



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 19, 2014	• A2 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 StoreSM 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.

Copyright © 2014 by D-Link Corporation, Inc.

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

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

Preface	i	L2TP	18
Manual Revisions	i	4G LTE / 3G	19
Trademarks	i	GRE Settings	21
Product Overview	1	Wireless Settings	22
Package Contents	1	Wireless Connection Setup Wizard	22
System Requirements	2	Manual Wireless Connection Setup	25
Introduction	3	Network Settings	30
Features	4	DHCP Server Settings	31
Hardware Overview	5	IPv6 Setup	32
Rear Panel	5	Static IPv6	33
Front Panel	6	LAN IPv6 Address Settings	34
LEDs	7	PPPoE	35
Installation	8	LAN IPv6 Link-Local Address	36
Before you Begin	8	6 to 4	37
Wireless Installation Considerations	9	6rd	38
Configuration	10	Autoconfiguration	39
Web-based Configuration Utility	10	Message Service	40
Setup	11	SMS Remote	40
Internet Connection Setup Wizard	12	VPN Settings	41
Manual Internet Connection Setup	14	VPN Setup Wizard	41
Static IP (assigned by ISP)	14	Manual VPN Setup	43
Dynamic IP (DHCP)	15	VPN Dynamic IP	44
PPPoE	16	Advanced	46
PPTP	17	Virtual Server	46
		Application Rules	47
		QoS Engine	48

MAC Address Filter	49	Connecting a Wireless Client	74
URL Filter	50	WPS Button	74
Outbound Filter	51	Windows® 8	75
Inbound Filter	52	WPA/WPA2	75
SNMP	53	Windows® 7	77
Routing	54	WPA/WPA2	77
Advanced Wireless	55	WPS	80
Advanced Network	57	Windows Vista®	84
DMZ	58	WPA/WPA2	85
Tools	59	Windows® XP	87
Admin	59	WPA/WPA2	88
Time	60	Troubleshooting	90
Syslog	61	Wireless Basics	94
Email Settings	62	What is Wireless?	95
System	63	Tips	97
Firmware	64	Wireless Modes	98
Dynamic DNS	65	Networking Basics	99
System Check	66	Check your IP address	99
Schedules	67	Statically Assign an IP address	100
Status	68	Technical Specifications	101
Device Info	68	FCC Regulations	103
Log	69		
Statistics	70		
Wireless	71		
IPv6 Status	72		
Support	73		

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 will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based cable or DSL modem • IEEE 802.11n, 802.11g, or 802.11b wireless clients • 10/100 Ethernet • 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 6 or higher • Firefox 3.0 or higher • Safari 3.0 or higher • Chrome 2.0 or higher Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

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 secure 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.

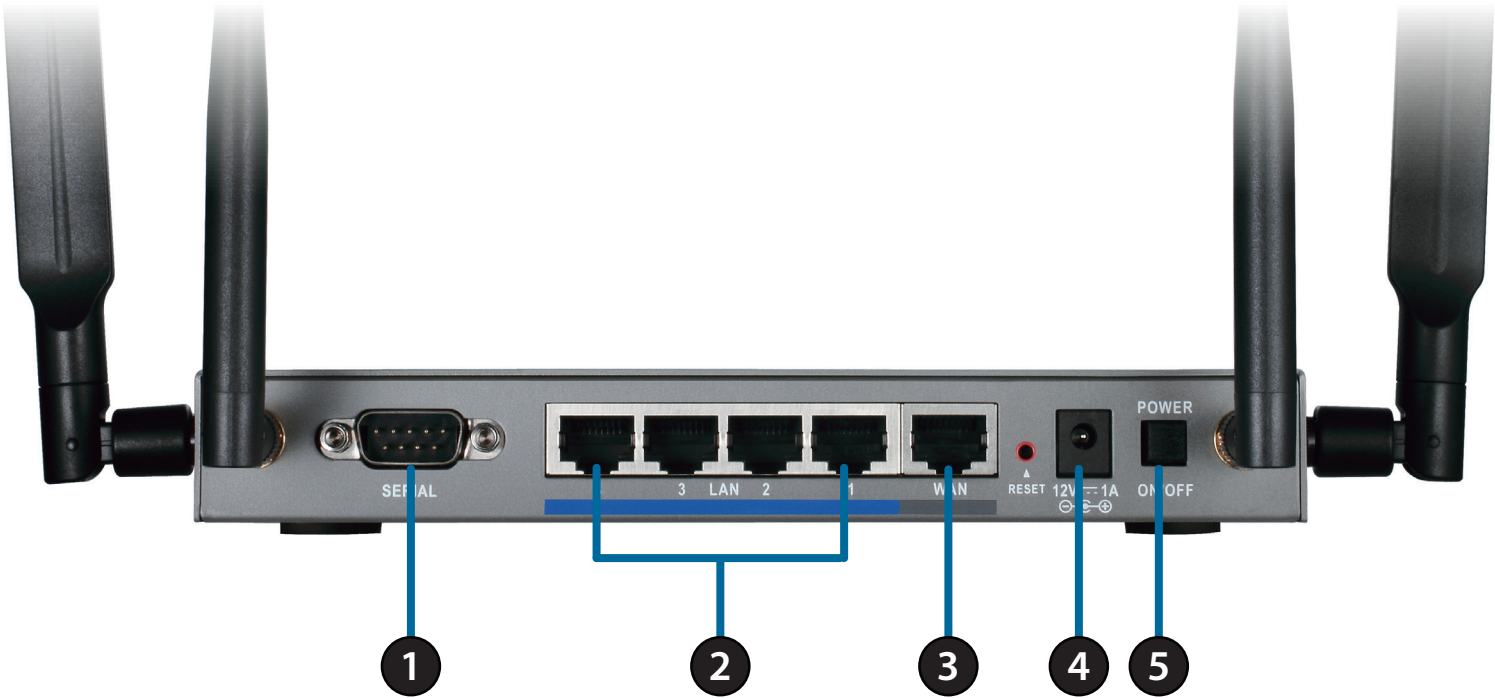
Features

- **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 56K 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 secure 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 includes 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.
- **Total Network Security** - The Wireless N router supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA/WPA2 standards ensures that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this router utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.
- **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

Rear Panel



1	Serial Port	Connect a computer to this port via a RS-232 cable to configure the router via CLI, or connect a dial-up modem to this port for WAN failover.
2	LAN Ports (1-4)	Connect Ethernet devices such as computers, switches, and NAS.
3	WAN Port	The auto MDI/MDIX Internet port connects to your cable or DSL modem via an Ethernet cable.
4	Power Receptor	Connects to the included power adapter.
5	Power Switch	Turns the device on or off.

Hardware Overview

Front Panel



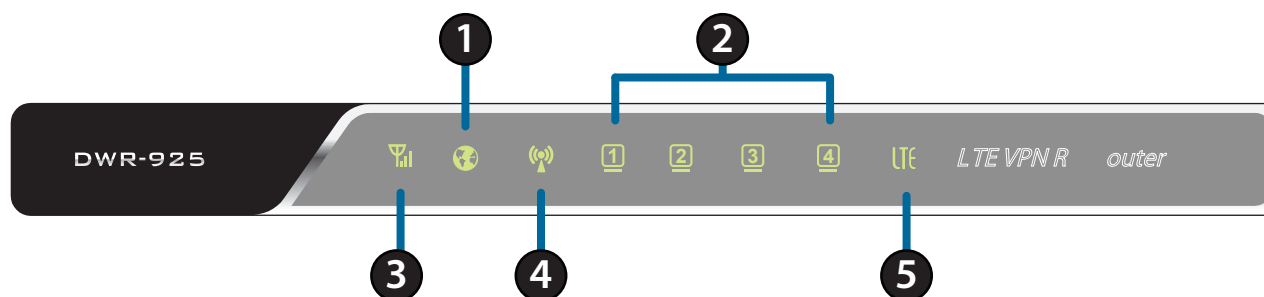
1

SIM Card Slot

Unscrew the cover and insert a 3G or 4G LTE SIM card into this slot for mobile broadband access.

Hardware Overview

LEDs



1	WAN	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
2	LAN (1-4)	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
3	Signal Strength	Blinking Red: No SIM card / signal or unverified PIN code Solid Red: Signal strength is at level one (weak) Solid Amber: Signal strength is at level two or three (medium) Solid Green: Signal strength is at level four or five (strong)
4	WLAN	Solid Green: WLAN is active and available Blinking Green: Data is being transferred via WLAN
5	LTE	Solid Green: UMTS/HSDPA/HSUPA/HSPA+/LTE connection is established Blinking: Data is being transferred via 3G or LTE

Installation

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

Before you Begin

1. Ensure that your DWR-925 is disconnected and powered off.
2. Insert a standard (U)SIM card into the SIM card slot on the back of the router as indicated by the SIM card logo next to the slot. The gold contacts should face downwards.

Caution: Always unplug/power down the router before installing or removing the SIM card. Never insert or remove the SIM card while the router is in use.

3. Connect the power adapter to the socket on the back panel of your DWR-925. Plug the other end of the power adapter into a wall outlet or power strip and turn the device on.
 - a. The Status LED will light up to indicate that power has been supplied to the router.
 - b. The LEDs on the front panel will flash on and off as the DWR-925 performs initialization and Internet connection processes.

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:

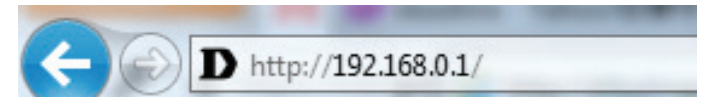
1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between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



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 90 for assistance.

A screenshot of the "LOGIN" page of the D-Link mobile router configuration utility. The page has an orange header with the word "LOGIN". Below the header, it says "Log in to the router :". There are two input fields: "User Name :" and "Password :". A "Log In" button is located to the right of the password field.

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.

A screenshot of the "STATUS > DEVICE INFO" page of the D-Link mobile router configuration utility. The page has a top navigation bar with tabs: "SETUP", "ADVANCED", "TOOLS", and "STATUS". The "STATUS" tab is selected. Below the navigation bar, there is a section titled "DEVICE INFORMATION" with an orange header. The text in this section says: "All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here." There is a "Refresh" button below this text. Below the "DEVICE INFORMATION" section, there is a "GENERAL" section with a black header. The text in this section says: "Time : Sun Sep 16, 2012 22:06:03 -0800" and "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 setup 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 14.

SETUP	ADVANCED	TOOLS	STATUS
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.			
Internet Connection Setup Wizard			
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.			
Manual Internet Connection Setup			

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.

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

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

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.

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

STEP 1: SET YOUR PASSWORD

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

Password :

Verify Password :

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 :

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.

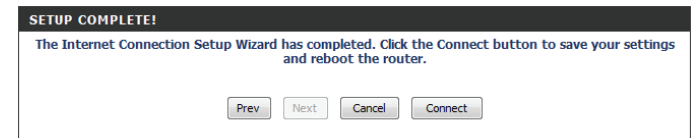
The subsequent configuration pages will differ depending on the selection you make on this page.

- | | |
|--|--|
| 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 14 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 15 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 16 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 17 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 18 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 19 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.



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 in 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.

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.

INTERNET CONNECTION TYPE	
Choose the mode to be used by the router to connect to the Internet.	
My Internet Connection is	Static IP
Failover Internet Type is	Disable (N/A)

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 :	(bytes) MTU default = 1500
MAC Address :	Clone

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.

The screenshot shows a web interface for configuring a Dynamic IP (DHCP) Internet connection. The title is "DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE". Below the title is a note: "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." The form contains several fields: "Host Name" with a text input box; "Primary DNS Server" with a text input box; "Secondary DNS Server" with a text input box; "MTU" with a text input box and a label "(bytes) MTU default = 1500"; "MAC Address" with a text input box and a "Clone" button; and "Auto-reconnect" with a checked checkbox and the label "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.

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

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

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

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

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

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

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

MAC Address: 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.

The screenshot shows the PPPoE configuration window. It has a title bar 'PPPoE' and a subtitle 'Enter the information provided by your Internet Service Provider (ISP)'. The fields are as follows:

- Username :** Text input field.
- Password :** Password input field.
- Verify Password :** Password input field.
- Service Name :** Text input field with '(optional)' label.
- IP Address :** Text input field.
- Primary DNS Server :** Text input field with '(optional)' label.
- Secondary DNS Server :** Text input field with '(optional)' label.
- MAC Address :** Text input field with a 'Clone' button next to it.
- Maximum Idle Time :** A numeric input field set to '600' with a 'seconds' label.
- MTU :** A numeric input field set to '0' with '(bytes) MTU default = 1492' label.
- Auto-reconnect :** A checkbox labeled 'Enable'.

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.

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 time period defined by the **Maximum Idle Time** setting.

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

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 : seconds

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.

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

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

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

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

The screenshot shows the L2TP configuration window. At the top, it says 'L2TP' and 'Enter the information provided by your Internet Service Provider (ISP)'. Below this, there are several fields: 'Address Mode' with radio buttons for 'Dynamic IP' and 'Static IP' (the latter is selected); 'L2TP IP Address', 'L2TP Subnet Mask', 'L2TP Gateway IP Address', and 'L2TP Server IP Address' each with a text input field; 'Username' and 'Password' with text input fields; 'Verify Password' with a text input field; 'Reconnect Mode' with radio buttons for 'Always-on' (selected) and 'Connect-on-demand'; and 'Maximum Idle Time' with a numeric input field set to '300' and the unit 'seconds'.

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.

3G Network Choose between **WCDMA/HSPA** or **CDMA2000/EV-DO**.

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** detection. The default authentication method is **Auto**.

APN: Enter the APN information (optional).

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

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

INTERNET CONNECTION TYPE	
Choose the mode to be used by the router to connect to the Internet.	
My Internet Connection is	4G LTE / 3G
Failover Internet Type is	Disable (N/A)
4G LTE / 3G INTERNET CONNECTION TYPE	
Enter the information provided by your Internet Service Provider (ISP).	
Country :	Others
Telecom :	Others
3G Network :	WCDMA/HSPA
Username :	(optional)
Password :	(optional)
Verify Password :	(optional)
Dialed Number :	*99#
Authentication :	Auto
APN :	internet (optional)
Pin Code :	
Reconnect Mode :	☒ Auto ☐ Manual
Maximum Idle Time :	600 seconds
Primary DNS Server :	172.22.1.201
Secondary DNS Server :	
Keep Alive :	☒ Disable ☐ Use Ping
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.

4G LTE /3G INTERNET CONNECTION TYPE
Enter the information provided by your Internet Service Provider (ISP).

Country : Others
Telecom : Others
3G Network : WCDMA/HSPA
Username : (optional)
Password : (optional)
Verify Password : (optional)
Dialed Number : *99#
Authentication : Auto
APN : internet (optional)
Pin Code :
Reconnect Mode : Auto Manual
Maximum Idle Time : 600 seconds
Primary DNS Server : 172.22.1.201
Secondary DNS Server :
Keep Alive : Disable Use Ping
Bridge ethernet ports : Enable
NAT disable : Enable

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 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	Enable
1							☐
2							☐
3							☐
4							☐
5							☐
6							☐
7							☐
8							☐

Default Gateway: None

TUNNELS INFORMATION

ID	Transmitted Packets	Transmitted Bytes	Received Packets	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

Refresh

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 25. 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 24.

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.

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

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

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

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) :

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 TKIP

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 ASCII

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 different 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.

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.

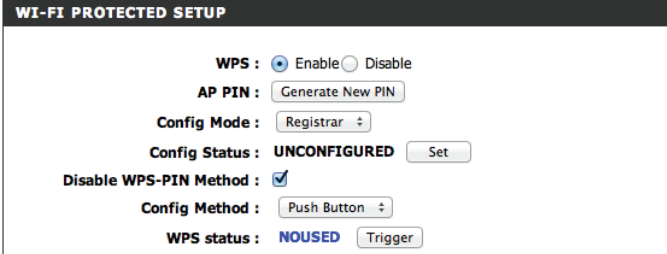
Config Status: Press **Set** to switch between **Configured** and **Unconfigured** states.

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.



The screenshot shows the 'WI-FI PROTECTED SETUP' configuration interface. It includes the following elements:

- WPS:** Radio buttons for 'Enable' (selected) and 'Disable'.
- AP PIN:** A 'Generate New PIN' button.
- Config Mode:** A dropdown menu currently set to 'Registrar'.
- Config Status:** A status indicator showing 'UNCONFIGURED' and a 'Set' button to toggle between 'Configured' and 'Unconfigured'.
- Disable WPS-PIN Method:** A checkbox that is checked.
- Config Method:** A dropdown menu currently set to 'Push Button'.
- WPS status:** A status indicator showing 'NOUSED' and a 'Trigger' button.

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.

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

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

802.11 Mode: **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.

SETUP	ADVANCED	TOOLS	STATUS
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 device supports three wireless security modes including: WEP, WPA and WPA2. Save Settings Don't Save Settings			
WIRELESS NETWORK SETTINGS Enable Wireless : ☒ Wireless Network Name : dlinkrouter (Also called the SSID) 802.11 Mode : B/G/N mixed Auto Channel Scan : ☐ Wireless Channel : 2.462 GHz - CH 11 Visibility Status : ☒ Visible ☐ Invisible			

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 SECURITY MODE	
Security Mode :	None ▾

WEP

- Authentication:** Select whether to use **Open** or **Shared** authentication.
- WEP Encryption:** Select whether to use **64-bit** or **128-bit** encryption.
- 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.

The screenshot shows the 'WIRELESS SECURITY MODE' configuration page. At the top, 'Security Mode' is set to 'WEP'. Below this, the 'WEP' section contains explanatory text about the standard and key entry requirements. It specifies that for 64-bit keys, 10 hex digits are needed, and for 128-bit keys, 26 hex digits are needed. It also notes that a text string can be entered and will be converted to a hexadecimal key. The configuration options at the bottom are: 'Authentication' set to 'Open', 'WEP Encryption' set to '64Bit', 'Default WEP Key' set to 'WEP Key 1', and 'WEP Key' set to 'HEX' with the value '1234567890' entered in the text box. A note below the text box indicates '(5 ASCII or 10 HEX)' characters are allowed.

WIRELESS SECURITY MODE

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.

Authentication : Open

WEP Encryption : 64Bit

Default WEP Key : WEP Key 1

WEP Key : HEX 1234567890
(5 ASCII or 10 HEX)

WPA-Personal

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

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

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

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 : WPA only

Cipher Type : AES

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 : 7c9aeccad9c6b0c05343ed8874754b747ffd2

(8~63 ASCII or 64 HEX)

WPA-Enterprise

WPA Mode: Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can support this security method.

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.

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	
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(COMP) 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 :	WPA only ▼
Cipher Type :	AES ▼
EAP (802.1X)	
When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.	
RADIUS Server IP Address :	0.0.0.0
RADIUS server Port :	1812
RADIUS server Shared Secret :	

Network Settings

This section will help you to change the internal network settings of your router and to configure the DHCP server settings. After modifying any settings, click **Save Settings** to save your changes.

Router IP Address: Enter the IP address of the router. The default IP address is **192.168.0.1**.

If you change the IP address, once you click **Save Settings**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

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

ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :

192.168.0.1

Default Subnet Mask :

255.255.255.0

Local Domain Name :

DHCP Server 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. After modifying any settings, click **Save Settings** to save your changes.

- Enable DHCP Server:

Select this box to enable the DHCP server on your router.
- DHCP IP Address Range:

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

Enter the lease time for IP address assignments.
- Primary DNS IP Address:

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

Enter the secondary DNS IP address that will be assigned to DHCP clients.
- 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.

DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server :

☒

DHCP IP Address Range :

50

 to

199

 (addresses within the LAN subnet)

DHCP Lease Time :

86400

 (Seconds)

Primary DNS IP Address :

Secondary DNS IP Address :

Primary WINS IP Address :

Secondary WINS IP Address :

IPv6 Setup

There are several 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.

SETUP	ADVANCED	TOOLS	STATUS
IPv6 Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method, please contact your Internet Service Provider. Save Settings Don't Save Settings			
6 TO 4 SETTINGS Choose the mode to be used by the router to connect to the IPv6 Internet. IPv6 : ☐ Disable ☒ Enable IPv6 Connection : Static IPv6			
ROUTER ADVERTISEMENT LIFETIME Remote IPv4 Address : Local IPv4 Address : 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:fe94:814 /64			

Static IPv6

- IPv6:

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

Select **Static IPv6** from the drop-down menu.
- Remote IPv4 Address:

Enter the remote IPv4 address.
- Local IPv4 Address:

Enter the local IPv4 address.
- 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:

Tick to enable the autoconfiguration feature.
- Autoconfiguration Type:

Select **SLAAC + Stateless DHCPv6** or **Stateful (DHCPv6)**.
- Router Advertisement Lifetime:

Enter the IPv6 Address Lifetime (in seconds).
- DS-Lite Enable:

Tick to enable DS-Lite.
- DS-Lite Configuration:

Tick **Manual Configuration** to configure this setting.
- AFTR IPv6 Address:

Enter the AFTR IPv6 address supplied by your service provider.

SETUP

ADVANCED

TOOLS

STATUS

IPv6

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

Save Settings

Don't Save Settings

6 TO 4 SETTINGS

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

IPv6 : ☐ Disable ☒ Enable

IPv6 Connection : Static IPv6

ROUTER ADVERTISEMENT LIFETIME

Remote IPv4 Address :

Local IPv4 Address :

Default Gateway :

Primary DNS Address :

Secondary DNS Address :

LAN IPV6 ADDRESS SETTINGS

Use this 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:fe94:814 /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration : ☒

Autoconfiguration Type : SLAAC+Stateless DHCPv6

Router Advertisement Lifetime : 300 seconds

DS-LITE

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

DS-Lite Enable : ☐

DS-Lite Configuration : ☒ DS-Lite DHCPv6 Option ☐ Manual Configuration

AFTR IPv6 Address :

LAN IPv6 Address Settings

IPv6:	Tick to Enable IPv6 tunneling.
IPv6 Connection:	Select LAN IPv6 Address Settings from the drop-down menu.
Primary/Secondary DNS Addresses:	Enter the primary and secondary DNS addresses here.
Enable DHCP-PD:	Tick 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:	Tick to enable the autoconfiguration feature.
Autoconfiguration Type:	Select SLAAC + Stateless DHCPv6 or Stateful (DHCPv6) .
Router Advertisement Lifetime:	Enter the IPv6 address lifetime (in seconds).
DS-Lite Enable:	Tick to enable DS-Lite.
DS-Lite Configuration:	Tick DS-Lite DHCPv6 Option or Manual Configuration .
AFTR IPv6 Address:	Enter the AFTR IPv6 address supplied by your service provider.

6 TO 4 SETTINGS

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

IPv6 : ☐ Disable ☒ Enable

IPv6 Connection : LAN IPv6 Address Settings

IPv6 DNS SETTINGS

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

☒ When configuring the router to access the IPv6 internet be sure to choose the correct IPv6 Connection Type from the drop down menu. If you are unsure of which option to choose, contact your internet Service Provider(ISP.)

☐ Use the following DNS address

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 ADDRESS SETTINGS

Use this 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 : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration : ☐

Autoconfiguration Type : SLAAC+Stateless DHCPv6

Router Advertisement Lifetime : seconds

DS-LITE

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

DS-Lite Enable : ☐

DS-Lite Configuration : ☒ DS-Lite DHCPv6 Option ☐ Manual Configuration

AFTR IPv6 Address :

PPPoE

IPv6:	Tick to Enable IPv6 tunneling.
IPv6 Connection:	Select LAN IPv6 Address Settings from the drop-down menu.
LAN IPv6 Address:	Enter the LAN IPv6 address.
Password:	Enter the password for your LAN IPv6.
Local IPv6 Address:	Enter your local IPv6 Address.
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:	Tick 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:	Tick to enable the autoconfiguration feature.
Autoconfiguration Type:	Select SLAAC + Stateless DHCPv6 or Stateful (DHCPv6) .
Router Advertisement Lifetime:	Enter the IPv6 address lifetime (in seconds).

6 TO 4 SETTINGS
 Choose the mode to be used by the router to connect to the IPv6 Internet.

IPv6 : ☐ Disable ☒ Enable
 IPv6 Connection : PPPoE

PPPOE SETTINGS
 LAN IPv6 Address :
 Password :
 Local IPv6 Address :
 MTU :

IPv6 DNS SETTINGS
 Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method, please contact your Internet Service Provider. : ☒ When configuring the router to access the IPv6 internet be sure to choose the correct IPv6 Connection Type from the drop down menu. If you are unsure of which option to choose, contact your Internet Service Provider (ISP.)
☐ 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 : /64

LAN ADDRESS AUTOCONFIGURATION SETTINGS
 Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Autoconfiguration : ☐
 Autoconfiguration Type : SLAAC+Stateless DHCPv6
 Router Advertisement Lifetime : seconds

LAN IPv6 Link-Local Address

- IPv6:

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

Select **LAN IPv6 Link-Local Address** from the drop-down menu.
- Remote IPv4 Address:

Enter the remote IPv4 address.
- Local IPv4 Address:

Enter the local IPv4 address.
- Local IPv6 Address:

Enter the local IPv6 address.
- DNS Setting:

Choose to automatically obtain the DNS server address or to set manually.
- 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:

Tick to enable the autoconfiguration feature.
- Autoconfiguration Type:

Select **SLAAC + Stateless DHCPv6** or **Stateful (DHCPv6)**.
- Router Advertisement Lifetime:

Enter the IPv6 address lifetime (in seconds).

6 TO 4 SETTINGS

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

IPv6 :

☐ Disable ☒ Enable

IPv6 Connection :

LAN IPv6 Link-Local Address ▾

LAN ADDRESS AUTOCONFIGURATION SETTINGS

Remote IPv4 Address :

Local IPv4 Address :

Local IPv6 Address :

/64

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.

LAN IPv6 Address :

/64

LAN IPv6 Link-Local Address :

/64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration :

☐

Autoconfiguration Type :

SLAAC +Stateless DHCPv6 ▾

Router Advertisement Lifetime :

seconds

6 to 4

- IPv6:

Tick **Enable** to activate IPv6 tunneling.
- IPv6 Connection:

Select **6 to 4** from the drop-down menu.
- 6 to 4 Address:

Displays the IPv6 settings supplied by your Internet Service Provider (ISP).
- Primary/Secondary DNS Address:

Enter the primary and secondary DNS server addresses.
- LAN IPv6 Address:

Displays the LAN (local) IPv6 address for the router.
- LAN IPv6 Link-Local Address:

Displays the router’s LAN link-local address.
- Enable Autoconfiguration:

Tick to enable the autoconfiguration feature.
- Autoconfiguration Type:

Select **Stateful (DHCPv6)** or **SLAAC+Stateless DHCPv6** autoconfiguration.
- Router Advertisement Lifetime:

Enter the IPv6 address lifetime (in seconds).

6 TO 4 SETTINGS

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

IPv6 :

☐ Disable

☒ Enable

IPv6 Connection :

6 to 4

6 TO 4 SETTINGS

6 to 4 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.

LAN IPv6 Address :

/64

LAN IPv6 Link-Local Address :

/64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration :

☐

Autoconfiguration Type :

SLAAC+Stateless DHCPv6

Router Advertisement Lifetime :

seconds

6rd

- IPv6:

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

Select **6rd** from the drop-down menu.
- Remote IPv4 Address:

Enter the IPv4 (remote) address here.
- IPv4 Mask Length:

Enter the mask length of the IPv4 address.
- Remote Prefix:

Enter the remote prefix of the IPv4 address.
- Prefix Length:

Enter the length of the remote prefix.
- Primary/Secondary DNS Addresses:

Enter the DNS server addresses.
- LAN IPv6 Address:

Displays the LAN (local) IPv6 address for the router.
- LAN IPv6 Link-Local Address:

Displays the router’s LAN link-local address.
- Enable Autoconfiguration:

Tick to enable the autoconfiguration feature.
- Autoconfiguration Type:

Select **Stateful (DHCPv6)** or **SLAAC+Stateless DHCPv6** autoconfiguration.
- Router Advertisement Lifetime:

Enter the IPv6 address lifetime (in seconds).

6 TO 4 SETTINGS

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

IPv6 :

☐ Disable ☒ Enable

IPv6 Connection :

6rd

6RD SETTINGS

Remote IPv4 Address :

IPv4 Mask Length :

Remote Prefix :

 ::

Prefix Length :

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 :

/64

LAN ADDRESS AUTOCONFIGURATION SETTINGS

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

Enable Autoconfiguration :

☐

Autoconfiguration Type :

SLAAC+Stateless DHCPv6

Router Advertisement Lifetime :

 seconds

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.

6 TO 4 SETTINGS

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

IPv6 :

☐ Disable

☒ Enable

IPv6 Connection :

Autoconfiguration Type

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 :

/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.

SMS Inbox

CREATE MESSAGE

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

Create Message

SMS Remote

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

Remote Management via SMS: Enable or disable remote management via SMS.

Access Control List: Enter phone numbers to receive messages and tick the checkbox next to **Notification** to enable this feature.

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.

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

Click **Next** to continue.

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

Click **Next** to continue.

Enter the **Remote Gateway** address.

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?

Prev Next Cancel

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

Prev Next Cancel

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

Remote Subnet :

Remote Netmask :

Prev Next Cancel

STEP 2: SET THE IP ADDRESS OF REMOTE GATEWAY

Remote Gateway :

Prev Next Cancel

Set your **Preshared Key**.

Click **Next** to continue.

STEP 3: SET THE PRE-SHARED KEY

Preshare Key :

Prev

Next

Cancel

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

Prev

Next

Cancel

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 :

Prev

Next

Cancel

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 passthrough. If you connect to another NAT router which doesn't support IPSec passthrough on the WAN side, you need to activate this option.

VPN Statistic: Tick this box to enable VPN Statistic options.

Max Number of Tunnels: The device supports 1~10 tunnels.

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 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

VPN Statistic : ☐ Enabled

Max. number of tunnels :

DYNAMIC VPN SETTING

VPN Dynamic IP Setting : ☐ Enable [More](#)

TUNNEL SETTINGS

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1	Tunnel#1	255.255.255.0/ 0.0.0.255	224.52.45.2	Connecting...	More Disconnect	☒
2					More	☐
3					More	☐
4					More	☐
5					More	☐

[XAUTH account](#)
[Refresh](#)

[PPTP Client](#)
[PPTP Server](#)
[L2TP Client](#)
[L2TP Server](#)

VPN Dynamic IP

- Tunnel Name:** Enter a name for your VPN.
- 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.
- Set IKE Proposal:** Tick this box to enable IKE Proposal.
- Set IPSEC Proposal:** Tick this box to enable IPsec Proposal.

The screenshot shows the 'VPN DYNAMIC IP SETTING' configuration window. It contains the following fields and options:

- Tunnel Name :** Text input field.
- Local Subnet :** Text input field.
- Local Netmask :** Text input field.
- Phase1 Key Life Time :** Text input field followed by 'seconds'.
- Phase2 Key Life Time :** Text input field followed by 'seconds'.
- Encapsulation Protocol :** Drop-down menu with 'ESP' selected.
- PFS Group :** Drop-down menu with 'Disable' selected.
- Preshare Key :** Text input field.
- Remote ID :** Drop-down menu with 'Type: Username' selected, followed by an 'ID:' text input field.
- Local ID :** Drop-down menu with 'Type: Username' selected, followed by an 'ID:' text input field.
- Dead Peer Detection (DPD) :**
 - ☐ Enable
 - If enabled, 'Timeout : 180 Second(s)' and 'Delay : 30 Second(s)' are shown.
- XAUTH :**
 - ☒ None
 - ☐ Server
- Set IKE Proposal :** ☐ Enable
- Set IPSEC Proposal :** ☐ Enable

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 67.

SETUP

ADVANCED

TOOLS

STATUS

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.

Save Settings

Don't Save Settings

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.

SETUP	ADVANCED	TOOLS	STATUS																																																				
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. Save Settings Don't Save Settings																																																							
Popular applications -- select one -- Copy to ID -- --																																																							
APPLICATION RULES <table border="1"> <thead> <tr> <th>ID</th> <th>Trigger</th> <th>Incoming Ports</th> <th>Enable</th> </tr> </thead> <tbody> <tr><td>1</td><td> </td><td> </td><td>☐</td></tr> <tr><td>2</td><td> </td><td> </td><td>☐</td></tr> <tr><td>3</td><td> </td><td> </td><td>☐</td></tr> <tr><td>4</td><td> </td><td> </td><td>☐</td></tr> <tr><td>5</td><td> </td><td> </td><td>☐</td></tr> <tr><td>6</td><td> </td><td> </td><td>☐</td></tr> <tr><td>7</td><td> </td><td> </td><td>☐</td></tr> <tr><td>8</td><td> </td><td> </td><td>☐</td></tr> <tr><td>9</td><td> </td><td> </td><td>☐</td></tr> <tr><td>10</td><td> </td><td> </td><td>☐</td></tr> <tr><td>11</td><td> </td><td> </td><td>☐</td></tr> <tr><td>12</td><td> </td><td> </td><td>☐</td></tr> </tbody> </table>				ID	Trigger	Incoming Ports	Enable	1			☐	2			☐	3			☐	4			☐	5			☐	6			☐	7			☐	8			☐	9			☐	10			☐	11			☐	12			☐
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 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 67.

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 67.

SETUP	ADVANCED	TOOLS	STATUS																																															
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. Save Settings Don't Save Settings																																																		
QOS ENGINE SETUP Enable QoS Packet Filter : ☐ Upstream bandwidth : kbps Use schedule rule: ---ALWAYS ON--- Copy to ID -- --																																																		
QOS RULES <table border="1"> <thead> <tr> <th>ID</th> <th>Local IP : Ports</th> <th>Remote IP : Ports</th> <th>QoS Priority</th> <th>Enable</th> <th>Use Rule#</th> </tr> </thead> <tbody> <tr><td>1</td><td> </td><td> </td><td>High ▼</td><td>☐</td><td><input data-rs="8" type="button" value="Add New Rule..."/></td></tr> <tr><td>2</td><td> </td><td> </td><td>High ▼</td><td>☐</td></tr> <tr><td>3</td><td> </td><td> </td><td>High ▼</td><td>☐</td></tr> <tr><td>4</td><td> </td><td> </td><td>High ▼</td><td>☐</td></tr> <tr><td>5</td><td> </td><td> </td><td>High ▼</td><td>☐</td></tr> <tr><td>6</td><td> </td><td> </td><td>High ▼</td><td>☐</td></tr> <tr><td>7</td><td> </td><td> </td><td>High ▼</td><td>☐</td></tr> <tr><td>8</td><td> </td><td> </td><td>High ▼</td><td>☐</td></tr> </tbody> </table>				ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#	1			High ▼	☐	<input data-rs="8" type="button" value="Add New Rule..."/>	2			High ▼	☐	3			High ▼	☐	4			High ▼	☐	5			High ▼	☐	6			High ▼	☐	7			High ▼	☐	8			High ▼	☐
ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#																																													
1			High ▼	☐	<input data-rs="8" type="button" value="Add New Rule..."/>																																													
2			High ▼	☐																																														
3			High ▼	☐																																														
4			High ▼	☐																																														
5			High ▼	☐																																														
6			High ▼	☐																																														
7			High ▼	☐																																														
8			High ▼	☐																																														

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 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 lick **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.

SETUP

ADVANCED

TOOLS

STATUS

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

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 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.

SETUP

ADVANCED

TOOLS

STATUS

URL FILTER

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

Save Settings

Don't Save Settings

URL FILTERING SETTING

URL Filtering : ☐ Enable

URL FILTERING RULES

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

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 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 67.

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.

SETUP

ADVANCED

TOOLS

STATUS

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

Inbound Filter

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

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 67.

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.

SETUP

ADVANCED

TOOLS

STATUS

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

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 access SNMP access, enter the IP address of the remote computer you will use to access this device; all other IP addresses will be denied remote SNMP access.

SETUP

ADVANCED

TOOLS

STATUS

SNMP

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

Save Settings

Don't Save Settings

SNMP

SNMP Local :
SNMP Remote :
Get Community :
Set Community :
IP 1 :
IP 2 :
IP 3 :
IP 4 :
SNMP Version :
WAN Access IP Address :

☐ Enabled ☒ Disabled

☐ Enabled ☒ Disabled

☒ V1 ☐ V2c

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.

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

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

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

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

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

Enable: Select this box to enable the rule.

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

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

- 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**.

SETUP	ADVANCED	TOOLS	STATUS
ADVANCED WIRELESS			
If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.			
Save Settings Don't Save 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		

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.

SETUP

ADVANCED

TOOLS

STATUS

ADVANCED WIRELESS

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

Save Settings

Don't Save 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 one of our 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.

SETUP

ADVANCED

TOOLS

STATUS

ADVANCED NETWORK

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

Save Settings

Don't Save 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.

SETUP

ADVANCED

TOOLS

STATUS

DMZ

DMZ setting

Save Settings

Don't Save Settings

FIREWALL SETTINGS

Enable SPI : ☐

DMZ HOST

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 :

Computer Name ▼

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

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

REMOTE MANAGEMENT

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. If you enter an asterisk (*) in this field, then anyone will be able to access the router. Adding an asterisk (*) into this field could present a security risk and is not recommended.

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

SETUP	ADVANCED	TOOLS	STATUS
ADMINISTRATOR SETTINGS			
To help secure your network, we recommend that you should choose a new password.			
Save Settings Don't Save Settings			
ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "admin")			
New Password :			
Confirm Password :			
REMOTE MANAGEMENT			
Enable Remote Management : ☒ Enabled			
IP Allowed to Access : 0.0.0.0			
Port : 1080 1080			

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.

SETUP	ADVANCED	TOOLS	STATUS
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. Save Settings Don't Save Settings			
TIME AND DATE CONFIGURATION			
Time :		Fri May 09, 2014 06:10:07	
Time Zone :		(GMT -12:00) Eniwetok, Kwajalein	
Enable Daylight Saving :		☐ Sync. your computer's time settings	
AUTOMATIC TIME AND DATE CONFIGURATION			
☒ Automatically synchronize with Internet time server			
NTP Server Used :		ntp1.dlink.com Update Now	

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.

SETUP

ADVANCED

TOOLS

STATUS

SYSLOG

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

Save Settings

Don't Save Settings

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.

SETUP

ADVANCED

TOOLS

STATUS

EMAIL SETTINGS

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

Save Settings

Don't Save Settings

EMAIL SETTINGS

Enable Email Notification :

☐

SMTP Server IP and Port :

:

SMTP Username :

SMTP Password :

Send E-mail alert to :

▲

▼

E-mail Subject :

Email Log Now

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.

Save Settings To Local Hard Drive

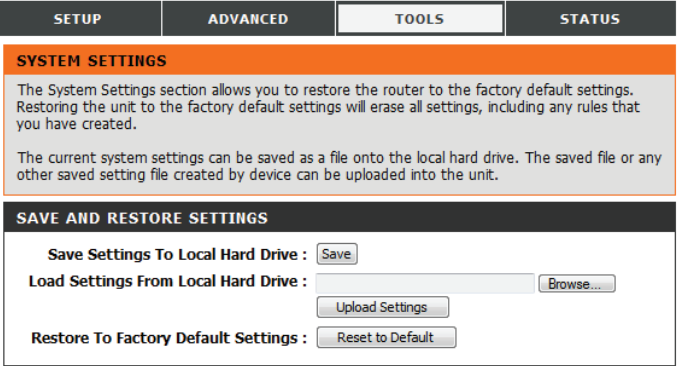
Use this option to save your current router configuration settings to a file. Click **Save** to open a file dialog, and then select a location and file name for the settings.

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.

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

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

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

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

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

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

SETUP	ADVANCED	TOOLS	STATUS
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 : Browse... Upgrade Cancel Accept unofficial firmware. ☐			

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.

SETUP	ADVANCED	TOOLS	STATUS										
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. Save Settings Don't Save Settings													
DYNAMIC DNS <table><tr><td>Enable DDNS :</td><td>☐</td></tr><tr><td>Provider :</td><td> DynDNS.org(Dynamic) </td></tr><tr><td>Host Name :</td><td> </td></tr><tr><td>Username / E-mail :</td><td> </td></tr><tr><td>Password / Key :</td><td> </td></tr></table>				Enable DDNS :	☐	Provider :	DynDNS.org(Dynamic)	Host Name :		Username / E-mail :		Password / Key :	
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.

SETUP	ADVANCED	TOOLS	STATUS
-------	----------	-------	--------

PING TEST

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

Save Settings

Don't Save Settings

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

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.

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.

SCHEDULES

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

Save Settings Don't Save Settings

SCHEDULE RULE

Enable Schedule : ☐

Rule#	Rule Name	Action
Previous page Next page Add New Rule...		

SCHEDULES

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

Save Settings Don't Save Settings

SCHEDULE RULE SETTING

Name of Rule 1 :

Policy : Inactivate 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 --		

Back

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.

General: Displays the current time and firmware version.

WAN: Displays the WAN connection details of the router.

LAN: Displays the LAN connection details of the router.

Wireless LAN: Displays the wireless LAN connection details of the router

LAN Computers: Displays the list of clients connected to the router.

SETUP	ADVANCED	TOOLS	STATUS						
DEVICE INFORMATION All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here. Refresh									
GENERAL Time : Mon Dec 31, 2012 23:17:18 -0800 Firmware Version : V1.00 , 2014/01/03									
WAN Connection Type : DHCP Client Network Status : Client Disconnected Remaining Lease Time : N/A Renew Release MAC Address : 78:54:2E:94:08:0D IP Address : 0.0.0.0 Subnet Mask : 0.0.0.0 Default Gateway : 0.0.0.0 DNS Server : 0.0.0.0 , 0.0.0.0									
LAN MAC Address : 78:54:2E:94:08:0E IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0 DHCP Server : Enabled									
WIRELESS LAN MAC Address : 78:54:2E:94:08:0E Wireless : Enabled SSID : dlink_DWR-755 Security : Auto(None) Channel : 11 802.11 Mode : B/G/N Mixed Wi-Fi Protected Setup : Enabled									
LAN COMPUTERS <table border="1"> <thead> <tr> <th>IP Address</th> <th>Name</th> <th>MAC</th> </tr> </thead> <tbody> <tr> <td>192.168.0.100</td> <td></td> <td>48-60-BC-15-F6-82</td> </tr> </tbody> </table>				IP Address	Name	MAC	192.168.0.100		48-60-BC-15-F6-82
IP Address	Name	MAC							
192.168.0.100		48-60-BC-15-F6-82							

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.

SETUP

ADVANCED

TOOLS

STATUS

VIEW LOG

View Log displays the activities occurring on the device.

Page: 1/7 (Log Number : 102)

Previous

Next

First Page

Last Page

Refresh

Download

Clear logs

Link To Log Settings

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.

SETUPADVANCEDTOOLSSTATUS

TRAFFIC STATISTICS

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

Refresh

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.

SETUP

ADVANCED

TOOLS

STATUS

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.)

Refresh

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.

SETUP

ADVANCED

TOOLS

STATUS

IPv6 NETWORK INFORMATION

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

Refresh

IPv6 CONNECTION INFORMATION

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.

DWR-925	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
MENU SETUP ADVANCED TOOLS STATUS LOGOUT  Internet Online Reboot	SUPPORT MENU Setup Advanced Tools Status				
	SETUP HELP Internet Wireless Settings Network Settings IPv6 Setup Message Service				
	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				
	STATUS HELP Device Info Log Statistics Wireless IPv6 Status				
WIRELESS					

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 secure with WPA2.

Windows® 8

WPA/WPA2

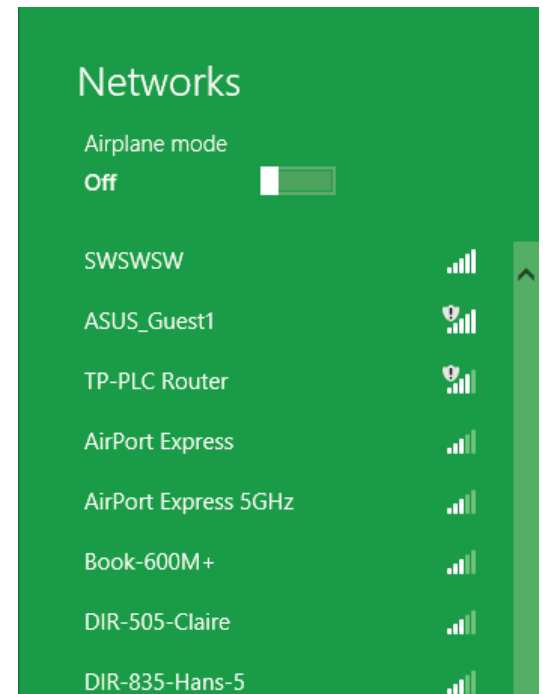
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

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



Wireless Icon

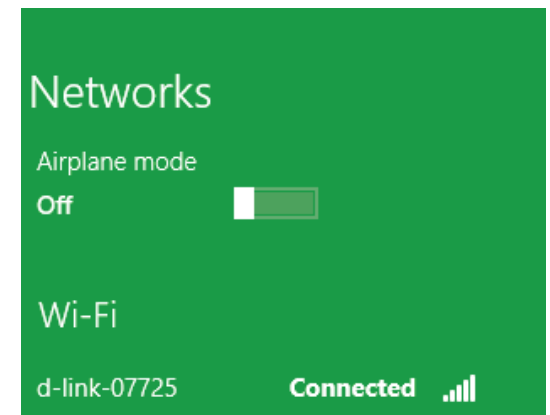
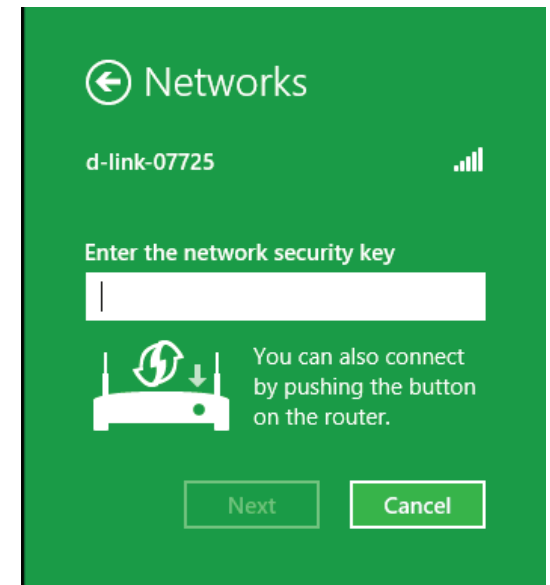
Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.



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.

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.

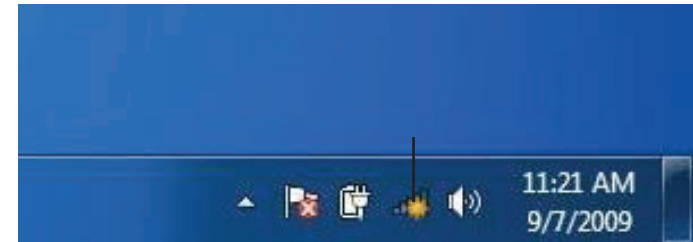


Windows® 7

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.

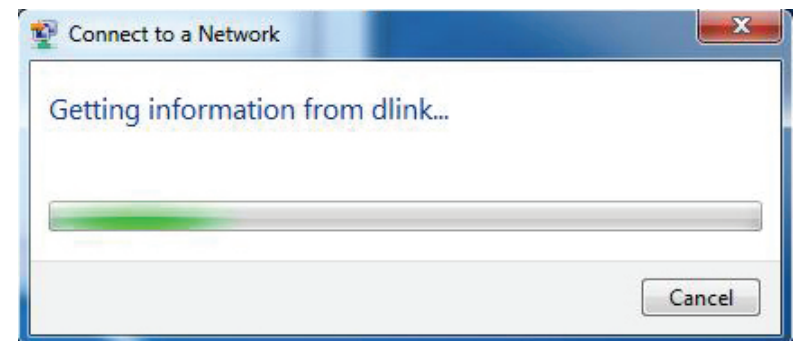


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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.

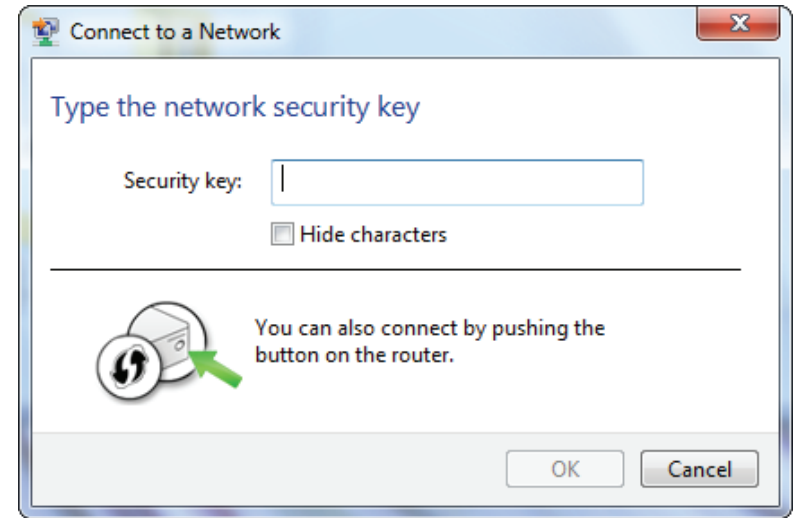


4. The following window appears while your computer tries to connect to the router.



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

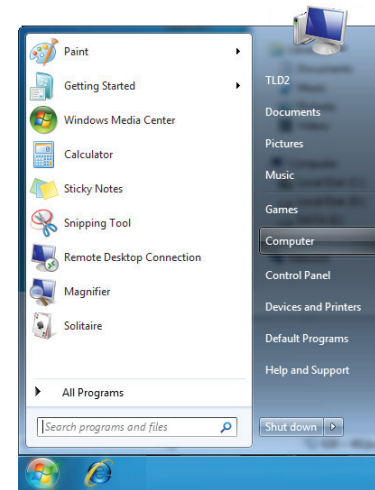
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



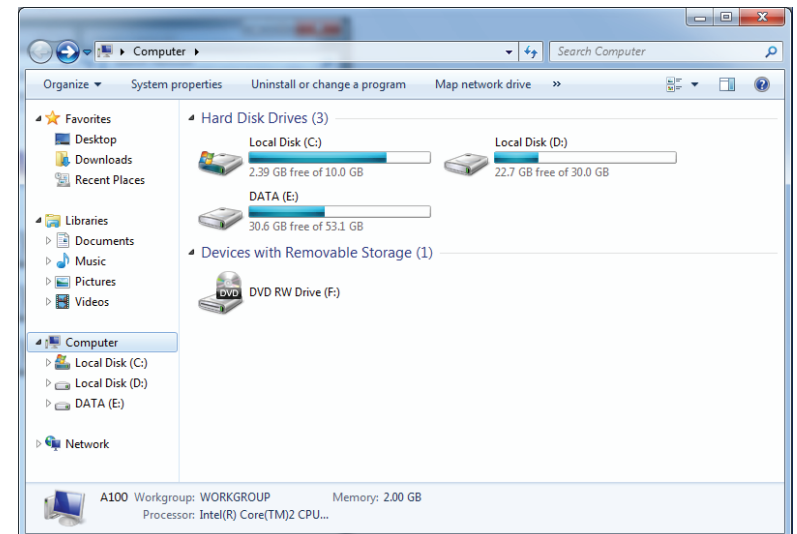
WPS

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:

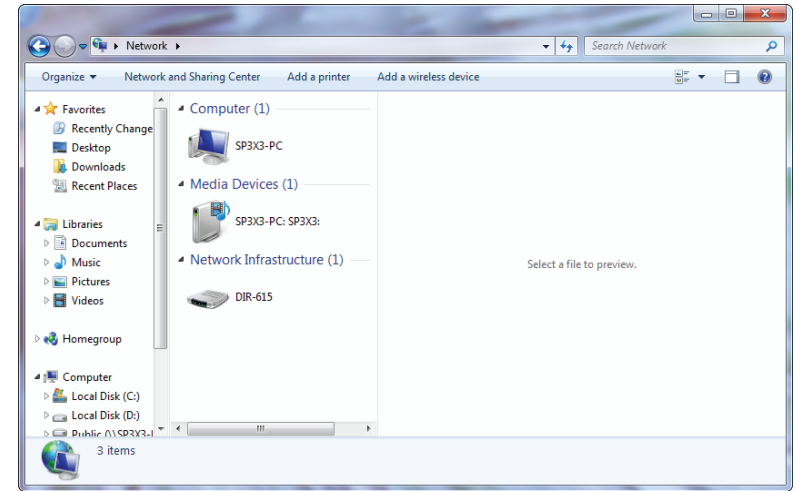
1. Click the **Start** button and select **Computer** from the Start menu.



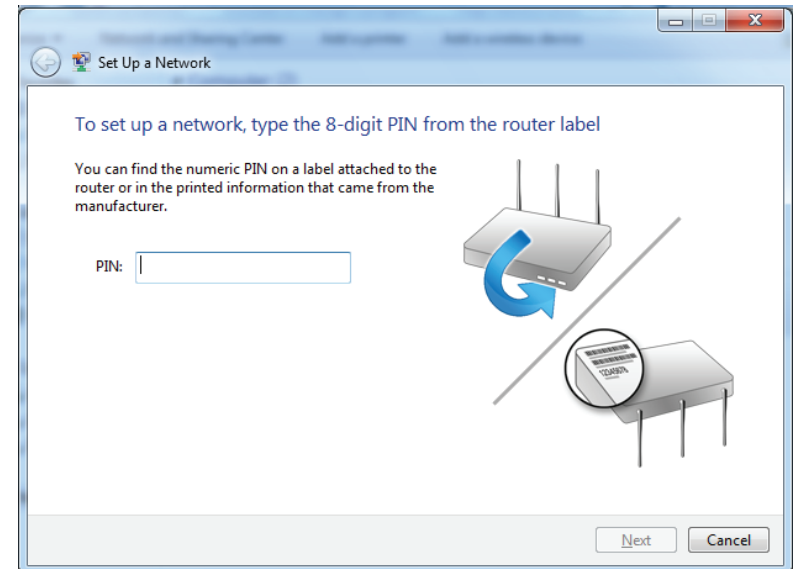
2. Click **Network** on the left side.



3. Double-click your D-Link router.



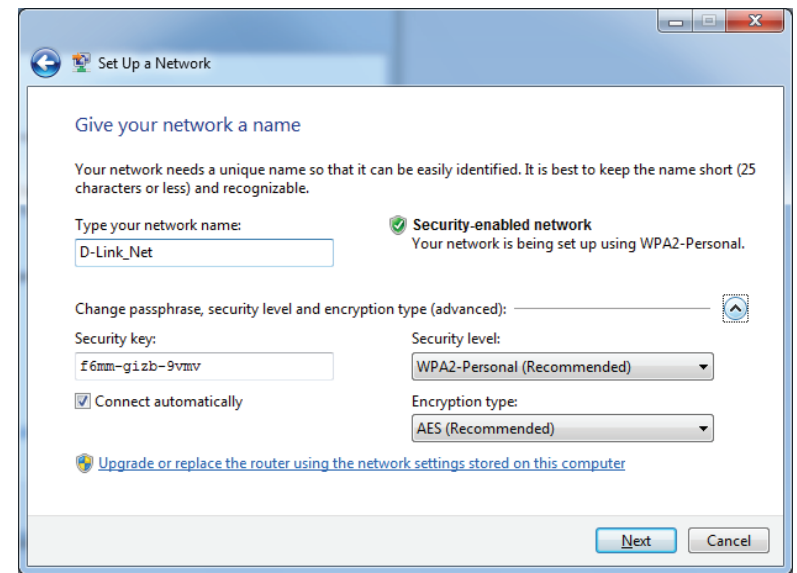
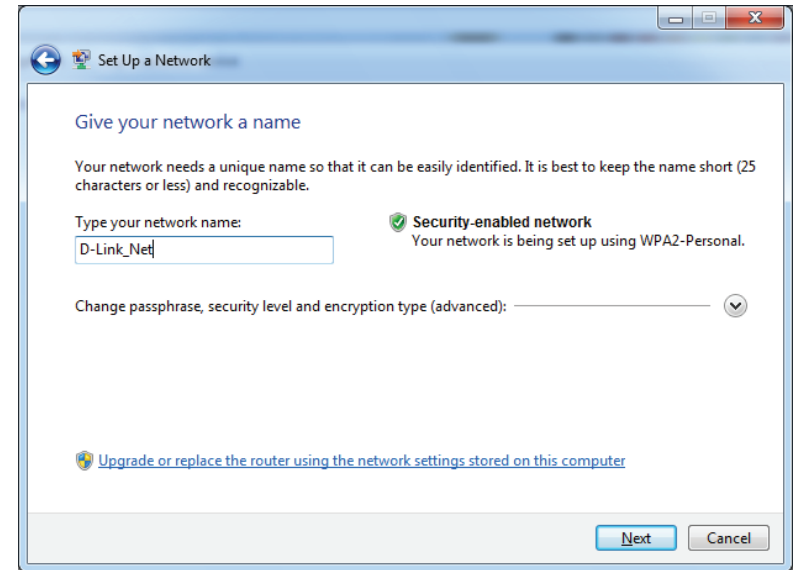
4. Input the WPS PIN number (displayed in the WPS window on the router's LCD screen or in the **Setup > Wireless Setup** menu in the router's Web UI) and click **Next**.



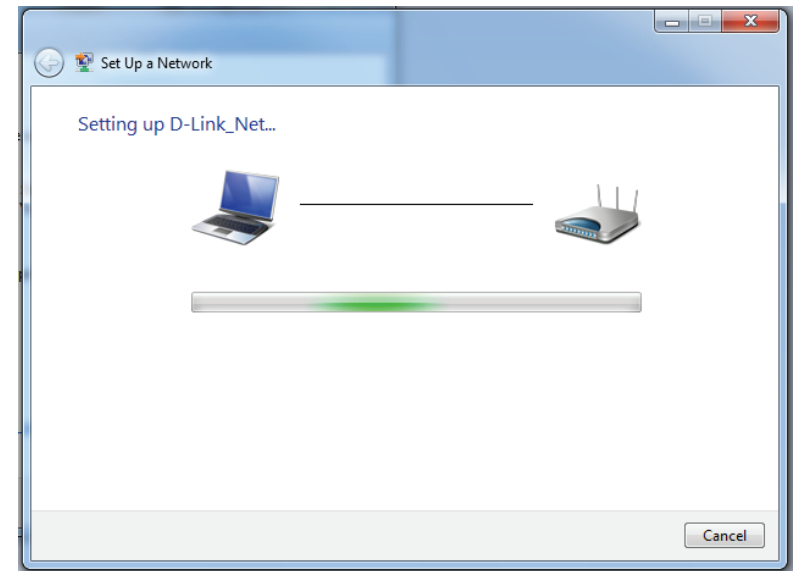
5. Type a name to identify the network.

6. To configure advanced settings, click the  icon.

Click **Next** to continue.



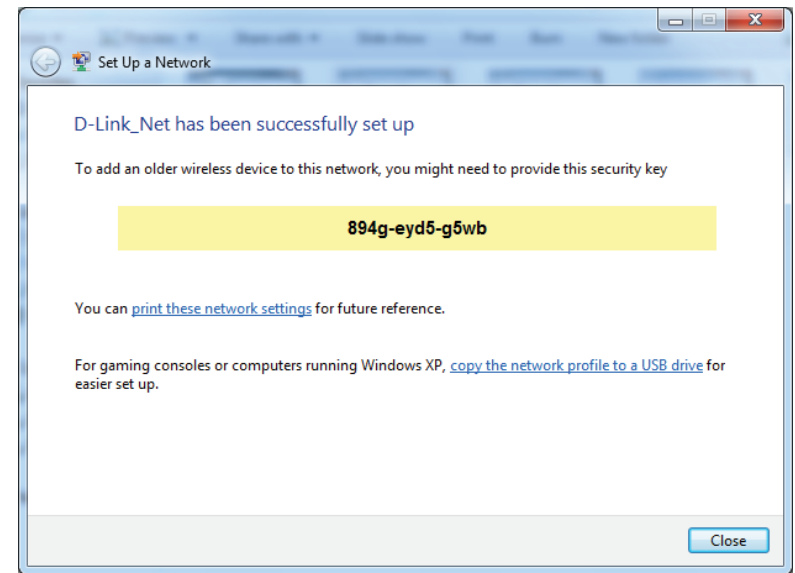
7. The following window appears while the router is being configured. Wait for the configuration to complete.



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

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

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



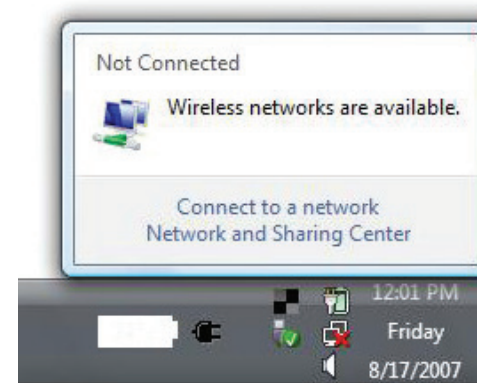
Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's 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.

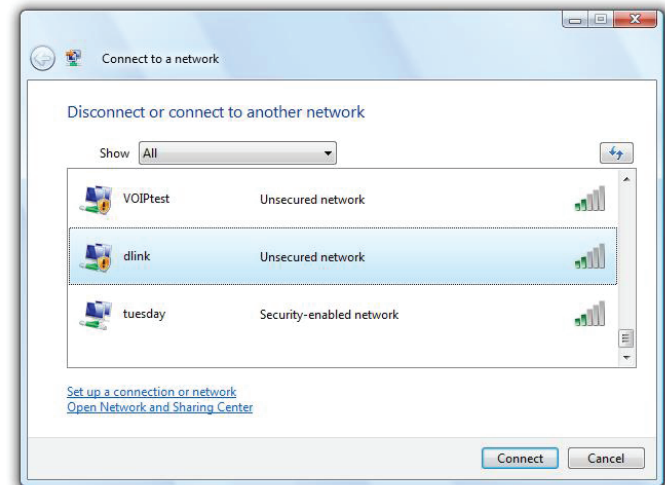
or

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.

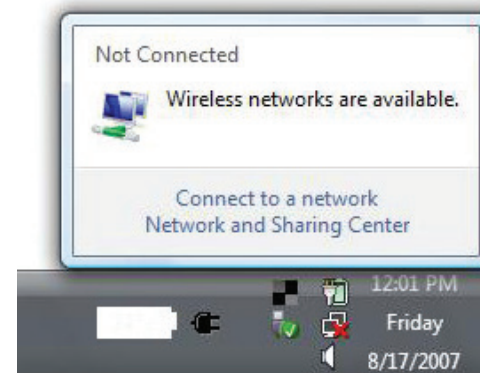
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



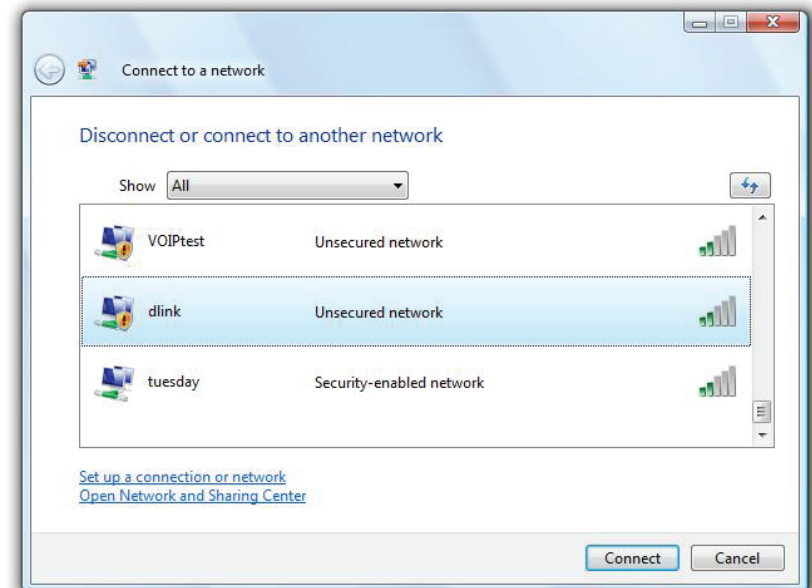
WPA/WPA2

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

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



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



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.



Windows® XP

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

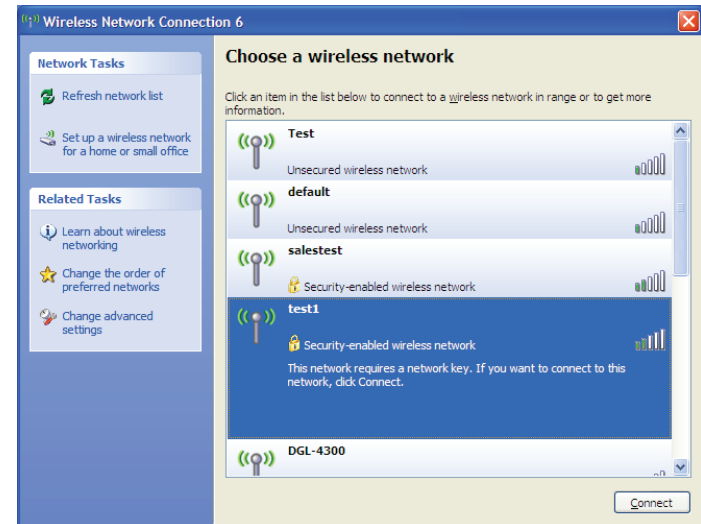
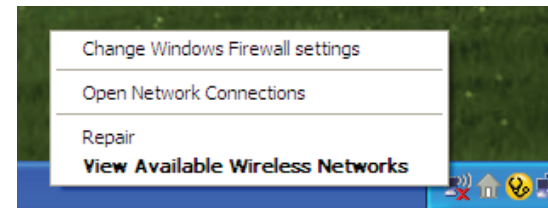
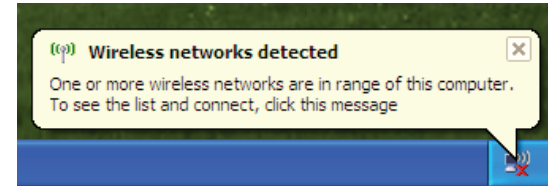
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

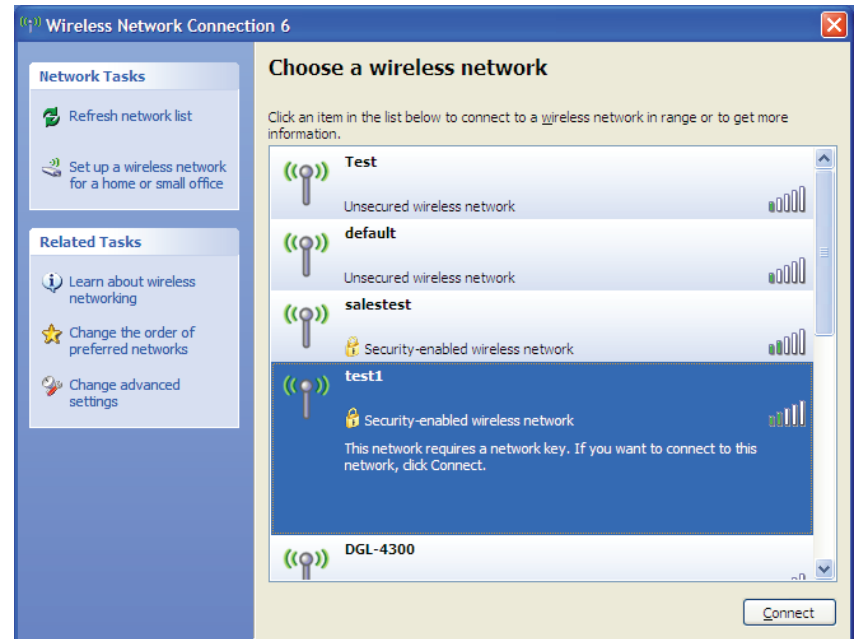
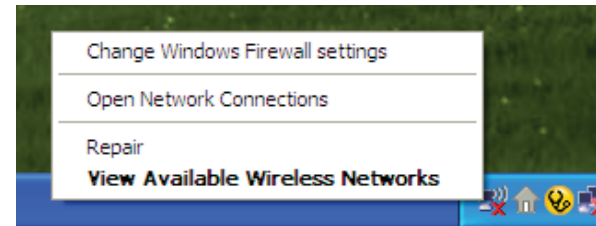
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

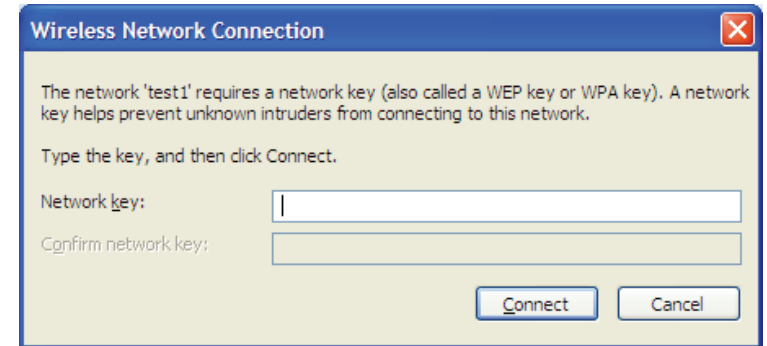
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

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



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.



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, let's say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with ($1452+28=1480$).

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

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

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

Home

- 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 the WPA or WEP security feature on the router. 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

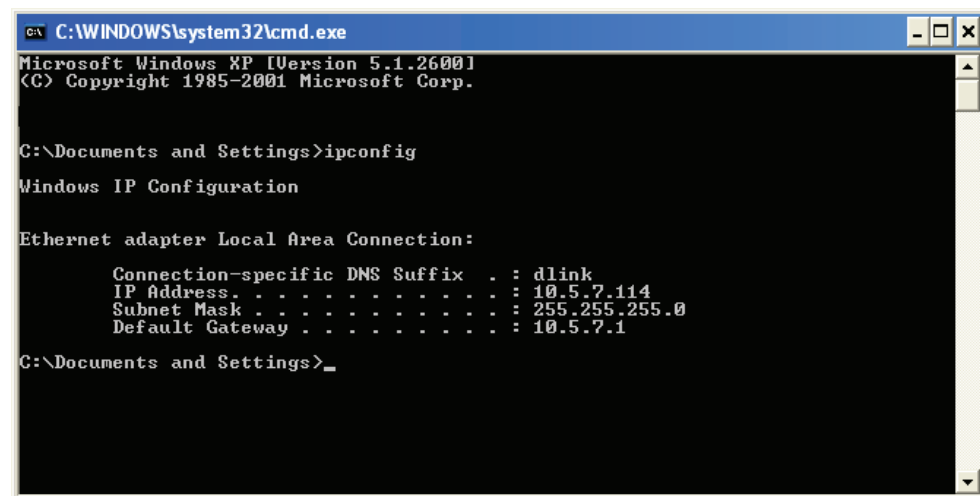
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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.



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>
```

Statically Assign an IP address

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

Step 1

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

Step 2

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

Step 3

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

Step 4

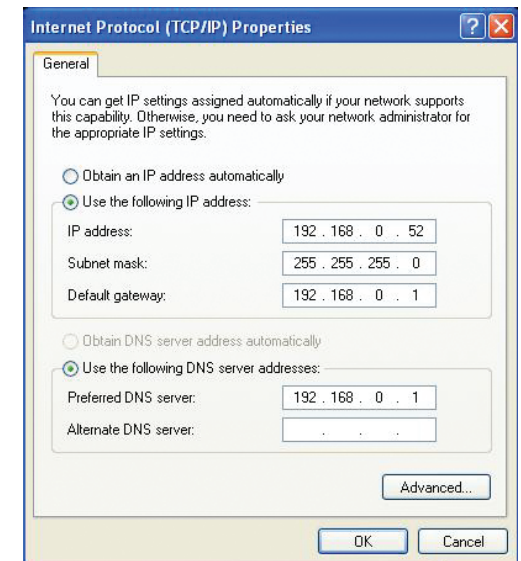
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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.

Step 5

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



Technical Specifications

LTE Bands

- 1900 / 1700 / 850 / 700 MHz

UMTS/HSDPA/HSUPA Bands

- 1900 / 1700 / 850 MHz

GPRS/EDGE Bands

- 850/900/1800/1900 MHz

Data Rates

- LTE Uplink: Up to 50 Mbps
- LTE Downlink: Up to 100 Mbps
- Up to 300 Mbps in 802.11n mode

Standards

- 802.11b
- 802.11g
- 802.11n

Wireless Security

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

Firewall

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

VPN

- L2TP/PPTP/IPSEC/GRE VPN

Antenna

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

Ports

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

SIM Slot

- Standard 6-pin 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 45 °C (32 to 112 °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

- FCC
- PTCRB
- RoHS

FCC Regulations

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

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

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

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

FCC RF Exposure Compliance (SAR)

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

FCC RF Exposure Compliance

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

This radio transmitter has been approved by FCC to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna types:

WWAN/WLAN: Dipole Antenna

Antenna gain (in dBi):

WWAN: 3.51 dBi

WLAN: 1.73 dBi