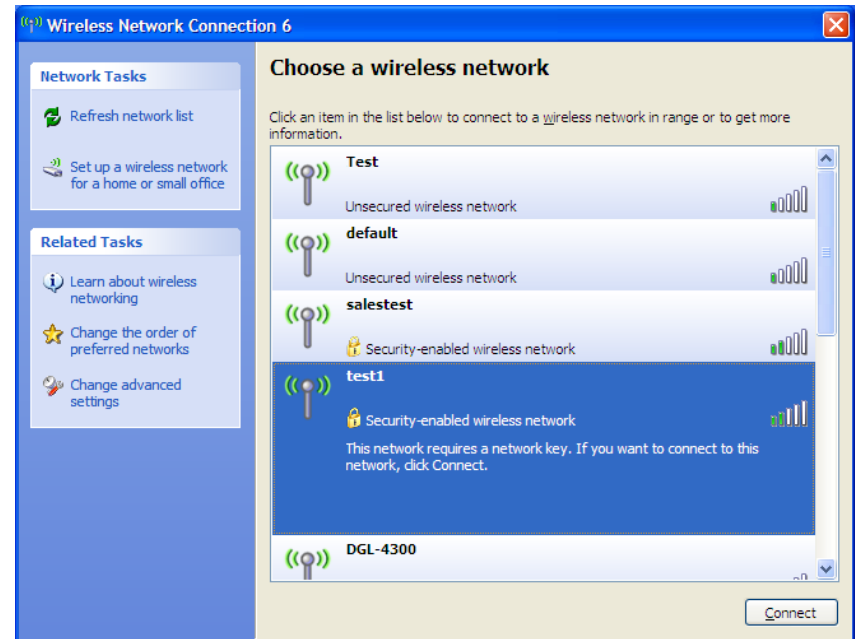
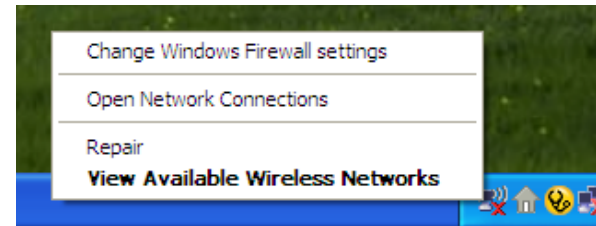
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



Configure WPA-PSK

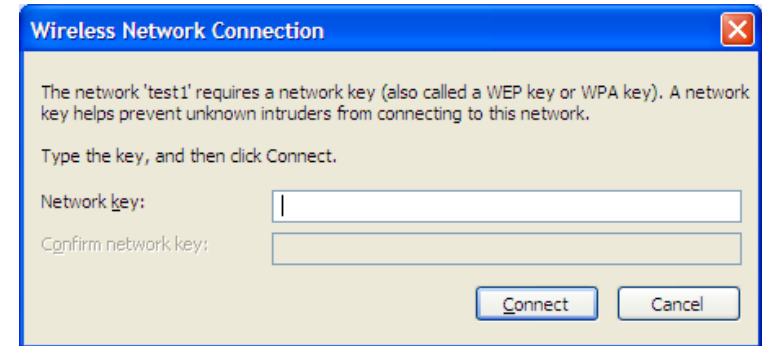
It is recommended to enable WEP on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WEP key being used.

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 chapter 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. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 6.0 or higher
 - Firefox 1.5 or higher
 - Netscape 8 or higher
 - Mozilla 1.7.12 (5.0) or higher
 - Opera 8.5 or higher
 - Safari 1.2 or higher (with Java 1.3.1 or higher)
 - Camino 0.8.4 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® 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 75.

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

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

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.

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

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

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

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

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

C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

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

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, let's 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 Settings** 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

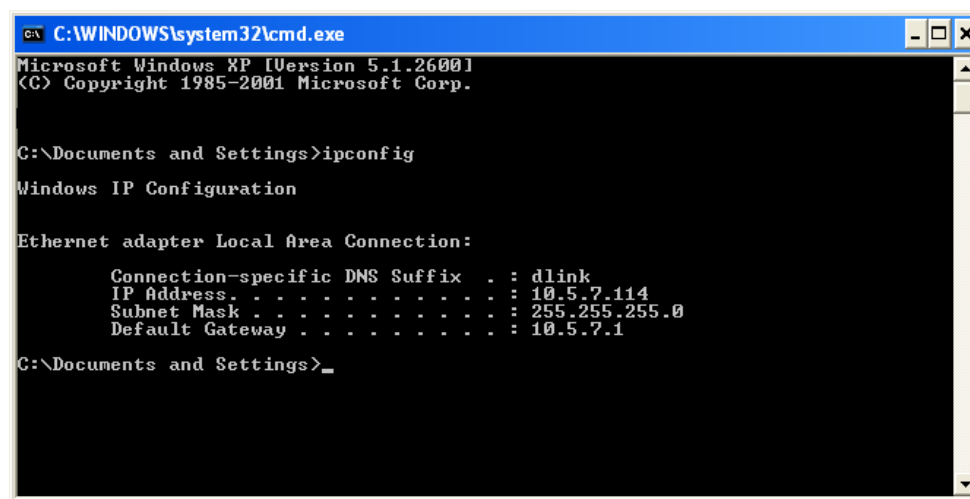
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



```
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 you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

Statically Assign an IP address

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

Step 1

Windows® XP - Click on **Start > Control Panel > Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places > Properties**.

Step 2

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

Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

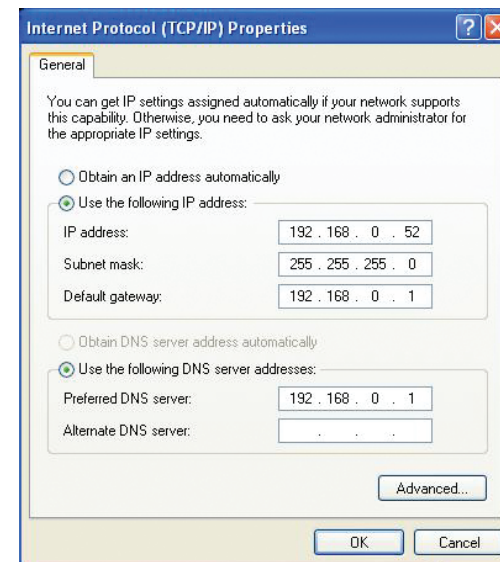
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: 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 not needed or you may enter a DNS server from your ISP.

Step 5

Click **OK** twice 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

- 15dBm \pm 2dB

External Antenna Type

- Two (2) detachable reverse SMA Antennas

LEDs

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

Operating Temperature

- 32°F to 131°F (0°C to 40°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- CE

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 - 192.168.0.200
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) 453-5465

Internet Support:

<http://support.dlink.com>

For customers within Canada:

Phone Support:

(800) 361-5265

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.

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 1.0
January 15, 2007