



User Manual

Wireless N300 Multi-WAN Router

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

Preface	i	3G / 4G LTE	21
Manual Revisions.....	i	Static IP	22
Trademarks	i	Failover Setting.....	23
Product Overview	1	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
Installation	6	Application Rules.....	36
Connect to Your Network	6	QoS Engine.....	37
Wireless Installation Considerations.....	7	MAC Address Filter	38
Configuration	8	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	Troubleshooting	80
Firmware	51	Wireless Modes.....	82
Dynamic DNS	52	Networking Basics	83
System Check.....	53	Check your IP address.....	83
Schedules	54	Statically Assign an IP address	84
Status	55	Technical Specifications	85
Device Information	55		
Logs	56		
Statistics	57		
Wireless	58		
Support	59		
Wireless Security	60		
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 easily 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. The DWR-116 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
LAN Port	Connects to wired computers or devices.
WAN Port	Connects to the Internet.
Power Port	Connects to the power adapter.

Hardware Overview

Front Panel and LEDs

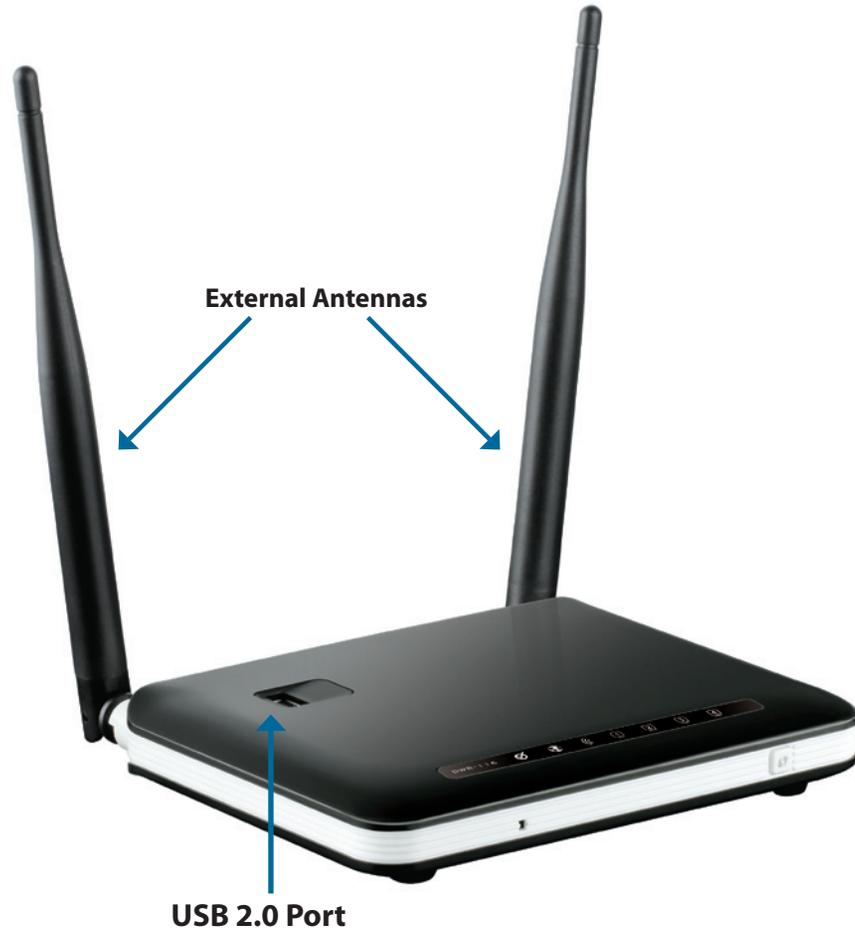


LED	Description			
	Color	Solid	Blinking	Blinking (Fast)
3G/4G LTE	Green	3G/4G LTE connection established	Data transmitting	-
WAN	Green	WAN connection established	Data transmitting	-
Wi-Fi	Green	Wi-Fi active and available	Data transmitting	Device in WPS mode
LAN 1 - LAN 4	Green	Ethernet connection established	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 39

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.

Quick Setup Wizard

If this is your first time installing the router, open your web browser. You will automatically be directed to the **Wizard Setup Screen**. If not, enter “**http://dlinkrouter** or **http://dlinkrouter.local** in the address bar”. Then, press Enter.

If you have already configured your settings and you would like to access the configuration utility, please refer to

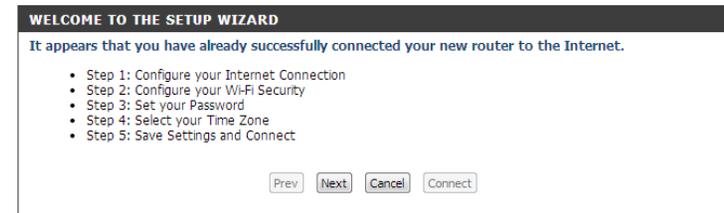
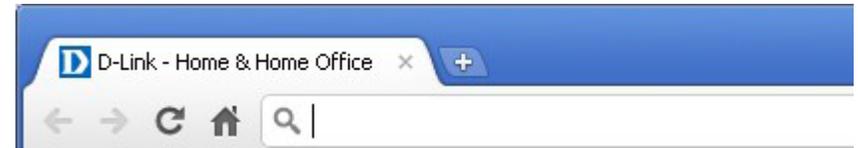
If this is your first time logging into the router, this wizard will start automatically.

This wizard is designed to guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

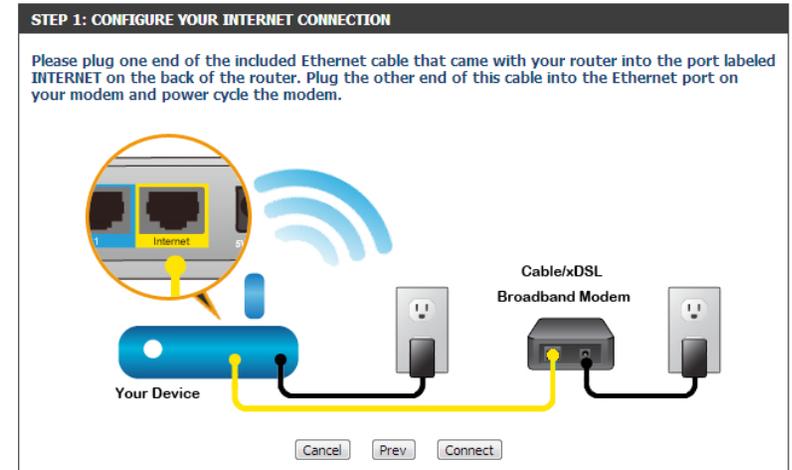
There are a number of languages that can be selected by using the drop down box in the upper right hand corner of the quick start wizard.

Click **Next** to continue.

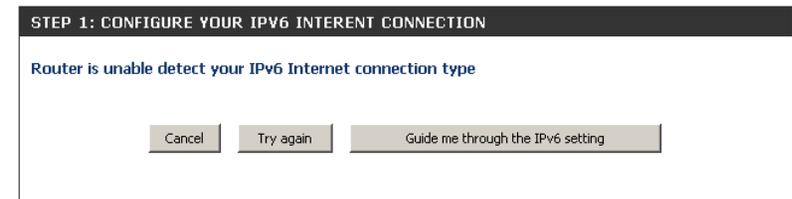
Please wait while your router detects your internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password.



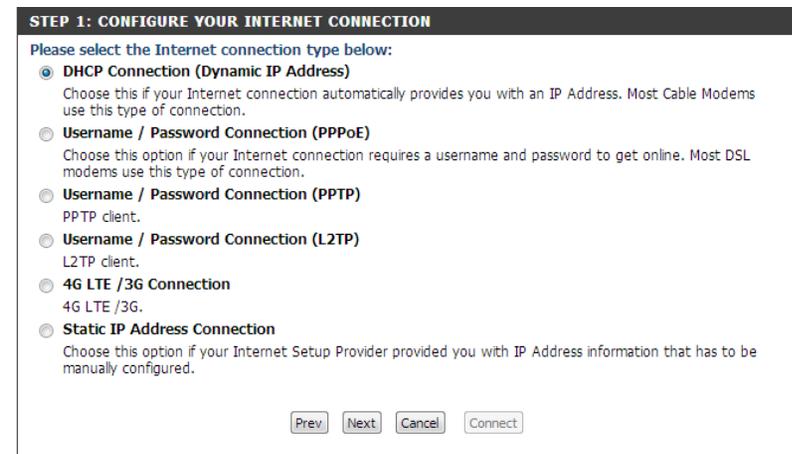
If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Connect your broadband modem to the Internet port and then click **Try Again**.



If the router detects an Ethernet connection but does not detect the type of Internet connection you have, this screen will appear. Click **Guide me through the Internet Connection Settings** to display a list of connection types to choose from.



Select your Internet connection type and click **Next** to continue.



If the router detected or you selected **DHCP**, you may enter a MAC address and host name, click **Next** to continue. You may also need to click the Clone button in order to copy the MAC address from your computer. If you are unsure, check with your ISP to find out what their requirements are.

DHCP CONNECTION (DYNAMIC IP ADDRESS)

To set up this connection, please make sure that you are connected to the Router with the PC that was originally connected to your broadband connection. If you are, then click the Clone MAC button to copy your computer's MAC Address to the Router.

MAC Address :

Host Name :

Note: You may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

If the router detected or you selected **PPPoE**, enter your PPPoE username and password and click **Next** to continue.

Note: Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.

SET USERNAME AND PASSWORD CONNECTION (PPPOE)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. If you do not have this information, please contact your ISP.

IP Address :

User Name :

Password :

Verify password :

Service Name : (optional)

Note: You may also need to provide a Service Name. If you do not have or know this information, please contact your ISP.

If the router detected or you selected **PPTP**, enter your PPTP username, password, and other information supplied by your ISP. Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (PPTP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify Password :

If the router detected or you selected **L2TP**, enter your L2TP username, password, and other information supplied by your ISP. Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify Password :

If the router detected or you selected **4G LTE / 3G Connection**, select whether to use auto-detection or manual configure the settings. If you choose to manually configure the settings, you will need to enter the following:

Country: Select the country that your service is from.

Telecom: Select the carrier from which you receive service from.

3G/4G Network: Select the network service type.

Username: The username, if needed to access your service.

Password: The password, if needed to access your service.

Dialed Number: The number which is needed to access the service provided.

Authentication: The authentication mode which is needed in order to access the service provided.

APN: The APN supplied by your service provider.

Pin Code: The pin code supplied by your service provider.

If the router detected or you selected **Static**, enter the IP and DNS settings supplied by your ISP. Click **Next** to continue.

SET 4G LTE /3G CONNECTION

Dial-Up Profile : Auto-Detection Manual

Country :

Telecom :

3G/4G Network :

Username : (optional)

Password : (optional)

Verify Password : (optional)

Dialed Number :

Authentication :

APN : (optional)

Pin Code :

SET STATIC IP ADDRESS CONNECTION

To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP.

IP Address :

Subnet Mask :

Gateway Address :

Primary DNS Address :

Secondary DNS Address :

The quick setup wizard will then ask you to configure a wireless SSID for your to easily identify the wireless network that you will create with your new D-Link router.

Click **Next** to continue.

Create a Wi-Fi password (between 8-63 characters). Your wireless clients will need to have this passphrase or key entered to be able to connect to your wireless network.

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.

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.

In order to secure your router, please enter a new password.

Click **Next** to continue.

STEP 2: CONFIGURE YOUR WI-FI SECURITY

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: CONFIGURE YOUR WI-FI SECURITY

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.

STEP 3: 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 menu and click **Next** to continue.

STEP 4: 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.

(GMT+08:00) Taipei

Cancel Prev Next

The quick setup wizard is now complete. You may now click the **Connect** button to save your configuration and continue.

SETUP COMPLETE!

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

Prev Next Cancel Connect

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 22.

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 :

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 18 for information about how to configure this type of connection.

Username / Password Connection (PPPoE): Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See page 18 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 19 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 19 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 20 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 21 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.

DHCP CONNECTION (DYNAMIC IP ADDRESS)

To set up this connection, please make sure that you are connected to the Router with the PC that was originally connected to your broadband connection. If you are, then click the Clone MAC button to copy your computer's MAC Address to the Router.

MAC Address :

Host Name :

Note: You may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

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.

SET USERNAME AND PASSWORD CONNECTION (PPPOE)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. If you do not have this information, please contact your ISP.

IP Address :

User Name :

Password :

Verify password :

Service Name : (optional)

Note: You may also need to provide a Service Name. If you do not have or know this information, please contact your ISP.

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.

SET USERNAME AND PASSWORD CONNECTION (PPTP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.

Address Mode : Dynamic IP Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify password :

Prev Next Cancel Connect

SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify password :

Prev Next Cancel Connect

3G/4G LTE Connection

Dial-Up Profile: Choose whether to have the router auto-detect the 3G settings necessary or to manually input the necessary values.

Country: Use the dropdown menu to select which country your 3G service provider is based from.

Telecom: Once you have selected the country from which your 3G provider resides in, a list of 3G service telecom providers will be available for you to choose from.

3G Network: Select the type of 3G network your provider uses.

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.

PIN: Enter the PIN code used with your SIM card.

SET 4G LTE / 3G CONNECTION

Dial-Up Profile : Auto-Detection Manual

Country : Angola

Telecom : Unitel

3G Network : WCDMA/HSPA

Username : (optional)

Password : (optional)

Verify Password : (optional)

Dialed Number :

Authentication : Auto

APN : (optional)

Pin Code :

Prev. Next Cancel Connect

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.

SET STATIC IP ADDRESS CONNECTION

To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP.

IP Address :

Subnet Mask :

Gateway Address :

Primary DNS Address :

Secondary DNS Address :

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.

SETUP COMPLETE!

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

Manual Internet Connection Setup

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** button in order to configure this setting. Please refer to “Failover Setting” on page 23 for more details on how to configure settings.

INTERNET CONNECTION

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP and 3G. If you are unsure of your connection method, please contact your Internet Service Provider.

Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

INTERNET CONNECTION TYPE

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

My Internet Connection is

Failover Internet Type is

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.

FAILOVER SETTING

Use this section to configure your Failover setting.
Please note that the LoadSharing / Failover does not support Internet Connection PPTP/L2TP.

FAILOVER SETTING :

Failover type : Load Sharing ▼

Remote Host for Keep Alive :

FAILOVER LIST

Primary WAN	Dynamic IP (DHCP)	
Secondary WAN	-	<input type="button" value="Add New Rule..."/>

FAILOVER SETTING

Use this section to configure your Failover setting.
Please note that the LoadSharing / Failover does not support Internet Connection PPTP/L2TP.

FAILOVER SETTING :

Failover type : Failover ▼

Remote Host for Keep Alive :

FAILOVER LIST

Primary WAN	Dynamic IP (DHCP)	
Secondary WAN	4G LTE /3G ▼	<input type="button" value="Add New Rule..."/>

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.

INTERNET CONNECTION TYPE

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

My Internet Connection is

Failover Internet Type is

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE

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

Host Name :

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1500

MAC Address :

Auto-reconnect : Enable

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.

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.

PPPOE

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

Username :

Password :

Verify Password :

Service Name : (optional)

IP Address :

Primary DNS Server : (optional)

Secondary DNS Server : (optional)

MAC Address :

Maximum Idle Time : seconds

MTU : (bytes) MTU default = 1492

Reconnect Mode : Always-on Manual

PPTP

Choose this Internet connection if your ISP provides you a 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.

INTERNET CONNECTION TYPE

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

My Internet Connection is PPTP (Username / Password) ▼

Failover Internet Type is Disable (N/A)

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 a 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 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.

INTERNET CONNECTION TYPE

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

My Internet Connection is L2TP (Username / Password) ▼

Failover Internet Type is Disable (N/A)

L2TP

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

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always-on Connect-on-demand

Maximum Idle Time : seconds

Save Settings
Don't Save Settings

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.

Dial-Up Profile: Choose whether to have the router auto-detect the 3G settings necessary or to manually input the necessary values.

Country: Use the dropdown menu to select which country your 3G service provider is based from.

Telecom: Once you have selected the country from which your 3G provider resides in, a list of 3G service telecom providers will be available for you to choose from.

3G Network: Select the type of 3G network your provider uses.

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.

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).

Dial-Up Profile : Auto-Detection Manual

Country : Angola

Telecom : Unitel

3G Network : WCDMA/HSPA

Username : (optional)

Password : (optional)

Verify Password : (optional)

Dialed Number :

Authentication : Auto

APN : (optional)

Pin Code :

Reconnect Mode : Auto Manual

Maximum Idle Time : 600 seconds

Primary DNS Server :

Secondary DNS Server :

Keep Alive : Disable Use Ping

Bridge ethernet ports : Enable

Save Settings

Don't Save Settings

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

Mode:

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

Time: Mode to disable.

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

Server:

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

Server:

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

Bridge Ethernet Activate this feature to change Ethernet WAN port to LAN port.

Ports:

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.

INTERNET CONNECTION TYPE

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

My Internet Connection is

Failover Internet Type is

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 :

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 35.

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 39.

WIRELESS CONNECTION

There are 3 ways to setup your wireless connection. You can use the Wireless Connection Setup wizard or you can manually configure the connection.

Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS CONNECTION SETUP WIZARD

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

[Wireless 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 WIRELESS CONNECTION OPTIONS

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

[Manual Wireless Connection Setup](#)

WI-FI PROTECTED SETUP

If you would like to configure the Wi-Fi Protected Setup of your Router, then click on the button below.

[Wi-Fi Protected Setup](#)

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.

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 :

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 can be between 5 to 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 :

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) : dlink_DWR-116

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 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. 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.

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.

WIRELESS NETWORK SETTINGS

Enable Wireless :

Wireless Network Name : (Also called the SSID)

802.11 Mode :

Auto Channel Scan :

Wireless Channel :

Visibility Status : Visible Invisible

WIRELESS SECURITY MODE

Security Mode :

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 your 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 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 :

WEP Encryption :

Default WEP Key :

WEP Key :
(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 : <input type="text" value="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 : <input type="text" value="WPA2 only"/>
Cipher Type : <input type="text" value="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 : <input type="text" value="d9p3-9paa-141"/> (8~63 ASCII or 64 HEX)

Save Settings

Don't Save Settings

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

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 :

Cipher Type :

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 :

RADIUS server Port :

RADIUS server Shared Secret :

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.

WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

Save Settings Don't Save Settings

WI-FI PROTECTED SETUP

WPS : Enabled Disabled

AP PIN : 97149309

Config Mode : Registrar ▼

Config Status : UNCONFIGURED

Disable WPS-PIN Method :

Config Method : Push Button ▼

WPS status : IDLE

Save Settings Don't Save Settings

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.

NETWORK SETTING

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP address to the computers on your network. 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.

Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.

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 :

Default Subnet Mask :

Local Domain Name :

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 : to (addresses within the LAN subnet)

DHCP Lease Time : (Seconds)

Primary DNS IP Address :

Secondary DNS IP Address :

Primary WINS IP Address :

Secondary WINS IP Address :

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 **Server:** 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.

NETWORK SETTING

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP address to the computers on your network. 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.

Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.

Save Settings

Don't Save Settings

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 :

Default Subnet Mask :

Local Domain Name :

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 : to (addresses within the LAN subnet)

DHCP Lease Time : (Seconds)

Primary DNS IP Address :

Secondary DNS IP Address :

Primary WINS IP Address :

Secondary WINS IP Address :

Save Settings

Don't Save Settings

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.

VIRTUAL SERVER

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

Well known services -- select one -- ID --

Use schedule rule ---ALWAYS ON---

VIRTUAL SERVERS LIST

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
9	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
10	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
11	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
12	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
13	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>

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.

APPLICATION RULES

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

Popular applications ID

APPLICATION RULES

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

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.

QOS ENGINE

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

QOS ENGINE SETUP

Enable QoS Packet Filter :

Upstream bandwidth : kbps

Use schedule rule ---ALWAYS ON--- **ID** --

QOS RULES

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▼	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>

MAC Address Filter

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

MAC Address Control: 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

A: filtering settings.

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

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 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 --
 ID -- --

MAC FILTERING RULES

ID	MAC Address	C	A
1	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

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	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

Save Settings Don't Save Settings

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.

OUTBOUND FILTER

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

OUTBOUND FILTER SETTING

Outbound Filter : Enable

Use schedule rule ---ALWAYS ON--- **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	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>

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 Rule: 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.

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.

INBOUND FILTER SETTING

Inbound Filter : Enable

Use schedule rule ---ALWAYS ON--- **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	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
2	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
3	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
4	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
5	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
6	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
7	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>
8	<input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> : <input type="text" value=""/>	<input type="checkbox"/>	<input type="button" value="Add New Rule..."/>

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.

SNMP

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

SNMP

SNMP Local : Enabled Disabled

SNMP Remote : Enabled Disabled

Get Community :

Set Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

SNMP Version : V1 V2c

WAN Access IP Address :

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.

ROUTING

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

RIP SETTING

RIP :
 Enable
 RIPv1
 RIPv2

ROUTING RULES

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

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.

Set the transmit power of the antennas.

Transmit Power:

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:

A Delivery Traffic Indication Message (DTIM) is a countdown informing clients of the next window

WMM Capable: for listening to broadcast and multicast messages. The default interval is 3.

TX Rates: 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.

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 WIRELESS

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

ADVANCED WIRELESS SETTINGS

Beacon Interval : (msec, range:1~1000, default: 100)

Transmit Power : ▾

RTS Threshold : (1~2347,default 2347)

Fragmentation : (256~2346,default 2346,even number only)

DTIM Interval : (range: 1~255)

WMM Capable Enable Disable

TX Rates : ▾

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.

ADVANCED NETWORK

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

UPNP

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

Enable UPnP :

WAN PING

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

Enable WAN Ping Respond :

DMZ

A firewall protects your network from the outside world. The DWR-116 offers a firewall type functionality. The *Stateful Packet Inspection (SPI)* feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

Enable SPI: *SPI (Stateful Packet Inspection)*, also known as dynamic packet filtering, helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

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

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

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

DMZ

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

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 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 the chosen password.

Confirm Password:

Remote management allows the DWR-116 to be configured from the Internet using a web browser.

Remote Management: 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.

ADMINISTRATOR SETTINGS

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

ADMINISTRATOR (THE DEFAULT LOGIN NAME IS "admin")

New Password :

Confirm Password :

REMOTE MANAGEMENT

Enable Remote Management : Enabled

IP Allowed to Access :

Port :

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.

TIME AND DATE

The Time and Date Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server.

TIME AND DATE CONFIGURATION

Time : Tue Mar 26, 2013 23:36:33

(GMT -08:00) Pacific Time (US & Canada) ▼

Time Zone :

AUTOMATIC TIME AND DATE CONFIGURATION

Automatically synchronize with Internet time server

NTP Server Used :

time.nist.gov ▼

SYNC. RESULT

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

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 :

Save Settings Don't Save Settings

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 Sever 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.

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

Save Settings Don't Save Settings

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.

SYSTEM SETTINGS

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

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

SAVE AND RESTORE SETTINGS

Save Settings To Local Hard Drive :

Load Settings From Local Hard Drive :

Restore To Factory Default Settings :

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.

Current Firmware Date: Displays your current 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.

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 : 2013/01/18

FIRMWARE UPGRADE

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

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

Upload :

Accept unofficial firmware.

LANGUAGE PACK UPGRADE

Upload :

Remove Language Pack :

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) with your dynamically assigned IP address.

Sign up for D-Link's free DDNS service at 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.

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

Enable DDNS :

Provider : DynDNS.org(Dynamic) ▼

Host Name :

Username / E-mail :

Password / Key :

Save Settings Don't Save Settings

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.

The screenshot displays the 'PING TEST' section of a system check utility. It features an orange header with the text 'PING TEST'. Below the header, a grey box contains the text: 'Ping Test sends "ping" packets to test a computer on the Internet.' Underneath this box are two buttons: 'Save Settings' and 'Don't Save Settings'. The main content area has a dark grey header with 'PING TEST' and a white background with the text: 'Ping Test is used to send "Ping" packets to test if a computer is on the Internet.' Below this text is a label 'Host Name or IP address :', a text input field, and a 'Ping' button. At the bottom of the form is a dark grey header with 'PING RESULT' and a large empty white box for displaying results. Below the entire form are two buttons: 'Save Settings' and 'Don't Save Settings'.

Schedules

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

Enable Schedule: Tick this check box to enable schedules.

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.

SCHEDULES

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

SCHEDULE RULE

Enable Schedule :

Rule#	Rule Name	Action
<input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Add New Rule..."/>		

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.

DEVICE INFORMATION

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

GENERAL

Time : Tue Mar 26, 2013 23:37:23 -0800
Firmware Version : V1.00 , 2013/01/18

WAN

Connection Type : 4G LTE /3G
 Network Status : Disconnected
 Connection Time : N/A
 Signal Strength :
 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

3G CARD

Link Status : Disconnected.(No Modem Detected)
Network Name : N/A

LAN

MAC Address : 90:94:E4:E6:D9:32
 IP Address : 192.168.0.1
 Subnet Mask : 255.255.255.0
 DHCP Server : Enabled

WIRELESS LAN

MAC Address : 90:94:E4:E6:D9:32
 Wireless : Enabled
 SSID : dlnk_DWR-116
 Security : Auto(None)
 Channel : 11
 802.11 Mode : B/G/N Mixed
 Wi-Fi Protected Setup : Enabled

LAN COMPUTERS

IP Address	Name	MAC
192.168.0.118	07871PCWIN7E	CC-52-AF-49-E6-75

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.

VIEW LOG

View Log displays the activities occurring on the device.

Page: 1/7 (Log Number : 98)

SYSTEM LOG

Time	Message
Mar 26 23:11:14	kernel: klogd started: BusyBox v1.3.2 (2013-01-18 15:24:41 CST)
Mar 26 23:11:15	O3G/modem_switch: MODEM_SWITCH [0x2001] [0xa80b]
Mar 26 23:11:16	BEID: BEID STATUS : 0 , STATUS OK!
Mar 26 23:11:17	syslog: Failure parsing line 12 of /etc/udhcpd.conf
Mar 26 23:11:17	syslog: server_config.pool_check = 1
Mar 26 23:11:17	syslog: start = 192.168.0, end = 192.168.0, lan_ip = 192.168.0, interface=br0, ifindex=0
Mar 26 23:11:17	udhcpd[1263]: udhcpd (v0.9.9-pre) started
Mar 26 23:11:21	commander: Init NAT Server ...
Mar 26 23:11:25	init: Starting pid 2406, console /dev/ttyS1: '/bin/ash'
Mar 26 23:11:26	commander: STOP WANTYPE 3G
Mar 26 23:11:30	commander: Synchronization Time Fail. System would re-sync later
Mar 26 23:11:35	O3G/modem_switch: MODEM_SWITCH [0x2001] [0xa80b]
Mar 26 23:11:38	O3G/modem_switch: OK, Driver buf "" , -61
Mar 26 23:11:38	rmand successfully sent. Box probably switched.
Mar 26 23:11:40	O3G/hotplug: 3G modem VendorID=2001 ProductID=7d00

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.

TRAFFIC STATISTICS

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

WAN STATISTICS INFORMATION

Statistics	Inbound	Outbound
Octets	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. It also displays the connection time and MAC address of the connected wireless clients.

WIRELESS CLIENT LIST

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

WIRELESS CLIENT TABLE

ID	MAC Address
----	-------------

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.

The screenshot displays the D-Link DWR-116 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar contains tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The SUPPORT tab is selected. On the left side, there is a vertical menu with options: MENU, SETUP, ADVANCED, TOOLS, STATUS, and LOGOUT. Below this menu, there is a status indicator for 'Internet Offline' and a 'Reboot' button. The main content area is titled 'SUPPORT MENU' and contains a list of links: Setup, Advanced, Tools, and Status. Below this, there are four sections of help information: 'SETUP HELP' with links for Internet, Wireless Settings, and Network Settings; 'ADVANCED HELP' with links for VIRTUAL SERVER, Application Rules, QoS Engine, MAC Address Filter, URL Filter, Outbound Filter, Inbound Filter, SNMP, Routing, Advanced Wireless, and Advanced Network; 'TOOLS HELP' with links for Admin, Time, SysLog, Email settings, System, Firmware, Dynamic DNS, System Check, and Schedules; and 'STATUS HELP' with links for Device Info, Log, Statistics, and Wireless. At the bottom of the interface, the word 'WIRELESS' is displayed.

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

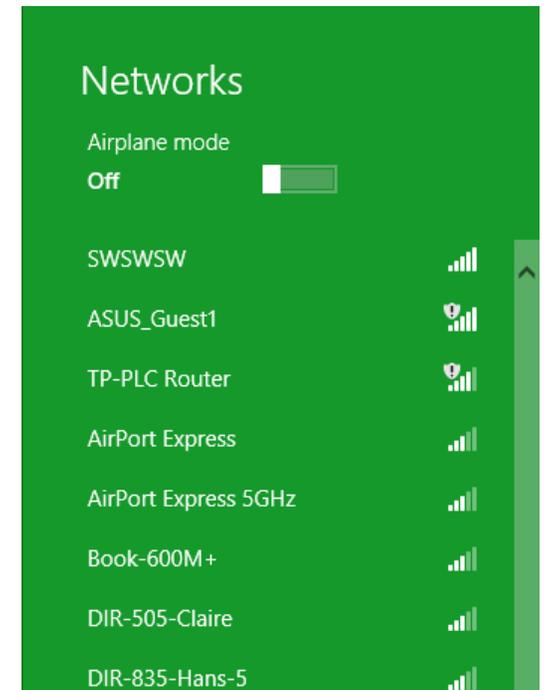
WPA/WPA2

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.

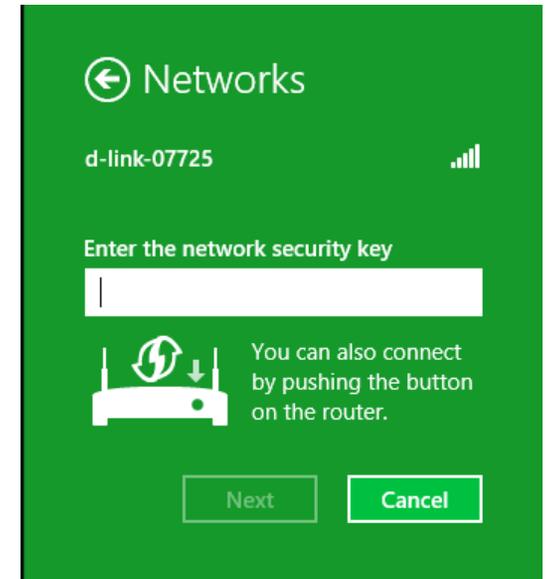


Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.

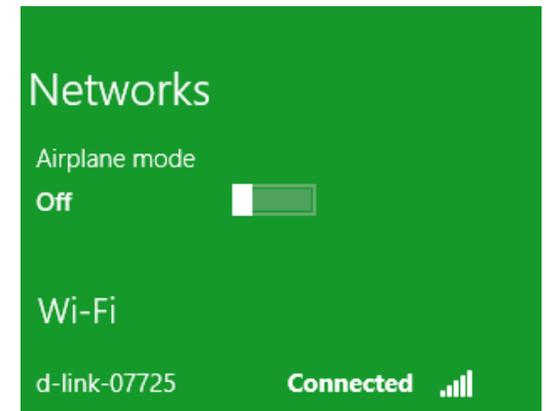


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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.



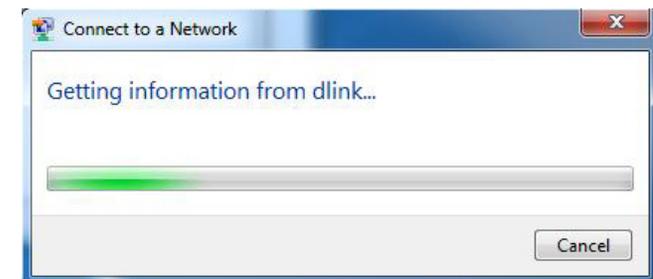
3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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.

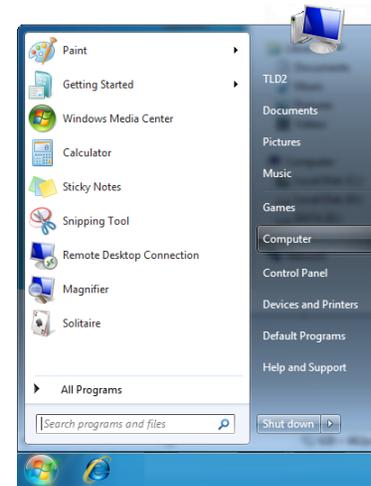
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



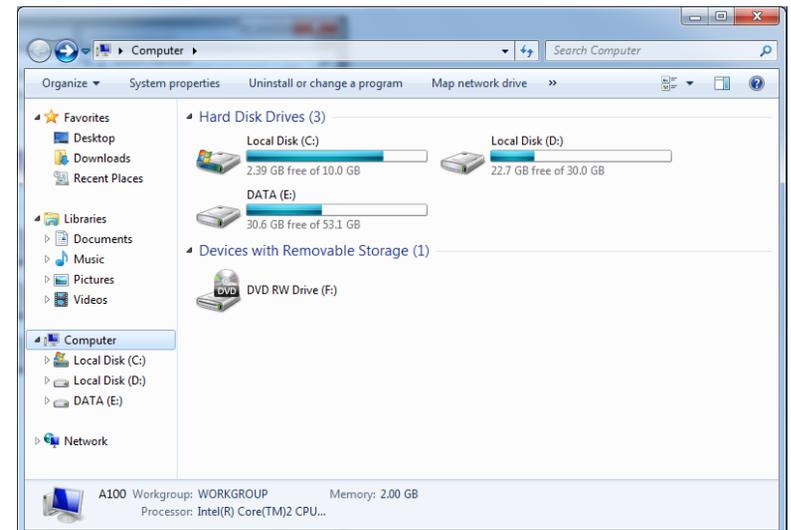
WPS

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:

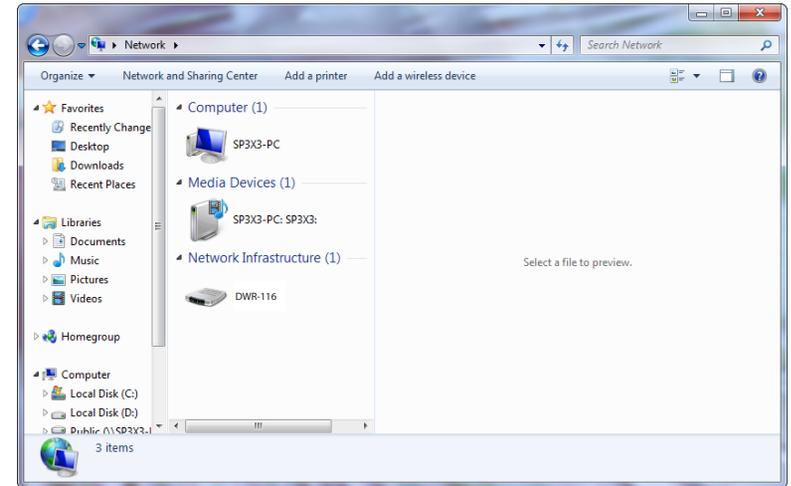
1. Click the **Start** button and select **Computer** from the Start menu.



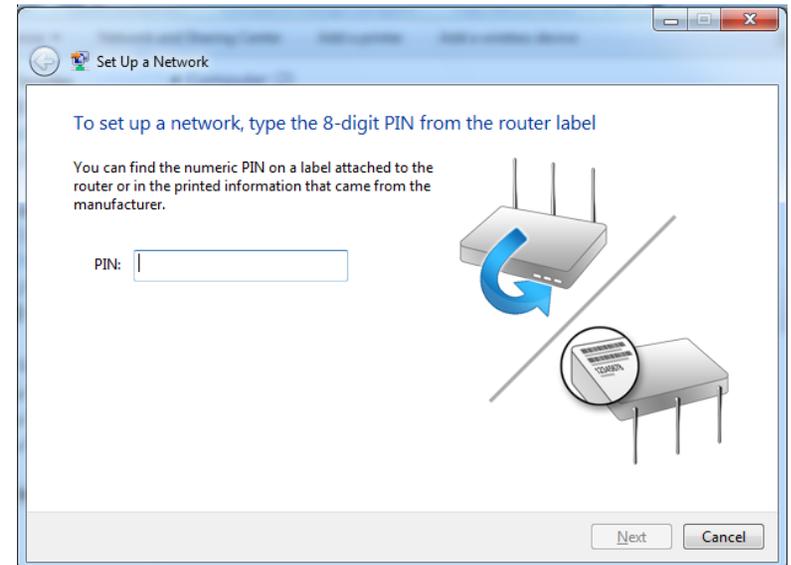
2. Click **Network** on the left side.



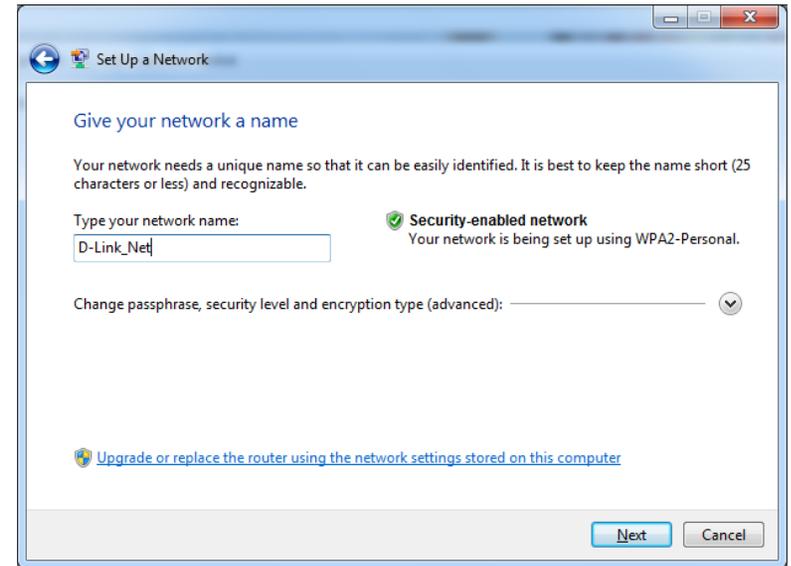
3. Double-click the DWR-116



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**.

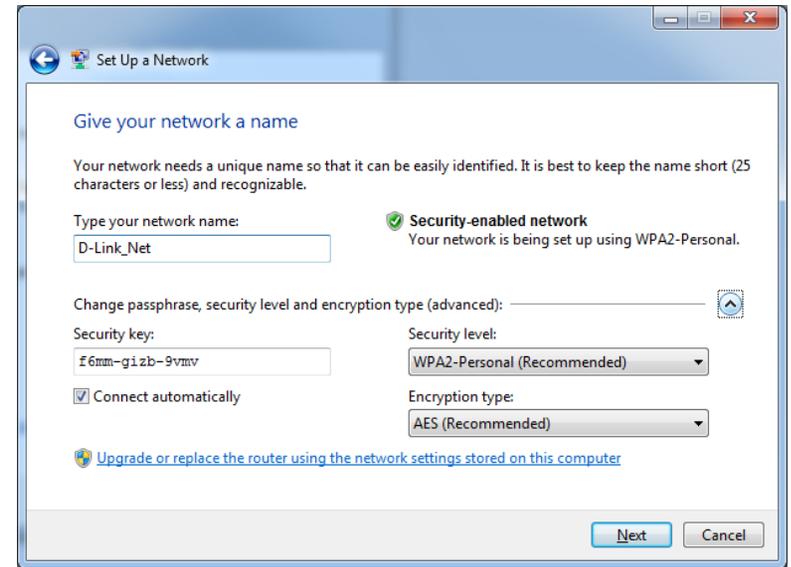


5. Type a name to identify the network.



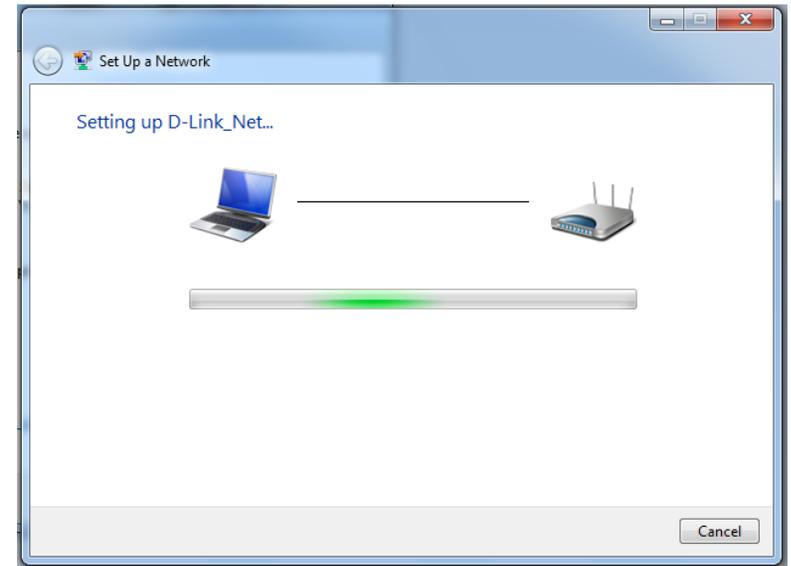
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



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

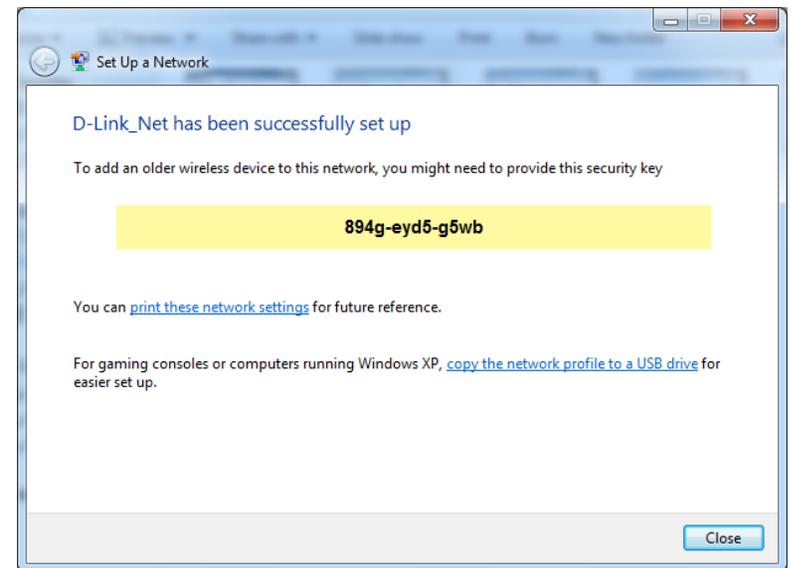
Wait for the configuration to complete.



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.

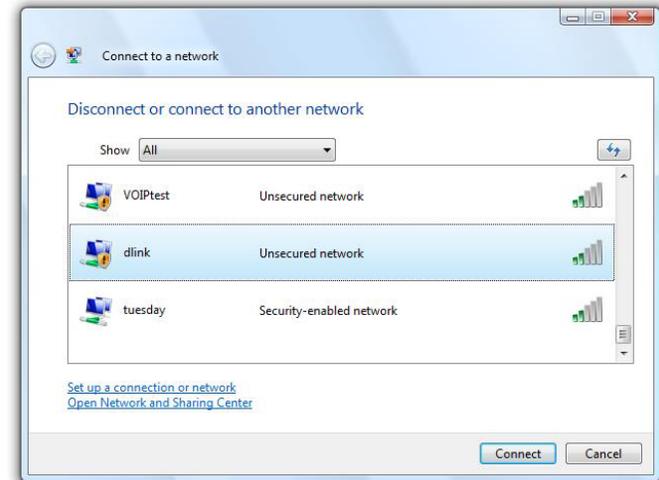
or

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.



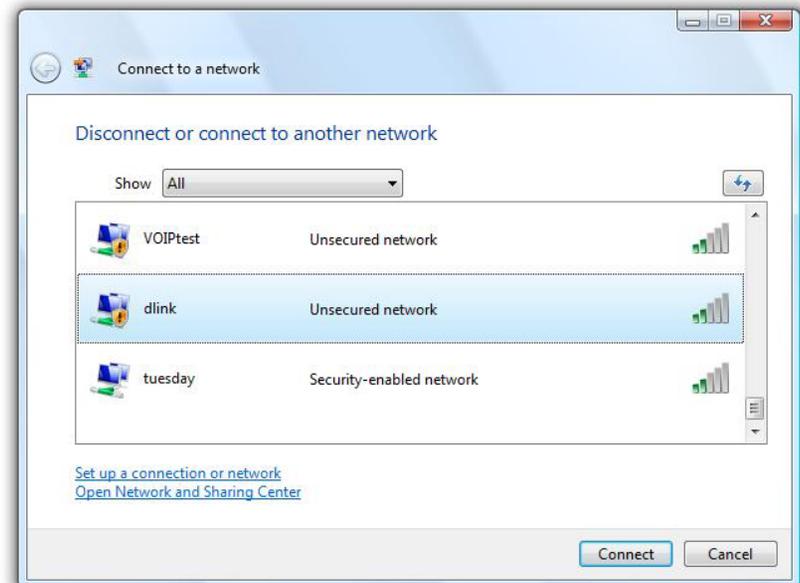
WPA/WPA2

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**.

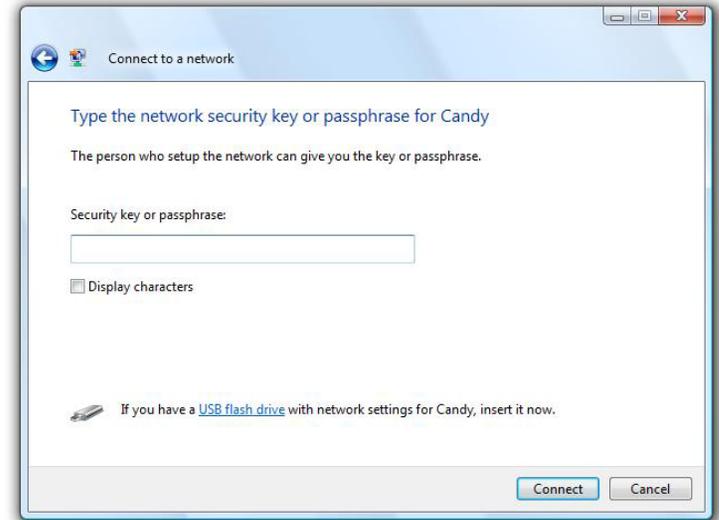


2. Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.



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.

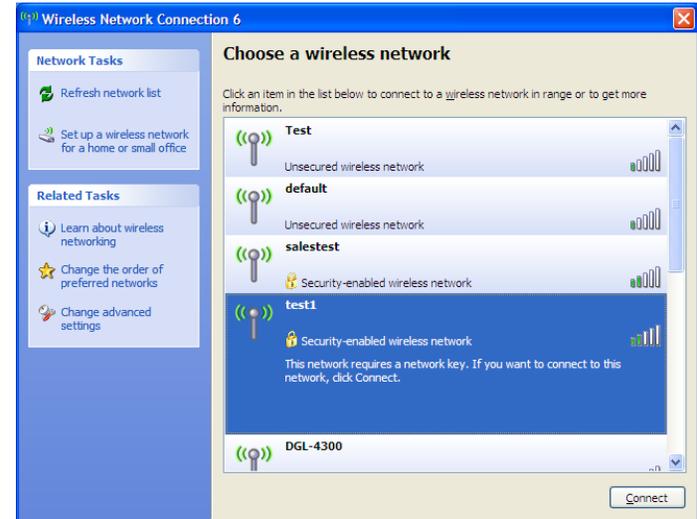
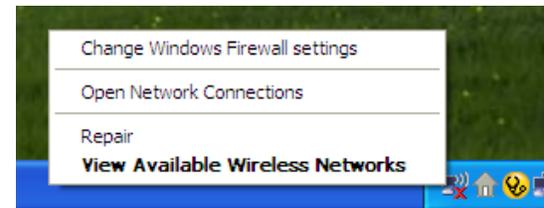
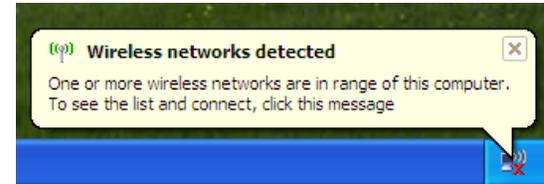
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

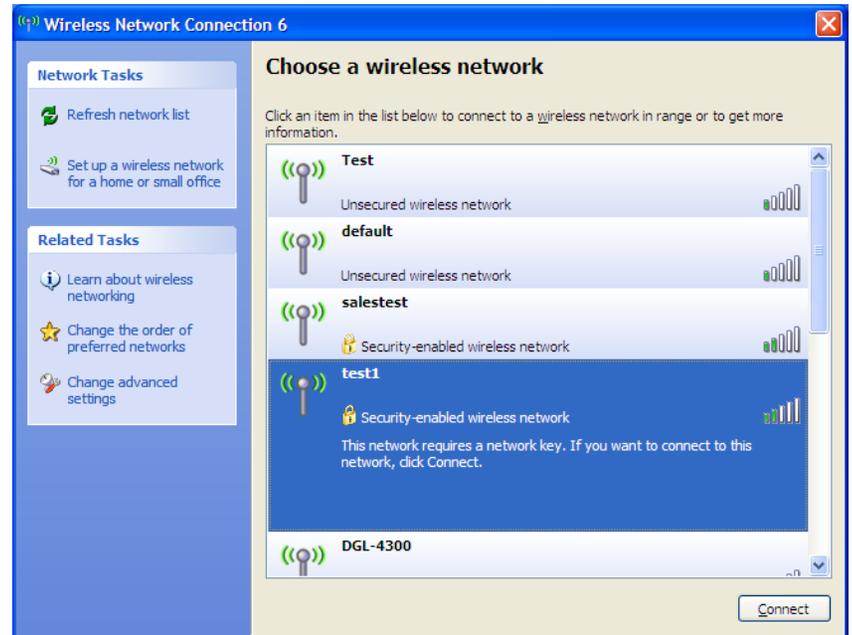
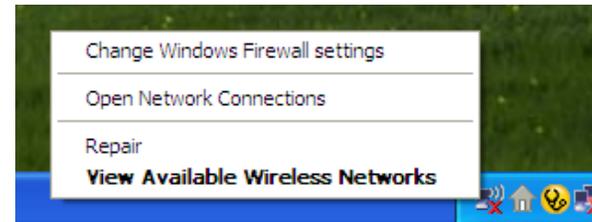
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

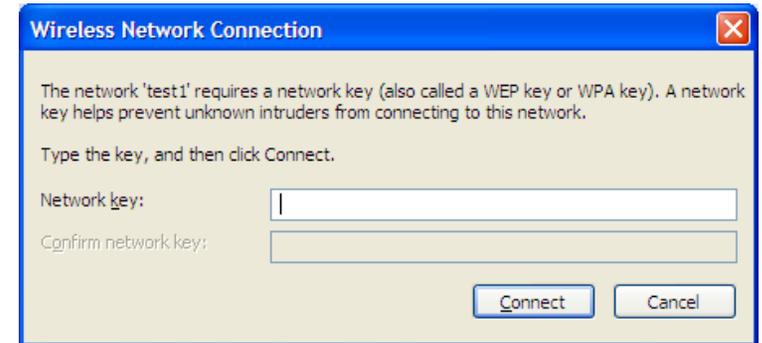
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

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

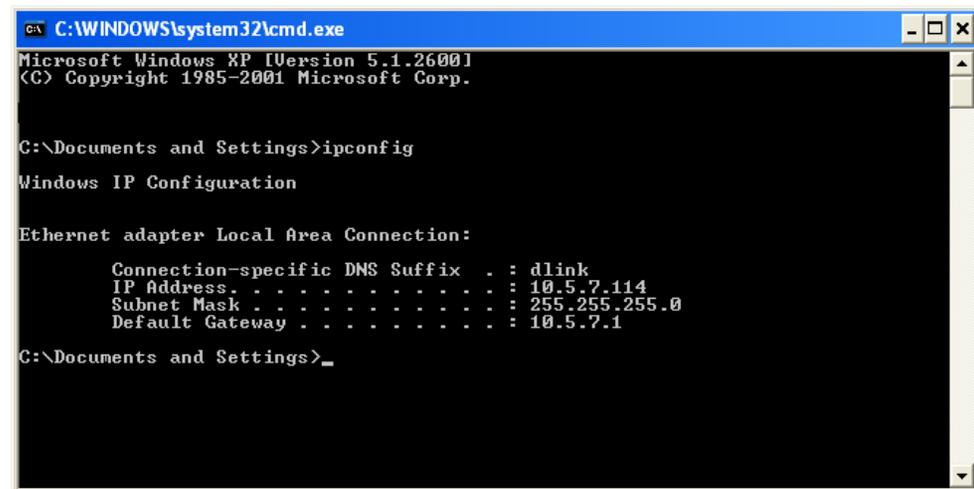
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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® 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

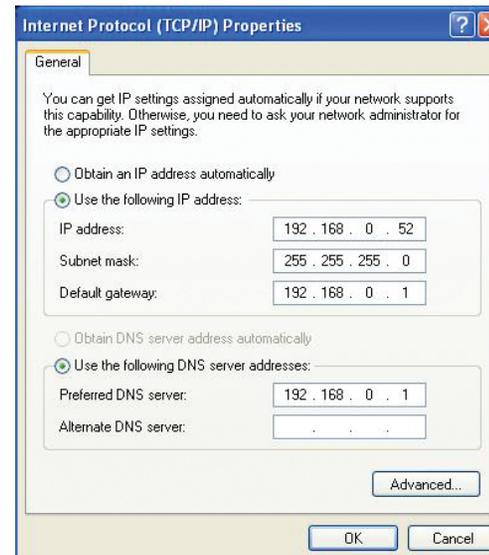
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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)
1x 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

Federal Communication Commission Interference Statement

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

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

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your 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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.