



User Manual

Wireless N150 Wi-Fi Router

DWR-111

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	October 25, 2013	DCS-6004L/DCS-6005L Revision A1 with firmware version 1.00

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 Systems, Inc.

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

Table of Contents

Package Contents.....	1	Router Settings.....	27
System Requirements.....	1	DHCP Server Settings.....	28
Introduction.....	2	Virtual Server.....	29
Front Panel and LEDs.....	3	Application Rules.....	30
Hardware Overview.....	4	QoS Engine.....	31
Back Panel.....	4	MAC Address Filter.....	32
Installation.....	5	URL Filter.....	33
Connect to Your Network.....	5	Outbound Filter.....	34
Wireless Installation Considerations.....	6	Inbound Filter.....	35
Configuration.....	7	SNMP.....	36
Web-based Configuration Utility.....	7	Routing.....	37
Setup Wizard.....	8	Advanced Wireless.....	38
Internet Connection Setup Wizard.....	8	Advanced Network.....	39
Manual Internet Connection Setup.....	12	DMZ.....	40
Internet Connection.....	13	Admin.....	41
Internet Connection Type.....	13	Time.....	42
Dynamic IP (DHCP).....	14	Syslog.....	43
PPPoE.....	15	E-mail Settings.....	44
PPTP.....	17	System.....	45
L2TP.....	19	Firmware.....	46
3G.....	21	Dynamic DNS.....	47
Static IP.....	23	System Check.....	48
Failover Setting.....	24	Schedules.....	49
Wireless Settings.....	25	Device Information.....	50
Network Settings.....	27	Logs.....	51
		Statistics.....	52

Wireless	53
Support	54
Wireless Security	55
What is WEP?	55
Configure WEP	56
What is WPA?	57
Configure WPA-PSK.....	58
Configure WPA (RADIUS)	59
Connect to a Wireless Network.....	60
Using Windows Vista™	60
Configure Wireless Security	61
Connect to a Wireless Network.....	63
Using Windows® XP	63
Configure WEP	64
Configure WPA-PSK.....	66
Troubleshooting	68
Wireless Basics	70
What is Wireless?	71
Tips.....	73
Wireless Modes.....	74
Networking Basics	75
Check your IP address.....	75
Statically Assign an IP address	76
Technical Specifications	77

Product Overview

Package Contents

- D-Link DWR-111 Wireless N150 Wi-Fi Router
- Power Adapter
- Manual and Warranty on CD
- External Wi-Fi antenna

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

Note: Using a power supply with a different voltage rating than the one included with the DWR-111 will cause damage and void the warranty for this product.

System Requirements

- A compatible 3G USB modem
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator™ Version 6.0 and above (for configuration)

Introduction

The D-Link Wireless N150 Wi-Fi Router allows users to access worldwide mobile broadband networks. Once connected, users can transfer data and stream media. Simply connect your USB modem and share your 3G Internet connection through a secure 802.11n wireless network or using the 10/100 Ethernet port.

The Wireless N150 Wi-Fi Router can be installed quickly and easily almost anywhere. This router is great for situations where an impromptu wireless network must be set up, or wherever conventional network access is unavailable. The DWR-111 can even be installed in buses, trains, or boats, allowing passengers to check e-mail or chat online while commuting.

Hardware Overview

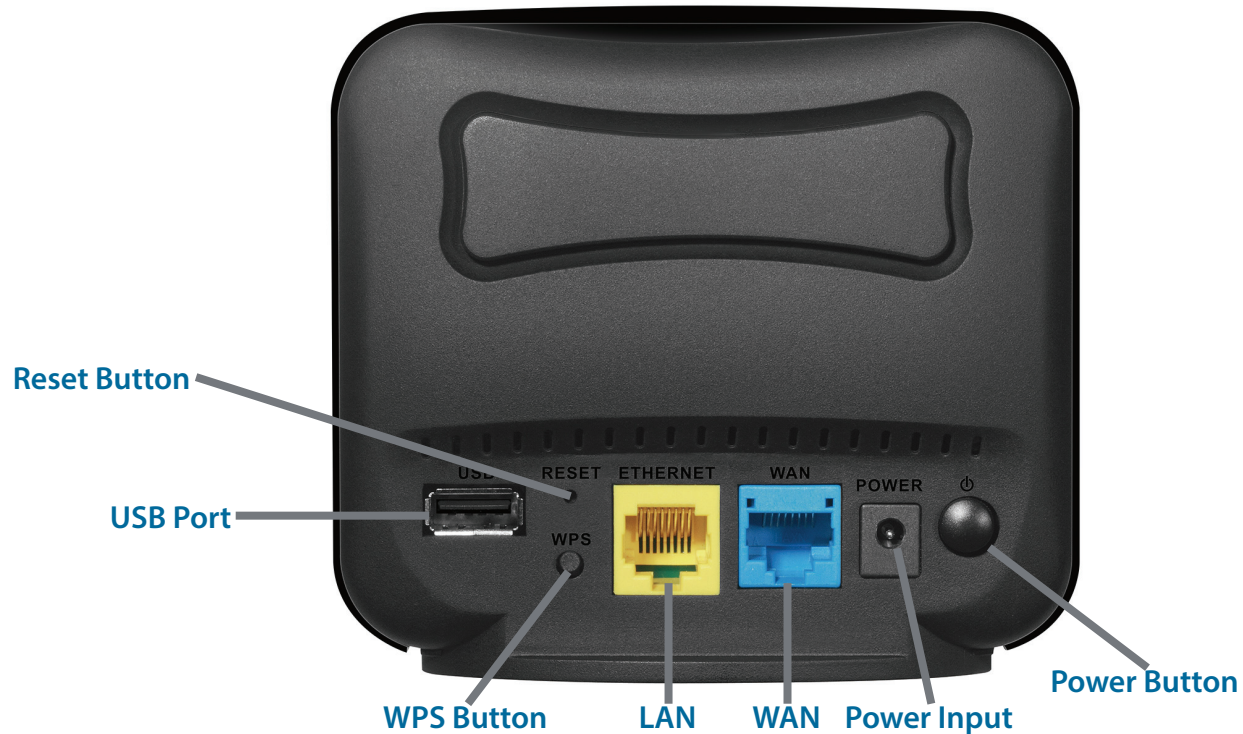
Front Panel and LEDs



LED	Description			
	Color	Solid	Blinking	Blinking (Fast)
Power	Green	The device is powered on		-
Internet	Green	Internet connection established		-
Wi-Fi	Green	Wi-Fi active and available	Data transmitting	Device in WPS mode
LAN	Green	Ethernet connection established	Data transmitting	-
USB	Green	3G connection established	Data transmitting	-
WAN	Green	WAN connection established	Data transmitting	-

Hardware Overview

Back Panel



Port	Function
Reset Button	Resets the device to its factory default settings.
USB Port	Connects to a USB modem.
WPS Button	Starts the WPS feature for connecting to other devices.
LAN Port	Connects to wired computers or devices.
WAN Port	Connects to the Internet.
Power Input	Connects to the power adapter.
Power Button	Turns the device on or off.

Installation

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

Connect to Your Network

Note: Ensure that your DWR-111 Wireless N150 Wi-Fi Router is disconnected and powered **off** before performing the installation steps below.

1. Connect a USB modem to the **USB** port on the back of the router.
2. Insert a LAN network cable into the **LAN** port on the back of the router. Plug the other end of the LAN 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-111 Wireless N150 Wi-Fi Router LAN Port is "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-111 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:

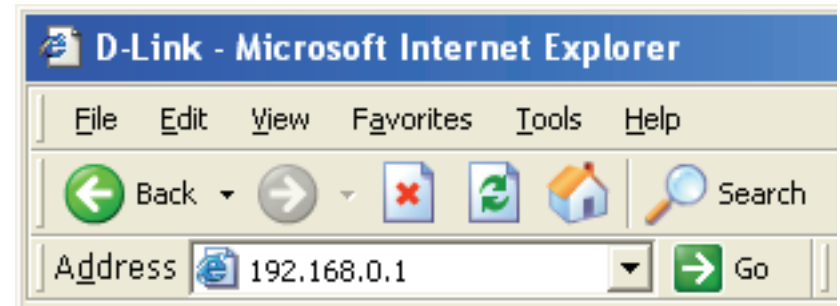
1. Minimize the number of walls and ceilings between the D-Link router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree 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 and drywall. Materials such as glass, metal, brick, insulation, concrete and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors and aluminum studs may also have a negative effect on range.
4. If you are using 2.4 GHz cordless phones, make sure that the 2.4 GHz phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

Configuration

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

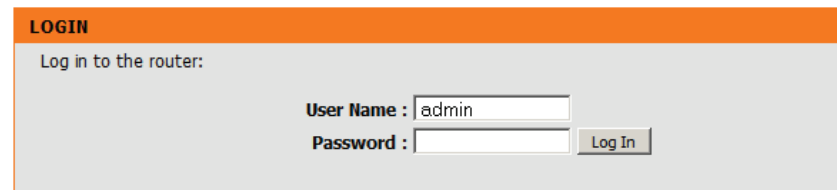
Web-based Configuration Utility

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



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

If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



Setup 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.

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 12.

INTERNET CONNECTION

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

INTERNET CONNECTION SETUP WIZARD

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

Internet Connection Setup Wizard

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

MANUAL INTERNET CONNECTION OPTIONS

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

Manual Internet Connection Setup

Internet Connection Setup Wizard

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

Click **Next** to continue.

WELCOME TO THE SETUP WIZARD

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

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

Prev Next Cancel Connect

Create a new password and then click **Next** to continue.
Click **Prev** to go back to the previous page or click **Cancel** to close the wizard.

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.

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-111 supports several kinds of WAN interfaces, allowing you to assign either a WAN or a WWAN(3G) 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 1: SET YOUR PASSWORD

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

Password :

Verify Password :

STEP 2: SELECT YOUR TIME ZONE

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

Time Zone :

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Please select the Internet connection type below:

DHCP Connection (Dynamic IP Address)

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

Username / Password Connection (PPPoE)

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

Username / Password Connection (PPTP)

PPTP client.

Username / Password Connection (L2TP)

L2TP client.

3G Connection

3G.

Static IP Address Connection

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

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

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 14 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 15 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 17 for information about how to configure this type of connection.

Username / Password Connection (L2TP): Choose this option if your Internet connection requires Layer 2 Tunneling Protocol (L2TP). See page 19 for information about how to configure this type of connection.

3G 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 21 for information about how to configure this type of connection.

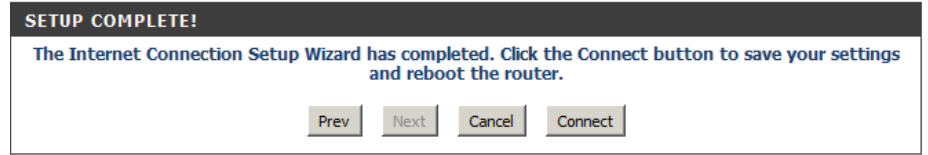
Static IP Address Connection: Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured. See page 23 for information about how to configure this type of connection.

You have completed the **Setup Wizard**.

Click **Connect** to save your settings.

A pop-up will appear, to confirm your settings.

Click **OK** to save your settings.



Manual Internet Connection Setup

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

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard** and refer to page 8.

INTERNET CONNECTION

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

INTERNET CONNECTION SETUP WIZARD

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

Internet Connection Setup Wizard

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

MANUAL INTERNET CONNECTION OPTIONS

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

Manual Internet Connection Setup

Internet Connection

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 Type is: This connection can serve as a backup for your default connection.

Host Name: Enter the name of the Internet host to be used as the backup connection.

Primary DNS Server: Enter the primary DNS server.

Secondary DNS Server: Enter the secondary DNS server.

MTU: Set the MTU (the default value is 1500).

MAC Address: Manually enter the MAC address or click **Clone** to copy the PC's MAC address.

Auto-reconnect: Check this check box to enable auto-reconnect.

NAT disable: Check this check box to disable network address translation.

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.

Save Settings

Don't Save Settings

Failover Setting...

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

NAT disable : Enable

Save Settings

Don't Save Settings

Dynamic IP (DHCP)

This section will help you to obtain IP Address information automatically from your ISP. Use this option if your ISP didn't provide you with IP Address information and/or a username and password.

Host Name: (Optional) Required by some ISPs.

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

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

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

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** 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

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.

Save Settings

Don't Save Settings

Failover Setting...

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 Load Sharing (3G)

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

NAT disable : Enable

Save Settings

Don't Save Settings

PPPoE

Choose this Internet connection if your ISP provides you 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 **Clone Your PC's MAC** 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. Set it to zero or enable Auto-reconnect will disable this feature.

Maximum Transmission Unit

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

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

NAT disable : Enable

(MTU): The default setting of PPPoE is 1492.

Reconnect Mode:

NAT disable: The device will dial-up PPPoE connection automatically if set to always, otherwise you will need to manually reconnect.

Check this check box to disable network address translation.

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

PPTP

Choose this Internet connection if your ISP provides you with 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 no traffic after time period of Maximum Idle Time expires.

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 PPTP (Username / Password) ▾

Failover Internet Type is Load Sharing (3G)

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

MAC Address :

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.

MAC Address:

If your ISP requires that you enter a MAC address to use with your PPTP account, enter it here. You can also click the **Clone** button, which will copy your computer's MAC address.

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

L2TP

Choose this Internet connection if your ISP provides you with 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 to you for L2TP dial-up.

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

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

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.

Save Settings

Don't Save Settings

Failover Setting...

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 Load Sharing (3G)

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

MAC Address :

Clone

Save Settings

Don't Save Settings

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.

MAC Address:

If your ISP requires that you enter a MAC address to use with your PPTP account, enter it here. You can also click the **Clone** button, which will copy your computer's MAC address.

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

3G

Choose this Internet connection if you already use a SIM card for 3G Internet service from your Telecom 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 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.

Reconnect Mode: Auto or Manual. Connect to 3G network automatically or manually.

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.

Save Settings

Don't Save Settings

Failover Setting...

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 Load Sharing (3G)

3G INTERNET CONNECTION TYPE

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

Dial-Up Profile : Auto-Detection Manual

Country :

Telecom :

3G Network :

Username : (optional)

Password : (optional)

Verify Password : (optional)

Dialed Number :

Authentication :

APN : (optional)

Pin Code :

Reconnect Mode : Auto Manual

Maximum Idle Time : seconds

Primary DNS Server :

Secondary DNS Server :

Maximum Idle Time: The time of no activity to disconnect established 3G session. Set it to zero or choose Auto in Reconnect Mode to disable this feature.

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

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

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

NAT disable: Disable or Use LCP Echo Request. It depends on ISP requirement.

Bridge Ethernet Ports: Disable Network Address Translation
Activate this feature to change Ethernet WAN port to LAN port.

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

Maximum Idle Time : seconds
Primary DNS Server :
Secondary DNS Server :
Keep Alive : Disable Use Ping
NAT disable : Enable
Bridge ethernet ports : Enable

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 Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

NAT disable:

Check this check box to disable network address translation.

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

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 Static IP ▼

Failover Internet Type is Load Sharing (3G)

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 :

NAT disable Enable

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..."/>

Wireless Settings

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

WIRELESS NETWORK SETTINGS

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-111".

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: A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may experience interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

WIRELESS NETWORK

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

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

Save Settings

Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless :

Wireless Network Name : (Also called the SSID)

802.11 Mode :

Auto Channel Scan :

Wireless Channel :

Visibility Status : Visible Invisible

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)

Save Settings

Don't Save Settings

Wireless Channel: Indicates the channel setting for the DWR-111. 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. 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.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by DWR-111. 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 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.

WIRELESS NETWORK

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

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

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless :
 Wireless Network Name : (Also called the SSID)
 802.11 Mode :
 Auto Channel Scan :
 Wireless Channel :
 Visibility Status : Visible Invisible

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)

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 to get into the 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.

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

The DWR-111 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 is automatically assigned to the clients on the network.

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

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

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 secondary DNS Server to DHCP clients.

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

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

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

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 :

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.

VIRTUAL SERVERS LIST

ID: Identifies the virtual server.

Service Ports: Internal port number for the service to be setup for public access.

Server IP: Port: Enter the last digits of 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="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
9	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
10	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
11	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
12	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
13	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
14	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
15	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
16	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" type="button" value="Add New Rule..."/>
17	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input style="float: right;" 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). **Applications Rules** let some of these applications work with the DWR-111.

APPLICATION RULES

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 -- select one -- **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 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 the applications.

QoS ENGINE SETUP

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).

QoS RULES

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="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High <input type="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High <input type="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High <input type="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High <input type="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High <input type="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High <input type="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High <input type="button" value="v"/>	<input type="checkbox"/>	<input type="text"/> <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 FILTERING SETTINGS

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: MAC FILTERING RULES

MAC Address: Identifies the rule.

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

If this box is selected, the rule will follow the connection control setting

A: specified in MAC filtering settings.

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

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

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: 90%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input style="width: 90%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input style="width: 90%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input style="width: 90%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input style="width: 90%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

URL Filter

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

URL Filtering: Select this box to enable URL Filtering.

URL FILTERING RULES

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 style="width: 100%;" type="text"/>	<input type="checkbox"/>
2	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>
3	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>
4	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>
5	<input style="width: 100%;" 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 the router. Outbound filter applies on all outbound packets.

OUTBOUND FILTER SETTING

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

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

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

OUTBOUND FILTER RULES LIST

ID: Identifies the filter.

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

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

Enable: 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="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <input type="button" value="Add New Rule..."/>

Inbound Filter

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

INBOUND FILTER SETTING

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

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

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

INBOUND FILTER RULES LIST

ID: Identifies the filter.

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

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

Enable: 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"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <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="text"/> <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-111. The DWR-111 supports SNMP v1 or v2c.

SNMP

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

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

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

Set Community: Enter the password **private** in this field to gain “Read and Write” access to the network using SNMP software.

IP 1, IP 2, IP 3, IP 4: Enter up to four IP addresses of any trap targets on your network.

SNMP Version: Select the SNMP version of your system.

WAN Access IP Address: Remote IP address that can be used to access the device for management via SNMP.

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.

Save Settings Don't Save Settings

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 :

Save Settings Don't Save Settings

Routing

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

RIP SETTING

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.

ROUTING RULES

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 of 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.

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

ROUTING

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

RIP SETTING

RIP : Enable RIPv1 RIPv2

ROUTING RULES

ID	Destination	Subnet Mask	Gateway	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.

Beacon Interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

Transmit Power: Set the transmit power of the antennas.

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

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

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

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

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

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

ADVANCED 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.

UPnP

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

WAN PING

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

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 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.

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

The screenshot shows the DMZ configuration page. At the top, there is an orange header with the text "DMZ". Below this, the word "DMZ" is displayed in a grey box. Underneath, there are two buttons: "Save Settings" and "Don't Save Settings".

The next section is titled "DMZ HOST" in a dark grey header. Below this, there is a paragraph of text explaining the DMZ option: "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." Below this text is a **Note** that repeats the warning about security risks. There is an "Enable DMZ" checkbox which is currently unchecked. Below that is a "DMZ IP Address" field with a text input box, a "<<" button, and a dropdown menu labeled "Computer Name".

At the bottom of the form, there are two buttons: "Save Settings" and "Don't Save Settings".

Admin

The **Admin** page allows you to change the Administrator password and enable Remote Management. The Admin 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.

ADMINISTRATOR

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

Confirm Password: Confirm the chosen password.

REMOTE MANAGEMENT

Enable Remote Management: Remote management allows the DWR-111 to be configured from the Internet using a web browser. A username and password is still required to access the Web-management interface. Usually only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from a 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-111.

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-111 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 : **Fri Jan 01, 2010 08:04:36**

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

Sync. your computer's time settings

AUTOMATIC TIME AND DATE CONFIGURATION

Automatically synchronize with Internet time server

NTP Server Used : time.nist.gov

time.nist.gov ▼

SYNC. RESULT

Syslog

The DWR-111 keeps a running log of events and activities occurring on the router. You may send these logs to a Syslog server on your network.

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

Syslog Server IP Address: Enter the address of the Syslog server that will be used to send the logs. You may also select your computer from the drop-down box (only if you want to receive an IP address from the router via DHCP).

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

E-mail Settings

E-mail 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

EMAIL SETTINGS

Enable Email Notification :

SMTP Server IP and Port : :

SMTP Username :

SMTP Password :

Send E-mail alert to :

E-mail Subject :

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 :

Save

Load Settings From Local Hard Drive :

Browse...

Upload Settings

Restore To Factory Default Settings :

Reset to Default

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-111 with unofficial firmware (not recommended).

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

The screenshot shows the firmware upgrade interface with three main sections:

- FIRMWARE UPGRADE:** An orange header section containing introductory text: "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:** A dark grey header section containing the current status: "Current Firmware Version : V1.00" and "Current Firmware Date : 2013/10/09".
- FIRMWARE UPGRADE:** A dark grey header section containing a red warning note: "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." Below this is a blue instruction: "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."

The bottom section contains the following controls:

- An "Upload:" label followed by a text input field and a "Browse..." button.
- "Upgrade" and "Cancel" buttons.
- An "Accept unofficial firmware." checkbox, which is currently unchecked.

Dynamic DNS

The 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: Dynamic Domain Name System 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 (Packet Internet Groper) and click **Ping**.

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

The screenshot displays the System Check utility interface. It is divided into three main sections:

- PING TEST (Orange Header):** Contains the text "Ping Test sends 'ping' packets to test a computer on the Internet." Below this text are two buttons: "Save Settings" and "Don't Save Settings".
- PING TEST (Dark Grey Header):** Contains 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 :" followed by a text input field and a "Ping" button.
- PING RESULT (Dark Grey Header):** This section is currently empty, intended for displaying the results of the ping test.

At the bottom of the interface, there 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 this button to specify the start time, end time, and name of the rule.

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

Delete: Delete the rule.

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

Policy: Select whether the schedule will be active or inactive based on the schedule set.

ID: The ID for the schedule.

Week Day: Select a day of the week that the schedule will be set for.

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..."/>		

SCHEDULE RULE SETTING

Name of Rule 1 :

Policy : except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --	<input type="text"/>	<input type="text"/>
2	-- choose one --	<input type="text"/>	<input type="text"/>
3	-- choose one --	<input type="text"/>	<input type="text"/>
4	-- choose one --	<input type="text"/>	<input type="text"/>
5	-- choose one --	<input type="text"/>	<input type="text"/>
6	-- choose one --	<input type="text"/>	<input type="text"/>
7	-- choose one --	<input type="text"/>	<input type="text"/>
8	-- choose one --	<input type="text"/>	<input type="text"/>

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 WAN IP settings for the router.

Load Sharing: Displays current 3G connection status and IP settings.

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

Wireless LAN: Displays the wireless MAC address and your wireless settings such as SSID, Channel, and Encryption type.

LAN Computers: Displays the list of 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 : Thu Dec 31, 2009 16:05:06 -0800

Firmware Version : V1.00 , 2013/10/09

WAN

Connection Type : DHCP Client

Network Status : Client Disconnected

Remaining Lease Time : N/A

MAC Address : 00:50:18:00:08:4B

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

LOAD SHARING

Load Sharing Connection type : 3G

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

Connection Time : -

LAN

MAC Address : 00:50:18:00:0F:4B

IP Address : 192.168.1.75

Subnet Mask : 255.255.255.0

DHCP Server : Disabled

WIRELESS LAN

MAC Address : 00:50:18:00:02:58

Wireless : Enabled

SSID : dlink_DWR-111

Security : Auto(None)

Channel : 11

802.11 Mode : B/G/N Mixed

Wi-Fi Protected Setup : Enabled

LAN COMPUTERS

IP Address	Name	MAC

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: 1/2 (Log Number : 17)

Previous
Next
First Page
Last Page

Refresh
Download
Clear logs

Link To Log Settings

SYSTEM LOG

Time	Message
Dec 31 15:59:57	kernel: klogd started: BusyBox v1.3.2 (2013-09-26 19:34:45 CST)
Dec 31 16:00:04	commander: Init NAT Server ...
Dec 31 16:00:10	commander: Start UPNP Daemon !!
Dec 31 16:00:12	init: Starting pid 2264, console /dev/ttyS1: '/bin/ash'
Dec 31 16:00:14	commander: Stop UPNP Daemon !!
Dec 31 16:00:16	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:00:16	commander: Start UPNP Daemon !!
Dec 31 16:00:28	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:00:40	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:00:52	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:01:04	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:01:17	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:01:29	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:01:41	commander: Synchronization Time Fail. System would re-sync later
Dec 31 16:01:54	commander: Synchronization Time Fail. System would re-sync later

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
Octects	0	0
Unicast Packets	0	0
Multicast Packets	0	0

Wireless

This table displays a list of wireless clients that are connected to your wireless router. 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 screenshot displays the D-Link DWR-111 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 currently selected. On the left side, there is a vertical menu with options: MENU, SETUP, ADVANCED, TOOLS, STATUS, and LOGOUT. Below the menu, there is a status indicator for 'Internet Offline' and a 'Reboot' button. The main content area is titled 'SUPPORT MENU' and contains four sections of help links:

- SUPPORT MENU**
 - [Setup](#)
 - [Advanced](#)
 - [Tools](#)
 - [Status](#)
- SETUP HELP**
 - [Internet](#)
 - [Wireless Settings](#)
 - [Network Settings](#)
- ADVANCED HELP**
 - [VIRTUAL SERVER](#)
 - [Application Rules](#)
 - [QOS Engine](#)
 - [MAC Address Filter](#)
 - [URL Filter](#)
 - [Outbound Filter](#)
 - [Inbound Filter](#)
 - [SNMP](#)
 - [Routing](#)
 - [Advanced Wireless](#)
 - [Advanced Network](#)
 - [DMZ](#)
- TOOLS HELP**
 - [Admin](#)
 - [Time](#)
 - [SysLog](#)
 - [Email settings](#)
 - [System](#)
 - [Firmware](#)
 - [Dynamic DNS](#)
 - [System Check](#)
 - [Schedules](#)
- STATUS HELP**
 - [Device Info](#)
 - [Log](#)
 - [Statistics](#)
 - [Wireless](#)

At the bottom of the interface, the word 'WIRELESS' is displayed in a dark bar.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DWR-111 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 **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 **Default WEP Key**, 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 **WEP Key**, 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.

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 :

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)

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 **WPA-Personal**.
3. Next to Cipher Type, select TKIP, AES, or Auto.
4. Next to PSK/EAP, select PSK.
5. Next to **Network Key**, enter a key (passphrase). The key is an alphanumeric 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. 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.

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 :

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 :

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 :

 (8~63 ASCII or 64 HEX)

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 **WPA-Enterprise Security**.
3. Next to **Cipher Type**, select **TKIP, AES, or Auto**.
4. Next to PSK/EAP, select **EAP**.
5. Next to **RADIUS Server IP Address** enter the IP Address of your RADIUS server.
6. Next to **RADIUS Server Port**, enter the port you are using with your RADIUS server. 1812 is the default port.
7. Next to **RADIUS Server Shared Secret**, enter the security key.
8. Click **Save Settings** to save your settings.

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 :

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 :

Connect to a Wireless Network Using Windows Vista™

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

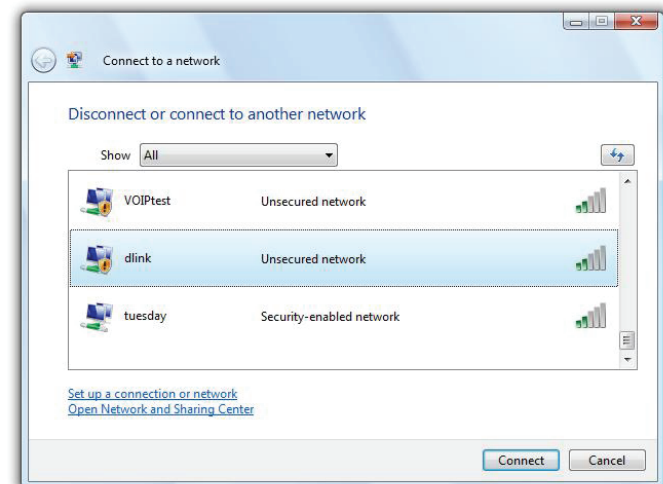
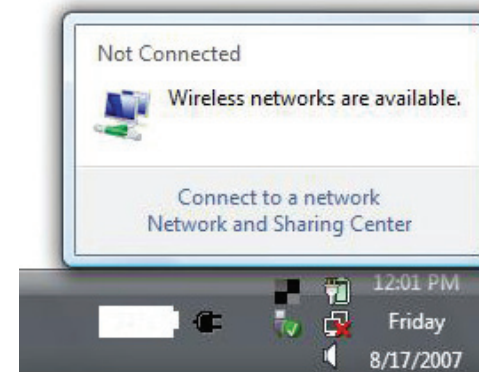
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

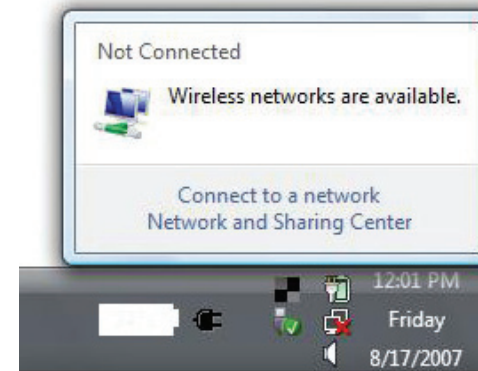
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



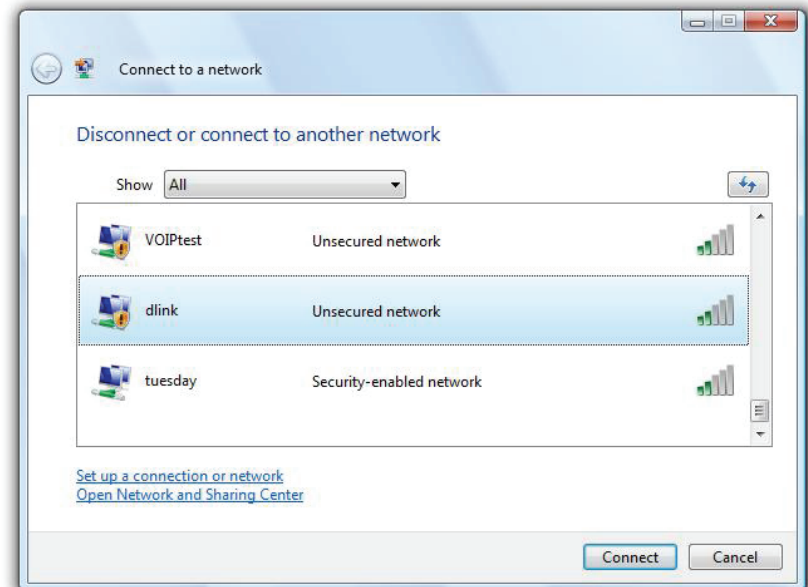
Configure Wireless Security

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

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

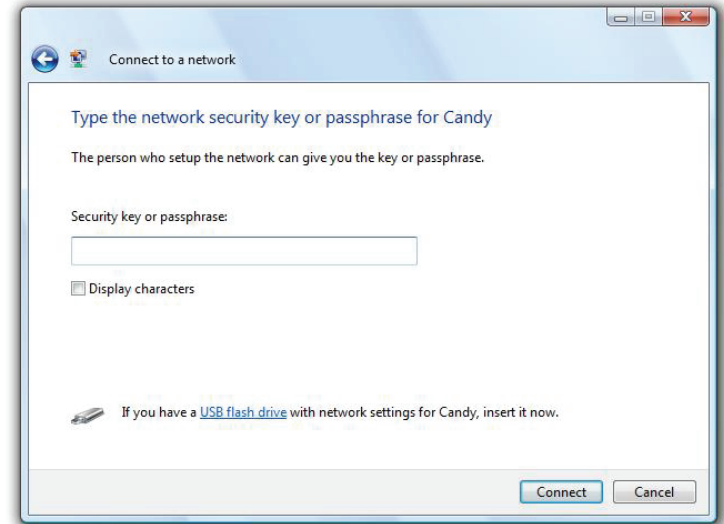


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



Connect to a Wireless Network Using Windows® XP

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

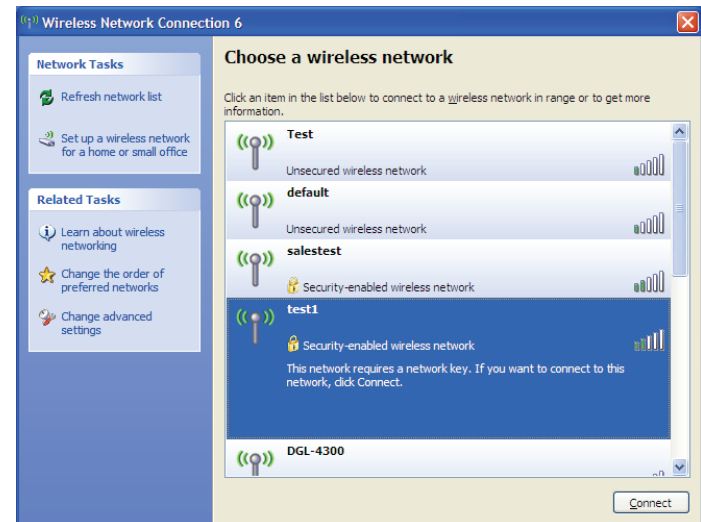
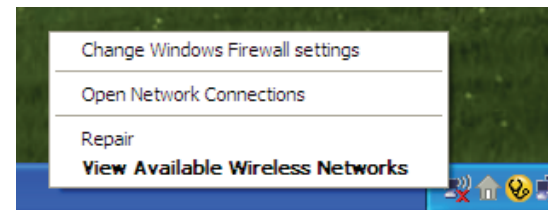
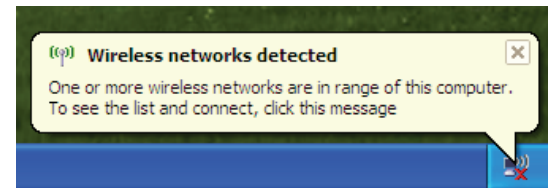
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

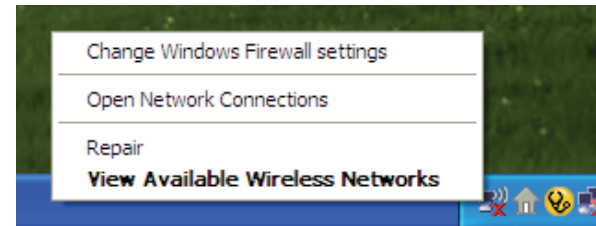
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



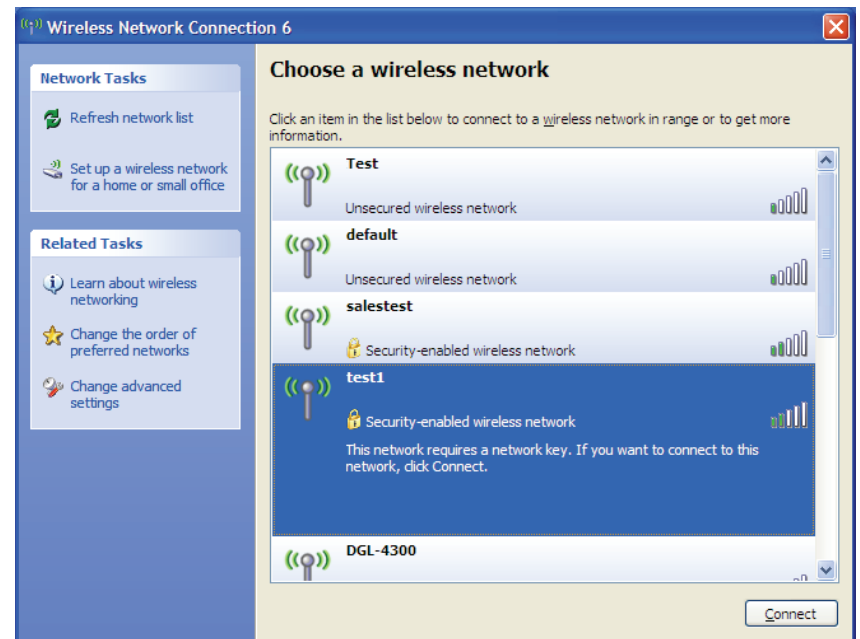
Configure WEP

It is recommended to enable WEP 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 WEP key being used.

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

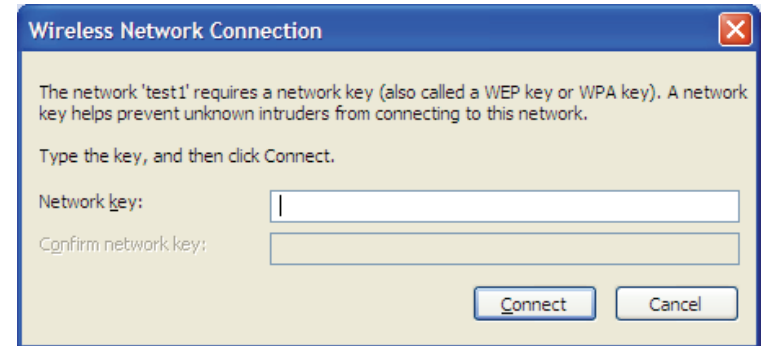


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the same WEP key that is on your router and click **Connect**.

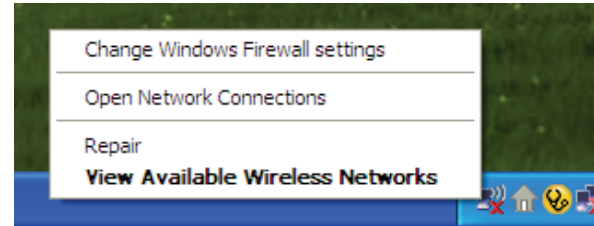
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



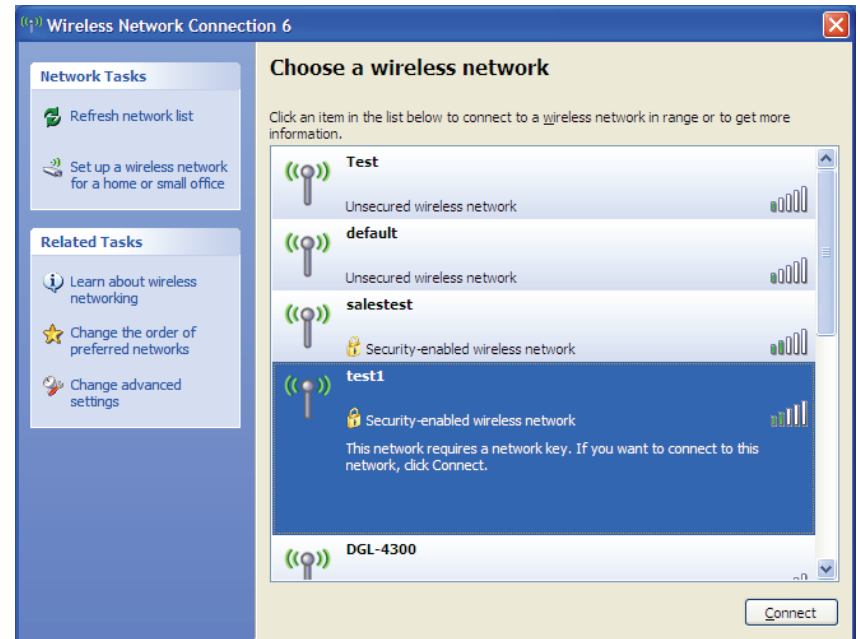
Configure WPA-PSK

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

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

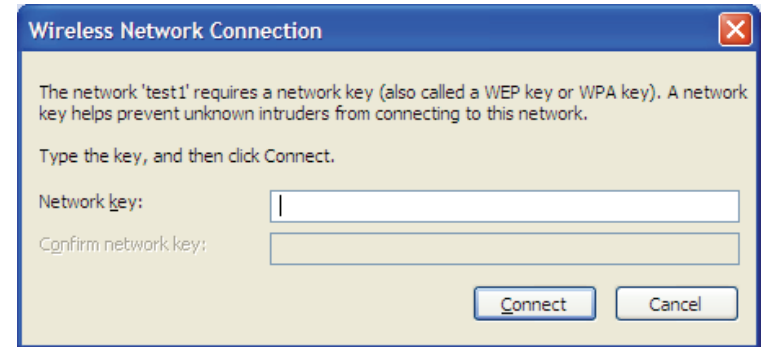


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-111. 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 Basics

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

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

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

- Gives everyone at home broadband access
- Surf the web, check e-mail, instant message, and etc
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

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

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots". Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

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

Tips

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

Centralize your Router or Access Point

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

Eliminate Interference

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

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more 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

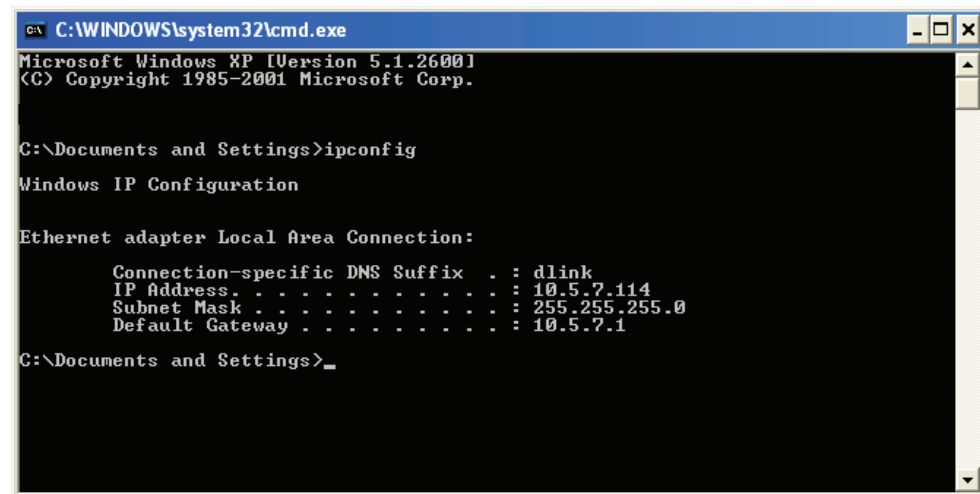
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

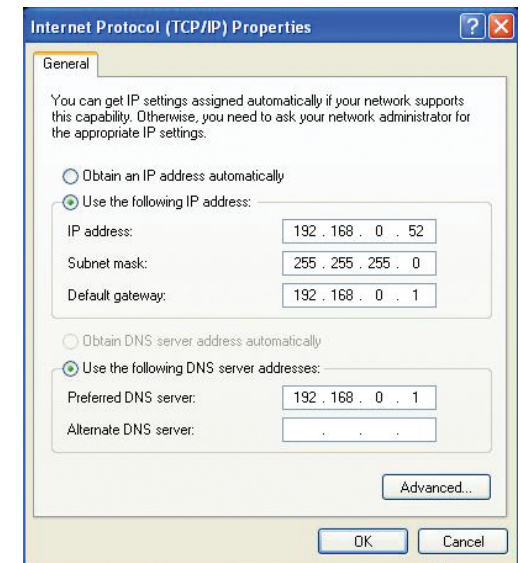
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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 **

- 1/2/5.5/11 Mbps in 802.11b mode
- 6/9/11/12/18/24/36/48/54 Mbps in 802.11g mode
- Up to 150 Mbps in 802.11n mode

Standards

- IEEE 802.11b
- IEEE 802.11g
- 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 passthrough

Antenna

- 1 Internal Wi-Fi antenna

Ports

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

LED Status Indicators

- Power
- Internet
- Wi-Fi
- LAN
- USB
- WAN

Power

- External 12V DC 0.5 A power adapter

Dimensions (L x W x H)

- 110 x 37 x 98 mm (4.33 x 1.45 x 3.85 inches)

Weight

- 240 grams (0.52 lbs)

Operating Temperature

- 0 to 40 °C (32 to 104 °F)

Operating Humidity

- 10% to 95% non-condensing

Certifications

- CE
- Wi-Fi Certified

* Supported frequency band is dependent upon regional hardware version.

** Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.