



# User Manual

## 4G LTE Router

DWR-922

---

# Preface

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

## Manual Revisions

Revision	Date	Description
1.00	January 23, 2017	• Initial release

## Trademarks

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

Copyright © 2017 by D-Link Corporation.

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

---

# Table of Contents

<b>Product Overview</b> .....	<b>1</b>	Dynamic IP Failover.....	26
Package Contents.....	1	PPPoE Failover.....	27
System Requirements.....	1	IPv6.....	28
Introduction.....	2	Link-local Only.....	28
Hardware Overview.....	3	Static IPv6.....	29
Front View.....	3	Autoconfiguration (SLAAC/DHCPv6).....	30
Back View.....	4	PPPoE.....	31
<b>Installation</b> .....	<b>5</b>	PPPoE.....	32
Before You Begin.....	5	Wi-Fi.....	33
Wireless Installation Considerations.....	6	Device List.....	33
<b>Configuration</b> .....	<b>7</b>	Wi-Fi Settings.....	33
Getting Started.....	7	WPS.....	35
Internet.....	8	Wi-Fi Advanced.....	37
WAN Service.....	8	LAN.....	39
Dynamic IP (DHCP).....	8	Device List.....	39
Static IP.....	10	LAN Settings.....	39
PPPoE (Username / Password).....	11	DHCP.....	40
PPTP.....	13	Advanced.....	41
L2TP.....	15	DNS.....	41
4G LTE / 3G.....	17	Applications.....	42
Wizard.....	19	DMZ.....	43
Multi-WAN.....	23	Virtual Server.....	44
Multi-WAN Configuration.....	24	URL Filter.....	45
4G LTE / 3G failover.....	24	Routing.....	46
Static IP Address Failover.....	25	QoS.....	47
		MAC Address Filter.....	48

Outbound Filter.....	49	<b>Troubleshooting .....</b>	<b>79</b>
Inbound Filter .....	50	<b>Wireless Basics .....</b>	<b>83</b>
SNMP .....	51	What is Wireless?.....	84
Advanced Network .....	52	Tips.....	86
Network Scan .....	53	Wireless Modes.....	87
System .....	54	<b>Networking Basics .....</b>	<b>88</b>
Time Settings .....	54	Check your IP address.....	88
Administration.....	55	Statically Assign an IP address .....	89
Reboot & Reset .....	56	Wireless Security .....	90
Firmware Upgrade.....	57	What is WPA? .....	90
System Logs.....	58	<b>Technical Specifications .....</b>	<b>91</b>
Schedules .....	59	<b>Regulatory Information .....</b>	<b>92</b>
Add New Rule.....	59		
Connection Reset .....	60		
<b>Connect a Wireless Client to your Router .....</b>	<b>61</b>		
WPS Button.....	61		
Windows® 10 .....	62		
Windows® 8.....	64		
WPA/WPA2 .....	64		
Windows® 7.....	66		
WPA/WPA2 .....	66		
WPS.....	69		
Windows Vista® .....	73		
WPA/WPA2 .....	74		
Windows® XP .....	76		
WPA/WPA2 .....	77		

# Package Contents



DWR-922 4G LTE Router with Presinstalled SIM/UICC



Power Adapter



3G/4G Antennas



RJ-45 Cable

If any of the above items are missing, please contact your reseller.

# System Requirements

- A compatible SIM/UICC card with service.\*
- Computer with Windows 10/8/7/Vista/XP, Mac OS 10.3 or above, or Linux-based operating system with a compatible network adapter.
- Java-enabled browser such as Internet Explorer 9, Safari 7, Chrome 28, or Firefox 23 or above (for configuration).

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

# Introduction

D-Link's DWR-922 4G LTE Router allows you to access mobile broadband networks from anywhere. Once connected, you can check e-mail, surf the web, and stream media. Use your carrier's SIM/UICC card to share your 3G/4G Internet connection through a secure wireless network or by using any of the four 10/100 Ethernet ports.

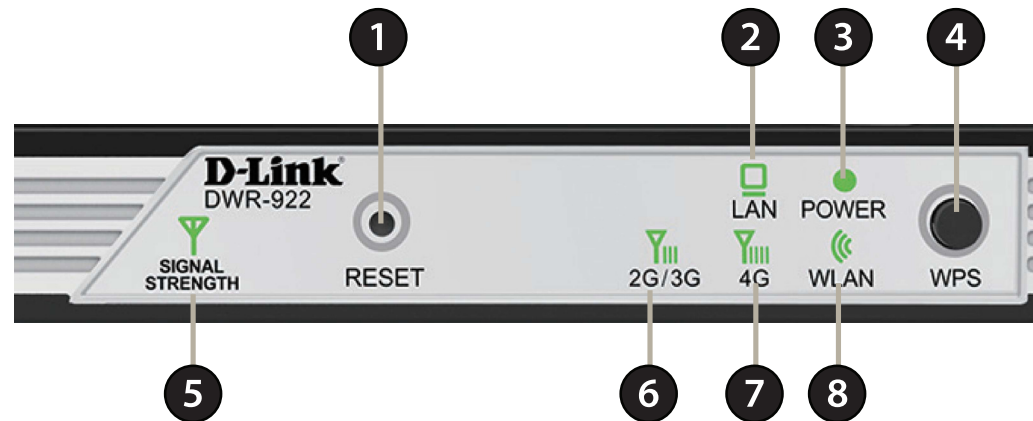
The DWR-922 lets you connect to your 3G/4G mobile connection with fast downlink speeds of up to 100 Mbps and uplink speeds up to 50 Mbps, giving you the speed to ensure fast, responsive Internet access. Surf the web with ease and stream music and video over the Internet to your PCs and mobile devices.

The DWR-922 utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks across the Internet. Industry standard WPA/WPA2 wireless encryption keeps your wireless network secure and your traffic safe, allowing you to share your 3G/4G connection without worrying about unauthorized users accessing your network.

The DWR-922 can be installed quickly and easily almost anywhere. It can be configured through almost any web browser without the need for special software. This router makes it possible to stay connected, even when conventional broadband services are unavailable.

# Hardware Overview

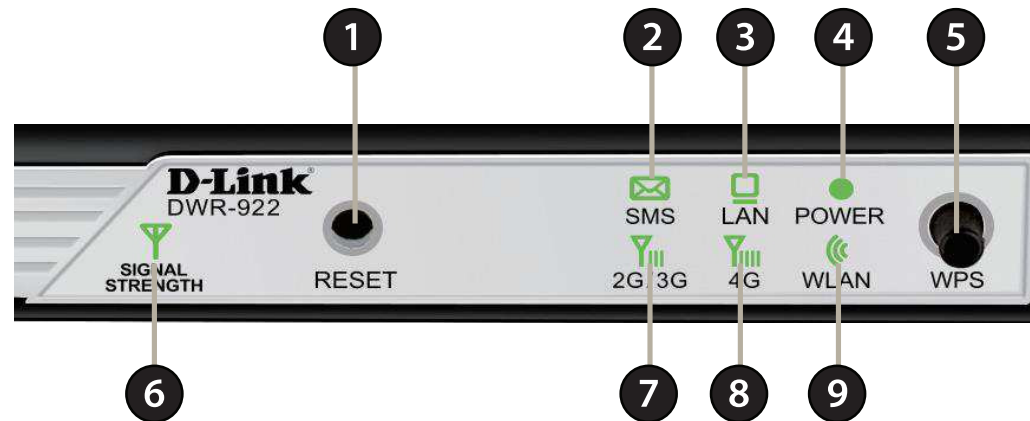
## Front View



1	<b>Reset Button</b>	Press this button with an unfolded paperclip and hold for ten seconds to reset the device.
2	<b>LAN LED</b>	Will be lit if an Ethernet connection is established, and will blink when data is being transferred.
3	<b>Power LED</b>	Will be lit if the device is powered on and working.
4	<b>WPS Button</b>	Press this button to initiate a new WPS connection. See <b>WPS Button</b> on page 61 for details.
5	<b>Signal Strength LED</b>	Will blink red if there is no SIM card or no signal. Solid red, amber, or green indicates the signal strength.
6	<b>2G/3G LED</b>	Will be lit if a 2G or 3G connection is established, and will blink when data is being transferred.
7	<b>4G LED</b>	Will be lit if a 4G LTE connection is established, and will blink when data is being transferred.
8	<b>WLAN LED</b>	Will be lit if the wireless function is enabled, and will blink when wireless data is being transferred.

# Hardware Overview

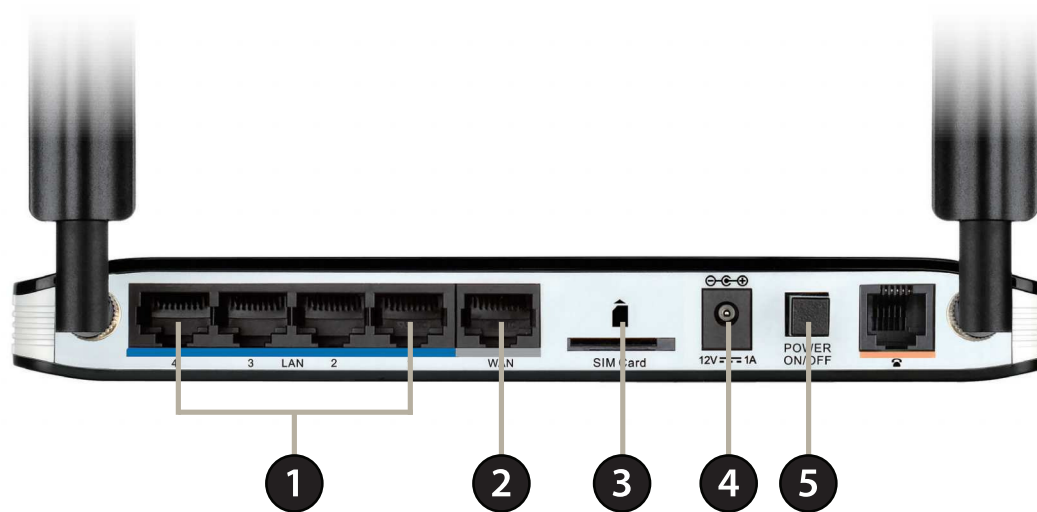
## Front View



<b>1</b>	<b>Reset Button</b>	Press this button with an unfolded paperclip and hold for ten seconds to reset the device.
<b>2</b>	<b>SMS LED</b>	Will be solid green if the SMS inbox is full, or blinking if there is an unread new SMS message.
<b>3</b>	<b>LAN LED</b>	Will be lit if an Ethernet connection is established, and will blink when data is being transferred.
<b>4</b>	<b>Power LED</b>	Will be lit if the device is powered on and working.
<b>5</b>	<b>WPS Button</b>	Press this button to initiate a new WPS connection. See <b>WPS Button</b> on page 62 for details.
<b>6</b>	<b>Signal Strength LED</b>	Will blink red if there is no SIM card / signal. Solid red/amber/green indicates the signal strength.
<b>7</b>	<b>2G/3G LED</b>	Will be lit if a 2G or 3G connection is established, and will blink when data is being transferred.
<b>8</b>	<b>4G LED</b>	Will be lit if a 4G LTE connection is established, and will blink when data is being transferred.
<b>9</b>	<b>WLAN LED</b>	Will be lit if the wireless function is enabled, and will blink when wireless data is being transferred.



## Back View



1	<b>Ethernet LAN Ports</b>	For connection to a network-enabled desktop or notebook computer.
2	<b>Ethernet WAN Port</b>	For connection to a DSL/cable modem or router.
3	<b>SIM Card Slot</b>	Accepts a standard (U)SIM card for 3G/4G LTE connectivity.
4	<b>Power Connector</b>	Connects to the included power adapter.
5	<b>Power Button</b>	Turns the device on or off.

# Installation

This section will guide 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 an attic or garage.

## Before You Begin

Ensure that your DWR-922 4G LTE Router is disconnected and powered off before performing the steps below..

1. Verify that your SIM/UICC card is installed and has been activated by your carrier.

**Caution:** Always unplug/power down the router before installing or removing the SIM/UICC card. Never insert or remove the SIM/UICC card while the router is in use.

2. Attach the included antennas to the back of the router, screwing them in clockwise. Arrange them so that they point upward.
3. Connect the power adapter to the socket on the back panel of your DWR-922. Plug the other end of the power adapter into a wall outlet or power strip. Make sure the power button is in the "On" position.
  - a. The Power LED will light up to indicate that power is being supplied to the router and the router is turned on.
  - b. The LEDs on the front panel will flash on and off as the DWR-922 Mobile Router performs initialization and Internet connection processes.
  - c. After a few moments, if a connection has been established, the following LEDs will turn solid green: Power, Signal Strength, WLAN, LAN (if connected), and either 2G/3G or 4G.

**Note:** By default, the DWR-922 uses the mobile network as the sole Internet connection. If you wish to use your mobile connection as a backup to a wired connection, or you wish to use a wired connection exclusively, you must use the Optional Advanced Setup procedure.

4. Connect via Wi-Fi using the SSID and password printed on the bottom of the router, or through Ethernet via one of the LAN ports on the back of your DWR-922.

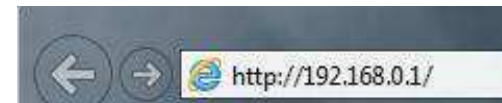
# Wireless Installation Considerations

The DWR-922 can be accessed using a wireless connection from anywhere within the operating range of your wireless network. Keep in mind that the quantity, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through may limit the range of the wireless signal. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

1. Minimize the number of walls and ceilings between the D-Link router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 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. Try to position access points, wireless routers, and computers so that the signal passes through open doorways and drywall. Materials such as glass, metal, brick, insulation, concrete, and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors, and aluminum studs may also have a negative effect on range.
4. If you are using 2.4 GHz cordless phones, make sure that the 2.4 GHz phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

# Configuration Getting Started

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



To log in to the configuration utility, **admin** is the default username and the default password is left blank.

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



Once you have successfully logged in, you will see the **Home** page. On this page you can view information about your Internet connection, the wireless/LAN status, and system information.

At the top of the page is a menu. Clicking on one of these icons will take you to the appropriate configuration section.



# Internet WAN Service

On this page you can configure your Internet connection. If you are not sure which settings to use, please contact your Internet Service Provider (ISP).

**My Internet Connection is:** Select the Internet connection type specified by your ISP. The corresponding settings will be displayed below. Please see the following sections for details on how to configure these different connection types.

## Dynamic IP (DHCP)

**Host Name:** If your ISP requires you to enter a host name, enter it here. In most cases, you may leave this blank.

**Primary DNS Server:** (Optional) Fill in with IP address of primary DNS server.

**Secondary DNS Server:** (Optional) Fill in with IP address of secondary DNS server.

**MTU:** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 0.

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

The screenshot shows the D-Link WAN Service Configuration page. The navigation bar includes Home, Internet, Wi-Fi, LAN, Advanced, and System. The main content area is titled 'WAN Service Configuration'. Under 'Internet Connection Type', 'Dynamic IP (DHCP)' is selected. The 'Dynamic IP (DHCP) Internet Connection Type' section contains the following fields and options:

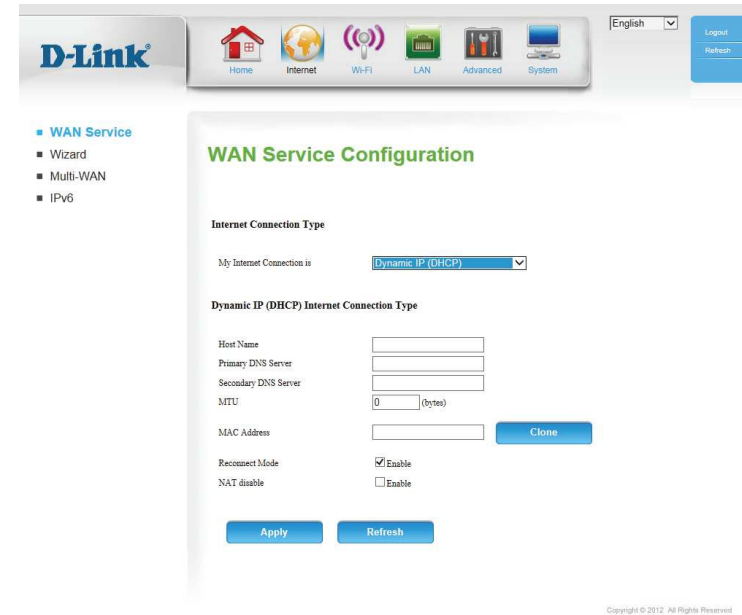
- Host Name: [Text input field]
- Primary DNS Server: [Text input field]
- Secondary DNS Server: [Text input field]
- MTU: [Text input field] (bytes)
- MAC Address: [Text input field] with a 'Clone' button
- Reconnect Mode:  Enable
- NAT disable:  Enable

'Apply' and 'Refresh' buttons are located at the bottom of the configuration area.

**Reconnect Mode:** This feature enables this product to renew the WAN IP address automatically when the lease time has expired.

**NAT disable:** Enabling this option will disable the NAT firewall function of the DWR-922, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



## Static IP

**IP Address:** Enter the IP address assigned to your network connection.

**Subnet Mask:** Enter the subnet mask.

**Default Gateway:** Enter the default gateway.

**Primary DNS Server:** Enter the primary DNS server.

**Secondary DNS Server:** Enter the secondary DNS server.

**MTU:** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 0.

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

**NAT disable:** Enabling this option will disable the NAT firewall function of the DWR-922, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for WAN Service Configuration. The 'Internet Connection Type' is set to 'Static IP'. The 'Static IP Address Internet Connection Type' section includes input fields for IP Address, Subnet Mask, Default Gateway, Primary DNS Server, and Secondary DNS Server. The MTU is set to 0 (bytes). The MAC Address field has a 'Clone' button next to it. The 'NAT disable' checkbox is unchecked. At the bottom, there are 'Apply' and 'Refresh' buttons.

## PPPoE (Username / Password)

**Username:** The username provided by your ISP for your PPPoE account.

**Password:** Password provided by your ISP for your PPPoE account.

**Verify Password:** Re-type your password in this field.

**Service Name:** Fill in if provided by your ISP. (Optional)

**IP Address:** Fill in if provided by your ISP. If not, keep the default value.

**Primary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).

**Secondary DNS Server:** Fill in if provided by your ISP. If not, keep the default value (optional).

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

**Maximum Idle Time:** The amount of time of inactivity before disconnecting an established PPPoE session. Set it to zero or enable auto-reconnect to disable this feature.

**MTU:** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 0.

**Reconnect Mode:** Choose **Always-on** when you want to establish PPTP connection all the time. If you choose **Connect-on-demand**, the device will establish a PPTP connection when local users want to connect to the Internet, and disconnect if there is no traffic after the time period defined by the **Maximum Idle Time** setting.

The screenshot shows the D-Link WAN Service Configuration page. The 'Internet Connection Type' is set to 'PPPoE (Username / Password)'. Under the 'PPPoE' section, there are input fields for Username, Password, Verify Password, Service Name (optional), IP Address, Primary DNS Server (optional), and Secondary DNS Server (optional). A 'Clone' button is next to the MAC Address field. The 'Reconnect Mode' is set to 'Always-on' (radio button selected), with options for 'Connect-on-demand' and 'Manual'. The 'Maximum Idle Time' is set to 300 seconds, and the 'MTU' is set to 0 bytes. There is a checkbox for 'NAT disable' which is currently unchecked. 'Apply' and 'Refresh' buttons are at the bottom.



**NAT disable:** Enabling this option will disable the NAT firewall function of the DWR-922, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for WAN Service Configuration. The top navigation bar includes the D-Link logo and icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. A language dropdown is set to English, and there are Login and Refresh buttons. On the left, a sidebar lists WAN Service options: Wizard, Multi-WAN, and IPv6. The main content area is titled 'WAN Service Configuration' and contains the following settings:

- Internet Connection Type:** My Internet Connection is set to PPPoE (Username / Password).
- PPPoE:**
  - Username: [text input]
  - Password: [text input]
  - Verify Password: [text input]
  - Service Name: [text input] (optional)
  - IP Address: [text input]
  - Primary DNS Server: [text input] (optional)
  - Secondary DNS Server: [text input] (optional)
  - MAC Address: [text input] with a Clone button.
- Reconnect Mode:** Radio buttons for Always-on (selected), Connect-on-demand, and Manual.
- Maximum Idle Time:** 300 seconds.
- MTU:** 0 bytes.
- NAT disable:** A checkbox labeled 'Enable' is currently unchecked.

At the bottom of the configuration area are 'Apply' and 'Refresh' buttons.

## PPTP

**Address Mode:** Choose **Static IP** only if your ISP provides you with a static IP address for PPTP. Otherwise, please choose **Dynamic IP**.

**PPTP IP Address:** Enter the information provided by your ISP (Only applicable for Static IP PPTP).

**PPTP Subnet Mask:** Enter the information provided by your ISP (Only applicable for Static IP PPTP).

**PPTP Gateway IP Address:** Enter the information provided by your ISP (Only applicable for Static IP PPTP).

**PPTP Server IP Address:** IP address of the PPTP server.

**Username:** User/account name that your ISP provides to you for PPTP dial-up.

**Password:** Password that your ISP provides to you for PPTP dial-up.

**Verify Password:** Re-enter your password for verification.

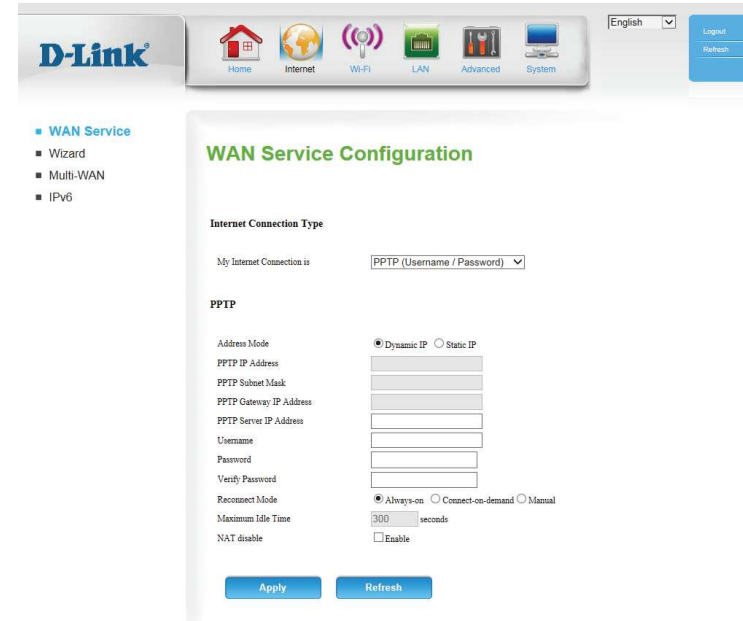
**Reconnect Mode:** Choose **Always-on** when you want to establish PPTP connection all the time. If you choose **Connect-on-demand**, the device will establish a PPTP connection when local users want to connect to the Internet, and disconnect if there is no traffic after the time period defined by the **Maximum Idle Time** setting.

**Maximum Idle Time:** The time of no activity to disconnect your PPTP session. Set it to zero or choose **Always-on** to disable this feature.

The screenshot shows the D-Link WAN Service Configuration page. The 'Internet Connection Type' is set to 'PPTP (Username / Password)'. Under the 'PPTP' section, the 'Address Mode' is set to 'Dynamic IP'. The 'PPTP IP Address', 'PPTP Subnet Mask', 'PPTP Gateway IP Address', and 'PPTP Server IP Address' fields are empty. The 'Username' and 'Password' fields are also empty. The 'Verify Password' field is empty. The 'Reconnect Mode' is set to 'Always-on'. The 'Maximum Idle Time' is set to '300 seconds'. The 'NAT disable' checkbox is unchecked. There are 'Apply' and 'Refresh' buttons at the bottom.

**NAT disable:** Enabling this option will disable the NAT firewall function of the DWR-922, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



## L2TP

**Address Mode:** Choose **Static IP** only if your ISP assigns you an IP address. Otherwise, please choose **Dynamic IP**.

**L2TP IP Address:** Enter the information provided by your ISP (Only applicable for Static IP L2TP).

**L2TP Subnet Mask:** Enter the information provided by your ISP (Only applicable for Static IP L2TP).

**L2TP Gateway IP Address:** Enter the information provided by your ISP (Only applicable for Static IP L2TP).

**L2TP Server IP Address:** IP address of the L2TP server.

**Username:** User/account name that your ISP provides to you for L2TP dial-up.

**Password:** Password that your ISP provides to you for L2TP dial-up.

**Verify Password:** Re-type your password in this field.

**Reconnect Mode:** Choose **Always-on** when you want to establish L2TP connection all the time. If you choose **Connect-on-demand** the device will establish L2TP connection when local users want to use Internet, and disconnect if no traffic after time period of Maximum Idle Time.

**Maximum Idle Time:** The time of no activity to disconnect your L2TP session. Set it to 0 or choose **Always-on to** disable this feature.

The screenshot shows the D-Link WAN Service Configuration page. The 'Internet Connection Type' is set to 'L2TP (Username / Password)'. Under the 'L2TP' section, the 'Address Mode' is set to 'Dynamic IP'. The 'L2TP IP Address', 'L2TP Subnet Mask', 'L2TP Gateway IP Address', and 'L2TP Server IP Address' fields are empty. The 'Username' and 'Password' fields are also empty. The 'Verify Password' field is empty. The 'Reconnect Mode' is set to 'Always-on'. The 'Maximum Idle Time' is set to '300 seconds'. The 'NAT disable' checkbox is unchecked. The 'Apply' and 'Refresh' buttons are visible at the bottom.

**NAT disable:** Enabling this option will disable the NAT firewall function of the DWR-922, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link WAN Service Configuration page. The top navigation bar includes the D-Link logo and icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. The main content area is titled "WAN Service Configuration" and includes a sidebar with "WAN Service" and sub-items: Wizard, Multi-WAN, and IPv6. The "Internet Connection Type" is set to "L2TP (Username / Password)". Under the "L2TP" section, the "Address Mode" is set to "Dynamic IP". The "Reconnect Mode" is set to "Always-on". The "Maximum Idle Time" is set to 300 seconds. The "NAT disable" checkbox is checked. At the bottom, there are "Apply" and "Refresh" buttons.

**WAN Service Configuration**

Internet Connection Type

My Internet Connection is

**L2TP**

Address Mode  Dynamic IP  Static IP

L2TP IP Address

L2TP Subnet Mask

L2TP Gateway IP Address

L2TP Server IP Address

Username

Password

Verify Password

Reconnect Mode  Always-on  Connect-on-demand  Manual

Maximum Idle Time  seconds

NAT disable  Enable

## 4G LTE / 3G

**Prefer Service Type:** Choose whether the DWR-922 should only use 4G networks, 3G networks, or use **Auto Mode** to automatically select a network.

**Username:** Fill in only if requested by carrier ISP (optional).

**Password:** Fill in only if requested by carrier (optional).

**Verify Password:** Re-type your password in this field (optional).

**Dialed Number:** If your carrier provides a dial-in number or code, enter it here. Empty by default.

**Authentication:** Select **PAP**, **CHAP**, or **Auto** detection. The default authentication method is **Auto**.

**APN:** Enter the APN information (optional).

**Pin Code:** If your SIM card has a PIN code, enter it here

**Reconnect Mode:** Select **Auto**, **Manual**, or **Connect-on-demand** to determine whether the router should reconnect to your 3G/4G network automatically or manually.

**Maximum Idle Time:** Set the maximum time your connection can be idle before disconnecting. Set it to 0 or choose **Auto** in Reconnect Mode to disable this feature.

**Roaming:** Enabling this option will allow you to connect when roaming away from your carrier's home network.

**Note:** Roaming connections may incur additional fees from your service provider.

The screenshot displays the 'WAN Service Configuration' interface for a D-Link router. The 'Internet Connection Type' is set to '4G LTE / 3G'. Under the '4G LTE / 3G Internet Connection Type' section, the 'Prefer Service Type' is 'Auto Mode'. The 'Username' and 'Password' fields are empty, with '(optional)' labels. The 'Verify Password' field is also empty. The 'Dialed Number' field is empty. The 'Authentication' is set to 'Auto'. The 'APN' is 'internet' with a 'Reset' button. The 'Pin Code' field is empty. The 'Reconnect Mode' is 'Auto' (selected with a radio button), with options for 'Connect-on-demand' and 'Manual'. The 'Maximum Idle Time' is set to '300 seconds'. The 'Roaming' option is unchecked. The 'Bridge ethernet ports', 'NAT disable', and 'Transparent Bridge' options are also unchecked. The 'Radio Frequency' is set to 'On' (selected with a radio button), with an 'Off' option. At the bottom, there are 'Apply' and 'Refresh' buttons.

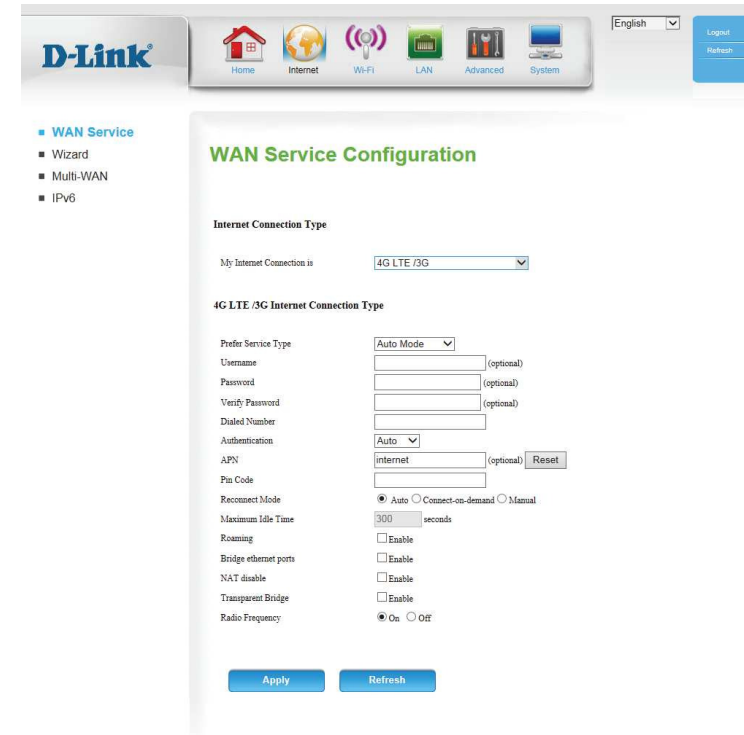
**Bridge Ethernet Ports:** Activate this feature to use the Ethernet WAN port as an additional LAN port.

**NAT disable:** Enabling this option will disable the NAT function of the DWR-922, allowing it to act as a link for your devices to your Internet connection, but without routing functions.

**Transparent Bridge:** Enabling the Transparent Bridge function disables the routing/NAT functions and passes the public WAN IP address given by your service provider directly through to the local client or PC. This can only be used if a single IP address has been assigned by your ISP. If transparent bridge is enabled, the above NAT Disable option will not be available

**Radio Frequency:** Turns the cellular radio on or off. This setting is intended to disable the cellular radio for areas where radio transmissions may be restricted.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



# Wizard

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

Click **Next** to continue.

**Note:** While using the wizard, you can click **Prev** to go back to the previous step, or you can click **Cancel** to close the wizard.

Select the Internet connection type you use. The connection types are explained on the following page. If you are unsure which connection type you should use, contact your Internet Service Provider (ISP).

Click **Prev** to go back to the previous page or click **Cancel** to close the wizard.

**Note:** The DWR-922 has a Multi-WAN Failover feature that allows the router to switch to a 3G/4G connection if the WAN connection is down or unavailable. To configure this feature, please refer to **Multi-WAN Configuration on page 24**.

## WELCOME TO THE SETUP WIZARD

It appears that you have already successfully connected your new router to the Internet.

- Step 1: Configure your Internet Connection
- Step 2: Configure your Wi-Fi Security
- Step 3: Set your Password
- Step 4: Select your Time Zone
- Step 5: Save Settings and Connect

Prev Next Cancel Connect

## STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Please select the Internet connection type below:

- DHCP Connection (Dynamic IP Address)**  
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- Username / Password Connection (PPPoE)**  
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (PPTP)**  
PPTP client.
- Username / Password Connection (L2TP)**  
L2TP client.
- 4G LTE / 3G Connection**  
4G LTE /3G.
- Static IP Address Connection**  
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

Prev Next Cancel Connect



The subsequent configuration pages will differ depending on the selection you make on this page.

**DHCP Connection (Dynamic IP Address):** Choose this if your ISP automatically provides you with an IP address. Most cable modems use this type of connection. See **Dynamic IP (DHCP)** on page 8 for information about how to configure this type of connection.

**Username / Password Connection (PPPoE):** Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See **PPPoE (Username / Password)** on page 11 for information about how to configure this type of connection.

**Username / Password Connection (PPTP):** Choose this option if your Internet connection requires Point-to-Point Tunneling Protocol (PPTP). See **PPTP** on page 13 for information about how to configure this type of connection.

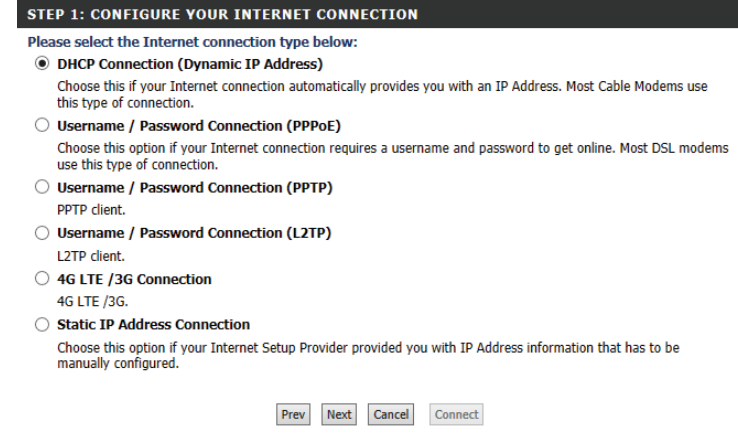
**Username / Password Connection (L2TP):** Choose this option if your Internet connection requires Layer 2 Tunneling Protocol (L2TP). See **L2TP** on page 15 for information about how to configure this type of connection.

**3G/4G Connection:** Choose this connection if you have installed a SIM card into the DWR-922. See **4G LTE / 3G** on page 17 for information about how to configure this type of connection.

**Static IP Address Connection:** Choose this option if your Internet Service Provider (ISP) provided you with IP address information that has to be manually configured. See **Static IP** on page 10 for information about how to configure this type of connection.

After entering the requested information, click **Next** to continue.

**Note:** If you are not sure what connection type to use or what settings to enter, check with your Internet Service Provider (ISP).



Enter a Wireless Network Name (SSID), then click **Next** to continue.

**STEP 2: CONFIGURE YOUR WI-FI SECURITY**

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 [default].

Wireless Network Name (SSID) :

Choose the best security level supported by your wireless clients. Click **Next** to continue.

**STEP 2: CONFIGURE YOUR WI-FI SECURITY**

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, or 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

**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 wireless adapters currently support WPA.

Unless you chose **None** in the previous step, enter a security password. Clients must enter this password to connect to your wireless network. Click **Next** to continue.

**STEP 2: CONFIGURE YOUR WI-FI SECURITY**

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password :

Note: You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

Create a new admin password and then click **Next** to continue. Users must enter this password to enter the setup utility.

**STEP 3: SET YOUR PASSWORD**

To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

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

**STEP 4: SELECT YOUR TIME ZONE**

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

Time Zone :

This completes the Internet Connection Setup Wizard. Click **Connect** to save your changes and reboot the router.

**SETUP COMPLETE!**

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

# Multi-WAN

The DWR-922's multi-WAN feature allows you to set your router to automatically switch to a secondary Internet connection if your primary Internet connection is lost. Note that you must first specify your primary Internet connection either on the **WAN Service** tab (see page 8) or the **Wizard** (see "Wizard" on page 19) before you can specify a secondary Internet connection. By default, the primary connection is 3G/4G.

**Failover type:** Select **Failover** to enable the failover function.

**Remote Host for Keep Alive:** This option should be set to an external IP address that can be used to ensure that the 3G/4G LTE connection will be kept from going offline due to inactivity. An example would be Google's public DNS servers (8.8.8.8 or 8.8.4.4) or your Internet service provider's DNS servers.

**Primary WAN:** This will automatically be set to the currently configured Internet connection type.

**Secondary WAN:** This can be set by clicking on **Add**, the available options will be shown in the drop down box that appears.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



## Multi-WAN Configuration

After selecting a secondary WAN and clicking apply, you will be directed to a setup screen for the relevant connection type.

### 4G LTE / 3G failover

**Username:** Fill in only if requested by your ISP (optional).

**Password:** Fill in only if requested by you ISP (optional).

**Verify Password:** Retype password if required above.

**Dialed Number:** If your ISP provides you with a dial-in number, enter it here. Empty by default.

**Authentication:** Select **PAP**, **CHAP** or **Auto** if requested by your carrier. The default authentication method is **Auto**.

**APN:** Enter the **APN** (Access Point Name) for your 3G/4G connection.

**Reset:** Press **Reset** to restore your APN setting to factory default. This button leaves all other settings unchanged, including those on this page.

**Pin Code:** If your SIM/UICC card has a PIN, enter it here (optional).

#### Radio

**Frequency:** Turns the cellular radio on or off. This setting is intended to disable the cellular radio for areas where radio transmissions may be restricted.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot displays the Multi-WAN configuration page. At the top, there is a navigation bar with icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. Below this, the page title "Multi-WAN" is shown in green. The configuration fields are as follows:

- Username:** Text input field with "(optional)" label.
- Password:** Text input field with "(optional)" label.
- Verify Password:** Text input field with "(optional)" label.
- Dialed Number:** Text input field.
- Authentication:** Dropdown menu set to "Auto".
- APN:** Text input field containing "internet" with "(optional)" label and a "Reset" button.
- Pin Code:** Text input field.
- Radio Frequency:** Radio buttons for "On" (selected) and "Off".

At the bottom of the page, there are two blue buttons: "Apply" and "Refresh".

## Static IP Address Failover

**IP Address:** Enter the IP address assigned to your network connection.

**Subnet Mask:** Enter the subnet mark.

**Default Gateway:** Enter the default gateway.

### Primary DNS

**Server:** Enter the primary DNS server.

### Secondary DNS

**Server:** Enter the secondary DNS server.

**MTU:** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 0.

**MAC Address:** The default MAC address is set to the WAN port's physical interface MAC address. Changing it is not recommended unless required to do so by your ISP. You can use the **Clone** button to replace the WAN port's MAC address with the MAC address of your PC.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the 'Multi-WAN' configuration interface. Under the heading 'Static IP Address Internet Connection Type', there are several input fields: 'IP Address', 'Subnet Mask', 'Default Gateway', 'Primary DNS Server', 'Secondary DNS Server', 'MTU' (with a value of 0 and '(bytes)' label), and 'MAC Address'. A 'Clone' button is located to the right of the MAC Address field. At the bottom of the form, there are two buttons: 'Apply' and 'Refresh'.

## Dynamic IP Failover

**Host Name:** If your ISP requires you to enter a host name, enter it here. In most cases, you may leave this blank.

### Primary DNS

**Server:** Enter the primary DNS server.

### Secondary DNS

**Server:** Enter the secondary DNS server.

**MTU:** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 0.

**MAC Address:** The default MAC address is set to the WAN port's physical interface MAC address. Changing it is not recommended unless required to do so by your ISP. You can use the **Clone** button to replace the WAN port's MAC address with the MAC address of your PC.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the 'Multi-WAN' configuration interface. The title 'Multi-WAN' is in green. Below it, the section 'Dynamic IP (DHCP) Internet Connection Type' is highlighted. The form contains the following fields and buttons:

- Host Name:
- Primary DNS Server:
- Secondary DNS Server:
- MTU:  (bytes)
- MAC Address:
-

## PPPoE Failover

**Username:** The username provided by your ISP for your PPPoE account.

**Password:** The password provided by your ISP for your PPPoE account

**Verify Password:** Re-type your password in this field.

**Service Name:** Fill in if provided by your ISP (optional).

**IP Address:** Fill in if provided by your ISP. If not, keep the default value.

### Primary DNS

**Server:** Enter the primary DNS server.

### Secondary DNS

**Server:** Enter the secondary DNS server.

**MAC Address:** The default MAC address is set to the WAN port's physical interface MAC address. Changing it is not recommended unless required to do so by your ISP. You can use the **Clone** button to replace the WAN port's MAC address with the MAC address of your PC.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

## Multi-WAN

### PPPoE

Username	<input type="text"/>
Password	<input type="password"/>
Verify Password	<input type="password"/>
Service Name	<input type="text"/> (optional)
IP Address	<input type="text"/>
Primary DNS Server	<input type="text"/> (optional)
Secondary DNS Server	<input type="text"/> (optional)
MAC Address	<input type="text"/> <input type="button" value="Clone"/>

Apply

Refresh



# IPv6

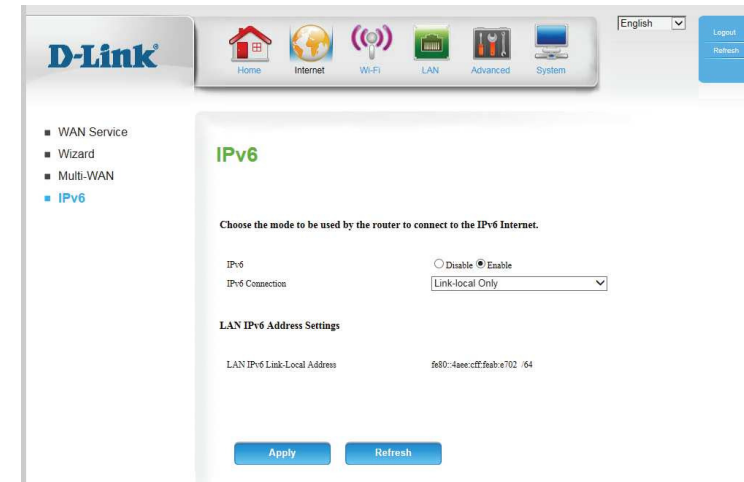
**IPv6:** To enable IPv6, select **Enable**.

**IPv6 Connection:** Select the IPv6 connection type specified by your ISP. The corresponding settings will be displayed below. Please see the following sections for details on how to configure these different connection types.

## Link-local Only

**LAN IPv6 Link-Local Address:** Displays the IPv6 address of the router.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



## Static IPv6

**IPv6 Address:** Enter the static IPv6 address of the router.

**Subnet Prefix Length:** Enter the subnet prefix length.

**Default Gateway:** Enter the default gateway address.

**DNS Addresses:** Enter the primary and secondary DNS server addresses.

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

**LAN IPv6 Link-Local Address:** Displays the router's LAN link-local address.

**Enable Autoconfiguration:** Check to enable the autoconfiguration feature for LAN devices.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **SLAAC + Stateless DHCPv6**. This will determine the configuration type for you IPv6 LAN.

**IPv6 Address Range (Start):** If you selected **Stateful (DHCPv6)**, enter the address range start.

**IPv6 Address Range (End):** If you selected **Stateful (DHCPv6)**, enter the address range end.

**Router Advertisement Lifetime:** Enter the IPv6 address lifetime (in seconds).

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link router's web interface for IPv6 configuration. The top navigation bar includes Home, Internet, Wi-Fi, LAN, Advanced, and System. The left sidebar lists WAN Service, Wizard, Multi-WAN, and IPv6 (selected). The main content area is titled 'IPv6' and contains the following sections:

- Choose the mode to be used by the router to connect to the IPv6 Internet:**
  - IPv6:  Disable  Enable
  - IPv6 Connection: Static IPv6 (dropdown)
- WAN IPv6 Address Settings:**
  - IPv6 Address: [text input]
  - Subnet Prefix Length: [text input]
  - Default Gateway: [text input]
  - Primary DNS Address: [text input]
  - Secondary DNS Address: [text input]
- LAN IPv6 Address Settings:**
  - LAN IPv6 Address: [text input]
  - LAN IPv6 Link-Local Address: fe80::4aee:cff:feab:e702 /64
- LAN Address Autoconfiguration Settings:**
  - Enable Autoconfiguration:
  - Autoconfiguration Type: Stateful (DHCPv6) (dropdown)
  - IPv6 Address Range(Start): [text input]
  - IPv6 Address Range(End): [text input]
  - IPv6 Address Lifetime: [text input] seconds

At the bottom, there are 'Apply' and 'Refresh' buttons.

## Autoconfiguration (SLAAC/DHCPv6)

**DNS Setting:** Select either **Obtain DNS server address automatically** or **Use the following DNS address**.

**DNS Addresses:** Enter the primary and secondary DNS server addresses.

**Enable DHCP-PD:** Check to enable the DHCP-PD feature.

**LAN IPv6 Address:** If you did not enable DHCP-PD, enter the LAN (local) IPv6 address for the router.

**LAN IPv6 Link-Local Address:** Displays the router's LAN link-local address.

**Enable Autoconfiguration:** Check to enable the autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **SLAAC + Stateless DHCPv6**. This will determine the configuration type for you IPv6 LAN.

**IPv6 Address Range (Start):** If you selected **Stateful (DHCPv6)**, enter the address range start.

**IPv6 Address Range (End):** If you selected **Stateful (DHCPv6)**, enter the address range end.

**IPv6 Address Lifetime:** Enter the IPv6 address lifetime (in seconds).

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot displays the D-Link web interface for IPv6 configuration. The top navigation bar includes the D-Link logo and icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. A sidebar on the left lists menu items: WAN Service, Wizard, Multi-WAN, and IPv6 (highlighted). The main content area is titled 'IPv6' and contains the following sections:

- Choose the mode to be used by the router to connect to the IPv6 Internet.**
  - IPv6:  Disable  Enable
  - IPv6 Connection: Autoconfiguration (SLAAC/DHCPv6)
- IPv6 DNS Settings**
  - DNS Setting:  Obtain DNS Server address Automatically  Use the following DNS address
  - Primary DNS Address: [Text Input]
  - Secondary DNS Address: [Text Input]
- LAN IPv6 Address Settings**
  - Enable DHCP-PD:
  - LAN IPv6 Address: [Text Input] /64
  - LAN IPv6 Link-Local Address: fe80::4aee:cff:8a3b:a702 /64
- LAN Address Autoconfiguration Settings**
  - Enable Autoconfiguration:
  - Autoconfiguration Type: Stateful (DHCPv6)
  - IPv6 Address Range (Start): [Text Input] /64
  - IPv6 Address Range (End): [Text Input] /64
  - IPv6 Address Lifetime: [Text Input] seconds

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Refresh'.

## PPPoE

**Username:** Enter your PPPoE user name.

**Password:** Enter your PPPoE password.

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

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

**DNS Setting:** Select either **Obtain DNS Server address Automatically** or **Use the following DNS address**.

**DNS Addresses:** Enter the primary and secondary DNS server addresses.

**Enable DHCP-PD:** Check to enable the DHCP-PD feature.

**LAN IPv6 Address:** If you did not enable DHCP-PD, enter the LAN (local) IPv6 address.

**LAN IPv6 Link-Local Address:** Displays the router's LAN link-local address.

**Enable Autoconfiguration:** Check to enable the autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **SLAAC + Stateless DHCPv6**. This will determine the configuration type for you IPv6 LAN.

### IPv6 Address

**Range (Start):** If you selected **Stateful (DHCPv6)**, enter the address range start.

### IPv6 Address

**Range (End):** If you selected **Stateful (DHCPv6)**, enter the address range end.

The screenshot shows the D-Link router's web interface for IPv6 configuration. The top navigation bar includes Home, Internet, Wi-Fi, LAN, Advanced, and System. The left sidebar shows a menu with WAN Service, Wizard, Multi-WAN, and IPv6 selected. The main content area is titled 'IPv6' and contains the following sections:

- Choose the mode to be used by the router to connect to the IPv6 Internet:**
  - IPv6:  Disable  Enable
  - IPv6 Connection: PPPoE (dropdown menu)
- PPPoE Settings:**
  - Username: [text input]
  - Password: [text input]
  - Service Name: [text input]
  - MTU: [text input]
- IPv6 DNS Settings:**
  - DNS Setting:  Obtain DNS Server address Automatically  Use the following DNS address
  - Primary DNS Address: [text input]
  - Secondary DNS Address: [text input]
- LAN IPv6 Address Settings:**
  - Enable DHCP-PD:
  - LAN IPv6 Address: [text input] /64
  - LAN IPv6 Link-Local Address: fe80::4aee:cff:feab:e702 /64
- LAN Address Autoconfiguration Settings:**
  - Enable Autoconfiguration:
  - Autoconfiguration Type: Stateful (DHCPv6) (dropdown menu)
  - IPv6 Address Range(Start): [text input] /64
  - IPv6 Address Range(End): [text input] /64
  - IPv6 Address Lifetime: [text input] seconds

At the bottom of the page, there are 'Apply' and 'Refresh' buttons.

# PPPoE

## IPv6 Address

**Lifetime:** Enter the IPv6 address lifetime (in seconds).

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for IPv6 configuration. The top navigation bar includes the D-Link logo and icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. The left sidebar lists navigation options: WAN Service, Wizard, Multi-WAN, and IPv6 (selected). The main content area is titled "IPv6" and contains the following sections:

- Choose the mode to be used by the router to connect to the IPv6 Internet.**
  - IPv6:  Disable  Enable
  - IPv6 Connection: PPPoE (dropdown menu)
- PPPoE Settings**
  - Username: [text input]
  - Password: [text input]
  - Service Name: [text input]
  - MTU: [text input]
- IPv6 DNS Settings**
  - DNS Setting:  Obtain DNS Server address Automatically  Use the following DNS address
  - Primary DNS Address: [text input]
  - Secondary DNS Address: [text input]
- LAN IPv6 Address Settings**
  - Enable DHCP-PD:
  - LAN IPv6 Address: [text input] /64
  - LAN IPv6 Link-Local Address: fe80::4aee:cff:feab:e702 /64
- LAN Address Autoconfiguration Settings**
  - Enable Autoconfiguration:
  - Autoconfiguration Type: Stateful (DHCPv6) (dropdown menu)
  - IPv6 Address Range(Start): [text input] /64
  - IPv6 Address Range(End): [text input] /64
  - IPv6 Address Lifetime: [text input] seconds

At the bottom of the configuration area, there are two buttons: "Apply" and "Refresh".

# Wi-Fi

## Device List

This page displays a list of currently-connected wireless clients, and their respective MAC addresses.



## Wi-Fi Settings

This page lets you set up your wireless network and choose a wireless security mode. Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

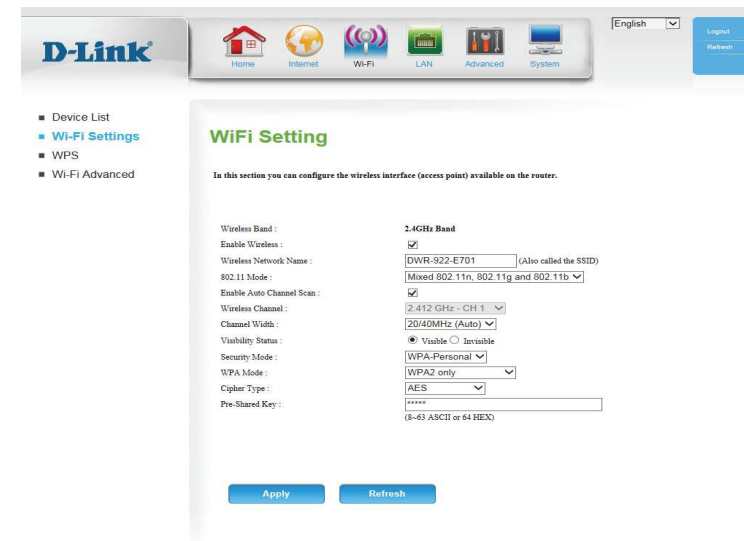
**Enable Wireless:** Check this box to enable wireless access. When you enable this option, the following parameters take effect.

**Wireless Network Name:** Also known as the SSID (Service Set Identifier), this is the name of your Wireless Local Area Network (WLAN). Enter a name using up to 32 alphanumeric characters. The SSID is case-sensitive.

**802.11 Mode:** Select the IEEE 802.11 standard used by your wireless clients.

**Enable Auto Channel Scan:** Enabling this feature will allow the router to automatically scan for the best wireless channel to use.

**Wireless Channel:** If Auto Channel Scan is disabled, select the desired channel here.



Copyright © 2012. All Rights Reserved.

**Channel Width:** A higher channel width allows for faster data transmission, at the possible expense of wireless coverage and compatibility with older wireless clients. Select the optimum channel width for your wireless network from the drop-down menu.

**Visibility Status:** The default setting is **Visible**. Select **Invisible** if you do not want to broadcast the SSID of your wireless network.

**Security Mode:** Select the desired wireless encryption mode. **WPA/WPA2** is recommended if your clients support it.

If you choose **WEP**, the following options will appear:

**WEP Key Length:** Select whether to use **64-bit** or **128-bit** encryption.

**Authentication:** Select whether to use **Open** or **Shared** authentication.

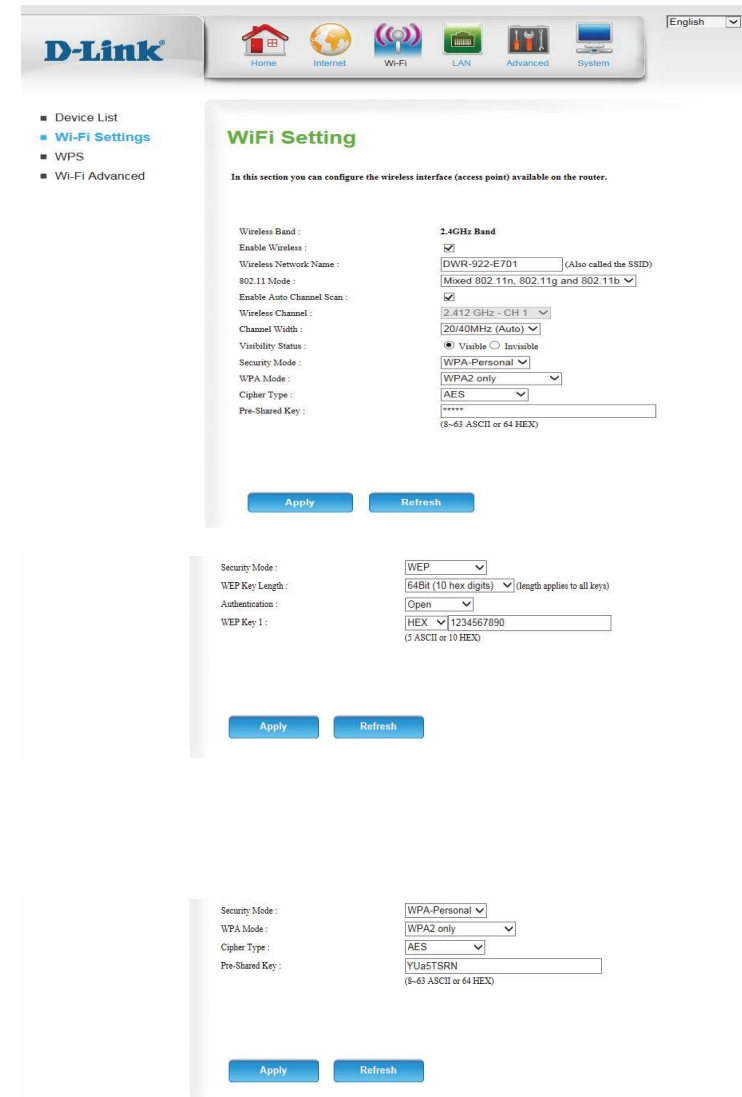
**WEP Key 1:** Set the WEP key/password for your wireless network. Based on whether you are using 64 or 128-bit encryption, and whether you are using a HEX or ASCII key, you will need to enter different numbers of characters for your key, as indicated below the WEP Key text box. ASCII keys may use letters and numbers only, and HEX keys may use numbers 0-9 and letters A-F only.

If you choose **WPA-Personal**, the following options will appear:

**WPA Mode:** Select whether to use **WPA2 only** or **Auto (WPA or WPA2)**. **WPA2 only** is the most secure, provided that all of your clients support it.

**Cipher Type:** Select whether to use the **TKIP** or **AES** cipher. The **AES** cipher is the most secure, provided that all of your clients can support it.

**Pre-Shared Key:** Enter the key/password you want to use for your wireless network. The key must be between 8 and 63 characters long, and may only contain letters and numbers.



# WPS

The Wi-Fi Protected Setup page allows you to create a wireless connection between your router and a device automatically by simply pushing a button or entering a PIN code.

**WPS:** Select whether you would like to **Enable** or **Disable** WPS features.

**AP PIN:** If you use Windows 7's **Connect to a network** wizard to do initial configuration of the router, you will have the option to enter the WPS PIN/AP PIN into the wizard when prompted. The factory default WPS PIN/AP PIN is printed on a label located on the bottom of the router. You can click the **Generate New PIN** button to change it to a randomly generated PIN.

**Config Mode:** Select whether the WPS config mode should be set to **Registrar** or **Enrollee**. In most cases, this should be set to **Registrar** so that you can use WPS to connect new wireless clients.

**Config Status:** If this is set to **CONFIGURED**, the router will be marked as “already configured” to computers that try to use WPS configuration, such as Windows 7's **Connect to a network** wizard. You can click the **Release** button to change the status to **UNCONFIGURED** to allow for WPS configuration of the router.

If this is set to **UNCONFIGURED**, you can click the **Set** button to change the status to **CONFIGURED** to block WPS configuration of the router.

**Disable WPS-PIN Method:** Enable this option to prevent clients from connecting to the router using the PIN method. If this option is enabled, clients must use the push-button method to connect.

The screenshot shows the D-Link WPS configuration interface. At the top, there is a navigation bar with icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. Below this is a sidebar menu with options: Device List, Wi-Fi Settings, WPS (selected), and Wi-Fi Advanced. The main content area is titled 'WPS' and contains the following settings:

- WPS:** Radio buttons for 'Enable' (selected) and 'Disable'.
- AP PIN:** Text field containing '12657940' and a 'Generate New PIN' button.
- Config Mode:** Dropdown menu set to 'Registrar'.
- Config Status:** Text field showing 'CONFIGURED' and a 'Release' button.
- Disable WPS-PIN Method:** Unchecked checkbox.
- Config Method:** Dropdown menu set to 'Push Button'.
- WPS status:** Text field showing 'CONFIGURED' and a 'Trigger' button.

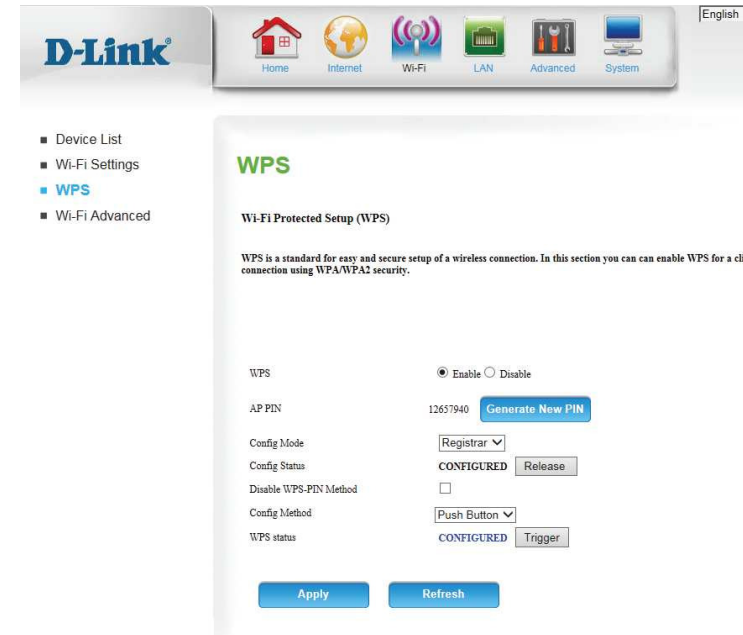
At the bottom of the configuration area, there are 'Apply' and 'Refresh' buttons.



**Config Method:** This lets you choose whether to use the **Push Button** connection method (PBC) or **PIN** method to connect to a wireless client when the **Trigger** button is clicked. If you choose the **PIN** method, you will need to enter an 8-digit PIN number that the wireless client needs to use to connect to your router.

**WPS status:** This will show the current WPS connection process status. Click the **Trigger** button to initiate a WPS connection.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



# Wi-Fi Advanced

This page contains settings which can negatively affect the performance of your router if configured improperly. Do not change these settings unless you are already familiar with them or have been instructed to make the change by one of our support personnel.

**Beacon Interval:** Specify a value for the beacon interval. Beacons are packets sent by an access point to synchronize a wireless network. 100 is the default setting and is recommended.

**Transmit Power:** Set the transmit power of the antennas.

**RTS Threshold:** This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.

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

**DTIM Interval:** Set the interval for DTIM. A Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default interval is 1.

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

**TX Rates:** Select the basic transfer rates based on the speed of wireless adapters on your wireless network. It is strongly recommended to keep this setting to **Best**.

The screenshot shows the D-Link Advanced Wireless Settings page. The page title is "Advanced Wireless Settings". Below the title, there is a note: "Specify advanced configuration settings for the gateway's radio from this page. AP security and association parameters can be modified from the default values if needed." The page is divided into sections for "Advanced 2.4G Wireless Settings". The settings are as follows:

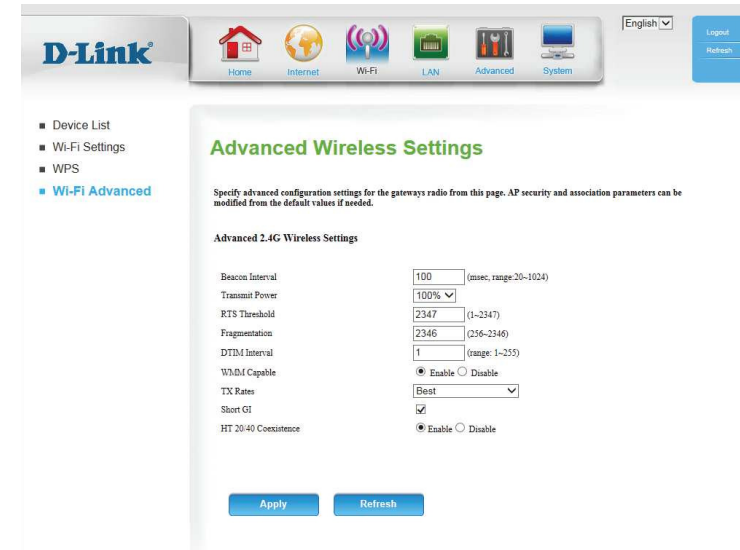
Setting	Value	Range/Options
Beacon Interval	100	(msec, range: 20-1024)
Transmit Power	100%	
RTS Threshold	2347	(1-2347)
Fragmentation	2346	(256-2346)
DTIM Interval	1	(range: 1-255)
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
TX Rates	Best	
Short GI	<input checked="" type="checkbox"/>	
HT 20/40 Coexistence	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

At the bottom of the settings area, there are two buttons: "Apply" and "Refresh".

**Short GI:** Check this box to reduce the guard interval to 400 ns. This can increase the throughput rate provided that the delay spread of the connection is also low. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

**HT 20/40 Coexistence:** Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel over-lapping and causing interference, the router will automatically change to 20 MHz.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

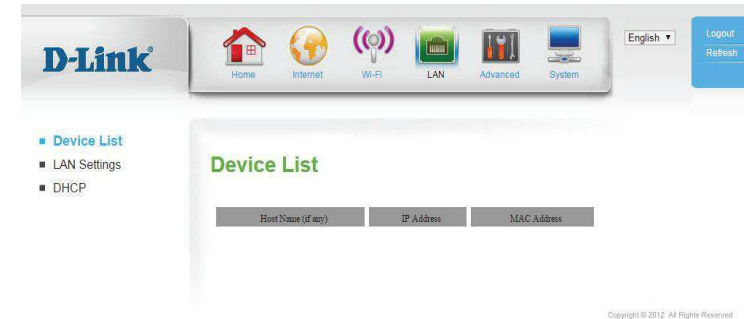


# LAN

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

## Device List

This page displays a list of currently-connected wired clients, and their respective MAC addresses.



## LAN Settings

**Router IP Address:** Enter the IP address you want to use for the router. The default IP address is **192.168.0.1**. If you change the IP address, you will need to enter the new IP address in your browser to get into the configuration utility.

**Default Subnet Mask:** Enter the subnet mask of the router. The default subnet mask is **255.255.255.0**.

**Local Domain Name:** Enter the local domain name for your network.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



# DHCP

The DWR-922 has a built-in DHCP (Dynamic Host Control Protocol) server. The DHCP server assigns IP addresses to devices on the network that request them. By default, the DHCP Server is enabled on the device. The DHCP address pool contains a range of IP addresses, which are automatically assigned to the clients on the network.

**Enable DHCP Server:** Select this box to enable the DHCP server on your router.

**DHCP IP Address Range:** Enter the range of IPs for the DHCP server to use to assign IP addresses to devices on your network. These values will represent the last octet of the IP addresses in the pool.

**DHCP Lease Time:** Enter the lease time for IP address assignments.

**Primary DNS IP Address:** Enter the primary DNS IP address that will be assigned to DHCP clients.

**Secondary DNS IP Address:** Enter the secondary DNS IP address that will be assigned to DHCP clients.

**DHCP Reservation:** Click **DHCP Reservation** to assign a dedicated IP to a specified MAC address to be saved by the DHCP server. The Fixed Mapping page will appear.

Select a DHCP client and click **Copy to**, or enter the MAC address and IP address manually, to assign the IP address to the MAC address. Click **Enable** to enable the rule.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link DHCP Server Configuration page. The 'Enable DHCP Server' checkbox is checked. The 'DHCP IP Address Range' is set to 50 to 199. The 'DHCP Lease Time' is set to 86400 seconds. There are input fields for 'Primary DNS IP Address' and 'Secondary DNS IP Address'. A 'DHCP Reservation' button is visible below the configuration fields. At the bottom of the page, there are 'Apply' and 'Refresh' buttons.

The screenshot shows the D-Link DHCP Reservation page. At the top, there is a dropdown menu for 'DHCP clients' with the text 'Select one --'. To the right of this dropdown are 'Copy to' and 'ID' dropdown menus. Below this is a table with the following columns: ID, MAC Address, IP Address, and Enable. The table has 10 rows, each with an ID from 1 to 10, empty input fields for MAC Address and IP Address, and a checkbox for Enable. At the bottom of the table, there are 'Previous page', 'Next page', and 'Back' buttons. At the very bottom of the page, there are 'Apply' and 'Refresh' buttons.

ID	MAC Address	IP Address	Enable
1			<input type="checkbox"/>
2			<input type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>
6			<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>
9			<input type="checkbox"/>
10			<input type="checkbox"/>

# Advanced DNS

On this page you can configure the Domain Name System (DNS) server, which manages the resolution of host/domain names to IP addresses.

**DDNS:** Tick this checkbox to enable the DDNS feature.

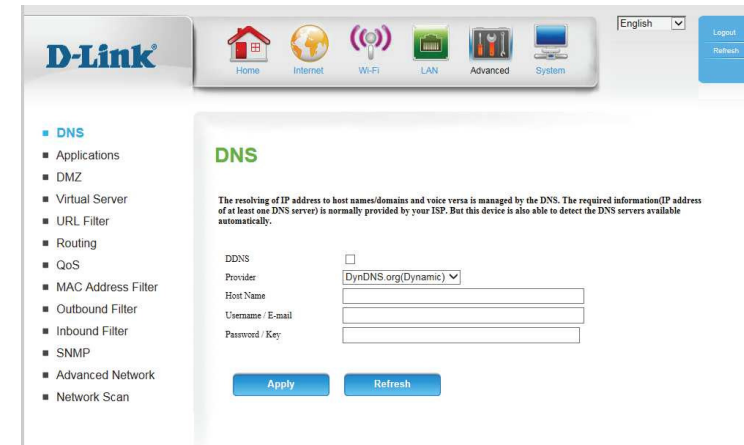
**Provider:** Select a DDNS service provider to use.

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

**Username / E-mail:** Enter the **Username** for your DDNS account.

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

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



The screenshot shows the D-Link Advanced DNS configuration interface. The top navigation bar includes the D-Link logo and icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. The left sidebar lists various configuration options, with DNS selected. The main content area is titled 'DNS' and contains a checkbox for 'DDNS', a dropdown menu for 'Provider' (set to 'DynDNS.org(Dynamic)'), and input fields for 'Host Name', 'Username / E-mail', and 'Password / Key'. There are 'Apply' and 'Refresh' buttons at the bottom of the form.

# Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, and Internet telephony. These applications may have difficulty working through NAT (Network Address Translation). **Applications** allows some of these applications to work with the DWR-922 by opening ports after detecting traffic being sent through a trigger port.

**Popular Applications:** Select from a list of popular applications. You can select a service, select a rule ID, then click the **Copy to** button to copy the default settings for that service to the specified rule ID.

**ID:** Specifies which rule to copy the selected **Popular applications** settings to when you click the **Copy to** button.

## APPLICATION RULES

**ID:** This identifies the rule.

**Trigger:** Enter the port to listen to in order to trigger the rule.

**Incoming Ports:** Specify the incoming port(s) to open when traffic comes over the **Trigger** port.

**Enable:** Check the box to enable the specified rule.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for the Applications configuration. The left sidebar contains a navigation menu with the following items: DNS, Applications (highlighted), DMZ, Virtual Server, URL Filter, Routing, QoS, MAC Address Filter, Outbound Filter, Inbound Filter, SNMP, Advanced Network, and Network Scan. The main content area is titled 'Applications' and includes a 'Popular applications' dropdown menu set to '-- Select one --', a 'Copy to' button, and an 'ID' dropdown menu. Below this is a table for 'Application Rules' with the following structure:

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

At the bottom of the table are 'Apply' and 'Refresh' buttons.

# DMZ

Sometimes you may want a computer exposed to the Internet for certain types of applications. If you choose to expose a computer, you can enable Demilitarized Zone (DMZ). This option will expose the chosen computer completely to the Internet. This is not recommended for normal use.

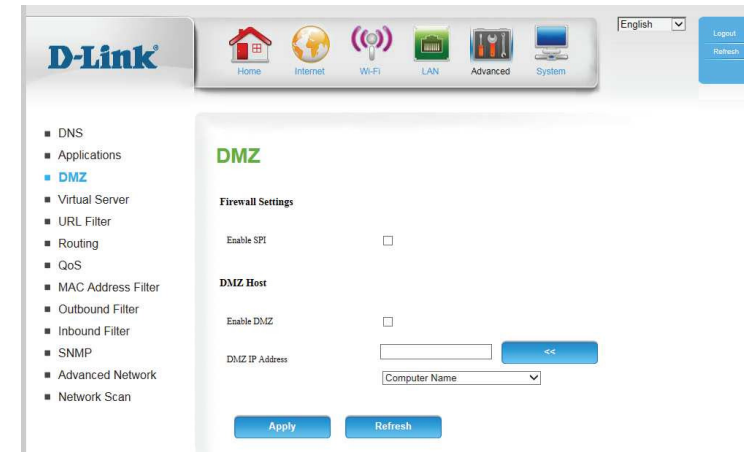
**Enable SPI:** Enabling Stateful Packet Inspection (SPI) helps to prevent cyber attacks by validating that the traffic passing through the session conforms to the protocol.

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

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

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

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.





# Virtual Server

The device can be configured as a virtual server so that users can access services such as Web or FTP via the public (WAN) IP address of the router. You can also allow the settings to run on a specified schedule.

**Well-known Services:** This contains a list of pre-defined services. You can select a service, select a rule ID, then click the **Copy to** button to copy the default settings for that service to the specified rule ID.

**ID:** Specifies which rule to copy the selected **Well known service** settings to when you click the **Copy to** button.

**Use schedule rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 59.

## VIRTUAL SERVERS LIST

**ID:** This identifies the rule.

**Service Ports** Enter the public port(s) you want to open.

**Server IP: Port:** Enter the IP address and port of the computer on your local network that you want to forward the Service Ports to.

**Enable:** Check the box to enable the specified rule.

**Schedule Rule #:** Specify the schedule rule number. To create schedules, click on the **Add New Rule** button. For further information on schedules, please refer to **Schedules** on page 59.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link Virtual Server configuration interface. On the left is a navigation menu with options like DNS, Applications, DMZ, Virtual Server (selected), URL Filter, Routing, QoS, MAC Address Filter, Outbound Filter, Inbound Filter, SNMP, Advanced Network, and Network Scan. The main area is titled 'Virtual Server' and contains a description: 'The Externally acts as server. It receives the requests of remote users under its public IP address and forwards them automatically to the Virtual Server. So a client in your network behind NAT or firewall can provide services as a Virtual Server. You just have to enable specific ports or port ranges and protocols (UDP/TCP). File sharing or web services for e.g. HTTP, FTP or POP3 are possible. The private IP addresses of the servers in the local network remain safe. If you have a dynamic IP address, you may want to enable DynDNS additionally.' Below the description are two dropdown menus: 'Well known services' (set to 'Select one') and 'Use schedule rule' (set to 'ALWAYS ON'). There is a 'Copy to' button and an 'ID' dropdown. Below this is a table titled 'Virtual Servers List' with columns: ID, Service Ports, Server IP: Port, Enable, and Schedule Rule. Two rows are visible, each with an 'Add New Rule...' button.

ID	Service Ports	Server IP: Port	Enable	Schedule Rule
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>

# URL Filter

**URL Filter** allows you to set up a list of websites that will be blocked from users on your network.

**URL Filtering:** Check the box to enable URL Filtering.

## URL FILTERING RULES

**ID:** This identifies the rule.

**URL:** Enter URL that you would like to block. All URLs that begin with this address will be blocked.

**Enable:** Check the box to enable the specified rule.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for configuring the URL Filter. The top navigation bar includes icons for Home, Internet, Wi-Fi, LAN, Advanced, and System, along with a language dropdown set to English and a Logout button. The sidebar on the left contains a tree view with the following items: DNS, Applications, DMZ, Virtual Server, **URL Filter** (highlighted), Routing, QoS, MAC Address Filter, Outbound Filter, Inbound Filter, SNMP, Advanced Network, and Network Scan. The main content area is titled "URL Filter" and contains the following text: "URL Filter provides the useful tools for restricting Internet access. Website URL Blocking allows you to quickly create a list of all web sites that you wish to allow or deny users from accessing." Below this is the "URL Filtering Setting" section, which includes a checkbox for "URL Filtering" that is checked and labeled "Enable". The "URL Filtering Rules" section features a table with the following structure:

ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

At the bottom of the main content area, there are two buttons: "Apply" and "Refresh".

# Routing

The **Routing** page allows you to specify custom routes that determine how data is moved around your network.

**RIP:** Check the box to enable routing, then select which routing protocol to use:

- **RIPv1:** Protocol in which the IP address is routed through the Internet.
- **RIPv2:** Enhanced version of RIPv1 with added features such as authentication, routing domain, next hop forwarding, and subnet-mask exchange.

## ROUTING RULES

**ID:** This identifies the rule.

**Destination:** Enter in the IP of the specified network that you want to access using the static route.

**Subnet Mask:** Enter in the subnet mask to be used for the specified network.

**Gateway:** Enter in the gateway IP address for the specified network.

**Hop:** Enter in the amount of hops it will take to reach the specified network.

**Note:** In a transmission path, each link is terminated at a network device such as a router or gateway. The number of hops equals the number of routers or gateways that data must pass through before reaching the destination.

**Enable:** Select this box to enable the rule.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for the Routing configuration page. The navigation menu on the left includes: DNS, Applications, DMZ, Virtual Server, URL Filter, **Routing**, QoS, MAC Address Filter, Outbound Filter, Inbound Filter, SNMP, Advanced Network, and Network Scan. The main content area is titled 'Routing' and contains the following settings:

**RIP Setting**

RIP:  Enable  RIPv1  RIPv2

**Routing Rules**

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

At the bottom of the page, there are two buttons: **Apply** and **Refresh**.

# QoS

The **QoS Engine** improves your online gaming or streaming media experience by ensuring that your game or media traffic is prioritized over other network traffic, such as FTP or web.

**Enable QoS Packet Filter:** Select this box to enable the QoS feature.

**Upstream Bandwidth:** Specify the maximum upstream bandwidth here (e.g. 400 Kbps).

**Use Schedule Rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 59.

## QOS RULES

**ID:** This identifies the rule.

**Local IP : Ports:** Specify the local IP address(es) and port(s) for the rule to affect.

**Remote IP : Ports:** Specify the remote IP address(es) and port(s) for the rule to affect.

**QoS Priority:** Select what priority level to use for traffic affected by the rule: **Low, Normal, or High**.

**Enable:** Check the box to enable the specified rule.

**Use Rule #:** Specify the schedule rule number. To create a new schedule, click on the **Add New Rule** button. For more information about schedules, please refer to **Schedules** on page 59.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for QoS configuration. The top navigation bar includes Home, Internet, WiFi, LAN, Advanced, and System. The left sidebar lists various network settings, with QoS selected. The main content area is titled 'QoS' and contains the 'QoS Engine Setup' section. This section has a checkbox for 'Enable QoS Packet Filter', an input field for 'Upstream bandwidth' (set to 400 kbps), a 'Use schedule rule' dropdown menu (set to 'ALWAYS ON'), and a 'Copy to' button. Below this is the 'QoS Rules' section, which features a table with 8 rows. Each row has columns for ID, Local IP, Remote IP, QoS Priority (set to High), and an Enable checkbox. To the right of each row is an 'Add New Rule...' button. At the bottom of the page are 'Apply' and 'Refresh' buttons.

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
2	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
3	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
4	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
5	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
6	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
7	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
8	<input type="text"/>	<input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...

# MAC Address Filter

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.

**MAC Address Control:** Check this box to enable MAC Filtering.

**Connection Control:** Check the box to allow wireless and wired clients with **C** selected to connect to this device. You can also select to **allow** or **deny** connections from unspecified MAC addresses.

**Association Control:** Check the box to allow wireless clients with **A** selected can associate to the wireless LAN. You can also select to **allow** or **deny** connections from unspecified MAC addresses.

## MAC FILTERING RULES

**ID:** This identifies the rule.

**MAC Address:** Specify the MAC address of the computer to be filtered.

**IP Address:** Specify the last section of the IP address.

**C:** If this box is ticked, the rule will follow the connection control setting specified in MAC filtering settings specified above.

**A:** If this box is ticked, the rule will follow the association control setting specified in MAC filtering settings specified above.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for configuring the MAC Address Filter. The navigation menu on the left includes: DNS, Applications, DMZ, Virtual Server, URL Filter, Routing, QoS, **MAC Address Filter** (selected), Outbound Filter, Inbound Filter, SNMP, Advanced Network, and Network Scan. The main content area is titled 'MAC Address Filter' and contains the following settings:

- MAC Filtering Settings:**
  - Enable
  - Connection control: Wireless and wired clients with **C** checked can connect to this device; and **allow** unspecified MAC addresses to connect.
  - Association control: Wireless clients with **A** checked can associate to the wireless LAN; and **allow** unspecified MAC addresses to associate.
- DHCP clients:** Select one --  ID --
- MAC Filtering Rules:**

ID	MAC Address	C	A
1	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the page, there are buttons for 'Previous page', 'Next page', 'Apply', and 'Refresh'.

# Outbound Filter

**Outbound Filter** enables you to control what packets are allowed to be sent out to the Internet. The outbound filter applies to all outbound packets.

**Outbound Filter:** Select this box to **Enable** outbound filtering.

**Use Schedule Rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 59.

## OUTBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all outgoing traffic except for traffic that matches the listed rules.

**ID:** This identifies the rule.

**Source IP : Ports:** Specify the local IP address and then specify the port after the colon.

**Destination IP :**

**Ports:** Specify the remote IP address and then the port after the colon.

**Enable:** Check the box to enable the specified rule.

**Schedule Rule #:** Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

**Previous Page:** Go back to the previous filter page.

**Next Page:** Advance to the next filter page.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for configuring the Outbound Filter. The page is titled "Outbound Filter" and is part of the "Advanced" settings. The "Outbound Filter Setting" section includes an "Enable" checkbox (checked), a "Use schedule rule" dropdown menu (set to "ALWAYS ON"), and a "Copy to" button. Below this is the "Outbound Filter Rules List" section, which contains a table with 8 rows. Each row has columns for "ID", "Source IP:Ports", "Destination IP:Ports", "Enable", and "Schedule Rule". The "Enable" column has a checkbox for each row, and the "Schedule Rule" column has a dropdown menu. Below the table are "Previous page" and "Next page" buttons. At the bottom of the page are "Apply" and "Refresh" buttons.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <a href="#">Add New Rule...</a>

# Inbound Filter

**Inbound Filter** enables you to control what packets are allowed to come in to your network from the Internet. The inbound filter only applies to packets that are destined for Virtual Servers or DMZ hosts.

**Inbound Filter:** Select this box to **Enable** the filter.

**Use Schedule Rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 59.

## INBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all incoming traffic except for traffic that matches the listed rules.

**ID:** This identifies the rule.

**Source IP : Ports:** Specify the local IP address and then specify the port after the colon.

**Destination IP : Ports:** Specify the remote IP address and then the port after the colon.

**Enable:** Check the box to enable the specified rule.

**Schedule Rule #:** Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

**Previous Page:** Go back to the previous filter page.

**Next Page:** Advance to the next filter page.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for the Inbound Filter configuration. The top navigation bar includes the D-Link logo and icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. The main content area is titled "Inbound Filter" and contains the following sections:

- Inbound Filter Setting:**
  - Enable
  - Use schedule rule: **ALWAYS ON** (dropdown menu)
  - Copy to** button
  - ID: **--** (dropdown menu)
- Inbound Filter Rules List:**
  - Allow all to pass except those match the following rules.
  - Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <b>Add New Rule...</b>

At the bottom of the page, there are buttons for **Previous page**, **Next page**, **Apply**, and **Refresh**.

# SNMP

**SNMP** (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DWR-922. The DWR-922 supports SNMP v1 and v2c.

**SNMP Local:** Select whether to **Enable** or **Disable** local SNMP administration.

**SNMP Remote:** Select whether to **Enable** or **Disable** remote SNMP administration.

**Get Community:** Enter the password **public** in this field to allow read-only access to network administration using SNMP. You can view the network, but no configuration is possible with this setting.

**Set Community:** Enter the password **private** in this field to enable read/write access to the network using SNMP.

**IP 1/IP 2/IP 3/IP 4:** Enter up to 4 IP addresses to use as trap targets for your network.

**SNMP Version:** Select the SNMP version of your system.

## WAN Access

**IP Address** If you want to limit remote access SNMP access, enter the IP address of the remote computer you will use to access this device; all other IP addresses will be denied remote SNMP access.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



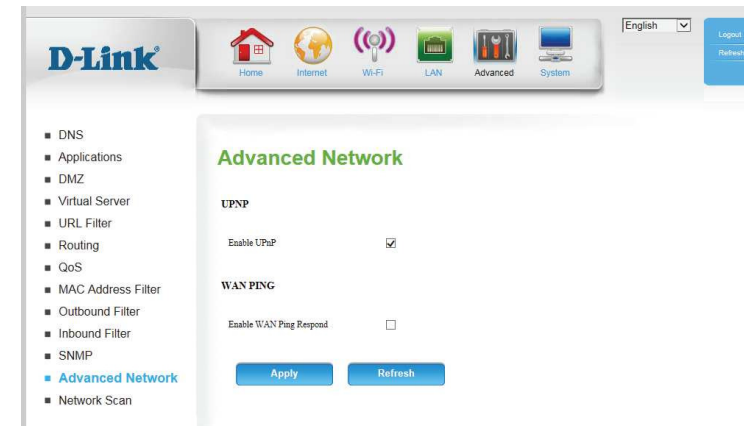
# Advanced Network

**Advanced Network** contains settings which can change the way the router handles certain types of traffic. We recommend that you do not change any of these settings unless you are already familiar with them or have been instructed to make the change by one of our support personnel.

**Enable UPnP:** Check the box to enable the Universal Plug and Play (UPnP™) feature. UPnP provides compatibility with various networking equipment, software, and peripherals.

**Enable WAN Ping Respond:** Select the box to allow the WAN port to be “pinged.” Blocking WAN pings may provide some extra security from hackers.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



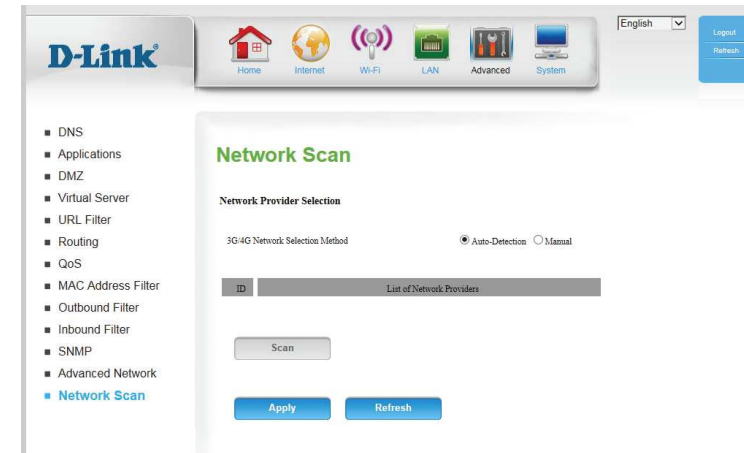
## Network Scan

This page lets you set whether to allow the DWR-922 to automatically select a 3G/4G network based on the inserted SIM/UICC card, and allows you to manually scan for networks and select one to connect to.

**3G/4G Network Selection Method:** Leave this setting on **Auto** to allow the DWR-922 to automatically select a cellular network to connect to. If you need to select a network manually, select **Manual**, click the **Scan** button, then select an available network to connect to.

**Note:** You will only be able to scan for networks if the DWR-922 is not currently connected to a 3G/4G network.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



# System Time Settings

This section will help you set the time zone that you are in and an NTP (Network Time Protocol) server to use. Daylight Saving can also be configured to adjust the time when needed.

**Time Zone:** Select the appropriate **Time Zone** from the drop-down box.

**Enable Daylight Saving:** Check the box to allow for daylight saving adjustments. Use the drop-down boxes to specify a start date and end date for daylight saving time adjustments.

**Sync your computer's time settings:** This button allows the router to set time zone and current time based on your computer's configuration. To use this setting, ensure that Automatic Synchronization is unchecked and applied.

**Automatically synchronize with Internet time server:** Check the box to allow the router to use an NTP server to update the router's internal clock.

**NTP Server Used:** Enter an NTP server to use for time synchronization, or use the drop-down box to select one. Click the **Update Now** button to synchronize the time with the NTP server.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link router's web interface for Time Settings. The page title is "Time Settings". Below the title, there is 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." The configuration fields are as follows:

- Time:** Mon Dec 31, 2012 19:37:44
- Time Zone:** (GMT -12:00) Eniwetok, Kwajalein
- Enable Daylight Saving:**
- Start:** 01/01 (Hour:Day:Month)
- End:** 23/31/Dec (Hour:Day:Month)
- Sync your computer's time settings:**
- Automatically synchronize with Internet time server:**
- NTP Server Used:** time.nist.gov
- Update Now:**

At the bottom of the page, there are buttons for **Apply** and **Refresh**. The footer of the page reads "Copyright © 2012 All Rights Reserved".

# Administration

The **Admin** page allows you to change the Administrator password and enable Remote Management. The admin has read/write access while users only have read-only access. Only the admin has the ability to change both admin and user account passwords.

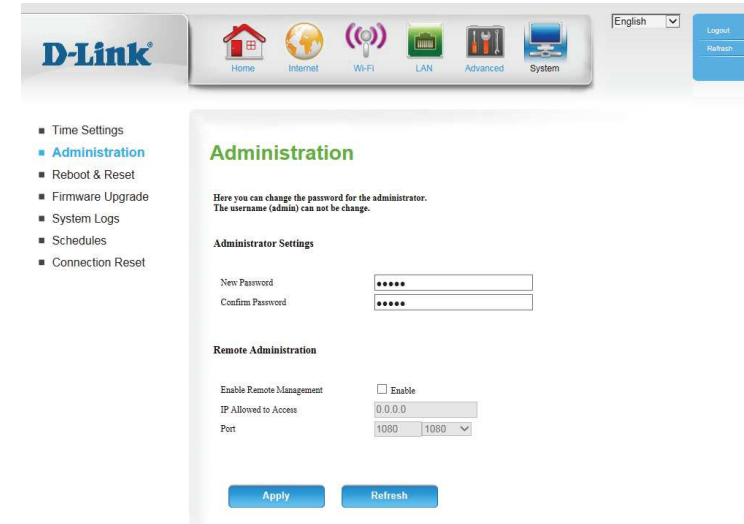
**Admin Password:** Enter and confirm the password that the admin account will use to access the router's management interface.

**Remote Management:** Tick this check box to enable remote management. Remote management allows the DWR-922 to be configured over the Internet through a web browser. A username and password will still be required to access the web-management interface.

**IP Allowed to Access:** Enter the Internet IP address of the PC that has access to the broadband router. If you enter an asterisk (\*) in this field, then anyone will be able to access the router. Adding an asterisk (\*) into this field could present a security risk and is not recommended.

**Port:** This is the port number used to access the router. 8080 is the port usually used for the web-management interface.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



The screenshot shows the D-Link Administration interface. At the top, there is a navigation bar with icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. The main content area is titled "Administration" and contains the following sections:

- Administrator Settings:** Includes fields for "New Password" and "Confirm Password", both masked with dots.
- Remote Administration:** Includes a checkbox for "Enable Remote Management" (unchecked), a text field for "IP Allowed to Access" (containing "0.0.0.0"), and a dropdown menu for "Port" (set to "1080").

At the bottom of the form, there are two buttons: "Apply" and "Refresh".

## Reboot & Reset

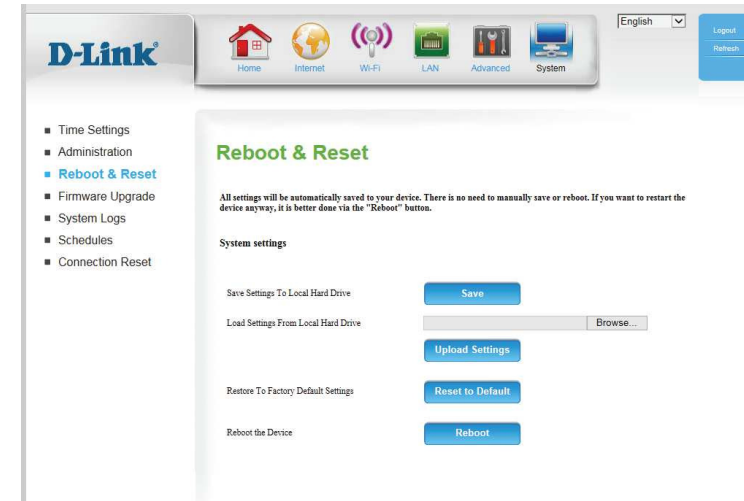
Here, you can save the current system settings to a local hard drive.

**Save Settings To Local Hard Drive** Use this option to save your current router configuration settings to a file. Click **Save** to open a file dialog, and then 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. Click **Choose File** and select the saved file and then click the **Upload Settings** button to upload the settings to the router.

**Restore To Factory Default Settings:** This option will restore all settings back to their defaults. Any settings that have not been backed up will be lost, including any rules that you have created.

**Reboot the Device:** This option will reboot the router.



# Firmware Upgrade

Here, you can upgrade the firmware of your router. Make sure the firmware you want to use is on the local hard drive of the computer and then click **Browse** to upload the file. You can check for and download firmware updates at the D-Link support site at <http://support.dlink.com>.

**Current Firmware Version:** Displays your current firmware's version.

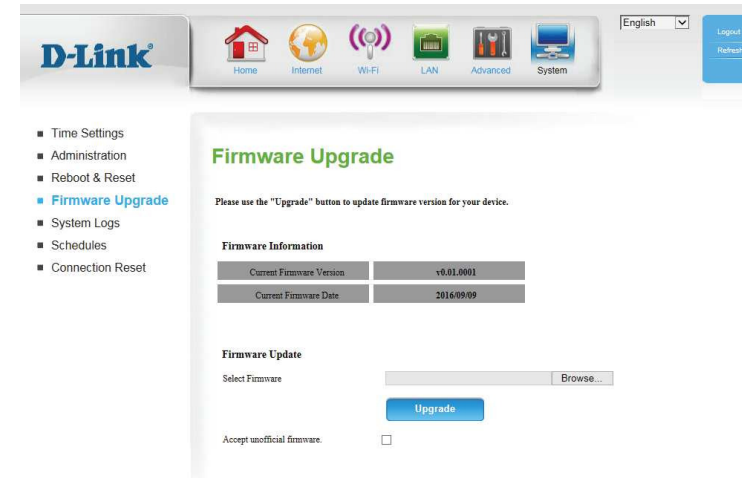
**Current Firmware Date:** Displays your current firmware's release date.

**Select Firmware:** After you have downloaded a new firmware, click **Browse** to locate the firmware on your computer, then click **Upload** to start the firmware upgrade.

**Warning:** You must use a wired connection to upload the firmware file; do not use a wireless connection. During the upgrade process, do not power off your computer or router, and do not refresh the browser window until the upgrade is complete.

**Accept Unofficial Firmware:** If the firmware you want to install is not an official D-Link release, you will need to check this box.

**Warning:** Unofficial firmware is not supported, and may cause damage to your device. Use of unofficial firmware is at your own risk.



# System Logs

The DWR-922 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 the box to send the router logs to a Syslog server.

**Syslog Server IP Address:** Enter the IP address of the Syslog server that the router will send the logs to.

Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

The screenshot shows the D-Link web interface for the DWR-922 router. The 'System Log' configuration page is active. The 'Enable Logging To Syslog Server' checkbox is unchecked. Below it is a text input field for the 'Syslog Server IP Address'. There are 'Apply' and 'Refresh' buttons. The 'View Logs' section displays a table of log entries.

Time	Message
Sep 18 13:30:48	kernel: klogd started: BusyBox v1.3.2 (2016-09-09 16:18:21 CST)
Sep 18 13:30:50	commander: CSID0001001F read err: -61
Sep 18 13:30:51	BEID: WAN = 48:EE:0C:AB:E7:01
Sep 18 13:30:51	BEID: LAN / WLAN0 = 48:EE:0C:AB:E7:02
Sep 18 13:30:51	BEID: BEID STATUS : 0, STATUS OK!
Sep 18 13:30:51	syslog: WAN 0 Get available PVID 2
Sep 18 13:30:51	syslog: ID : id=2, m=1, Using VLAN Count 0
Sep 18 13:30:51	syslog: Set NAT (request vid: 1)lan 0 id 1 tagged: 0, member: 2 3 4 5 0
Sep 18 13:30:51	syslog: ID : id=1, m=2, Using VLAN Count 1
Sep 18 13:30:51	syslog: 1: 0:Br0 using MAC: 48:EE:0C:AB:E7:02
Sep 18 13:30:51	syslog: br0 added
Sep 18 13:30:51	syslog: ifconfig eth2.1 hw ether 48EE0CABE702
Sep 18 13:30:51	syslog: Get Wan 0, wantype: 10
Sep 18 13:30:51	syslog: Start set virtual wan
Sep 18 13:30:51	syslog: 1 Enabled: 0

Page: 1/44 (Log Number : 651)

Navigation buttons: Previous page, Next page, First Page, Last Page, Refresh, Download, Clear logs

# Schedules

This section allows you to manage schedule rules for various firewall and parental control features. Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.

**Enable Schedule:** Check this box to enable schedules.

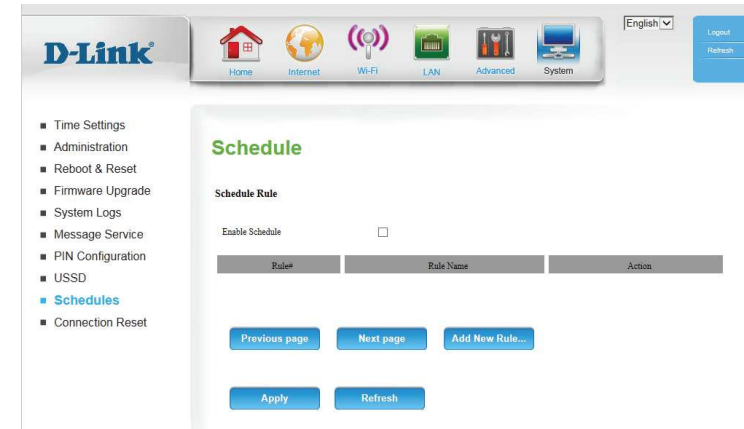
**Edit:** Click this icon to edit the selected rule. (see below)

**Delete:** Click this icon to delete the selected rule.

**Previous Page:** Click this button to go to the previous page of rules.

**Next Page:** Click this button to go to the next page of rules.  
Click this button to specify the start time, end time, and name of the rule.

**Add New Rule..:** Click this button to create a new rule. (see below)



## Add New Rule

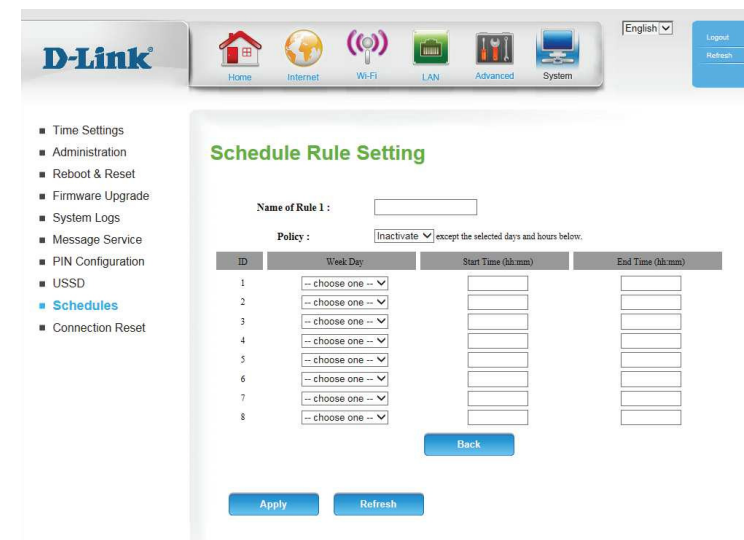
**Name of Rule #:** Enter a name for your new schedule.

**Policy:** Select Activate or Inactivate to decide whether features that use the schedule should be active or inactive except during the times specified.

**Week Day:** Select a day of the week for the start time and end time.

**Start Time (hh:mm):** Enter the time at which you would like the schedule to become active.

**End Time (hh:mm):** Select the time at which you would like the schedule to become inactive.





# Connection Reset

This feature allows you to reset the Internet connection on your router by periodically resetting the connection. You can choose to have this happen on a predetermined schedule by configuring the options on this page.

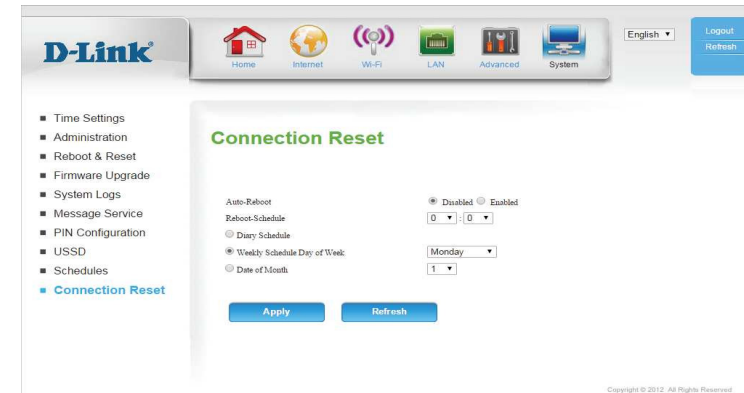
**Auto-Reboot:** Select whether the connection reset feature should be enabled or disabled.

**Reboot-Schedule:** If the connection reset feature is enabled, select when it should activate via the hour and minute from the dropdown boxes.

**Daily Schedule:** Select this option if you want the connection reset feature to activate on a daily schedule.

**Weekly Schedule Day of Week:** Select this option if you want the connection reset feature to activate only on a certain day of the week.

**Date of Month:** Select this option if you want the connection reset feature to activate only on a certain day of the month.



# Connect a Wireless Client to your Router

## WPS Button

The easiest and most secure way to connect your wireless devices to the router is with WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DWR-922 router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

**Step 1** - Press the WPS button on the DWR-922 for about 6 seconds. The WLAN LED on the front will start to blink.



**Step 2** - Within 2 minutes, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

**Step 3** - Allow up to 1 minute for your connection to be configured. Once the Internet light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

# Connecting to a Wireless Network

## Windows® 10

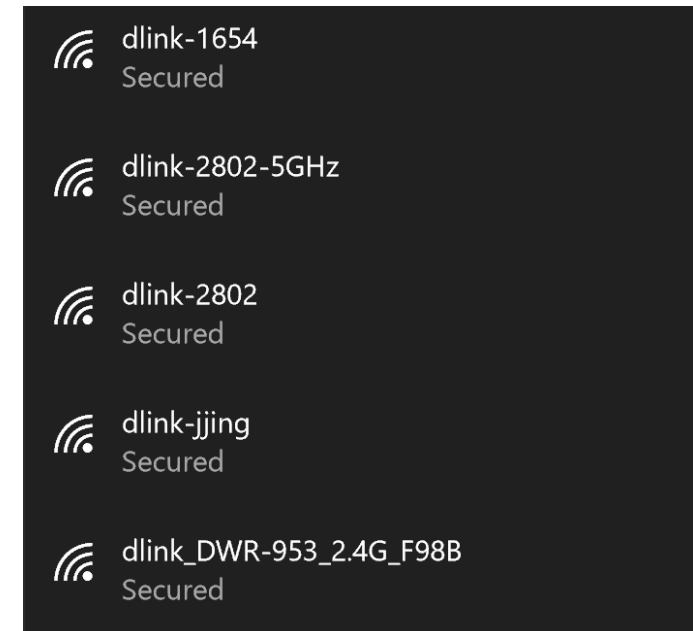
To connect to a wireless network using Windows 10, you will need to know the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to.

To join an existing network, locate the wireless network icon in the taskbar, next to the time display and click on it.



Wireless Icon

Clicking on this icon will display a list of wireless networks which are within range of your computer. Select the desired network by clicking on its SSID.



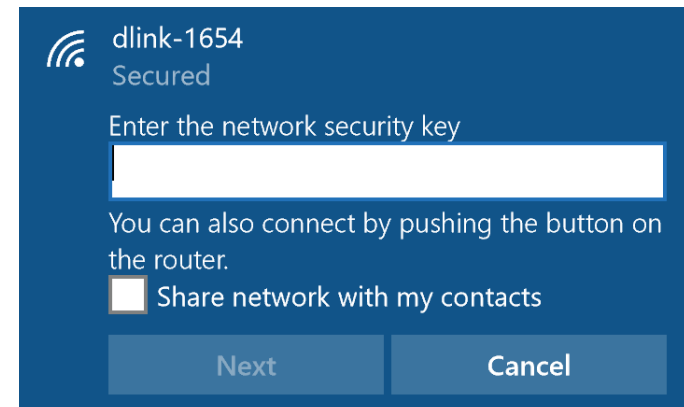
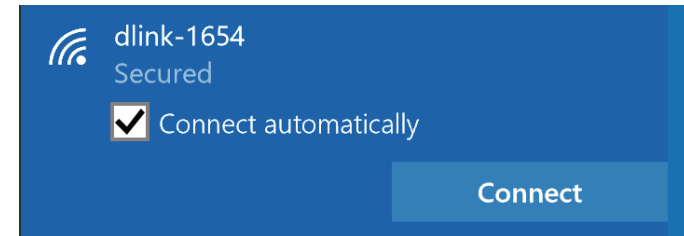
To connect to the network, click **Connect**.

To automatically connect when your device is in range, click the **Connect Automatically** check box. Your computer will now automatically connect to this wireless network whenever it is detected.

You will then be prompted to enter the Wi-Fi password (network security key) for the wireless network. Enter the password into the box and click **Next** to connect to the network.

You can also use Wi-Fi Protected Setup (WPS) to connect to the wireless network. Press the WPS button on your device and you will be automatically connected.

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



# Windows® 8

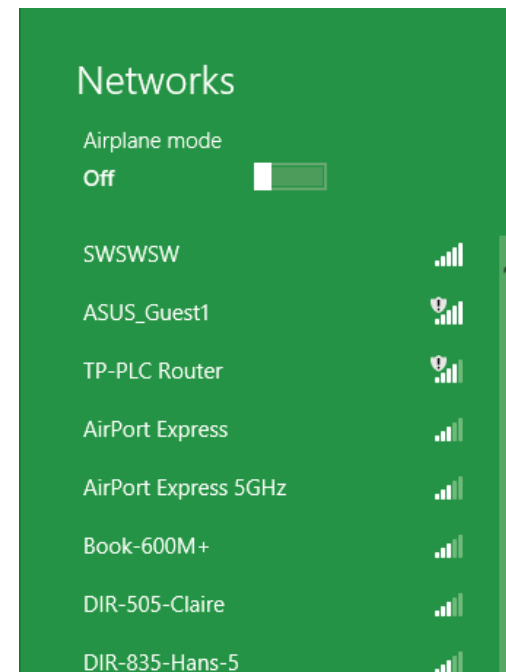
## WPA/WPA2

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

To join an existing network, locate the wireless network icon in the taskbar next to the time display.



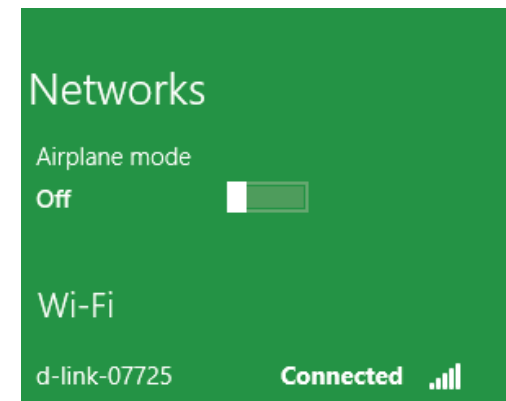
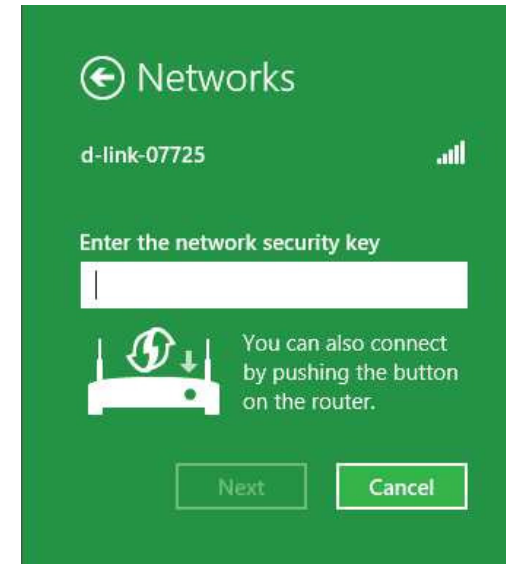
Clicking on this icon will display a list of wireless networks that are within connecting proximity of your computer. Select the desired network by clicking on the network name.



You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router during this step to enable the WPS function.

When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected to.



# Windows® 7

## WPA/WPA2

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

1. Click on the wireless icon in your system tray (lower-right corner).



Wireless Icon

2. The utility will display any available wireless networks in your area.

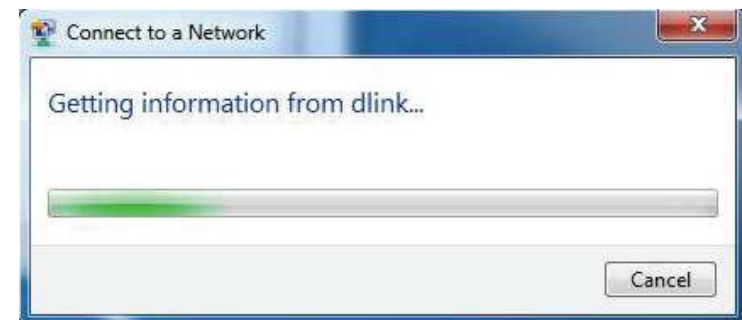


3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to **Networking Basics** on page 88 for more information.



4. The following window appears while your computer tries to connect to the router.





5. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

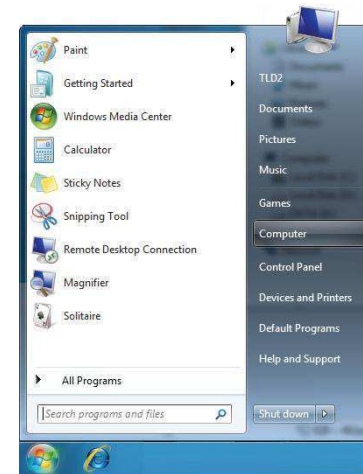
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as the one on the wireless router.



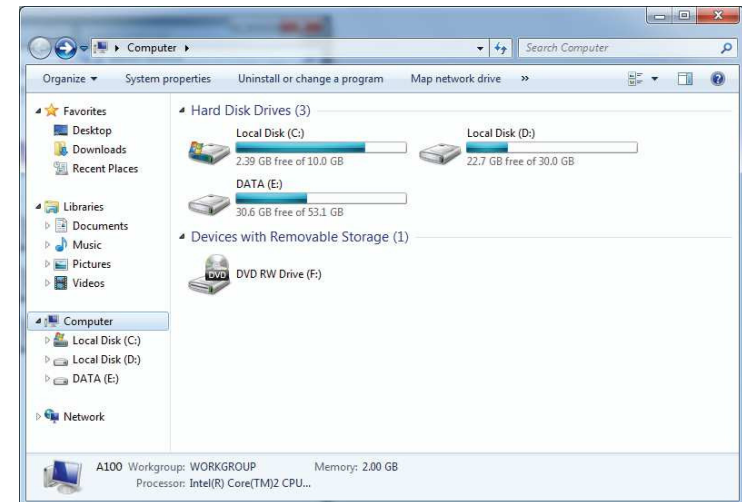
# WPS

The WPS feature of the DWR-922 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

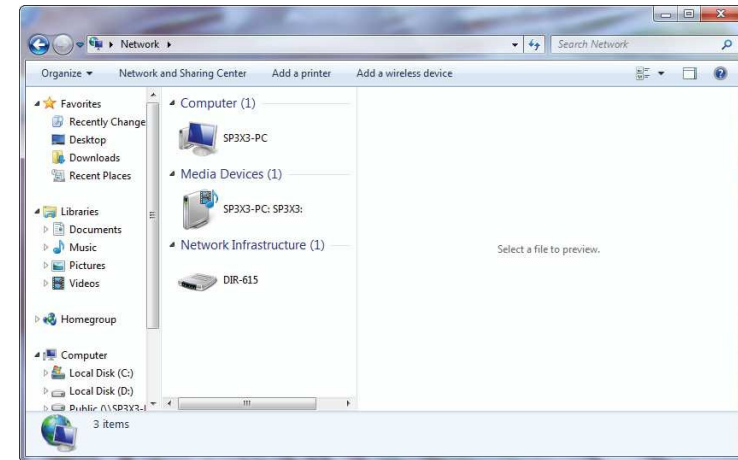
1. Click the **Start** button and select **Computer** from the Start menu.



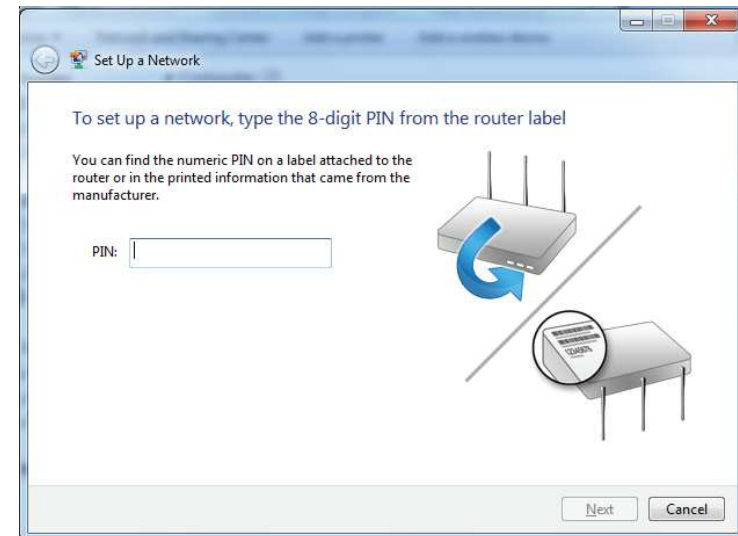
2. Click **Network** on the left side.



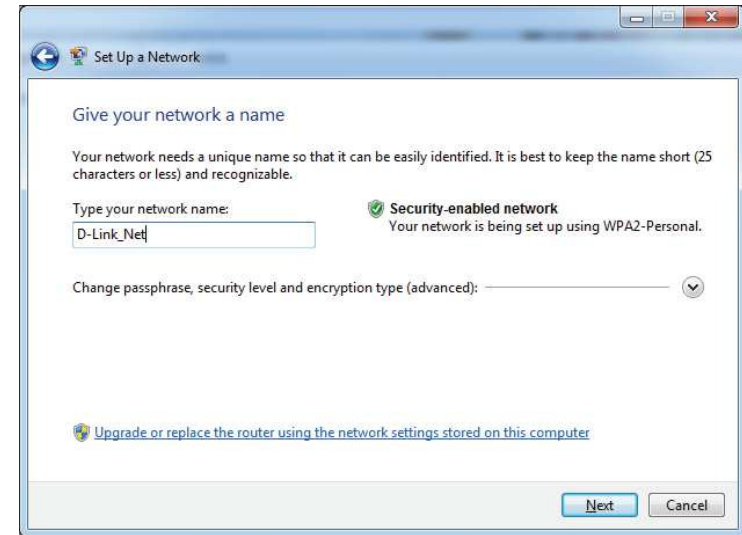
3. Double-click the DWR-922.




4. Input the WPS PIN number (on the router label) in the **Setup > Wireless Setup** menu in the Router's Web UI) and click **Next**.

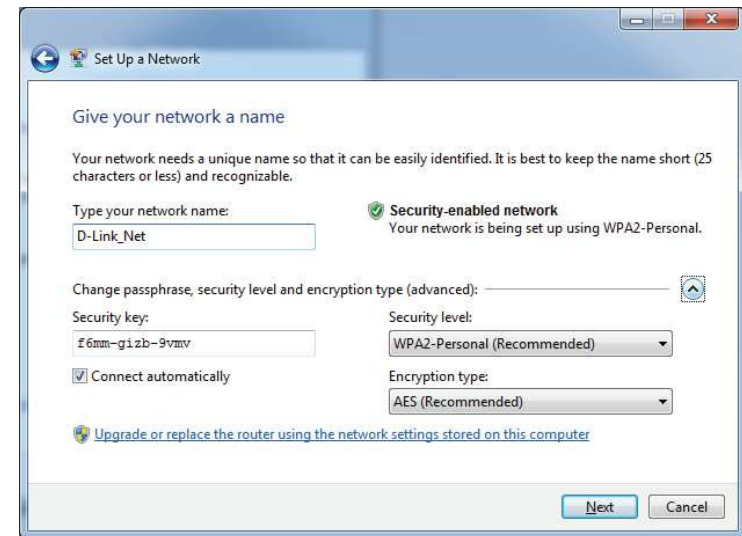


5. Type a name to identify the network.



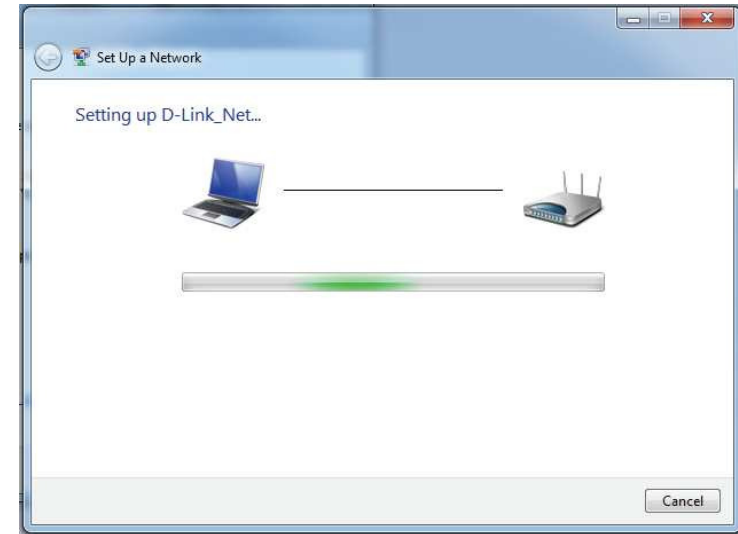
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



7. The following window appears while the router is being configured.

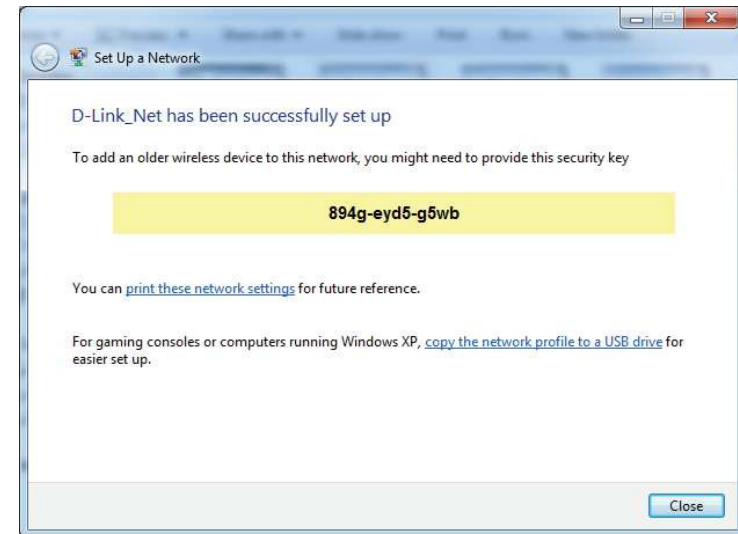
Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been set up successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click **Close** to complete WPS setup.



# Windows Vista®

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

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

or

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

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

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



## WPA/WPA2

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

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

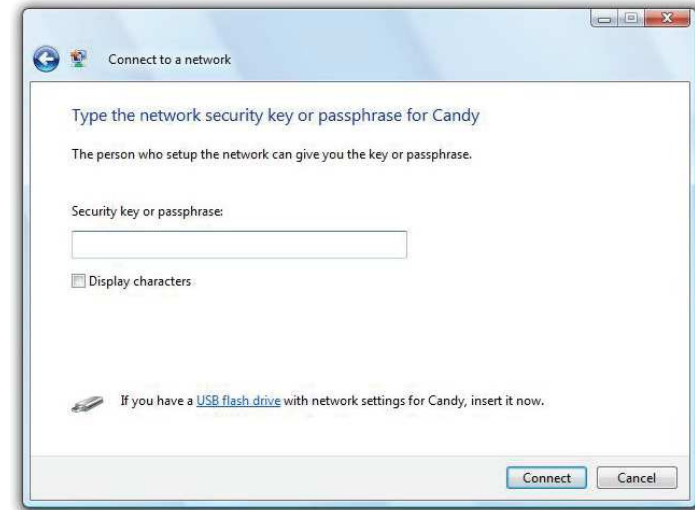


2. Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

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





# 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, 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.

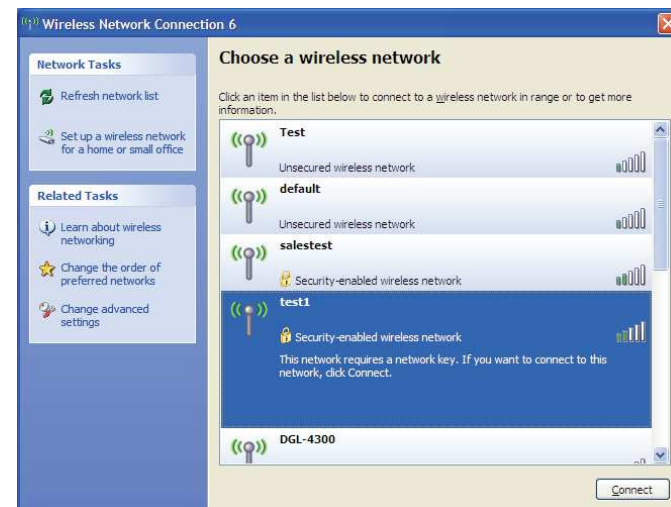
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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 Wi-Fi 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.



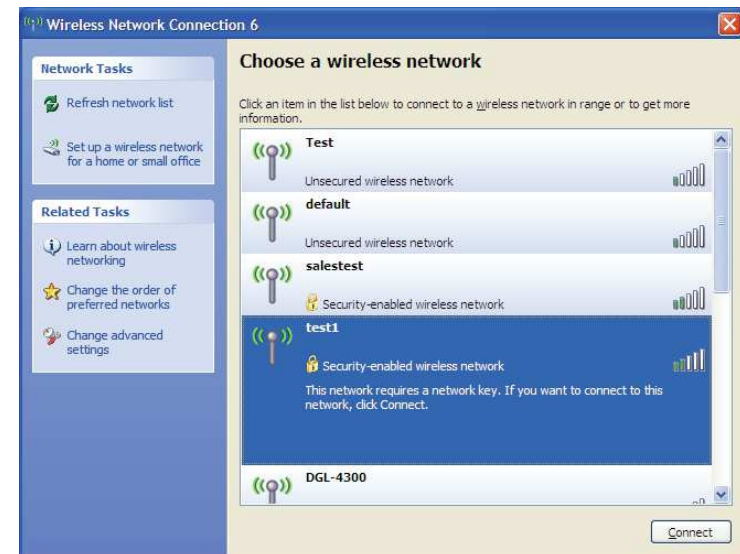
## WPA/WPA2

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

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

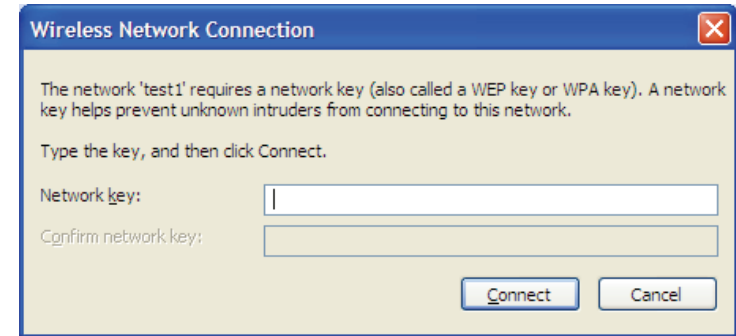


2. Highlight the Wi-Fi network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK Wi-Fi password 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 Wi-Fi password 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 DWR-922. 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 these 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, nor do you 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:
  - Microsoft Internet Explorer® 7 or higher
  - Mozilla Firefox 3.5 or higher
  - Google™ Chrome 8 or higher
  - Apple Safari 4 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 ZoneAlarm, BlackICE, 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 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. 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, 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).

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, XP, Vista®, and 7 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.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
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:

- Navigate to the Internet configuration page (see **Internet** on page 8 for details).
- To change the MTU, enter the number in the MTU field and click **Apply** 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 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 similarly to how cordless phones work, through radio signals that 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 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, university 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. This 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 Uses/Benefits**

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

### **Small Office and Home Office Uses/Benefits**

- 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 the 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 the 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 DWR-922 wireless network CardBus adapters.

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

An ad hoc network contains only clients, such as laptops with wireless CardBus adapters. All the adapters must be in ad hoc mode to communicate.

# Networking Basics

## Check your IP address

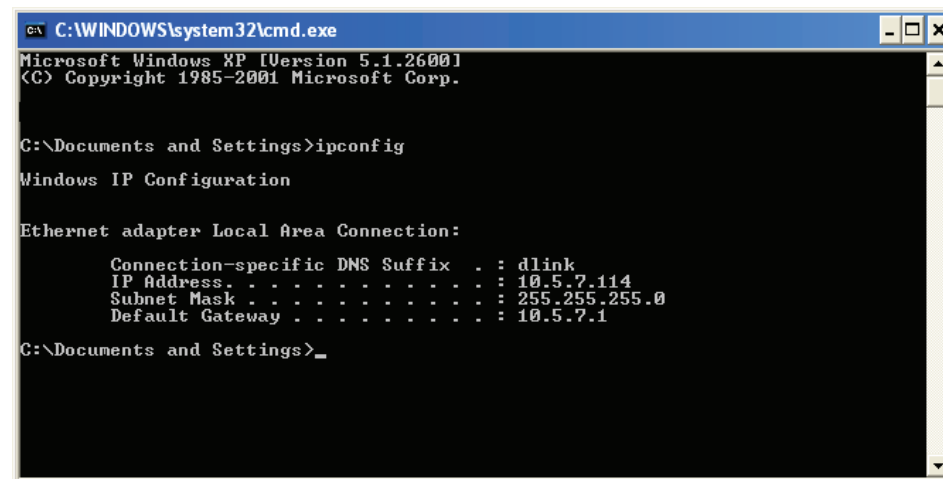
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type **cmd** in the **Start Search** box.)

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

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

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

## Statically Assign an IP address

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

### Step 1

Windows® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.

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

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

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

### Step 2

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

### Step 3

Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

### Step 4

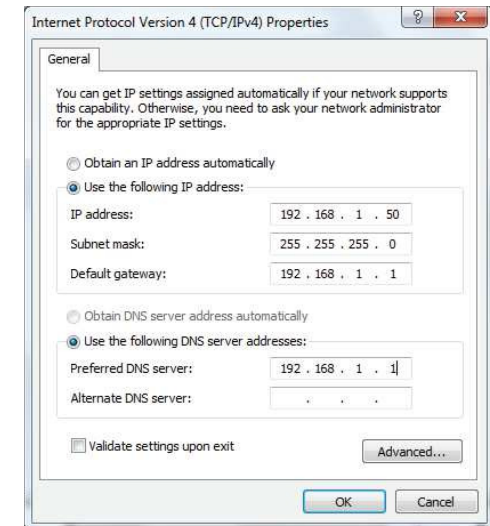
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.1.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 the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.0.1).

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

### Step 5

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



## Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DWR-922 offers the following types of security:

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

### What is WPA?

WPA (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.

# Technical Specifications

## LTE Band<sup>1</sup>

- Category 3: Band 1/2/4/5/7/8/12/17/38
- 
- 

## Pentaband UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+ Band<sup>1</sup>

- 850/900/1700/1900/2100 MHz

## GSM Quad-band<sup>1</sup>

- 850 / 900 / 1800 / 1900 MHz

## Data Rates<sup>2</sup>

- Up to 300 Mbps with 802.11n clients
- 6 / 9 / 11 / 12 / 18 / 24 / 36 / 48 / 54 Mbps in 802.11g mode
- 1 / 2 / 5.5 / 11 Mbps in 802.11b mode
- LTE Uplink: Up to 50 Mbps
- LTE Downlink: Up to 100 Mbps

## Standards

- IEEE 802.11b/g, compatible with IEEE 802.11n devices
- IEEE 802.3i
- IEEE 802.3u

## Wireless Security

- 64 / 128-bit WEP (Wired Equivalent Privacy)
- WPA & WPA2 (Wi-Fi Protected Access)

## Firewall

- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)

## VPN

- L2TP/PPTP/IPSEC/VPN Pass-through

## Antenna

- Two detachable 3G/4G antennas

## Ports

- Four LAN ports (RJ-45)
- WAN port (RJ-45)

## SIM/UICC Slot

- Standard Mini-SIM/UICC slot

## LED Status Indicators

- Power, SMS
- LAN
- WLAN
- 2G / 3G
- 4G
- Signal Strength

## Dimensions

- 190 x 116 x 22.4 mm (7.43 x 4.57 x 0.88 in)

## Operating Temperature

- 0 to 40 °C (32 to 104 °F)

## Operating Humidity

- 10% to 90% (Non-condensing)

## Certifications

- FCC
- RoHS

<sup>1</sup> Supported frequency band is dependent upon regional hardware version.

<sup>2</sup> Maximum wireless signal rate derived from IEEE Standard 802.11g/b/n 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.



# Regulatory Information

## **Federal Communication Commission Interference Statement**

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

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

## **Non-modifications Statement:**

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

## **Caution:**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

## **Note**

The country code selection is for non-USA models only and is not available to all USA models. Per FCC regulations, all WiFi product marketed in the USA must be fixed to USA operational channels only.

**IMPORTANT NOTICE:**

**FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.