

# USER MANUAL

DIR-320

VERSION 1.00



**D-Link**<sup>®</sup>

**WIRELESS**

# Table of Contents

PACKAGE CONTENTS .....	1	<i>Wi-Fi Protected Setup</i> .....	34
SYSTEM REQUIREMENTS .....	1	<i>Wireless Security - WEP</i> .....	35
FEATURES .....	2	<i>Wireless Security – WPA/EAP</i> .....	36
<b>HARDWARE OVERVIEW</b> .....	<b>3</b>	<i>Wireless Security – WPA/PSK</i> .....	37
<i>LED Indicators</i> .....	4	LAN SETUP .....	38
<b>INSTALLATION</b> .....	<b>5</b>	<i>Router IP Settings</i> .....	39
BEFORE YOU BEGIN.....	5	<i>LAN DHCP Server Settings</i> .....	40
WIRELESS INSTALLATION CONSIDERATIONS .....	6	PRINTER SETUP .....	41
CONNECT TO CABLE/DSL/SATELLITE MODEM .....	7	<i>Printer Setup Wizard</i> .....	41
<b>CONFIGURATION</b> .....	<b>8</b>	TIME AND DATE .....	44
<i>Web-based Configuration Utility</i> .....	8	PARENTAL CONTROL.....	45
CONFIGURE INTERNET CONNECTION - SETUP WIZARD.....	9	ADVANCED SETUP .....	46
<i>Internet Connection Setup Wizard</i> .....	10	<i>Port Forwarding</i> .....	47
CONFIGURE INTERNET CONNECTION – MANUAL SETUP .....	17	<i>Application Rules</i> .....	48
<i>Dynamic IP Address</i> .....	18	<i>Access Control</i> .....	49
<i>Static IP Address</i> .....	19	<i>Firewall &amp; DMZ</i> .....	50
<i>PPPoE</i> .....	20	<i>Advanced Wireless</i> .....	51
<i>PPTP</i> .....	22	<i>Advanced Network</i> .....	53
<i>L2TP</i> .....	24	<i>Routing</i> .....	54
<i>BigPond</i> .....	25	<i>QoS Engine</i> .....	55
<i>PPTP Russia</i> .....	26	<i>Guest Zone</i> .....	56
<i>PPPoE Russia</i> .....	27	<i>Traffic Management</i> .....	58
CONFIGURE WIRELESS CONNECTION - SETUP WIZARD.....	28	MAINTENANCE.....	59
<i>Wireless Connection Setup Wizard</i> .....	29	<i>Device Administration</i> .....	59
WIRELESS CONNECTION – MANUAL SETUP .....	32	<i>Save and Restore</i> .....	60
<i>Wireless Network Settings</i> .....	33	<i>Firmware Update</i> .....	61
		<i>DDNS Setting</i> .....	62

## Table of Contents

---

<i>System Check</i> .....	63
<i>Schedules</i> .....	64
<i>Log Settings</i> .....	65
STATUS .....	66
<i>Device Information</i> .....	66
<i>Log</i> .....	67
<i>Statistics</i> .....	68
<i>Active Session</i> .....	69
<i>Wireless Client List</i> .....	70
<b>TECHNICAL SPECIFICATIONS</b> .....	<b>71</b>

## Package Contents

- DIR-320 Wireless Broadband Router
- Power Adapter
- CD-ROM with User Manual
- One straight-through Ethernet cable
- One Quick Installation Guide

**IMPORTANT:** Using a power supply with a different voltage rating than the one included with the DIR-320 will cause damage and void the warranty for this product.

## System Requirements

- Broadband Internet connection via Cable or ADSL modem
- Computer with:
  - 200MHz Processor
  - 64MB Memory
  - CD-ROM Drive
  - Ethernet Adapter with TCP/IP Protocol Installed
  - Internet Explorer v6 or later, FireFox v1.5
  - Computer with Windows 2000, Windows XP, or Windows Vista



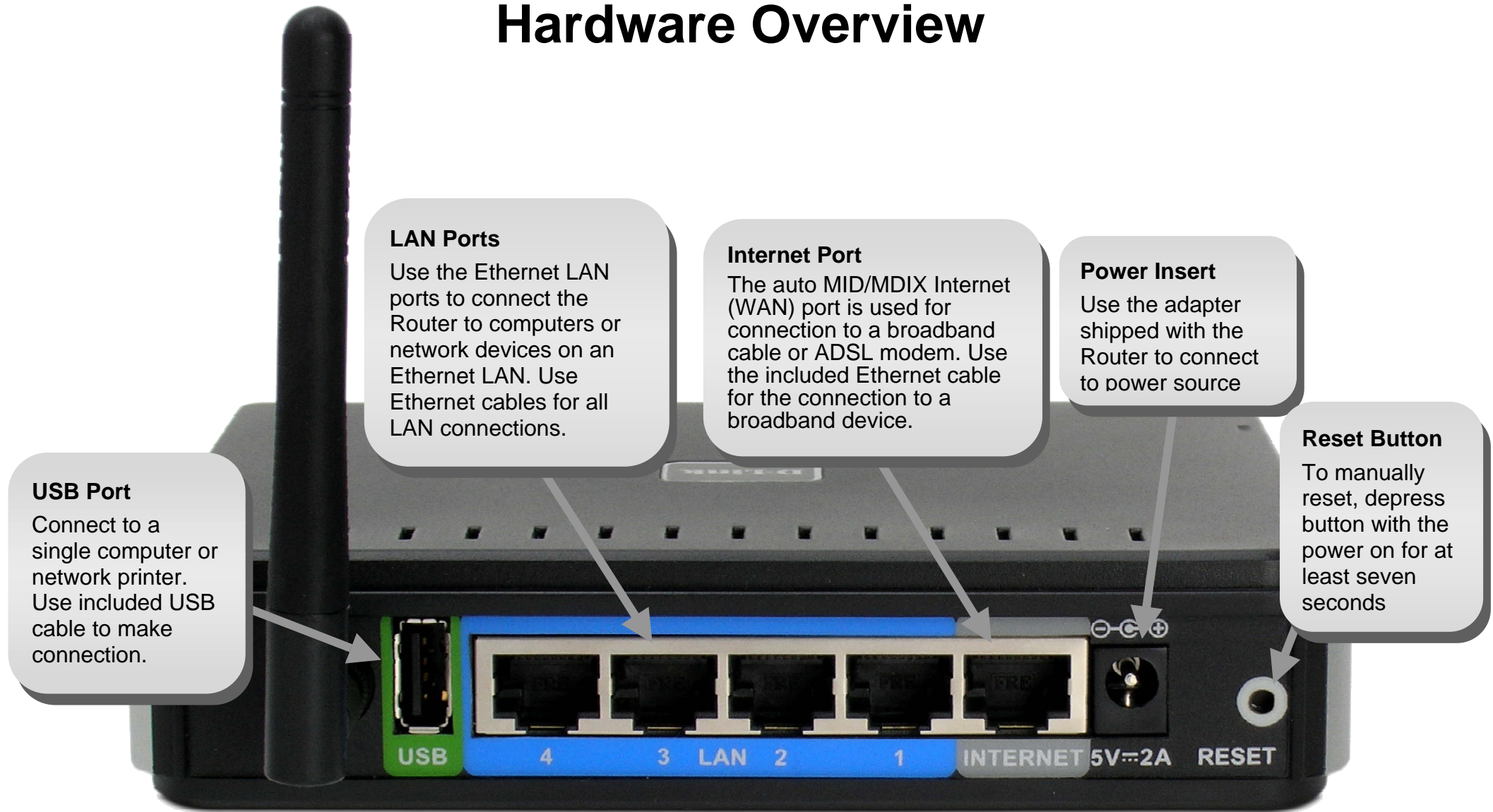


## Features

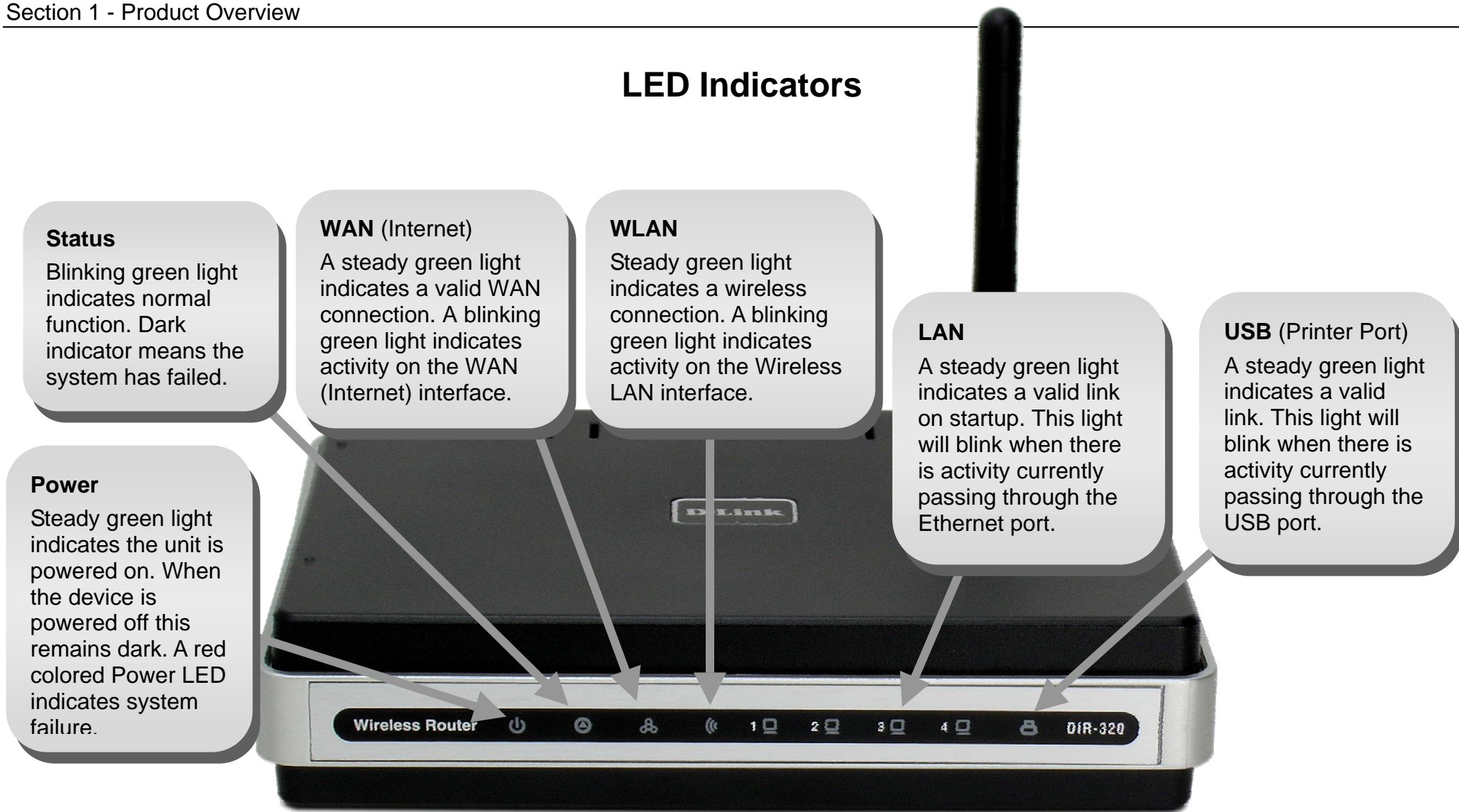
- **Faster Wireless Networking** - The DIR-320 provides up to 54Mbps\* wireless connection with other 802.11g wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11g wireless router gives you the freedom of wireless networking at speeds x faster than 802.11b.
- **Compatible with 802.11b and 802.11g Devices** - The DIR-320 is still fully compatible with the IEEE 802.11b standard, so it can connect with existing 802.11b PCI, USB and FireWire adapters.
- **Advanced Firewall Features** - The Web-based user interface displays a number of advanced network management features including:
  - **Content Filtering** - Easily applied content filtering based on MAC Address, URL, and/or Domain Name.
  - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.
  - **Secure Multiple/Concurrent Sessions** - The DIR-320 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-320 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-320 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.
- **Print Server** – Built-in printer server ideal for network printer sharing. Connect printer directly to the router via USB port. The Print Server Setup Wizard with automatic detection of most USB capable printer makes short work of printer setup for the network.

\*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



## LED Indicators



### Status

Blinking green light indicates normal function. Dark indicator means the system has failed.

### WAN (Internet)

A steady green light indicates a valid WAN connection. A blinking green light indicates activity on the WAN (Internet) interface.

### WLAN

Steady green light indicates a wireless connection. A blinking green light indicates activity on the Wireless LAN interface.

### LAN

A steady green light indicates a valid link on startup. This light will blink when there is activity currently passing through the Ethernet port.

### USB (Printer Port)

A steady green light indicates a valid link. This light will blink when there is activity currently passing through the USB port.

### Power

Steady green light indicates the unit is powered on. When the device is powered off this remains dark. A red colored Power LED indicates system failure.

# Installation

This section will walk you through the installation process. Placement of the Wireless Broadband Router is very important. Do not place the router in an enclosed area such as a closet, cabinet, or in the attic or garage. Place the Wireless Broadband Router in a location where it can be easily connected to Ethernet devices, the telephone line as well as to a power source.

## Before You Begin

Please read and make sure you understand all the prerequisites for proper installation of your new router. Have all the necessary information and equipment on hand before beginning the installation.

### **Operating Systems**

The DIR-320 uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, Windows XP, and Windows Vista.

### **Web Browser**

Any common web browser can be used to configure the router using the web configuration management software. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

### **Ethernet Port (NIC Adapter)**

Any computer that uses the router must be able to connect to it through the Ethernet port on the router. Most notebook computers and fully assembled desktop computers are now sold with an Ethernet port already installed. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the router.

### **Wireless LAN**

Computers using the Wireless network can access the Internet or use the embedded 802.1g wireless access point. Wireless workstations must have an 802.1g or 802.1b wireless network card installed to use the Wireless Broadband Router. In addition the workstations must be configured to operate on the same channel and SSID as the Wireless Broadband Router. If wireless security is used, the wireless workstations must be properly configured for the security settings used.

## Wireless Installation Considerations

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

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

## Connect to Cable/DSL/Satellite Modem

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

1. Place the router in an open and central location. Do not plug the power adapter into the router.
2. Turn the power off on your modem. If there is no on/off switch, then unplug the modem's power adapter. Shut down your computer.
3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the port labeled "Internet" on the router.
4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.
5. Turn on or plug in your modem. Wait for the modem to boot (about 30 seconds).
6. Plug the power adapter to the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot.
7. Turn on your computer.
8. Verify the link lights on the router. The power light, WAN light, and the LAN light (the port that your computer is plugged into) should be lit. If not, make sure your computer, modem, and router are powered on and verify the cable connections are correct.
9. Use the instructions found in this manual to complete the configuration of the router.

# Configuration

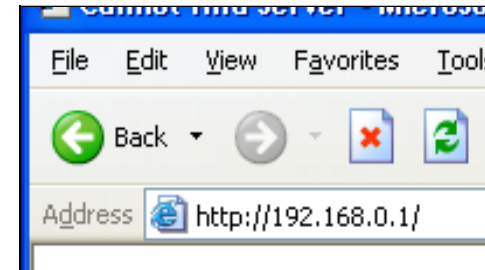
This section will show you how to set up and configure your new D-Link router using the Web-based configuration utility.

## Web-based Configuration Utility

### Connect to the Router

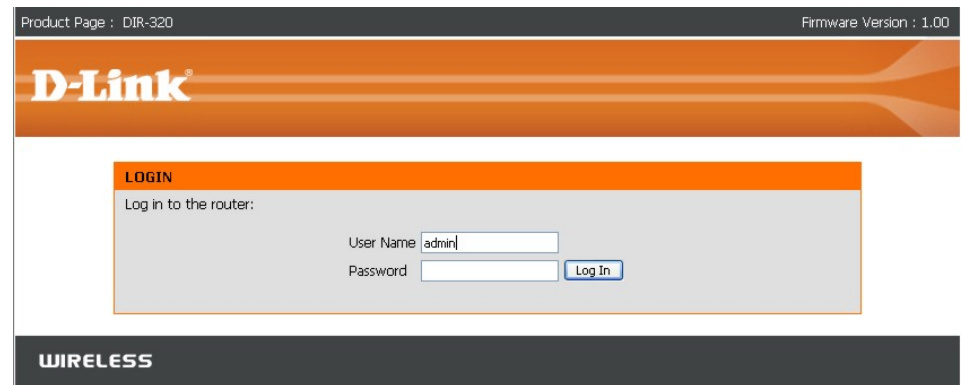
To configure the WAN connection used by the router it is first necessary to communicate with the router through its management interface, which is HTML-based and can be accessed using a web browser. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the router. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client.

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 **User Name** in the entry field. If this is the first time configuring the router, leave the **Password** field blank, there is no default password.

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





# Configure Internet Connection - Setup Wizard

When you successfully connect to the web manager, the main **Internet Connection** menu displays two options for configuring the Internet connection.

Click on the **Internet Connection Setup Wizard** to quickly configure the Internet connection. The Setup Wizard procedure is described in the pages following this one.

To configure the connection in more detail, click on the Manual Internet Connection Setup button. Manual Internet connection setup is described in Internet Connection - Configure Internet Connection – Manual Setup on page 17 below.

The screenshot displays the D-Link DIR-320 web manager interface. At the top, the D-Link logo is visible. Below it, a navigation bar contains tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The main content area is divided into three sections:

- INTERNET CONNECTION:** A message recommending the Internet Connection Setup Wizard for first-time users, with a button labeled "Internet Connection Setup Wizard".
- INTERNET CONNECTION SETUP WIZARD:** A section explaining the wizard's purpose and including a "Note" about following the Quick Installation Guide. It features a button labeled "Internet Connection Setup Wizard".
- MANUAL INTERNET CONNECTION OPTIONS:** A section for manual configuration, including a button labeled "Manual Internet Connection Setup".

On the left side, a sidebar menu lists various setup options: Internet Setup, Wireless Setup, LAN Setup, Printer Setup, Time and Date, Parental Control, and Logout. Below the menu, there is an "Internet Offline" status indicator and a "Reboot" button.

On the right side, a "Helpful Hints.." section provides guidance for new and advanced users, with bullet points explaining the benefits of the wizard and manual setup options.



## Internet Connection Setup Wizard

Use the Internet Connection Setup Wizard to quickly configure the Internet connection.

### Setup Wizard

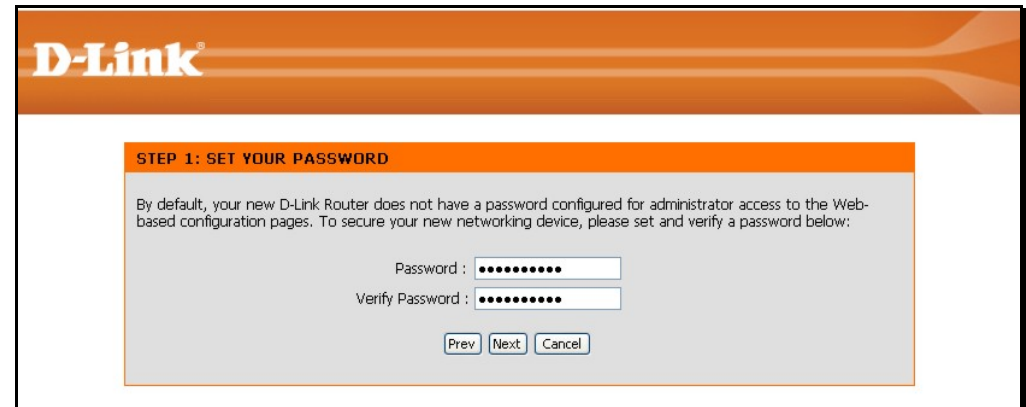
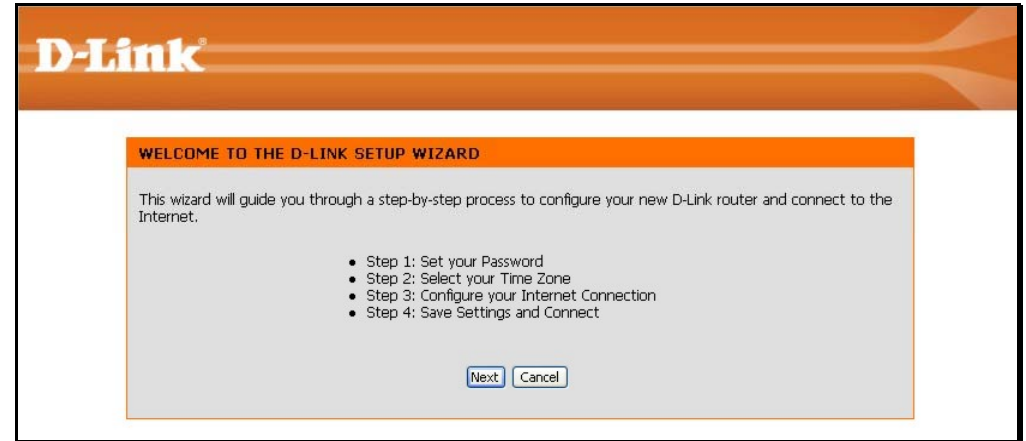
Click the **Internet Connection Setup Wizard** button and follow the instructions in the menus that appear.

The initial window summarizes the setup process. These steps are as follows:

1. Set the new password.
2. Select the time zone.
3. Configure the connection to the Internet.
4. Save settings and reboot the router.

Click the **Next** button to proceed. You may stop using the Setup Wizard at any time by clicking the **Cancel** button. |

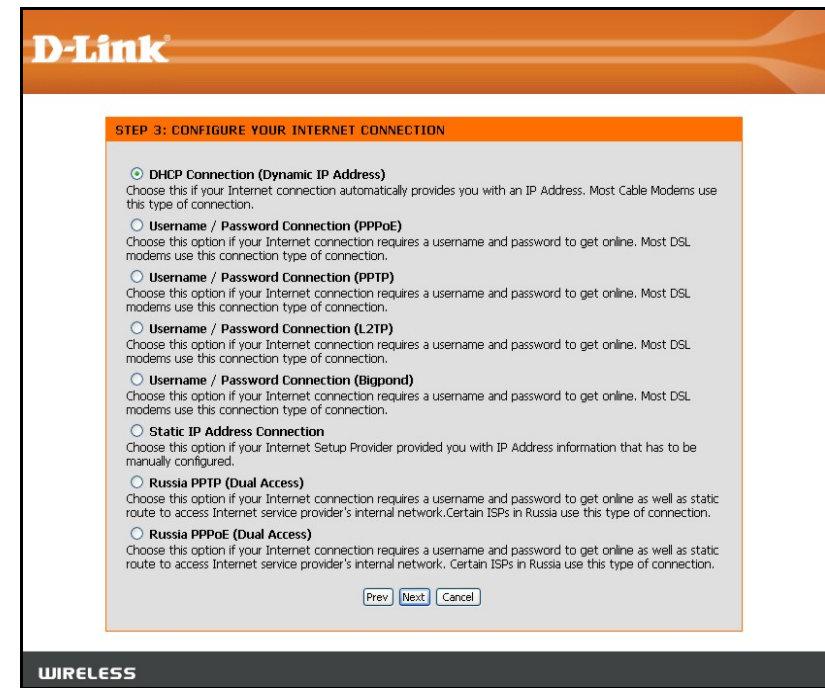
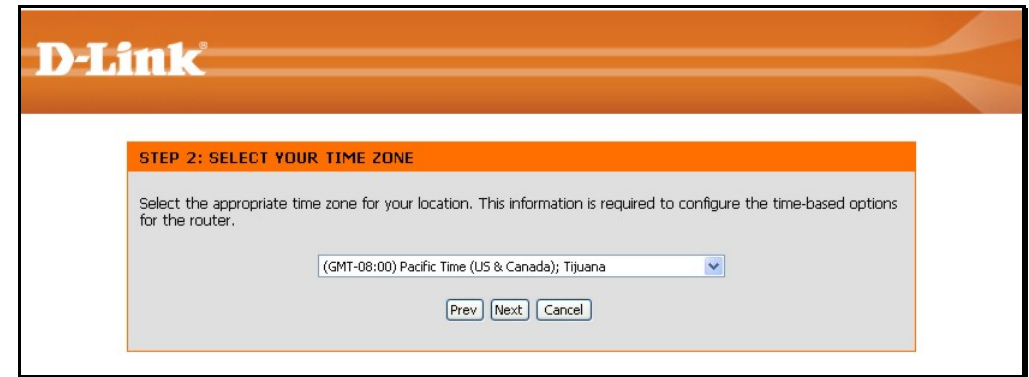
Change the administrator account password, enter a new password in the first **Password** entry field, re-type it exactly as before in the Verify Password field, and click **Next**. If you wish to return to the previous window during the setup process, click the **Prev** button.



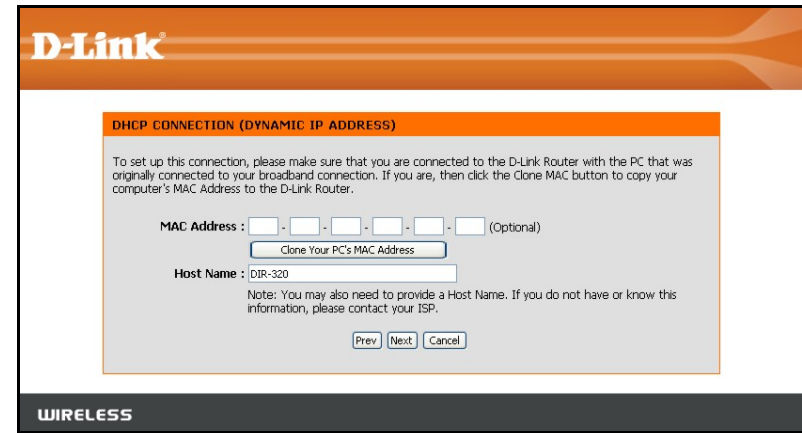
Choose the time zone you are in from the pull-down menu and click **Next**. This sets the system time used for the router. If you wish to return to the previous window during the setup process, click the **Prev** button.

Select the Internet Connection Type used for the Internet connection. Your ISP has given this information to you. The connection types available are **DHCP (Dynamic IP Address)**, **Username/Password (PPPoE)**, **Username/Password (PPTP)**, **Username/Password (L2TP)**, **Username/Password (Bigpond)**, **Static IP Address Connection**, **Russia PPTP (Dual Access)** and **Russia PPPoE (Dual Access)**. Each connection type has different settings that are configured in the next menu

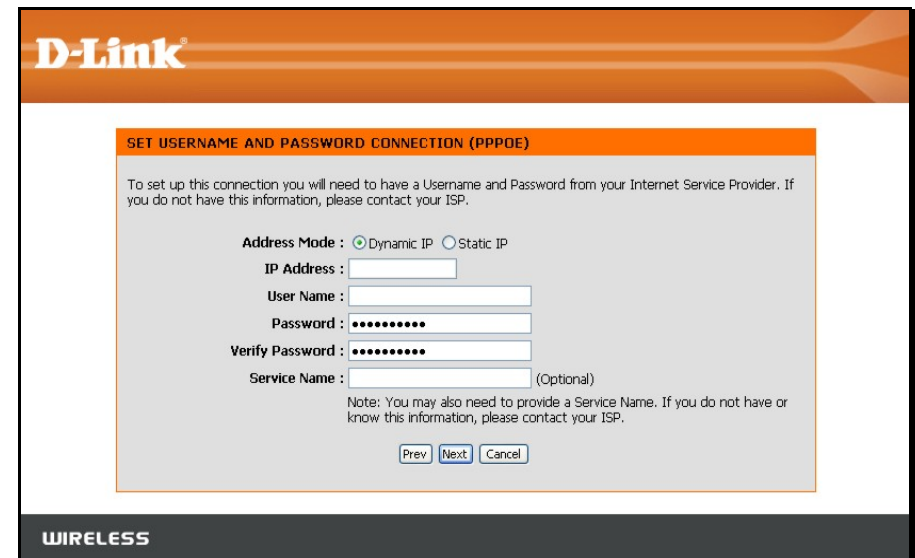
Select the **Connection Type** specific to your service and click **Next**. Follow the instructions below for the type of connection you have selected.



**DHCP (Dynamic IP Address)** - For Dynamic IP Address connections, you may want to copy the MAC address of your Ethernet adapter to the router. Some ISPs use the unique MAC address of your computer's Ethernet adapter for identification and for IP address assignment (DHCP) when you first access their network. This can prevent the router (which has a different MAC address) from being allowed access to the ISP's network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, click the **Clone MAC Address** button. Click **Next** to continue.



**Username/Password (PPPoE)** - For PPPoE connections, select the **Address Mode** Dynamic IP or Static IP, type in the **Username** and **Password** used to identify and verify your account to the ISP. Retype the password again and if necessary, type a **Service Name** or domain name. For Static IP address mode, type the IP Address assigned to your account. Your ISP should provide this IP address along with other account information. Click **Next** to continue.



## Section 3 – Configuration

**Username/Password (PPTP)** - To configure the PPTP client connection, enter the IP and account information for the router. Your ISP will give this information to you if you are establishing a PPTP connection to the ISP. Click **Next** to continue.



**NOTE:** The broadband device used for your Cable or ADSL network connection must support PPTP pass-through so the VPN session can be established.

**Username/Password (L2TP)** - To configure the L2TP client connection, enter the IP and account information for the router. Your ISP will give this information to you if you are establishing a L2TP connection to the ISP. Click **Next** to continue.



**NOTE:** The broadband device used for your Cable or ADSL network connection must support L2TP pass-through so the VPN session can be established.

The screenshot shows the 'SET USERNAME AND PASSWORD CONNECTION (PPTP)' configuration page. At the top, the D-Link logo is visible. Below the title, a note states: 'To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.' The form includes the following fields: 'Address Mode' with radio buttons for 'Dynamic IP' (selected) and 'Static IP'; 'PPTP IP Address'; 'PPTP Subnet Mask'; 'PPTP Gateway IP Address'; 'PPTP Server IP Address (may be same as gateway)'; 'User Name'; 'Password'; and 'Verify Password'. At the bottom of the form are 'Prev', 'Next', and 'Cancel' buttons. The 'WIRELESS' logo is at the bottom of the page.

The screenshot shows the 'SET USERNAME AND PASSWORD CONNECTION (L2TP)' configuration page. At the top, the D-Link logo is visible. Below the title, a note states: 'To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.' The form includes the following fields: 'Address Mode' with radio buttons for 'Dynamic IP' (selected) and 'Static IP'; 'L2TP IP Address'; 'L2TP Subnet Mask'; 'L2TP Gateway IP Address'; 'L2TP Server IP Address (may be same as gateway)'; 'User Name'; 'Password'; and 'Verify Password'. At the bottom of the form are 'Prev', 'Next', and 'Cancel' buttons. The 'WIRELESS' logo is at the bottom of the page.

**Username/Password (Bigpond)** - BigPond Cable connections use this. Enter the account and server information, as provided to you by BigPond. Click **Next** to continue.

The screenshot shows the D-Link wireless configuration interface. At the top, the D-Link logo is displayed. Below it, the title 'SET USERNAME AND PASSWORD CONNECTION (BIGPOND)' is shown in an orange header. The main content area contains the following text: 'To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need BigPond IP address. If you do not have this information, please contact your ISP.' Below this text are several input fields: 'Auth Server' with a dropdown menu set to 'sm-server', 'Bigpond Server IP Address (may be same as gateway)', 'Bigpond User Name', 'Bigpond Password' (masked with dots), and 'Bigpond Verify Password' (masked with dots). At the bottom of the form are three buttons: 'Prev', 'Next', and 'Cancel'. The word 'WIRELESS' is printed in the bottom left corner of the page.

**Static IP Address Connection** - For Static IP Address connection types, you must type in the **IP Address**, **Subnet Mask**, **Gateway Address**, **Primary DNS Address** and **Secondary DNS Address** (optional). Your ISP should provide this information to you. Click **Next** to continue.

The screenshot shows the D-Link wireless configuration interface. At the top, the D-Link logo is displayed. Below it, the title 'SET STATIC IP ADDRESS CONNECTION' is shown in an orange header. The main content area contains the following text: 'To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP.' Below this text are several input fields: 'IP Address', 'Subnet Mask', 'Gateway Address', 'Primary DNS Address', and 'Secondary DNS Address'. At the bottom of the form are three buttons: 'Prev', 'Next', and 'Cancel'. The word 'WIRELESS' is printed in the bottom left corner of the page.

**Russia PPTP (Dual Access)** - To configure the PPTP client connection, enter the IP and account information for the router. Your ISP will give this information to you if you are establishing a PPTP connection to the ISP. Click **Next** to continue.



**NOTE:** The broadband device used for your Cable or ADSL network connection must support PPTP pass-through so the VPN session can be established.

The screenshot shows the 'SET USERNAME AND PASSWORD CONNECTION (PPTP)' configuration page. It includes a header with the D-Link logo and a 'WIRELESS' label at the bottom. The main content area has a title bar and a note: 'To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.' Below the note are several input fields: 'Address Mode' with radio buttons for 'Dynamic IP' (selected) and 'Static IP'; 'PPTP IP Address'; 'PPTP Subnet Mask'; 'PPTP Gateway IP Address'; 'PPTP Server IP Address (may be same as gateway)'; 'User Name'; 'Password'; and 'Verify Password'. At the bottom of the form are 'Prev', 'Next', and 'Cancel' buttons.

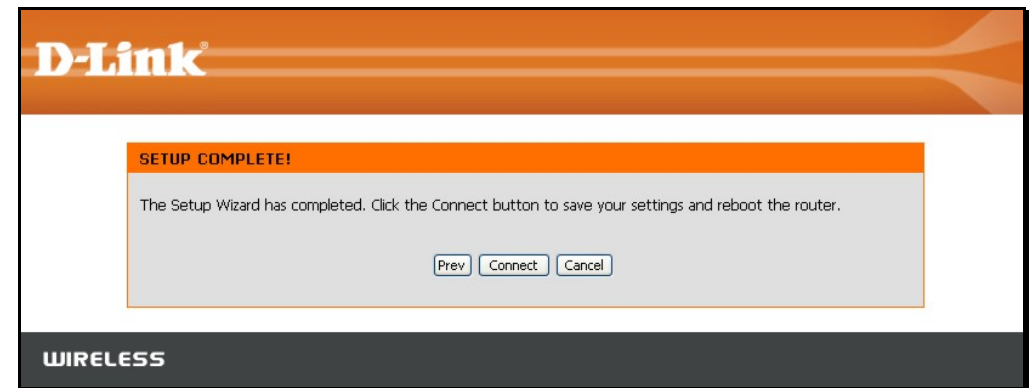
**Russia PPPoE (Dual Access)** - For PPPoE connections, select the **Address Mode** Dynamic IP or Static IP, type in the **Username** and **Password** used to identify and verify your account to the ISP. Retype the password again and if necessary, type a **Service Name** or domain name. For Static IP address mode, type the IP Address assigned to your account. Your ISP should provide this IP address along with other account information. An additional set of IP settings might be required to create a static route to the ISP. Enter the WAN IP settings used to create this route (as given by the ISP) and click **Next** to continue.

The screenshot shows the 'SET USERNAME AND PASSWORD CONNECTION (PPPOE)' configuration page. It includes a header with the D-Link logo and a 'WIRELESS' label at the bottom. The main content area has a title bar and a note: 'To set up this connection you will need to have a Username and Password from your Internet Service Provider. If you do not have this information, please contact your ISP.' Below the note are several input fields: 'Address Mode' with radio buttons for 'Dynamic IP' (selected) and 'Static IP'; 'IP Address'; 'User Name'; 'Password'; 'Verify Password'; and 'Service Name (Optional)'. A sub-note states: 'Note: You may also need to provide a Service Name. If you do not have or know the information, please contact your ISP.' Below this is a section for 'WAN Physical Setting' with radio buttons for 'Dynamic IP' (selected) and 'Static IP', and input fields for 'IP Address', 'Subnet Mask', 'Gateway', 'Primary DNS Address', and 'Secondary DNS Address (Optional)'. At the bottom of the form are 'Prev', 'Next', and 'Cancel' buttons.

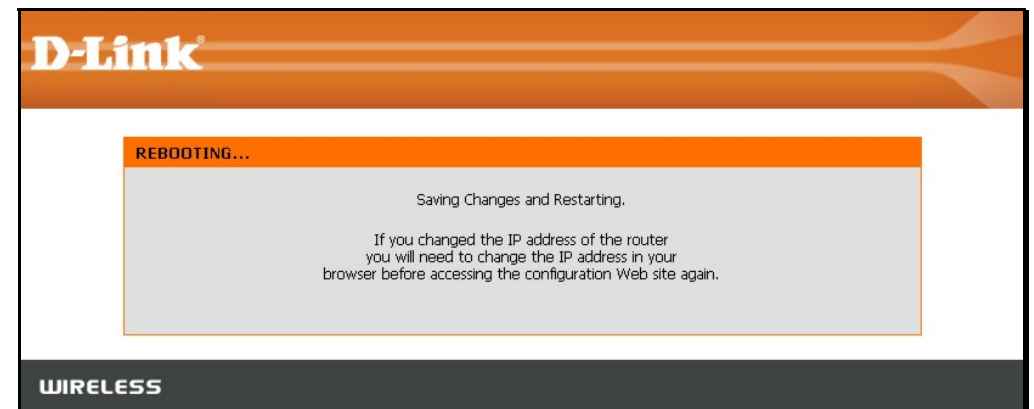
## Section 3 – Configuration

---

When you are satisfied that the settings have been entered correctly click on the **Connect** button to save the new configuration settings.



During the save and restart procedure, the display informs that it is rebooting. Once the reboot is complete, begin to use the router.





## Configure Internet Connection – Manual Setup

The Internet connection can be configured manually without using the Setup Wizard. To configure Internet connection settings manually click on the **Manual Internet Connection Setup** button in the Internet Connection menu.

In the new menu select the **Internet Connection** type used for your service from the **My Internet Connection is:** pull-down menu. Follow the instructions in the next sections according to the type of Internet connection you want to configure.

SETUP	ADVANCED	MAINTENANCE	STATUS
<b>INTERNET CONNECTION</b>			
If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.			
<b>INTERNET CONNECTION SETUP WIZARD</b>			
If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.			
<input type="button" value="Internet Connection Setup Wizard"/>			
<b>Note:</b> Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.			
<b>MANUAL INTERNET CONNECTION OPTIONS</b>			
If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.			
<input type="button" value="Manual Internet Connection Setup"/>			



## Dynamic IP Address

To configure a Dynamic IP Address Internet connection, follow these steps:

1. Select the *Dynamic IP (DHCP)* option from the **My Internet Connection is:** pull-down menu.
2. Under the **Dynamic IP** heading, type a Host Name if needed, and DNS IP address information. The **Primary DNS Address** will be normally be required, the **Secondary DNS Address** is used for a back up DNS server.
3. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISP's network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the **MAC Address** field and click the **Clone MAC Address** button.
4. Leave the **MTU** value at the default setting (default = 1500) unless you have specific reasons to change this (see table below for more information).
5. Click on the Save Settings button to save and apply the new Internet connection settings.

A Dynamic IP Address connection configures the Router to automatically obtain its global IP address from a DHCP server on the ISP's network.

The screenshot shows a configuration window titled "DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE". Below the title is a descriptive text: "Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password." The form contains several input fields and buttons: "Host Name" with the value "DIR-320"; "MAC Address" with a template of six boxes separated by dashes, and a "Clone MAC Address" button; "Primary DNS Address" and "Secondary DNS Address" (optional) fields; and "MTU" with the value "1500". At the bottom are "Save Settings" and "Don't Save Settings" buttons.

## Static IP Address

To configure a Static IP type Internet connection, follow these steps:

1. Select the *Static IP* option from the **My Internet Connection is:** pull-down menu.
2. Under the **Static IP** heading, type IP address information provided by your ISP, type an **IP Address**, **Subnet Mask** and **ISP Gateway Address**. The **Primary DNS Address** will be normally be required, the **Secondary DNS Address** is used for a back up DNS server.
3. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the **MAC Address** field and click the **Clone MAC Address** button.
4. Leave the **MTU** value at the default setting (default = 1500) unless you have specific reasons to change this (see table below for more information).
5. Click on the Save Settings button to save and apply the new Internet connection settings.

When the Router is configured to use Static IP Address assignment for the Internet connection, you must manually assign a global IP Address, Subnet Mask, and ISP Default Gateway IP address. Most users will also need to configure DNS server IP settings. Follow the instruction below to configure the Router to use Static IP Address assignment for the Internet connection.

**STATIC IP ADDRESS INTERNET CONNECTION TYPE**

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

IP Address :  (assigned by your ISP)

Subnet Mask :

ISP Gateway Address :

MAC Address :  -  -  -  -  -   
(optional)

Primary DNS Address :

Secondary DNS Address :  (optional)

MTU :

## PPPoE

PPP or Point-to-Point protocol is a standard method of establishing a network connection/session between networked devices. Different forms of PPP include PPPoA and PPPoE (discussed below) involve an authentication process that requires a username and password to gain access to the network. PPPoE (PPP over Ethernet), as described in RFC 2516, is a method of using PPP through the Ethernet network.

To configure a PPPoE Internet connection, follow these steps:

1. Select the *PPPoE (Username / Password)* option from the **My Internet Connection is:** pull-down menu.
2. Choose the IP address assignment option (Dynamic PpoE or Static PPPoE). Static IP address assignment requires manual entry of IP settings information.
3. Under the **PPPoE** heading, type the **User Name** and **Password** used for your account. A typical User Name will be in the form user1234@isp.co.ru. The Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP. Type the password again in **Confirm Password**.
4. For Static PPPoE connections, enter IP settings provided by the ISP and, if necessary enter MAC address (see table below)
5. Leave the **MTU** value at the default setting (default = 1492) unless you have specific reasons to change this (see table below for more information).
6. Choose the desired **Connection Setting**. Select from: Always ON, Connection On Demand, or Manual. Most users will want to choose the default connection setting, Always ON.

**PPPOE**

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

Dynamic PPPoE    Static PPPoE

User Name :

Password :

Retype Password :

Service Name :  (optional)

IP Address :

MAC Address :  -  -  -  -  -  (optional)

Primary DNS Address :

Secondary DNS Address :  (optional)

Maximum Idle Time :  Minutes

MTU :

Connect mode select :  Always  Manual  Connect-on demand

See table below for parameter description.

## Section 3 – Configuration

Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. The information that is to be provided in this window must be given to you by your ISP and must be carefully configured. Any small discrepancy will send the wrong message to your ISP's server and inhibit your connection.

There are two ways to configure the PPOE connection on the router, one is for a **Dynamic PPPoE** configuration, which means the router will implement some settings automatically through DHCP, such as the router's IP address and the default gateway. The other is through a **Static PPPoE** connection, in which the user must configure the IP address and the DNS addresses automatically.

PPPoE	Description
<b>User Name</b>	The user name supplied to you by your ISP.
<b>Password</b>	The password supplied to you by your ISP.
<b>Retype Password</b>	Retype the password entered in the Password field.
<b>Service Name</b>	Enter the service name supplied to you by your ISP, if required.
<b>IP Address</b>	Enter the IP address given to you by your ISP. This field is only to be completed if the Static PPPoE button is selected.
<b>MAC Address</b>	This field will instruct the user to enter the Media Access Control (MAC) address of the Ethernet Card of your computer, if instructed to do so by your ISP. To quickly accomplish this, click the <b>Clone MAC address</b> button, which will automatically copy the MAC address of your Ethernet card and enter it into the space provided, which will replace the MAC address of the router.
<b>Primary DNS Address</b>	This entry is for the IP address of your primary domain name server, which should also be provided to you by your ISP. The router will first try the Primary DNS Address to resolve a website's URL IP address. If this IP address fails, the router will then try the Secondary DNS Address. This field is only to be completed if the Static PPPoE button is selected.
<b>Secondary DNS Address</b>	The IP address of the secondary domain name server will be used to resolve a website's URL IP address if the Primary DNS Address fails. The information in this field should also be provided by your ISP and is only to be completed if the Static PPPoE button is selected.
<b>Maximum Idle Time</b>	A value of 0 means that the PPP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the Router after the WAN connection has been idle for the amount of time specified. The default value = 5.
<b>MTU</b>	This field refers to the Maximum Transfer Unit, which is the maximum size of a packet, in bytes, that will be accepted by the router. The default setting is 1492 bytes. This field should not be altered unless instructed by your ISP.
<b>Connect Mode Select</b>	This function, with <b>Connect-on-demand</b> selected, will allow the router to connect any workstation on your LAN to the Internet upon request. If this function is set at <b>Always-on</b> , no request from the workstation will be needed to connect to the Internet. If <b>Manual</b> is selected, it will be necessary for the workstation on the LAN to manually connect to the Internet through this router.

## PPTP

The **P**oint to **P**oint **T**unneling **P**rotocol is used to transfer information securely between VPNs (Virtual Private Routers). Encryption methods are employed in the transfer of information between you and your ISP using a key encryption. This option is specific for European users where ISPs support the PPTP protocol for the uplink connection. To connect to your ISP's server using this protocol, the information in this window must be provided to you by your ISP and then properly implemented.

There are two ways to enable the router to become a PPTP client, one is through assigning the router an IP address dynamically, which means that the DHCP protocol will be implemented by the Router to automatically configure the IP settings. The user may input the IP settings manually by choosing the Static IP option above the configuring area. To configure the router to be a PPTP client, complete the entry fields and click the **Save Settings** button.

**PPTP**

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

Dynamic IP     Static IP

IP Address :  (assigned by your ISP)

Subnet Mask :

Gateway :

DNS :

MAC Address :  -  -  -  -  -   
 (optional)

Server IP/Name :

PPTP Account :

PPTP Password :

PPTP Retype Password :

Maximum Idle Time :  Minutes

MTU :

Connect mode select :  Always  Manual  Connect-on demand

See table below for parameter description.

## Section 3 – Configuration

PPTP/L2TP	Description
<b>IP Address</b>	Enter the IP address of the router into this field. This address must be supplied to you by your ISP. This field will not be necessary to configure if the Dynamic IP option is chosen above the configuring field.
<b>Subnet Mask</b>	Enter the IP address of the Subnet Mask into this field. This address must be supplied to you by your ISP. This field will not be necessary to configure if the Dynamic IP option is chosen above the configuring field.
<b>Gateway</b>	Enter the IP address of the gateway into this field. This address must be supplied to you by your ISP. This field will not be necessary to configure if the Dynamic IP option is chosen above the configuring field.
<b>DNS</b>	Enter the IP address of the DNS. This field will not be necessary to configure if the Dynamic IP option is chosen above the configuring field.
<b>MAC Address</b>	This field will instruct the user to enter the Media Access Control (MAC) address of the Ethernet Card of your computer, if instructed to do so by your ISP. To quickly accomplish this, click the <b>Clone MAC address</b> button, which will automatically copy the MAC address of your Ethernet card and enter it into the space provided, which will replace the MAC address of the router.
<b>Server IP/Name</b>	Enter the Server IP address for this protocol into this field. This is the IP address of the server computer that will be used, along with your computer, to create the Virtual Private Network. This field must be completed for both the Dynamic IP and Static IP options
<b>PPTP/L2TP Account</b>	Enter the PPTP/L2TP account name, provided to you by your ISP, here.
<b>PPTP/L2TP Password</b>	Enter your password for this PPTP/L2TP account here, as stated to you by your ISP.
<b>PPTP/L2TP Retype Password</b>	Retype the password entered in the <b>PPTP/L2TP Password</b> field.
<b>Maximum Idle Time</b>	A value of 0 in this field means that the PPTP/L2TP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the Router after the WAN connection has been idle for the amount of time specified. The default value = 5.
<b>MTU</b>	This field refers to the Maximum Transfer Unit, which is the maximum size of a packet, in bytes, that will be accepted by the router. The default setting is 1460 bytes. This field should not be altered unless instructed by your ISP.
<b>Connect Mode Select</b>	This function, with <b>Connect-on-demand</b> selected, will allow the router to connect any workstation on your LAN to the Internet upon request. If this function is set at <b>Always-on</b> , no request from the workstation will be needed to connect to the Internet. If <b>Manual</b> is selected, it will be necessary for the workstation on the LAN to manually connect to the Internet through this router.

## L2TP

**L2PT**, or **Layer 2 Tunneling Protocol** is a VPN protocol that will ensure a direct connection to the server using an authentication process that guarantees the data originated from the claimed sender and was not damaged or altered in transit. Once connected to the VPN tunnel, it seems to the user that the client computer is directly connected to the internal network. To set up your L2PT connection, enter the data that was provided to you by your ISP.

There are two ways to enable the router to become a L2TP client, one is through assigning the router an IP address dynamically, which means that the DHCP protocol will be implemented by the Router to automatically configure the IP settings. The user may input the IP settings manually by choosing the Static IP option above the configuring area. To configure the router to be a L2TP client, complete the following fields and click the **Save Settings** button.

**L2TP**

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

Dynamic IP     Static IP

IP Address :  (assigned by your ISP)

Subnet Mask :

Gateway :

DNS :

MAC Address :  -  -  -  -  -   
 (optional)

Server IP/Name :

L2TP Account :

L2TP Password :

L2TP Retype Password :

Maximum Idle Time :  Minutes

MTU :

Connect mode select :  Always  Manual  Connect-on demand

See table on previous page for parameter description.



## BigPond

BigPond Cable connections use this menu to configure account and connection information. Enter the account information, as provided to you by BigPond. Click **Next** to continue.

BigPond Connection Setting	Description
<b>Auth Server</b>	Enter the name of the Authentication Server as provided to you by BigPond.
<b>User Name</b>	The account name of the account that has been assigned to you by BigPond.
<b>Password</b>	The password of the account that was supplied to you by BigPond.
<b>Confirm Password</b>	Retype the password that was entered in the BigPond Password field. Ensure that these two passwords are identical or an error will occur.
<b>Login Server IP/Name</b>	Enter the Server IP address for this protocol into this field. This is the IP address of the server computer that will be used, along with your computer, to create the Virtual Private Network. This field must be completed for both the Dynamic IP and Static IP options
<b>MAC Address</b>	This field will instruct the user to enter the Media Access Control (MAC) address of the Ethernet Card of your computer, if instructed to do so by your ISP. To quickly accomplish this, click the <b>Clone MAC address</b> button, which will automatically copy the MAC address of your Ethernet card and enter it into the space provided, which will replace the MAC address of the router.

**BIGPOND**

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

User Name :

Password :

Retype Password :

Auth Server :  ▼

Login Server IP/Name :  (optional)

MAC Address :  -  -  -  -  -  (optional)



## PPTP Russia

The PPTP Russia setup is identical to the previously described PPTP setup on page 22 except an option to use a MAC address that will always be associated with the connection. The MAC address is entered manually or copied from the computer.

To configure a PPTP Russia Internet connection, configure as previously described for PPTP connections and type in the MAC address that will be used or clone the computer's MAC address by clicking on the **Clone MAC Address** button.

### RUSSIA PPTP (DUAL ACCESS)

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

Dynamic IP  Static IP

IP Address :  (assigned by your ISP)

Subnet Mask :

Gateway :

DNS :

MAC Address :  -  -  -  -  -   
(optional)

Server IP/Name :

PPTP Account :

PPTP Password :

PPTP Retype Password :

Maximum Idle Time :  Minutes

MTU :

Connect mode select :  Always  Manual  Connect-on demand

## PPPoE Russia

Some PPPoE connections use a static IP route to the ISP in addition to the global IP settings for the connection. This requires an added step to define IP settings for the physical WAN port.

To configure a PPPoE Russia Internet connection, configure as previously described for PPPoE connections on page 20 and add the WAN Physical IP settings as instructed from the ISP.

**RUSSIA PPPoE (DUAL ACCESS)**

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

Dynamic PPPoE    Static PPPoE

User Name :

Password :

Retype Password :

Service Name :  (optional)

IP Address :

MAC Address :  -  -  -  -  -  (optional)

Primary DNS Address :

Secondary DNS Address :  (optional)

Maximum Idle Time :  Minutes

MTU :

Connect mode select :  Always  Manual  Connect-on demand

---

**WAN PHYSICAL SETTING**

Dynamic IP    Static IP

IP Address :

Subnet Mask :

Gateway :

Primary DNS Address :

Secondary DNS Address :  (optional)

## Configure Wireless Connection - Setup Wizard

Configure the router's wireless access point with the **Wireless Connection Setup Wizard** and follow the instructions that follow. Or use the manual configuration option. To configure basic wireless and wireless security settings manually click on the **Manual Wireless Connection Setup** button.

SETUP	ADVANCED	MAINTENANCE	STATUS
<b>WIRELESS CONNECTION</b>			
There are 2 ways to setup your wireless connection. You can use the Wireless Connection Setup wizard or you can manually configure the connection.			
<b>Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.</b>			
<b>WIRELESS CONNECTION SETUP WIZARD</b>			
If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Wireless Router to the Internet, click on the button below.			
<input type="button" value="Wireless Connection Setup Wizard"/>			
<b>Note:</b> Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.			
<b>MANUAL WIRELESS CONNECTION OPTIONS</b>			
If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.			
<input type="button" value="Manual Wireless Connection Setup"/>			

## Wireless Connection Setup Wizard

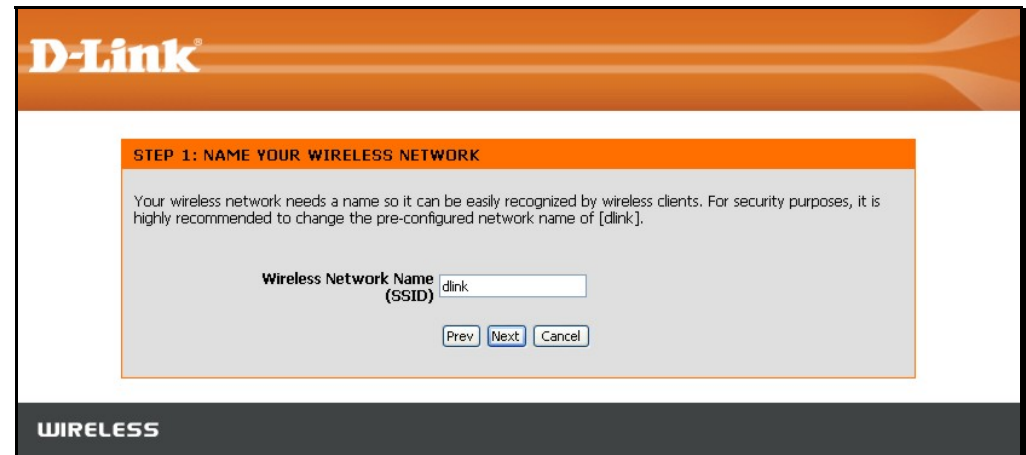
Use the Wireless Connection Setup Wizard to quickly configure the Internet connection. Click on the **Wireless Connection Setup Wizard** button in the Wireless Connection menu to begin using the wizard.

The first wizard menu provides a summary of the setup procedure. The procedure is the same for all security types used. If you want to make specific changes to wireless security settings, use the manual wireless connection setup option. The steps for wireless connection setup are:

1. Name your wireless network
2. Secure your wireless network
3. Set your wireless security password

Click the **Next** button to proceed.

Type the **SSID** or name of your wireless network and click **Next** to proceed. Any wireless client or device that associates with the router must have this SSID.



## Section 3 – Configuration

Select the level of security for the wireless network. The choice will determine the method used for security. The security options are:

- Best – using WPA2
- Better – using WPA
- Good – using WEP
- None – no security for the wireless connection

Remember that all wireless clients that will associate with the router must use the same security settings.

Click **Next** to continue to proceed.

The screenshot shows the D-Link configuration wizard interface. At the top is the D-Link logo. Below it, the title "STEP 2: SECURE YOUR WIRELESS NETWORK" is displayed in an orange header. The main content area contains the following text: "This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet." followed by "In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings." and "There are three levels of wireless security -Good Security, Better Security, or Best Security. The level you choose depends on the security features your wireless adapters support." Below this text are four radio button options: "BEST" (selected), "BETTER", "GOOD", and "NONE". Each option has a brief description of when to use it. At the bottom of the main content area, there is a note: "Note: All D-Link wireless adapters currently support WPA." and three buttons: "Prev", "Next", and "Cancel". The word "WIRELESS" is printed in a dark bar at the very bottom of the screen.

Type the password used for security. The password will be converted into the appropriate form used with the security option chosen before.

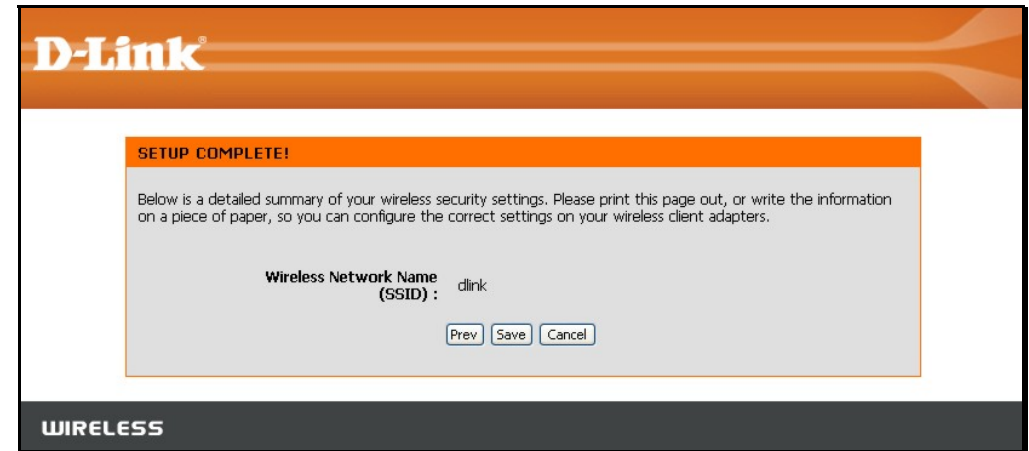
Click **Next** to continue to proceed.

The screenshot shows the D-Link configuration wizard interface. At the top is the D-Link logo. Below it, the title "STEP 3: SET YOUR WIRELESS SECURITY PASSWORD" is displayed in an orange header. The main content area contains the following text: "Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated." Below this text is a text input field labeled "Wireless Security Password:" with a note "(2 to 20 characters)" underneath it. At the bottom of the main content area, there is a note: "Note: You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key." and three buttons: "Prev", "Next", and "Cancel". The word "WIRELESS" is printed in a dark bar at the very bottom of the screen.

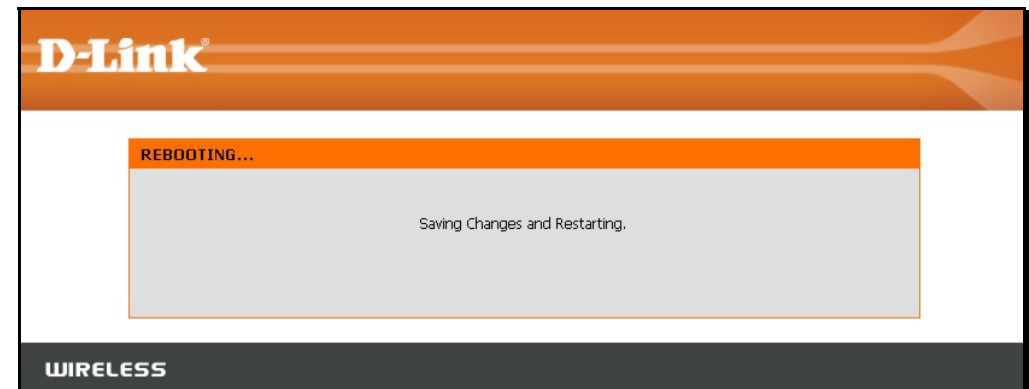
## Section 3 – Configuration

Wireless setup is completed. Review the wireless settings SSID and security information. It is a good idea to keep a record of the wireless settings in order to configure clients that will associate with the router.

Click **Next** to continue to save the new wireless settings and restart the router.



Restarting will take several seconds. Once the router has restarted the wireless settings just configured will be applied.



## Wireless Connection – Manual Setup

The wireless connection can be configured manually without using the Setup Wizard. To configure wireless connection settings manually click on the **Manual Wireless Connection Setup** button in the Wireless Connection menu.

The two essential settings for wireless LAN operation are the **Wireless Network Name** or SSID and **Wireless Channel** number. The SSID (Service Set Identifier) is used to identify a group of wireless LAN components. The SSID can be broadcast in order to allow properly configured wireless stations to learn the SSID and join the group.

SETUP	ADVANCED	MAINTENANCE	STATUS
<b>WIRELESS CONNECTION</b>			
There are 2 ways to setup your wireless connection. You can use the Wireless Connection Setup wizard or you can manually configure the connection. <b>Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.</b>			
<b>WIRELESS CONNECTION SETUP WIZARD</b>			
If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Wireless Router to the Internet, click on the button below.			
<input type="button" value="Wireless Connection Setup Wizard"/>			
<b>Note:</b> Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.			
<b>MANUAL WIRELESS CONNECTION OPTIONS</b>			
If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.			
<input type="button" value="Manual Wireless Connection Setup"/>			

## Wireless Network Settings

Use the **Enable Wireless** check box to disable or enable the wireless interface. Wireless function is enabled by default.

The **Wireless Network Name** or SSID can be changed to suit your wireless network. Remember that any wireless device using the access point must have the same SSID and use the same channel. The SSID can be a continuous character string (i.e. no spaces) of up to 16 characters in length.

Wireless stations that support WPS can be configured automatically using the Wi-Fi Protected Setup menu.

To manually configure security settings, select the **Wireless Security Mode** from the pull-down menu and configure the settings for the security method used. Follow the instructions below for the type of security used.

Click the **Save Settings** button to save any changes to the wireless network settings.

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

Enable :

Current PIN : 33473918

Wi-Fi Protected Status : Enabled / Configured

---

WIRELESS NETWORK SETTINGS

Enable Wireless :

Wireless Network Name :  (Also called the SSID)

Enable Auto Channel Selection :

Wireless Channel :

Transmission Rate :  (Mbit/s)

WMM Enable :  (Wireless QoS)

Enable Hidden Wireless :  (Also called the SSID Broadcast)

---

WIRELESS SECURITY MODE

Security Mode :

---

WEP

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

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

Authentication :

WEP Encryption :

Default WEP Key :

WEP Key :  (13 ASCII or 26 HEX)



## Wi-Fi Protected Setup

Wi-Fi Protected Setup or WPS makes wireless security configuration much quicker simpler for wireless stations that support this feature.



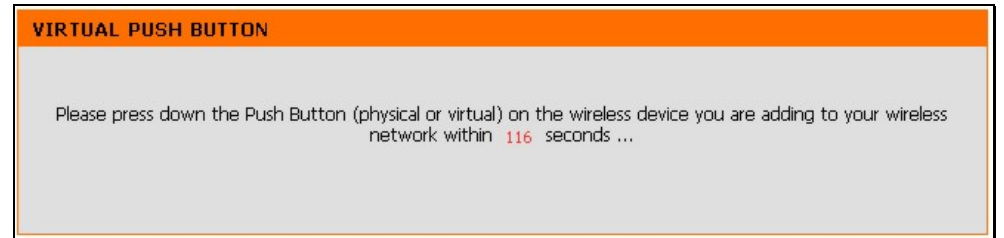
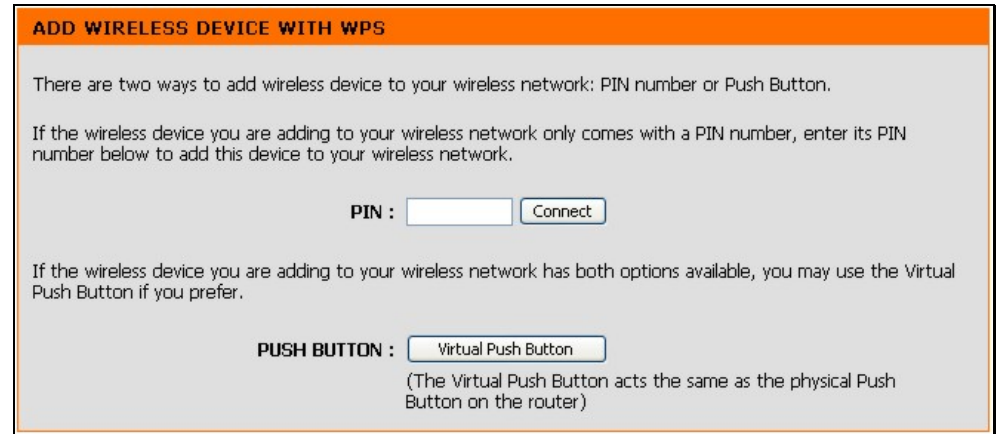
**NOTE:** The Generate New PIN button is for the Router's own PIN. This is used when the Router needs to connect to other WPS enabled access points.

To connect a new wireless station with WPS, click on the **Add Wireless Device with WPS** button. A new menu appears.

There are two methods available to connect a WPS wireless station, a manual PIN entry or automatic method.

To use the PIN entry method, type the new station's PIN number in the space provided and click on the **Connect** button. The router begins searching the wireless network for the device. Now begin the WPS connection procedure with the device attempting connection. The router will search for 120 seconds. If it fails to find the device, a message appears explaining that the WPS connection failed.

To use the automatic WPS method, click on the **Virtual Push Button**. The router begins searching the wireless network for the device. Now begin the WPS connection procedure with the device attempting connection. The router will search for 120 seconds. If it fails to find the device, a message appears explaining that the WPS connection failed.



## Wireless Security - WEP

WEP security requires the following parameters be defined:

- **Authentication:** Select Open Key or Shared Key.
- **Encryption:** Select the encryption level, 64-bit or 128-bit.
- **Default WEP Key:** Up to four keys can be configured. Choose the key being configured.
- **WEP Key:** Type an ASCII or Hex key of appropriate length for the encryption level, 10 characters for 64-bit Hex or 26 characters for 128-bit Hex.

Click the **Save Settings** button to save any changes to the wireless network security settings.



**NOTE:** If encryption of any kind, at any level is applied to the router, all wireless devices using the router on the network must comply with all security measures.

### WIRELESS SECURITY MODE

Security Mode :

---

### WEP

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

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

Authentication :

WEP Encryption :

Default WEP Key :

WEP Key :  (13 ASCII or 26 HEX)

## Wireless Security – WPA/EAP

Wi-Fi Protected Access was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP.

Enter the appropriate parameters for the type of security selected from this menu. WPA EAP or WPA2 EAP must enter the following:

- **Cypher Type:** Choose TKIP, AES or Both.
- **PSK/EAP:** Choose EAP.
- **RADIUS Server IP Address:** The IP address of the RADIUS server.
- **Port:** The port number used for 802.1x.
- **Shared Secret:** The password or character string used for wireless station authentication.

The screenshot shows a configuration window titled "WIRELESS SECURITY MODE". At the top, "Security Mode" is set to "Enable WPA Only Wireless Security (enhanced)". Below this, the "WPA ONLY" section is active. It contains the text "WPA Only requires stations to use high grade encryption and authentication." and two dropdown menus: "Cipher Type" set to "Both" and "PSK / EAP" set to "EAP". Under the "802.1X" heading, there are three input fields: "RADIUS Server IP Address", "Port", and "Shared Secret". At the bottom of the window are two buttons: "Save Settings" and "Don't Save Settings".

## Wireless Security – WPA/PSK

Enter the appropriate parameters for the type of security from this menu.

WPA-PSK or WPA2-PSK must enter the following:

- **Cypher Type:** Choose TKIP, AES or Both.
- **PSK/EAP:** Choose PSK.
- **Network Key:** The password or character string used for wireless station authentication (10 characters for 64-bit Hex).

The screenshot shows a configuration window titled "WIRELESS SECURITY MODE". At the top, there is a dropdown menu for "Security Mode" set to "Enable WPA Only Wireless Security (enhanced)". Below this is a section titled "WPA ONLY" with a descriptive text: "WPA Only requires stations to use high grade encryption and authentication." Underneath, there are two dropdown menus: "Cipher Type" set to "TKIP" and "PSK / EAP" set to "PSK". A text input field for "Network Key" is present, followed by the note "(8~63 ASCII or 64 HEX)". At the bottom of the window are two buttons: "Save Settings" and "Don't Save Settings".

# LAN Setup

Use the Network Settings menu to configure Router LAN IP Settings and DHCP Server Settings. When you are finished, click the **Save Settings** button at the top of the window.

**NETWORK SETTING**

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP address 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.

**Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.**

---

**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 address to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range :  to  (addresses within the LAN subnet)

DHCP Lease Time :  (minutes)

---

**DHCP CLIENT LIST**

Host Name	IP Address	MAC Address	Expired Time
25 - DHCP RESERVATION			
Remaining number of clients that can be configured : 25			
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="←"/> <input type="text" value="Computer Name"/> <input type="button" value="▼"/>

## Router IP Settings

### Router Settings

This section is used to configure the internal network settings of the Router. This IP address is private to your internal network and cannot be seen on the Internet. The default **Router IP Address** is 192.168.0.1 and the **Default Subnet Mask** is 255.255.255.0. The **Local Domain Name** is for the local Domain set on your network, if you have given it a name previously. This field is for your personal use and unnecessary for proper configuration of this window.

In addition, the Router can be configured to relay DNS from your ISP or another available service to workstations on your LAN. When **Enable DNS Relay** is checked, the Router will accept DNS requests from hosts on the LAN and forward them to the ISP (or alternative) DNS servers. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most clients using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, will leave DNS relay enabled.

### 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 address to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range :  to  (addresses within the LAN subnet)

DHCP Lease Time :  (minutes)

## LAN DHCP Server Settings

### DHCP Server Settings

Dynamic Host Configuration Protocol (DHCP) allows the gateway to automatically obtain the IP address from a DHCP server on the service provider’s network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the Router requests an IP address. If DHCP is not enabled on the Router, it is necessary for the user to assign a static IP address to each computer on your LAN.

To set up DHCP for your LAN, first enable the Router as a DHCP server by clicking the **Enable DHCP Server** radio button in the window above. The next step is to set a range of IP addresses that you wish to allot to the devices on your LAN by entering a starting and ending number of addresses within the LAN subnet in the **DHCP IP Address Range**. This may be in a range from 2 to 254 (192.168.0.2 – 192.168.0.254).

Computers on your LAN will have an IP address within this range then automatically assigned to them. Finally, choose the **DHCP Lease Time**, which is the time the Server will set for devices using DHCP to re-request an IP Address. Clients authorized for DHCP will be listed in the Dynamic DHCP Client List near the bottom of the window.

Click **Save Settings** to implement information set in this table. The DHCP Server is enabled by default. DHCP may also be statically configured as well. This method allows the router to assign the same IP address information to a specific computer on the network, defined by its MAC address. This computer will get the same DHCP implemented IP address information every time the computer is turned on and this IP address will be specific to that computer’s IP address on the local network. No other computer can be assigned this address. This is useful for computers on the LAN that are hosting applications such as HTTP or FTP. First, the user must enter the **Host Name** and the **IP Address** for that computer in the spaces provided. Next, the user must enter the **MAC Address** of the computer in the space provided. Click **Save Settings** to implement these static settings.

**DHCP SERVER SETTINGS**

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range :  to  (addresses within the LAN subnet)

DHCP Lease Time :  (minutes)

---

**DHCP CLIENT LIST**

Host Name	IP Address	MAC Address	Expired Time
<b>25 - DHCP RESERVATION</b>			
Remaining number of clients that can be configured : 25			
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<< Computer Name ▾

---

**LOCK CLIENT LIST FOR LAN**

Use this section to lock all PC clients which are on network to an IP/MAC address bundle list, only PCs on the list can access the network after enable the function. It makes sure that no unauthorized client can access LAN network.

Enable LOCK CLIENT LIST :



# Printer Setup

## Printer Setup Wizard

Use the Printer Setup Wizard to configure the Router's USB Printer connection. To establish the connection to a USB equipped printer, click the Printer Setup link to view the Printer Setup Wizard launch menu. Follow the instructions below to install the printer driver on your computer. Some printers, especially very recent release printers, might require the Printer CD-ROM containing the printer driver that came with the printer. This procedure must be followed by any computer that will use the printer.

To use a printer connected to the USB printer port on the DIR-320:

1. Have the CD-ROM with the printer driver available, it might be needed for the installation.
2. Power on the printer; follow the instructions included with the printer to plug in the power cable and turn the power on.
3. Complete the USB connection from the DIR-320 USB to the USB port on the printer. Check the LED indicator on the DIR-320 front panel for the USB connection to make sure a physical connection is established.
4. From the Printer Setup menu, click the Setup Wizard button to launch the Printer Setup Wizard.



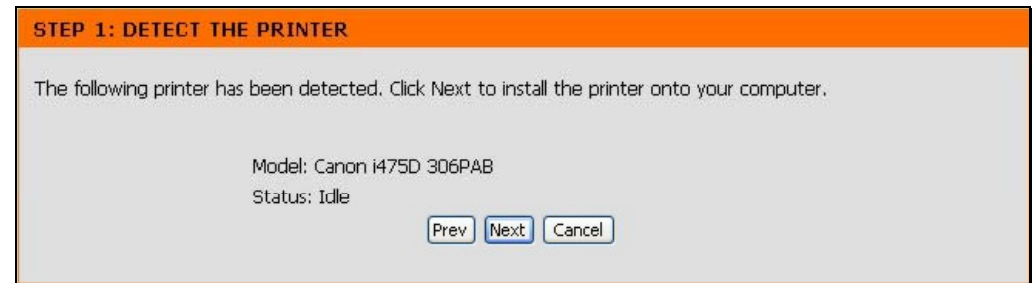


## Section 3 – Configuration

The first Printer Setup Wizard menu lists the steps used for installation. Click the **Next** button to detect the printer.



The printer should be detected immediately. The model name will be displayed if detected. If no printer is detected a warning tells you the printer installation cannot be completed. Check the cable connections and make sure the printer is powered on. Click **Next** if a printer is detected.



It is now necessary to install the correct printer driver on your computer. Click the **Next** button to launch the file.



## Section 3 – Configuration

---

A setup will launch or attempt to launch on your computer. Often the browser settings prevent the file from launching until permission is granted. This file must be executed to install the printer driver. In Windows Internet Explorer permission can be granted to launch downloaded application. See the example from Windows Internet Explorer as seen in XP below. If asked to insert the CD-ROM containing the printer driver, insert the CD-ROM in the CD-ROM drive of your computer and install the printer driver according to the instructions for the printer.

### STEP 3: INSERT THE PRINTER DRIVER CD IF REQUESTED

**Please wait while the setup executable completes the setup process. When done, click Finish below to close the Printer Setup wizard.**

The setup executable you have just launched will begin by displaying a progress bar and will notify you when setup is complete. If the progress bar did not appear, refer to the Troubleshooting Tips section below.

The setup executable will search for a compatible printer driver on your computer. If one cannot be found, you will be prompted to insert the driver CD that shipped with the printer. Alternatively, you can direct the setup executable to a folder on your computer containing a printer driver you have downloaded from the printer manufacturer's web site.

#### Troubleshooting Tips

- If the setup executable did not launch automatically after downloading to your computer, you may need to open the file-download folder using a file browser and double-click on the icon labeled Printer\_Config.exe.

Finish

## Time and Date

The system time is the time used by the DIR-320 for scheduling services. You can configure, update, and maintain the time on the internal system clock.

To configure system time on the Router, select the method used to maintain time. The options available include the default **Automatically synchronize with D-Link's Internet timeserver using** Simple Network Time Protocol (SNTP), to use your computer's system clock, deselect the Automatic option and click the **Sync. your computer's time settings** button. Time can be set manually using the manual pull-down menus at the bottom of the menu.

Click on the **Save Settings** button to save and apply the new time configuration.

### TIME AND DATE

The Time and Date 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

### TIME AND DATE CONFIGURATION

Time : **01/01/2000 01:44:11**  
Time Zone :    
Enable Daylight Saving :

### AUTOMATIC TIME AND DATE CONFIGURATION

Automatically synchronize with D-Link's Internet time server  
NTP Server Used :

### SET THE TIME AND DATE MANUALLY

Year	<input type="text" value="2007"/> <input type="button" value="v"/>	Month	<input type="text" value="Sep"/> <input type="button" value="v"/>	Day	<input type="text" value="15"/> <input type="button" value="v"/>
Hour	<input type="text" value="17"/> <input type="button" value="v"/>	Minute	<input type="text" value="2"/> <input type="button" value="v"/>	Second	<input type="text" value="1"/> <input type="button" value="v"/>

# Parental Control

Use this menu to deny access to specified websites and to set Internet access time periods.

URL or Uniform Resource Locator is a specially formatted text string that uniquely defines an Internet website. This menu will allow users to block computers on the LAN from accessing certain URLs.

To configure this menu for URL blocking, enter the website's address into the **Website URL** field, select the desired **Schedule** and click the **Add New** button for that entry. Schedules can be created using the Schedules menu in the Maintenance directory. Click on the **Save Settings** button to save and apply the new web access control configuration.

**25 - PARENTAL CONTROL RULES**

Configure Parental Control below:

Turn Parental Control OFF

Remaining number of rules that can be created: 25

	Website URL	Schedule	
<input type="checkbox"/>		Always	Add New
<input type="checkbox"/>		Always	Add New
<input type="checkbox"/>		Always	Add New
<input type="checkbox"/>		Always	Add New
<input type="checkbox"/>		Always	Add New
<input type="checkbox"/>		Always	Add New
<input type="checkbox"/>		Always	Add New
<input type="checkbox"/>		Always	Add New

Save Settings    Don't Save Settings

# Advanced Setup

The **Advanced** directory tab offers several configuration menus including **Port Forwarding**, **Application Rules**, **Access Control**, **Firewall & DMZ**, **Advanced Wireless**, **Advanced Network**, **Routing**, **QoS Engine**, **Guest Zone**, and **Traffic Manager**. Click the corresponding link in the left panel of the window. Port Forwarding is the first menu listed and the first to appear when accessing the Advanced directory.

The screenshot shows the D-Link DIR-320 Advanced Setup interface. The top navigation bar includes tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The left sidebar lists various configuration options, with 'Port Forwarding' selected. The main content area is titled 'ADVANCED PORT FORWARDING RULES' and contains a description of the feature, 'Save Settings' and 'Don't Save Settings' buttons, and a table for configuring rules. The table has columns for Name, IP Address, Application Name, Computer Name, Public Port, Private Port, and Traffic Type. Below the table, there are 'Helpful Hints...' and 'Reboot' buttons.

25 - ADVANCED PORT FORWARDING RULES						
Remaining number of rules that can be created: 25						
	Name	Application Name	Computer Name	Public Port	Private Port	Traffic Type
<input type="checkbox"/>	<input type="text"/>	<< Application Name	<< Computer Name	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	Any
<input type="checkbox"/>	<input type="text"/>	<< Application Name	<< Computer Name	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	Any
<input type="checkbox"/>	<input type="text"/>	<< Application Name	<< Computer Name	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	Any
<input type="checkbox"/>	<input type="text"/>	<< Application Name	<< Computer Name	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	Any

## Port Forwarding

The Advanced Port Forwarding menu allows configuration for remote users access to various services outside of their LAN through a public IP address, such as FTP (File Transfer Protocol) or HTTPS (Secure Web). After configuring the Router for these features, the Router will redirect these external services to an appropriate server on the users LAN. The Router has 13 pre-configured external services already set, or manually set the port or port range used for the rules.

To enable an already existing Port Forwarding Rule, click on its corresponding checkbox and configure the appropriate fields listed below. To configure other Port Forwarding Rules for the Router, use the pull-down menus to select the computer or specify an IP address, type the port or port range or select an application form the pull-down menu, select the traffic type and click the **Save Settings** button at the top of the window.

**ADVANCED PORT FORWARDING RULES**

The Advanced Port Forwarding option allow 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 service such as FTP or Web Servers.

**25 - ADVANCED PORT FORWARDING RULES**

Remaining number of rules that can be created: 25

			Port	Traffic Type
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name <div style="border: 1px solid gray; padding: 2px; display: inline-block;">                         Application Name                     </div>	Public Port <input type="text"/> ~ <input type="text"/>	<input type="button" value="Any"/>
	IP Address <input type="text"/>	<< Computer Name <div style="border: 1px solid gray; padding: 2px; display: inline-block;">                         Computer Name                     </div>	Private Port <input type="text"/>	
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name <div style="border: 1px solid gray; padding: 2px; display: inline-block;">                         Application Name                     </div>	Public Port <input type="text"/>	
	IP Address <input type="text"/>	<< Computer Name <div style="border: 1px solid gray; padding: 2px; display: inline-block;">                         Computer Name                     </div>	Private Port <input type="text"/>	

<<

Application Name

v

- Application Name
- FTP
- HTTP
- HTTPS
- DNS
- SMTP
- POP3
- Telnet
- IPSec
- PPTP
- NetMeeting
- DCS-1000
- DCS-2000/DCS-5300
- i2eye



## Application Rules

Use the Application Rules menu to configure applications that require multiple connections, such as Internet Telephony, video conferencing, and Internet gaming. The following window lists six Special Applications that commonly use more than one connection. To configure one of these applications, tick its corresponding checkbox and then modify the fields listed below the following figure. The user may add a new application by modifying the fields listed and then clicking the **Save Settings** button at the top of the window.

To enable an already existing Application Rule, click on its corresponding checkbox. To configure other Application Rules for the Router, type the port or port range or select an application form the pull-down menu, type a name for the rule and select the traffic type and click the **Save Settings** button at the top of the window.

**APPLICATION RULE**

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

**25 - APPLICATION RULES**

Remaining number of rules that can be created: 25

			Port	Traffic Type
<input type="checkbox"/>		<< Application Name	Trigger [Text Field]	Any
<input type="checkbox"/>		<< Application Name	Firewall [Text Field]	Any
<input type="checkbox"/>		<< Application Name	[Text Field]	Any

Application Name

- Application Name
- Battle.net
- Dialpad
- ICU II
- MSN Gaming Zone
- PC-to-Phone
- Quick Time 4

## Access Control

Access Control, or MAC filtering, is a basic security measure that should be used on any network that is exposed to a security risk. A packet filter system examines data packets and scrutinizes them in order to control network access. Filtering rules determine whether packets are passed through the Router from either side of the gateway. The rules are created and controlled by the network administrator and can be precisely defined. These rules are used to block access to the LAN from outside the network and/or to deny access to the WAN from within the network.

### MAC Filters

All computers are uniquely identified by their MAC (Media Access Control) address. The following window will allow users to deny computers access to the Internet or only allow certain computers access to the Internet, based on their MAC address. To access this window, click the **Advanced** tab along the top of the configuration window, then the **Access Control** tab to the left hand side.

To configure MAC filters, manually enter a MAC address to be filtered by ticking its corresponding checkbox and then configuring the desired fields on the window above. Select *Turn MAC Filtering OFF*, *Turn MAC Filtering ON and ALLOW computers listed to access the network*, and *Turn MAC Filtering ON and DENY computers listed to access the network* from the drop-down menu. When you are finished, click the **Save Settings** button at the top of the window.

**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.

---

**25 - MAC FILTERING RULES**

Configure MAC Filtering below:

Turn MAC Filtering OFF ▼

Remaining number of rules that can be created: **25**

	MAC Address		DHCP Client List	Schedule	
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼	<input type="button" value="Add New"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼	<input type="button" value="Add New"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼	<input type="button" value="Add New"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼	<input type="button" value="Add New"/>



## Firewall & DMZ

The Firewall & DMZ menu is used to define enforce specific predefined policies intended to protect against certain common types of attacks.

A DoS "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person. To enable this function, tick the **Enable DoS Prevention** checkbox.

### Firewall Rules

To configure rules for the firewall, modify the following fields and click the **Save Settings** button at the top of the window to set the rule in the Routers memory. Newly configured firewall rules will be displayed in the **Firewall Rules List** at the bottom of the window.

### Internal Attack Prevention

This is used for ARP attacks. The router will drop ARP inquiry packets when it detects an extraordinarily high volume of ARP requests.

### DMZ Host

Firewalls may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a firewall bypass can be set up using a DMZ IP address. The DMZ IP address is a "visible" address and does not benefit from the full protection of the firewall function. Therefore it is advisable that other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to use isolate the device with the DMZ IP address from the rest of the LAN.

For example, if you want to use video conferencing and still use a firewall, you can place the server in the DMZ. The IP address of this server will then be the DMZ IP address. You can designate the server's IP address as the DMZ by typing in the IP address in the **DMZ IP Address** space provided and then enabling its status by ticking the **Enable DMZ Host** checkbox. Click the **Save Settings** button at the top of the window when you are finished.

**FIREWALL & DMZ SETTINGS**

Firewall rules can be used to allow or deny traffic passing through the router. You can specify a single port by utilizing the input box on the top or a range of ports by utilizing both input boxes.

DMZ means "Demilitarized Zone". DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contains Web servers, FTP servers and others.

---

**FIREWALL SETTING**

Enable SPI :

---

**INTERNAL ATTACK PREVENTION**

Prevent Attack Type

ARP Attack :

---

**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 :  << Computer Name >>

---

**50 - FIREWALL RULES**

Remaining number of rules that can be created: 50

	Name	Interface	IP Address	Protocol	Port Range	Schedule
<input type="checkbox"/>	<input type="text"/>	Source >	<input type="text"/>	TCP >	<input type="text"/>	Always > <input type="button" value="Add New"/>
	Action	Dest >	<input type="text"/>		<input type="text"/>	
	Allow >		<input type="text"/>		<input type="text"/>	
<input type="checkbox"/>	<input type="text"/>	Source >	<input type="text"/>	TCP >	<input type="text"/>	Always > <input type="button" value="Add New"/>
	Action	Dest >	<input type="text"/>		<input type="text"/>	
	Allow >		<input type="text"/>		<input type="text"/>	

## Advanced Wireless

The Advanced Wireless menu is used to configure settings that can increase the performance of your router. Click **Save Settings** when you have completed your changes.

See the table below for descriptions of the advanced wireless settings parameters.

### ADVANCED WIRELESS SETTINGS

These options are for users that wish to change the behavior of their 802.11g wireless radio from the standard setting. We do not recommend changing these settings from the factory default. Incorrect settings may impact the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

### ADVANCED WIRELESS SETTINGS

Transmit Power :

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

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

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

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

Preamble Type :  Short Preamble  Long Preamble

CTS Mode :  None  Always  Auto

802.11g Only Mode

<b>Performance Parameter</b>	<b>Description</b>
<b>Transmit power</b>	Allows the user to adjust the transmit power of the router. A high transmit power allows a greater area range of accessibility to the router. When multiple overlapping access points are present, it may be desirable to reduce transmission power.
<b>Beacon Interval</b>	Beacons are emitted from the router in order to synchronize the wireless network. You may set the Beacon Interval range between 20-100 microseconds per beacon sent. The default is 100.
<b>RTS Threshold</b>	The RTS (Request to Send) Threshold controls the size of data packets issued to a RTS packet. A lower level will send packets more frequently which may consume a great amount of the available bandwidth. A high threshold will allow the router to recover from interference or collisions which is more prevalent in a network with high traffic or high electromagnetic interference. The default setting is 2346.
<b>Fragmentation</b>	The fragmentation threshold will determine if packets are to be fragmented. Packets over the 2346 byte limit will be fragmented before transmission. 2346 is the default setting.
<b>DTIM Period</b>	DTIM (Delivery Traffic Indication Message) Period is a countdown informing clients of the next menu for listening to broadcast and multicast messages. The default setting is 1.
<b>Preamble Type</b>	Long Preamble should be used where 802.11b clients are present.
<b>CTS Mode</b>	Clear to Send mode should only be used when wireless clients are close enough to each other to “hear” or detect the presence of ther other clients. The Auto option will use CTS mode only when associating clients are in close proximity to each other.
<b>802.11g Only Mode</b>	The router can be forced to associate with exclusively 802.11g devices.
<b>Fragmentation</b>	The fragmentation threshold will determine if packets are to be fragmented. Packets over the 2346 byte limit will be fragmented before transmission. 2346 is the default setting.

## Advanced Network

The Advanced Network Settings menu is used to disable or enable UPnP, disable Ping responses on the WAN port and change WAN port speed.

### UPnP

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network.

Diverse networking media including Ethernet, 802.11b/g Wireless, Firmware, phone line and power line networking can support UPnP. To enable UPnP, tick the **Enable UPnP** checkbox.

### WAN Ping

This feature allow users to either allow or block a Ping test from outside computers looking to check the connectivity of your device. This is usually attempted by hackers trying to access your router or computer from a remote device on the WAN side of the connection. Tick the **Enable WAN Ping Respond** checkbox to allow WAN pinging of your device.

### WAN Port Speed

This section allows the user to set the wire speed over which the router will transmit packets. The user has three options:

- *10Mbps* – Selecting this option from the drop-down menu will set the wire speed at 10 megabytes per second.
- *100Mbps* – Selecting this option from the drop-down menu will set the wire speed at 100 megabytes per second.
- *10/100 Mbps Auto* – Selecting this option from the drop-down menu will allow the wire speed to be automatically set by the Router depending on the wire speed available at any given time.

**ADVANCED NETWORK SETTINGS :**

These options are for users that wish to change the LAN settings. We do not recommend changing these settings from factory default. Chaning these settings may affect the behavior of your network.

**UPNP**

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

Enable UPnP :

**WAN PING**

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

Enable WAN Ping Respond :

**WAN PORT SPEED**

10/100Mbps Auto

**GAMING MODE**

If you are having difficulties playing some online games - please enable this mode.

Enable GAMING mode :

**MULTICAST STREAMS**

Enable Multicast Streams :

Wireless enhance mode :

### Gaming Mode

When gaming mode is enabled, the router's QoS settings are adjusted automatically to accommodate Internet gaming. Gaming mode is enabled by default.

### Multicast Streams

These options are used to enable and optimize multicast streaming. Open multicast ports receive enhanced priority during streaming. The wireless enhance mode enables multicast streaming optimization for the wireless LAN.

## Routing

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway. Static routing on the WAN is only supported if your WAN connection protocol is not using PPPoE.

To add a static route to a specific destination IP address, choose the **Interface**, enter a **Destination** IP address, select a suitable **Subnet Mask**, and type in the **Gateway** IP address. Click the **Save Settings** button at the top of the menu when you are finished.

**ROUTING :**

The Routing option allows you to define fixed routes to defined destinations.

**50 - STATIC ROUTING**

Remaining number of rules that can be created: 50

	Interface	Destination	Subnet Mask	Gateway
<input type="checkbox"/>	WAN			
<input type="checkbox"/>	WAN			
<input type="checkbox"/>	WAN			
<input type="checkbox"/>	WAN			

## QoS Engine

With some routers, all wired and wireless traffic, including VoIP, Video Streaming, Online Gaming, and Web browsing are mixed together into a single data stream. By handling data this way, applications like video streaming could pause or delay. With D-Link Intelligent QoS Technology, both wired and wireless traffic are analyzed and separated into multiple data streams. These streams are then categorized by sensitivity to delay, so applications like VoIP, Video Streaming, and Online Gaming are given higher priority automatically. This enables multiple applications to stream smoothly to your TV or PC.

Click the **Save Settings** button to implement the new QoS changes.

The screenshot shows a web interface for configuring the QoS Engine. It is divided into three main sections: QoS (Quality of Service), Bandwidth, and a final QoS section. The QoS section has an orange header and contains a paragraph of text explaining the Smart QoS feature, along with 'Save Settings' and 'Don't Save Settings' buttons. The Bandwidth section has a dark grey header and contains two dropdown menus for 'Uplink Speed' and 'Downlink Speed', both currently set to '64 Kbps', and a paragraph of text advising to contact the ISP. The final QoS section has a dark grey header and contains a single checkbox labeled 'Lag eliminated (VoIP, Streaming)'. At the bottom of this section are 'Save Settings' and 'Don't Save Settings' buttons.

**QoS (QUALITY OF SERVICE)**

Use this section to configure D-Link's Smart QoS. This Smart QoS improves your VoIP voice quality or streaming by ensuring that your VoIP or streaming traffic is prioritized over other network traffic, such as FTP or Web. For best performance, please tick the "lag eliminated" option to automatically set the priority for your applications.

Save Settings Don't Save Settings

**BANDWIDTH**

Uplink Speed : 64 Kbps

Downlink Speed : 64 Kbps

Please contact with your Internet Service Provider to make sure your xDSL or cable uplink bandwidth, the accurately uplink bandwidth setting is allowed QoS engine operates smoothly and efficiency.

**QoS**

Lag eliminated (VoIP, Streaming)

Save Settings Don't Save Settings



## Guest Zone

The Guest Zone feature of the router allows an additional subnet to be added. This is especially useful for placing wireless stations in an IP subnet separate from wired Ethernet stations. The four Ethernet ports can also be configured to use the Guest Zone so one or more Ethernet ports can be on a separate IP subnet.

To use a guest zone, click to select the **Enable Guest Zone** box, if desired select a schedule when the Guest Zone is effective. To create a new schedule, click the **Add New** button to go to the Schedules menu.

The Guest Zone can be applied to any Ethernet port by selecting it from the **Include LAN Port** menu.

To create a new wireless SSID for the Guest Zone, check to select the **Include Wireless** box, then configure the new Wireless Network Name (SSID) and the security used for the new SSID.

The default IP subnet for the guest zone is 192.168.1.0. To change the IP address scheme for the guest zone type the new Router IP Address and Subnet Mask in space provided.

If the **Enable Guest Zone Client Isolation** option is selected, the router will not exchange traffic between clients on the guest zone's newly created subnet. Guest zone clients will be able to access the Internet only.

Click the **Save Settings** button to implement the changes.

**GUEST ZONE SELECTION**

Enable Guest Zone :  Always Add New

Include LAN Port :  1  2  3  4

Include Wireless :

Wireless Network Name :  (Also called the SSID)

Security Mode : Disable Wireless Security (not recommended)

---

**ROUTER SETTING FOR GUEST ZONE**

Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.

Router IP Address : 192.168.1.1

Default Subnet Mask : 255.255.255.0

---

**GUEST ZONE CLIENT ISOLATION**

Enable the function to prevent one guest client to access other clients in the Guest Zone. The guest client can access to the Internet only.

Enable Guest Zone Client Isolation :

Guest Zone menu (upper portion)



## Section 3 – Configuration

Routing between the guest zone and the original host subnet can be enabled by clicking the **Enable Routing Between Zones** box. If this option is not selected, the two subnets will behave as separate networks with access to the Internet connection, but not to computers on the other subnet.

The DHCP server for the guest zone is configured exactly the same as the DHCP server to the original host zone. DHCP clients on the guest zone are listed below the DHCP server setup menu.

The **Enable Guest Zone Client** option will create static IP addresses for all current DHCP clients and leasers. When this is enabled, no more DHCP clients are allowed, the list is locked.

Click the **Save Settings** button to implement the changes.

### ROUTING BETWEEN HOST ZONE AND GUEST ZONE

Use this section to enable routing between Host Zone and Guest Zone, Guest clients can not access Host clients' data without enable the function.

Enable Routing Between Zones :

### DHCP SERVER SETTINGS FOR GUEST ZONE

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range :  to  (addresses within the LAN subnet)

DHCP Lease Time :  (minutes)

### DHCP CLIENT LIST FOR GUEST ZONE

Host Name	IP Address	MAC Address	Expired Time
-----------	------------	-------------	--------------

### LOCK CLIENT LIST FOR GUEST ZONE

Use this section to lock all PC clients which are on network to an IP/MAC address bundle list, only PCs on the list can access the network after enable the function. It makes sure that no unauthorized client can access Guest Zone network.

Enable LOCK CLIENT LIST :

**Guest Zone menu (lower portion)**

## Traffic Management

The Traffic Manager is used to control Internet connection bandwidth for individual computers on the wired or wireless network. Up to 26 clients can be added to the list for bandwidth control.

### TRAFFIC MANAGEMENT

Use this section to configure the traffic management of your router. The traffic management allows you to set bandwidth control to certain clients. You can select up/down link bandwidth to reserve the minimum bandwidth for the client.

#### SETUP

Enable Traffic Management :

#### 26 - BANDWIDTH CONTROL LIST FOR HOST ZONE

Remaining number of rules that can be created: 26

	Computer Name	Up Link	Down Link	
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text" value="v"/>	<< Computer Name v
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text" value="v"/>	<< Computer Name v
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text" value="v"/>	<< Computer Name v

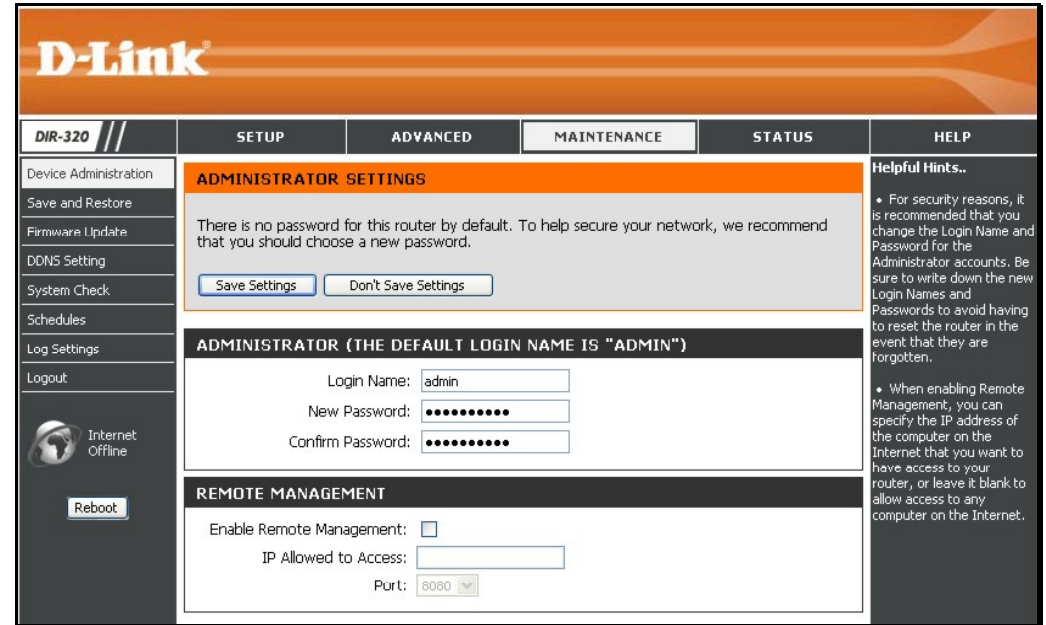
# Maintenance

The menus of the Maintenance directory include **Device Administration**, **Save and Restore**, **Firmware Update**, **DDNS Setting**, **System Clock**, **Schedules** and **Log Settings**.

## Device Administration

The Device Administrator menu is used to change the administrator's login name and password as well as remote management set up. To change the login name or password, enter the new **Login Name** and password into the **New Password** field and repeat the password in the **Confirm Password** field. Click **Save Settings** to set your new password.

This window will also allow the user to enable remote management of the device from a remote computer. To configure this function, click **Enable Remote Management** under the **Remote Management** heading and type IP address of the system used for remote management. Click **Save Settings** to set these configurations into the memory of the Router.



## Save and Restore

Current system settings can be saved as a file onto the local hard drive by clicking the **Save** button. The saved file or any other saved setting file can be loaded back on the Router. To reload a system settings file, click on **Browse** to browse the local hard drive and locate the system file to be used. You may also reset the Router back to factory settings by clicking on **Restore Device**.

The screenshot shows a web interface titled "SAVE AND RESTORE SETTINGS". At the top, there is an orange header bar with the title. Below the header, a grey box contains the following text: "Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings, or restore the factory default settings." Below this, there is a dark grey header bar with the title "SAVE AND RESTORE SETTINGS". The main content area contains four rows of controls: "Save Settings To Local Hard Drive : Save", "Load Settings From Local Hard Drive : [text input] Browse...", "Restore To Factory Default Settings : Restore Device", and "Clear Language Pack : Clear".

**SAVE AND RESTORE SETTINGS**

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings, or restore the factory default settings.

**SAVE AND RESTORE SETTINGS**

Save Settings To Local Hard Drive :

Load Settings From Local Hard Drive :

Restore To Factory Default Settings :

Clear Language Pack :

## Firmware Update

View the version of the currently loaded firmware and update the system firmware with the Firmware Update menu. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to browse the local hard driver and locate the firmware to be used for the update. Please check the D-Link support site for firmware updates at D-Link Technical support website of your country.

In order to keep pace with changes in standards and technology, the DIR-320 allows you to easily update the embedded firmware. You may obtain the latest version of the DIR-320 firmware by logging onto the D-Link web site at [www.dlink.com](http://www.dlink.com). If you are connected to the Internet, you can access the D-Link web site by clicking on **Check Now**. The **Firmware Upgrade** window lists the version of the firmware the Router is currently using. If you would like to update, follow the instructions given on the D-Link web site firmware update page to download the new firmware. You can then use the DIR-320 Firmware Upgrade Utility included with the Router to transfer the new firmware to the Router. Once you have downloaded the new firmware to your computer, use the **Browse** button to find where it is located on your computer, or if you know the path of the file, enter it into the space provided. Click **Apply** to begin the download. After the new firmware has been successfully downloaded into your Router, restart the device to let the changes take effect.

**FIRMWARE UPDATE**

There may be new firmware for your DIR-320 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.

**CURRENT FIRMWARE INFO**

<b>Current Firmware Version</b>	1.00
<b>Firmware Date</b>	Mon 08 Oct 2007

**Check Online Now for Latest Firmware Version**

**UPDATE SETTING**

Update :

## DDNS Setting

The DIR-320 supports DDNS or Dynamic Domain Name Service. Dynamic DNS allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specific host from various locations on the Internet. With this function enabled, remote access to a host will be allowed by clicking a URL hyperlink in the following form: *dlinkddns.com* Because many ISPs assign public IP addresses using DHCP, it can be difficult to locate a specific host on the LAN using the standard DNS. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS servers.

To implement Dynamic DNS, first tick the **Enable DDNS** checkbox in the window above, then choose the **Server Address** from the list in the pull-down menu. Next, enter the **Host Name** of the LAN to be accessed, and the **Username** and **Password** for the DDNS account. Click the **Save Settings** button to save changes made. Use the **DDNS Account Testing** button to make sure the DDNS service is functioning.

**DYNAMIC DNS**

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

[Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.](http://www.DLinkDDNS.com)

Save Settings    Don't Save Settings

**DYNAMIC DNS SETTINGS**

Enable DDNS :

Server Address : dlinkddns.com(Free) ▼

Host Name :

Username :

Password :

DDNS Account Testing

## System Check

This menu is used to monitor port performance and connectivity, the menus displayed are **VCT Info** and **Ping Test**.

### VCT Info

The Virtual Cable Tester displays the current status of all ports.

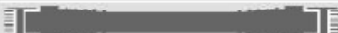
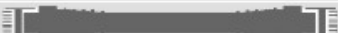
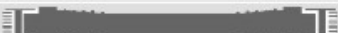


### Ping Test

The Ping Test section allows you to ping any IP address from the Router to test connectivity to the address. To Ping a device, enter the IP address of the device that you wish to ping into the **Host Name or IP Address** field and click **Ping** to start the Ping mechanism. The results of the Ping will be shown under the **Ping Result** heading.

**SYSTEM CHECK**

The System Check tool can be used to verify the physical connectivity on both the LAN and Internet interfaces. The Ping Test tool can be used to verify the status of the Internet.

**VCT INFO**

Ports	Link Status		
Internet		Disconnected	<a href="#">More Info</a>
LAN1		100Mbps FULL Duplex	<a href="#">More Info</a>
LAN2		100Mbps FULL Duplex	<a href="#">More Info</a>
LAN3		100Mbps FULL Duplex	<a href="#">More Info</a>
LAN4		Disconnected	<a href="#">More Info</a>

**PING TEST**

Ping Test is used to send "Ping" packets to test if a computer is on the Internet.

Host Name or IP Address :  [Ping](#)

**PING RESULT**



## Schedules

This window is used to create implementation schedules. This is the same menu accessed using the **Make New Schedule** button in the rules menu of various settings pages.

### Schedule rule setup menu

Complete the **Add Schedule Rule** settings on the window above and then click the **Save Settings** button at the top of the window.



NOTE: Make sure the time in Router is synchronized with your local time to have the schedule setting work properly.

If the router is reset or powered off, the schedule function will not work as expected since the router time will be incorrect.

**SCHEDULES**

The Schedule configuration option is used to manage schedule rules for "Access Control", "Firewall Rules" and "Parental Control".

**10 - ADD SCHEDULE RULE**

**Name :**

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

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**All Day - 24 hrs :**

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

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

**SCHEDULE RULES LIST**

Name	Day(s)	Time Frame

## Log Settings

The system log displays chronological event log data, including System Activity, Debug Information, Attacks, Dropped Packets, and Notice. Check the desired category of Log Type in the bottom half of the window above and then click the **Save** button and follow the prompts to save the file.

Alerts can be sent to an email account. Use the Send By Mail settings to configure Email account information. Click the **Send Me Now** button to email alerts to a previously configured email account.

The screenshot shows a web-based configuration interface for log settings. It is divided into four main sections:

- LOG SETTINGS:** An orange header bar. Below it, a grey box contains the text "Logs can be saved by sending it to an admin email address." and two buttons: "Save Settings" and "Don't Save Settings".
- SAVE LOG FILE:** A dark grey header bar. Below it, a grey box contains the text "Save Log File To Local Hard Drive" and a "Save" button.
- LOG TYPE:** A dark grey header bar. Below it, a table lists log categories with checkboxes:

Log Type	<input checked="" type="checkbox"/> System Activity
	<input type="checkbox"/> Debug Information
	<input checked="" type="checkbox"/> Attacks
	<input type="checkbox"/> Dropped Packets
	<input checked="" type="checkbox"/> Notice
- SEND BY MAIL:** A dark grey header bar. Below it, two input fields are shown: "SMTP Server / IP Address" and "Email Address". A "Send Mail Now" button is positioned to the right of the "Email Address" field.

# Status

The **Status** directory menus are used to check information about the Router, including **Device Information**, **Log**, **Statistics**, and **Active Session**.

## Device Information

The Device Information display is used to view information regarding the settings of the Router, both on the LAN side and WAN side of the connection. The firmware version is also displayed here as well as in the firmware upgrade menu.

DIR-320	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP						
Device Info Log Statistics Active Session Wireless Logout  Internet Offline Reboot	<b>DEVICE INFORMATION</b> All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.  <b>Firmware Version : 1.00 , Mon 08 Oct 2007</b>			<b>Helpful Hints..</b> • All of your LAN, Internet and WIRELESS 802.11G connection details are displayed here.							
	<b>LAN</b> MAC Address : 00:18:02:62:8d:35 IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0 DHCP Server : Enabled										
	<b>INTERNET</b> MAC Address : 00:18:02:62:8d:37 DHCP client : Disconnected Connection : <input type="button" value="DHCP Renew"/> <input type="button" value="DHCP Release"/> IP Address : 0.0.0.0 Subnet Mask : 0.0.0.0 Default Gateway : 0.0.0.0 DNS : 0.0.0.0										
	<b>WIRELESS 802.11G</b> SSID : dlink Channel : 6 Encryption : Disabled										
	<b>PRINTER SERVER INFORMATION</b> <table border="1"> <thead> <tr> <th>Queue Name</th> <th>Printer Name</th> <th>Printer Server Status</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>			Queue Name	Printer Name	Printer Server Status					
Queue Name	Printer Name	Printer Server Status									

## Log

The Log displays events occurring within the router by time and date, and also view the source and destination of the event. The user may use the **First Page**, **Last Page**, **Previous** and **Next** buttons to scroll through the log events listed in the window. To clear the log events, click **Clear**.

Click the **Link to Log Settings** button to change what events are displayed in the log.

**VIEW LOG**

View Log displays the activities occurring on the DIR-320.

**LOG FILES**

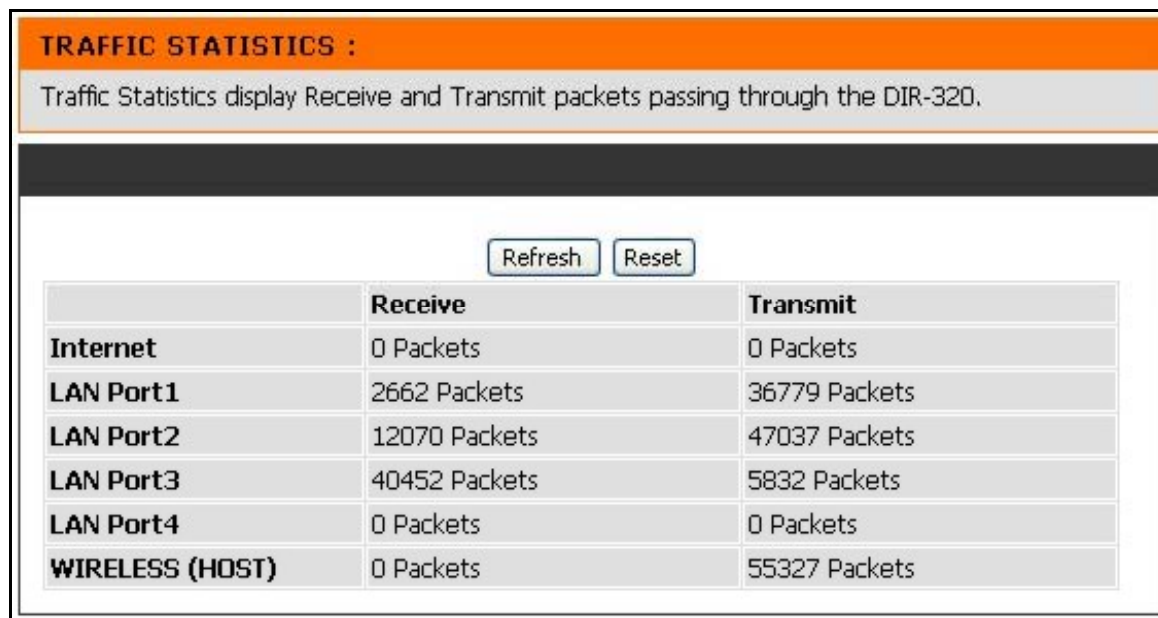
First Page Last Page Previous Next Clear Link To Log Settings

Page 1 of 24

Time	Message
Sep 15 17:34:03	Remote management is disabled.
Sep 15 17:34:03	Block WAN PING is disabled.
Sep 15 17:34:03	DMZ disabled.
Sep 15 17:33:37	PPPoE: Sending PADI for session1.
Sep 15 17:33:27	PPPoE: Sending PADI for session1.
Sep 15 17:33:22	PPPoE: Sending PADI for session1.
Sep 15 17:31:54	Remote management is disabled.
Sep 15 17:31:54	Block WAN PING is disabled.
Sep 15 17:31:54	DMZ disabled.
Sep 15 17:31:33	PPPoE: Sending PADI for session1.

The Statistics displays shows transmitted and received packets occurring on the Router. To refresh the window, click **Refresh**. To restart the packet count, click **Reset**.

## Statistics



**TRAFFIC STATISTICS :**

Traffic Statistics display Receive and Transmit packets passing through the DIR-320.

	Receive	Transmit
Internet	0 Packets	0 Packets
LAN Port1	2662 Packets	36779 Packets
LAN Port2	12070 Packets	47037 Packets
LAN Port3	40452 Packets	5832 Packets
LAN Port4	0 Packets	0 Packets
WIRELESS (HOST)	0 Packets	55327 Packets

## Active Session

Source and Destination packets passing through the Router are displayed listed by TCP/UDP type in the Active Session display. To refresh the window, click the **Refresh** button.

The screenshot shows a web interface for monitoring active sessions. It features three main sections: 'ACTIVE SESSION' with a refresh button, 'NAPT SESSION' with session counts, and 'NAPT ACTIVE SESSION' with a table header.

ACTIVE SESSION			
Active Session display Source and Destination packets passing through the DIR-320.			
<input type="button" value="Refresh"/>			
NAPT SESSION			
TCP Session : 0			
UDP Session : 0			
Total : 0			
NAPT ACTIVE SESSION			
IP Address	TCP Session	UDP Session	

## Wireless Client List

The Connected Wireless Client List displays all wireless clients currently connected and the mode of the connection.

CONNECTED WIRELESS CLIENT LIST		
The Wireless Client table below displays Wireless clients Connected to the AP (Access Point).		
Connect Time	MAC Address	Mode



# Technical Specifications

## Standards

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

## Wireless Signal Rates\*

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

## Security

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

\* 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.

## Modulation Technology

- | 802.11g | 802.11b |
|---------|---------|
| • BPSK  | • DQPSK |
| • QPSK  | • DBPSK |
| • 16QAM | • DSSS  |
| • 64QAM | • CCK   |
| • OFDM  |         |

## Wireless Frequency Range

2400 ~ 2497 MHz ISM band

## Wireless Operating Range

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

## External Antenna Type

Single detachable reverse SMA

## Appendix – Technical Specifications

### **VPN Pass Through/ Multi-Sessions**

- PPTP
- IPSec

### **Device Management**

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

### **Advanced Firewall Features**

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

### **Power**

**Input:** DC 5V 2A

### **Operating Temperature**

32°F to 104°F (0°C to 40°C)

## Appendix – Technical Specifications

### **Humidity**

Operating humidity 10% - 90% maximum (non-condensing)

### **Safety and Emissions**

FCC

### **LEDs**

- Power
- Status
- Internet
- 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

**Web-based management function navigator**

<b>SETUP</b>	<b>ADVANCED</b>	<b>MAINTENANCE</b>	<b>STATUS</b>	<b>HELP</b>
Internet Setup	Port Forwarding	Device Administration	Device Info	Menu
Wireless Setup	Application Rules	Save and Restore	Logs	Logout
LAN Setup	Access Control	Firmware Update	Statistics	
Printer Setup	Firewall & DMZ	DDNS Setting	Active Session	
Time and Date	Advanced Wireless	System Check	LAN Clients	
Parental Control	Advanced Network	Schedules	Logout	
Logout	Routing	Log Settings		
	QoS Engine	Logout		
	Guest Zone			
	Traffic management			
	Logout			