



## User Manual

### Wireless N300 Multi-WAN Router

DWR-116

---

## 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
1.0	May 24, 2013	• Initial release for Revision A1

### 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.

Copyright © 2013 by D-Link Corporation.

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

# Table of Contents

<b>Preface</b> .....	<b>i</b>	3G / 4G LTE .....	21
Manual Revisions.....	i	Static IP.....	22
Trademarks .....	i	Failover Setting.....	23
<b>Product Overview</b> .....	<b>1</b>	Wireless Connection Setup Wizard .....	24
Package Contents.....	1	Wireless Settings.....	28
System Requirements .....	1	Wi-Fi Protected Setup .....	32
Introduction .....	2	Network Settings .....	33
Hardware Overview .....	3	Router Settings.....	33
Back Panel .....	3	DHCP Server Settings .....	34
Front Panel and LEDs.....	4	Advanced .....	35
Top .....	5	Virtual Server .....	35
<b>Installation</b> .....	<b>6</b>	Application Rules.....	36
Connect to Your Network .....	6	QoS Engine.....	37
Wireless Installation Considerations.....	7	MAC Address Filter .....	38
<b>Configuration</b> .....	<b>8</b>	URL Filter.....	39
Web-based Configuration Utility .....	8	Outbound Filter.....	40
Setup.....	9	Inbound Filter .....	41
Internet Connection Setup Wizard.....	9	SNMP .....	42
Manual Internet Connection Setup .....	16	Routing.....	43
Internet Connection Type.....	16	Advanced Wireless .....	44
Dynamic IP (DHCP).....	17	Advanced Network .....	45
PPPoE .....	18	Tools .....	46
PPTP .....	19	Admin .....	46
L2TP .....	20	Time.....	47
		Syslog.....	48
		Email Settings .....	49

System .....	50	<b>Troubleshooting</b> .....	<b>80</b>
Firmware .....	51	Wireless Modes.....	82
Dynamic DNS .....	52	<b>Networking Basics</b> .....	<b>83</b>
System Check .....	53	Check your IP address .....	83
Schedules .....	54	Statically Assign an IP address .....	84
Status .....	55	<b>Technical Specifications</b> .....	<b>85</b>
Device Information .....	55		
Logs .....	56		
Statistics .....	57		
Wireless .....	58		
Support .....	59		
<b>Wireless Security</b> .....	<b>60</b>		
What is WEP?.....	60		
Configure WEP .....	61		
What is WPA?.....	62		
Configure WPA-PSK.....	63		
Configure WPA (RADIUS) .....	64		
Windows® 8.....	65		
WPA/WPA2 .....	65		
Windows® 7.....	67		
WPA/WPA2 .....	67		
WPS.....	69		
Windows Vista®.....	73		
WPA/WPA2 .....	74		
WPS/WCN 2.0 .....	76		
Windows® XP .....	77		
WPA/WPA2 .....	78		

## Package Contents

- D-Link DWR-116 Wireless N300 Multi-WAN Router
- Power Adapter
- Manual and Warranty on CD
- External Wi-Fi antenna

**Note:** Using a power supply with a different voltage rating than the one included with the DWR-116 will cause damage and void the warranty for this product.

## System Requirements

- A compatible 3G/4G LTE USB modem

**Computer with the following:**

- Windows®, Macintosh, or Linux-based operating system
- An installed Ethernet adapter

**Browser Requirements:**

- Internet Explorer® 7 and higher
- Mozilla Firefox 12.0 and higher
- Google™ Chrome 20.0 and higher
- Apple Safari 4 and higher

## Introduction

The D-Link Wireless N300 Multi-WAN Router allows users to access mobile broadband networks worldwide. Once connected, users can transfer data and stream media. Simply connect your USB modem to share your 3G/4G LTE Internet connection through a secure 802.11n wireless network or using the 10/100 Ethernet port.

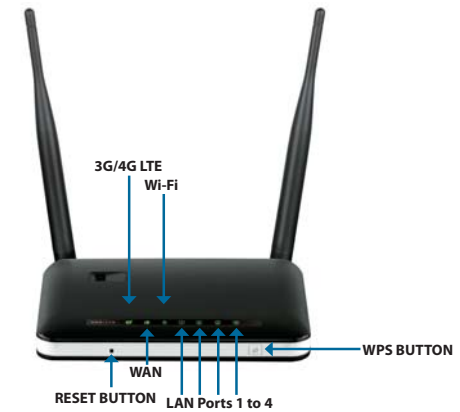
The Wireless N300 Multi-WAN Router can be installed quickly and easily almost anywhere. This router is great for situations where an impromptu wireless network must be set up, or wherever conventional network access is unavailable. The DWR-116 can even be installed in buses, trains, or boats, allowing passengers to check e-mail or chat online while commuting.

## Hardware Overview Back Panel



Port	Function
<b>LAN Port</b>	Connects to wired computers or devices.
<b>WAN Port</b>	Connects to the Internet.
<b>Power Port</b>	Connects to the power adapter.

## Hardware Overview Front Panel and LEDs



LED	Description			
	Color	Solid	Blinking	Blinking (Fast)
<b>3G/4G LTE</b>	Green	3G/4G LTE connection established	Data transmitting	-
<b>WAN</b>	Green	WAN connection established	Data transmitting	-
<b>Wi-Fi</b>	Green	Wi-Fi active and available	Data transmitting	Device in WPS mode
<b>LAN 1 - LAN 4</b>	Green	Ethernet connection established	Data transmitting	-

**Note:** WPS mode can be activated by pressing, and holding the WPS button until the Wi-Fi LED begins to flash rapidly. You can find more details about activating WPS mode in the section titled "Wi-Fi Protected Setup" on page 32

## Hardware Overview

### Top



Port	Function
USB Port	Connects to 3G/4G LTE Modem Dongle
Antennas	External WiFi Antennas

## 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 or cabinet, or in an attic or garage.

### Connect to Your Network

**Note:** Ensure that your DWR-116 Wireless N300 Multi-WAN Router is disconnected and powered **off** before performing the installation steps below.

1. Connect a USB modem to the **USB** port located on the top of the router.
2. Insert an Ethernet network cable into the **LAN** port on the back of the router. Plug the other end of the Ethernet cable into the LAN port of your computer or laptop. The Ethernet LED will turn green if the Ethernet connection is successfully established.

**Note:** The DWR-116 Wireless N300 Multi-WAN Router's LAN ports are "Auto-MDI/MDIX." Therefore, patch or crossover Ethernet cables can be used.

3. Configure the device using the setup utility.

## Wireless Installation Considerations

The DWR-116 can be accessed using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the quantity, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

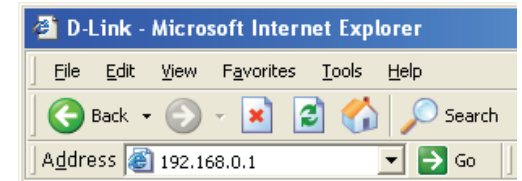
1. Minimize the number of walls and ceilings between the router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick. Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Try to position access points, wireless routers, and computers so that the signal passes through open doorways or drywall. Materials such as glass, metal, brick, insulation, concrete and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors and aluminum studs may also have a negative effect on range.
4. If you are using 2.4 GHz cordless phones, make sure that the 2.4 GHz phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

## Configuration

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. The default IP address of the router is 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 the **Troubleshooting** section for assistance.



## Setup Internet Connection Setup Wizard

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. This wizard will guide you through a step-by-step process to configure your D-Link router to connect to the Internet. Click **Internet Connection Setup Wizard** to begin.

If you want to enter your settings without running the wizard, click **Manual Internet Connection Setup** and skip to page "Manual Internet Connection Setup" on page 16.

**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](#)

Create a new password that will be used to access the router and then click **Next** to continue.

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

**STEP 1: SET YOUR PASSWORD**

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

Password :

Verify Password :

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

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

**STEP 2: SELECT YOUR TIME ZONE**

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

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

Select the Internet connection type. The connection types are explained on the following page. If you are unsure of the correct connection type, you may have to 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-116 supports several kinds of WAN interfaces, allowing you to assign either a WAN or a WWAN(3G/4G LTE) connection as the backup WAN. If the Primary WAN is down or unavailable, configure the backup WAN to **Enable**, and all the traffic will be routed through backup WAN. This feature is called **WAN Failover**. You can use WAN Failover if you need redundancy to your Internet connection or any other network.

**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 during step 3 of the wizard.

**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 page 12 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 page 12 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 page 13 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 page 13 for information about how to configure this type of connection.

**3G/4G LTE Connection:** Choose this option if your Internet Setup Provider provided you with a user name and password to use with your 3G / 4G LTE enabled USB Dongle. See page 14 for information about how to configure this type of connection.

**Static IP Address Connection:** Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured. See page 14 for information about how to configure this type of connection.

#### DHCP Connection (Dynamic IP Address):

**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.

**Host Name:** Enter the host name for your router or computer.

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

#### Username / Password Connection (PPPoE):

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

**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.

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

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



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

**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.

**PPTP Subnet Mask:** Enter the information provided by your ISP.

**PPTP Gateway IP Address:** Enter the information provided by your ISP.

**PPTP Server IP Address:** IP address of PPTP server.

**User Name:** User/account name that your ISP provides to you for PPTP dialup.

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



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

**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.

**L2TP Subnet Mask:** Enter the information provided by your ISP.

**L2TP Gateway IP Address:** Enter the information provided by your ISP.

**L2TP Server IP Address:** IP address of PPTP server.

**User Name:** User/account name that your ISP provides to you for PPTP dialup.

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



**3G/4G LTE Connection**

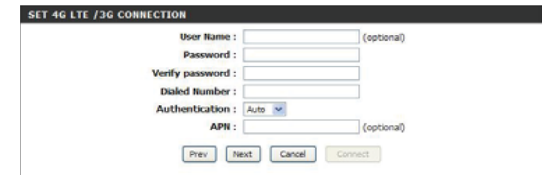
**User Name:** (Optional) Fill in only if requested by ISP.

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

**Dialed Number:** Enter the number to be dialed.

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

**APN:** (Optional) Enter the APN information.



**Static IP Address Connection**

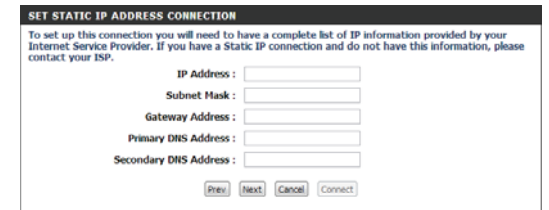
**IP Address:** Enter the IP address assigned to your network connection.

**Subnet Mask:** Enter the subnet mask.

**Gateway Address:** Enter the default gateway.

**Primary DNS Address:** Enter the primary DNS server.

**Secondary DNS Address:** Enter the secondary DNS server.

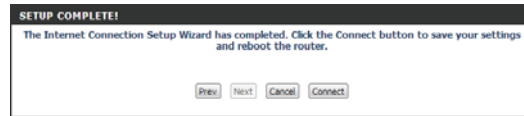


You have completed the **Setup Wizard**.

Click **Connect** to save your settings.

A popup will appear, to confirm your settings.

Click **OK** to save your settings.

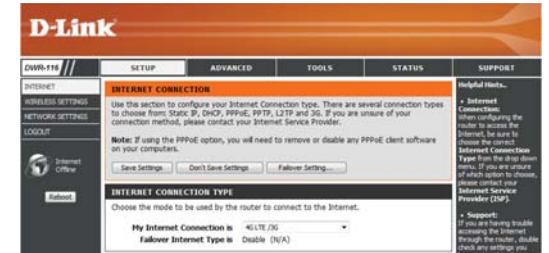


## Manual Internet Connection Setup Internet Connection Type

Several different Internet connection types can be selected depending upon the specifications of your Internet Service Provider (ISP).

**My Internet Connection is:** Select the Internet connection type specified by your Internet Service Provider (ISP). The corresponding settings will be displayed below. Please see the following pages for details on how to configure these different connection types.

**Failover Internet Connection is:** This connection can serve as a backup for your default connection. Click on the **Failover Setting** dropdown box in order to configure this setting. Please refer to page "Failover Setting" on page 23 for more details on how to configure settings.



## 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.

**Host Name:** (Optional) Required by some ISPs.

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

**Secondary DNS Server:** (Optional) Fill in with IP address of 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 WAN IP address automatically when the lease time is expiring.

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

## PPPoE

Choose this Internet connection if your ISP provides you with a PPPoE account.

**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:** Fill in with the same password in Password field.

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

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

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

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

**MAC Address:** MAC address of WAN interface. You can also copy MAC address of your PC to its WAN interface by pressing the **Clone** button. The **Restore MAC** button will reset the router to its default MAC address.

**Maximum Idle Time:** The amount of time of inactivity before disconnecting established PPPoE session. Setting it to zero or enabling **Reconnect Mode: Always-on** setting will disable this feature.

**Maximum Transmission Unit (MTU):** You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default setting of PPPoE is 1492.

**Auto-reconnect:** The device will dial-up PPPoE connection automatically.

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

## PPTP

Choose this Internet connection if your ISP provides you PPTP account.

**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:** IP address of 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:** Fill in with the same password in Password field.

**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 PPTP connection when local users want to surf the Internet, and disconnect if there is no traffic after the time period set under Maximum Idle Time.

**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.

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

## L2TP

Choose this Internet connection if your ISP provides you L2TP account.

**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:** IP address of 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:** Fill in with the same password in Password field.

**Reconnect Mode:** Choose Always-on when you want to establish L2TP connection all the time. Choose Connect-on-demand and the device will establish L2TP connection when local users want to surf 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 zero or choose Always-on to disable this feature.

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

## 3G / 4G LTE

Choose this Internet connection if you already use a SIM card for 3G/4G LTE Internet service from your mobile service provider company. 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.

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

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

**Dialed Number:** Enter the number to be dialed.

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

**APN:** (Optional) Enter the APN information.

**PIN:** Enter the PIN associated with your SIM card.

**Reconnect Mode:** Choose whether the device will reconnect to the 3G/4G network automatically or manually

**Maximum Idle Time:** The time of no activity required to disconnect the established 3G/4G LTE session. Set it to zero or choose Auto in Reconnect Mode to disable.

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

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

**Keep Alive:** Disable or Use LCP Echo Request. This depends on ISP requirement.

**Bridge Ethernet Ports:** Activate this feature to change Ethernet WAN port to LAN port.

## Static IP

Choose this Internet connection if your ISP assigns you a static IP address.

**IP Address:** Enter the IP address assigned to your network connection.

**Subnet Mask:** Enter the subnet mask.

**Default Gateway:** Enter the default gateway.

**Primary DNS Server:** Enter the primary DNS server.

**Secondary DNS Server:** Enter the secondary DNS server.

**MTU:** 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 Ethernet card.

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

## Failover Setting

This connection can serve as a backup for your default connection.

**Failover Type:** This option can be set to either **Load Sharing** or to **Failover**. With **Load Sharing**, the data usage is distributed evenly over the two different internet connections. With **Failover**, the secondary Internet connection will be in standby mode, until the primary Internet connection fails.

**Remote Host for Keep Alive:** This option should be set to an external IP address that can be used to ensure that the 3G/4G LTE connection will be kept from going offline due to inactivity. An example would be Google's public DNS servers (8.8.8.8 or 8.8.4.4) or your Internet service providers DNS servers.

**Primary WAN:** This will automatically be set to the connection type selected during the **Internet connection Setup Wizard**, or set to the **My Internet Connection** is option which is found on the Manual Internet Connections settings page.

**Secondary WAN:** This can be set by clicking on **Add New Rule**, the available options will be shown in the drop down box that appears.

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



## Wireless Connection Setup Wizard

This section will help you to manually configure the wireless settings of your router. Please note that changes made on 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 28.

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 "Wi-Fi Protected Setup (WPS)" on page 32.

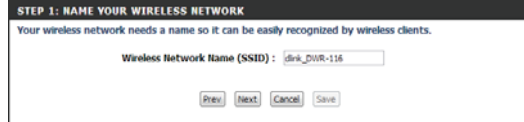


This wizard will guide you through a step-by-step process to configure your D-Link router's wireless. Click **Next** to continue.

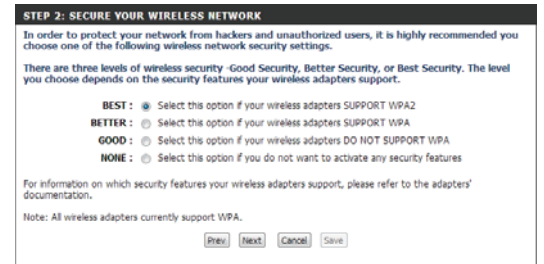
**Note:** While using the wizard, you can click **Prev** to go back to the previous page or you can click **Cancel** to close the wizard



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

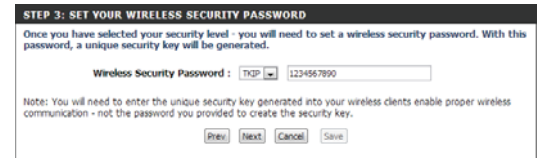


Select a level of wireless security to use, then click **Next** to continue.



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.

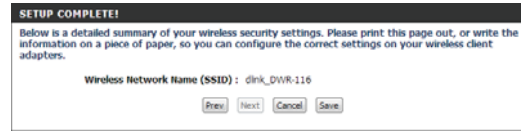
Click **Next** to continue.



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 can be between 5 to 13 alphanumeric characters. Click **Next** to continue.



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



## Wireless Settings

This section will help you to manually configure the wireless settings of your router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

**Enable Wireless:** Select this checkbox to enable wireless access. When you set this option, the following parameters take effect.

**Wireless Network** Also known as the SSID (Service Set Identifier), **Name:** 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. The default name is "dlink\_DWR-116".

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

**Auto Channel Scan:** Click **Auto Channel Scan** to automatically select the channel that it will operate on. This option is recommended because the router will choose the channel with the least amount of interference.

**Wireless Channel:** Choose the clearest channel to help optimize the performance and coverage of your wireless network. By default the channel is set to 11. This can be changed to fit the channel setting for an existing wireless network or to customize your wireless network.

**Visibility Status:** Select **Invisible** if you do not want the SSID of your wireless network to be broadcast by the DWR-116. The SSID of your router will not be seen by site survey utilities. Therefore while setting up your wireless clients, you will have to manually enter your SSID to connect to the router.





**Security Mode:** This device supports three wireless security modes, **WEP**, **WPA-Personal**, **WPA-Enterprise** or **None**. WEP is the original wireless encryption standard. WPA provides a higher level of security and WPA-Personal does not require an authentication server. When WPA-Enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

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

If you choose **WEP**, the following options will appear:

**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.

**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 2  
**WEP Key :** HEX 1234567890 (5 ASCII or 10 HEX)

If you choose **WPA-Personal**, the following options will appear:

**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 8 to 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(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 :** WPA2 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 :** d9p3-9paa-141 (8~63 ASCII or 64 HEX)

If you choose **WPA-Enterprise**, the following options will appear:

**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.

**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 : WPA2 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 :

Save Settings    Don't Save Settings

## Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the "Initial setup" as well as the "Add New Device" processes. The process is just as easy as pressing a button for the Push-Button Method or correctly entering an 8-digit code.

**Enable:** Enable/disable the Wi-Fi Protected Setup feature.

**AP PIN:** Shows the current PIN.

**Generate New PIN:** Create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the wireless client.

**Config Mode:** Select whether the router is the **Enrollee** or the **Registrar**. If this is set to enrollee, the router will try to connect to other devices. If it is set to registrar, other devices will try to connect to the router.

**Config Status:** Displays the current state of WPS configuration. Clicking the **Release** button will disable any previously paired devices from connecting. You will need to reconfigure WPS on those devices to connect them again.

**Disable WPS-PIN Method:** This checkbox will disable pin authentication for WPS. You will have to use the push button on the router and the device you are trying to connect in order to establish a WPS pairing.

**Config Method:** Select whether the WPS authentication will use Pin code or push button method.

**WPS Status:** Displays the current state of the router's WPS system.

**Trigger:** The **Trigger** button acts like the physical WPS push button, and will search for devices nearby that are trying to establish a WPS connection.

**Note:** The DWR-116 has a WPS push button on the front panel that will activate WPS mode by pressing and holding the button for approximately 6 seconds. The Wi-Fi LED will begin to flash rapidly when WPS mode has been activated.



## Network Settings Router Settings

This section will help you to change the internal network settings of your router and to configure the DHCP Server settings.

**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, you will need to enter the new IP address in your browser in order to access the web-based configuration utility.

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

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

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

The screenshot shows the D-Link DWR-116 web interface. The 'NETWORK SETTINGS' section includes instructions for configuring the internal network and a note about changing the router's IP address. The 'ROUTER SETTINGS' section contains fields for Router IP Address (192.168.0.1), Default Subnet Mask (255.255.255.0), and Local Domain Name. The 'DHCP SERVER SETTINGS' section is active, showing 'Enable DHCP Server' checked, 'DHCP IP Address Range' set to 50 to 255, 'DHCP Lease Time' set to 3600 seconds, and fields for Primary and Secondary DNS and WINS IP addresses. 'Save Settings' and 'Don't Save Settings' buttons are at the bottom.

## DHCP Server Settings

The DWR-116 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.

**Enable DHCP:** Select this box to enable the DHCP server on your router.

**DHCP IP Address Range:** Enter the starting and ending IP address for the server's IP address pool.

**DHCP Lease Time:** The time period for the IP address lease. Enter the lease time in minutes.

**Primary DNS IP Address:** Assign a primary DNS Server to DHCP clients.

**Secondary DNS IP Address:** Assign a DNS Server to DHCP clients.

**Primary WINS IP Address:** Assign a primary WINS Server to DHCP clients.

**Secondary WINS IP Address:** Assign a WINS Server to DHCP clients.

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

The screenshot shows the D-Link DWR-116 web interface. The 'NETWORK SETTING' section includes instructions for configuring the internal network and a note about changing the router's IP address. The 'ROUTER SETTINGS' section contains fields for Router IP Address (192.168.0.1), Default Subnet Mask (255.255.255.0), and Local Domain Name. The 'DHCP SERVER SETTINGS' section is active, showing 'Enable DHCP Server' checked, 'DHCP IP Address Range' set to 50 to 255, 'DHCP Lease Time' set to 3600 seconds, and fields for Primary and Secondary DNS and WINS IP addresses. 'Save Settings' and 'Don't Save Settings' buttons are at the bottom.

## 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.

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

**Copy to:** Copies the rule to the line of the specified ID.

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

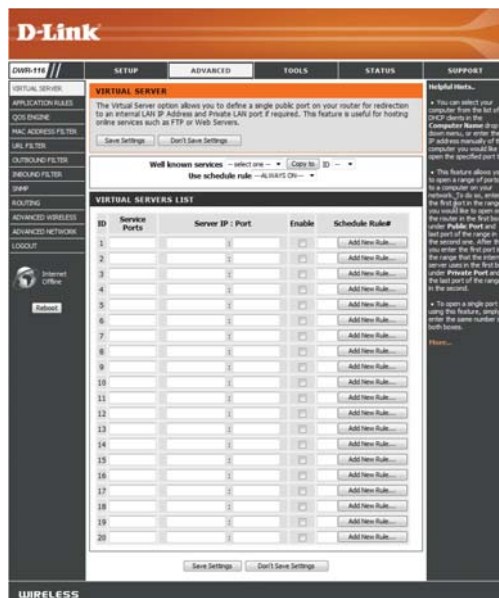
**ID:** Identifies the virtual server.

**Server IP : Port:** Enter the IP address of the computer on your local network that you want to allow the incoming service. In the next box, enter the port number that you would like to open.

**Enable:** Select this box to enable the rule.

**Schedule Rule #:** Specify the schedule rule number.

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



## Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). **Application Rules** allow some of these applications work with the DWR-116.

**Popular Applications:** Select from a list of popular applications.

**Copy to ID:** Copies the predefined application rule to the line of the specified ID.

**ID:** Identifies the rule.

**Trigger:** The name of the trigger.

**Incoming Ports:** Specify the incoming port for the trigger rule.

**Enable:** Select this box to enable the rule.

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



## QoS Engine

The **QoS Engine** improves your online experience by ensuring that certain applications 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 the applications.

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

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

**ID:** Identifies the rule.

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

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

**QoS Priority:** Select **Low**, **Normal**, or **High**.

**Enable:** Select a checkbox to enable the particular QoS rules individually.

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



## MAC Address Filter

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

**MAC Address Control:** Select this box to enable MAC filtering.

**Connection Control:** Wireless and wired clients with **C** selected can connect to this device and **allow/deny** connections from unspecified MAC addresses.

**Association Control:** Wireless clients with **A** selected can associate to the wireless LAN; and **allow/deny** connections from unspecified MAC addresses.

**ID:** Identifies the rule.

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

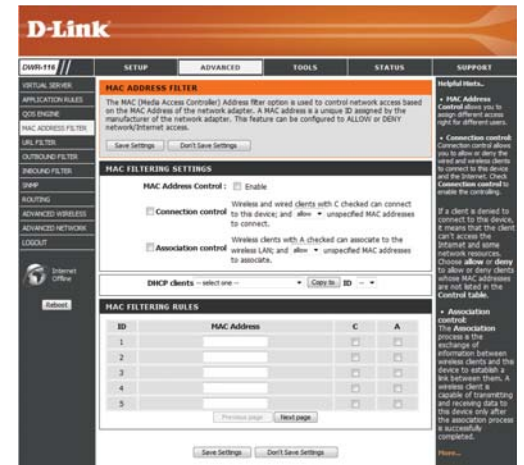
**IP Address:** Specify the last section of the IP address.

**Wake On LAN:** Click **Trigger** to configure Wake On LAN.

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

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

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



## URL Filter

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

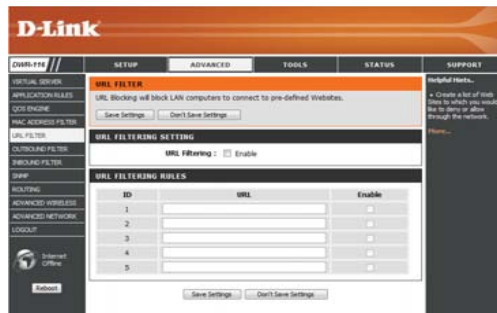
**URL Filtering:** Select this box to enable URL Filtering.

**ID:** Identifies the rule.

**URL:** Enter URL that you would like to block.

**Enable:** Click to enable the specific URL filter.

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



## Outbound Filter

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

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

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

**Copy to ID:** Copies the predefined filter to the specified ID

**ID:** Identifies the filter.

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

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

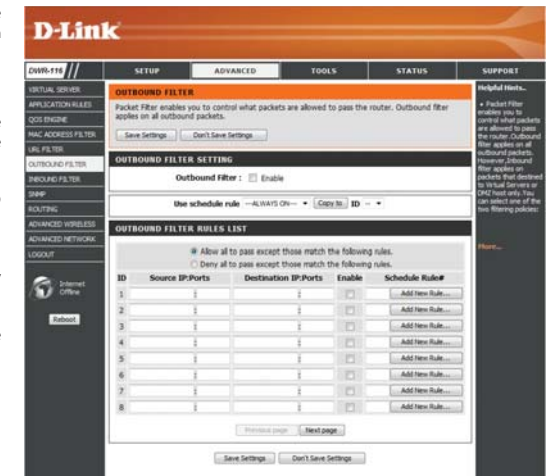
**Enable:** Select this box to enable the filter.

**Schedule Rule #:** Specify the schedule rule number.

**Previous Page:** Go back to the previous filter page.

**Next Page:** Advance to the next filter page.

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



## Inbound Filter

**Inbound Filter** enables you to control what packets are allowed to pass through the router. Inbound filter only applies to packets that are destined for Virtual Servers or DMZ hosts.

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

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

**Copy to ID:** Copies the predefined filter to the specified ID

**ID:** Identifies the filter.

**Source IP:** Specify the local IP address

**Source Ports:** Specify the local port after the colon.

**Destination IP:** Specify the remote IP address

**Destination Ports:** Specify the remote port after the colon.

**Enable:** Select this box to enable the filter.

**Schedule Rule #:** Specify the schedule rule number.

**Previous Page:** Go back to the previous filter page.

**Next Page:** Advance to the next filter page.

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

The screenshot shows the 'Inbound Filter' configuration page. At the top, there's a navigation bar with 'D-Link' and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The main content area is titled 'INBOUND FILTER' and includes a description: '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.' Below this, there's an 'Inbound Filter' section with an 'Enable' checkbox. The 'Inbound Filter Setting' section has a 'Use schedule rule' dropdown set to 'ALWAYS ON' and a 'Copy to ID' field. The 'Inbound Filter Rules List' section contains a table with 8 rows, each with an 'ID' field and an 'Add New Rule...' button. At the bottom, there are 'Save Settings' and 'Don't Save Settings' buttons.

## 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-116. The DWR-116 supports SNMP v1 or v2c.

**SNMP Local:** Select **Enabled** to allow local SNMP administration. Select **Disabled** to disallow local SNMP administration.

**SNMP Remote:** Select **Enabled** to allow local SNMP administration. Select **Disabled** to disallow local SNMP administration.

**Get Community:** Enter the password 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 in this field to gain "Read and Write" access to the network using SNMP software. Enter up to four IP addresses of any trap targets on your network.

**IP 1, IP 2, IP 3,** Select the SNMP version of your system.

**IP 4:**

**SNMP Version:**

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

The screenshot shows the 'SNMP' configuration page. It features a navigation bar with 'D-Link' and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The main content area is titled 'SNMP' and includes a description: 'Use Simple Network Management Protocol (SNMP) for management purposes.' Below this, there are sections for 'SNMP Local' and 'SNMP Remote', each with 'Enabled' and 'Disabled' radio buttons. There are also input fields for 'Set Community:', 'IP 1:', 'IP 2:', 'IP 3:', and 'IP 4:'. A 'SNMP Version' section has radio buttons for 'V1' and 'V2c'. At the bottom, there's a 'WAN Access IP Address' field and 'Save Settings' and 'Don't Save Settings' buttons.

## Routing

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

**RIP:** Select this box to enable routing.

**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.

**ID:** Identifies the rule.

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

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

**Gateway:** Enter the gateway IP address to the specified network.

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

**Enable:** Select this box to enable the rule.



## Advanced Wireless

**Advanced Wireless** contains settings which can negatively affect the performance of your router if configured improperly. Do not change these settings unless you are already familiar with them or have been instructed to do so.

**Beacon Interval:** Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 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.

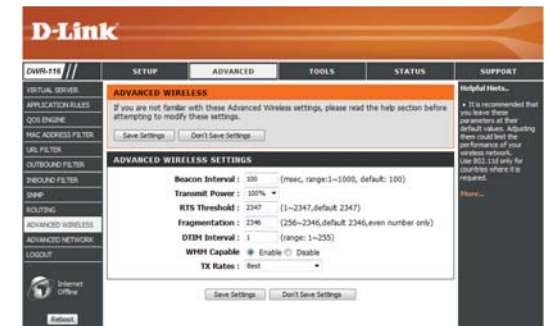
**Fragmentation:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented. 2346 is the default setting.

**DTIM Interval:** 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**.

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





## 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 do so.

**Enable UPnP:** Click **Enable UPnP** to use the Universal Plug and Play (UPnP™) feature. UPnP provides compatibility with networking equipment, software and peripherals.

**Enable WAN Ping Respond:** Select the box to allow the WAN port to be "pinged." Blocking the Ping option may provide some extra security from hackers.

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



## Tools Admin

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

**New Password:** Enter a password that the admin account will use to access the router's management interface.

**Confirm Password:** Confirm the chosen password.

**Remote Management:** Remote management allows the DWR-116 to be configured from the Internet using a web browser. A username and password is still required to access the web-management interface. Usually only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

**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. Example: 8080 is the port used for the web-management interface.

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



## Time

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

**Time:** Displays the current time and date of the DWR-116.

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

**Automatically synchronize with Internet time server:** Select this checkbox to automatically synchronize the DWR-116 with an Internet time server.

**NTP Server Used:** Choose the NTP Server used for synchronizing time and date.

**Sync. Result:** Shows the result of the last time synchronization.

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



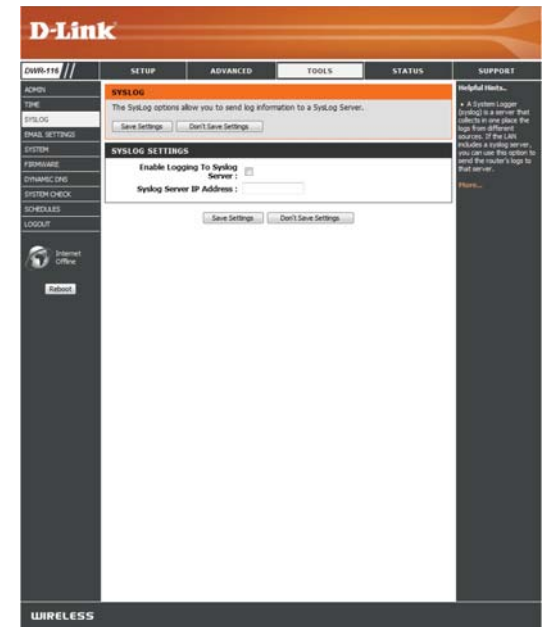
## Syslog

The DWR-116 keeps a running log of events and activities occurring on the router. You may send these logs to a Syslog server on your network.

**Enable Logging to Syslog Server:** Select this box to send the router logs to a Syslog server.

**Syslog Server IP Address:** Enter the address of the Syslog server that will be used to send the logs.

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



## Email Settings

**Email Settings** allows you to send the system log files, router alert messages, and firmware update notifications to an e-mail address.

**Enable E-mail Notification:** When this option is enabled, router activity logs are e-mailed to a designated e-mail address.

**SMTP Server IP and Port:** Enter the SMTP server IP address followed by a colon and the port number (e.g. 123.123.123.1:25).

**SMTP Username:** Enter the SMTP username.

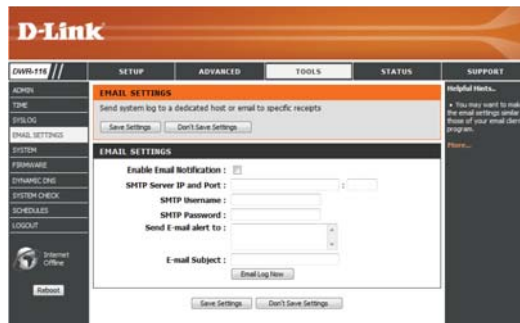
**SMTP Password:** Enter the SMTP password.

**Send E-mail Alert to:** Enter the e-mail address where you would like the e-mail sent to.

**E-mail Subject:** Enter a subject for the e-mail.

**E-mail Log Now:** Click this button to access the e-mail log.

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



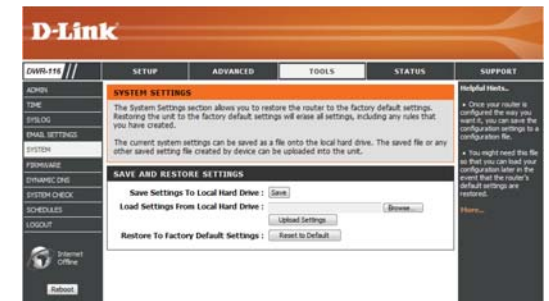
## System

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

**Save Settings To Local Hard Drive:** Use this option to save your current router configuration settings to a file and onto your computer. 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 the previously saved router configuration settings. Browse to find the saved file and then click **Upload Settings** to transfer those 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. Please check the D-Link support site for firmware updates at <http://support.dlink.com>. You can download firmware upgrades to your hard drive from the D-Link support site.

**Current Firmware Version:** Displays your current firmware version.

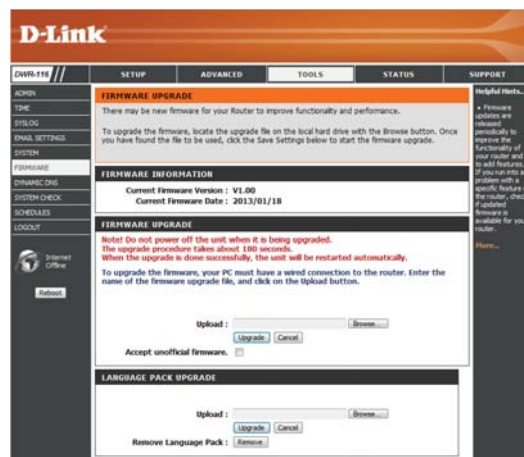
**Firmware Version:**

**Current Firmware Date:** Displays your current firmware date.

**Firmware Date:**

**Browse:** After you have downloaded the new firmware, click **Browse** to locate the firmware on your computer. Tick **Accept unofficial firmware** if you want to update the DWR-116 with unofficial firmware (not recommended).

Click **Upload** to start the firmware upgrade.



## Dynamic DNS

The Dynamic Domain Name System (DDNS) feature allows you to host a server (Web, FTP, or Game Server) using a domain name that you have purchased ([www.whateveryournameis.com](http://www.whateveryournameis.com)) with your dynamically assigned IP address.

Sign up for D-Link's free DDNS service at [www.dlinkddns.com](http://www.dlinkddns.com).

**Enable DDNS:** DDNS is a method of keeping a domain name linked to a changing IP Address. Select this box to enable DDNS.

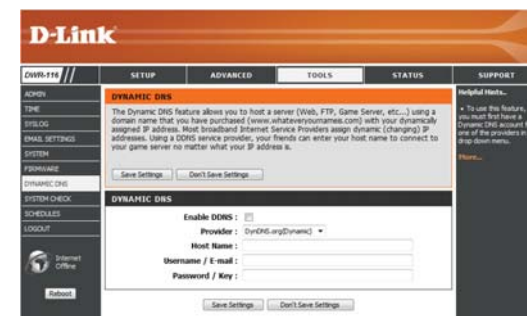
**Provider:** Select your DDNS provider from the drop-down box.

**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.

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



## 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.

**Host Name or IP Address:** Enter a host name or the IP address that you want to ping and click **Ping**.

**PING Result:** The status of your Ping attempt will be displayed in the Ping Result box.



## Schedules

This section allows you to manage schedule rules for various firewall and parental control features.

**Enable:** Tick this check box to enable schedules.

**Schedule:**

**Add New Rule...:** Click on this button to create a new rule. The following options will be available.

**Edit:** Edit the rule's start and end time.

**Delete:** Delete the rule.

**Name of Rule 1:** Enter a name for your new schedule.

**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.

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



## Status Device Information

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

**General:** Displays the current time and firmware version.

**WAN:** Displays the MAC address and the private (local) IP settings for the router.

**3G/4G LTE Card:** Displays 3G/4G LTE card info, link status, and the LAN network name.

**Wireless LAN:** Displays the MAC address and the public IP settings for the router.

**LAN Computers:** Displays the wireless MAC address and your wireless settings such as SSID, channel, and encryption type. Also displays the list of currently connected DHCP clients.

## Logs

Here you can view logs and define events that you want to view. This router also has an internal syslog server, so you can send the log files to a computer that is running a syslog utility.

## Statistics

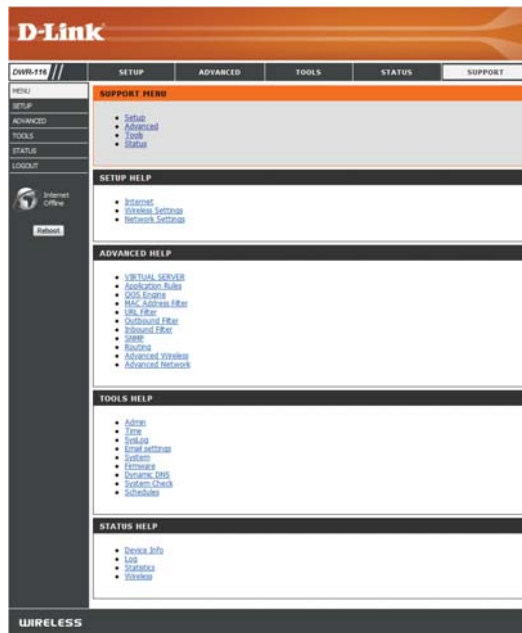
Here you can view the packets transmitted and received passing through your router on both WAN and LAN ports. The traffic counter will reset if the device is rebooted.

## Wireless

This table displays a list of wireless clients that are connected to your wireless router. It also displays the connection time and MAC address of the connected wireless clients.

## Support

The **SUPPORT** pages provide help information for each section of the device's interface. To view the Support pages, click on **SUPPORT** at the top of the screen.



## Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DWR-116 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

### What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.



## Configure WEP

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WEP Security**.
3. Next to *Authentication*, select **Open** or **Shared Key**.
4. Select either **64-bit** or **128-bit** encryption from the drop-down box next to *WEP Encryption*.
5. Next to *Key Type*, select either **Hex** or **ASCII**.  
Hex (recommended) - Letters A-F and numbers 0-9 are valid.  
ASCII - All numbers and letters are valid.
6. Next to *Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.
7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.

## What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy). The 2 major improvements over WEP:

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

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

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

## Configure WPA-PSK

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WPA-Personal Security** or **Enable WPA2-Personal Security**.
3. Next to *Cipher Mode*, select **TKIP, AES, or Auto**.
4. Next to *PSK/EAP*, select **PSK**.
5. Next to *Passphrase*, enter a key (passphrase). The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?\*&\_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.
6. Enter the passphrase again next to *Confirmed Passphrase*.
7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK (or WPA2-PSK) on your adapter and enter the same passphrase as you did on the router.

## Configure WPA (RADIUS)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **Enable WPA-Personal Security** or **Enable WPA2-Personal Security**.
3. Next to *Cipher Mode*, select **TKIP, AES, or Auto**.
4. Next to *PSK/EAP*, select **EAP**.
5. Next to *RADIUS Server 1* enter the IP Address of your RADIUS server.
6. Next to *Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
7. Next to *Shared Secret*, enter the security key.
8. If you have a secondary RADIUS server, enter its IP address, port, and secret key.
9. Click **Apply Settings** to save your settings.

## Windows® 8 WPA/WPA2

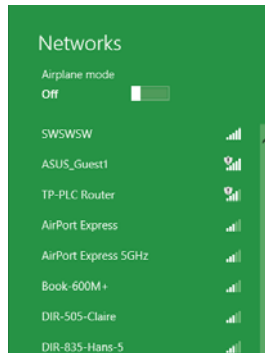
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

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.

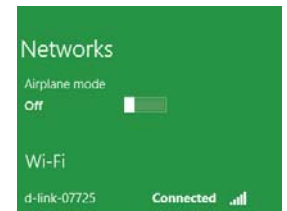


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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 with a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



## Windows® 7 WPA/WPA2

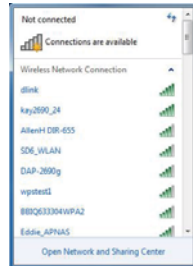
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

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.

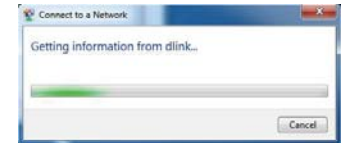


3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to 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 (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

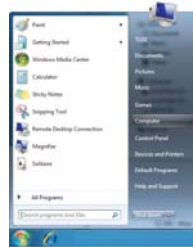
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



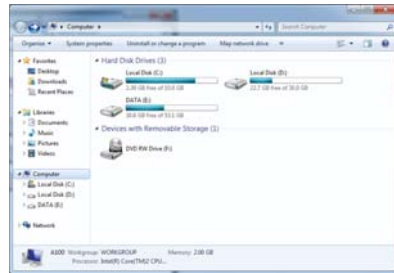
## WPS

The WPS feature of the DWR-116 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

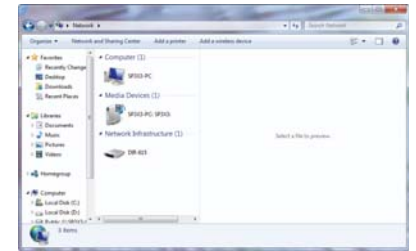
1. Click the **Start** button and select **Computer** from the Start menu.



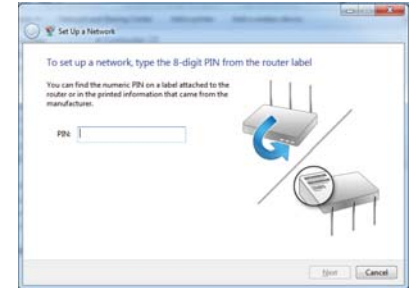
2. Click **Network** on the left side.



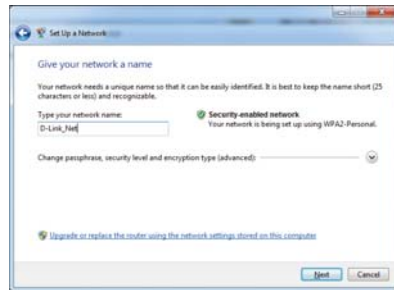
3. Double-click the DWR-116




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**.

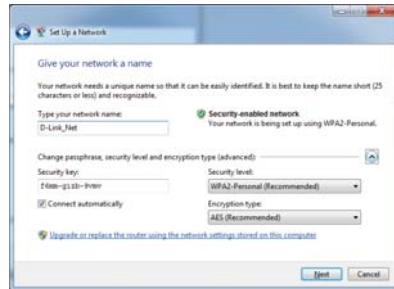


5. Type a name to identify the network.



6. To configure advanced settings, click the  icon.

Click **Next** to continue.



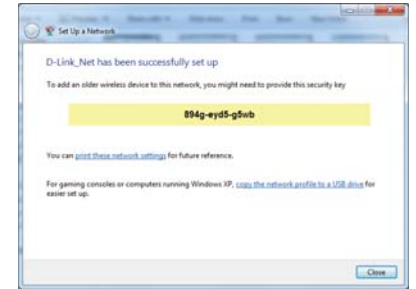
7. The following window appears while the Router is being configured.

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, 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.

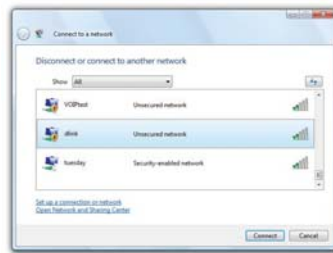
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

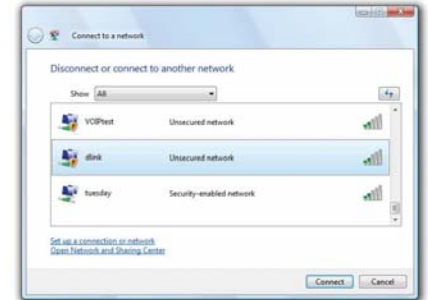
## WPA/WPA2

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



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

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

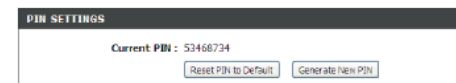


## WPS/WCN 2.0

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and not configured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the **Enable** checkbox in the **Basic > Wireless** section. Use the Current PIN that is displayed on the **Advanced > Wi-Fi Protected Setup** section or choose to click the **Generate New PIN** button or **Reset PIN to Default** button.



If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.



## Windows® XP

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

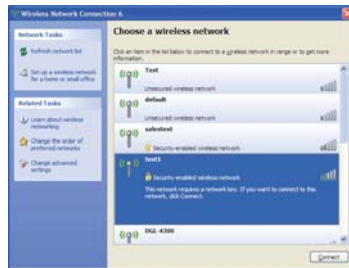
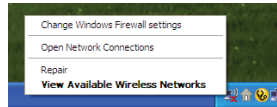
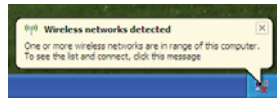
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

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

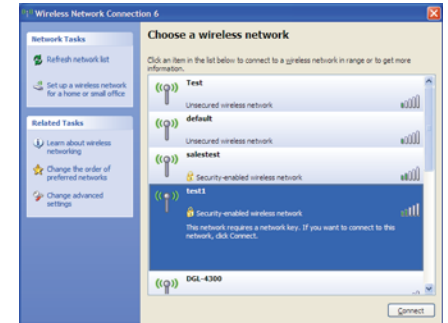
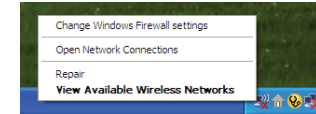


## WPA/WPA2

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

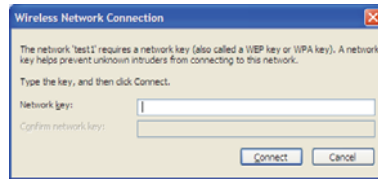
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.

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



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

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



## Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-116. 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 on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 6.0 or higher
  - Netscape 8 or higher
  - Mozilla 1.7.12 (5.0) or higher
  - Opera 8.5 or higher
  - Safari 1.2 or higher (with Java 1.3.1 or higher)
  - Camino 0.8.4 or higher
  - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

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

## 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 WNA-2330 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

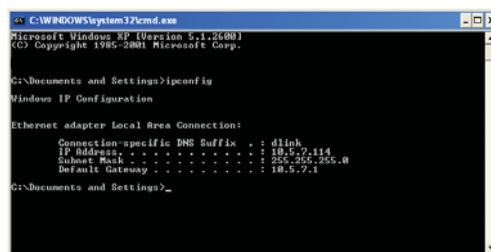
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows® 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>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dLink
    IP Address . . . . . : 192.168.0.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

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® 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 Default Gateway the same as the LAN IP address of your router (192.168.0.1).

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

#### Step 5

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



## Technical Specifications

### Data Rates \*\*

300,150,135,120,90,60,45,30,15 Mbps in 802.11n mode  
6/9/11/12/18/24/36/48/54Mbps in 802.11g mode  
1/2/5.5/11Mbps in 802.11b mode

### Standards

IEEE 802.11n compliant (2Tx2R)  
IEEE 802.11b/g  
IEEE 802.3  
IEEE 802.3u

### Frequency

2.4 - 2.4835 GHz

### Wireless Security

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

### Firewall

IP Filtering  
Network Address Translation (NAT)  
MAC Filtering

### VPN

L2TP/PPTP/IPSEC VPN Pass-through

### Ports

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

### Antenna

2 x External 5 dBiWi-Fi antenna

### LED Status Indicators

3G / 4G LTE  
WAN  
Wi-Fi  
LAN 1, LAN 2, LAN 3, LAN 4

### Power

External 5 V DC 2 A power adapter

### Dimensions (L x W x H)

• 148.5 x 113.5 x 25 mm (5.85 x 4.47 x .98 inches)

### Operating Temperature

Operating: 0 to 40 °C (32 to 104 °F)

### Operating Humidity

Operating: 10% to 95% non-condensing