



User Manual

4G LTE Router

DWR-921

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.

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 © 2012 by D-Link Corporation, Inc.

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

FCC Regulations

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 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 or more 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.

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

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Table of Contents

Preface	i	PPTP	17
Trademarks	i	L2TP	19
FCC Regulations	ii	3G/4G	20
Product Overview	1	Wireless Settings.....	22
Package Contents.....	1	Wireless Connection Setup Wizard.....	22
System Requirements	1	Manual Wireless Connection Setup	24
Introduction	2	Wireless Settings	25
Hardware Overview	3	Wireless Security Mode	26
Rear Panel.....	3	Wi-Fi Protected Setup (WPS)	29
Front Panel	4	Network Settings	31
LEDs	5	Router Settings.....	31
Installation	6	DHCP Server Settings.....	32
Connect to Your Network	6	Message Service.....	33
Wireless Installation Considerations.....	7	SMS Inbox.....	33
Configuration	8	Create Message	34
Web-based Configuration Utility	8	Advanced	35
Setup	9	Virtual Server	35
Internet.....	9	Application Rules.....	37
Internet Connection Setup Wizard.....	9	QoS Engine.....	38
Manual Internet Connection Setup	12	MAC Address Filter	39
Internet Connection	12	URL Filter.....	40
Static IP	13	Outbound Filter.....	41
Dynamic IP (DHCP)	14	Inbound Filter	42
PPPoE	15	SNMP	43
		Routing.....	44
		Advanced Wireless	45

Advanced Network	46	Wireless Basics	76
Tools	47	What is Wireless?	77
Admin	47	Tips.....	79
Time	48	Wireless Modes.....	80
Syslog	49	Networking Basics	81
E-mail Settings	50	Check your IP address	81
System	51	Statically Assign an IP address	82
Firmware	52	Technical Specifications	83
Dynamic DNS	53		
System Check	54		
Schedules	55		
Status	56		
Device Info	56		
Log	57		
Statistics	58		
Wireless	59		
Support	60		
Connecting to a Wireless Network	61		
Using Windows 7	61		
Configuring Wireless Security	63		
Using Windows Vista™	66		
Configuring Wireless Security	67		
Using Windows® XP	69		
Configure WEP	70		
Configure WPA-PSK.....	72		
Troubleshooting	74		

Product Overview

Package Contents

- D-Link DWR-921 4G LTE Router
- Power adapter
- Manual and Warranty on CD
- (2) Antennas

Note: Using a power supply with a different voltage rating than the one included with the DWR-921 will cause damage and void the warranty for this product.

System Requirements

- A compatible (U)SIM card with service.*
- Computer with Windows, Mac OS, or Linux-based operating system with an installed Ethernet adapter
- Internet Explorer 6 or Firefox 7 or above (for configuration)

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

Introduction

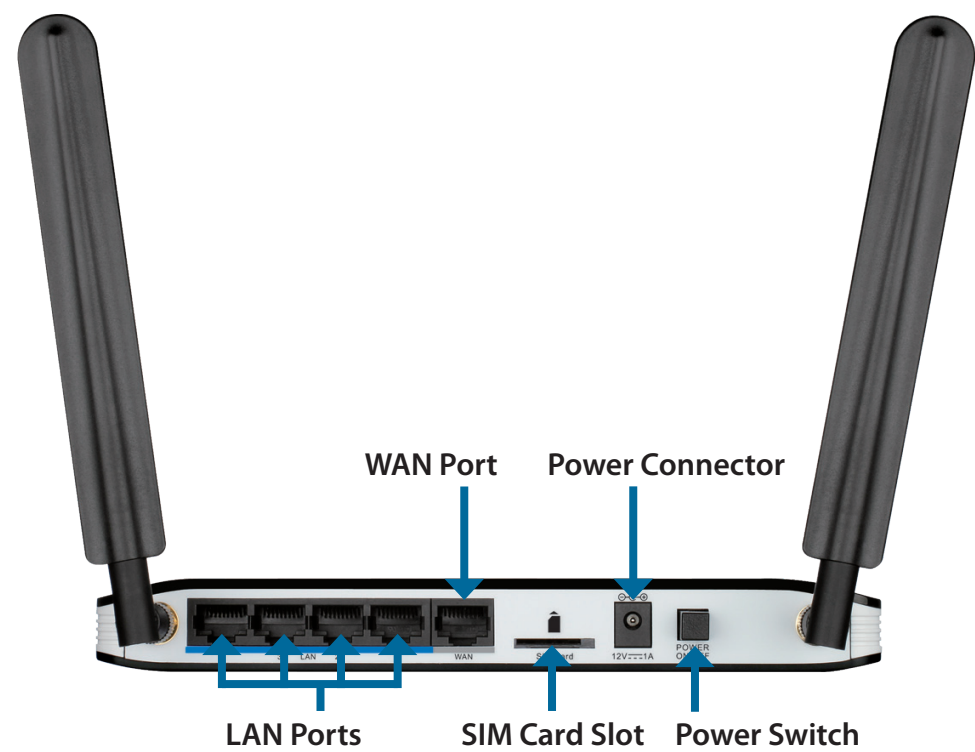
The D-Link 4G LTE Router allows users to access worldwide mobile broadband networks. Once connected, users can transfer data, stream media, and send SMS messages. Simply insert your UMTS/HSUPA SIM card, and share your 3G/4G Internet connection through a secure 802.11n wireless network or using any of the four 10/100 Ethernet ports.

Keep your wireless network safe with WPA/WPA2 wireless encryption. The DWR-921 utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks across the Internet, and includes MAC address filtering to control access to your network.

The 4G LTE Router can be installed quickly and easily almost anywhere. This router is great for situations where an impromptu wireless network must be set up, or wherever conventional network access is unavailable. The DWR-921 can even be installed in buses, trains, or boats, allowing passengers to check e-mail or chat online while commuting.

Hardware Overview

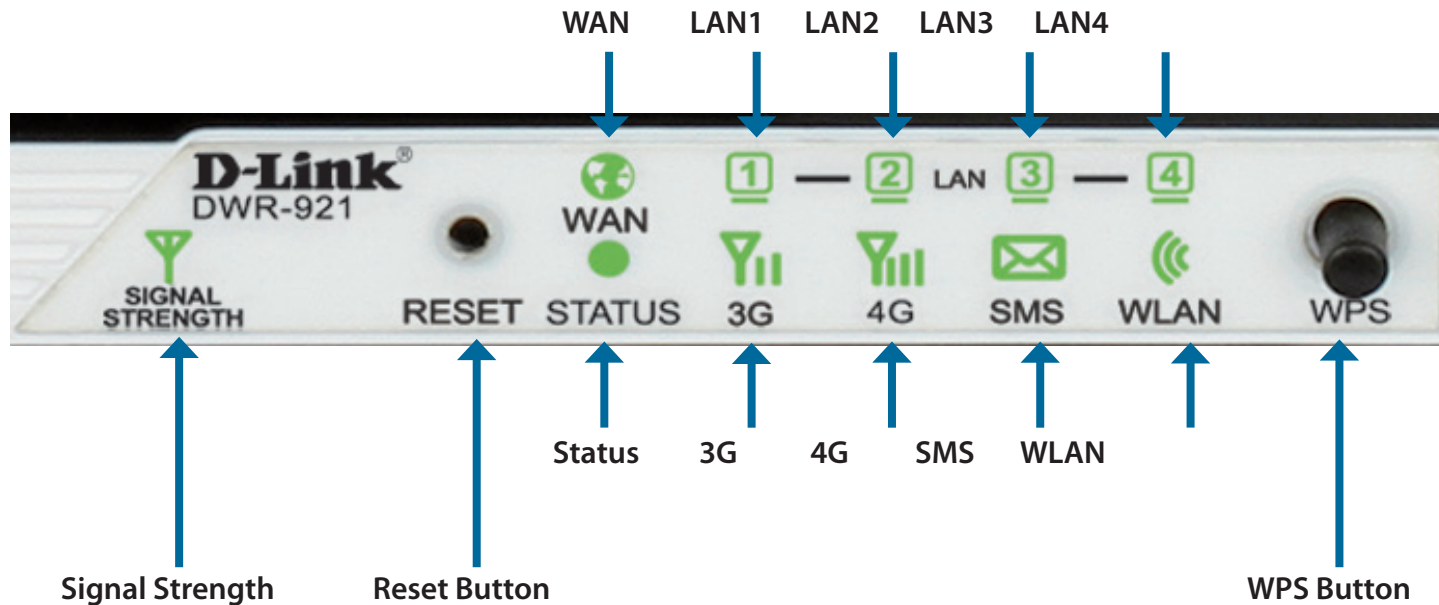
Rear Panel



Port	Function
LAN Ports (RJ-45)	Connects to a network device such as a desktop or notebook computer through an Ethernet cable.
WAN Port (RJ-45)	Connects to a DSL/Cable modem or router through an Ethernet cable.
SIM	Accepts a standard (U)SIM card for 3G/4G connectivity.
Power	Connects to the included power adapter.
Power Switch	Turns the device on or off.

Hardware Overview

Front Panel



Button Name	Function
Reset	Press this button with an unfolded paperclip to reset the device.
WPS	Press this button to initiate a new WPS connection. Refer to "Wi-Fi Protected Setup" on page 29 for more details.

Hardware Overview

LEDs

LED Name	Function
Signal Strength	Blinking Red: No SIM card / signal or unverified PIN code Solid Red: Signal strength is at level one (weak) Solid Amber: Signal strength is at level two or three (medium) Solid Green: Signal strength is at level four or five (strong)
Status	Blinking Green: Device is working
WAN	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
LAN 1-4	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
Status	Blinking Green: Device is working
3G	Solid Green: UMTS/HSDPA/HSUPA connection has been established Blinking Green: Data is being transferred via 3G
4G	Solid Green: LTE connection has been established Blinking: Data is being transferred via 4G
SMS	Solid Green: SMS storage is full Blinking Green: There is an unread SMS message
WLAN	Solid Green: WLAN is active and available Blinking Green: Data is being transferred over the WLAN

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.

Connect to Your Network

1. Ensure that your DWR-921 4G LTE Router is disconnected and powered off.
2. Insert a standard (U)SIM card into the SIM card slot on the back of the router as indicated by the SIM card logo next to the slot. The gold contacts should face downwards.

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

3. Insert your Internet/WAN network cable into the WAN port on the back of the router.

Note: The 3G/4G connection can also be used as a backup WAN. Once a backup is configured, the router will automatically use 3G for the Internet connection if the Ethernet WAN is not available.

4. Insert the Ethernet cable into the LAN Port 1 on the back panel of the DWR-921 4G LTE Router and an available Ethernet port on the network adapter in the computer you will use to configure the router.

Note: The DWR-921 4G LTE Router LAN Ports are Auto-MDI/MDIX, so both patch and crossover Ethernet cables can be used.

5. Connect the power adapter to the socket on the back panel of your DWR-921 4G LTE Router. Plug the other end of the power adapter into a wall outlet or power strip and turn the device on.
 - a. The Status LED will light up to indicate that power has been supplied to the router.
 - b. The LEDs on the front panel will flash on and off as the DWR-921 4G LTE 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, Status, WAN, WLAN, and any LAN Port LEDs that are connected computers or other devices.

Wireless Installation Considerations

The DWR-921 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:

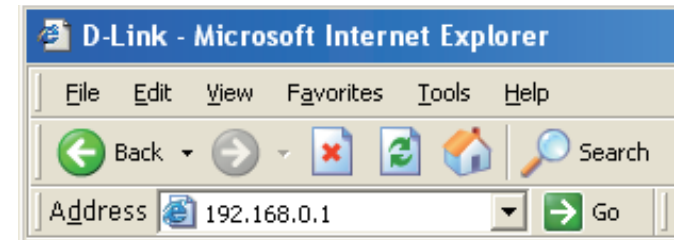
1. Minimize the number of walls and ceilings between the D-Link router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree 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

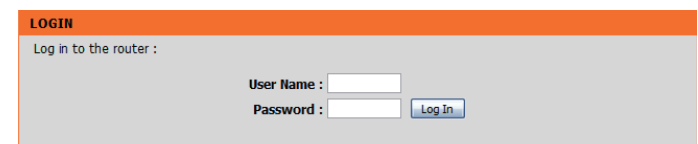
This section will show you how to configure your new D-Link mobile router using the web-based configuration utility.

Web-based Configuration Utility

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



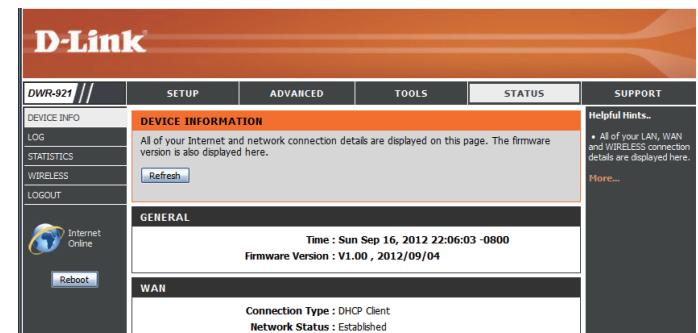
To log in to the configuration utility, enter **admin** as the username, and then enter the password. By default, the password is blank.



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

The configuration utility will open to the **STATUS > DEVICE INFO** page. You can view different configuration pages by clicking on the categories at the top of the screen (SETUP/ADVANCED/TOOLS/STATUS/SUPPORT), and then selecting a configuration page from the bar on the left side.

The following pages will describe each section in detail, starting with the **SETUP** pages.



Setup

The **SETUP** pages allow you to configure your Internet and wireless settings, as well as manage your SMS inbox. To view the Setup configuration pages, click on **SETUP** at the top of the screen.

Internet

The Internet page allows you to configure how your router connects to the Internet. There are two ways to set up your Internet connection.

You can click on the **Internet Connection Setup Wizard** button to start a wizard that will guide you through setting up your Internet settings.

If you want to manually configure your settings, click **Manual Internet Connection Setup** and skip to “Manual Internet Connection Setup” on page 12.

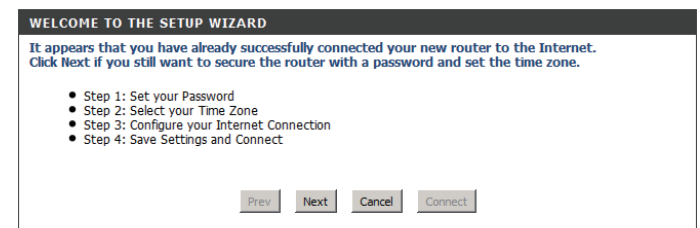


Internet Connection Setup Wizard

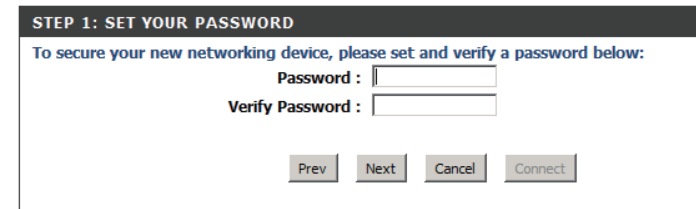
This wizard will guide you through a step-by-step process to configure your D-Link router to connect to the Internet.

Click **Next** to continue.

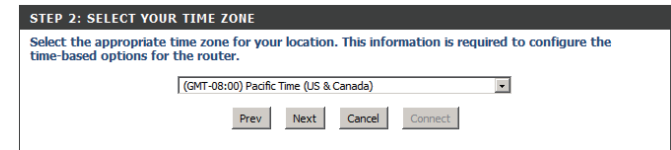
Note: While using the wizard, you can click **Prev** to go back to the previous step, or you can click **Cancel** to close the wizard.



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



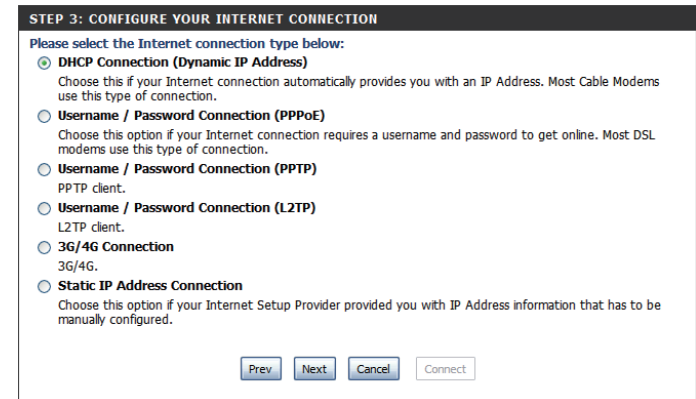
Select your time zone from the drop-down box and then click **Next** to continue.



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-921 has a 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 “Internet Connection” on page 12.



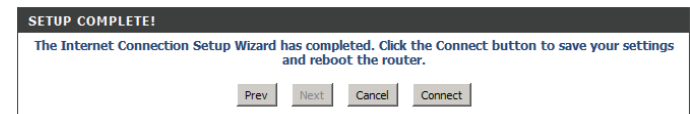
The subsequent configuration pages will differ depending on the selection you make on this page.

- 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. See “Dynamic IP (DHCP)” on page 14 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” on page 15 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 17 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 19 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-921. See “3G/4G” on page 20 for information about how to configure this type of connection.
- Static IP Address Connection:** Choose this option if your Internet Service Provider provided you with IP Address information that has to be manually configured. See “Static IP” on page 13 for information about how to configure this type of connection.

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

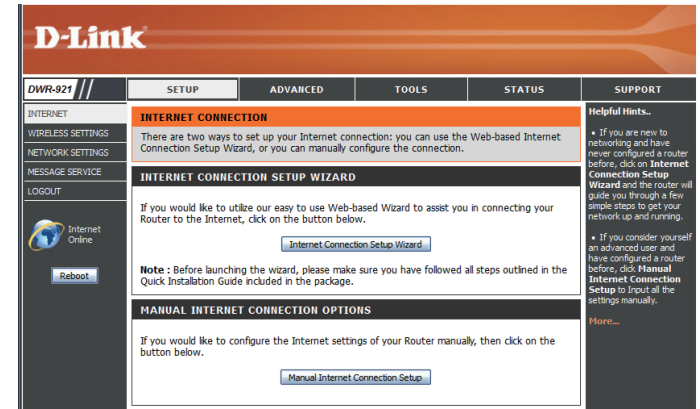
Note: If you are not sure what connection type to use or what settings to enter, check with your Internet service provider.

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



Manual Internet Connection Setup

To set up your Internet connection manually, click **Manual Internet Connection Setup**.



Internet Connection

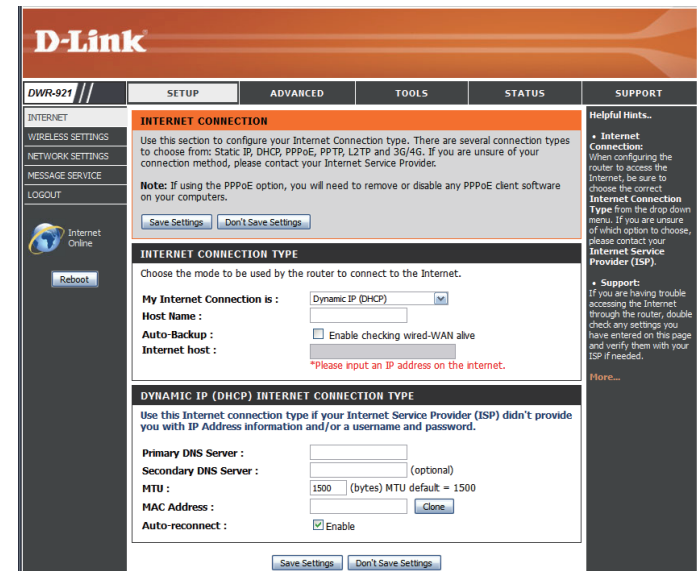
Several different Internet Connection types can be selected depending upon the specifications of your Internet Service Provider (ISP). You can also set up the Auto-Backup feature, which allows you to use a 3G/4G connection for your Internet connection if your main connection fails.

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

Host Name: If the Internet Host you are using for the Auto-Backup feature requires you to enter a Host Name, enter it here. In most cases, you may leave this blank.

Auto-Backup: When this box is checked, the router will switch over to a 3G/4G connection if the Internet Host (specified below) is unreachable.

Internet Host: Enter an IP address for the router to use to check if it is connected to the Internet. If Auto-Backup is enabled and the IP address cannot be reached, the router will switch over to a 3G/4G connection.



Static IP

Choose this Internet connection if your ISP assigns you a static IP address. After modifying any settings, click **Save Settings** to save your changes.

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 1500.

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

STATIC IP ADDRESS INTERNET CONNECTION TYPE	
Enter the static address information provided by your Internet Service Provider (ISP).	
IP Address :	<input type="text"/>
Subnet Mask :	<input type="text"/>
Default Gateway :	<input type="text"/>
Primary DNS Server :	<input type="text"/>
Secondary DNS Server :	<input type="text"/>
MTU :	<input type="text" value="1500"/> (bytes) MTU default = 1500
MAC Address :	<input type="text"/> <input type="button" value="Clone"/>

Dynamic IP (DHCP)

This section will help you to obtain IP Address information automatically from your ISP. Use this option if your ISP didn't provide you with IP Address information and/or a username and password. After modifying any settings, click **Save Settings** to save your changes.

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

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

Auto-reconnect: This feature enables this product to renew the WAN IP address automatically when the lease time has expired.

The screenshot shows a web interface for configuring a Dynamic IP (DHCP) Internet connection. The title is "DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE". Below the title is a note: "Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password." The configuration fields are: "Primary DNS Server:" with an empty text box; "Secondary DNS Server:" with an empty text box and "(optional)" text; "MTU:" with a text box containing "1500" and "(bytes) MTU default = 1500"; "MAC Address:" with an empty text box and a "Clone" button; and "Auto-reconnect:" with a checked checkbox and the label "Enable". At the bottom are two buttons: "Save Settings" and "Don't Save Settings".

PPPoE

Choose this Internet connection if your ISP provides you with a PPPoE account. After modifying any settings, click **Save Settings** to save your changes.

Username: The username/account name that your ISP provides to you for PPPoE dial-up.

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

Verify Password: Fill in with the same password in Password field.

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

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

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

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

MAC Address: MAC address of WAN interface. You can also copy MAC address of your PC to its WAN interface by clicking the **Clone** button.

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

PPPoE

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

Username :

Password :

Verify Password :

Service Name : (optional)

IP Address :

Primary DNS Server : (optional)

Secondary DNS Server : (optional)

MAC Address :

Maximum Idle Time : seconds

MTU : (bytes) MTU default = 1492

Auto-reconnect : ☐ Enable

- Maximum Transmission Unit (MTU):

The default setting of PPPoE is 1492.
- Auto-reconnect:

The device will automatically reconnect to your PPPoE connection automatically.

PPPOE

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

Username :

Password :

Verify Password :

Service Name :

(optional)

IP Address :

Primary DNS Server :

(optional)

Secondary DNS Server :

(optional)

MAC Address :

Clone

Maximum Idle Time :

300

seconds

MTU :

1492

(bytes) MTU default = 1492

Auto-reconnect :

☐ Enable

Save Settings

Don't Save Settings

PPTP

Choose this Internet connection if your ISP provides you with a PPTP account. After modifying any settings, click **Save Settings** to save your changes.

Address Mode: Choose Static IP only if your ISP assigns you an IP address. 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 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 surf Internet, and disconnect if there is no traffic after the time period defined by the **Maximum Idle Time** setting.

The screenshot shows a 'PPTP' configuration window with the title 'Enter the information provided by your Internet Service Provider (ISP)'. The window contains the following fields and options:

- Address Mode :** Radio buttons for 'Dynamic IP' and 'Static IP' (selected).
- PPTP IP Address :** Text input field.
- PPTP Subnet Mask :** Text input field.
- PPTP Gateway IP Address :** Text input field.
- PPTP Server IP Address :** Text input field.
- Username :** Text input field.
- Password :** Text input field.
- Verify Password :** Text input field.
- Reconnect Mode :** Radio buttons for 'Always-on' (selected) and 'Connect-on-demand'.
- Maximum Idle Time :** A numeric input field set to '300' followed by the text 'seconds'.

At the bottom of the window are two buttons: 'Save Settings' and 'Don't Save Settings'.

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.

PPTP

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

Address Mode :

☐ Dynamic IP ☒ Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode :

☒ Always-on ☐ Connect-on-demand

Maximum Idle Time :

300

seconds

Save Settings

Don't Save Settings

L2TP

Choose this Internet connection if your ISP provides you with an L2TP account. After modifying any settings, click **Save Settings** to save your changes.

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 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: Fill in with the same password in Password field.

Reconnect Mode: Choose Always-on when you want to establish L2TP connection all the time. Choose Connect-on-demand the device will establish L2TP connection when local users want to surf 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 'L2TP' configuration window. At the top, it says 'Enter the information provided by your Internet Service Provider (ISP)'. Below this, there are several fields and options:

- Address Mode :** Two radio buttons: 'Dynamic IP' (unselected) and 'Static IP' (selected).
- L2TP IP Address :** A text input field.
- L2TP Subnet Mask :** A text input field.
- L2TP Gateway IP Address :** A text input field.
- L2TP Server IP Address :** A text input field.
- Username :** A text input field.
- Password :** A text input field.
- Verify Password :** A text input field.
- Reconnect Mode :** Two radio buttons: 'Always-on' (selected) and 'Connect-on-demand' (unselected).
- Maximum Idle Time :** A numeric input field with '300' entered and the unit 'seconds'.

At the bottom right, there are two buttons: 'Save Settings' and 'Don't Save Settings'.

3G/4G

Choose this Internet connection if you already use a SIM card for 3G/4G Internet service from your mobile service company. The fields here may not be necessary for your connection. The information on this page should only be used if required by your service provider. After modifying any settings, click **Save Settings** to save your changes.

Prefer Service Type: Choose whether the DWR-921 should only use 4G networks, 3G networks, or use Auto Mode to automatically select a network.

Account/Profile Name: Fill in a name to identify the following 3G/4G configuration.

Country/Telecom: Select your country and telecom to automatically fill in some of the required settings.

Username: (Optional) Fill in only if requested by ISP.

Password: (Optional) Fill in only if requested by ISP.

Dialed Number: Enter the number to be dialed.

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

APN: (Optional) Enter the APN information.

Pin Code: Enter the PIN associated with your SIM card.

Reconnect Mode: Select Auto or Manual to decide 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.

3G/4G INTERNET CONNECTION TYPE

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

Prefer Service Type :

Dial-Up Profile : ☐ Auto-Detection ☒ Manual

Country :

Telecom :

3G Network :

Account/Profile Name :

Username : (optional)

Password : (optional)

Verify Password : (optional)

Dialed Number :

Authentication :

APN :

Pin Code :

Reconnect Mode : ☒ Auto ☐ Manual

Maximum Idle Time : seconds

Primary DNS Server :

Secondary DNS Server :

Keep Alive : ☒ Disable ☐ Use Ping

Bridge ethernet ports : ☐ Enable

Roaming : ☐ Enable

DNS check : ☒ Enable

NAT disable : ☐ Enable

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

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

Keep Alive: Select Disable or Use Ping depending on the settings required by your ISP. If you select Use Ping, set the ping interval and the IP address to ping.

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

Roaming: Enabling this option will allow you to connect when roaming.

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

DNS Check: Enabling this will send periodic DNS checks to make sure your connection is alive, and if the check fails, it will restart your 3G connection to resume connectivity.

NAT Disable: Enabling this option will disable the NAT function of the DWR-921, allowing it to act as a link for your devices to your Internet connection, but without routing functions.

3G/4G INTERNET CONNECTION TYPE

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

Prefer Service Type :

Dial-Up Profile : ☐ Auto-Detection ☒ Manual

Country :

Telecom :

3G Network :

Account/Profile Name :

Username : (optional)

Password : (optional)

Verify Password : (optional)

Dialed Number :

Authentication :

APN :

Pin Code :

Reconnect Mode : ☒ Auto ☐ Manual

Maximum Idle Time : seconds

Primary DNS Server :

Secondary DNS Server :

Keep Alive : ☒ Disable ☐ Use Ping

Bridge ethernet ports : ☐ Enable

Roaming : ☐ Enable

DNS check : ☒ Enable

NAT disable : ☐ Enable

Wireless Settings

This section will help you to manually configure the wireless settings of your router. Please note that changes made on this section may also need to be duplicated on your wireless devices and clients.

The Wireless Settings page allows you to configure how your router connects to the Internet. There are several ways to set up your wireless connection.

You can click on the **Wireless Connection Setup Wizard** button to start a wizard that will guide you through setting up your wireless settings.

If you want to manually configure your settings, click the **Manual Wireless Connection Setup** button and skip to “Manual Wireless Connection Setup” on page 24.

You can also set up a wireless connection to a device automatically, or configure your router automatically through Windows by clicking the **Wi-Fi Protected Setup** button. This is described in “Wi-Fi Protected Setup (WPS)” on page 29.



Wireless Connection Setup Wizard

This wizard will guide you through a step-by-step process to configure your D-Link router's wireless .

Click **Next** to continue.

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



Enter a name for your wireless network, then click **Next** to continue.

Select a level of wireless security to use, then click **Next** to continue.

If you chose **BEST** or **BETTER**, select whether to use TKIP or AES encryption, then enter a password to use for your wireless network. It is recommended that you use AES if your wireless computers and devices support it, as it is more secure. Click **Next** to continue.

If you chose **GOOD**, select whether to use a HEX or ASCII password, then enter a password to use for your wireless network. If you choose HEX, you will need to enter a 10 or 26 digit password using only hex characters (0-9, A-F). If you choose ASCII, the password can be up to 5 or 13 alphanumeric characters. Click **Next** to continue.

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

STEP 1: NAME YOUR WIRELESS NETWORK

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

Wireless Network Name (SSID) :

STEP 2: SECURE YOUR WIRELESS NETWORK

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

There are three levels of wireless security - Good Security, Better Security, 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

BETTER : ☐ Select this option if your wireless adapters SUPPORT WPA

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

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

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

Note: All wireless adapters currently support WPA.

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

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.

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

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.

SETUP COMPLETE!

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

Wireless Network Name (SSID) :

Manual Wireless Connection Setup

To set up your wireless connection manually, click **Manual Wireless Connection Setup**.



Wireless Settings

This page lets you set up your wireless network and choose a wireless security mode. After modifying any settings, click **Save Settings** to save your changes.

Enable Wireless: Select this checkbox to enable wireless access. When you set 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: **B/G mixed:** Enable this mode if your network contains a mix of 802.11b and 802.11g devices.

N only: Enable this mode if your network only has 802.11n devices.

B/G/N mixed: Enable this mode if you have a mix of 802.11n, 802.11g, and 802.11b clients.

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

Wireless Channel: A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may experience interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network, or enable Auto Channel Scan for the router to automatically select the best channel.

Visibility Status: This setting determines whether the SSID will be **Visible** or **Invisible** to wireless clients looking for wireless networks. Setting this to **Invisible** can increase the security of your network by hiding it, but clients will need to manually enter the SSID of your network to connect.

D-Link

DWR-921 // SETUP ADVANCED TOOLS STATUS SUPPORT

WIRELESS NETWORK

Use this section to configure the wireless settings for this device. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Network Name : My D-Link Network (Also called the SSID)

802.11 Mode : B/G/N mixed

Auto Channel Scan : ☒

Wireless Channel : 11 (Auto)

Visibility Status : ☒ Visible ☐ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

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

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

WPA Mode : WPA2 only

Cipher Type : AES

Helpful Hints...

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enabling Hidden Mode is another way to secure your network. With the option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

More...

Wireless Security Mode

You can choose from several different wireless security modes. After selecting a mode, the settings for that mode will appear. After modifying any settings, click **Save Settings** to save your changes.

Security Mode: You can choose from 4 different security modes.

- **None:** No security will be used. This setting is not recommended.
- **WEP:** WEP encryption will be used. This setting is only recommended if your wireless devices cannot support WPA or WPA2.
- **WPA-Personal:** WPA-PSK encryption will be used. This setting is recommended for most users.
- **WPA-Enterprise:** WPA-EAP encryption will be used. This setting is only recommended if you have a RADIUS authentication server. Otherwise, **WPA-Personal** should be used.

D-Link

DWR-921 // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
WIRELESS SETTINGS
NETWORK SETTINGS
MESSAGE SERVICE
LOGOUT

Internet Online
Reboot

WIRELESS NETWORK

Use this section to configure the wireless settings for this device. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Network Name : My D-Link Network (Also called the SSID)

802.11 Mode : B/G/N mixed

Auto Channel Scan : ☒

Wireless Channel : 2.412 GHz - CH 1

Visibility Status : ☒ Visible ☐ Invisible

WIRELESS SECURITY MODE

Security Mode : WPA Personal

WPA

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

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

WPA Mode : WPA2 only

Cipher Type : AES

Helpful Hints...

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Here...

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

Authentication: Select whether to use Open or Shared authentication.

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

Default WEP Key: Select which WEP key (1-4) to use as the default key. This will also change the WEP Key text box to that WEP key for your to configure(1-4).

WEP Key: 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.

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

Authentication : Open
WEP Encryption : 64Bit
Default WEP Key : WEP Key 1
WEP Key : HEX 1234567890
(5 ASCII or 10 HEX)

Save Settings Don't Save Settings

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

WPA Mode: Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can 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.

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

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

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

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

WPA Mode : WPA only
Cipher Type : AES

PRE-SHARED KEY

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

Network Key : 7c9aeccad9c6b0c05343ed8874754b747ffd
(8~63 ASCII or 64 HEX)

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

WPA Mode: Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can 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.

RADIUS Server IP Address: Enter the IP address of your RADIUS server.

RADIUS Server Port: Enter the port used for your RADIUS server.

RADIUS Server Shared Secret: Enter the Shared Secret/password for your RADIUS server.

WIRELESS SECURITY MODE	
Security Mode :	WPA-Enterprise ▼
WPA	
<p>Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.</p> <p>To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).</p>	
WPA Mode :	WPA only ▼
Cipher Type :	AES ▼
EAP (802.1X)	
<p>When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.</p>	
RADIUS Server IP Address :	0.0.0.0
RADIUS server Port :	1812
RADIUS server Shared Secret :	

Wi-Fi Protected Setup (WPS)

To open the Wi-Fi Protected Setup page, click **Wi-Fi Protected Setup**.



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.

You can also use Windows 7 to do initial configuration of your router by using the **Connect to a network** wizard in Windows, and entering the WPS PIN/AP PIN of the router when prompted. After modifying any settings, click **Save Settings** to save your changes.



WPS: Select whether you would like to enable or disable WPS features.

AP PIN (also known as WPS PIN): If you use Windows 7's **Connect to a network** wizard to do initial configuration of the router, you will need 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.

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 need 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.

The screenshot displays the 'WI-FI PROTECTED SETUP' interface. It includes the following elements:

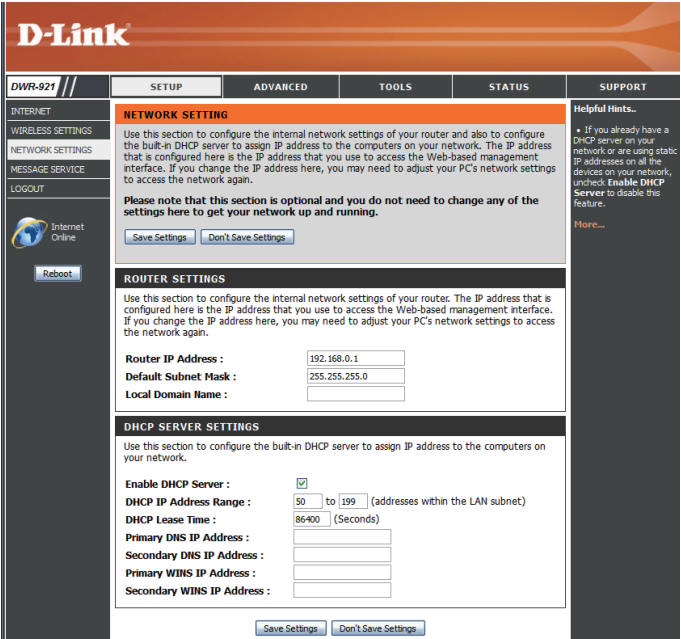
- WPS :** Radio buttons for 'Enable' (selected) and 'Disable'.
- AP PIN :** The value '48757751' is shown next to a 'Generate New PIN' button.
- Config Mode :** A dropdown menu currently set to 'Registrar'.
- Config Status :** The status is 'UNCONFIGURED', with a 'Set' button next to it.
- Disable WPS-PIN Method :** A checkbox that is checked.
- Config Method :** A dropdown menu set to 'Push Button'.
- WPS status :** The status is 'IDLE', with a 'Trigger' button next to it.
- At the bottom, there are two buttons: 'Save Settings' and 'Don't Save Settings'.

Network Settings

This section will help you to change the internal network settings of your router and to configure the DHCP Server settings. After modifying any settings, click **Save Settings** to save your changes.

Router 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.



DHCP Server Settings

The DWR-921 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 is automatically assigned to the clients on the network. After modifying any settings, click **Save Settings** to save your changes.

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.

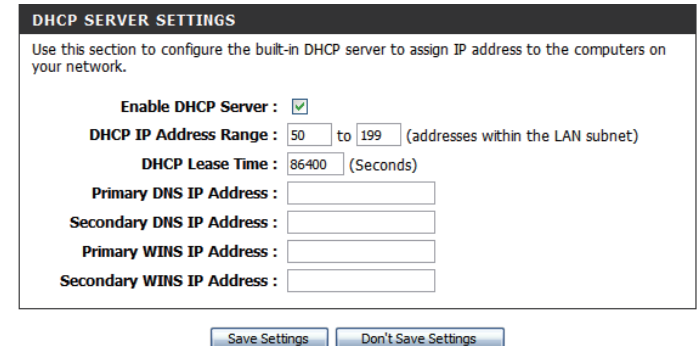
DHCP Lease Time: Enter lease time for IP address assignments.

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.

Primary WINS IP Address: Enter the primary WINS IP Address that will be assigned to DHCP clients.

Secondary WINS IP Address: Enter the secondary WINS IP Address that will be assigned to DHCP clients.



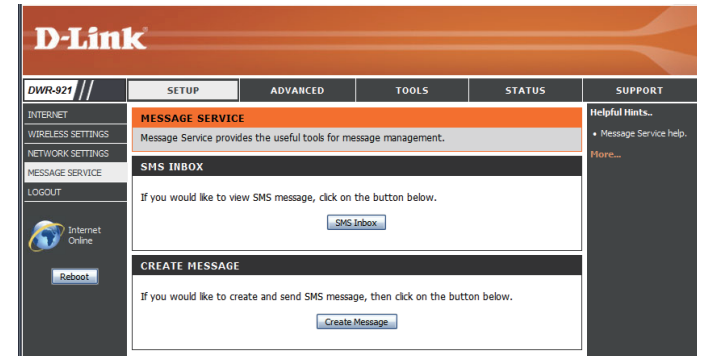
The screenshot shows the 'DHCP SERVER SETTINGS' configuration page. At the top, it says 'Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.' Below this, there are several settings: 'Enable DHCP Server' is checked with a green box; 'DHCP IP Address Range' is set to '50' to '199' with a note '(addresses within the LAN subnet)'; 'DHCP Lease Time' is set to '86400' with a note '(Seconds)'; 'Primary DNS IP Address', 'Secondary DNS IP Address', 'Primary WINS IP Address', and 'Secondary WINS IP Address' are all empty text input fields. At the bottom right, there are two buttons: 'Save Settings' and 'Don't Save Settings'.

Message Service

If your ISP provides **SMS** service, you can check and send messages from this page.

SMS Inbox: Click this button to view SMS messages that you have received.

Create Message: Click this button to create a new message to send.



SMS Inbox

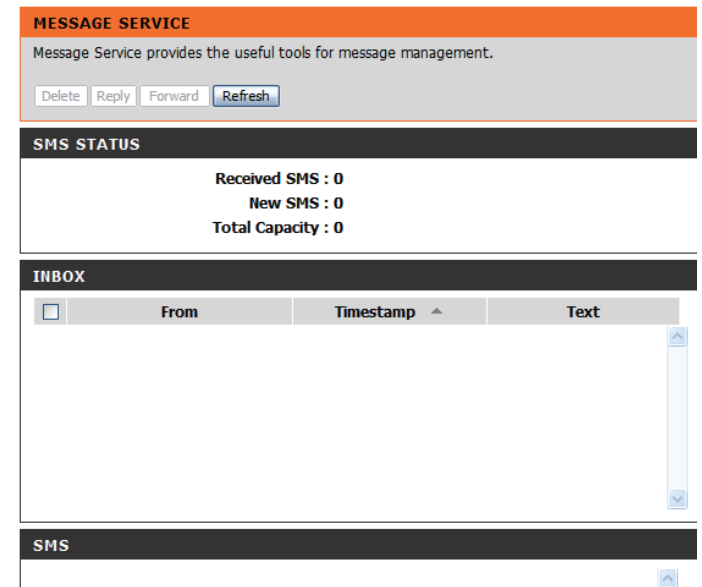
This page shows all messages that are stored on the SIM card. Select a message to display its contents in the SMS window. After you read it, you can delete it, or reply to the sender. Click the **Refresh** button to update the list.

Delete: Deletes the selected SMS message.

Reply: Opens a Create Message window to reply to the selected SMS message.

Forward: Opens a Create Message windows to forward the selected SMS message to another recipient.

Refresh: Click this button to check for new messages.



Create Message

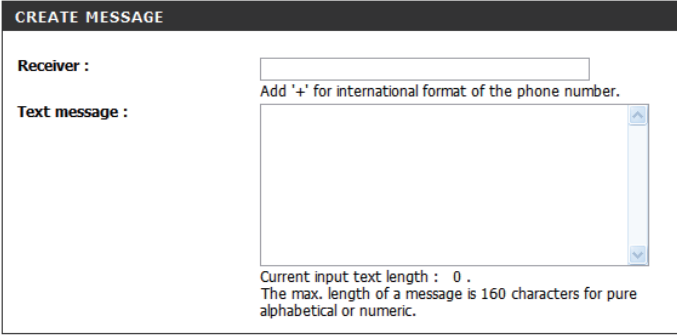
This page allows you to send an SMS to your contacts. Just fill in the phone number of the recipient, and type the content of message. Then push the "Send Message" button to send out this message. If you would like to add more than one recipient, you must put a semicolon (;) between each of the phone numbers.

Receiver: Type the phone number of the recipient.

Text Message: Type the message that you would like to send.

Send Message: Click this button to send the message.

Cancel: Click this button to clear the message.



The screenshot shows a web form titled "CREATE MESSAGE". It has two main input areas: "Receiver :" with a text box and a hint "Add '+' for international format of the phone number.", and "Text message :" with a larger text area. Below the text area, it says "Current input text length : 0 ." and "The max. length of a message is 160 characters for pure alphabetical or numeric." At the bottom, there are two buttons: "Send message" and "Cancel".

Advanced

The **ADVANCED** pages allow you to configure the more advanced settings of the router, such as Virtual Server(Port Forwarding), MAC and URL filtering, and advanced wireless and network settings. To view the Advanced configuration pages, click on **ADVANCED** at the top of the screen.

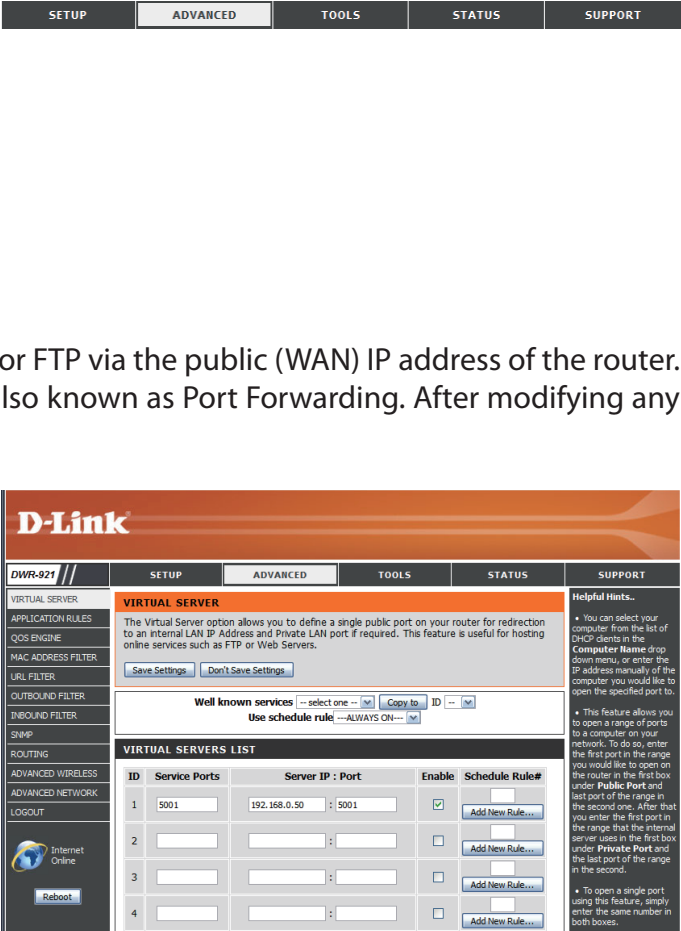
Virtual Server

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. The Virtual Server function is also known as Port Forwarding. After modifying any settings, click **Save Settings** to save your changes.

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 55.



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: Tick the checkbox to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. To create schedules, please refer to “Schedules” on page 55.

VIRTUAL SERVERS LIST				
ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1	5001	192.168.0.50 : 5001	<input checked="" type="checkbox"/>	<div><div></div>Add New Rule...</div>
2		:	<input type="checkbox"/>	<div><div></div>Add New Rule...</div>
3		:	<input type="checkbox"/>	<div><div></div>Add New Rule...</div>
4		:	<input type="checkbox"/>	<div><div></div>Add New Rule...</div>
5		:	<input type="checkbox"/>	<div><div></div>Add New Rule...</div>
6		:	<input type="checkbox"/>	<div><div></div>Add New Rule...</div>
7		:	<input type="checkbox"/>	<div><div></div>Add New Rule...</div>
8		:	<input type="checkbox"/>	<div><div></div>Add New Rule...</div>

Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, and Internet telephony among others. These applications may have difficulty working through NAT (Network Address Translation). **Application Rules** allow some of these applications to work with the DWR-921 by opening ports after detecting traffic being sent through a trigger port. After modifying any settings, click **Save Settings** to save your changes.

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 application** 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: Tick the checkbox to enable the specified rule.

D-Link

DWR-921 // SETUP ADVANCED TOOLS STATUS SUPPORT

APPLICATION RULES

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

Save Settings Don't Save Settings

Popular applications -- select one -- Copy to ID -- ID

ID	Trigger	Incoming Ports	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"/>
11			<input type="checkbox"/>
12			<input type="checkbox"/>

Reboot

Helpful Hints...

• Check the Application Name drop down menu for a list of pre-defined applications that you can select from. If you select one of the pre-defined applications, click the arrow button next to the drop down menu to fill out the appropriate fields.

More...

QoS Engine

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. For best performance, use the Automatic Classification option to automatically set the priority for your applications. After modifying any settings, click **Save Settings** to save your changes.

QOS ENGINE SETUP

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 55.

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: Tick the checkbox to enable the specified rule.

Use Rule #: Specify the schedule rule number. To create schedules, please refer to “Schedules” on page 55.

The screenshot shows the D-Link DWR-921 Web UI. The left sidebar contains navigation links: VIRTUAL SERVER, APPLICATION RULES, QOS ENGINE, MAC ADDRESS FILTER, URL FILTER, OUTBOUND FILTER, INBOUND FILTER, SNMP, ROUTING, ADVANCED WIRELESS, ADVANCED NETWORK, and LOGOUT. The main content area is titled 'QOS ENGINE' and includes a 'QOS ENGINE SETUP' section with checkboxes for 'Enable QoS Packet Filter' and a text field for 'Upstream bandwidth'. Below this is a 'Use schedule rule' dropdown set to 'ALWAYS ON' and a 'Copy to' button. The 'QOS RULES' section contains a table with 5 rows, each with fields for ID, Local IP : Ports, Remote IP : Ports, QoS Priority (set to High), Enable (checkbox), and Use Rule# (with an 'Add New Rule...' button). The right sidebar has a 'Helpful Hints...' section.

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1			High	<input type="checkbox"/>	Add New Rule...
2			High	<input type="checkbox"/>	Add New Rule...
3			High	<input type="checkbox"/>	Add New Rule...
4			High	<input type="checkbox"/>	Add New Rule...
5			High	<input type="checkbox"/>	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. After modifying any settings, click **Save Settings** to save your changes.

MAC FILTERING SETTINGS

MAC Address Control: Tick this box to enable MAC Filtering.

Connection Control: Wireless and wired clients with **C** selected can connect to this device and **allow/deny** connections from unspecified MAC addresses.

Association Control: Wireless clients with **A** selected can associate to the wireless LAN and **allow/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.

Wake On LAN: Click **Trigger** to configure Wake On LAN.

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

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

A:

The screenshot shows the D-Link DWR-921 Advanced Setup page. The 'MAC ADDRESS FILTER' section is active, displaying the following settings:

- 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.
 - Save Settings** (button)
 - Don't Save Settings** (button)
- MAC FILTERING SETTINGS:**
 - MAC Address Control:** ☐ Enable
 - Connection control:** ☐ Wireless and wired clients with **C** checked can connect to this device; and **allow** ☐ **deny** ☐ unspecified MAC addresses to connect.
 - Association control:** ☐ Wireless clients with **A** checked can associate to the wireless LAN; and **allow** ☐ **deny** ☐ unspecified MAC addresses to associate.
- DHCP clients:** -- select one -- **Copy to ID** ☐ **ID** ☐
- MAC FILTERING RULES:**

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

Helpful Hints... (scrollable text on the right side of the page)

URL Filter

URL Filter allows you to set up a list of websites that will be blocked from users on your network. After modifying any settings, click **Save Settings** to save your changes.

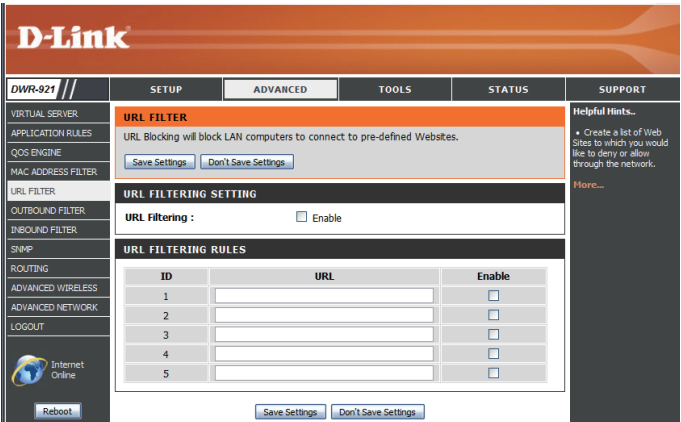
URL Filtering: Select this box to enable URL Filtering.

URL FILTERING RULES

ID: This identifies the rule.

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

Enable: Tick the checkbox to enable the specified rule.



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. After modifying any settings, click **Save Settings** to save your changes.

OUTBOUND FILTER SETTING

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 55.

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: Tick the checkbox to enable the specified rule.

Schedule Rule #: Specify the schedule rule number.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

D-Link

DWR-921 // SETUP ADVANCED TOOLS STATUS SUPPORT

OUTBOUND FILTER

Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets.

Save Settings Don't Save Settings

OUTBOUND FILTER SETTING

Outbound Filter : ☐ Enable

Use schedule rule : ALWAYS ON [v] Copy to ID [v]

OUTBOUND 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="checkbox"/>	Add New Rule...
2	[]	[]	<input type="checkbox"/>	Add New Rule...
3	[]	[]	<input type="checkbox"/>	Add New Rule...
4	[]	[]	<input type="checkbox"/>	Add New Rule...
5	[]	[]	<input type="checkbox"/>	Add New Rule...

Internet Online Reboot

Helpful Hints...

• Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies.

More...

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. After modifying any settings, click **Save Settings** to save your changes.

INBOUND FILTER SETTING

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 55.

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.

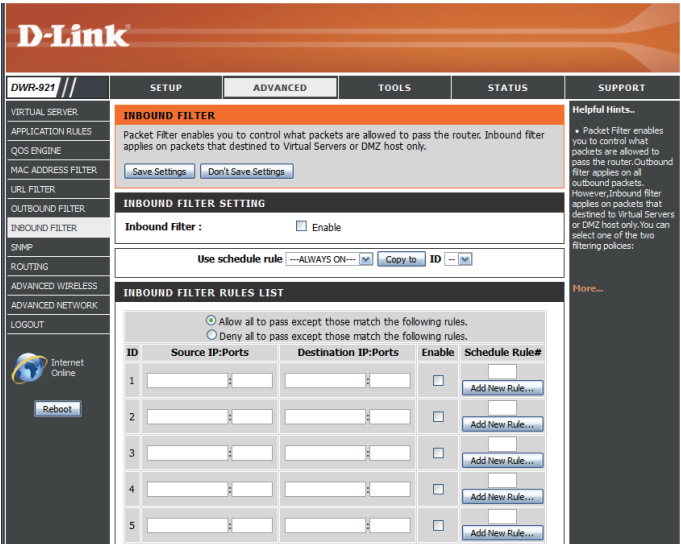
Destination IP : Ports: Specify the remote IP address and then the port after the colon.

Enable: Tick the checkbox to enable the specified rule.

Schedule Rule #: Specify the schedule rule number.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.



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-921. The DWR-921 supports SNMP v1 and v2c. After modifying any settings, click **Save Settings** to save your changes.

SNMP

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.

The screenshot shows the D-Link DWR-921 web interface. The top navigation bar includes 'DWR-921', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration categories. The main panel is titled 'SNMP' and contains the following settings:

- SNMP Local:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- SNMP Remote:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Get Community:** A text input field.
- Set Community:** A text input field.
- IP 1:** A text input field.
- IP 2:** A text input field.
- IP 3:** A text input field.
- IP 4:** A text input field.
- SNMP Version:** Radio buttons for 'V1' (selected) and 'V2c'.
- WAN Access IP Address:** A text input field.

At the bottom of the main panel are 'Save Settings' and 'Don't Save Settings' buttons. A 'Reboot' button is located in the bottom left corner of the sidebar area. A 'Helpful Hints...' section is visible on the right side of the interface.

Routing

The **Routing** page allows you to specify custom routes that determine how data is moved around your network. After modifying any settings, click **Save Settings** to save your changes.

RIP SETTING

RIP: Select this 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.

D-Link

DWR-921

SETUP ADVANCED TOOLS STATUS SUPPORT

ROUTING

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

Save Settings Don't Save Settings

RIP SETTING

RIP : ☐ Enable ☐ RIPv1 ☐ RIPv2

ROUTING RULES

ID	Destination	Subnet Mask	Gateway	Hop	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"/>

Save Settings Don't Save Settings

Helpful Hints...

- Each route has a check box next to it, check this box if you want the route to be enabled.
- The destination IP address is the address of the host or network you wish to reach.
- The netmask field identifies the portion of the destination IP in use.
- The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

More...

Advanced Wireless

Advanced Wireless 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. After modifying any settings, click **Save Settings** to save your changes.

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.

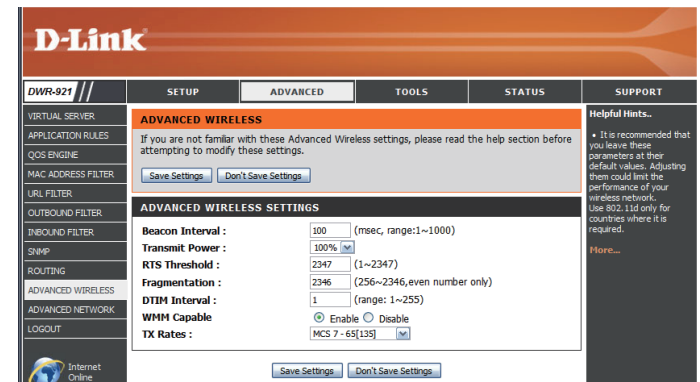
RTS Threshold: This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.

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 3.

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 **Auto**.



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. After modifying any settings, click **Save Settings** to save your changes.

Enable UPnP: Tick this checkbox to use 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.

D-Link

DWR-921 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADVANCED NETWORK

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

Save Settings Don't Save Settings

UPNP

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

Enable UPnP : ☒

WAN PING

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

Enable WAN Ping Respond : ☒

Save Settings Don't Save Settings

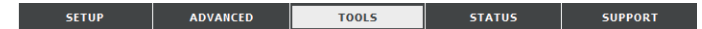
Helpful Hints...

- UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.
- For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

More...

Tools

The **TOOLS** pages allow you to adjust various system settings for your router, such as the system time, firmware, and custom schedules. To view the Tools pages, click on **TOOLS** at the top of the screen.



Admin

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. After modifying any settings, click **Save Settings** to save your changes.

ADMINISTRATOR

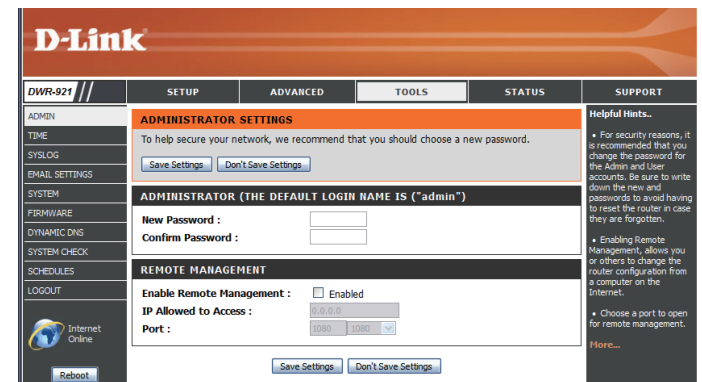
Admin Password: Enter and confirm the password that the admin account will use to access the router's management interface.

REMOTE MANAGEMENT

Remote Management: Tick this check box to enable remote management. Remote management allows the DWR-921 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.



Time

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. After modifying any settings, click **Save Settings** to save your changes.

TIME AND DATE CONFIGURATION

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

Enable Daylight Saving: Tick this checkbox to allow for daylight saving adjustments. Use the dropdown boxes to specify a start date and end date for daylight saving time adjustments.

AUTOMATIC TIME AND DATE CONFIGURATION

Tick the **Automatically synchronize with Internet time server** checkbox 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 dropdown box to select one. Click the **Update Now** button to synchronize the time with the NTP server.

The screenshot shows the D-Link DWR-921 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a menu with options like ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, SCHEDULES, and LOGOUT. The main content area is titled 'TIME AND DATE' and contains the following sections:

- TIME AND DATE:** A introductory text block explaining the purpose of the section, followed by 'Save Settings' and 'Don't Save Settings' buttons.
- TIME AND DATE CONFIGURATION:** A section with fields for 'Time' (displaying 'Mon Sep 17, 2012 14:15:12'), 'Time Zone' (a dropdown menu showing '(GMT-08:00) Pacific Time (US & Canada)'), and 'Enable Daylight Saving' (an unchecked checkbox).
- AUTOMATIC TIME AND DATE CONFIGURATION:** A section with a checked checkbox for 'Automatically synchronize with Internet time server', an 'NTP Server Used' dropdown menu (showing 'time-nw.nist.gov'), and an 'Update Now' button.
- SYNC. RESULT:** A large empty text area for displaying synchronization results.

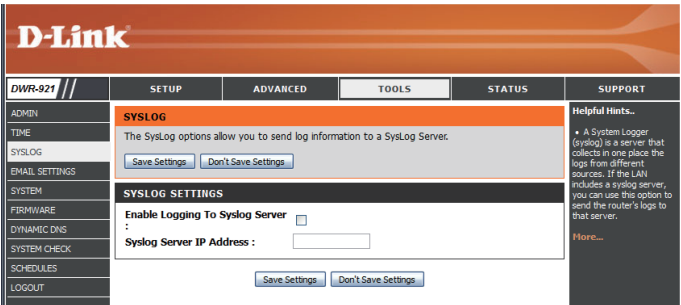
At the bottom of the main content area are 'Save Settings' and 'Don't Save Settings' buttons. A 'Reboot' button is also visible in the left sidebar.

Syslog

The DWR-921 keeps a running log of events and activities occurring on the router. You may send these logs to a syslog server on your network. After modifying any settings, click **Save Settings** to save your changes.

Enable Logging to Syslog Server: Tick this checkbox 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.



E-mail Settings

E-mail Settings allow you to send the system log files, router alert messages, and firmware update notifications to an e-mail address. After modifying any settings, click **Save Settings** to save your changes.

Enable E-mail Notification: When this option is enabled, router activity logs will be e-mailed to the specified e-mail address.

SMTP Sever IP and Port: Enter the SMTP server IP address the router will use to send e-mails. Enter the complete IP address followed by a colon(:) and the port number. (e.g. 123.123.123.1:25).

SMTP Username: Enter the username for the SMTP account.

SMTP Password: Enter the password for the SMTP account.

Send E-mail Alert to: Enter the e-mail address where you would like the router to send e-mails to.

E-mail Subject: Enter a subject for the e-mail.

E-mail Log Now: Click this button to send the current logs to the specified e-mail address.

The screenshot shows the D-Link DWR-921 Web UI. The top navigation bar includes 'D-Link', 'DWR-921', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar contains a menu with 'ADMIN', 'TIME', 'SYSLOG', 'EMAIL SETTINGS' (highlighted), 'SYSTEM', 'FIRMWARE', 'DYNAMIC DNS', 'SYSTEM CHECK', 'SCHEDULES', and 'LOGOUT'. The main content area is titled 'EMAIL SETTINGS' and contains the following fields: 'Enable Email Notification' (checkbox), 'SMTP Server IP and Port' (text box), 'SMTP Username' (text box), 'SMTP Password' (text box), 'Send E-mail alert to:' (text box), and 'E-mail Subject:' (text box). There are 'Save Settings' and 'Don't Save Settings' buttons at the top and bottom of the form. A 'Reboot' button is in the sidebar. A 'Helpful Hints...' section is on the right.

System

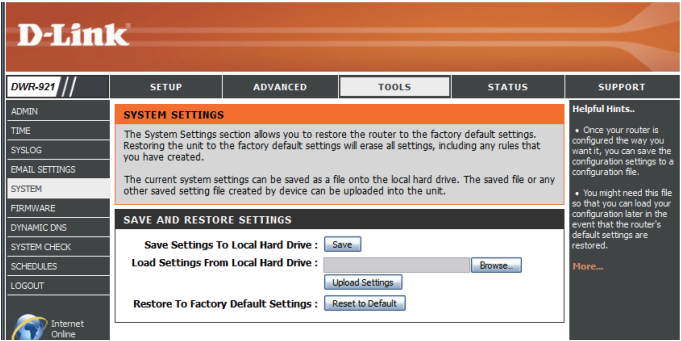
Here, you can save the current system settings to a local hard drive. After modifying any settings, click **Save Settings** to save your changes.

- 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 **Browse...** 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.



Firmware

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>. After modifying any settings, click **Save Settings** to save your changes.

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

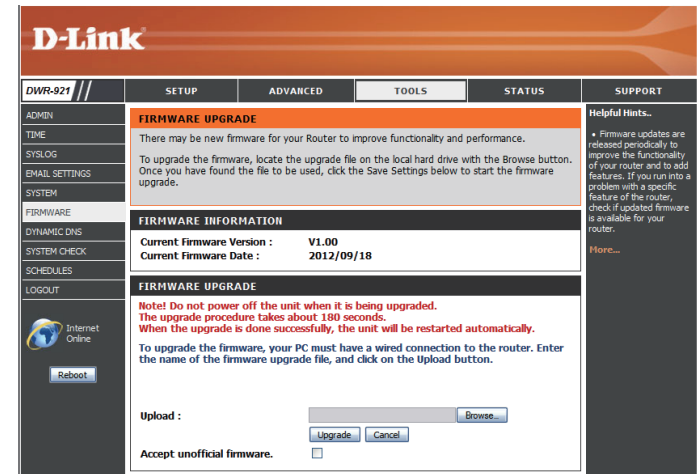
Current Firmware Date: Displays your current firmware's release date.

Upload: 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 computer to upload the firmware file; do not use a wireless computer. 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 checkbox.

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



Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, or Game Server) using a domain name that you have purchased (such as www.exampledomain.com) with your dynamically assigned IP address. You can use one of the listed DDNS service, or you can sign up for D-Link's free DDNS service at www.dlinkddns.com. After modifying any settings, click **Save Settings** to save your changes.

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.

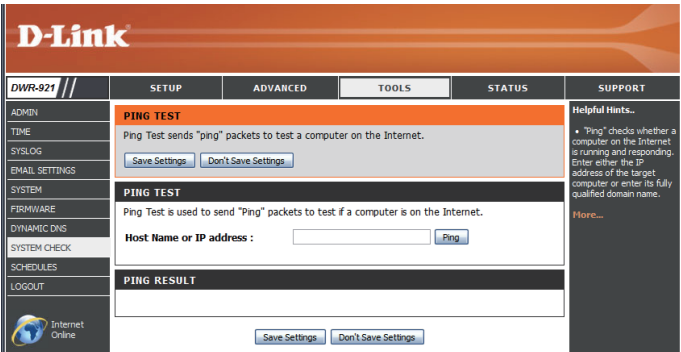
Password / Key: Enter the **Password** for your DDNS account.

The screenshot shows the D-Link DWR-921 web interface. The top navigation bar includes 'D-Link', 'DWR-921', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS (selected), SYSTEM CHECK, SCHEDULES, and LOGOUT. Below the sidebar is an 'Internet Online' status indicator with a 'Reboot' button. The main content area is titled 'DYNAMIC DNS' and contains a checkbox to enable the feature, followed by a descriptive paragraph. Below this are 'Save Settings' and 'Don't Save Settings' buttons. A second 'DYNAMIC DNS' section contains input fields for 'Provider' (with a dropdown menu showing 'DyDNS.org(Dynamic)' and a 'Go' button), 'Host Name', 'Username / E-mail', and 'Password / Key', each with a corresponding input field. At the bottom of this section are 'Save Settings' and 'Don't Save Settings' buttons. A 'Helpful Hints...' sidebar on the right provides additional information and a 'Here...' link.

System Check

This useful diagnostic utility can be used to check if a computer is connected to the network. It sends ping packets and listens for responses from the specific host. After modifying any settings, click **Save Settings** to save your changes.

Host Name or IP Address: Enter a host name or the IP address that you want to ping and click the **Ping** button. The results of the ping attempt will be displayed in the **PING RESULT** section below.



Schedules

This section allows you to manage schedule rules for various firewall and parental control features. After modifying any settings, click **Save Settings** to save your changes.

Enable Schedule: Tick this checkbox to enable schedules.

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

Delete: Click this button 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)

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.

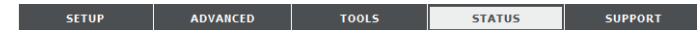
End Time (hh:mm): Select the time at which you would like the schedule to become inactive.

After making your changes, click **Save Settings** to save the schedule.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	Monday	08:00	19:00
2	Tuesday	08:00	19:00
3	Wednesday	08:00	19:00
4	Thursday	08:00	19:00
5	Friday	08:00	19:00
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

Status

The **STATUS** pages allow you to see the current status of the router for various categories, including WAN, 3G, network, and wireless. To view the Status pages, click on **STATUS** at the top of the screen.



Device Info

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

General: Displays the current time and firmware version.

WAN: Displays the WAN connection details of the router.

3G Card: Displays the 3G connection details of the router.

LAN: Displays the LAN connection details of the router.

Wireless LAN: Displays the wireless LAN connection details of the router.

LAN Computers: Displays the list of clients connected to the router.

D-Link

DWR-921

SETUP ADVANCED TOOLS **STATUS** SUPPORT

DEVICE INFO
LOG
STATISTICS
WIRELESS
LOGOUT

DEVICE INFORMATION
All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.
[Refresh](#)

GENERAL
Time : Sun Sep 16, 2012 22:16:11 -0800
Firmware Version : V1.00 , 2012/09/04

WAN
Connection Type : DHCP Client
Network Status : Established
Remaining Lease Time : 6 Hour 2 Min 5 Sec
[Renew](#) [Release](#)
MAC Address : 84:C9:B2:E2:FC:7E
IP Address : 172.17.5.131
Subnet Mask : 255.255.255.0
Default Gateway : 172.17.5.254
DNS Server : 192.168.168.249 , 192.168.168.201

3G/4G CARD
Card Info : N/A
Link Status : Connecting...
Network Name : N/A

LAN
MAC Address : 84:C9:B2:E2:FC:7F
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN
MAC Address : 84:C9:B2:E2:FC:7F
Wireless : Enabled
SSID : dlink_DWR-921
Security : Auto(None)
Channel : 11
802.11 Mode : B/G/N Mixed

LAN COMPUTERS

IP Address	Name	MAC
192.168.0.50	06955pcwinxp	00-19-B9-43-71-1E

WIRELESS

Helpful Hints...
• All of your LAN, WAN and WIRELESS connection details are displayed here.
[More...](#)

Log

Here, you can view and download the system log.

Previous: Click this button to go to the previous page of the log.

Next: Click this button to go to the next page of the log.

First Page: Click this button to skip to the first page of the log.

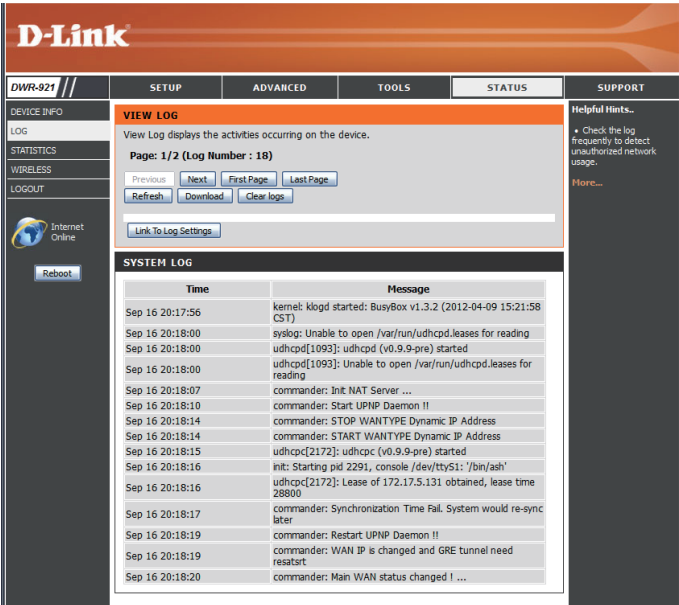
Last Page: Click this button to skip to the last page of the log.

Refresh: Click this button to refresh the system log.

Download: Click this button to download the current system log to your computer.

Clear Logs: Click this button to clear the system log.

Link To Log Settings: Click this button for a link that goes to the Log Settings page.



Statistics

Here you can view the packets transmitted and received by your router for both the WAN and LAN ports. The traffic counter will reset if the device is rebooted. Click the **Refresh** button to refresh the WAN statistics.

The screenshot shows the D-Link DWR-921 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains links for DEVICE INFO, LOG, STATISTICS (highlighted), WIRELESS, and LOGOUT, along with an Internet Online status indicator and a Reboot button. The main content area is titled 'TRAFFIC STATISTICS' and includes a description, a Refresh button, and a 'WAN STATISTICS INFORMATION' table. A 'Helpful Hints..' section is visible on the right.

Statistics	Inbound	Outbound
Octets	395173674	26541068
Unicast packets	381673	212624
Multicast packets	56653	0

Helpful Hints..

- This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized.

[More...](#)

Wireless

This table displays a list of wireless clients that are connected to your wireless router. Click **Refresh** to refresh the list.

D-Link

DWR-921


DEVICE INFO

LOG

STATISTICS

WIRELESS

LOGOUT

 Internet Online

Reboot

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

WIRELESS CLIENT LIST

View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

Refresh

WIRELESS CLIENT TABLE

ID	MAC Address
1	28-E0-2C-DC-0A-BE

Helpful Hints..

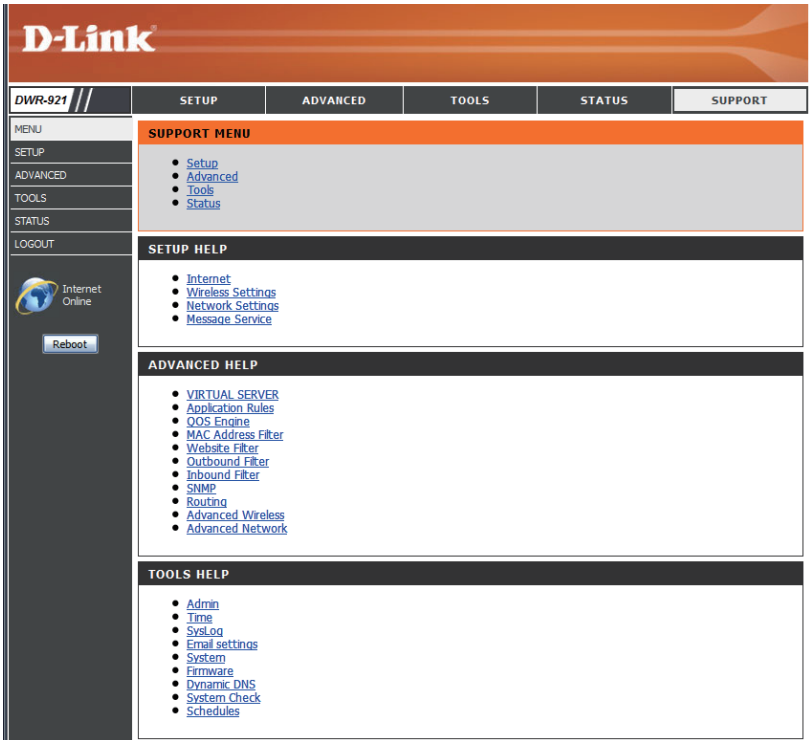
- This is a list of all wireless clients that are currently connected to your wireless router.

More...

Support

The **SUPPORT** pages provide help information for each section of the device's interface. To view the Support pages, click on **SUPPORT** at the top of the screen.

SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
-------	----------	-------	--------	---------



Connecting to a Wireless Network Using Windows 7

Windows 7 users may use the built-in wireless utility to connect to a wireless network. If you are using another company's utility or Windows 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows 7 utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility. You can also click on the wireless icon in your system tray (lower-right corner).

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



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

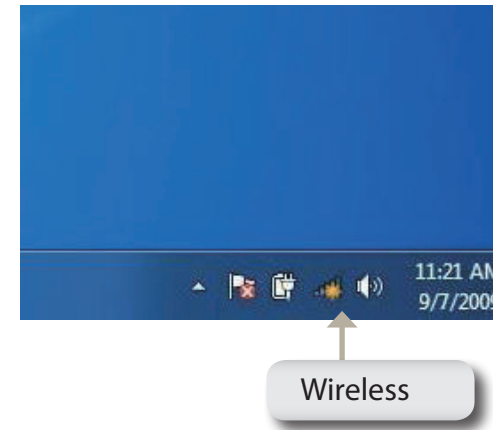
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to “Networking Basics” on page 81 for more information.



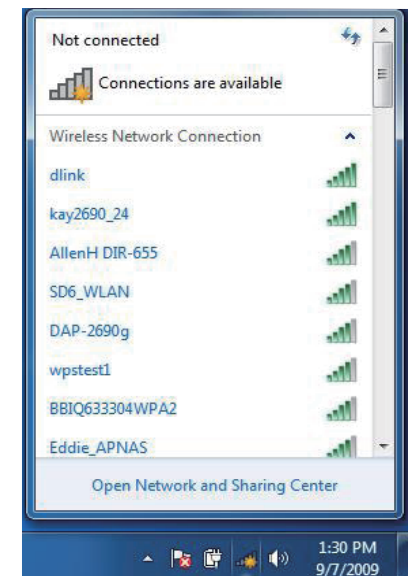
Configuring Wireless Security

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

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



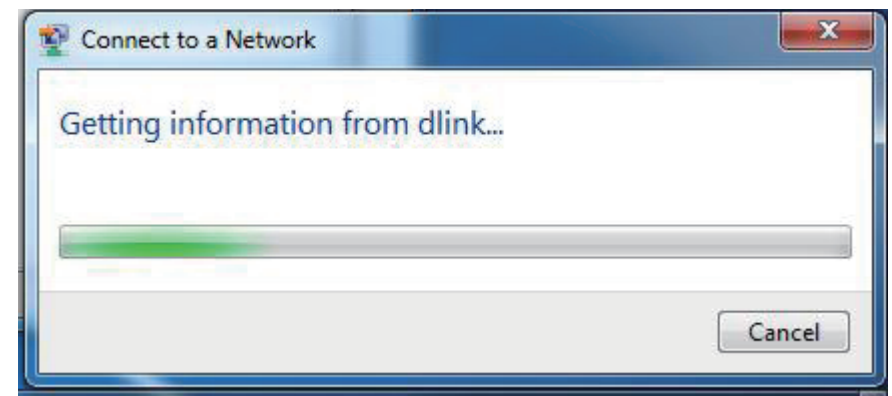
2. The utility will display any available wireless networks in your area.



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



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



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

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



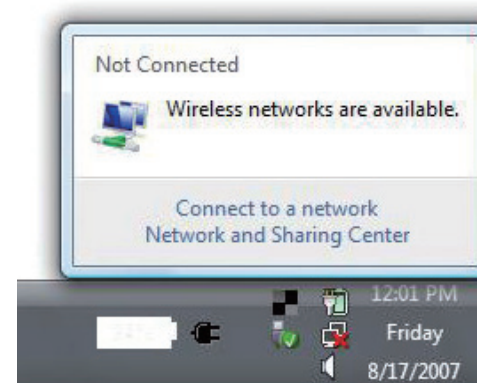
Using Windows Vista™

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

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

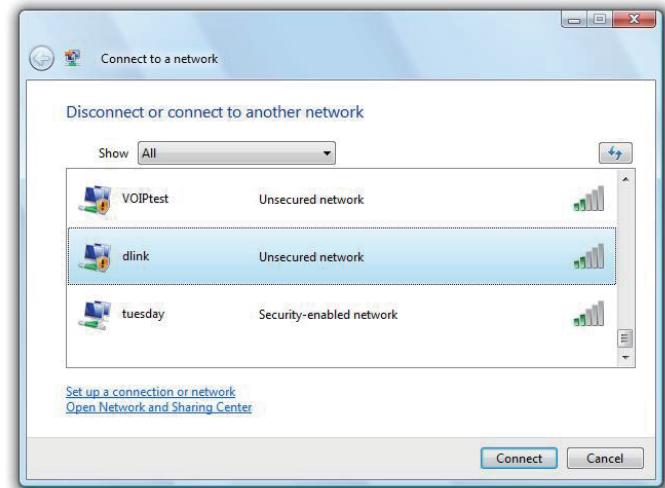
or

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.

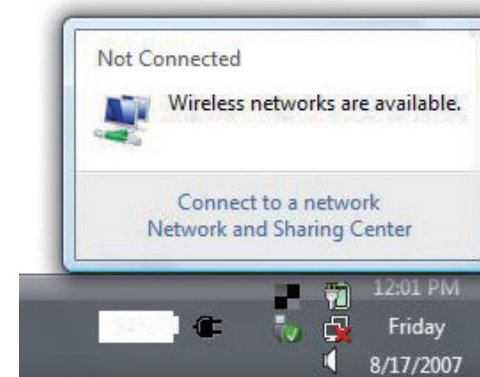
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Networking Basics" on page 81 for more information.



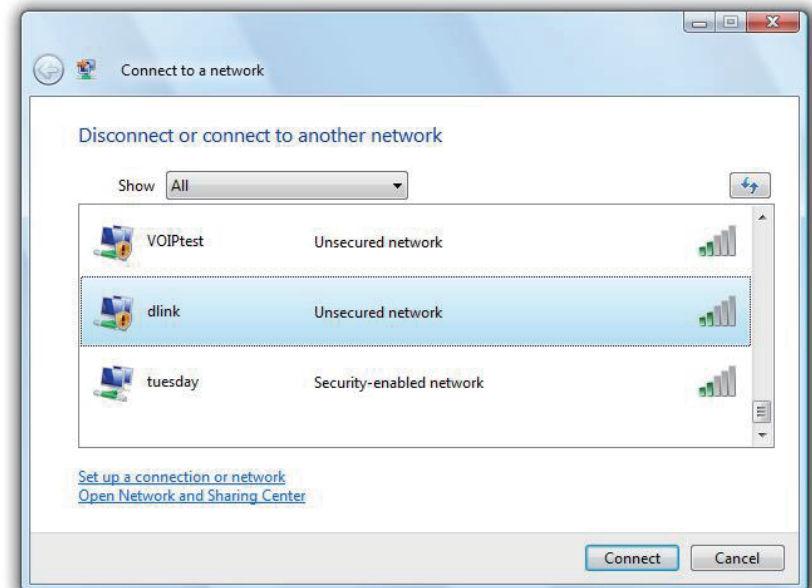
Configuring Wireless Security

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

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

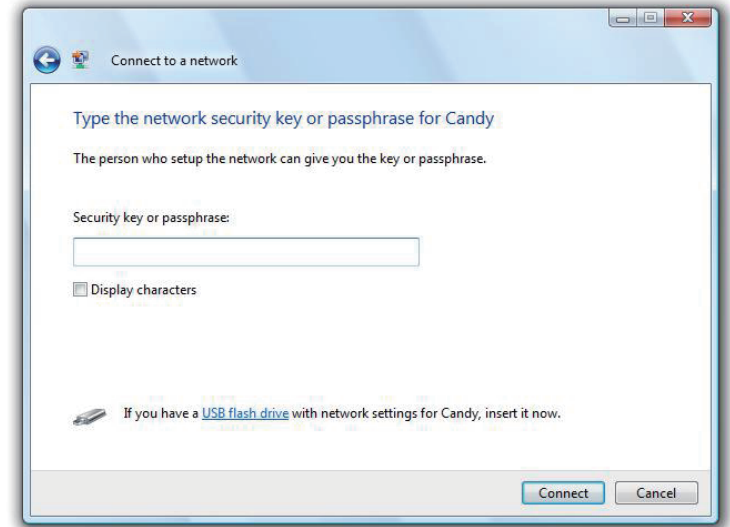


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



Connect to a Wireless Network Using Windows® XP

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

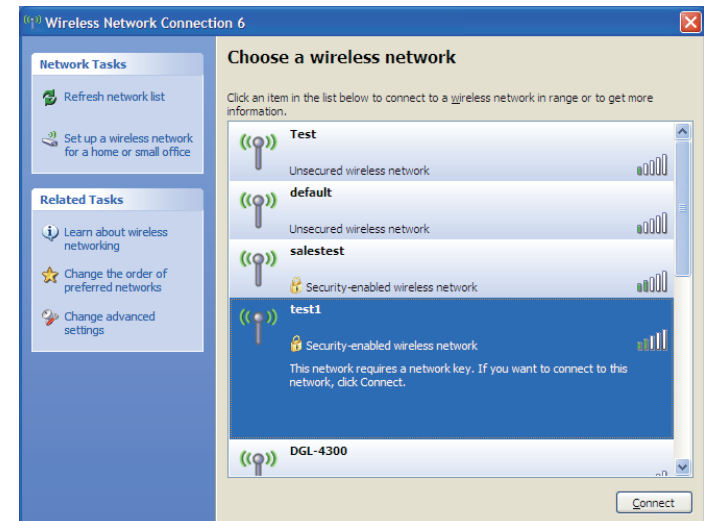
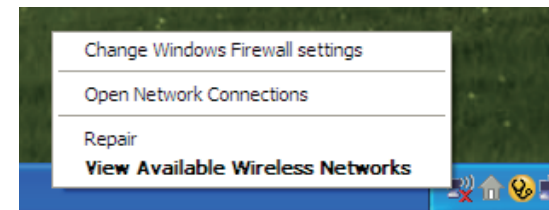
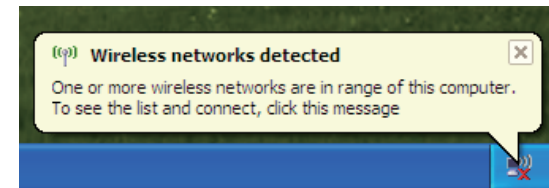
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

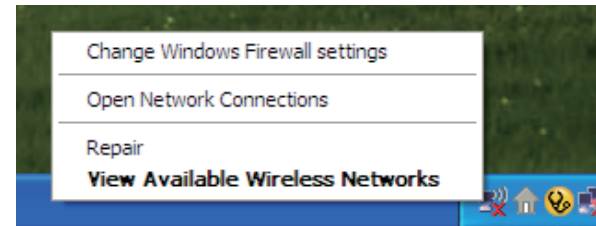
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Networking Basics" on page 81 for more information.



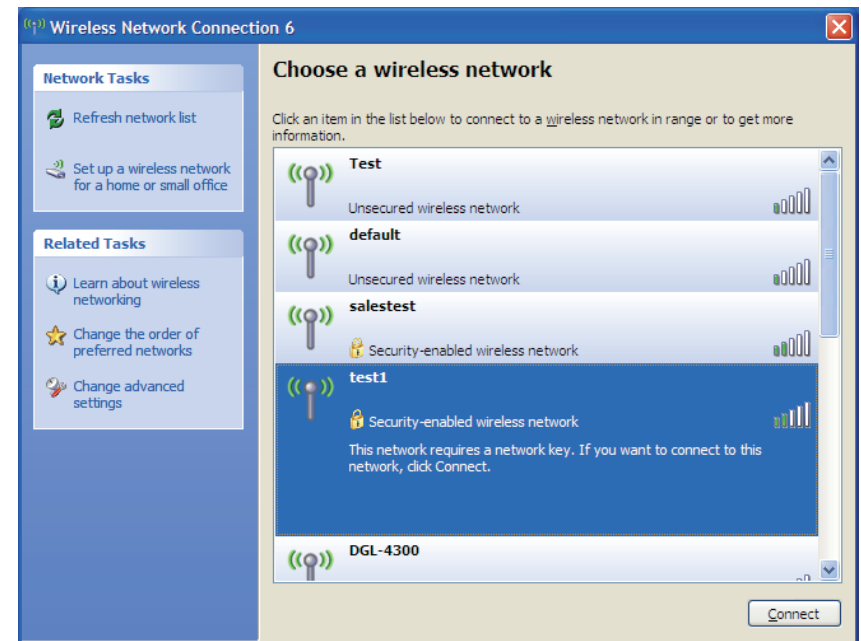
Configure WEP

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

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

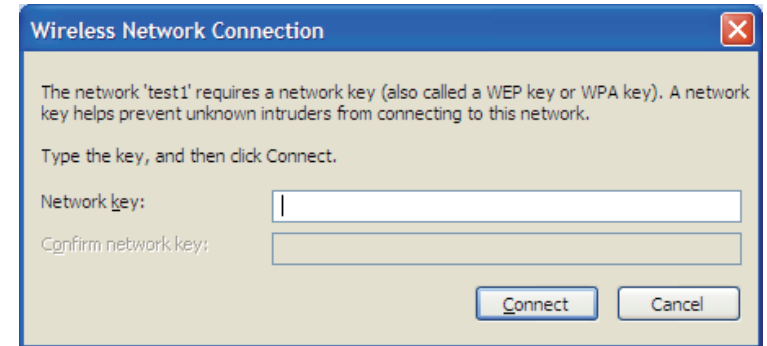


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

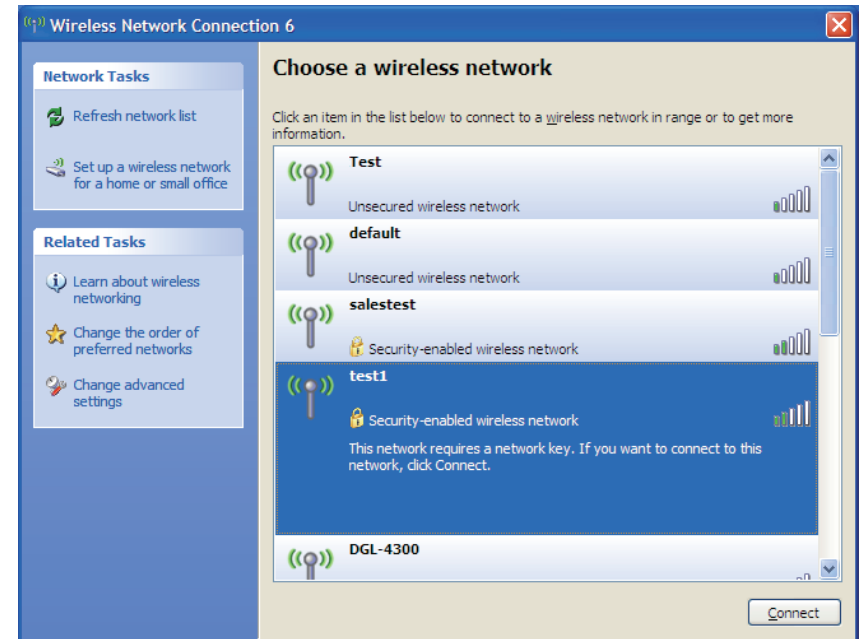
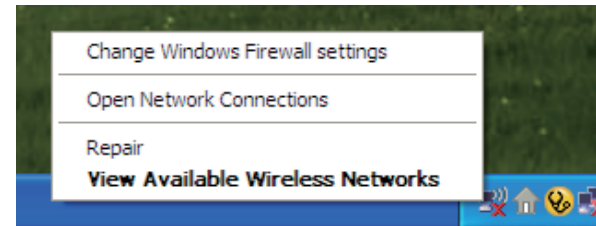
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



Configure WPA-PSK

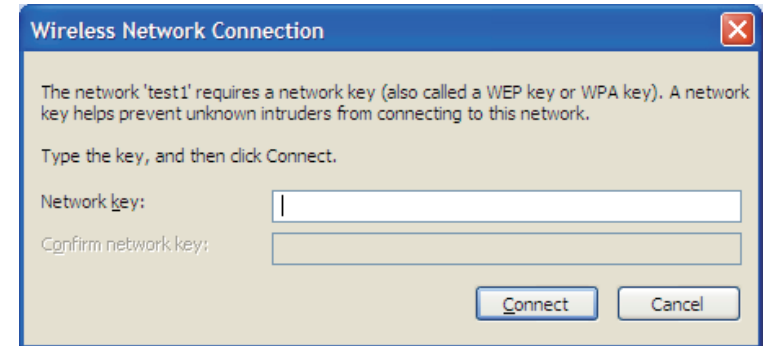
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

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



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

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-921. Read the following descriptions if you are having problems.

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - • Internet Explorer 6 or higher
 - • Netscape 8 or higher
 - • Mozilla 1.7.12 (5.0) or higher
 - • Opera 8.5 or higher
 - • Safari 1.2 or higher (with Java 1.3.1 or higher)
 - • Camino 0.8.4 or higher
 - • Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

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

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

If you forgot your password, you must reset your router. Please note that 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, and the default username is **admin** and the password should be left blank.

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your Router or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

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

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

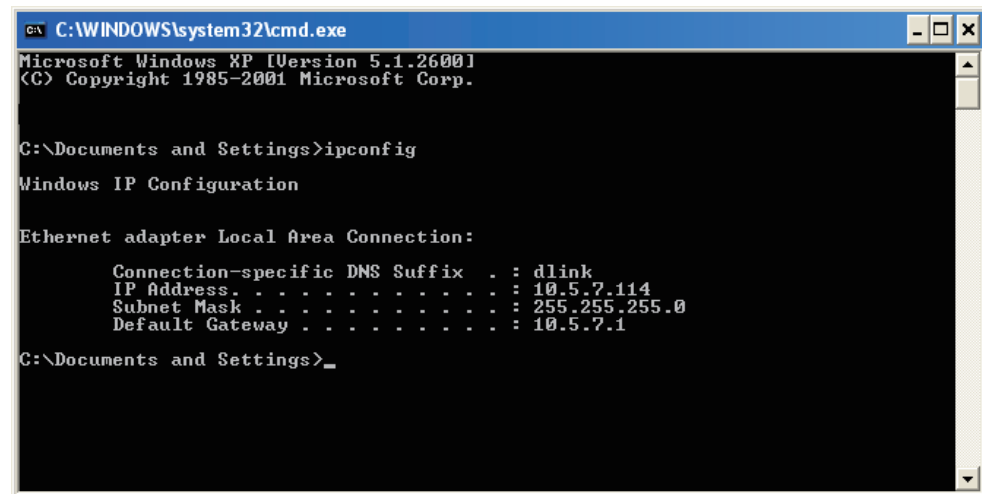
Check your IP address

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® 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.



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>
```

If 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.

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® 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 (TCP/IP)** and click **Properties**.

Step 4

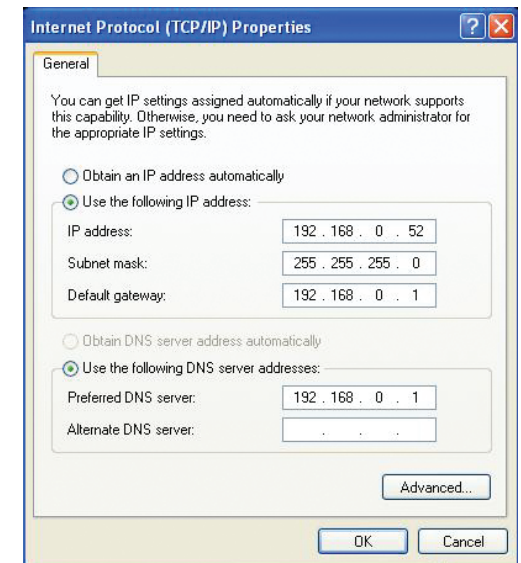
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

Step 5

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



Technical Specifications

LTE Band

- 800 / 900 / 1800 / 2600 MHz

UMTS/HSDPA/HSUPA Band ¹

- 900 / 2100 MHz
- Power Class 3

Data Rates ²

- Up to 150 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

- 802.11b/g, compatible with 802.11n devices
- 802.3
- 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)

USIM Slot

- Standard 6-pin SIM card interface

LED Status Indicators

- WAN
- LAN
- WLAN
- 3G
- 4G
- SMS
- Signal

Dimensions (L x W x H)

- 190 x 111.5 x 23.5 mm (7.48 x 4.39 x 0.93 inches)

Operating Temperature

- 0 to 40 °C (32 to 104 °F)

Operating Humidity

- 10% to 90% (Non-condensing)

Certifications

- CE
- Wi-Fi Certified

¹ Supported frequency band is dependent upon regional hardware version.

² Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.