

USER MANUAL

DIR-652

VERSION 1.0



D-Link[®]

WIRELESS

Preface

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

Manual Revisions

1.0	January 20, 2010	• Initial version

Trademarks

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

Copyright © 2008-2010 by D-Link Systems, Inc.

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

Table of Contents

Preface	i	Wireless Settings	21
Manual Revisions	i	Network Settings.....	22
Trademarks	i	DHCP Server Settings	23
Product Overview	1	DHCP Reservation.....	25
Package Contents	1	Virtual Server	27
System Requirements	1	Port Forwarding	29
Introduction.....	2	Application Rules	30
Features	3	QoS Engine	31
Hardware Overview	4	Network Filters.....	33
Connections.....	4	Access Control.....	34
LEDs	5	Access Control Wizard.....	34
Installation	6	Website Filters	37
Before you Begin	6	Inbound Filters	38
Wireless Installation Considerations.....	7	Firewall Settings	39
Getting Started	8	SPI	39
Configuration	9	NAT Endpoint Filtering	39
Web-based Configuration Utility	9	DMZ	39
Setup Wizard	10	SPI	40
Manual Configuration.....	14	NAT Endpoint Filtering	40
Dynamic (Cable)	14	DMZ	40
PPPoE (DSL)	15	Routing	41
PPTP	16	Advanced Wireless Settings	42
L2TP.....	18	Transmit Power	42
Static (assigned by ISP).....	20	Mode	42
		WISH Settings	43

Table of Contents

Wi-Fi Protected Setup (WPS)	45	Schedules	72
Advanced Network Settings.....	47	Device Information.....	73
UPnP.....	47	Logs	74
Internet Ping Block.....	47	Statistics	75
Internet Port Speed.....	47	Internet Sessions.....	75
Multicast Streams.....	47	Wireless	76
Guest Zone	48	IPv6.....	76
IPv6	49	Support	77
Link-Local Connectivity	49	Wireless Security.....	78
Static IPv6 (Stateful)	50	What is WPA?	78
Static IPv6 (Stateless).....	51	Wireless Security Setup Wizard	79
DHCPv6 (Stateful).....	52	Configure WPA-Personal (PSK).....	82
DHCPv6 (Stateless).....	53	Configure WPA-Enterprise (RADIUS)	83
IPv6 over PPPoE (Stateful).....	54	Using Windows® 7 and WPS for Wireless	
IPv6 over PPPoE (Stateless)	56	Configuration	85
6 to 4 Tunneling (Stateful).....	58	Connecting to a Wireless Network Using Windows®	
6 to 4 Tunneling (Stateless)	59	7.....	89
IPv6 in IPv4 Tunneling (Stateful).....	60	Connecting to a Wireless Network Using Windows	
IPv6 in IPv4 Tunneling (Stateless)	61	Vista®	92
Administrator Settings.....	62	Connecting to a Wireless Network	94
Time Settings.....	64	Using Windows® XP.....	94
SysLog	65	Troubleshooting	96
Email Settings.....	66	Wireless Basics	100
System Settings.....	68	What is Wireless?	101
Update Firmware	69	Tips.....	103
DDNS.....	70	Wireless Modes	104
System Check.....	71		

Table of Contents

Networking Basics	105
Check your IP address	105
Statically Assign an IP address	106
Technical Specifications.....	107
Certifications.....	108

Package Contents

- D-Link DIR-652 Wireless N Gigabit Home Router
- 2 Detachable Antennas
- Power Adapter
- Ethernet Cable - CAT5
- CD-ROM with Manual



Note: Using a power supply with a different voltage rating than the one included with the DIR-652 will cause damage and void the warranty.

System Requirements

- Ethernet-based Cable or DSL modem
- Windows®, Macintosh, or Linux-based operating system with an installed Ethernet adapter, or an 802.11n, 802.11g, or 802.11b wireless adapter
- Internet Explorer 6.0, Mozilla 1.7.12, Firefox 1.5, or Safari 1.0 (with Java 1.3.1 or higher) or higher (for configuration)
- Installation Wizard requires Windows® XP with Service Pack 2

Introduction

TOTAL PERFORMANCE

Combines award winning router features and 802.11n wireless technology to provide the best wireless performance.

TOTAL SECURITY

The most complete set of security features including Active Firewall and WPA2 to protect your network against outside intruders.

TOTAL COVERAGE

Provides greater wireless signal rates even at farther distances for best-in-class Whole Home Coverage.

ULTIMATE PERFORMANCE

The D-Link Wireless N Gigabit Home Router (DIR-652) is a 802.11n compliant device that delivers real world performance of up to 650% faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the Wireless N Gigabit Home Router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this Router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

EXTENDED WHOLE HOME COVERAGE

Powered by 802.11n technology, this high performance router provides superior coverage throughout your entire home while reducing dead spots. The Wireless N Gigabit Home Router is designed for use in bigger homes and for users who demand higher performance networking. Add a D-Link Wireless N notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

TOTAL NETWORK SECURITY

The Wireless N Gigabit Home Router supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA and WEP standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this Wireless N Gigabit Home Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

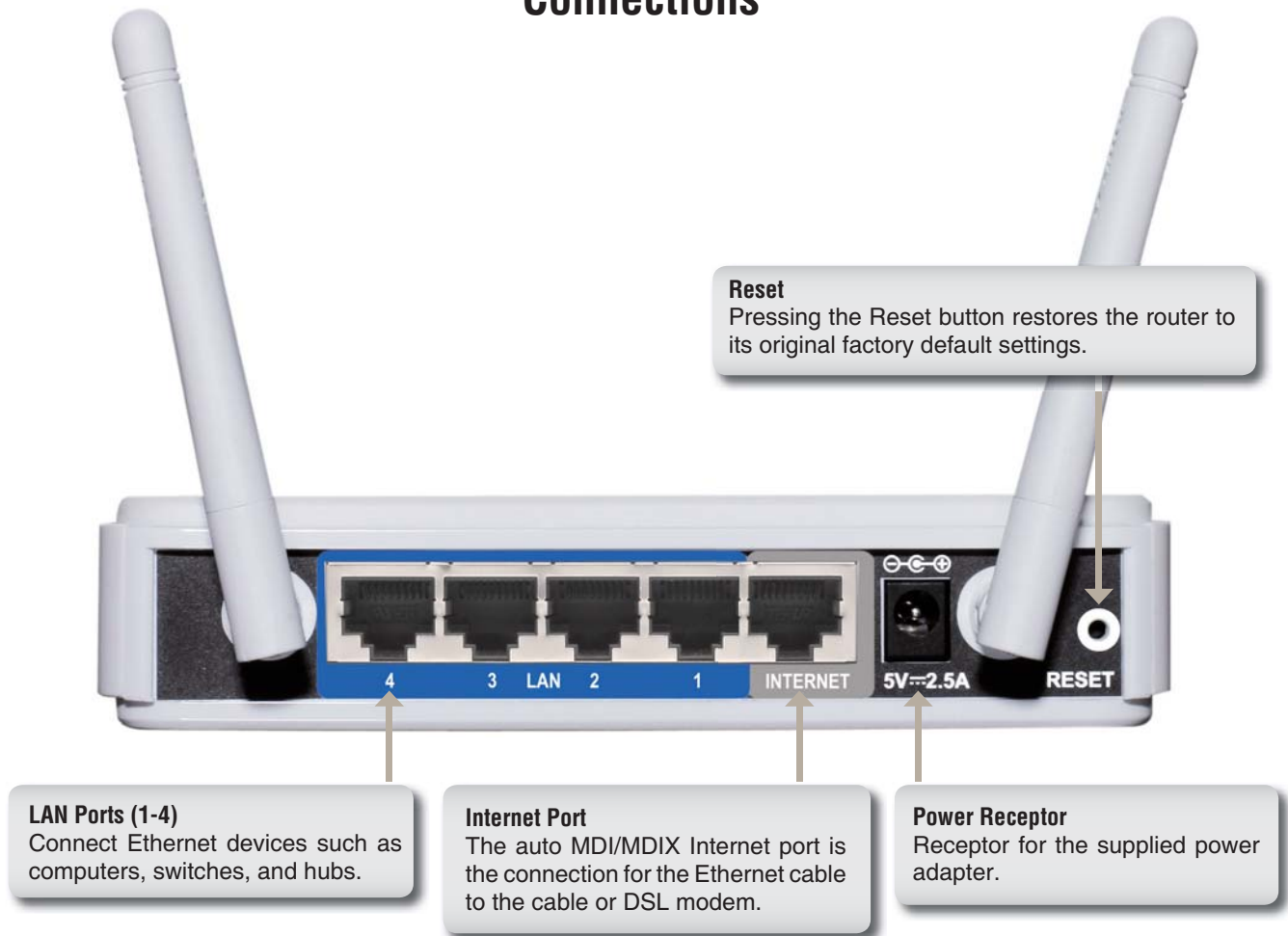
* Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.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

Features

- **Faster Wireless Networking** - The DIR-652 provides up to 300Mbps* wireless connection with other 802.11n 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 802.11n wireless router gives you the freedom of wireless networking at speeds 650% faster than 802.11g.
- **Compatible with 802.11g Devices** - The DIR-652 is still fully compatible with the IEEE 802.11g standard, so it can connect with existing 802.11g PCI, USB and Cardbus 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-652 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-652 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-652 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.

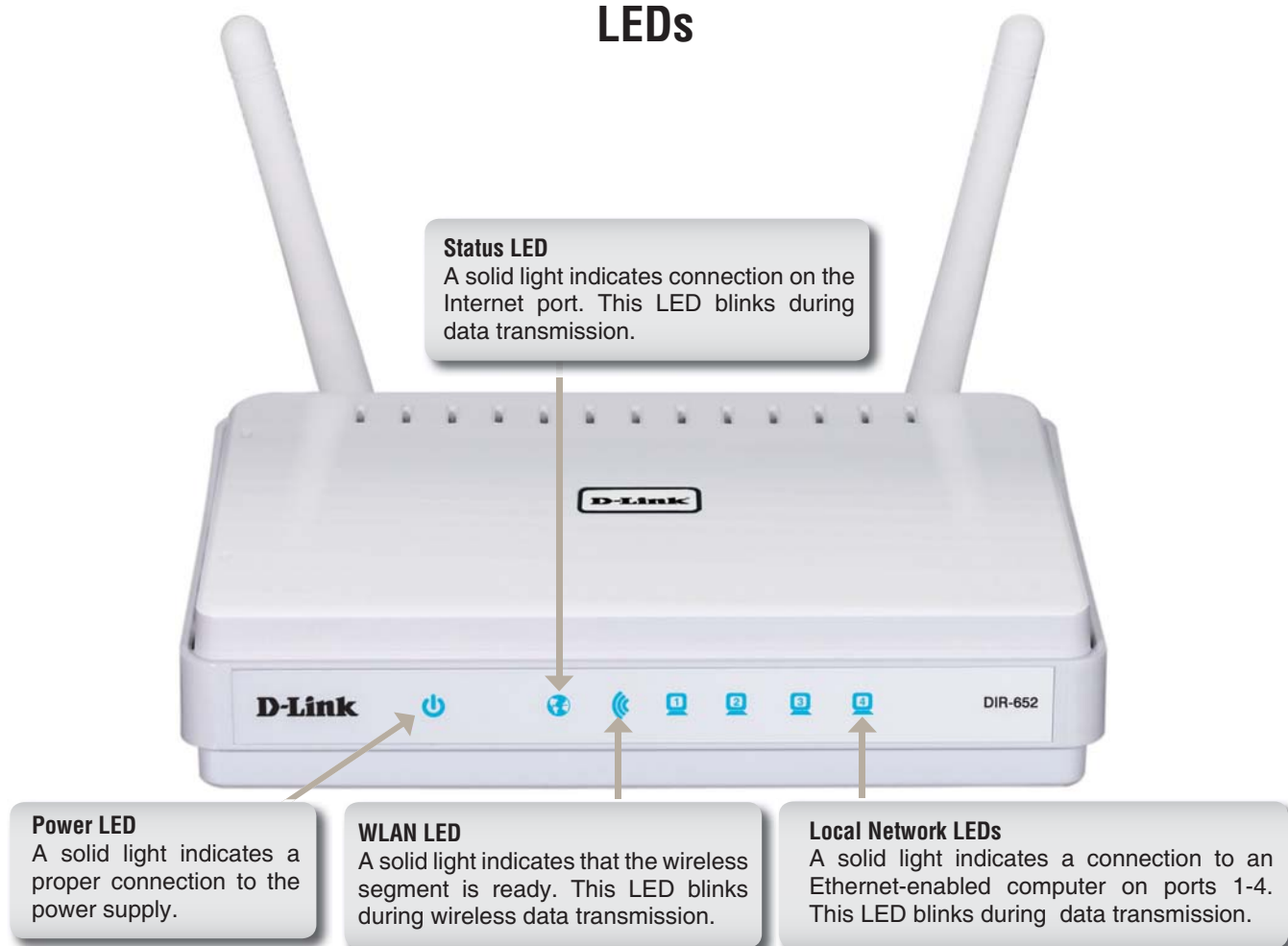
* Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.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

Hardware Overview Connections



Hardware Overview

LEDs



Installation

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

Before you Begin

Please configure the router with the computer that was last connected directly to your modem. Also, you can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).

If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.

Wireless Installation Considerations

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

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

Getting Started

The DIR-652 includes a Quick Router Setup Wizard CD. Follow the simple steps below to run the Setup Wizard to guide you quickly through the installation process.

Insert the included CD-ROM into your CD-ROM drive. The step-by-step instructions that follow are shown in Windows® XP. The steps and screens are similar for the other Windows operating systems.

If the CD Autorun function does not automatically start on your computer, go to **Start > Run....** In the run box type **"D:\D-Link.exe"** (where **D:** represents the drive letter of your CD-ROM drive).

When the autorun screen appears, click on the **Start** button.



Note: It is recommended to write down the SSID and Security Key, followed by the login password on the provided CD holder.

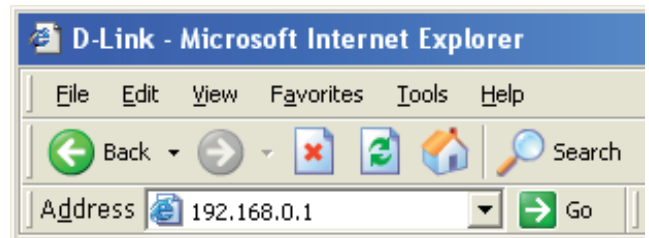
Configuration

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

Web-based Configuration Utility

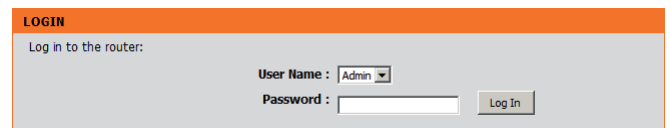
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.0.1).

You may also connect using the NetBIOS name in the address bar (<http://dlinkrouter>).



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

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



Setup Wizard

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

If you want to enter your settings without running the wizard, click **Manual Configuration** and skip to page 14.

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

If you want to configure your wireless settings, click **Launch Wireless Security Setup Wizard** and skip to page 63.

INTERNET CONNECTION

There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.

INTERNET CONNECTION SETUP WIZARD

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

[Internet Connection Setup Wizard](#)

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

MANUAL INTERNET CONNECTION OPTIONS

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

[Manual Internet Connection Setup](#)

WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

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

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

[Wireless Network Setup Wizard](#)

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

[Add Wireless Device with WPS](#)

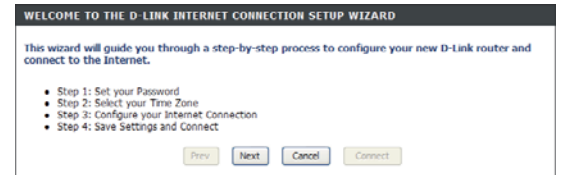
MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with W-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

[Manual Wireless Network Setup](#)

Section 3 - Configuration

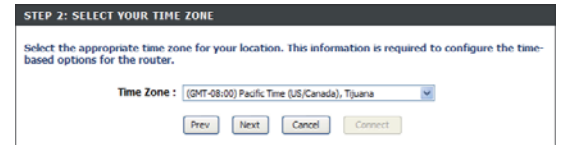
Click **Next** to continue.



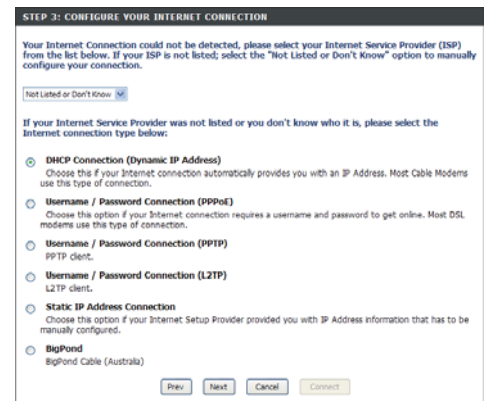
Create a new password and then click **Next** to continue.



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



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



Section 3 - Configuration

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

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

DHCP CONNECTION (DYNAMIC IP ADDRESS)

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

MAC Address : 00:00:00:00:00:00 (optional)
Clone Your PC's MAC Address

Host Name :

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

Prev Next Cancel Connect

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

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

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

SET USERNAME AND PASSWORD CONNECTION (PPPoE)

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

Address Mode : Dynamic IP Static IP

IP Address : 0.0.0.0

User Name :

Password : *****

Verify Password : *****

Service Name : (optional)

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

Prev Next Cancel Connect

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

SET USERNAME AND PASSWORD CONNECTION (PPTP)

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

Address Mode : Dynamic IP Static IP

PPTP IP Address : 0.0.0.0

PPTP Subnet Mask : 255.255.255.0

PPTP Gateway IP Address : 0.0.0.0

PPTP Server IP Address (may be same as gateway) : 0.0.0.0

User Name :

Password : *****

Verify Password : *****

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

Prev Next Cancel Connect

Section 3 - Configuration

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

SET USERNAME AND PASSWORD CONNECTION (L2TP)

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

Address Mode: Dynamic IP Static IP

L2TP IP Address:

L2TP Subnet Mask:

L2TP Gateway IP Address:

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

User Name:

Password:

Verify Password:

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

SET STATIC IP ADDRESS CONNECTION

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

IP Address:

Subnet Mask:

Gateway Address:

Primary DNS Address:

Secondary DNS Address:

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

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

SETUP COMPLETE!

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

Manual Configuration Dynamic (Cable)

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

Enable Advanced DNS Service: Advanced Domain Name System (DNS) services enhances your Internet performance by getting you the information and web pages you are looking for faster and more reliably. In addition, it improves your overall Internet experience by correcting many common typo mistakes automatically, taking you where you intended to go and saving you valuable time.

Disclaimer: D-Link makes no warranty as to the availability, reliability, functionality and operation of the Advanced DNS service or its features. The Host Name is optional but may be required by some ISPs. Leave blank if you are not sure.

Use UnICASTing: Check the box if you are having problems obtaining an IP address from your ISP.

Primary/Secondary DNS Server: Enter the Primary and secondary DNS server IP addresses assigned by your ISP. These addresses are usually obtained automatically from your ISP. Leave at 0.0.0.0 if you did not specifically receive these from your ISP.

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

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

The screenshot shows the configuration interface for the Internet Connection Type. It is divided into three sections:

- INTERNET CONNECTION TYPE:** A dropdown menu is set to "Dynamic IP (DHCP)".
- ADVANCED DNS SERVICE:** A checkbox for "Enable Advanced DNS Service" is checked.
- DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :** This section contains several fields and a button:
 - Host Name: []
 - Use UnICASTing: (compatibility for some DHCP Servers)
 - Primary DNS Server: [0.0.0.0]
 - Secondary DNS Server: [0.0.0.0]
 - MTU: [1500] (bytes) MTU default = 1500
 - MAC Address: [00:16:17:44:4a:ef]
 - Clone Your PC's MAC Address button

Internet Setup PPPoE (DSL)

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

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

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

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

User Name: Enter your PPPoE user name.

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

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

Reconnection Mode: Select either **Always on**, **On demand**, or **Manual**.

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

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

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

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

INTERNET CONNECTION TYPE

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

My Internet Connection is : PPPoE (Username / Password) ▾

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

PPPOE INTERNET CONNECTION TYPE :

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

Address Mode : Dynamic IP Static IP

IP Address :

Username :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server : (optional)

Secondary DNS Server : (optional)

MTU : (bytes) MTU default = 1492

MAC Address :

Internet Setup PPTP

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

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

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

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

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

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

Username: Enter your PPTP username.

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

Reconnect Mode: Select either **Always on**, **On demand**, or **Manual**.

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

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

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

INTERNET CONNECTION TYPE

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

My Internet Connection is : PPTP (Username / Password) ▾

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

PPTP INTERNET CONNECTION TYPE :

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

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1400

MAC Address :

Section 3 - Configuration

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

Internet Setup L2TP

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

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

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

L2TP Subnet

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

L2TP Gateway: Enter the Gateway IP Address provided by your ISP.

L2TP Server IP: Enter the Server IP provided by your ISP (optional).

Username: Enter your L2TP username.

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

Reconnect Mode: Select either **Always on**, **On demand**, or **Manual**.

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

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

INTERNET CONNECTION TYPE

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

My Internet Connection is : L2TP (Username / Password) ▾

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

L2TP INTERNET CONNECTION TYPE :

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

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1400

MAC Address :

Clone Your PC's MAC Address

Section 3 - Configuration

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

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

Internet Setup Static (assigned by ISP)

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

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

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

Default Gateway: Enter the Gateway assigned by your ISP.

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

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

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

INTERNET CONNECTION TYPE

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

My Internet Connection is : ▼

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

STATIC IP ADDRESS INTERNET CONNECTION TYPE :

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

IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1500

MAC Address :

Wireless Settings

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

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

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

Enable Auto Channel Scan: The setting can be selected to allow the DIR-652 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-652. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

802.11 Mode: Select one of the following:
802.11g Only - Select if all of your wireless clients are 802.11g.
802.11n Only - Select only if all of your wireless clients are 802.11n.
Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 11g wireless clients.

Channel Width: Select the Channel Width:
Auto 20/40 - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.
20MHz - Select if you are not using any 802.11n wireless clients.
40MHz - Select if using only 802.11n wireless clients.

Transmission Rate: Select the transmit rate. It is strongly suggested to select **Best (Auto)** for best performance.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-652. If Invisible is selected, the SSID of the DIR-652 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-652

WIRELESS

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

WIRELESS NETWORK SETTINGS

Enable Wireless : Always New Schedule

Wireless Network Name : (Also called the SSID)

802.11 Mode : 802.11n only

Enable Auto Channel Scan :

Wireless Channel : 2.437 GHz - CH 6

Transmission Rate : Best (automatic) (Mbit/s)

Channel Width : 20 MHz

Visibility Status : Visible Invisible

WIRELESS SECURITY MODE

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

Security Mode : None

Network Settings

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

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

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

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

Local Domain: Enter the Domain name (Optional).

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

The screenshot shows two configuration pages. The top page is titled "NETWORK SETTINGS" and contains a text box with instructions: "Use this section to configure the internal network settings of your router and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again." Below the text are two buttons: "Save Settings" and "Don't Save Settings".

The bottom page is titled "ROUTER SETTINGS" and contains the same instructions. Below the text are four input fields: "Router IP Address" with the value "192.168.0.1", "Subnet Mask" with the value "255.255.255.0", "Local Domain Name" which is empty and followed by "(optional)", and "Enable DNS Relay" which has a checked checkbox.

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-652 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-652. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

Enable DHCP Server: Check this box to enable the DHCP server on your router. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

Note: If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

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

Always Broadcast: Enable this feature to broadcast your networks DHCP server to LAN/WLAN clients.

NetBIOS Announcement: NetBIOS allows LAN hosts to discover all other computers within the network, enable this feature to allow the DHCP Server to offer NetBIOS configuration settings.

Learn NetBIOS from WAN: Enable this feature to allow WINS information to be learned from the WAN side, disable to allow manual configuration.

DHCP SERVER SETTINGS

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

Enable DHCP Server:

DHCP IP Address Range: to

DHCP Lease Time: (minutes)

Always broadcast: (compatibility for some DHCP Clients)

NetBIOS announcement:

Learn NetBIOS from WAN:

NetBIOS Scope: (optional)

NetBIOS node type :

- Broadcast only (use when no WINS servers configured)
- Point-to-Point (no broadcast)
- Mixed-mode (Broadcast then Point-to-Point)
- Hybrid (Point-to-Point then Broadcast)

Primary WINS IP Address:

Secondary WINS IP Address:

NetBIOS Scope: This feature allows the configuration of a NetBIOS 'domain' name under which network hosts operates. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated."

NetBIOS Mode Type: Select the different type of NetBIOS node: **Broadcast only**, **Point-to-Point**, **Mixed-mode**, and **Hybrid**.

Primary/Secondary WINS IP Address: Enter your Primary (and Secondary) WINS IP address(es).

DHCP Reservation

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

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

Enable: Check this box to enable the reservation.

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

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

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

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

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

Number of Dynamic DHCP Clients: In this section you can see what LAN devices are currently leasing IP addresses.

Revoke: Click **Revoke** to cancel the lease for a specific LAN device and free an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

ADD DHCP RESERVATION

Enable:

Computer Name: << Computer Name ▾

IP Address:

MAC Address:

DHCP RESERVATIONS LIST			
Enable	Computer Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS: 2					
Hardware Address	Assigned IP	Hostname	Expires		
00:0c:f1:fe:ee:cd	192.168.0.197	PMLab16	22 Hours 48 Minutes	Revoke	Reserve
00:16:17:44:4a:d9	192.168.0.199	PMLab15	14 Hours 54 Minutes	Revoke	Reserve

Note: *The Revoke option will not disconnect a PC with a current network session from the network; you would need to use MAC Address Filter to do that. Revoke will only free up a DHCP Address for the very next requester. If the previous owner is still available, those two devices may both receive an IP Address Conflict error, or the second device may still not receive an IP Address; in that case, you may still need to extend the "DHCP IP Address Range" to address the issue, it is located in the DHCP Server section.*

Reserve: The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

Virtual Server

The DIR-652 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DIR-652 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-652 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-652 redirects the external service request to the appropriate server within the LAN network.

The DIR-652 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

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

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

Section 3 - Configuration

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

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

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

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

Protocol Type: Select **TCP**, **UDP**, or **Both** or from the drop-down menu.

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

Inbound Filter: Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

D-Link

DIR-652 // SETUP ADVANCED TOOLS STATUS SUPPORT

VIRTUAL SERVER

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

Save Settings Don't Save Settings

24 -- VIRTUAL SERVERS LIST

	Name	IP Address	Private Port	Public Port	Protocol	Schedule	Inbound Filter
<input type="checkbox"/>	<< Application Nam	<< Computer Name	0	0	TCP	Always	Allow All
<input type="checkbox"/>	<< Application Nam	<< Computer Name	0	0	TCP	Always	Allow All
<input type="checkbox"/>	<< Application Nam	<< Computer Name	0	0	TCP	Always	Allow All
<input type="checkbox"/>	<< Application Nam	<< Computer Name	0	0	TCP	Always	Allow All
<input type="checkbox"/>	<< Application Nam	<< Computer Name	0	0	TCP	Always	Allow All

Helpful Hints...

Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.

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

Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools > Schedules** screen and create a new schedule.

Select a filter that restricts the Internet hosts that can access this virtual server to hosts that you trust.

Port Forwarding

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

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

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

TCP/UDP: Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.

Example: 24,1009,3000-4000

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

Inbound Filter: Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.



Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DIR-652. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-652 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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

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

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

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

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

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

D-Link

DIR-652 // SETUP ADVANCED TOOLS STATUS SUPPORT

APPLICATION RULES

This option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

Save Settings Don't Save Settings

24 -- APPLICATION RULES

	Name	Application	Port	Traffic Type	Schedule
<input type="checkbox"/>		<< Application Name	Trigger 0	TCP	Always
			Firewall 0	TCP	
<input type="checkbox"/>		<< Application Name	Trigger 0	TCP	Always
			Firewall 0	TCP	
<input type="checkbox"/>		<< Application Name	Trigger 0	TCP	Always
			Firewall 0	TCP	

Helpful Hints...

Use this feature if you are trying to execute one of the listed network applications and it is not communicating as expected.

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools -> Schedules**

QoS Engine

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.

Enable Traffic Shaping: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Uplink Speed: This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

Measured Uplink Speed: This displays the detected uplink speed.

Manual Uplink Speed: The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbps/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.

The screenshot shows the D-Link DIR-652 web interface. The left sidebar contains a navigation menu with items like VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE (highlighted), NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WISH, WI-FI PROTECTED SETUP, ADVANCED NETWORK, GUEST ZONE, and IPV6. The main content area is titled 'QOS ENGINE' and includes a description: 'Use this section to configure D-Link's QoS Engine powered by QoS Engine™ Technology. This QoS Engine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.' Below this are 'Save Settings' and 'Don't Save Settings' buttons. The 'WAN TRAFFIC SHAPING' section has three checked options: 'Enable Traffic Shaping', 'Automatic Uplink Speed', and 'Measured Uplink Speed' (set to 'Not Estimated'). The 'Manual Uplink Speed' is set to '128 kbps'. The 'QOS ENGINE SETUP' section has three checked options: 'Enable QoS Engine', 'Automatic Classification', and 'Dynamic Fragmentation'. The '10 -- QOS ENGINE RULES' section shows two rule entries, each with a checkbox, name, priority (1), protocol (TCP), and IP/port ranges.

Section 3 - Configuration

Enable QoS Engine: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Classification: This option is enabled by default. This will allow your router to automatically determine the network priority of running programs.

Dynamic Fragmentation: This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones.

The screenshot shows the D-Link DIR-652 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections, with QoS ENGINE selected. The main content area is divided into several sections:

- QOS ENGINE:** A section with a description and two buttons: "Save Settings" and "Don't Save Settings".
- WAN TRAFFIC SHAPING:** Contains checkboxes for "Enable Traffic Shaping" (checked), "Automatic Uplink Speed" (checked), and "Dynamic Fragmentation" (checked). It also shows "Measured Uplink Speed" as "Not Estimated" and "Manual Uplink Speed" set to "128 kbps".
- QOS ENGINE SETUP:** Contains checkboxes for "Enable QoS Engine" (checked), "Automatic Classification" (checked), and "Dynamic Fragmentation" (checked).
- 10 -- QOS ENGINE RULES:** A table with two rows of rule configurations. Each row includes fields for Name, Priority (set to 1), Protocol (set to TCP), Local IP Range (0.0.0.0 to 255.255.255.255), Local Port Range (0 to 65535), Remote IP Range (0.0.0.0 to 255.255.255.255), and Remote Port Range (0 to 65535).

On the right side of the interface, there is a "Helpful Hints ..." section with text explaining that if the Measured Uplink Speed is incorrect, disabling Automatic Uplink Speed and entering the Manual Uplink Speed may be required for optimal performance.

Network Filters

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

Configure MAC Filtering: Select Turn MAC Filtering Off, allow MAC addresses listed below, or deny MAC addresses listed below from the drop-down menu.

MAC Address: Enter the MAC address you would like to filter. To find the MAC address on a computer, please refer to the Networking Basics section in this manual.

Select a DHCP client from the drop-down menu

DHCP Client List: and click << to copy that MAC Address.

The screenshot shows the D-Link DIR-652 web interface. The main navigation menu includes: SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER (selected), ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WISH, WIFI PROTECTED SETUP, ADVANCED NETWORK, GUEST ZONE, and IPV6.

The main content area is titled "MAC ADDRESS FILTER". It contains a text box explaining the feature: "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." Below this text are two buttons: "Save Settings" and "Don't Save Settings".

Below the main content is a section titled "24 --- MAC FILTERING RULES". It includes a dropdown menu to "Configure MAC Filtering below:" with the option "Turn MAC Filtering OFF" selected. Below this is a table with two columns: "MAC Address" and "DHCP Client List". Each row in the table has an input field for the MAC address, a "<<" button, a dropdown menu for the DHCP Client List (all showing "Computer Name"), and a "Clear" button.

On the right side of the interface, there is a "Helpful Hints..." section. It contains two paragraphs of text: "Create a list of MAC addresses that you would either like to allow or deny access to your network." and "Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu, then click the arrow to add that device's MAC address to the list." Below this is a "More..." link.

Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

Add Policy: Click the **Add Policy** button to start the Access Control Wizard.



Access Control Wizard

Click **Next** to continue with the wizard.



Section 3 - Configuration

Enter a name for the policy and then click **Next** to continue.

The screenshot shows a window titled "STEP 1: CHOOSE POLICY NAME". Below the title bar, it says "Choose a unique name for your policy." There is a text input field labeled "Policy Name:" which is currently empty. At the bottom of the window, there are four buttons: "Prev", "Next", "Save", and "Cancel".

Select a schedule (I.E. Always) from the drop-down menu and then click **Next** to continue.

The screenshot shows a window titled "STEP 2: SELECT SCHEDULE". Below the title bar, it says "Choose a schedule to apply to this policy." There is a drop-down menu currently showing "Always" with a small "v" icon to its right. Below the menu is a text field containing "Details: Always". At the bottom of the window, there are four buttons: "Prev", "Next", "Save", and "Cancel".

Enter the following information and then click **Next** to continue.

- **Address Type** - Select IP address, MAC address, or Other Machines.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.

The screenshot shows a window titled "STEP 3: SELECT MACHINE". Below the title bar, it says "Select the machine to which this policy applies." and "Specify a machine with its IP or MAC address, or select 'Other Machines' for machines that do not have a policy." There are three radio buttons for "Address Type": "IP" (which is selected), "MAC", and "Other Machines". Below this, there are two rows of input fields. The first row is for "IP Address" with a value of "0.0.0.0" and a "Computer Name" dropdown menu. The second row is for "Machine Address" with a "Computer Name" dropdown menu. Below these fields is a button labeled "Copy Your PC's MAC Address". At the bottom of the window, there are four buttons: "Prev", "Next", "Save", and "Cancel".

Section 3 - Configuration

Select the filtering method and then click **Next** to continue.

STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

Method: Log Web Access Only Block All Access Block Some Access

Apply Web Filter:

Apply Advanced Port Filters:

Prev Next Save Cancel

Enter the rule:

- Enable** - Check to enable the rule.
- Name** - Enter a name for your rule.
- Dest IP Start** - Enter the starting IP address.
- Dest IP End** - Enter the ending IP address.
- Protocol** - Select the protocol.
- Dest Port Start** - Enter the starting port number.
- Dest Port End** - Enter the ending port number.

STEP 5: PORT FILTER

Add Port Filters Rules.

Specify rules to prohibit access to specific IP addresses and ports.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535

Prev Next Save Cancel

To enable web logging, select **Enabled**.

Click **Save** to save the access control rule.

STEP 6: CONFIGURE WEB ACCESS LOGGING

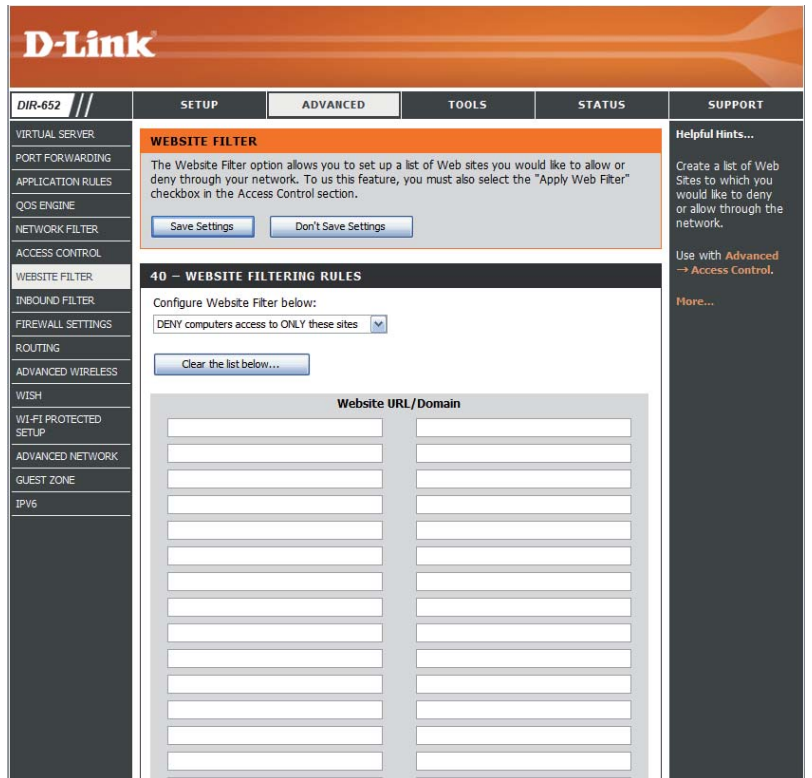
Web Access Logging: Disabled Enabled

Prev Next Save Cancel

Website Filters

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

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



Inbound Filters

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound Filters can be used with Virtual Server, Port Forwarding, or Remote Administration features.

Name: Enter a name for the inbound filter rule.

Action: Select **Allow** or **Deny**.

Enable: Check to enable rule.

Source IP Start: Enter the starting IP address. Enter 0.0.0.0 if you do not want to specify an IP range.

Source IP End: Enter the ending IP address. Enter 255.255.255.255 if you do not want to specify and IP range.

Save: Click the **Save** button to apply your settings. You must click **Save Settings** at the top to save the settings.

Inbound Filter Rules List: This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.

D-Link

DIR-652 // SETUP ADVANCED TOOLS STATUS SUPPORT

INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.

ADD INBOUND FILTER RULE

Name :

Action :

Remote IP Range	Enable	Remote IP Start	Remote IP End
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	<input type="checkbox"/>	0.0.0.0	255.255.255.255

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range

Helpful Hints...

Give each rule a **Name** that is meaningful to you.

Each rule can either **Allow** or **Deny** access from the WAN.

Up to eight ranges of WAN IP addresses can be controlled by each rule. The checkbox by each IP range can be used to disable ranges already defined.

The starting and ending IP addresses are WAN-side address.

Click the **Add** or **Update** button to store a finished rule in the Rules List below.

Click the **Edit** icon in the Rules List to change a rule.

Click the **Delete** icon in the Rules List to permanently remove a rule.

Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-652 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

Enable SPI: SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

NAT Endpoint Filtering: Select one of the following for TCP and UDP ports:

Endpoint Independent - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

Address Restricted - Incoming traffic must match the IP address of the outgoing connection.

Address + Port Restriction - Incoming traffic must match the IP address and port of the outgoing connection.

The screenshot shows the D-Link DIR-652 Firewall Settings page. The interface includes a navigation menu on the left with options like VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS (selected), ROUTING, ADVANCED WIRELESS, WISH, WI-FI PROTECTED SETUP, ADVANCED NETWORK, GUEST ZONE, and IPV6. The main content area is titled 'FIREWALL SETTINGS' and contains several sections:

- FIREWALL SETTINGS:** A summary box stating 'The Firewall Settings allow you to set a single computer on your network outside of the router.' with 'Save Settings' and 'Don't Save Settings' buttons.
- FIREWALL SETTINGS:** A section where 'Enable SPI' is checked.
- NAT ENDPOINT FILTERING:** A section with two sub-sections:
 - UDP Endpoint Filtering:** Radio buttons for 'Endpoint Independent', 'Address Restricted' (selected), and 'Port And Address Restricted'.
 - TCP Endpoint Filtering:** Radio buttons for 'Endpoint Independent', 'Address Restricted', and 'Port And Address Restricted' (selected).
- ANTI-SPOOF CHECKING:** A section where 'Enable anti-spoof checking' is unchecked.
- DMZ HOST:** A section explaining the DMZ option and providing a 'Note' about security risks. It includes an 'Enable DMZ Host' checkbox (unchecked) and a 'DMZ IP Address' field with a dropdown menu for 'Computer Name'.

On the right side, there is a 'Helpful Hints...' section with text: 'Enable the DMZ option only as a last resort. If you are having trouble using an application from a computer behind the router, first try opening ports associated with the application in the Virtual Server or Port Forwarding sections.' and a 'More...' link.

Section 3 - Configuration

Enable DMZ Host: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Note: *Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.*

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

The screenshot shows the D-Link DIR-652 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections, with FIREWALL SETTINGS selected. The main content area is divided into several sections:

- FIREWALL SETTINGS:** A summary box stating "The Firewall Settings allow you to set a single computer on your network outside of the router." with "Save Settings" and "Don't Save Settings" buttons.
- FIREWALL SETTINGS:** A section with "Enable SPI:
- NAT ENDPOINT FILTERING:** A section with two sub-sections:
 - UDP Endpoint Filtering:** Radio buttons for "Endpoint Independent", "Address Restricted" (selected), and "Port And Address Restricted".
 - TCP Endpoint Filtering:** Radio buttons for "Endpoint Independent", "Address Restricted", and "Port And Address Restricted".
- ANTI-SPOOF CHECKING:** A section with "Enable anti-spoof checking:
- DMZ HOST:** A section with a description: "The DMZ (Demilitarized Zone) option lets you 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." and a note: "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." Below this are fields for "Enable DMZ Host: " and "DMZ IP Address: [0.0.0.0] << [Computer Name]".

On the right side, there is a "Helpful Hints..." section with text: "Enable the DMZ option only as a last resort. If you are having trouble using an application from a computer behind the router, first try opening ports associated with the application in the Virtual Server or Port Forwarding sections." and a "More..." link.

Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

Destination IP: Enter the IP address of packets that will take this route.

Netmask: Enter the netmask of the route, please note that the octets must match your destination IP address.

Gateway: Enter your next hop gateway to be taken if this route is used.

Metric: The route metric is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

Interface: Select the interface that the IP packet must use to transit out of the router when this route is used.

D-Link

DIR-652 // SETUP ADVANCED TOOLS STATUS SUPPORT

ROUTING :
This Routing page allows you to specify custom routes that determine how data is moved around your network.
Save Settings Don't Save Settings

32 --ROUTE LIST

	Name	Destination IP	Netmask	Gateway	Metric	Interface
<input type="checkbox"/>		0.0.0.0			1	WAN
<input type="checkbox"/>		0.0.0.0			1	WAN
<input type="checkbox"/>		0.0.0.0			1	WAN
<input type="checkbox"/>		0.0.0.0			1	WAN
<input type="checkbox"/>		0.0.0.0			1	WAN
<input type="checkbox"/>		0.0.0.0			1	WAN
<input type="checkbox"/>		0.0.0.0			1	WAN

Helpful Hints...
Each route has a check box next to it, check this box if you want the route to be enabled.
The name field allows you to specify a name for identification of this route, e.g. "Network 2".
The destination IP address is the address of the host or network you wish to reach.
The netmask field identifies the portion of the destination IP in use.
The gateway IP address is the IP address of the router, if any, used to reach the specified destination.
More...

Advanced Wireless Settings

Transmit Power: Set the transmit power of the antennas.

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

RTS Threshold: This value should remain at its default setting of 2342. If inconsistent data flow is a problem, only a minor modification should be made.

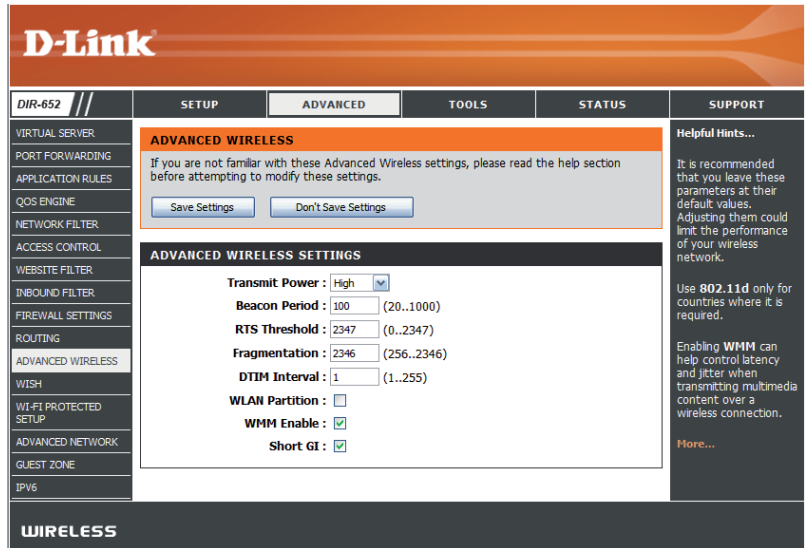
Fragmentation: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

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

WLAN Partition: Enable this option to prevent associated wireless clients from communicating with each other.

WMM Function: WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.



WISH Settings

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

Enable WISH: Enable this option if you want to allow WISH to prioritize your traffic.

HTTP: Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center: Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic: When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

The screenshot shows the D-Link DIR-652 configuration interface. The 'WISH' section is active, with 'Enable WISH' checked. Under 'PRIORITY CLASSIFIERS', 'HTTP' and 'Windows Media Center' are checked, while 'Automatic' is unchecked. The 'WISH RULES' section contains a table with three rows, each representing a rule configuration.

Name	Priority	Protocol	Host 1 IP Range	Host 2 IP Range	Host 1 Port Range	Host 2 Port Range
<input type="checkbox"/>	Best Effort (BE)	TCP	0.0.0.0 to 255.255.255.255	0.0.0.0 to 255.255.255.255	0 to 65535	0 to 65535
<input type="checkbox"/>	Best Effort (BE)	TCP	0.0.0.0 to 255.255.255.255	0.0.0.0 to 255.255.255.255	0 to 65535	0 to 65535
<input type="checkbox"/>	Best Effort (BE)	TCP	0.0.0.0 to 255.255.255.255	0.0.0.0 to 255.255.255.255	0 to 65535	0 to 65535

WISH Rules: A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

Name: Create a name for the rule that is meaningful to you.

Priority: The priority of the message flow is entered here. The four priorities are defined as:

- BK:** Background (least urgent)
- BE:** Best Effort.
- VI:** Video
- VO:** Voice (most urgent)

Protocol: The protocol used by the messages.

Host IP Range: The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host Port Range: The rule applies to a flow of messages for which host's port number is within the range set here.

The screenshot shows a configuration window titled "24 -- WISH RULES". It contains several input fields and dropdown menus:

- Name:** An empty text input field.
- Priority:** A dropdown menu set to "Best Effort (BE)".
- Protocol:** A dropdown menu set to "TCP".
- Host 1 IP Range:** Two text input fields, the first containing "0.0.0.0" and the second containing "255.255.255.255", with "to" between them.
- Host 1 Port Range:** Two text input fields, the first containing "0" and the second containing "65535", with "to" between them.
- Host 2 IP Range:** Two text input fields, the first containing "0.0.0.0" and the second containing "255.255.255.255", with "to" between them.
- Host 2 Port Range:** Two text input fields, the first containing "0" and the second containing "65535", with "to" between them.

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy, as depressing a button for the Push-Button Method or correctly entering the 8-digit code for the PIN code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

Enable: Enable the Wi-Fi Protected Setup feature.

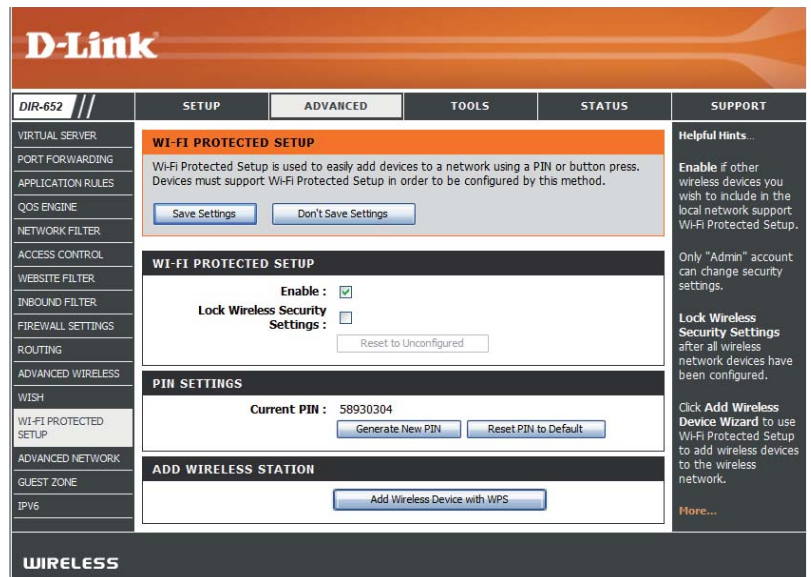
Lock Wireless Security Settings: Locking the wireless security settings prevents the settings from being changed by the Wi-Fi Protected Setup feature of the router. Devices can still be added to the network using Wi-Fi Protected Setup. However, the settings of the network will not change once this option is checked.

PIN Settings: A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.

Current PIN: Shows the current value of the router’s PIN.

Generate New PIN: Creates a random number that is a valid PIN. This becomes the router’s PIN. You can then use this PIN when creating a connection using the WPS-PIN method.

Reset PIN to Default: Restores the default PIN of the router.

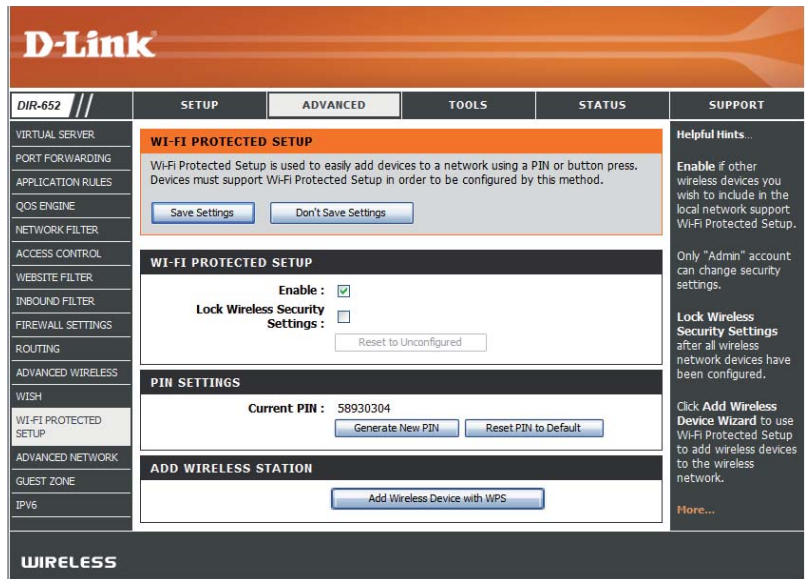


Add Wireless Station: This Wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

Add Wireless Device Wizard: Start the wizard.



Advanced Network Settings

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

PPPoE Pass Through: This feature enables the Router to allow a “dial-up” or separate bridged PPP connection to an individual PC. In this instance the Router will serve as a bridge.

Internet Ping: Unchecking the box will not allow the DIR-652 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be “pinged.”

Internet Port Speed: You may set the port speed of the Internet port to 10Mbps, 100Mbps, 1000Mbps, or Auto 10/100/1000Mbps. Some older cable or DSL modems may require you to set the port speed to 10Mbps.

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

The screenshot shows the D-Link DIR-652 Advanced Network Settings page. The left sidebar contains a navigation menu with options: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WISH, WI-FI PROTECTED SETUP, ADVANCED NETWORK, GUEST ZONE, and IPV6. The main content area is titled 'ADVANCED NETWORK' and includes a warning: 'If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.' Below this are buttons for 'Save Settings' and 'Don't Save Settings'. The settings are organized into sections: UPNP (with 'Enable UPnP' checked), PPPoE PASS THROUGH (with 'Enable PPPoE Pass Through' checked), WAN PING (with 'Enable WAN Ping Respond' checked, 'WAN Ping Inbound Filter' set to 'Allow All', and 'Details' set to 'Allow_All'), WAN PORT SPEED (with 'WAN Port Speed' set to '10/100/1000Mbps Auto'), and MULTICAST STREAMS (with 'Enable Multicast Streams' unchecked). A 'Helpful Hints...' section on the right provides additional information about UPnP and WAN Ping.

Guest Zone

The Guest Zone feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network.

Enable Guest Zone: Check to enable the Guest Zone feature.

Schedule: The schedule of time when the Guest Zone will be active. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the section, or by clicking the **Tools > Schedules** button.

Wireless Band: This shows which wireless band will be used for the Guest Zone.

Wireless Network Name: Enter a wireless network name (SSID) that is different from your main wireless network.

Enable Routing Between Zones: Check to allow network connectivity between the different zones created.

Security Mode: Select the type of security or encryption you would like to enable for the guest zone.

The screenshot shows the D-Link DIR-652 web interface. The top navigation bar includes 'DIR-652', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'GUEST ZONE' highlighted. The main content area is titled 'GUEST ZONE' and contains the following text: '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.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'GUEST ZONE SELECTION' section contains the following configuration options:

- Enable Guest Zone: Always
- Wireless Band: 2.4GHz Band
- Wireless Network Name: dlink_guest (Also called the SSID)
- Enable Routing Between Zones:
- Security Mode: None

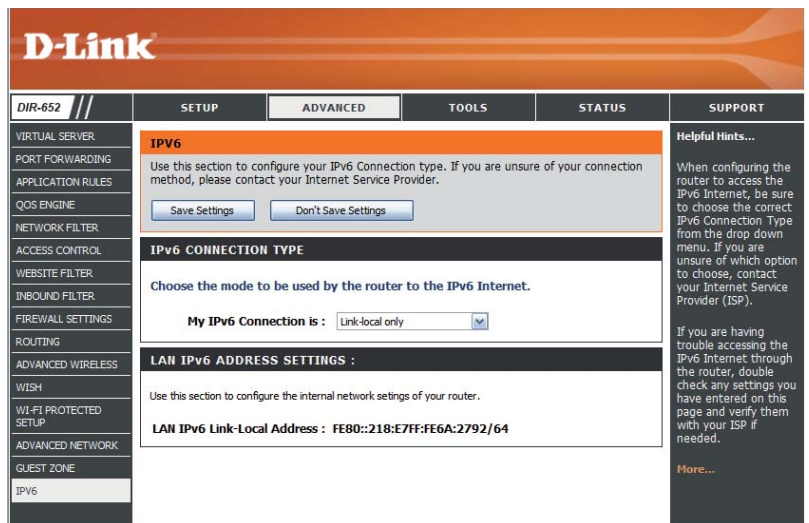
The right sidebar contains 'Helpful Hints...' and 'More...' links. The footer of the page reads 'WIRELESS' and 'Copyright © 2004-2008 D-Link Corporation, Inc.'

IPv6

Link-Local Connectivity

My IPv6 Connection: Select **Link-Local Only** from the drop-down menu.

LAN IPv6 Displays the IPv6 address of the **Address Settings:** router.



Static IPv6 (Stateful)

IPv6 Connection Type: Select **Static IPv6** from the drop-down menu.

WAN IPv6 Address Settings: Enter the address settings supplied by your Internet provider (ISP).

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

IPv6 Address Range Start: Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range End: Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 Address Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	Static IPv6

WAN IPv6 ADDRESS SETTINGS :	
Enter the IPv6 address information provided by your Internet Service Provider (ISP).	
IPv6 Address :	<input type="text"/>
Subnet Prefix Length :	<input type="text"/>
Default Gateway :	<input type="text"/>
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>

LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.	
LAN IPv6 Address :	<input type="text"/> /64
LAN IPv6 Link-Local Address :	FE80::240:F4FF:FE03:1A9C/64

ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable Autoconfiguration :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	Stateful (DHCPv6)
IPv6 Address Range(Start):	<input type="text"/> : <input type="text"/> /64
IPv6 Address Range(End):	<input type="text"/> : <input type="text"/> /64
IPv6 Address Lifetime:	30 (minutes)

Static IPv6 (Stateless)

IPv6 Connection Type: Select **Static IPv6** from the drop-down menu.

WAN IPv6 Address Settings: Enter the address settings supplied by your Internet provider (ISP).

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateless**. Refer to the previous page for Stateful.

Router Advertisement Lifetime: Enter the Router Advertisement Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	<input type="text" value="Static IPv6"/>
WAN IPv6 ADDRESS SETTINGS :	
Enter the IPv6 address information provided by your Internet Service Provider (ISP).	
IPv6 Address :	<input type="text"/>
Subnet Prefix Length :	<input type="text"/>
Default Gateway :	<input type="text"/>
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.	
LAN IPv6 Address :	<input type="text"/> /64
LAN IPv6 Link-Local Address :	FE80::218:E7FF:FE6A:2792/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable Autoconfiguration :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	<input type="text" value="Stateless"/>
Router Advertisement Lifetime:	<input type="text" value="30"/> (minutes)

DHCPv6 (Stateful)

IPv6 Connection Type: Select **DHCPv6** from the drop-down menu.

IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

IPv6 Address Range Start: Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range End: Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 Address Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	<input type="text" value="DHCPv6"/>
IPv6 DNS SETTINGS :	
Obtain DNS server address automatically or enter a specific DNS server address.	
<input checked="" type="radio"/> Obtain DNS server address automatically <input type="radio"/> Use the following DNS address	
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.	
LAN IPv6 Address :	<input type="text"/> /64
LAN IPv6 Link-Local Address :	FE80::240:F4FF:FE03:1A9C/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable Autoconfiguration :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	<input type="text" value="Stateful (DHCPv6)"/>
IPv6 Address Range(Start):	<input type="text"/> :: <input type="text"/>
IPv6 Address Range(End):	<input type="text"/> :: <input type="text"/>
IPv6 Address Lifetime:	<input type="text" value="30"/> (minutes)

DHCPv6 (Stateless)

IPv6 Connection Type: Select **DHCPv6** from the drop-down menu.

IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateless**. Refer to the previous page for Stateful.

Router Advertisement Lifetime: Enter the Router Advertisement Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	<input type="text" value="DHCPv6"/>
IPv6 DNS SETTINGS :	
Obtain DNS server address automatically or enter a specific DNS server address.	
<input checked="" type="radio"/> Obtain DNS server address automatically <input type="radio"/> Use the following DNS address	
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.	
LAN IPv6 Address :	<input type="text"/> /64
LAN IPv6 Link-Local Address :	FE80::240:F4FF:FE03:1A9C/64
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable Autoconfiguration :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	<input type="text" value="Stateless"/>
Router Advertisement Lifetime:	<input type="text" value="30"/> (minutes)

IPv6 over PPPoE (Stateful)

IPv6 Connection Type: Select **PPPoE** from the drop-down menu.

PPPoE: Enter the PPPoE account settings supplied by your Internet provider (ISP).

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

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

User Name: Enter your PPPoE user name.

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

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

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

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

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is :

PPPOE :

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

Address Mode Dynamic IP Static IP

IP Address :

User Name :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

MTU : (bytes)

IPv6 DNS SETTINGS :

Obtain DNS server address automatically or enter a specific DNS server address.

Obtain DNS server address automatically

Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

IPv6 Address Range Start: Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range End: Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 Address Lifetime (in minutes).

LAN IPv6 ADDRESS SETTINGS :

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : FE80::240:F4FF:FE03:1A9C/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful (DHCPv6) ▼

IPv6 Address Range(Start): ::

IPv6 Address Range(End): ::

IPv6 Address Lifetime: (minutes)

IPv6 over PPPoE (Stateless)

IPv6 Connection Type: Select **PPPoE** from the drop-down menu.

PPPoE: Enter the PPPoE account settings supplied by your Internet provider (ISP).

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

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

User Name: Enter your PPPoE user name.

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

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

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

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

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is :

PPPOE :

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

Address Mode Dynamic IP Static IP

IP Address :

User Name :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

MTU : (bytes)

- IPv6 DNS Settings:** Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.
- Primary/Secondary DNS Address:** Enter the primary and secondary DNS server addresses.
- LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.
- LAN Link-Local Address:** Displays the Router's LAN Link-Local Address.
- Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.
- Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**.
- Router Advertisement Lifetime:** Enter the Router Advertisement Lifetime (in minutes).

IPv6 DNS SETTINGS :

Obtain DNS server address automatically or enter a specific DNS server address.

Obtain DNS server address automatically
 Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 ADDRESS SETTINGS :

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : FE80::240:F4FF:FE03:1A9C/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type :

Router Advertisement Lifetime: (minutes)

6 to 4 Tunneling (Stateful)

IPv6 Connection Type: Select **6 to 4** from the drop-down menu.

6 to 4 Settings: Enter the IPv6 settings supplied by your Internet provider (ISP).

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

IPv6 Address Range Start: Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range End: Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 Address Lifetime (in minutes).

IPv6 CONNECTION TYPE	
Choose the mode to be used by the router to the IPv6 Internet.	
My IPv6 Connection is :	<input type="text" value="6 to 4"/>
6to4 SETTINGS :	
Enter the IPv6 address information provided by your Internet Service Provider (ISP).	
6to4 Address :	<input type="text" value="0:0:0:0:0:0:0:0"/>
Primary DNS Address :	<input type="text"/>
Secondary DNS Address :	<input type="text"/>
LAN IPv6 ADDRESS SETTINGS :	
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.	
LAN IPv6 Address :	<input type="text" value="2002:0:0:0001"/> ::1/64
LAN IPv6 Link-Local Address :	<input type="text" value="FE80::240:F4FF:FE03:1A9C/64"/>
ADDRESS AUTOCONFIGURATION SETTINGS	
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.	
Enable Autoconfiguration :	<input checked="" type="checkbox"/>
Autoconfiguration Type :	<input type="text" value="Stateful (DHCPv6)"/>
IPv6 Address Range(Start):	<input type="text" value="2002:0:0:0001"/> :: <input type="text"/>
IPv6 Address Range(End):	<input type="text" value="2002:0:0:0001"/> :: <input type="text"/>
IPv6 Address Lifetime:	<input type="text" value="30"/> (minutes)

6 to 4 Tunneling (Stateless)

IPv6 Connection Type: Select **6 to 4** from the drop-down menu.

6 to 4 Settings: Enter the IPv6 settings supplied by your Internet provider (ISP).

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateless**. Refer to the previous page for Stateful.

Router Advertisement Lifetime: Enter the Router Advertisement Lifetime (in minutes).

IPv6 CONNECTION TYPE
Choose the mode to be used by the router to the IPv6 Internet.
My IPv6 Connection is : <input type="text" value="6 to 4"/>

6to4 SETTINGS :
Enter the IPv6 address information provided by your Internet Service Provider (ISP).
6to4 Address : 0:0:0:0:0:0:0
Primary DNS Address : <input type="text"/>
Secondary DNS Address : <input type="text"/>

LAN IPv6 ADDRESS SETTINGS :
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.
LAN IPv6 Address : 2002:0:0:0001 ::1/64
LAN IPv6 Link-Local Address : FE80::240:F4FF:FE03:1A9C/64

ADDRESS AUTOCONFIGURATION SETTINGS
Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.
Enable Autoconfiguration : <input checked="" type="checkbox"/>
Autoconfiguration Type : <input type="text" value="Stateless"/>
Router Advertisement Lifetime: <input type="text" value="30"/> (minutes)

IPv6 in IPv4 Tunneling (Stateful)

IPv6 Connection Type: Select **IPv6 in IPv4 Tunnel** from the drop-down menu.

IPv6 in IPv4 Tunnel Settings: Enter the settings supplied by your Internet provider (ISP).

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN IPv6 Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

IPv6 Address Lifetime: Enter the IPv6 Address Lifetime (in minutes).

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is : IPv6 in IPv4 Tunnel ▾

IPv6 in IPv4 TUNNEL SETTINGS :

Enter the IPv6 in IPv4 Tunnel information provided by your Tunnel Broker.

Remote IPv4 Address :

Remote IPv6 Address :

Local IPv4 Address :

Local IPv6 Address :

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 ADDRESS SETTINGS :

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : FE80::240:F4FF:FE03:1A9C/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type : Stateful (DHCPv6) ▾

IPv6 Address Range(Start): :

IPv6 Address Range(End): :

IPv6 Address Lifetime: 30 (minutes)

IPv6 in IPv4 Tunneling (Stateless)

My IPv6 Connection: Select **IPv6 in IPv4 Tunnel** from the drop-down menu.

IPv6 in IPv4 Tunnel Settings: Enter the settings supplied by your Internet provider (ISP).

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

LAN Link-Local Address: Displays the Router's LAN Link-Local Address.

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)** or **Stateless**. Refer to the previous page for Stateful.

IPv6 Address Range Start: Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range End: Enter the end IPv6 Address for the DHCPv6 range for your local computers.

Router Advertisement Lifetime: Enter the Router Advertisement Lifetime (in minutes).

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is :

IPv6 in IPv4 TUNNEL SETTINGS :

Enter the IPv6 in IPv4 Tunnel information provided by your Tunnel Broker.

Remote IPv4 Address :

Remote IPv6 Address :

Local IPv4 Address :

Local IPv6 Address :

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 ADDRESS SETTINGS :

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : FE80::218:E7FF:FE6A:2792/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration :

Autoconfiguration Type :

Router Advertisement Lifetime: (minutes)

Administrator Settings

This page allows you to adjust the Admin and User account settings. The Admin account can view and change settings, while the User account can only view settings and cannot make any changes. Only the admin account has the ability to change both admin and user account passwords. After making your changes, click the **Save Settings** button.

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

User Password: Enter the new password for the User login. If you login as the User, you cannot change the settings (you can only view them).

Gateway Name: Enter a name for the DIR-652 router.

Enable Graphical Authentication: Enables a challenge-response test to require users to type letters or numbers from a distorted image displayed on the screen to prevent online hackers and unauthorized users from gaining access to your router's network settings.

Enable HTTPS Server: Check to enable HTTPS to connect to the router securely.

Enable Remote Management: Remote management allows the DIR-652 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

ADMINISTRATOR SETTINGS

The 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
Verify Password :

USER PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
Verify Password :

SYSTEM NAME

Gateway Name :

ADMINISTRATION

Enable Graphical Authentication :

Enable HTTPS Server :

Enable Remote Management :

Remote Admin Port : **Use HTTPS :**

Remote Admin [Inbound Filter](#) :

Details :

Remote Admin Port: The port number used to access the DIR-652.

Example: `http://x.x.x.x:8080` whereas `x.x.x.x` is the Internet IP address of the DIR-652 and 8080 is the port used for the Web Management interface. If you have enabled and checked, you must enter as part of the URL to access the router remotely.

Remote Admin Inbound Filter: You may select “Allow All” to allow all traffic, or “Deny All” to deny all traffic. You may also specify a your own user-configured Inbound Filter. To set an Inbound Filter, simply click the Inbound Filter link and complete the instructions on that page.

Details: This area will display the Inbound Filter that is currently in place.

The screenshot shows the ADMINISTRATION page with the following configuration options:

- Enable Graphical Authentication :
- Enable HTTPS Server :
- Enable Remote Management :
- Remote Admin Port : Use HTTPS :
- Remote Admin [Inbound Filter](#) :
- Details :

Time Settings

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

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

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

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

NTP Server Used: Enter the NTP server or select one from the drop-down menu.

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

The screenshot shows the D-Link DIR-652 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: ADMIN, TIME (selected), SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'TIME' and contains the following sections:

- TIME:** A summary box explaining the Time Configuration option and providing 'Save Settings' and 'Don't Save Settings' buttons.
- TIME CONFIGURATION:**
 - Current Router Time: Thursday, December 03, 2009 4:17:58 PM
 - Time Zone: (GMT-08:00) Pacific Time (US/Canada), Tijuana
 - Enable Daylight Saving:
 - Daylight Saving Offset: +1:00
 - Daylight Saving Dates: DST Start (Mar 3rd Sun 1:00 AM) and DST End (Nov 2nd Sun 1:00 AM)
- AUTOMATIC TIME CONFIGURATION:**
 - Enable NTP Server:
 - NTP Server Used: << Select NTP Server
- SET THE DATE A.D TIME MANUALLY:**
 - Date And Time: Year (2009), Month (Dec), Day (3), Hour (04), Minute (17), Second (54), PM
 - Copy Your Computer's Time Settings button

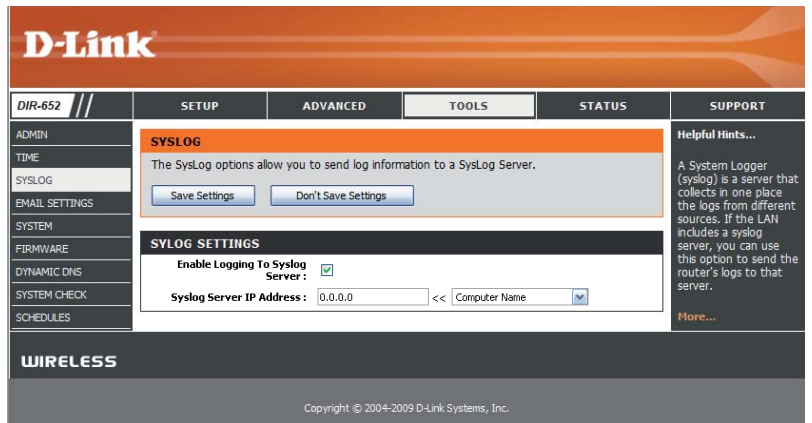
On the right side of the interface, there is a 'Helpful Hints ...' section with the text: 'Good timekeeping is important for accurate logs and scheduled firewall rules. More...'

SysLog

The Broadband Router keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network.

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

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



Email Settings

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

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

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

To Email Address: Enter the e-mail address where you want the e-mail sent.

SMTP Server Address: Enter the SMTP server address for sending e-mail. If your SMTP server requires authentication, select this option.

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

Account Name: Enter your account for sending e-mail.

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

The screenshot shows the D-Link DIR-652 web interface. The top navigation bar includes 'DIR-652 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS (highlighted), SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'EMAIL SETTINGS' and contains the following sections:

- EMAIL SETTINGS:** A message states, 'The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.
- EMAIL NOTIFICATION:** A section with the label 'Enable Email Notification : .
- EMAIL SETTINGS:** A form with the following fields:
 - From Email Address :
 - To Email Address :
 - SMTP Server Address :
 - Enable Authentication :
 - Account Name :
 - Password :
 - Verify Password :
- EMAIL LOG WHEN FULL OR ON SCHEDULE:** A section with the following options:
 - On Log Full :
 - On Schedule :
 - Schedule :
 - Detail :

On the right side of the interface, there is a 'Helpful Hints...' section with the text: 'You may want to make the email settings similar to those of your email client program.' and a 'More...' link.

Section 3 - Configuration

On Log Full: When this option is selected, logs will be sent via e-mail when the log is full.

On Schedule: Selecting this option will send the logs via e-mail according to schedule.

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

The screenshot displays the D-Link DIR-652 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options, with EMAIL SETTINGS highlighted. The main content area is divided into three sections:

- EMAIL SETTINGS:** Contains a message: "The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address." Below this are two buttons: "Save Settings" and "Don't Save Settings".
- EMAIL NOTIFICATION:** Features a checkbox labeled "Enable Email Notification :".
- EMAIL SETTINGS:** A form with the following fields:
 - From Email Address : [text input]
 - To Email Address : [text input]
 - SMTP Server Address : [text input]
 - Enable Authentication :
 - Account Name : [text input with "user" pre-filled]
 - Password : [password input with "****" mask]
 - Verify Password : [password input with "****" mask]
- EMAIL LOG WHEN FULL OR ON SCHEDULE:** A form with the following fields:
 - On Log Full :
 - On Schedule :
 - Schedule : [dropdown menu with "Never" selected]
 - Detail : [text input with "undefined" pre-filled]

On the right side of the interface, there is a "Helpful Hints..." section with a "More..." link. The text reads: "You may want to make the email settings similar to those of your email client program."

System Settings

Save to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. You will then see a file dialog, where you can select a location and file name for the settings.

Load from Local Hard Drive: Use this option to load previously saved router configuration settings. First, use the Browse control to find a previously save file of configuration settings. Then, click the Load button to transfer those settings to the router.

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

Reboot Device: Click to reboot the router.

The screenshot shows the D-Link DIR-652 web interface. At the top, there is a navigation bar with tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a menu with the following items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM (highlighted), FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSTEM SETTINGS' and contains the following text and buttons:

SYSTEM SETTINGS
The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

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

Save To Local Hard Drive:

Load From Local Hard Drive:

Restore To Factory Default:
Restore all settings to the factory defaults.

Reboots the Device:

Helpful Hints...
Once your router is configured the way you want it, you can save the configuration settings to a configuration file.
You might need this file so that you can load your configuration later in the event that the router's default settings are restored.
To save the configuration, click the **Save Configuration** button.
[More...](#)

At the bottom of the page, there is a 'WIRELESS' section and a copyright notice: Copyright © 2004-2009 D-Link Systems, Inc.

Update Firmware

You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at <http://support.dlink.com>. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Upgrade: Click on **Check Online Now for Latest Firmware Version** to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

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

The screenshot displays the D-Link DIR-652 web interface. At the top, the D-Link logo is visible. Below it, a navigation menu includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a list of menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE (highlighted), DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'FIRMWARE' and contains the following sections:

- FIRMWARE:** A message stating, "There may be new firmware for your DIR-652 to improve functionality and performance. 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 Upload button below to start the firmware upgrade."
- FIRMWARE INFORMATION:** Displays "Current Firmware Version : 1.00" and "Current Firmware Date : Thu, 3, Dec, 2009". It includes a "Check Online Now for Latest Firmware Version : [Check Now]" button.
- FIRMWARE UPGRADE:** Contains a note: "Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools -> System screen." Below this, it states: "To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button." There is a text input field, a "Browse..." button, and an "Upload" button.

On the right side of the interface, there is a "Helpful Hints..." section with text: "Firmware updates are released periodically to improve the functionality of your router and to add features. If you run into a problem with a specific feature of the router, check if updated firmware is available for your router." and a "More..." link. At the bottom of the page, the text "WIRELESS" and "Copyright © 2004-2009 D-Link Systems, Inc." are visible.