D-Link®

Version 1.01 | 12/25/2018

User Manual

4G LTE VPN Router

DWR-925

Preface

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

Manual Revisions

Revision	Date	Description
1.00	December 25, 2018	• Initial release

Trademarks

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

Apple®, Apple logo®, Safari®, iPhone®, iPad®, iPod touch®, and Macintosh® are trademarks of Apple Inc., registered in the U.S. and other countries. App Store^{SM} is a service mark of Apple Inc.

Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.

Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

The purpose of this product is to create a constant network connection for your devices. As such, it does not have a standby mode or use a power management mode. If you wish to power down this product, please simply unplug it from the power outlet.

Table of Contents

Package Contents

- DWR-925 4G LTE VPN Router
- Ethernet Cable
- Detachable Antenna
- Power Adapter

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

***Note:** Using a power supply with a different voltage rating than the one included with the DWR-925 may cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• IEEE 802.11n, 802.11g, or 802.11b wireless clients or • 10/100 Ethernet • An Ethernet-based cable or DSL modem or • A compatible (U)SIM card with service.* *Subject to services and service terms available from your carrier.
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 10 or higher • Firefox 36 or higher • Safari 8 or higher • Chrome 40 or higher

Introduction

The D-Link DWR-925 4G LTE VPN Router is an easy to deploy high-performance Virtual Private Network (VPN) router with mobile connectivity to allow easy access to mobile broadband networks. Create a powerful private network for your home or small office with easy setup tools, advanced configuration options, and built-in security features. The DWR-925 4G LTE VPN Router lets you connect to your 3G / 4G mobile connection with fast downlink speeds of up to 100 Mbps and uplink speeds up to 50 Mbps, giving you the speed you need for fast, responsive Internet access.

Support for 802.11n/g/b wireless delivers real-world performance of up to 14x faster than an 802.11g wireless connection. With regards to redundancy, the auto-failover feature automatically switches between mobile broadband and fixed-line broadband to ensure you stay connected to the Internet in case one connection fails. In addition, this router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

The DWR-925 4G LTE VPN Router lets you create a high-speed Virtual Private Network (VPN) for access over the Internet or a wired network connection. Advanced VPN configuration options can be set using the comprehensive setup wizard and includes management, negotiation modes, and authentication support using an internal user database. With the DWR-925 you'll have all the tools you need to create the ideal VPN solution for your network.

Features

- **Reliable and Versatile** - The D-Link DWR-925 lets you connect to your 3G / 4G mobile connection with fast downlink speeds of up to 100 Mbps and uplink speeds up to 50 Mbps, giving you the speed you need for fast, responsive Internet access. The auto-failover feature automatically switches between mobile broadband and fixed-line broadband to ensure you stay connected to the Internet in case one connection fails. The serial port connects to a dial-up modem as a failover option or can be configured as a console port if necessary, providing extra flexibility and versatility.

- **Virtual Private Network Features** - The DWR-925 lets you create a high-speed Virtual Private Network (VPN) for access over the Internet or a wired network connection. It supports IPsec, PPTP, L2TP, and GRE protocols in Server Mode, and also handles pass-through traffic. Advanced VPN configuration options can be set using the comprehensive setup wizard and include multiple encryption options, key management, negotiation modes, and VPN authentication support using an internal user database.

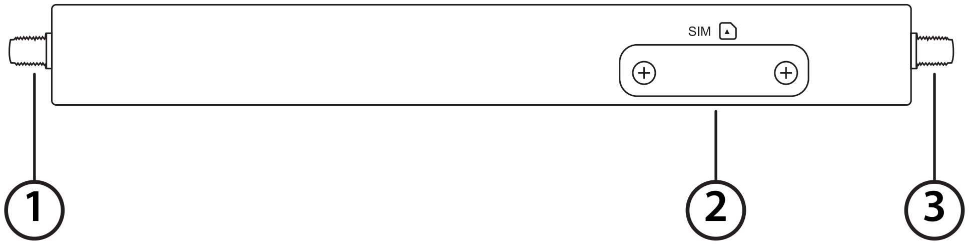
- **Extended Whole Home Coverage** - Powered by Wireless N technology, this high-performance router provides superior Whole Home Coverage while reducing dead spots. The router is designed for use in bigger homes and for users who demand higher performance networking. Add a Wireless N notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

- **Quality of Service (QoS)** - For smooth, uninterrupted streaming, this router includes a Quality of Service (QoS) engine that prioritizes according to data type so your VoIP calls and online gaming stay smooth and responsive.

* Maximum wireless signal rate derived from IEEE Standard 802.11b, 802.11g and 802.11n 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 conditions will adversely affect wireless signal range.

Hardware Overview

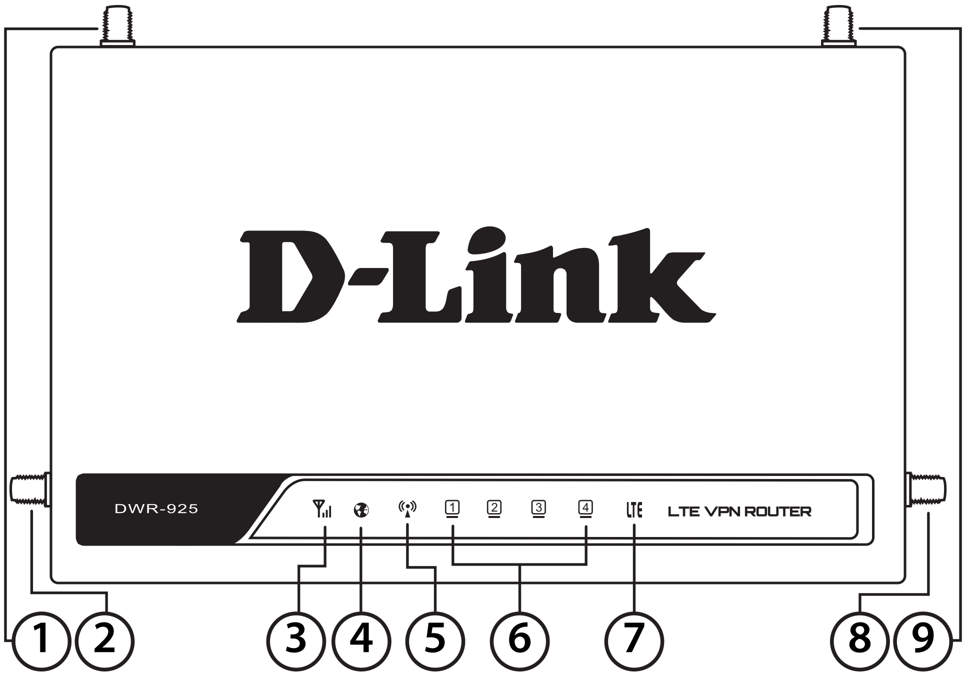
Front Panel



#	Item	Description
1	**3G/4G MAIN**	SMA female connector - Main Antenna for 3G/4G.
2	**Mini-SIM Slot**	The router uses a 2FF-size or mini-SIM for 3G/4G.
3	**3G/4G DRX**	SMA female connector - Diveristy Antenna for 3G/4G.

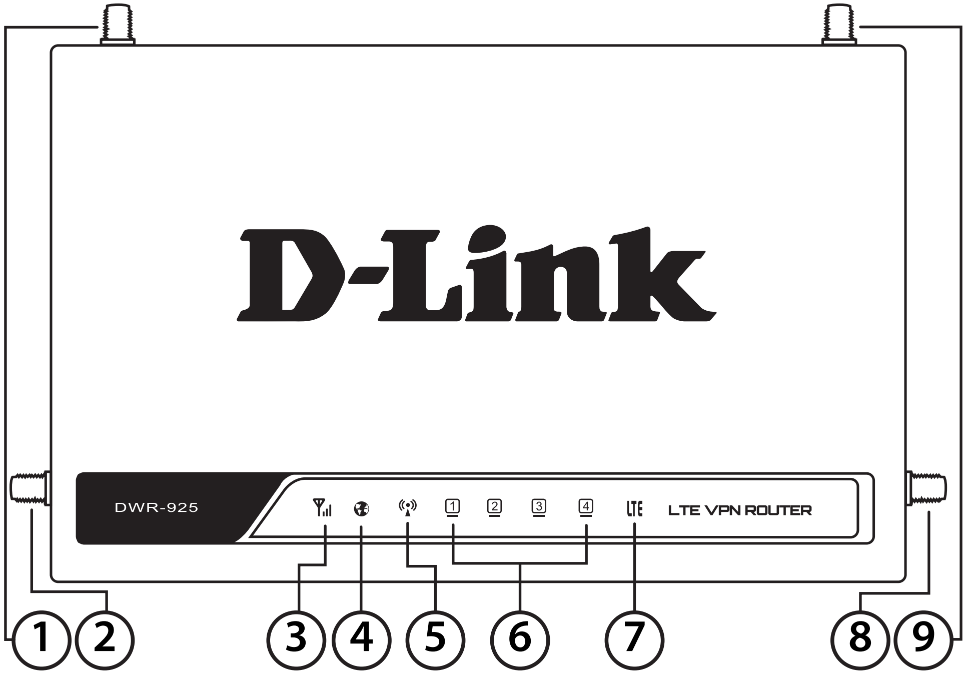
Note: The included antennas are interchangeable. Third party antennas may require connection to specific ports.

Hardware Overview
Top Panel



#	Item	Description	
1	**SMA Connector Main**	SMA female connector - Primary antenna.	
2	**Wi-Fi Antenna 2**	SMA male connector - Wi-Fi 2.	
3	**Signal Strength**	Blinking Red	No SIM, no signal, or unverified PIN.
		Solid Red	Weak signal.
		Solid Amber	Medium Signal.
		Solid Green	Strong Signal.
4	**WAN**	Solid Green	Ethernet WAN connection established.
		Blinking Green	Data being transferred.
5	**WLAN**	Solid Green	WLAN active and available.
		Blinking Green	Data being transferred.

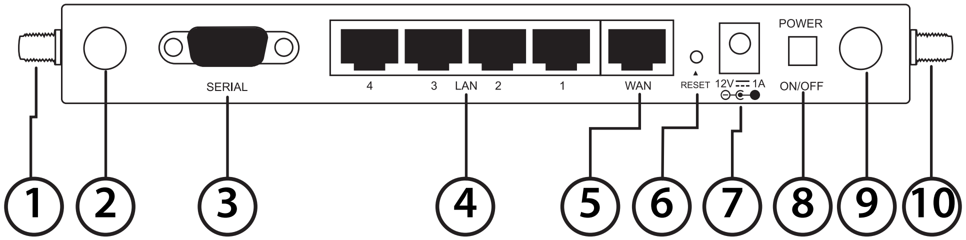
Hardware Overview
Top Panel (Cont)



#	Item	Description	
6	**LAN**	Solid Green	Connected to SIM A LTE Network.
		Flashing Green	Fallback to SIM A 3G/2G network.
		Off	No Service/SIM Error/APN Error.
7	**WWAN**	Solid Green	Indicates a 2G/3G/4G WLAN connection
		Blinking Green	Indicates data transfer.
8	**Wi-Fi Antenna 1**	SMA male connector - Wi-Fi 1.	
9	**3G/4G DRX**	SMA female connector - Diversity Antenna for 3G/4G	

Note: The included antennas are interchangeable. Third party antennas may require connection to specific ports.

Hardware Overview
Rear Panel



#	Item	Description
1	**3G/4G MAIN**	SMA female connector - Auxiliary Antenna for 3G/4G
2	**Wi-Fi Antenna 2**	SMA male connector - Wi-Fi 2.
3	**Serial Port**	The serial port allows the use of an external dial-up modem for fall-back or configuration via CLI
4	**LAN Ethernet 1-4**	Connect Ethernet devices such as computers, switches, external APs, and NAS.
5	**WAN Ethernet**	Allows optional use of Ethernet as primary or fallback WAN connection
6	**Reset**	Press and hold for 10 seconds to restore factory defaults.
7	**Power input**	12VDC 1A barrel connector.
8	**Power On/Off**	Press to toggle power.
9	**Wi-Fi Antenna 1**	SMA male connector - Wi-Fi 1.
10	**3G/4G DRX**	SMA female connector - Diversity Antenna for 3G/4G

Note: The included antennas are interchangeable. Third party antennas may require connection to specific ports.

Hardware Installation

Before you Begin

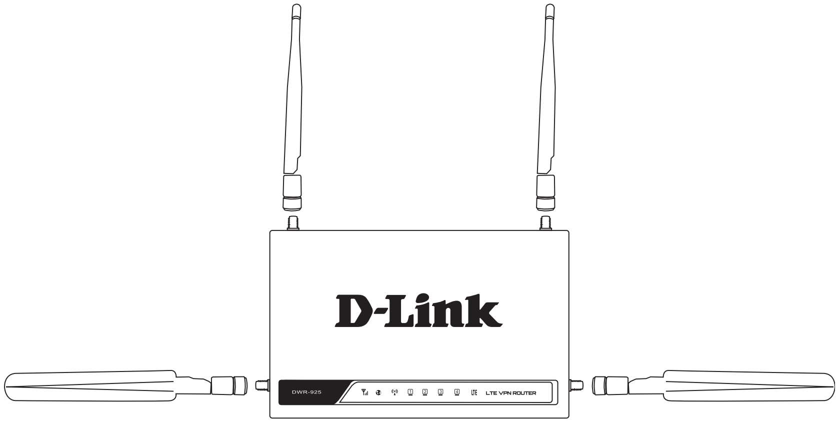
Observe the following precautions to help prevent shutdowns, equipment failures, and personal injury:

- Install the DWR-925 in a cool and dry place. Refer to the technical specifications in the user manual for the acceptable operating temperature and humidity ranges.
- Install the router in a site free from strong electromagnetic sources, vibration, dust, excessive moisture, and direct sunlight.
- Place antennas in an unobstructed area with clear mobile signal. Avoid metal boxes, brick walls, and other dense materials. It is recommended to use the web interface to confirm signal strength before permanent installation.
- Visually inspect the power connector and make sure that it is fully secure.
- Do not stack any devices on top of the router.

Attaching the External Antennas

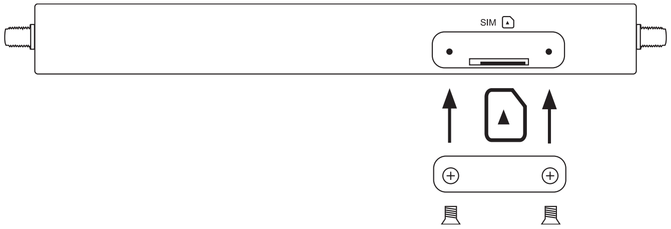
The DWR-925 requires four external antennas to function correctly, two blade antennas for the 3G/4G, and two Wi-Fi antennas. The included antennas are interchangeable, but third party antennas may require connection to specific ports.

1. Attach the blade antennas to the SMA connectors on the side of the router. Turn clockwise to fasten each antenna. If you are using 3rd party antennas that require specific ports, the port on the left side of the device is the "MAIN" antenna, and the "AUX" or "DRX" antenna.
2. Attach the Wi-Fi antennas to the SMA connectors on the back of the router. Turn clockwise to fasten each antenna.
3. Position the antennas where they will receive optimal signal. Arrange them so they point upward.



Note: The included antennas are interchangeable. Third party antennas may require connection to specific ports.

Installing the SIM card



The DWR-925 is equipped with a Mini-SIM. An active SIM card is required for 3G/4G access.

1. Unscrew the SIM slot cover on the front of the device.
2. Insert a mini-SIM card into the slot with the contacts facing down.
3. Gently press the mini-SIM into the slot until it locks into place. To remove, press again and the SIM card will be ejected.
4. Replace the cover and screws.

Note: SIM behavior must be configured from the web UI before an Internet connection can be established.

Powering the Router

The router requires a 12-volt power supply and a minimum of 1 amp.

Using the Included AC Adapter

1. Attach the barrel connector of included AC adapter to the DWR-925 power port on the rear panel.
2. Attach the AC adapter to an appropriate AC socket.

Connecting Devices

After the DWR-925 has been successfully installed, the router can be connected to the end device via the following connection methods:

Over Ethernet

The Ethernet port can be connected to an end device. Use a standard Category 5/5e/6 RJ-45 Ethernet cable to connect the end device to the router. The port will auto-negotiate to the highest possible port speed based on the connected device. Note that the DWR-925 supports a maximum transfer speed of 100 Mbps over Ethernet.

Over Wi-Fi

If you have configured Wi-Fi, connect using the SSID and security settings listed on the bottom of the router. If you Wi-Fi has previously been configured, use those settings instead. The router supports up to 802.11n speeds on the 2.4 GHz network. Maximum transfer speeds are dependent on network conditions.

Wireless Installation Considerations

The D-Link wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

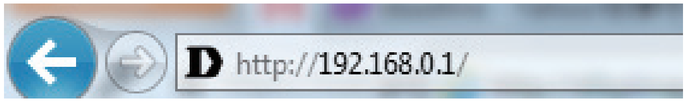
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

Configuration

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

Web-based Configuration Utility

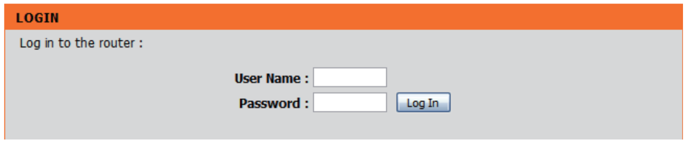
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (**http://192.168.0.1**).



http://192.168.0.1/

Type **Admin** and then enter the password. By default, the password is blank.

If you get a **Page Cannot be Displayed** error, please refer to “Troubleshooting” on page 98 for assistance.

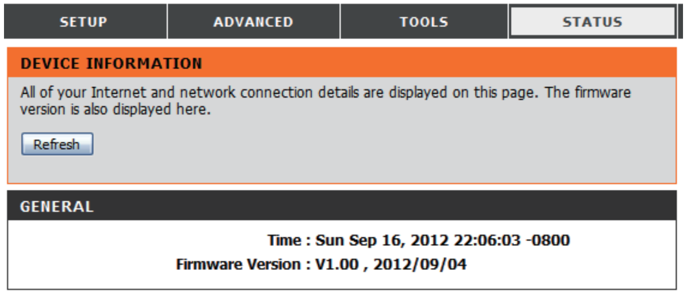


LOGIN

Log in to the router :

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

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



DEVICE INFORMATION

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

GENERAL

Time : Sun Sep 16, 2012 22:06:03 -0800

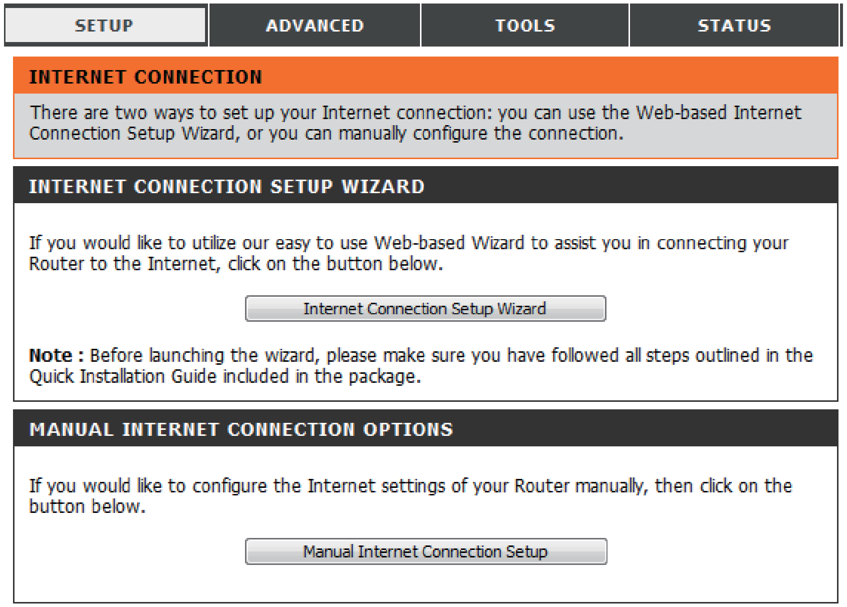
Firmware Version : V1.00 , 2012/09/04

Setup

The setup wizard guides you through the initial setup of your router. There are two ways to set up your Internet connection. You can use the web-based **Internet Connection Setup Wizard** or you can manually configure using the **Manual Internet Connection Setup** wizard.

Click **Internet Connection Setup Wizard** to begin.

If you want to enter your settings without running the wizard, click **Manual Internet Connection Setup** and refer to "Manual Internet Connection Setup" on page 17.



INTERNET CONNECTION

There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.

INTERNET CONNECTION SETUP WIZARD

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your Router to the Internet, click on the button below.

Note : Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

MANUAL INTERNET CONNECTION OPTIONS

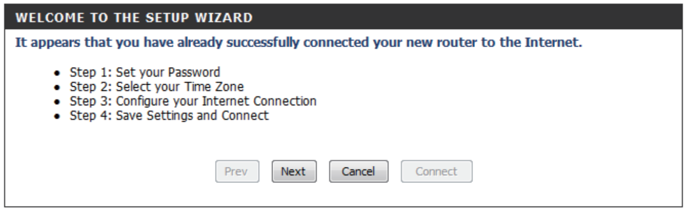
If you would like to configure the Internet settings of your Router manually, then click on the button below.

Internet Connection Setup Wizard

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

Click **Next** to continue.

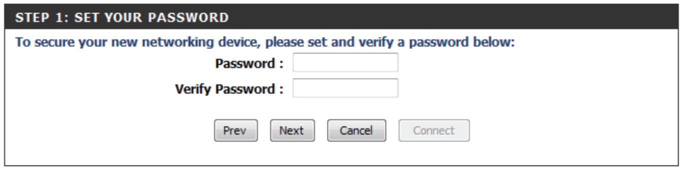
Note: While using the wizard, you can click **Prev** to go back to the previous step or you can click **Cancel** to close the wizard.


WELCOME TO THE SETUP WIZARD

It appears that you have already successfully connected your new router to the Internet.

- Step 1: Set your Password
- Step 2: Select your Time Zone
- Step 3: Configure your Internet Connection
- Step 4: Save Settings and Connect

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

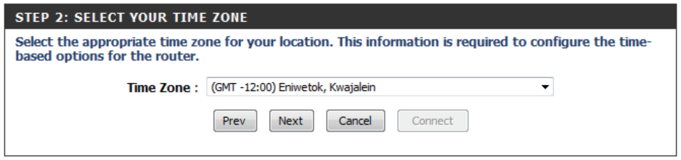

STEP 1: SET YOUR PASSWORD

To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

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


STEP 2: SELECT YOUR TIME ZONE

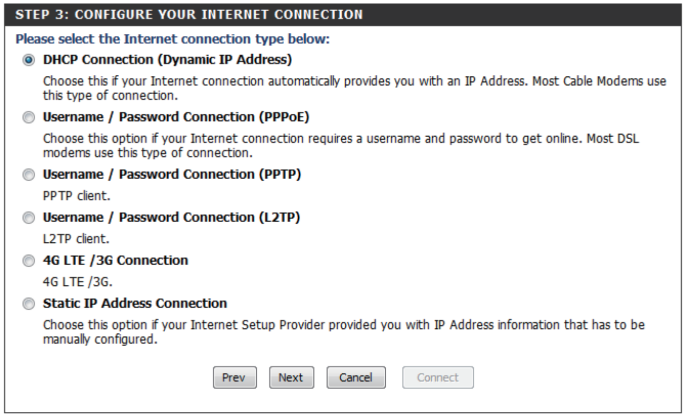
Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

Time Zone : (GMT -12:00) Eniwetok, Kwajalein

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

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

Note: The DWR-925 has a WAN failover feature that allows the router to switch to a 3G / 4G connection if the WAN connection is down or unavailable.


STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Please select the Internet connection type below:

● **DHCP Connection (Dynamic IP Address)**

Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

○ **Username / Password Connection (PPPoE)**

Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

○ **Username / Password Connection (PPTP)**

PPTP client.

○ **Username / Password Connection (L2TP)**

L2TP client.

○ **4G LTE /3G Connection**

4G LTE /3G.

○ **Static IP Address Connection**

Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

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

Static IP Address Connection: Choose this option if your Internet Service Provider provided you with IP address information that has to be manually configured. See “Static IP (assigned by ISP)” on page 17 for information about how to configure this type of connection.

DHCP Connection (Dynamic IP Address): Choose this if your Internet connection automatically provides you with an IP address. Most cable modems use this type of connection. See “Dynamic IP (DHCP)” on page 18 for information about how to configure this type of connection.

Username / Password Connection (PPPoE): Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See “PPPoE” on page 19 for information about how to configure this type of connection.

Username / Password Connection (PPTP): Choose this option if your Internet connection requires Point-to-Point Tunneling Protocol (PPTP). See “PPTP” on page 20 for information about how to configure this type of connection.

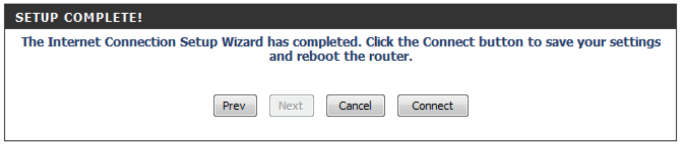
Username / Password Connection (L2TP): Choose this option if your Internet connection requires Layer 2 Tunneling Protocol (L2TP). See “L2TP” on page 22 for information about how to configure this type of connection.

4G LTE / 3G Connection: Choose this connection if you have installed a SIM card into the DWR-925. See “4G LTE / 3G” on page 24 for information about how to configure this type of connection.

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

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

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



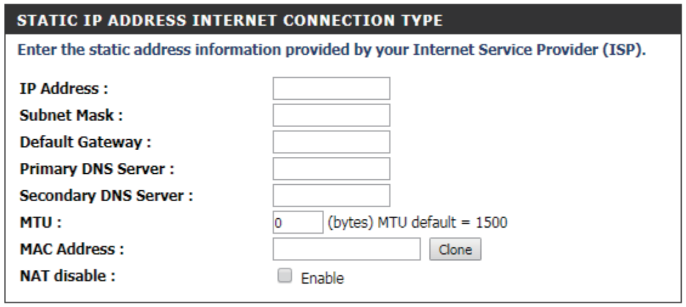
SETUP COMPLETE!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

Manual Internet Connection Setup

Static IP (assigned by ISP)

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format. After modifying any settings, click **Save Settings** to save your changes.



STATIC IP ADDRESS INTERNET CONNECTION TYPE

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

IP Address :	
Subnet Mask :	
Default Gateway :	
Primary DNS Server :	
Secondary DNS Server :	
MTU :	0 (bytes) MTU default = 1500
MAC Address :	Clone
NAT disable :	□ Enable

Failover Internet Type Is: This will display the failover Internet type, if available.

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

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

Default Gateway: Enter the gateway assigned by your ISP.

Primary / Secondary DNS Servers: The DNS server information will be supplied by your ISP (Internet Service Provider.)

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

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

NAT Disable: Activate this feature to disable NAT through this router. IP addresses will be directly assigned by your ISP.

Dynamic IP (DHCP)

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

Host Name: (Optional) Fill in the host name of your DNS server.

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

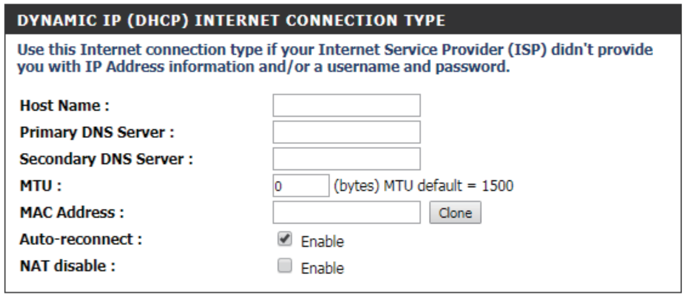
Secondary DNS Server: (Optional) Fill in with IP address of the secondary DNS server.

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

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

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

NAT Disable: Activate this feature to disable NAT through this router. IP addresses will be directly assigned by your ISP.



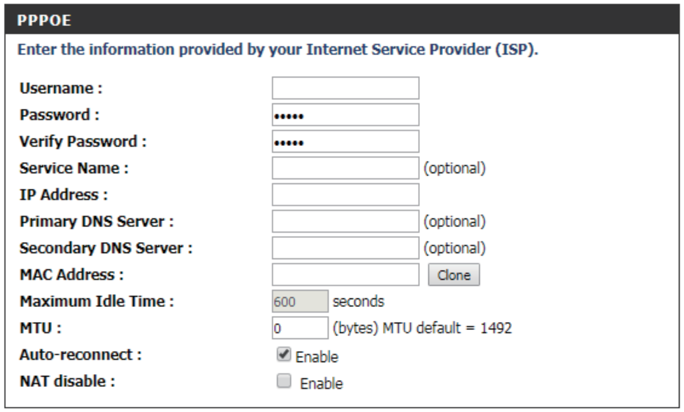
DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :	
Primary DNS Server :	
Secondary DNS Server :	
MTU :	0 (bytes) MTU default = 1500
MAC Address :	Clone
Auto-reconnect :	☑ Enable
NAT disable :	☐ Enable

PPPoE

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



PPPOE

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

Username :	
Password :	•••••
Verify Password :	•••••
Service Name :	(optional)
IP Address :	
Primary DNS Server :	(optional)
Secondary DNS Server :	(optional)
MAC Address :	Clone
Maximum Idle Time :	600 seconds
MTU :	0 (bytes) MTU default = 1492
Auto-reconnect :	☑ Enable
NAT disable :	□ Enable

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

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

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

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

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

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

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

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

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

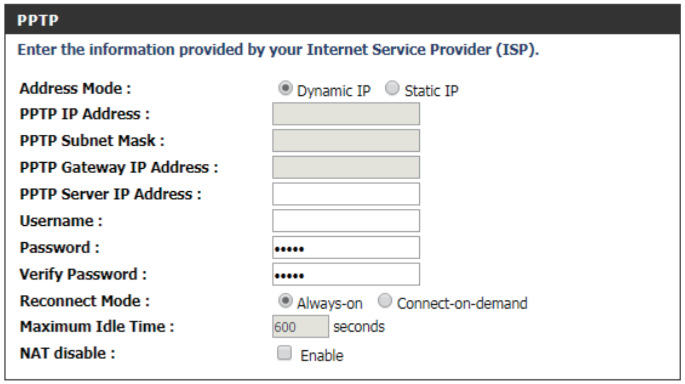
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

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

NAT Disable: Activate this feature to disable NAT through this router. IP addresses will be directly assigned by your ISP.

PPTP

Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Click **Save Settings** to save your changes.



PPTP

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

Address Mode :	● Dynamic IP ○ Static IP
PPTP IP Address :	
PPTP Subnet Mask :	
PPTP Gateway IP Address :	
PPTP Server IP Address :	
Username :	
Password :	•••••
Verify Password :	•••••
Reconnect Mode :	● Always-on ○ Connect-on-demand
Maximum Idle Time :	600 seconds
NAT disable :	□ Enable

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

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

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

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

PPTP Server IP Address: Enter the IP address of the PPTP server.

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

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

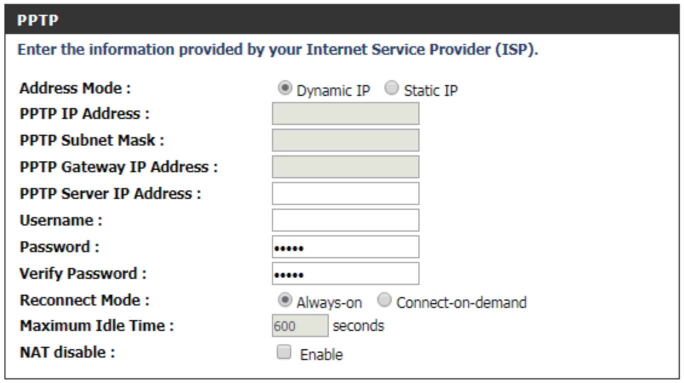
Verify Password: Re-enter your password for verification.

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

PPTP (cont)

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

NAT Disable: Activate this feature to disable NAT through this router. IP addresses will be directly assigned by your ISP.



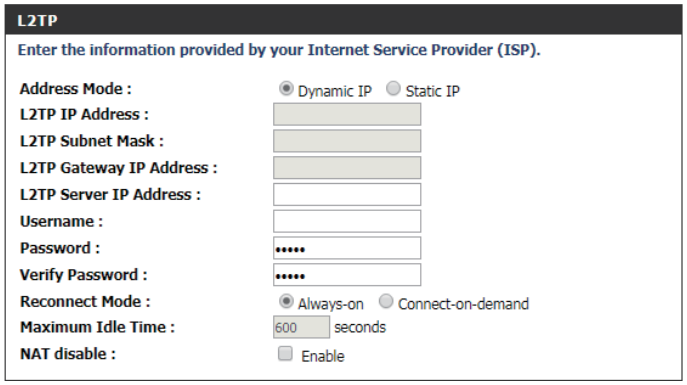
PPTP

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

Address Mode :	● Dynamic IP ○ Static IP
PPTP IP Address :	
PPTP Subnet Mask :	
PPTP Gateway IP Address :	
PPTP Server IP Address :	
Username :	
Password :	•••••
Verify Password :	•••••
Reconnect Mode :	● Always-on ○ Connect-on-demand
Maximum Idle Time :	600 seconds
NAT disable :	□ Enable

L2TP

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



L2TP

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

Address Mode :	● Dynamic IP ○ Static IP
L2TP IP Address :	
L2TP Subnet Mask :	
L2TP Gateway IP Address :	
L2TP Server IP Address :	
Username :	
Password :	•••••
Verify Password :	•••••
Reconnect Mode :	● Always-on ○ Connect-on-demand
Maximum Idle Time :	600 seconds
NAT disable :	□ Enable

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

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

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

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

L2TP Server IP Address: Enter the IP address of your L2TP server.

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

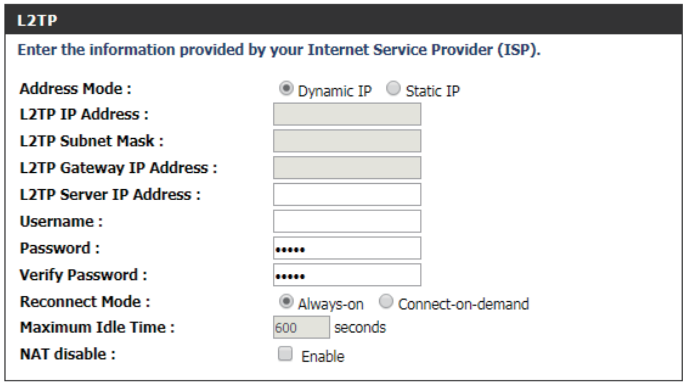
Password: The password that your ISP provides to you for L2TP dial-up.

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

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

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

NAT Disable: Activate this feature to disable NAT through this router. IP addresses will be directly assigned by your ISP.



L2TP

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

Address Mode :	◉ Dynamic IP ○ Static IP
L2TP IP Address :	
L2TP Subnet Mask :	
L2TP Gateway IP Address :	
L2TP Server IP Address :	
Username :	
Password :	•••••
Verify Password :	•••••
Reconnect Mode :	◉ Always-on ○ Connect-on-demand
Maximum Idle Time :	600 seconds
NAT disable :	□ Enable

4G LTE / 3G

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

Country: Select your country.

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

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

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

Verify Password: Re-type your password.

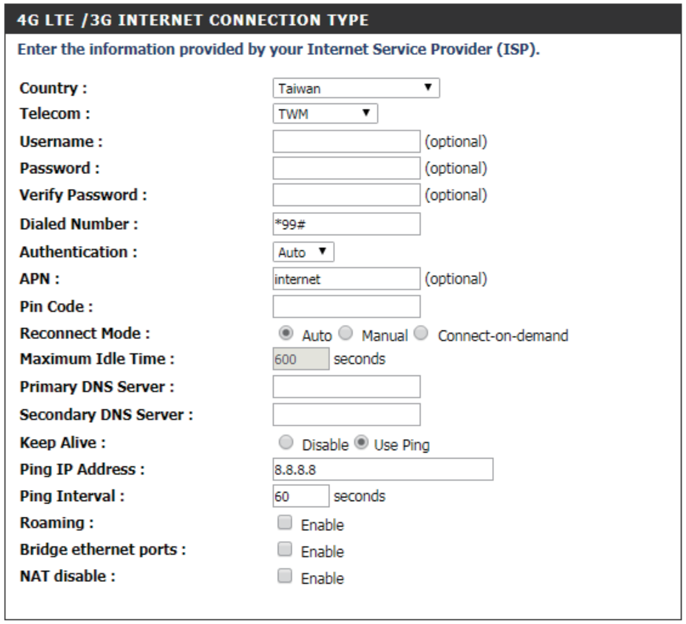
Dialed Number: Enter the number to be dialed.

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

APN: Enter the APN information (optional).

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

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



4G LTE /3G INTERNET CONNECTION TYPE

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

Country :	Taiwan ▼
Telecom :	TWM ▼
Username :	(optional)
Password :	(optional)
Verify Password :	(optional)
Dialed Number :	*99#
Authentication :	Auto ▼
APN :	internet (optional)
Pin Code :	
Reconnect Mode :	● Auto ○ Manual ○ Connect-on-demand
Maximum Idle Time :	600 seconds
Primary DNS Server :	
Secondary DNS Server :	
Keep Alive :	○ Disable ● Use Ping
Ping IP Address :	8.8.8.8
Ping Interval :	60 seconds
Roaming :	□ Enable
Bridge ethernet ports :	□ Enable
NAT disable :	□ Enable

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

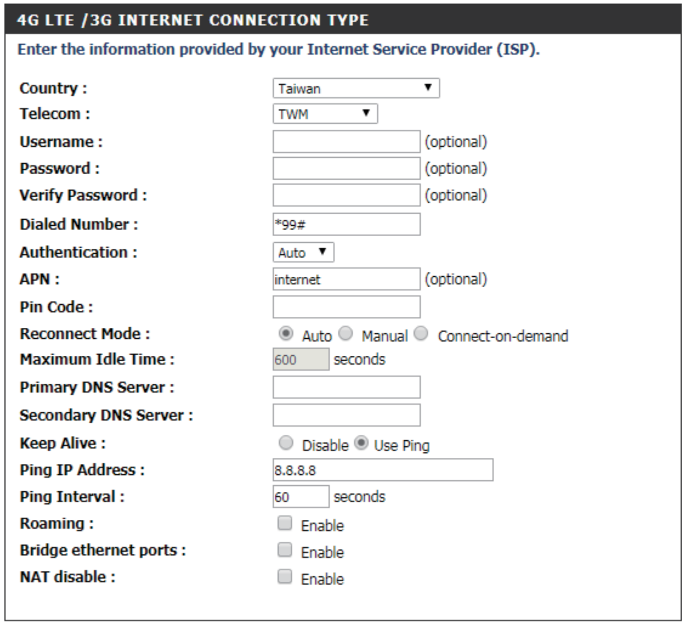
Primary DNS Server: Fill in if provided by your ISP. If not, keep the default value (optional).

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

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

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

NAT disable: Activate this feature to disable NAT through this router. IP addresses will be directly assigned by your ISP.



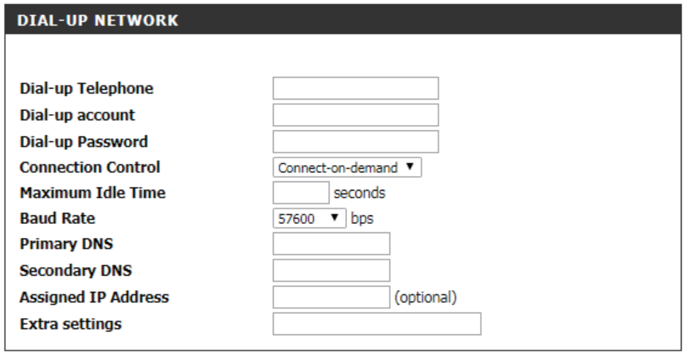
4G LTE /3G INTERNET CONNECTION TYPE

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

Country :	Taiwan ▼
Telecom :	TWM ▼
Username :	(optional)
Password :	(optional)
Verify Password :	(optional)
Dialed Number :	*99#
Authentication :	Auto ▼
APN :	internet (optional)
Pin Code :	
Reconnect Mode :	● Auto ○ Manual ○ Connect-on-demand
Maximum Idle Time :	600 seconds
Primary DNS Server :	
Secondary DNS Server :	
Keep Alive :	○ Disable ● Use Ping
Ping IP Address :	8.8.8.8
Ping Interval :	60 seconds
Roaming :	□ Enable
Bridge ethernet ports :	□ Enable
NAT disable :	□ Enable

Dial-Up Settings

Choose this setting to connect via an external dial-up modem via the serial port on the back of the router.



DIAL-UP NETWORK

Dial-up Telephone	
Dial-up account	
Dial-up Password	
Connection Control	Connect-on-demand ▼
Maximum Idle Time	seconds
Baud Rate	57600 ▼ bps
Primary DNS	
Secondary DNS	
Assigned IP Address	(optional)
Extra settings	

Dial-up Telephone: Enter the phone number to be dialed for the dial-up connection.

Dial-up account: Enter the username for the dial-up account.

Dial-up Password: Enter the password for the dial-up accounts:

Connection Control: Specify the circumstances where the router will attempt to connect. Choose **Connect-on-demand**, **Always-on** or **Manually.**

Maximum Idle Time: Enter the maximum idle time in seconds before the connection will be terminated.

Baud Rate: This specified the baud rate of the serial port. Actual dial-up connection speeds are determined by the external modem, ISP, and network conditions.

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

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

Assigned IP Address: Fill in only if requested by ISP (optional).

Extra settings: Enter any additional settings or modem commands here.

GRE Settings

This page allows you to set up GRE tunnels and view information about the amount of data transmitted and received. Generic Routing Encapsulation (GRE) is an IP packet encapsulation protocol used when IP packets must be sent from one network to another. Click **Save Settings** to apply changes.

Name: Choose a name for the GRE tunnel.

Tunnel IP: Enter the IP address for the tunnel.

Peer IP: Enter a Peer IP for the tunnel.

Key: Define a key.

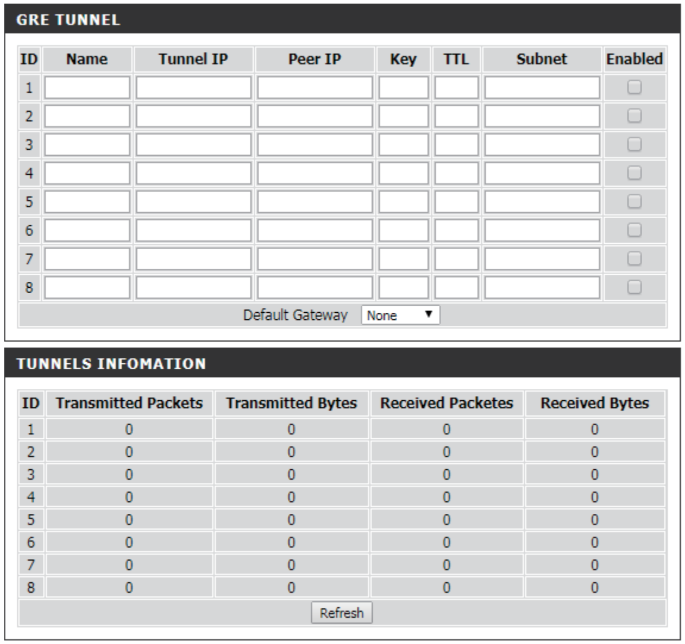
TTL: Set the time to live (TTL) or lifespan in seconds for the GRE tunnel.

Subnet: Enter the subnet address.

Enable: Tick this box to enable the individual GRE tunneling rule.

Default Gateway: Choose a gateway from the drop-down menu (if any).

Refresh: Update the information on current GRE tunnels.



GRE TUNNEL

ID	Name	Tunnel IP	Peer IP	Key	TTL	Subnet	Enabled
1							□
2							□
3							□
4							□
5							□
6							□
7							□
8							□

Default Gateway: None ▾

TUNNELS INFOMATION

ID	Transmitted Packets	Transmitted Bytes	Received Packetes	Received Bytes
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

Wireless Settings

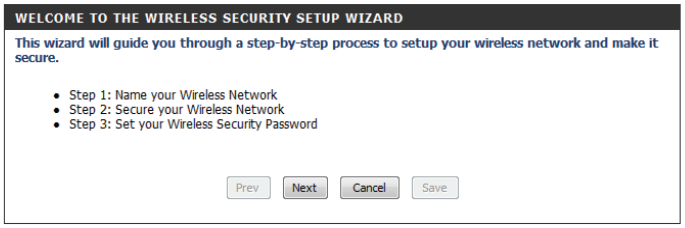
Wireless Connection Setup Wizard

This section will help you to manually configure the wireless settings of your router. Please note that changes made in this section may also need to be duplicated on your wireless devices and clients. The Wireless Settings page allows you to configure how your router connects to the Internet. There are several ways to set up your wireless connection. You can click on the **Wireless Connection Setup Wizard** button to start a wizard that will guide you through setting up your wireless settings. If you want to manually configure your settings, click the **Manual Wireless Connection Setup** button and skip to “Manual Wireless Connection Setup” on page 31. You can also set up a wireless connection to a device automatically or configure your router automatically through Windows by clicking the **Wi-Fi Protected Setup** button. This is described in “Add Wireless Device with WPS” on page 30.

This wizard will guide you through a step-by-step process to configure your router’s wireless settings.

Click **Next** to continue.

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

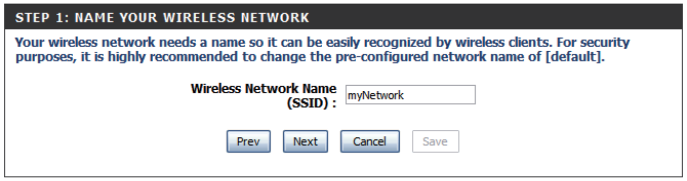


WELCOME TO THE WIRELESS SECURITY SETUP WIZARD

This wizard will guide you through a step-by-step process to setup your wireless network and make it secure.

- Step 1: Name your Wireless Network
- Step 2: Secure your Wireless Network
- Step 3: Set your Wireless Security Password

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

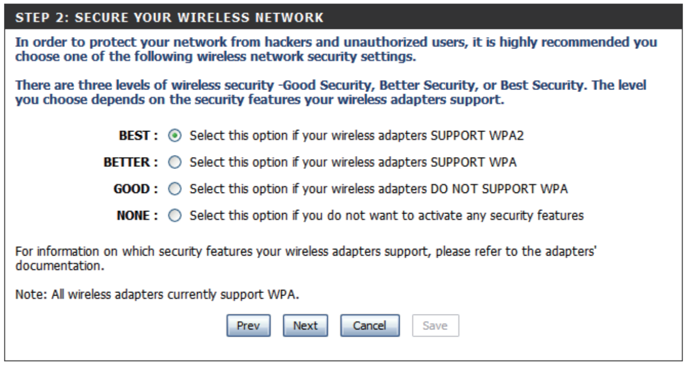


STEP 1: NAME YOUR WIRELESS NETWORK

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

Wireless Network Name (SSID) : myNetwork

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



STEP 2: SECURE YOUR WIRELESS NETWORK

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

There are three levels of wireless security -Good Security, Better Security, or Best Security. The level you choose depends on the security features your wireless adapters support.

BEST : ● Select this option if your wireless adapters SUPPORT WPA2

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

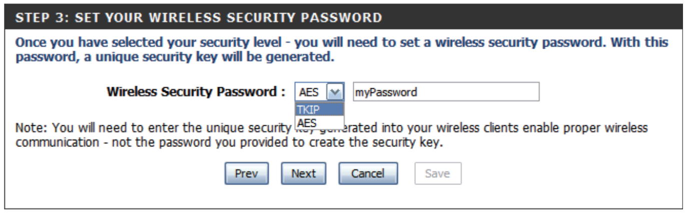
GOOD : ○ Select this option if your wireless adapters DO NOT SUPPORT WPA

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

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

Note: All wireless adapters currently support WPA.

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

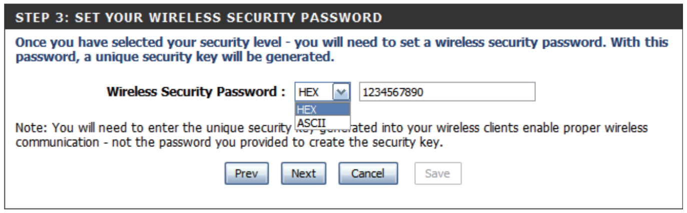

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password : AES myPassword

Note: You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

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

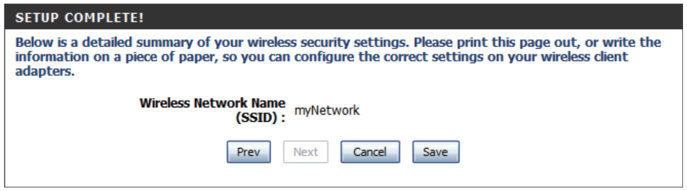

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

Once you have selected your security level - you will need to set a wireless security password. With this password, a unique security key will be generated.

Wireless Security Password : HEX 1234567890

Note: You will need to enter the unique security key generated into your wireless clients enable proper wireless communication - not the password you provided to create the security key.

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

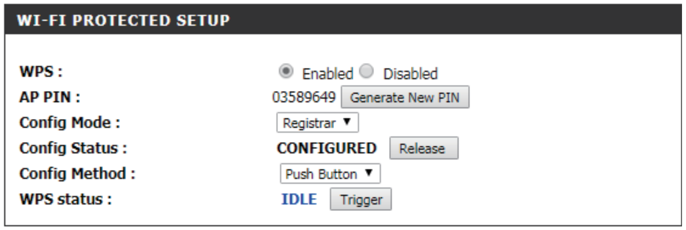

SETUP COMPLETE!

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

Wireless Network Name (SSID) : myNetwork

Add Wireless Device with WPS

Wi-Fi Protected Setup (WPS) is a simplified method for securing your wireless network during the initial setup as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across various products as well as manufacturers. The process is as easy as pressing a button for the Push-button method or entering the 8-digit code for the PIN method. Using WPS gets you connected quickly and easily, with the most secure wireless encryption method, WPA2.



WI-FI PROTECTED SETUP

WPS : ● Enabled ○ Disabled

AP PIN : 03589649

Config Mode : Registrar

Config Status : CONFIGURED

Config Method : Push Button

WPS status : IDLE

WPS: Enable the Wi-Fi Protected Setup feature.

AP PIN: A PIN is a unique number that can be used to add the router to an existing network or to create a new network. Pushing this button will generate a new, random PIN.

Config Mode: Choose either **Enrollee** or **Registrar** from the drop-down menu.

Config Status: Press **Set** to switch between **Configured** and **Unconfigured** states.

Disable WPS-PIN Method: Tick this box to use the Push Button method only.

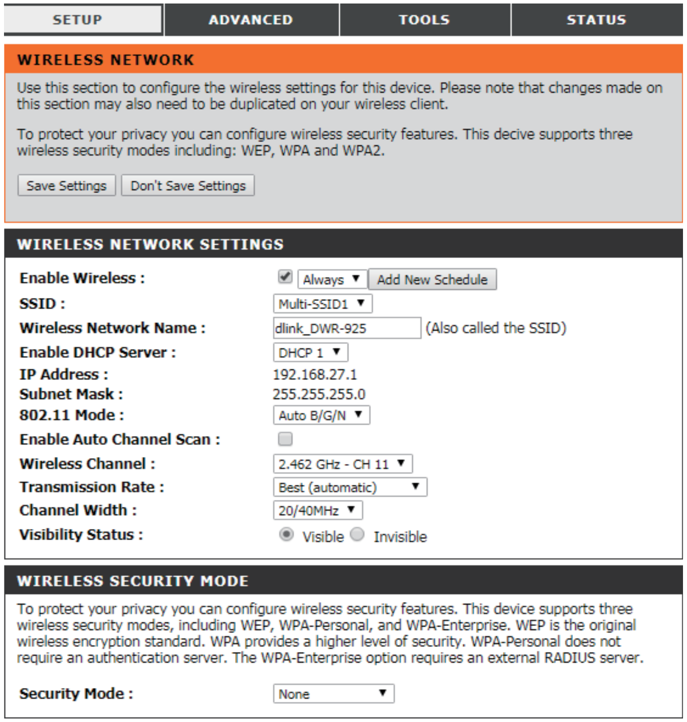
Config Method: Select **Push Button** or **PIN** method from the drop-down menu. For the Push Button method, to add a wireless client simply push the WPS button on the device and click **Trigger**. In order to use the PIN method, you must know the wireless client’s 8 digit PIN and click **Trigger**.

Note: Once you click **Trigger**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

WPS Status: Indicates whether WPS is **In Use** or **Not In Use**. The **Trigger** button will activate WPS for up to 120 seconds.

Manual Wireless Connection Setup

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



WIRELESS NETWORK

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

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

WIRELESS NETWORK SETTINGS

Enable Wireless :	☑ Always ▼
SSID :	Multi-SSID1 ▼
Wireless Network Name :	dlink_DWR-925 (Also called the SSID)
Enable DHCP Server :	DHCP 1 ▼
IP Address :	192.168.27.1
Subnet Mask :	255.255.255.0
802.11 Mode :	Auto B/G/N ▼
Enable Auto Channel Scan :	□
Wireless Channel :	2.462 GHz - CH 11 ▼
Transmission Rate :	Best (automatic) ▼
Channel Width :	20/40MHz ▼
Visibility Status :	● Visible ○ Invisible

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : None ▼

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

SSID: The multiple SSID feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network. They can be configured independently. To configure your second SSID, select Multi-SSID2

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

802.11 Mode: **B/G mixed:** Enable this mode if your network contains a mix of 802.11b and 802.11g devices.
N only: Enable this mode if your network only has 802.11n devices.
B/G/N mixed: Enable this mode if you have a mix of 802.11n, 802.11g, and 802.11b clients.

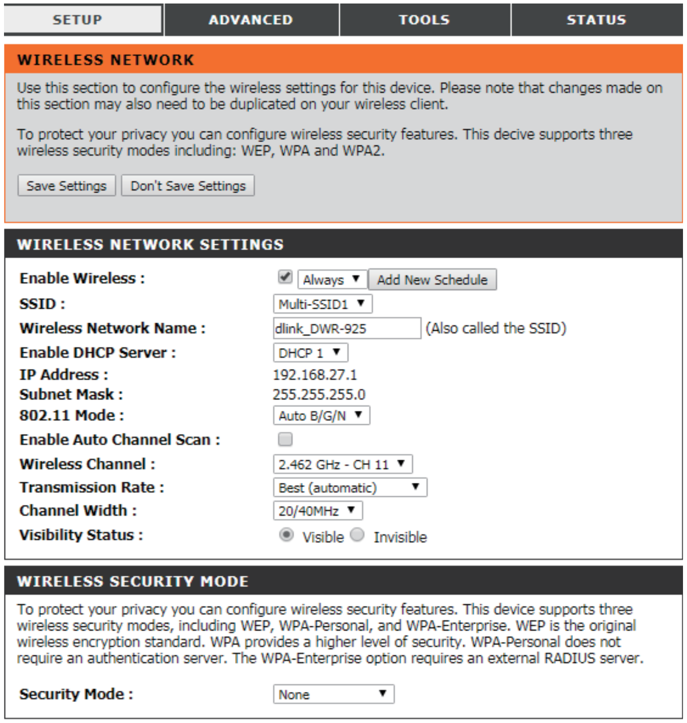
Auto Channel Scan: Enabling this feature will allow the router to automatically scan for the best wireless channel to use.

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

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

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

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



WIRELESS NETWORK

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

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

WIRELESS NETWORK SETTINGS

Enable Wireless :	☑ Always ▼
SSID :	Multi-SSID1 ▼
Wireless Network Name :	dlink_DWR-925 (Also called the SSID)
Enable DHCP Server :	DHCP 1 ▼
IP Address :	192.168.27.1
Subnet Mask :	255.255.255.0
802.11 Mode :	Auto B/G/N ▼
Enable Auto Channel Scan :	☐
Wireless Channel :	2.462 GHz - CH 11 ▼
Transmission Rate :	Best (automatic) ▼
Channel Width :	20/40MHz ▼
Visibility Status :	● Visible ○ Invisible

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : None ▼

WEP

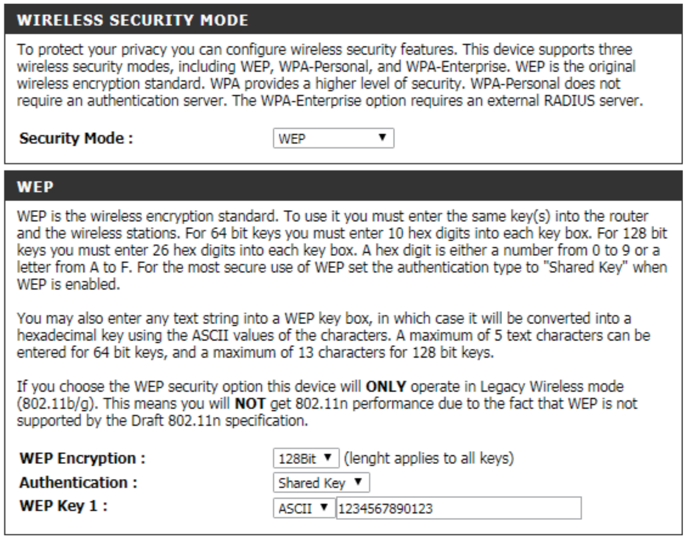
WEP Encryption: Select whether to use **64-bit** or **128-bit** encryption.

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

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

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

***Note:** For the best protection, it is strongly advised to select **WPA-Personal** or **WPA-Enterprise** and then select **WPA2 Only** if your clients support it. WEP is a legacy standard with known vulnerabilities and is included for compatibility purposes only. Use strong passwords and the latest encryption wherever possible to encrypt your wireless traffic.*



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WEP ▼

WEP

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

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

If you choose the WEP security option this device will **ONLY** operate in Legacy Wireless mode (802.11b/g). This means you will **NOT** get 802.11n performance due to the fact that WEP is not supported by the Draft 802.11n specification.

WEP Encryption : 128Bit ▼ (lenght applies to all keys)
Authentication : Shared Key ▼
WEP Key 1 : ASCII ▼ 1234567890123

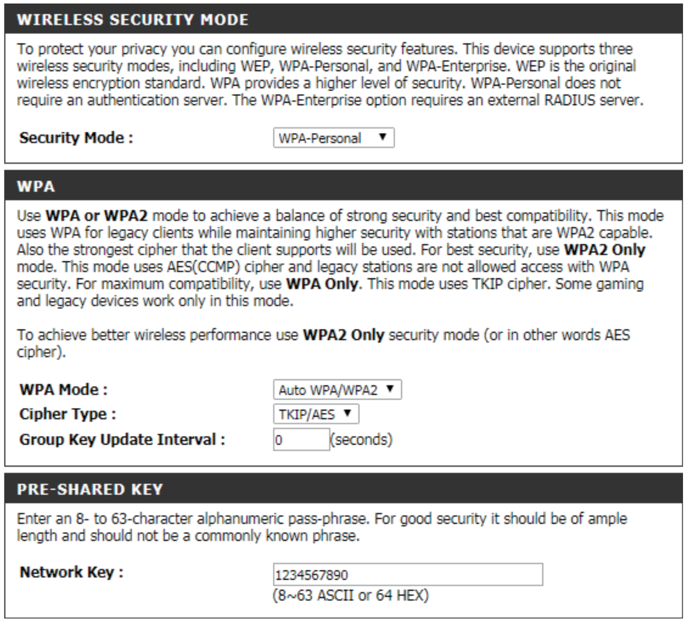
WPA-Personal

WPA Mode: Select whether to use **Auto WPA/WPA2**, **WPA2 only,** or **WPA only**. **WPA2 only** is the strongest encryption, provided that all of your clients can support it.

Cipher Type: Select whether to use the **TKIP/AES**, **TKIP**, or **AES** cipher. The **AES** cipher is the strongest encryption, provided that all of your clients can support it.

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

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



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal ▼

WPA

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

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

WPA Mode : Auto WPA/WPA2 ▼

Cipher Type : TKIP/AES ▼

Group Key Update Interval : 0 (seconds)

PRE-SHARED KEY

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

Network Key : 1234567890
(8~63 ASCII or 64 HEX)

WPA-Enterprise

WPA Mode: Select whether to use **Auto WPA/WPA2**, **WPA2 only,** or **WPA only**. **WPA2 only** is the strongest encryption, provided that all of your clients can support it.

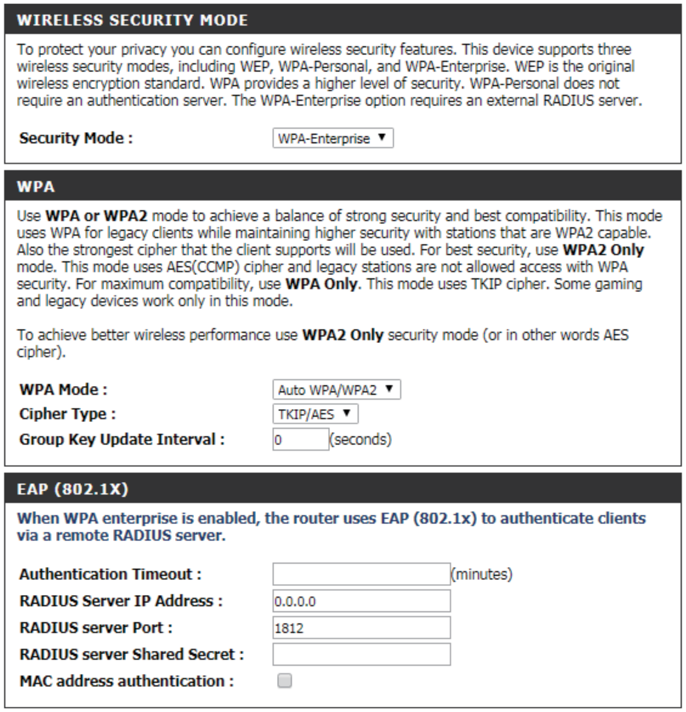
Cipher Type: Select whether to use the **TKIP/AES**, **TKIP,** or **AES** cipher. The **AES** cipher is the most secure, provided that all of your clients can support it.

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

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

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

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



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Enterprise ▼

WPA

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

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

WPA Mode :	Auto WPA/WPA2 ▼
Cipher Type :	TKIP/AES ▼
Group Key Update Interval :	0 (seconds)

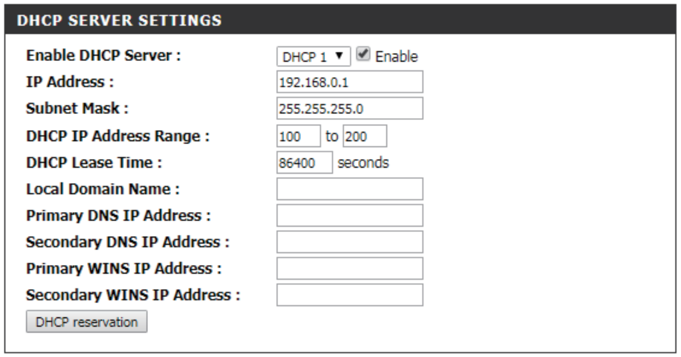
EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout :	(minutes)
RADIUS Server IP Address :	0.0.0.0
RADIUS server Port :	1812
RADIUS server Shared Secret :	
MAC address authentication :	□

Network Settings

The DWR-925 has a built-in DHCP (Dynamic Host Control Protocol) server. The DHCP server assigns IP addresses to devices on the network that request them. By default, the DHCP server is enabled on the device. The DHCP address pool contains a range of IP addresses, which are automatically assigned to the clients on the network. The DWR-925 supports up to 4 DHCP servers. After modifying any settings, click **Save Settings** to save your changes.



DHCP SERVER SETTINGS

Enable DHCP Server :	DHCP 1 ▼ ☑ Enable
IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
DHCP IP Address Range :	100 to 200
DHCP Lease Time :	86400 seconds
Local Domain Name :	
Primary DNS IP Address :	
Secondary DNS IP Address :	
Primary WINS IP Address :	
Secondary WINS IP Address :	

Enable DHCP Server: The DWR-925 supports up to 4 DHCP servers. Select a server, then select the box to enable the DHCP server. By default, only one is enabled.

IP Address: Enter the IP address of the router on each DHCP. The default IP address is **192.168.0.1** for DHCP 1.

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

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

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

Local Domain Name: Enter the local domain name (optional). Only available on DHCP 1.

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

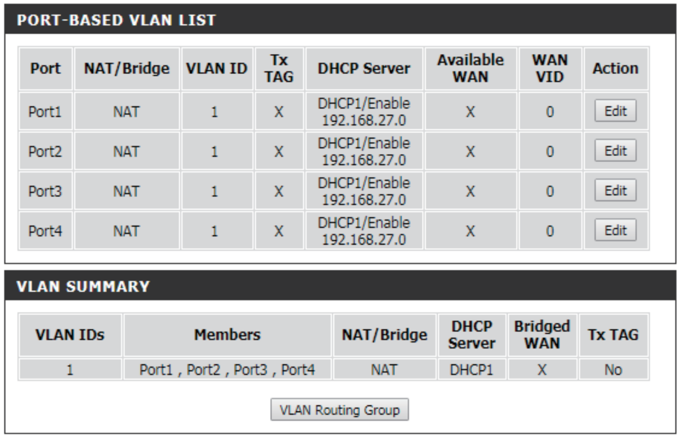
Secondary DNS IP Address: Enter the secondary DNS IP address that will be assigned to DHCP clients.

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

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

VLAN

A virtual LAN (VLAN) allows the partitioning of a single network into multiple virtual ones. While all traffic occurs within the same physical broadcast domains (Ethernet, Wi-Fi, etc.), by tagging each packet as part of a different VLAN, they can function as though they were on separate networks. On the DWR-925, local VLANs 1-4 are bound to DHCP servers 1-4. Alternatively, for non-NAT (Bridging) modes, WAN VIDs can be used.



PORT-BASED VLAN LIST

Port	NAT/Bridge	VLAN ID	Tx TAG	DHCP Server	Available WAN	WAN VID	Action
Port1	NAT	1	X	DHCP1/Enable 192.168.27.0	X	0	Edit
Port2	NAT	1	X	DHCP1/Enable 192.168.27.0	X	0	Edit
Port3	NAT	1	X	DHCP1/Enable 192.168.27.0	X	0	Edit
Port4	NAT	1	X	DHCP1/Enable 192.168.27.0	X	0	Edit

VLAN SUMMARY

VLAN IDs	Members	NAT/Bridge	DHCP Server	Bridged WAN	Tx TAG
1	Port1 , Port2 , Port3 , Port4	NAT	DHCP1	X	No

Port: Indicates the physical LAN port on the back of the device.

NAT/Bridge: Indicates whether the port is in **NAT** or **Bridge** mode. This can be changed by clicking **Edit**.

VLAN ID: Indicates the current **VLAN ID.** These correspond to DHCP servers 1-4

Tx TAG: Allows the adding of VLAN tags in bridging mode.

DHCP Server: Indicates the current DHCP server, status, and subnet. This can be changed when the port is in **NAT** mode by clicking edit.

Available WAN: When multiple WANs are enabled and the port is in Bridge mode, WANs can be bound to specific bridges here by clicking edit.

WAN VID: If a port is in Bridge mode, you can specify a WAN VID for bridging.

Action: Click **Edit** to edit the corresponding row.

VLAN Summary: This section lists all interfaces by VLAN.

VLAN Routing Group:

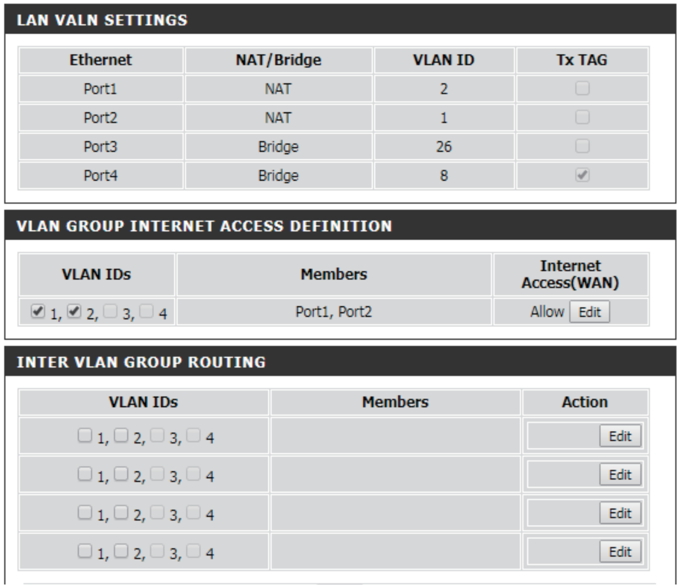
VLAN Routing Group

This page allows customization of advanced VLAN routes and grouping VLANs together to provide finer control of network access.

LAN VLAN Settings: This table indicates the VLAN Bridge, VLAN ID, and Tx TAG status of each Ethernet port.

VLAN Group Internet Access Definition: This section allows fine control of WAN access by VLAN ID. After clicking **Edit**, select the VLAN IDs to which to grant Internet/WAN access.

Inter VLAN Group Routing: This section allows VLANs to communicate with each other over LAN, while still being isolated from others or WAN. Click **Edit** to set up groups of VLANs that will be bridged. VLAN IDs can be listed more than once.



LAN VALN SETTINGS

Ethernet	NAT/Bridge	VLAN ID	Tx TAG
Port1	NAT	2	□
Port2	NAT	1	□
Port3	Bridge	26	□
Port4	Bridge	8	☑

VLAN GROUP INTERNET ACCESS DEFINITION

VLAN IDs	Members	Internet Access(WAN)
☑ 1, ☑ 2, □ 3, □ 4	Port1, Port2	Allow Edit

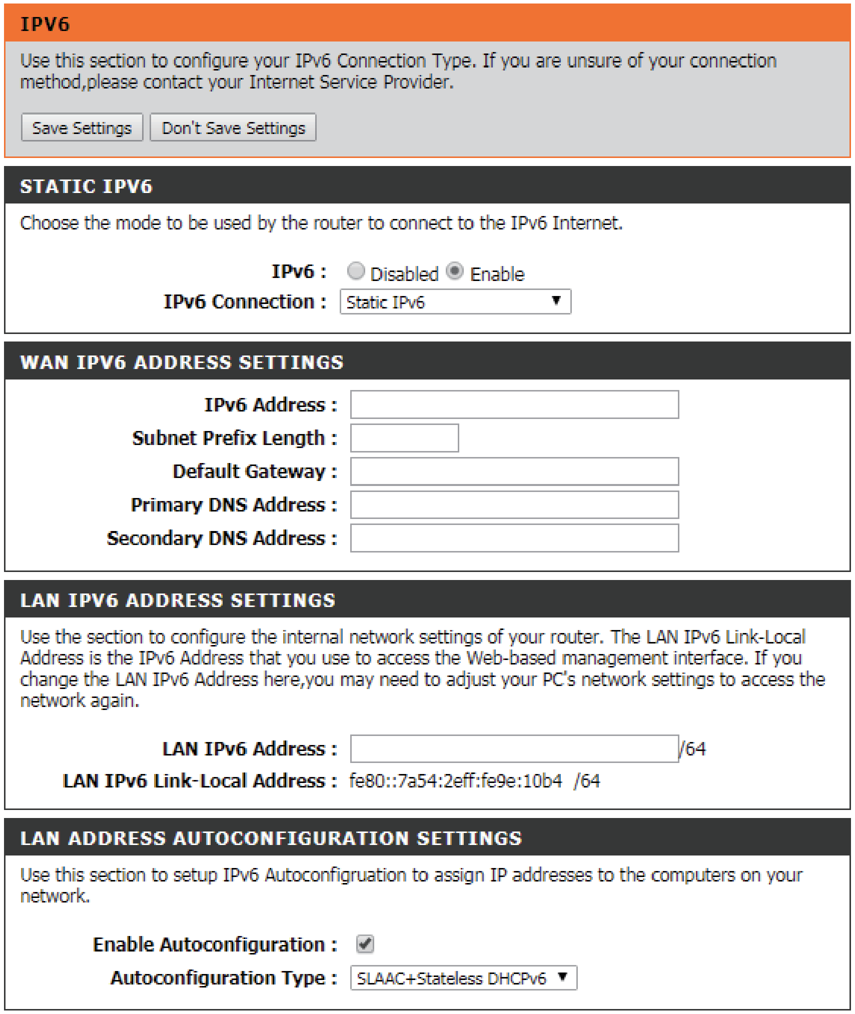
INTER VLAN GROUP ROUTING

VLAN IDs	Members	Action
□ 1, □ 2, □ 3, □ 4		Edit
□ 1, □ 2, □ 3, □ 4		Edit
□ 1, □ 2, □ 3, □ 4		Edit
□ 1, □ 2, □ 3, □ 4		Edit

IPv6 Setup

There are several IPv6 connection types to choose from: Static IPv6, LAN IPv6 Address, PPPoE, LAN IPv6 Link-Local, 6 to 4, 6rd, and Autoconfiguration. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider (ISP).

Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.



IPV6

Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method,please contact your Internet Service Provider.

STATIC IPV6

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ○ Disabled ● Enable
IPv6 Connection : Static IPv6 ▼

WAN IPV6 ADDRESS SETTINGS

IPv6 Address :
Subnet Prefix Length :
Default Gateway :
Primary DNS Address :
Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64
LAN IPv6 Link-Local Address : fe80::7a54:2eff:fe9e:10b4 /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfigruation to assign IP addresses to the computers on your network.

Enable Autoconfiguration : ☑
Autoconfiguration Type : SLAAC+Stateless DHCPv6 ▼

Static IPv6

IPv6: Select to **Enable** IPv6 tunneling.

IPv6 Connection: Select **Static IPv6** from the drop-down menu.

IPv6 Address: Enter the WAN Static IPv6 address here.

Subnet Prefix Length: Enter the WAN subnet prefix length here.

Default Gateway: Enter the default gateway.

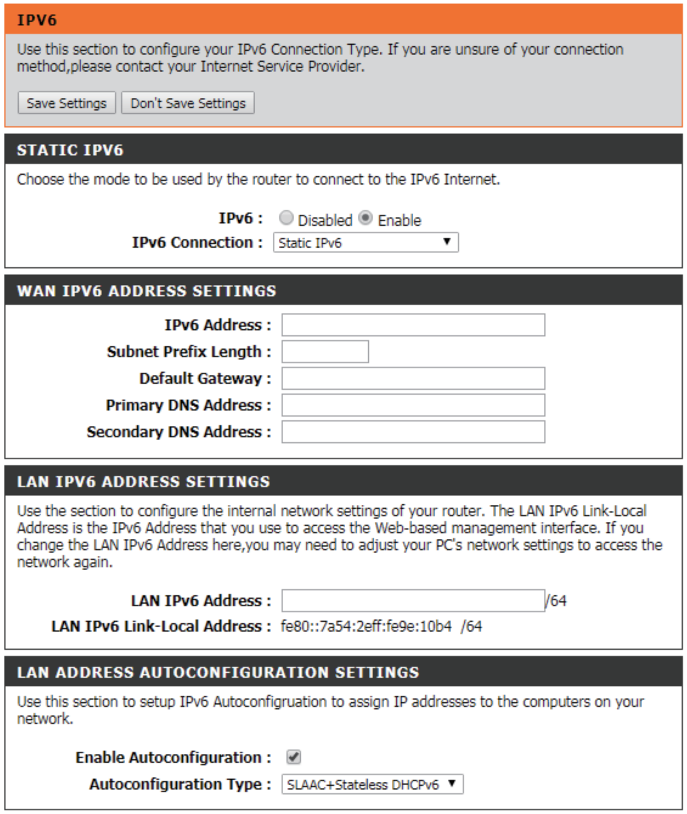
Primary/Secondary DNS Addresses: Enter the primary and secondary DNS addresses here.

LAN IPv6 Address: Enter the LAN IPv6 address.

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

Enable Autoconfiguration: Check to enable the autoconfiguration feature.

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



IPV6

Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method,please contact your Internet Service Provider.

STATIC IPV6

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ○ Disabled ● Enable
IPv6 Connection : Static IPv6

WAN IPV6 ADDRESS SETTINGS

IPv6 Address :
Subnet Prefix Length :
Default Gateway :
Primary DNS Address :
Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

LAN IPv6 Address : /64
LAN IPv6 Link-Local Address : fe80::7a54:2eff:fe9e:10b4 /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfigruation to assign IP addresses to the computers on your network.

Enable Autoconfiguration : ☑
Autoconfiguration Type : SLAAC+Stateless DHCPv6

Autoconfiguration

IPv6: Tick to **Enable** IPv6 tunneling.

IPv6 Connection: Select **Autoconfiguration Type** from the drop-down menu.

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

Primary/Secondary DNS Addresses: Enter the primary and secondary DNS addresses here.

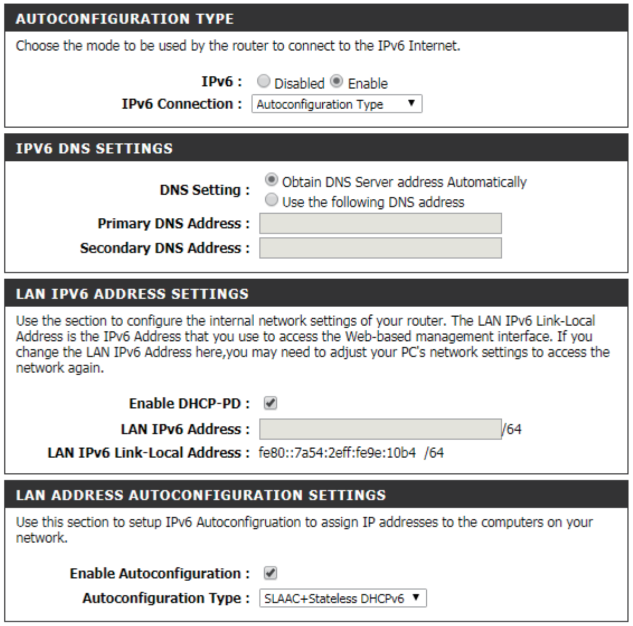
Enable DHCP-PD: Check to enable DHCP-PD.

LAN IPv6 Address: Enter the LAN IPv6 address.

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-local address.

Enable Autoconfiguration: Check to enable the autoconfiguration feature.

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



AUTOCONFIGURATION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ○ Disabled ● Enable

IPv6 Connection : Autoconfiguration Type ▼

IPV6 DNS SETTINGS

DNS Setting : ● Obtain DNS Server address Automatically ○ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::7a54:2eff:fe9e:10b4 /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfigruation to assign IP addresses to the computers on your network.

Enable Autoconfiguration : ☑

Autoconfiguration Type : SLAAC+Stateless DHCPv6 ▼

PPPoE

IPv6: Tick to **Enable** IPv6 tunneling.

IPv6 Connection: Select **PPPoE** from the drop-down menu.

Username: Enter the PPPoE Username provided by your ISP.

Password: Enter the password for your LAN IPv6.

Service Name: Enter the name of the service for reference.

MTU: You may need to change the Maximum Transmission Unit (MTU) for optimal performance.

Primary/Secondary DNS Addresses: Enter the primary and secondary DNS addresses here.

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

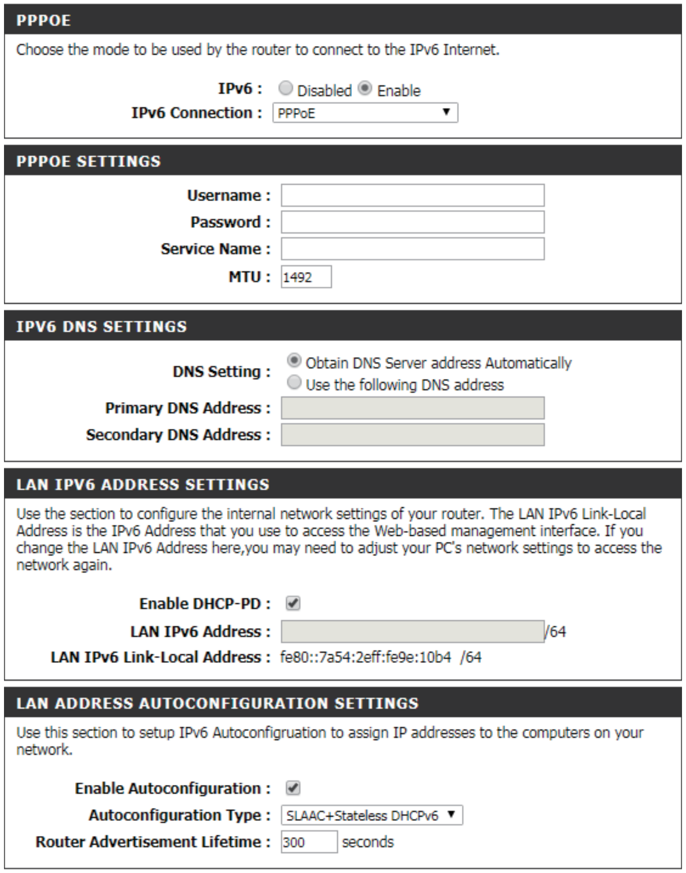
LAN IPv6 Address: Enter the LAN IPv6 address.

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-local address.

Enable Autoconfiguration: Check to enable the autoconfiguration feature.

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

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



PPPOE

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ○ Disabled ● Enable

IPv6 Connection : PPPoE ▼

PPPOE SETTINGS

Username :

Password :

Service Name :

MTU : 1492

IPV6 DNS SETTINGS

DNS Setting : ● Obtain DNS Server address Automatically ○ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::7a54:2eff:fe9e:10b4 /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfigruation to assign IP addresses to the computers on your network.

Enable Autoconfiguration : ☑

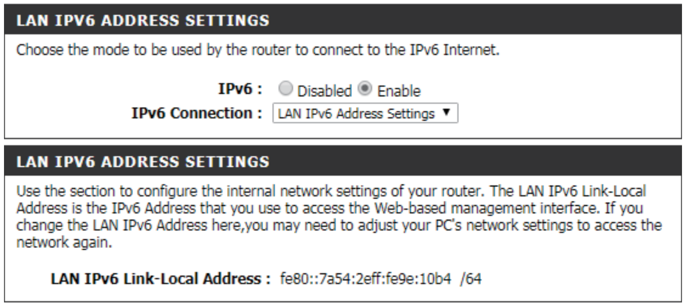
Autoconfiguration Type : SLAAC+Stateless DHCPv6 ▼

Router Advertisement Lifetime : 300 seconds

LAN IPv6 Address Settings

IPv6: Select **Enable** to enable IPv6 over LAN, otherwise select **Disable.**

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-local address.



LAN IPV6 ADDRESS SETTINGS

Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ○ Disabled ● Enable

IPv6 Connection : LAN IPv6 Address Settings ▼

LAN IPV6 ADDRESS SETTINGS

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here,you may need to adjust your PC's network settings to access the network again.

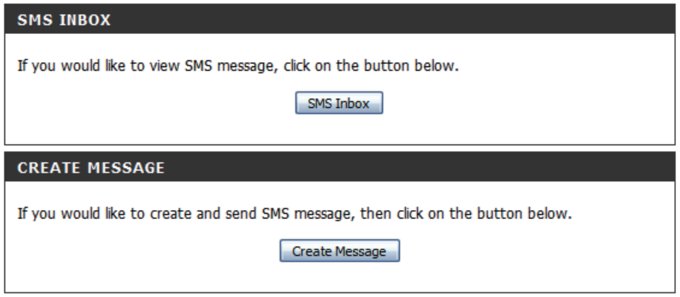
LAN IPv6 Link-Local Address : fe80::7a54:2eff:fe9e:10b4 /64

Message Service

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

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

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



SMS INBOX

If you would like to view SMS message, click on the button below.

CREATE MESSAGE

If you would like to create and send SMS message, then click on the button below.

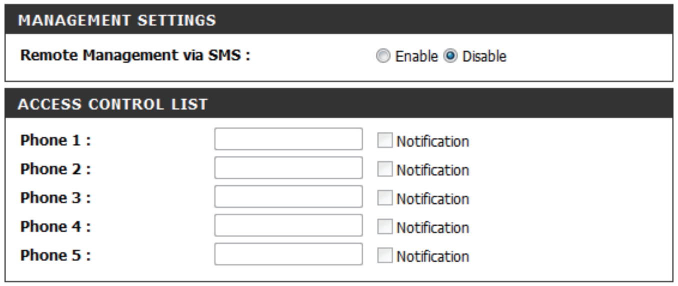
SMS Notification

This page enables or disables notification management via SMS as well as sets the phones that will receive notifications. Click the **Save Settings** to update your settings.

Notification Management via SMS: Enable or disable notification management via SMS.

Access Control List: Enter phone numbers from which notification controls will be granted. Check **Notification** to send those numbers notifications.

Note: This mechanism does not prevent caller ID spoof. Use with caution.



MANAGEMENT SETTINGS

Remote Management via SMS : ○ Enable ● Disable

ACCESS CONTROL LIST

Phone 1 :		□ Notification
Phone 2 :		□ Notification
Phone 3 :		□ Notification
Phone 4 :		□ Notification
Phone 5 :		□ Notification

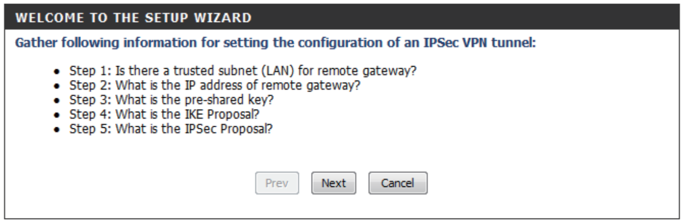
VPN Settings

VPN Setup Wizard

The DWR-925 allows you to set up VPN using the automated **VPN Setup Wizard** or using **Manual VPN Setup**. VPN settings are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication, and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

This window explains the steps you will be guided through to set up an IPsec VPN tunnel.

Click **Next** to continue.



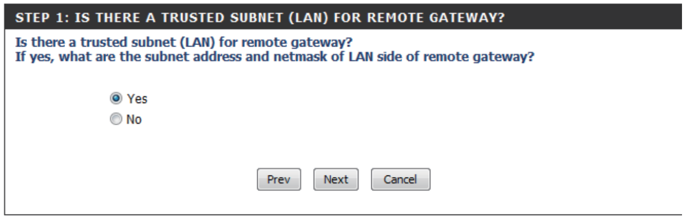
WELCOME TO THE SETUP WIZARD

Gather following information for setting the configuration of an IPSec VPN tunnel:

- Step 1: Is there a trusted subnet (LAN) for remote gateway?
- Step 2: What is the IP address of remote gateway?
- Step 3: What is the pre-shared key?
- Step 4: What is the IKE Proposal?
- Step 5: What is the IPSec Proposal?

If there is a trusted subnet for the remote gateway, select **Yes**, otherwise choose **No**.

Click **Next** to continue.



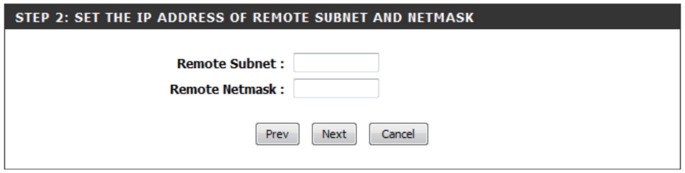
STEP 1: IS THERE A TRUSTED SUBNET (LAN) FOR REMOTE GATEWAY?

Is there a trusted subnet (LAN) for remote gateway?
If yes, what are the subnet address and netmask of LAN side of remote gateway?

● Yes
○ No

If you chose **Yes,** you will now need to enter the **Remote Subnet** and **Remote Netmask**.

Click **Next** to continue.

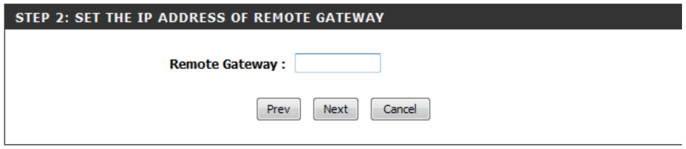


STEP 2: SET THE IP ADDRESS OF REMOTE SUBNET AND NETMASK

Remote Subnet :
Remote Netmask :

Enter the **Remote Gateway** address.

Click **Next** to continue.

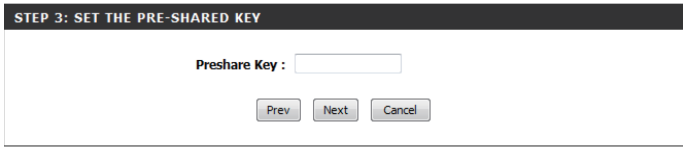


STEP 2: SET THE IP ADDRESS OF REMOTE GATEWAY

Remote Gateway :

Set your **Preshared Key**.

Click **Next** to continue.

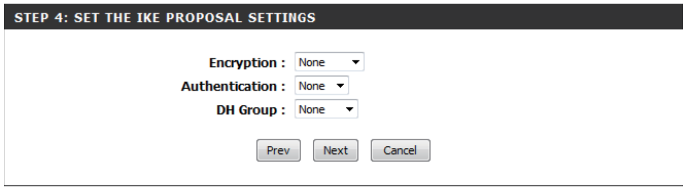


STEP 3: SET THE PRE-SHARED KEY

Preshare Key :

Set your IKE Proposal Settings by choosing your **Encryption**, **Authentication**, and **DH Group** settings from the drop-down menus.

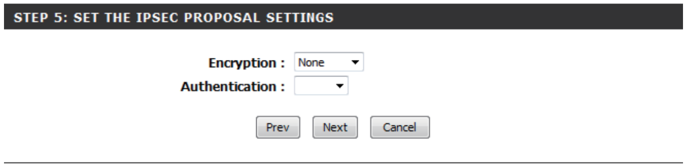
Click **Next** to continue.



STEP 4: SET THE IKE PROPOSAL SETTINGS

Encryption : None
Authentication : None
DH Group : None

Set the type of encryption and authentication of your IPsec proposal settings and click **Next.**

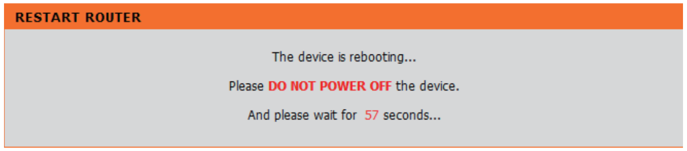


STEP 5: SET THE IPSEC PROPOSAL SETTINGS

Encryption : None
Authentication :

When setup is completed, the name and security details will be displayed and the router will reboot.

Click **Save** to finish.



RESTART ROUTER

The device is rebooting...

Please DO NOT POWER OFF the device.

And please wait for 57 seconds...

Manual VPN Setup

This section will help you create and configure your **VPN** settings. The router supports IPsec as the server endpoint. IPsec (Internet Protocol Security) is a set of protocols defined by the IETF (Internet Engineering Task Force) to provide IP security at the network layer.

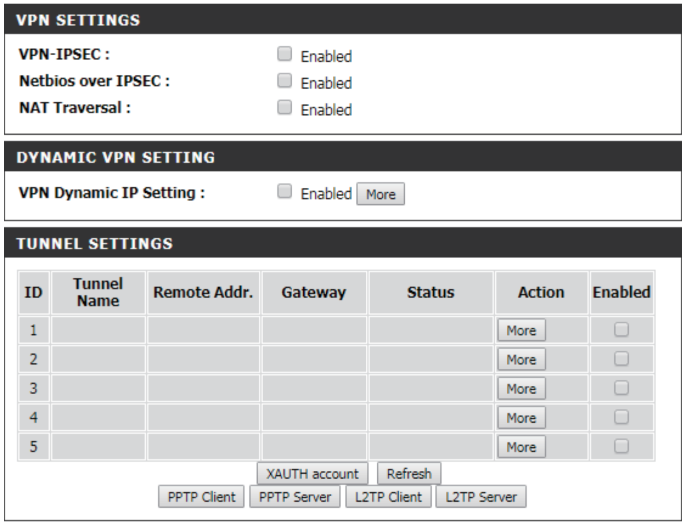
VPN-IPSEC: Tick this box to enable IPsec VPN function.

Netbios over IPSEC: Tick this box to receive Netbios from Network Neighborhood.

NAT Traversal: Some NAT routers will block IPsec packets if it doesn't support IPsec pass-through. If you connect to another NAT router which doesn't support IPsec pass-through on the WAN side, you need to activate this option.

VPN Dynamic IP Setting: Tick this box to enable this features and click **More** to configure VPN Dynamic IP on a separate page. Please see the next page for more details.

Tunnel Settings: Tunnel details are displayed here. Click **More** to configure a new tunnel or click **Disconnect** to disconnect from an existing tunnel. Select the **Enable** checkbox to activate this rule.
In the tunnel settings page, you can click **More** under Action for detailed tunnel settings.
XAUTH account: select it to store XAUTH account information such as user name and password.
PPTP Client / **PPTP Server**: DWR-925 can act as either client or server under PPTP, click it to configure this setting.
L2TP Client / **L2TP Server**: DWR-925 can act as either client or server under L2TP, click it to configure this setting.
Click **Refresh** to view your current settings.



VPN SETTINGS

VPN-IPSEC : □ Enabled
Netbios over IPSEC : □ Enabled
NAT Traversal : □ Enabled

DYNAMIC VPN SETTING

VPN Dynamic IP Setting : □ Enabled More

TUNNEL SETTINGS

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enabled
1					More	□
2					More	□
3					More	□
4					More	□
5					More	□

VPN Dynamic IP

Tunnel Name: Enter a name for your VPN.

Interface: Select a WAN interface over which the VPN will operate.

Local Subnet/Netmask: Enter the local (LAN) subnet and mask. (ex. 192.168.0.0/24)

Phase1/2 Key Life Time: Enter the amount of time in seconds that the Phase 1 and Phase 2 keys should last.

Encapsulation Protocol: Choose either **ESP**, **AH** or **ESP + AH** from the drop-down menu.

PFS Group: **Enable** or **Disable** the PFS Group option using the drop-down menu. PFS is an additional security protocol.

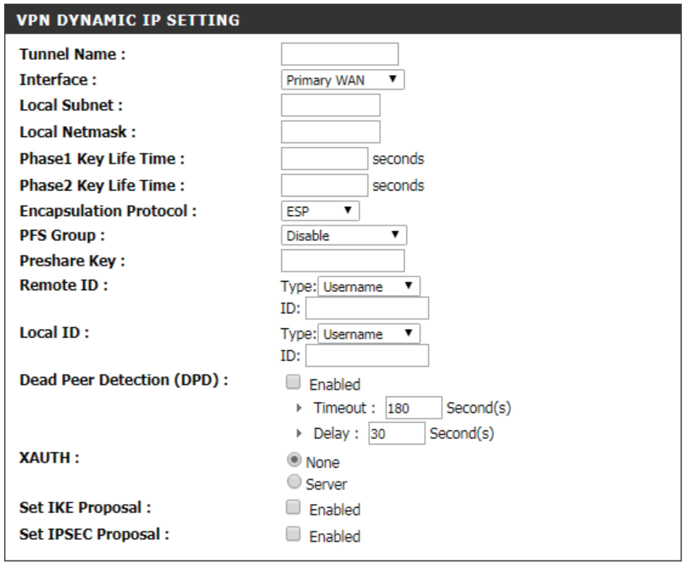
Preshare Key: Manually enter an ASCII passphrase in the box.

Remote ID: Choose from **Username**, **FQDN**, **User@FQDN**, or **Key ID** using the drop-down menu and then the ID in the box.

Local ID: Choose from **Username**, **FQDN**, **User@FQDN**, or **Key ID** using the drop-down menu and then the ID in the box.

Dead Peer Detection (DPD): Tick this box to enable Dead Peer Detection, then enter the time in seconds after which a peer is determined to be no longer active. You may also enter a delay period in seconds.

XAUTH: Tick this box to include additional username and password authentication requirements for the VPN. Select **Server** or **None**. Then enter the user name and password if required by the remote VPN server endpoint configured in xAuth Server Mode.

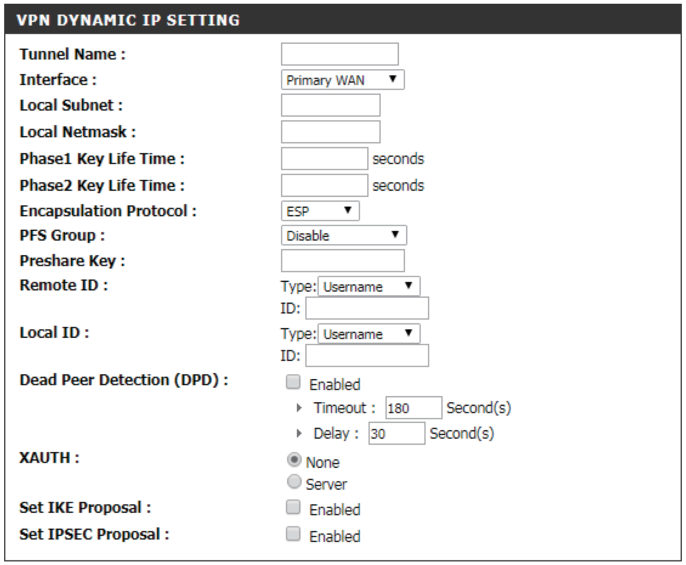


VPN DYNAMIC IP SETTING

Tunnel Name :	
Interface :	Primary WAN ▼
Local Subnet :	
Local Netmask :	
Phase1 Key Life Time :	seconds
Phase2 Key Life Time :	seconds
Encapsulation Protocol :	ESP ▼
PFS Group :	Disable ▼
Preshare Key :	
Remote ID :	Type: Username ▼ ID:
Local ID :	Type: Username ▼ ID:
Dead Peer Detection (DPD) :	□ Enabled Timeout : 180 Second(s) Delay : 30 Second(s)
XAUTH :	● None ○ Server
Set IKE Proposal :	□ Enabled
Set IPSEC Proposal :	□ Enabled

Set IKE Proposal: Tick this box to enable IKE Proposal.

Set IPSEC Proposal: Tick this box to enable IPsec Proposal.

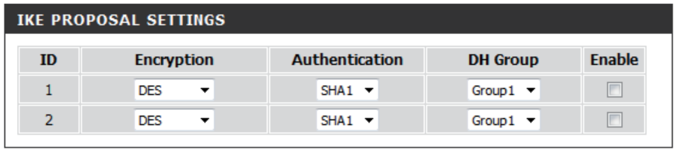


VPN DYNAMIC IP SETTING

Tunnel Name :	
Interface :	Primary WAN ▼
Local Subnet :	
Local Netmask :	
Phase1 Key Life Time :	seconds
Phase2 Key Life Time :	seconds
Encapsulation Protocol :	ESP ▼
PFS Group :	Disable ▼
Preshare Key :	
Remote ID :	Type: Username ▼ ID:
Local ID :	Type: Username ▼ ID:
Dead Peer Detection (DPD) :	□ Enabled Timeout : 180 Second(s) Delay : 30 Second(s)
XAUTH :	● None ○ Server
Set IKE Proposal :	□ Enabled
Set IPSEC Proposal :	□ Enabled

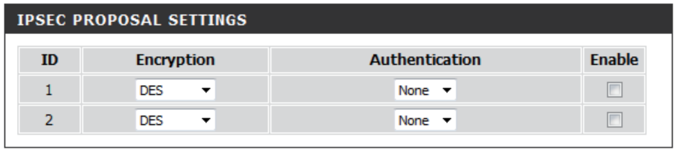
IKE Proposal Settings: Use this area to **Enable** IKE Proposals. Then determine the **Encryption** and **Authentication** types, as well as the **DH Group** from the drop-down menus.

IPSEC Proposal Settings: Use this area to **Enable** IPsec Proposals. Then determine the **Encryption** and **Authentication** types from the drop-down menus.



IKE PROPOSAL SETTINGS

ID	Encryption	Authentication	DH Group	Enable
1	DES ▼	SHA1 ▼	Group1 ▼	□
2	DES ▼	SHA1 ▼	Group1 ▼	□



IPSEC PROPOSAL SETTINGS

ID	Encryption	Authentication	Enable
1	DES ▼	None ▼	□
2	DES ▼	None ▼	□

Advanced

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. Click **Save Settings** to save your changes or click **Don't Save Settings** to discard your changes.

Well-known services: This contains a list of pre-defined services.

Copy to: Copies the rule to the line of the ID selected in the drop-down menu.

Use schedule rule: You may select **Always On** or choose the number of a schedule rule that you have defined.

VIRTUAL SERVERS LIST

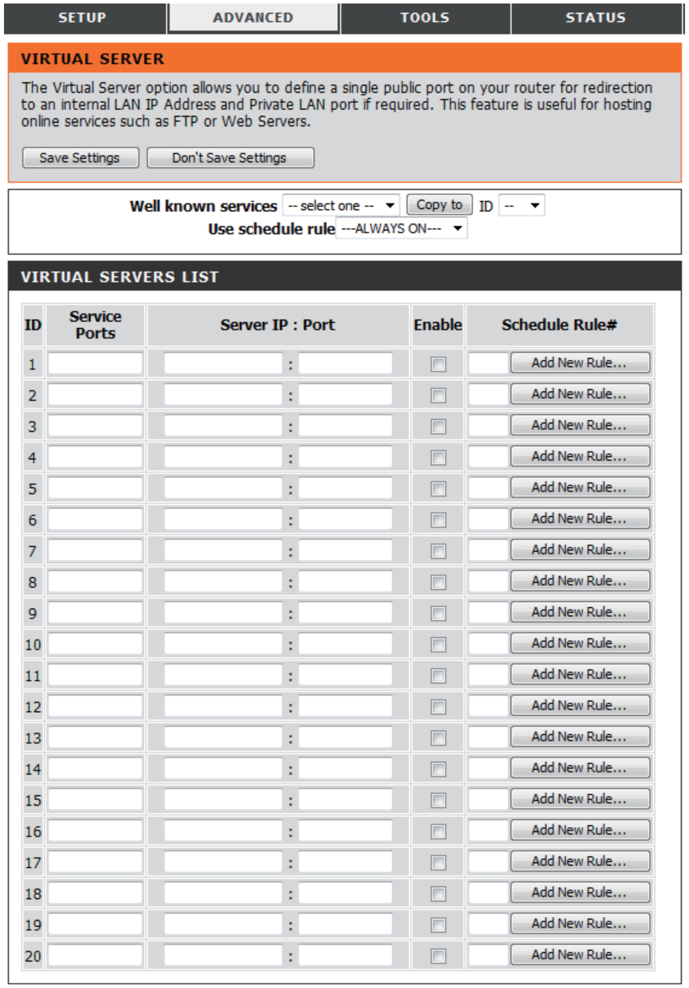
ID: This identifies the rule.

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

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

Enable: Tick the 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 72.



VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

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...
3		:	□	Add New Rule...
4		:	□	Add New Rule...
5		:	□	Add New Rule...
6		:	□	Add New Rule...
7		:	□	Add New Rule...
8		:	□	Add New Rule...
9		:	□	Add New Rule...
10		:	□	Add New Rule...
11		:	□	Add New Rule...
12		:	□	Add New Rule...
13		:	□	Add New Rule...
14		:	□	Add New Rule...
15		:	□	Add New Rule...
16		:	□	Add New Rule...
17		:	□	Add New Rule...
18		:	□	Add New Rule...
19		:	□	Add New Rule...
20		:	□	Add New Rule...

Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, and Internet telephony. These applications may have difficulty working through NAT (Network Address Translation). Application Rules allow some of these applications to work with the DWR-925 by opening ports after detecting traffic being sent through a trigger port. After modifying any settings, click **Save Settings** to save your changes.

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

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

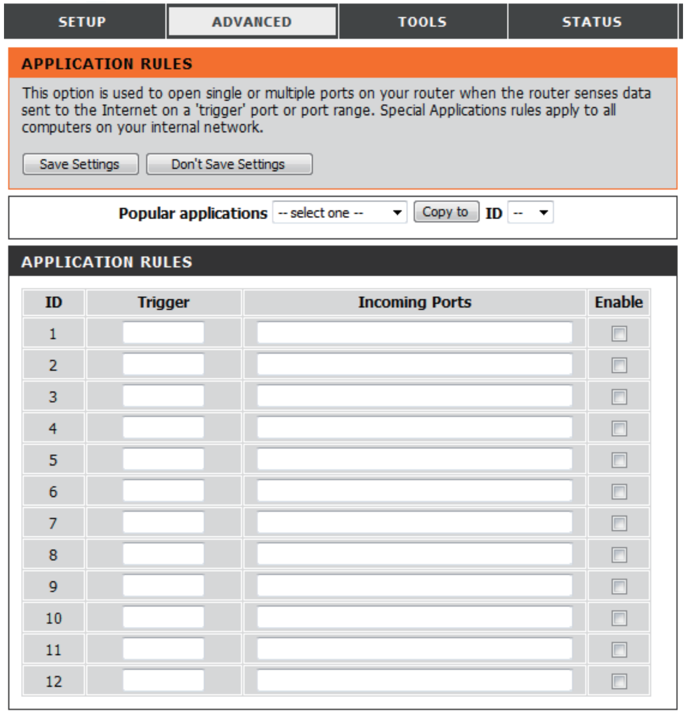
APPLICATION RULES

Trigger: This identifies the rule.

Incoming Ports: Enter the port to listen to in order to trigger the rule.

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

Tick the box to enable the specified rule.



APPLICATION RULES

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

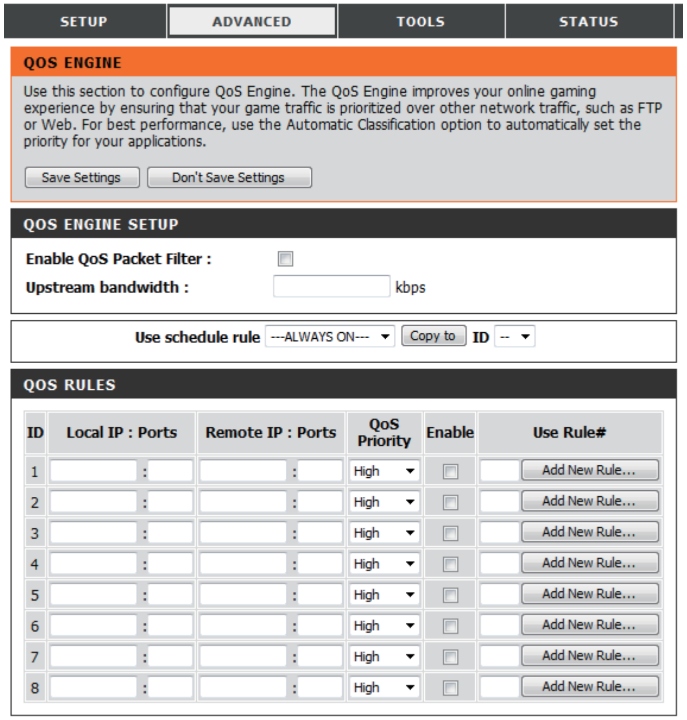
Popular applications: -- select one -- Copy to ID: --

APPLICATION RULES

ID	Trigger	Incoming Ports	Enable
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐
11			☐
12			☐

QoS Engine

The QoS engine improves your online gaming or streaming media experience by ensuring that your game or media traffic is prioritized over other network traffic, such as FTP or web. For best performance, use the Automatic Classification option to automatically set the priority for your applications. After modifying any settings, click **Save Settings** to save your changes.



QOS ENGINE

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

QOS ENGINE SETUP

Enable QoS Packet Filter : □

Upstream bandwidth : kbps

Use schedule rule ---ALWAYS ON--- Copy to 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...

QOS ENGINE SETUP

Enable QoS Packet Filter: Select this box to enable the QoS feature.

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

Use schedule rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 72.

QOS RULES

ID: This identifies the rule.

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

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

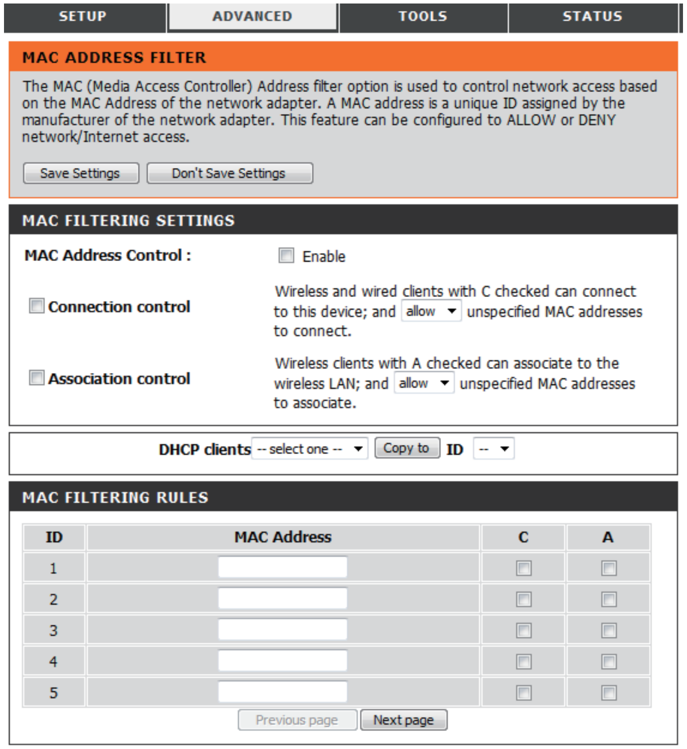
QoS Priority: Select what priority level to use for traffic affected by the rule: **Low, Normal, or High**.

Enable: Tick the 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 72.

MAC Address Filter

The MAC (Media Access Controller) address filter option is used to control network access based on the MAC address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to allow or deny network/Internet access. After modifying any settings, click **Save Settings** to save your changes.



MAC ADDRESS FILTER

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

Save Settings | Don't Save Settings

MAC FILTERING SETTINGS

MAC Address Control : □ Enable

□ Connection control — Wireless and wired clients with C checked can connect to this device; and allow ▾ unspecified MAC addresses to connect.

□ Association control — Wireless clients with A checked can associate to the wireless LAN; and allow ▾ unspecified MAC addresses to associate.

DHCP clients -- select one -- ▾ Copy to ID -- ▾

MAC FILTERING RULES

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

Previous page | Next page

MAC FILTERING SETTINGS

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

Connection Control: Tick 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: Tick 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.

DHCP clients: Select a DHCP client from the drop-down list and click **Copy to** and select an ID to apply the filter.

MAC FILTERING RULES

ID: This identifies the rule.

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

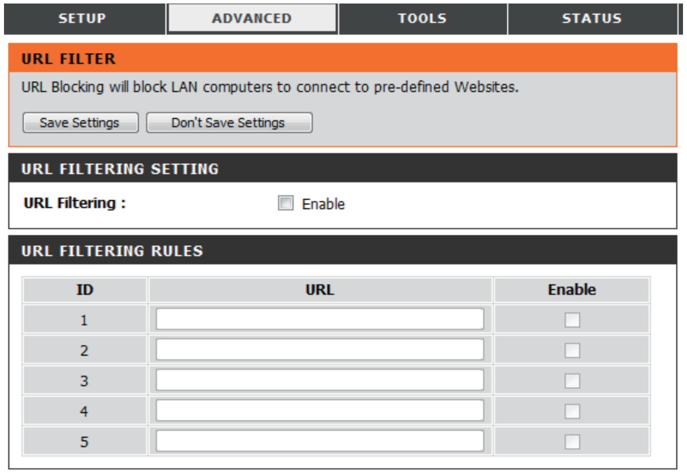
C: If this box is ticked, the rule will follow the connection control setting specified in MAC filtering settings specified above.

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

Click **Next page** to see more filters.

URL Filter

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



URL FILTER

URL Blocking will block LAN computers to connect to pre-defined Websites.

URL FILTERING SETTING

URL Filtering : □ Enable

URL FILTERING RULES

ID	URL	Enable
1		□
2		□
3		□
4		□
5		□

URL Filtering: Tick the box to enable URL filtering.

URL FILTERING RULES

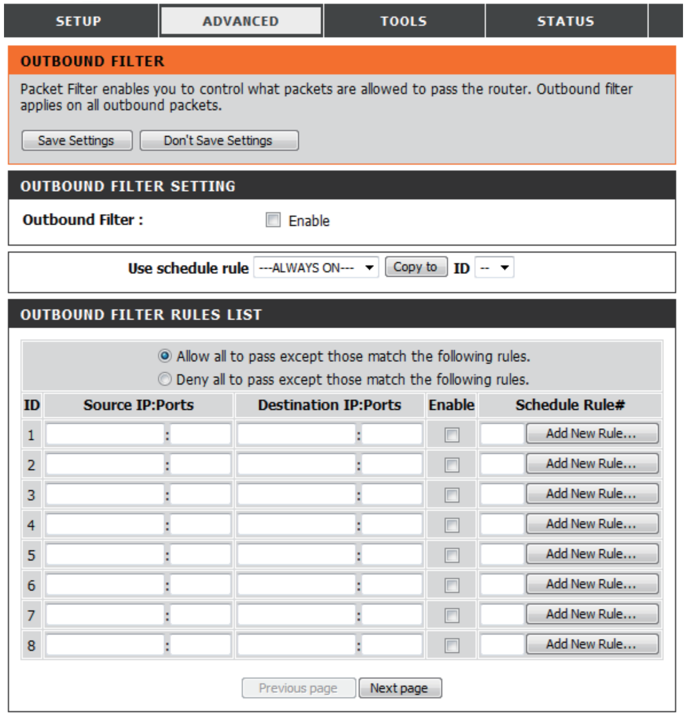
ID: This identifies the rule.

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

Enable: Tick the box to enable the specified rule.

Outbound Filter

The outbound filter enables you to control what packets are allowed to be sent out to the Internet. The outbound filter applies to all outbound packets. After modifying any settings, click **Save Settings** to save your changes.



OUTBOUND FILTER

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

Save Settings | Don't Save Settings

OUTBOUND FILTER SETTING

Outbound Filter : □ Enable

Use schedule rule ---ALWAYS ON--- 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

OUTBOUND FILTER SETTING

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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 72.

OUTBOUND FILTER RULES LIST

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

ID: This identifies the rule.

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

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

Enable: Tick the box to enable the specified rule.

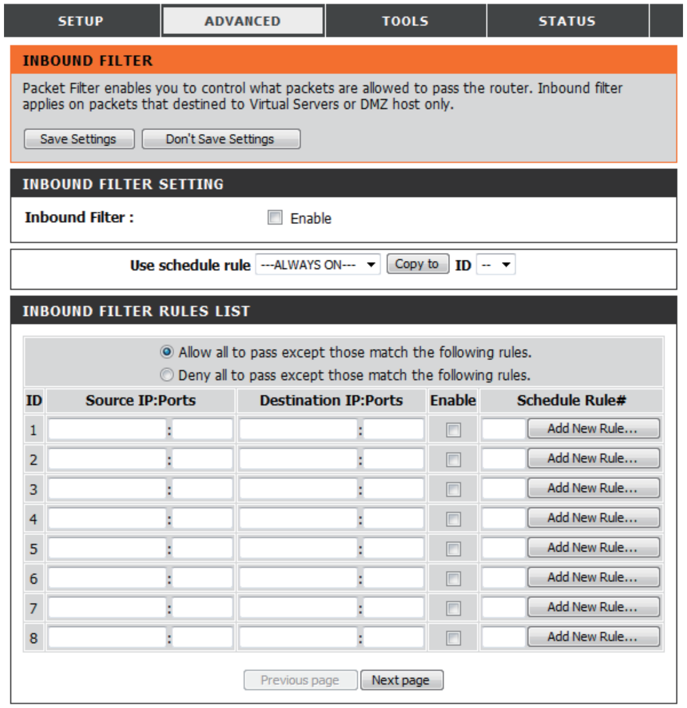
Schedule Rule #: Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

Inbound Filter

The inbound filter enables you to control what packets are allowed to come into your network from the Internet. The inbound filter only applies to packets that are destined for Virtual Servers or DMZ hosts. After modifying any settings, click **Save Settings** to save your changes.



INBOUND FILTER

Packet Filter enables you to control what packets are allowed to pass the router. Inbound filter applies on packets that destined to Virtual Servers or DMZ host only.

Save Settings | Don't Save Settings

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

INBOUND FILTER SETTING

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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to "Schedules" on page 72.

INBOUND FILTER RULES LIST

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

ID: This identifies the rule.

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

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

Enable: Tick the 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.

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-925. The DWR-925 supports SNMP v1 and v2c. After modifying any settings, click **Save Settings** to save your changes.

SNMP

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

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

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

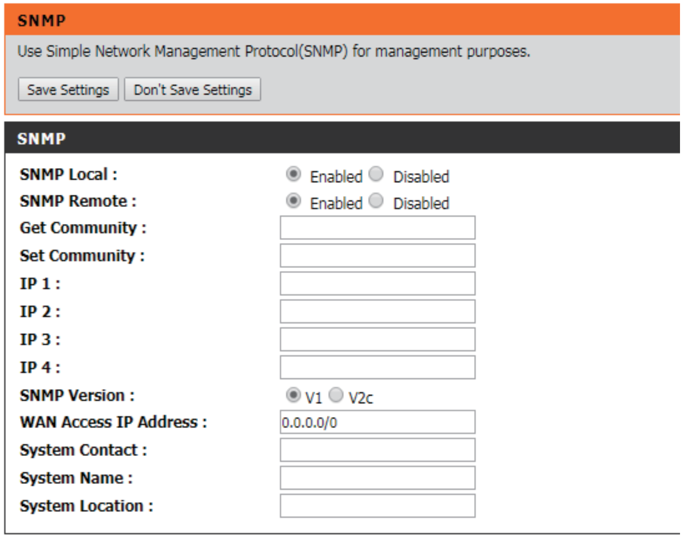
Set Community: Enter the password **private** in this field to enable read/write access to the network using SNMP.

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

SNMP Version: Select the SNMP version of your server.

WAN Access IP Address: If you want to limit remote 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.

System Contact/Name/ Location Enter contact and reference information. This information is for reference only and will be displayed when administering the router over SNMP.



SNMP

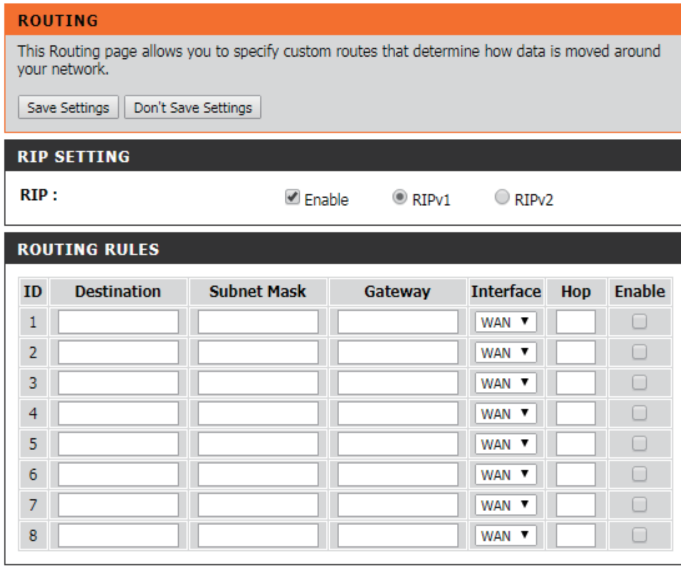
Use Simple Network Management Protocol(SNMP) for management purposes.

SNMP

SNMP Local :	● Enabled ○ Disabled
SNMP Remote :	● Enabled ○ Disabled
Get Community :	
Set Community :	
IP 1 :	
IP 2 :	
IP 3 :	
IP 4 :	
SNMP Version :	● V1 ○ V2c
WAN Access IP Address :	0.0.0.0/0
System Contact :	
System Name :	
System Location :	

Routing

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



ROUTING

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

RIP SETTING

RIP : ☑ Enable ● RIPv1 ○ RIPv2

ROUTING RULES

ID	Destination	Subnet Mask	Gateway	Interface	Hop	Enable
1				WAN		□
2				WAN		□
3				WAN		□
4				WAN		□
5				WAN		□
6				WAN		□
7				WAN		□
8				WAN		□

RIP SETTING

RIP: Tick 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 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 the gateway IP address for the specified network.

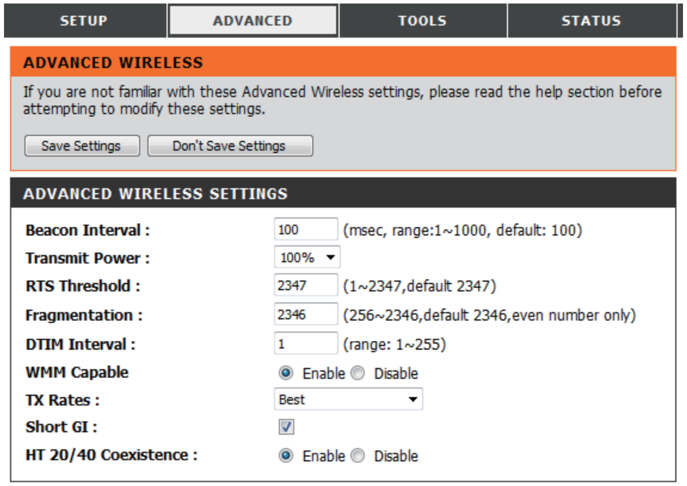
Interface: Select the interface over which the rule will be routed.

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

Advanced Wireless

Advanced wireless contains settings which can negatively affect the performance of your router if configured improperly. Do not change these settings unless you are already familiar with them or have been instructed to make the change by support personnel. After modifying any settings, click **Save Settings** to save your changes.



ADVANCED WIRELESS

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

ADVANCED WIRELESS SETTINGS

Beacon Interval :	100 (msec, range:1~1000, default: 100)
Transmit Power :	100%
RTS Threshold :	2347 (1~2347,default 2347)
Fragmentation :	2346 (256~2346,default 2346,even number only)
DTIM Interval :	1 (range: 1~255)
WMM Capable	● Enable ○ Disable
TX Rates :	Best
Short GI :	☑
HT 20/40 Coexistence :	● Enable ○ Disable

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

Transmit Power: Set the transmit power of the antennas.

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

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

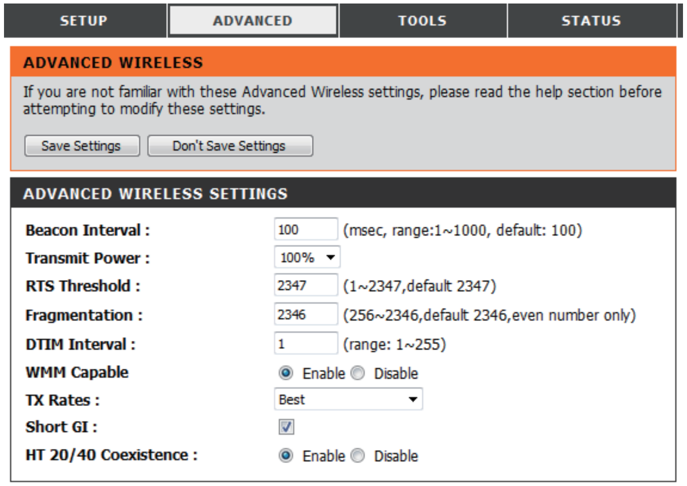
DTIM Interval: Set the interval for DTIM. A Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default interval is 3.

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

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

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

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



ADVANCED WIRELESS

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

ADVANCED WIRELESS SETTINGS

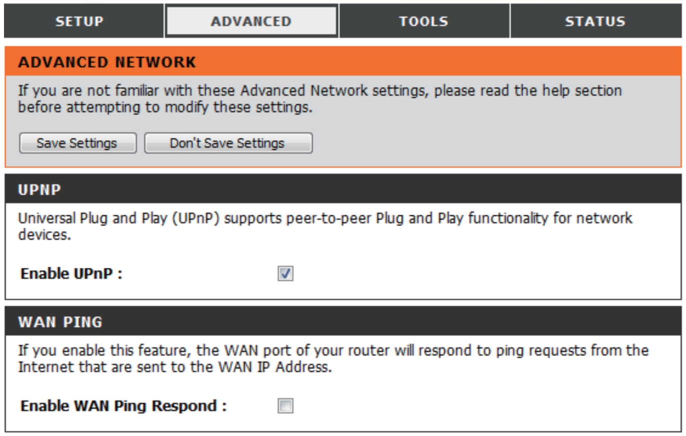
Beacon Interval :	100 (msec, range:1~1000, default: 100)
Transmit Power :	100%
RTS Threshold :	2347 (1~2347,default 2347)
Fragmentation :	2346 (256~2346,default 2346,even number only)
DTIM Interval :	1 (range: 1~255)
WMM Capable	● Enable ○ Disable
TX Rates :	Best
Short GI :	☑
HT 20/40 Coexistence :	● Enable ○ Disable

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

Enable UPnP: Tick 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.



ADVANCED NETWORK

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

UPNP

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

Enable UPnP : ☑

WAN PING

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

Enable WAN Ping Respond : □

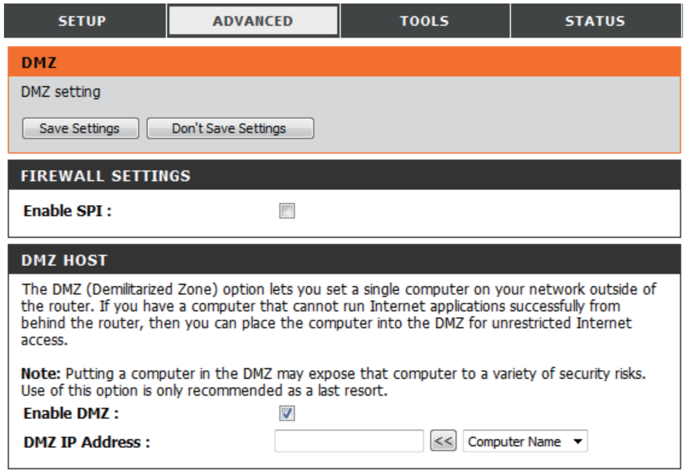
DMZ

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Enable SPI: Tick this box to enable SPI.

Enable DMZ: Tick this box to enable a DMZ area that allows a specific computer unrestricted access. This option is not recommended and should be used with caution.

DMZ IP Address: Specify an IP address for the DMZ zone and select the computer to associate it with.



DMZ setting

Enable SPI : □

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting 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.

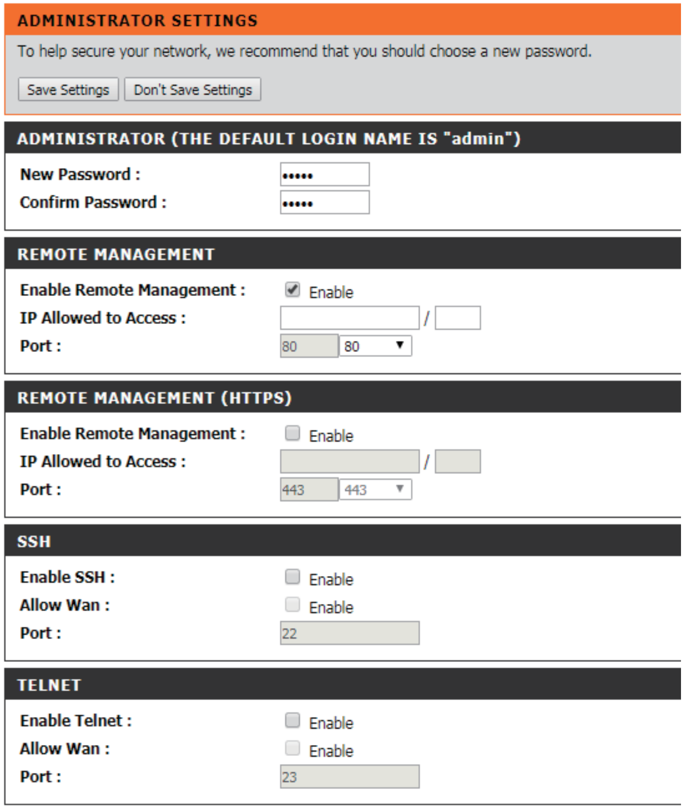
Enable DMZ : ☑

DMZ IP Address :

Tools

Admin

The Admin page allows you to change the Administrator password and enable Remote Management. The admin has read/write access while users only have read-only access. Only the admin has the ability to change both admin and user account passwords. After modifying any settings, click **Save Settings** to save your changes.



ADMINISTRATOR SETTINGS

To help secure your network, we recommend that you should choose a new password.

ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "admin")

New Password :	•••••
Confirm Password :	•••••

REMOTE MANAGEMENT

Enable Remote Management :	☑ Enable
IP Allowed to Access :	/
Port :	80 80 ▼

REMOTE MANAGEMENT (HTTPS)

Enable Remote Management :	☐ Enable
IP Allowed to Access :	/
Port :	443 443 ▼

SSH

Enable SSH :	☐ Enable
Allow Wan :	☐ Enable
Port :	22

TELNET

Enable Telnet :	☐ Enable
Allow Wan :	☐ Enable
Port :	23

ADMINISTRATOR

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

REMOTE MANAGEMENT/ REMOTE MANAGEMENT (HTTPS)

Enable Remote Management: Tick this check box to enable remote management. Remote management allows the DWR-925 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. Leave this field blank to allow any remote IP to access the router. This is not recommended.

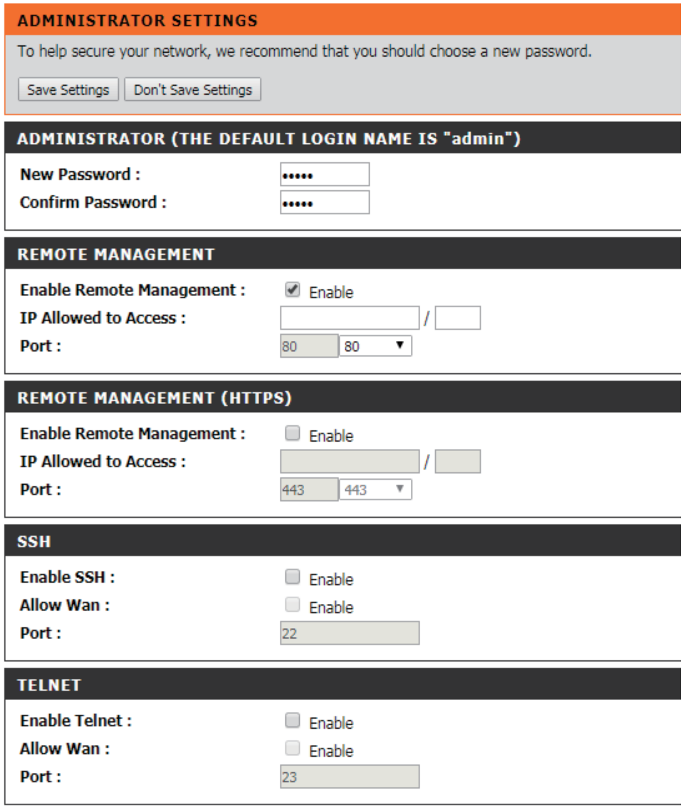
Port: This is the port number used to access the router. **80** (HTTP) or **443** (HTTPS) is the port usually used for the web-management interface.

SSH/Telnet

Enable SSH/Telnet: Check this box to access the router via SSH or Telnet over LAN.

Allow WAN: Check this box to enable CLI access over WAN.
Note: this may open the router to attacks over the internet, and is not recommended.

Port: Specify the port for the CLI service. The default port is **22** for SSH and **23** for Telnet.



ADMINISTRATOR SETTINGS

To help secure your network, we recommend that you should choose a new password.

ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "admin")

New Password :	•••••
Confirm Password :	•••••

REMOTE MANAGEMENT

Enable Remote Management :	☑ Enable
IP Allowed to Access :	/
Port :	80 80 ▼

REMOTE MANAGEMENT (HTTPS)

Enable Remote Management :	□ Enable
IP Allowed to Access :	/
Port :	443 443 ▼

SSH

Enable SSH :	□ Enable
Allow Wan :	□ Enable
Port :	22

TELNET

Enable Telnet :	□ Enable
Allow Wan :	□ Enable
Port :	23

Time

This section will help you set the time zone that you are in and an NTP (Network Time Protocol) server to use. Daylight Saving can also be configured to adjust the time when needed. After modifying any settings, click **Save Settings** to save your changes.

TIME AND DATE CONFIGURATION

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

Enable Daylight Saving: Tick this box to enable daylight saving auto-adjustment. Click **Sync your computer's time settings** to sync the router to your computer's clock.

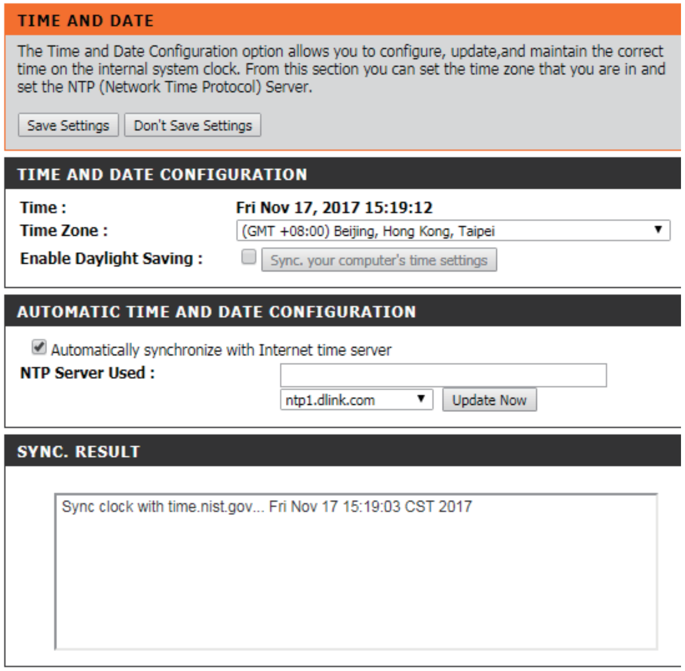
AUTOMATIC TIME AND DATE CONFIGURATION

Tick the **Automatically synchronize with Internet time server** 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.

SYNC RESULT

This section indicates the result of NTP synchronization. The contents of this box depend on network connectivity and NTP server selection.



TIME AND DATE

The Time and Date 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.

TIME AND DATE CONFIGURATION

Time : Fri Nov 17, 2017 15:19:12

Time Zone : (GMT +08:00) Beijing, Hong Kong, Taipei

Enable Daylight Saving : □

AUTOMATIC TIME AND DATE CONFIGURATION

☑ Automatically synchronize with Internet time server

NTP Server Used : ntp1.dlink.com

SYNC. RESULT

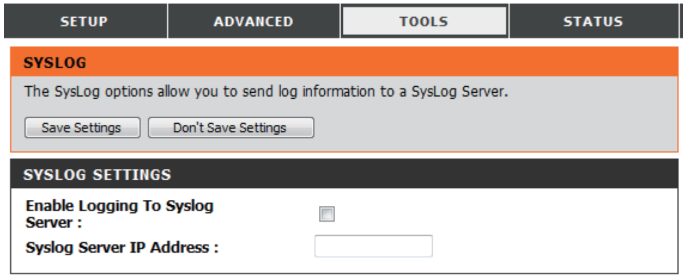
Sync clock with time.nist.gov... Fri Nov 17 15:19:03 CST 2017

Syslog

The DWR-925 keeps a running log of events and activities occurring on the router. You may send these logs to a Syslog server on your network. After modifying any settings, click **Save Settings** to save your changes.

Enable Logging to Syslog Server: Tick 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.



SYSLOG

The SysLog options allow you to send log information to a SysLog Server.

SYSLOG SETTINGS

Enable Logging To Syslog Server : □

Syslog Server IP Address :

Email Settings

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

Enable Email Notification: When this option is enabled, router activity logs will be emailed to the specified email address.

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

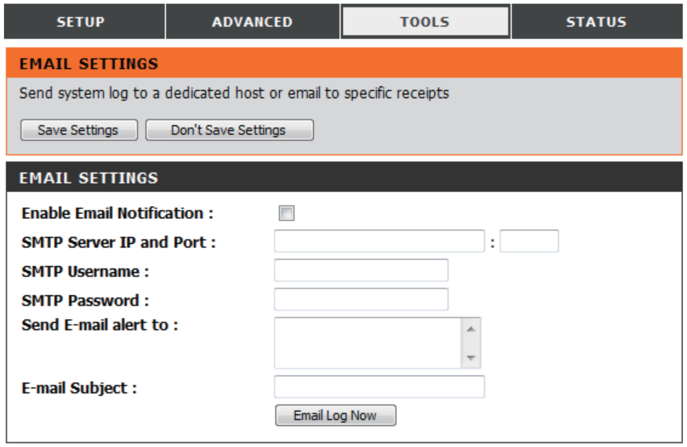
SMTP Username: Enter the username for the SMTP account.

SMTP Password: Enter the password for the SMTP account.

Send Email Alert to: Enter the email address where you would like the router to send emails to.

Email Subject: Enter a subject for the email.

Email Log Now: Click this button to send the current logs to the specified email address.



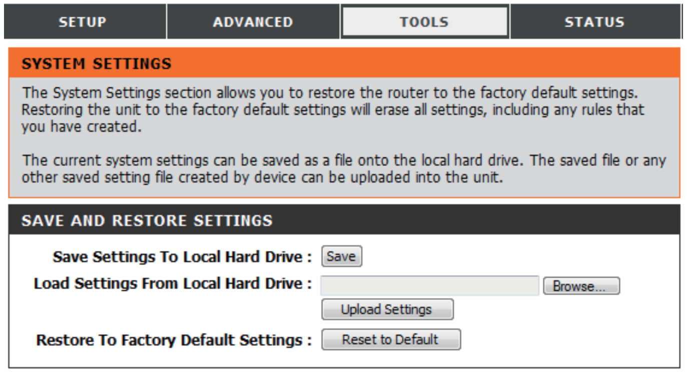
EMAIL SETTINGS

Send system log to a dedicated host or email to specific receipts

EMAIL SETTINGS

System

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



SYSTEM SETTINGS

The System Settings section allows you to restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

SAVE AND RESTORE SETTINGS

Save Settings To Local Hard Drive : Save

Load Settings From Local Hard Drive : Browse... Upload Settings

Restore To Factory Default Settings : Reset to Default

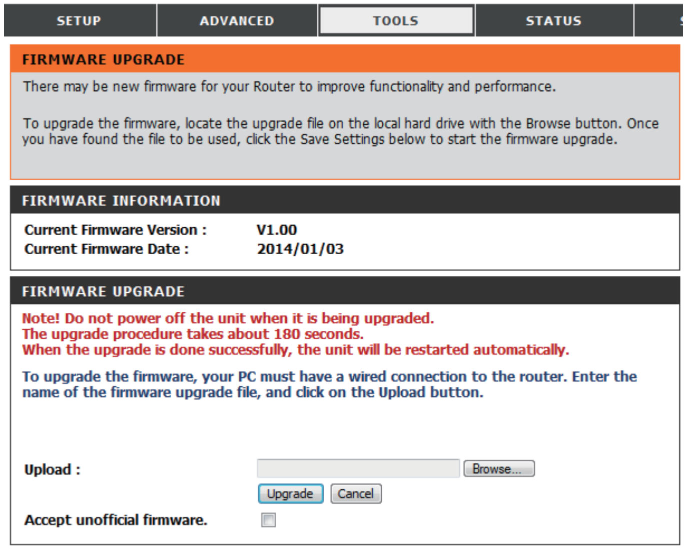
Save Settings To Local Hard Drive Use this option to save your current router configuration settings to a file. Click **Save** to open a file dialog, and then select a location and file name for the settings.

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

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

Firmware

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



FIRMWARE UPGRADE

There may be new firmware for your Router to improve functionality and performance.

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Save Settings below to start the firmware upgrade.

FIRMWARE INFORMATION

Current Firmware Version : V1.00
Current Firmware Date : 2014/01/03

FIRMWARE UPGRADE

Note! Do not power off the unit when it is being upgraded.
The upgrade procedure takes about 180 seconds.
When the upgrade is done successfully, the unit will be restarted automatically.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

Accept unofficial firmware. □

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

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

Upload: After you have downloaded 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.

Dynamic DNS

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

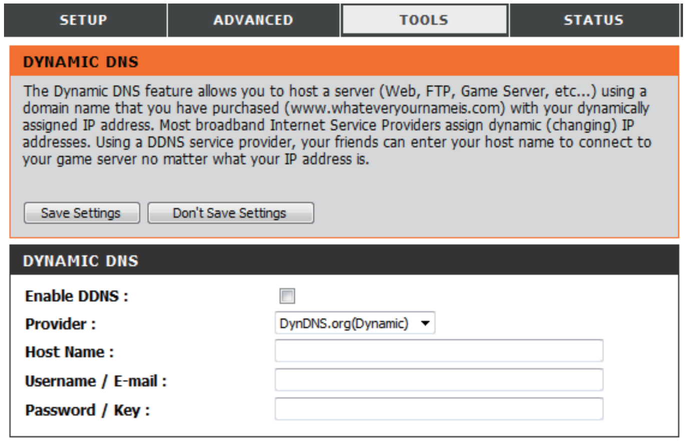
Enable DDNS: Tick this checkbox to enable the DDNS feature.

Provider: Select a DDNS service provider to use.

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

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

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



DYNAMIC DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

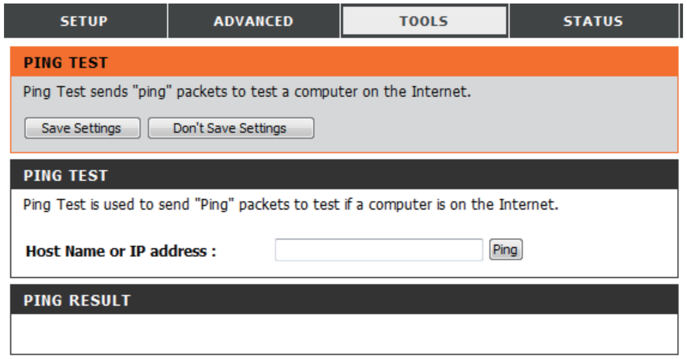
DYNAMIC DNS

Enable DDNS :	□
Provider :	DynDNS.org(Dynamic)
Host Name :	
Username / E-mail :	
Password / Key :	

System Check

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

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



PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

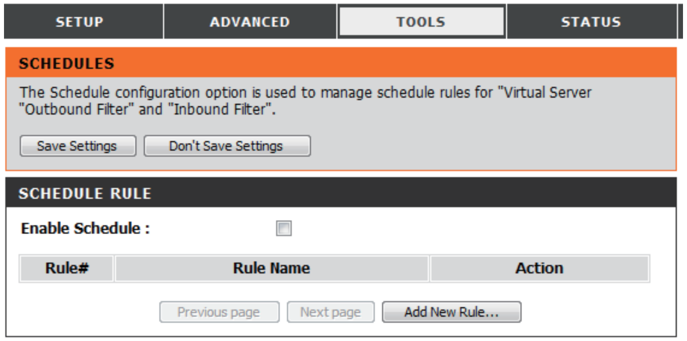
Ping Test is used to send "Ping" packets to test if a computer is on the Internet.

Host Name or IP address :

PING RESULT

Schedules

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



SCHEDULES

The Schedule configuration option is used to manage schedule rules for "Virtual Server "Outbound Filter" and "Inbound Filter".

SCHEDULE RULE

Enable Schedule : □

Rule#	Rule Name	Action

Enable Schedule: Tick 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)

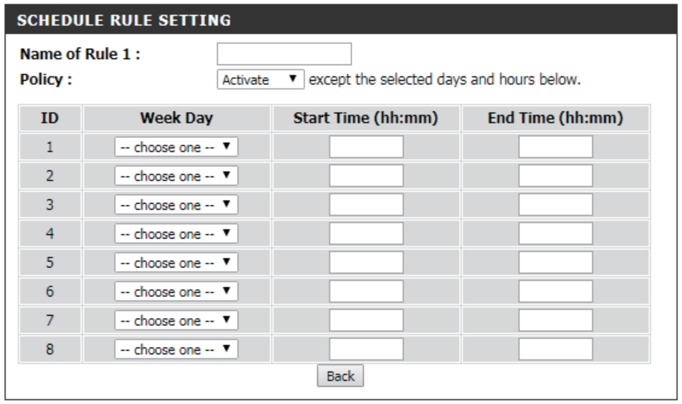
Name of Rule #: Enter a name for your new schedule.

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.



SCHEDULE RULE SETTING

Name of Rule 1 :

Policy : Activate ▼ except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▼		
2	-- choose one -- ▼		
3	-- choose one -- ▼		
4	-- choose one -- ▼		
5	-- choose one -- ▼		
6	-- choose one -- ▼		
7	-- choose one -- ▼		
8	-- choose one -- ▼		

Connection Reset

This section allows configuration of automatic reboot on a schedule determined by the user. Note that times are based on the router's internal clock. After modifying any settings, click **Save Settings** to save your changes.

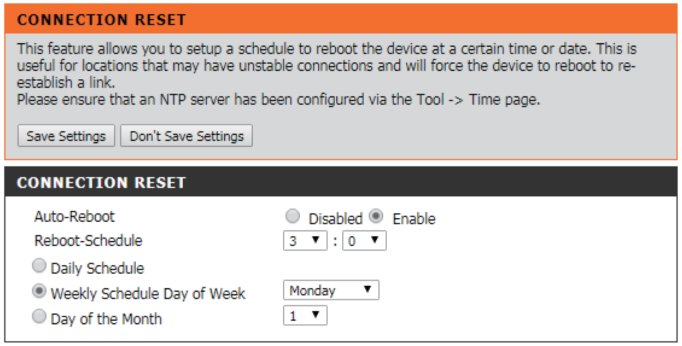
Auto-Reboot: Select **Enable** to enable the auto reboot function.

Reboot-Schedule: Select specify a time of day in 24 hour format, where 10:30 would refer to 10:30 AM and 22:30 would refer to 10:30 PM

Daily Schedule: Select **Daily Schedule** to reboot every day at the time specified above.

Weekly Schedule Day of Week: Select **Weekly Schedule Day of the Week** to reboot once per week on the day specified here at the time specified above.

Day of the Month: Select **Day of the Month** and specify the calendar day of each month to initiate a reboot. Note that if that exact date does not occur during that month, no reboot will be performed. For example, setting **31** would mean that there would be no reboot during the month of February.



CONNECTION RESET

This feature allows you to setup a schedule to reboot the device at a certain time or date. This is useful for locations that may have unstable connections and will force the device to reboot to re-establish a link.
Please ensure that an NTP server has been configured via the Tool -> Time page.

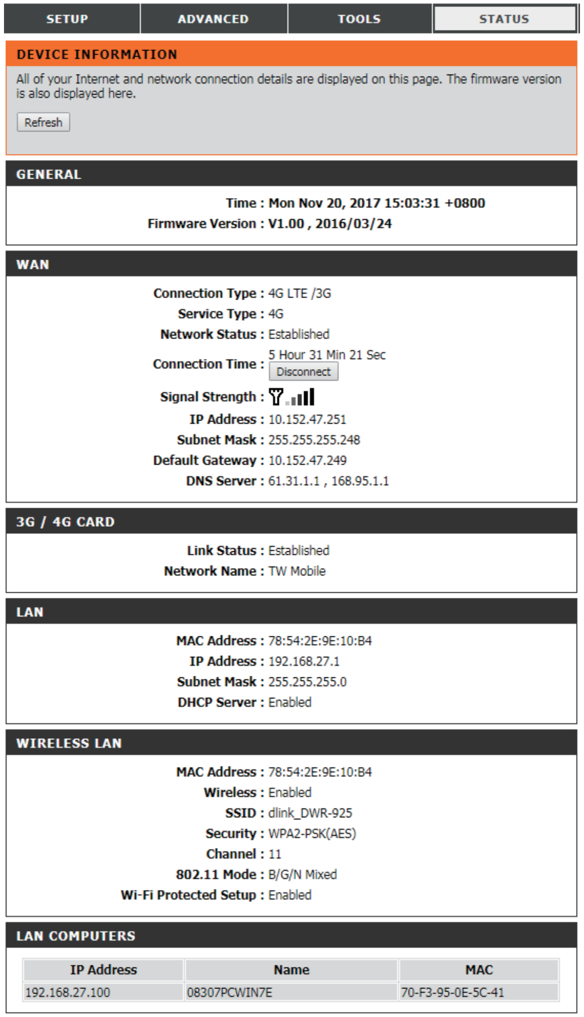
CONNECTION RESET

Auto-Reboot ○ Disabled ● Enable
Reboot-Schedule 3 : 0
○ Daily Schedule
● Weekly Schedule Day of Week Monday
○ Day of the Month 1

Status

Device Info

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here. If your Internet connection is set up for a Dynamic IP address then a Release button and a Renew button will be displayed. Use Release to disconnect from your ISP and use Renew to connect to your ISP. Other forms of connection will offer Connect/Disconnect options.



DEVICE INFORMATION

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

GENERAL

Time : Mon Nov 20, 2017 15:03:31 +0800
Firmware Version : V1.00 , 2016/03/24

WAN

Connection Type : 4G LTE /3G
Service Type : 4G
Network Status : Established
Connection Time : 5 Hour 31 Min 21 Sec
Signal Strength :
IP Address : 10.152.47.251
Subnet Mask : 255.255.255.248
Default Gateway : 10.152.47.249
DNS Server : 61.31.1.1 , 168.95.1.1

3G / 4G CARD

Link Status : Established
Network Name : TW Mobile

LAN

MAC Address : 78:54:2E:9E:10:B4
IP Address : 192.168.27.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

MAC Address : 78:54:2E:9E:10:B4
Wireless : Enabled
SSID : dlink_DWR-925
Security : WPA2-PSK(AES)
Channel : 11
802.11 Mode : B/G/N Mixed
Wi-Fi Protected Setup : Enabled

LAN COMPUTERS

IP Address	Name	MAC
192.168.27.100	08307PCWIN7E	70-F3-95-0E-5C-41

Log

Here, you can view and download the system log.

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

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

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

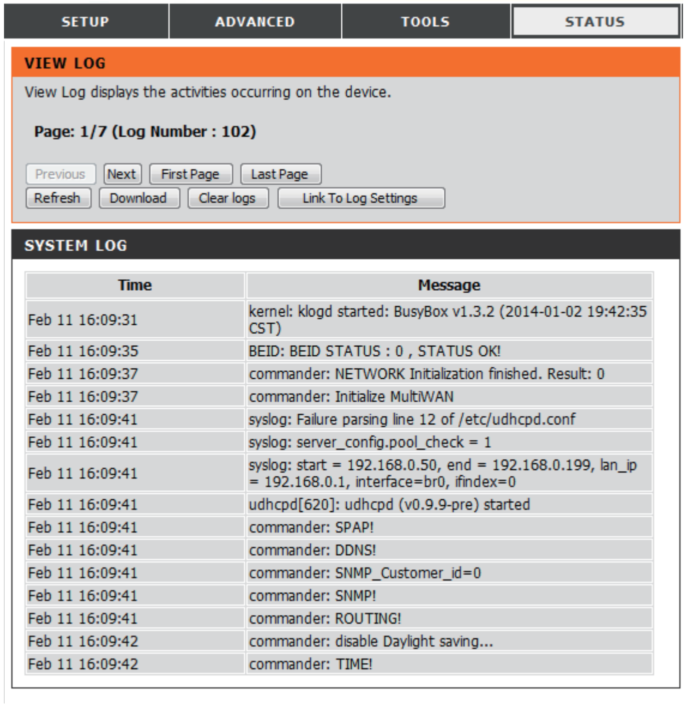
Last Page: Click this button to skip to the last page of the log.

Refresh: Click this button to refresh the system log.

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

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

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



VIEW LOG

View Log displays the activities occurring on the device.

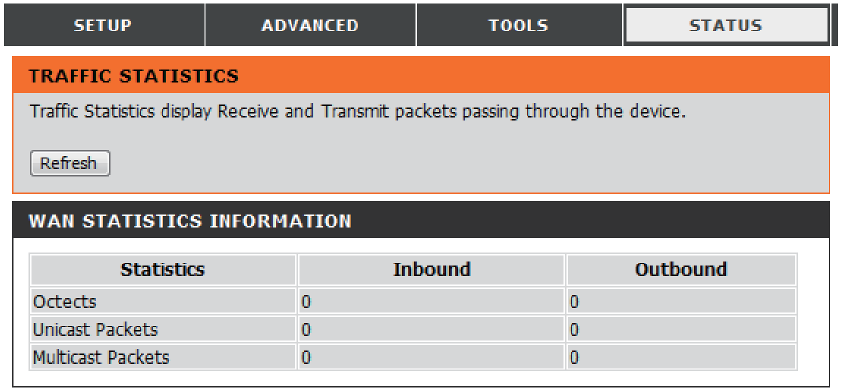
Page: 1/7 (Log Number : 102)

SYSTEM LOG

Time	Message
Feb 11 16:09:31	kernel: klogd started: BusyBox v1.3.2 (2014-01-02 19:42:35 CST)
Feb 11 16:09:35	BEID: BEID STATUS : 0 , STATUS OK!
Feb 11 16:09:37	commander: NETWORK Initialization finished. Result: 0
Feb 11 16:09:37	commander: Initialize MultiWAN
Feb 11 16:09:41	syslog: Failure parsing line 12 of /etc/udhcpd.conf
Feb 11 16:09:41	syslog: server_config.pool_check = 1
Feb 11 16:09:41	syslog: start = 192.168.0.50, end = 192.168.0.199, lan_ip = 192.168.0.1, interface=br0, ifindex=0
Feb 11 16:09:41	udhcpd[620]: udhcpd (v0.9.9-pre) started
Feb 11 16:09:41	commander: SPAP!
Feb 11 16:09:41	commander: DDNS!
Feb 11 16:09:41	commander: SNMP_Customer_id=0
Feb 11 16:09:41	commander: SNMP!
Feb 11 16:09:41	commander: ROUTING!
Feb 11 16:09:42	commander: disable Daylight saving...
Feb 11 16:09:42	commander: TIME!

Statistics

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



TRAFFIC STATISTICS

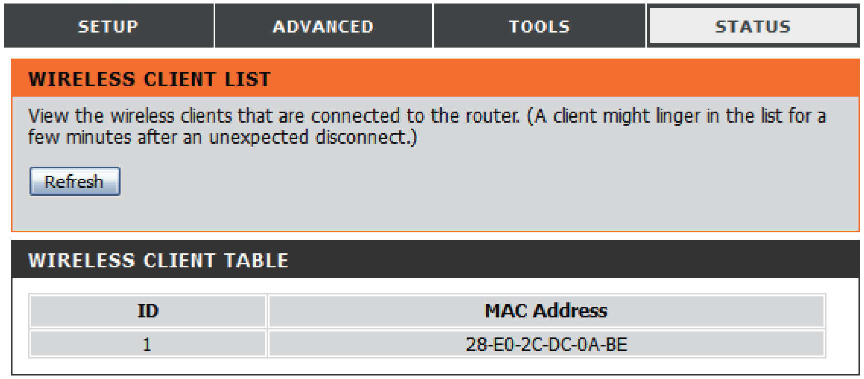
Traffic Statistics display Receive and Transmit packets passing through the device.

WAN STATISTICS INFORMATION

Statistics	Inbound	Outbound
Octects	0	0
Unicast Packets	0	0
Multicast Packets	0	0

Wireless

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



WIRELESS CLIENT LIST

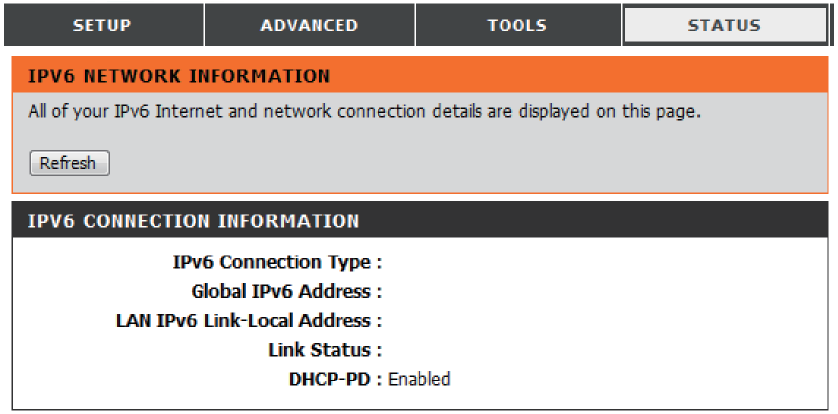
View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

WIRELESS CLIENT TABLE

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

IPv6 Status

This page displays the IPv6 network connection details. Click **Refresh** to refresh the list.



All of your IPv6 Internet and network connection details are displayed on this page.

IPv6 Connection Type :

Global IPv6 Address :

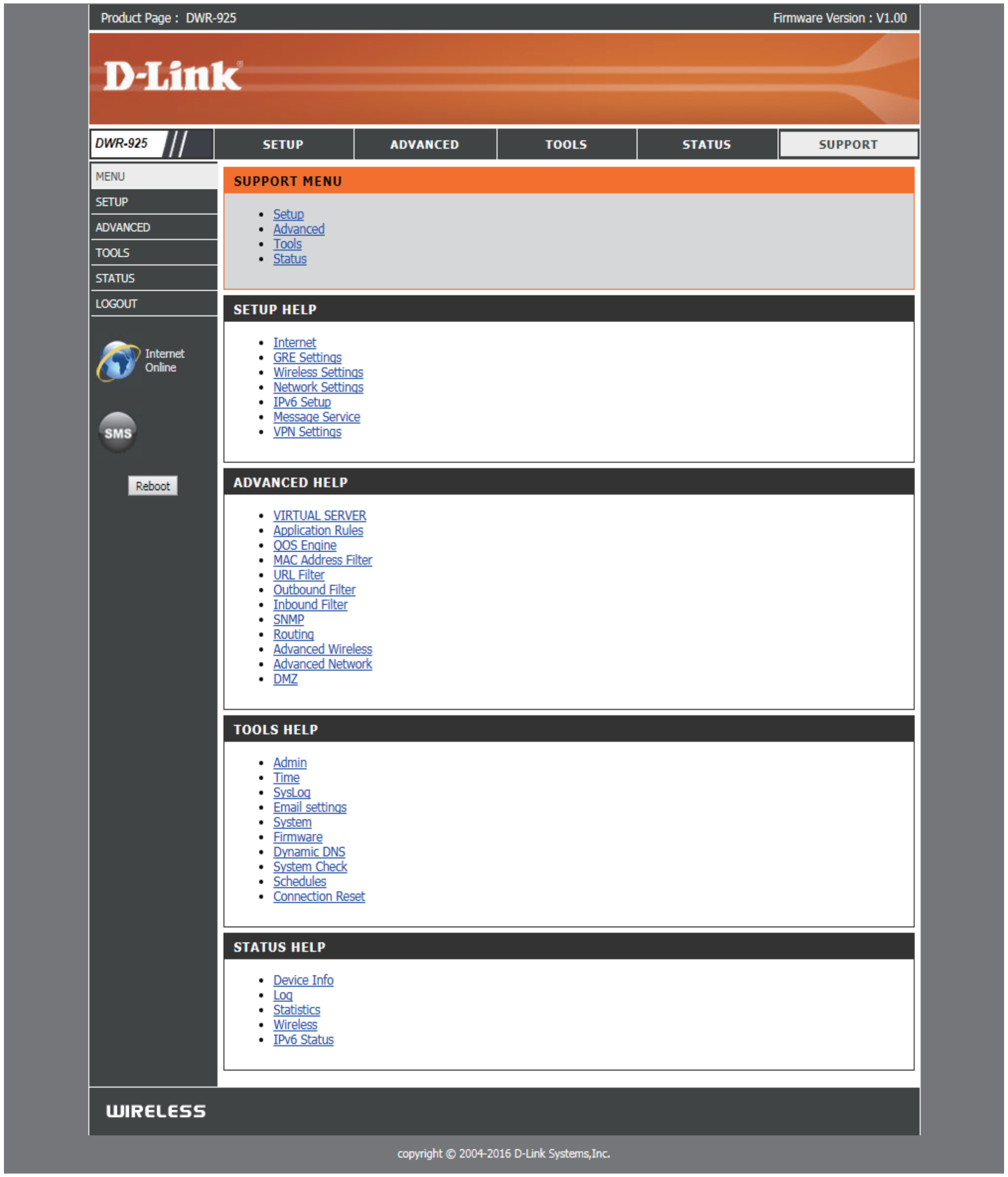
LAN IPv6 Link-Local Address :

Link Status :

DHCP-PD : Enabled

Support

This screen gives you more information about the various parts of the configuration interface. Click on a link to learn more about that topic.



SUPPORT MENU

- Setup
- Advanced
- Tools
- Status

SETUP HELP

- Internet
- GRE Settings
- Wireless Settings
- Network Settings
- IPv6 Setup
- Message Service
- VPN Settings

ADVANCED HELP

- VIRTUAL SERVER
- Application Rules
- QOS Engine
- MAC Address Filter
- URL Filter
- Outbound Filter
- Inbound Filter
- SNMP
- Routing
- Advanced Wireless
- Advanced Network
- DMZ

TOOLS HELP

- Admin
- Time
- SysLog
- Email settings
- System
- Firmware
- Dynamic DNS
- System Check
- Schedules
- Connection Reset

STATUS HELP

- Device Info
- Log
- Statistics
- Wireless
- IPv6 Status

Connecting a Wireless Client

WPS Button

The easiest and most secure way to connect your wireless devices to the router is 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 router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. To connect a client, follow the steps below:

To connect your wireless devices to the router using WPS:

Step 1 - Enable the WPS feature on your router. The Power/Status LED will start to blink.

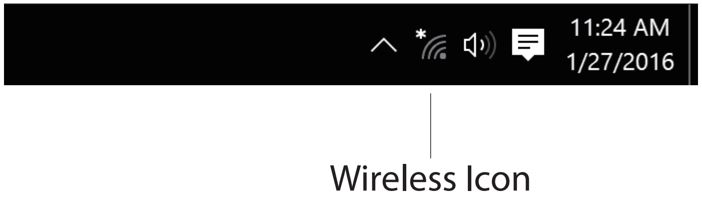
Step 2 - Within 2 minutes, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

Step 3 - Allow up to 2 minutes to configure. Once the Power/Status LED stops blinking, you will be connected and your wireless connection will be encrypted with WPA2.

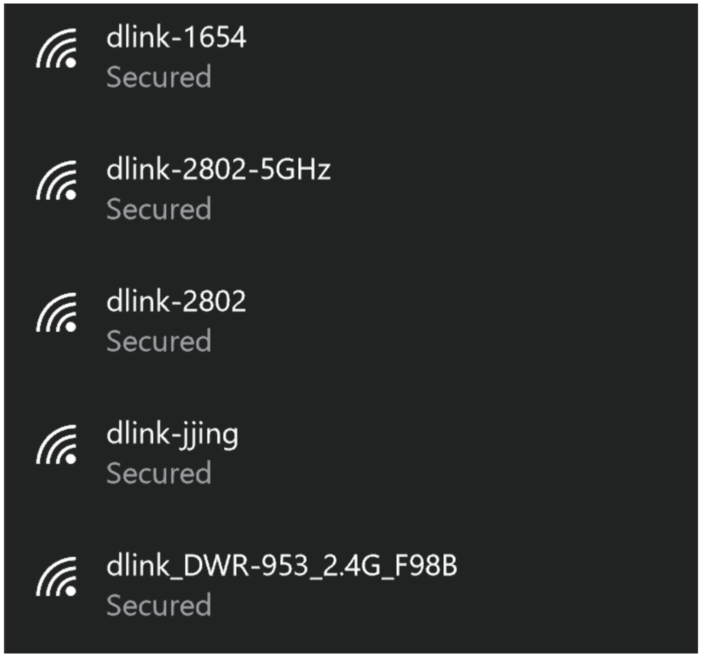
Windows® 10

When connecting to the DWR-925 wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to. If your product has a Wi-Fi configuration card, you can find the default network name and Wi-Fi password here. Otherwise, refer to the product label for the default Wi-Fi network SSID and password, or enter the Wi-Fi credentials set during the product configuration.

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

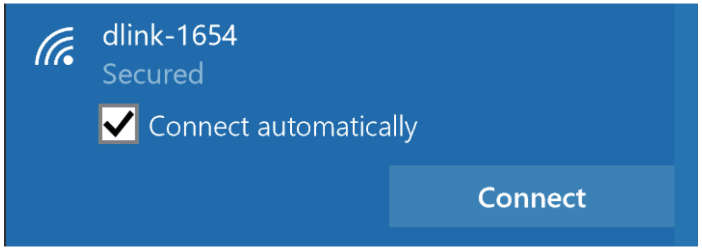


Clicking on this icon will display a list of wireless networks which in range of your computer. Select the desired network by clicking on the SSID.



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

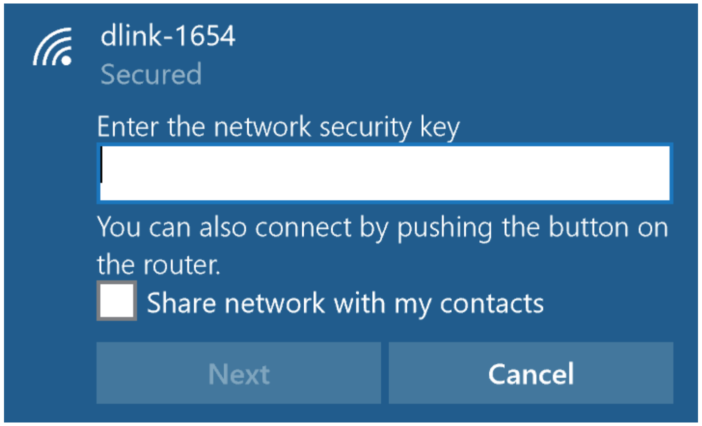
To automatically connect to the router when your device detects the SSID, click the **Connect Automatically** check box**.**



dlink-1654
Secured
☑ Connect automatically

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. Your computer will now automatically connect to this wireless network when it is detected.

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



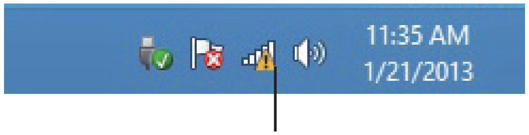
dlink-1654
Secured
Enter the network security key
You can also connect by pushing the button on the router.
□ Share network with my contacts

Windows® 8

WPA/WPA2

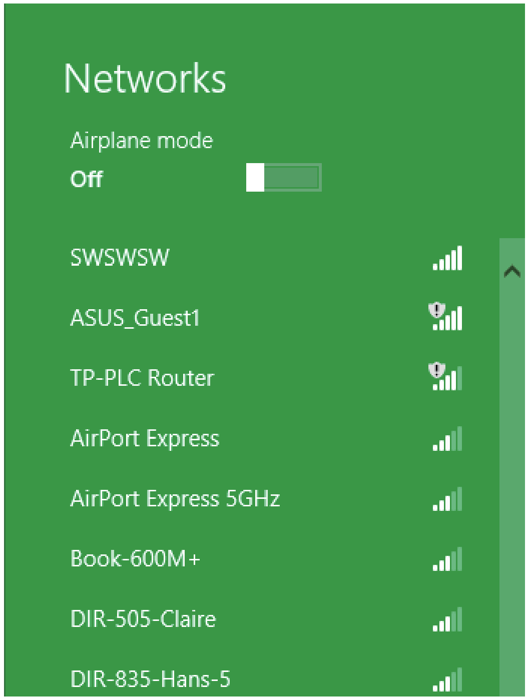
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

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



Wireless Icon

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.



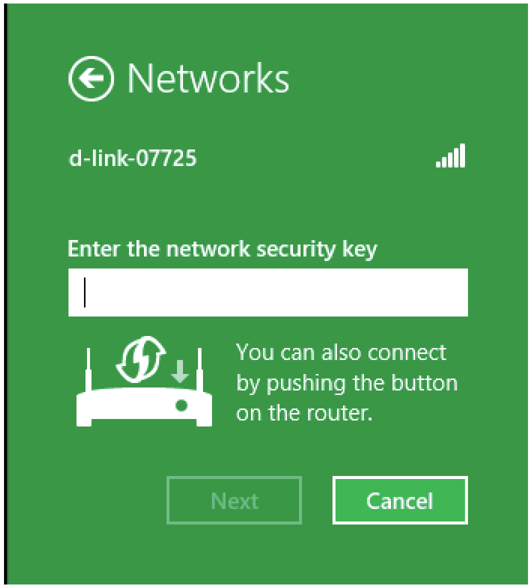
Networks

Airplane mode
Off

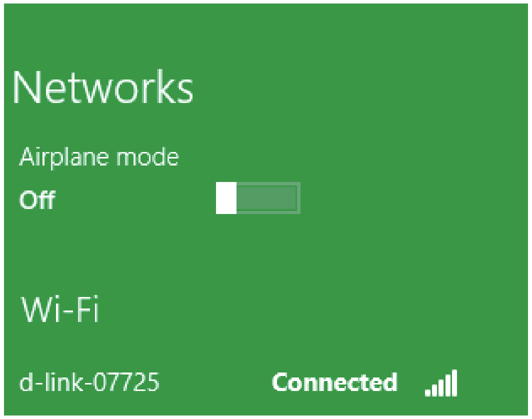
SWSWSW
ASUS_Guest1
TP-PLC Router
AirPort Express
AirPort Express 5GHz
Book-600M+
DIR-505-Claire
DIR-835-Hans-5

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 at this point to enable the WPS function.


Networks
d-link-07725
Enter the network security key
You can also connect by pushing the button on the router.
Next
Cancel

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.

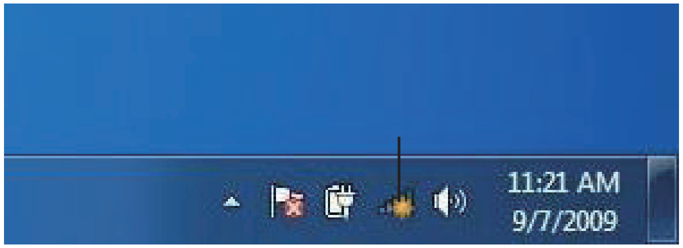


Windows® 7

WPA/WPA2

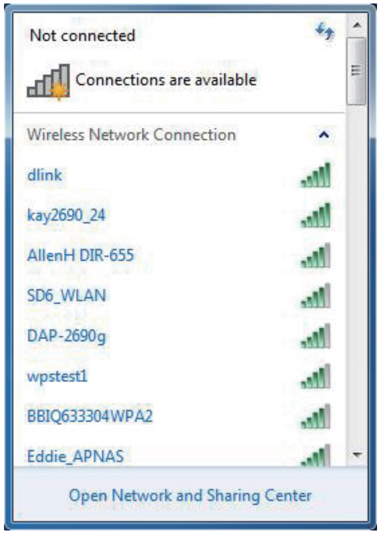
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

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



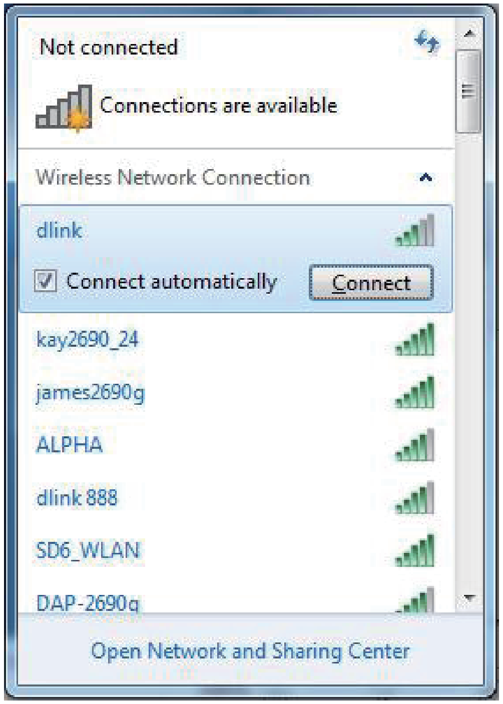
Wireless Icon

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.

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



Not connected

Connections are available

Wireless Network Connection

dlink

☑ Connect automatically

kay2690_24

james2690g

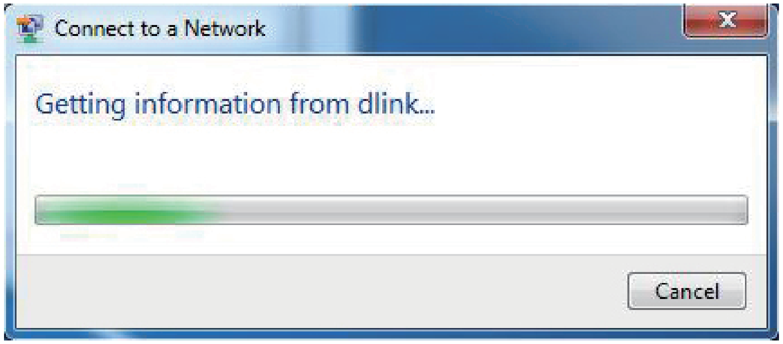
ALPHA

dlink 888

SD6_WLAN

DAP-2690g

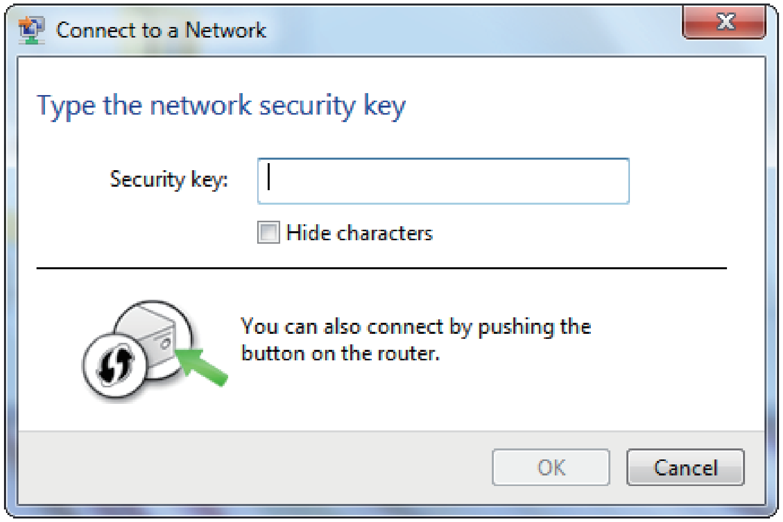
4. The following window appears while your computer tries to connect to the router.



Connect to a Network

Getting information from dlink...

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



Connect to a Network

Type the network security key

Security key:

□ Hide characters

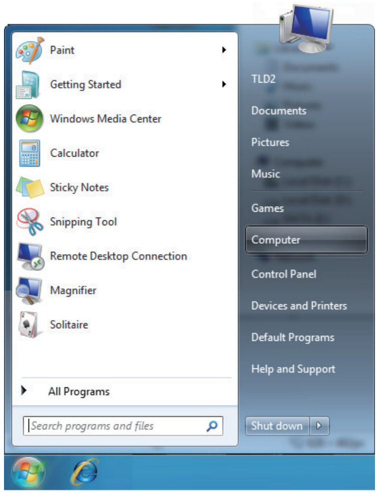
You can also connect by pushing the button on the router.

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 on the wireless router.

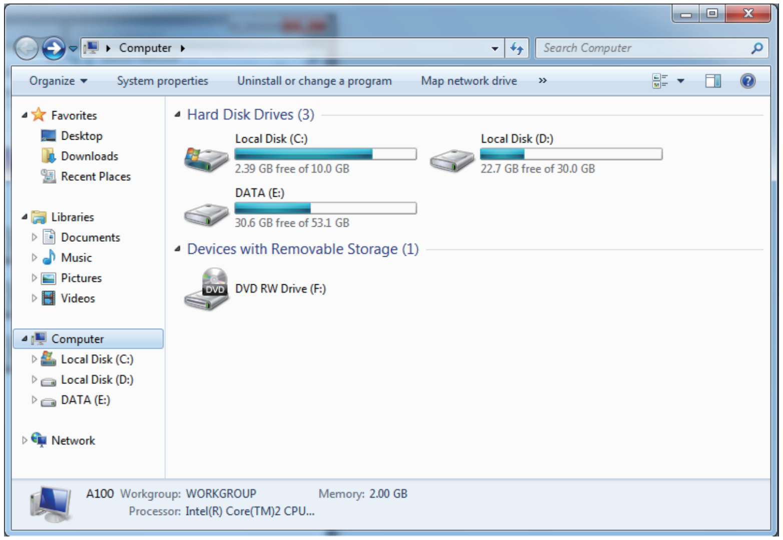
WPS

The WPS feature of the DWR-925 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

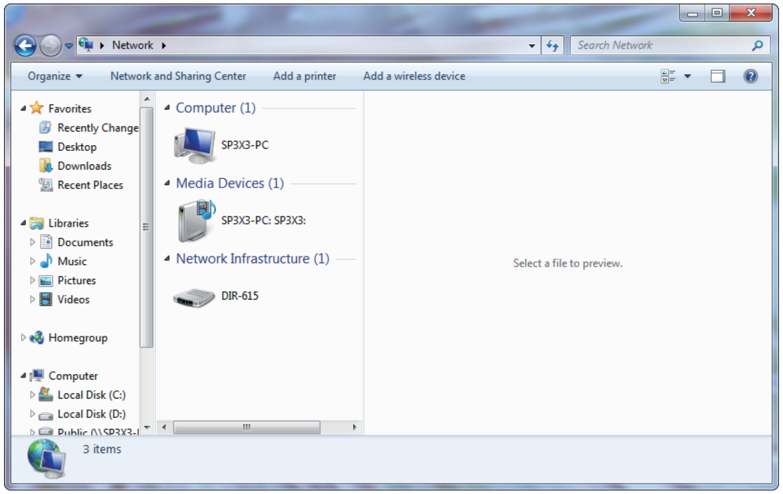
1. Click the **Start** button and select **Computer** from the Start menu.



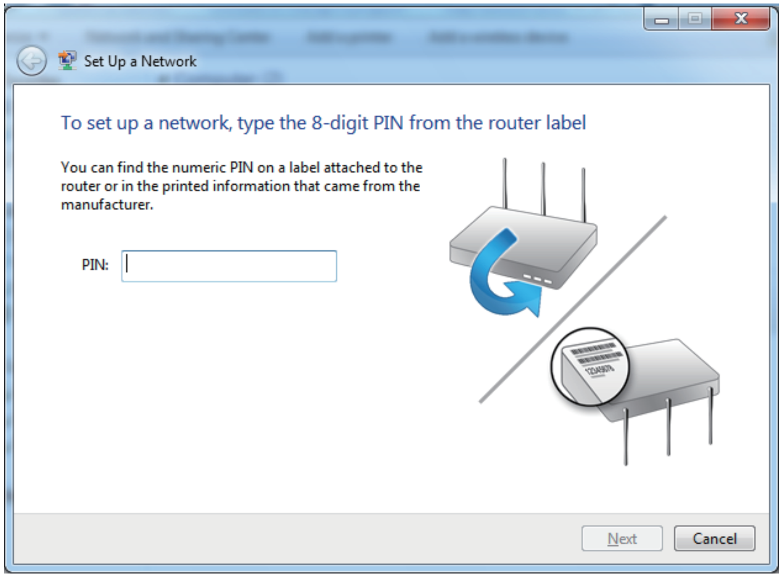
2. Click **Network** on the left side.



3. Double-click your D-Link router.



4. Input the WPS PIN number (displayed in the WPS window on the router's LCD screen or in the Setup > Wireless Setup menu in the router's Web UI) and click Next.

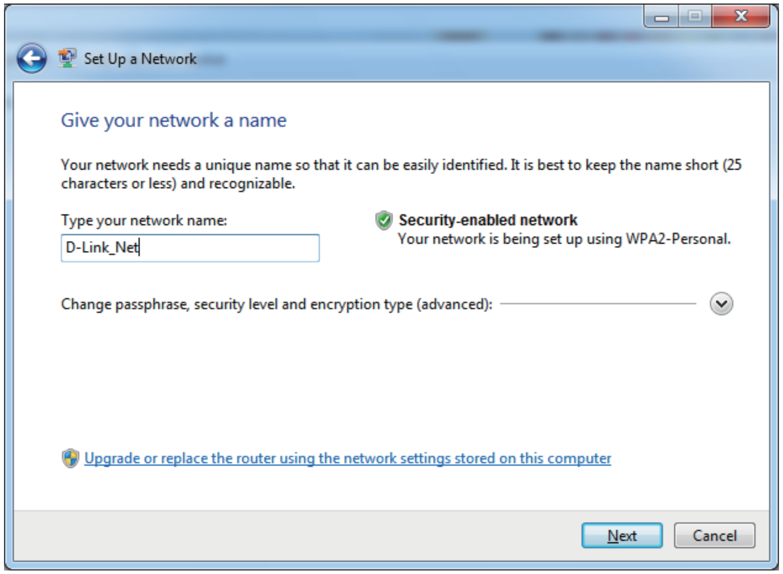


To set up a network, type the 8-digit PIN from the router label

You can find the numeric PIN on a label attached to the router or in the printed information that came from the manufacturer.

PIN:

5. Type a name to identify the network.



Set Up a Network

Give your network a name

Your network needs a unique name so that it can be easily identified. It is best to keep the name short (25 characters or less) and recognizable.

Type your network name: D-Link_Net

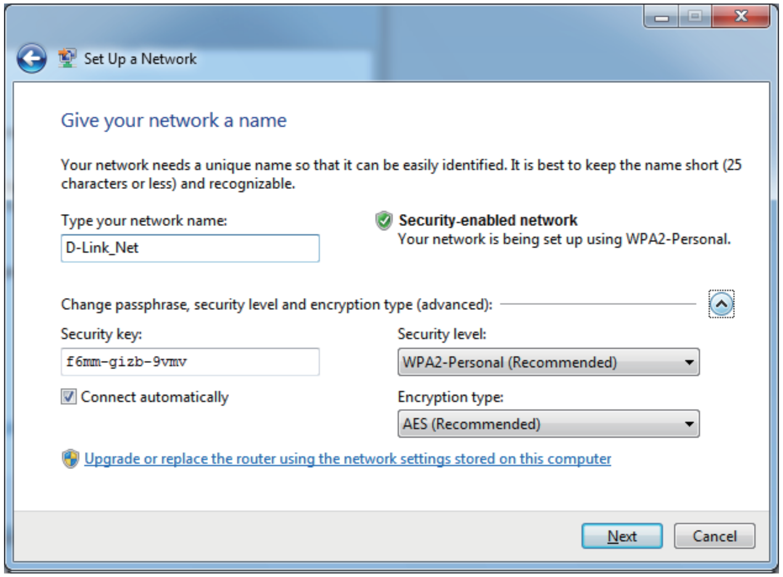
Security-enabled network
Your network is being set up using WPA2-Personal.

Change passphrase, security level and encryption type (advanced):

Upgrade or replace the router using the network settings stored on this computer

6. To configure advanced settings, click the ⌄ icon.

Click **Next** to continue.



Set Up a Network

Give your network a name

Your network needs a unique name so that it can be easily identified. It is best to keep the name short (25 characters or less) and recognizable.

Type your network name: D-Link_Net

Security-enabled network
Your network is being set up using WPA2-Personal.

Change passphrase, security level and encryption type (advanced):

Security key: f6mm-gizb-9vmv

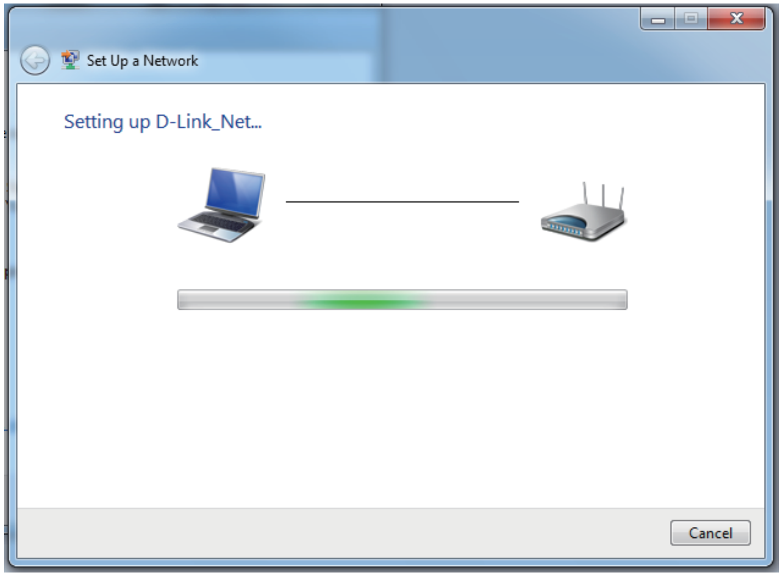
Security level: WPA2-Personal (Recommended)

☑ Connect automatically

Encryption type: AES (Recommended)

Upgrade or replace the router using the network settings stored on this computer

7. The following window appears while the router is being configured. Wait for the configuration to complete.

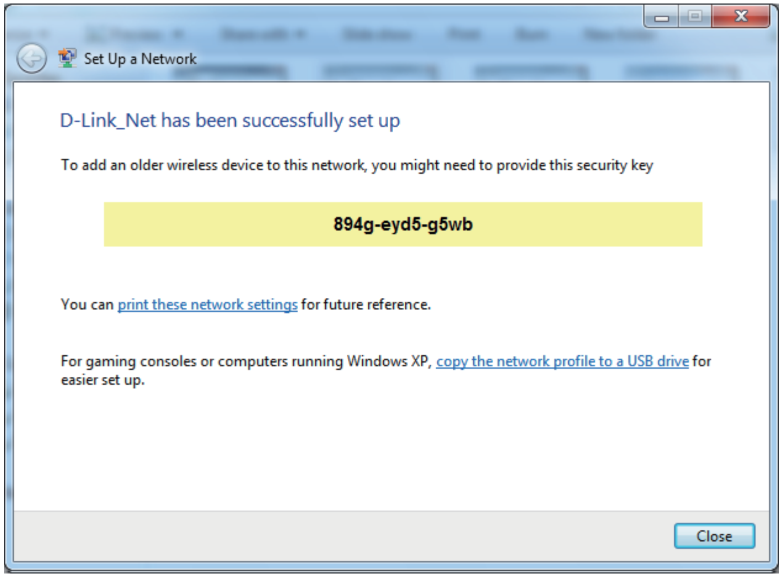


Setting up D-Link_Net...

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.



D-Link_Net has been successfully set up

To add an older wireless device to this network, you might need to provide this security key

894g-eyd5-g5wb

You can print these network settings for future reference.

For gaming consoles or computers running Windows XP, copy the network profile to a USB drive for easier set up.

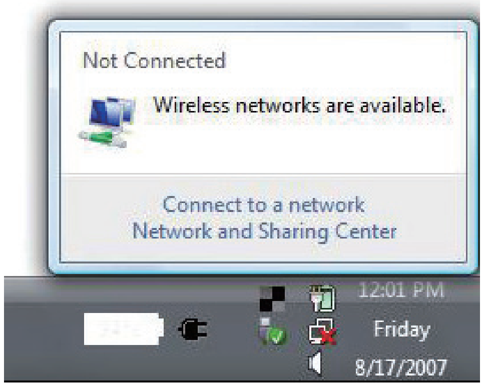
Windows Vista®

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.

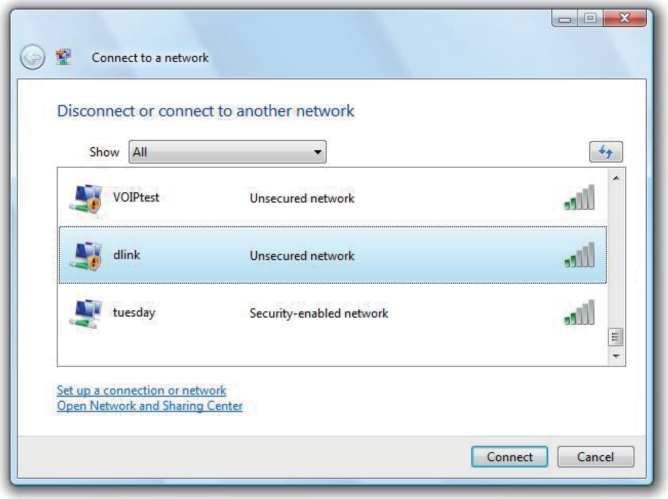
or

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.

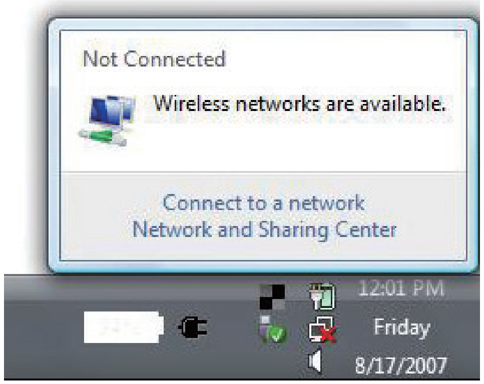
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



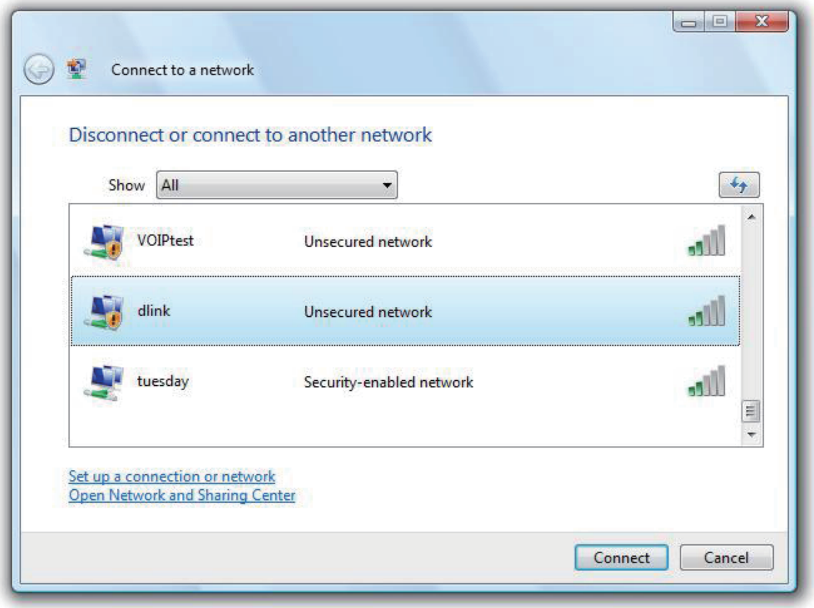
WPA/WPA2

It is recommended to enable 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 the screen). Select Connect to a network.



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


Connect to a network

Disconnect or connect to another network

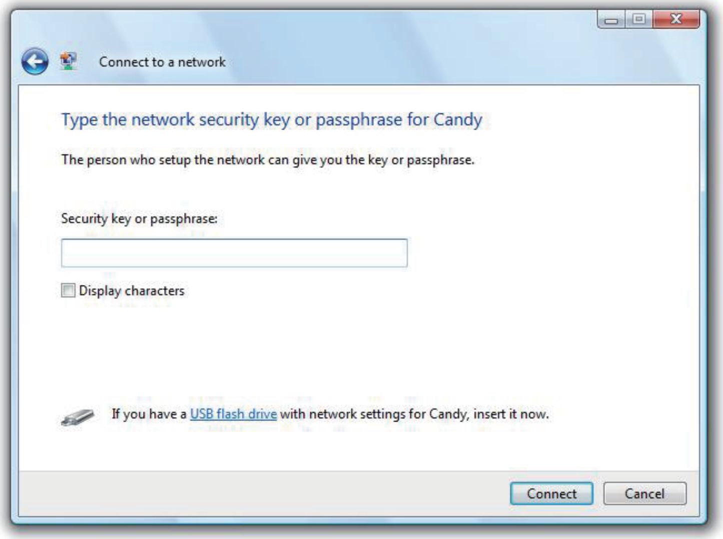
Show All

VOIPtest	Unsecured network	
dlink	Unsecured network	
tuesday	Security-enabled network	

Set up a connection or network
Open Network and Sharing Center

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

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



Connect to a network

Type the network security key or passphrase for Candy

The person who setup the network can give you the key or passphrase.

Security key or passphrase:

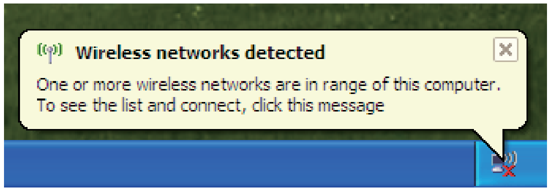
□ Display characters

If you have a USB flash drive with network settings for Candy, insert it now.

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.

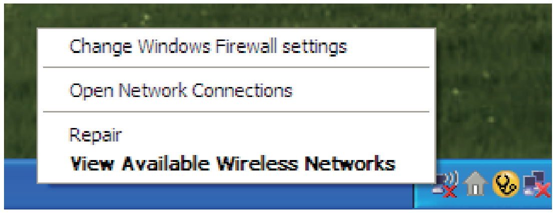
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.


Wireless networks detected

One or more wireless networks are in range of this computer. To see the list and connect, click this message

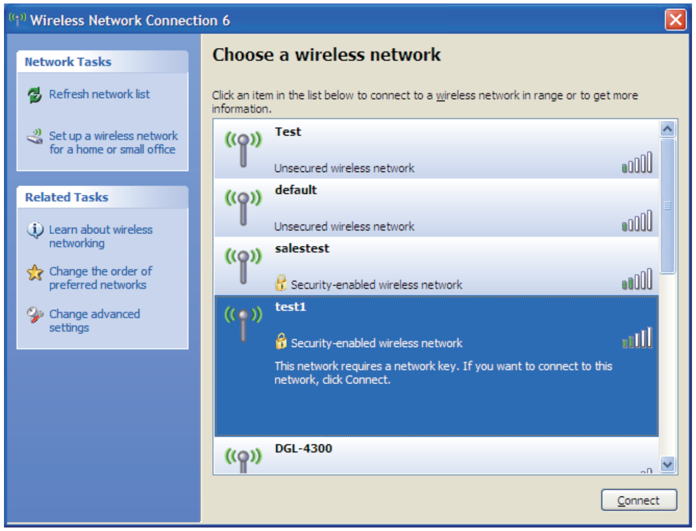
or

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


Change Windows Firewall settings
Open Network Connections
Repair
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 you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Connect

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

salestest
Security-enabled wireless network

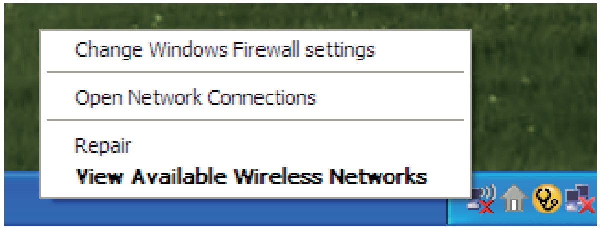
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

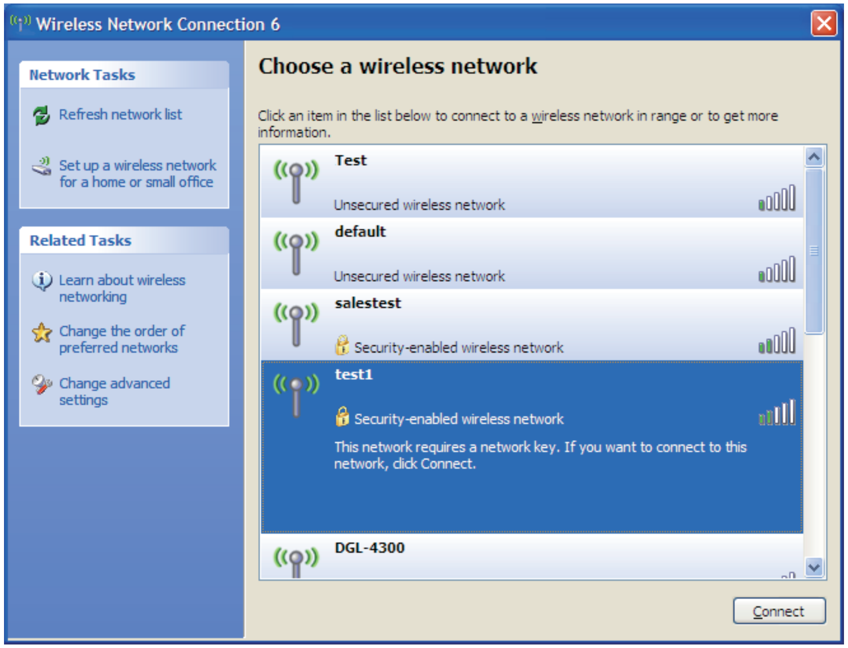
WPA/WPA2

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**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

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


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

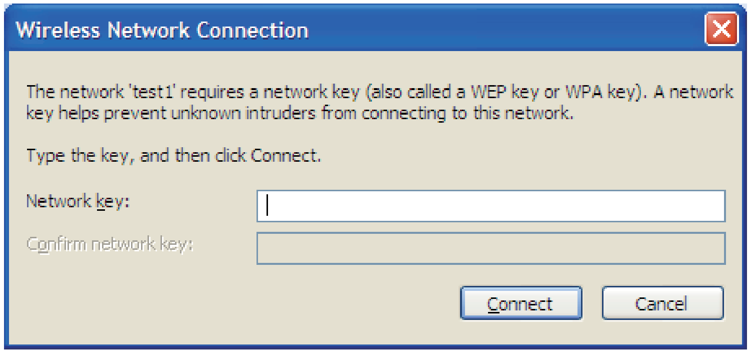
salestest
Security-enabled wireless network

test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

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

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



Wireless Network Connection

The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-925. 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 the following 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® 6.0 and higher
  - Mozilla Firefox 3.0 and higher
  - Google™ Chrome 2.0 and higher
  - Apple Safari 3.0 and higher

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

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

- Configure your Internet settings:

Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.

Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.

Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.

Close your web browser (if open) and open it.

- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.

- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

If you forgot your password, you must reset your router. Unfortunately 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, the username is **admin** and leave the password box empty.

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

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

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

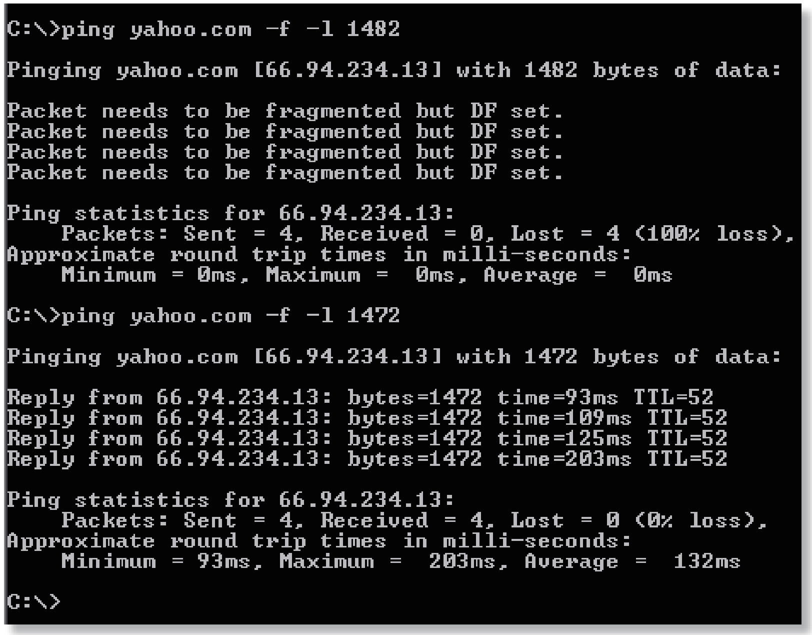
Click on **Start** and then click **Run**.

Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).

Once the window opens, you’ll need to do a special ping. Use the following syntax:

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

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



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

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

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

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

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

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

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

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

C:\>
```

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

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

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

- Open your browser, enter the IP address of your router (**192.168.0.1**) and click **OK**.

- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.

- Click on **Setup** and then click **Manual Configure**.

Wireless Basics

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

- 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

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

Where is wireless used?

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

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

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on WPA2 encryption. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

Infrastructure – All wireless clients will connect to an access point or wireless router.

Ad-Hoc – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DWR-925 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

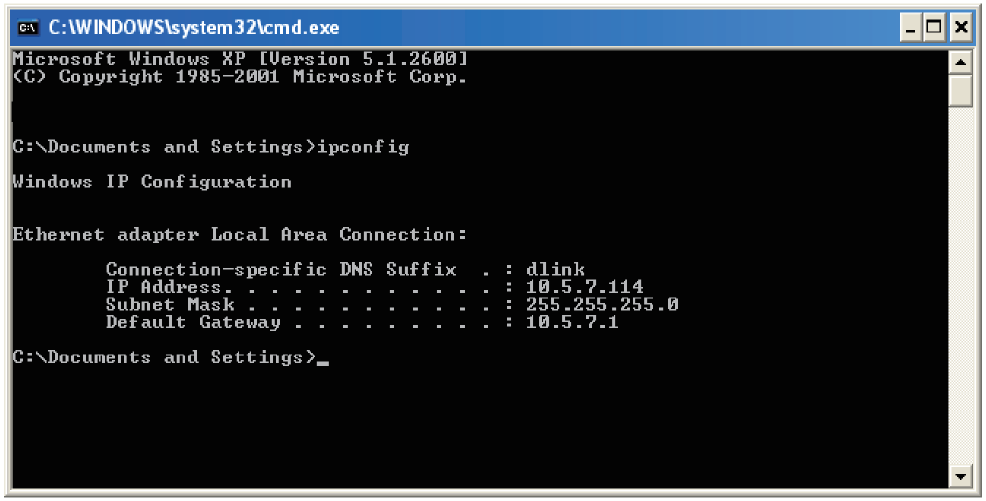
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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.



```
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**.

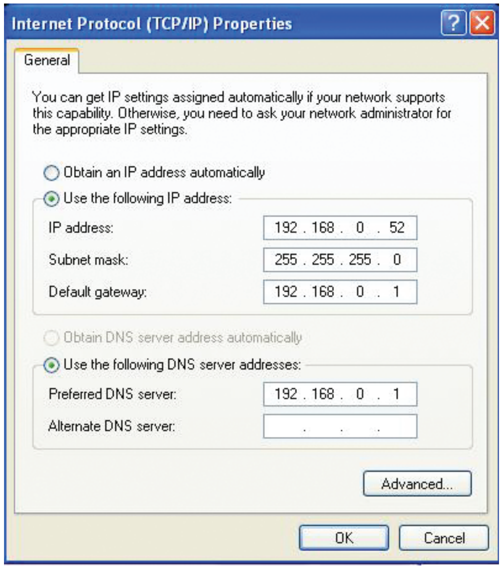
Step 2
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3
Highlight **Internet Protocol (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 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 Secondary DNS is not needed or you may enter a DNS server from your ISP.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 0 . 52
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server: . . .

Step 5
Click **OK** twice to save your settings.

Technical Specifications

Cellular Frequency Support

- LTE Cat. 3
- FDD Bands 1/3/7/8/20, TDD Band 40
- UMTS 850/900/1900/2100
- Quad-Band GSM/GPRS/EDGE

Cellular Data Throughput [2]

- LTE FDD up to 100 Mbps Downlink/50 Mbps Uplink
- LTE TDD up to 61 Mbps Downlink/18 Mbps Uplink
- UMTS/HSPA-DC Up to 42 Mbps Downlink/ 5.76 Uplink
- EDGE up to 236.8 kbps symmetrical

Wi-Fi Data Rates [2]

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

Standards

- 802.11n/g/b
- 802.11u
- 802.11i

Wireless Encryption

- 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/GRE VPN

Antenna

- 2x Detachable 3G / 4G antennas
- 2x Detachable Wi-Fi antennas

Ports

- 4x LAN (RJ-45)
- 1x WAN (RJ-45)
- 1x Serial

SIM Slot

- Standard 6-pin mini-SIM card interface

LED Status Indicators

- Signal strength
- WAN
- LAN
- WLAN
- LTE

Dimensions (L x W x H)

- 185 x 114.5 x 25.4 mm (7.28 x 4.51 x 1.00 inches)

Operating Temperature

- 0 to 50 °C (32 to 122 °F)

Storage Temperature

- -10 to 70 °C (14 to 158 °F)

Operating Humidity

- 10% to 90% (Non-condensing)

Storage Humidity

- 0 to 95% non-condensing

Certifications

- RCM
- RoHS
- Wi-Fi Certified

[1] Supported frequency band is dependent upon regional hardware version.
[2] Data rates are theoretical. Data transfer rate depends on network capacity and signal strength.