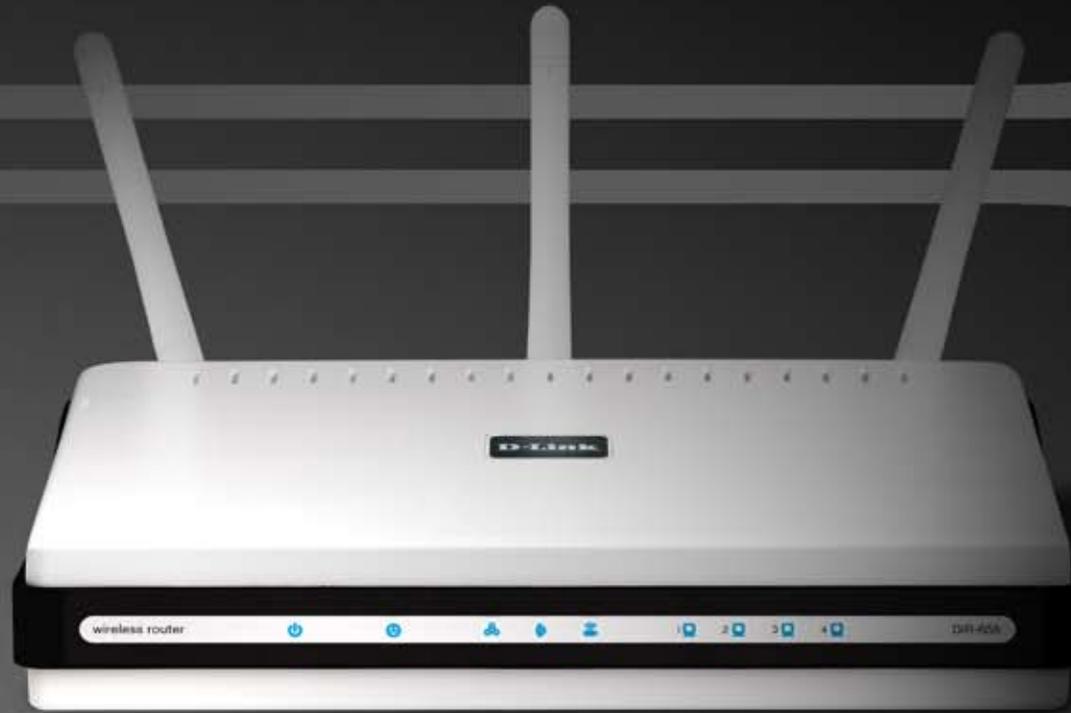


# USER MANUAL

DIR-655

VERSION 1.1



**D-Link**<sup>®</sup>

**WIRELESS**

---

# Table of Contents

<b>Product Overview</b> .....	<b>4</b>	Virtual Server .....	30
Package Contents .....	4	Port Forwarding .....	32
System Requirements .....	4	Application Rules .....	33
Introduction .....	5	QoS Engine .....	34
Features .....	6	Network Filters .....	35
Hardware Overview .....	7	Access Control .....	36
Connections .....	7	Access Control Wizard .....	36
LEDs .....	8	Website Filters .....	39
<b>Installation</b> .....	<b>9</b>	Inbound Filters .....	40
Before you Begin .....	9	Firewall Settings .....	41
Wireless Installation Considerations .....	10	Application Level Gateway (ALG) Configuration .....	42
Getting Started .....	11	VPN Passthrough .....	42
<b>Configuration</b> .....	<b>12</b>	RTSP .....	42
Web-based Configuration Utility .....	12	H.323 .....	42
Setup Wizard .....	13	SIP (VoIP) .....	42
Manual Configuration .....	17	MMS .....	42
Dynamic (Cable) .....	17	Advanced Wireless Settings .....	43
PPPoE (DSL) .....	18	Transmit Power .....	43
PPTP .....	19	802.11d Mode .....	43
L2TP .....	21	WISH Settings .....	44
Static (assigned by ISP) .....	23	Advanced Network Settings .....	46
Big Pond .....	24	UPnP .....	46
Wireless Settings .....	25	Internet Ping Block .....	46
Network Settings .....	27	Internet Port Speed .....	46
DHCP Server Settings .....	28	Multicast Streams .....	46
DHCP Reservation .....	29		

Administrator Settings.....	47	Configure WPA-PSK .....	73
Change Password.....	47	<b>Troubleshooting .....</b>	<b>75</b>
Remote Management.....	47	<b>Wireless Basics .....</b>	<b>79</b>
Time Settings.....	48	What is Wireless? .....	80
SysLog.....	49	Tips.....	82
Email Settings.....	50	Wireless Modes .....	83
System Settings.....	51	<b>Networking Basics .....</b>	<b>84</b>
Update Firmware .....	52	Check your IP address .....	84
DDNS.....	53	Statically Assign an IP address .....	85
System Check.....	54	<b>Technical Specifications.....</b>	<b>86</b>
Schedules .....	55		
Device Information.....	56		
Log.....	57		
Stats.....	58		
Active Sessions .....	58		
Wireless .....	59		
WISH .....	59		
Support .....	60		
<b>Wireless Security.....</b>	<b>61</b>		
What is WEP? .....	61		
What is WPA? .....	62		
Wireless Security Setup Wizard .....	63		
Configure WEP .....	66		
Configure WPA-Personal (PSK).....	67		
Configure WPA-Enterprise (RADIUS) .....	68		
<b>Connect to a Wireless Network.....</b>	<b>70</b>		
Using Windows® XP.....	70		
Configure WEP .....	71		

# Package Contents

- D-Link DIR-655 Xtreme N™ Router
- 3 Detachable Antennas
- Power Adapter
- CAT5 Ethernet Cable
- CD-ROM with Installation Wizard, User Manual, and Special Offers



**Note:** Using a power supply with a different voltage rating than the one included with the DIR-655 will cause damage and void the warranty for this product.

# System Requirements

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

# 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 Xtreme N™ Router (DIR-655) is a draft 802.11n compliant device that delivers real world performance of up to 650% faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the Xtreme N™ Router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this Router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

## **EXTENDED WHOLE HOME COVERAGE**

Powered by Xtreme N™ technology, this high performance router provides superior Whole Home Coverage while reducing dead spots. The Xtreme N™ Router is designed for use in bigger homes and for users who demand higher performance networking. Add a Xtreme N™ notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

## **TOTAL NETWORK SECURITY**

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

\* Maximum wireless signal rate derived from IEEE Standard 802.11g and 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.

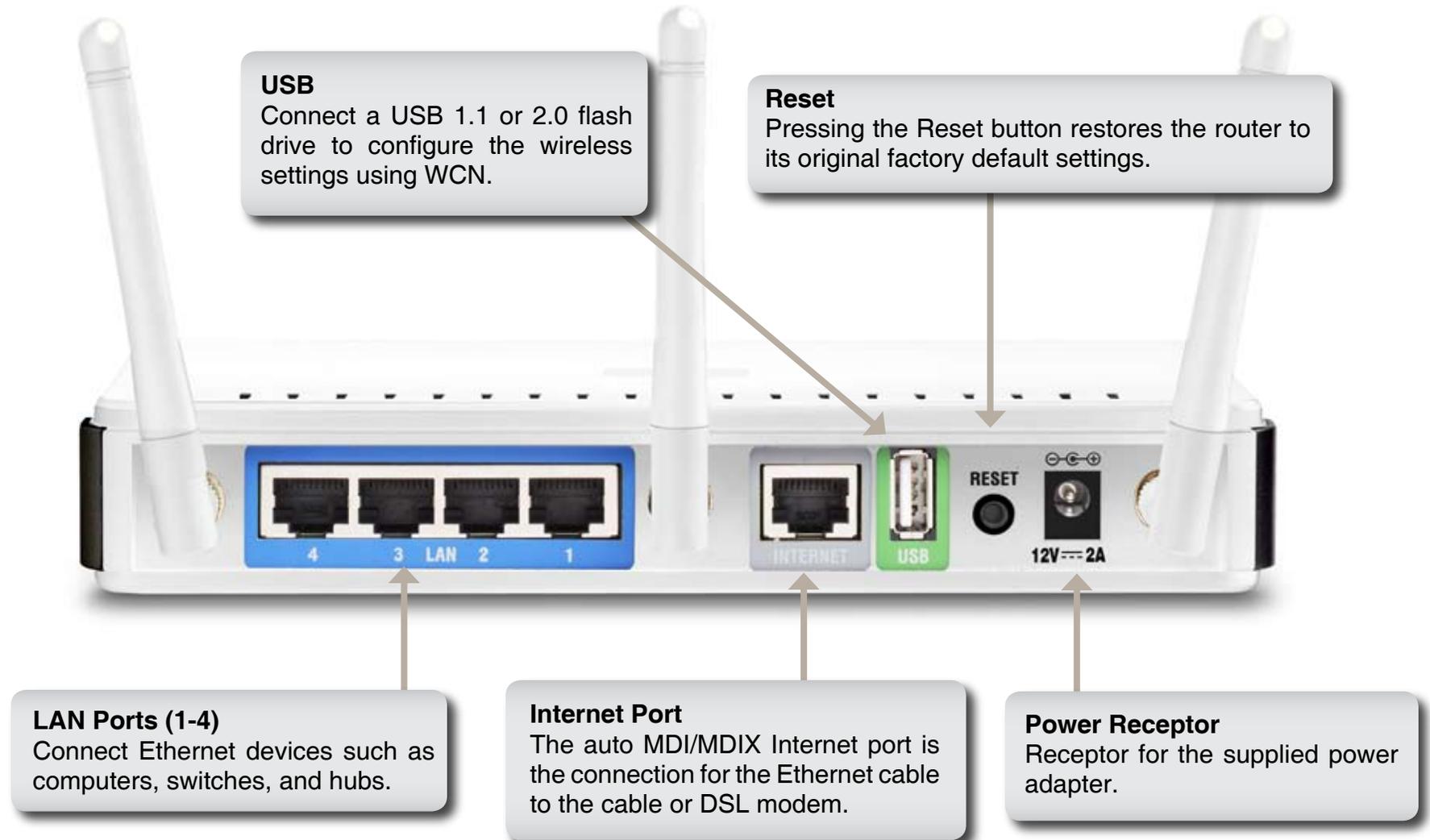
# Features

- **Faster Wireless Networking** - The DIR-655 provides up to 300Mbps\* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11n wireless router gives you the freedom of wireless networking at speeds 650% faster than 802.11g.
- **Compatible with 802.11b and 802.11g Devices** - The DIR-655 is still fully compatible with the IEEE 802.11b standard, so it can connect with existing 802.11b PCI, USB and Cardbus adapters.
- **Advanced Firewall Features** - The Web-based user interface displays a number of advanced network management features including:
  - **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-655 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-655 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-655 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.

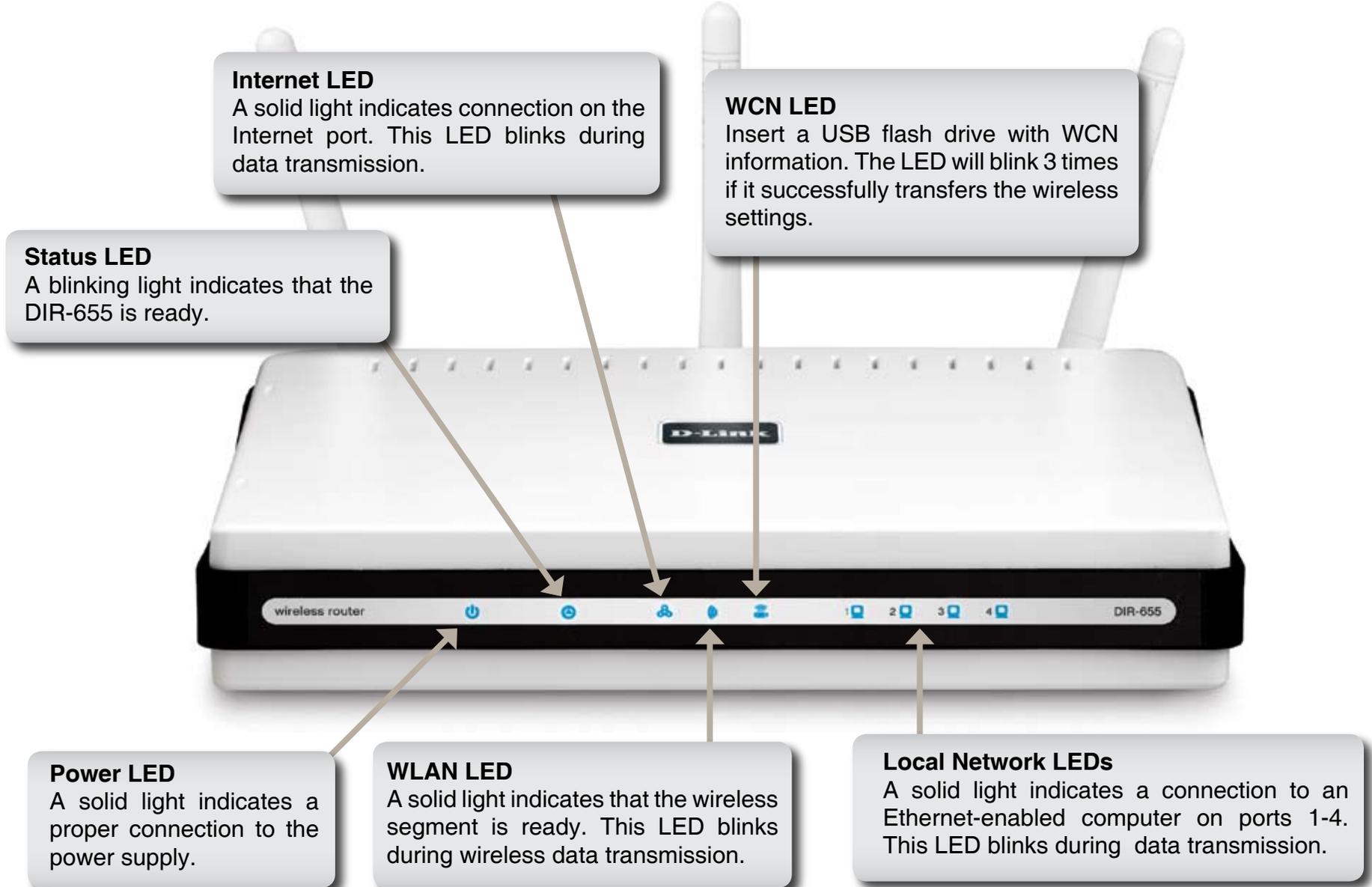
# Hardware Overview

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

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

# Wireless Installation Considerations

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

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

# Getting Started

The EBR-2310 includes a Quick Router Setup Wizard CD. Follow the simple steps below to run the Setup Wizard to guide you quickly through the installation process.

Insert the **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:\DIR655.exe"** (where **D:** represents the drive letter of your CD-ROM drive).

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

Click **Install Router**



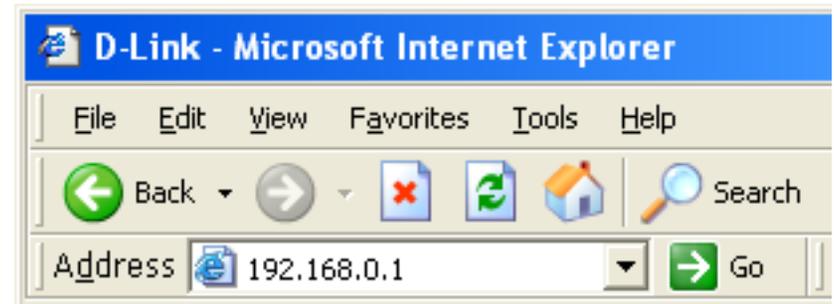
**Note:** It is recommended to write down the SSID and Security Key, followed by the login password on the provided CD holder.

# Configuration

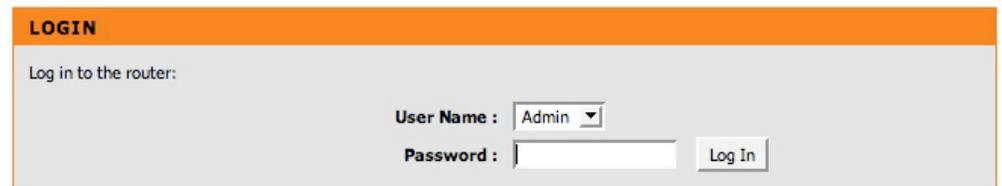
This section will show you how to configure your new D-Link wireless router using the web-based configuration utility.

## Web-based Configuration Utility

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



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

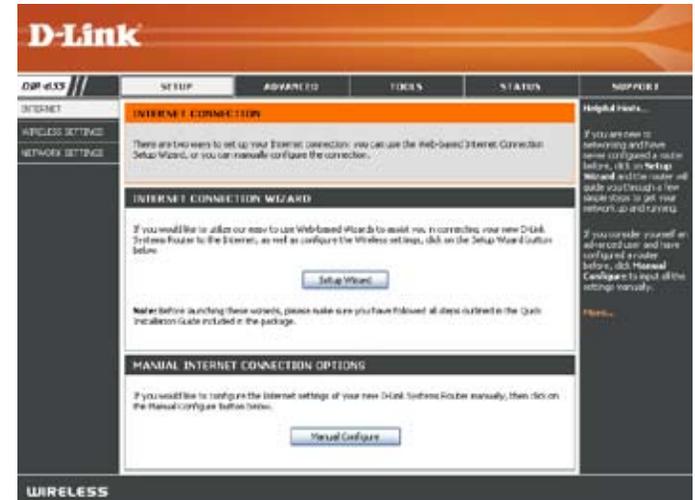


If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.

# Setup Wizard

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

If you want to enter your settings without running the wizard, click **Manual Configuration** and skip to page 19.



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

If you want to configure your wireless settings, click **Launch Wireless Security Setup Wizard** and skip to page 62.

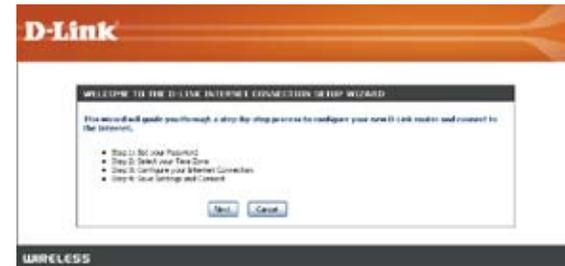


Click **Next** to continue.

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

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

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



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

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

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

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

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

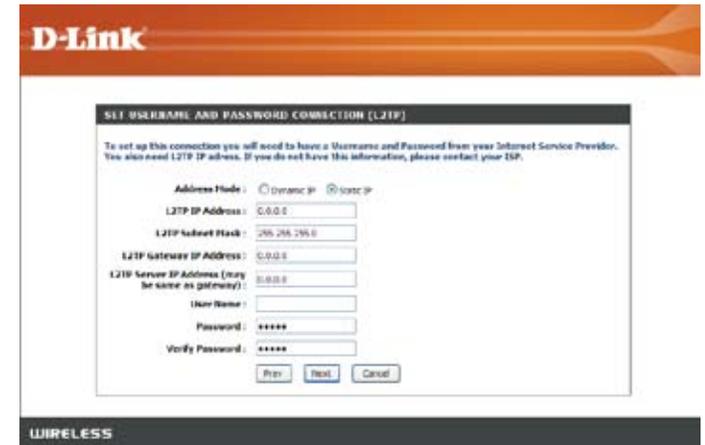
If you selected PPTP, enter your PPTP username and password. Click **Next** to continue.

The screenshot shows the 'DHCP CONNECTION (DYNAMIC IP ADDRESS)' configuration page. It includes a 'MAC Address' field with a 'Clone Your PC's MAC Address' button. Below it is a 'Host Name' field. A note at the bottom states: 'Note: You may also need to provide a Host Name. If you do not have or know the information, please contact your ISP.' There are 'Prev', 'Next', and 'Cancel' buttons at the bottom.

The screenshot shows the 'SET USERNAME AND PASSWORD CONNECTION (PPPOE)' configuration page. It features radio buttons for 'Dynamic IP' and 'Static IP'. Below are fields for 'IP Address', 'User Name', 'Password', 'Verify Password', and 'Service Name'. A note at the bottom states: 'Note: You may also need to provide a Service Name. If you do not have or know this information, please contact your ISP.' There are 'Prev', 'Next', and 'Cancel' buttons at the bottom.

The screenshot shows the 'SET USERNAME AND PASSWORD CONNECTION (PPTP)' configuration page. It features radio buttons for 'Dynamic IP' and 'Static IP'. Below are fields for 'PPTP IP Address', 'PPTP Subnet Mask', 'PPTP Gateway IP Address', 'PPTP Server IP Address (may be same as gateway)', 'User Name', 'Password', and 'Verify Password'. There are 'Prev', 'Next', and 'Cancel' buttons at the bottom.

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

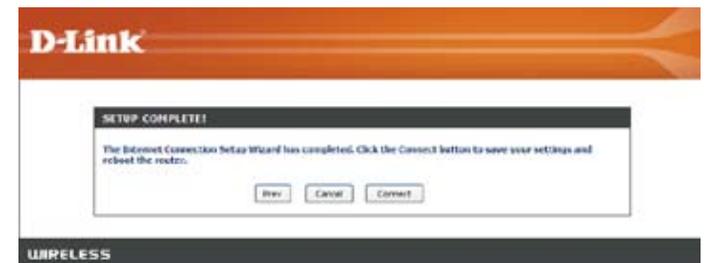


If you selected Static, enter your network settings supplied by your Internet provider. Click **Next** to continue.



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

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



# Manual Configuration

## Dynamic (Cable)

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

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

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

**DNS Addresses:** Enter the Primary DNS server IP address assigned by your ISP.

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

**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.

**D-Link**

DIR-655

SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET WIRELESS SETTINGS NETWORK SETTINGS

**WAN**

**Internet Connection**

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are unsure of your connection method, please contact your Internet Service Provider.

**Note:** If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Save Settings Don't Save Settings

**INTERNET CONNECTION TYPE**

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

My Internet Connection is: Dynamic IP (DHCP)

**DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :**

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

Host Name:

Use Unicasting:  (compatibility for some DHCP Servers)

Primary DNS Server:

Secondary DNS Server:

MTU:  (bytes) MTU default = 1500

MAC Address:

Clone Your PC's MAC Address

**Helpful Hints...**

When configuring the router to access the Internet, be sure to choose the correct **Internet Connection Type** from the drop down menu. If you are unsure of which option to choose, contact your **Internet Service Provider (ISP)**.

If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.

More...

**WIRELESS**

# Internet Setup

## PPPoE (DSL)

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

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

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

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

**User Name:** Enter your PPPoE user name.

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

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

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

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

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

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

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

The screenshot shows the D-Link router's web interface for configuring the Internet connection. The page is titled "Internet Setup" and is for a "DIR-655" router. The "WAN" tab is selected, and the "Internet Connection" section is active. The "My Internet Connection is:" dropdown menu is set to "PPPoE (Username/Password)". Below this, the "PPPoE INTERNET CONNECTION TYPE" section is visible, which includes fields for "Address Mode" (Dynamic IP or Static IP), "IP Address", "Username", "Password", "Verify Password", "Service Name", "Reconnection Mode" (Always on, On-Demand, or Manual), "Maximum Idle Time", "Primary DNS Server", "Secondary DNS Server", "MTU", and "MAC Address". A "Clone Your PC's MAC Address" button is located at the bottom of the MAC Address field.

# Internet Setup

## PPTP

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

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

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

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

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

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

**Username:** Enter your PPTP username.

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

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

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

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

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SETUP' tab is active, and the 'WAN' section is selected. The 'Internet Connection' page is displayed, showing the 'Internet Connection Type' dropdown menu set to 'PPTP (Username / Password)'. Below this, the 'PPTP INTERNET CONNECTION TYPE' section is visible, containing various configuration fields:

- Address Mode:** Radio buttons for 'Dynamic IP' and 'Static IP' (selected).
- PPTP IP Address:** Text input field with '0.0.0.0' entered.
- PPTP Subnet Mask:** Text input field with '255.255.255.0' entered.
- PPTP Gateway IP Address:** Text input field with '0.0.0.0' entered.
- PPTP Server IP Address:** Text input field with '0.0.0.0' entered.
- Username:** Text input field.
- Password:** Password input field with '\*\*\*\*\*' entered.
- Verify Password:** Password input field with '\*\*\*\*\*' entered.
- Reconnect Mode:** Radio buttons for 'Always on', 'On demand' (selected), and 'Manual'.
- Maximum Idle Time:** Text input field with '20' entered, followed by '(minutes, 0=infinite)'. There is also a checkbox for 'Auto-reconnect'.
- Primary DNS Server:** Text input field with '0.0.0.0' entered.
- Secondary DNS Server:** Text input field with '0.0.0.0' entered.
- MTU:** Text input field with '1400' entered, followed by '(bytes) MTU default = 1400'.
- MAC Address:** Text input field with '00:00:00:00:00:00' entered.

At the bottom of the form is a 'Clone Your PC's MAC Address' button. On the right side of the interface, there is a 'Helpful Hints...' section with text about configuring the router and a 'More...' link.

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

## L2TP

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

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

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

**L2TP Subnet Mask:** Enter the Subnet Mask supplied by your ISP (Static only).

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

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

**Username:** Enter your L2TP username.

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

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

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

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

The screenshot shows the D-Link DIR-655 router's configuration interface. The main heading is "WAN" and the sub-heading is "Internet Connection". Below this, there is a note about choosing the connection type and a "Save Settings" button. The "INTERNET CONNECTION TYPE" section shows "My Internet Connection is: L2TP (Username / Password)". The "L2TP INTERNET CONNECTION TYPE" section has "Address Mode" set to "Static IP". The following fields are filled with "0.0.0.0": L2TP IP Address, L2TP Subnet Mask, L2TP Gateway IP Address, and L2TP Server IP Address. The "Username" and "Password" fields are empty, with "Verify Password" also empty. The "Reconnect Mode" is set to "On demand". Other fields include "Maximum Idle Time" (20 minutes), "Primary DNS Server" (0.0.0.0), "Secondary DNS Server" (0.0.0.0), "MTU" (1400 bytes), and "MAC Address" (00:00:00:00:00:00). A "Clone Your PC's MAC Address" button is at the bottom.

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

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

# Internet Setup

## Static (assigned by ISP)

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

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

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

**Default Gateway:** Enter the Gateway assigned by your ISP.

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

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

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

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar has 'INTERNET', 'WIRELESS SETTINGS', and 'NETWORK SETTINGS'. The main content area is titled 'WAN' and 'Internet Connection'. It contains instructions for configuring the Internet Connection type, a note about PPPoE, and two buttons: 'Save Settings' and 'Don't Save Settings'. Below this is the 'INTERNET CONNECTION TYPE' section, where 'My Internet Connection is:' is set to 'Static IP'. The 'STATIC IP ADDRESS INTERNET CONNECTION TYPE' section prompts the user to enter static address information from their ISP. Fields include IP Address (0.0.0.0), Subnet Mask (255.255.255.0), Default Gateway (0.0.0.0), Primary DNS Server (0.0.0.0), Secondary DNS Server (0.0.0.0), MTU (1500 bytes, default 1500), and MAC Address (00:00:00:00:00:00). A 'Clone Your PC's MAC Address' button is located at the bottom of the form. A 'Helpful Hints...' sidebar on the right provides additional guidance.

# Internet Setup

## Big Pond

**BigPond Server:** Enter the IP address of the login server.

**BigPond Username:** Enter your BigPond username.

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

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

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

**MAC Address:**

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

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SETUP' tab is active, and the 'WAN' section is selected. The 'Internet Connection' section is titled 'Internet Connection' and contains instructions on how to choose a connection type. Below this, there are 'Save Settings' and 'Don't Save Settings' buttons. The 'INTERNET CONNECTION TYPE' section has a dropdown menu set to 'BigPond (Australia)'. The 'BIG POND INTERNET CONNECTION TYPE' section contains fields for 'BigPond Server', 'BigPond User Id', 'BigPond Password', 'Verify Password', 'Primary DNS Server', 'Secondary DNS Server', 'MTU' (set to 1500), and 'MAC Address'. A 'Clone Your PC's MAC Address' button is located at the bottom of this section. A 'Helpful Hints...' sidebar on the right provides additional guidance.

# Wireless Settings

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

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

**Enable Auto Channel Scan:** The **Auto Channel Scan** setting can be selected to allow the DIR-655 to choose the channel with the least amount of interference.

**Wireless Channel:** Indicates the channel setting for the DIR-655. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

**802.11 Mode:** Select one of the following:

**802.11g Only** - Select if all of your wireless clients are 802.11g.

**Mixed 802.11g and 802.11b** - Select if you are using both 802.11b and 802.11g wireless clients.

**802.11b Only** - Select if all of your wireless clients are 802.11b.

**802.11n Only** - Select only if all of your wireless clients are 802.11n.

**Mixed 802.11n, 802.11b, and 802.11g** - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

**Channel Width:**

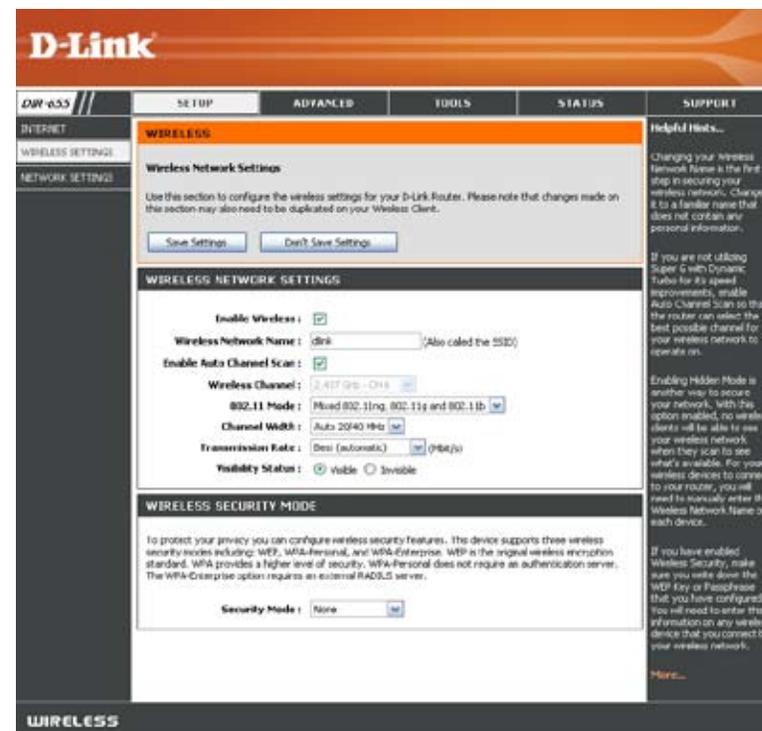
Select the Channel Width:

**Auto 20/40** - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.

**20MHz** - Select if you are not using any 802.11n wireless clients.

**Transmission Rate:**

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



**Visibility Status:**

Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-655. If Invisible is selected, the SSID of the DIR-655 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-655 in order to connect to it.

**Wireless Security:**

Refer to page 60 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.

**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 displays the D-Link DIR-655 web interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'NETWORK SETTINGS' section is highlighted in orange. It contains instructions for configuring internal network settings and a 'Save Settings' button. Below this is the 'ROUTER SETTINGS' section, which includes fields for 'Router IP Address' (192.168.0.1), 'Subnet Mask' (255.255.255.0), 'Local Domain Name' (optional), and a checked 'Enable DNS Relay' checkbox. The 'DHCP SERVER SETTINGS' section includes a checked 'Enable DHCP Server' checkbox, 'DHCP IP Address Range' (192.168.0.100 to 192.168.0.199), 'DHCP Lease Time' (1440 minutes), and a checked 'Always broadcast' checkbox. The 'ADD DHCP RESERVATION' section has a checked 'Enable' checkbox, fields for 'Computer Name', 'IP Address' (0.0.0.0), and 'MAC Address' (00:00:00:00:00:00), and a 'Copy Your PC's MAC Address' button. Below this is a 'DHCP RESERVATIONS LIST' table with columns for 'Enable', 'Computer Name', 'MAC Address', and 'IP Address'. At the bottom, it shows 'NUMBER OF DYNAMIC DHCP CLIENTS : 1' and a table with columns for 'Computer Name', 'IP Address', 'MAC Address', and 'Expire Time', listing a client named 'prescott' with IP 192.168.0.156 and an expire time of 23 Hours 18 Minutes. The bottom of the page features a 'WIRELESS' banner.

## DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-655 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-655. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

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

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

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

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

**Add DHCP Reservation:** Refer to the next page for the DHCP Reservation function.

**DHCP SERVER SETTINGS**

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

**Enable DHCP Server :**

**DHCP IP Address Range :** 192.168.0.100 to 192.168.0.199

**DHCP Lease Time :** 1440 (minutes)

**Always broadcast :**  (compatibility for some DHCP Clients)

---

**ADD DHCP RESERVATION**

**Enable :**

**Computer Name :**  << Computer Name

**IP Address :** 0.0.0.0

**MAC Address :** 00:00:00:00:00:00

---

**DHCP RESERVATIONS LIST**

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

---

**NUMBER OF DYNAMIC DHCP CLIENTS : 1**

Computer Name	IP Address	MAC Address	Expire Time		
prescott	192.168.0.156	00:11:09:2a:94:11	23 Hours 18 Minutes	<a href="#">Revoke</a>	<a href="#">Reserve</a>

## 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 v

**IP Address :**

**MAC Address :**

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address		

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Computer Name	IP Address	MAC Address	Expire Time		
prescott	192.168.0.156	00:11:09:2a:94:11	23 Hours 18 Minutes	<a href="#">Revoke</a>	<a href="#">Reserve</a>

## Virtual Server

The DIR-655 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-655 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-655 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-655 redirects the external service request to the appropriate server within the LAN network.

The DIR-655 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](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 33.

**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.

**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.

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

**D-Link**

DIR-655

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

**Helpful Hints...**

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

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

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

Select a filter that restricts the Internet hosts that can access the 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 port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.

Example: 24,1009,3000-4000

**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.

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

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'PORT FORWARDING' section is active. Below the navigation bar, there is a 'PORT FORWARDING' section with a description: '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)'. There are 'Save Settings' and 'Don't Save Settings' buttons. Below this is the '24 -- PORT FORWARDING RULES' section, which contains a table with the following columns: Name, IP Address, Application Name, Computer Name, Ports to Open, and Schedule. The table lists several rules for TCP and UDP ports, each with a dropdown menu for Application Name and a dropdown menu for Computer Name. The 'Ports to Open' column shows TCP and UDP ports, and the 'Schedule' column shows 'Always' and 'Schedule' options. To the right of the table is a 'Helpful Hints...' section with additional instructions.

# 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-655. 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-655 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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

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

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

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

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

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

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**APPLICATION RULES**

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

Save Settings Don't Save Settings

24 -- APPLICATION RULES

	Name	Application	Port	Traffic Type	Schedule
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger	TCP	Always
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Firewall	TCP	Always
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger	TCP	Always
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Firewall	TCP	Always
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Trigger	TCP	Always
<input type="checkbox"/>	<input type="text"/>	<< Application Name	Firewall	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 StreamEngine:** This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

**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.

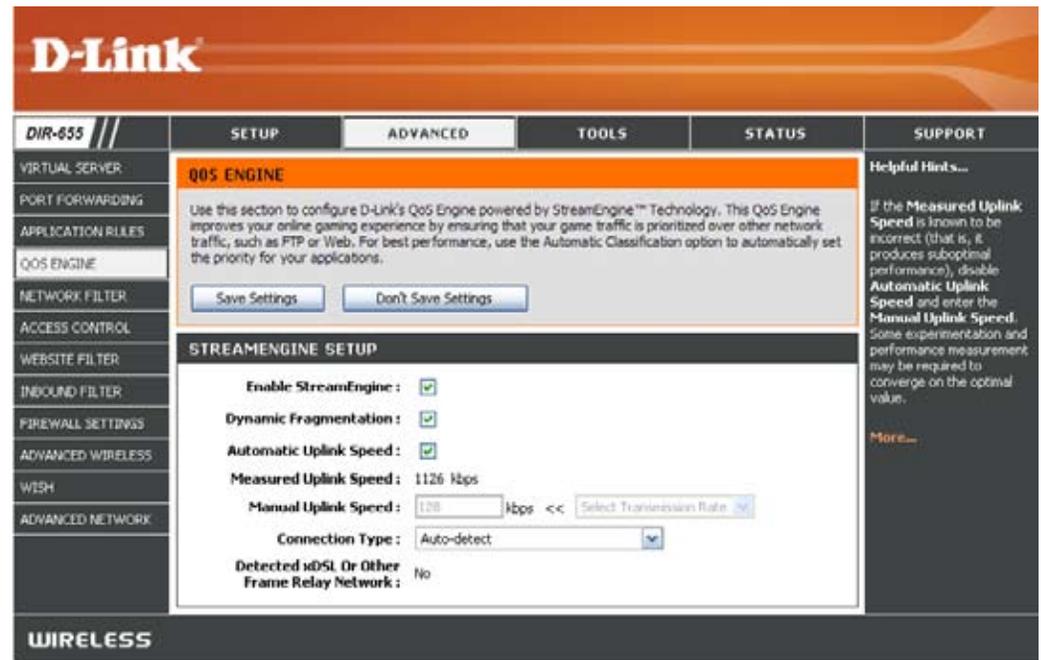
**Automatic Uplink Speed:** This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

**Measured Uplink Speed:** This displays the detected uplink speed.

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



## 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.

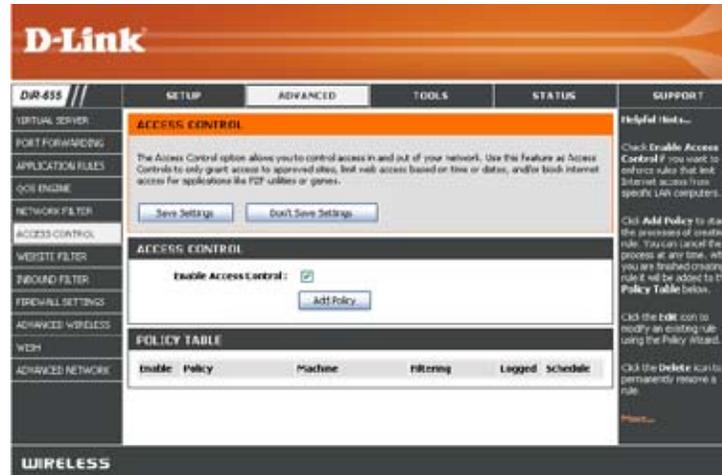
**DHCP Client:** Select a DHCP client from the drop-down menu and click << to copy that MAC Address.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'NETWORK FILTER' selected. The main content area is titled 'MAC ADDRESS FILTER' and contains the following text: 'The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.' Below this text are 'Save Settings' and 'Don't Save Settings' buttons. The section '24 -- MAC FILTERING RULES' is expanded, showing 'Configure MAC Filtering below:' with a dropdown menu set to 'Turn MAC Filtering OFF'. Below this is a table with two columns: 'MAC Address' and 'DHCP Client List'. The table contains five rows, each with an empty input field for the MAC address, a '<<' button, a 'Computer Name' dropdown menu, and a 'Clear' button. On the right side, there is a 'Helpful Hints...' section with instructions on how to create a list of MAC addresses and how to use the 'Clear' button to remove entries from the list.

# Access Control

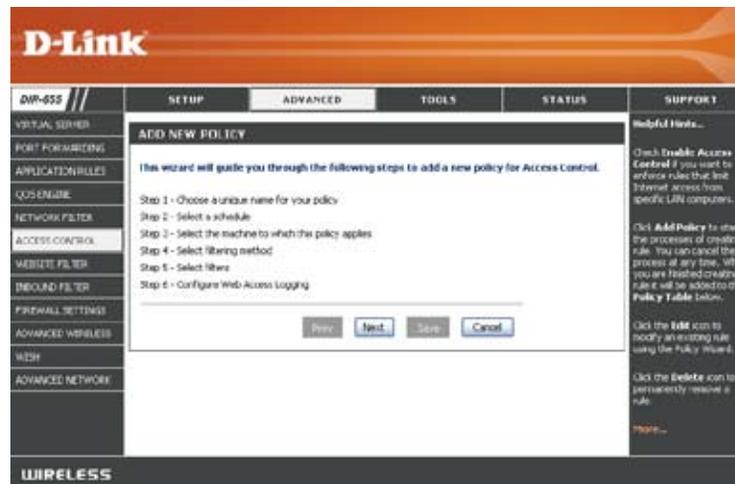
The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

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



## Access Control Wizard

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



## Access Control Wizard (continued)

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

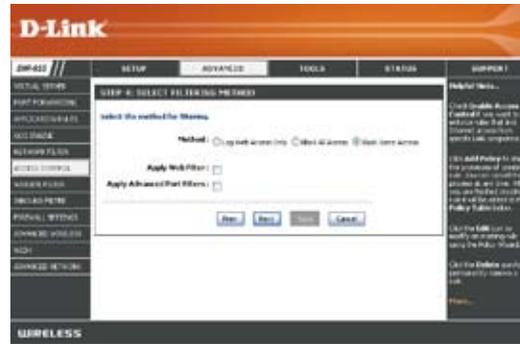
Select a schedule (I.E. Always) from the drop-down menu and then click **Next** to continue.

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.

## Access Control Wizard (continued)

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



Enter the rule:

Enable - Check to enable the rule.

Name - Enter a name for your rule.

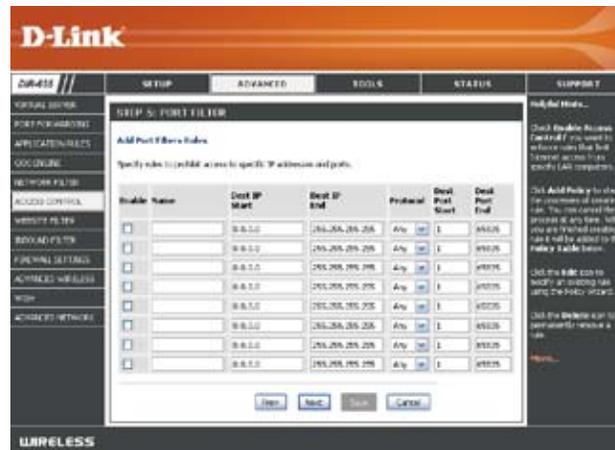
Dest IP Start - Enter the starting IP address.

Dest IP End - Enter the ending IP address.

Protocol - Select the protocol.

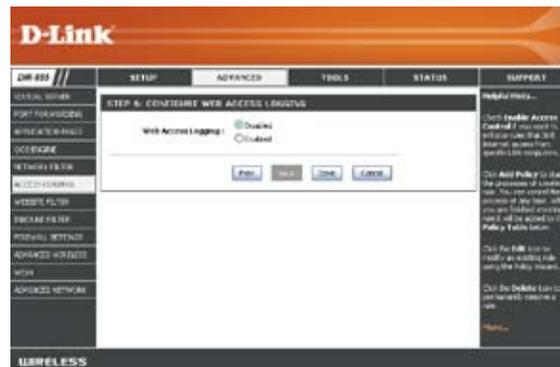
Dest Port Start - Enter the starting port number.

Dest Port End - Enter the ending port number.



To enable web logging, click Enable.

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



## Website Filters

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

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

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'WEBSITE FILTER' sub-tab is active. The main content area is titled 'WEBSITE FILTER' and contains the following text: 'The Web Filter option allows you to set up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. Underneath is a section titled '40 -- WEBSITE FILTERING RULES' with a 'Clear the list below...' button. Below this is a table with two columns, both labeled 'Website URL/Domain'. The table has four empty rows for input. On the right side of the interface, there is a 'Helpful Hints...' section with text: 'Create a list of Web sites to which you would like to allow access from the devices on your network. Use with 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.

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

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

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

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

**D-Link**

DIR-655

SETUP | **ADVANCED** | TOOLS | STATUS | SUPPORT

**INBOUND FILTER**

**Inbound Filter Rules**

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.

Save Settings | Don't Save Settings

**ADD INBOUND FILTER RULE**

Name:

Action: **Deny**

Source IP Range	Enable	Source IP Start	Source 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

Save | Clear

**INBOUND FILTER RULES LIST**

Name	Action	Source IP Range

**WIRELESS**

**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 **Save** 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-655 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

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

**NAT Endpoint Filtering:** Select one of the following for TCP and UDP ports:  
**Endpoint Independent** - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

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

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

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

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

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

The screenshot shows the D-Link DIR-655 Firewall Settings page. The page is titled "D-Link" and has a navigation menu with "SETUP", "ADVANCED", "TOOLS", "STATUS", and "SUPPORT". The "FIREWALL SETTINGS" section is active, showing the following options:

- 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
- DMZ HOST:**
  - Enable DMZ:**
  - DMZ IP Address:** 0.0.0.0 (Computer Name)
- NON-UDP/TCP/ICMP LAN SESSIONS:**
  - Enable:**
- APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION:**
  - PPTP:**
  - IPsec (VPN):**
  - RTSP:**
  - Wireless/MIN Messenger:**  (automatically disabled if UPnP is enabled)
  - FTP:**
  - H.323 (NetMeeting):**
  - SIP:**
  - Wake-On-LAN:**
  - PPS:**

## 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.

**MSN Messenger:** Allows all of the Windows/MSN Messenger functions to work properly through the router.

**FTP:** Allows FTP clients and servers to transfer data across NAT. Refer to the *Advanced > Virtual Server* page if you want to host an FTP server.

**H.323 (Netmeeting):** Allows Microsoft NetMeeting clients to communicate across NAT. Note that if you want your buddies to call you, you should also set up a virtual server for NetMeeting. Refer to the *Advanced > Virtual Server* page for information on how to set up a virtual server.

**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.

**Wake-On-LAN:** Allows Ethernet network adapters with Wake-On-LAN (WOL) to function.

**MMS:** Allows Windows Media Player, using MMS protocol, to receive streaming media from the Internet.

## 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.

**802.11d:** This enables 802.11d operation. 802.11d is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it.

**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.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is active, and the 'ADVANCED WIRELESS' sub-tab is selected. The main content area displays the following settings:

- Transmit Power: High
- Beacon Period: 100 (range: 20..1000)
- RTS Threshold: 2346 (range: 1..65535)
- Fragmentation Threshold: 2346 (range: 256..65535)
- DTIM Interval: 1 (range: 1..255)
- 802.11d Enable:
- WMM Enable:
- Short GI:

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

It is recommended that you leave these parameters at their default values. Adjusting them could limit the performance of your wireless network.

Use 802.11d only for countries where it is required.

Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

More...

# 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

The screenshot shows the D-Link DIR-655 router's configuration interface. The 'ADVANCED' tab is selected, and the 'WISH' settings are displayed. The 'Enable WISH' checkbox is checked. Under 'PRIORITY CLASSIFIERS', 'HTTP', 'Windows Media Center', and 'Automatic' are all checked. The 'Automatic' option has a note '(default if not matched by anything else)'. Below, there are two sections for 'WISH RULES', each with a checkbox and fields for Name, Priority (Best Effort (BE)), Protocol (TCP), Host 1 IP Range (0.0.0.0 to 255.255.255.255), and Host 1 Port Range (0 to 65535).

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

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

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

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

**BK:** Background (least urgent)

**BE:** Best Effort.

**VI:** Video

**VO:** Voice (most urgent)

Name	Priority	Protocol	Host 1 IP Range	Host 1 Port Range	Host 2 IP Range	Host 2 Port Range
	Best Effort (BE)	6 << TCP	0.0.0.0 to 255.255.255.255	0 to 65535	0.0.0.0 to 255.255.255.255	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.

# Advanced Network Settings

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

**Internet Ping:** Unchecking the box will not allow the DIR-655 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be “pinged”.

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

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

The screenshot displays the D-Link DIR-655 Advanced Network Settings interface. The main content area is titled 'ADVANCED NETWORK' and contains several sections:

- UPNP:** A section titled 'Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.' It features a checkbox for 'Enable UPnP' which is checked.
- WAN PING:** A section titled '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 includes a checkbox for 'Enable WAN Ping Respond' (unchecked), a dropdown menu for 'WAN Ping Inbound Filter' set to 'Allow All', and a text field for 'Details' containing 'Everyone allowed'.
- WAN PORT SPEED:** A section with a dropdown menu for 'WAN Port Speed' set to 'Auto 10/100Mbps'.
- MULTICAST STREAMS:** A section with a checkbox for 'Enable Multicast Streams' which is checked.

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

UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.

For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

The WAN speed is usually detected automatically. If you are having problems connecting to the WAN, try selecting the speed manually.

If you are having trouble receiving multicast streams from the Internet, make sure the Multicast Streams option is enabled.

More...

# Administrator Settings

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

**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-655 router.

**Remote Management:** Remote management allows the DIR-655 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-655. Example: <http://x.x.x.x:8080> whereas x.x.x.x is the Internet IP address of the DIR-655 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.

The screenshot shows the D-Link DIR-655 web management interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains the following sections:

- ADMINISTRATOR SETTINGS:** A text box explaining that the 'admin' and 'user' accounts can access the management interface. Below this are 'Save Settings' and 'Don't Save Settings' buttons.
- ADMIN PASSWORD:** A section with the instruction 'Please enter the same password into both boxes, for confirmation.' It contains two input fields for 'Password' and 'Verify Password'.
- USER PASSWORD:** A section with the instruction 'Please enter the same password into both boxes, for confirmation.' It contains two input fields for 'Password' and 'Verify Password'.
- SYSTEM NAME:** A section with a 'Gateway Name' field containing the text 'D-Link DIR-655'.
- ADMINISTRATION:** A section with an 'Enable Remote Management' checkbox (checked), a 'Remote Admin Port' field containing '8080', and a 'Remote Admin Inbound Filter' dropdown menu set to 'Allow All'. Below these is a 'Details' field containing 'Everyone allowed'.

On the right side of the interface, there is a 'Helpful Hints...' section with several paragraphs of text providing additional information and instructions.

# 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-655 web interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'TIME' section is selected in the left sidebar. The main content area is titled 'TIME CONFIGURATION' and contains the following elements:

- Time Configuration:** A section with a description: "The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed." Below this are 'Save Settings' and 'Don't Save Settings' buttons.
- TIME CONFIGURATION:** A section with the following fields:
  - 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: A table with columns for DST Start, DST End, Month, Week, Day of Week, and Time.
 

DST Start	DST End	Month	Week	Day of Week	Time
Apr	Oct	1st	Sun	2 am	2 am
- AUTOMATIC TIME CONFIGURATION:** A section with:
  - Enable NTP Server:
  - NTP Server Used: << Select NTP Server
- SET THE DATE AND TIME MANUALLY:** A section with:
  - Date And Time: Year (2004), Month (Jan), Day (31), Hour (2), Minute (50), Second (45), PM
  - Copy Your Computer's Time Settings button

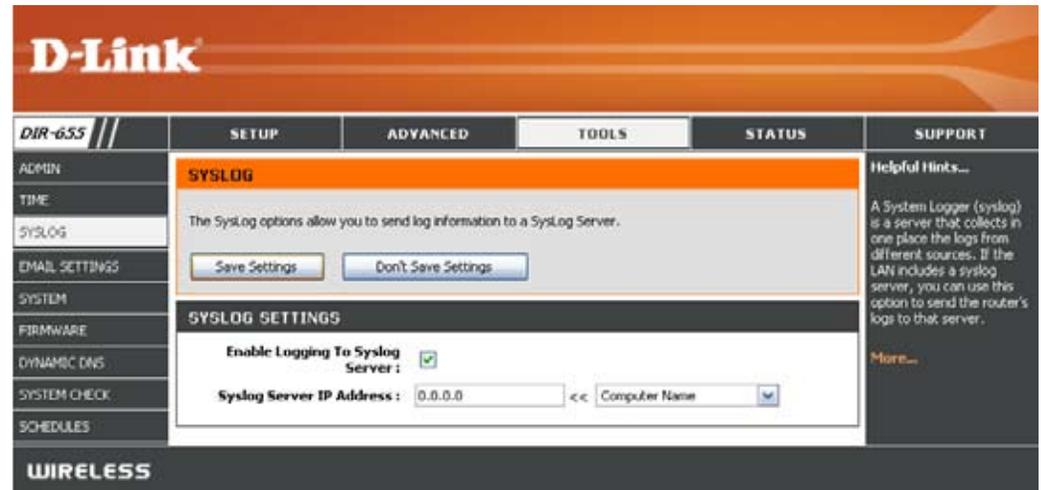
The bottom of the page features a 'WIRELESS' logo.

# 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 e-mailed to a designated email address.

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

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

**SMTP Server Address:** 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**.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS (selected), SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'EMAIL SETTINGS' and contains the following sections:

- Email Settings:** A text box explaining the feature and two buttons: 'Save Settings' and 'Don't Save Settings'.
- ENABLE:** A section with a checked checkbox for 'Enable Email Notification'.
- EMAIL SETTINGS:** A form with the following fields:
  - From Email Address: [text input]
  - To Email Address: [text input]
  - SMTP Server Address: [text input]
  - Enable Authentication:
  - Account Name: [text input]
  - Password: [text input]
  - Verify Password: [text input]
- EMAIL LOG WHEN FULL OR ON SCHEDULE:** A section with:
  - On Log Full:
  - On Schedule:
  - Schedule: [dropdown menu showing 'Never']
  - Details: [text input showing 'Never']

The bottom of the page features a 'WIRELESS' section.

# System Settings

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

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

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

**Reboot Device:** Click to reboot the router.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSTEM SETTINGS' and contains the following text and buttons:

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:**

The right sidebar contains a 'Helpful Hints...' section with the following text: '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.' Below this is a 'More...' link.

# Update Firmware

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

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

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

**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 displays the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various settings categories: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'FIRMWARE' and contains the following sections:

- Firmware Upgrade:** A section with a description: 'The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance.' It includes a 'Check Online Now for Latest Firmware Version' button and an 'Email Notification of Newer Firmware Version' checkbox.
- FIRMWARE INFORMATION:** Displays 'Current Firmware Version: 1.0', 'Latest Firmware Version: 1.0', and 'Current Firmware Date: 2006/03/22'. It features a 'Check Online Now for Latest Firmware Version' button.
- FIRMWARE UPGRADE:** Contains a note: 'Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools -> Admin screen.' It also states: 'To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.' This section includes an 'Upload:' text box, a 'Browse...' button, and an 'Upload' button.
- FIRMWARE UPGRADE NOTIFICATION OPTIONS:** Contains two checkboxes: 'Automatically Check Online for Latest Firmware Version' (checked) and 'Email Notification of Newer Firmware Version' (unchecked).

The bottom of the interface shows the 'WIRELESS' section.

# DDNS

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

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

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

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

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

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

**Timeout:** Enter a time (in hours).

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'DYNAMIC DNS' and contains the following text: 'Dynamic DNS (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 your host name to connect to your game server no matter what your IP address is.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'DYNAMIC DNS' section is expanded to show the following configuration options: 'Enable Dynamic DNS' (checked), 'Server Address' (dropdown menu showing 'www.DynDNS.org (Free)'), 'Host Name' (text input field with a hint '(e.g.: myhost.mydomain.net)'), 'Username or Key' (text input field), 'Password or Key' (text input field), 'Verify Password or Key' (text input field), and 'Timeout' (text input field with '(hours)' next to it). The bottom of the page features a 'WIRELESS' banner.

# System Check

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

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



# Schedules

**Name:** Enter a name for your new schedule.

**Days:** Select a day, a range of days, or All Week to include every day.

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

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

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

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration categories: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES (which is highlighted). The main content area is titled 'SCHEDULES' and contains the following sections:

- SCHEDULES:** A section with a description: "The Schedule configuration option is used to manage schedule rules for various firewall and parental control features." Below this are two buttons: "Save Settings" and "Don't Save Settings".
- ADD SCHEDULE RULE:** A form for creating a new schedule rule. It includes:
  - 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:** Two input fields for hours and minutes, followed by a dropdown for AM/PM. A note "(hour:minute, 12 hour time)" is present.
  - End Time:** Two input fields for hours and minutes, followed by a dropdown for AM/PM. A note "(hour:minute, 12 hour time)" is present.
  - Buttons for "Save" and "Clear".
- SCHEDULE RULES LIST:** A table with columns for "Name", "Day(s)", and "Time Frame". The table is currently empty.

The right sidebar, titled "Helpful Hints...", provides additional information:
 

- 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-655. 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** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

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

**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).

**IGMP Multicast Memberships:** Displays the Multicast Group IP Address.

The screenshot displays the D-Link DIR-655 web interface. The top navigation bar includes tabs for DEVICE INFO, SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The main content area is titled "DEVICE INFORMATION" and contains the following sections:

- GENERAL:** Shows the time as Saturday, January 31, 2004 18:56:42 AM and the firmware version as 0.99 (DIR655).
- WAN:** Shows connection type as DHCP Client, status as Connected, network status as Enabled, and connection type as Dynamic IP. It includes a "DHCP Release" button. IP settings include MAC Address: 00:00:00:00:00:00, IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1, Primary DNS Server: 192.168.1.1, and Secondary DNS Server: 0.0.0.0.
- LAN:** Shows MAC Address: 00:00:00:00:00:00, IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, and DHCP Server: Enabled.
- WIRELESS LAN:** Shows Wireless Radio: On, MAC Address: 00:00:00:00:00:00, Network Name (SSID): link, Channel: 11, and Security Type: None.
- LAN COMPUTERS:** A table showing connected devices:
 

IP Address	Name (if any)	MAC
192.168.1.10	link	00:00:00:00:00:00
- IGMP MULTICAST MEMBERSHIPS:** Shows Multicast Group Address: 229.255.255.255 and 224.0.0.0.

# Log

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 displayed in the log.

**Apply Log Settings:** Will filter the log results so that only the selected options 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.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar contains 'DEVICE INFO', 'LOGS', 'STATISTICS', 'INTERNET SESSIONS', 'WIRELESS', and 'WIRELESS SESSIONS'. The main content area is titled 'LOGS' and contains the following sections:

- System Logs:** A description stating: "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:** A section with two groups of checkboxes:
  - What to View:**  Firewall & Security,  System,  Router Status
  - View Levels:**  Critical,  Warning,  Informational
 Below these is an 'Apply Log Settings Now' button.
- LOG DETAILS:** A section with buttons for 'Refresh', 'Clear', 'Email Now', and 'Save Log'. Below the buttons is a list of log entries:
  - [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

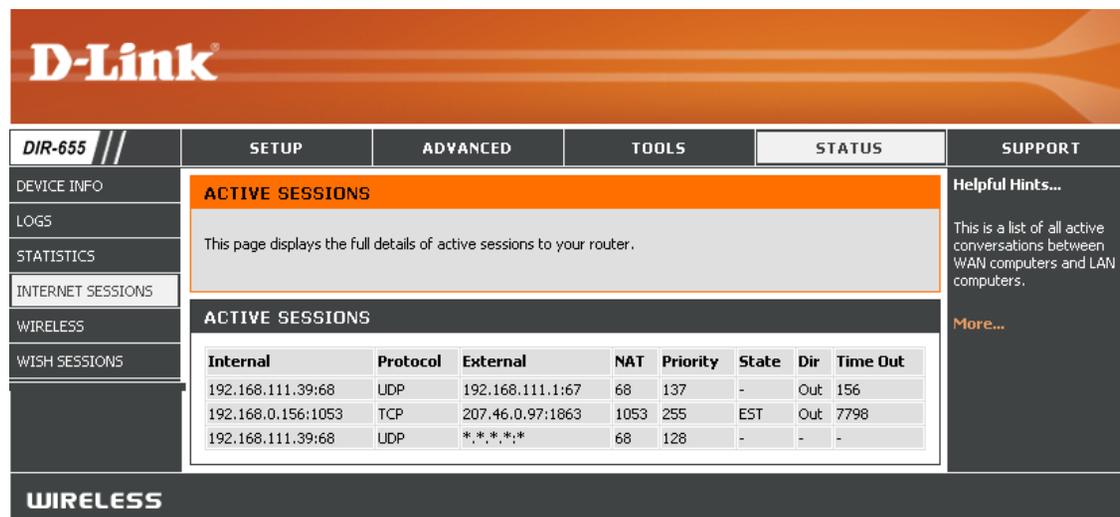
The right sidebar contains 'Helpful Hints...' with text: "Check the log frequently to detect unauthorized network usage. You can also have the log mailed to you periodically. Refer to Tools -> Email. More..."

# Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-655 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.



# Active Sessions



# 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-655 web interface. The 'WIRELESS' tab is selected in the left sidebar. The main content area displays the 'Associated Wireless Client List' with a table of one connected client. The table has columns for MAC Address, IP Address, Mode, Rate, and Signal(%).

MAC Address	IP Address	Mode	Rate	Signal(%)
00:03:2F:11:23:20	192.168.0.127	11g	54	100

Below the table, it indicates 'NUMBER OF WIRELESS CLIENTS : 1'. The right sidebar contains 'Helpful Hints...' and a 'More...' link.

# WISH

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

The screenshot shows the D-Link DIR-655 web interface with the 'WISH SESSIONS' tab selected. The main content area displays a description of WISH sessions and a table with columns for Originator, Target, Protocol, State, Priority, and Time Out.

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

The right sidebar contains 'Helpful Hints...' and a 'More...' link.

# Support

The screenshot shows the D-Link DIR-655 web interface. At the top is the D-Link logo. Below it is a navigation bar with tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The SUPPORT tab is active. On the left is a vertical menu with options: MENU, SETUP, ADVANCED, TOOLS, STATUS, and GLOSSARY. The main content area is titled 'SUPPORT MENU' and contains several sections:

- SUPPORT MENU**
  - Setup
  - Advanced
  - Tools
  - Status
  - Glossary
- SETUP HELP**
  - Internet Connection
  - WAN
  - Wireless
  - Network Settings
- ADVANCED HELP**
  - Virtual Server
  - Port Forwarding
  - Application Rules
  - QoS ENGINE
  - Routing
  - Access Control
  - Web Filter
  - MAC Address Filter
  - Firewall
  - Inbound Filter
  - Advanced Wireless
- TOOLS HELP**
  - Admin
  - Time
  - Sniffing
  - Email Settings
  - System
  - Firmware
  - Dynamic DNS
  - Windows Connect Now
  - System Check
  - Schedules
  - Sentinel Services
- STATUS HELP**
  - Device Info
  - Wireless
  - Routing
  - Logs
  - Statistics
  - Active Sessions

At the bottom of the page, there is a 'WIRELESS' section header.

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-655 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

## What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

# What is WPA?

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

The 2 major improvements over WEP:

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

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

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

# Wireless Security Setup Wizard

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



Click **Next** to continue.



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

**STEP 1: NAME YOUR WIRELESS NETWORK**

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name of [dlink].

Wireless Network Name (SSID):

Select the level of security for your wireless network:

- Best - WPA2 Authentication
- Better - WPA Authentication
- Good - WEP Encryption
- None - No security

Click **Next** to continue.

**STEP 2: SECURE YOUR WIRELESS NETWORK**

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are three levels of wireless security -Good Security, Better Security, AND Best Security. The level you choose depends on the security features your wireless adapters support.

**BEST**  Select this option if your wireless adapters SUPPORT WPA2

**BETTER**  Select this option if your wireless adapters SUPPORT WPA

**GOOD**  Select this option if your wireless adapters DO NOT SUPPORT WPA

**NONE**  Select this option if you do not want to activate any security features

For information on which security features your wireless adapters support, please refer to the adapters' documentation.

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

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

If you selected Good, enter 13 characters or 26 Hex digits.

Click **Next** to continue.

**STEP 3: SET YOUR WIRELESS SECURITY PASSWORD**

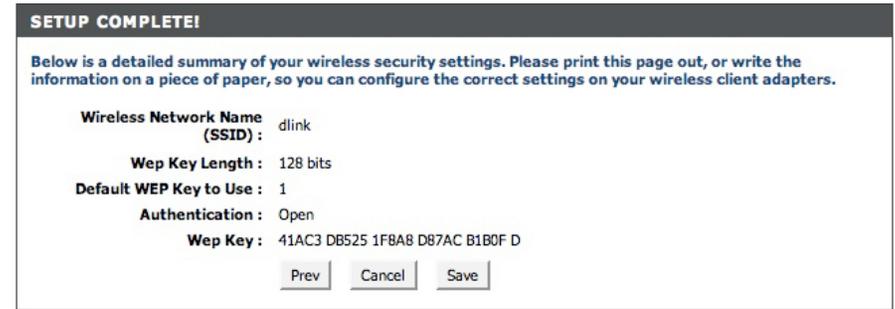
You have selected your security level - you will need to set a wireless security password.

Wireless Security Password:   
(8 to 63 characters)

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

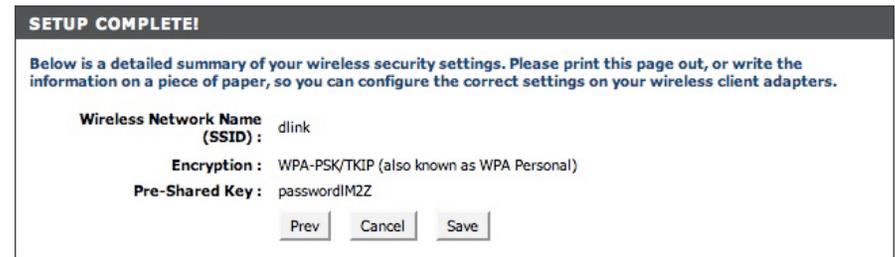
If you selected Good, the following screen will show you your WEP key to enter on your wireless clients.

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



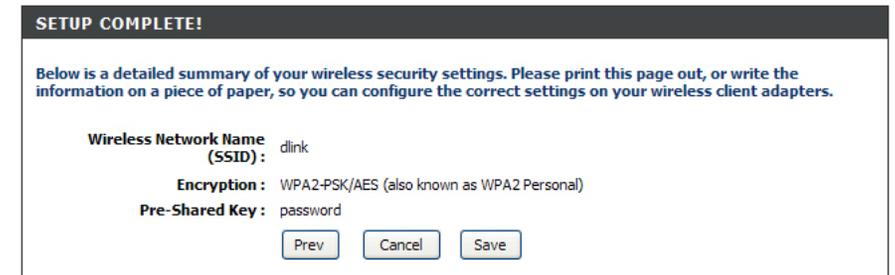
If you selected Better, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

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



If you selected Best, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

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



If you selected WPA-Enterprise, the RADIUS information will be displayed. Click **Save** to finish the Security Wizard.

# Configure WEP

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WEP**.
3. Next to *WEP Key Length*, select the level of encryption (64 or 128-bit).  
**Hex** - (recommended) Letters A-F and numbers 0-9 are valid.
4. Next to *WEP Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.
5. Next to *Authentication*, select **Shared Key**.
6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.

**WIRELESS SECURITY MODE**

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

Security Mode :

---

**WEP**

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

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

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

WEP Key Length :  (length applies to all keys)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Default WEP Key :

Authentication :

# Configure WPA-Personal (PSK)

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

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

**WIRELESS SECURITY MODE**

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

Security Mode :

---

**WPA**

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

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

WPA Mode :

Group Key Update Interval :  (seconds)

---

**PRE-SHARED KEY**

Pre-Shared Key :

# Configure WPA-Enterprise (RADIUS)

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WPA-Enterprise**.
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
5. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).
6. Next to *RADIUS Server IP Address* enter the IP Address of your RADIUS server.
7. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
8. Next to *RADIUS Server Shared Secret*, enter the security key.

**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:

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. 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.
10. Click **Advanced** to enter settings for a secondary RADIUS Server.
11. 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® XP

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

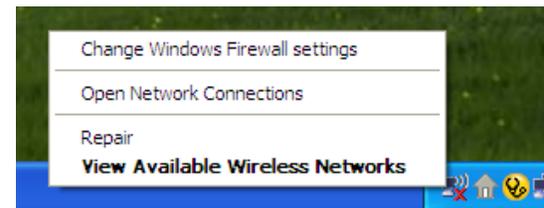
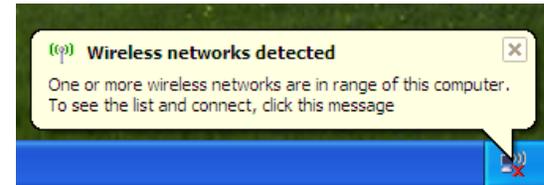
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

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



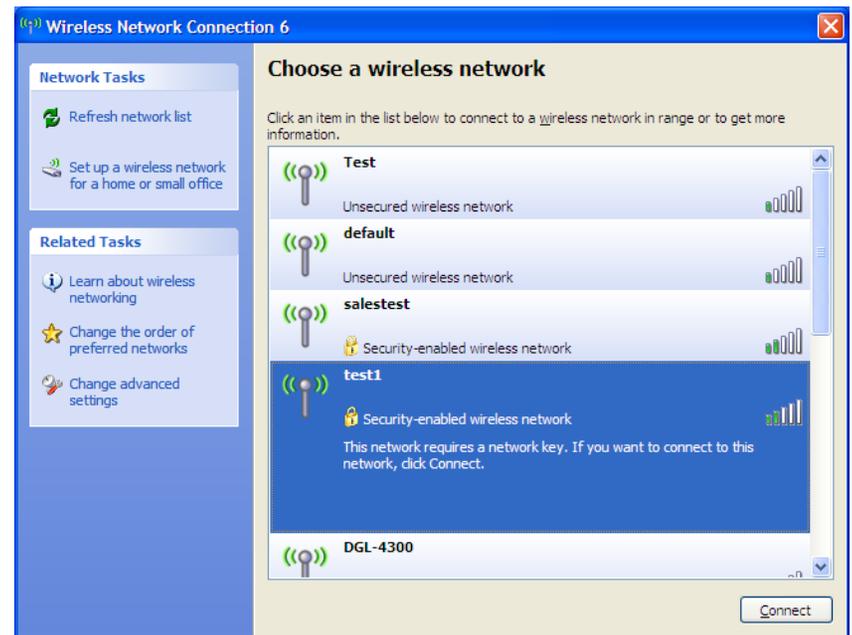
# Configure WEP

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

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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



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

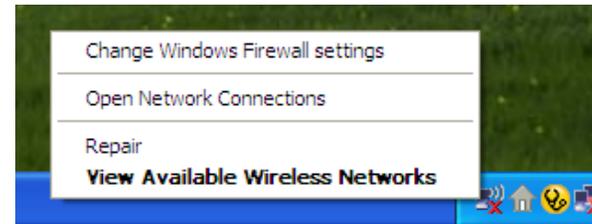
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



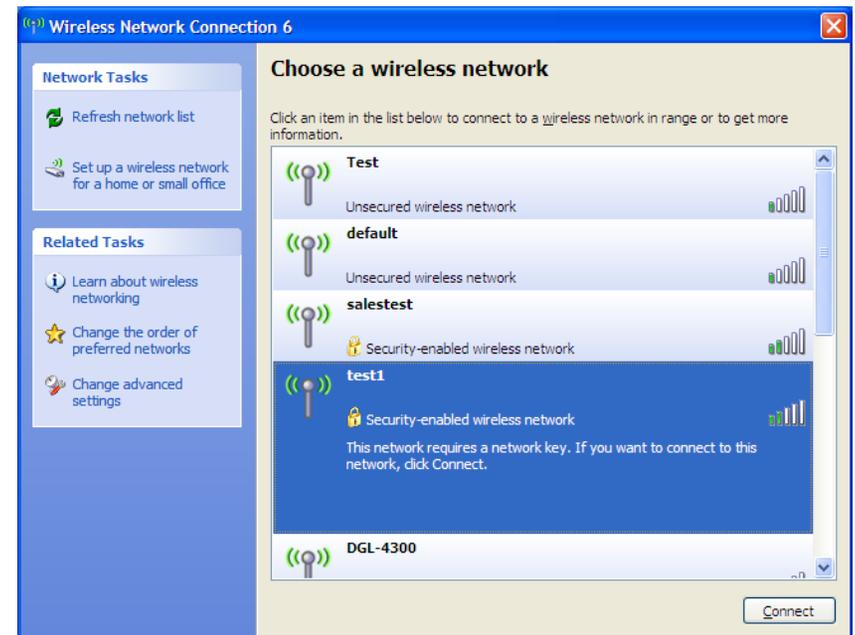
# Configure WPA-PSK

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

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.

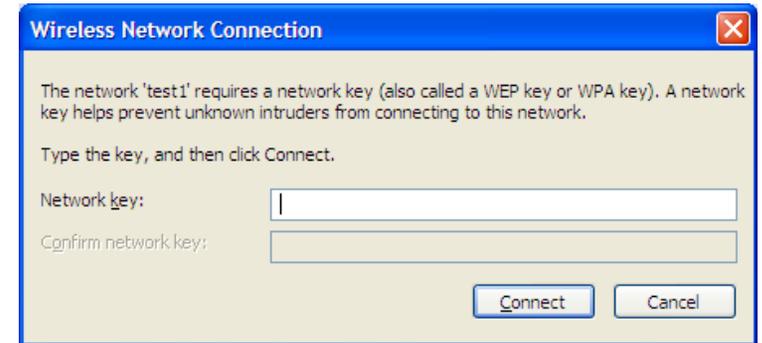


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-655. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C:\>
```

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

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

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

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

# Wireless Basics

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

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

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

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

## **What is Wireless?**

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

## **Why D-Link Wireless?**

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

## **How does wireless work?**

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

### **Wireless Local Area Network (WLAN)**

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

## **Wireless Personal Area Network (WPAN)**

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

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

## **Who uses wireless?**

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

### **Home**

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

### **Small Office and Home Office**

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

## **Where is wireless used?**

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

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

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

## **Tips**

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

### **Centralize your router or Access Point**

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

### **Eliminate Interference**

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

## Security

Don't let your next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

# Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-655 wireless network Cardbus adapters.

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

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

# Networking Basics

## Check your IP address

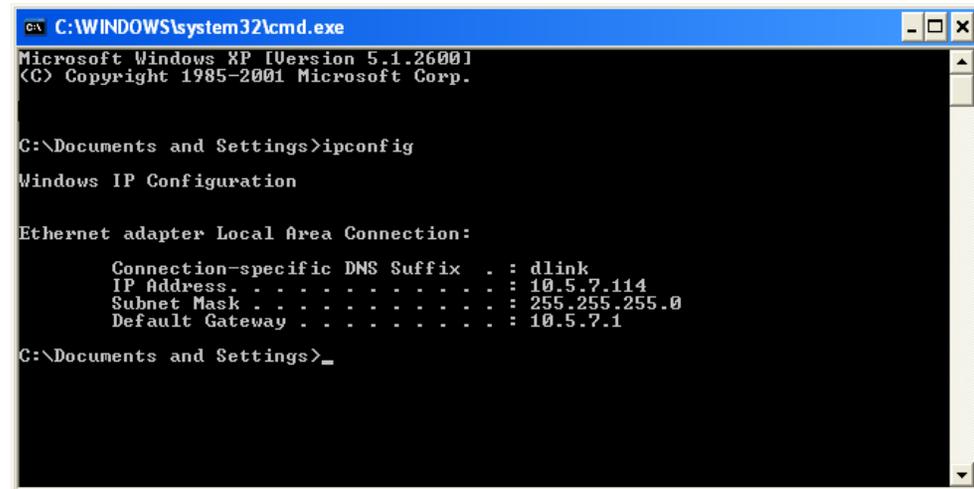
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

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

## Statically Assign an IP address

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

### Step 1

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

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

### Step 2

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

### Step 3

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

### Step 4

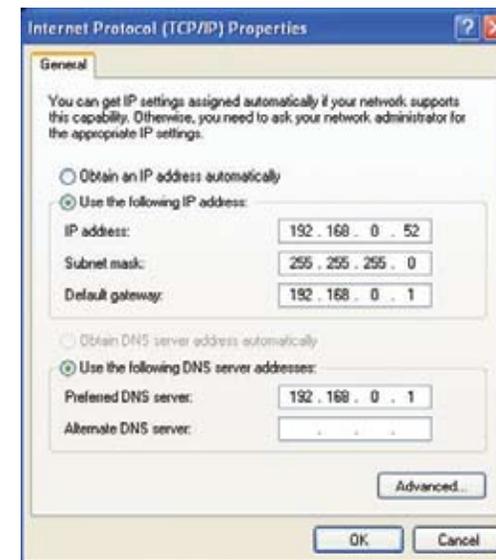
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

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

### Step 5

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



# Technical Specifications

## Standards

- IEEE 802.11n (draft)
- 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\*

- 108Mbps
- 54Mbps
- 36Mbps
- 18Mbps
- 11Mbps
- 6Mbps
- 2Mbps
- 48Mbps
- 24Mbps
- 12Mbps
- 9Mbps
- 5.5Mbps
- 1Mbps

## MSC (0-15)

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

## Frequency Range

2.4GHz to 2.483GHz

## Transmitter Output Power

15dBm  $\pm$  2dB

## External Antenna Type

Three (3) detachable reverse SMA Antennas

## LEDs

- Power
- Internet
- Status
- WLAN
- LAN (10/100)
- USB

## Operating Temperature

32°F to 131°F ( 0°C to 55°C)

## Humidity

95% maximum (non-condensing)

## Safety & Emissions

- FCC
- CE

## Dimensions

- L = 7.6 inches
- W = 4.6 inches
- H = 1.2inches

\* 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.