D-Link®

Version 1.00 | 08/15/2014

User Manual

4G LTE Router

DWR-922

Preface

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

Manual Revisions

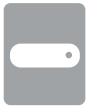
Revision	Date	Description
1.00	August 15, 2014	• Initial release

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.

Table of Contents

Package Contents



DWR-922 4G LTE Router

Power Adapter

3G/4G Antennas

RJ-45 and RJ-11 Cables

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

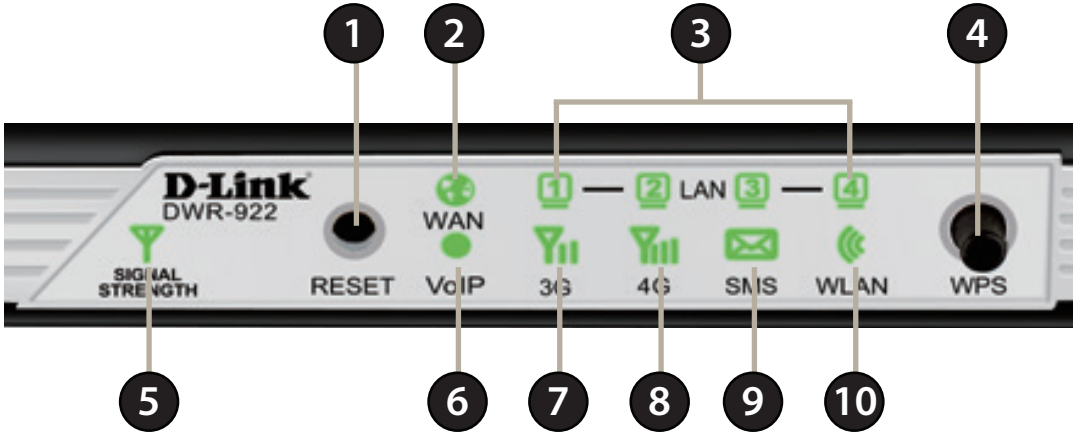
The D-Link 4G LTE Router allows users to access worldwide mobile broadband networks. Once connected, users can transfer data, stream media, and send SMS messages. Simply insert your 3G / 4G SIM card, and share your 3G / 4G Internet connection through a secure 802.11n wireless network or using any of the four 10/100/1000 Ethernet ports.

Keep your wireless network safe with WPA/WPA2 wireless encryption. The DWR-922 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.

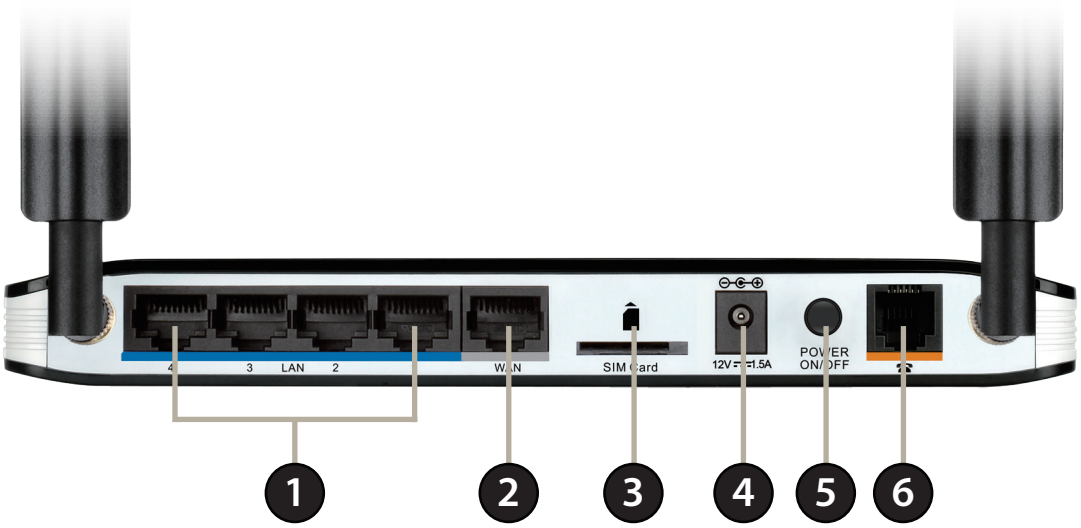
Hardware Overview

Front View



1	**Reset Button**	Press this button with an unfolded paperclip and hold for ten seconds to reset the device.
2	**WAN LED**	Will be lit if an Internet connection is established, and will blink when data is being transferred.
3	**LAN LEDs 1-4**	Will be lit if an Ethernet connection is established, and will blink when data is being transferred.
4	**WPS Button**	Press this button to initiate a new WPS connection. See **Add Wireless Device with WPS** on page 18 for details.
5	**Signal Strength LED**	Will blink red if there is no SIM card / signal. Solid red/amber/green indicates the signal strength.
6	**VoIP LED**	Will be lit if a VoIP connection is active.
7	**3G LED**	Will be lit if a 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	**SMS LED**	Will be solid green if the SMS inbox is full, or blinking if there is an unread new SMS message.
10	**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.
6	**Phone Port**	For connection to a phone handset.

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-922 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-922 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-922 4G LTE Router LAN Ports are Auto-MDI/MDIX, so both patch and crossover Ethernet cables can be used.

5. If you have a telephone handset and wish to use the DWR-922 to make VoIP calls, connect one end of the RJ-11 cable to your handset and the other end to the phone port on the back panel of the DWR-922.

Note: Do not directly connect the DWR-922 to a telecommunication network or a building's telephone socket.

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

1. Minimize the number of walls and ceilings between the D-Link router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick. Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

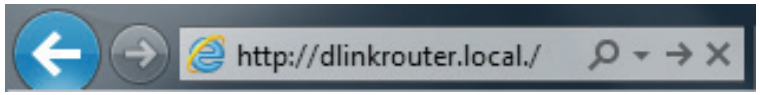
3. Try to position access points, wireless routers, and computers so that the signal passes through open doorways and drywall. Materials such as glass, metal, brick, insulation, concrete, and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors,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

4. If you are using 2.4 GHz cordless phones, make sure that the 2.4 GHz phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

Configuration

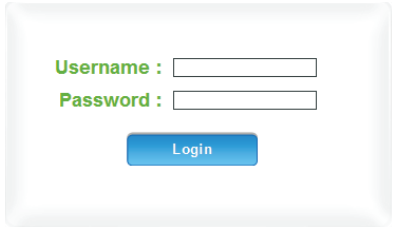
Getting Started

To access the configuration utility, open a web-browser such as Internet Explorer and enter the address of the router (**http://dlinkrouter.local./** or **192.168.1.1** by default).



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

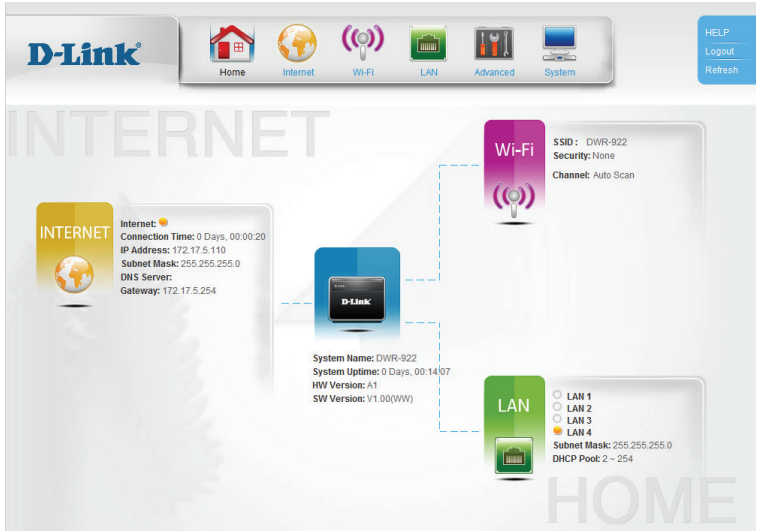
If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



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.

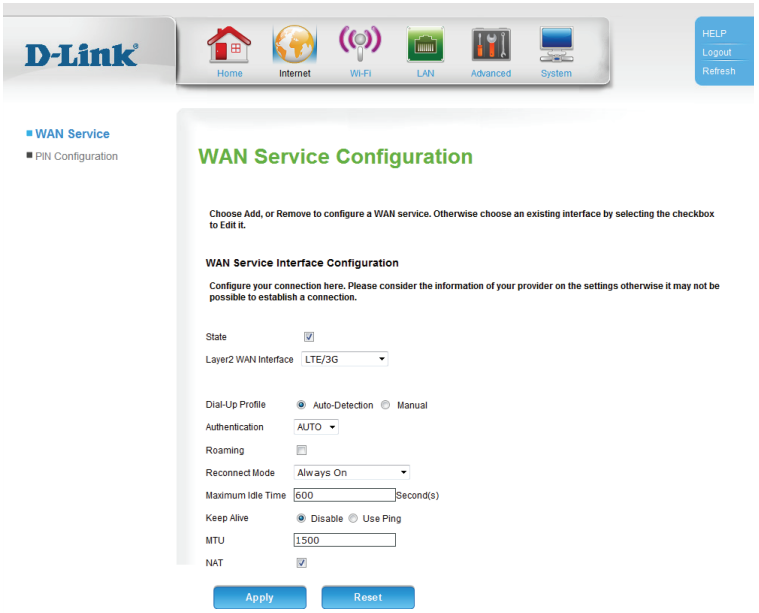


Internet

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).

Layer2 WAN Connection: Select your Internet connection type: **LTE/3G** or **Ethernet WAN**.



LTE/3G

Dial-Up Profile: If **Auto-Detection** does not work, then try selecting **Manual** and filling out the information (supplied by your LTE/3G ISP).

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

Roaming: Check the box to enable international LTE / 3G roaming.

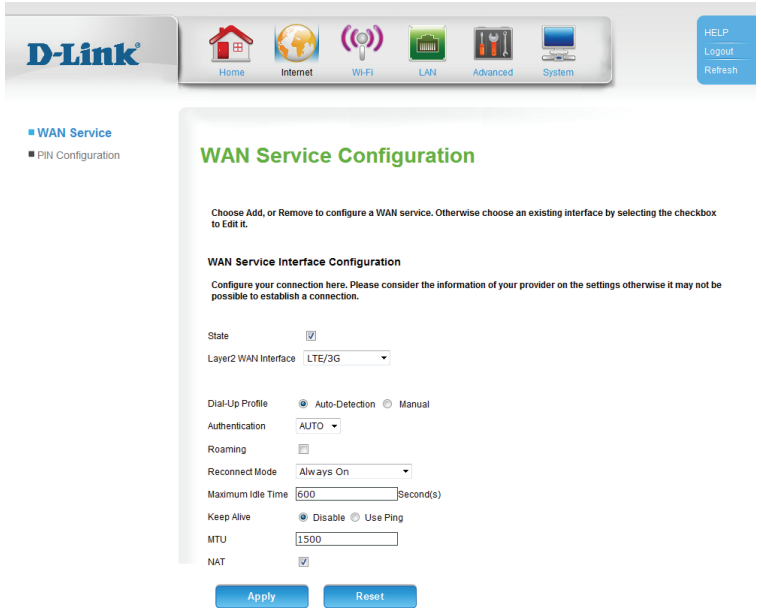
Reconnect Mode: Select either **Always On**, **Connect on Demand**, or **Manual**.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity (if you selected **Always On** above, this setting will have no effect).

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

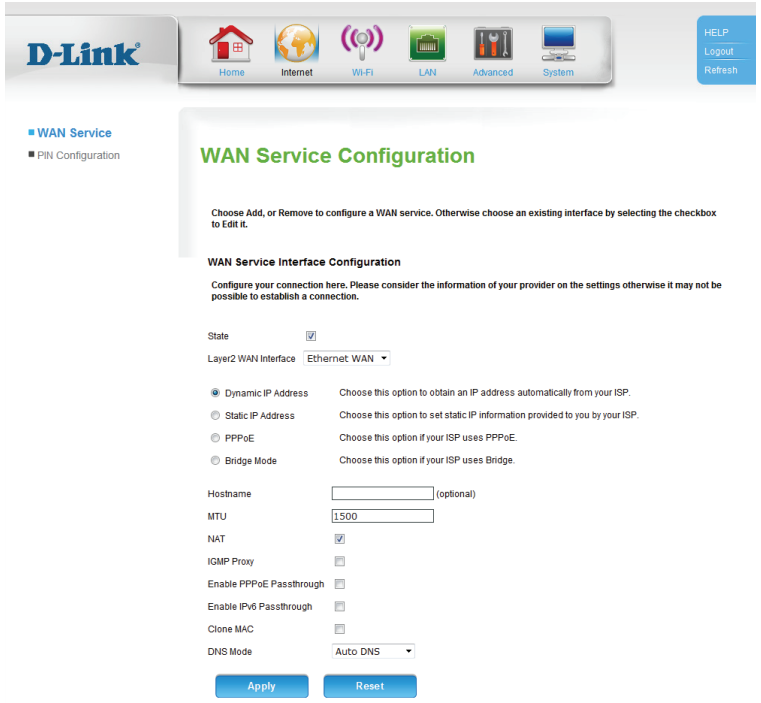
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your ISP. The default value is 1500.

NAT: Check the box to enable Network Address Translation (NAT).



Ethernet WAN

Select your Internet connection type from the list of options. This information cab be obtained from your ISP. The page will update with the appropriate options for the selection connection type.



Dynamic IP Address

Hostname: The hostname is optional but may be required by some ISPs. Leave it blank if you are not sure.

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

NAT: Check the box to enable Network Address Translation (NAT).

IGMP Proxy: Check the box to enable IGMP proxy.

Enable PPPoE Passthrough: Check the box to enable PPPoE passthrough.

Enable IPv6 Passthrough: Check the box to enable IPv6 passthrough.

Clone MAC: Check the box to clone your client's MAC address to the WAN port.

DNS Mode: If your ISP provided DNS server addresses to use, select **Manual DNS** and enter the primary and (if applicable) secondary addresses. Otherwise, select **Auto DNS** to automatically assign a DNS server, or **DNS Disabled** to disable DNS.

Static IP Address

IP Address: Enter the IP address provided by your ISP.

Subnet Mask: Enter the subnet mask provided by your ISP.

Gateway Address: Enter the gateway address provided by your ISP.

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

NAT: Check the box to enable Network Address Translation (NAT).

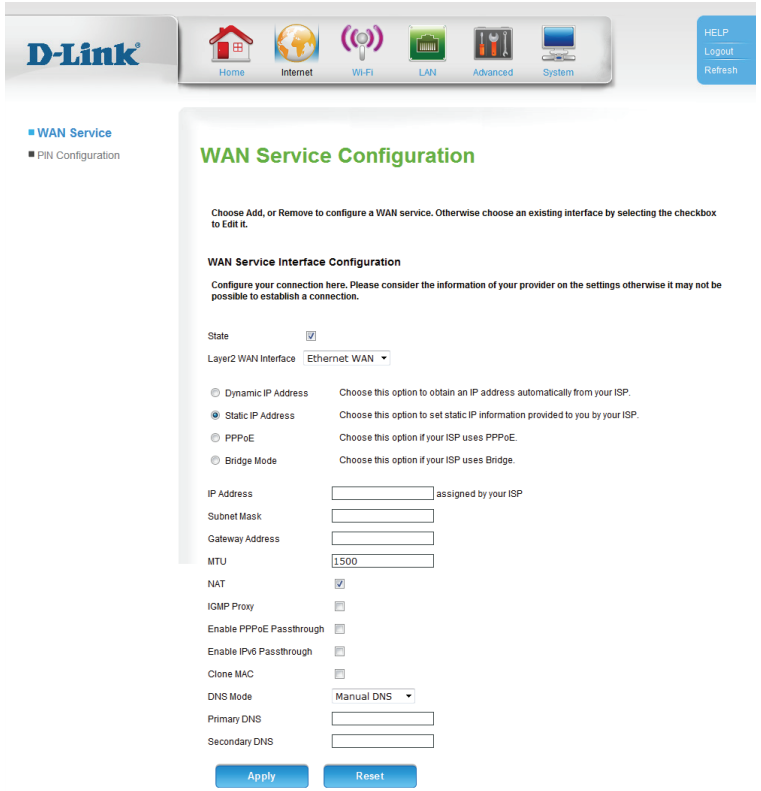
IGMP Proxy: Check the box to enable IGMP proxy.

Enable PPPoE Passthrough: Check the box to enable PPPoE passthrough.

Enable IPv6 Passthrough: Check the box to enable IPv6 passthrough.

Clone MAC: Check the box to clone your client's MAC address to the WAN port.

DNS Mode: If your ISP provided DNS server addresses to use, select **Manual DNS** and enter the primary and (if applicable) secondary addresses. Otherwise, select **Auto DNS** to automatically assign a DNS server, or **DNS Disabled** to disable DNS.



PPPoE

Username: Enter the PPPoE username provided by your ISP.

Password: Enter the PPPoE password provided by your ISP.

PPPoE Service Name: Enter the PPPoE service name provided by your ISP if applicable.

AC Name: Enter the PPPoE access concentrator (AC) name provided by your ISP if applicable.

IP Control: If your ISP provided a static IP address, select **Static IP Address**, otherwise leave this setting at the default, **Dynamic IP Address**.

Static IP Address: If you selected **Static IP Address** above, enter the address provided by your ISP here.

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

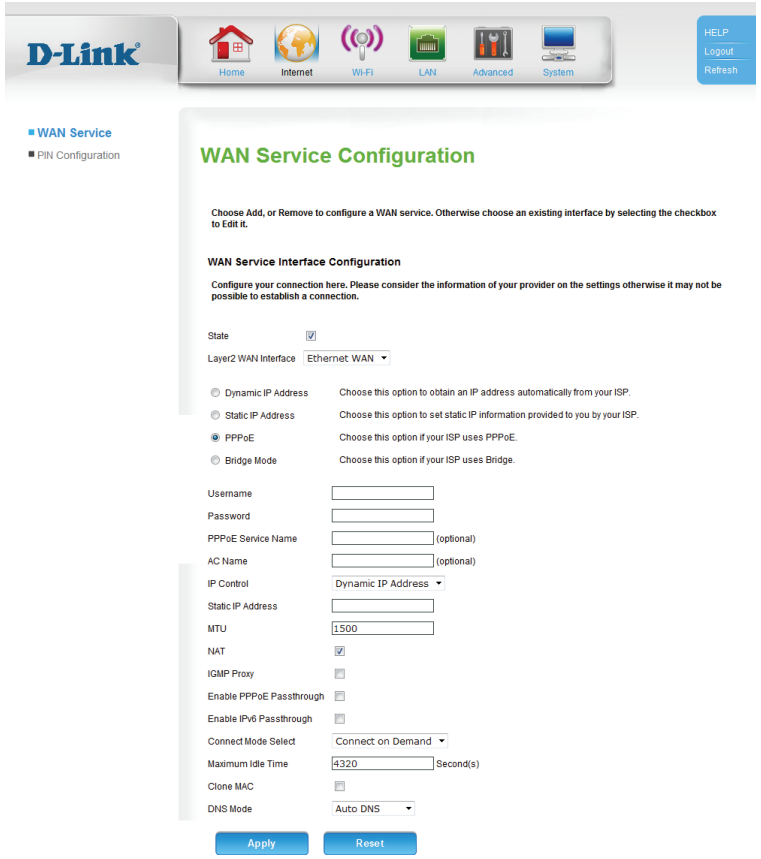
NAT: Check the box to enable Network Address Translation (NAT).

IGMP Proxy: Check the box to enable IGMP proxy.

Enable PPPoE Passthrough: Check the box to enable PPPoE passthrough.

Enable IPv6 Passthrough: Check the box to enable IPv6 passthrough.

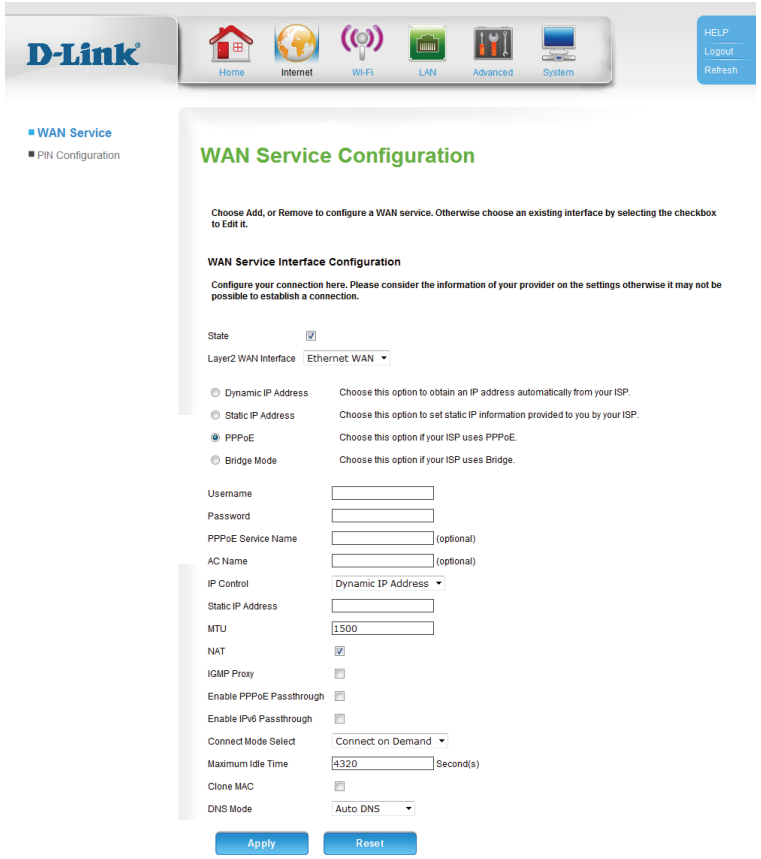
Connect Mode Select: Select either **Always On**, **Connect on Demand**, or **Manual**.



Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity (if you selected **Always On** above, this setting will have no effect).

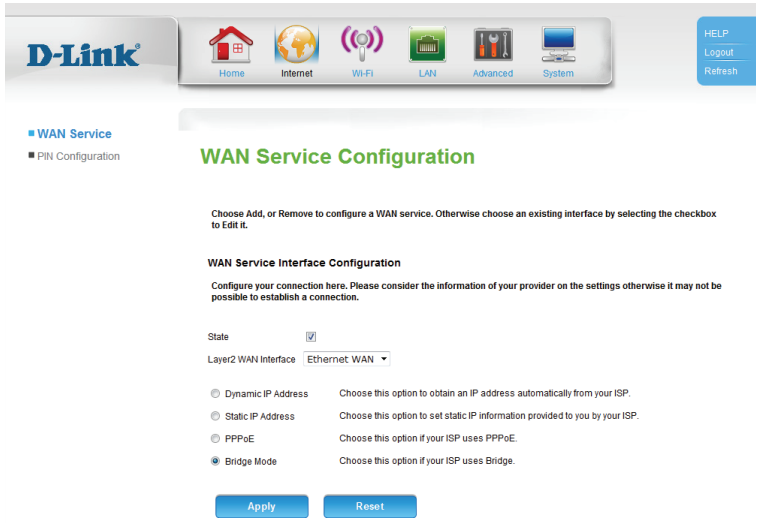
Clone MAC: Check the box to clone your client's MAC address to the WAN port.

DNS Mode: If your ISP provided DNS server addresses to use, select **Manual DNS** and enter the primary and (if applicable) secondary addresses. Otherwise, select **Auto DNS** to automatically assign a DNS server, or **DNS Disabled** to disable DNS.



Bridge Mode

If you selected **Bridge Mode**, there are no further settings to configure.

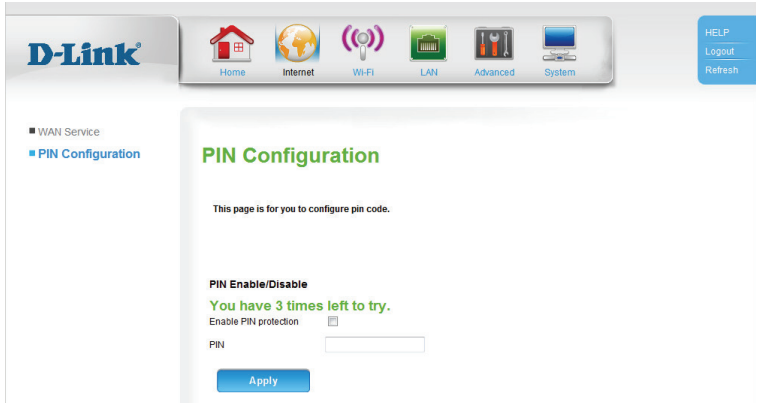


PIN Configuration

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.



Wi-Fi

Wireless Setup

On this page you can configure your wireless settings.

Wireless Function Enable: Check the box to enable the router's wireless functionality.

Wi-Fi Protected Setup: Check **Enable** to enable Wi-Fi Protected Setup (WPS).

Current PIN: Displays the current WPS PIN. Click **Generate New PIN** to generate a new WPS PIN, or **Reset PIN to default** to reset the WPS PIN to its default value.

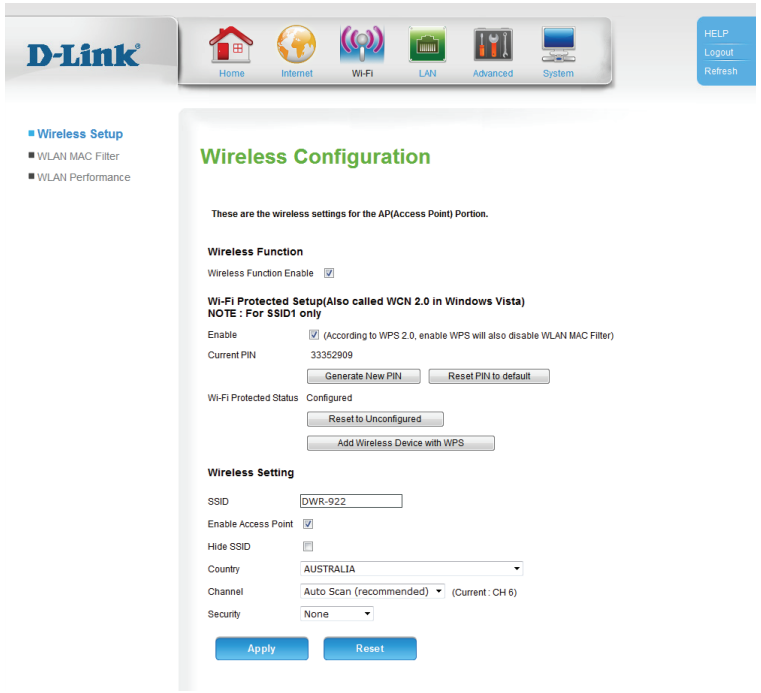
Wi-Fi Protected Status: Displays the configuration status of WPS. If you want to revert to unconfigured status, select **Reset to Unconfigured**.

Add Wireless Device with WPS: Click this button to connect a wireless device using WPS. See below for details.

SSID: Create a name for your wireless network using up to 32 characters.

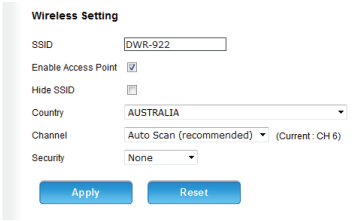
Hide SSID: Check the box if you do not want to broadcast the SSID of your wireless network.

Country: Select your country from the drop-down menu.



Channel: Select the wireless channel. The default is **Auto Scan (recommended)**.

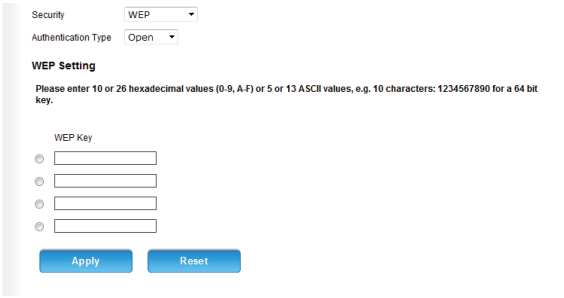
Security: Select the desired wireless encryption mode. **WPA/WPA2** is recommended if your clients support it. See below for details.



Wireless Security

WEP

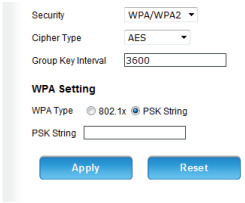
Authentication Type: Select whether to use **Open** or **Shared** authentication.



WEP Key: For a 64-bit key, enter 10 hexadecimal (0-9, A-F) values or 5 ASCII values. For a 128-bit key, enter 26 hexadecimal values or 13 ASCII values.

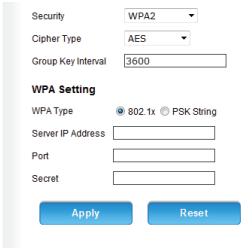
WPA/WPA2

These settings apply to both **WPA2** and **WPA/WPA2** encryption types.



Cipher Type: Select **AES** or **TKIP+AES**. **AES** is the most secure, but **TKIP+AES** allows for compatibility with clients that don't support **AES**.

Group Key Interval: Enter the group key interval, or leave it at the default value (3600).



WPA Type: Select either **802.1x** to use a RADIUS server for authentication, or **PSK String** to use a Pre-Shared Key (PSK).

PSK String: If you are using a Pre-Shared Key (PSK), choose a key (between 8 and 63 characters) here.

Server IP Address: If you are using a RADIUS server for authentication, enter the server IP address here.

Port: Enter the port used by your RADIUS server.

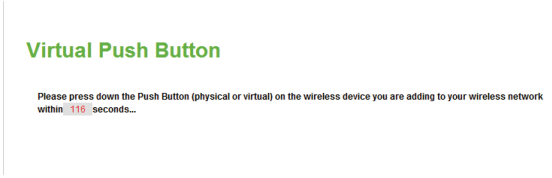
Secret: Enter the shared secret/password for your RADIUS server.

Add Wireless Device with WPS

PIN: If the device you are connecting has a PIN, enter it here and click **Connect**.

PUSH BUTTON: If the device you are connecting has a Push Button, click **Virtual Push Button**. This has the same function as the physical WPS button in the front of the router.

If you clicked **Virtual Push Button**, you will be prompted to push the button on the device you are connecting within 120 seconds.



WLAN MAC Filter

On this page you can set access rules for the wireless function. You can choose to allow or deny specific MAC addresses.

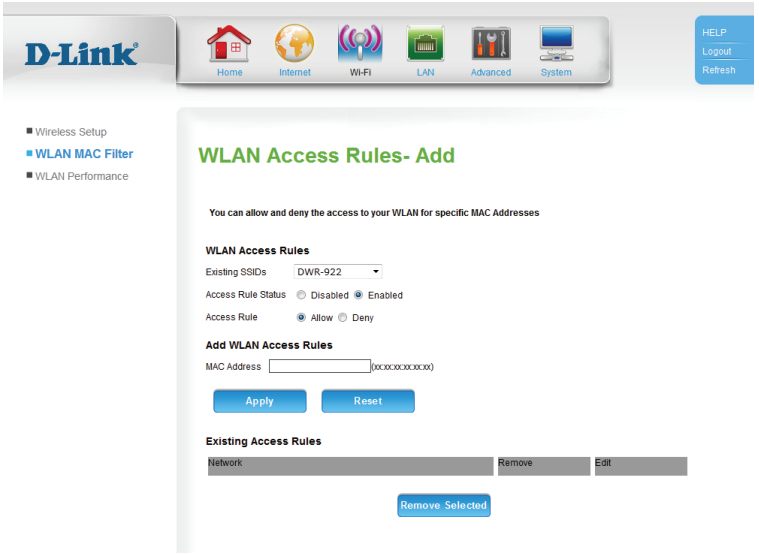
Existing SSIDs: Select the SSID to apply the rule to.

Access Rule Status: Select whether the rule is currently **Enabled** or **Disabled**.

Access Rule: Select whether to **Allow** or **Deny** the client.

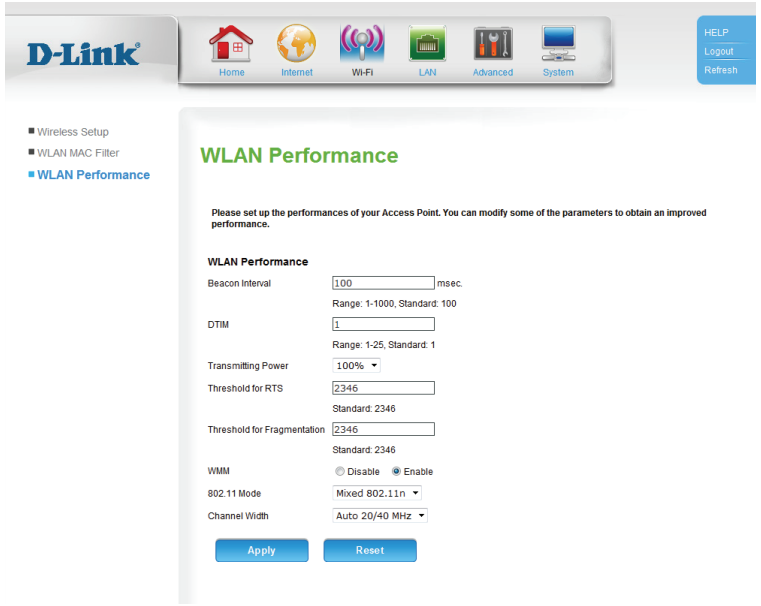
MAC Address: Enter the MAC address of the client.

Existing Access Rules: Displays a list of the current rules. To remove a rule, select it and click **Remove Selected**.



WLAN Performance

On this page you can configure advanced wireless settings. In most cases, it is recommended that you leave these settings at their defaults, unless you intend to increase wireless performance in a specific way.



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 and recommended setting.

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.

Transmitting Power: Set the transmitting power of the antennas.

Threshold for RTS: This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

Threshold for Fragmentation: The fragmentation threshold determines whether packets will be fragmented. Packets exceeding the specified value will be fragmented before transmission. 2346 is the default setting.

WMM: 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.

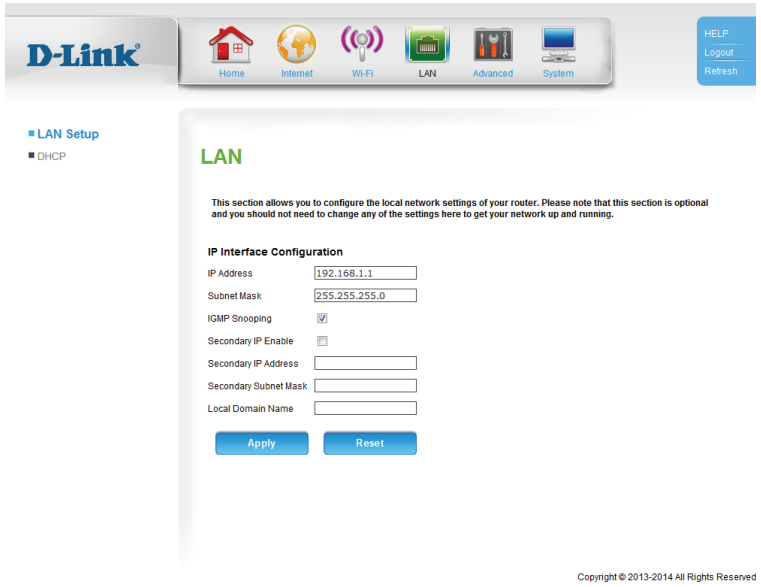
802.11 Mode: Select the desired wireless networking standards to use. The available options will depend on the wireless frequency band, as well as the currently selected security mode.

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.

LAN

LAN Setup

On this page you can configure the local network settings of your router.



IP Address: Enter the IP address of the router. The default is **192.168.1.1**. If you change the IP address, you will need to enter the new IP address in your browser to get into the configuration utility.

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

IGMP Snooping: Check the box to enable IGMP snooping.

Secondary IP Enable: Check the box to assign a secondary IP address to the router.

Secondary IP Address: If a secondary IP address is enabled, enter the new IP address.

Secondary Subnet Mask: If a secondary IP address is enabled, enter the subnet mask.

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

DHCP

On this page you can configure the Dynamic Host Configuration Protocol (DHCP) settings.

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

IP Range: Enter the range of IPs for the DHCP server to use to assign IP addresses to devices on your network.

Subnet Mask: Enter the subnet mask for the DHCP server to use

DNS Server: Enter the IP address of the DHCP server (the default is the router's IP address).

Secondary DNS Server: Enter the IP address of a secondary DNS server, if applicable.

Domain Name: Enter the domain name.

IP Router: Enter the IP address of the IP router.

DHCP Lease Time: Enter the lease time for DHCP assignments. The default is 86400.

DHCP Static Address Configuration: Check **Enable** to assign a new static IP address. Enter the MAC address of the client to assign, and the IP address that you want to assign to it.

Advanced

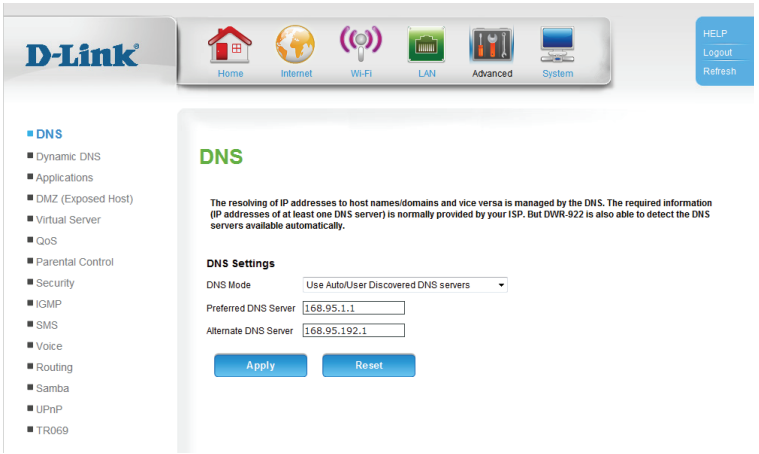
DNS

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

DNS Mode: Select **Use Auto/User Discovered DNS servers**, **Use only automatically detected DNS servers**, or **Use only manually specified DNS servers**.

Preferred DNS Server: Enter the primary DNS server address.

Alternate DNS Server: Enter an alternate DNS server address.



Dynamic DNS

On this page you can configure the Dynamic Domain Name System (DDNS) settings. Using a dynamic DNS service provider, people can enter your domain name in their web browser to connect to your server no matter what your IP address is.

Dynamic DNS Settings: Select whether to **Enable** or **Disable** DDNS.

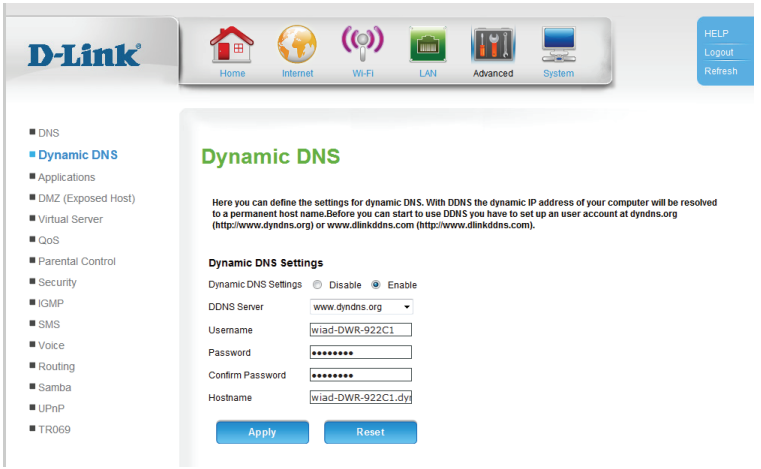
DDNS Server: Select your DDNS server.

Username: Enter your username for the DDNS server.

Password: Enter your password for the DDNS server.

Confirm Password: Re-enter your password for the DDNS server.

Hostname: Enter the hostname that you registered with your dynamic DNS service provider.



Applications

On this page you can configure Application Layer Gateway (ALG) settings, allowing certain protocols to work through the NAT/firewall. You can also specify special application rules, to open ports on your firewall and allow certain applications access to your network.

Enable PPTP: Check the box to enable PPTP.

Enable L2TP: Check the box to enable L2TP.

Enable IPSec: Check the box to enable IPSec.

Enable Application: Select whether to **Enable** or **Disable** the specified application.

Interface: Select the interface to apply the application rule to.

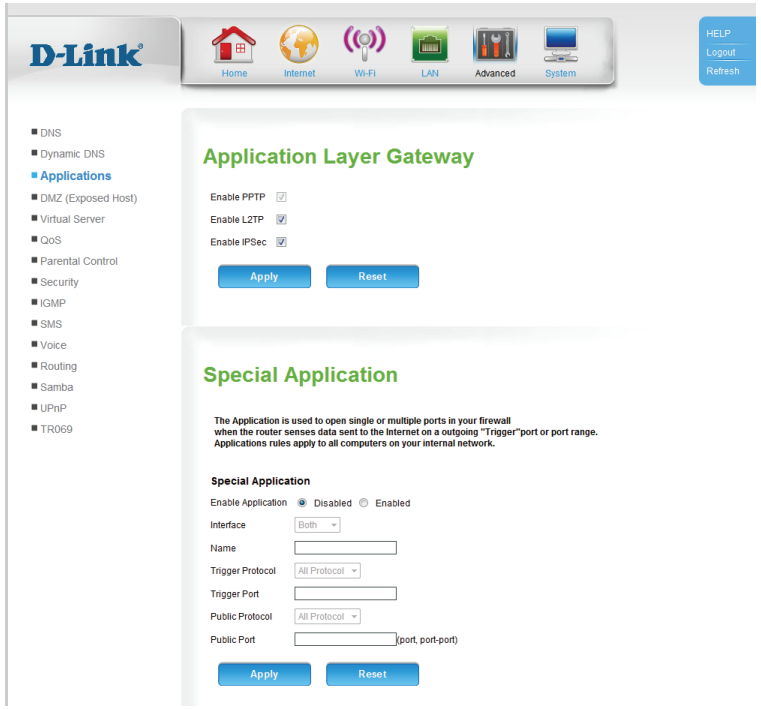
Name: Enter a name for the application rule.

Trigger Protocol: Select the protocol to use to trigger the rule.

Trigger Port: Enter the port or range of ports to listen to in order to trigger the rule.

Public Protocol: Select the protocol that will be used to access the application.

Public Port: Enter the port or range of ports that will be used to access the application.

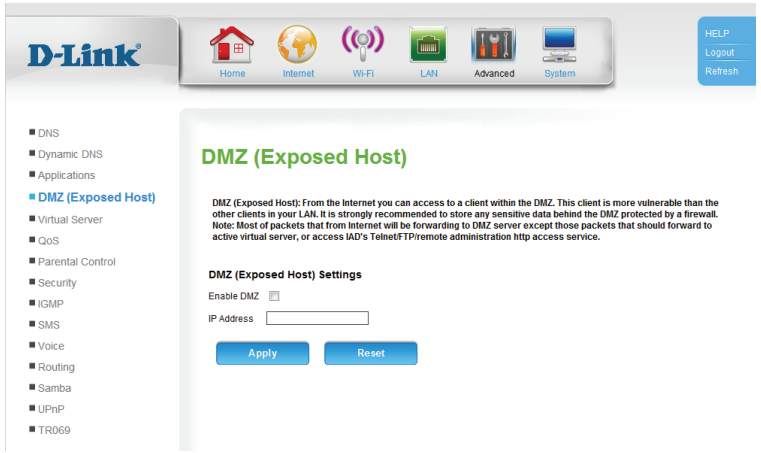


DMZ (Exposed Host)

On this page you can enable or disable Demilitarized Zone (DMZ). This completely exposes the client to threats over the Internet, and is not recommended in ordinary situations.

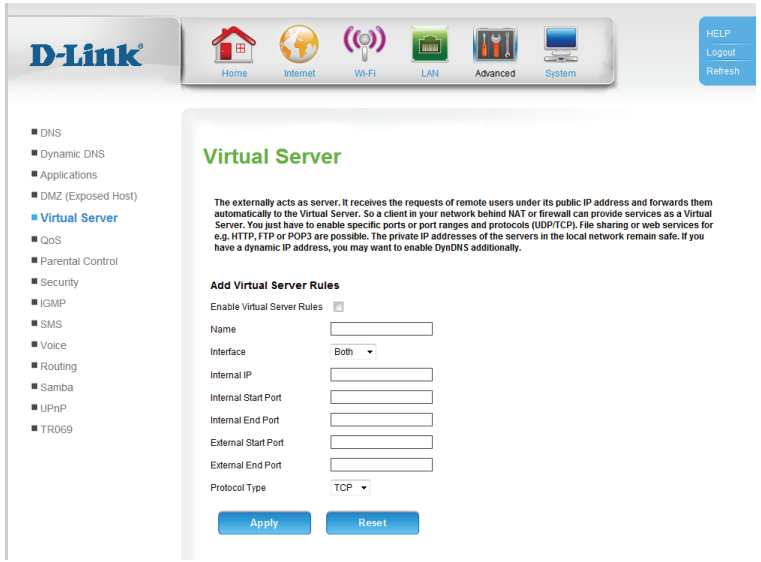
Enable DMZ: Check the box to enable DMZ.

IP Address: Enter the IP address of the client you wish to expose.



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.



Enable Virtual Server Rules: Check the box to enable the virtual server.

Name: This identifies the rule.

Interface: Select the interface to apply the rule to.

Internal IP: Enter the local IP address to use as the virtual server.

Internal Start Port: Enter the starting local port you want to forward to.

Internal End Port: Enter the ending local port you want to forward to.

External Start Port: Enter the starting public port you want to open.

External End Port: Enter the ending public port you want to open.

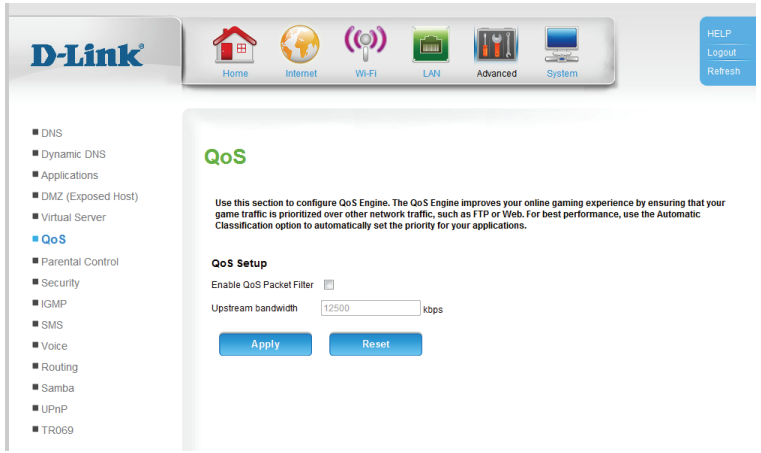
Protocol Type: Select the protocol type, **TCP** or **UDP** for the virtual server rule.

QoS

On this page you can configure the router's Quality of Service (QoS) engine, which prioritizes important network traffic, such as online gaming, Internet phone calls, and video streaming, over ordinary traffic, such as web browsing and file transferring.

Enable QoS Packet Filter: Check the box to enable Quality of Service (QoS).

Upstream bandwidth: Set this as closely as possible to your Internet upload bandwidth. If you are not sure, leave it at its default value, for best results.



Parental Control

On this page you can restrict Internet access to particular URLs, or whole domains.

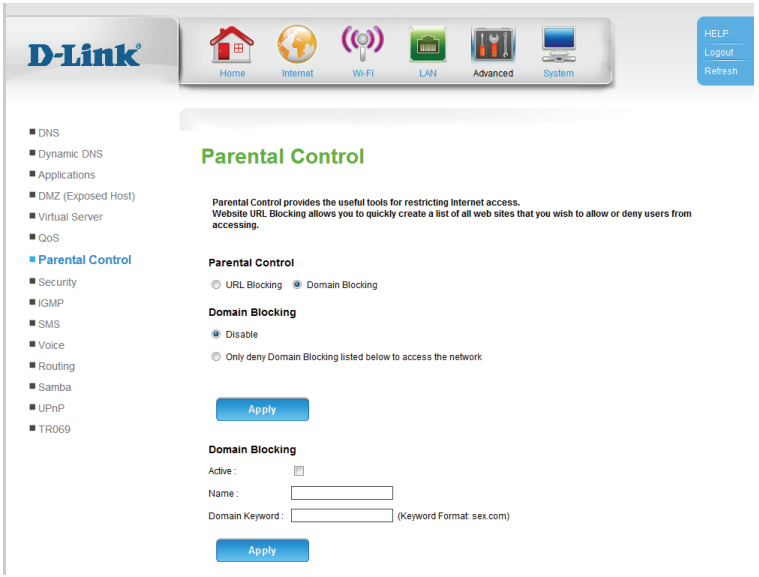
Parental Control: To enable parental control, select either **URL Blocking** or **Domain Blocking**. Next, select **Only deny URL/Domain Blocking listed below to access the network**. Lastly, fill out the details that appear below.

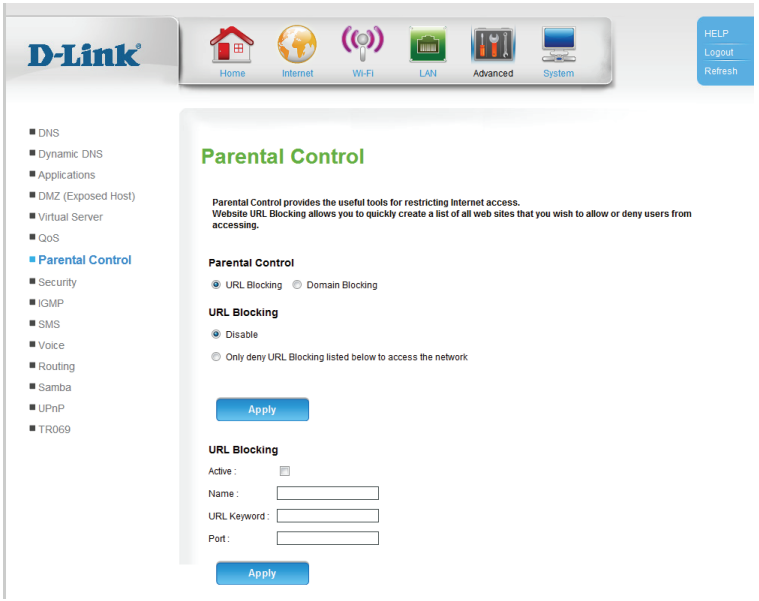
Active: Check the box to enable the rule.

Name: Enter the name of the rule.

URL Keyword / Domain: Enter part of the URL or the domain you want to filter.

Port: Enter the port number of the URL, if required.

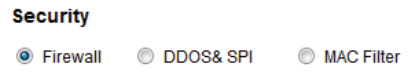




Security

This page allows you to configure your firewall, DDoS, SPI, and MAC filter settings.

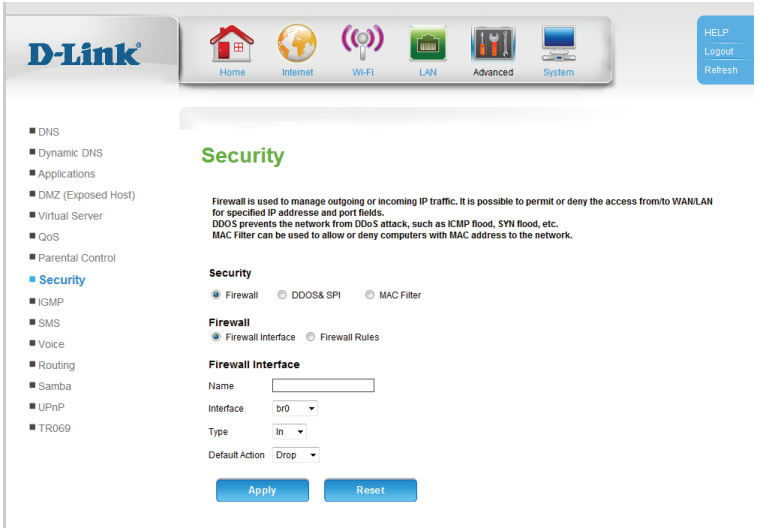
Security: Select either **Firewall**, **DDoS & SPI**, or **MAC Filter** to bring up the relevant settings for that security type



Firewall

The **Firewall** option allows you to configure the DWR-922's firewall, and allow or deny access to your network over specific ports and addresses.

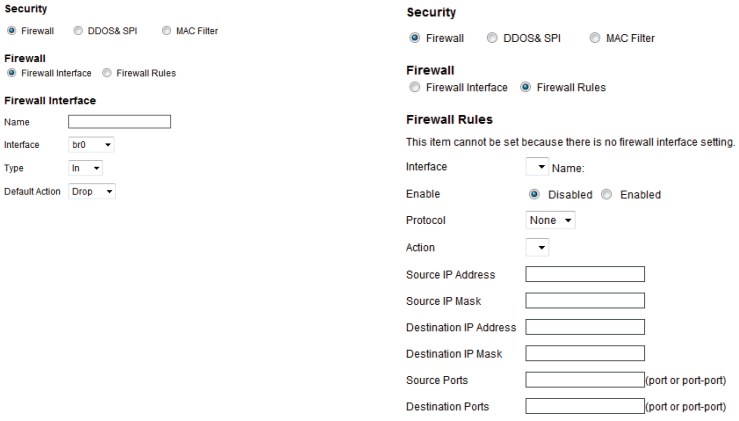
Firewall Interface: To configure a new firewall interface, first enter a **Name**, and specify the **Interface**, **Type**, and the **Default Action**. Click **Apply** to save the new interface.



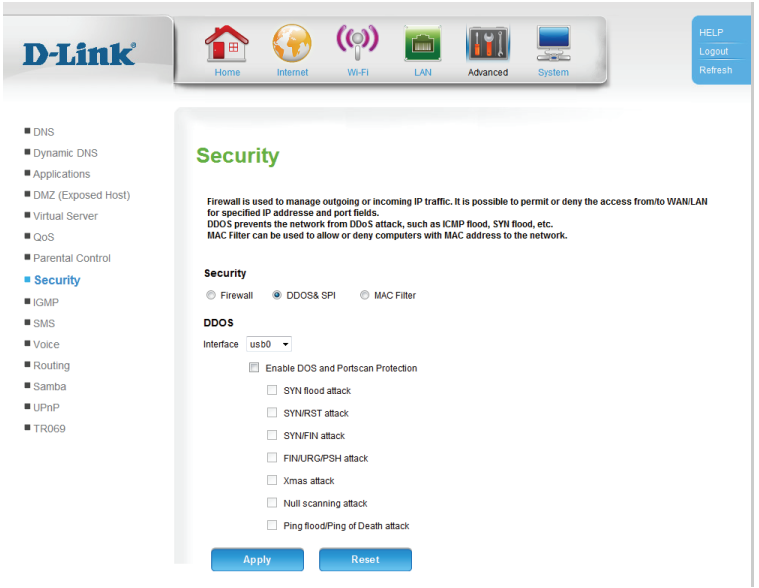
Firewall Rules: To configure the firewall rules, you must have first configured a firewall interface (see above). Select an interface you have configured from the drop-down menu. You can select whether the rule is **Enabled** or **Disabled**, to temporarily turn it on or off without removing it entirely.

Next, fill out the source and destination IP and port information, and select the **Protocol** and **Action**. Selecting an action will override the default action set in the firewall interface.

Click **Apply** to save the rule.



DDoS & SPI



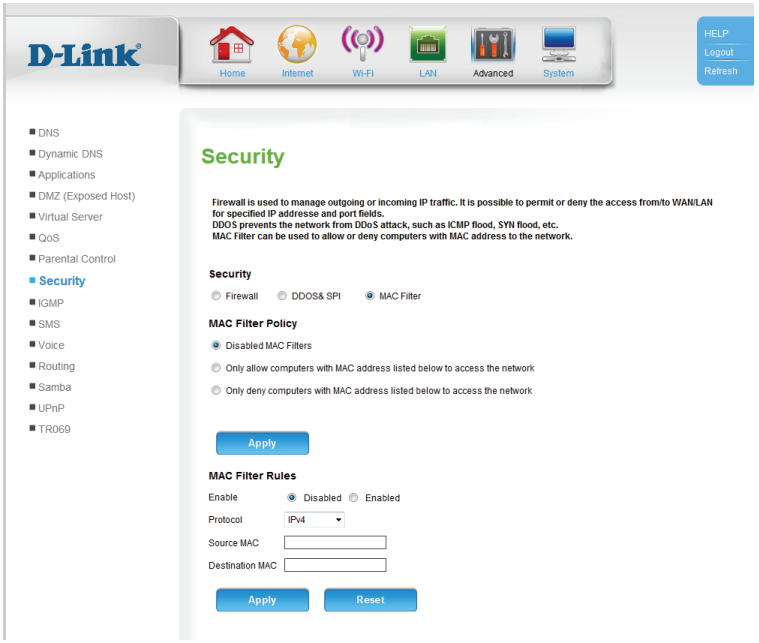
The **DDoS & SPI** feature protects against Distributed Denial of Service (DDoS) attacks, and helps to prevent cyber attacks by validating that the traffic passing through the session conforms to the protocol.

Interface: Select the network interface.

DDoS & SPI: Check the box to enable DDoS & SPI protection.

Click **Apply** to save your settings.

Mac Filter



The **MAC Filter** allows you to control which MAC addresses have access to the network.

MAC Filter Policy: To enable the MAC filter, select **Only allow computers...** or **Only deny computers...**. If you are only allowing the specified MAC addresses to access the network, then devices will not be able to connect unless you create a rule and enter their MAC address.

Click **Apply** to save your settings.

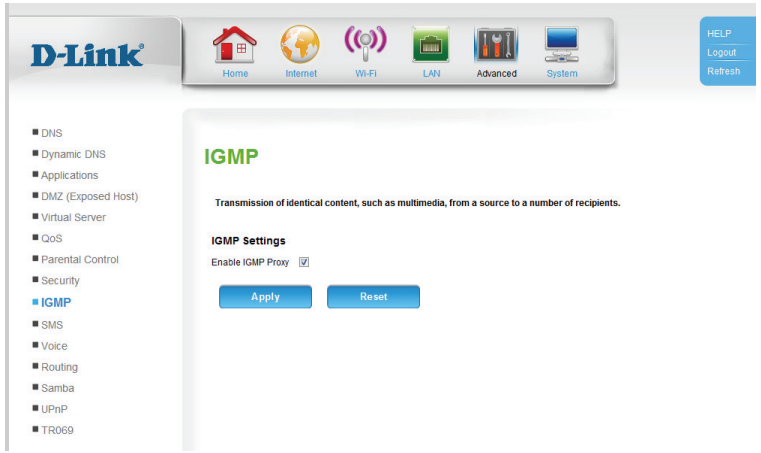
MAC Filter Rules: Select whether the rule is **Enabled** or **Disabled**, to temporarily turn it on or off without removing it entirely. Select the **Protocol**, and then enter the **Source MAC** and **Destination MAC** addresses.

Click **Apply** to save the rule.

IGMP

This page allows you to configure the router's Internet Group Management Protocol (IGMP) settings. IGMP is a method to transmit data to multiple recipients.

Enable IGMP Proxy: Check the box to enable router to act as an IGMP proxy.

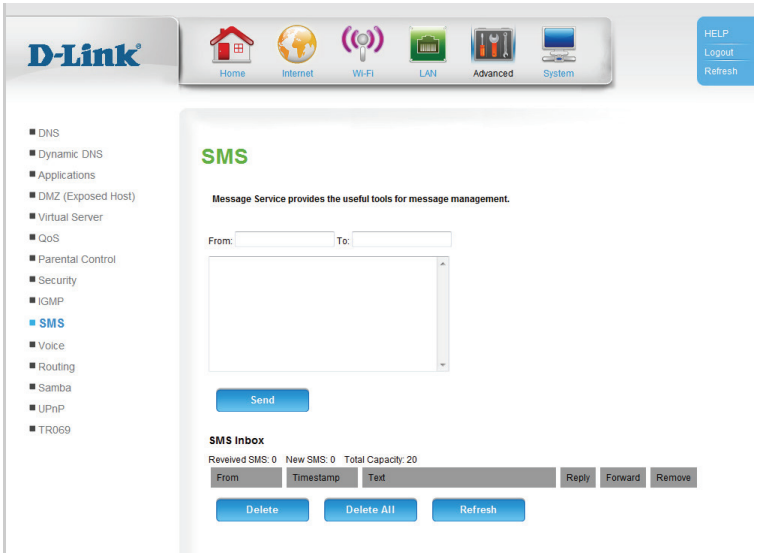


SMS

On this page you can send and receive SMS messages.

From/To: Enter the **From** and **To** phone numbers, and type the message below. When you wish to send the message, click **Send**.

SMS Inbox: You will see a list of all received messages. Click on the message to view it, **Delete** to delete the selected message, **Delete All** to delete all messages, and **Refresh** to check for new messages.



Voice

This page allows you to set up voice features. Each section can be accessed by selecting the appropriate option under **Voice Settings**.

Lines and Accounts

This page allows you to configure up to 5 VoIP profiles, 5 VoIP lines, and 1 analog account. These accounts establish inbound and outbound voice connections.

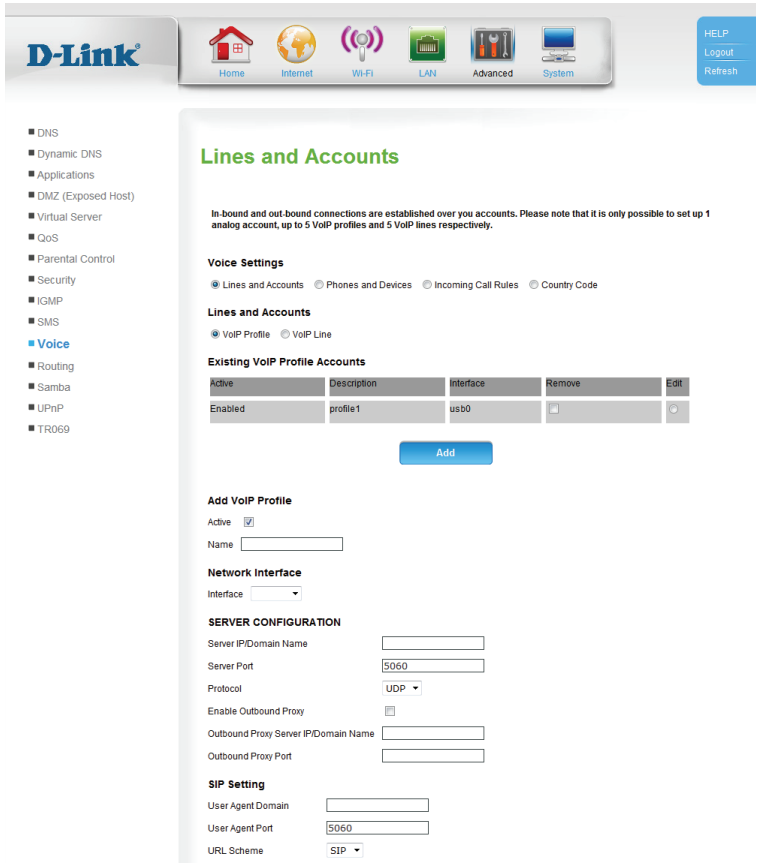
VoIP Profile

Here you can see a list of existing VoIP profile accounts. To remove an account, click that account's **Remove** button, and to edit the account click its **Edit** button.

To add a new profile account, click **Add**. More options will appear.

For the new profile to be active, make sure **Active** is selected, and give the new profile a **Name**.

Select the **Network Interface** that the profile will use.



Server IP / Domain Name: Enter the VoIP server IP address or domain name.

Server Port: Enter the server port number, or leave it at its default.

Protocol: Select the desired protocol to use for VoIP communications.

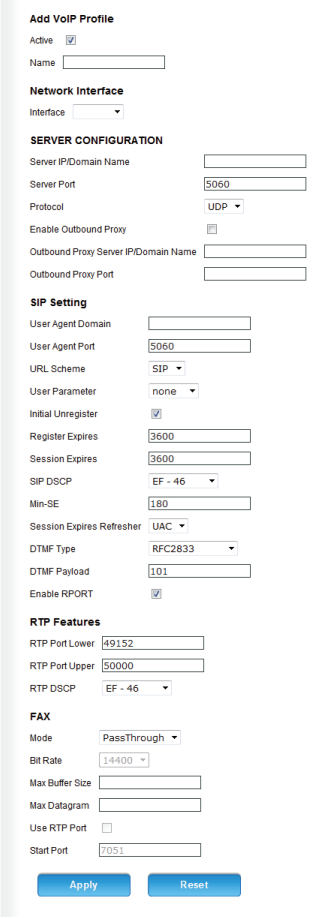
Enable Outbound Proxy: Check the box to use a network proxy for outbound VoIP communications. Enter the details below.

Outbound Proxy Server IP / Domain Name: Enter the outbound proxy server IP address or domain name.

Outbound Proxy Port: Enter the port number for the outbound proxy server.

The remaining settings are for advanced users. Please check with your phone provider, or leave the settings at their defaults if you are not sure.

Click **Apply** when you are done.



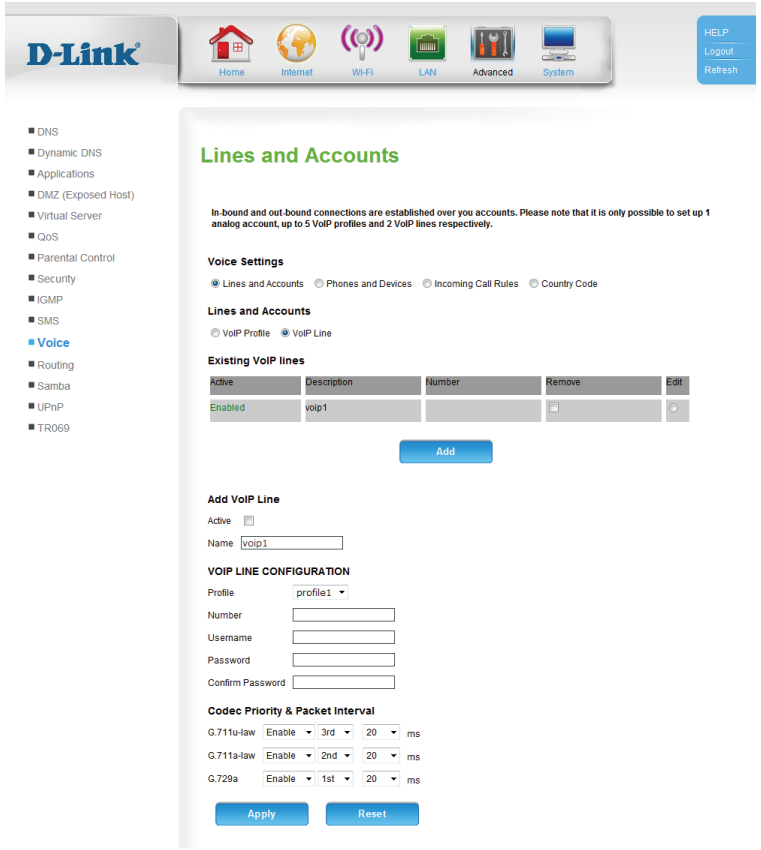
VoIP Line

Here you can see a list of existing VoIP lines. To remove a line, click that line's **Remove** button, and to edit the account click its **Edit** button.

To add a new line, click **Add**. More options will appear.

For the new line to be active, make sure **Active** is selected, and give the new line a **Name**.

Please check with your phone provider for the correct settings.



Profile: Select a VoIP profile from the drop-down menu. These can be configured under **VoIP Profile**.

Number: Enter the phone number of the line.

Username: Enter the username.

Password: Enter the password.

Confirm Password: Re-enter the password, for confirmation.

Codec Priority & Packet Interval: For each codec, you can specify the priority and packet interval from the drop-down menus. Leave at the defaults if you are not sure.

Click **Apply** when you are done.

Phones and Devices

This page allows you to configure your connected phone devices. Each section can be accessed by selecting the appropriate option under **Phones and Devices**.

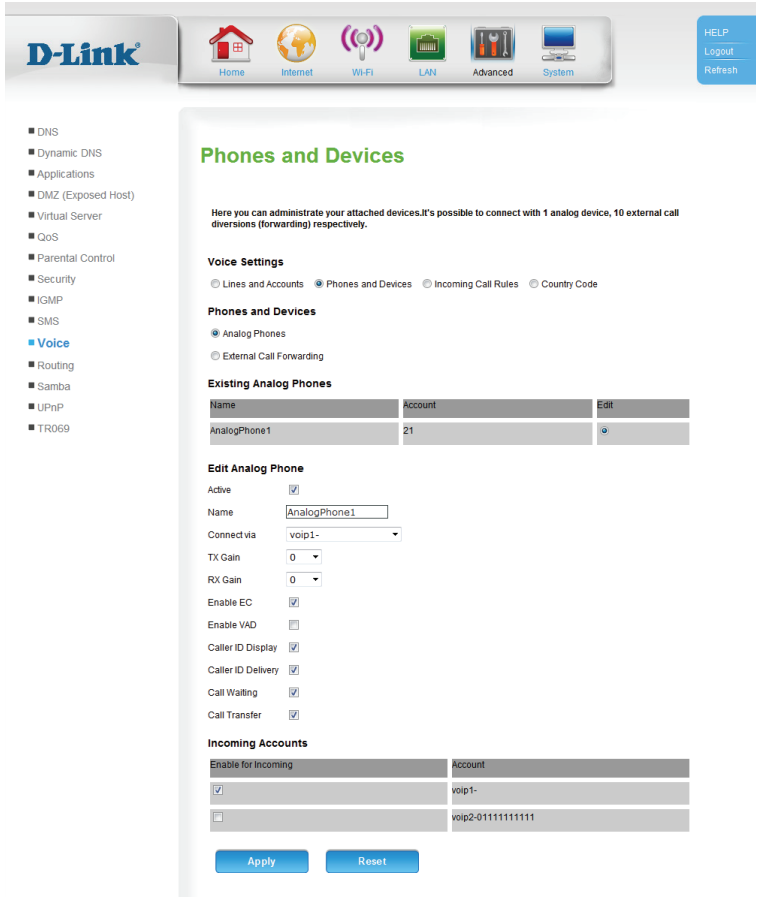
Analog Phones

Existing Analog Phones: Displays a list of connected analog phones.

Edit Analog Phone: First, select a device by clicking on the **Edit** radio button in the **Existing Analog Phones** table above. Next, configure the phone settings below. If you are not sure, leave the settings at their defaults, or contact your phone manufacturer.

Incoming Accounts: Check the **Enable for Incoming** box to enable the phone to received calls from the specified accounts.

Click **Apply** when you are done.

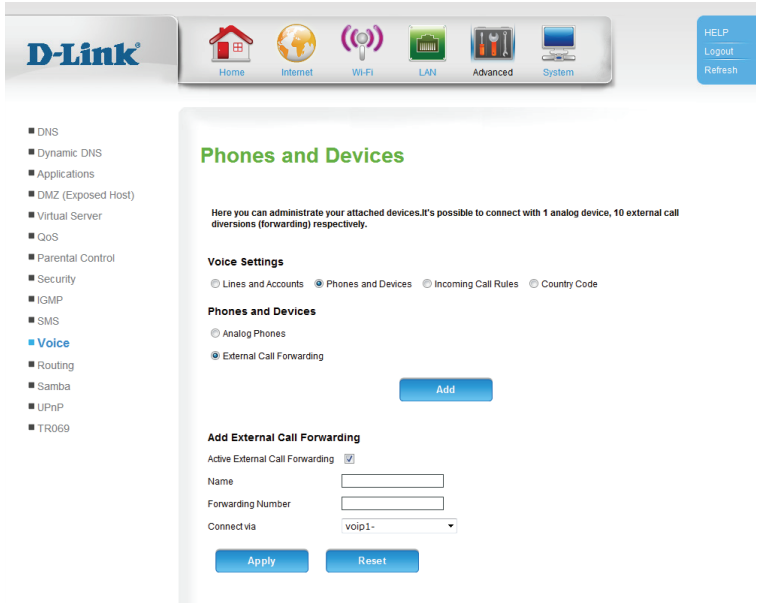


External Call Forwarding

Click **Add** to configure a new call diversion (forwarding). More settings will appear.

Add External Call Forwarding: Check **Active External Call Forwarding** to enable the new rule. Enter a **Name** of your choice, and enter the **Forwarding Number** to forward incoming calls to. Finally, select the VoIP account that the rule should use, under the **Connect via** drop-down menu.

Click **Apply** when you are done.



Incoming Call Rules

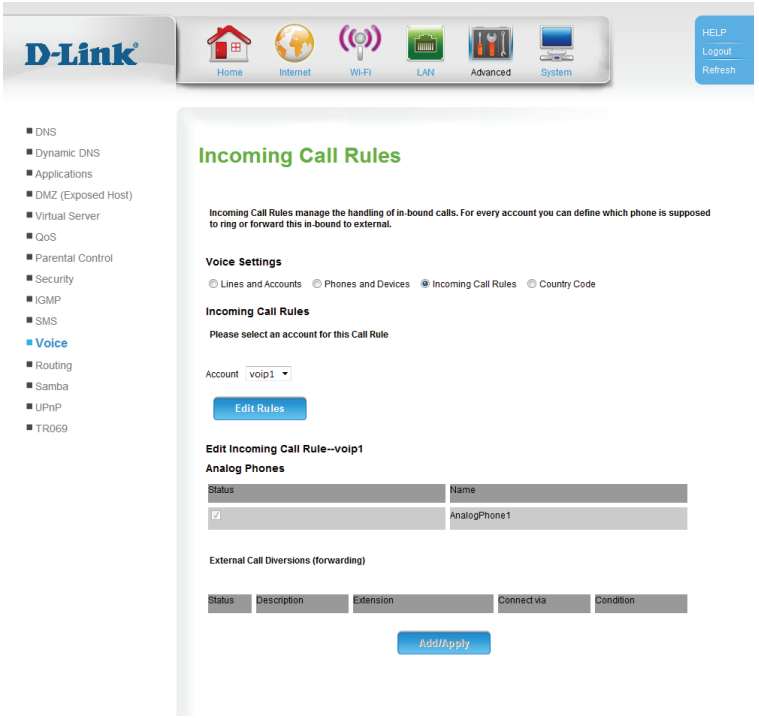
This page allows you to configure the inbound call rules.

Account: Select a previously-configured VoIP account from the drop-down menu.

Click **Edit Rules** to display a list of currently-configured rules.

Analog Phones: Displays a list of analog phone devices and their statuses.

External Call Diversions (forwarding): Click **Add/Apply** to add a new rule.

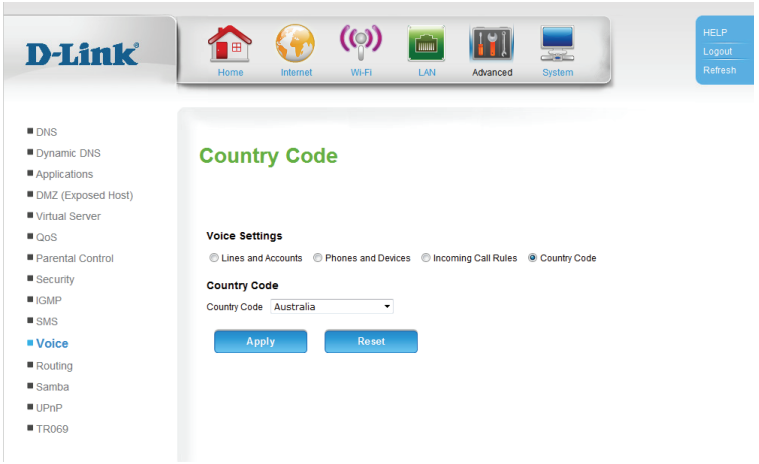


Country Code

This page allows you to specify the default country code of outbound phone calls.

Country Code: Select the country from the drop-down menu. The appropriate country code will be applied to each outgoing call.

Click **Apply** when you are done.



Routing

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

Enable Routing Rule: Check the box to enable the rule.

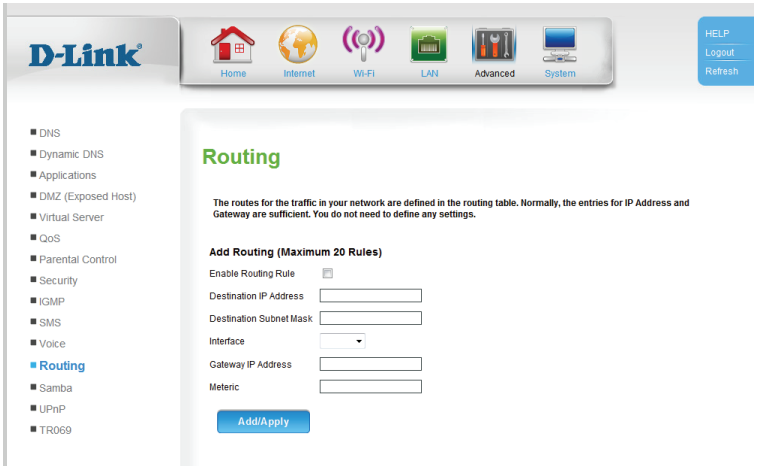
Destination IP Address: Enter the IP of the specified network that you want to access using the static route.

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

Interface: Select the interface to be used for the rule.

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

Metric: Enter the metric to be used for the rule.



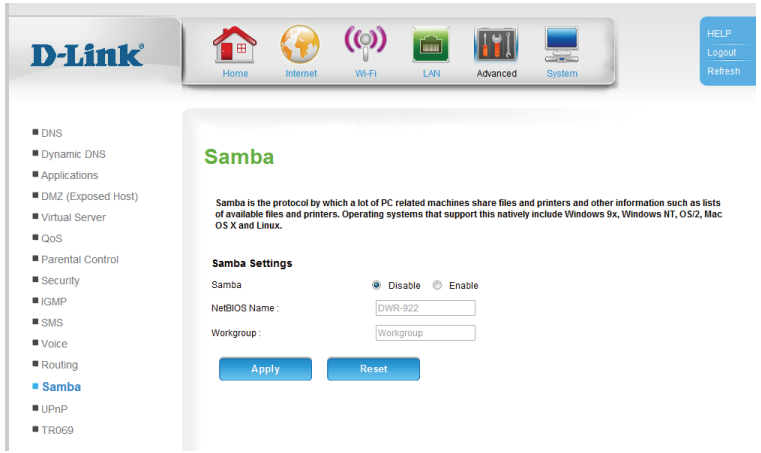
Samba

This page allows you to configure the router's Samba file and printer sharing settings.

Samba: Select **Enable** to enable Samba sharing, or **Disable** to disable it.

NetBIOS Name: Enter a name to identify the device when sharing data.

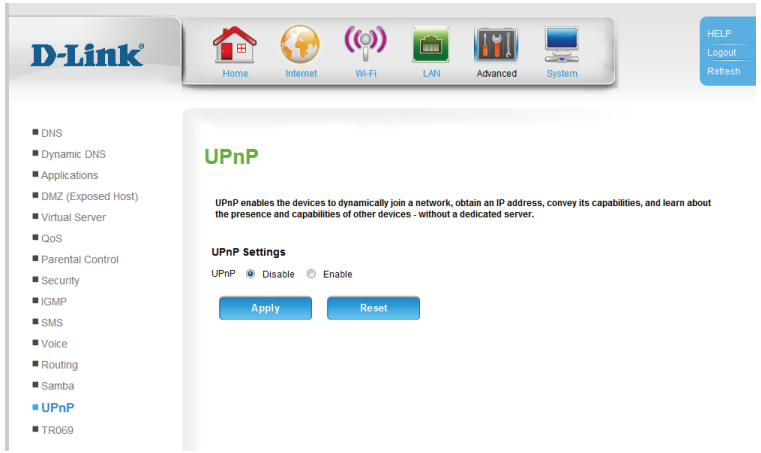
Workgroup: Enter the name of the workgroup to share data with.



UPnP

This page allows you to configure the router's Universal Plug and Play (UPnP) settings. UPnP provides compatibility with various networking equipment, software, and peripherals.

UPnP: Check the box to enable the Universal Plug and Play (UPnP) feature.



TR069

This page allows you to configure the router's TR069 settings. TR-069 provides standardized remote device management for residential gateways, which allows your router to be configured remotely by your ISP (if supported), or any service providing Auto-Configuration Servers (ACS). If you wish to configure TR069 but lack the required settings, contact your Internet Service Provider (ISP).

TR069: Check the box to enable TR069.

Interface: Select the interface to use.

Username: Enter your ACS username.

Password: Enter your ACS password.

ACS URL: Enter the ACS URL.

CPE URI: Enter the CPE URI.

CPE Port: Enter the CPE Port.

Inform Configure: Select either **Disable** or **Periodic**.

Periodic Interval: If you selected **Periodic** above, enter the interval here.

Schedule Time: Select the **Month**, **Day**, **Year**, **Hour**, **Minute**, and **Second**.

STUN Enable: Select **Enable** to enable Session Traversal Utilities for NAT (STUN).

STUN Server Address: If you selected **Enable** above, enter the STUN server address.

STUN Server Port: Enter the STUN server port.

STUN Username: Enter the STUN username.

STUN Password: Enter the STUN password.

STUN UDP Listen Port: Enter the STUN UDP listen port.

System

Time Settings

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

Time: Displays the router's current time.

Sync with NTP Servers: Check the box to automatically update the time in accordance with the currently configured NTP servers.

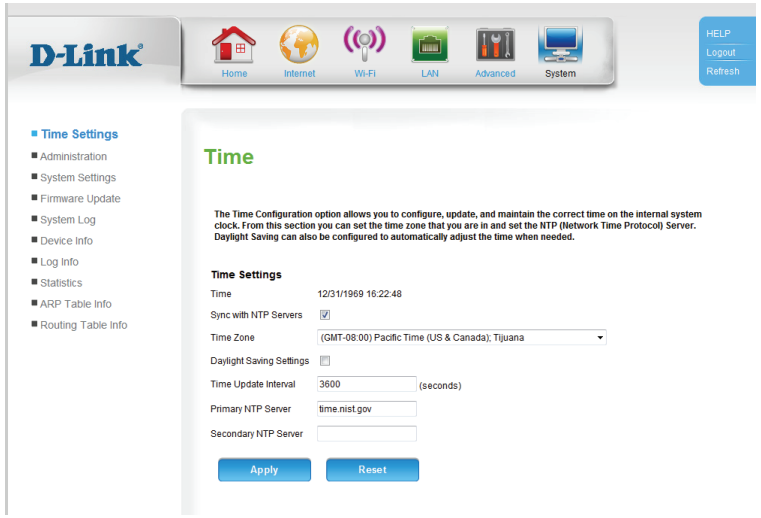
Time Zone: Select your time zone from the drop-down menu.

Daylight Saving Settings: Check the box to enable daylight saving adjustments.

Time Update Interval: Enter the interval in seconds between time updates from the currently configured NTP server.

Primary NTP Server: Enter the address of the primary NTP server.

Secondary NTP Server: Enter the address of the secondary (backup) NTP server.



Administration

On this page you can configure the router's username and password, the remote management address, and the various protocols with which to access the network.

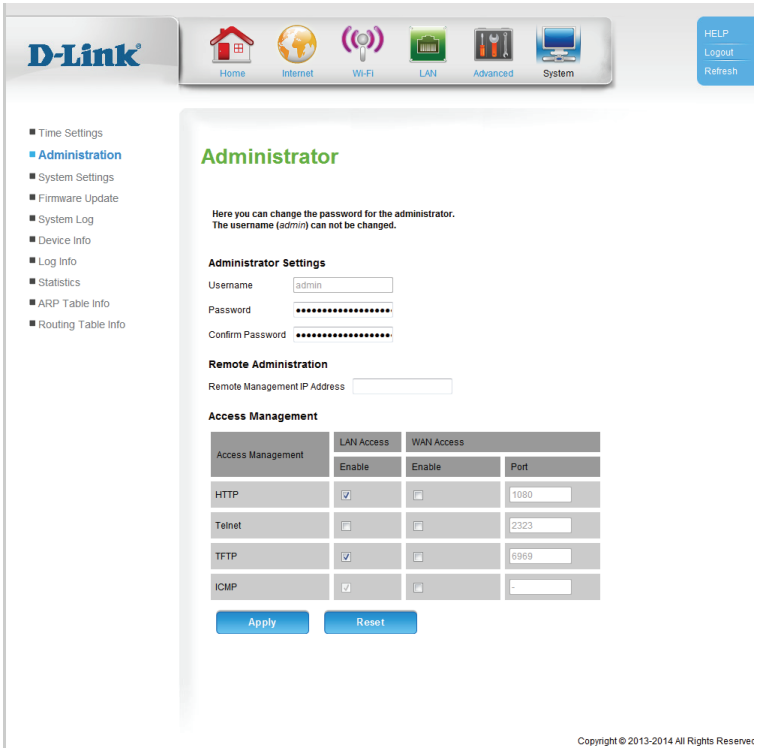
Username: The username is always **admin**, and cannot be changed.

Password: Enter the new password to access the configuration interface of the router.

Confirm Password: Re-enter the new password for verification.

Remote Management IP Address: To enable remote management, enter the IP address that the router will use for remote management.

Access Management: For each protocol, check the **Enable** box under either **LAN Access**, **WAN Access**, or both, and specify a **Port**.



System Settings

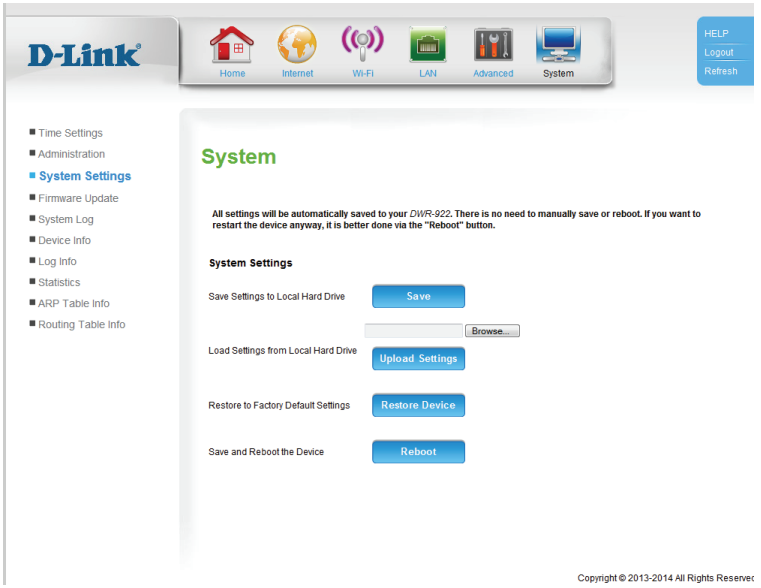
On this page you can save your current configuration settings to a local hard drive for backup and re-use, load previously saved settings, restore the factory default settings, and reboot the device.

Save Settings to Local Hard Drive: To save the current configuration, click **Save**.

Load Settings from Local Hard Drive: To load a previously saved configuration, click **Browse...** and navigate to the saved configuration file. Lastly, click **Upload Settings**.

Restore to Factory Default Settings: To restore the router to its default settings, click **Restore Device**. Note that any unsaved settings will be lost.

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

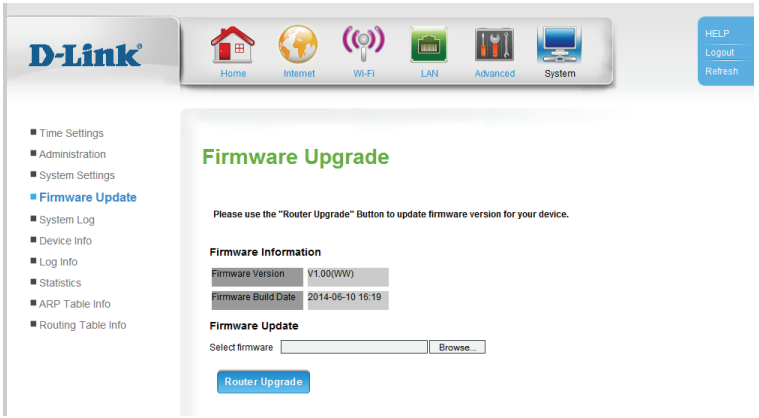


Firmware Update

This page displays your router's current firmware version, and allows you to upgrade your router's firmware.

Firmware Information: Displays your router's current firmware version and build date.

Firmware Update: To upgrade your router's firmware, click **Browse...** and navigate to the firmware file on your computer's hard drive. Click **Router Upgrade** to start the upgrade process.



System Log

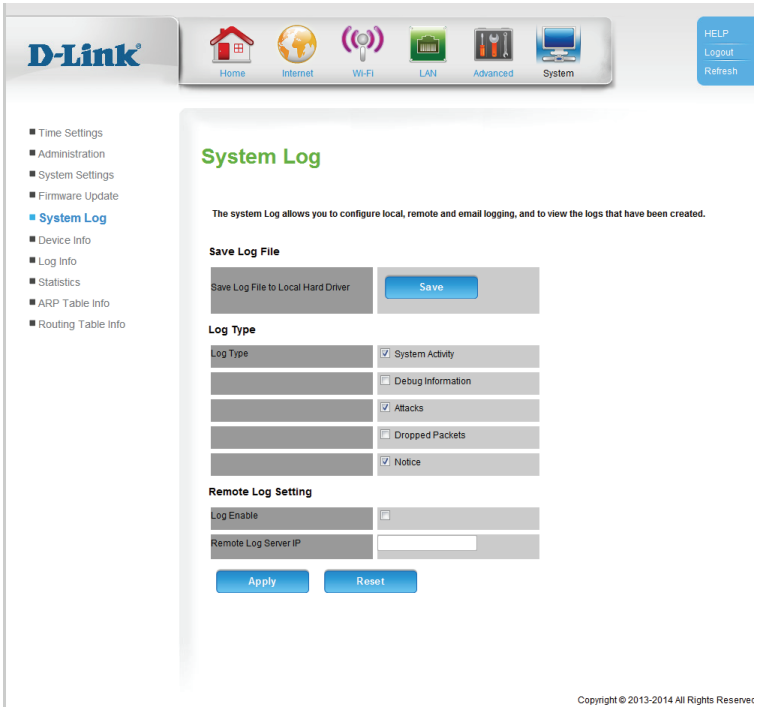
This page allows you to configure your log settings, and save your log to a local hard drive.

Save Log File to Local Hard Drive: To save a copy of the system log to your local hard drive, click **Save**.

Log Type: Check the boxes for each information type you want to include in the system log.

Log Enable: Check the box to enable remote logging.

Remote Log Server IP: If you checked the box to enable remote logging, enter the IP address of the log server.



Device Info

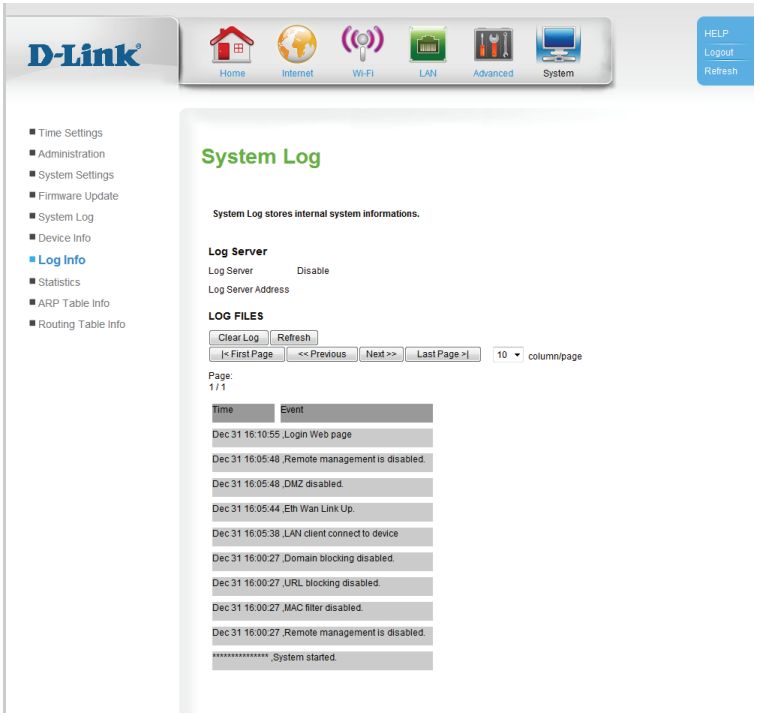
This page provides general information about your router and Internet connection.

Log Info

This page allows you to check the status of the system log, and view it.

Log Server: Displays the current log server status, if enabled, and its current address.

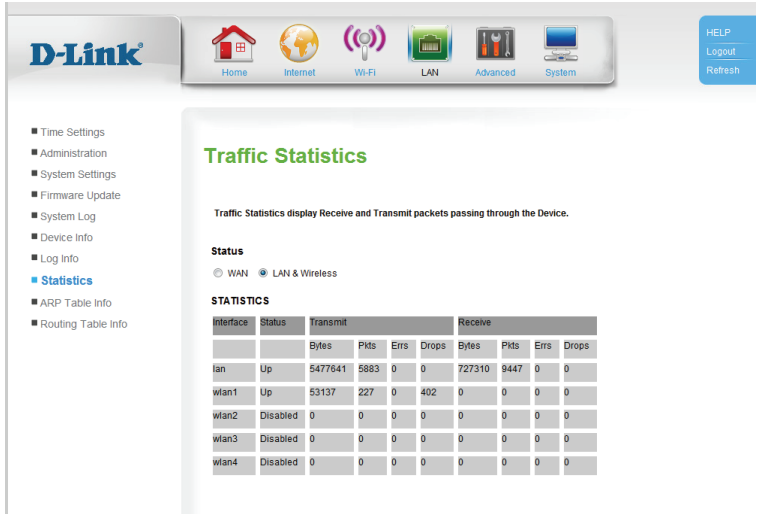
LOG FILES: The log is displayed below. Click **Refresh** to update it, **Clear Log** to clear it, and the navigation buttons below to select different pages in the log.



Statistics

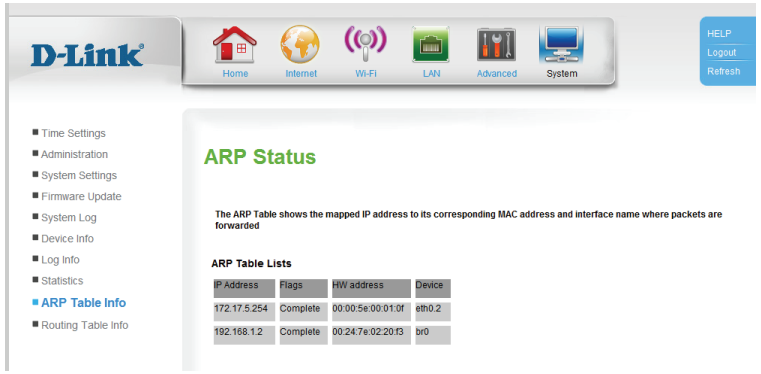
This page displays the router's WAN and local network traffic statistics.

Status: Select whether to view the **WAN** statistics or the **LAN & Wireless** statistics. The selected information will appear below.



ARP Table Info

This page displays the Address Resolution Protocol (ARP) information. Each IP address is shown with its corresponding MAC address and interface.



Routing Table Info

This page displays the current routing tables.

Connect a Wireless Client to your Router

WPS Button

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

Step 1 - Press the WPS button on the DWR-922 for about 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).

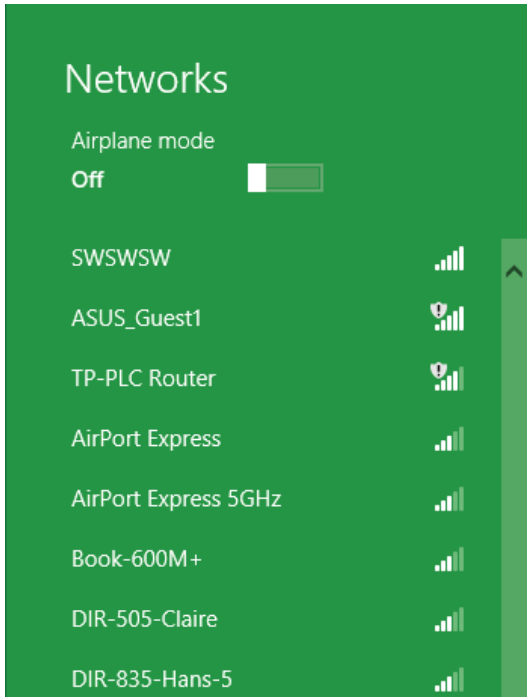
Step 3 - Allow up to 1 minute for your connection to be configured. Once the Internet light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

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.

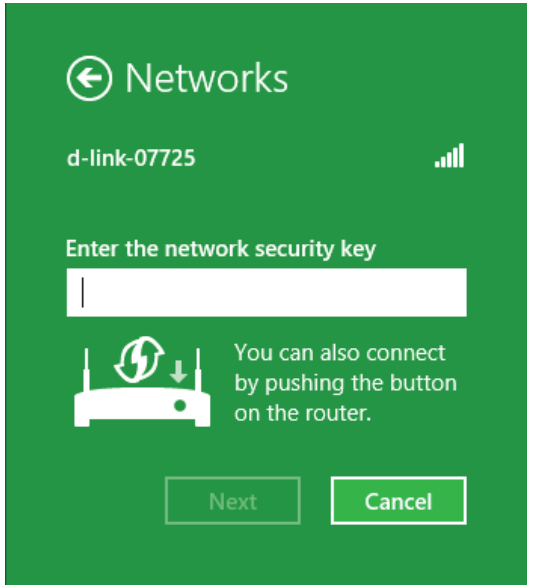
To join an existing network, locate the wireless network icon in the taskbar next to the time display.

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.

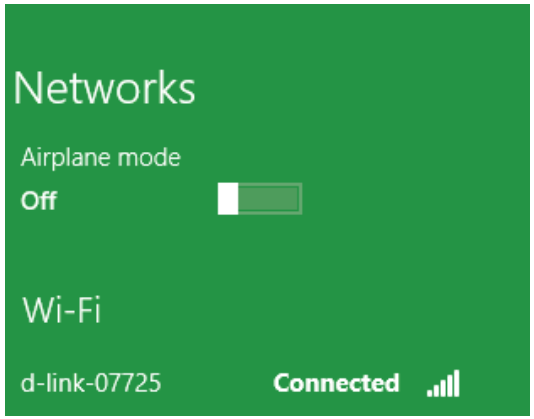


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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.

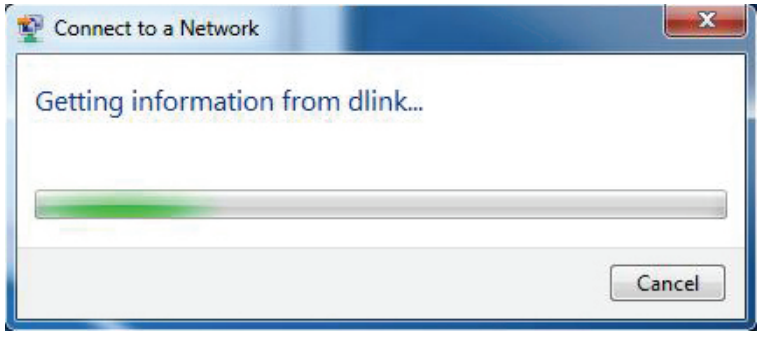
1. Click on the wireless icon in your system tray (lower-right corner).

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

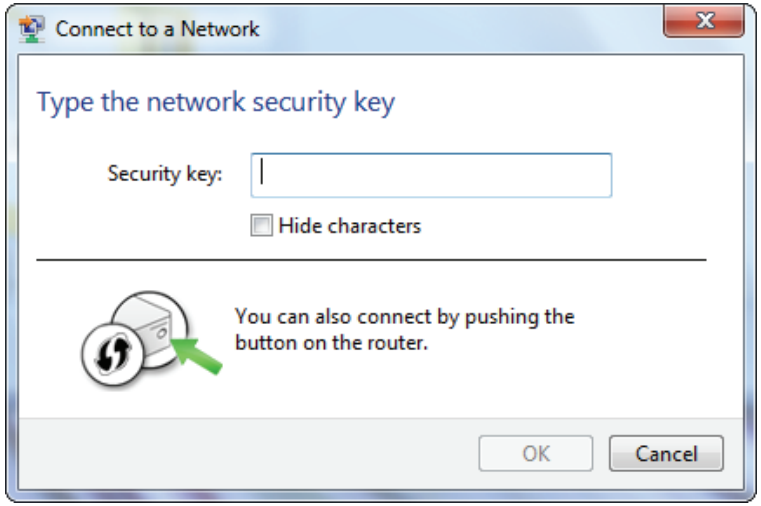
3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

   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 81 for more information.

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



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

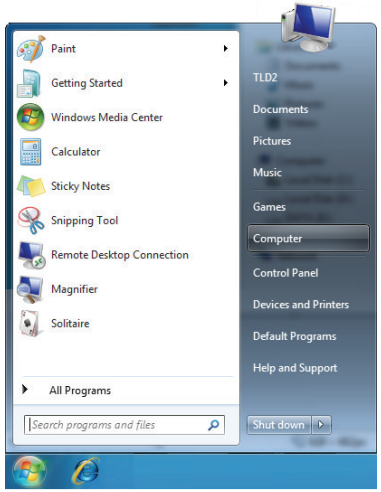


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as the one on the wireless router.

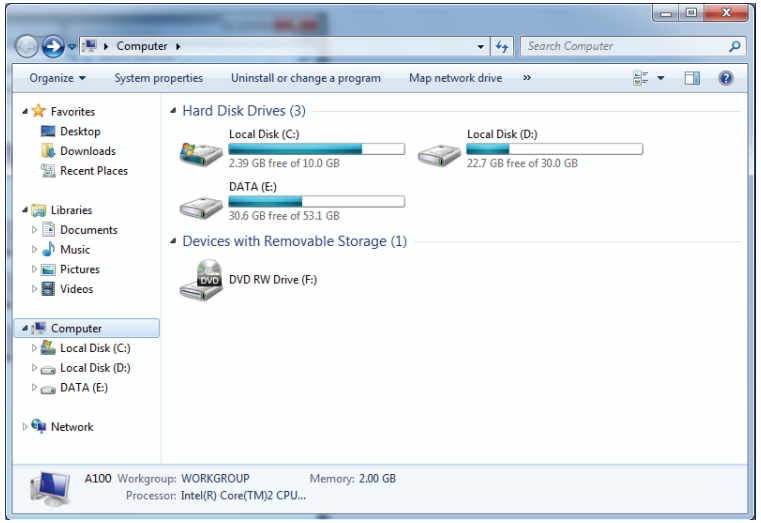
WPS

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

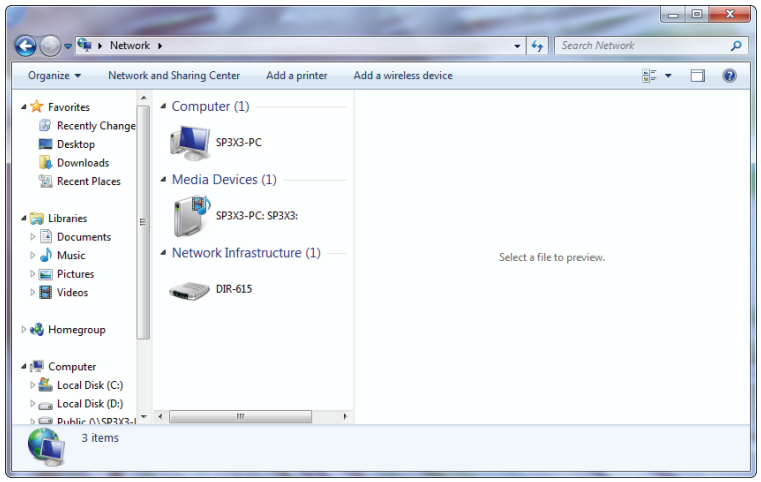
1. Click the **Start** button and select **Computer** from the Start menu.



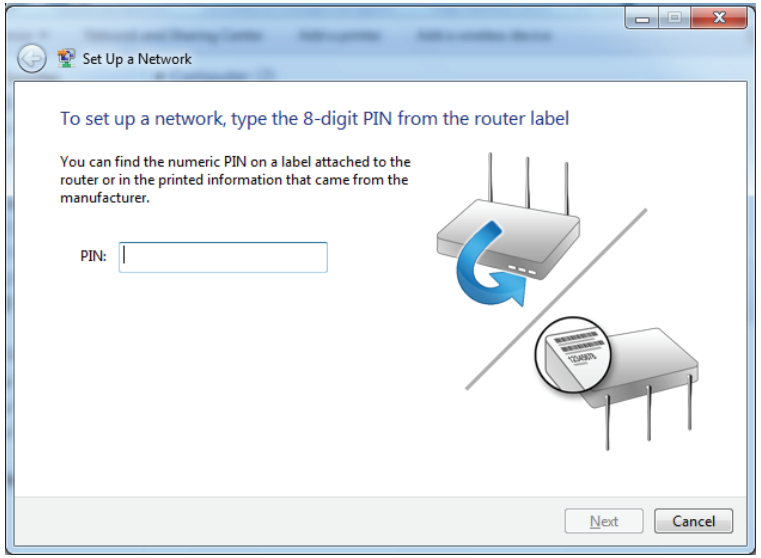
2. Click **Network** on the left side.



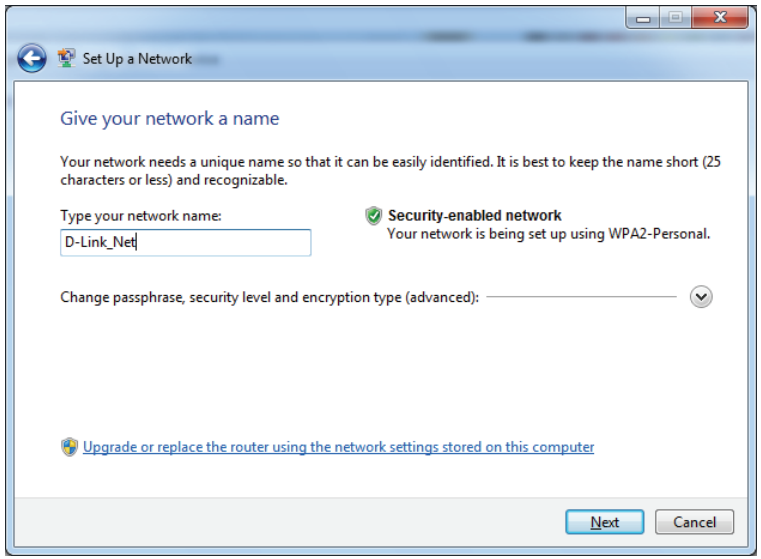
3. Double-click the DWR-922.



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

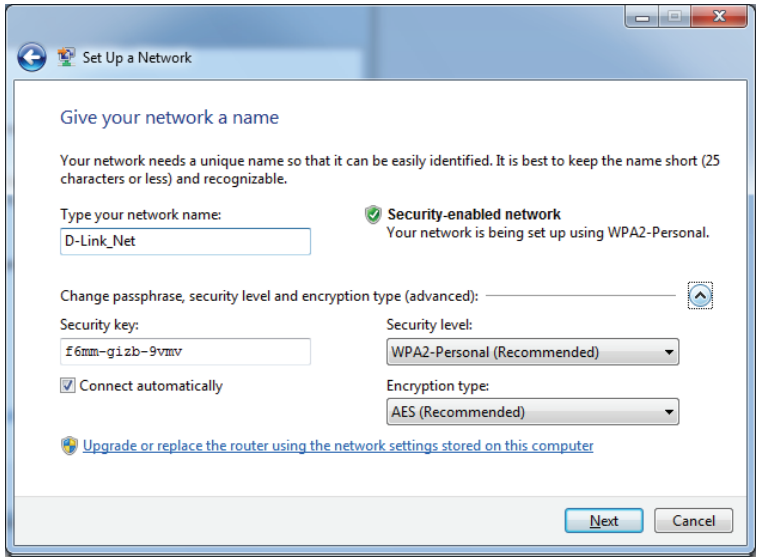


5. Type a name to identify the network.



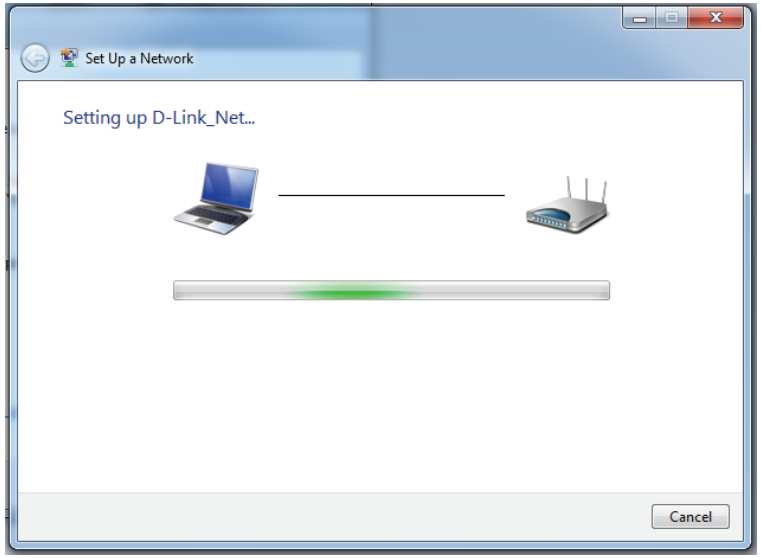
6. To configure advanced settings, click the icon.

Click **Next** to continue.



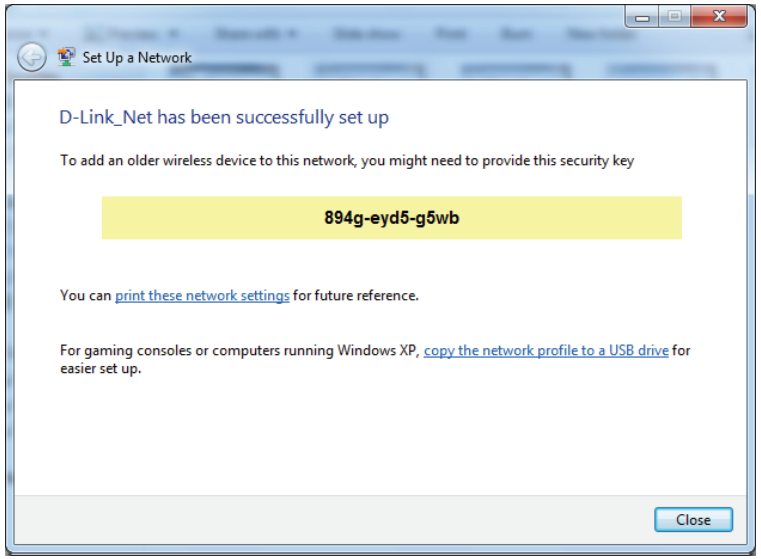
7. The following window appears while the router is being configured.

   Wait for the configuration to complete.



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

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



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

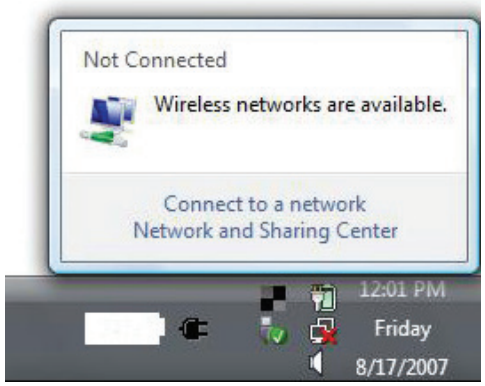
Windows Vista®

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

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

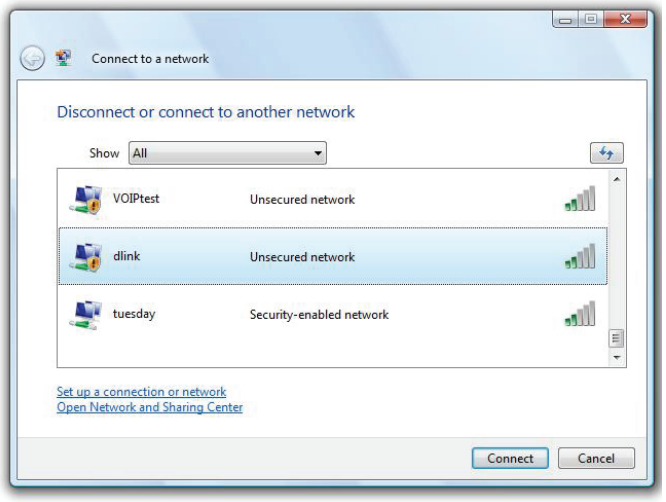
or

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



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

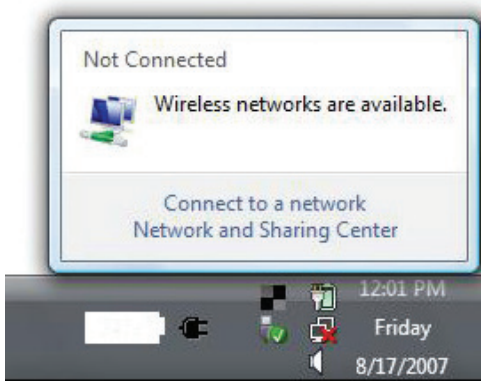
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



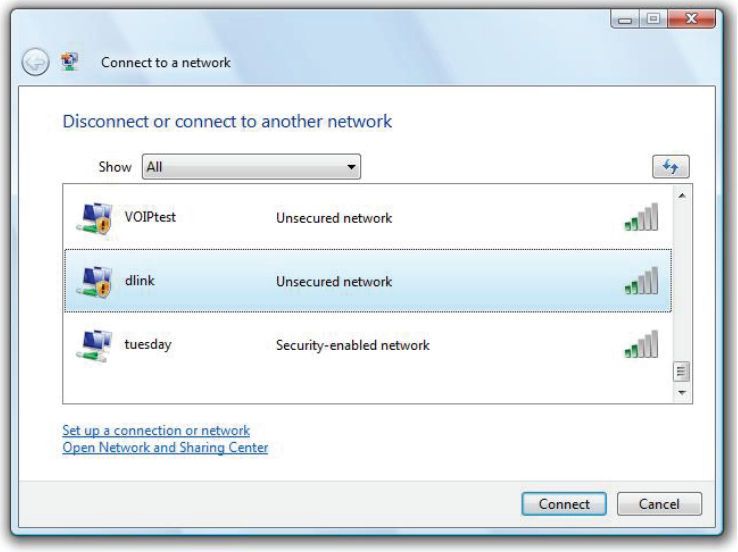
WPA/WPA2

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

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



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



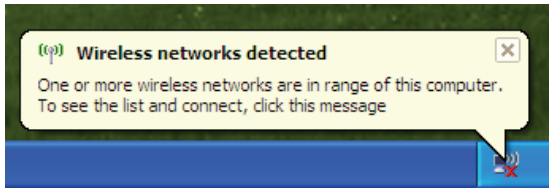
3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

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

Windows® XP

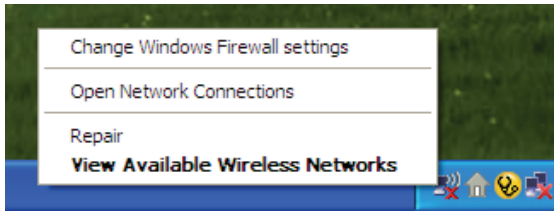
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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

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



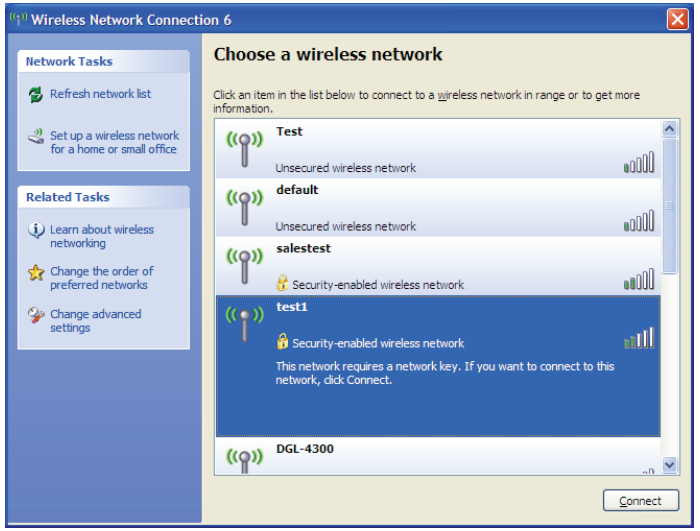
or

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



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

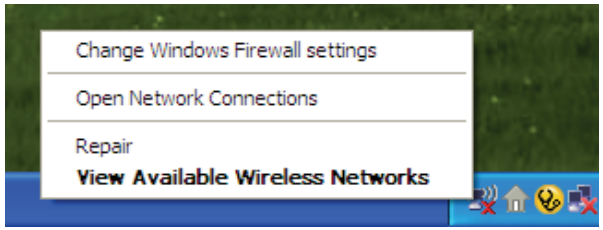
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



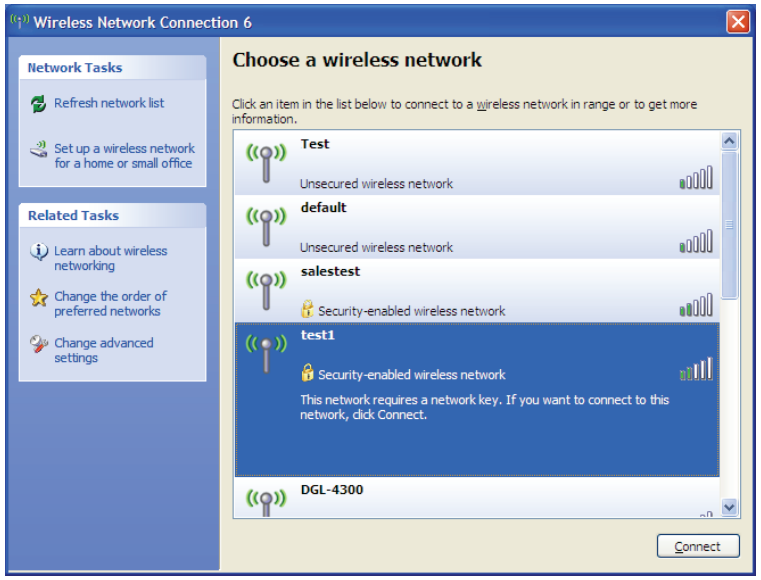
WPA/WPA2

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

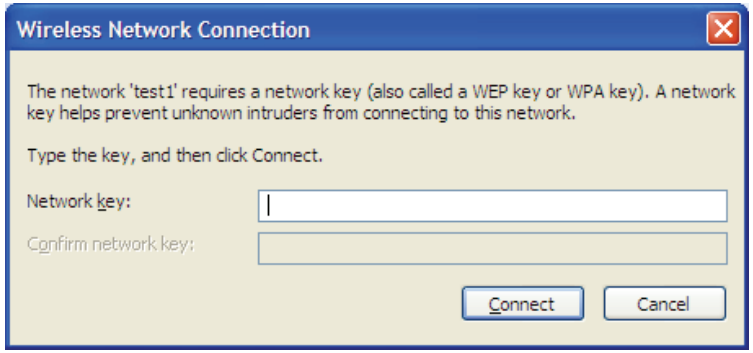
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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



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



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

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-922. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to these examples.

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

When entering the IP address of the D-Link router (**192.168.1.1** 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 Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
    - Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.
    - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
    - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
    - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your 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 **192.168.1.1**. 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?

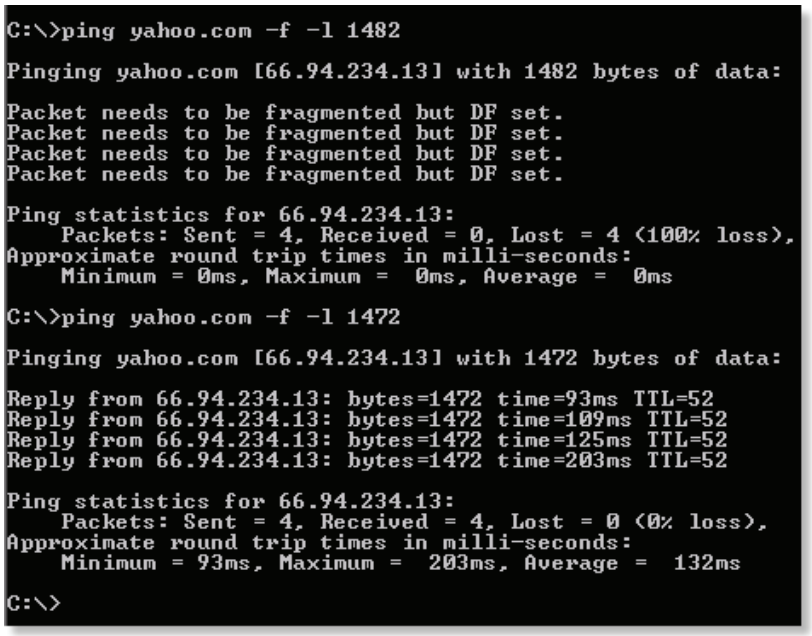
If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

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**



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

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

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

- Open your browser, enter the IP address of your router (**192.168.1.1**) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU, enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

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

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people 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-922 wireless network CardBus adapters.

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

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

Networking Basics

Check your IP address

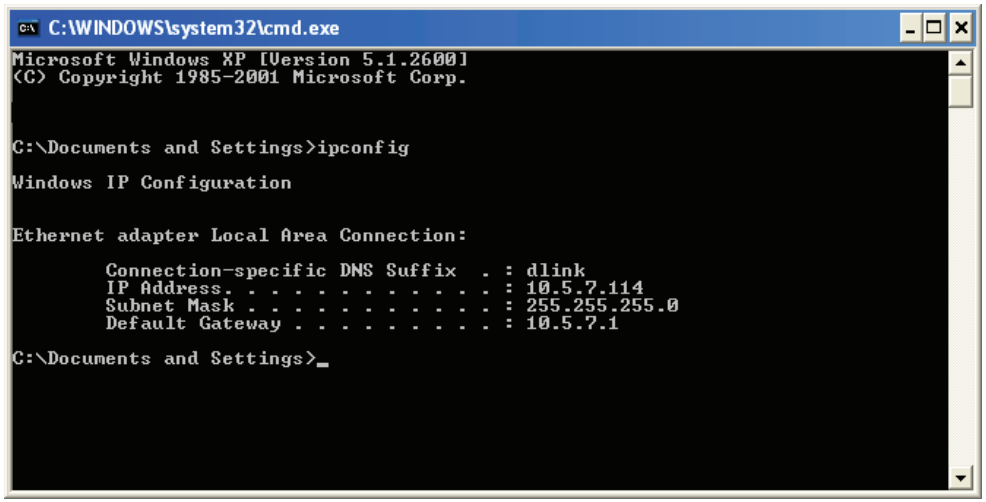
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



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

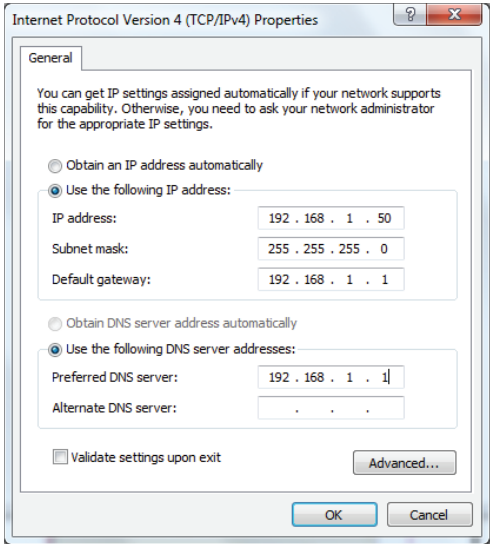
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

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 192.168.1.1, 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. 192.168.1.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.1.1). The Alternate DNS is not needed or you may enter a DNS server from your ISP.

Step 5

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

Wireless Security

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

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

What is WPA?

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

The 2 major improvements over WEP:

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

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

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

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

Technical Specifications

LTE Band
- 800 / 900 / 1800 / 2600 MHz

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

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 100 Mbps

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

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

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

VPN
- L2TP/PPTP/IPSEC/VPN Pass-through

Antenna
- Two detachable 3G/4G antennas

Ports
- Four LAN ports (RJ-45)
- WAN port (RJ-45)
- Phone port (RJ-11)

USIM Slot
- Standard 6-pin SIM card interface

LED Status Indicators
- WAN
- LAN
- WLAN
- 3G
- 4G
- SMS
- VoIP
- 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.