D-Link®

Version 3.01 | 05/20/2015

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.

Manual Revisions

Revision	Date	Description
3.01	May 20, 2015	• Initial release

Trademarks

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

Copyright © 2015 by D-Link Corporation.

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

Table of Contents

Product Overview 1
Package Contents 1
System Requirements 1
Introduction 2
Hardware Overview 3
Front View 3
Back View 4

Installation 5
Before You Begin 5
Wireless Installation Considerations 6

Configuration 7
Getting Started 7
Internet 8
WAN Service 8
Dynamic IP (DHCP) 8
Static IP 10
PPPoE (Username / Password) 11
PPTP 13
L2TP 15
4G LTE / 3G 17
Wizard 19
Failover 23
IPv6 24
Link-local Only 24
Static IPv6 25
Autoconfiguration (SLAAC/DHCPv6) 26
PPPoE 27
Wi-Fi 28
Device List 28
Wi-Fi Settings 28
WPS 30
Wi-Fi Advanced 32
LAN 34
Device List 34
LAN Settings 34
DHCP 35
Advanced 36
DNS 36
Applications 37
DMZ 38
Virtual Server 39
URL Filter 40
Routing 41
QoS 42
MAC Address Filter 43
Outbound Filter 44
Inbound Filter 45
SNMP 46
Advanced Network 47
Network Scan 48
System 49

Time Settings 49
Administration 50
Reboot & Reset 51
Firmware Upgrade 52
System Log 53
Message Service 54
SMS Inbox 54
Create Message 54
PIN Configuration 55
USSD 56
Schedules 57
Add New Rule 57
Connection Reset 58

Connect a Wireless Client to your Router 59
WPS Button 59
Windows® 8 60
WPA/WPA2 60
Windows® 7 62
WPA/WPA2 62
WPS 65
Windows Vista® 69
WPA/WPA2 70
Windows® XP 72
WPA/WPA2 73

Troubleshooting 75

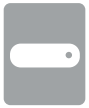
Wireless Basics 79
What is Wireless? 80
Tips 82
Wireless Modes 83

Networking Basics 84
Check your IP address 84
Statically Assign an IP address 85
Wireless Security 86
What is WPA? 86

Technical Specifications 87

Regulatory Information 88

Package Contents



DWR-921 4G LTE Router

Power Adapter

3G/4G Antennas

RJ45 Cable

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

System Requirements

- A compatible (U)SIM card with service.*
- Computer with Windows, Mac OS, or Linux-based operating system with an installed Ethernet adapter
- Java-enabled browser such as Internet Explorer 6, Safari 4.0, Chrome 20.0, or Firefox 7 or above (for configuration)

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

Introduction

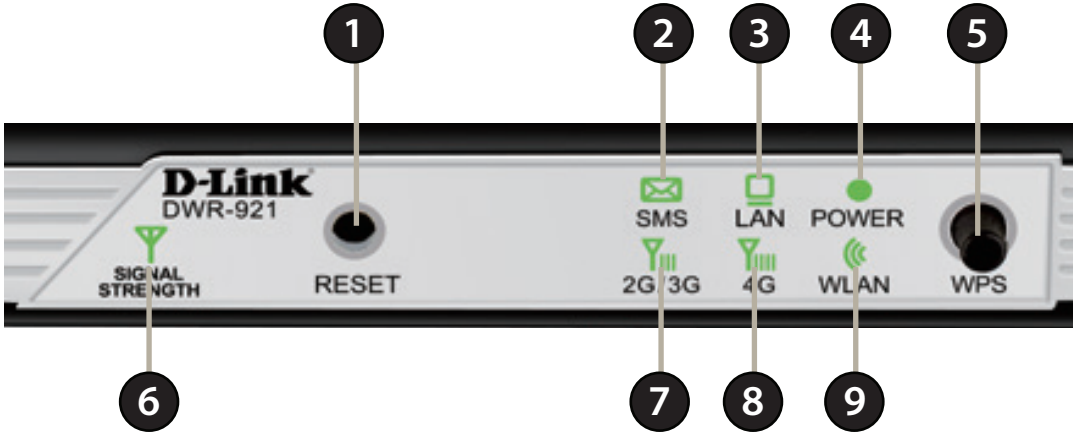
The D-Link 4G LTE Router allows users to access worldwide mobile broadband networks. Once connected, users can transfer data, stream media, and send SMS messages. Simply insert your 3G / 4G SIM card, and share your 3G / 4G Internet connection through a secure 802.11n wireless network or using any of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

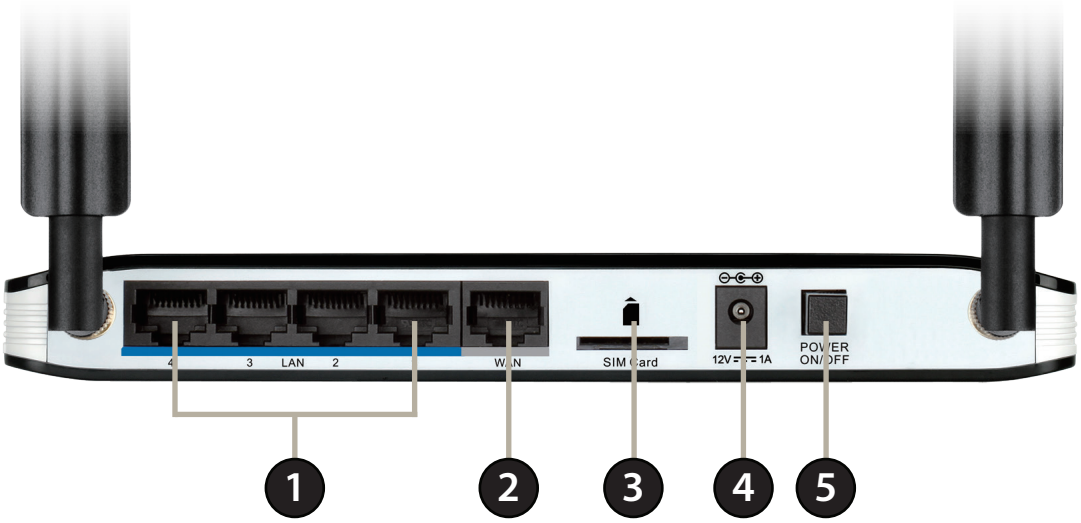
Hardware Overview

Front View



1	**Reset Button**	Press this button with an unfolded paperclip and hold for ten seconds to reset the device.
2	**SMS LED**	Will be solid green if the SMS inbox is full, or blinking if there is an unread new SMS message.
3	**LAN LED**	Will be lit if an Ethernet connection is established, and will blink when data is being transferred.
4	**Power LED**	Will be lit if the device is powered on and working.
5	**WPS Button**	Press this button to initiate a new WPS connection. See **WPS Button** on page 59 for details.
6	**Signal Strength LED**	Will blink red if there is no SIM card / signal. Solid red/amber/green indicates the signal strength.
7	**2G/3G LED**	Will be lit if a 2G or 3G connection is established, and will blink when data is being transferred.
8	**4G LED**	Will be lit if a 4G LTE connection is established, and will blink when data is being transferred.
9	**WLAN LED**	Will be lit if the wireless function is enabled, and will blink when wireless data is being transferred.

Back View



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

Installation

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

Before You Begin

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 / 4G 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.

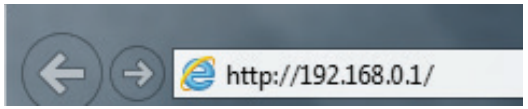
3. Try to position access points, wireless routers, and computers so that the signal passes through open doorways and drywall. Materials such as glass, metal, brick, insulation, concrete, and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors, 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

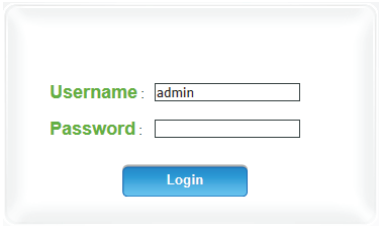
Getting Started

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



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

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



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

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

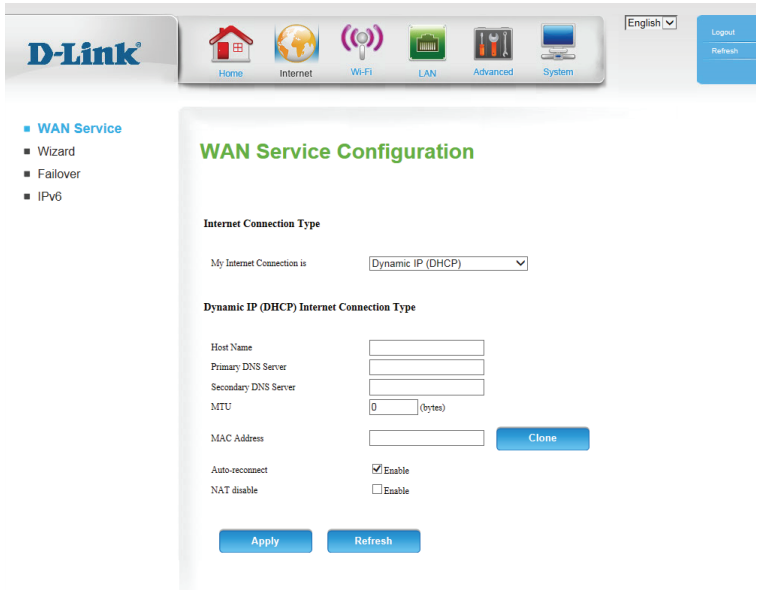
On each page, fill out the desired settings and click **Apply** when you are done or **Reset** to revert to the old settings.

Internet

WAN Service

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

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



Dynamic IP (DHCP)

Host Name: If the Internet host you are using requires you to enter a host name, enter it here. In most cases, you may leave this blank.

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

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

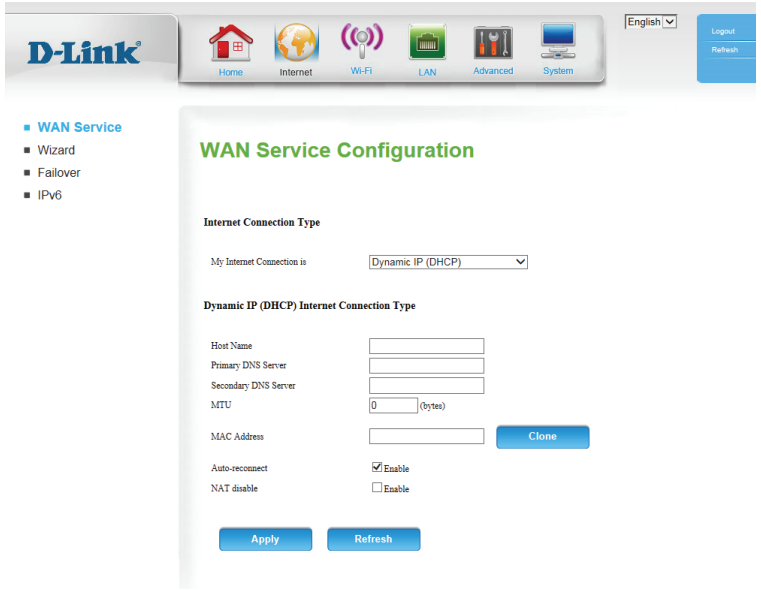
MTU: You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 0.

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

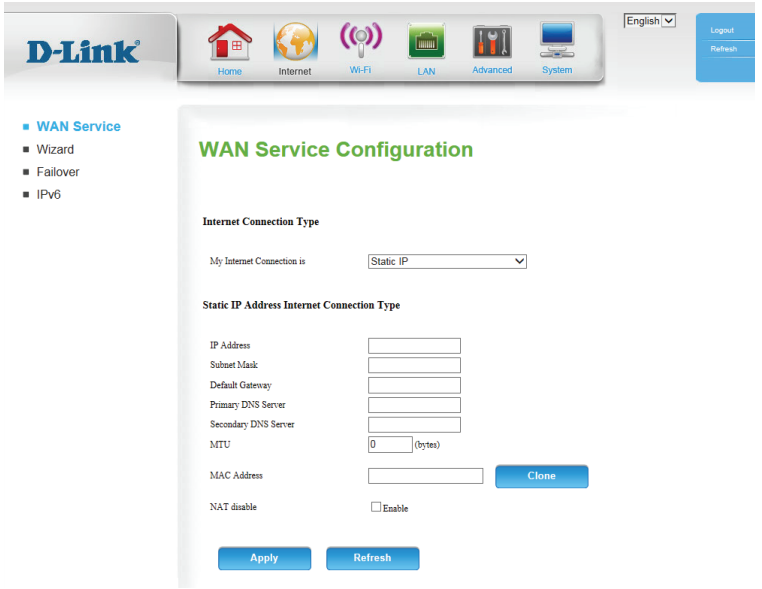
Auto-reconnect: This feature enables this product to renew the WAN IP address automatically when the lease time has expired.

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

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



Static IP



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

Subnet Mask: Enter the subnet mask.

Default Gateway: Enter the default gateway.

Primary DNS Server: Enter the primary DNS server.

Secondary DNS Server: Enter the secondary DNS server.

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

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

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

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

PPPoE (Username / Password)

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: Re-type your password in this field.

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

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

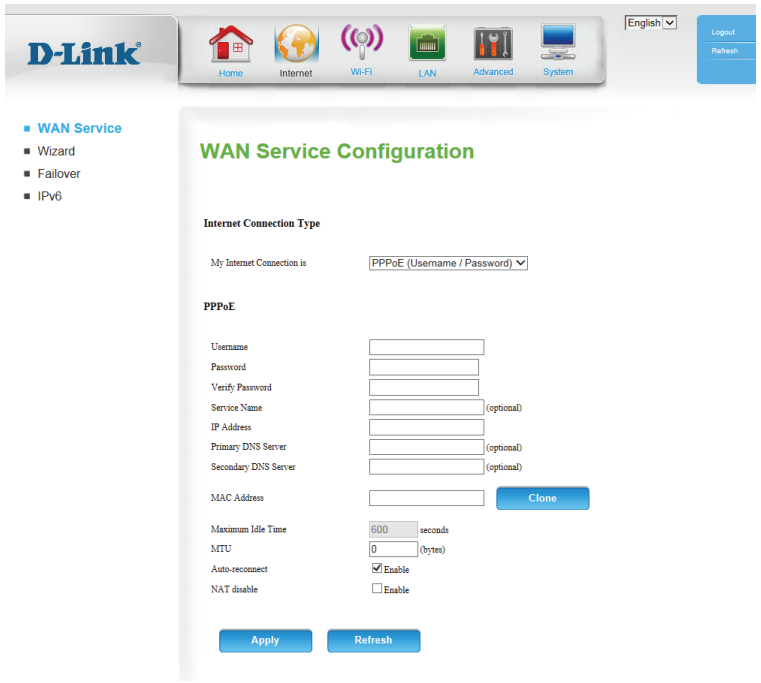
Primary DNS Server: Fill in if provided by your ISP. If not, keep the default value (optional).

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

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

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

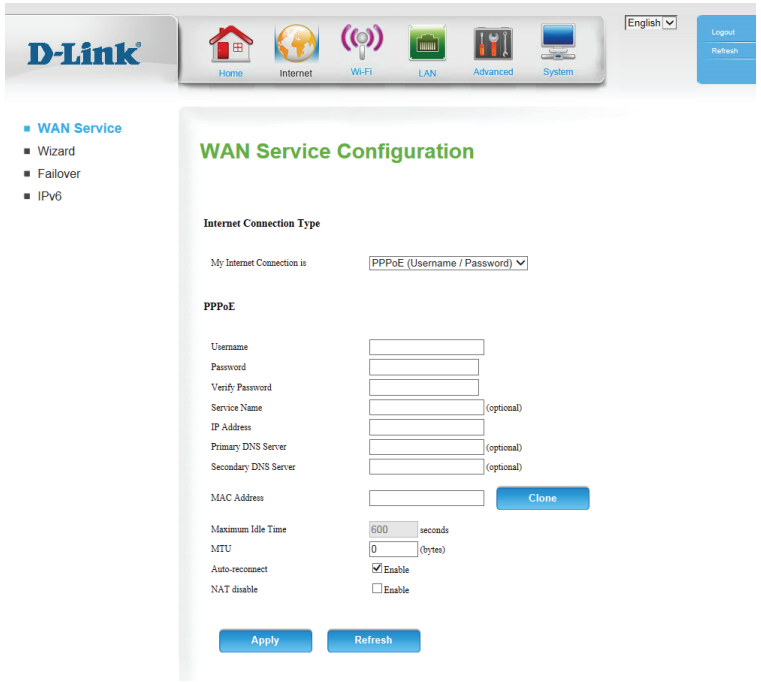
MTU: You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 0.



Auto-reconnect: The device will automatically reconnect to your PPPoE connection automatically.

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.

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



PPTP

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.

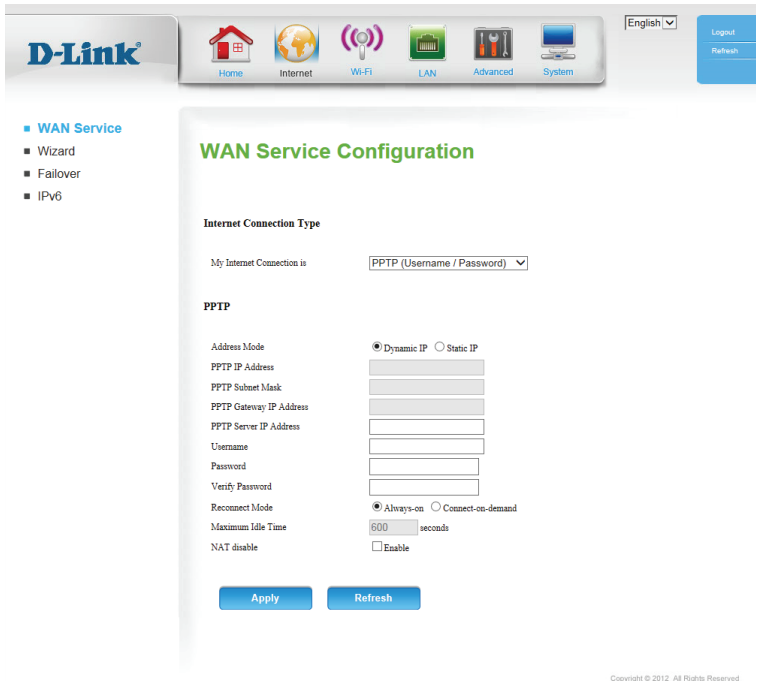
Username: User/account name that your ISP provides to you for PPTP dial-up.

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

Verify Password: Re-enter your password for verification.

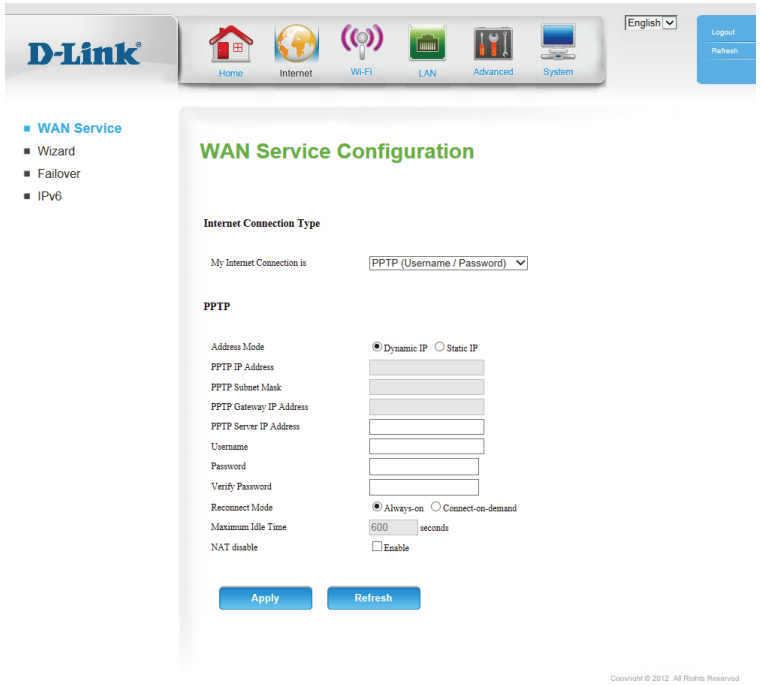
Reconnect Mode: Choose **Always-on** when you want to establish PPTP connection all the time. If you choose **Connect-on-demand**, the device will establish a PPTP connection when local users want to connect to the Internet, and disconnect if there is no traffic after the time period defined by the **Maximum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

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



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.

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



L2TP

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

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

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

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

L2TP Server IP Address: IP address of L2TP server.

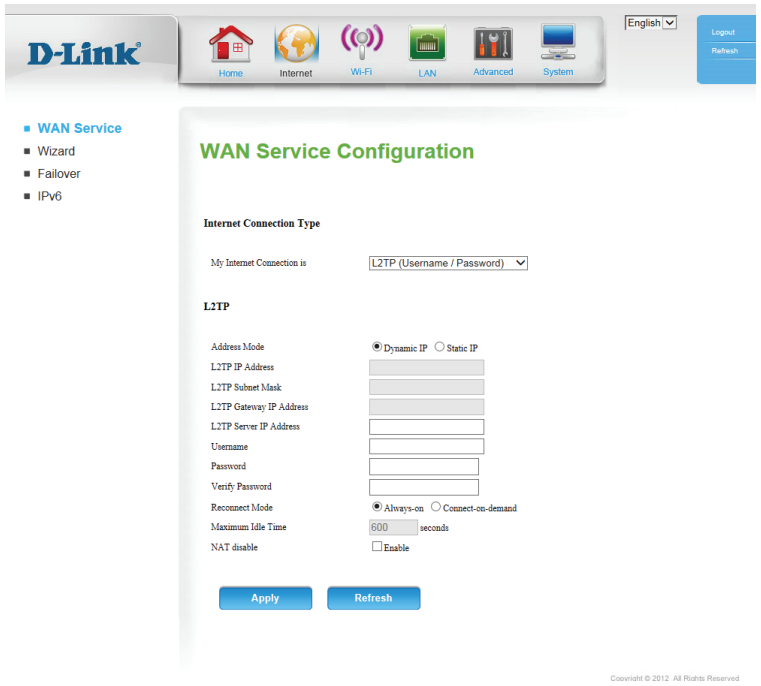
Username: User/account name that your ISP provides to you for L2TP dial-up.

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

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

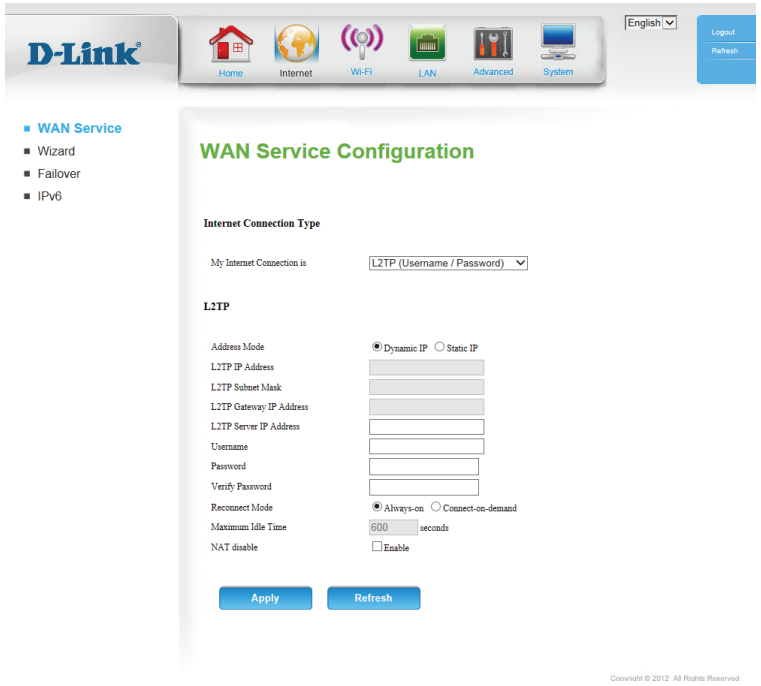
Reconnect Mode: Choose **Always-on** when you want to establish L2TP connection all the time. If you choose **Connect-on-demand** the device will establish L2TP connection when local users want to use Internet, and disconnect if no traffic after time period of Maximum Idle Time.

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



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.

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



4G LTE / 3G

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

Dial Up Profile: Select **Auto-Detection** to have the router automatically detect the settings for your connection. Select **Manual** to enter the details of your connection manually.

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

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

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

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

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

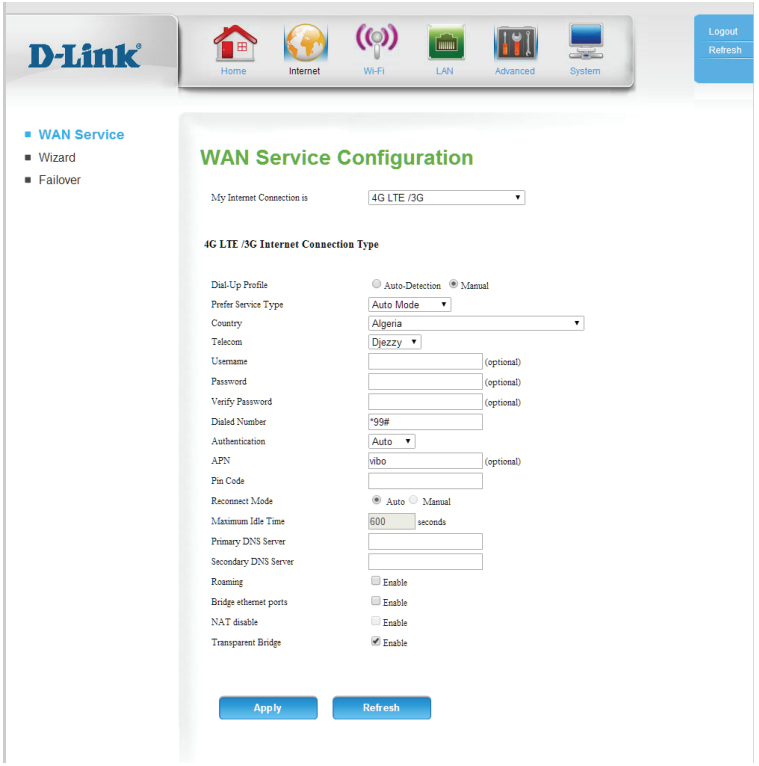
Dialed Number: Enter the number to be dialed.

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

APN: Enter the APN information (optional).

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

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



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

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

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

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

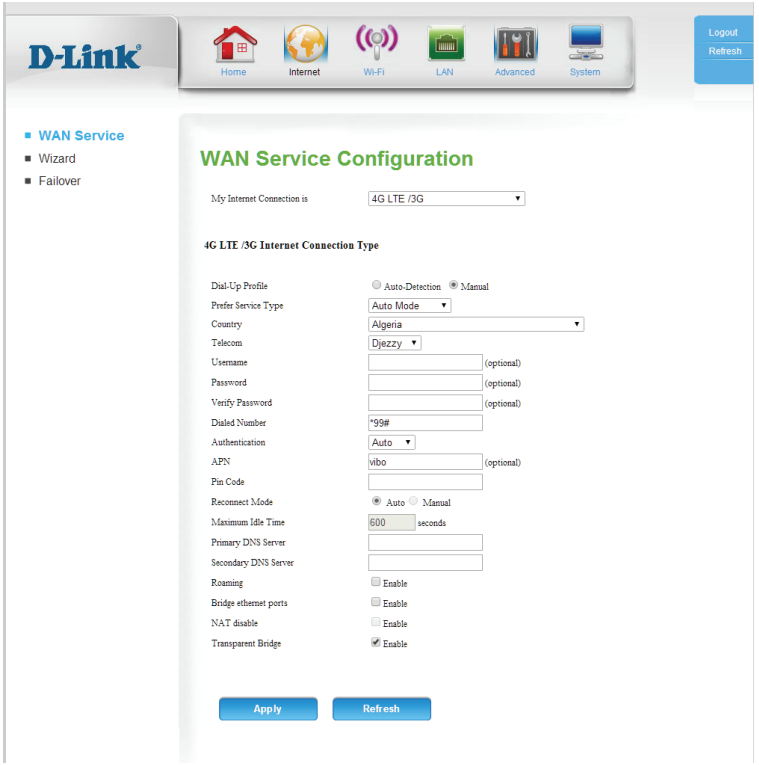
Note: Roaming connections may incur additional fees from your service provider.

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

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

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

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

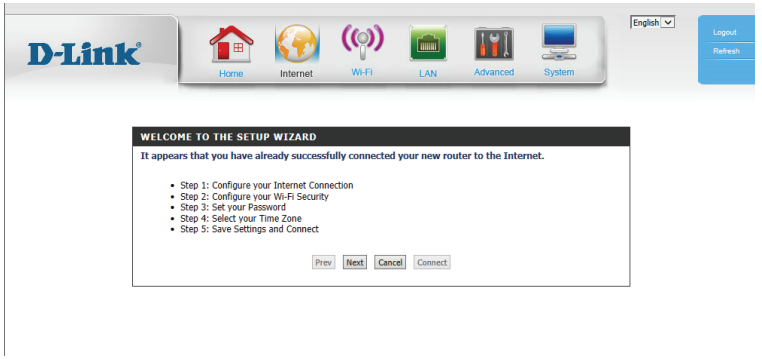


Wizard

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

Click **Next** to continue.

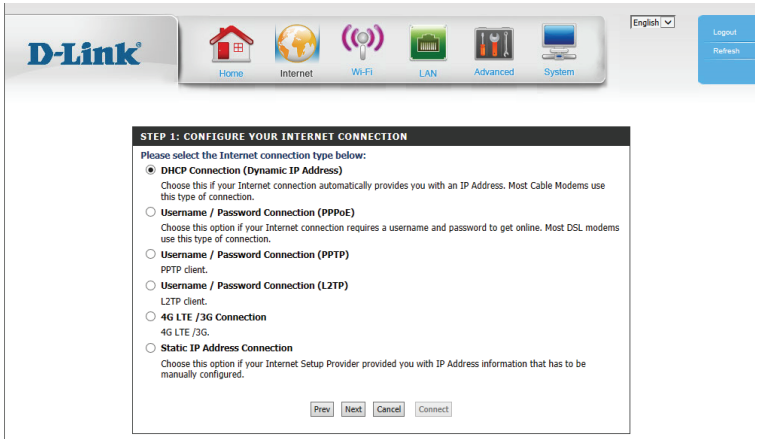
Note: While using the wizard, you can click **Prev** to go back to the previous step, or you can click **Cancel** to close the wizard.



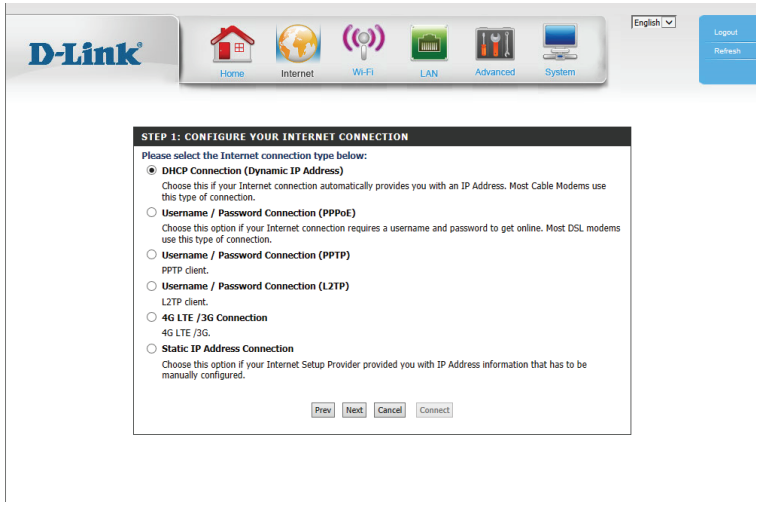
Select the Internet connection type you use. The connection types are explained on the following page. If you are unsure which connection type you should use, contact your Internet Service Provider (ISP).

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

Note: The DWR-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 **Failover** on page 23.



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 8 for information about how to configure this type of connection.

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

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

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

3G/4G Connection: Choose this connection if you have installed a SIM card into the DWR-921. See **4G LTE / 3G** on page 17 for information about how to configure this type of connection.

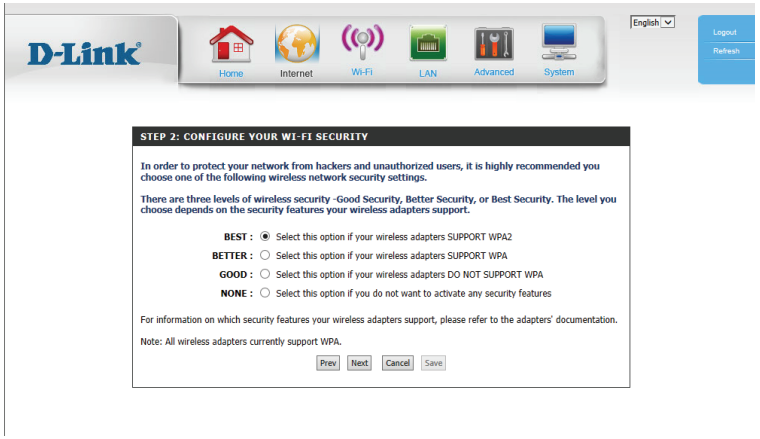
Static IP Address Connection: Choose this option if your Internet Service Provider (ISP) provided you with IP address information that has to be manually configured. See **Static IP** on page 10 for information about how to configure this type of connection.

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

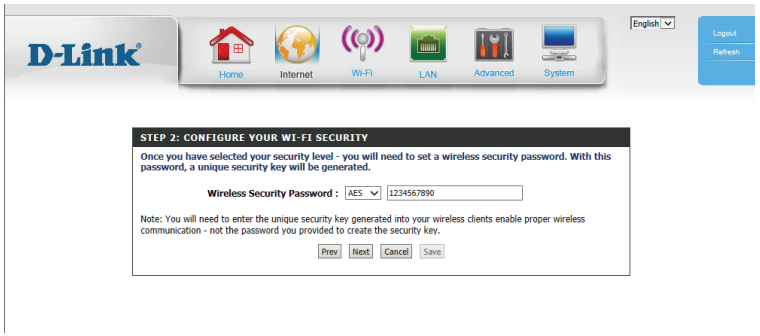
Note: If you are not sure what connection type to use or what settings to enter, check with your Internet Service Provider (ISP).

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

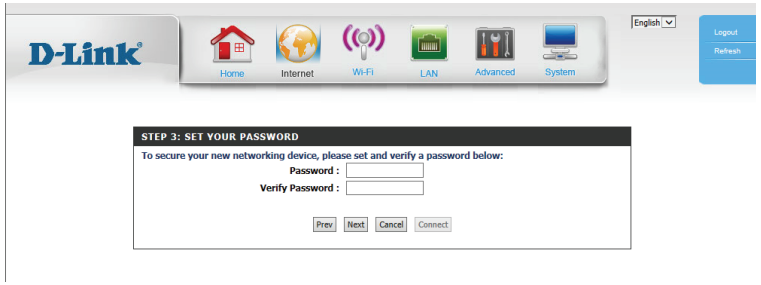
Choose the best security level supported by your wireless clients. Click **Next** to continue.



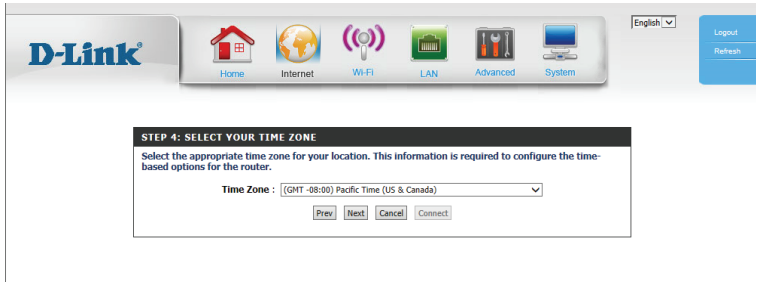
Unless you chose **None** in the previous step, enter a security password. Clients must enter this password to connect to your wireless network. Click **Next** to continue.



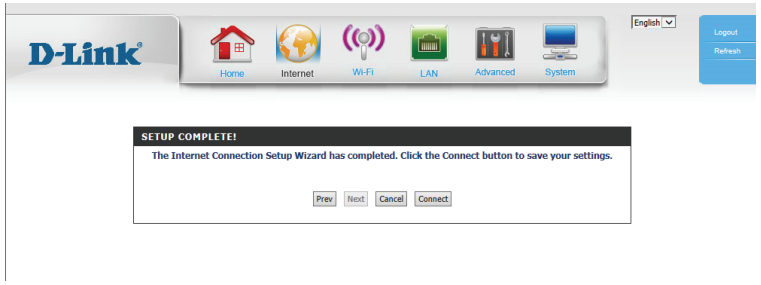
Create a new password and then click **Next** to continue.



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



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



Failover

The DWR-921's WAN failover feature allows the router to switch to a 3G/4G connection as a backup if the WAN connection is down or unavailable.

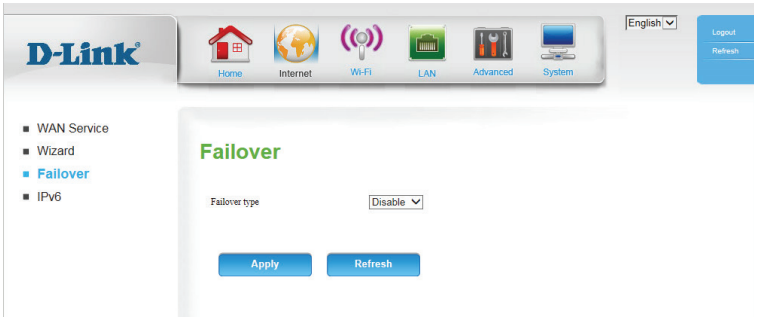
Failover type: Select **Failover** to enable the failover function.

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

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

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

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



IPv6

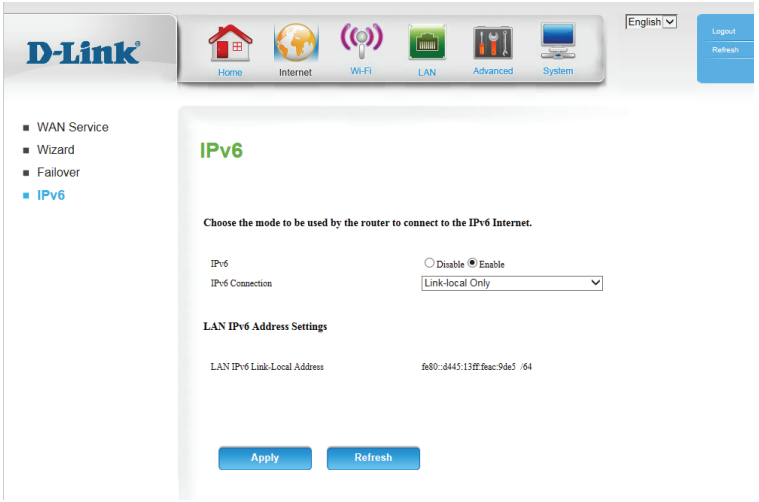
IPv6: To enable IPv6, select **Enable**.

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

Link-local Only

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

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



Static IPv6

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

Subnet Prefix Length: Enter the subnet prefix length.

Default Gateway: Enter the default gateway address.

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

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

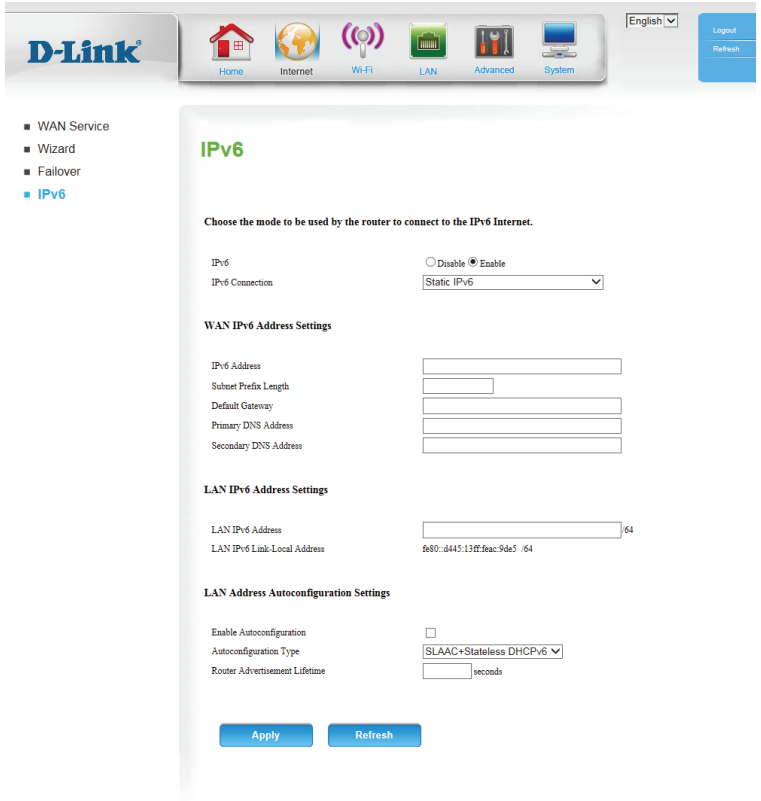
LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Autoconfiguration: Check to enable the autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS**, or **SLAAC + Stateless DHCPv6**.

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

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



Autoconfiguration (SLAAC/DHCPv6)

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

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

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

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

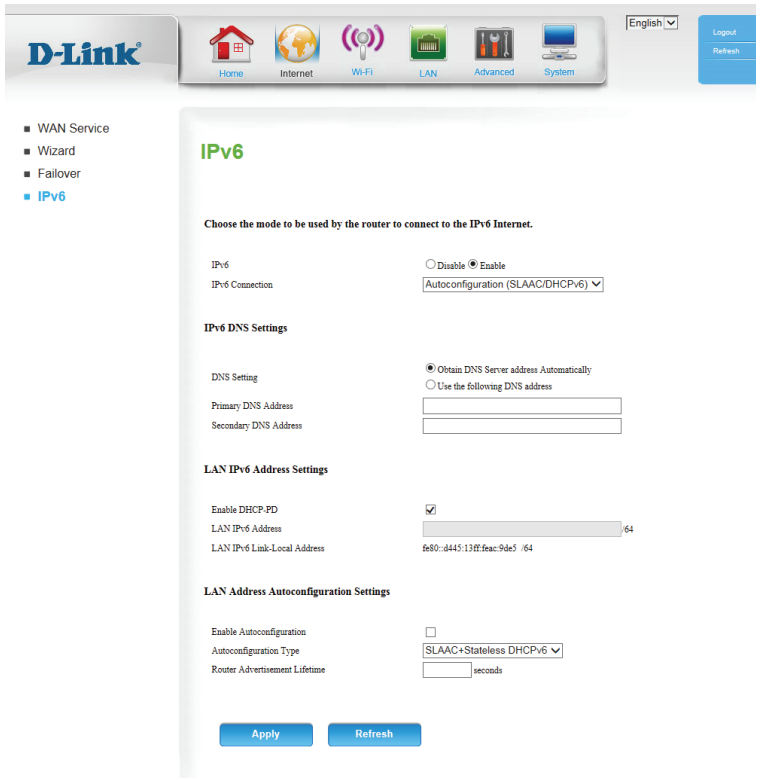
LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Autoconfiguration: Check to enable the autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS**, or **SLAAC + Stateless DHCPv6**.

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

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



PPPoE

Username: Enter your PPPoE user name.

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

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

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

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

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

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

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

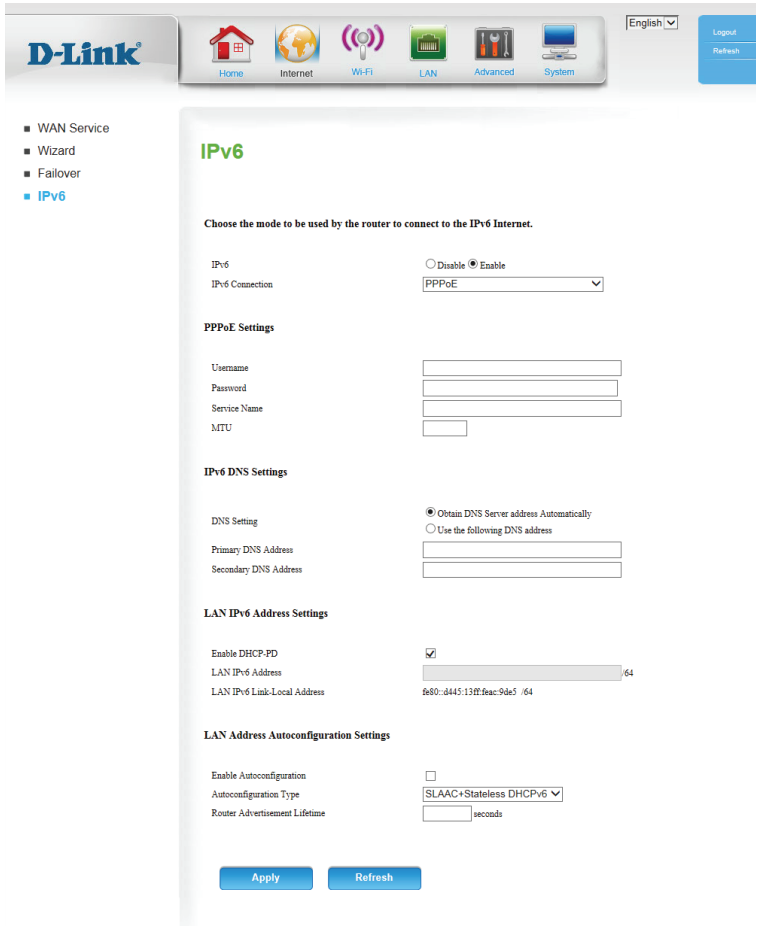
LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Autoconfiguration: Check to enable the autoconfiguration feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS**, or **SLAAC + Stateless DHCPv6**.

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

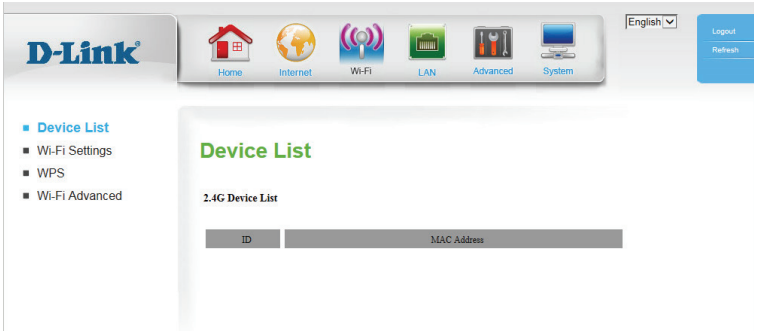
Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



Wi-Fi

Device List

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



Wi-Fi Settings

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

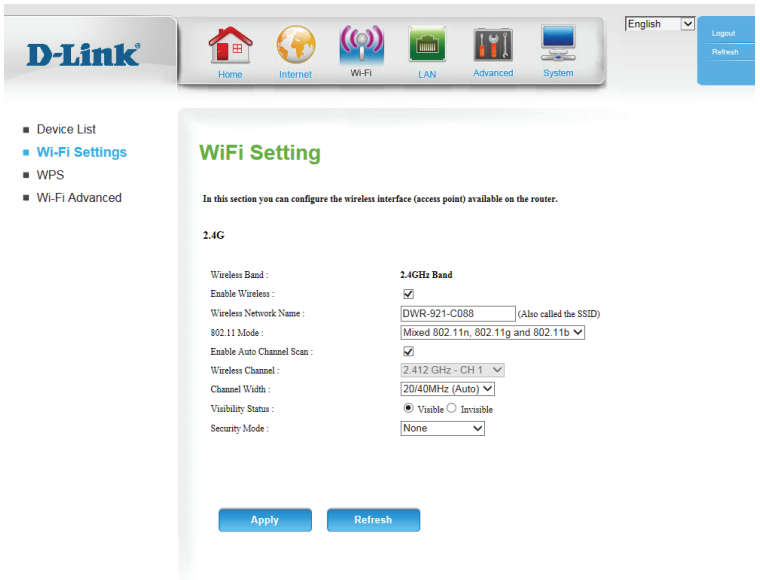
Enable Wireless: Check this box to enable wireless access. When you enable this option, the following parameters take effect.

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

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

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

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



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

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

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

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

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

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

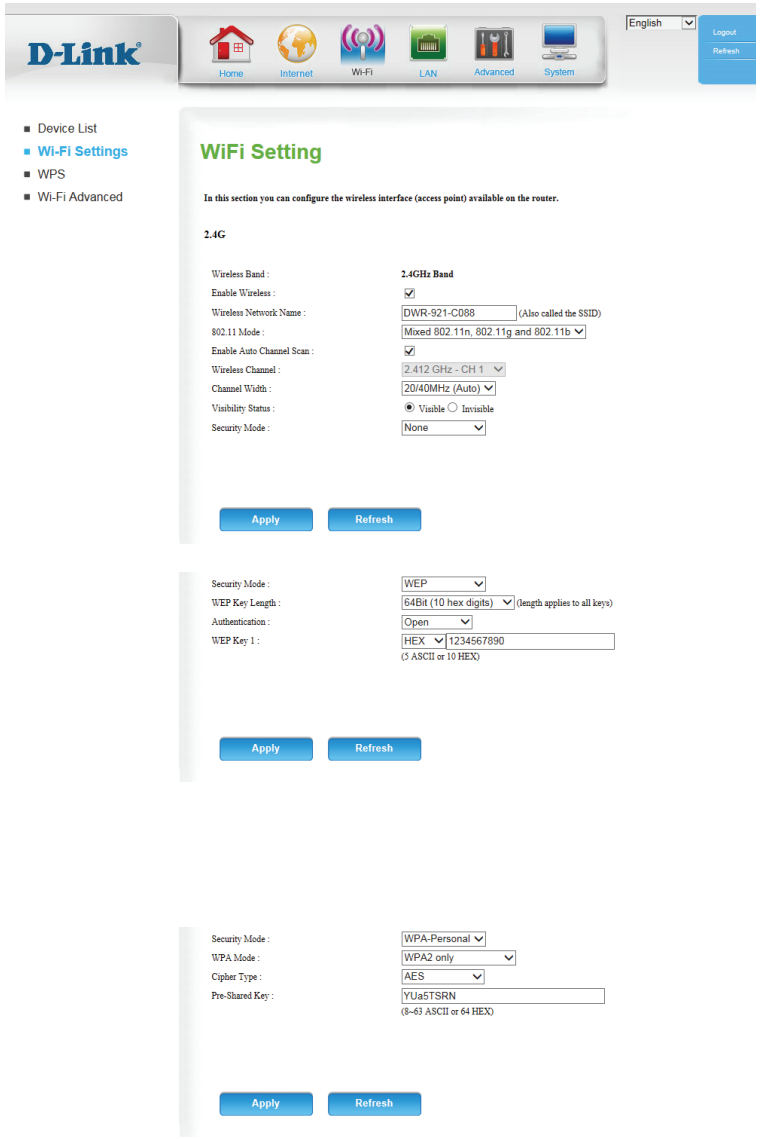
WEP Key 1: Set the WEP key/password for your wireless network. Based on whether you are using 64 or 128-bit encryption, and whether you are using a HEX or ASCII key, you will need to enter different numbers of characters for your key, as indicated below the WEP Key text box. ASCII keys may use letters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

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

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

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



WPS

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

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

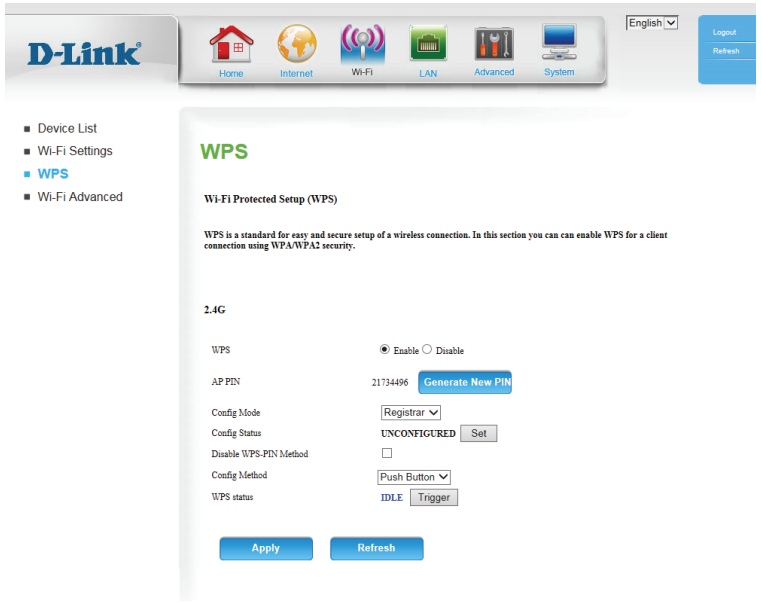
AP PIN: If you use Windows 7's **Connect to a network** wizard to do initial configuration of the router, you will need to enter the WPS PIN/AP PIN into the wizard when prompted. The factory default WPS PIN/AP PIN is printed on a label located on the bottom of the router. You can click the **Generate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

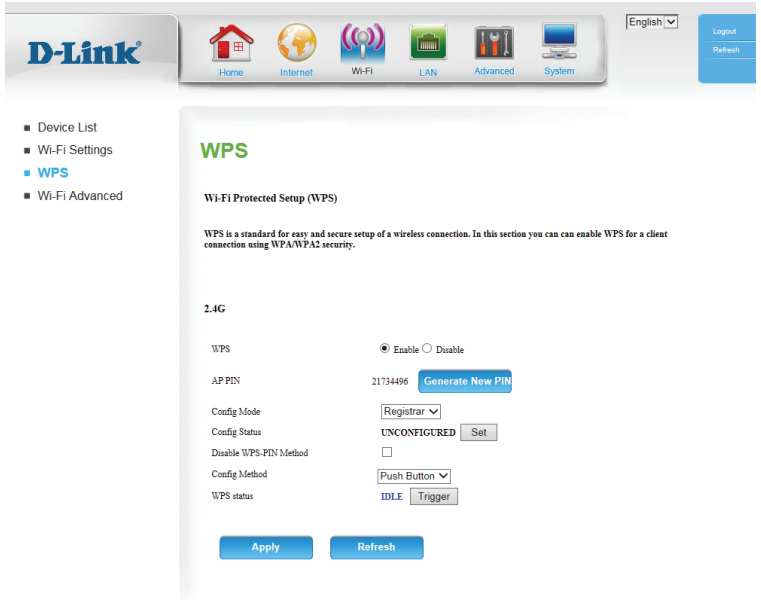
Disable WPS-PIN Method: Enable this option to prevent clients from connecting to the router using the PIN method. If this option is enabled, clients must use the push-button method to connect.



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

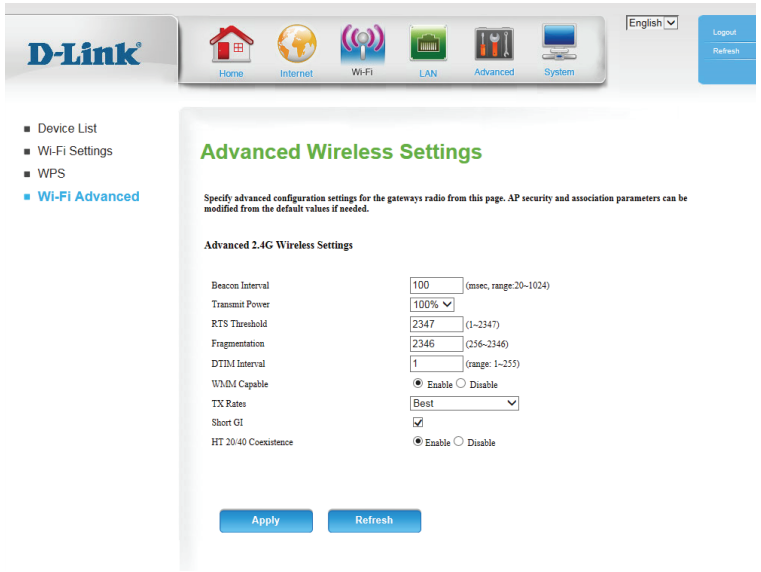
WPS status: This will show the current WPS connection process status. Click the **Trigger** button to initiate a WPS connection.

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



Wi-Fi Advanced

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



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

Transmit Power: Set the transmit power of the antennas.

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

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

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

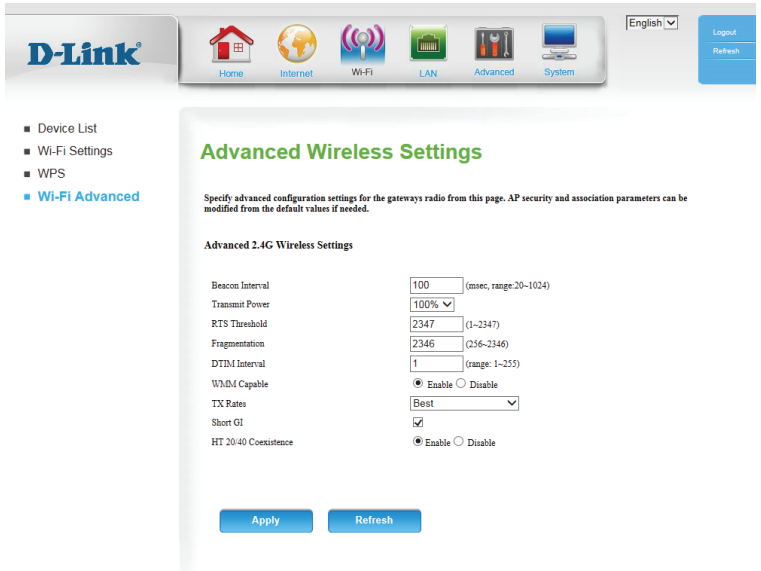
WMM Capable: WMM (Wi-Fi Multimedia) is a QoS (Quality of Service) system for your wireless network. Enable this option to improve the quality of video and voice applications for your wireless clients.

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

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

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

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

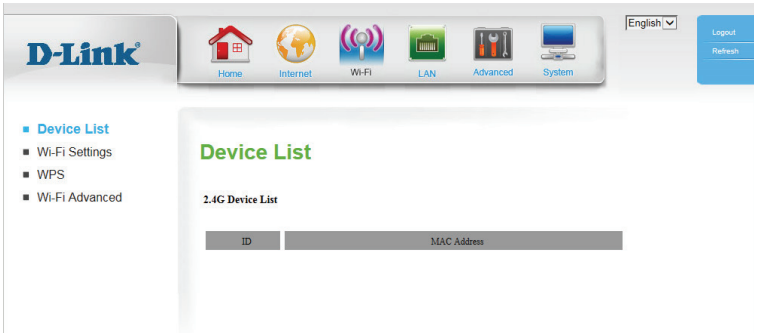


LAN

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

Device List

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



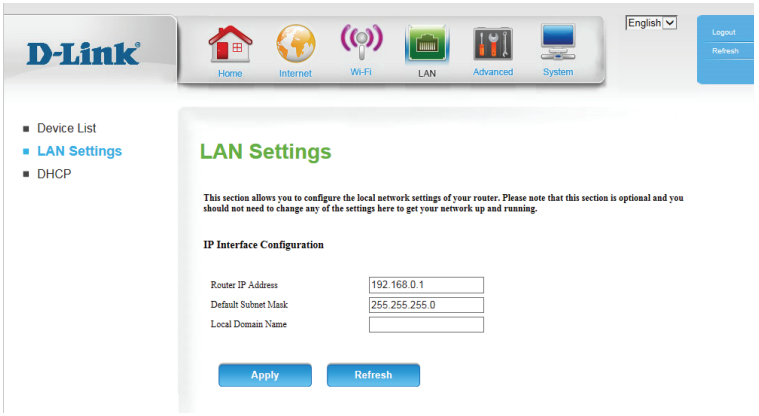
LAN Settings

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

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

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

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



DHCP

The DWR-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 are automatically assigned to the clients on the network.

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

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

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

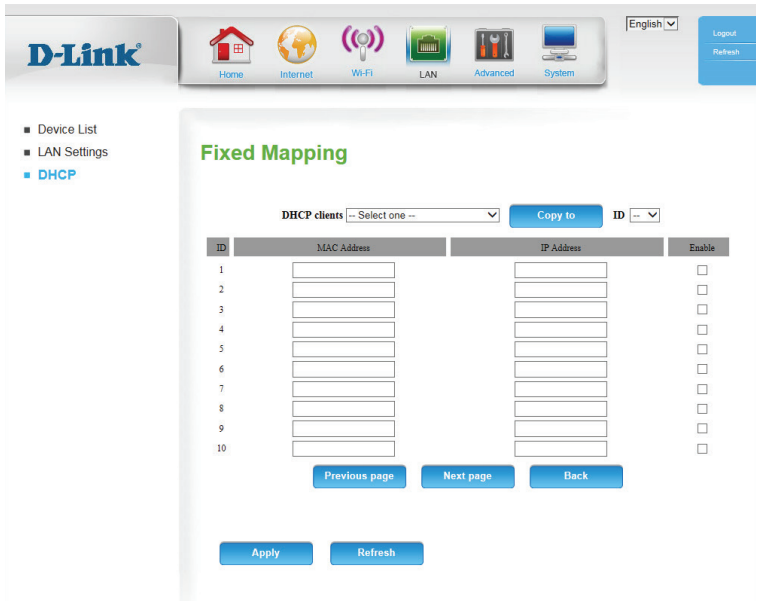
Primary DNS IP Address: Enter the primary DNS IP address that will be assigned to DHCP clients.

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

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

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

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



Advanced

DNS

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

DDNS: Tick this checkbox to enable the DDNS feature.

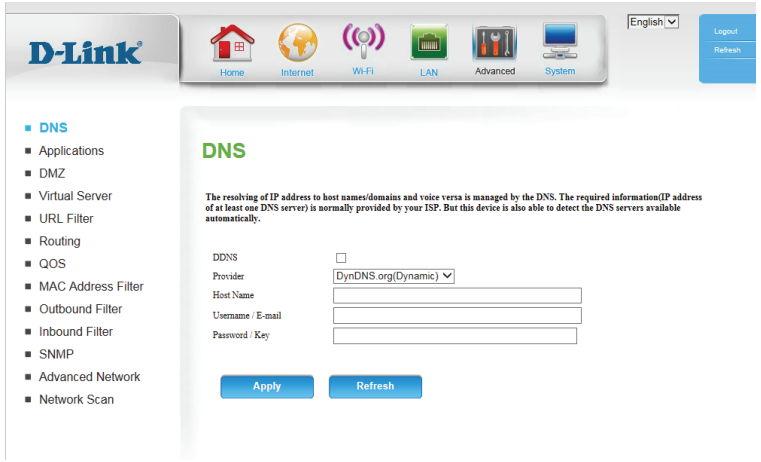
Provider: Select a DDNS service provider to use.

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

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

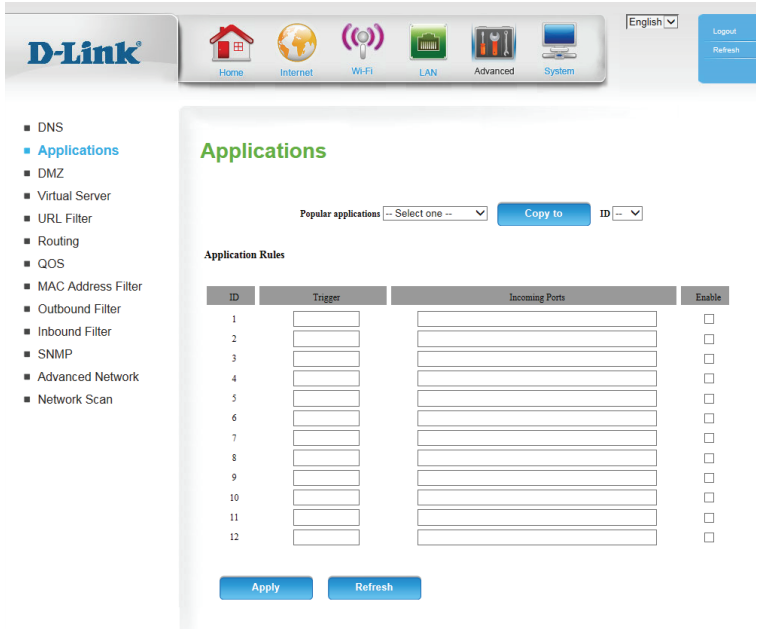
Password / Key: Enter the **Password** for your DDNS account.

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



Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, and Internet telephony. These applications may have difficulty working through NAT (Network Address Translation). **Applications** allows some of these applications to work with the DWR-921 by opening ports after detecting traffic being sent through a trigger port.



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

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

APPLICATION RULES

ID: This identifies the rule.

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

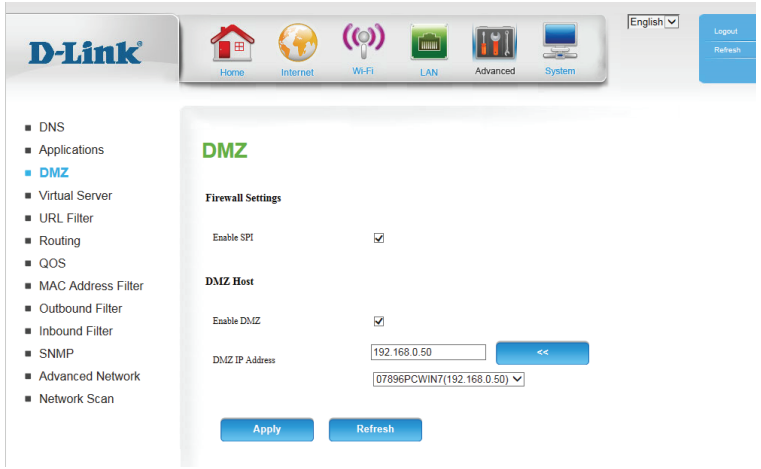
Incoming Ports: Specify the incoming port(s) to open when traffic comes over the **Trigger** port.

Enable: Check the box to enable the specified rule.

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

DMZ

Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable Demilitarized Zone (DMZ). This option will expose the chosen computer completely to the outside world.



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

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

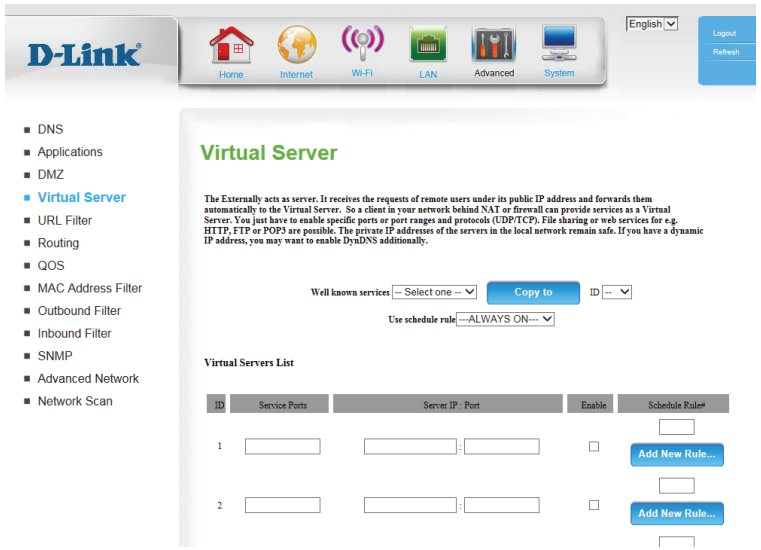
Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

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

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

Virtual Server

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



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

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

Use schedule rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 57.

VIRTUAL SERVERS LIST

ID: This identifies the rule.

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

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

Enable: Check the box to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. To create schedules, click on the **Add New Rule** button. For further information on schedules, please refer to **Schedules** on page 57.

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

URL Filter

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

URL Filtering: Check the box to enable URL Filtering.

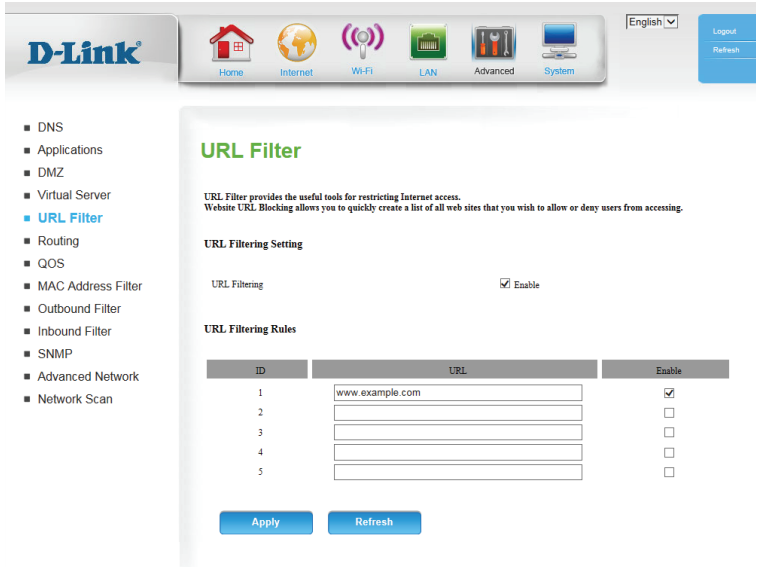
URL FILTERING RULES

ID: This identifies the rule.

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

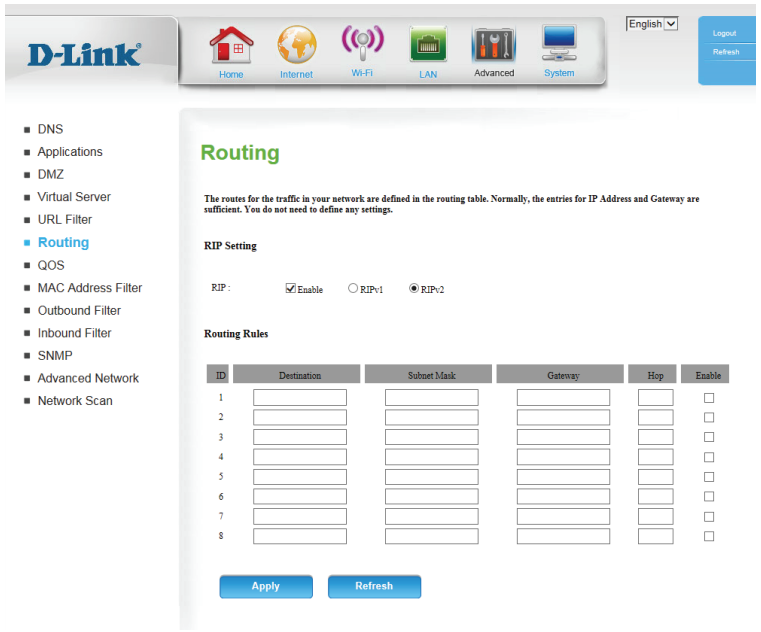
Enable: Check the box to enable the specified rule.

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



Routing

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



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

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

ROUTING RULES

ID: This identifies the rule.

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

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

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

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

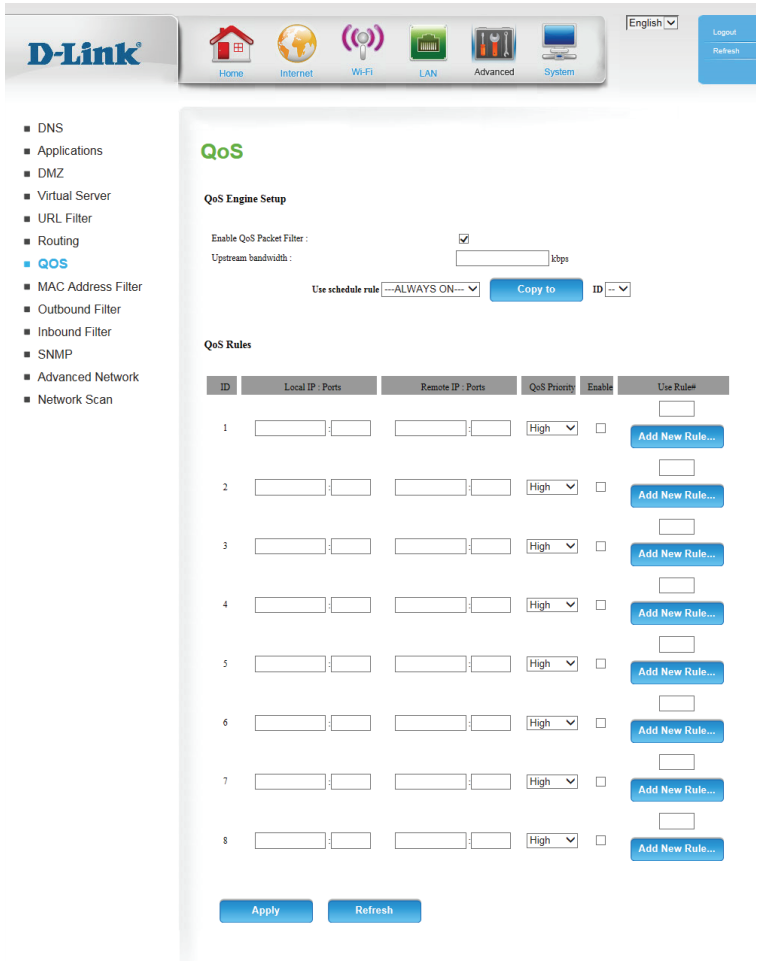
Note: In a transmission path, each link is terminated at a network device such as a router or gateway. The number of hops equals the number of routers or gateways that data must pass through before reaching the destination.

Enable: Select this box to enable the rule.

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

QoS

The **QoS Engine** improves your online gaming or streaming media experience by ensuring that your game or media traffic is prioritized over other network traffic, such as FTP or web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.



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 57.

QOS RULES

ID: This identifies the rule.

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

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

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

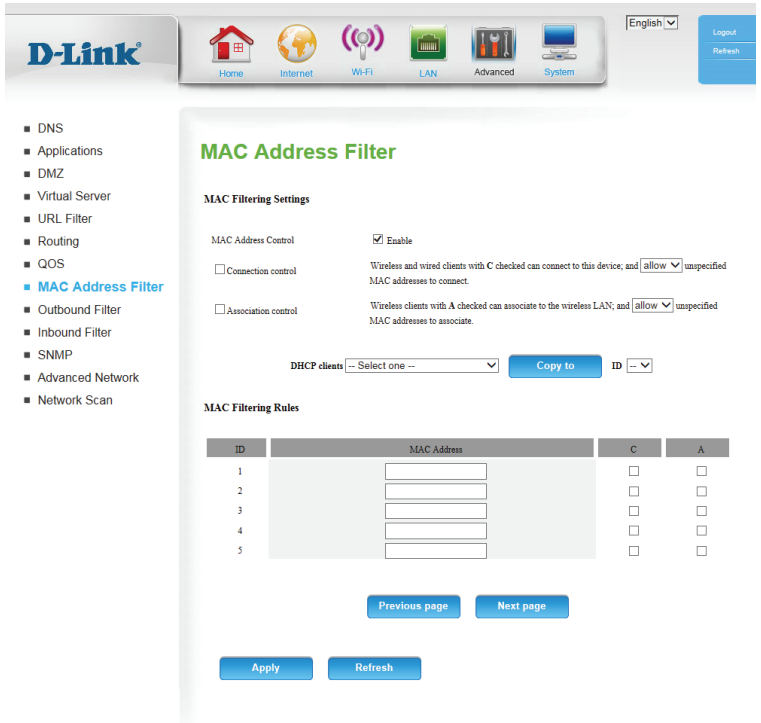
Enable: Check the box to enable the specified rule.

Use Rule #: Specify the schedule rule number. To create a new schedule, click on the **Add New Rule** button. For more information about schedules, please refer to **Schedules** on page 57.

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



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

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

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

MAC FILTERING RULES

ID: This identifies the rule.

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

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

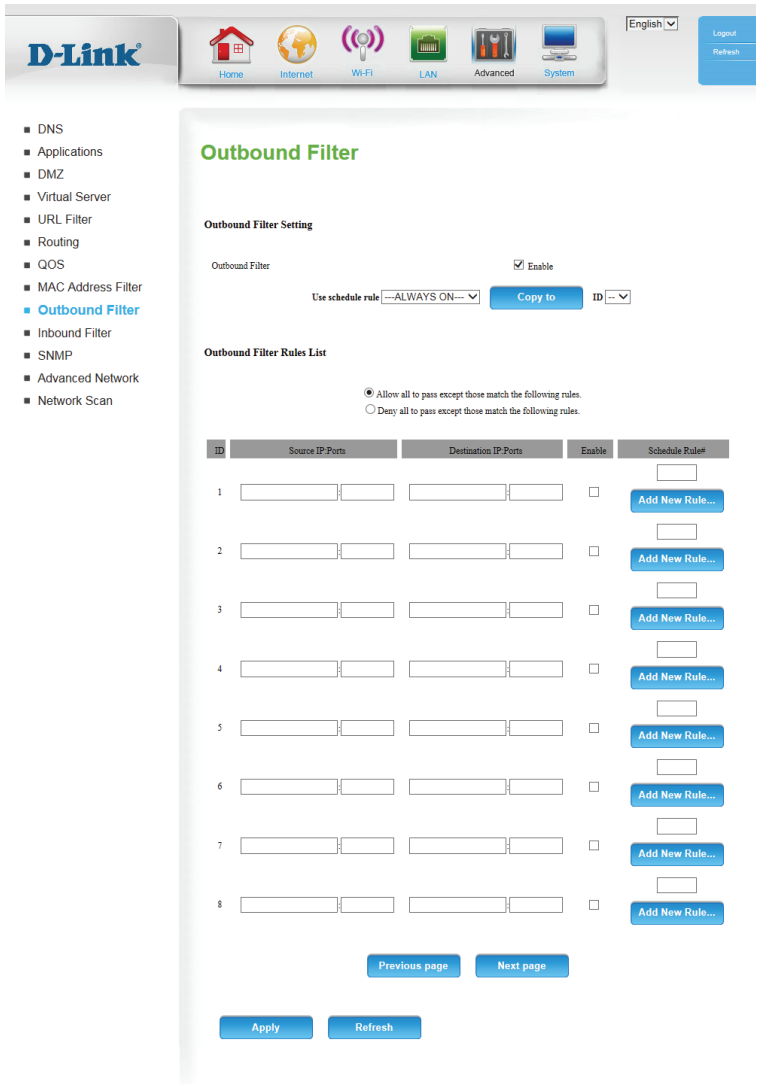
C: If this box is ticked, the rule will follow the connection control setting specified in MAC filtering settings specified above.

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

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

Outbound Filter

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



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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 57.

OUTBOUND FILTER RULES LIST

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

ID: This identifies the rule.

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

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

Enable: Check the box to enable the specified rule.

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

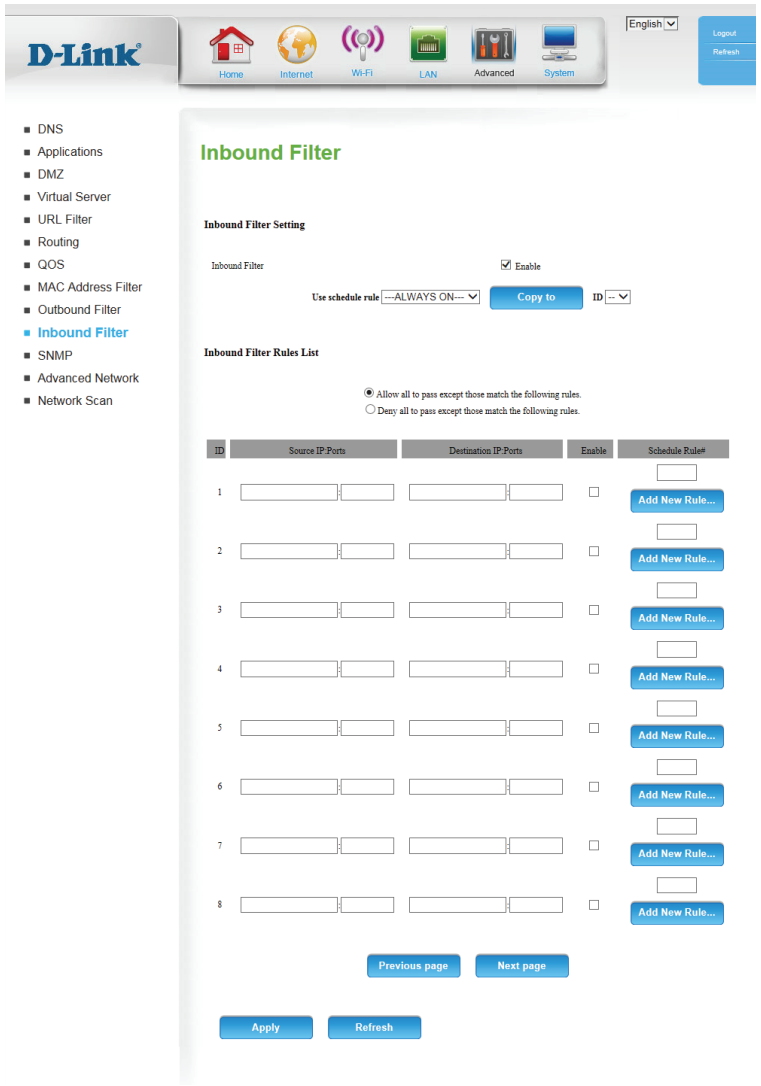
Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

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

Inbound Filter

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



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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 57.

INBOUND FILTER RULES LIST

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

ID: This identifies the rule.

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

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

Enable: Check the box to enable the specified rule.

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

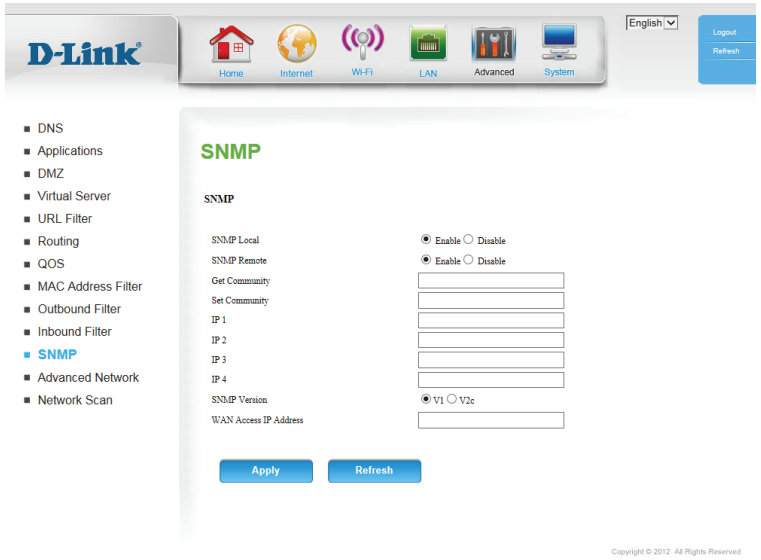
Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

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

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.



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.

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

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

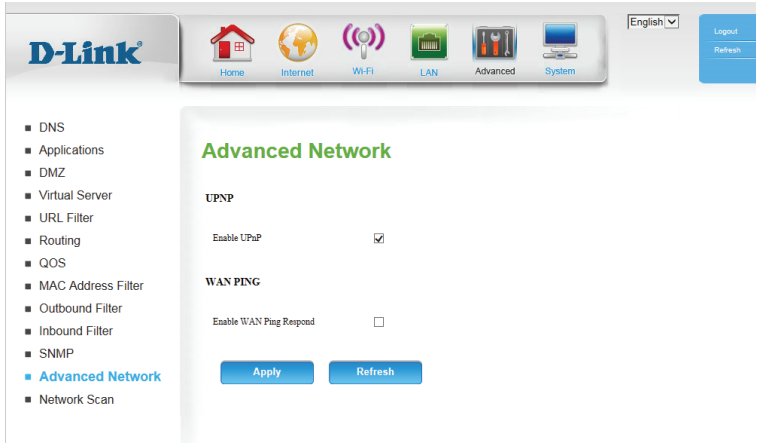
Advanced Network

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

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

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

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



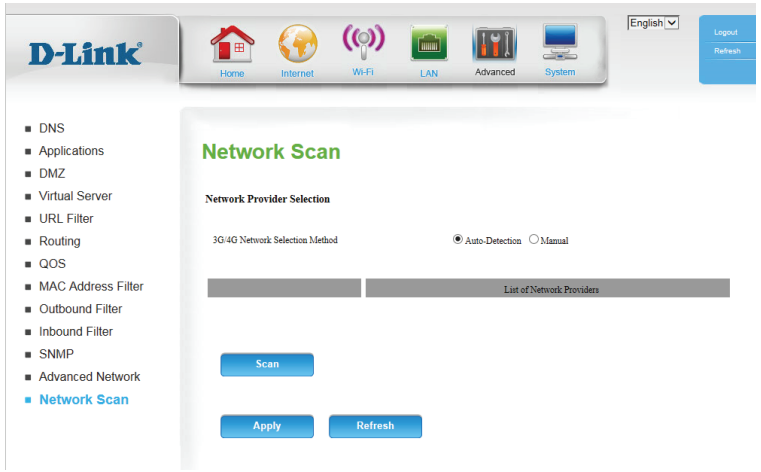
Network Scan

This page lets you set whether to allow the DWR-921 to automatically select a 3G/4G network based on the inserted SIM card, and allows you to manually scan for networks and select one to connect to.

3G/4G Network Selection Method: Leave this setting on **Auto** to allow the DWR-921 to automatically select a cellular network to connect to. If you need to select a network manually, select **Manual**, click the **Scan** button, then select an available network to connect to.

Note: You will only be able to scan for networks if the DWR-921 is not currently connected to a 3G/4G network.

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



System

Time Settings

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

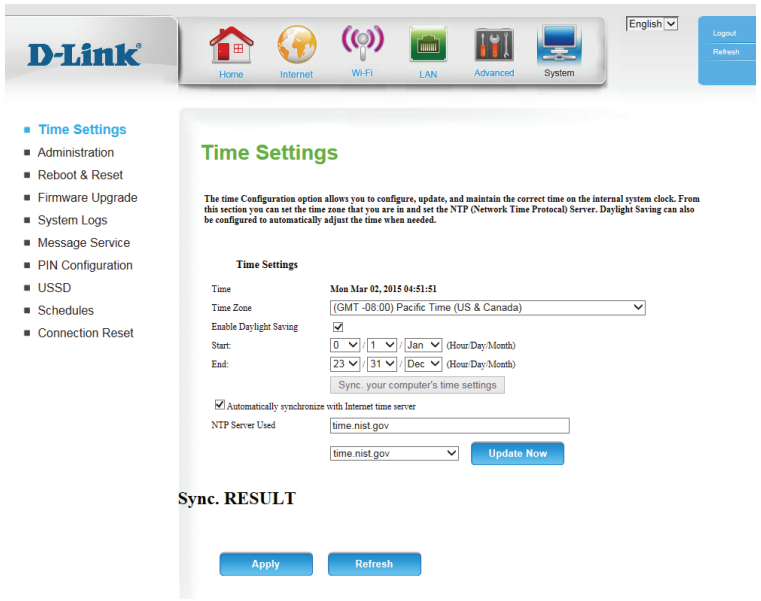
Time Zone: Select the appropriate **Time Zone** from the drop-down box.

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

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

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

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



Administration

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

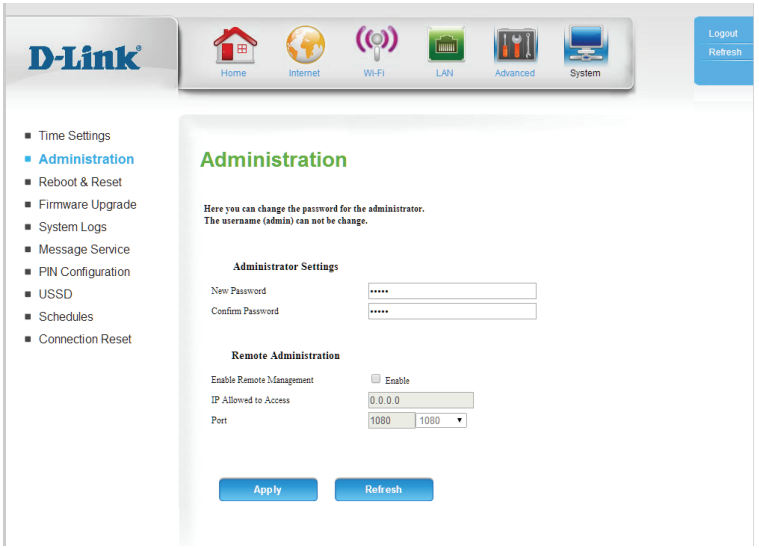
Admin Password: Enter and confirm the password that the admin account will use to access the router's management interface.

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

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



Reboot & Reset

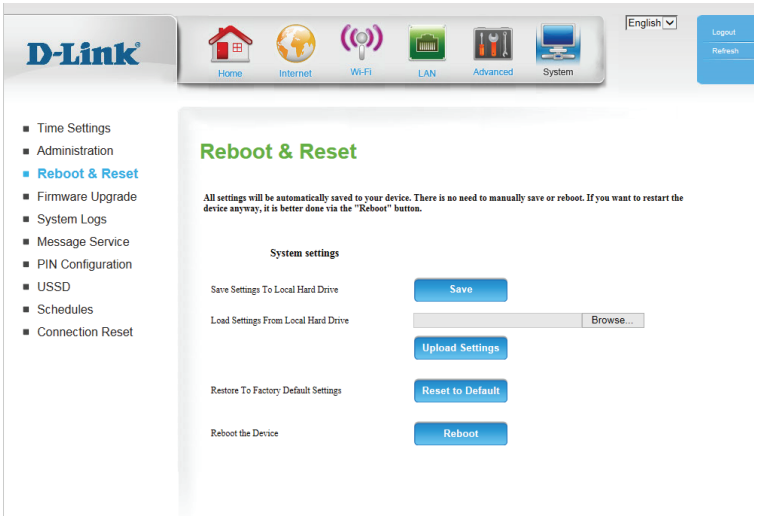
Here, you can save the current system settings to a local hard drive.

Save Settings To Local Hard Drive Use this option to save your current router configuration settings to a file. Click **Save** to open a file dialog, and then select a location and file name for the settings.

Load Settings From Local Hard Drive: Use this option to load previously saved router configuration settings. Click **Browse...** and select the saved file and then click the **Upload Settings** button to upload the settings to the router.

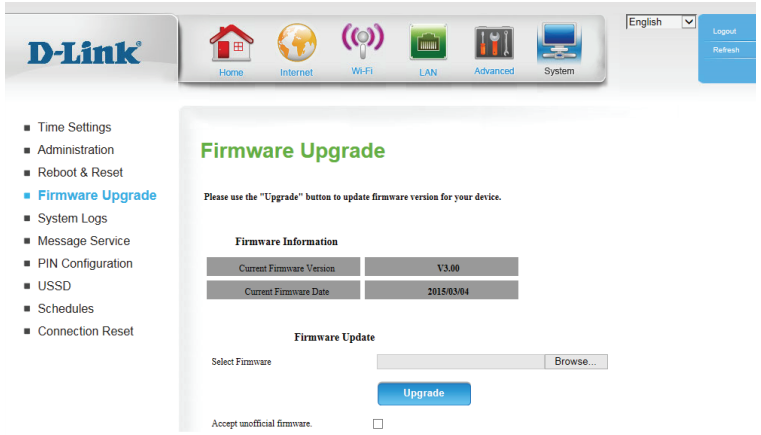
Restore To Factory Default Settings: This option will restore all settings back to their defaults. Any settings that have not been backed up will be lost, including any rules that you have created.

Reboot the Device: This option will reboot the router.



Firmware Upgrade

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



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

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

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

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

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

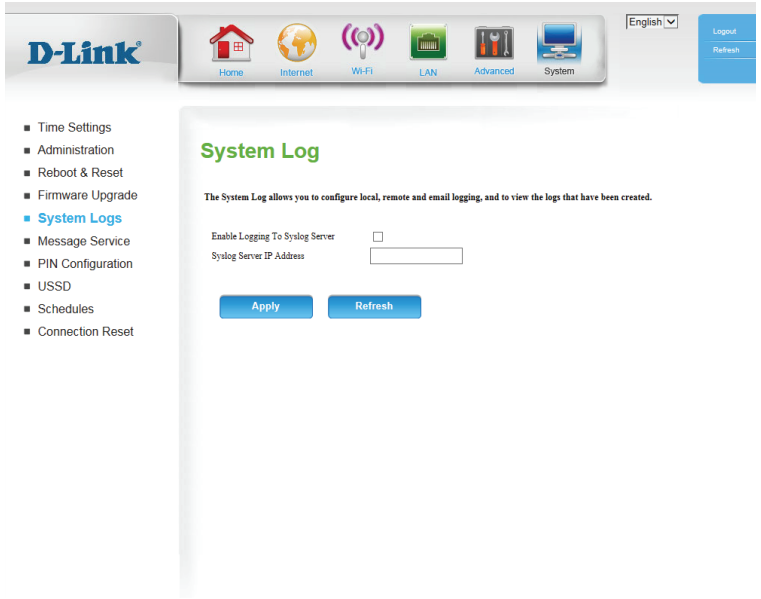
System Log

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.

Enable Logging to Syslog Server: Check the box to send the router logs to a Syslog server.

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

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



Message Service

SMS Inbox

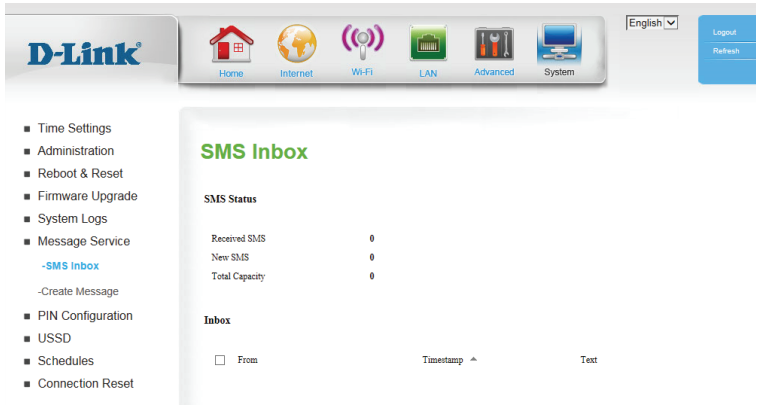
This page shows all messages that are stored on the SIM card. Select a message to display its contents in the SMS window. After you read it, you can delete it, or reply to the sender. Click the Refresh button to update the list.

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

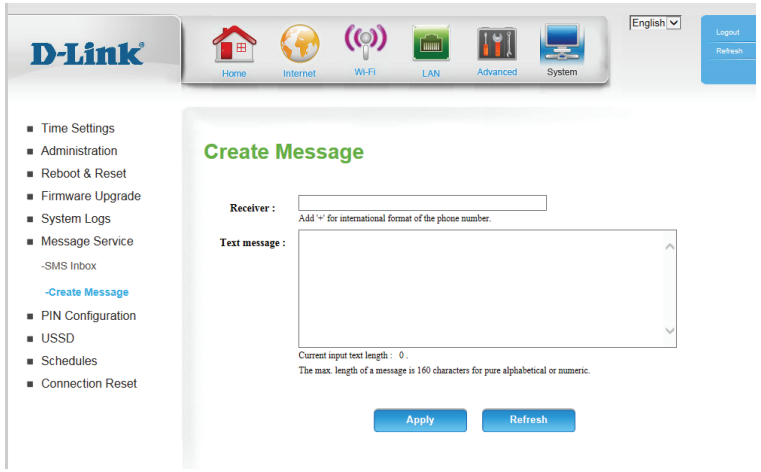
This page allows you to send an SMS to your contacts. Just fill in the phone number of the recipient, and type the content of message. Then click the "Send Message" button to send out this message. If you would like to add more than one recipient, you must put a semicolon (;) between each of the phone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

Receiver: Type the phone number of the recipient.

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

Apply: Click this button to send the message.

Refresh: Click this button to clear the message.

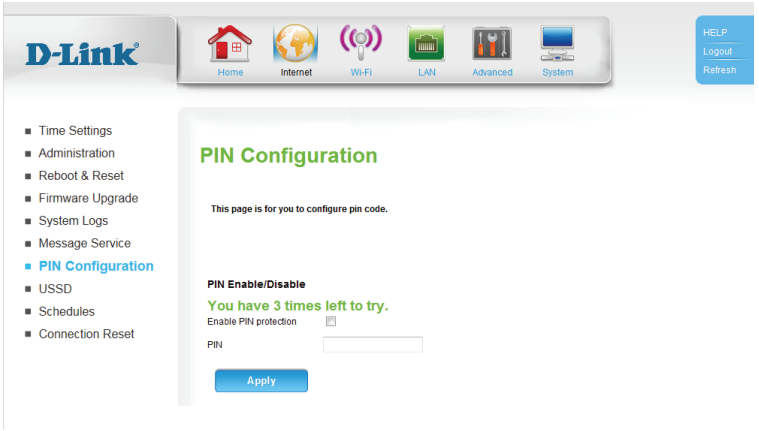


PIN Configuration

On this page you can configure your SIM card's PIN.

To change your SIM's PIN, enter the new PIN in the **PIN** text field. If you also wish to enable or disable PIN protection, check **Enable PIN protection**. This will mean that you have to input your PIN whenever a device using your SIM card is switched on.

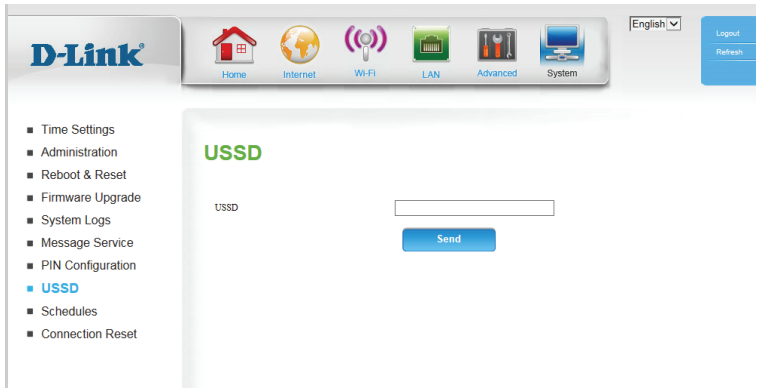
Click **Apply** when you are done.



USSD

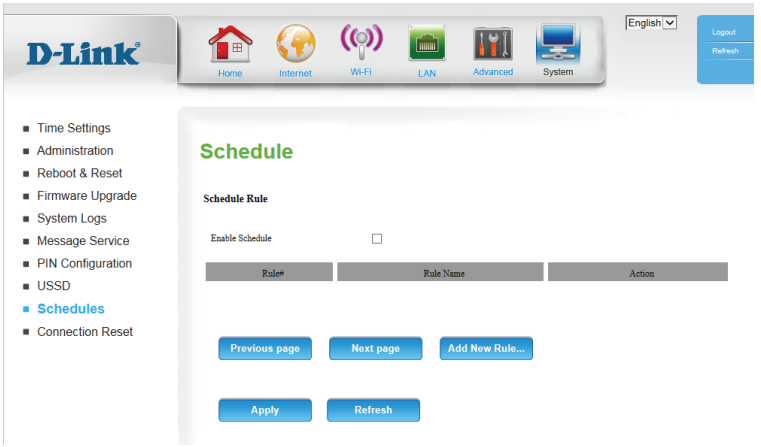
Unstructured Supplementary Service Data (USSD) allows ISP-specific applications to be activated with an SMS message.

USSD: Enter an application activation code and click **Send**. This will allow you to activate applications by sending an SMS message to your ISP.



Schedules

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



Enable Schedule: Check this box to enable schedules.

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

Delete: Click this icon to delete the selected rule.

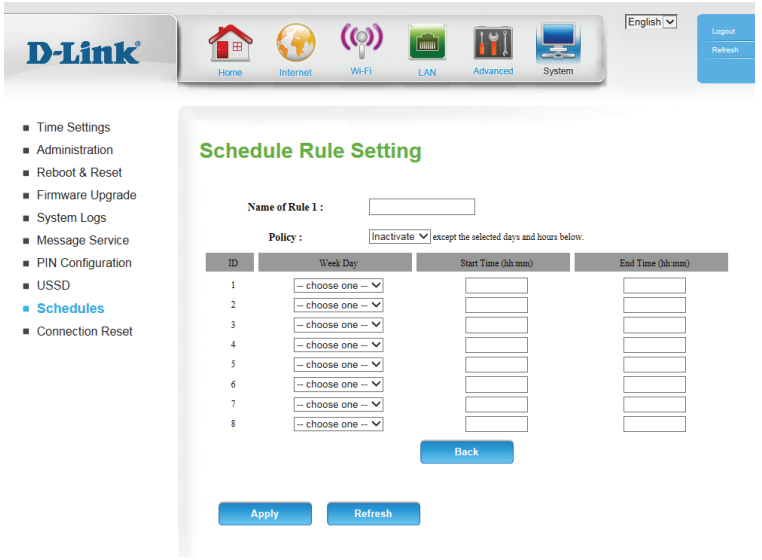
Previous Page: Click this button to go to the previous page of rules.

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

Click this button to specify the start time, end time, and name of the rule.

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

Add New Rule



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

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

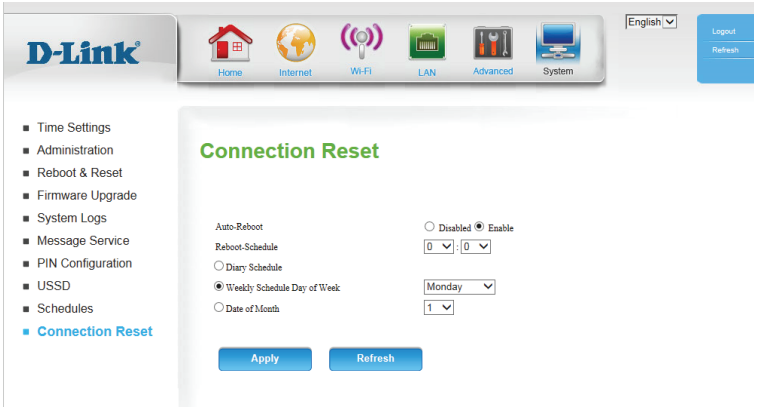
Week Day: Select a day of the week for the start time and end time.

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

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

Connection Reset

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



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

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

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

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

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

Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is with WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DWR-921 router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the DWR-921 for about 1 second. The Internet LED on the front will start to blink.

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

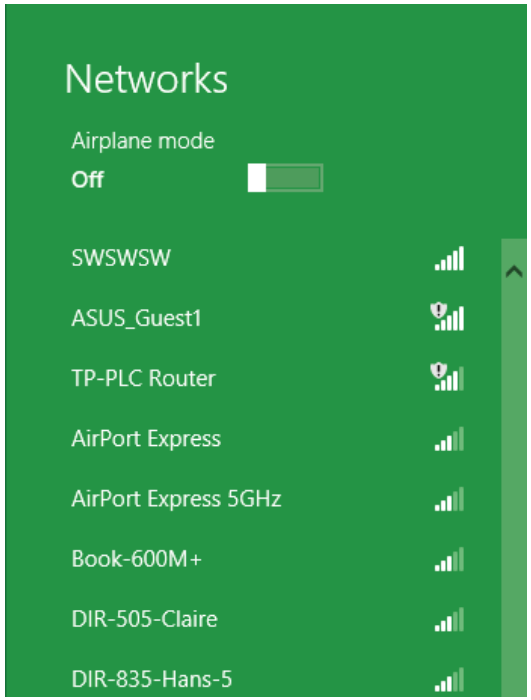
Step 3 - Allow up to 1 minute for your connection to be configured. Once the Internet light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

Windows® 8
WPA/WPA2

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

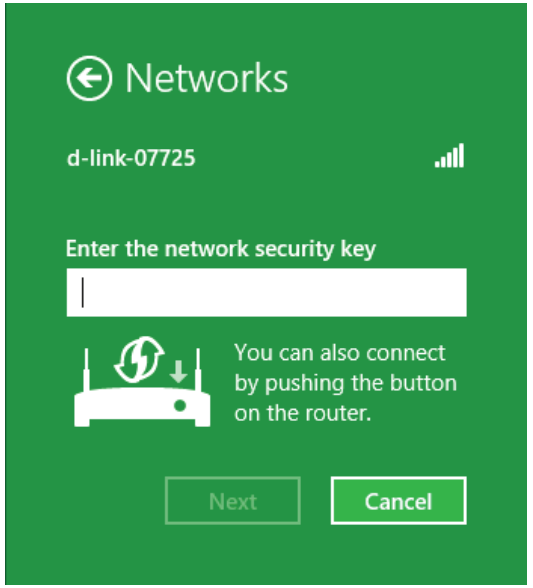
To join an existing network, locate the wireless network icon in the taskbar next to the time display.

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

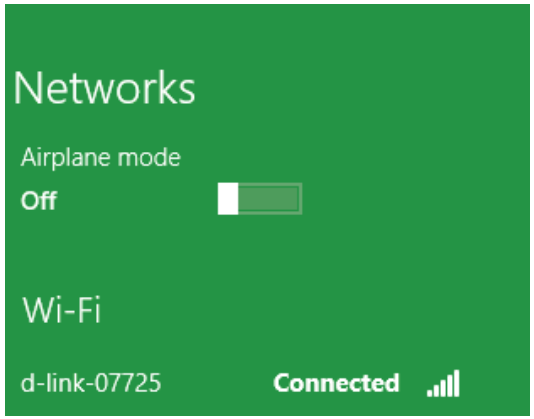


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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



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



Windows® 7
WPA/WPA2

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

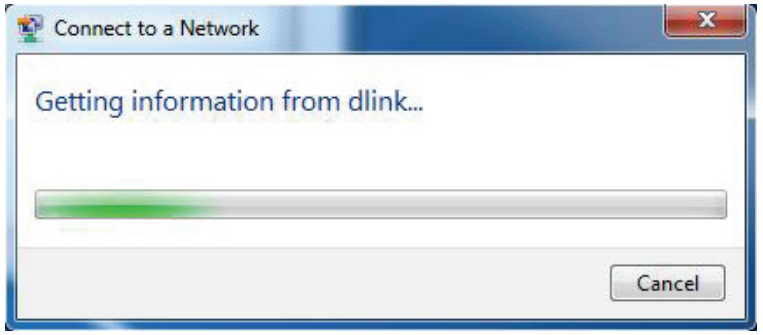
1. Click on the wireless icon in your system tray (lower-right corner).

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

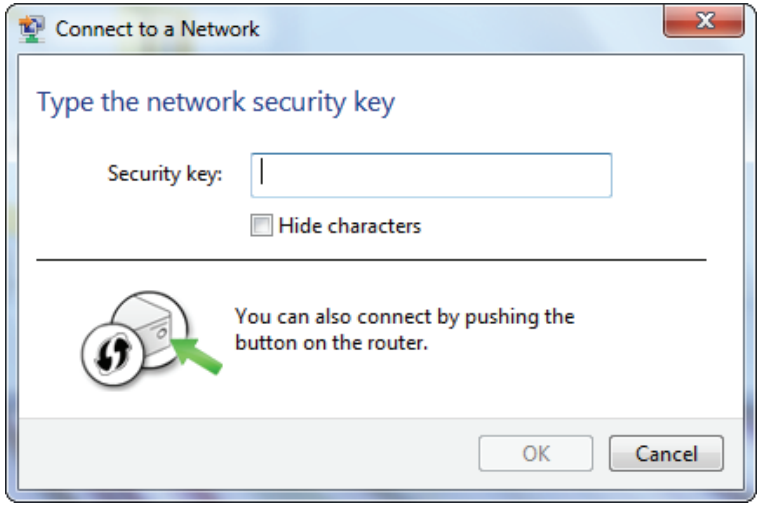
3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to **Networking Basics** on page 84 for more information.

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



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

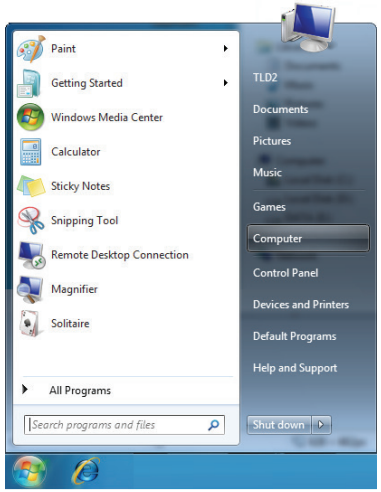


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as the one on the wireless router.

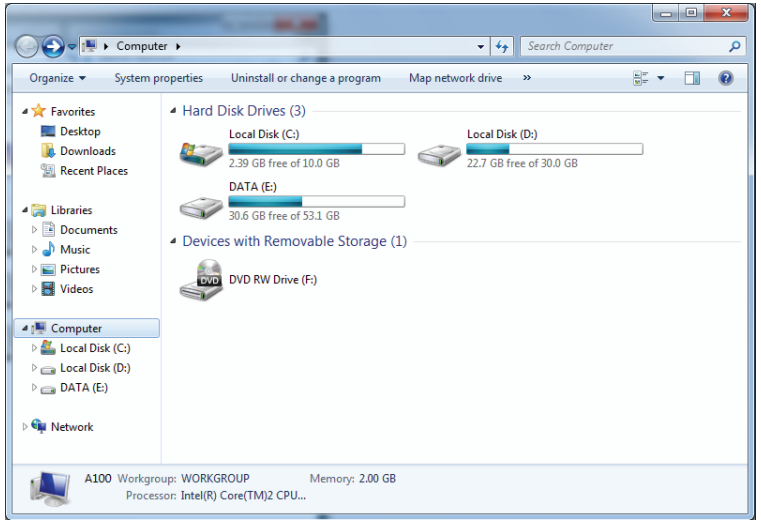
WPS

The WPS feature of the DWR-921 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

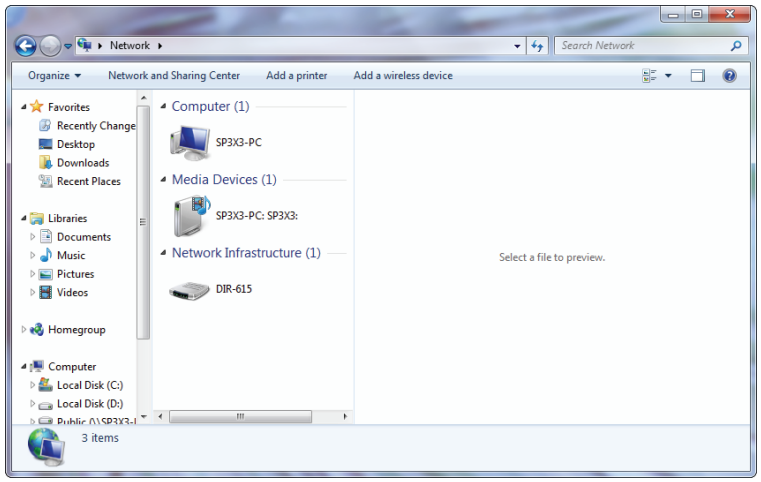
1. Click the **Start** button and select **Computer** from the Start menu.



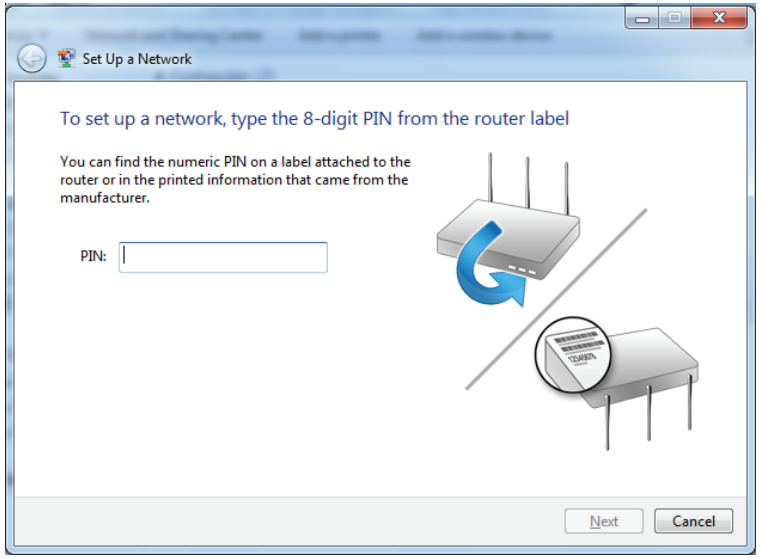
2. Click **Network** on the left side.



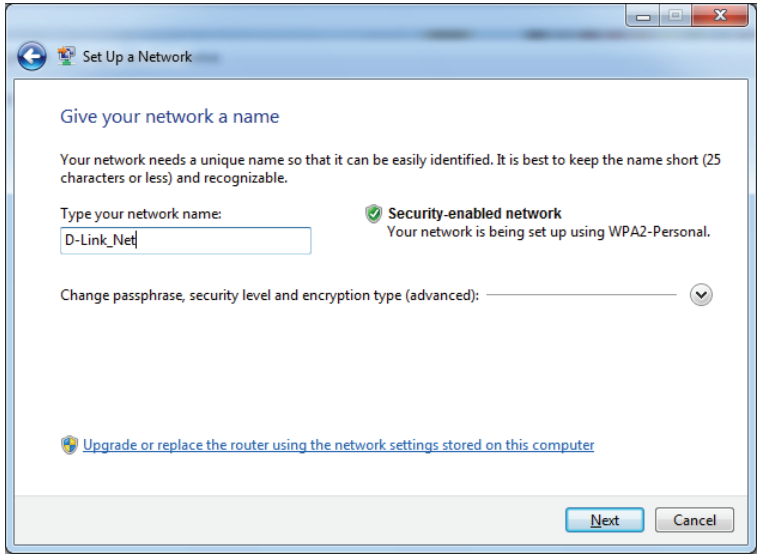
3. Double-click the DWR-921.



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

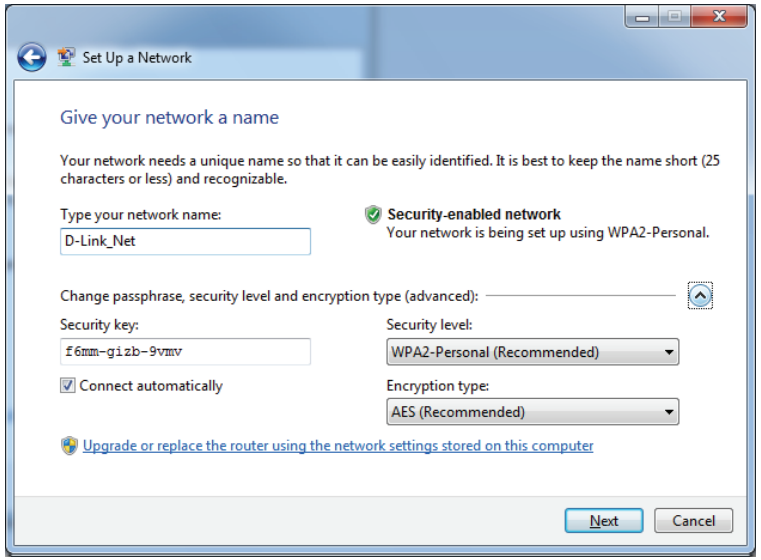


5. Type a name to identify the network.



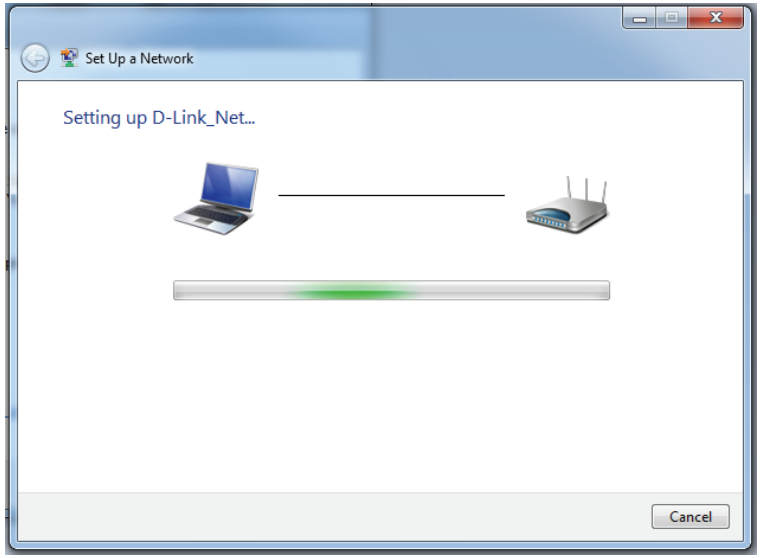
6. To configure advanced settings, click the icon.

Click **Next** to continue.



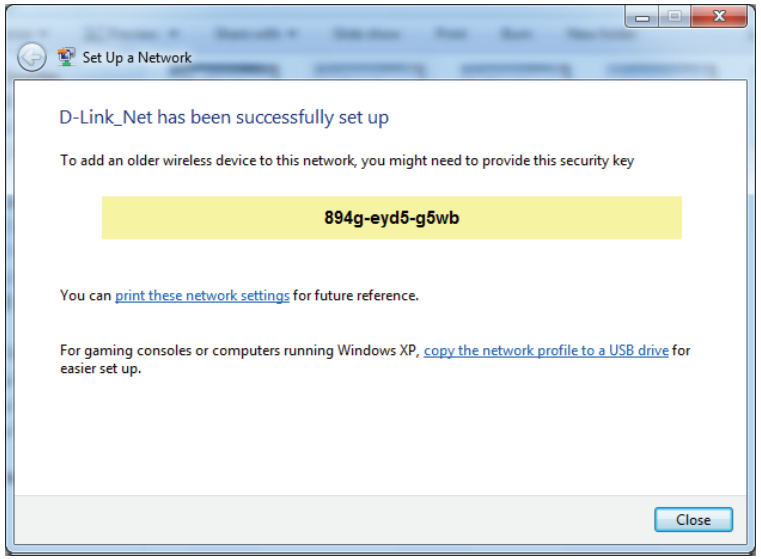
7. The following window appears while the router is being configured.

   Wait for the configuration to complete.



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

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



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

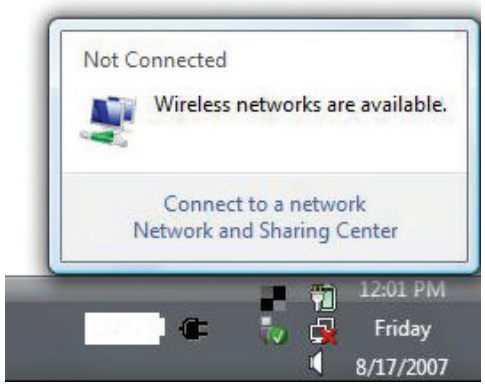
Windows Vista®

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

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

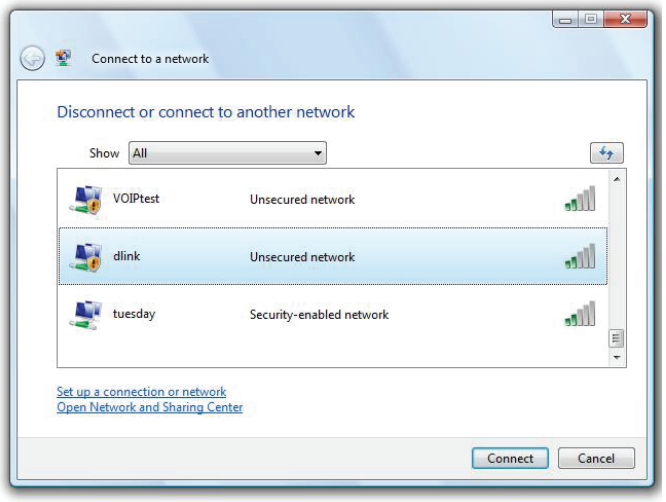
or

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



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

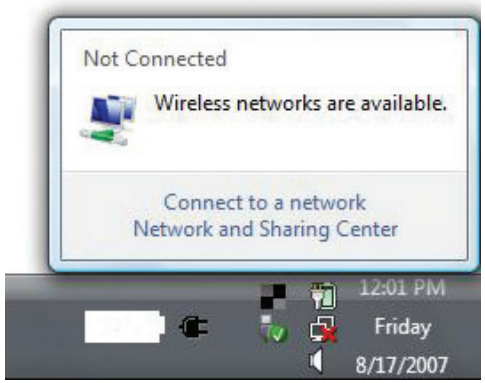
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



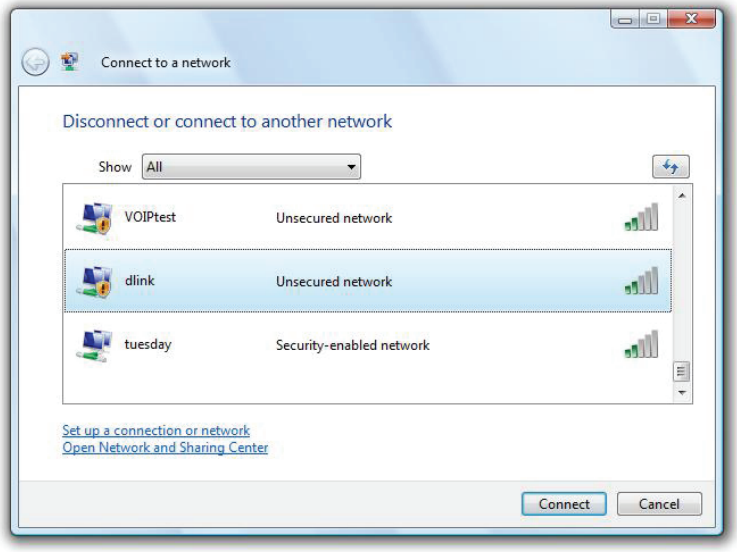
WPA/WPA2

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

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



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



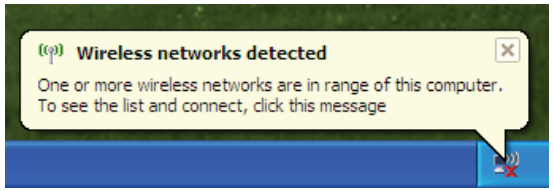
3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

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

Windows® XP

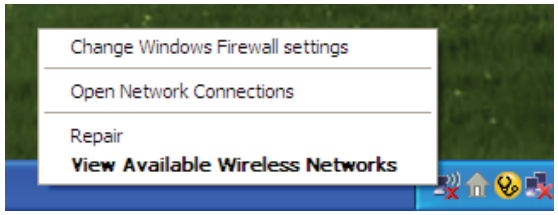
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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

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



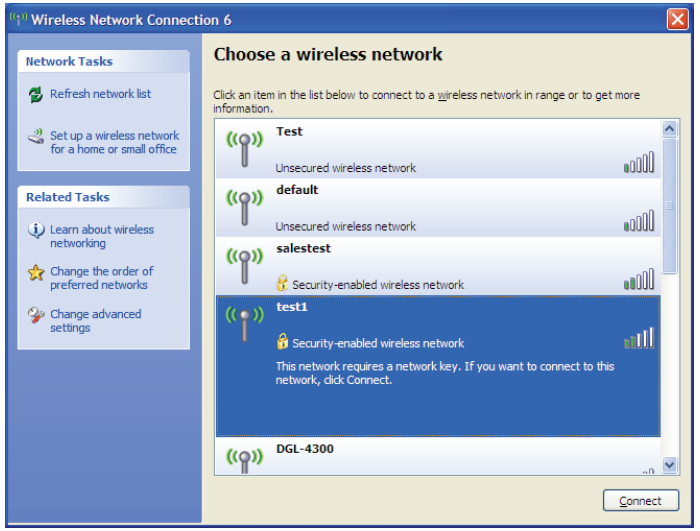
or

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



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

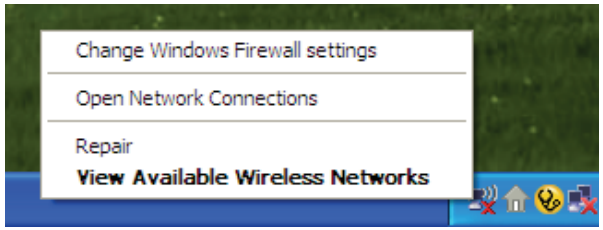
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



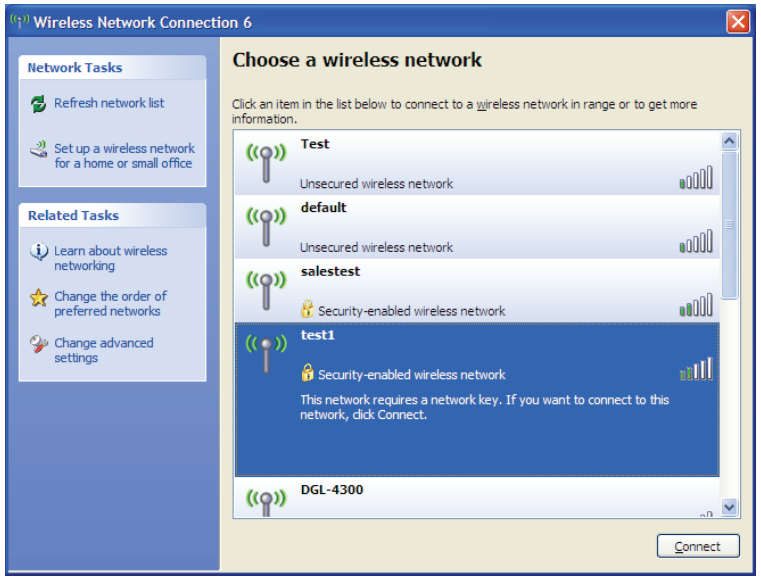
WPA/WPA2

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

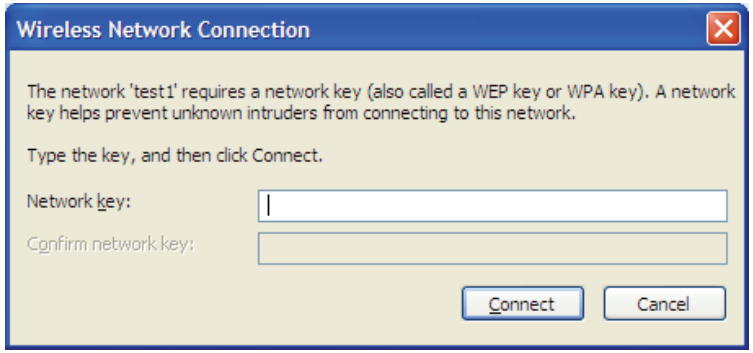
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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



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



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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-921. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to these examples.

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

When entering the IP address of the D-Link router (**192.168.0.1** for example), you are not connecting to a website, nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:

  - Microsoft Internet Explorer® 7 or higher
  - Mozilla Firefox 3.5 or higher
  - Google™ Chrome 8 or higher
  - Apple Safari 4 or higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable, or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

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

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

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

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

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

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

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

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

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

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

```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

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

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

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

C:\>
```

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

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

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

- Navigate to the Internet configuration page (see **Internet** on page 8 for details).
- To change the MTU, enter the number in the MTU field and click **Apply** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home Uses/Benefits

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

Small Office and Home Office Uses/Benefits

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

Where is wireless used?

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

Using a D-Link CardBus Adapter with your laptop, you can access the hotspot to connect to the Internet from remote locations like: airports, hotels, coffee shops, libraries restaurants, and convention centers.

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

Tips

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

Centralize your router or access point

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

Eliminate interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad hoc** – Directly connecting to another computer for peer-to-peer communication using wireless network adapters on each computer, such as two or more DWR-921 wireless network CardBus adapters.

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

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

Networking Basics

Check your IP address

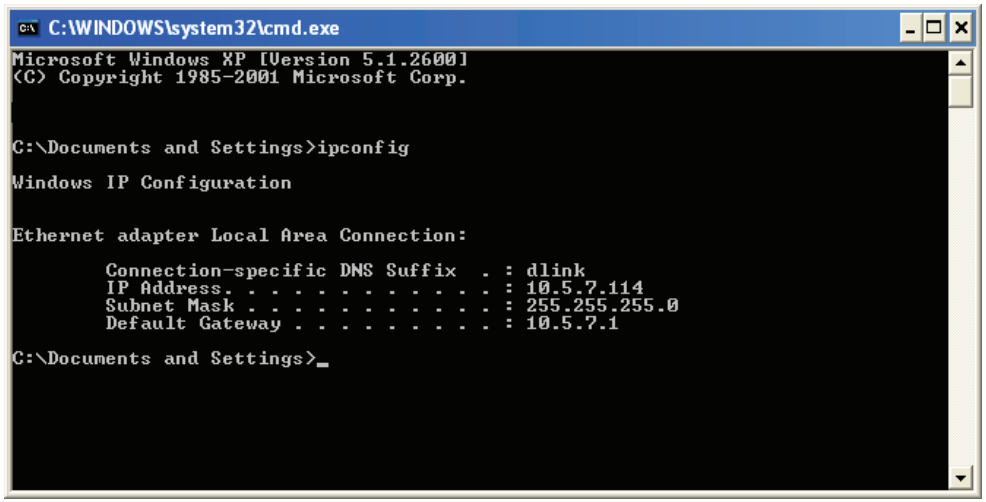
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



Statically Assign an IP address

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

Step 1

Windows® 7 - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
Windows Vista® - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections.**
Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2

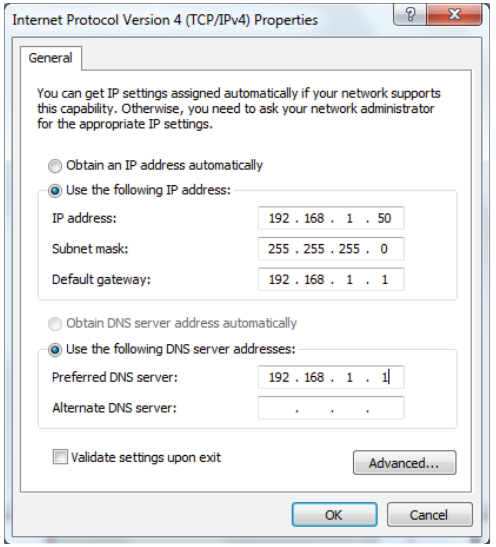
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

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

Step 4

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



Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.1.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.0.1).

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

Step 5

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

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DWR-921 offers the following types of security:

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

What is WPA?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

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

Technical Specifications

LTE Band[1]
- 800 / 900 / 1800 / 2600 MHz

UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+ Band[1]
- 900 / 2100 MHz
- Power Class 3

GSM Quad-band[1]
- 850 / 900 / 1800 / 1900 MHz

Data Rates[2]
- Up to 300 Mbps with 802.11n clients
- 6 / 9 / 11 / 12 / 18 / 24 / 36 / 48 / 54 Mbps in 802.11g mode
- 1 / 2 / 5.5 / 11 Mbps in 802.11b mode
- LTE Uplink: Up to 50 Mbps
- LTE Downlink: Up to 150 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
- Power
- LAN
- WLAN
- 2G / 3G
- 4G
- SMS
- Signal Strength

Dimensions
- 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/b/n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Regulatory Information

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. For more information, please refer to the Declaration of Conformity.

Notice of Wireless Radio LAN Usage in The European Community

• At the time of writing this addendum, some countries such as Italy, Greece, Portugal and Spain have not allowed operation of radio devices in the 5 GHz bands, although operation of 2.4 GHz radio devices are allowed. Please check with your local authority to confirm.
• This device is restricted to indoor use when operated in the European Community using channels in the 5.15-5.35 GHz band to reduce the potential for interference.
• This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France where restrictive use applies. This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIR P in the frequency range of 2454 –2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.
This equipment may be operated in AL, AD , BE , BG, DK, DE , FI, FR, GR, GW, IS, IT , HR , LI,
LU, MT , MK, MD , MC , NL, NO, AT , OL, PT, RO, SM, SE, RS, SK, ES, CI , HU , CY.

Usage Notes:

• To remain in conformance with European National spectrum usage regulations, frequency and channel limitations will be applied on the products according to the country where the equipment will be deployed.
• This device is restricted from functioning in Ad-hoc mode while operating in 5 GHz. Ad-hoc mode is direct peer-to-peer communication between two client devices without an Access Point.
• Access points will support DFS (Dynamic Frequency Selection) and TPC (Transmit Power
Control) functionality as required when operating in 5 GHz within the EU.

CE

2.4 GHz wireless frequency operation in EEC countries

Region	Frequency Band	Max output power (EIRP)
Metropolitan	2400 - 2454 MHz	100 mW
Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte	2454 - 2483.5 MHz	100 mW indoor, 10 mW outdoor
Reunion et Guyane	2400 - 2483.5 MHz	100 mW
Rest of EU community	2420 - 2483.5 MHz	100 mW

R&TTE 1999/5/EC			
WLAN 2.4 - 2.4835 GHz			
IEEE 802.11b/g/n			
Spectrum Regulation	**MHz, Europa (ETSI)**	**max. EIRP Innenbereich**	**max. EIRP Außenbereich**
Europa	2400 - 2483.5 MHz	100 mW	100 mW
Frankreich	2400 - 2454 MHz	100 mW	100 mW
	2454 - 2483.5 MHz	100 mW	10 mW

European Community Declaration of Conformity:

Česky [Czech]	D-Link tímto prohlašuje, že tento DWR-921 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede D-Link erklærer herved, at følgende udstyr DWR-921 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt D-Link, dass sich das Gerät DWR-921 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab D-Link seadme DWR-921 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, D-Link, declares that this DWR-921 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente D-Link declara que el DWR-921 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ D-Link ΔΗΛΩΝΕΙ ΟΤΙ DWR-921 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente D-Link déclare que l'appareil DWR-921 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente D-Link dichiara che questo DWR-921 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo D-Link deklarē, ka DWR-921 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo D-Link deklaruoja, kad šis DWR-921 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart D-Link dat het toestel DWR-921 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Malti [Maltese]	Hawnhekk, D-Link, jiddikjara li dan DWR-921 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, D-Link nyilatkozom, hogy a DWR-921 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym D-Link oświadcza, że DWR-921 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	D-Link declara que este DWR-921 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	D-Link izjavlja, da je ta DWR-921 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	D-Link týmto vyhlasuje, že DWR-921 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	D-Link vakuuttaa täten että DWR-921 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Warning Statement
The power outlet should be nearby the device and easily accessible.

Safety Instructions

Please adhere to the following safety guidelines to help ensure your own personal safety and protect your system from potential damage. Any acts taken that are inconsistent with ordinary use of the product, including improper testing, etc., and those not expressly approved by D-Link may result in the loss of product warranty.
Unless expressly approved by an authorized representative of D-Link in writing, you may not and may not permit others to:
• Disassemble or reverse engineer the device or attempt to derive source code (underlying ideas, algorithms, or structure) from the device or from any other information provided by D-Link, except to the extent that this restriction is expressly prohibited by local law.
• Modify or alter the device.
• Remove from the device any product identification or other notices, including copyright notices and patent markings, if any.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the device and other equipment, observe the following precautions:

Power Sources

• Observe and follow service markings.
• Do not push any objects into the openings of your device unless consistent with the authorized operation of the device. Doing so can cause a fire or an electrical shock by shorting out interior components.
• The powering of this device must adhere to the power specifications indicated for this product.
• Do not overload wall outlets and/or extension cords as this will increase the risk of fire or electrical shock.
• Do not rest anything on the power cord or on the device (unless the device is made and expressly approved as suitable for stacking).
• Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
• Operate the device only from the type of external power source indicated on the electrical ratings label.
• To help avoid damaging your device, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at your location.
• Also be sure that attached devices are electrically rated to operate with the power available in your location.
• Use only approved power cable(s). If you have not been provided a power cable for your device or for any AC -powered option intended for your device, purchase a power cable that is approved for use in your country and is suitable for use with your device. The power cable must be rated for the device and for the voltage and current marked on the device's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the device.
• To help prevent an electrical shock, plug the device and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
• Observe extension cable and power strip ratings. Ensure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
• To help protect your device from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
• Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
• When connecting or disconnecting power to hot-pluggable power supplies, if offered with your device, observe the following

guidelines.
• Install the power supply before connecting the power cable to the power supply.
• Unplug the power cable before removing the power supply.
• If the system has multiple sources of power, disconnect power from the device by unplugging all power cables from the power supplies.

Servicing/Disassembling
• Do not service any product except as expressly set forth in your system documentation.
• Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to an electrical shock. Only a trained service technician should service components inside these compartments.
• To reduce the risk of electrical shock, never disassemble this device. None of its internal parts are user-replaceable; therefore, there is no reason to access the interior.
• Do not spill food or liquids on your system components, and never operate the device in a wet environment. If the device gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
• Use the device only with approved equipment.
• Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

Environment
• Do not use this device near water (e.g. near a bathtub, sink, laundry tub, fish tank, in a wet basement or near a swimming pool).
• Do not use this device in areas with high humidity.
• This device must not be subjected to water or condensation.
• Keep your device away from radiators and heat sources. Also, do not block cooling vents.

Cleaning
• Always unplug the power before cleaning this device.
• Do not use liquid or aerosol cleaners of any kind. Use only compressed air that is recommended for electronic devices.
• Use a dry cloth for cleaning.

Protecting Against Electrostatic Discharge
Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from

your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.
You can also take the following steps to help prevent damage from electrostatic discharge (ESD):
1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads, and an antistatic grounding strap.

ErP Power Usage

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed.

Network Standby: 2.3 watts
Switched Off: 0.13 watts

Disposing of and Recycling Your Product

ENGLISH

This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in the household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will accept products for free. By recycling the product and its packaging in this manner you help to conserve the environment and protect human health.

D-Link and the Environment

At D-Link, we understand and are committed to reducing any impact our operations and products may have on the environment. To minimise this impact D-Link designs and builds its products to be as environmentally friendly as possible, by using recyclable, low toxic materials in both products and packaging.

D-Link recommends that you always switch off or unplug your D-Link products when they are not in use. By doing so you will help to save energy and reduce CO2 emissions.

To learn more about our environmentally responsible products and packaging please visit www.dlinkgreen.com

DEUTSCH DE

Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde entsprechend amtlich ausgewiesenen Sammelstelle, sobald das Produkt das Ende seiner Nutzungsdauer erreicht hat. Für die Annahme solcher Produkte erheben einige dieser Stellen keine Gebühren. Durch ein auf diese Weise durchgeführtes Recycling des Produkts und seiner Verpackung helfen Sie, die Umwelt zu schonen und die menschliche Gesundheit zu schützen.

D-Link und die Umwelt

D-Link ist sich den möglichen Auswirkungen seiner Geschäftstätigkeiten und seiner Produkte auf die Umwelt bewusst und fühlt sich verpflichtet, diese entsprechend zu mindern. Zu diesem Zweck entwickelt und stellt D-Link seine Produkte mit dem Ziel größtmöglicher Umweltfreundlichkeit her und verwendet wiederverwertbare, schadstoffarme Materialien bei Produktherstellung und Verpackung.

D-Link empfiehlt, Ihre Produkte von D-Link, wenn nicht in Gebrauch, immer auszuschalten oder vom Netz zu nehmen. Auf diese Weise helfen Sie, Energie zu sparen und CO2-Emissionen zu reduzieren.
Wenn Sie mehr über unsere umweltgerechten Produkte und Verpackungen wissen möchten, finden Sie entsprechende Informationen im Internet unter www.dlinkgreen.com.

FRANÇAIS FR

Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et règlementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront vos produits gratuitement. En recyclant le produit et son emballage de cette manière, vous aidez à préserver l'environnement et à protéger la santé de l'homme.

D-Link et l'environnement

Chez D-Link, nous sommes conscients de l'impact de nos opérations et produits sur l'environnement et nous engageons à le réduire. Pour limiter cet impact, D-Link conçoit et fabrique ses produits de manière aussi écologique que possible, en utilisant des matériaux recyclables et faiblement toxiques, tant dans ses produits que ses emballages.
D-Link recommande de toujours éteindre ou débrancher vos produits D-Link lorsque vous ne les utilisez pas. Vous réaliserez ainsi des économies d'énergie et réduirez vos émissions de CO2.
Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le www.dlinkgreen.com

ESPAÑOL ES

Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida útil; algunos de ellos aceptan recogerlos de forma gratuita. Al reciclar el producto y su embalaje de esta forma, contribuye a preservar el medio ambiente y a proteger la salud de los seres humanos.

D-Link y el medio ambiente

En D-Link, comprendemos y estamos comprometidos con la reducción del impacto que puedan tener nuestras actividades y nuestros productos en el medio ambiente. Para reducir este impacto, D-Link diseña y fabrica sus productos para que sean

lo más ecológicos posible, utilizando materiales reciclables y de baja toxicidad tanto en los productos como en el embalaje.

D-Link recomienda apagar o desenchufar los productos D-Link cuando no se estén utilizando. Al hacerlo, contribuirá a ahorrar energía y a reducir las emisiones de CO2.
Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio www.dlinkgreen.com

ITALIANO IT

La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto di raccolta indicato dalle autorità locali. Alcuni questi punti di raccolta accettano gratuitamente i prodotti da riciclare. Scegliendo di riciclare il prodotto e il relativo imballaggio, si contribuirà a preservare l'ambiente e a salvaguardare la salute umana.

D-Link e l'ambiente

D-Link cerca da sempre di ridurre l'impatto ambientale dei propri stabilimenti e dei propri prodotti. Allo scopo di ridurre al minimo tale impatto, D-Link progetta e realizza i propri prodotti in modo che rispettino il più possibile l'ambiente, utilizzando materiali riciclabili a basso tasso di tossicità sia per i prodotti che per gli imballaggi.
D-Link raccomanda di spegnere sempre i prodotti D-Link o di scollegarne la spina quando non vengono utilizzati. In questo modo si contribuirà a risparmiare energia e a ridurre le emissioni di anidride carbonica.
Per ulteriori informazioni sui prodotti e sugli imballaggi D-Link a ridotto impatto ambientale, visitate il sito all'indirizzo www.dlinkgreen.com

NEDERLANDS NL

Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te brengen dat hiertoe werd aangeduid door uw plaatselijke autoriteiten, sommige autoriteiten accepteren producten zonder dat u hiervoor dient te betalen.
Door het product en de verpakking op deze manier te recyclen helpt u het milieu en de gezondheid van de mens te beschermen.

D-Link en het milieu

Bij D-Link spannen we ons in om de impact van onze handelingen en producten op het milieu te beperken. Om deze impact te beperken, ontwerpt en bouwt D-Link zijn producten zo milieuvriendelijk mogelijk, door het gebruik van recycleerbare producten met lage toxiciteit in product en verpakking.

D-Link raadt aan om steeds uw D-Link producten uit te schakelen of uit de stekker te halen wanneer u ze niet gebruikt. Door dit te doen bespaart u energie en beperkt u de CO2-emissies.

Breng een bezoek aan www.dlinkgreen.com voor meer informatie over onze milieuverantwoorde producten en verpakkingen

POLSKI PL

Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie do tego celu podmioty przyjmą takie produkty nieodpłatnie, dlatego prosimy dostarczyć go do punktu zbiórki wskazanego przez lokalne władze.

Poprzez proces recyklingu i dzięki takiemu postępowaniu z produktem oraz jego opakowaniem, pomogą Państwo chronić środowisko naturalne i dbać o ludzkie zdrowie.

D-Link i środowisko

W D-Link podchodzimy w sposób świadomy do ochrony otoczenia oraz jesteśmy zaangażowani w zmniejszanie wpływu naszych działań i produktów na środowisko naturalne. W celu zminimalizowania takiego wpływu firma D-Link konstruuje i wytwarza swoje produkty w taki sposób, aby były one jak najbardziej przyjazne środowisku, stosując do tych celów materiały nadające się do powtórnego wykorzystania, charakteryzujące się małą toksycznością zarówno w przypadku samych produktów jak i opakowań.

Firma D-Link zaleca, aby Państwo zawsze prawidłowo wyłączali z użytku swoje produkty D-Link, gdy nie są one wykorzystywane. Postępując w ten sposób pozwalają Państwo oszczędzać energię i zmniejszać emisje CO2.

"Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną internetową www.dlinkgreen.com."

ČESKY CZ

Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odneste jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklací výrobku i obalu pomáháte chránit životní prostředí i lidské zdraví.

D-Link a životní prostředí

"Ve společnosti D-Link jsme si vědomi vlivu našich provozů a výrobků na životní prostředí a snažíme se o minimalizaci těchto vlivů. Proto své výrobky navrhujeme a vyrábíme tak, aby byly co nejekologičtější, a ve výrobcích i obalech používáme recyklovatelné a nízkotoxické materiály."

"Společnost D-Link doporučuje, abyste své výrobky značky D-Link vypnuli nebo vytáhli ze zásuvky vždy, když je nepoužíváte. Pomůžete tak šetřit energii a snížit emise CO2."

Více informací o našich ekologických výrobcích a obalech najdete na adrese www.dlinkgreen.com.

MAGYAR HU

Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által kijelölt gyűjtőhelyre. A termékek egyes helyeken ingyen elhelyezhetők. A termék és a csomagolás újrahasznosításával segíti védeni a környezetet és az emberek egészségét.

A D-Link és a környezet

A D-Linknél megértjük és elkötelezettek vagyunk a műveleteink és termékeink környezetre gyakorolt hatásainak csökkentésére. Az ezen hatás csökkentése érdekében a D-Link a lehető leginkább környezetbarát termékeket tervez és gyárt azáltal, hogy újrahasznosítható, alacsony károsanyag-tartalmú termékeket gyárt és csomagolásokat alkalmaz.

A D-Link azt javasolja, hogy mindig kapcsolja ki vagy húzza ki a D-Link termékeket a tápforrásból, ha nem használja azokat. Ezzel segít az energia megtakarításában és a széndioxid kibocsátásának csökkentésében.

Környezetbarát termékeinkről és csomagolásainkról további információkat a www.dlinkgreen.com weboldalon tudhat meg.

NORSK NO

Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning.
Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet.
For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.
D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO2-utslipp.
"For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til www.dlinkgreen.com"

DANSK DK

Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever
produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.
D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO2-udledningerne.
Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på www.dlinkgreen.com

SUOMI FI

Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittelemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

"Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta www.dlinkgreen.com"

SVENSKA SE

Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar www.dlinkgreen.com

PORTUGUÊS PT

Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando meteriais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite www.dlinkgreen.com