

USER MANUAL

DIR-635

VERSION 2.01



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

| Revision | Date | Description |
|----------|-------------------|--|
| 2.0 | December 23, 2008 | Added SharePort™ Network USB Utility support |

Other Reference Document

If you use the USB port of this router as a network port to share your USB hard drive, flash drive or printer, read the *SharePort™ Network USB Utility Manual* for additional instructions.

Trademarks

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

Copyright © 2009 by D-Link Corporation

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

Table of Contents

| | | | |
|--|-----------|----------------------------------|----|
| Preface | i | Static (assigned by ISP)..... | 24 |
| Manual Revisions | i | 3G Mobile Connection..... | 25 |
| Trademarks..... | i | Wireless Settings | 26 |
| Product Overview | 1 | Manual Wireless Settings..... | 27 |
| Package Contents | 1 | Network Settings..... | 29 |
| System Requirements | 1 | Router Settings..... | 30 |
| Introduction..... | 2 | DHCP Server Settings | 29 |
| Features..... | 3 | DHCP Reservation | 31 |
| Hardware Overview | 4 | USB Settings..... | 32 |
| Connections | 4 | Virtual Server | 33 |
| LEDs | 5 | Port Forwarding | 35 |
| Installation | 6 | Application Rules | 36 |
| Before you Begin | 6 | QoS Engine | 37 |
| Wireless Installation Considerations..... | 7 | Network Filters..... | 39 |
| Connect to Cable/DSL/Satellite Modem | 8 | Access Control..... | 40 |
| Connect to Another Router | 9 | Access Control Wizard | 41 |
| Getting Started | 11 | Website Filters | 43 |
| Configuration | 12 | Inbound Filters..... | 44 |
| Web-based Configuration Utility..... | 12 | Firewall Settings..... | 44 |
| Setup Wizard..... | 13 | ALG Configuration..... | 46 |
| Manual Internet Connection Setup..... | 17 | Routing | 47 |
| Dynamic (Cable) | 18 | Advanced Wireless Settings..... | 48 |
| PPPoE (DSL)..... | 19 | WISH Settings..... | 49 |
| PPTP..... | 20 | Wi-Fi Protected Setup (WPS)..... | 51 |
| L2TP | 22 | Advanced Network Settings | 53 |

| | | | |
|---|-----------|--------------------------------------|-----------|
| Administrator Settings | 54 | Troubleshooting | 82 |
| Time Settings | 55 | Wireless Basics | 86 |
| SysLog | 56 | What is Wireless?..... | 86 |
| Email Settings | 57 | Tips | 89 |
| System Settings | 58 | Wireless Modes..... | 90 |
| Update Firmware..... | 59 | Networking Basics | 91 |
| DDNS | 60 | Check your IP address..... | 91 |
| System Check | 61 | Statically Assign an IP address..... | 92 |
| Schedules | 62 | Technical Specifications..... | 93 |
| Device Information..... | 63 | | |
| Log..... | 64 | | |
| Statistics | 65 | | |
| Internet Sessions | 65 | | |
| Wireless | 66 | | |
| WISH Settings..... | 66 | | |
| Support..... | 67 | | |
| Wireless Security..... | 68 | | |
| What is WPA?..... | 68 | | |
| Wireless Security Setup Wizard..... | 69 | | |
| Add Wireless Device with WPS Wizard..... | 71 | | |
| Configure WPA-Personal (PSK)..... | 72 | | |
| Configure WPA-Enterprise (RADIUS) | 73 | | |
| Connect to a Wireless Network..... | 75 | | |
| Using Windows Vista® | 75 | | |
| Configure Wireless Security | 76 | | |
| Connect Using WCN 2.0 in Windows Vista® | 78 | | |
| Using Windows® XP | 79 | | |
| Configure WPA-PSK..... | 80 | | |

Package Contents

- D-Link DIR-635 RangeBooster N™ 650
- 3 Detachable Antennas
- Power Adapter
- CAT5 Ethernet Cable
- CD-ROM with Installation Wizard and User Manual



Note: *Using a power supply with a different voltage rating than the one included with the DIR-635 will cause damage and void the warranty for this product.*

System Requirements

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

Introduction

TOTAL PERFORMANCE

Combines award winning router features and Draft 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 RangeBooster N™ 650 (DIR-635) is a draft 802.11n compliant device that delivers real world performance which is many times 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 RangeBooster N™ 650 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 RangeBooster N™ technology, this high performance router provides superior Whole Home Coverage while reducing dead spots. The RangeBooster N™ 650 is designed for use in bigger homes and for users who demand higher performance networking. Add a RangeBooster N™ 650 notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

TOTAL NETWORK SECURITY

The RangeBooster N™ 650 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/WPA2 and WEP standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this RangeBooster N™ 650 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 Draft 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.

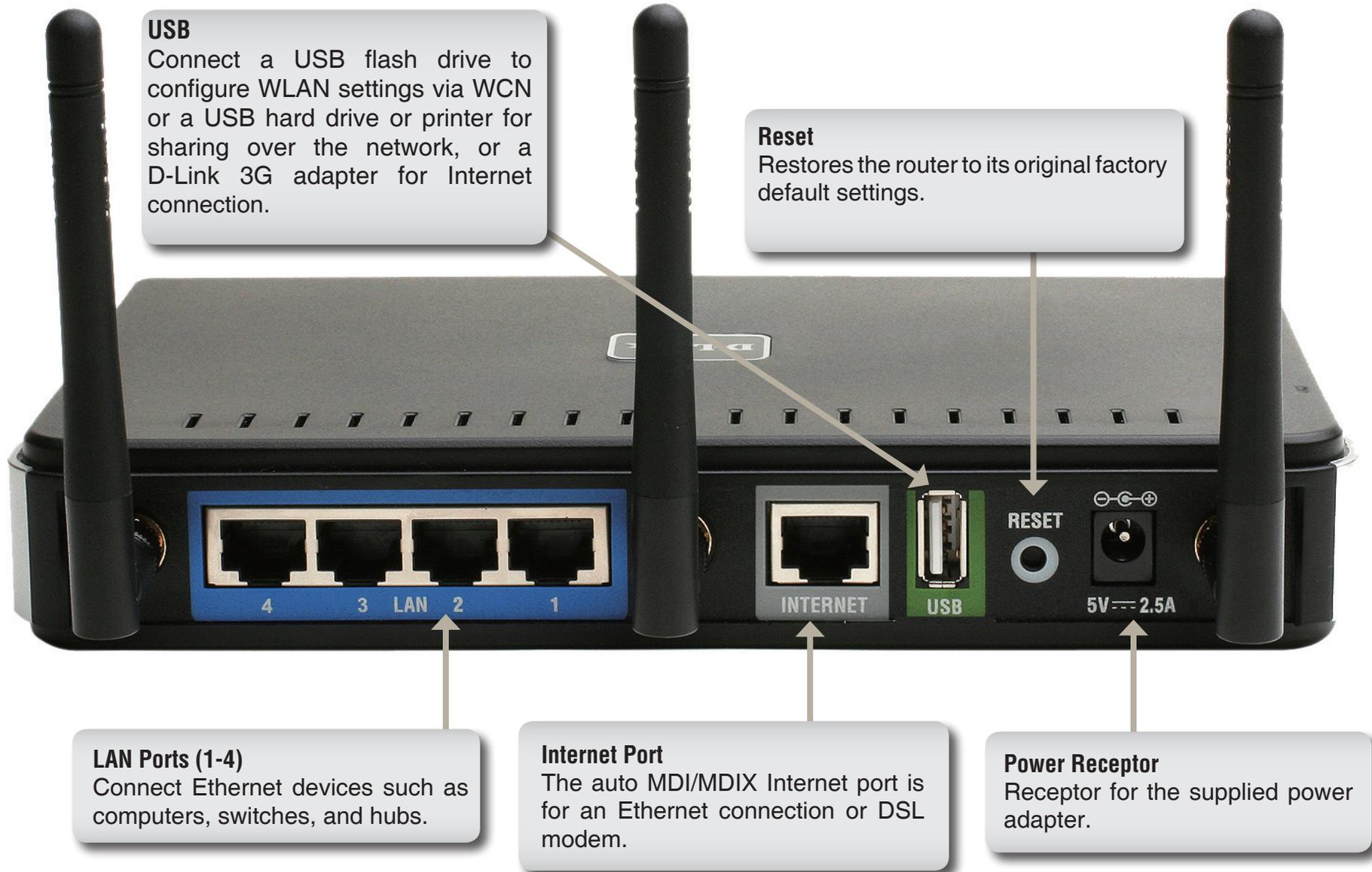
Features

- **Faster Wireless Networking** - The DIR-635 provides very high speed* 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 many times faster than 802.11g.
- **Compatible with 802.11b and 802.11g Devices** - The DIR-635 is still fully compatible with the IEEE 802.11b standard, so it can connect with existing 802.11b and g devices.
- **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-635 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-635 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-635 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 Draft 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.

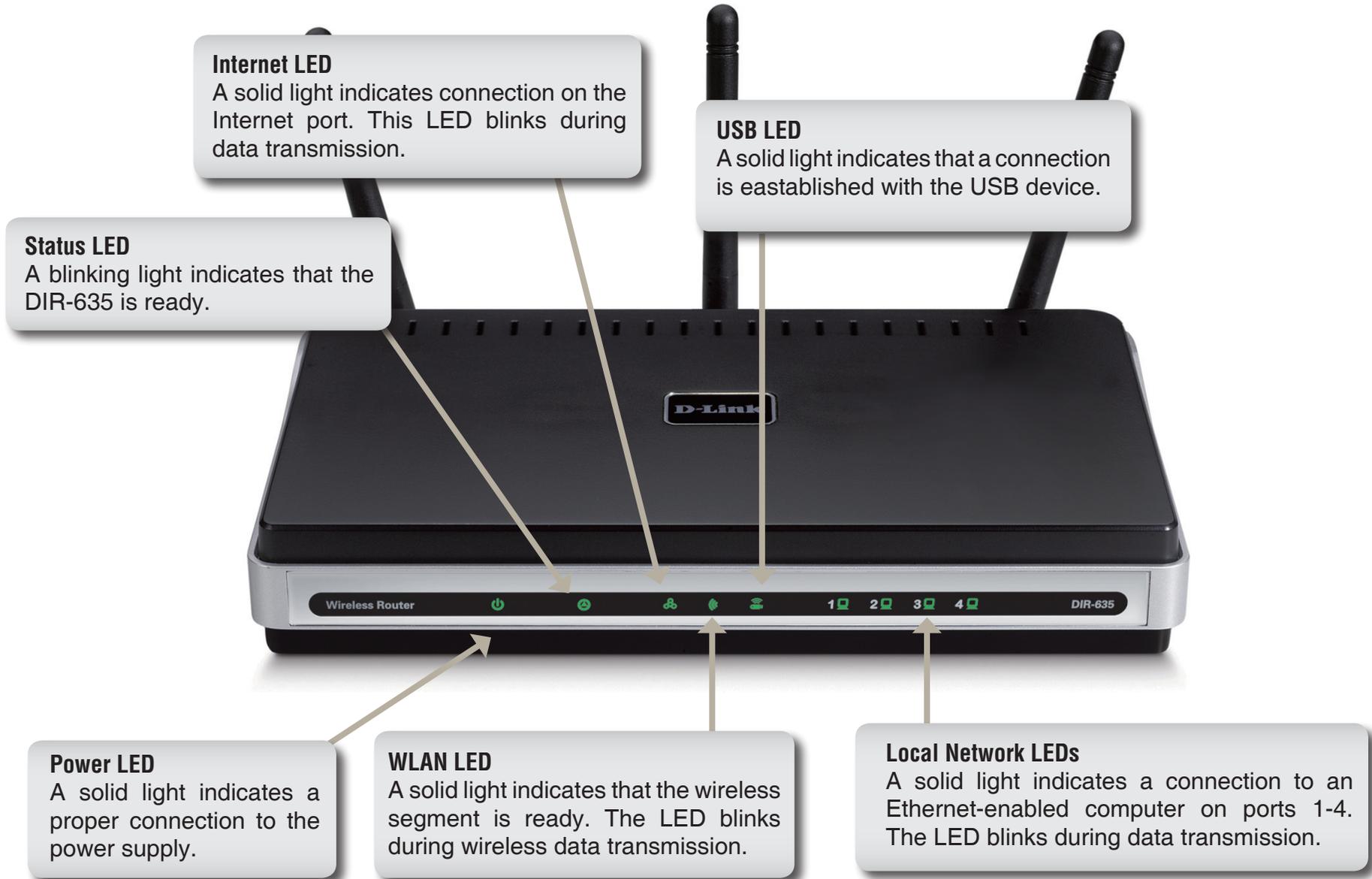
Hardware Overview

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.
- 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.
- When running the Setup Wizard from the D-Link CD, make sure the computer you are running the CD from is connected to the Internet and online or the wizard will not work. If you have disconnected any hardware, re-connect your computer back to the modem and make sure you are online.

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. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Connect to Cable/DSL/Satellite Modem

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

1. Place the router in an open and central location. Do not plug the power adapter into the router.
2. Turn the power off on your modem. If there is no on/off switch, then unplug the modem's power adapter. Shut down your computer.
3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.
4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.
5. Turn on or plug in your modem. Wait for the modem to boot (about 30 seconds).
6. Plug the power adapter to the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot.
7. Turn on your computer.
8. Refer to page 12 to configure your new D-Link wireless router using the web-based configuration utility.

Connect to Another Router

If you are connecting the D-Link router to another router to use as a wireless access point and/or switch, you will have to do the following before connecting the router to your network:

- Disable UPnP™
- Disable DHCP
- Change the LAN IP address to an available address on your network. The LAN ports on the router cannot accept a DHCP address from your other router.

To connect to another router, please follow the steps below:

1. Plug the power into the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). Please see the **Networking Basics** section for more information. If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.
2. Open a web browser and enter **http://192.168.0.1** and press **Enter**. When the login window appears, set the user name to **Admin** and leave the password box empty. Click **Log In** to continue.
3. Click **Advanced** and then click **Advanced Network**. Uncheck **Enable UPnP** and click **Save Settings** to continue.
4. Click **Setup** and then click **Network Settings**. Uncheck **Enable DHCP Server** and click **Save Settings** to continue.
5. Under **Router Settings**, enter an IP address and the subnet mask of your network. Click **Save Settings** to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as mentioned in step 1.

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

Getting Started

The DIR-635 includes a **Quick Router Setup Wizard** CD. Follow the simple steps below to run the **Setup Wizard**, which guides you quickly through the installation process.

Insert the **Quick Router Setup Wizard** CD in the 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: \ Autorun.exe` (where D: represents the drive letter of your CD-ROM drive).

When the autorun screen appears, click **Install Router**.



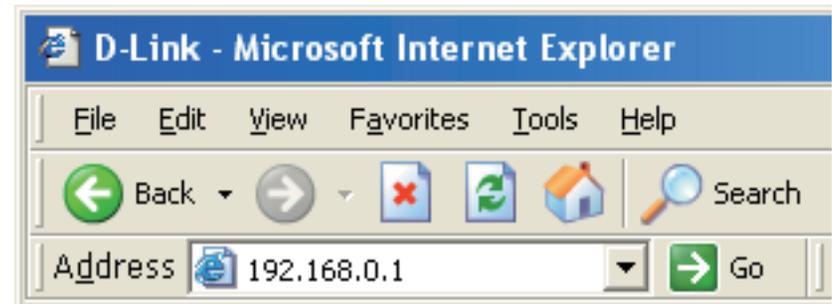
Note: It is highly recommended that you note down the SSID, Security Key and login password somewhere safe such as on the router's CD holder.

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).



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

A screenshot of the "LOGIN" page for the router configuration utility. The page has an orange header with the word "LOGIN" in white. Below the header, it says "Log in to the router:". There are two input fields: "User Name" with a dropdown menu showing "Admin" and "Password" with an empty text box. A "Log In" button is located to the right of the password field.

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

Setup Wizard

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

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

Click **Next** to continue.

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

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.

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.

WELCOME TO THE D-LINK INTERNET CONNECTION SETUP WIZARD

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

- Step 1: Set your Password
- Step 2: Select your Time Zone
- Step 3: Configure your Internet Connection
- Step 4: Save Settings and Connect

STEP 1: SET YOUR PASSWORD

By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

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

STEP 2: SELECT YOUR TIME ZONE

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

Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana

Prev Next Cancel Connect

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

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

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

Not Listed or Don't Know

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

- DHCP Connection (Dynamic IP Address)**
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- Username / Password Connection (PPPoE)**
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (PPTP)**
PPTP client.
- Username / Password Connection (L2TP)**
L2TP client.
- Static IP Address Connection**
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

Prev Next Cancel Connect

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

DHCP CONNECTION (DYNAMIC IP ADDRESS)

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

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

Host Name :

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

DNS SETTINGS

Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0

Prev Next Cancel Connect

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

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

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

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

SET USERNAME AND PASSWORD CONNECTION (PPPOE)

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

Address Mode : Dynamic IP Static IP

IP Address :

User Name :

Password :

Verify Password :

Service Name : (optional)

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

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

SET USERNAME AND PASSWORD CONNECTION (PPTP)

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

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

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

User Name :

Password :

Verify Password :

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

SET USERNAME AND PASSWORD CONNECTION (L2TP)

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

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

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

User Name :

Password :

Verify Password :

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

SET STATIC IP ADDRESS CONNECTION

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

IP Address :

Subnet Mask :

Gateway Address :

Primary DNS Address :

Secondary DNS Address :

Click **Connect** to save your settings.

SETUP COMPLETE!

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

Click **Reboot Now** to reboot the router so the new settings can take effect. Once the router is finished rebooting, click **Continue**. Please allow one or two minutes to connect.

REBOOT NEEDED

Your changes have been saved. The router must be rebooted for the changes to take effect. You can reboot now, or you can continue to make other changes and reboot later.

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

Manual Internet Connection Setup

Click **Manual Internet Connection Setup** to begin.

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard** and refer to page 13.

The screenshot shows a web-based configuration interface for an Internet connection. It is divided into three main sections:

- INTERNET CONNECTION**: An orange header section containing the text: "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 WIZARD**: A dark grey header section containing the text: "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." Below this text is a button labeled "Internet Connection Setup Wizard". A **Note** follows: "Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package."
- MANUAL INTERNET CONNECTION OPTIONS**: A dark grey header section containing the text: "If you would like to configure the Internet settings of your new D-Link Systems Router manually, then click on the button below." Below this text is a button labeled "Manual Internet Connection Setup".

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.

Host Name: 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.

INTERNET CONNECTION TYPE

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

My Internet Connection is : Dynamic IP (DHCP) ▾

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

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

Host Name : DIR-615

Use Unicasting : (compatibility for some DHCP Servers)

Primary DNS Address : 192.168.1.105

Secondary DNS Address : 0.0.0.0

MTU : 1500 (bytes)MTU default = 1500

MAC Address : 00:40:f4:03:21:ac

Clone Your PC's MAC Address

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 IP** 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. This function does not apply if you have selected **Reconnect Mode** as **Always on**.

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

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

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) ▼

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. This function does not apply if you have selected **Reconnect Mode** as **Always on**.

INTERNET CONNECTION TYPE

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

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

PPTP 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 :

Clone Your PC's MAC Address

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

MTU: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. 1400 is the default MTU value.

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. This function does not apply if you have selected **Reconnect Mode** as **Always on**.

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) ▼

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 :

MTU: You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. 1400 is the default MTU value.

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

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 :

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 :

Internet Setup

3G Mobile Connection

If you want to connect your router to the Internet through a 3G mobile service, navigate to **USB SETTINGS** and select **SETUP**. The **USB SETTINGS** screen will display. Select **3G USB Adapter** from the **My Plug of USB type is** field and click **Save Settings**. The **INTERNET CONNECTION TYPE** screen will display as seen below:

Country: Select your country from the list.

ISP: Displays the name of your **Internet Service Provider (ISP)**.

Username: Enter a username. This field is optional.

Password: Enter a password. This field is optional.

Dial Number: Enter the dial-up number.

Authentication Protocol: Choose the authentication type from the drop-down list. The default setting is **Auto**.

APN: Enter a name for the access point. This field is optional.

Reconnect Mode: Select **Always-on**, **On-Demand**, or **Manual**. to reconnect to the network.

Maximum Idle Time: Enter the maximum idle time during which the Internet connection is maintained during inactivity. This function does not apply if you have selected **Reconnect Mode** as **Always on**.

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

INTERNET CONNECTION TYPE

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

My Internet Connection is : ▼

WWAN INTERNET CONNECTION TYPE :

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

Country : ▼

ISP : ▼

Username : (optional)

Password : (optional)

Dial Number :

Authentication Protocol : ▼

APN : (optional)

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

MTU : (bytes) (128~1492)

Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Security Setup Wizard** and refer to page 69.

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 71.

If you want to manually configure the wireless settings on your router click **Manual Wireless Network Setup** and refer to the next page.

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 Wi-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](#)

Manual 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: Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click **Add New** to create a new schedule.

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.

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

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DIR-635 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-635. 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.

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

WIRELESS NETWORK SETTINGS

Enable Wireless : Always New Schedule

Wireless Network Name : (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

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

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 you are using 802.11n wireless clients only.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-635. If Invisible is selected, the SSID of the DIR-635 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-635 in order to connect to it.

Wireless Security: Refer to page 68 for more information regarding wireless security.

Network Settings

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

Router Settings

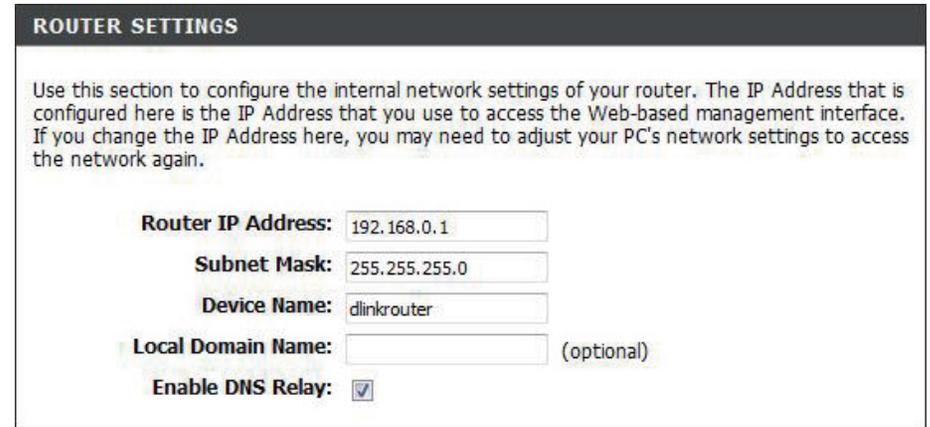
Router IP Address: Enter the IP address of the router. The default IP address is 192.168.0.1.

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

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 a web interface titled "ROUTER SETTINGS". It contains a text box with instructions: "Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again." Below this are several input fields: "Router IP Address" with the value "192.168.0.1", "Subnet Mask" with "255.255.255.0", "Device Name" with "dlinkrouter", "Local Domain Name" (empty) with "(optional)" to its right, and "Enable DNS Relay" with a checked checkbox.

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-635 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-635. 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.
Server: 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.

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

WINS IP Address: Enter your WINS IP address

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:

DHCP Reservation

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

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

Enable: Check this box to enable the reservation.

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

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

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

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

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

ADD DHCP RESERVATION

Enable:

Computer Name: << Computer Name ▾

IP Address:

MAC Address:

DHCP RESERVATIONS LIST

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

NUMBER OF DYNAMIC DHCP CLIENTS:1

| Hardware Address | Assigned IP | Hostname | Expires | | |
|-------------------|---------------|--------------|--------------------|------------------------|-------------------------|
| 00:16:36:a6:58:11 | 192.168.0.172 | Ferrari-5000 | 22 Hours 3 Minutes | Revoke | Reserve |

USB Settings

Use this section to configure your USB port. There are three configurations to choose from: Network USB, WCN Configuration and 3G USB Adapter.

USB Settings: Select one of these three configurations: **Network USB**, **WCN Configuration** or **3G USB Adapter**.

If you select **Network USB** from the drop-down list, you will need to configure the router's USB port by running the **SharePort™ Network USB Utility** from your computer so other users of your network may access the USB device connected to this port. Refer to the manual of this utility for complete instructions.

If you select **3G USB Adapter** from the drop-down list, you need to connect your router to the Internet through a 3G mobile service. Refer to the *Internet Setup 3G Mobile Connection* on page 25 for details.

Network USB: Please set the **Network USB Detection interval**. The router will automatically detect the USB device.

The screenshot shows the D-Link DIR-635 web interface for USB settings. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists 'INTERNET', 'WIRELESS SETTINGS', 'NETWORK SETTINGS', and 'USB SETTINGS', with 'USB SETTINGS' selected. The main content area is titled 'USB SETTINGS' and contains the following text: 'Use this section to configure your USB port. There are several configurations to choose from: Network USB, 3G USB Adapter and WCN Configuration. Note: If using the Network USB option, users will need to install the Network USB Utility into their computers to share the USB device through the router.' Below this are 'Save Settings' and 'Don't Save Settings' buttons. A section titled 'USB SETTINGS' asks to 'Choose the type of USB device to be plugged into the USB port.' with a dropdown menu showing 'My plug of USB type is : Network USB'. A section titled 'NETWORK USB' asks to 'Please set Network USB Detection interval time, the router will automatically detect the USB device.' with a text input field containing '10' and the label 'sec (range:3-600 sec.)'. A right sidebar contains 'Helpful Hints...' with instructions on installing device drivers and the Network USB Utility, and a 'More...' link.

Virtual Server

The DIR-635 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-635 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-635 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-635 redirects the external service request to the appropriate server within the LAN network.

The DIR-635 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

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

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

This will allow you to open a single port. If you would like to open a range of ports, refer to page 35.

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** from the drop-down menu.

Schedule: The schedule when the Virtual Server Rule is 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-635

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 | Port | Traffic Type | Inbound Filter |
|--------------------------|---------------------|------------------|-----------|--------------|--------------------------|
| <input type="checkbox"/> | << Application Name | << Computer Name | Public 0 | Both | Schedule Always |
| <input type="checkbox"/> | << Application Name | << Computer Name | Private 0 | Protocol 0 | Inbound Filter Allow All |
| <input type="checkbox"/> | << Application Name | << Computer Name | Public 0 | Both | Schedule Always |
| <input type="checkbox"/> | << Application Name | << Computer Name | Private 0 | Protocol 0 | Inbound Filter Allow All |
| <input type="checkbox"/> | << Application Name | << Computer Name | Public 0 | Both | Schedule Always |
| <input type="checkbox"/> | << Application Name | << Computer Name | Private 0 | Protocol 0 | Inbound Filter Allow All |
| <input type="checkbox"/> | << Application Name | << Computer Name | Public 0 | Both | Schedule Always |
| <input type="checkbox"/> | << Application Name | << Computer Name | Private 0 | Protocol 0 | Inbound Filter Allow All |
| <input type="checkbox"/> | << Application Name | << Computer Name | Public 0 | Both | Schedule Always |
| <input type="checkbox"/> | << Application Name | << Computer Name | Private 0 | Protocol 0 | Inbound Filter Allow All |
| <input type="checkbox"/> | << Application Name | << Computer Name | Public 0 | Both | Schedule Always |

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. If you do not see the filter you need in the list of filters, go to the **Advanced → Inbound Filter** screen and create a new filter.

More...

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** or ports that you want to open. Enter a single port or a range and use a comma to separate the ports.

Example: 24,1009,3000-4000

Schedule: Schedule when the Virtual Server Rule is 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-635

SETUP ADVANCED TOOLS STATUS SUPPORT

PORT FORWARDING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

Save Settings Don't Save Settings

24 -- PORT FORWARDING RULES

| | Name | IP Address | Application Name | Computer Name | Ports to Open | Inbound Filter | Schedule |
|--------------------------|------|------------|------------------|------------------|---------------|----------------|----------|
| <input type="checkbox"/> | | 0.0.0.0 | << | Application Name | TCP | Allow All | Always |
| <input type="checkbox"/> | | 0.0.0.0 | << | Computer Name | UDP | Allow All | Always |
| <input type="checkbox"/> | | 0.0.0.0 | << | Application Name | TCP | Allow All | Always |
| <input type="checkbox"/> | | 0.0.0.0 | << | Computer Name | UDP | Allow All | Always |
| <input type="checkbox"/> | | 0.0.0.0 | << | Application Name | TCP | Allow All | Always |
| <input type="checkbox"/> | | 0.0.0.0 | << | Computer Name | UDP | Allow All | Always |

Helpful Hints...

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.

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 LAN computer to which you would like to open the specified port.

Select a schedule for when the rule 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.

You can enter ports in various formats:
 Range (50-100)
 Individual (80, 68, 888)
 Mixed (1020-5000, 689)

More...

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-635. 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-635 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: Select either a single port or a range of ports. This port triggers the pre-defined application.

Traffic Type: Select the protocol for 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 for the firewall port- **TCP**, **UDP**, or **Both**.

Schedule: The schedule when the Application Rule is 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-635 // 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 | Trigger | Firewall | Traffic Type | Schedule |
|--------------------------|----------------------|---------------------|----------------------|----------------------|--------------|----------|
| <input type="checkbox"/> | <input type="text"/> | << Application Name | <input type="text"/> | <input type="text"/> | TCP | Always |
| <input type="checkbox"/> | <input type="text"/> | << Application Name | <input type="text"/> | <input type="text"/> | TCP | Always |
| <input type="checkbox"/> | <input type="text"/> | << Application Name | <input type="text"/> | <input type="text"/> | TCP | Always |
| <input type="checkbox"/> | <input type="text"/> | << Application Name | <input type="text"/> | <input type="text"/> | TCP | Always |
| <input type="checkbox"/> | <input type="text"/> | << Application Name | <input type="text"/> | <input type="text"/> | TCP | Always |

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** screen and create a new schedule.

More...

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: 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.

Connection Type: By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you have configured as either **Static** or **DHCP** in the Internet settings, setting this option to **xDSL** or **Other Frame Relay Network** ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing **xDSL** or **Other Frame Relay Network** causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

Detected xDSL: When **Connection Type** is set to automatic, the automatically detected connection type is displayed here.

The screenshot displays the D-Link DIR-635 configuration interface for the QoS Engine. The main navigation menu includes SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The QoS ENGINE section is active, showing a brief introduction and 'Save Settings' / 'Don't Save Settings' buttons. Below this is the WAN TRAFFIC SHAPING section, where 'Enable Traffic Shaping' is checked, 'Automatic Uplink Speed' is checked, and 'Measured Uplink Speed' is 11588 kbps. 'Manual Uplink Speed' is set to 128 kbps. 'Connection Type' is set to 'Auto-detect' and 'Detected xDSL or Other Frame Relay Network' is 'Yes'. The QoS ENGINE SETUP section shows 'Enable QoS Engine', 'Automatic Classification', and 'Dynamic Fragmentation' all checked. The QoS ENGINE RULES section shows a table with 10 rules, including Name, Priority, Protocol, Local IP Range, and Remote IP Range.

| Name | Priority | Protocol | Local IP Range | Remote IP Range |
|------|----------|----------|----------------------------|----------------------------|
| | 1 | TCP | 0.0.0.0 to 255.255.255.255 | 0.0.0.0 to 255.255.255.255 |

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.

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.

DHCP Client: Select a DHCP client from the drop-down menu and click << to copy that MAC Address.

Clear: Select to remove the MAC address.

The screenshot shows the D-Link DIR-635 web interface. The top navigation bar includes 'DIR-635', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'MAC ADDRESS FILTER' page is displayed. The page contains a description of the MAC filter, 'Save Settings' and 'Don't Save Settings' buttons, and a section titled '24 -- MAC FILTERING RULES'. This section includes a dropdown menu for 'Configure MAC Filtering below:' set to 'Turn MAC Filtering OFF'. Below this is a table with columns for 'MAC Address' and 'DHCP Client List'. The table has five rows, each with an empty 'MAC Address' field, a '<<' button, a 'Computer Name' dropdown menu, and a 'Clear' button. A 'Helpful Hints...' sidebar on the right provides instructions on how to use the DHCP Client List and the Clear button.

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 **Add Policy** to start the **Access Control Wizard**.

The screenshot shows the D-Link DIR-635 web interface. The main navigation menu includes SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The 'ADVANCED' menu is expanded to show 'ACCESS CONTROL'. The 'ACCESS CONTROL' section contains a description: 'The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.' Below this is a 'Save Settings' button and a 'Don't Save Settings' button. The 'Enable Access Control' checkbox is checked, and an 'Add Policy' button is visible. The 'POLICY TABLE' section at the bottom has columns for Enable, Policy, Machine, Filtering, Logged, and Schedule. A 'Helpful Hints...' sidebar on the right provides instructions: 'Check **Enable Access Control** if you want to enforce rules that limit Internet access from specific LAN computers. Click **Add Policy** to start the processes of creating a rule. You can cancel the process at any time. When you are finished creating a rule it will be added to the **POLICY Table** below. Click the **Edit** icon to modify an existing rule.'

Access Control Wizard

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

The screenshot shows the 'ADD NEW POLICY' wizard dialog box. It contains the following text: 'This wizard will guide you through the following steps to add a new policy for Access Control.' The steps are: Step 1 - Choose a unique name for your policy, Step 2 - Select a schedule, Step 3 - Select the machine to which this policy applies, Step 4 - Select filtering method, Step 5 - Select filters, and Step 6 - Configure Web Access Logging. At the bottom, there are four buttons: 'Prev', 'Next', 'Save', and 'Cancel'. The 'Next' button is highlighted.

Access Control Wizard (continued)

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

STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name :

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

STEP 2: SELECT SCHEDULE

Choose a schedule to apply to this policy.

Always

Details : Always

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.

STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type : IP MAC Other Machines

IP Address : << Computer Name

Machine Address : << Computer Name

Copy Your PC's MAC Address

Machine

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 :

Access Control Wizard (continued)

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 | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |
| <input type="checkbox"/> | | 0.0.0.0 | 255.255.255.255 | Any | 0 | 65535 |

Prev Next Save Cancel

To enable web logging, click **Enable**.

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

STEP 6: CONFIGURE WEB ACCESS LOGGING

Web Access Logging : Disabled Enabled

Prev Next Save Cancel

Your newly created policy will now show up under **Policy Table**.

D-Link

DIR-635 // SETUP ADVANCED TOOLS STATUS SUPPORT

ACCESS CONTROL

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

Save Settings Don't Save Settings

ACCESS CONTROL

Enable Access Control: Add Policy

POLICY TABLE

| Enable | Policy | Machine | Filtering | Logged | Schedule |
|-------------------------------------|--------|---------------|-------------------|--------|----------|
| <input checked="" type="checkbox"/> | dlink | 192.168.0.199 | Block Some Access | No | Always |

Helpful Hints...

Check **Enable Access Control** if you want to enforce rules that limit internet access from specific LAN computers.

Click **Add Policy** to start the processes of creating a rule. You can cancel the process at any time. When you are finished creating a rule it will be added to the **Policy Table** below.

Click the **Edit** icon to modify an existing rule using the **Policy Wizard**.

Click the **Delete** icon to permanently remove a rule.

More...

Website Filters

Website Filters are used to allow you to set up a list of allowed Web sites that can be used by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the Access Control section (page 40).

Add Website Filtering Rule: Select **Allow** or **Deny**.

Website URL/ Domain: Enter the keywords or URLs that you want to allow or block. Click **Save Settings**.

The screenshot displays the D-Link DIR-635 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 WEBSITE FILTER highlighted. The main content area is titled '40 -- WEBSITE FILTERING RULES' and contains the following elements:

- WEBSITE FILTER** section: A descriptive text box explaining the feature, followed by 'Save Settings' and 'Don't Save Settings' buttons.
- 40 -- WEBSITE FILTERING RULES** section: A configuration area with a dropdown menu set to 'DENY computers access to ONLY these sites' and a 'Clear the list below...' button.
- Website URL/Domain** section: A table with two columns for entering website information.

On the right side, there is a 'Helpful Hints...' section with instructions: 'Create a list of Web Sites to which you would like to deny or allow through the network.' and 'Use with **Advanced** → **Access Control**. More...'

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.

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

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

Add: Click **Add** 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-635 // 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.

More...

Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-635 offers a firewall type functionality.

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

Anti-Spoof Checking: Enable this feature to protect your network from certain kinds of spoofing attacks.

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.*

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

FIREWALL SETTINGS

Enable SPI :

NAT ENDPOINT FILTERING

UDP Endpoint Filtering:

Endpoint Independent

Address Restricted

Port And Address Restricted

TCP Endpoint Filtering:

Endpoint Independent

Address Restricted

Port And Address Restricted

ANTI-SPOOF CHECKING

Enable anti-spoof checking:

DMZ HOST

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.

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

Enable DMZ:

DMZ IP Address : <<

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP :

IPSec (VPN) :

RTSP :

SIP :

Application Level Gateway (ALG) Configuration

Here you can enable or disable ALG's. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

PPTP: Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

IPSEC (VPN): Allows multiple VPN clients to connect to their corporate network using IPsec. Some VPN clients support traversal of IPsec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

RTSP: Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

SIP: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

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-635 // 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 | Metric | Interface |
|--------------------------|---------|----------------|--------|-----------|
| <input type="checkbox"/> | | 0.0.0.0 | 1 | WAN |
| | Netmask | 0.0.0.0 | | |
| | Gateway | 0.0.0.0 | | |
| <input type="checkbox"/> | | 0.0.0.0 | 1 | WAN |
| | Netmask | 0.0.0.0 | | |
| | Gateway | 0.0.0.0 | | |
| <input type="checkbox"/> | | 0.0.0.0 | 1 | WAN |
| | Netmask | 0.0.0.0 | | |
| | Gateway | 0.0.0.0 | | |

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.

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 2346. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation Threshold: 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: WLAN Partition prevents 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.

ADVANCED WIRELESS SETTINGS

| | | |
|----------------------------------|-------------------------------------|-------------|
| Transmit Power : | High | ▼ |
| Beacon Period : | 100 | (20..1000) |
| RTS Threshold : | 2346 | (0..2347) |
| Fragmentation Threshold : | 2346 | (256..2346) |
| DTIM Interval : | 1 | (1..255) |
| WLAN Partition : | <input type="checkbox"/> | |
| WMM Enable : | <input checked="" type="checkbox"/> | |
| Short GI : | <input checked="" type="checkbox"/> | |

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.

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.

WISH

WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications.

Save Settings Don't Save Settings

WISH

Enable WISH :

PRIORITY CLASSIFIERS

HTTP :

Windows Media Center :

Automatic : (default if not matched by anything else)

24 -- WISH RULES

| Name | Priority | Protocol |
|--|----------------------------|---------------------------------|
| <input type="text"/> | Best Effort Low(BE LO) ▼ | 6 << TCP ▼ |
| <input type="checkbox"/> Host 1 IP Range | 0.0.0.0 to 255.255.255.255 | Host 1 Port Range 0 to 65535 |
| Host 2 IP Range | 0.0.0.0 to 255.255.255.255 | Host 2 Port Range 0 to 65535 |
| <input type="checkbox"/> Name | Best Effort Low(BE LO) ▼ | 6 << TCP ▼ |
| Host 1 IP Range | 0.0.0.0 to 255.255.255.255 | Host 1 Port Range 0 to 65535 |

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)

| Name | Priority | Protocol |
|--|----------------------------|---------------------------------|
| | Best Effort (BE) | 6 << TCP |
| <input type="checkbox"/> Host 1 IP Range | 0.0.0.0 to 255.255.255.255 | Host 1 Port Range 0 to 65535 |
| Host 2 IP Range | 0.0.0.0 to 255.255.255.255 | Host 2 Port Range 0 to 65535 |

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.

Wi-Fi Protected Setup

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 the process for different products as well as manufactures. The process is just as easy, as pressing 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.

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

Generate New PIN: Create a random number that is a valid PIN. This becomes the router’s PIN. You can then copy this PIN to the user interface of the registrar.

WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

Save Settings Don't Save Settings

WI-FI PROTECTED SETUP

Enable :

Lock Wireless Security Settings :

Reset to Unconfigured

PIN SETTINGS

Current PIN : 24681353

Reset PIN to Default Generate New PIN

ADD WIRELESS STATION

Add Wireless Device with WPS

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 to press the configuration button on the device. If the device supports Wi-Fi Protected Setup, you can add it to the network by pressing the configuration button on the device and then switch 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 if you have pressed the **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 with

WPS: Start the wizard.

Advanced Network Settings

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

WAN Ping: Unchecking the box will not allow the DIR-635 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be pinged.

WAN Ping Inbound Filter: Select from the drop-down menu if you would like to apply the Inbound Filter to the WAN ping. Refer to page 44 for more information regarding Inbound Filter.

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

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

The screenshot displays the D-Link DIR-635 Advanced Network Settings interface. The main content area is divided into several sections:

- ADVANCED NETWORK:** Contains a warning message and two buttons: "Save Settings" and "Don't Save Settings".
- UPNP:** States "Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices." and includes a checked checkbox for "Enable UPnP".
- WAN PING:** Includes a warning: "If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address." It features an unchecked checkbox for "Enable WAN Ping Respond", a dropdown menu for "WAN Ping Inbound Filter" set to "Allow All", and a "Details" field also set to "Allow All".
- WAN PORT SPEED:** Shows a dropdown menu for "WAN Port Speed" set to "Auto 10/100Mbps".
- MULTICAST STREAMS:** Includes an unchecked checkbox for "Enable Multicast Streams".

The left sidebar lists various configuration categories, with "ADVANCED NETWORK" selected. The right sidebar contains "Helpful Hints..." and "More..." links.

Administrator Settings

This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while the user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

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 can only see the settings, but cannot change them.

Gateway Name: Enter a name for the DIR-635 router.

Enable Remote Management: Remote management allows the DIR-635 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.

Remote Admin Port: The port number used to access the DIR-635. Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DIR-635 and 8080 is the port used for the Web Management interface.

Inbound Filter: 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.

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

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 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-635 web interface for Time Configuration. The interface is divided into several sections:

- Navigation:** A top menu bar with tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. A left sidebar lists various configuration options like ADMIN, TIME, SYSLOG, etc.
- TIME Configuration:**
 - Time Configuration:** A section with a description and two buttons: "Save Settings" and "Don't Save Settings".
 - TIME CONFIGURATION:**
 - Current Router Time:** Saturday, January 31, 2004 2:50:54 PM
 - Time Zone:** (GMT-08:00) Pacific Time (US/Canada), Tijuana
 - Enable Daylight Saving:**
 - Daylight Saving Offset:** +1:00
 - Daylight Saving Dates:**

| DST Start | Month | Week | Day of Week | Time |
|-----------|-------|------|-------------|------|
| Apr | 1st | Sun | 2 am | |
| DST End | Oct | 5th | Sun | 2 am |
 - AUTOMATIC TIME CONFIGURATION:**
 - Enable NTP Server:**
 - NTP Server Used:** << Select NTP Server
 - SET THE DATE AND TIME MANUALLY:**
 - Date And Time:**

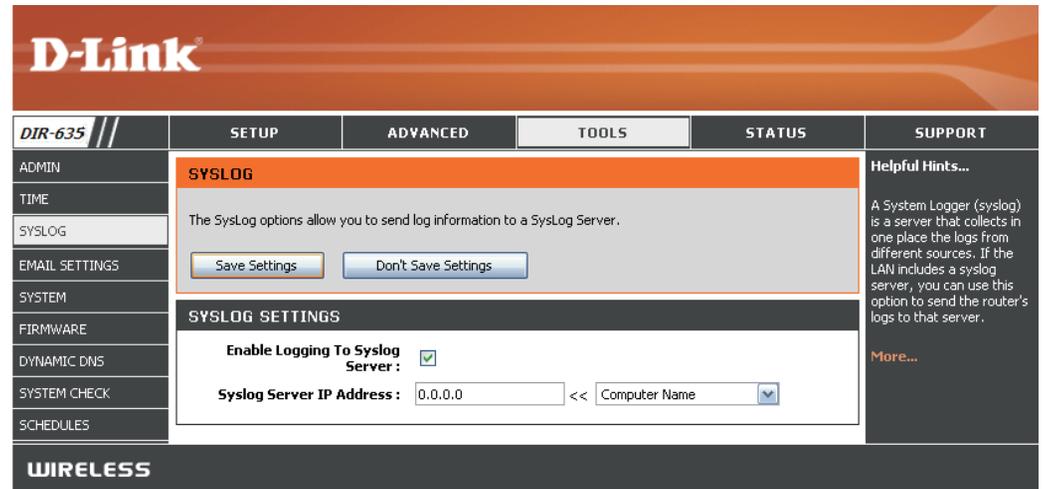
| | | | | | | | | | | | | |
|------|------|-------|-----|-----|----|------|---|--------|----|--------|----|----|
| Year | 2004 | Month | Jan | Day | 31 | Hour | 2 | Minute | 50 | Second | 45 | PM |
|------|------|-------|-----|-----|----|------|---|--------|----|--------|----|----|
 - Copy Your Computer's Time Settings** button
- Support:** A sidebar on the right with "Helpful Hints..." and "More..." links.

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

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

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

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

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

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

Account Name: Enter your account for sending email.

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

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

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

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

EMAIL SETTINGS

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

ENABLE

Enable Email Notification :

EMAIL SETTINGS

From Email Address:

To Email Address:

SMTP Server Address:

SMTP Server Port:

Enable Authentication :

Account Name:

Password:

Verify Password:

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full:

On Schedule:

Schedule :

Details :

System Settings

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

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

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

Reboot Device: Select to reboot the router.

The screenshot displays the D-Link DIR-635 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar includes 'DIR-635', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SYSTEM SETTINGS' section is highlighted in orange. The main content area contains the following text and controls:

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 Settings To Local Hard Drive:

Load Settings From Local Hard Drive:

Restore To Factory Default Settings:

Reboot 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 interface, the word 'WIRELESS' is displayed.

Update Firmware

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

Firmware Upgrade: Click **Check Online Now for Latest Firmware Version** to find out if there is an updated firmware. 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.

Notifications Options: Check **Automatically Check Online for Latest Firmware Version** to have the router check automatically to see if there is a new firmware upgrade.

Check **Email Notification of Newer Firmware Version** to have the router send an email when there is a new firmware available.

The screenshot shows the D-Link DIR-635 web interface. The top navigation bar includes 'DIR-635', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'FIRMWARE' section is active, displaying the following information:

- FIRMWARE INFORMATION**
 - Current Firmware Version : 1.00
 - Current Firmware Date : 10 May 2007
 - Latest Firmware Version : 1.00
 - [Click here to access firmware online.](#)
- FIRMWARE UPGRADE**
 - 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.
 - 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.
 - Upload :

On the right side, there is a 'Helpful Hints...' section with text: 'Firmware updates are released periodically to improve the functionality of your router and 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.

DDNS

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

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

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

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

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

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

Timeout: Enter the period (in hours).

Status: Displays the current connection status.

DYNAMIC DNS

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

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.

DYNAMIC DNS

Enable Dynamic DNS:

Server Address: << Select Dynamic DNS Server >>

Host Name: (e.g.: me.mydomain.net)

Username or Key:

Password or Key:

Verify Password or Key:

Timeout: (hours)

Status: Disconnect

System Check

Ping Test: Enter the IP Address that you wish to ping, and click **Ping**.

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



The screenshot displays the D-Link DIR-635 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The TOOLS tab is selected, and the PING TEST tool is active. The interface features a sidebar menu with options like ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area contains a PING TEST section with a text input field for 'Host Name or IP Address', a 'Ping' button, and a 'Stop' button. Below this is a PING RESULT section with a text area for displaying results. A 'Helpful Hints...' section on the right provides instructions on how to use the ping test. The bottom of the page features a 'WIRELESS' section.

| DIR-635 | SETUP | ADVANCED | TOOLS | STATUS | SUPPORT |
|-----------------|--|----------|-------|--------|--|
| ADMIN | PING TEST | | | | Helpful Hints... "Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name. More... |
| TIME | Ping Test sends "ping" packets to test a computer on the Internet. | | | | |
| SYSLOG | PING TEST | | | | |
| EMAIL SETTINGS | Host Name or IP Address : <input type="text"/> <input type="button" value="Ping"/> <input type="button" value="Stop"/> | | | | |
| SYSTEM | PING RESULT | | | | |
| FIRMWARE | Enter a host name or IP address above and click 'Ping' | | | | |
| DYNAMIC DNS | | | | | |
| SYSTEM CHECK | | | | | |
| SCHEDULES | | | | | |
| WIRELESS | | | | | |

Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

Name: Enter a name for your new schedule.

Days: Select a day, a range of days, or all week to include every day.

Time: Check All Day - 24hrs or enter a start and end time for your schedule.

Save: Click **Save** to save your schedule. You must click **Save Settings** at the top for your schedules to go into effect.

Schedule Rules The list of schedules will be listed here. Click the **List:** **Edit** icon to make changes or click the **Delete** icon to remove the schedule.

The screenshot shows the D-Link DIR-635 web interface. The top navigation bar includes 'DIR-635 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various settings: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES (which is highlighted). Below the sidebar is a language dropdown set to 'English'. The main content area is titled 'SCHEDULES' and contains the following sections:

- SCHEDULES**: A header section with a description: "The Schedule configuration option is used to manage schedule rules for various firewall and parental control features."
- ADD SCHEDULE RULE**: A form with the following fields:
 - Name**: A text input field.
 - Day(s)**: Radio buttons for 'All Week' and 'Select Day(s)'. Under 'Select Day(s)', there are checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat.
 - All Day - 24 hrs**: A checkbox.
 - Start Time**: A time selection field with hour (12), minute (0), and AM/PM dropdown. A note indicates "(hour:minute, 12 hour time)".
 - End Time**: A time selection field with hour (12), minute (0), and AM/PM dropdown. A note indicates "(hour:minute, 12 hour time)".
 - Buttons**: 'Save' and 'Clear' buttons.
- SCHEDULE RULES LIST**: A table with columns for 'Name', 'Day(s)', and 'Time Frame'. The table is currently empty.

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

Schedules are used with a number of other features to define when those features are in effect.

Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

Click **Save** to add a completed schedule to the list below.

Click the **Edit** icon to change an existing schedule.

Click the **Delete** icon to permanently delete a schedule.

[More...](#)

Device Information

This page displays the current information for the DIR-635. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a release and renew button will be displayed. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

If your Internet connection is set up for **PPPoE**, a **Connect** and a **Disconnect** button will be displayed on the screen. Use **Disconnect** to drop the **PPPoE** connection and use **Connect** to establish the **PPPoE** connection.

General: Displays the router's time and firmware version.

WAN: Displays the MAC address and the public IP settings for the router.

LAN: Displays the MAC address and the private (local) IP settings for the router.

Wireless LAN: Displays the wireless MAC address and your wireless settings such as SSID and Channel.

LAN Computers: Displays computers and devices that are connected to the router via Ethernet and that are receiving an IP address assigned by the router (DHCP).

DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : 2004年1月31日 下午 05:35:59
Firmware Version : 2.30WW, 2008/11/13

WAN

Connection Type : DHCP Client
QoS Engine : Active
Cable Status : Connected
Network Status : Established
Connection Up Time : 0 Day 0 Hour 52 Min 24 Sec

MAC Address : 00:03:64:00:01:23
IP Address : 172.17.5.143
Subnet Mask : 255.255.255.0
Default Gateway : 172.17.5.254
Primary DNS Server : 192.168.168.250
Secondary DNS Server : 192.168.168.201

LAN

MAC Address : 00:03:64:00:01:24
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

Wireless Radio : Enabled
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Channel Width : 20MHz
Channel : 5
WISH : Active
Wi-Fi Protected Setup : Enabled/Not Configured

SSID List

| Network Name (SSID) | MAC Address | Security Mode |
|---------------------|-------------------|---------------|
| dlink | 00:03:7f:be:f1:35 | Disabled |

LAN COMPUTERS

| IP Address | Name (if any) | MAC |
|---------------|-----------------|-------------------|
| 192.168.0.199 | 06623NBWINXPSP2 | 00:1c:23:0d:3d:af |

Logs

The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

What to View: You can select the types of messages that you want to display from the log. **Firewall & Security**, **System**, and **Router Status** messages can be selected.

View Levels: There are three levels of message importance: **Informational**, **Warning**, and **Critical**. Select the levels that you want display in the log.

Apply Log Settings: The log results are filtered so that only the selected appear.

Refresh: Updates the log details on the screen so it displays any recent activity.

Clear: Clears all of the log contents.

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

Save Log: This option will save the router to a log file on your computer.

D-Link

DIR-635

SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO

LOGS

STATISTICS

INTERNET SESSIONS

WIRELESS

WISH SESSIONS

LOGS

System Logs

Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

LOG OPTIONS

What to View: Firewall & Security System Router Status

View Levels: Critical Warning Informational

Apply Log Settings Now

LOG DETAILS

Refresh Clear Email Now Save Log

[INFO] Sat Jan 31 11:54:25 2004 Log viewed by IP address 192.168.0.156
 [INFO] Sat Jan 31 11:22:36 2004 Allowed configuration authentication by IP address 192.168.0.156
 [INFO] Sat Jan 31 11:22:23 2004 Latest firmware version 1.0 is available
 [INFO] Sat Jan 31 11:22:23 2004 Firmware upgrade server support.dlink.com is at IP address 64.7.210.130
 [INFO] Sat Jan 31 11:22:23 2004 Starting WAN Services
 [INFO] Sat Jan 31 11:22:23 2004 Estimated rate of link is 996 kbps
 [INFO] Sat Jan 31 11:21:59 2004 Lease 192.168.0.156 renewed by client 0011092A9411
 [INFO] Sat Jan 31 11:21:59 2004 Assigned new lease 192.168.0.156 to client 0011092A9411
 [WARN] Sat Jan 31 11:21:59 2004 Lease expired 192.168.0.156 - was reassigned because a client specifically requested this address
 [INFO] Sat Jan 31 11:21:53 2004 Initialization complete, starting DHCP server
 [INFO] Sat Jan 31 11:21:51 2004 Estimating speed of WAN interface
 [INFO] Sat Jan 31 11:21:51 2004 WAN interface is up. Connection to Internet established with IP Address 192.168.111.65 and default gateway 192.168.111.1
 [INFO] Sat Jan 31 11:21:51 2004 Obtained IP Address using DHCP. IP address is 192.168.111.65
 [INFO] Sat Jan 31 11:21:51 2004 DHCP Server Parameter 15 was added to the parameter database
 [INFO] Sat Jan 31 11:21:50 2004 DHCP Server Parameter 19 was added to the parameter database
 [INFO] Sat Jan 31 11:21:50 2004 DHCP Server Parameter 3 was added to the parameter database
 [INFO] Sat Jan 31 11:21:50 2004 DHCP Server Parameter 1 was added to the parameter database
 [INFO] Sat Jan 31 11:21:48 2004 Bringing up WAN using DHCP
 [INFO] Sat Jan 31 11:21:48 2004 WAN interface cable has been connected
 [INFO] Sat Jan 31 11:21:46 2004 DHCP Server Parameter 6 was added to the parameter database
 [INFO] Sat Jan 31 11:21:46 2004 LAN interface is up
 [INFO] Sat Jan 31 11:21:46 2004 LAN Ethernet Carrier Detected
 [INFO] Sat Jan 31 11:21:46 2004 Device initialized
 [INFO] Sat Jan 31 11:21:46 2004 Wireless Link is up
 [INFO] Sat Jan 31 11:21:46 2004 Stored configuration to non-volatile memory
 [INFO] Sat Jan 31 11:21:45 2004 No Internet access policy is in effect. Unrestricted Internet access allowed to everyone
 [INFO] Thu Jan 01 00:00:00 1970 Loaded configuration from non-volatile memory

Helpful Hints...

Check the log frequently to detect unauthorized network usage.

You can also have the log mailed to you periodically. Refer to **Tools** → **Email**.

More...

WIRELESS

Statistics

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-635 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.

D-Link

DIR-635 // SETUP ADVANCED TOOLS STATUS SUPPORT

TRAFFIC STATISTICS

Network Traffic Stats
Traffic Statistics display Receive and Transmit packets passing through your router.
Refresh Statistics Clear Statistics

LAN STATISTICS

| | |
|------------------------|------------------------|
| Sent : 36459 | Received : 22978 |
| TX Packets Dropped : 0 | RX Packets Dropped : 0 |
| Collisions : 0 | Errors : 0 |

WAN STATISTICS

| | |
|------------------------|------------------------|
| Sent : 19151 | Received : 31403 |
| TX Packets Dropped : 0 | RX Packets Dropped : 0 |
| Collisions : 0 | Errors : 0 |

WIRELESS STATISTICS

| | |
|------------------------|------------------|
| Sent : 10330 | Received : 25649 |
| TX Packets Dropped : 0 | Errors : 0 |

WIRELESS

Internet Sessions

D-Link

DIR-635 // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET SESSIONS

This page displays the full details of active internet sessions to your router.

| Local | NAT | Internet | Protocol | State | Dir | Priority | Time Out |
|---------------------|-------|-------------------|----------|-------|-----|----------|----------|
| 192.168.0.174:49565 | 49565 | 208.111.144.64:80 | TCP | TW | Out | 128 | 239 |
| 192.168.0.174:49564 | 49564 | 64.7.210.130:80 | TCP | EST | Out | 136 | 7787 |
| 192.168.0.174:49563 | 49563 | 64.7.210.130:80 | TCP | EST | Out | 175 | 7787 |
| 192.168.0.174:49562 | 49562 | 216.246.93.56:80 | TCP | EST | Out | 129 | 7769 |
| 192.168.0.174:49561 | 49561 | 64.210.194.51:80 | TCP | LA | Out | 128 | 194 |
| 192.168.0.174:49558 | 49558 | 208.111.144.64:80 | TCP | LA | Out | 128 | 164 |
| 192.168.0.174:49553 | 49553 | 216.246.93.59:80 | TCP | CL | Out | 128 | 169 |

Wireless

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

The screenshot shows the D-Link DIR-635 web interface. The top navigation bar includes 'DIR-635', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists 'DEVICE INFO', 'LOGS', 'STATISTICS', 'INTERNET SESSIONS', 'WIRELESS', and 'WISH SESSIONS'. The main content area is titled 'WIRELESS' and contains the following information:

Associated Wireless Client List
Use this option to view the wireless clients that are connected to your wireless router.

NUMBER OF WIRELESS CLIENTS : 1

| MAC Address | IP Address | Mode | Rate | Signal(%) |
|-------------------|---------------|------|------|-----------|
| 00:03:2F:11:23:28 | 192.168.0.127 | 11g | 54 | 100 |

On the right side, there is a 'Helpful Hints...' section with the text: 'This is a list of all wireless clients that are currently connected to your wireless router.' and a 'More...' link.

WISH Sessions

The WISH Sessions page displays full details of wireless clients that are connected when WISH is enabled.

The screenshot shows the D-Link DIR-635 web interface. The top navigation bar includes 'DIR-635', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists 'DEVICE INFO', 'LOGS', 'STATISTICS', 'INTERNET SESSIONS', 'WIRELESS', and 'WISH SESSIONS'. The main content area is titled 'WISH SESSIONS' and contains the following information:

WISH SESSIONS
The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

WISH SESSIONS

| Originator | Target | Protocol | State | Priority | Time Out |
|------------|--------|----------|-------|----------|----------|
|------------|--------|----------|-------|----------|----------|

On the right side, there is a 'Helpful Hints...' section with the text: 'This is a list of all active conversations involving wireless clients in the local network.' and a 'More...' link.

Support

D-Link

DIR-635 //

SETUP ADVANCED TOOLS STATUS SUPPORT

MENU
SETUP
ADVANCED
TOOLS
STATUS

English ▾

SUPPORT MENU

- [Setup](#)
- [Advanced](#)
- [Tools](#)
- [Status](#)

SETUP HELP

- [Internet Connection](#)
- [WAN](#)
- [Wireless](#)
- [Network Settings](#)
- [USB Settings](#)

ADVANCED HELP

- [Virtual Server](#)
- [Port Forwarding](#)
- [Application Rules](#)
- [QoS Engine](#)
- [Access Control](#)
- [Website Filter](#)
- [Network Filter](#)
- [Firewall Settings](#)
- [Routing](#)
- [Inbound Filter](#)
- [Advanced Wireless](#)
- [WISH](#)
- [Wi-Fi Protected Setup](#)
- [Advanced Network](#)

TOOLS HELP

- [Admin](#)
- [Time](#)
- [Syslog](#)
- [Email Settings](#)
- [System](#)
- [Firmware](#)
- [Dynamic DNS](#)
- [System Check](#)
- [Schedules](#)

STATUS HELP

- [Device Info](#)
- [Wireless](#)
- [Logs](#)
- [Statistics](#)
- [Internet Sessions](#)
- [WISH Sessions](#)

WIRELESS

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-635 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WPA?

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

The 2 major improvements over WEP:

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

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

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

Wireless Security Setup Wizard

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

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 Wi-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](#)

Type your desired wireless network name (SSID).

Automatically: Select this option to automatically generate the router's network key and click **Next**.

Manually: Select this option to manually enter your network key and click **Next**.

STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Give your network a name, using up to 32 characters.

Network Name (SSID) :

Automatically assign a network key(Recommended)
To prevent outsiders from accessing your network, the router will automatically assign a security to your network.

Manually assign a network key
Use this options if you prefer to create our own key.

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

[Prev](#) [Next](#) [Cancel](#) [Save](#)

If you selected **Automatically**, the summary window will display your settings. Write down the security key and enter this on your wireless clients. Click **Save** to save your settings.

SETUP COMPLETE!

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

Wireless Network Name (SSID) : dlink

Security Mode 2 : Auto (WPA or WPA2) - Personal

Cipher Type : TKIP and AES

Pre-Shared Key :
d6982bfc80a9c5ff56caee3691aca439de94ce5024fc5b6bed63ba3dc3caa586

Prev Next Cancel Save

If you selected **Manually**, the following screen will appear.

STEP 2: SET YOUR WIRELESS SECURITY PASSWORD

You have selected your security level - you will need to set a wireless security password.

The WPA (Wi-Fi Protected Access) key must meet one of following guidelines:

- Between 8 and 64 characters (A longer WPA key is more secure than a short one)
- Exactly 64 characters using 0-9 and A-F

Use the same Wireless Security Password on both 2.4GHz and 5GHz band

2.4GHz Band Wireless Security Password :

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

Prev Next Cancel Save

Add Wireless Device with WPS Wizard

From the **Setup > Wireless Settings** screen, click **Add Wireless Device with WPS**.



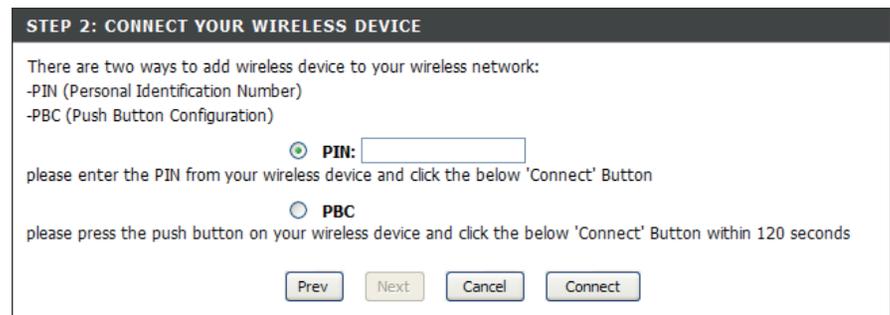
Select **Auto** to add a wireless client using WPS (Wi-Fi Protected Setup). Once you select **Auto** and click **Connect**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

If you select **Manual**, a settings summary screen will appear. Write down the security key and enter this on your wireless clients.



PIN: Select this option to use **PIN** method. In order to use this method you must know the wireless client's 8 digit PIN and click **Connect**.

PBC: Select this option to use **PBC** (Push Button) method to add a wireless client. Click **Connect**.



Configure WPA-Personal (PSK)

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1).
2. Click **Setup** and then click **Wireless Settings**.
3. **Security Mode:** Select **WPA-Personal** for this mode option.
4. **WPA Mode:** Select **Auto**, **WPA2 Only**, or **WPA Only**. Select **Auto**, if you have wireless clients using both WPA and WPA2.
5. **Cypher Type:** Select **TKIP** and **AES**, **TKIP**, or **AES**.
6. **Group Key Update Interval:** Enter the time interval required for the group key to broadcast and multicast data is changed (3600 is default).
7. **Pre-Shared Key:** Enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.
8. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

WIRELESS SECURITY MODE

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

Security Mode : WPA-Personal ▼

WPA

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

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

WPA Mode : Auto (WPA or WPA2) ▼

Cipher Type : TKIP and AES ▼

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : ●●●●●●●●

Configure WPA-Enterprise (RADIUS)

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

1. Log into the web-based configuration by opening a web browser and enter the IP address of the router (192.168.0.1).
2. Click **Setup** and then click **Wireless Settings**.
2. **Security Mode:** Select **WPA-Enterprise** for this mode option.
3. **WPA Mode:** Select **Auto**, **WPA2 Only**, or **WPA Only**. Select **Auto** if you have wireless clients using both WPA and WPA2.
4. **Cypher Type:** Select **TKIP** and **AES**, **TKIP**, or **AES**.
5. **Group Key Update Interval:** Enter the time interval required for the group key to broadcast and multicast data is changed. The default value is 3600.
6. **Authentication Timeout:** Enter the time interval for a client to re-authenticate. The default value is 60 minutes.
7. **RADIUS Server IP Address:** Enter the IP Address of your RADIUS server.
8. **RADIUS Server Port:** Enter the port number of your RADIUS server. 1812 is the default port number.

WIRELESS SECURITY MODE

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

Security Mode :

WPA

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

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

WPA Mode :

Cipher Type :

Group Key Update Interval : (seconds)

EAP (802.1X)

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

Authentication Timeout : (minutes)

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

MAC Address Authentication :

9. **RADIUS Server Shared Secret:** Enter the security key.
10. If the **MAC Address Authentication** box is selected then the user will need to connect from the same computer whenever logging into the wireless network.
11. Click **Advanced** to enter settings for a secondary RADIUS Server.
12. Click **Apply Settings** to save your settings.

EAP (802.1X)

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

Authentication Timeout : (minutes)

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

MAC Address Authentication :

Optional backup RADIUS server:

Second RADIUS server IP Address :

Second RADIUS server Port :

Second RADIUS server Shared Secret :

Second MAC Address Authentication :

Connect to a Wireless Network Using Windows Vista®

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

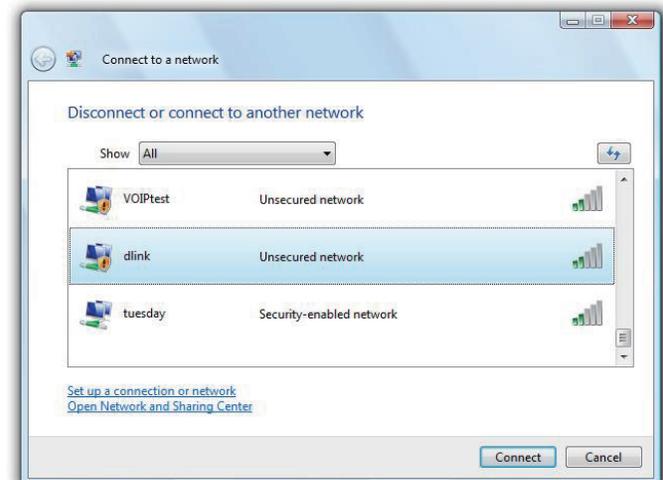
If you receive the **Wireless Networks Detected** dialog box, click on the center of the box to access the utility.

or

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

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

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



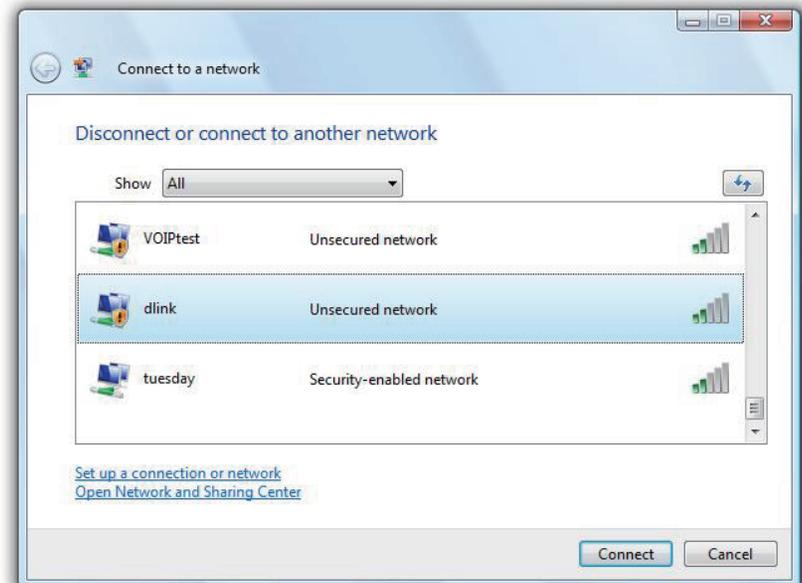
Configure Wireless Security

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

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

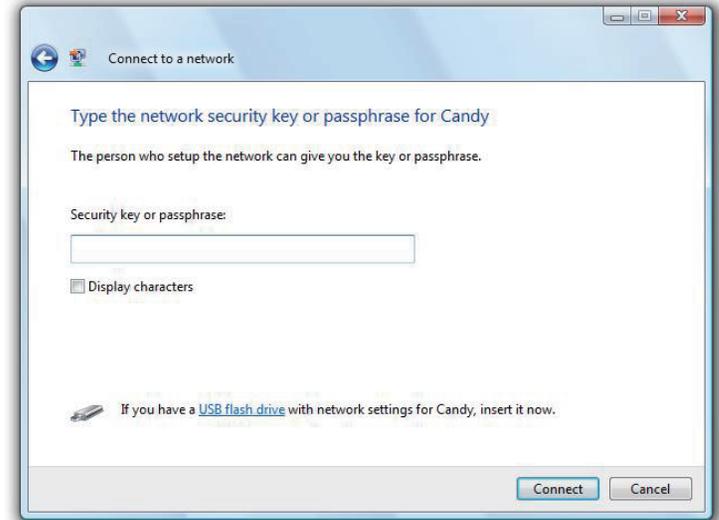


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



Connect Using WCN 2.0 in Windows Vista®

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and not configured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the **Enable** checkbox in the **Basic > Wireless** section. Use the Current PIN that is displayed on the **Advanced > Wi-Fi Protected Setup** section or choose to click **Generate New PIN** or **Reset PIN to Default**.

For additional information, please refer to page 68.



If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Connect to a Wireless Network Using Windows® XP

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

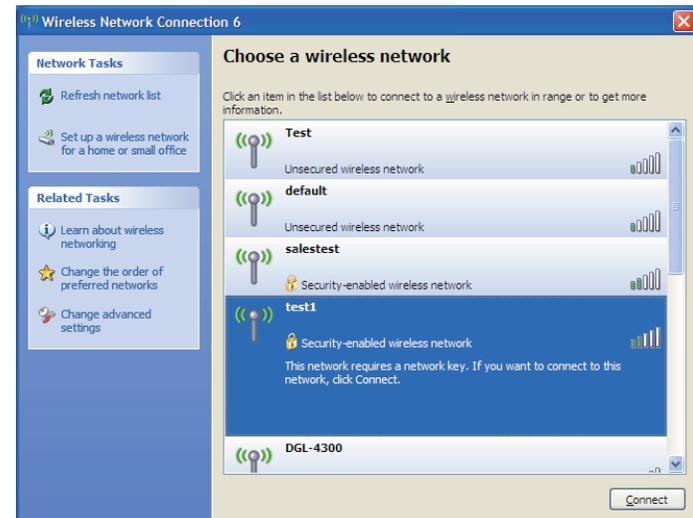
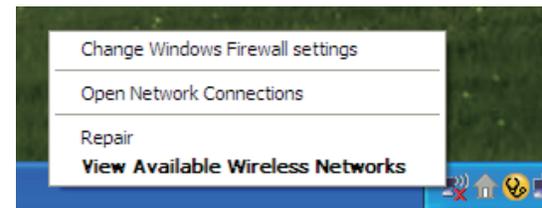
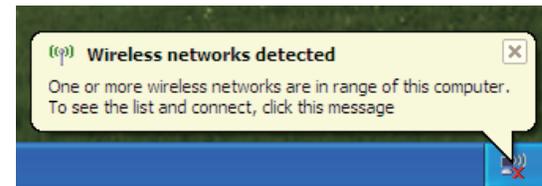
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

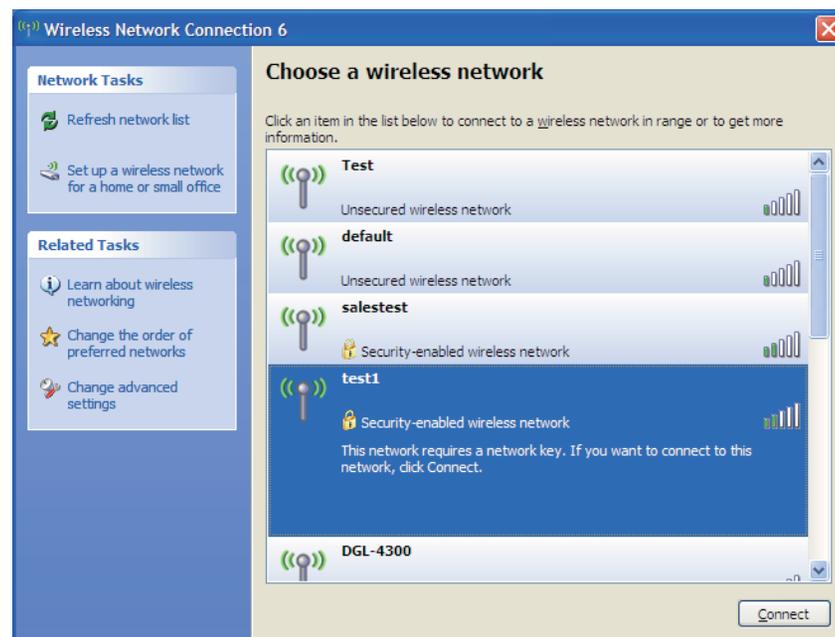
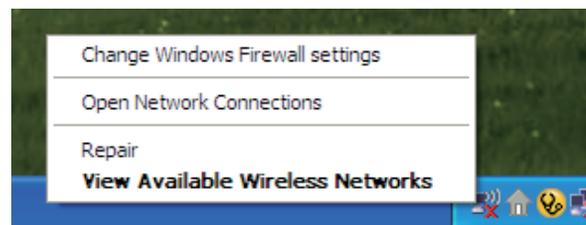
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



Configure WPA-PSK

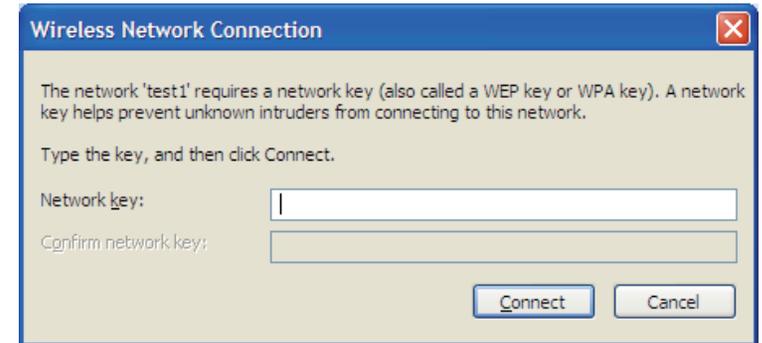
It is recommended that you enable WPA-PSK on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA-PSK key being used.

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



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

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-635. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

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

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to **Never Dial a Connection**. Click **LAN Settings**. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and then re-open it again.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is admin and leave the password box empty.

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

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

Note: AOL DSL+ users must use MTU of 1400.

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

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

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

Example: ping yahoo.com -f -l 1472

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

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

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

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

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

Do not allow your neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to the *Product Manual* for further information.

Wireless Modes

There are basically two modes of networking:

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

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

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

Networking Basics

Check your IP address

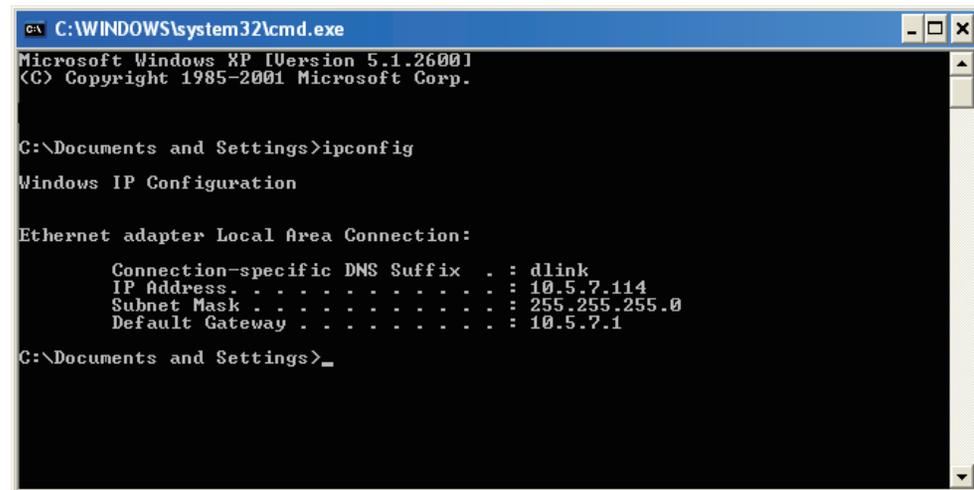
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Go to **Start > Run**. In the run box type **cmd** and then click **OK**. (Windows® Vista users type cmd in the **Start Search** box.)

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

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

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

Statically Assign an IP address

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

Step 1

Windows® Vista - Go to **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections**

Windows® XP - Go to **Start > Control Panel > Network Connections**

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

Step 2

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

Step 3

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

Step 4

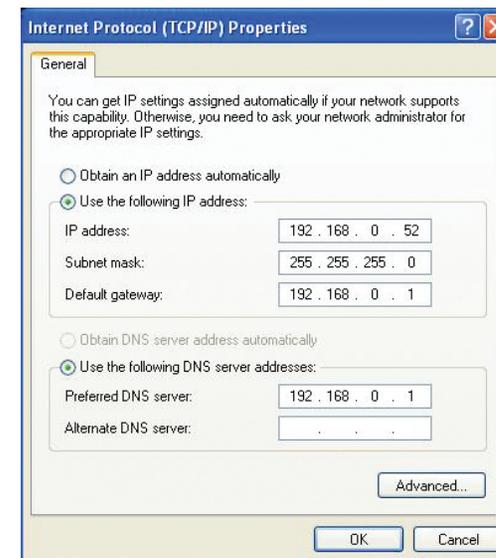
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make sure your IP address is 192.168.0.X, where X is a number between 2 and 99. Also, ensure that the number you choose is not in use on the network. The **Default Gateway** should be set similar to the LAN IP address of your router (192.168.0.1).

The **Primary DNS** should be the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click **OK** twice to save your settings.



Technical Specifications

Standards

- IEEE 802.11n (draft 2.0)
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

Security

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

Wireless Signal Rates*

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

MSC (0-15)

- 130Mbps (270)
- 117Mbps (243)
- 104Mbps (216)
- 78Mbps (162)
- 66Mbps (135)
- 58.5Mbps (121.5)
- 52Mbps (108)
- 39Mbps (81)
- 26Mbps (54)
- 19.5Mbps (40.5)
- 12Mbps (27)
- 6.5Mbps (13.5)

Frequency Range

2.4GHz to 2.483GHz

External Antenna Type

Three detachable reverse SMA Antennas

Power Input

- 5 VDC, 2.5A
- Through external power adapter

LEDs

- Power
- Status
- WAN
- WLAN
- USB
- LAN (10/100) (per port)

Dimensions

116.84 x 193.04 x 30.48 mm
(4.6 x 7.6 x 1.2 inches)

Weight

368.3 grams (0.8 lb)

Operating Temperature

0°C to 40°C (32°F to 104°F)

Humidity

95% maximum (non-condensing)

Certifications

- FCC Class B
- CE
- C-Tick
- IC
- Wi-Fi
- Wi-Fi Protected Setup (WPS)
- Works with Windows Vista

* Maximum wireless signal rate derived from IEEE Standard 802.11g and Draft 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 factors will adversely affect wireless signal range.