

USER MANUAL

DIR-451

VERSION 1.3



Preface

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

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

Preface	i	Application Rules	21
Trademarks	i	Network Filter.....	22
Product Overview	1	Website Filter	23
Package Contents.....	1	Firewall Settings.....	24
System Requirements	1	Advanced Wireless Settings	25
Introduction.....	2	Advanced Network Settings.....	26
Features.....	3	Administrator Login Name:.....	27
Hardware Overview	5	Administrator Password:.....	27
Connections	5	Remote Management:.....	27
LEDs	6	Administrator Settings.....	27
Installation	7	Time Settings	28
Connect to your Network	7	System Settings.....	29
Wireless Installation Considerations.....	9	Firmware Upgrade	30
Configuration	10	DDNS.....	31
Web-based Configuration Utility	10	System Check.....	32
Setup Wizard	11	Schedules	33
UMTS/HSDPA Setup	14	Log Settings.....	34
Wireless Settings	15	Syslog	35
Network Settings.....	17	Email Settings.....	36
DHCP Server Settings	18	Device Information	37
Virtual Server	19	Log.....	38
Port Forwarding	20	Stats.....	39
		Wireless Stats.....	39
		Support	40

Wireless Security	41	Warranty	66
What is WEP?	41	GNU/Linux GPL	72
Configure WEP	42	GNU General Public License	73
What is WPA?	43	Registration	79
Configure WPA-PSK	44		
Configure WPA (RADIUS).....	45		
Connect to a Wireless Network	46		
Using Windows Vista™	46		
Configure Wireless Security.....	47		
Using Windows® XP	49		
Configure WEP	50		
Configure WPA-PSK	52		
Troubleshooting	54		
Wireless Basics	56		
What is Wireless?	57		
Tips	59		
Wireless Modes	60		
Networking Basics	61		
Check your IP address	61		
Statically Assign an IP address	62		
Technical Specifications	63		
Contacting Technical Support	65		

Package Contents

- D-Link DIR-451 Mobile Router
- Power Adapter
- Ethernet Cable
- Manual and Warranty on CD



Note: Using a power supply with a different voltage rating than the one included with the DIR-451 will cause damage and void the warranty for this product.

System Requirements

- A compatible 32-bit PCMCIA (UMTS or HSDPA) card with service*.
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator™ Version 6.0 and above (for configuration)

* **Subject to services and service terms available from your carrier.**

Introduction

D-Link announces a fast, mobile network router which allows you to share a high speed Internet connection virtually anywhere by connecting an UMTS or HSDPA notebook adapter or USB-enable phone. You can get a high speed Internet connection just about anywhere within your wireless broadband network. This router is extremely useful in situations where a wired broadband connection is not available. Quickly set up a Wi-Fi hotspot and provide your workgroup with an Internet connection to check email and browse the web or share file. Maximize your investment in your mobile Internet access subscription by using this router as a fixed broadband Internet solution for the home instead of paying additional fees for cable or DSL.

ADVANCED NETWORK SECURITY

The 3G Mobile Router creates a secure Wi-Fi® network by supporting the latest wireless security features to prevent unauthorized access. Support for WEP, WPA, and WPA2 ensure that you will be able to secure your Wi-Fi network, regardless of your client devices. In addition, the 3G Mobile Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

EASY TO INSTALL AND USE

The D-Link 3G Mobile Router sets up in minutes, making it easy to use while on-the-go. Remaining backward compatible with 802.11b devices, this router ensures that it will work with legacy wireless equipment you already own. This eliminates the necessity of incurring additional expenses with upgrading your current wireless equipment. You can also directly connect Ethernet-based devices to its built-in 4-port full-duplex 10/100 switch.

Set up a wireless network with the D-Link 3G Mobile Router DIR-451 and provide your users with a secure, high-speed connection to the Internet anytime, anywhere*.

* Requires third party mobile Internet access subscription. Check with your service provider for service coverage and applicable fees. D-Link does not guarantee compatibility with all UMTS or HSDPA wireless networks or third party Internet PC cards.

Features

Device Interfaces

- LAN Ethernet Support
 - 4 Port 10/100 Mbps switch
 - Complies with IEEE 802.3u specification
 - Supports Auto-Negotiation
 - Supports Auto-MDI/MDIX
 - Supports IEEE 802.3x Flow Control in Full Duplex mode
- 3G Module Slot
 - Connecting an UMTS or HSDPA Notebook Adapter

Function support

- Network Address Translation
- Stateful Packet Inspection
 - TCP Connection state & sequence number validation
- Virtual Server
 - Virtual Server is used to allow Internet users access to LAN services.
- Port Triggering / Special Applications support
 - Special Application is used to run applications that require multiple connections.
- MAC Address Filtering
 - Apply to WLAN and/or LAN. Select type of filter - Allow list or Deny list 20 Entries.
- DHCP Server
 - Set up as a DHCP Server to distribute IP addresses to the LAN.
- DNS Relay
 - WAN DNS Servers if available OR DNS requests directed to the Gateway IP address.
- Access Control
 - Allow Policy Based on Schedule & IP Address
 - Allow all WEB access OR Allow access to a specified list of domain names (40 Domains)

- Web base setup wizard
 - Step by step setting procedure
- L2TP Pass Through
- PPTP Pass Through
- IPsec Pass Through

CONFIGURATION & ADMINISTRATION

- Web based interface
- Web Based Configuration Wizard
- Dynamic DNS
- E-mail Reporting
- Statistics
- Firmware upgrade
- Current Time & Daylight savings adjustment
- Configuration Save & Restore
- Remote management
- Device Manager

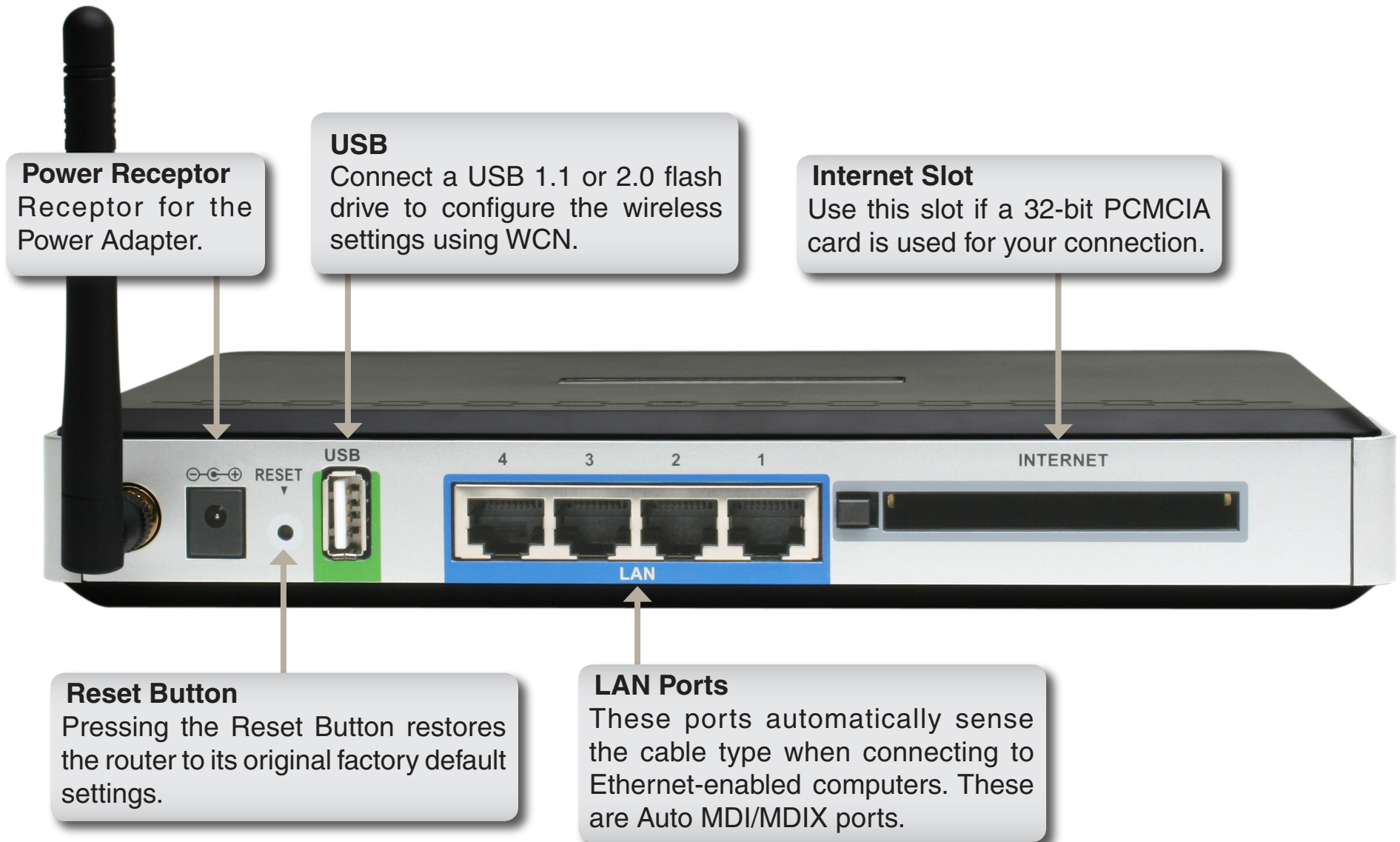
WIRELESS FEATURES

- SuperG & Turbo (108 Mbps) modes
- Wireless Security:
 - WEP 64/128 bit
 - WPA
 - WPA-PSK
- Channel Select
- SSID Broadcast
- Tx Power Adjust
- WMM
- WCN 1.0

* 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



Hardware Overview

LEDs

WAN LED

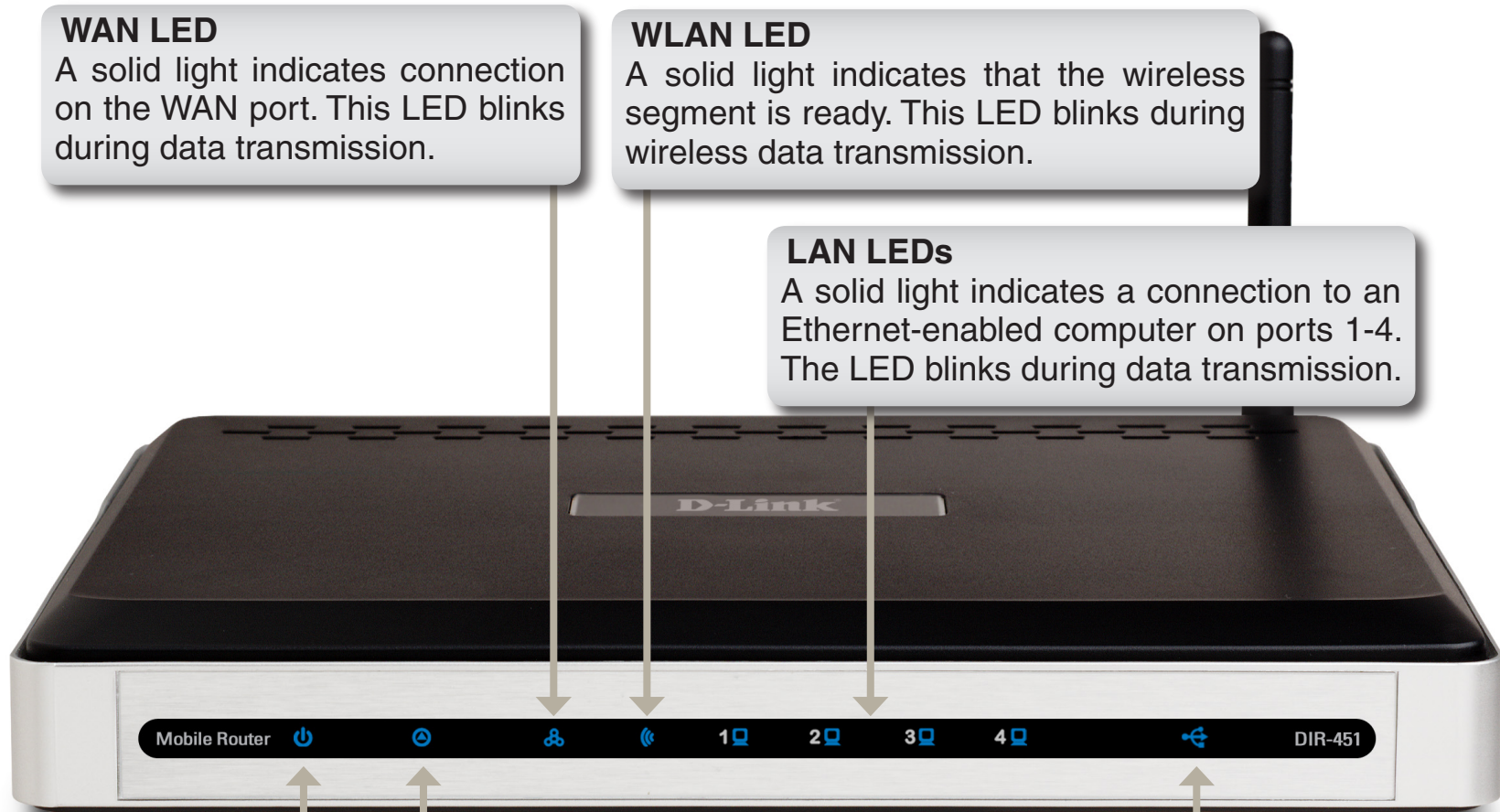
A solid light indicates connection on the WAN port. This LED blinks during data transmission.

WLAN LED

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

LAN LEDs

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



Power LED

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

Status LED

A blinking blue light indicates that the DIR-451 is functioning properly.

USB LED

Insert a USB flash drive with WCN information. The LED will blink 3 times if it successfully transfers the wireless settings.

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.

Connect to your Network

Note: Ensure that the power to your DIR-451 Mobile Router is not connected before performing the installation steps below.

32-bit PCMCIA (UMTS or HSDPA) Card Connection

Note: To preserve the life of your phone's battery, it is recommended that you use your phone's charging cradle when connected to the DIR-451 Mobile Router.

1. Attach the antenna.
 - a. Remove the antenna from its plastic wrapper.
 - b. Screw the antenna in a clockwise direction to the back panel of the unit.
 - c. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.
2. Insert your wireless 32-bit PCMCIA (UMTS or HSDPA) card into the internet 32-bit PCMCIA Card Slot.
3. Insert the Ethernet cable into LAN Port 1 on the back panel of the DIR-451 Mobile Router, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.

Note: The DIR-451 Mobile Router LAN Ports are "Auto-MDI/MDIX." This provides either patch or crossover Ethernet cable LAN Port access.

4. Connect the power adapter to the receptor on the back panel of your DIR-451 Mobile Router. Then plug the other end of the power adapter into the wall outlet or power strip.
 - a. The Power LED will turn ON to indicate power has been applied.
 - b. Other LEDs will flash ON and OFF as the DIR-451 Mobile Router performs initialization and Internet connection processes. This will take a few minutes.
 - c. When complete, the following LEDs will illuminate blue: Power, Status, WAN, WLAN, and LAN Port 1 (or your specific LAN Port connection).

Wireless Installation Considerations

The D-Link mobile 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:

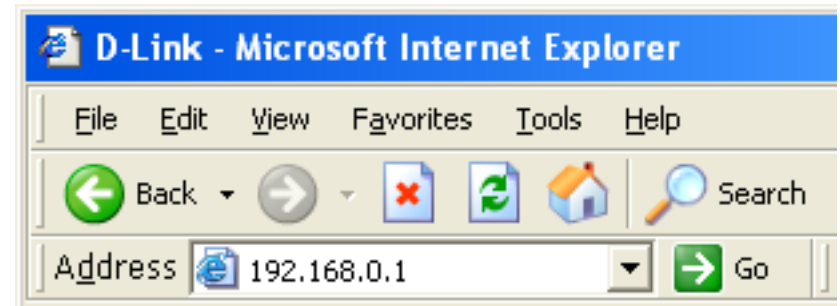
1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between 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.

Configuration

This section will show you how to configure your new D-Link mobile 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).



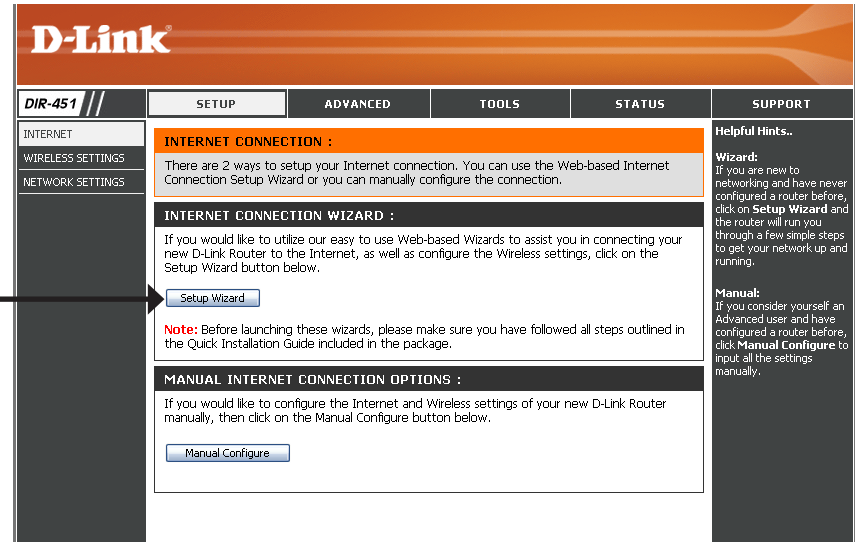
Type **admin** for the username and leave the password blank.



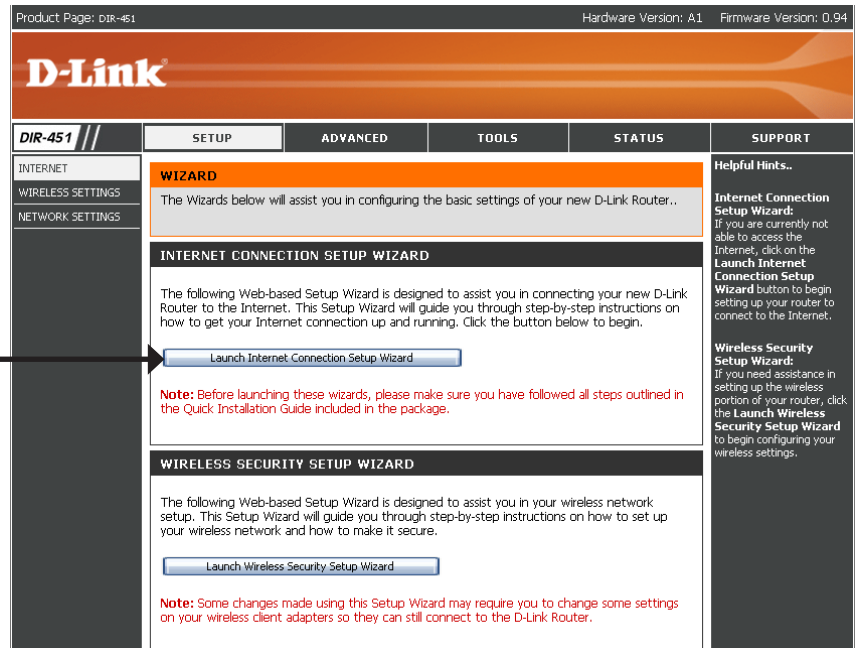
If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.

Setup Wizard

You may run the setup wizard to quickly setup your router. Click **Setup Wizard** to launch the wizard.

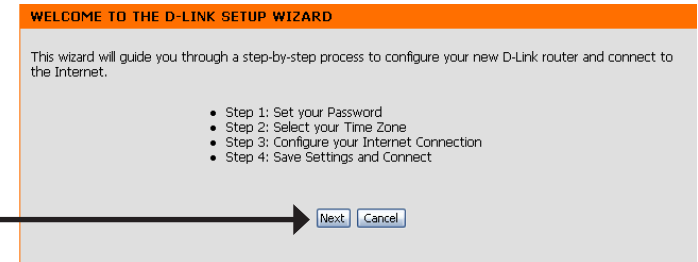


Click **Launch Internet Connection Setup Wizard** to begin.



Click **Next** to continue.

Click **Next**



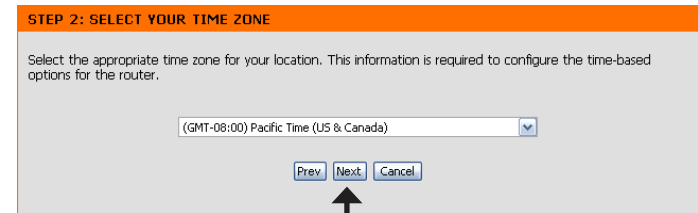
Create a new password and then click **Next** to continue.

Click **Next**



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

Click **Next**



Select the Country, ISP and Card from the drop-down list and then click **Username / Password Connection (WWAN)**. Click **Next** to continue.

Click **Next**

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Your Internet Connection could not be detected, please select your Internet Service Provider (ISP) from the list below.

Country - ISP - Card List
 Indonesia -- Select your ISP -- -- Select your card --

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

Username / Password Connection (WWAN)
 Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this connection type of connection.

Prev Next Cancel

Enter your WWAN user name, password, and server information. If you do not have this information, please contact your ISP. For other information, you can look at the *UMTS/HSDPA Setup* section on the next page.

Click **Next**

SET USERNAME AND PASSWORD CONNECTION (WWAN)

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

WWAN User Name : ISPDA@CINGULARGPRS.COM (optional)
 WWAN Password : (optional)
 WWAN Verify Password : (optional)
 WWAN Server Name : (optional)
 WWAN Dial Number : *99***1#
 WWAN APN : isp.cingular

Auto-Reconnect : Enabled Disabled
 Keep-alive Interval : 60 (seconds)
 Keep-alive Server 1 : (optional)
 Keep-alive Server 2 : (optional)

Prev Next Cancel

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

Click **Continue**

SETUP COMPLETE!

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

Prev Connect Cancel

UMTS/HSDPA Setup

Country-ISP-Card: This will divide connection into following three types.
Country: Select the card issue country from the first drop-down menu.
ISP: Select the card issue provider from the second drop-down menu.
Card: Select the card name from the third drop-down menu.

User Name: Enter your username for your UMTS/HSDPA connection.

Password: Enter your Password for your UMTS/HSDPA connection.

Retype Password: Enter your Password again for confirmation.

Server Name: Enter the name of your network server (optional).

Dial Number: The default is *99***1#. This field should not be altered except when required by your service provider.

APN: Enter the access point name (APN).

Auto-Reconnect: Select Enable to have the router automatically reconnect to the Internet if the connection is dropped.

Keep Alive Interval: Enter the time to send keep alive package. If user does not input any keep alive sever at below, it will keep send keep alive package to the default server. (www.dlinkdns.com, ntp1.dlink.com, www.dlink.com, www.dlink.com, www.d-link.com.tw). If all servers fail to response, the 3G router will hang up 3G connection and re-dial to carrier/operation.

Keep Alive Servers: Enter the IP address(es) of keep alive server(s). If user inputs keep alive servers, this router will send keep alive package to those servers. If those servers fail to response, the 3G router will hang up 3G connection and re-dial to carrier/operation.

The screenshot shows the D-Link DIR-451 wireless settings page. The main content area is titled "INTERNET CONNECTION" and contains the following fields and options:

- INTERNET CONNECTION TYPE :** Choose the mode to be used by the router to connect to the Internet. My Internet Connection is: **WWAN** (dropdown menu).
- WWAN :** Enter the information provided by your Internet Service Provider (ISP).
 - Country - ISP - Card : USA (dropdown), Cingular (dropdown), Sierra Wireless AirCard 860 (dropdown)
 - User Name : ISPDA@CINGULARGPRS.COM (optional)
 - Password : [masked] (optional)
 - Retype Password : [masked] (optional)
 - Server Name : [text field] (optional)
 - Dial Number : *99***1#
 - APN : isp.cingular
 - Auto-Reconnect : Enabled Disabled
 - Keep-alive Interval : 60 (seconds)
 - Keep-alive Server 1 : [text field] (optional)
 - Keep-alive Server 2 : [text field] (optional)

On the right side, there is a "Helpful Hints..." section with "WWAN:" and "Support:" information.

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-451. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. The **Auto Channel Scan** setting can be selected to allow the DIR-451 to choose the channel with the least amount of interference.

Super G Mode: Super G is a group of performance enhancement features that increase end user application throughput in an 802.11g network. Super G is backwards compatible to standard 802.11g devices. For top performance, all wireless devices on the network should be Super G capable. Select either **Disabled**, **Super G without Turbo**, or **Super G with Dynamic Turbo**.

- **Disabled** - Standard 802.11g support, no enhanced capabilities.
- **Super G without turbo** - Capable of Packet Bursting, FastFrames, Compression, but no Turbo mode.
- **Super G with Dynamic Turbo** - Capable of Packet Bursting, FastFrames, Compression, and Dynamic Turbo. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are Super G with Dynamic Turbo enabled.

The screenshot displays the D-Link DIR-451 web interface for wireless settings. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar shows 'INTERNET', 'WIRELESS SETTINGS', and 'NETWORK SETTINGS'. The main content area is titled 'WIRELESS NETWORK' and contains the following 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.
 - Buttons: Save Settings, Don't Save Settings
- WIRELESS NETWORK SETTINGS :**
 - Enable Wireless :
 - Wireless Network Name : (Also called the SSID)
 - Wireless Channel : (dropdown)
 - Enable Auto Channel Scan :
 - Super G Mode : (dropdown)
 - Enable Extended Range Mode :
 - 802.11g Only Mode :
 - Visibility Status : Visible Invisible
- WIRELESS SECURITY MODE :**
 - Security Mode : (dropdown)

Helpful Hints... on the right side:

- Wireless Network Name:** 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.
- Auto Channel:** 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.
- Visibility Status:** Visibility Status is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router,

Extended Range Mode: Extended Range Mode helps reduce dead spots by improving the reception algorithm, which allows your wireless clients to associate with the DIR-451 at farther distances. Select either **Enabled** or **Disabled**.

802.11g Only Mode: Enable this mode if your network is made up of purely 802.11g devices. If you have both 802.11b and 802.11g wireless clients, uncheck the box.

Visibility status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-451. If Invisible is selected, the SSID of the DIR-451 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-451 in order to connect to it.

Please refer to **Section 4 - Wireless Security** for information on setting up security and encryption.

Network Settings

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

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.

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

Local Domain: Enter the Domain name (Optional).

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

Refer to the next page for DHCP information.

Product Page: DIR-451
Hardware Version: A1
Firmware Version: 0.94

D-Link

DIR-451
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT

INTERNET

WIRELESS SETTINGS

NETWORK 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 :

Default Subnet Mask :

Local Domain Name :

Enable DNS Relay :

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 : Computer Name

IP Address : 192 . 168 . 0 .

MAC Address : - - - - -

DHCP RESERVATIONS LIST :

Enable	Computer Name	MAC Address	IP Address
<input type="checkbox"/>			

DYNAMIC DHCP CLIENT LIST :

Host Name	IP Address	MAC Address
msimaster	192.168.0.100	00:11:09:2a:94:11

Helpful Hints..

DHCP Server:
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.

DHCP Reservation:
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-451 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-451. 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 the 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.

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

DHCP SERVER SETTINGS :			
Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.			
Enable DHCP Server :	<input checked="" type="checkbox"/>		
DHCP IP Address Range :	100 to 200 (addresses within the LAN subnet)		
DHCP Lease Time :	10080 (minutes)		
ADD DHCP RESERVATION :			
Enable :	<input type="checkbox"/>		
Computer Name :	<input type="text"/> << Computer Name ▾		
IP Address :	192 . 168 . 0 . <input type="text"/>		
MAC Address :	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>		
DHCP RESERVATIONS LIST :			
Enable	Computer Name	MAC Address	IP Address
DYNAMIC DHCP CLIENT LIST :			
Host Name	IP Address	MAC Address	
171	192.168.0.100	00:0c:f1:fa:6d:5b	

Virtual Server

This will allow you to open and redirect a single port.

Rule: Check the box to enabled the rule.

Name: Enter a name for the rule. You may select an application from the drop-down menu and click << to fill in the fields automatically.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. You may select a computer from the drop-down menu and click <<.

Public Port/ Private Port: Enter the port that you want to open. In most cases, the public and private will be the same port.

Traffic Type: Select **TCP**, **UDP**, or **ANY**.

Schedule: Select Always or a created schedule from the drop-down menu.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

VIRTUAL SERVER RULES :

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

20 - VIRTUAL SERVER RULES

			Port	Traffic Type	Schedule
<input type="checkbox"/>	Name [] << Application Name [v]	IP Address 0.0.0.0 << Computer Name [v]	Public 0	TCP [v]	Always [v]
<input type="checkbox"/>	Name [] << Application Name [v]	IP Address 0.0.0.0 << Computer Name [v]	Public 0	TCP [v]	Always [v]
<input type="checkbox"/>	Name [] << Application Name [v]	IP Address 0.0.0.0 << Computer Name [v]	Public 0	TCP [v]	Always [v]
<input type="checkbox"/>	Name [] << Application Name [v]	IP Address 0.0.0.0 << Computer Name [v]	Public 0	TCP [v]	Always [v]
<input type="checkbox"/>	Name [] << Application Name [v]	IP Address 0.0.0.0 << Computer Name [v]	Public 0	TCP [v]	Always [v]
<input type="checkbox"/>	Name [] << Application Name [v]	IP Address 0.0.0.0 << Computer Name [v]	Public 0	TCP [v]	Always [v]

Helpful Hints..

Application Names: 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.

Computer Names: 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.

Schedules: 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.

Rule: Check the box to enabled the rule.

Name: Enter a name for the rule. You may select an application from the drop-down menu and click << to fill in the fields automatically.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. You may select a computer from the drop-down menu and click <<.

Start Port/ Enter the range of ports that you want to open.

End Port: If you want to open 1 port, enter the same port in both boxes.

Traffic Type: Select **TCP**, **UDP**, or **ANY**.

Schedule: Select Always or a created schedule from the drop-down menu.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

20- PORT FORWARDING RULES

	Name	IP Address	Start	End	Traffic Type	Schedule
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always
<input type="checkbox"/>	<input type="text"/> << Application Name	<input type="text"/> << Computer Name	<input type="text"/> 0	<input type="text"/> 0	TCP	Always

Helpful Hints..

Application Names: 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.

Computer Names: 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.

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

Port Ranges: This feature allows you to open a range of ports to a computer on your network. To do so, enter the first port in the range you would like to open in the **Start** field and last port of the range in the **End** field.

Single Ports: To open a single port using this feature, simply enter the same number in both the **Start** and **End** fields.

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-451.

Rule: Check the box to enabled the rule.

Name: Enter a name for the rule.

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

Firewall Port: This is the port number on the WAN 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 **TCP**, **UDP**, or **ANY**.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

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

20 -APPLICATION RULES

			Port	Traffic Type
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger 0 - 0 Firewall <input type="text"/>	Any
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger 0 - 0 Firewall <input type="text"/>	Any
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger 0 - 0 Firewall <input type="text"/>	Any
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger 0 - 0 Firewall <input type="text"/>	Any
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger 0 - 0 Firewall <input type="text"/>	Any

Helpful Hints..

Application Name: 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.

Network Filter

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

Configure MAC Filter: 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 on the network.

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.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

MAC FILTERING :

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

Save Settings Don't Save Settings

20 - MAC FILTERING RULES

Configure MAC Filtering below:
Turn MAC Filtering OFF

MAC Address		DHCP Client List	
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR
00-00-00-00-00-00	<<	Computer Name	CLEAR

Helpful Hints..

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

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

Clearing an Entry: Click the CLEAR button to remove the MAC address from the MAC Filtering list.

Website Filter

URL and domain blocking 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 **Apply**. The text to be blocked will appear in the list. To delete the text, just highlight it and click **Delete**.

Configure Website Filter: Select **Turn Website Filtering OFF**, **Turn Website Filtering ON** and **ALLOW** computers access to **ONLY** these sites, or **Turn Website Filtering ON** and **DENY** computers access to **ONLY** these sites.

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.

Clear the List Below: Click to remove all the entries.

The screenshot shows the D-Link DIR-451 Advanced Settings page. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various settings categories, with 'WEBSITE FILTER' selected. The main content area is titled 'WEBSITE FILTERING RULES :'. It contains a description of the feature and two buttons: 'Save Settings' and 'Don't Save Settings'. Below this, there is a section titled '40 - WEBSITE FILTERING RULES' with a dropdown menu set to 'Turn Website Filtering OFF' and a 'Clear the list below...' button. At the bottom, there is a table with two columns, both labeled 'Website URL/Domain', containing 10 empty input fields for adding rules.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 //

SETUP ADVANCED TOOLS STATUS SUPPORT

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

WEBSITE FILTERING RULES :

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.

Save Settings Don't Save Settings

40 - WEBSITE FILTERING RULES

Configure Website Filtering below:

Turn Website Filtering OFF

Clear the list below...

Website URL/Domain	Website URL/Domain

Helpful Hints..

Website Filtering:
Create a list of Websites that you would like the devices on your network to be allowed or denied access to.

Keywords:
Keywords can be entered in this list in order to block any URL containing the keyword entered.

Firewall Settings

This section will allow you to setup a DMZ host and to enable VPN passthrough.

If you have a client PC that cannot run Internet applications properly from behind the DIR-451, then you can set the client up for unrestricted Internet access. It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP address of the internal computer that will be the DMZ host. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

Enable DMZ Host: Check this box to enable DMZ.

DMZ IP Address: Enter the IP address of the computer you would like to open all ports to.

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

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

Enable IPsec Passthrough: Check this box to allow IPsec VPN traffic to pass through the router.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // 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

VPN PASSTHROUGH :

Enable PPTP Passthrough :

Enable L2TP Passthrough :

Enable IPsec Passthrough :

Helpful Hints..

DMZ:
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.

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

Support:
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**.

Transmit Power: Set the transmit power of the antennas.

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 2346. 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 (Wi-Fi Multimedia) is QoS (Quality of Service) for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451

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

Transmit Power : 100%

Beacon interval : 100 (msec, range:25~1000, default:100)

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

Fragmentation : 2346 (range: 256~2346, default:2346, even number only)

DTIM interval : 3 (range: 1~255, default:3)

Preamble Type : Short Preamble Long Preamble

WMM Function : Disable Enable

Helpful Hints..

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

WAN Ping: Unchecking the box will not allow the DIR-451 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the WAN port to be “pinged”.

Multicast streams: Check the box to allow multicast traffic to pass through the router from the Internet.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // 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 :

MULTICAST STREAMS :
Enable Multicast Streams:

Helpful Hints..
WAN Ping Respond: 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.
Gaming Mode: Gaming Mode should be used when you are playing games on the Internet from behind the router.
Multicast Streams: 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 and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

Administrator Login Name: Enter a new Login Name for the Administrator account.

Administrator Password: Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

Remote Management: Remote management allows the DIR-451 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: The Internet IP address of the computer that has access to the Broadband Router. If you input an asterisk (*) into this field, then any computer will be able to access the Router. Putting an asterisk (*) into this field would present a security risk and is not recommended.

Port: The port number used to access the DIR-451.
Example: http://x.x.x.x:8080 whereas x.x.x.x is the WAN IP address of the DIR-451 and 8080 is the port used for the Web-Management interface.

The screenshot shows the D-Link DIR-451 web management interface. The top navigation bar includes 'DIR-451', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various settings categories: ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES, LOG SETTINGS, SYSLOG, and EMAIL SETTINGS. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains the following sections:

- ADMINISTRATOR SETTINGS :** A message states: "There is no password for this router by default. To help secure your network, we recommend that you should choose a new password." Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.
- ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "ADMIN") :** This section contains three password fields: 'Login name :', 'New Password :', and 'Confirm Password :', each with a masked input field.
- REMOTE MANAGEMENT :** This section includes an 'Enable Remote Management' checkbox, an 'IP Address' input field (containing an asterisk '*'), and a 'Port' dropdown menu (set to 80).

On the right side of the interface, there is a 'Helpful Hints..' section with two sub-sections:

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

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.

Automatic: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. This field is optional.

Manual: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second. Click **Set Time**. You can also click **Copy Your Computer's Time Settings**.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSTEM
FIRMWARE
DDNS
SYSTEM CHECK
SCHEDULES
LOG SETTINGS
SYSLOG
EMAIL SETTINGS

TIME :
Time Configuration

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 NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.

Save Settings Don't Save Settings

TIME CONFIGURATION :

Time : **Wed Dec 31 16:22:27 std 1969 (GMT -08:00)**
Time Zone : (GMT-08:00) Pacific Time (US & Canada) [v]
Enable Daylight Saving :

Month Day
DST Start Jan 01
DST End Jan 01

AUTOMATIC TIME CONFIGURATION :

Enable NTP server :
NTP Server Used : [] << Select NTP Server [v]

SET THE DATE AND TIME MANUALLY :

Current Gateway Time :

Year 2002 Month Jan Day 01
Hour 00 Minute 00 Second 00 AM [v]
Copy Your Computer's Time Settings

Helpful Hints..
Time Settings:
If you plan on using the scheduling feature of this router, then making sure the time is correct is extremely important. Either enter the time manually by clicking the **Copy Your Computer's Time Settings** button, or use the **Automatic Time Configuration** option to have your router synchronize with a time server on the Internet.

System Settings

Save Settings to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** 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 **Load** button to transfer those settings to the router.

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

Reboot: Click to reboot the router.

The screenshot shows the D-Link DIR-451 web interface. At the top, it displays 'Product Page: DIR-451', 'Hardware Version: A1', and 'Firmware Version: 0.94'. The D-Link logo is prominently displayed. Below the logo is a navigation menu with tabs for 'DIR-451', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SYSTEM SETTINGS' section is highlighted in orange. It contains the following text and controls:

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

SYSTEM SETTINGS :

- Save Settings To Local Hard Drive :
- Load Settings From Local Hard Drive :
- Restore To Factory Default Settings :
- Reboots the DIR-451 :

On the right side, under 'Helpful Hints..', there is a section titled 'Saving System Settings:' with the following text: 'Once your router is configured they way you want it, you can save these settings to a configuration file that can later be loaded in the event that the router's default settings are restored. To do this, click the **Save** button next to where it says Save Settings to Local Hard Drive.'

Firmware Upgrade

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.

Firmware Upgrade: Click on the link in this screen to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Browse: After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive. Click **Save Settings** to complete the firmware upgrade.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADMIN
TIME
SYSTEM
FIRMWARE
DDNS
SYSTEM CHECK
SCHEDULES
LOG SETTINGS
SYSLOG
EMAIL SETTINGS

FIRMWARE UPGRADE :

There may be new firmware for your DIR-451 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 below to start the firmware upgrade.

Save Settings Don't Save Settings

CURRENT FIRMWARE INFO :

Current Firmware Version 0.94
Firmware Date Thu, 10 Aug 2006

Browse...

Helpful Hints..

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

DDNS

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

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

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

Username: Enter the Username for your DDNS account.

Password: Enter the Password for your DDNS account.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

D-Link

DIR-451 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADMIN
TIME
SYSTEM
FIRMWARE
DDNS
SYSTEM CHECK
SCHEDULES
LOG SETTINGS
SYSLOG
EMAIL 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-451, you can setup your DDNS service and the DIR-451 will automatically update your DDNS server every time it receives a new WAN IP address.

Save Settings Don't Save Settings

DDNS SETTINGS :

Enable DDNS :

Server Address : DynDns.org

Host Name :

Username :

Password :

Helpful Hints..

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

System Check

Virtual Cable Tester (VCT) Info: VCT is an advanced feature that integrates a LAN cable tester on every Ethernet port on the router. Through the graphical user interface (GUI), VCT can be used to remotely diagnose and report cable faults such as opens, shorts, swaps, and impedance mismatch. This feature significantly reduces service calls and returns by allowing users to easily troubleshoot their cable connections.

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**.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

The screenshot shows the D-Link DIR-451 web interface. The top navigation bar includes 'DIR-451', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'TOOLS' tab is selected, displaying the 'FAST ETHERNET VIRTUAL CABLE TESTER (VCT)'. Below this, the 'VCT INFO' section contains a table with the following data:

Ports	Link Status
LAN1	Disconnected, No cable detected
LAN2	Connected, 100Mbps, full-duplex
LAN3	Disconnected, No cable detected
WAN	Disconnected, No cable detected

Below the table is the 'PING TEST' section, which includes a text box for 'Host Name or IP Address' and a 'Ping' button. The 'PING RESULT:' section shows the following output:

```

PING 192.168.0.1 (192.168.0.1): 56 data bytes
Ping 192.168.0.1: icmp_seq=0 ttl=64 time=0.9 ms
Ping 192.168.0.1: icmp_seq=1 ttl=64 time=0.7 ms
Ping 192.168.0.1: icmp_seq=2 ttl=64 time=0.7 ms
Ping 192.168.0.1: icmp_seq=3 ttl=64 time=0.7 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 0% packet loss
round-trip min/avg/max = 0.7/0.7/0.9 ms

```

Schedules

Name: Enter a name for your new schedule.

Day(s): 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.

The screenshot displays the configuration page for the D-Link DIR-451. At the top, it shows 'Product Page: DIR-451', 'Hardware Version: A1', and 'Firmware Version: 0.94'. The D-Link logo is prominently displayed. Below the logo is a navigation menu with tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SCHEDULES' section is active, showing a sidebar with a menu of options including ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES (highlighted), LOG SETTINGS, SYSLOG, and EMAIL SETTINGS. The main content area is titled 'SCHEDULES :' and contains the following text: 'The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'ADD SCHEDULE RULE :' section includes a 'Name :' text input field, a 'Day(s) :' section with an 'All Week' checkbox and a day range selector (Sun to Sun), an 'All Day - 24 hrs :' checkbox, and 'Start Time :' and 'End Time :' fields with AM/PM dropdowns and '(hour:minute, 12 hour time)' instructions. The 'SCHEDULE RULES LIST :' section has a table with columns for 'Name :', 'Day(s) :', and 'Time Frame :'. On the right side, there is a 'Helpful Hints..' section with the text: 'Schedules: Define schedules that can later be applied to Virtual Server and Port Forwarding rules.'

Log Settings

Send Email Now: This option will send a copy of the router log to the email address configured in the **Tools > Email Settings** screen. Refer to page 39.

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

Log Type: Check **System Activity** to enable logging.

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 1.01

D-Link

DIR-451 // SETUP ADVANCED **TOOLS** STATUS SUPPORT

ADMIN
TIME
SYSTEM
FIRMWARE
DDNS
SYSTEM CHECK
SCHEDULES
LOG SETTINGS
SYSLOG
EMAIL SETTINGS

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

LOG FILES :
Send Email Now
Save Log File To Local Hard Drive
Log Type System Activity

Helpful Hints..
Emailing the Log:
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.

Syslog

The DIR-451 router keeps a running log of events and activities occurring on the router. You may send these logs to a SysLog server on your network.

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

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

The screenshot displays the D-Link DIR-451 router's configuration interface. The top navigation bar includes 'DIR-451 //', 'SETUP', 'ADVANCED', 'TOOLS' (selected), 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSTEM, FIRMWARE, DDNS, SYSTEM CHECK, SCHEDULES, LOG SETTINGS, SYSLOG (selected), and EMAIL SETTINGS. The main content area is titled 'SYSLOG :' and contains the following text: 'The SysLog options allow you to send log information to a SysLog Server.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'SYSLOG SETTINGS :' section includes an unchecked checkbox for 'Enable Logging To Syslog Server :', a text input field for 'Syslog Server IP Address :', a '<<' button, and a dropdown menu for 'Computer Name'. On the right side, there is a 'Helpful Hints..' section with the text: 'A System Logger (syslog) is a server that collects in one place the logs from different sources. If the LAN includes a syslog server, you can use this option to send the router's logs to that server.'

Email Settings

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

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

From Email Address: This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

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

SMTP Server Address/Name: Enter the SMTP server address for sending email. If your SMTP server requires authentication, select this option.

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

Account Name: Enter your account for sending email.

Password: Enter the password associated with the account.

Confirm Password: Re-type the password associated with the account.

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

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

The screenshot shows the D-Link DIR-451 web interface. The main content area has tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The 'EMAIL SETTINGS' page is active, showing the following options:

- ENABLE :** Enable Email Notification :
- EMAIL SETTINGS :**
 - From Email Address :
 - To Email Address :
 - SMTP Server Address/Name :
 - Enable Authentication :
 - Account Name :
 - Password :
 - Confirm Password :
- EMAIL LOG WHEN ON SCHEDULE :**
 - On Schedule :
 - Schedule :
 - Details :

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

Device Information

This page displays the current information for the DIR-451. It will display the LAN, WAN, and Wireless information.

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, Channel, and Encryption type.

The screenshot shows the D-Link DIR-451 web interface. At the top, it displays 'Product Page: DIR-451', 'Hardware Version: A1', and 'Firmware Version: 0.94'. The D-Link logo is prominently displayed. Below the logo, there is a navigation menu with tabs for 'DIR-451', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'STATUS' tab is selected, and the 'DEVICE INFO' sub-tab is active. The main content area is titled 'DEVICE INFORMATION' and contains the following details:

DEVICE INFORMATION :
All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.
Firmware Version: 0.94 , Thu, 10 Aug 2006

LAN :
MAC Address : 00:00:60:00:00:01
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WAN:
Connection : 3G
Signal Strength :
IP Address : 0.0.0.0
Subnt Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS : 168.95.1.1 168.95.1.2

WIRELESS 802.11G :
SSID : dlink
Channel : 2
Encryption : Disabled

Log

First Page: View the first page of the log.

Last Page: View the last page of the log.

Previous: View the previous page.

Next: View the next page.

Clear: Clear the log.

The screenshot displays the D-Link DIR-451 web interface. At the top, it shows 'Product Page: DIR-451' and 'Hardware Version: A1 Firmware Version: 0.94'. The D-Link logo is prominently displayed. Below the logo, there is a navigation menu with tabs for 'DIR-451 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'STATUS' tab is selected. On the left side, there is a sidebar menu with options: 'DEVICE INFO', 'LOG', 'STATS', and 'WIRELESS'. The 'LOG' option is selected. The main content area shows the 'VIEW LOG' section, which includes a description: 'View Log displays the activities occurring on the DIR-451.' Below this, there is a 'LOG FILES' section with navigation buttons: 'First Page', 'Last Page', 'Previous', 'Next', and 'Clear'. The log shows '0/0' entries. A table header is visible with columns for 'Time' and 'Message'. The message content is 'This Log message is disable.'

Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-451 on both the WAN and the LAN ports. The traffic counter will reset if the device is rebooted.

The screenshot shows the D-Link DIR-451 web interface. The top navigation bar includes 'DIR-451', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar contains 'DEVICE INFO', 'LOG', 'STATS', and 'WIRELESS'. The main content area is titled 'TRAFFIC STATISTICS :'. Below the title, it states: 'Traffic Statistics display Receive and Transmit packets passing through the DIR-451.' There are 'Refresh' and 'Reset' buttons. A table displays the following data:

	Receive	Transmit
WAN	0 packets, 0 bytes	0 packets, 0 bytes
LAN	469 packets, 61723 bytes	1003 packets, 414118 bytes
WIRELESS 11g	9685 packets, 200852 bytes	693 packets, 131912 bytes

Wireless Stats

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 client.

The screenshot shows the D-Link DIR-451 web interface. The top navigation bar includes 'DIR-451', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar contains 'DEVICE INFO', 'LOG', 'STATS', and 'WIRELESS'. The main content area is titled 'CONNECTED WIRELESS CLIENT LIST :'. Below the title, it states: 'The Wireless Client table below displays Wireless clients Connected to the AP (Access Point). to the AP (Access Point).' A table displays the following data:

Connected Time	MAC Address
----------------	-------------

Support

Product Page: DIR-451 Hardware Version: A1 Firmware Version: 0.94

The screenshot displays the D-Link DIR-451 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar contains the following tabs: DIR-451, SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The SUPPORT tab is currently selected. The main content area is titled 'SUPPORT MENU' and is organized into four categories: Setup, Advanced, Tools, and Status. Each category contains a list of links to various configuration and utility pages.

DIR-451	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
MENU	SUPPORT MENU <ul style="list-style-type: none">Setup<ul style="list-style-type: none">InternetWireless SettingsNetwork settingsAdvanced<ul style="list-style-type: none">Virtual ServerPort ForwardingApplication RulesNetwork FilterWebsite FilterFirewall SettingsAdvanced WirelessAdvanced NetworkTools<ul style="list-style-type: none">AdminTimeSystemFirmware UpgradeDDNSSystem CheckSchedulesLog settingsStatus<ul style="list-style-type: none">Device InfoLogStatsWireless				

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-451 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.

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 **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WEP Security**.
3. Next to *Authentication*, select **Open** or **Shared Key**.
4. Select either **64-bit** or **128-bit** encryption from the drop-down menu next to *WEP Encryption*.
5. Next to *Key Type*, select either **Hex** or **ASCII**.
Hex (recommended) - Letters A-F and numbers 0-9 are valid.
ASCII - All numbers and letters are valid.
6. Next to *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.

WEP :

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

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

Authentication :	<input type="text" value="Open"/>
WEP Encryption :	<input type="text" value="64Bit"/>
Key Type :	<input type="text" value="HEX"/>
Default WEP Key :	<input type="text" value="WEP Key 1"/>
WEP Key 1 :	<input type="text" value="0000000000"/>
WEP Key 2 :	<input type="text" value="0000000000"/>
WEP Key 3 :	<input type="text" value="0000000000"/>
WEP Key 4 :	<input type="text" value="0000000000"/>

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.

Configure WPA-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 **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WPA-Personal Security** or **Enable WPA2-Personal Security**.
3. Next to *Cipher Mode*, select **TKIP**, **AES**, or **Auto**.
4. Next to *PSK/EAP*, select **PSK**.
5. Next to *Passphrase*, enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.
6. Enter the passphrase again next to *Confirmed Passphrase*.
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 WPA-PSK (or WPA2-PSK) on your adapter and enter the same passphrase as you did on the router.

WPA-PERSONAL :

WPA-Personal requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

Passphrase :

Confirmed Passphrase :

Configure WPA (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 **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WPA-Personal Security** or **Enable WPA2-Personal Security**.
3. Next to *Cipher Mode*, select **TKIP, AES, or Auto**.
4. Next to *PSK/EAP*, select **EAP**.
5. Next to *RADIUS Server 1* enter the IP Address of your RADIUS server.
6. Next to *Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
7. Next to *Shared Secret*, enter the security key.
8. If you have a secondary RADIUS server, enter its IP address, port, and secret key.
9. Click **Apply Settings** to save your settings.

WPA-PERSONAL :

WPA-Personal requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

802.1X

RADIUS Server 1 : IP

Port

Shared Secret

RADIUS Server 2 : IP

Port

Shared Secret

Connect to a Wireless Network Using Windows Vista™

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

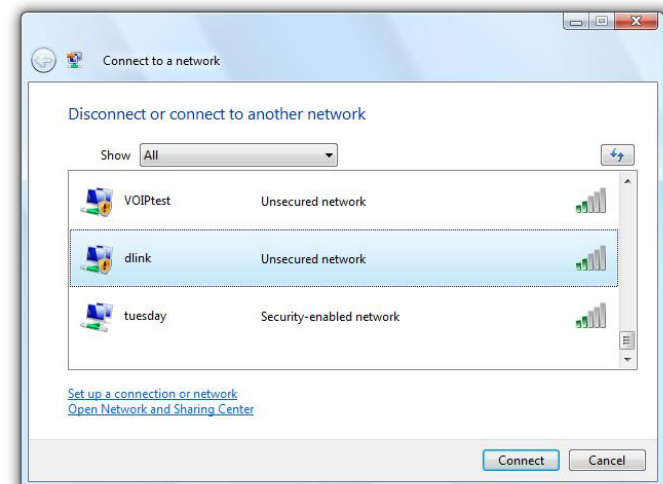
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

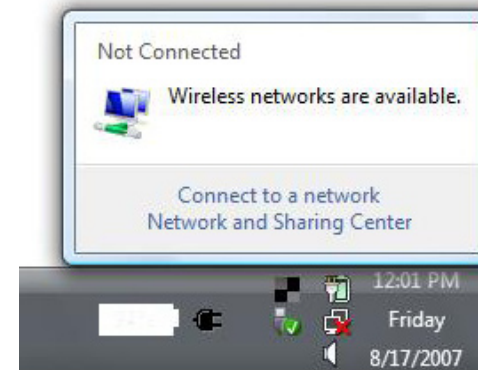
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



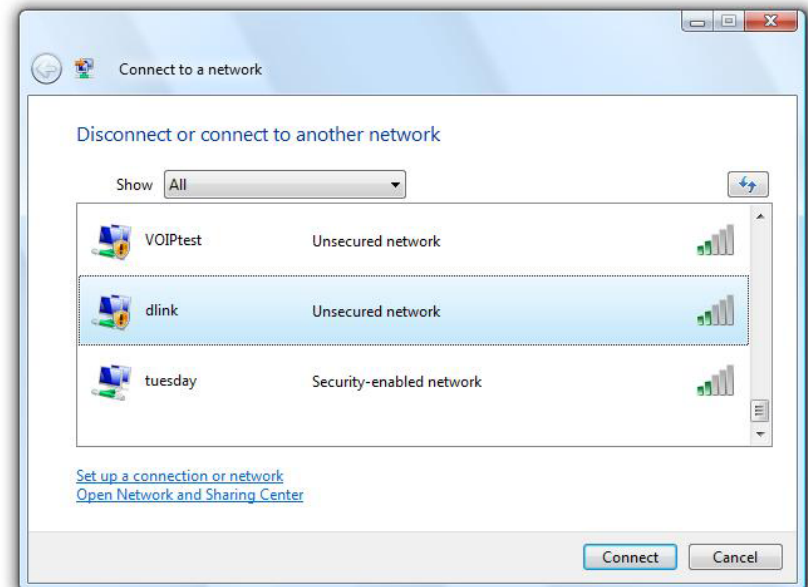
Configure Wireless Security

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

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

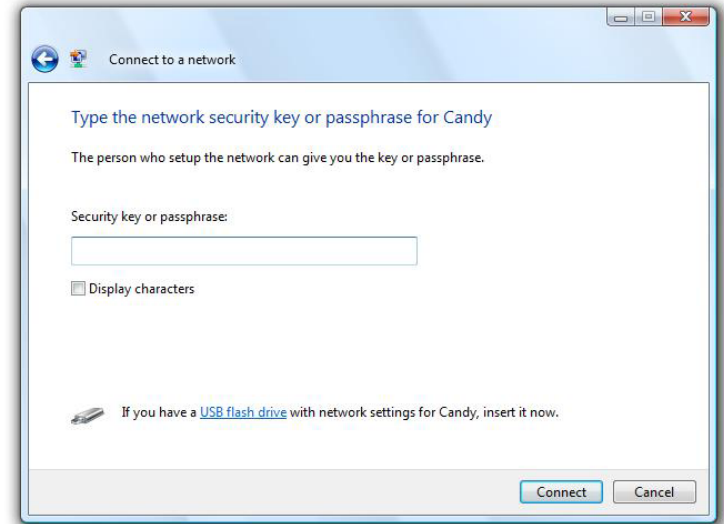


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



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.

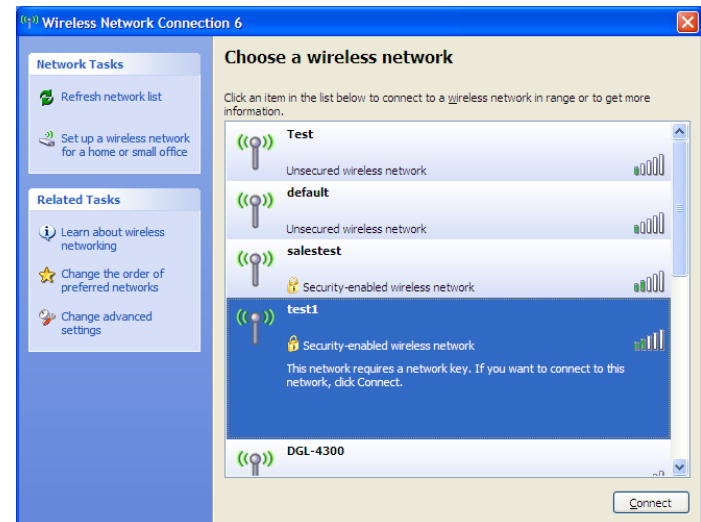
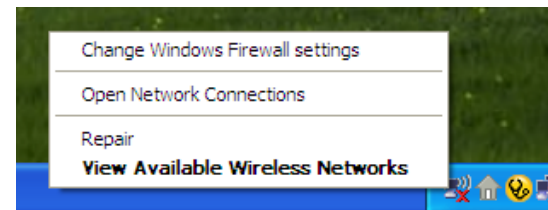
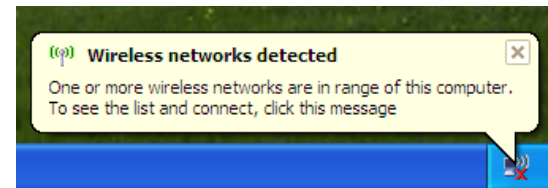
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

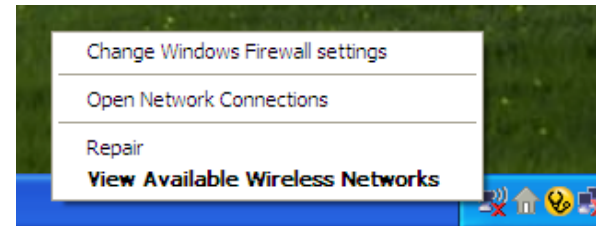
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



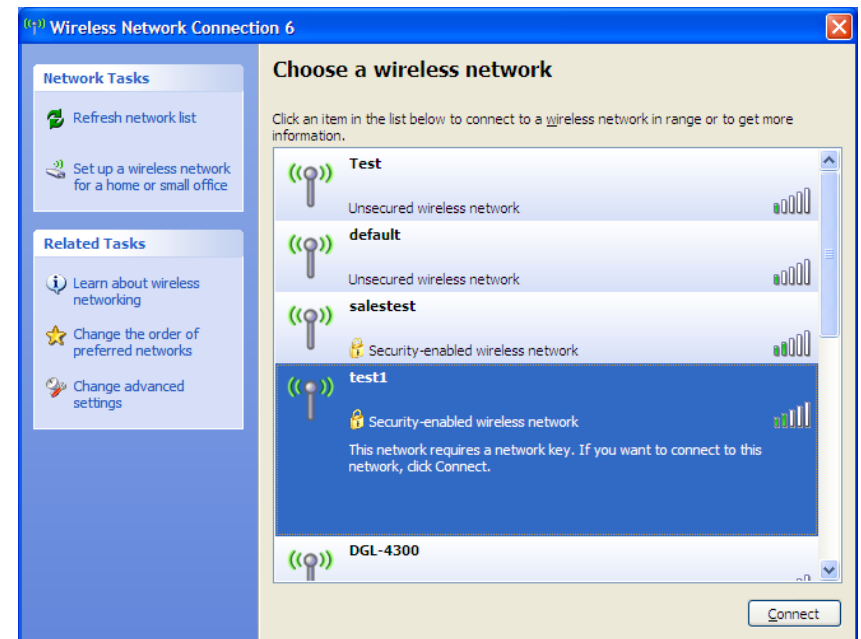
Configure WEP

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**.

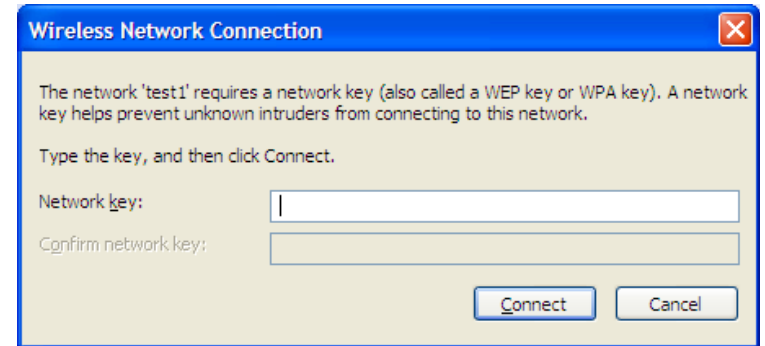


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

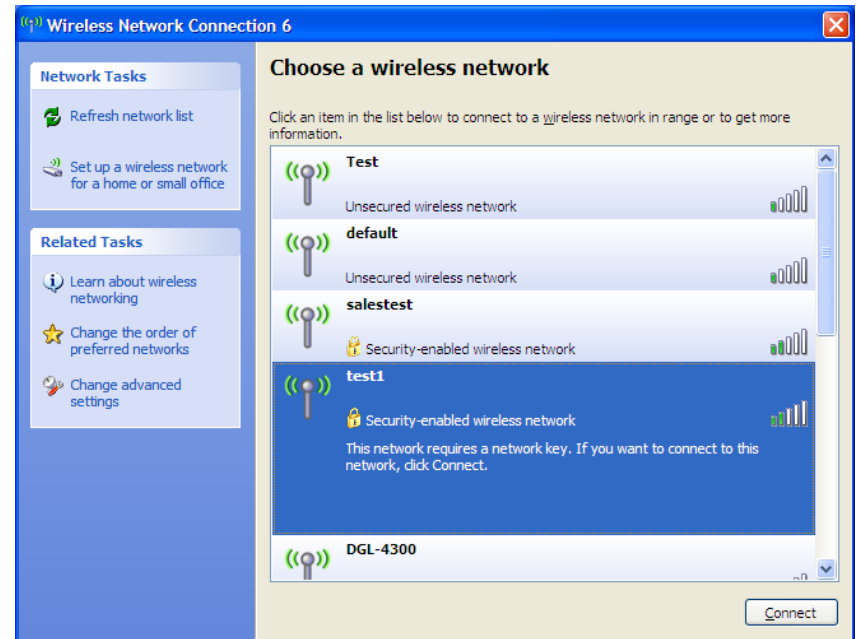
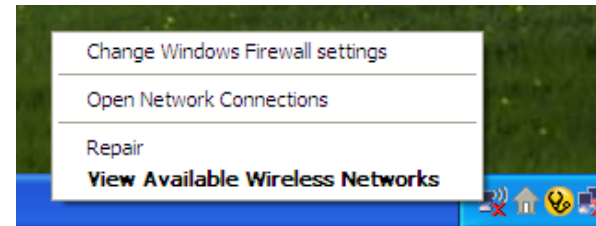
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



Configure WPA-PSK

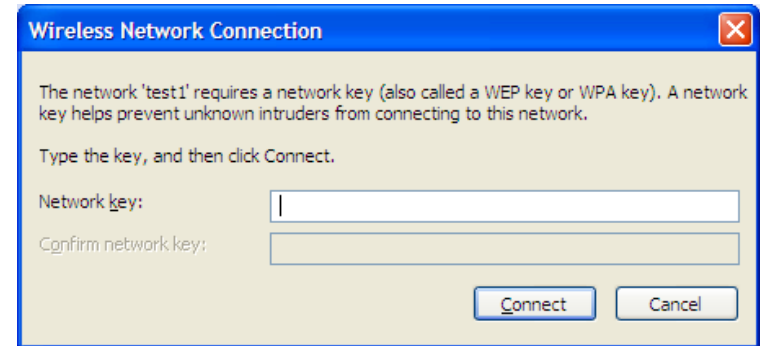
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

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-451. 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
 - 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
 - Firefox 1.5 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.

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.

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 WNA-2330 wireless network Cardbus adapters.

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

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

Networking Basics

Check your IP address

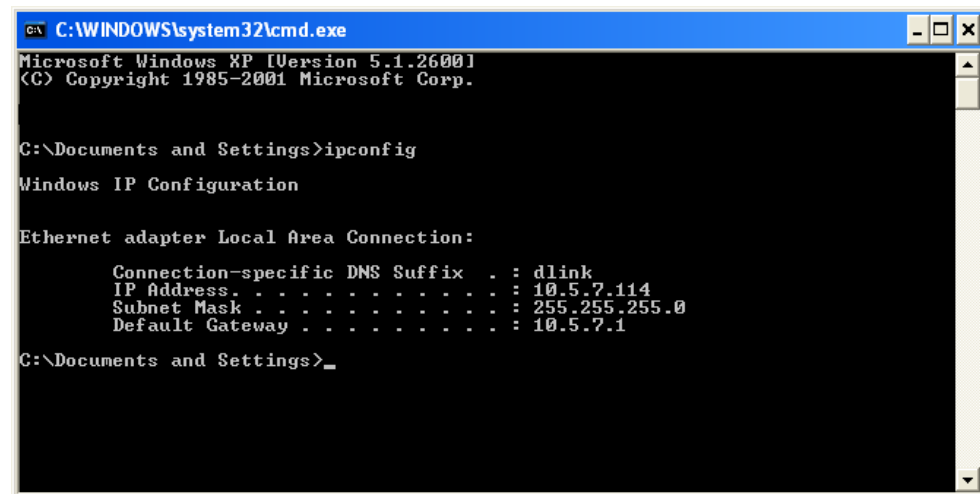
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows® Vista™ users type **cmd** in the **Start Search** box.)

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

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

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



```
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>_
```

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® Vista™ - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**

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

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

Step 2

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

Step 3

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

Step 4

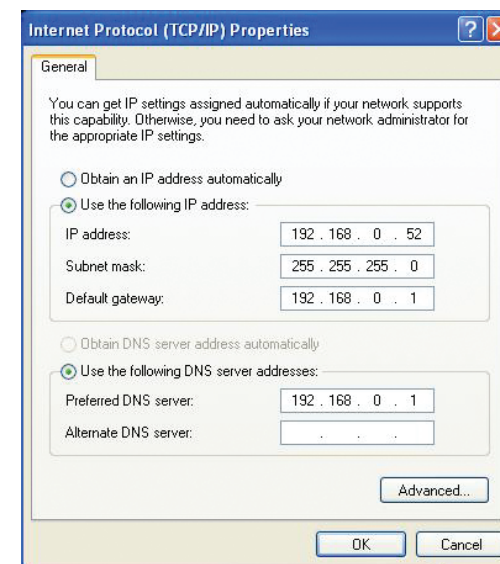
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: 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

Wireless Signal Rates*

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

Security

- WPA - Wi-Fi Protected Access (TKIP, MIC, IV Expansion, Shared Key Authentication)
- 802.1x
- 64/128-bit WEP
- WPA/WPA2
- WPA/PSK
- WPA2/PSK

Modulation Technology

Orthogonal Frequency Division Multiplexing (OFDM)

Receiver Sensitivity

- 54Mbps OFDM, 10% PER,-68dBm)
- 48Mbps OFDM, 10% PER,-68dBm)
- 36Mbps OFDM, 10% PER,-75dBm)

- 24Mbps OFDM, 10% PER,-79dBm)
- 18Mbps OFDM, 10% PER,-82dBm)
- 12Mbps OFDM, 10% PER,-84dBm)
- 11Mbps CCK, 8% PER,-82dBm)
- 9Mbps OFDM, 10% PER,-87dBm)
- 6Mbps OFDM, 10% PER,-88dBm)
- 5.5Mbps CCK, 8% PER,-85dBm)
- 2Mbps QPSK, 8% PER,-86dBm)
- 1Mbps BPSK, 8% PER,-89dBm)

VPN Pass Through/ Multi-Sessions

- PPTP
- L2TP
- IPSec

Device Management

- Web-based Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java-enabled browsers
- DHCP Server and Client

Wireless Frequency Range

2.4GHz to 2.462GHz

Wireless Operating Range

- Indoors - up to 328 ft. (100 meters)
- Outdoors- up to 1312 ft. (400 meters)

Wireless Transmit Power

15dBm ± 2dBm

External Antenna Type

Single detachable reverse SMA

Advanced Firewall Features

- NAT with VPN Pass-through (Network Address Translation)
- MAC Filtering
- URL Filtering
- Domain Blocking
- Scheduling

Operating Temperature

32°F to 131°F (0°C to 55°C)

Humidity

95% maximum (non-condensing)

Safety and Emissions

FCC

LEDs

- Power
- Status
- WAN
- WLAN (Wireless Connection)
- LAN (10/100)
- USB

Dimensions

- L = 5.6 (142mm)
- W = 4.3 (109mm)
- H = 1.2 inches (31mm)

Weight

7.8 oz (0.22kg)

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.

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-451)
- 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) 45-DLink

(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 D-Link 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 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.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Industry Canada 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 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

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 1.3
December 7, 2007