

DMZ

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

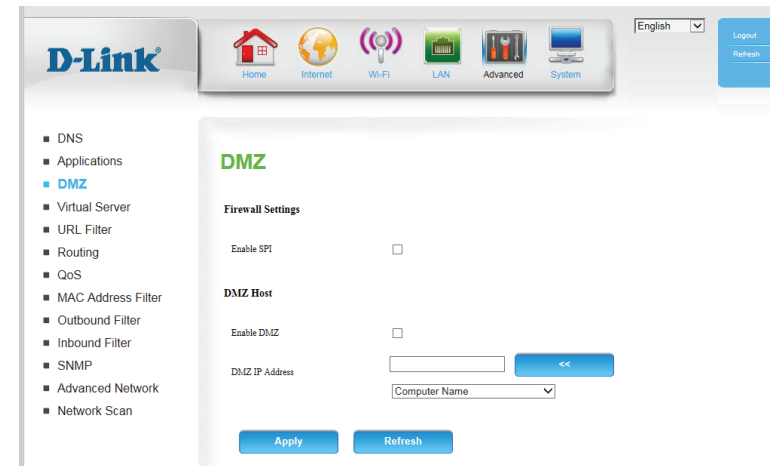
Enable SPI: Enabling Stateful Packet Inspection (SPI) helps to prevent cyber attacks by validating that the traffic passing through the session conforms to the protocol.

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

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

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

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



Virtual Server

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

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

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

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

VIRTUAL SERVERS LIST

ID: This identifies the rule.

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

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

Enable: Check the box to enable the specified rule.

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

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

D-Link

Home Internet Wi-Fi LAN Advanced System

English Logout Refresh

Virtual Server

The Externally acts as server. It receives the requests of remote users under its public IP address and forwards them automatically to the Virtual Server. So a client in your network behind NAT or firewall can provide services as a Virtual Server. You just have to enable specific ports or port ranges and protocols (UDP/TCP). File sharing or web services for e.g. HTTP, FTP or POP3 are possible. The private IP addresses of the servers in the local network remain safe. If you have a dynamic IP address, you may want to enable DynDNS additionally.

Well known services: -- Select one -- **Copy to** ID: --

Use schedule rule: -- ALWAYS ON --

Virtual Servers List

ID	Service Ports	Server IP: Port	Enable	Schedule Rule
1		:	☐	Add New Rule...
2		:	☐	Add New Rule...

URL Filter

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

URL Filtering: Check the box to enable URL Filtering.

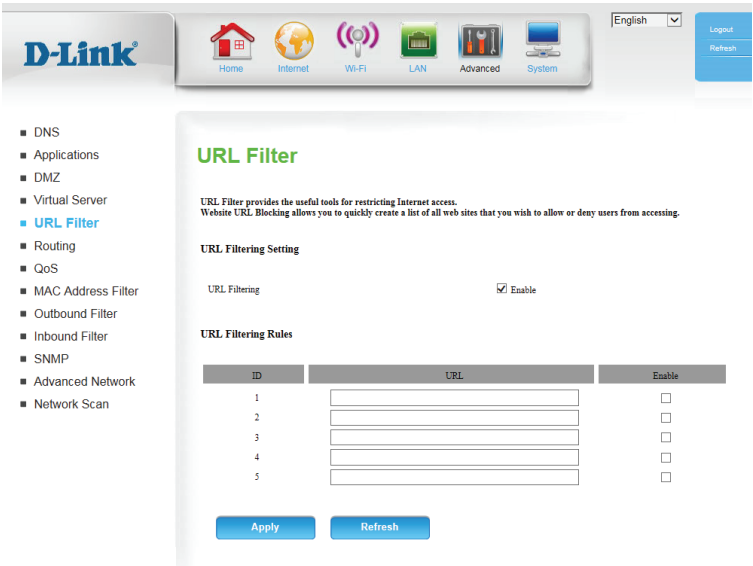
URL FILTERING RULES

ID: This identifies the rule.

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

Enable: Check the box to enable the specified rule.

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



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.

D-Link

Home Internet Wi-Fi LAN Advanced System

English Logout Refresh

- DNS
- Applications
- DMZ
- Virtual Server
- URL Filter
- **Routing**
- QoS
- MAC Address Filter
- Outbound Filter
- Inbound Filter
- SNMP
- Advanced Network
- Network Scan

Routing

The routes for the traffic in your network are defined in the routing table. Normally, the entries for IP Address and Gateway are sufficient. You do not need to define any settings.

RIP Setting

RIP : ☐ Enable ☒ RIPv1 ☐ RIPv2

Routing Rules

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐

Apply Refresh

QoS

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

Enable QoS Select this box to enable the QoS feature.

Packet Filter:

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

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

QOS RULES

ID: This identifies the rule.

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

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

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

Enable: Check the box to enable the specified rule.

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

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

D-Link

Home Internet Wi-Fi LAN Advanced System

English Logout Refresh

- DNS
- Applications
- DMZ
- Virtual Server
- URL Filter
- Routing
- **QoS**
- MAC Address Filter
- Outbound Filter
- Inbound Filter
- SNMP
- Advanced Network
- Network Scan

QoS

QoS Engine Setup

Enable QoS Packet Filter: ☐

Upstream bandwidth: kbps

Use schedule rule: ALWAYS ON ID:

QoS Rules

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	:	:	High	☐	Add New Rule...
2	:	:	High	☐	Add New Rule...
3	:	:	High	☐	Add New Rule...
4	:	:	High	☐	Add New Rule...
5	:	:	High	☐	Add New Rule...
6	:	:	High	☐	Add New Rule...
7	:	:	High	☐	Add New Rule...
8	:	:	High	☐	Add New Rule...

MAC Address Filter

The **MAC (Media Access Controller) Address Filter** option is used to control network access based on the MAC address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

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

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

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

MAC FILTERING RULES

ID: This identifies the rule.

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

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

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

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

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

D-Link Home Internet Wi-Fi LAN Advanced System

English Logout Refresh

- DNS
- Applications
- DMZ
- Virtual Server
- URL Filter
- Routing
- QoS
- MAC Address Filter**
- Outbound Filter
- Inbound Filter
- SNMP
- Advanced Network
- Network Scan

MAC Address Filter

MAC Filtering Settings

MAC Address Control ☐ Enable

☐ Connection control Wireless and wired clients with C checked can connect to this device, and unspecified MAC addresses to connect.

☐ Association control Wireless clients with A checked can associate to the wireless LAN, and unspecified MAC addresses to associate.

DHCP clients ID

MAC Filtering Rules

ID	MAC Address	C	A
1		☐	☐
2		☐	☐
3		☐	☐
4		☐	☐
5		☐	☐

Outbound Filter

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

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

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

OUTBOUND FILTER RULES LIST

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

ID: This identifies the rule.

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

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

Enable: Check the box to enable the specified rule.

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

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

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

Outbound Filter

Outbound Filter Setting

Outbound Filter ☐ Enable

Use schedule rule: ALWAYS ON Copy to ID:

Outbound Filter Rules List

☒ Allow all to pass except those match the following rules.
☐ Deny all to pass except those match the following rules.

ID	Source IP: Ports	Destination IP: Ports	Enable	Schedule Rule
1			☐	Add New Rule...
2			☐	Add New Rule...
3			☐	Add New Rule...
4			☐	Add New Rule...
5			☐	Add New Rule...
6			☐	Add New Rule...
7			☐	Add New Rule...
8			☐	Add New Rule...

Previous page Next page

Apply Refresh

Inbound Filter

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

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

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

INBOUND FILTER RULES LIST

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

ID: This identifies the rule.

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

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

Enable: Check the box to enable the specified rule.

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

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

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

D-Link

Home Internet Wi-Fi LAN Advanced System

English Logout Refresh

- DNS
- Applications
- DMZ
- Virtual Server
- URL Filter
- Routing
- QoS
- MAC Address Filter
- Outbound Filter
- **Inbound Filter**
- SNMP
- Advanced Network
- Network Scan

Inbound Filter

Inbound Filter Setting

Inbound Filter ☐ Enable

Use schedule rule: ALWAYS ON Copy to ID:

Inbound Filter Rules List

☒ Allow all to pass except those match the following rules.
☐ Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1			☐	Add New Rule...
2			☐	Add New Rule...
3			☐	Add New Rule...
4			☐	Add New Rule...
5			☐	Add New Rule...
6			☐	Add New Rule...
7			☐	Add New Rule...
8			☐	Add New Rule...

Previous page Next page

Apply Refresh

SNMP

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

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

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

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

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

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

SNMP Version: Select the SNMP version of your system.

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

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

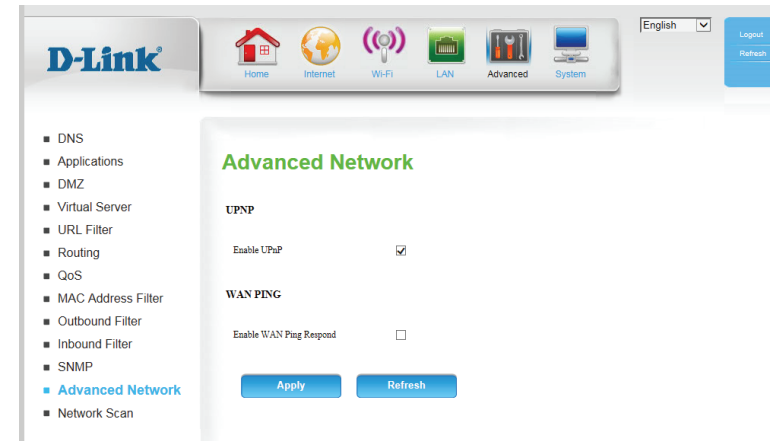
Advanced Network

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

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

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

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



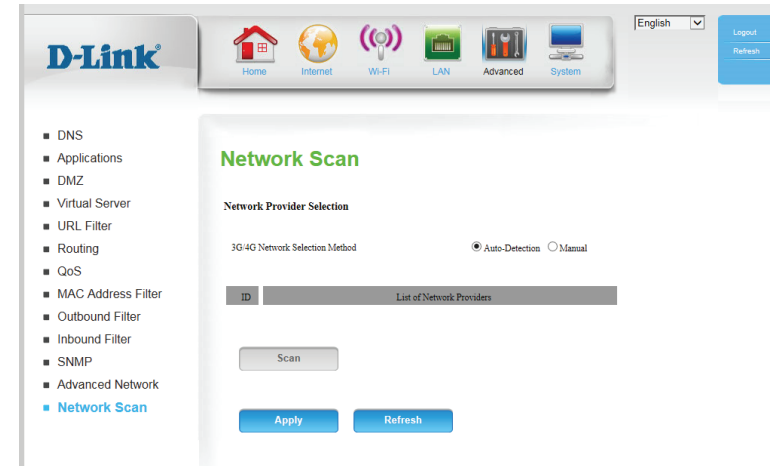
Network Scan

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

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

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

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



System Time Settings

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

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

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

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

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

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

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

D-Link

Home Internet Wi-Fi LAN Advanced System

English Logout Refresh

Time Settings

■ Time Settings
■ Administration
■ Reboot & Reset
■ Firmware Upgrade
■ System Logs
■ Schedules
■ Connection Reset

The time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Time: Mon Dec 31, 2012 19:37:44
Time Zone: (GMT -12:00) Eniwetok, Kwajalein
Enable Daylight Saving: ☒
Start: 0 1 Jan (Hour Day/Month)
End: 23 31 Dec (Hour Day/Month)
Sync your computer's time settings
☒ Automatically synchronize with Internet time server
NTP Server Used: time.nist.gov
time.nist.gov Update Now

Sync. RESULT

Apply Refresh

Copyright © 2012. All Rights Reserved

Administration

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

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

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

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

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

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

The screenshot shows the D-Link web management interface. At the top, there's a navigation bar with icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. The 'Administration' section is highlighted in the left sidebar. The main content area is titled 'Administration' and contains the following sections:

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

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

Reboot & Reset

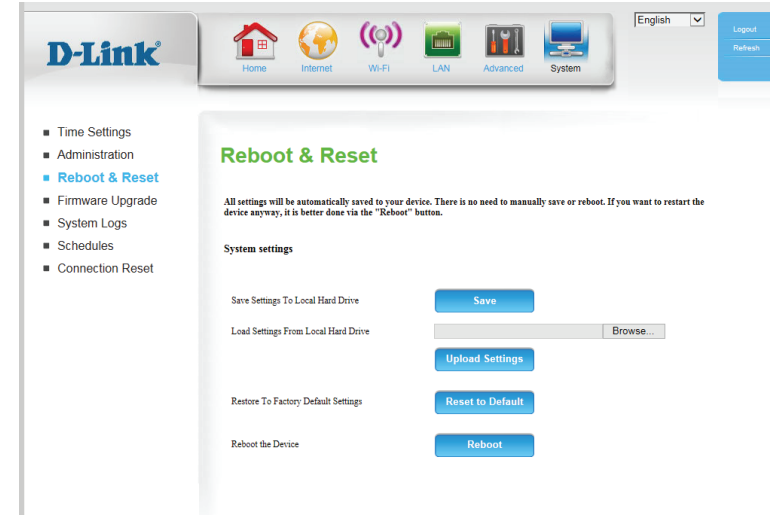
Here, you can save the current system settings to a local hard drive.

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

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

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

Reboot the Device: This option will reboot the router.



Firmware Upgrade

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

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

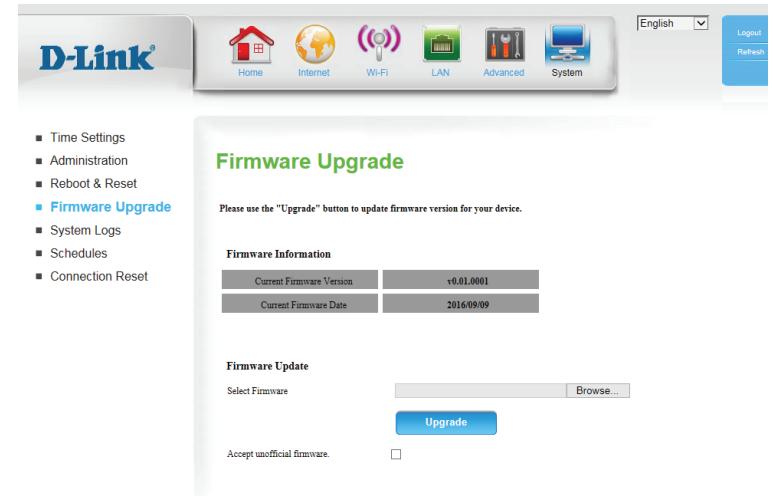
Current Firmware Date: Displays your current firmware's release date.

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

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

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

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



System Logs

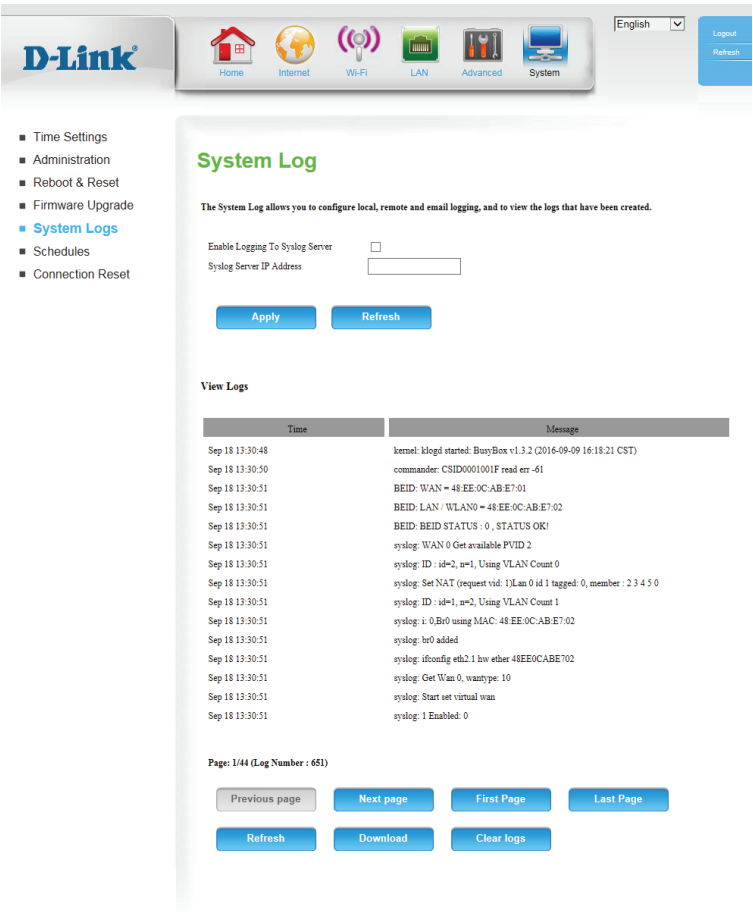
The DWR-922 keeps a running log of events and activities occurring on the router. You may send these logs to a Syslog server on your network.

- Enable Logging to Syslog Server:

Check the box to send the router logs to a Syslog server.
- Syslog Server IP Address:

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

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



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.

The screenshot shows the D-Link router's web interface. The top navigation bar includes the D-Link logo and icons for Home, Internet, Wi-Fi, LAN, Advanced, and System. The left sidebar lists various settings categories, with 'Connection Reset' highlighted. The main content area is titled 'Connection Reset' and contains the following configuration options:

- Auto-Reboot:** A radio button selection between 'Disabled' (selected) and 'Enabled'.
- Reboot-Schedule:** Two dropdown menus for selecting the hour (0) and minute (0).
- Reboot-Schedule:** A radio button selection between 'Daily Schedule' (selected), 'Weekly Schedule Day of Week' (Monday), and 'Date of Month' (1).
- Buttons:** 'Apply' and 'Refresh' buttons at the bottom.

Copyright © 2012 All Rights Reserved

Connect a Wireless Client to your Router

WPS Button

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

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



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

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

Connecting to a Wireless Network

Windows® 10

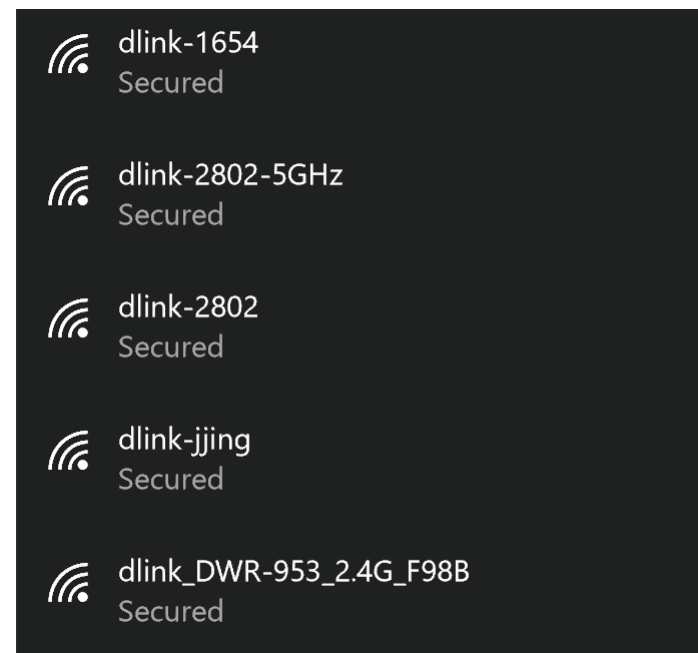
To connect to a wireless network using Windows 10, you will need to know the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to.

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



Wireless Icon

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



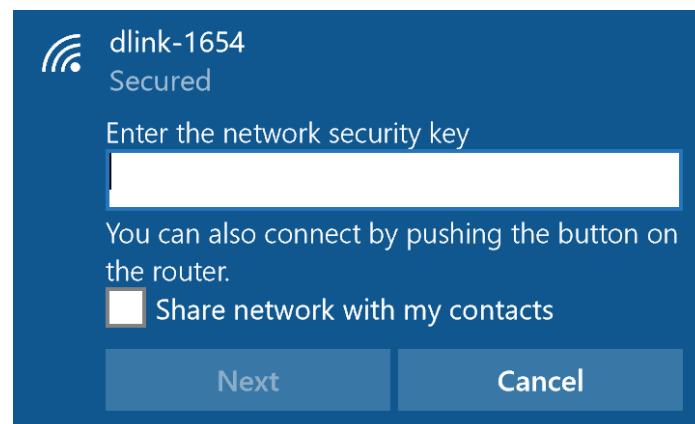
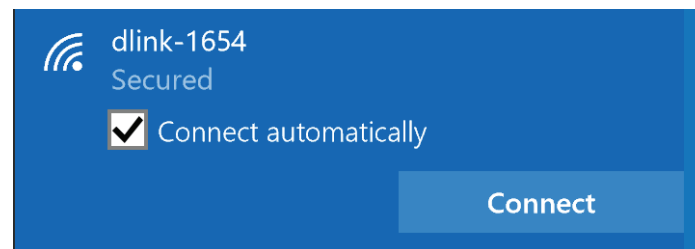
To connect to the network, click **Connect**.

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

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

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

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



Windows® 8

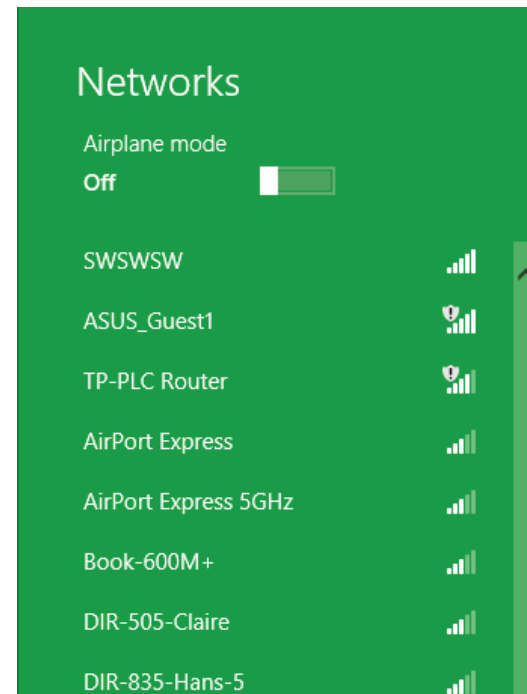
WPA/WPA2

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

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



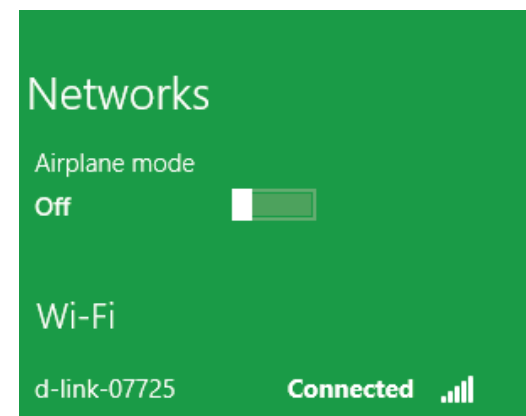
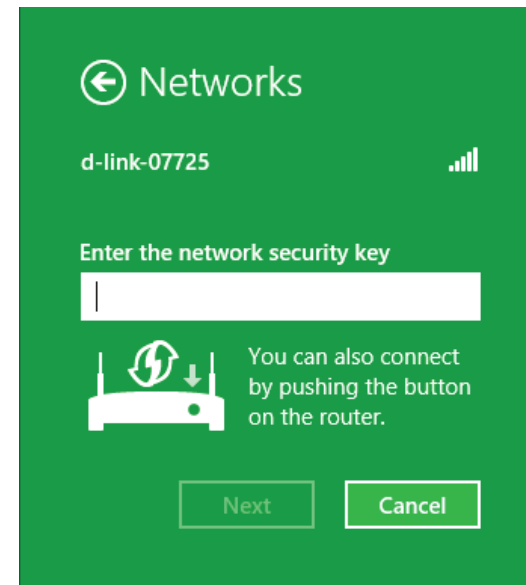
Clicking on this icon will display a list of wireless networks that are within connecting proximity of your computer. Select the desired network by clicking on the network name.



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

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

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

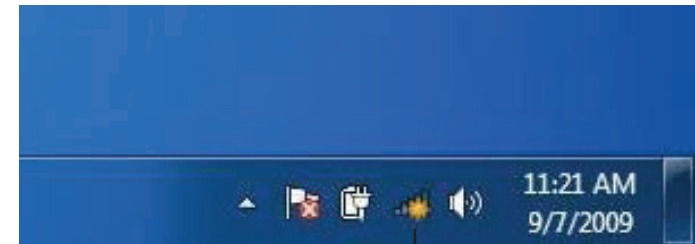


Windows® 7

WPA/WPA2

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

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



Wireless Icon

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

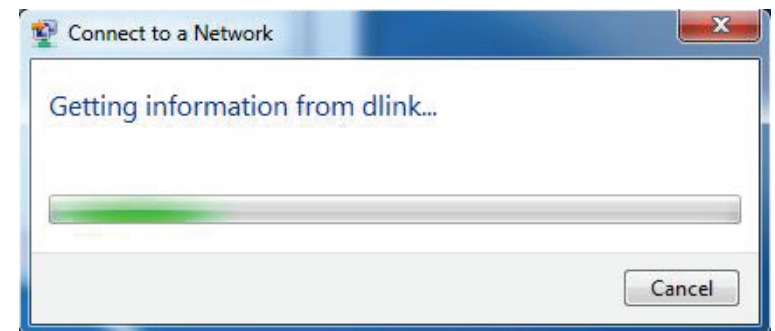


3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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

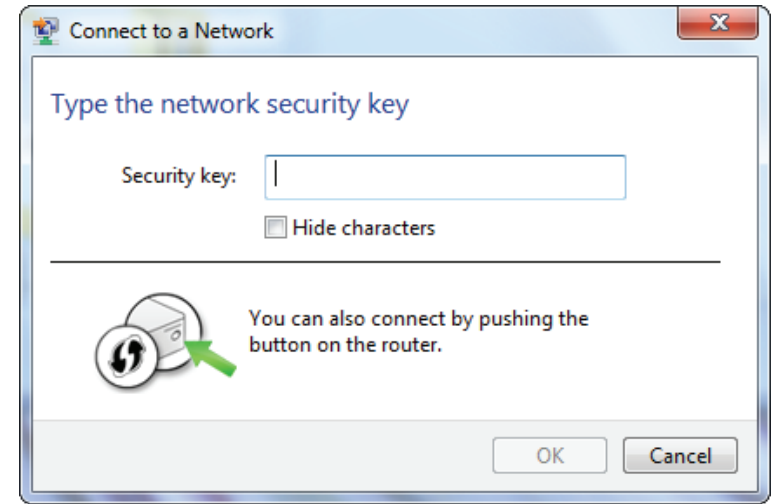


4. The following window appears while your computer tries to connect to the router.



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

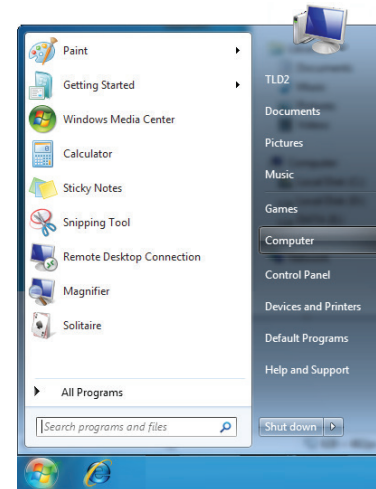
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as the one on the wireless router.



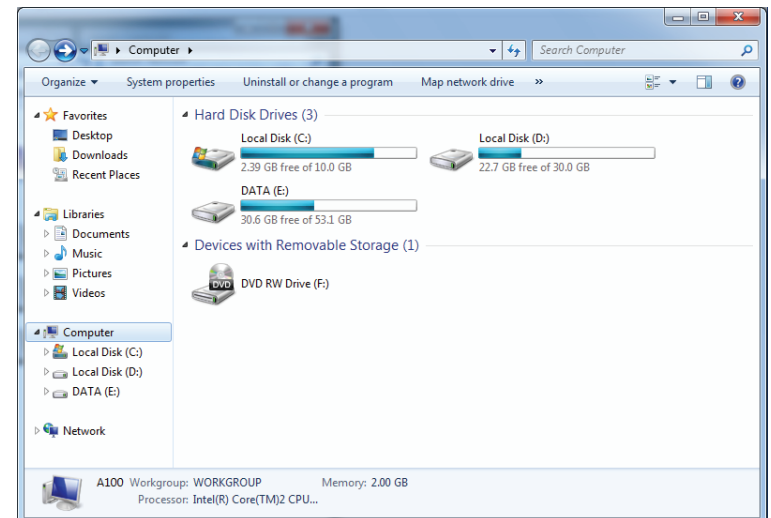
WPS

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

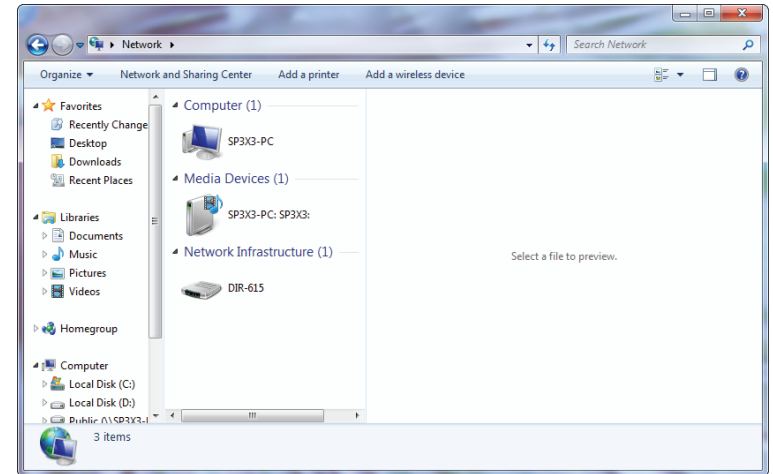
1. Click the **Start** button and select **Computer** from the Start menu.



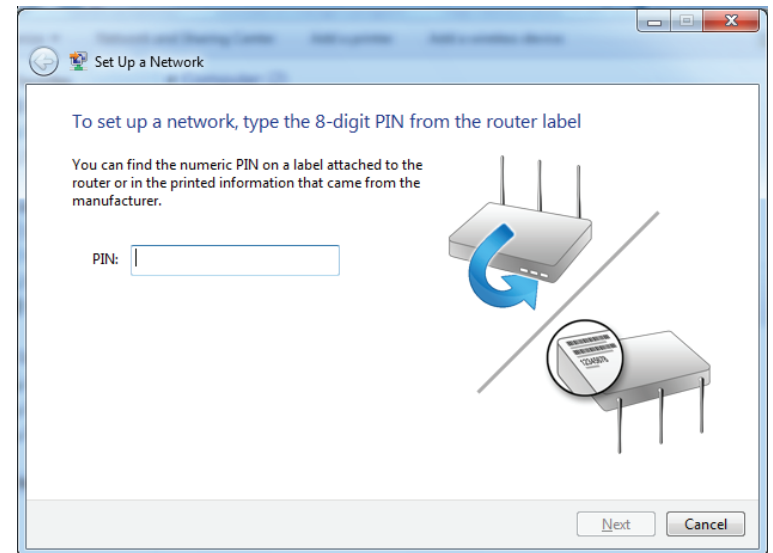
2. Click **Network** on the left side.



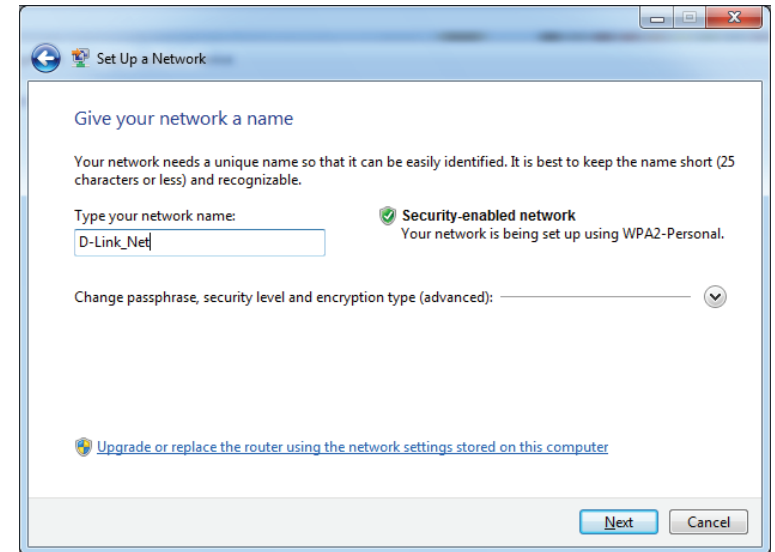
3. Double-click the DWR-922.



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

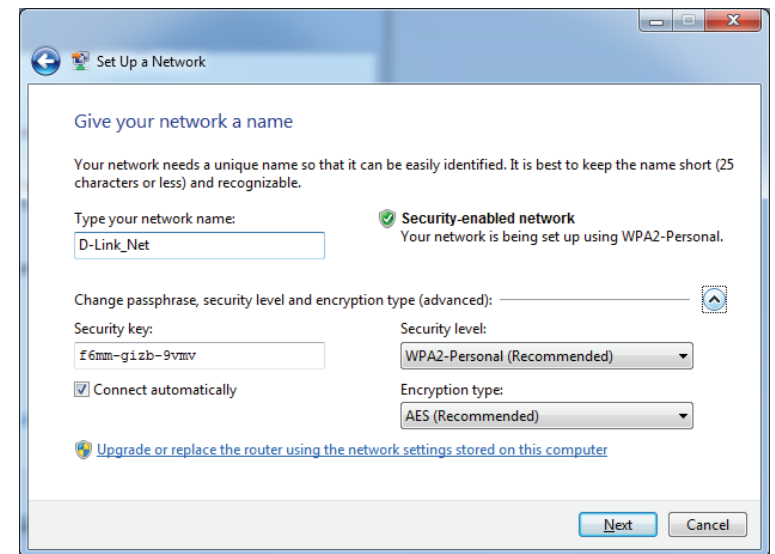


5. Type a name to identify the network.



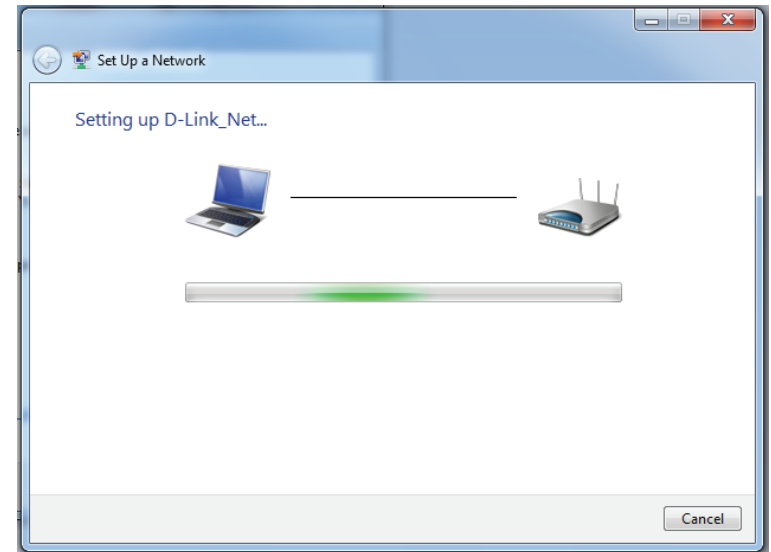
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



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

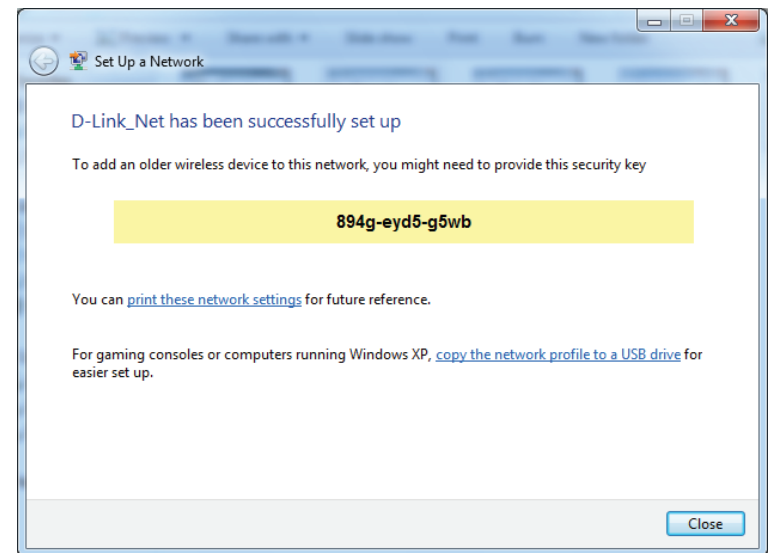
Wait for the configuration to complete.



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

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

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



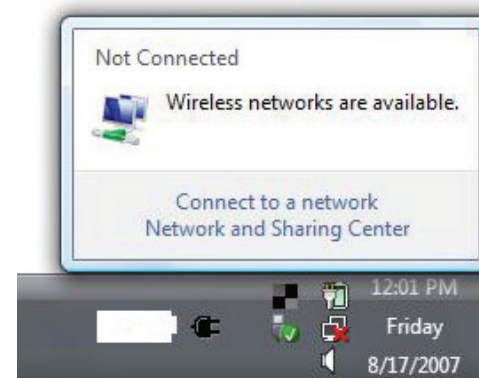
Windows Vista®

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

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

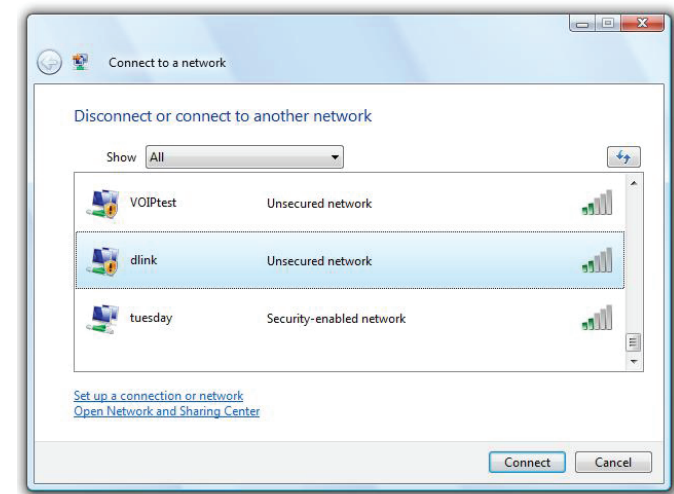
or

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



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

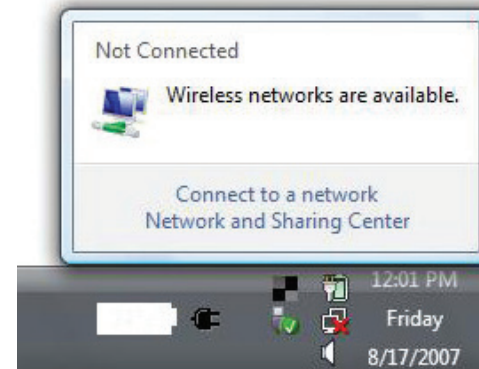
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



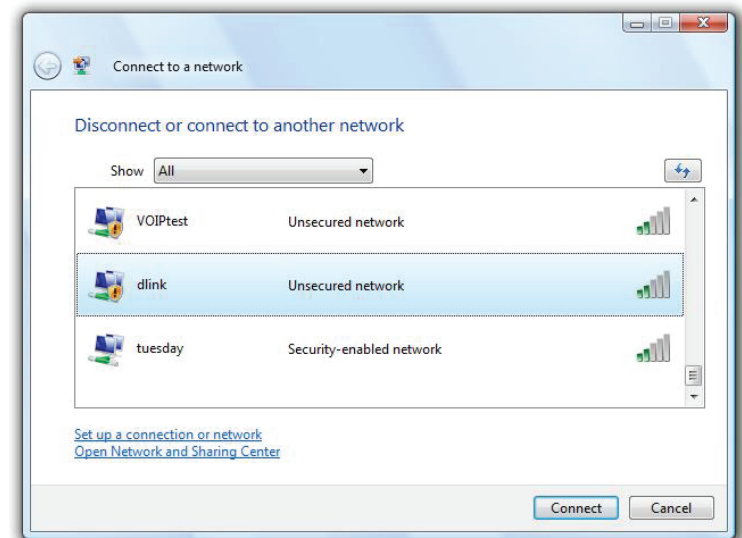
WPA/WPA2

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

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



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



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

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



Windows® XP

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

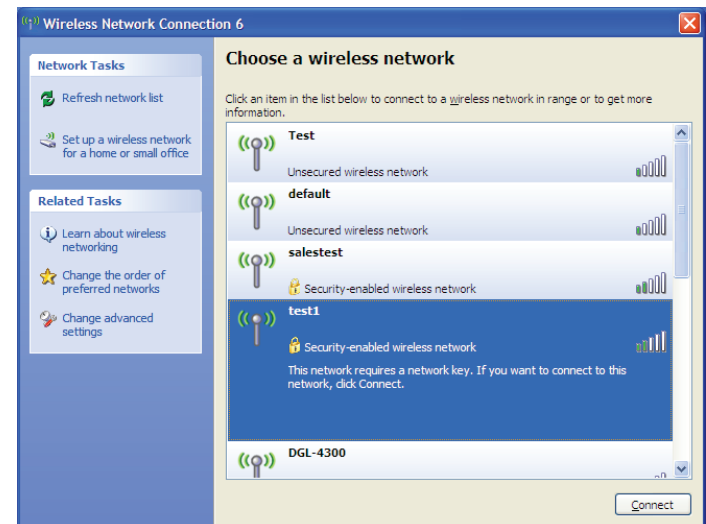
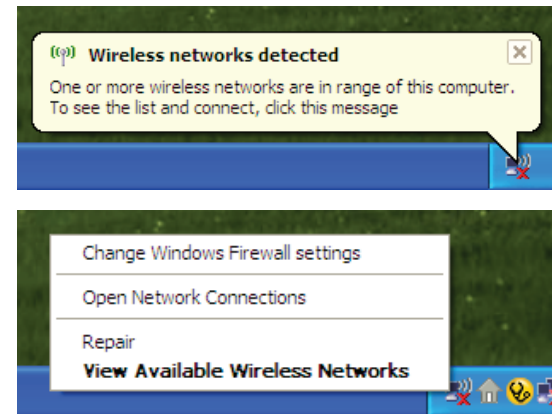
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

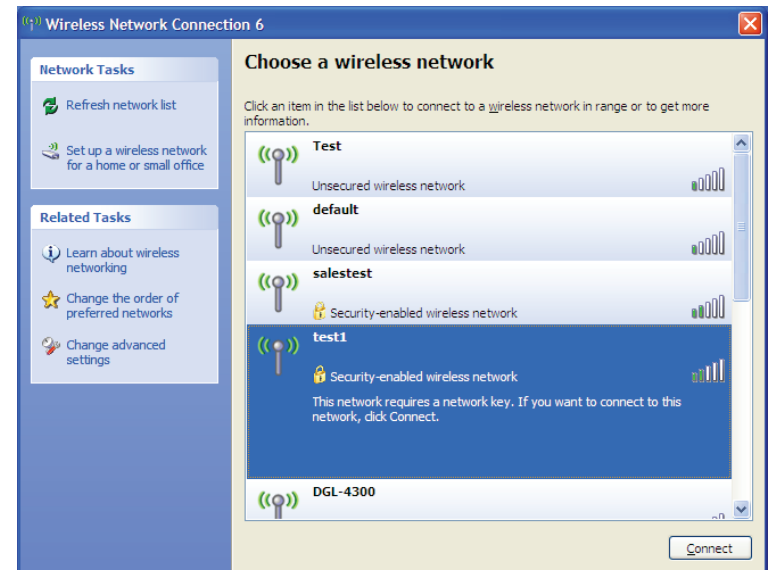
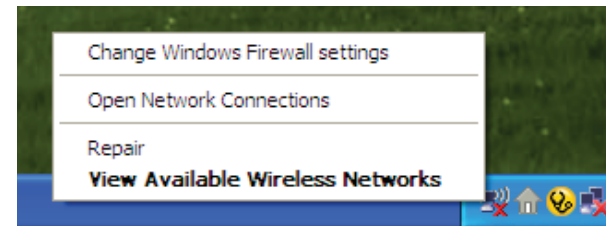
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

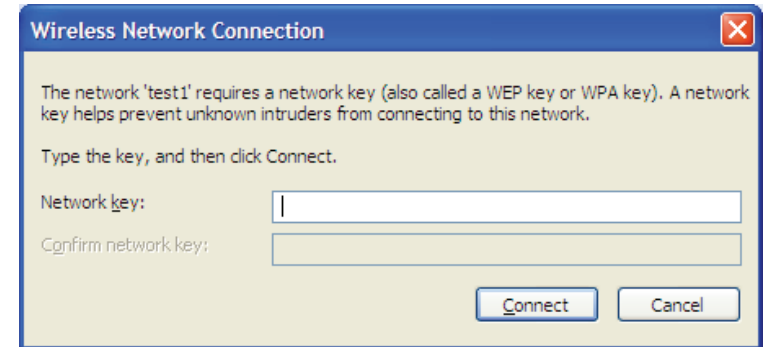
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.
2. Highlight the Wi-Fi network (SSID) you would like to connect to and click **Connect**.



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

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



Troubleshooting

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

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Microsoft Internet Explorer® 7 or higher
 - Mozilla Firefox 3.5 or higher
 - Google™ Chrome 8 or higher
 - Apple Safari 4 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable, or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

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

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

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

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

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

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

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

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

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

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

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms
C:\>
```

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

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

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

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

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home Uses/Benefits

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

Small Office and Home Office Uses/Benefits

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

Where is wireless used?

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

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

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

Tips

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

Centralize your router or access point

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

Eliminate interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad hoc** – Directly connecting to another computer for peer-to-peer communication using wireless network adapters on each computer, such as two or more DWR-922 wireless network CardBus adapters.

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

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

Networking Basics

Check your IP address

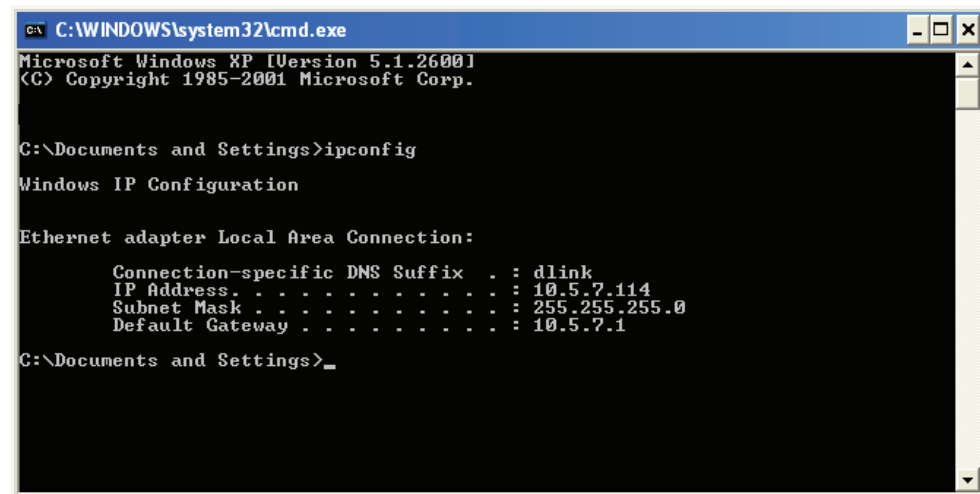
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>
```

Statically Assign an IP address

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

Step 1

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

Step 2

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

Step 3

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

Step 4

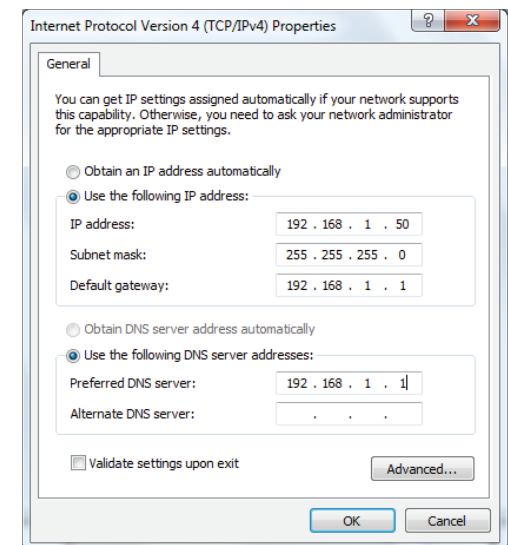
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

Step 5

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



Wireless Security

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

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

What is WPA?

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

The 2 major improvements over WEP:

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

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

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

Technical Specifications

LTE Band¹

- Category 3: Band 2/4/5/13/17/25

CDMA Mode 1xRTT and EV-DO Rev A.

- BC0/1/10 (800/1900 MHz)

Pentaband UMTS/HSDPA/HSUPA/HSPA+/DC-HSPA+ Band¹

- 850/900/1700/1900/2100 MHz

GSM Quad-band¹

- 850 / 900 / 1800 / 1900 MHz

Data Rates²

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

Standards

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

Wireless Security

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

Firewall

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

VPN

- L2TP/PPTP/IPSEC/VPN Pass-through

Antenna

- Two detachable 3G/4G antennas

Ports

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

SIM/UICC Slot

- Standard Mini-SIM/UICC slot

LED Status Indicators

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

Dimensions

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

Operating Temperature

- 0 to 40 °C (32 to 104 °F)

Operating Humidity

- 10% to 90% (Non-condensing)

Certifications

- FCC
- RoHS

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

Federal Communication Commission Interference Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

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

FCC RF Exposure Compliance

This equipment complies with radio frequency (RF) exposure limits adopted by the Federal Communications Commission for an uncontrolled environment. This equipment should operate with minimum distance 20 cm between the radiator & your body.

The antenna gain, including cable loss, must not exceed 6.5 dBi at 800 MHz and/or 850 MHz, 3.0 dBi at 1900 MHz, 9.0 dBi at 700 MHz and 6 dBi at 1700 MHz.