

# Wi-Fi Settings

## Wi-Fi Status

This page displays your current Wi-Fi status and Wi-Fi settings.

### General Information

**Wi-Fi WPS** Displays whether Wi-Fi Protected Setup (WPS) is enabled and the configuration method used.

**Wi-Fi 2.4 GHz** Displays whether Wi-Fi is enabled.

**Current Wi-Fi Clients** Displays the number of clients connected to your Wi-Fi network.

### Wi-Fi Status

**SSID Name** Displays the name of your Wi-Fi network.

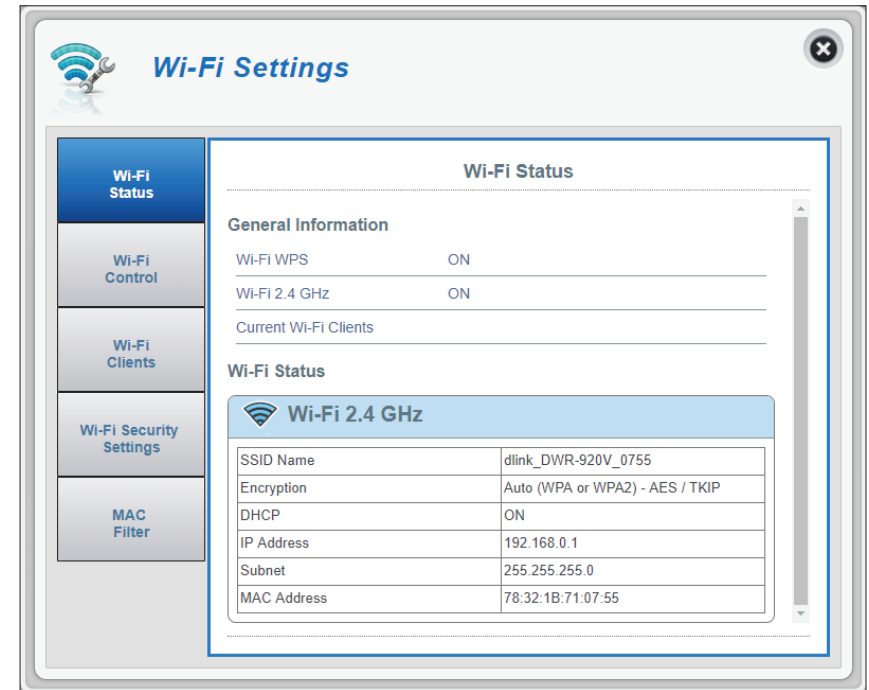
**Encryption** Displays your current Wi-Fi security encryption mode.

**DHCP** Displays whether DHCP server is enabled.

**IP Address** Your router's IP address.

**Subnet** Your router's subnet mask.

**MAC Address** Your router's MAC address.



# Wi-Fi Control

## Wi-Fi 2.4 GHz

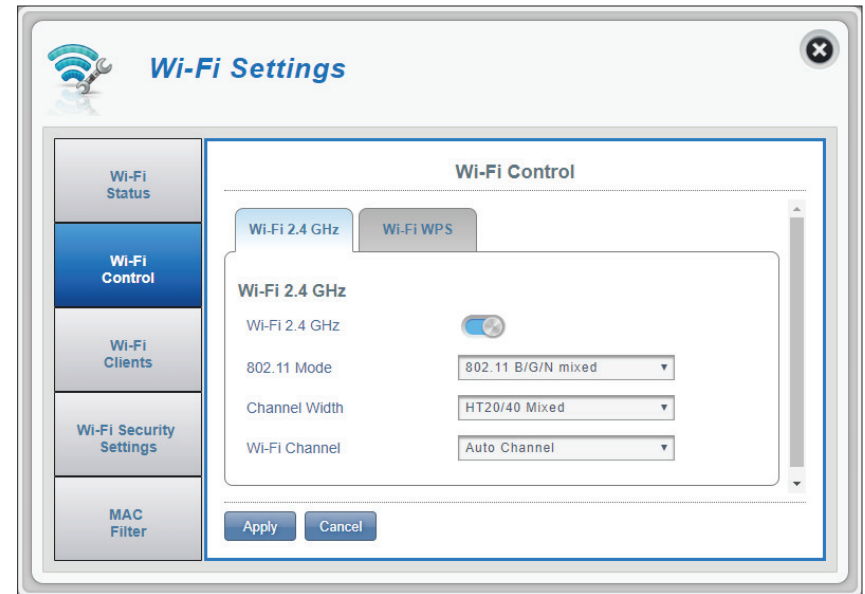
**Wi-Fi 2.4 GHz** Toggle the switch to enable/disable Wi-Fi functionality on your router.

**802.11 Mode** The type of Wi-Fi connection currently being accepted by the router. Select **802.11 N Only for best performance** or **802.11 B/G/N Mixed** for broadest compatibility. **B/G/N Mixed** is the default setting.

**Channel Width** The current channel width being used by your router. A wider 40 Mhz channel may increase performance but could cause interference with other Wi-Fi devices. This router will automatically reduce to 20 Mhz if interference is detected. Choose **HT20** if you have devices that do not support 40 Mhz channels.

**Wi-Fi Channel** Choose the clearest channel to help optimize the performance and coverage of your wireless network. By default the channel is set to **Auto Channel**. This can be changed to fit the channel setting for an existing wireless network or to customize your wireless network. Note that not all channels are available in all regions. If you cannot see your SSID from your device, try manually setting a low-numbered channel.

Click **Apply** to save changes.



## Wi-Fi WPS

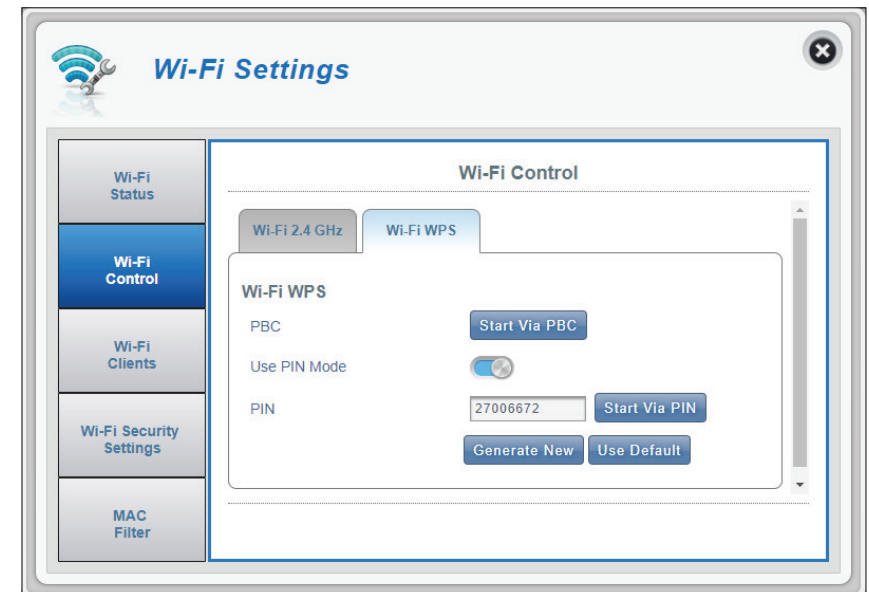
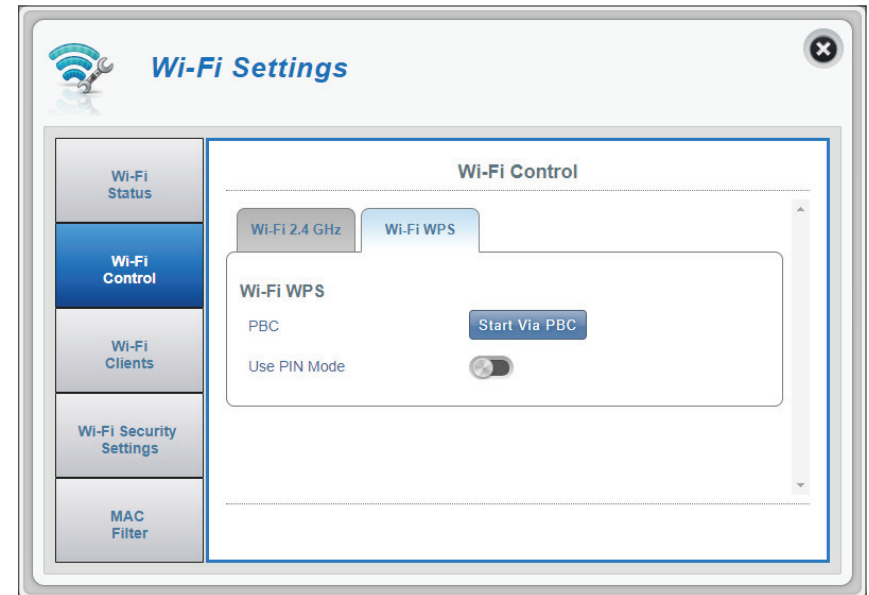
**PBC** Push Button Configuration (PBC) enables you to easily connect your devices to the DWR-920V by pushing a PBC button on both devices. Press your device's PBC button and then click **Start Via PBC**, to begin the WPS process.

**Use PIN Mode** Move the toggle to enable PIN protection for use with the WPS feature.

**Note:** WPS PIN Mode is disabled by default. This mode is less secure and is not recommended. It is retained in this product for compatibility purposes only.

**PIN** The PIN is a unique number that can be used to configure your router. Click **Generate New** to generate a new random PIN, or select **Use Default** to restore the factory PIN. Note that if the WPS PIN feature is enabled, using a new PIN is strongly recommended.

Click **Apply** to save changes.



# Wi-Fi Clients

This page shows your current client list and allows you to filter clients by host name, IP address and MAC address. This filtering option enables you to allow or deny access to specific wireless clients.

## Wi-Fi 2.4 GHz Clients List

**Host Name** A unique name for each wireless client that is connected to your router.

**IP Address** The IP address of the wireless client that is connected to your router.

**MAC Address** The hardware address of the client's wireless adapter.

**Access** Toggle this switch to allow or deny access to specific clients.

**Note:** If you deny access to a Wi-Fi client, you will see their MAC address in the **MAC Filter on page 41**. If required, you can re-allow access to the client there.

Click **Apply** to save changes.



# Wi-Fi Security Settings

In this page you can view your Wi-Fi security settings, here you can alter things like your SSID name, SSID visibility and access Wi-Fi security features.

## Wi-Fi 2.4 GHz SSID

**SSID For Wi-Fi 2.4 GHz** Displays the name of your Wi-Fi network. Click in the box to edit.

**SSID Visibility** Click the toggle to change your SSID visibility to clients.

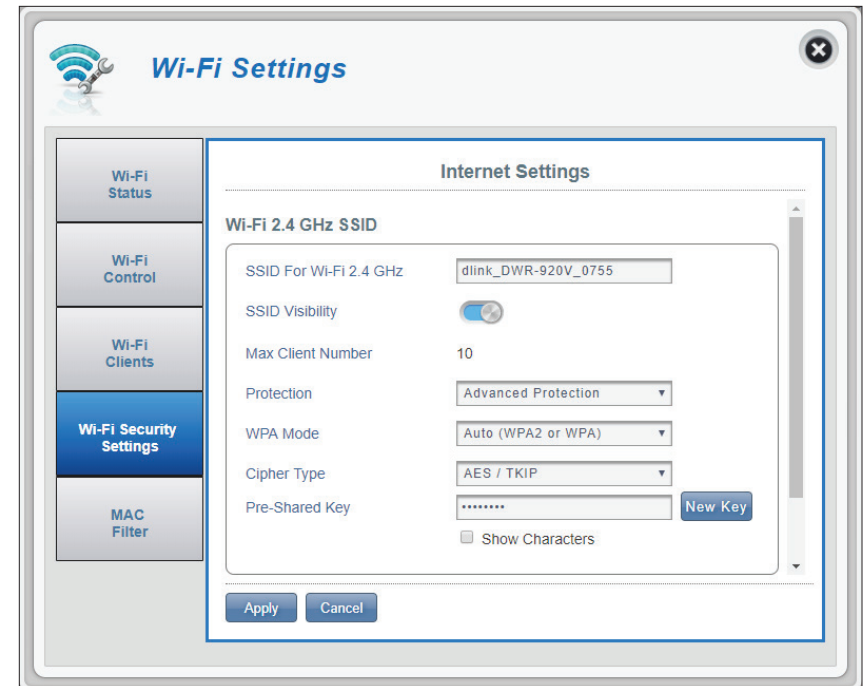
**Max Client Number** The maximum number of clients allowed on your network.

**Protection** By default **Advanced Protection** is selected. You may also select **Basic Protection** or **No Protection**.

### If you selected Advanced Protection:

**WPA Mode** **Auto (WPA or WPA2)** - The router will automatically determine the version of WPA to be used based on the client that is connecting to it.

**WPA2** - Clients will only be able to associate with the router using the WPA2 standard. Clients which do not support WPA2 will not be able to associate with the router.



**Cipher Type AES** - A newer cipher used by the WPA2 standard.

**Note:** Use of this cipher type is required in order to achieve 802.11n speeds.

**AES/TKIP** - TKIP is an encryption method commonly used by older devices. Select this option for greater compatibility with old and new devices.

**Pre-Shared Key** The pre-shared key is the password which clients require in order to connect to your network. Enter a password of between 8 and 63 characters in length.

Click **Apply** to save changes.

### If you selected Basic Protection:

**Authentication Type: Shared** - The encryption key used authenticate wireless client and encrypt data.

**WEP Passphrase:** Enter your passphrase to be used when connecting to the router. Once you have entered a passphrase, click **Generate** to create keys automatically, or enter them manually below.

**Key 1-4:** You can predetermine up to 4 WEP keys. Select the WEP key you wish to use by clicking on the radial buttons next to the keys. Select whether you wish to use **64 bit** or **128 bit** characters in your key using the slider menu. Enter the desired key in the field provided.

Click **Apply** to save the current settings.

**Wi-Fi Settings**

**Internet Settings**

**Wi-Fi 2.4 GHz SSID**

SSID For Wi-Fi 2.4 GHz:

SSID Visibility: ☒

Max Client Number: 10

Protection: Basic Protection

Authentication Type: Auto

WEP Passphrase:

Default Key	Key Type	Key No	Generated Keys
<input checked="" type="radio"/>	128	Key 1	12345678901234567890123456
<input type="radio"/>	64	Key 2	
<input type="radio"/>	128	Key 3	
<input type="radio"/>	128	Key 4	

# MAC Filter

This page allows you to set MAC filters (Media Access Control) which allow or deny LAN (Local Area Network) computers from accessing the network. A MAC address is a unique ID assigned by the manufacturer for devices that connect to a network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the router.

## MAC Filter Settings

**MAC Filter** Toggle this switch to enable/disable the MAC filter.

**MAC Filter For Black List** Here is a list of clients' MAC addresses that have been denied access to your network.

**ID** ID number given to client blacklisted clients by your router.

**Delete** Check this box to delete clients from the black list.

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

**Add New** Select the **Add New** button and manually enter the MAC address of the client that you wish to deny access to your network.

**Note:** You can view the current list of clients connected to your network and their MAC addresses in **Wi-Fi Clients** on page 38.

Click **Apply** to save changes.



# Applications

## Short Messages

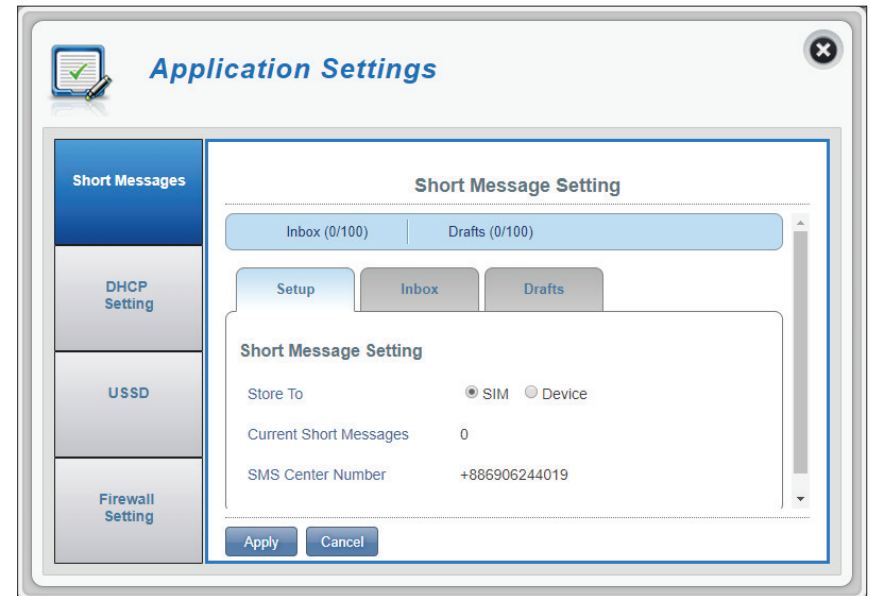
On the Short Messages Settings page you can organize, send and receive Short Message Service (SMS) messages by selecting between a **Setup**, **Inbox** and **Drafts** tab. These messages can either be saved to the router's internal memory or on the SIM/UICC card itself.

### Setup

**Store To** Choose between the location to store contact numbers, either on your SIM/UICC card or the DWR-920V device.

**Current Short Messages** The current number of messages received.

**SMS Center Number** Your SIM/UICC card's contact number.  
Click **Apply** to save changes.





## Inbox

**ID** A chronological number given to each message you receive.

**Delete** Check this box to select and delete a message in your inbox.

**From** The SMS sender's number.

**Time** The time the message was received.

**Content** The SMS message's content.

**Add New** Click **Add New** to send a new message.

Click **Apply** to save changes.

### If you clicked Add New:

**Send to** Enter the phone number of the intended recipient here.

**Content** Type your message content here.

Click **Send** to send your message. Click **Save as Draft** to save the message as a draft and send it later.

The screenshot shows the 'Application Settings' window with the 'Short Message Setting' tab selected. The 'Inbox' sub-tab is active, displaying a table of messages. The table has columns for ID, Delete, From, Time, and Content. A search bar and a 'Records: Display' dropdown (set to 10) are at the top. A '+ Add New' button is below the table. 'Apply' and 'Cancel' buttons are at the bottom.

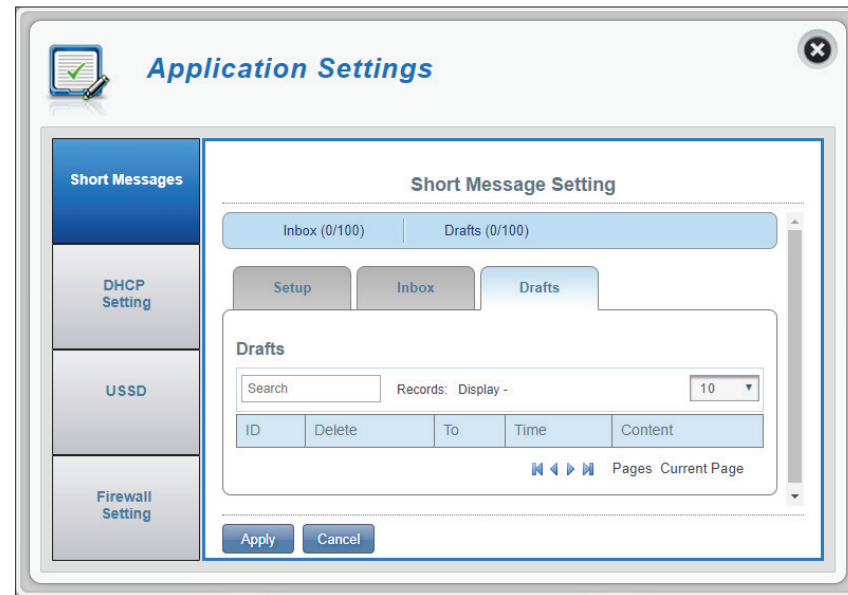
ID	Delete	From	Time	Content
[Empty table body]				

The screenshot shows the 'Application Settings' window with the 'Short Message Setting' tab selected. The 'Send SMS' sub-tab is active, displaying a form to compose a message. It includes a 'Send to' text field and a 'Content' text area. Below the text area, there is a character count: 'Input 0 characters. For pure english message, the max number of characters is 1000. For not pure english message, the max number of characters is 500.' 'Send', 'Save as Draft', and 'Cancel' buttons are at the bottom.

## Drafts

- ID** A chronological number given to each message you save to draft.
- Delete** Check this box to select and delete a message in your drafts folder.
- To** The SMS recipient's number.
- Time** The time the message was last edited.
- Content** The SMS message's content.

Click **Apply** to save changes.



# DHCP Setting

Here you can disable or enable your router's DHCP Service, configure the IP address for the DWR-920V, and set the range of IP addresses assigned by the DHCP server.

## DHCP Service

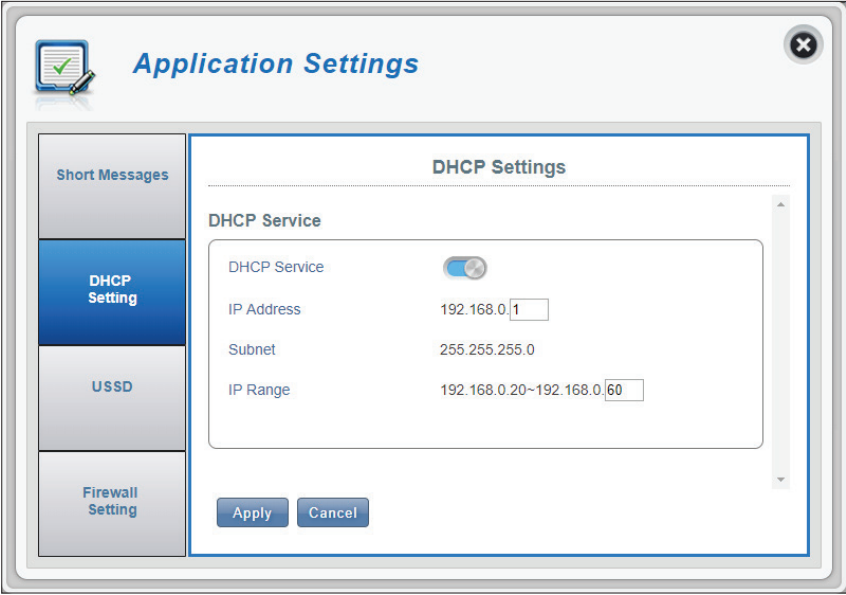
**DHCP Service** Enable or disable the DHCP Service.

**IP Address** Click on the last digit to alter your router's current IP address.

**Subnet** The subnet mask that your router is using.

**IP Range** Click on the last digits to alter the range of IP addresses assigned by the DHCP server.

Click **Apply** to save changes.



The screenshot shows the 'Application Settings' window with a sidebar containing 'Short Messages', 'DHCP Setting' (selected), 'USSD', and 'Firewall Setting'. The main area is titled 'DHCP Settings' and contains the following fields:

DHCP Service	
DHCP Service	<input checked="" type="checkbox"/>
IP Address	192.168.0.1
Subnet	255.255.255.0
IP Range	192.168.0.20~192.168.0.60

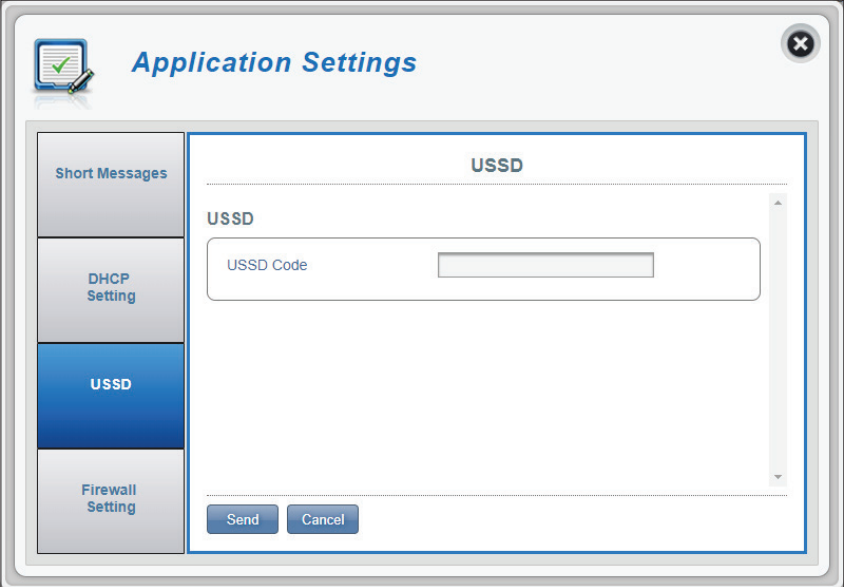
At the bottom of the main area are 'Apply' and 'Cancel' buttons.

# USSD

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

## USSD

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



The screenshot shows a web-based configuration interface titled "Application Settings". On the left is a vertical sidebar with four menu items: "Short Messages", "DHCP Setting", "USSD" (which is highlighted in blue), and "Firewall Setting". The main content area is titled "USSD" and contains a single text input field labeled "USSD Code". Below the input field are two buttons: "Send" and "Cancel". The window has a standard title bar with a close button in the top right corner.

# Firewall Setting

A firewall helps protect your network from external cyber attack and intrusions. This page allows you to alter your router's firewall settings.

## Firewall Settings

**Firewall Enable** Clicking this toggle activates the IP Filter. For more information see **IP Filter** on page 49.

**DMZ Settings** Toggling the DMZ (Demilitarized Zone) will expose a chosen computer to the outside world by completely disabling all firewalls and routing all inbound traffic to the target IP.

**Note:** *This feature is only recommended for advanced users. Enabling this option will potentially expose your computer to attacks over the Internet.*

**PPTP Pass Through** Allows clients to connect to their corporate network or VPN using the PPTP protocol.

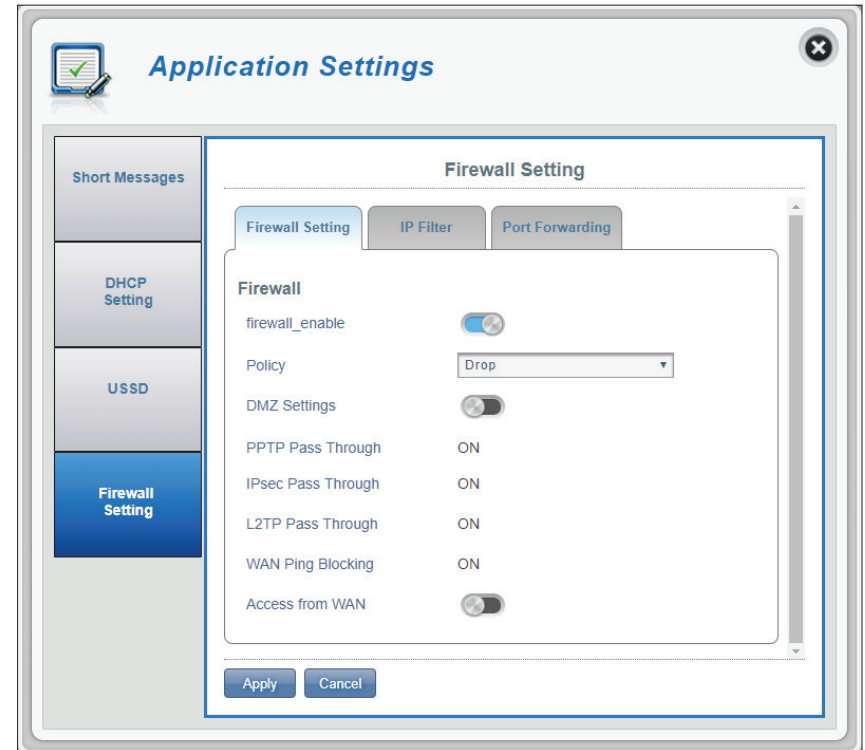
**IPsec Pass Through** Allows clients to connect to their corporate network or VPN using the IPsec protocol.

**L2TP Pass Through** Allows clients to connect to their corporate network or VPN using the L2TP protocol.

**WAN Ping Blocking** When enabled the DWR-920V will not respond to pings from WAN.

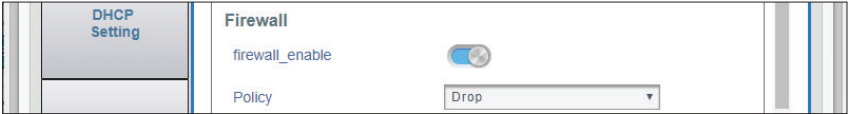
**Access from WAN** Clicking this toggle allows access from WAN. This setting may open your router to external security threats and is not recommended for most users.

Click **Apply** to save changes.



If you selected Firewall Enable:

**Policy** Choose **Drop** to block all IP addresses defined in the **IP Filter** section or **Accept** to only allow those addresses access to your network.



If you selected DMZ Settings:

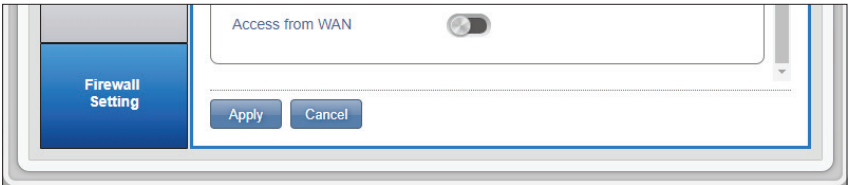
**DMZ IP Address** Enter the IP address of the DMZ.



If you selected Access from WAN:

**Access from WAN** Allows the configuration interface to be access over WAN. This setting is not recommended.

Click **Apply** to save changes.



## IP Filter

The DWR-920V can filter certain IP addresses and ports. IP filtering allows you to direct specific traffic to a specified local client based on source IP address or protocol. The DWR-920V supports a maximum of 50 filters.

**ID** ID number given to new IP filters.

**Delete** Click here to select the filters you wish to delete.

**Protocol** The protocol for the IP filter rule.

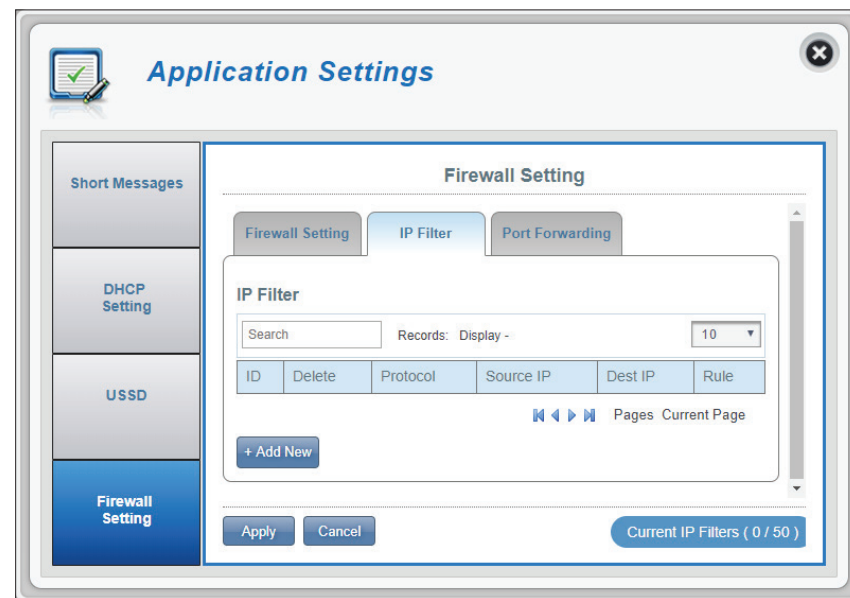
**Source IP** The source IP address to be filtered.

**Dest IP** The destination IP address to be filtered.

**Rule** The rule that the filter will follow; either to drop or to accept.

Click **Add New** to add a new rule.

Click **Apply** to save changes.



If you selected **Add New IP Filter**:

## Add IP Filter

**Protocol** Select the protocol for ports that you want to allow or deny access to. Choose between **TCP**, **UDP** or **ICMP** or all of the above.

**Source IP** Enter the source IP address that you wish to filter.

**Subnet** Enter the subnet mask of the source IP address you wish to filter.

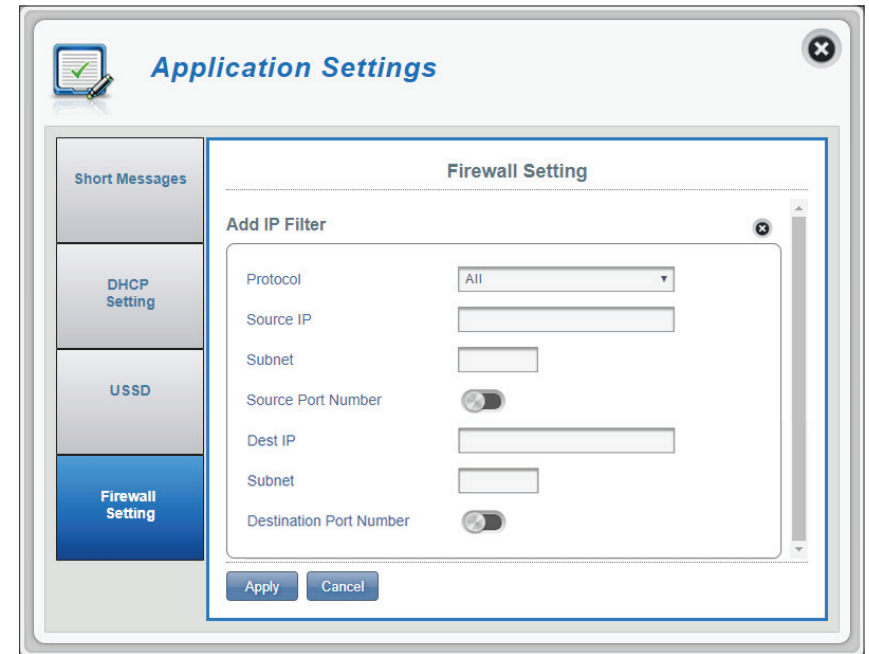
**Source Port Number** Enable this feature if you wish enter a single port or a range of ports to be filtered based on origin. Disabling this feature will cause all incoming connection fitting other criteria to be filtered.

**Source Port Range** This option will appear if Source Port Number is toggled. Enter an incoming port range to which your filter will apply.

**Dest IP** Type in the destination IP address. Leave this blank to apply your filter to incoming connections to any destination IP

**Destination Port Number** Click the toggle if you wish enter a single port or a range of ports to be filtered. Separate port numbers with a comma.

**Destination Port Range** Enter a destination port range to which your filter will apply.





## Port Forwarding

This page will allow you to open a single port or a range of ports to specific IP addresses. The DWR-920V supports a maximum of 50 filters.

**ID** ID number given to the new rule.

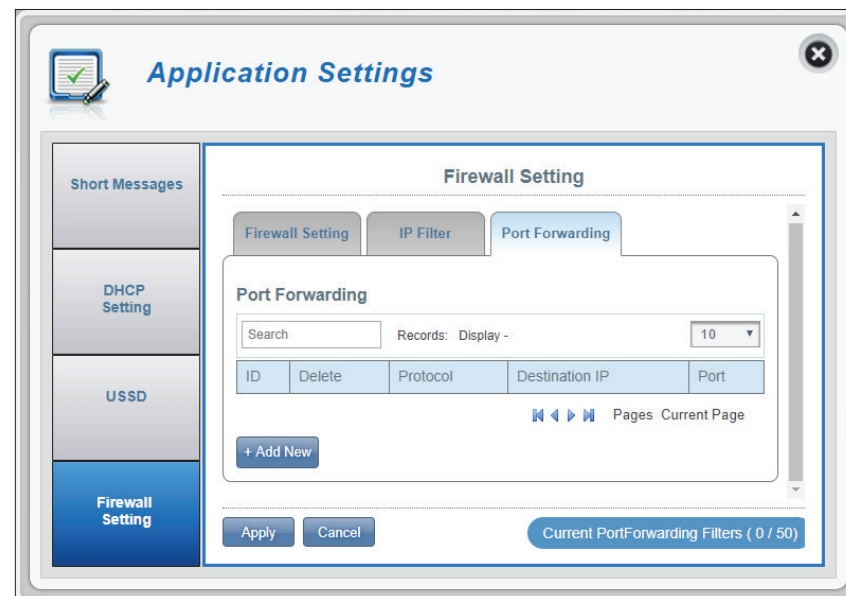
**Delete** Click here to select the rules you wish to delete.

**Protocol** The selected protocol for the IP filter rule.

**Destination IP** The IP address that will be port forwarded to.

**Port** The port number that incoming traffic will be forwarded from.

Click **Add New** to add a new port.



## If you selected Add Port Forwarding

### Add Port Forwarding

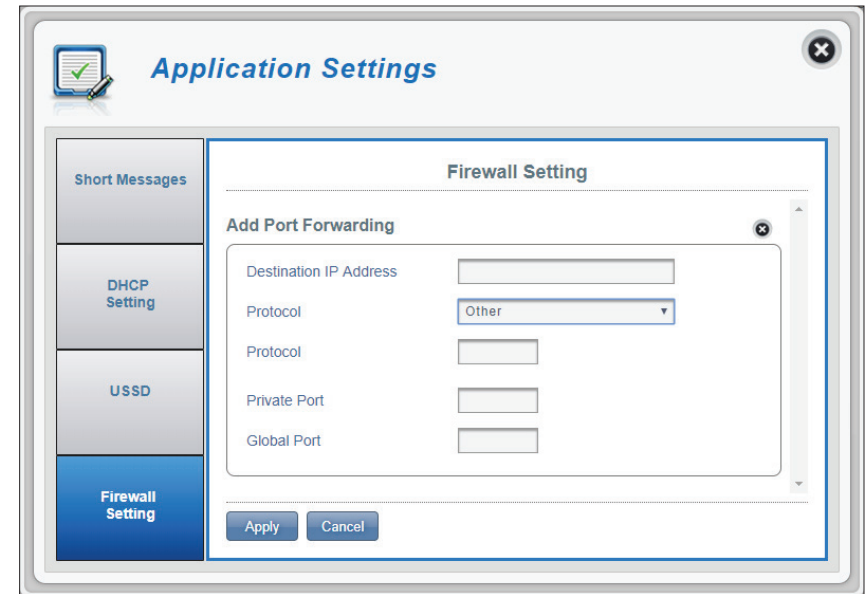
**Destination IP Address** The IP address you want to allow port forwarding on.

**Protocol** Select the protocol for ports that you want to allow or deny access to. Choose between **TCP, UDP** or **Other**. If you select **Other** you will be asked to specify the protocol in addition to the ports.

**Private Port** Select the port number or numbers for your service on your local network. Enter a single port or a range. If entering multiple ports, separate port numbers with a comma.

**Global Port** Select the port number or numbers for your service to be exposed to the Internet. Enter a single port or a range. If entering multiple ports, separate port numbers with a comma.

Click **Apply** to save your changes.



# System System Information

## About DWR-920V

**FW Version** The current firmware version of the DWR-920V.

**Hardware Version** The current firmware version of the DWR-920V.

**IMEI** International Mobile Equipment Identity is a unique number assigned to every mobile device.

**SIM/UICC IMSI** The SIM/USIM/UICC card has a unique number called an International Mobile Subscriber Identity (IMSI). This is used to identify and authenticate users on cellular devices.

**Model Name** The model name of your D-Link router.

**System Uptime** The length of time since last restart.



**Note:** The FW version number and Modem Version number displayed on the image above may differ from the model you have purchased due to firmware updates or regional variation.

# Admin Settings

## Account

This tab allows you to customize your own username and password as well as adjust the UI's automatic logout timer.

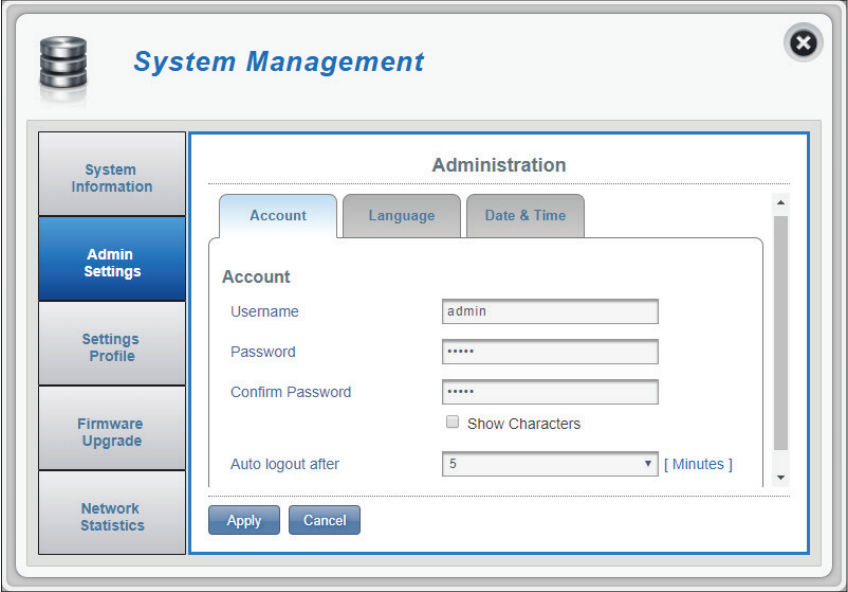
**Username** Adjust your login username here.

**Password** Enter your new password here.

**Confirm Password** Confirm the new password here.

**Auto logout after** Click on the drop-down arrow to select the length of time before being automatically logged out of the interface.

Click **Apply** to save your changes.



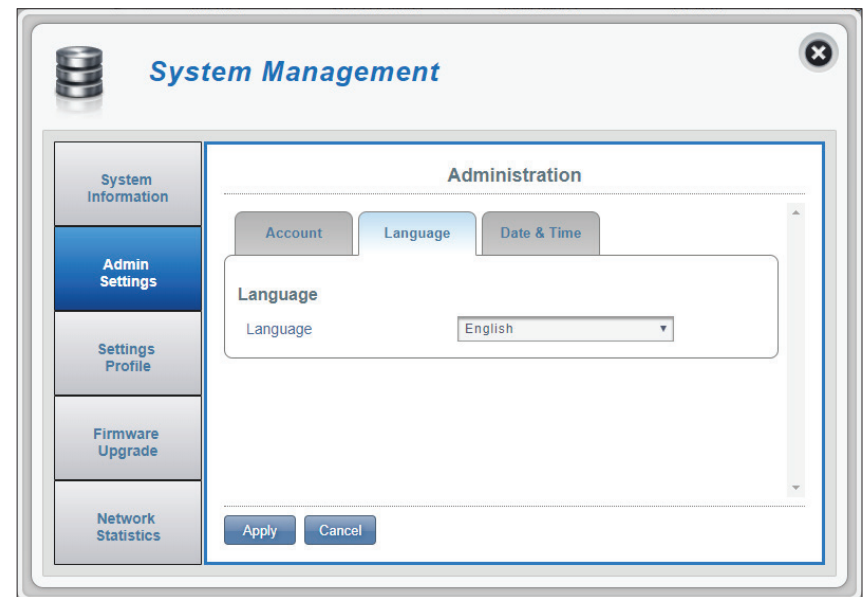
The screenshot shows a web-based configuration interface titled "System Management". On the left is a sidebar with navigation links: "System Information", "Admin Settings" (highlighted), "Settings Profile", "Firmware Upgrade", and "Network Statistics". The main content area is titled "Administration" and contains three tabs: "Account" (selected), "Language", and "Date & Time". Under the "Account" tab, there are four input fields: "Username" (containing "admin"), "Password" (masked with "\*\*\*\*\*"), "Confirm Password" (masked with "\*\*\*\*\*"), and "Auto logout after" (a dropdown menu showing "5" and "[ Minutes ]"). There is also a checkbox labeled "Show Characters" which is currently unchecked. At the bottom of the form are "Apply" and "Cancel" buttons.

## Language

This tab allows you to change the default language of the router's web interface.

**Language** Select your desired language here.

Click **Apply** to save your changes.



## Date & Time

In this section, you can adjust the date, time, and network time synchronization settings of your router.

**SNTP** Click the toggle to **Enable** or **Disable** automatic time synchronization with a Simple Network Time Protocol (SNTP) server.

**Primary, Secondary and Tertiary SNTP Server** Enter an SNTP server address which will be used to synchronize the router's time and date.

**Time Zone** Select your current Coordinated Universal Time zone (UTC).

**Synchronization Cycle** You can specify in hours how frequently the DWR-920V will update the time from an SNTP server.

**Daylight Saving** Select to **Enable** if your region uses Daylight Saving Time. If you have selected **Enable**, enter the details of your region's Daylight Saving scheme below.

Click **Apply** to save your changes.

The screenshot shows the 'System Management' web interface. On the left is a sidebar with navigation links: System Information, Admin Settings (highlighted), Settings Profile, Firmware Upgrade, and Network Statistics. The main content area is titled 'Administration' and contains three tabs: Account, Language, and Date & Time (selected). The 'Date & Time' tab displays the following settings:

- SNTP**: A toggle switch is turned on.
- Primary SNTP Server**: 1.my.pool.ntp.org
- Secondary SNTP Server**: 2.my.pool.ntp.org
- Tertiary SNTP Server**: 3.my.pool.ntp.org
- Time Zone**: UTC+8 (selected from a dropdown)
- Synchronization Cycle**: 1 [Hours]
- Selected Date and Time**: 2018-09-25 11:38 AM
- Daylight Saving**: A toggle switch is turned off.
- Start Date**: First Sunday of April at 2 o'clock
- End Date**: Last Sunday of October at 2 o'clock

At the bottom of the configuration panel are 'Apply' and 'Cancel' buttons.

**If you disabled automatic synchronization with an SNTP server.**

**Time Zone** Select your current Coordinated Universal Time zone (UTC).

**Date & Time** Adjust the dials with your mouse to set the date and time.

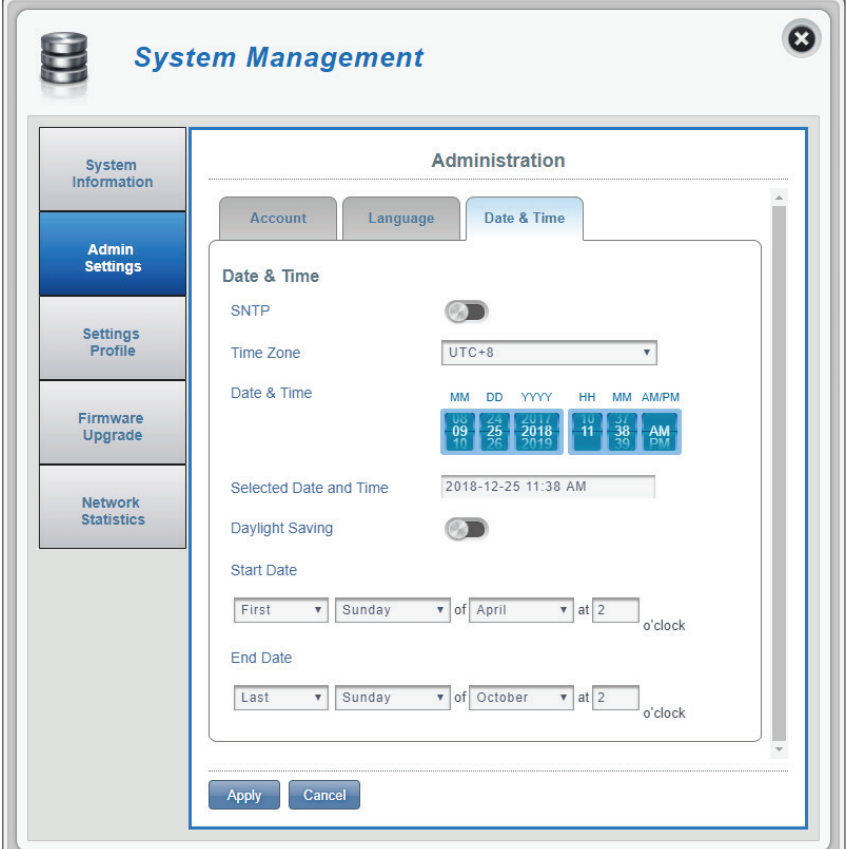
**Selected Date and Time** Displays your new adjusted time.

**Daylight Saving** Toggle if your location observes daylight savings.

**Start Date** Enter in the details of when daylight savings begins in your location.

**End Date** Enter in the details of when daylight savings ends in your location.

Click **Apply** to save your changes.



The screenshot shows the 'System Management' web interface. On the left is a sidebar with navigation links: System Information, Admin Settings (highlighted), Settings Profile, Firmware Upgrade, and Network Statistics. The main content area is titled 'Administration' and contains three tabs: Account, Language, and Date & Time (selected). Under the 'Date & Time' tab, there is a 'Date & Time' section with a toggle for 'SNTP' (disabled), a 'Time Zone' dropdown set to 'UTC+8', and a 'Date & Time' dial showing '09:10' on '25/10/2018' at '11:38 AM'. Below this is a 'Selected Date and Time' field showing '2018-12-25 11:38 AM'. A 'Daylight Saving' toggle is also present. The 'Start Date' section shows 'First Sunday of April at 2 o'clock', and the 'End Date' section shows 'Last Sunday of October at 2 o'clock'. At the bottom are 'Apply' and 'Cancel' buttons.

# Settings Profile

## Import Profiles

In the **Import Profiles** tab, you can import previously saved settings for the router.

**Select** Browse your computer for previously exported settings.

Click **Apply Import** to proceed.





## Export Profiles

In the **Export Profiles** tab you can export your current configuration to a computer.

**To Get Current Profile** Click the **Click Me** button to download the current settings of your DWR-920V.

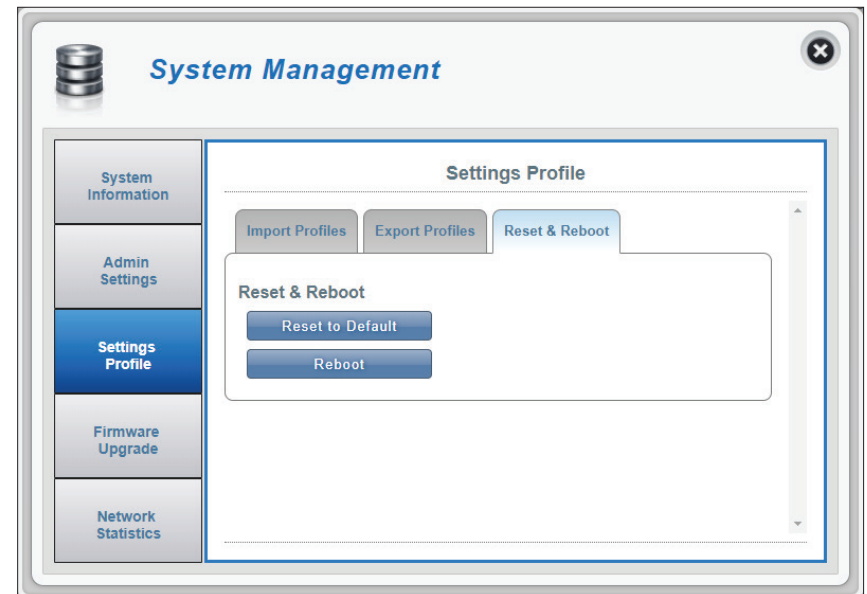


## Reset and Reboot

In the **Reset and Reboot** tab you can reboot your router or reset it to factory default settings. You can also manually reset your router by removing the battery cover and using an implement such as a straightened paperclip to press and hold the reset button on the router for 5 seconds.

**Reset to Default** Select the **Reset to Default** button to reset the DWR-920V to factory default settings.

**Reboot** Select the **Reboot** button to reboot the DWR-920V.



# Firmware Upgrade

This page allows you to manually upgrade your router's firmware.

## Upgrade My Router

**Upgrade My Router** Select **Manual** to manually upgrade your router's firmware. To upgrade automatically, select **Remote Server** from the drop down menu and then click **Check Remote Server** and follow the on-screen instructions.

**Open File** If you have selected a manual upgrade, select the appropriate file for the upgrade.

**Current Version** The current version of your firmware.

**Note:** The FW version number displayed on the image to the right may differ from your router due to firmware updates or regional variation.

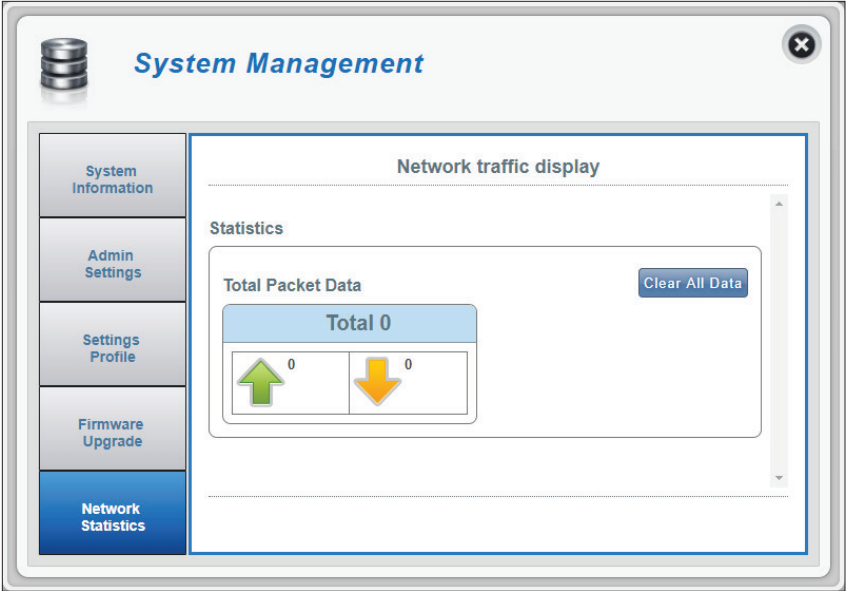
Click the **Start Update** button.

The screenshot shows the 'System Management' interface with the 'Firmware Upgrade' section active. On the left sidebar, 'Firmware Upgrade' is highlighted. The main content area is titled 'Upgrade My Router'. It features a dropdown menu for 'Upgrade My Router' set to 'Manual'. Below it, the 'Open File' section has a 'Choose File' button and the text 'No file chosen'. The 'Current Version' is displayed as '01.01.WW'. At the bottom, there is a 'Start Update' button.

The screenshot shows the 'System Management' interface with the 'Firmware Upgrade' section active. On the left sidebar, 'Firmware Upgrade' is highlighted. The main content area is titled 'Upgrade My Router'. It features a dropdown menu for 'Upgrade My Router' set to 'Remote Server'. Below it, the 'Current Version' is displayed as '01.01.WW'. At the bottom, there is a 'Check Remote Server' button.

# Network Statistics

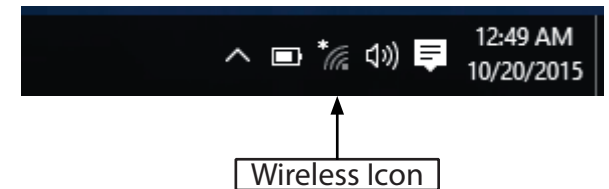
This page displays the packets transmitted and received by your router. The traffic counter will reset if the device is rebooted. Click the **Clear All Data** button to refresh the statistics.



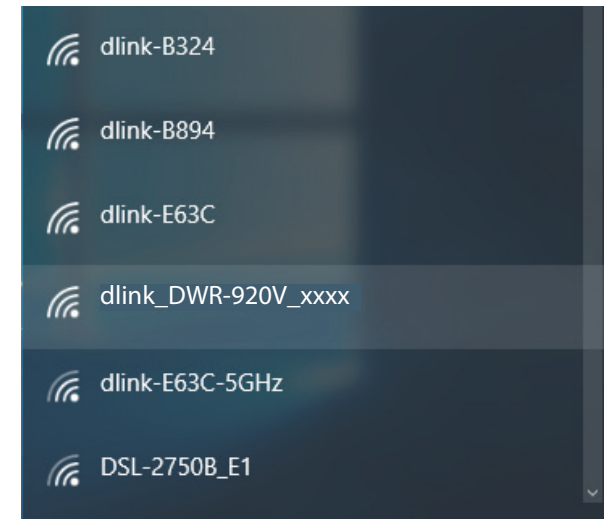
# Connecting to a Wireless Network Using Windows 10

When connecting to the DWR-920V wirelessly for the first time, you will need to know the default network name (SSID) and security key (Wi-Fi password) being used. These can be found on a label on the underside of the battery cover.

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

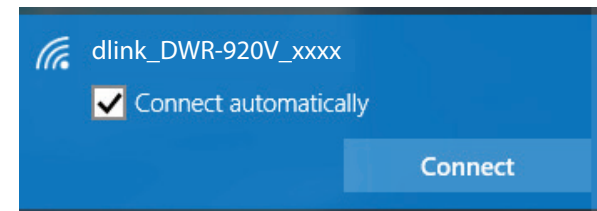


Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the SSID.

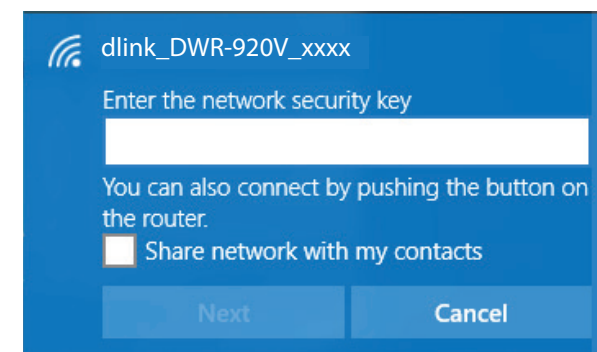


To connect to the SSID, click **Connect**.

To automatically connect with the router when your device next detects the SSID, click the **Connect Automatically** check box.



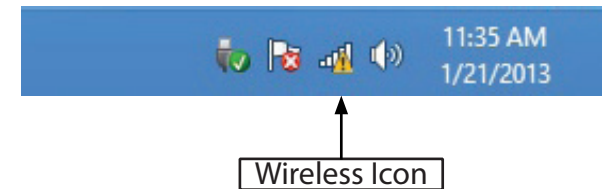
You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next** to connect to the network.



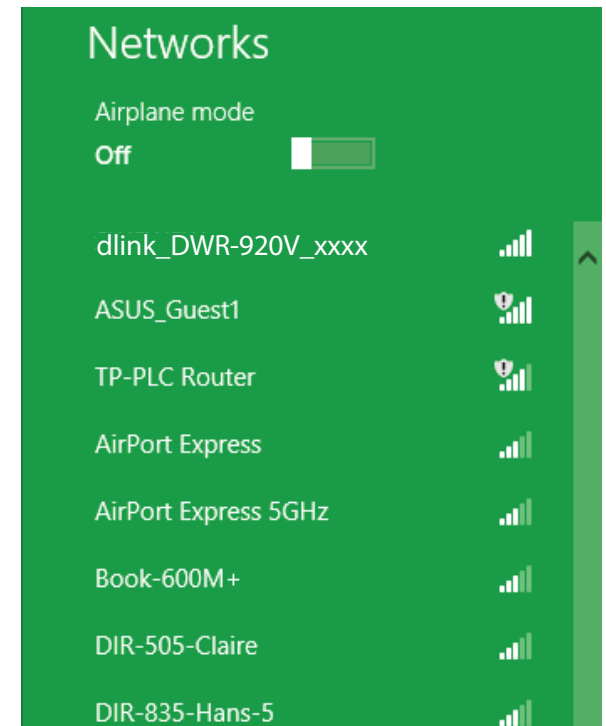
# Using Windows 8

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

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

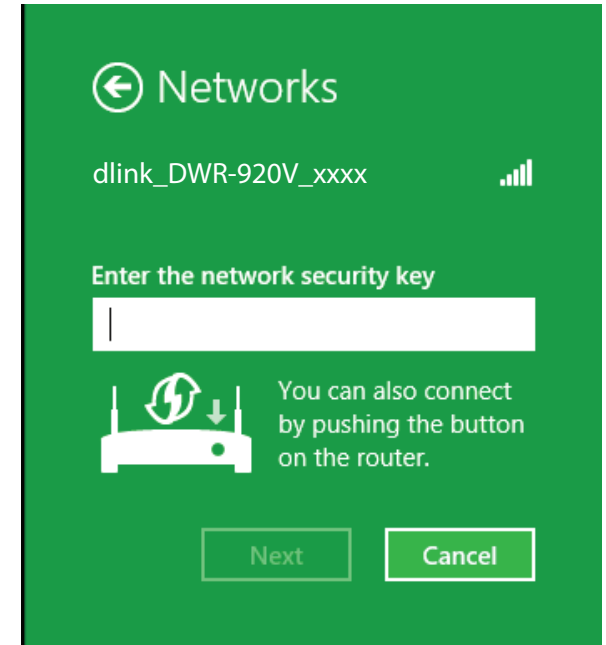


Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.

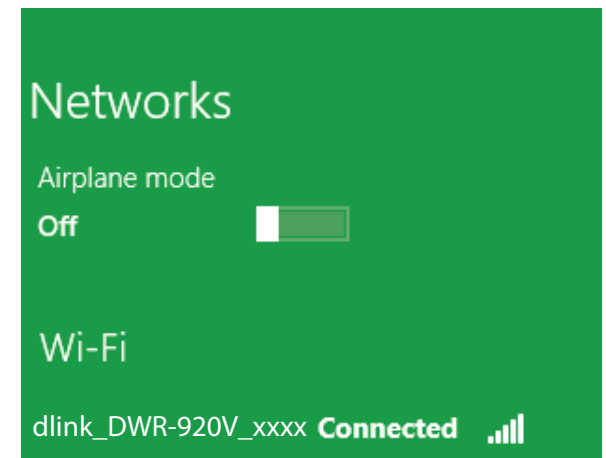


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. If this is the first time connecting to your router, a unique security key for your router will be displayed on a sticker in the router's battery bay. Enter the password into the box and click Next.

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 at this point 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.



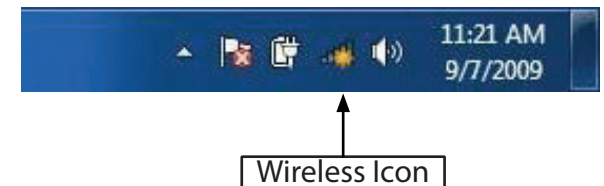


# Connecting to a Wireless Network Using Windows 7

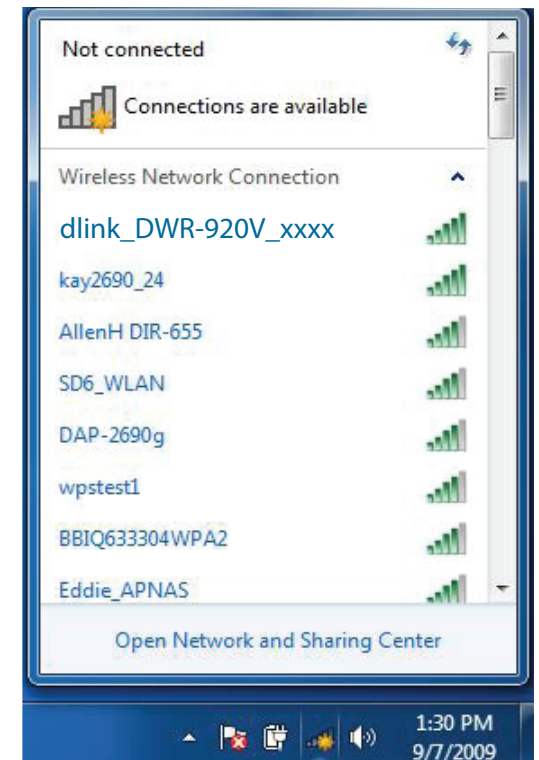
Windows 7 users may use the built-in wireless utility to connect to a wireless network. If you are using another company's utility or Windows 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option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

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

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



Wireless Icon



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

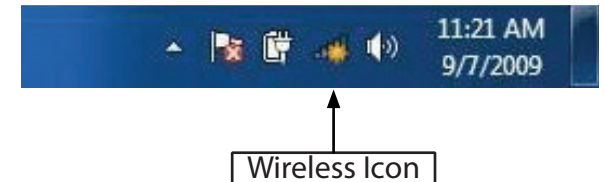
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to **Networking Basics** on page 78 for more information.



## Configuring Wireless Encryption

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

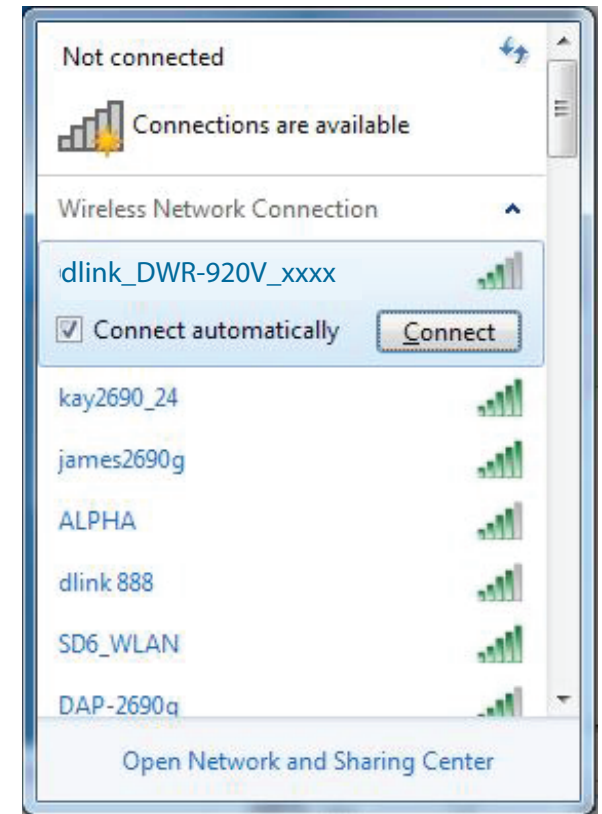
1. Click on the wireless icon in your system tray (lower-right corner).



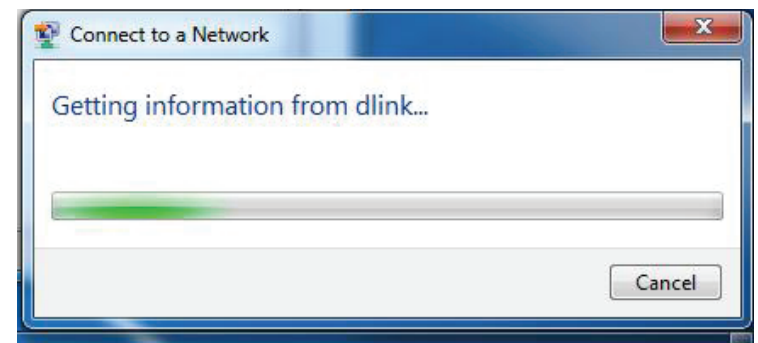
2. The utility will display any available wireless networks in your area.



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

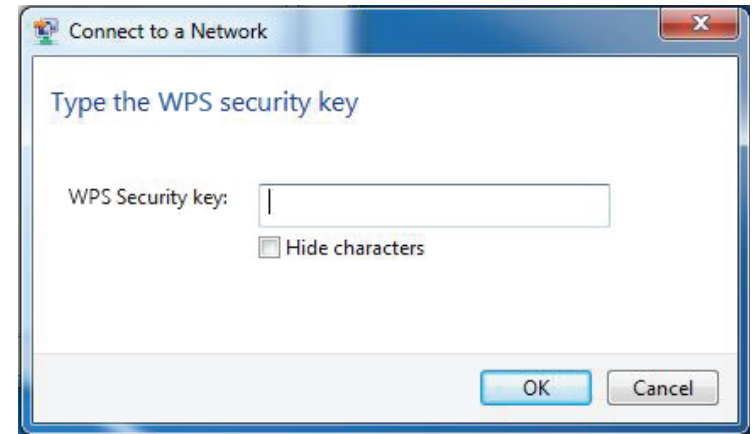


4. The following window appears while your computer tries to connect to the router.



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

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



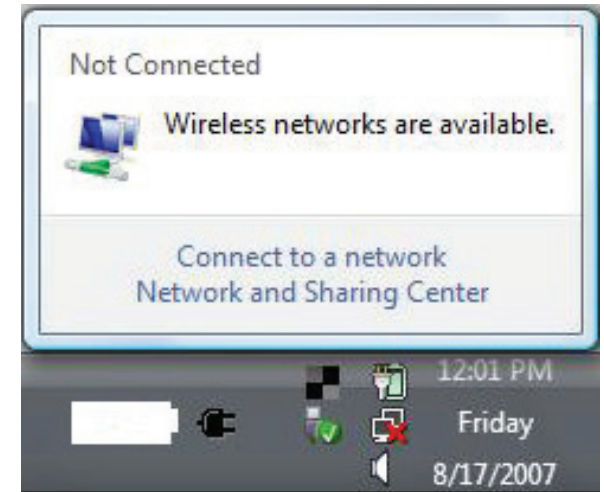
# Using Windows Vista™

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

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

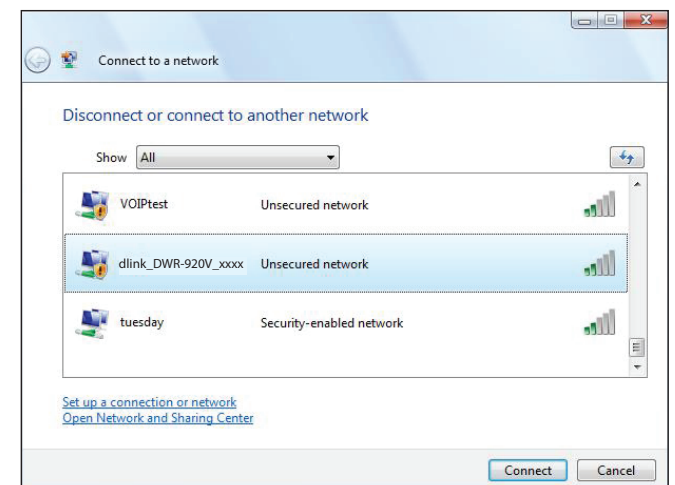
or

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



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

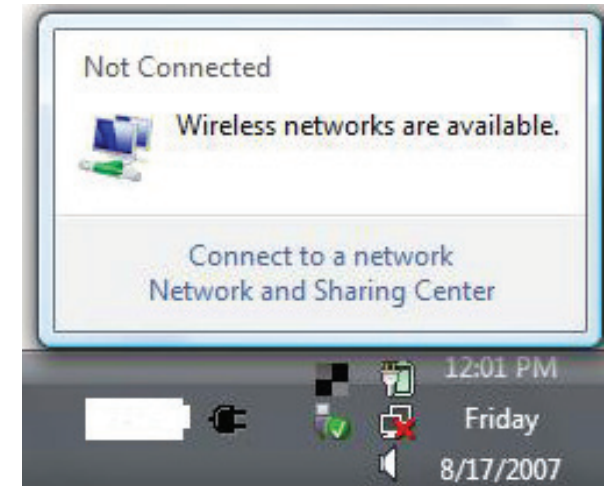
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to **Networking Basics** on page 78 for more information.



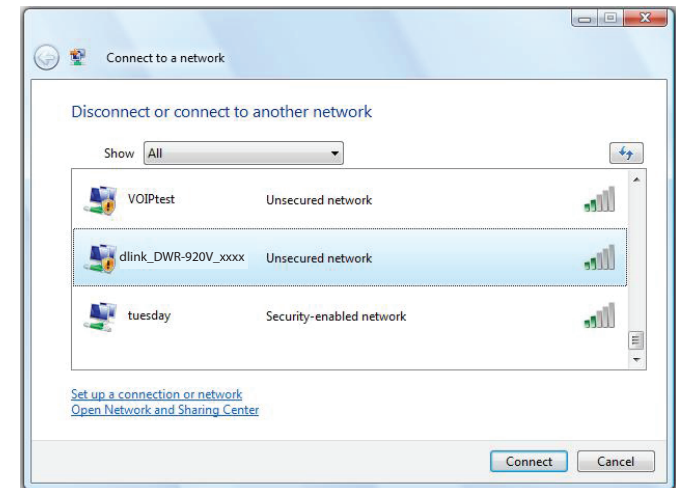
## Configuring Wireless Encryption

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

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

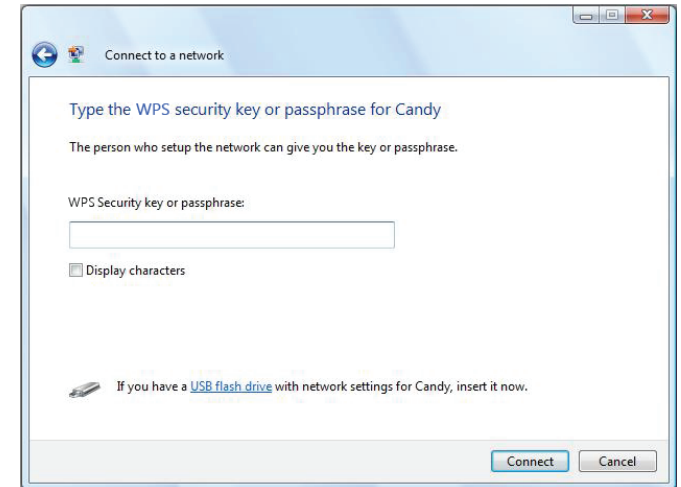


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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





# Connect to a Wireless Network

## Using Windows® XP

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

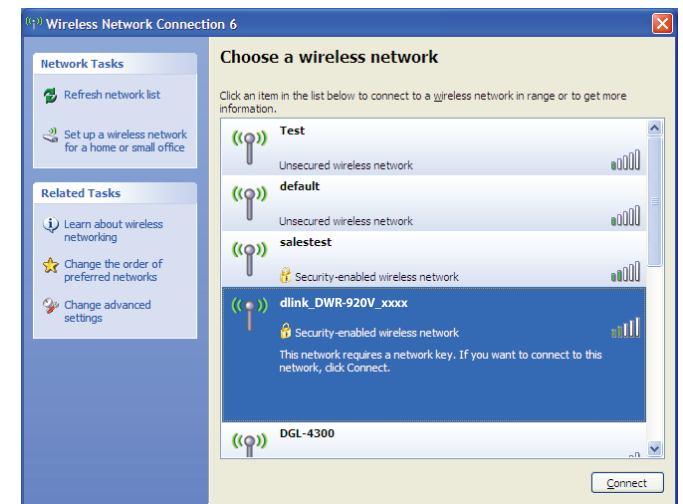
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to **Networking Basics** on page 78 for more information.



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-920V. Read the following descriptions if you are having problems.

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

When entering the IP address of your router (192.168.0.1 for example), you are not connecting to a website on the Internet 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:
  - Internet Explorer 9 or higher, Chrome 28.0, Firefox 23.0, or Safari 6.
- If attempting to connect wirelessly, ensure that the wireless indicator on the OLED display is lit. Also, ensure that you are connected to the correct SSID for your mobile router.
- Make sure that the computer you are using is not connected to any other devices (such as routers or switches) which might have the same IP address as the DWR-920V, as this may cause an IP address conflict. If you have a conflict, temporarily unplug any other devices from your computer while you configure the DWR-920V. You can also change the IP address of the DWR-920V in the Network section of the configuration utility. You may also need to renew your computer's IP address configuration. To do this, start the Command utility: Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows Vista users type **cmd** in the **Start Search** box.) This will bring up a black screen with white text. At the command prompt, type **ipconfig /release** and wait for the process to be completed. Next, type **ipconfig /renew** which will renew your computer's IP address configuration.
- 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 **Default Level** 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 re-open it.

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

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

# Networking Basics

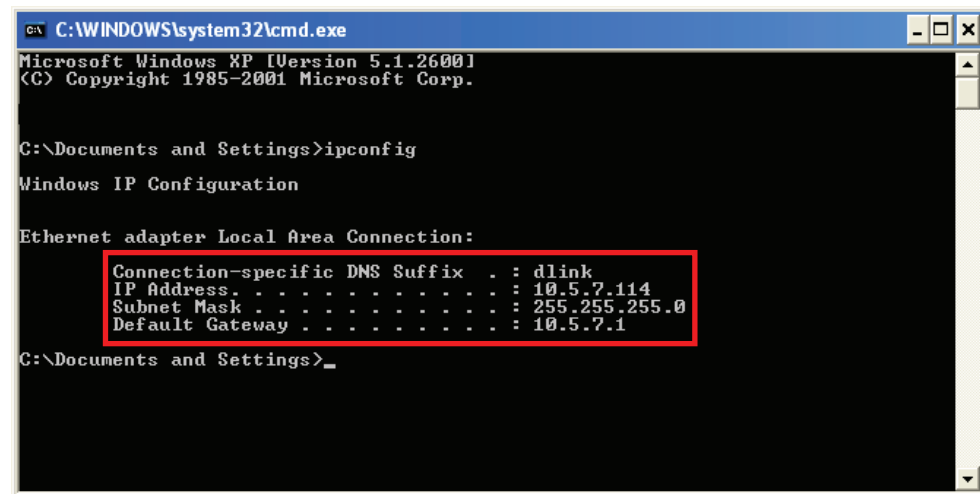
## Check your IP address

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

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

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

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>
```

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

## Statically Assign an IP address

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

### Step 1

- Windows® 8 Click on **Start > Control Panel > Network and Internet Connections > Network Connections > Configure your Internet Protocol (IP) settings.**
- Windows® 7 Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**
- 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.**

### Step 2

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

### Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties.**

### Step 4

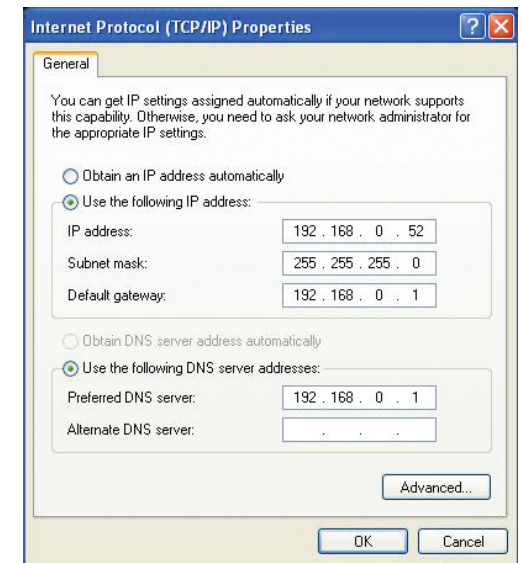
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

### Step 5

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



# Technical Specifications

## Radio Frequency Bands<sup>1</sup>

- LTE: Band 4/12/41/66
- DC-HSPA+/HSPA+/HSUPA/HSDPA/WCDMA: B2/B5

## Cellular Access<sup>2</sup>

- LTE up to 150 Mbps Down/50 Mbps Up
- DC-HSPA+ up to 42 Mbps Up/5.76 Mbps Down
- HSPA+ up to 21 Mbps Up/ 5.76 Mbps Down
- HSPA up to 7.2 Mbps/5.76 Mbps Down
- UMTS up to 384 Kbps Up/384 Kbps Down
- EDGE up to 237 Kbps Up/118 Kbps Down
- GPRS up to 85.6 Kbps Up/42.8 Kbps Down

## Wi-Fi Access Point

- 802.11n
- 802.11g
- 802.11b

## Antenna

- 2 x 2.4G Internal Wi-Fi Antennas

## SIM/UICC Slot

- Standard mini-SIM/UICC card interface

## Indicators

- LED Indicators

## Wireless Encryption

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

## Firewall

- NAT
- Port Range Forwarding
- DMZ
- UPnP

## Dimensions (L x W x H)

- 121 x 117.3 x 43.5 mm (4.76 x 4.62 x 1.71 in)

## Weight

- 205 g (7.23 oz)

## Operating Temperature

- 0 to 40 °C (32 to 104 °F)

## Storage Temperature

- -10 to 70 °C (14 to 158 °F)

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

<sup>2</sup> Data rates are theoretical. Data transfer rate depends on network capacity, signal strength, and other factors.

# Regulatory Information

## **Federal Communication Commission Interference Statement**

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

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

## **Non-modifications Statement:**

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

## **Caution:**

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

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

## **FCC Radiation Exposure Statement**

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and consider removing the no-collocation statement.