

USER MANUAL

DWR-512

VERSION 1.0



D-Link[®]

WIRELESS

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.

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 © 2011 by D-Link Corporation, Inc.

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

FCC Regulations

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

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

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

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

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Table of Contents

Preface	i	PPPoE.....	16
Trademarks	i	PPTP	17
FCC Regulations	ii	L2TP.....	18
Product Overview	1	3G	19
Package Contents	1	Wireless Settings	21
System Requirements	1	Wireless Connection Setup Wizard.....	21
Introduction.....	2	Manual Wireless Connection Setup	23
Hardware Overview	3	Wireless Settings	24
Rear Panel.....	3	Wireless Security Mode	25
Front Panel	4	Wi-Fi Protected Setup.....	28
LEDs	5	Network Settings.....	30
Installation	6	Router Settings	30
Connect to Your Network	6	DHCP Server Settings	31
Connect a Telephone	7	Message Service	32
Wireless Installation Considerations.....	8	SMS Inbox.....	32
Configuration	9	Create Message	33
Web-based Configuration Utility	9	Advanced.....	34
Setup	10	Virtual Server	34
Internet.....	10	Application Rules	36
Internet Connection Setup Wizard	10	QoS Engine	37
Manual Internet Connection Setup.....	13	MAC Address Filter.....	38
Internet Connection.....	13	URL Filter.....	39
Static IP	14	Outbound Filter	40
Dynamic IP (DHCP)	15	Inbound Filter.....	41
		SNMP	42
		Routing	43

Advanced Wireless	44	Wireless Basics	75
Advanced Network.....	45	What is Wireless?.....	76
Tools	46	Tips.....	78
Admin.....	46	Wireless Modes	79
Time.....	47	Networking Basics	80
Syslog	48	Check your IP address	80
E-mail Settings.....	49	Statically Assign an IP address	81
System.....	50	Technical Specifications.....	82
Firmware	51		
Dynamic DNS	52		
System Check.....	53		
Schedules	54		
Status	55		
Device Info	55		
Log	56		
Statistics	57		
Wireless	58		
Support	59		
Connecting to a Wireless Network	60		
Using Windows 7	60		
Configuring Wireless Security.....	62		
Using Windows Vista™	65		
Configuring Wireless Security.....	66		
Using Windows® XP.....	68		
Configure WEP	69		
Configure WPA-PSK.....	71		
Troubleshooting	73		

Product Overview

Package Contents

- D-Link DWR-512 HSUPA 3G Router
- Power Adapter
- Manual and Warranty on CD
- 3G Antenna

Note: Using a power supply with a different voltage rating than the one included with the DWR-512 will cause damage and void the warranty for this product.

System Requirements

- A compatible (U)SIM card with service.*
- Computers with Windows®, Macintosh®, or Linux-based operating system with an installed Ethernet adapter
- Internet Explorer 6 or Netscape Navigator™ Version 6.0 and above (for configuration)

*Subject to services and service terms available from your carrier.

Introduction

The D-Link HSUPA 3G Router allows users to access worldwide mobile broadband networks. Once connected, users can transfer data, stream media, send SMS messages, and make mobile phone calls. Simply insert your UMTS/HSUPA SIM card, and share your 3G Internet connection through a secure 802.11n wireless network or using any of the four 10/100 Ethernet ports.

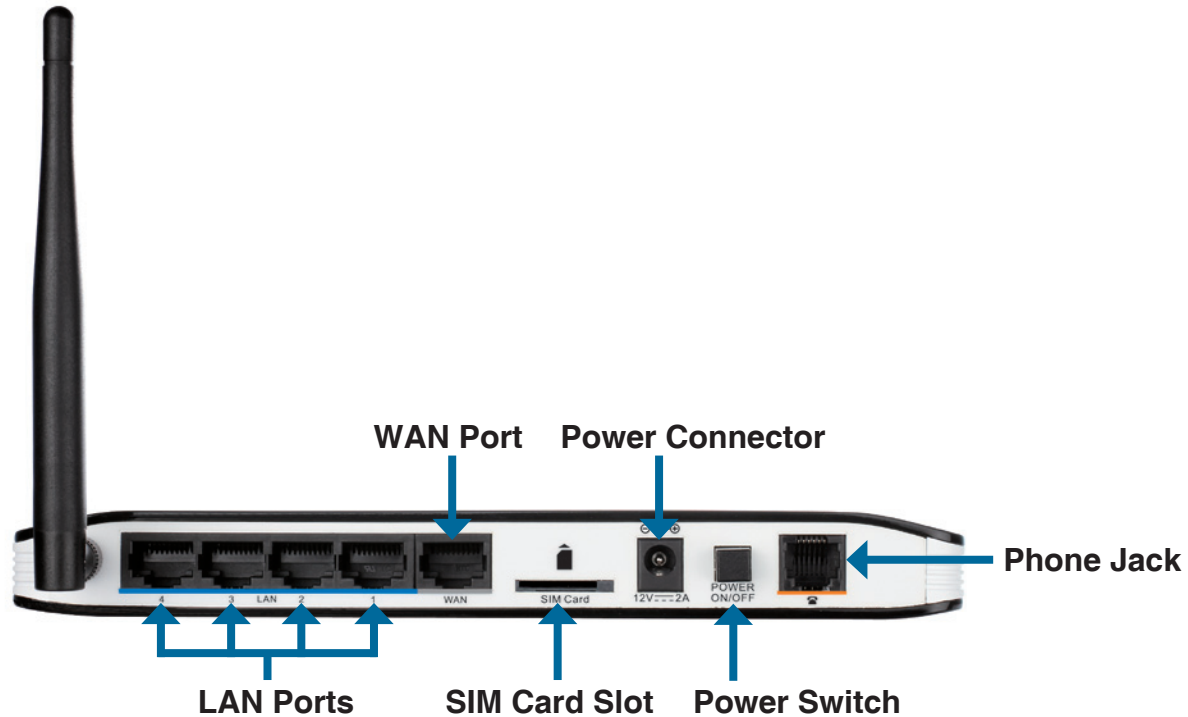
While accessing your 3G Internet connection, you will still have the ability to answer incoming mobile calls and respond to SMS messages. An RJ-11 jack allows you to attach a standard analog phone for high-quality mobile calls over a GSM network. Enjoy the comfort and convenience of your favorite office phone anywhere you go.

Keep your wireless network safe with WPA/WPA2 wireless encryption. The DWR-512 utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks across the Internet, and includes MAC address filtering to control access to your network.

The HSUPA 3G 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-512 can even be installed in buses, trains, or boats, allowing passengers to check e-mail or chat online while commuting.

Hardware Overview

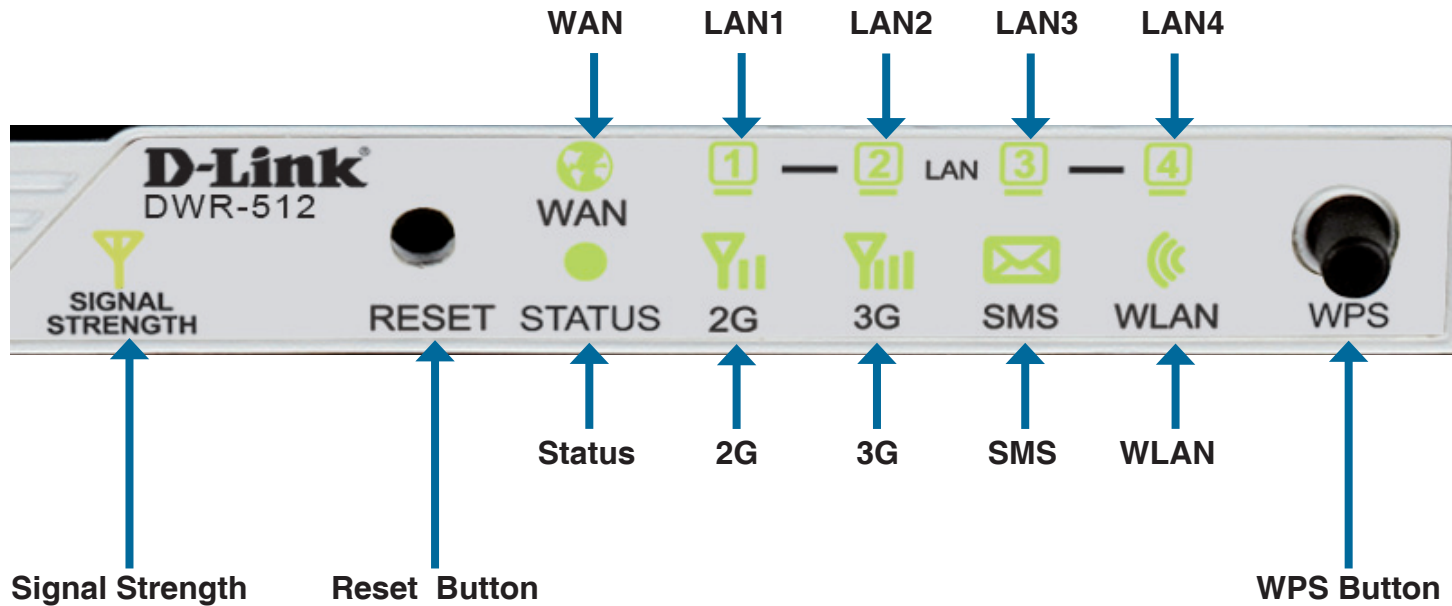
Rear Panel



Port	Function
LAN Ports (RJ-45)	Connects to a network device such as a desktop or notebook computer through an Ethernet cable.
WAN (RJ-45)	Connects to a DSL/Cable modem or router through an Ethernet cable.
SIM	Accepts a standard (U)SIM card for 3G connectivity.
Power	Connects to the included power adapter.
Power Switch	Turns the device on or off.
Phone (RJ-11)	Connects to a telephone through a standard RJ-11 telephone cable.

Hardware Overview

Front Panel



Button Name	Function
Reset	Press this button with an unfolded paperclip to reset the device.
WPS	Press this button to initiate a new WPS connection.

Hardware Overview

LEDs

LED Name	Function
Status	Blinking Green: Device is working
WAN	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
LAN 1-4	Solid Green: Ethernet connection has been established Blinking Green: Data is being transferred
Signal Strength	Blinking Red: No SIM card / signal or unverified PIN code Solid Red: Signal strength is at level one (weak) Solid Amber: Signal strength is at level two or three (medium) Solid Green: Signal strength is at level four or five (strong)
WPS	Slow Blinking Green: WPS is functioning normally Fast Blinking Green: WPS is functioning in PBC mode
2G	Solid Green: EDGE or GPRS connection has been established Blinking Green: Data is being transferred via 2G/2G
3G	Solid Green: UMTS/HSDPA/HSUPA connection is established Blinking: Data is being transferred via 2G
SMS	Solid Green: SMS storage is full Blinking Green: There is an unread SMS message
WLAN	Solid Green: WLAN is active and available Blinking Green: Data is being transferred over the WLAN

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

1. Ensure that your DWR-512 HSUPA 3G Router is disconnected and powered off.
2. Insert a standard (U)SIM card into the SIM card slot on the back of the router as indicated by the SIM card logo next to the slot. The gold contacts should face downwards.

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

3. Insert your Internet/WAN network cable into the WAN port on the back of the router.

Note: The 3G connection can also be used as a backup WAN. Once a backup is configured, the router will automatically use 3G for the Internet connection if the Ethernet WAN is not available.

4. Insert the Ethernet cable into the LAN Port 1 on the back panel of the DWR-512 HSUPA 3G Router and an available Ethernet port on the network adapter in the computer you will use to configure the router.

Note: The DWR-512 HSUPA 3G Router LAN Ports are Auto-MDI/MDIX, so both patch and crossover Ethernet cables can be used.

5. Connect the power adapter to the socket on the back panel of your DWR-512 HSUPA 3G Router. Plug the other end of the power adapter into a wall outlet or power strip and turn the device on.
 - a. The Status LED will light up to indicate that power has been supplied to the router.
 - b. The LEDs on the front panel will flash on and off as the DWR-512 HSUPA 3G Router performs initialization and Internet connection processes.
 - c. After a few moments, if a connection has been established, the following LEDs will turn solid green: Power, Status, WAN, WLAN, and any LAN Port LEDs that are connected computers or other devices.

Connect a Telephone

The RJ-11 jack on the back of the router allows you to connect a standard analog telephone for voice calls.

Simply plug the phone cable into the RJ-11 jack.

You can then use your handset to dial out as you typically would with a standard landline phone.

Your attached phone will also ring for any incoming voice calls.

Note: Calls made will be charged at a rate determined by your mobile service provider.



Wireless Installation Considerations

The DWR-512 can be accessed using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind that the quantity, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through may limit the range of the wireless signal. 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:

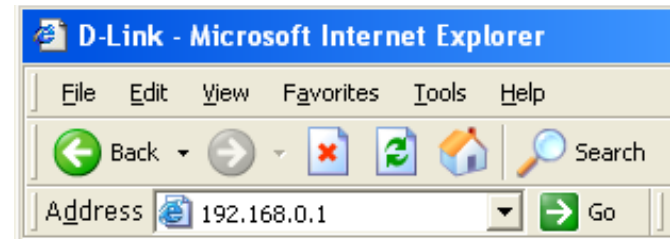
1. Minimize the number of walls and ceilings between the D-Link router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree 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.

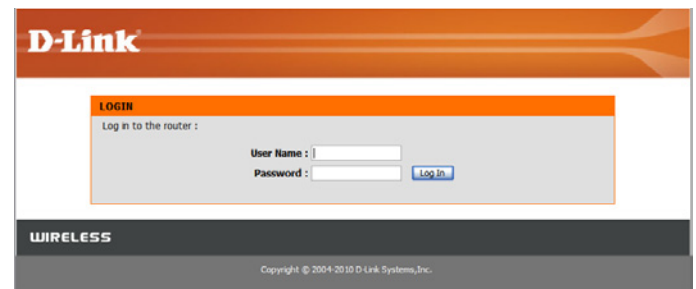
Web-based Configuration Utility

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** by default).



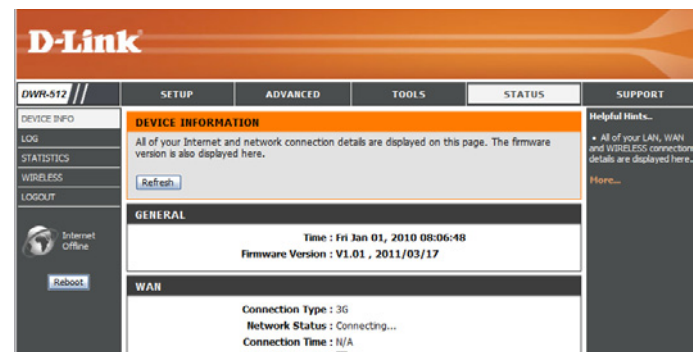
To log in to the configuration utility, enter **admin** as the username, and then enter the password. By default, the password is blank.

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



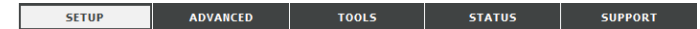
The configuration utility will open to the **STATUS > DEVICE INFO** page. You can view different configuration pages by clicking on the categories at the top of the screen (SETUP/ADVANCED/TOOLS/STATUS/SUPPORT), and then selecting a configuration page from the bar on the left side.

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



Setup

The **SETUP** pages allow you to configure your Internet and wireless settings, as well as manage your SMS inbox. To view the Setup configuration pages, click on **SETUP** at the top of the screen.

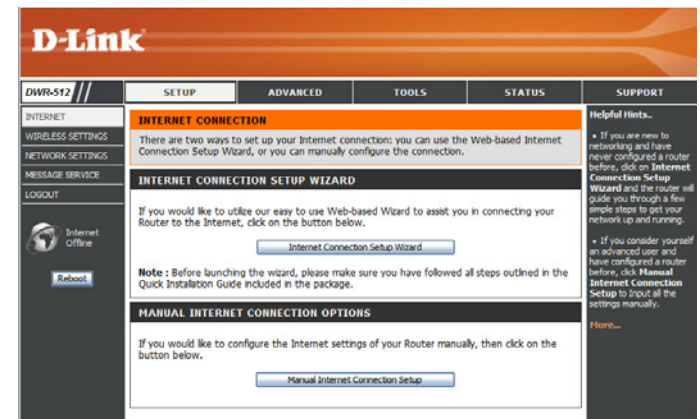


Internet

The Internet page allows you to configure how your router connects to the Internet. There are two ways to set up your Internet connection.

You can click on the **Internet Connection Setup Wizard** button to start a wizard that will guide you through setting up your Internet settings.

If you want to manually configure your settings, click **Manual Internet Connection Setup** and skip to “Manual Internet Connection Setup” on page 13.

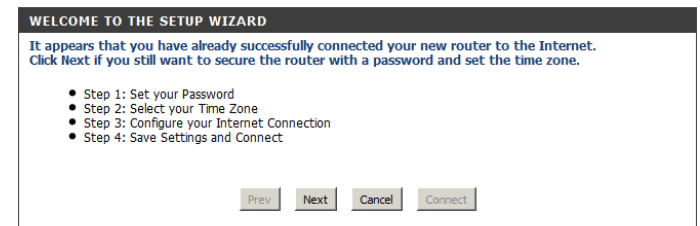


Internet Connection Setup Wizard

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.

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



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

STEP 1: SET YOUR PASSWORD

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

Password :

Verify Password :

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

STEP 2: SELECT YOUR TIME ZONE

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

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

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

Note: The DWR-512 has a WAN Failover feature that allows the router to switch to a 3G connection if the WAN connection is down or unavailable. To configure this feature, please refer to “Internet Connection” on page 13.

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Please select the Internet connection type below:

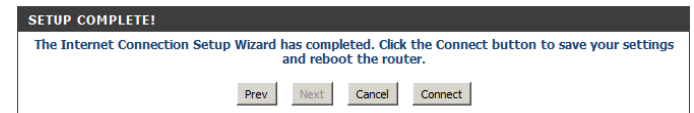
- DHCP Connection (Dynamic IP Address)**
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- Username / Password Connection (PPPoE)**
Choose this option if your Internet connection requires a username and password to 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 “Dynamic IP (DHCP)” on page 15 for information about how to configure this type of connection.
- Username / Password Connection (PPPoE):** Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See “PPPoE” on page 16 for information about how to configure this type of connection.
- Username / Password Connection (PPTP):** Choose this option if your Internet connection requires Point-to-Point Tunneling Protocol (PPTP). See “PPTP” on page 17 for information about how to configure this type of connection.
- Username / Password Connection (L2TP):** Choose this option if your Internet connection requires Layer 2 Tunneling Protocol (L2TP). See “L2TP” on page 18 for information about how to configure this type of connection.
- 3G Connection:** Choose this connection if you have installed a SIM card into the DWR-512. See “3G” on page 19 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 “Static IP” on page 14 for information about how to configure this type of connection.

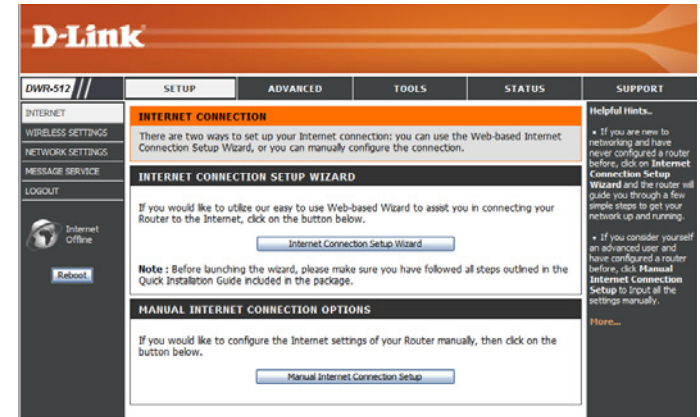
After entering the requested information,click **Next** to continue.

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



Manual Internet Connection Setup

To set up your Internet connection manually, click **Manual Internet Connection Setup**.



Internet Connection

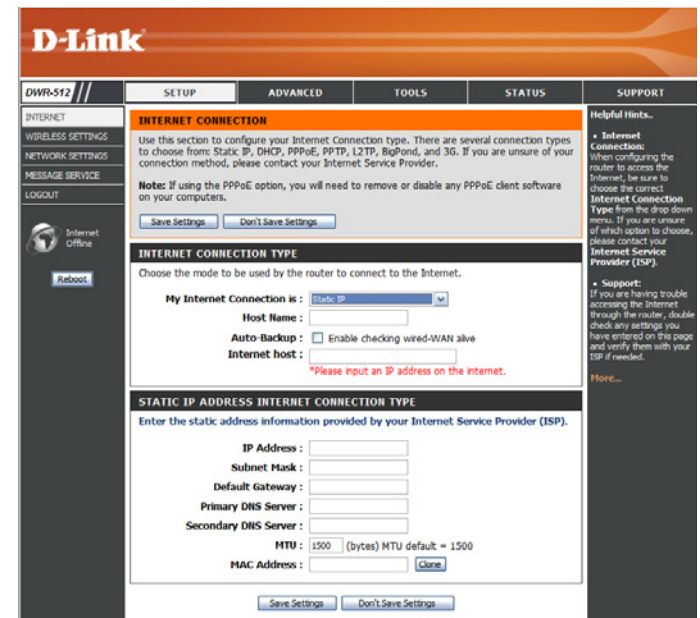
Several different Internet Connection types can be selected depending upon the specifications of your Internet Service Provider (ISP). You can also set up the Auto-Backup feature, which allows you to use a 3G connection for your Internet connection if your main connection fails.

My Internet Connection 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.

Host Name: If the Internet Host you are using for the Auto-Backup feature requires you to enter a Host Name, enter it here. In most cases, you may leave this blank.

Auto-Backup: When this box is checked, the router will switch over to a 3G connection if the Internet Host (specified below) is unreachable.

Internet Host: Enter an IP address for the router to use to check if it is connected to the Internet. If Auto-Backup is enabled and the IP address cannot be reached, the router will switch over to a 3G connection.



Static IP

Choose this Internet connection if your ISP assigns you a static IP address. After modifying any settings, click **Save Settings** to save your changes.

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.

The screenshot shows a configuration window titled "STATIC IP ADDRESS INTERNET CONNECTION TYPE". Below the title is a subtitle: "Enter the static address information provided by your Internet Service Provider (ISP)". The form contains several input fields and buttons:

- IP Address:** Input field with "0.0.0.0" entered.
- Subnet Mask:** Input field with "255.255.255.0" entered.
- Default Gateway:** Input field with "0.0.0.0" entered.
- Primary DNS Server:** Input field with "0.0.0.0" entered.
- Secondary DNS Server:** Input field with "0.0.0.0" entered.
- MTU:** Input field with "1500" entered, followed by "(bytes) MTU default = 1500".
- MAC Address:** Input field with "00-00-00-00-01-00" entered.
- Buttons: "Save", "Restore MAC", "Save Settings", and "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. After modifying any settings, click **Save Settings** to save your changes.

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 the WAN IP address automatically when the lease time has expired.

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 : (optional)

MTU : (bytes) MTU default = 1500

MAC Address :

Auto-reconnect : Enable

PPPoE

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

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

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

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

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

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

Auto-reconnect : Enable

PPTP

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

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

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 Internet, and disconnect if no traffic after time period of Maximum Idle Time.

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

The screenshot shows the PPTP configuration window with the following fields and values:

- 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

Buttons at the bottom: **Save Settings** and **Don't Save Settings**.

L2TP

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

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

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

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

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

L2TP Server IP Address: 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 the device will establish L2TP connection when local users want to surf Internet, and disconnect if no traffic after time period of Maximum Idle Time.

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

The screenshot shows the L2TP configuration window with the following fields and values:

- Address Mode:** Dynamic IP Static IP
- L2TP IP Address:** 0.0.0.0
- L2TP Subnet Mask:** 255.255.255.0
- L2TP Gateway IP Address:** 0.0.0.0
- L2TP Server IP Address:** (empty field)
- Username:** (empty field)
- Password:** (empty field)
- Verify Password:** (empty field)
- Reconnect Mode:** Always-on Connect-on-demand
- Maximum Idle Time:** 300 seconds

Buttons at the bottom: Save Settings, Don't Save Settings

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

Account/Profile Name: Fill in a name to identify the following 3G configuration.

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: Select 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: Select Auto or Manual to decide whether the router should reconnect to your 3G network automatically or manually.

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

Primary DNS Server: (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.

3G INTERNET CONNECTION TYPE

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

Account/Profile Name :

Username : (optional)

Password : (optional)

Dialed Number :

Authentication : (optional)

APN : (optional)

Pin :

Reconnect Mode : Auto Manual

Maximum Idle Time : seconds

Primary DNS Server :

Secondary DNS Server :

Keep Alive : Disable Use LCP Echo Request

Bridge ethernet ports : Enable

Keep Alive: Select Disable or Use LCP Echo Request depending on the settings required by your ISP.

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

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

Account/Profile Name :

Username : (optional)

Password : (optional)

Dialed Number :

Authentication : Auto

APN : (optional)

Pin :

Reconnect Mode : Auto Manual

Maximum Idle Time : seconds

Primary DNS Server :

Secondary DNS Server :

Keep Alive : Disable Use LCP Echo Request

Bridge ethernet ports : Enable

Wireless Settings

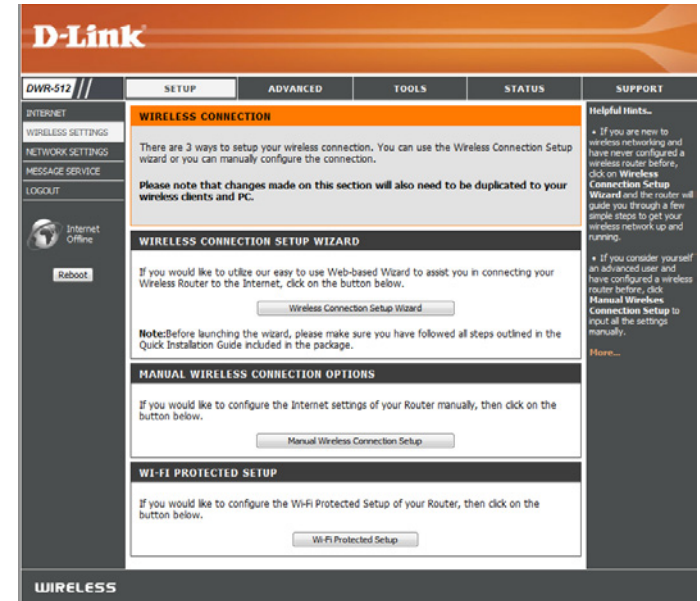
This section will help you to manually configure the wireless settings of your router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

The Wireless Settings page allows you to configure how your router connects to the Internet. There are several ways to set up your wireless connection.

You can click on the **Wireless Connection Setup Wizard** button to start a wizard that will guide you through setting up your wireless settings.

If you want to manually configure your settings, click the **Manual Wireless Connection Setup** button and skip to “Manual Wireless Connection Setup” on page 23.

You can also set up a wireless connection to a device automatically, or configure your router automatically from a by clicking the **Wi-Fi Protected Setup** button. This is described in “Wi-Fi Protected Setup” on page 28.

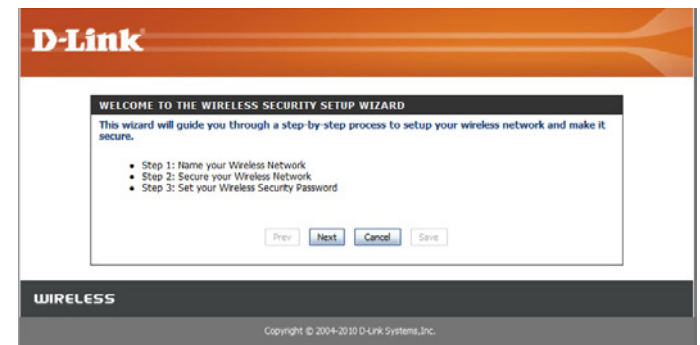


Wireless Connection Setup Wizard

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

Click **Next** to continue.

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



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

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

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

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

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

STEP 1: NAME YOUR WIRELESS NETWORK

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

Wireless Network Name (SSID) : myNetwork

Prev Next Cancel Save

STEP 2: SECURE YOUR WIRELESS NETWORK

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

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

BEST : Select this option if your wireless adapters SUPPORT WPA2

BETTER : Select this option if your wireless adapters SUPPORT WPA

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

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

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

Note: All wireless adapters currently support WPA.

Prev Next Cancel Save

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

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

Wireless Security Password : AES myPassword

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

Prev Next Cancel Save

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

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

Wireless Security Password : HEX 1234567890

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

Prev Next Cancel Save

SETUP COMPLETE!

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

Wireless Network Name (SSID) : myNetwork

Prev Next Cancel Save

Manual Wireless Connection Setup

To set up your wireless connection manually, click **Manual Wireless Connection Setup**.

The screenshot displays the D-Link web interface for the DWR-512 router. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar shows menu items: INTERNET, WIRELESS SETTINGS, NETWORK SETTINGS, MESSAGE SERVICE, and LOGOUT. The main content area is titled "WIRELESS CONNECTION" and contains the following sections:

- WIRELESS CONNECTION**: A header section with a note: "There are 3 ways to setup your wireless connection. You can use the Wireless Connection Setup wizard or you can manually configure the connection." Below this is a warning: "Please note that changes made on this section will also need to be duplicated to your wireless clients and PC."
- WIRELESS CONNECTION SETUP WIZARD**: A section with the text: "If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your Wireless Router to the Internet, click on the button below." A button labeled "Wireless Connection Setup Wizard" is provided.
- MANUAL WIRELESS CONNECTION OPTIONS**: A section with the text: "If you would like to configure the Internet settings of your Router manually, then click on the button below." A button labeled "Manual Wireless Connection Setup" is provided.
- WI-FI PROTECTED SETUP**: A section with the text: "If you would like to configure the Wi-Fi Protected Setup of your Router, then click on the button below." A button labeled "Wi-Fi Protected Setup" is provided.

On the right side, there is a "Helpful Hints..." section with two bullet points: "• If you are new to wireless networking and have never configured a wireless router before, click on Wireless Connection Setup Wizard and the router will guide you through a few simple steps to get your wireless network up and running." and "• If you consider yourself an advanced user and have configured a wireless router before, click Manual Wireless Connection Setup to input all the settings manually." Below this is a "More..." link.

The bottom of the page features a "WIRELESS" tab.

Wireless Settings

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

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

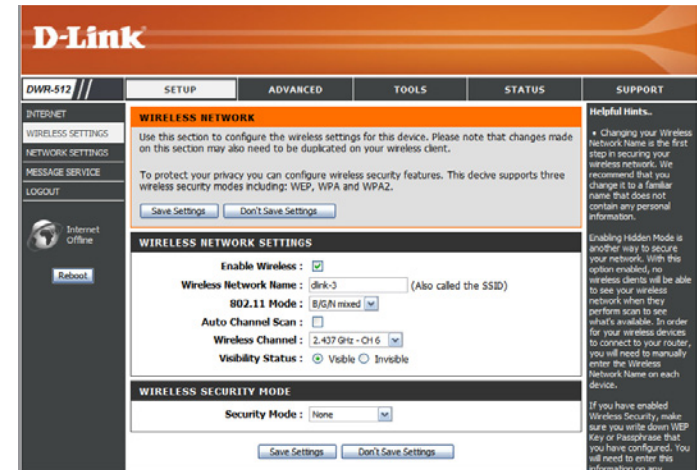
Wireless Network Name: Also known as the SSID (Service Set Identifier), this is the name of your Wireless Local Area Network (WLAN). Enter a name using up to 32 alphanumeric characters. The SSID is case-sensitive.

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

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

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

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



Wireless Security Mode

You can choose from several different wireless security modes. After selecting a mode, the settings for that mode will appear. After modifying any settings, click **Save Settings** to save your changes.

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

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

The screenshot shows the D-Link web interface for the DWR-512 router. The main navigation bar includes 'D-Link', 'DWR-512', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar has links for 'INTERNET', 'WIRELESS SETTINGS', 'NETWORK SETTINGS', 'MESSAGE SERVICE', and 'LOGOUT'. The main content area is titled 'WIRELESS NETWORK' and contains the following sections:

- WIRELESS NETWORK:** A header section with a sub-header 'WIRELESS NETWORK' and a description: '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.' It includes 'Save Settings' and 'Don't Save Settings' buttons.
- WIRELESS NETWORK SETTINGS:** A section with the following settings:
 - Enable Wireless:
 - Wireless Network Name: dlink-3 (Also called the SSID)
 - 802.11 Mode: 802.11 mixed
 - Auto Channel Scan:
 - Wireless Channel: 2.437 GHz - Ch 6
 - Visibility Status: Visible Invisible
- WIRELESS SECURITY MODE:** A section with 'Security Mode' set to 'None' and 'Save Settings' and 'Don't Save Settings' buttons.

On the right side, there is a 'Helpful Hints...' section with the following text: 'Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information. Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device. If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any'

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

- Authentication:** Select whether to use Open or Shared authentication.
- WEP Encryption:** Select whether to use **64-bit** or **128-bit** encryption.
- Default WEP Key:** Select which WEP key (1-4) to use as the default key. This will also change the WEP Key text box to that WEP key for your to configure(1-4).
- WEP Key:** Set the WEP key/password for your wireless network. Based on whether you are using 64 or 128-bit encryption, and whether you are using a HEX or ASCII key, you will need to enter different numbers of characters for your key, as indicated below the WEP Key text box. ASCII keys may use letters and numbers only, and HEX keys may use numbers 0-9 and letters A-F only.

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

Authentication : Open
WEP Encryption : 64bit
Default WEP Key : WEP Key 1
WEP Key : HEX 1234567890
(5 ASCII or 10 HEX)

Save Settings
Don't Save Settings

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

- WPA Mode:** Select whether to use **WPA2 only** or **WPA only**. **WPA2 only** is the most secure, provided that all of your clients can support it.
- Cipher Type:** Select whether to use the **TKIP** or **AES** cipher. The **AES** cipher is the most secure, provided that all of your clients can support it.
- Network Key:** Enter the key/password you want to use for your wireless network. The key must be 8 to 63 characters long, and may only contain letters and numbers.

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(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 : WPA2 only
Cipher Type : TKIP

PRE-SHARED KEY

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

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

Save Settings
Don't Save Settings

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

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

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

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

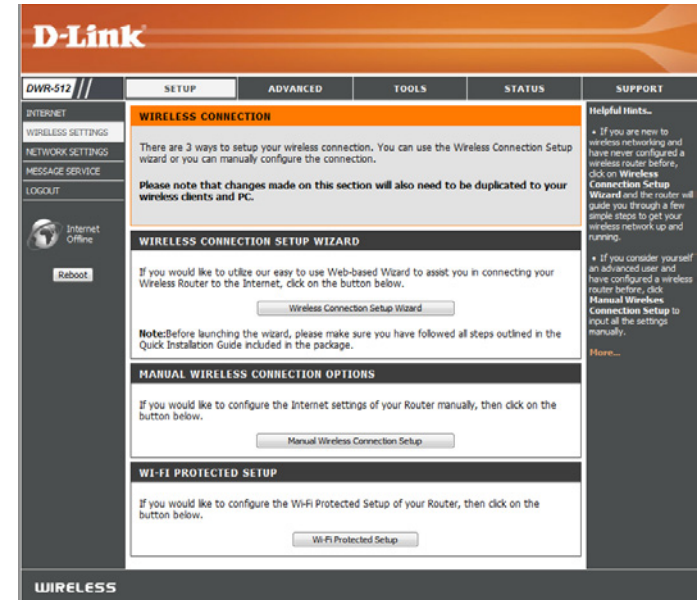
RADIUS Server Port: Enter the port used for your RADIUS server.

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

WIRELESS SECURITY MODE	
Security Mode :	<input type="text" value="WPA-Enterprise"/>
WPA	
Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only . This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.	
To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).	
WPA Mode :	<input type="text" value="WPA2 only"/>
Cipher Type :	<input type="text" value="TKIP"/>
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 :	<input type="text" value="0.0.0.0"/>
RADIUS server Port :	<input type="text" value="1812"/>
RADIUS server Shared Secret :	<input type="text"/>

Wi-Fi Protected Setup

To open the Wi-Fi Protected Setup page, click **Wi-Fi Protected Setup**.



The Wi-Fi Protected Setup page allows you to create a wireless connection between your router and a device automatically by simply pushing a button or entering a PIN code.

You can also use Windows 7 to do initial configuration of your router by using the **Connect to a network** wizard in Windows, and entering the WPS PIN/AP PIN of the router when prompted. After modifying any settings, click **Save Settings** to save your changes.



WPS: Select whether you would like to enable or disable WPS features.

AP PIN (also known as WPS PIN): If you use Windows 7's **Connect to a network** wizard to do initial configuration of the router, you will need to enter the WPS PIN/AP PIN into the wizard when prompted. The factory default WPS PIN/AP PIN is printed on a label located on the bottom of the router. You can click the **Generate New PIN** button to change it to a randomly generated PIN.

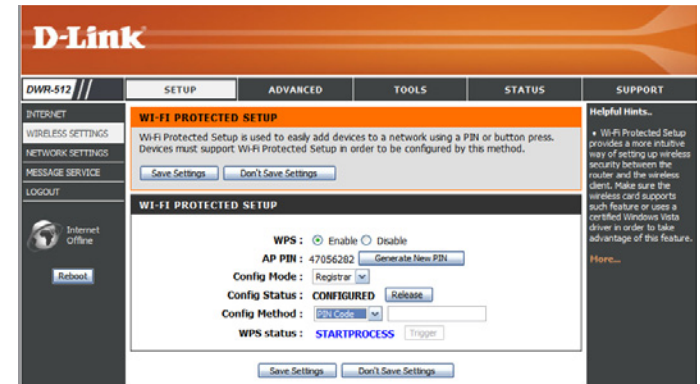
Config Mode: Select whether the WPS config mode should be set to **Registrar** or **Enrollee**. In most cases, this should be set to **Registrar** so that you can use WPS to connect new wireless clients.

Config Status: If this is set to **CONFIGURED**, the router will be marked as “already configured” to computers that try to use WPS configuration, such as Windows 7's **Connect to a network** wizard. You can click the **Release** button to change the status to **UNCONFIGURED** to allow for WPS configuration of the router.

If this is set to **UNCONFIGURED**, you can click the **Set** button to change the status to **CONFIGURED** to block WPS configuration of the router.

Config Method: This lets you choose whether to use the **Push Button** connection method (PBC) or **PIN** method to connect to a wireless client when the **Trigger** button is clicked. If you choose the **PIN** method, you will need to enter a 8-digit PIN number that the wireless client need to use to connect to your router.

WPS Status: This will show the current WPS connection process status. Click the **Trigger** button to initiate a WPS connection.



Network Settings

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

Router Settings

Router IP Address: Enter the IP address you want to use for 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.

The screenshot displays the D-Link DWR-512 web-based management interface. The page is titled "D-Link" and "DWR-512". The navigation menu includes "SETUP", "ADVANCED", "TOOLS", "STATUS", and "SUPPORT". The "NETWORK SETTING" section is active, showing instructions for configuring the internal network settings and the built-in DHCP server. The "ROUTER SETTINGS" section contains fields for "Router IP Address" (192.168.0.1), "Default Subnet Mask" (255.255.255.0), and "Local Domain Name". The "DHCP SERVER SETTINGS" section includes a checkbox for "Enable DHCP Server" (checked), a "DHCP IP Address Range" (50 to 199), a "DHCP Lease Time" (86400 seconds), and fields for "Primary DNS IP Address", "Secondary DNS IP Address", "Primary WINS IP Address", and "Secondary WINS IP Address". "Save Settings" and "Don't Save Settings" buttons are visible at the bottom of each section.

DHCP Server Settings

The DWR-512 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. After modifying any settings, click **Save Settings** to save your changes.

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

DHCP IP Address Range: Enter the range of IPs for the DHCP server to use to assign IP addresses to devices on your network.

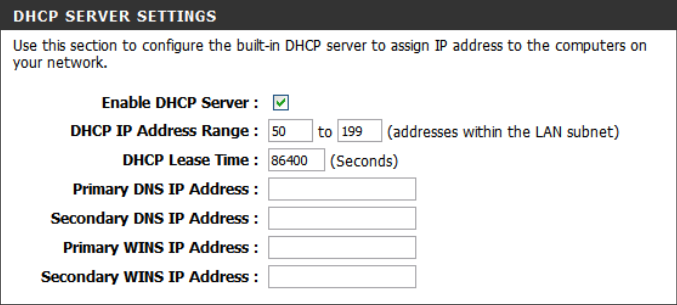
DHCP Lease Time: Enter lease time for IP address assignments.

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

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

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

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



The screenshot shows the 'DHCP SERVER SETTINGS' configuration page. It includes a title bar, a descriptive paragraph, and several configuration fields with their current values. At the bottom, there are two buttons: 'Save Settings' and 'Don't Save Settings'.

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 :	<input checked="" type="checkbox"/>
DHCP IP Address Range :	50 to 199 (addresses within the LAN subnet)
DHCP Lease Time :	86400 (Seconds)
Primary DNS IP Address :	<input type="text"/>
Secondary DNS IP Address :	<input type="text"/>
Primary WINS IP Address :	<input type="text"/>
Secondary WINS IP Address :	<input type="text"/>

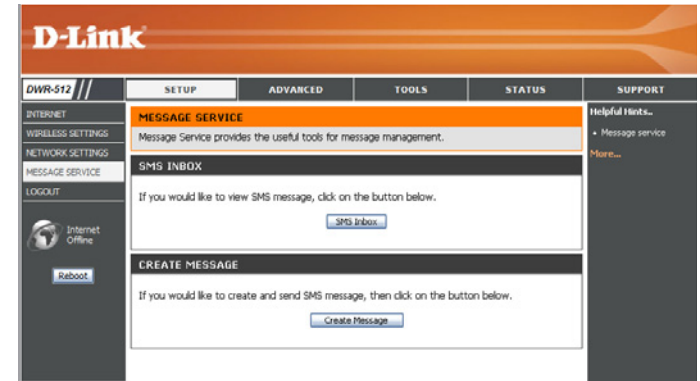
Save Settings Don't Save Settings

Message Service

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

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

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



SMS Inbox

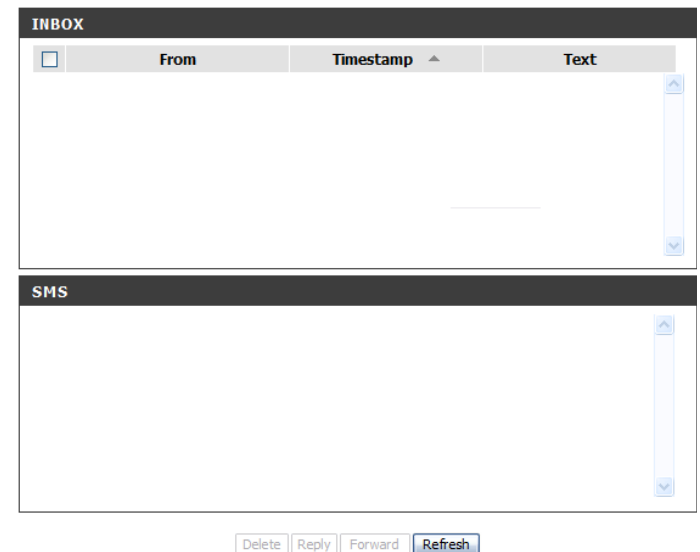
This page shows all messages that are stored on the SIM card. Select a message to display its contents in the SMS window. After you read it, you can delete it, or reply to the sender. Click the **Refresh** button to update the list.

Delete: Deletes the selected SMS message.

Reply: Opens a Create Message window to reply to the selected SMS message.

Forward: Opens a Create Message windows to forward the selected SMS message to another recipient.

Refresh: Click this button to check for new messages.



Create Message

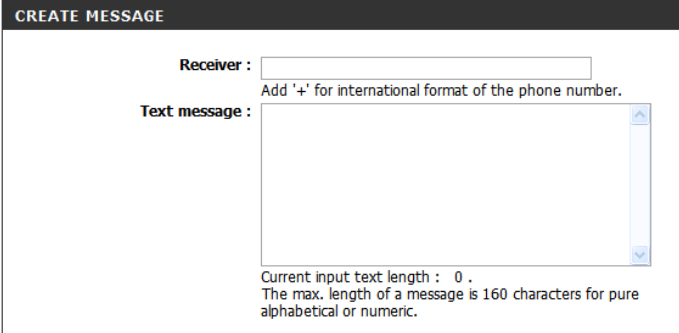
This page allows you to send an SMS to your contacts. Just fill in the phone number of the recipient, and type the content of message. Then push the “Send Message” button to send out this message. If you would like to add more than one recipient, you must put a semicolon (;) between each of the phone numbers.

Receiver: Type the phone number of the recipient.

Text Message: Type the message that you would like to send.

Sent Message: Click this button to send the message.

Cancel: Click this button to clear the message.



CREATE MESSAGE

Receiver :
Add '+' for international format of the phone number.

Text message :

Current input text length : 0 .
The max. length of a message is 160 characters for pure alphabetical or numeric.

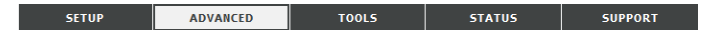
Advanced

The **ADVANCED** pages allow you to configure the more advanced settings of the router, such as Virtual Server (Port Forwarding), MAC and URL filtering, and advanced wireless and network settings. To view the Advanced configuration pages, click on **ADVANCED** at the top of the screen.

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. You can also allow the settings to run on a specified schedule. The Virtual Server function is also known as Port Forwarding. After modifying any settings, click **Save Settings** to save your changes.

- Well-known Services:** This contains a list of pre-defined services. You can select a service, select a rule ID, then click the **Copy to** button to copy the default settings for that service to the specified rule ID.
- ID:** Specifies which rule to copy the selected **Well known service** settings to when you click the **Copy to** button.
- Use schedule rule:** Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 54.



D-Link

DWR-512

SETUP ADVANCED TOOLS STATUS SUPPORT

VIRTUAL SERVER

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

Save Settings Don't Save Settings

Well known services -- select one -- Copy to ID -- Use schedule rule -- ALWAYS ON --

VIRTUAL SERVERS LIST

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1			<input type="checkbox"/>	Add New Rule...
2			<input type="checkbox"/>	Add New Rule...
3			<input type="checkbox"/>	Add New Rule...
4			<input type="checkbox"/>	Add New Rule...
5			<input type="checkbox"/>	Add New Rule...
6			<input type="checkbox"/>	Add New Rule...
7			<input type="checkbox"/>	Add New Rule...
8			<input type="checkbox"/>	Add New Rule...
9			<input type="checkbox"/>	Add New Rule...
10			<input type="checkbox"/>	Add New Rule...
11			<input type="checkbox"/>	Add New Rule...
12			<input type="checkbox"/>	Add New Rule...
13			<input type="checkbox"/>	Add New Rule...
14			<input type="checkbox"/>	Add New Rule...
15			<input type="checkbox"/>	Add New Rule...
16			<input type="checkbox"/>	Add New Rule...
17			<input type="checkbox"/>	Add New Rule...
18			<input type="checkbox"/>	Add New Rule...
19			<input type="checkbox"/>	Add New Rule...
20			<input type="checkbox"/>	Add New Rule...

Helpful Hints...

- You can select your computer from the list of DHCP clients in the Computer Name drop down menu, or enter the IP address manually of the computer you would like to open the specified port to.
- This feature allows you to open a range of ports to a computer on your network. To do so, enter the first port in the range you would like to open on the router in the first box under **Public Port** and last port of the range in the second one. After that you enter the first port in the range that the internal server uses in the first box under **Private Port** and the last port of the range in the second.
- To open a single port, using this feature, simply enter the same number in both boxes.

More...

Internet Offline

Reboot

VIRTUAL SERVERS LIST

ID: This identifies the rule.

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: Tick the checkbox to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. To create schedules, please refer to “Schedules” on page 54.

The screenshot shows the D-Link DWR-512 web interface. The top navigation bar includes 'D-Link', 'DWR-512', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'VIRTUAL SERVER' section is active. Below the navigation, there are sections for 'VIRTUAL SERVER' configuration, including 'Well known services' and 'Use schedule rule'. The main area is titled 'VIRTUAL SERVERS LIST' and contains a table with columns for ID, Service Ports, Server IP : Port, Enable, and Schedule Rule #. The table lists 20 rows, each with an 'Add New Rule...' button. On the right side, there is a 'Helpful Hints...' section with instructions on how to use the Virtual Server feature.

ID	Service Ports	Server IP : Port	Enable	Schedule Rule #
1			<input type="checkbox"/>	Add New Rule...
2			<input type="checkbox"/>	Add New Rule...
3			<input type="checkbox"/>	Add New Rule...
4			<input type="checkbox"/>	Add New Rule...
5			<input type="checkbox"/>	Add New Rule...
6			<input type="checkbox"/>	Add New Rule...
7			<input type="checkbox"/>	Add New Rule...
8			<input type="checkbox"/>	Add New Rule...
9			<input type="checkbox"/>	Add New Rule...
10			<input type="checkbox"/>	Add New Rule...
11			<input type="checkbox"/>	Add New Rule...
12			<input type="checkbox"/>	Add New Rule...
13			<input type="checkbox"/>	Add New Rule...
14			<input type="checkbox"/>	Add New Rule...
15			<input type="checkbox"/>	Add New Rule...
16			<input type="checkbox"/>	Add New Rule...
17			<input type="checkbox"/>	Add New Rule...
18			<input type="checkbox"/>	Add New Rule...
19			<input type="checkbox"/>	Add New Rule...
20			<input type="checkbox"/>	Add New Rule...

Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, and Internet telephony among others. These applications may have difficulty working through NAT (Network Address Translation). **Application Rules** allow some of these applications work with the DWR-512 by opening ports after detecting traffic being sent through a trigger port. After modifying any settings, click **Save Settings** to save your changes.

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

APPLICATION RULES

- ID:** This identifies the rule.
- Trigger:** Enter the port to listen to in order to trigger the rule.
- Incoming Ports:** Specify the incoming port(s) to open when traffic comes over the **Trigger** port.
- Enable:** Tick the checkbox to enable the specified rule.



QoS Engine

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

QOS ENGINE SETUP

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

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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 54.

QOS RULES

ID: This identifies the rule.

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

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

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

Enable: Tick the checkbox to enable the specified rule.

Use Rule #: Specify the schedule rule number. To create schedules, please refer to “Schedules” on page 54.

The screenshot shows the D-Link DWR-512 configuration interface. The 'QOS ENGINE' section is active, displaying the following settings:

- Enable QoS Packet Filter:**
- Upstream bandwidth:** [] kbps
- Use schedule rule:** [ALWAYS ON] [Copy to] [ID] []

The 'QOS RULES' table is as follows:

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

Buttons: Save Settings, Don't Save Settings

MAC Address Filter

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

MAC FILTERING SETTINGS

- MAC Address Control:** Tick this box to enable MAC Filtering.
- Connection Control:** 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.

MAC FILTERING RULES

- ID:** This identifies the rule.
- MAC Address:** Specify the MAC Address of the computer to be filtered.
- IP Address:** Specify the last section of the IP address.
- Wake On LAN:** Click **Trigger** to configure Wake On LAN.
- C:** If this box is ticked, the rule will follow the connection control setting specified in MAC filtering settings specified above.
- A:** If this box is ticked, the rule will follow the association control setting specified in MAC filtering settings specified above.

D-Link

DWR-512 // SETUP ADVANCED TOOLS STATUS SUPPORT

MAC ADDRESS FILTER

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

Save Settings Don't Save Settings

MAC FILTERING SETTINGS

MAC Address Control: Enable

Connection control: Wireless and wired clients with **C** checked can connect to this device; and allow deny unspecified MAC addresses to connect.

Association control: Wireless clients with **A** checked can associate to the wireless LAN; and allow deny unspecified MAC addresses to associate.

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

MAC FILTERING RULES

ID	MAC Address	IP Address	C	A
1			<input type="checkbox"/>	<input type="checkbox"/>
2			<input type="checkbox"/>	<input type="checkbox"/>
3			<input type="checkbox"/>	<input type="checkbox"/>
4			<input type="checkbox"/>	<input type="checkbox"/>
5			<input type="checkbox"/>	<input type="checkbox"/>

Previous page Next page

Reboot

Helpful Hints...

- **MAC Address Control:** allows you to assign different access rights for different users and to assign a specific IP address to a certain MAC address.
- **Connection control:** Connection control allows you to allow or deny the wired and wireless clients to connect to this device and the Internet. Check Connection control to enable the controlling.
- If a client is denied to connect to this device, it means that the client can't access the Internet and some network resources. Choose allow or deny to allow or deny clients whose MAC addresses are not listed in the Control table.
- **Association control:** The Association process is the exchange of information between wireless clients and the device to establish a link between them. A wireless client is capable of transmitting and receiving data to the device only after

URL Filter

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

URL Filtering: Select this box to enable URL Filtering.

URL FILTERING RULES

ID: This identifies the rule.

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

Enable: Tick the checkbox to enable the specified rule.

D-Link

DWR-512 // SETUP ADVANCED TOOLS STATUS SUPPORT

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

ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

Save Settings Don't Save Settings

Helpful Hints...
 • Create a list of Web Sites to which you would like to deny or allow through the network.
 More...

Internet Offline
 Reboot

Outbound Filter

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

OUTBOUND FILTER SETTING

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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 54.

OUTBOUND FILTER RULES LIST

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

ID: This identifies the rule.

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

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

Enable: Tick the checkbox to enable the specified rule.

Schedule Rule #: Specify the schedule rule number.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

The screenshot shows the D-Link DWR-512 web interface. The main content area is titled "OUTBOUND FILTER" and contains the following sections:

- OUTBOUND FILTER:** A section with a "Save Settings" button and a "Don't Save Settings" button.
- OUTBOUND FILTER SETTING:** A section with an "Outbound Filter" checkbox (currently unchecked) and a "Use schedule rule" dropdown menu set to "ALWAYS ON". There is a "Copy to" button and an "ID" field.
- OUTBOUND FILTER RULES LIST:** A table with 8 rows. Each row has columns for "ID", "Source IP:Ports", "Destination IP:Ports", "Enable", and "Schedule Rule#". The "Enable" column has checkboxes, and the "Schedule Rule#" column has "Add New Rule..." buttons. Below the table are "Previous page" and "Next page" buttons.

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

Inbound Filter

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

INBOUND FILTER SETTING

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

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to “Schedules” on page 54.

INBOUND FILTER RULES LIST

ID: This identifies the rule.

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

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

Enable: Tick the checkbox to enable the specified rule.

Schedule Rule #: Specify the schedule rule number.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

D-Link

DWR-512 // SETUP ADVANCED TOOLS STATUS SUPPORT

INBOUND FILTER

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

Save Settings Don't Save Settings

INBOUND FILTER SETTING

Inbound filter : Enable

Use schedule rule : ALWAYS ON -- Copy to ID --

INBOUND FILTER RULES LIST

Allow all to pass except those match the following rules.
 Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1			<input type="checkbox"/>	Add New Rule...
2			<input type="checkbox"/>	Add New Rule...
3			<input type="checkbox"/>	Add New Rule...
4			<input type="checkbox"/>	Add New Rule...
5			<input type="checkbox"/>	Add New Rule...
6			<input type="checkbox"/>	Add New Rule...
7			<input type="checkbox"/>	Add New Rule...
8			<input type="checkbox"/>	Add New Rule...

Previous page Next page

Save Settings Don't Save Settings

Helpful Hints...

* Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies.

More...

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-512. The DWR-512 supports SNMP v1 and v2c. After modifying any settings, click **Save Settings** to save your changes.

SNMP

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

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

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

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

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

SNMP Version: Select the SNMP version of your system.

WAN Access IP Address If you want to limit remote access SNMP access, enter the IP address of the remote computer you will use to access this device. All other IP addresses will be denied remote SNMP access.

The screenshot shows the D-Link DWR-512 web interface. The top navigation bar includes 'D-Link', 'DWR-512', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration categories like 'VIRTUAL SERVER', 'APPLICATION RULES', 'QOS ENGINE', etc. The main content area is titled 'SNMP' and contains the following configuration options:

- Use Simple Network Management Protocol(SNMP) for management purposes.
- Save Settings / Don't Save Settings
- 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. After modifying any settings, click **Save Settings** to save your changes.

RIP SETTING

- RIP:** Select this box to enable routing, then select which routing protocol to use:
- **RIPv1:** Protocol in which the IP address is routed through the internet.
 - **RIPv2:** Enhanced version of RIPv1 with added features such as Authentication, Routing Domain, Next Hop Forwarding, and Subnet-mask Exchange.

ROUTING RULES

ID: This identifies the rule.

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

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

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

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

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

Enable: Select this box to enable the rule.

The screenshot shows the D-Link DWR-512 web interface. The main content area is titled "ROUTING" and contains the following sections:

- ROUTING:** This Routing page allows you to specify custom routes that determine how data is moved around your network. Buttons: Save Settings, Don't Save Settings.
- RIP SETTING:** RIP: Enable RIPv1 RIPv2
- ROUTING RULES:** A table with 8 rows and 6 columns: ID, Destination, Subnet Mask, Gateway, Hop, and Enable.

Buttons at the bottom: Save Settings, Don't Save Settings.

Helpful Hints... (Right sidebar):

- Each route has a check box next to it, check this box if you want the route to be enabled.
- The destination IP address is the address of the host or network you wish to reach.
- The netmask field identifies the portion of the destination IP in use.
- The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

Advanced Wireless

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

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

Transmit Power: Set the transmit power of the antennas.

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

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

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

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

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

