



User Manual

DC-HSPA+ Mobile Router

DWR-830

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 15, 2013	• Initial release

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2013 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.

Table of Contents

Preface.....	i	Home.....	15
Manual Revisions.....	i	Wizard.....	16
Trademarks	i	Internet.....	18
Product Overview.....	1	Connection	18
Package Contents.....	1	Configuration.....	20
System Requirements	1	IPv4 - PDP Context.....	20
Introduction	2	IPv4 - Static Setting	21
Hardware Overview	3	IPv4 - 4to6.....	22
Left Side.....	3	IPv6 - PDP Context.....	23
OLED Display	4	IPv6 - Static Setting	24
Installation	6	IPv6 - DHCPv6	25
Connect to Your Network	6	IPv6 - Tethering.....	26
Insert a microSD Card	6	IPv6 - 6to4.....	27
Driver Installation	7	IPv6 - 6rd	28
Wireless Installation Considerations.....	8	2G/3G Modem	29
Configuration.....	9	SIM	30
Initial Connection to the Router	9	PLMN	31
Connect via USB.....	9	Network	32
Connect via Wi-Fi	10	Wi-Fi.....	33
Web-based Configuration.....	12	DHCP	34
Configuration Utility	12	DHCPv6	36
Home	13	NAT.....	40
Navigation.....	13	NAT 64.....	42
Device Status.....	14	SMS.....	43
		New Message	43
		Local	43

Wi-Fi.....	44	Standby Mode	67
Basic.....	44	Password.....	68
Wireless Security	46	Date and Time	69
Wired Equivalent Privacy (WEP)	46	Language.....	71
Wi-Fi Protected Access (WPA).....	47	System Log.....	72
WLAN Authentication and Privacy Infrastructure (WAPI).....	48	Connecting to a Wireless Network	73
Wi-Fi Protected Setup (WPS)	49	Using Windows 8	73
MAC Filter	50	Connecting to a Wireless Network	75
Station Lists.....	51	Using Windows 7	75
Advanced	52	Configuring Wireless Security	77
IPv4	52	Using Windows Vista™	80
IPv6	53	Configuring Wireless Security	81
RIP.....	54	Using Windows® XP	83
LAN IPv6 RA	55	Configure WEP	84
IPv6 Multicast.....	58	Configure WPA-PSK.....	86
Security	59	Troubleshooting	88
Firewall	59	Networking Basics	90
IP Filter	59	Check your IP address.....	90
IPv6 Filter	60	Statically Assign an IP address	91
MAC Filter	61	Technical Specifications	92
DDOS.....	62	Warnings and Declarations	93
URL Filter	63		
Application	64		
About	64		
Configuration	65		
Firmware Upgrade.....	66		

Product Overview

Package Contents



D-Link DWR-830 DC-HSPA+ Mobile Router



Battery



USB Cable



Power Adapter

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

System Requirements

- A compatible (U)SIM card with mobile data service¹
- A computer with Windows®, Macintosh®, or Linux-based operating systems
- Internet Explorer 8, Firefox 12.0, Chrome 20.0, or Safari 4.0

¹ Subject to services and service terms available from your carrier.

Introduction

The D-Link DWR-830 HSPA+ Mobile Router lets you share a fast mobile Internet connection with multiple PCs and mobile devices wherever you go. It offers 3G HSPA+ compatibility for fast downlink and uplink data rates, so you get the high-speed upload and download speeds even when you're on the go. Set up a personal mobile network anywhere, anytime allowing you and those around you to access the Internet, and share files.

High-Speed Mobile Internet with 3G Connectivity

The DWR-830 HSPA+ Mobile Router gives you high-speed access to the Internet wherever you are and lets you share it on the go. Using HSPA+ technology, you can achieve download speeds of up to 21.6 Mbps and upload speeds of up to 5.76 Mbps¹. The built-in 3G antenna provides a reliable connection to your 3G service provider, and a separate Wi-Fi antenna gives extended coverage to the computers and mobile devices connected to the DWR-830.

Mobile Internet for All of Your Devices

The HSPA+ Mobile Router lets you share your fast mobile connection over Wi-Fi from a device small enough to fit in your pocket. With the DWR-830, you can get online with your notebook, smartphone, tablet, or any other wireless device using a single 3G mobile connection. The DWR-830 provides high-speed Wireless N coverage to give high-speed wireless access to everybody – whether you are with colleagues on a business trip, or travelling with friends and family.

Built-in Software for Instant Access Anywhere

The DWR-830 is truly plug and play, with drivers built right into the router so you can connect without the need to install anything. Open a browser, connect the router, and you can set up your network right from a web interface. This means that notebooks and netbooks without a CD-ROM drive can connect and get up and running in no time. Once the device is set up, you can simply power it on to start up your portable mobile network, meaning that you can share your mobile Internet connection without even needing a computer.

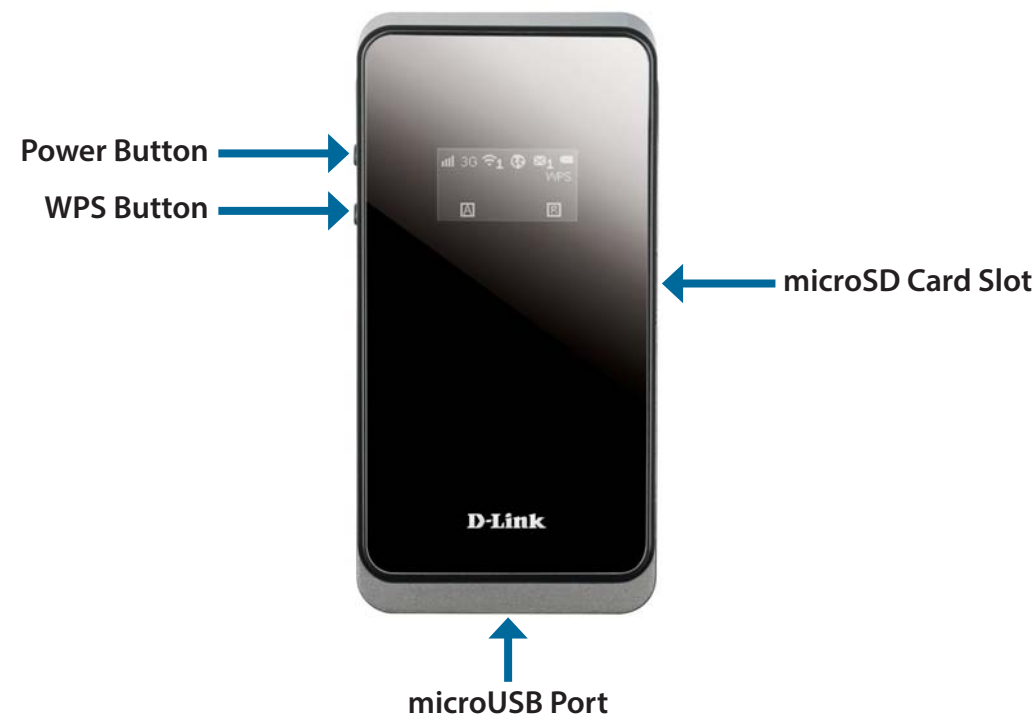
Designed for True Portability

The DWR-830 HSPA+ Mobile Router is small and slim enough to carry around in your purse, bag, or pocket. It features a microSD card slot for optional removable storage (up to 32 GB), allowing you to always have your files and contacts on hand. The built-in 2380 mAh rechargeable Li-Ion battery can provide up to six hours of mobile usage, meaning that you can share your mobile Internet connection in the car, in the park, or anywhere, and work or play longer without needing to recharge.

¹ All references to speed are for comparison purposes only. Actual speeds will vary depending on a range of factors including mobile network coverage, signal strength, network activity, and environmental conditions.

Hardware Overview

Left Side

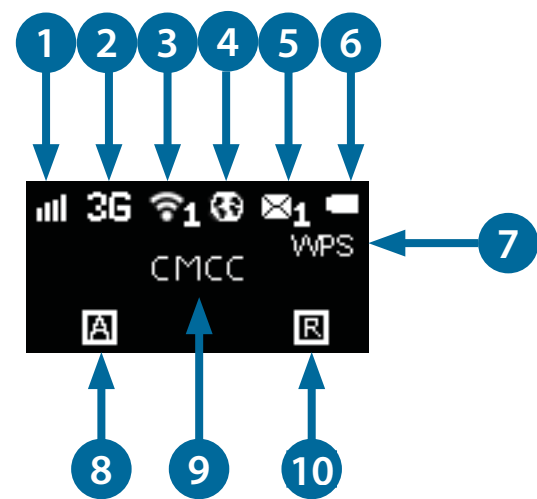


Power Button	Press and hold this button for 6 seconds to power on/off the device.
WPS Button	Press this button to add new wireless devices quickly and easily using Wi-Fi Protected Setup (WPS). Press and hold for more than 5 seconds to turn the wireless function on/off.
microSD Card Slot	Insert a microSD Card (up to 32GB) to access and share files and media wherever you go.
micro USB Connector	Use the included cable to connect to a powered USB port to charge the device, or to access the configuration utility.

Hardware Overview

OLED Display

The current status of the DWR-830’s functions including mobile network, Wi-Fi, security, Internet status, signal strength, and battery level will be shown on the OLED display. Please refer to the table below for the specific indications which are shown on the display.



Number	Function	Icon	Indication
1	Network Strength	0-5 Bars	Indicates the strength of the current mobile network connection
2	Network Type	H+	Currently connected to DC-HSPA+ or HSPA+ mobile network
		H	Currently connected to HSPA mobile network
		3G	Currently connected to WCDMA mobile network
		2G	Currently connected to GPRS/EDGE network
		No SIM	No SIM card detected in device

3	Wi-Fi & Clients		Indicates that the Wi-Fi network is currently tuned on
		Number	Indicates the number of clients currently connected to the device by Wi-Fi
4	Internet Connection Status	Internet	If this icon is displayed, there is an Internet connection present
5	SMS	Number	There are unread SMS messages in the inbox
6	Battery Status	Empty-Full	Displays the current battery level. If charging, the animation will indicate charging status and current battery level
7	Wi-Fi Protected Setup	WPS	The device is ready for WPS association with wireless clients
8	Connection Method	A	The device is set to connect to the mobile network automatically
		M	The device is set to connect to the mobile network manually
		D = On Demand	The device will connect to the preferred mobile network when internet access is required.
9	Operator	Name	The name of the mobile network operator to which device is currently connected
10	Roaming	R	The device is currently roaming on a network other than the home network

Installation

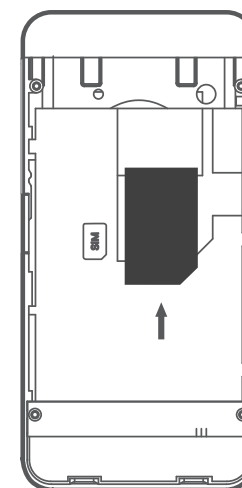
This section will guide you through the installation process.

Connect to Your Network

1. Ensure that your DWR-830 DC-HSPA+ Mobile Router is powered off.
2. Remove the back cover and take out the battery. Slide your (U)SIM card into the slot provided, ensuring that the alignment is the same as indicated by the logo next to the slot. The gold contacts on the card should be facing downwards.

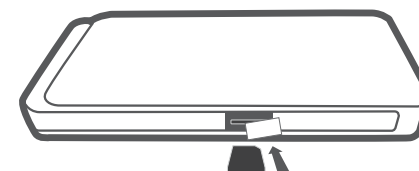
Caution: Always unplug and turn off the router before installing or removing the SIM card.
Never insert or remove the SIM card while the router is in use.

3. Press and hold the power button on the side of the router.
 - a. "D-Link" will be displayed on the screen as the router performs its initialization processes.
 - b. After a few moments, the OLED display will show the current status of the router's various functions. For more details on the OLED display, please refer to "OLED Display" on page 4.



Insert a microSD Card

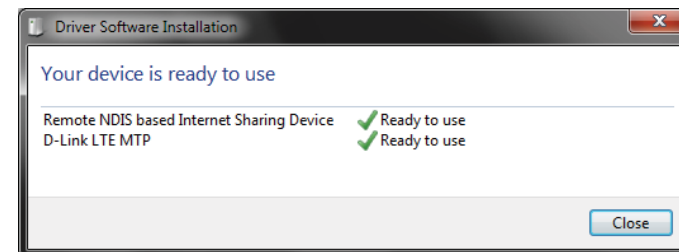
1. Ensure that your DWR-830 DC-HSPA+ Mobile Router is powered off.
2. Open the cover of the microSD slot on the side of the router.
3. Insert the microSD card into the slot and push it in until it locks into place.



Driver Installation

When you plug the DWR-830 into your computer, any necessary drivers will immediately install (with your permission).

Note: These drivers are Windows-only. Mac and Linux users will still be able to configure the DWR-830 using the web configuration utility described in “Configuration Utility” on page 12.



Wireless Installation Considerations

The DWR-830 can be accessed using a wireless connection from anywhere within the operating range of its 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 adversely affect wireless signals. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

1. Minimize the number of walls and ceilings between the router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters) appears to be almost 3 feet (1 meter) thick at a 45-degree angle. At a 2-degree angle it appears 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 a 2.4 GHz cordless phone, 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 configuration utility that can be obtained through a software interface or a web-based user interface.

Initial Connection to the Router

When configuring the router for the first time, you will need to establish a direct connection with the router in order to access the web-based configuration utility. This can be done using the included USB cable, or by connecting wirelessly to the DWR-830. Once you have configured your router, you will be able to connect using the Wi-Fi settings that you have specified in the configuration process. Ensure that the router is powered on and has sufficient battery power before commencing the setup process.

Connect via USB

To connect to the router via USB, plug the provided micro USB cable into the micro USB port on the bottom of the router, and plug the other end into an available USB port on your computer. Your router is now ready for configuration, please refer to “Configuration Utility” on page 12 to continue the setup process.

Connect via Wi-Fi

Note: The following example uses Windows 7's built-in wireless connection utility. If you are using a different operating system, or a third party connection utility, the process may be different. Please refer to the documentation that came with your operating system or wireless client for further information on how to connect to a wireless network.

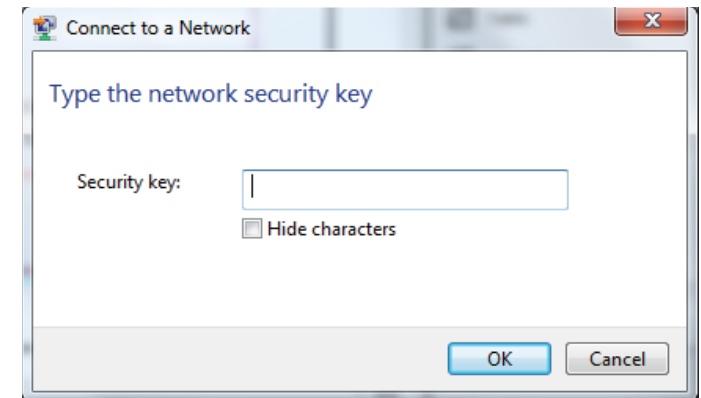
To connect to the router using Wi-Fi, open your operating system's wireless networking utility and scan for available networks to connect to. By default, the network name (SSID) of the DWR-830 will be in the format **dlink_DWR-830xxxx**, where "xxxx" represents the last four character's of the router's MAC address.



Once you have located this network with your wireless utility, connect to the network using your wireless networking utility.

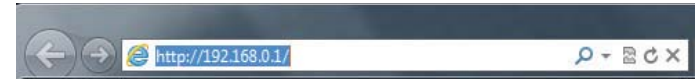


You will then be prompted to enter the network security key for your router. The unique security key for your router will be displayed on a sticker in the router's battery bay. Enter the security key in the box provided and click **OK**. Your wireless connection utility should confirm that the connection is successful, and you can move to the next step to continue to configuration process.



Web-based Configuration

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



Configuration Utility

Once you have reached the configuration utility through the installed software or your web browser, you will need to log in. Enter **admin** as the username, and then enter the password. By default, the password is blank. You can also select your language from the drop-down menu.

Click **Login** to continue.

A screenshot of the D-Link configuration utility login page. The page has a light blue background. On the left, there is a "Login" section with three input fields: "Account", "Password", and "Language". The "Language" field is a drop-down menu currently showing "English". Below these fields is a blue "Login" button. On the right side of the page, the "D-Link" logo is displayed in a large, bold, black font.

Home

Navigation

Throughout the interface you will find a menu bar at the top of the page which includes tabs for easy navigation, and a summary bar in the upper right corner with a quick view of essential information.



Home The **Home** tab will return you the home page, where a summary of the system information is shown.

Wizard: Click on this tab to start the setup wizard, which will guide you through the basic setup process.

Internet: The **Internet** tab gives you Internet setup and settings options.

Network: The **Network** tab allows you to configure the network settings for your Local Area Network (LAN).

SMS: From the **SMS** you can view and send SMS messages via your mobile network.

Wi-Fi: The **Wi-Fi** allows you to configure your Wi-Fi network, as well as add new devices using WPS.

Advanced: Use this tab to configure advanced network settings such as routing and IPv6.

Security: The **Security** tab allows you to configure firewall and security settings to protect your network from WAN-side intrusions.

Application: From this tab, you can manage the administrative configuration of your router, such as time and date, firmware, language, and remote management.

Device Status

A summary of the device's current status will be displayed on the information panel at the top of the right-hand side of the navigation bar. The following is a description of the indications, from left to right.



SIM: This icon shows whether or not a compatible (U)SIM card has been inserted into the device.

SMS: The number to the right of this icon indicates the number of unread messages in the SMS inbox.

Signal Strength: Indicates the current strength of the mobile network signal being received.

Operator Name: The name of the mobile network operator to which the device is currently connected.

Roaming: Indicates that the device is connected to a network other than your service provider's home network.

Internet: Indicates that there is an Internet connection present.

Wi-Fi Network: Indicates that the router's Wi-Fi network is currently active. The number to the right of this icon indicates the number of wireless clients currently connected to the router's Wi-Fi network.

Logout: Click this button to log out of the configuration interface.

Home

The **Home** page acts as a dashboard to quickly display your configuration settings and provide a summary of the current status of your network's status.

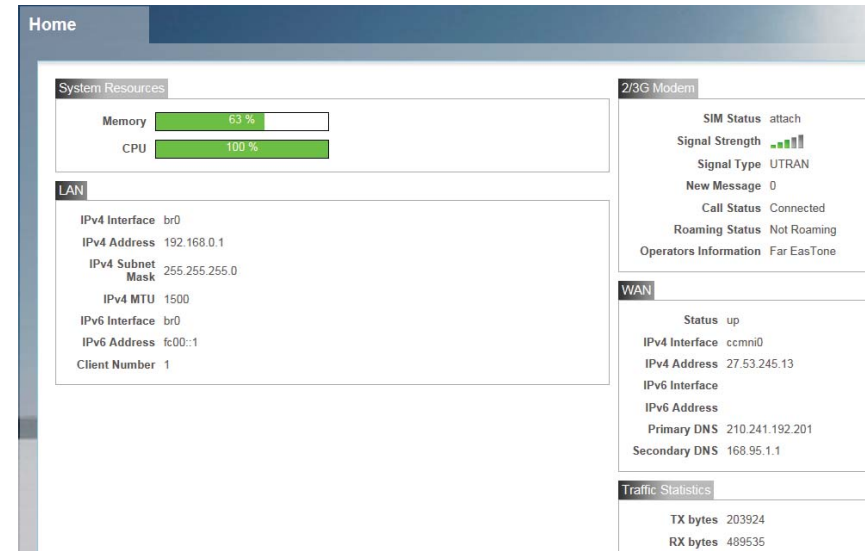
System Resources: This area displays the percentage of the router's memory and CPU currently being used by the system.

LAN: This area displays a summary of the current settings for the router's LAN.

2G/3G Modem: This area shows the current status of your 2G or 3G mobile network connection.

WAN: This area displays a summary of the router's current WAN settings. These details will reflect the mobile network connection which is being received from the service provider.

Traffic Statistics: This area shows the amount of data which has been sent (TX) and received (RX) over the mobile network. This information may not reflect the amount recorded by your mobile service provider.



Wizard

The **Wizard** page will guide you through the steps required to configure the basic settings of your router such as the IP address, network name (SSID), and password. Click on the Wizard button on the navigation bar to commence the wizard.

LAN CONFIGURATION

- IP Address:** If you wish to change the router’s IP address, enter the new address here. If you change the IP address from the default, you will need to enter the new address in your Internet browser’s address bar in order to access the web-based configuration utility.
- IP Subnet Mask:** If you wish to change the router’s subnet mask, enter it here.

Click **Next** to continue.

2/3G CONFIGURATION

If you wish to change the 2G or 3G service provider or connection type, click on a profile in the list to highlight it, and click **Set** to set that profile as the default.

Click **Next** to continue, or **Back** to return to the previous step.

Step 1
LAN Settings

Step 2
WAN Settings

Step 3
WiFi Settings

LAN Configuration

IP Address192.168.0.5

IP Subnet Mask255.255.255.0

Next

Step 1
LAN Settings

Step 2
WAN Settings

Step 3
WiFi Settings

Please consult with service provider for these settings. If not sure, leave them with default value.

2/3G Configuration

Type	Profile
2/3G Data Connection	PID-7

Set

Profile	Type	Name	APN	User	Password
PID-7	System	遠傳電信 (Far EastOne)	internet		
PID-8	System	遠傳電信 (Far EastOne) (Fetnet01)	fetnet01		

Total Num : 2

Back

Next

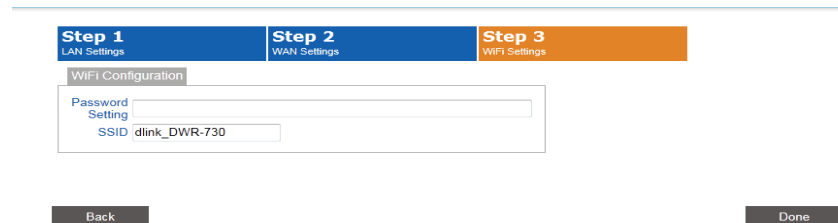
Wi-Fi CONFIGURATION

Password Setting: Choose a password for your wireless security. Clients will need this password in order to access your network wirelessly. If you are currently connected to the router using Wi-Fi, you will need to reconnect to the router using your new password once the wizard has been completed.

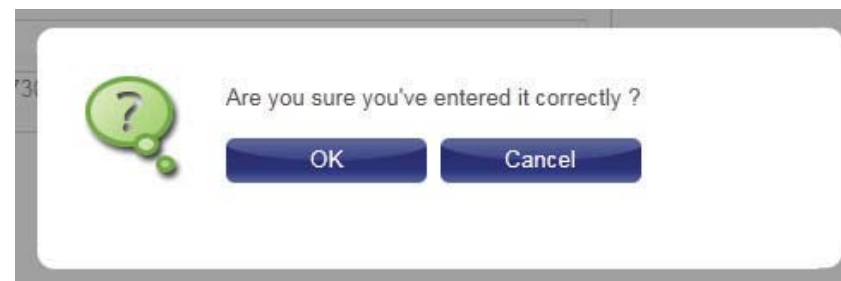
SSID: If you wish to change your wireless network name (SSID), enter a new name in the field provided. If you change the SSID, you may need to re-connect to the router using the new SSID before you can access your network or the configuration utility.

Click **Done** to complete the wizard, or click **Back** to return to the previous page.

After you have clicked **Done**, a confirmation window will appear. Click **OK** to save the configuration.



The image shows the 'Step 3: WiFi Settings' screen of a configuration wizard. At the top, there are three tabs: 'Step 1 LAN Settings', 'Step 2 WAN Settings', and 'Step 3 WiFi Settings'. The 'Step 3' tab is selected and highlighted in orange. Below the tabs, the title 'WiFi Configuration' is displayed. Underneath, there are two input fields: 'Password Setting' and 'SSID'. The 'SSID' field contains the text 'dlink_DWR-730'. At the bottom of the screen, there are two buttons: 'Back' on the left and 'Done' on the right.



Internet Connection

This page allows you to configure the Internet settings for your mobile network connection. Use the tabs in the left-hand column to navigate through the different settings categories.

CONNECTION OPERATION

Flight Mode: Flight mode turns off all communications so that the device can be powered on safely when in an aircraft. Select whether you want to **Enable** or **Disable** flight mode from the drop-down menu, and click **Change** to effect the change.

Preferred Cellular Network: Select your preferred cellular network connection mode:
Auto Mode - The router will automatically connect to your preferred mobile network and remain connected while the device is powered on.
Manual Mode - You must manually connect to the preferred mobile network.
On Demand - The router will connect to the preferred mobile network when Internet access is required.

Click **Change** to effect the change.


Roaming Mode: Select whether you would like to **Enable** or **Disable** mobile network roaming from the drop-down menu.

Caution: Roaming on networks other than your own may incur additional usage charges.



Connection: Shows the type and status of the current mobile connection. To change the connection profile, select a user profile from the table below and click **Set** to activate the profile. Click **Disconnect** to manually disconnect the current mobile data service.

Profiles: The profiles table shows the details of currently configured user profiles. To add a new user profile, navigate to the **User Profile** tab at the top of this section.

Type	State	Signal	Profile			
2/3G Data Connection 1	Connected		PID-7			
				Set	Disconnect	

Profile	Type	Name	APN	Protocol	User	Password
PID-7	System	遠傳電信 (Far East one)	internet	IPv4		
PID-8	System	遠傳電信 (Far East one) (Fetnet01)	fetnet01	IPv4		

Total Num : 2

USER PROFILE

Click **Add** to add a new user profile.

Name: Enter a name to identify the new user profile.

APN: Enter the Access Point Name (APN) for the connection. If you do not know this information, please contact your service provider.

Protocol: Select the protocol to be used for the connection from the drop-down menu.

User: Enter the username to be used for this connection.

Password: Enter the password to be used for this connection.

Delete: Click the delete icon to delete this profile from the list.

Click **OK** to save the profile.

Click **Apply** to apply the profile settings and return to the Internet menu.

Profile	Name	APN	Protocol	User	Password	
	<input type="text"/>	<input type="text"/>	IPv4	<input type="text"/>	<input type="text"/>	

Total Num : 1

Add **OK**

Apply

Configuration

This section allows you to specify the settings for your Internet connection depending on the type of connection you wish to use, or as specified by your Internet Service Provider. Use the IPv4 and IPv6 tabs at the top of the section to select the IP address mode.

IPv4 - PDP Context

Connection Type: Select **PDP Context** from the drop-down menu.

DNS Setting: Enter up to three DNS servers as provided to you by your service provider.

Click **Apply** to apply the changes.



The screenshot shows a web interface for configuring an IPv4 connection. At the top, there are tabs for 'Configuration', 'IPv4 WAN', and 'IPv6 WAN'. The 'Configuration' tab is active. Below the tabs, there is a 'Connection Configuration' section with a 'Configuration Type' dropdown menu set to 'PDP Context'. Below this, there is a 'DNS Setting' section with three input fields labeled 'DNS1', 'DNS2', and 'DNS3'. An 'Apply' button is located at the bottom right of the form.

IPv4 - Static Setting

Use this setting if your Internet Service Provider has supplied you with a static (non-changing) IPv4 address. If you are missing any of the information required in this section, please contact your ISP.

Connection Type: Select **Static Setting** from the drop-down menu.

IP Address: Enter the static IP address provided to you by your ISP.

Mask: Enter the subnet mask provided to you by your ISP.

Gateway: Enter the default gateway provided to you by your ISP.

MTU: Enter the maximum transmission unit for this connection.
The default MTU is 1400.

DNS Setting: Enter up to three DNS servers as provided to you by your ISP.

Click **Apply** to apply the changes.



The screenshot shows a web-based configuration interface for IPv4 WAN settings. At the top, there are tabs for 'Configuration', 'IPv4 WAN', and 'IPv6 WAN'. The 'Configuration' tab is active. Below it, the 'Connection Configuration' section shows 'Configuration Type' set to 'Static Setting'. The 'Static Setting' section contains input fields for 'IP Address', 'Mask', 'Gateway', and 'MTU' (with a default value of 1400). The 'DNS Setting' section contains input fields for 'DNS1', 'DNS2', and 'DNS3'. An 'Apply' button is located at the bottom right of the form.

IPv4 - 4to6

Use this setting if you wish to use IPv4 through an IPv6 tunnel.

Connection Type: Select **4to6** from the drop-down menu.

Remote IPv6 Address: Enter the remote IPv6 address for your connection.

Remote IPv4 Address: Enter the remote IPv4 address for your connection.

Local IPv6 Address: Select **User Define** from the drop-down menu to define your own local IPv6 address, or select **WAN IPv6 Address** to use the remote IPv6 address.

Local IPv4 Address: Enter the local IPv4 address for your connection.

DNS Setting: Enter up to three DNS servers as provided to you by your ISP.

Click **Apply** to apply the changes.

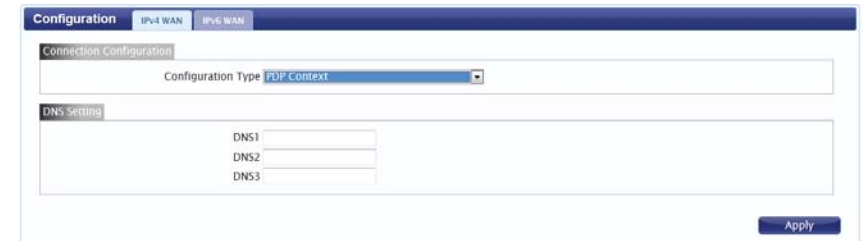
The screenshot shows the 'Configuration' tab with sub-tabs for 'IPv4 WAN' and 'IPv6 WAN'. The 'IPv6 WAN' sub-tab is active. Under 'Connection Configuration', the 'Configuration Type' is set to '4to6'. Below this, the '4to6 Tunnel' section contains fields for 'Remote IPv6 Address', 'Remote IPv4 Address', 'Local IPv6 Address' (with a dropdown menu currently showing 'User Define'), and 'Local IPv4 Address'. The 'DNS Setting' section below has three input fields for 'DNS1', 'DNS2', and 'DNS3'. An 'Apply' button is located at the bottom right of the configuration area.

IPv6 - PDP Context

Connection Type: Select **PDP Context** from the drop-down menu.

DNS Setting: Enter up to three DNS servers as provided to you by your ISP.

Click **Apply** to apply the changes.



The screenshot shows a web interface for configuring IPv6 WAN. At the top, there are tabs for 'Configuration', 'IPv4 WAN', and 'IPv6 WAN'. The 'Configuration' tab is active. Below the tabs, there is a section titled 'Connection Configuration'. Inside this section, there is a label 'Configuration Type' followed by a drop-down menu that has 'PDP Context' selected. Below this, there is a section titled 'DNS Setting'. This section contains three input fields labeled 'DNS1', 'DNS2', and 'DNS3'. At the bottom right of the form, there is an 'Apply' button.

IPv6 - Static Setting

Use this setting if your Internet Service Provider has supplied you with a static (non-changing) IPv6 address. If you are missing any of the information required in this section, please contact your ISP.

Connection Type: Select **Static Setting** from the drop-down menu.

Static IP: Enter the static IPv6 address that has been supplied to you by your service provider.

Gateway: Enter the IPv6 gateway that has been supplied to you by your service provider.

MTU: Enter the maximum transmission unit for this connection.
The default MTU is 1280.

DNS Setting: Enter up to three DNS servers as provided to you by your ISP.

Click **Apply** to apply the changes.



The screenshot shows a web-based configuration interface for IPv6 settings. At the top, there are tabs for 'Configuration', 'IPv6 WAN', and 'IPv6 LAN'. The 'Configuration' tab is active. Below the tabs, there is a 'Connection Configuration' section with a 'Configuration Type' dropdown menu set to 'Static Setting'. Underneath, there is a 'Static Setting' section with fields for 'Static IP fe80::' (with a '/ 64' suffix), 'Gateway', and 'MTU 1280'. Below that is a 'DNS Setting' section with three fields for 'DNS1', 'DNS2', and 'DNS3'. An 'Apply' button is located at the bottom right of the form.

IPv6 - DHCPv6

Use this setting if your Internet connection settings and IP address are to be obtained automatically from your ISP.

Connection Type: Select **DHCPv6** from the drop-down menu.

DNS Setting: Enter up to three DNS servers as provided to you by your service provider.

Click **Apply** to apply the changes.



The screenshot shows a web interface for configuring IPv6 WAN settings. At the top, there are tabs for 'IPv4 WAN' and 'IPv6 WAN'. The 'IPv6 WAN' tab is selected. Below the tabs, there is a 'Connection Configuration' section with a 'Configuration Type' dropdown menu set to 'DHCPv6'. Below this is a 'DNS Setting' section with three input fields labeled 'DNS1', 'DNS2', and 'DNS3'. An 'Apply' button is located at the bottom right of the form.


IPv6 - Tethering

Use this option to tether an IPv6 connection.

Connection Type: Select **Tethering** from the drop-down menu.

DNS Setting: Enter up to three DNS servers as provided to you by your service provider.

Click **Apply** to apply the changes.



The screenshot shows a web interface for configuring IPv6 WAN. At the top, there are tabs for 'Configuration', 'IPv4 WAN', and 'IPv6 WAN'. The 'Configuration' tab is active. Below the tabs, there is a 'Connection Configuration' section with a 'Configuration Type' dropdown menu set to 'TetheringShared /64 subnet, IETF Draft'. Below this is a 'DNS Setting' section with three input fields labeled 'DNS1', 'DNS2', and 'DNS3'. An 'Apply' button is located at the bottom right of the form.

IPv6 - 6to4

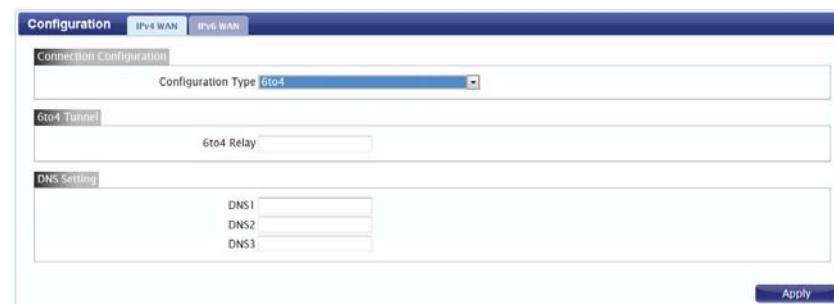
Use this setting if you wish to use IPv6 through an IPv4 tunnel.

Connection Type: Select **6to4** from the drop-down menu.

6to4 Relay: Enter the address of the 6to4 relay server to be used for this connection.

DNS Setting: Enter up to three DNS servers as provided to you by your ISP.

Click **Apply** to apply the changes.



The screenshot shows the 'Configuration' page for the 'IPv6 WAN' section. The 'Connection Configuration' tab is active, showing a 'Configuration Type' dropdown menu set to '6to4'. Below this, the '6to4 Tunnel' section contains a '6to4 Relay' input field. The 'DNS Setting' section contains three input fields for 'DNS1', 'DNS2', and 'DNS3'. An 'Apply' button is located at the bottom right of the configuration area.

IPv6 - 6rd

Use this setting if you wish to use the IPv6 Rapid Deployment (RD) protocol.

Connection Type: Select **6rd** from the drop-down menu.

6rd Configuration: Select **Manual** from the drop-down menu to manually enter your 6rd connection information. Select **DHCP 6rd Option** to receive connection information automatically from your service provider.

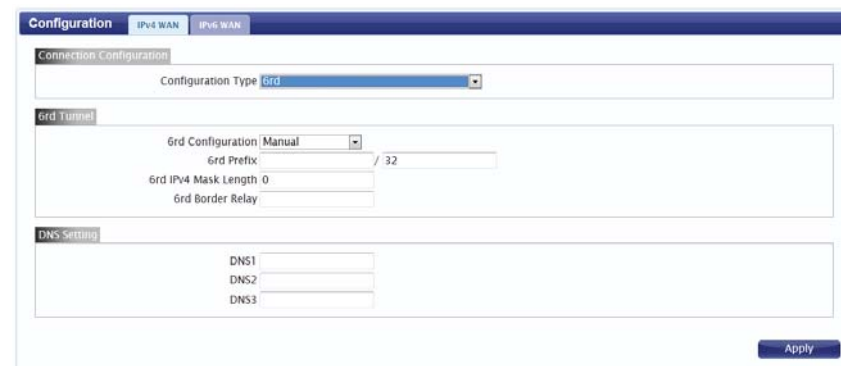
6rd Prefix: Enter the 6rd prefix supplied by your service provider.

6rd IPv4 Mask Length: Enter the mask length supplied by your service provider.

6rd Border Relay: Enter the border relay supplied by your service provider.

DNS Setting: Enter up to three DNS servers as provided to you by your ISP.

Click **Apply** to apply the changes.



The screenshot shows the 'Configuration' page for IPv6 WAN. The 'Connection Configuration' section has 'Configuration Type' set to '6rd'. The '6rd Tunnel' section has '6rd Configuration' set to 'Manual', '6rd Prefix' set to '32', '6rd IPv4 Mask Length' set to '0', and '6rd Border Relay' set to an empty field. The 'DNS Setting' section has 'DNS1', 'DNS2', and 'DNS3' set to empty fields. An 'Apply' button is at the bottom right.

2G/3G Modem

This section displays information about your 2G or 3G modem connection.

INFORMATION

Information: Displays information about your 2G or 3G modem.

SETTINGS

Network: Select your preferred modem type from the drop-down menu:


Auto - The modem will automatically select the modem type depending on the network it is connected to.

3G Only - The modem will only connect to 3G networks.

2G Only - The modem will only connect to 2G networks.

If you wish to change the modem type, select your new modem type and click **Change** to effect the change.
Re-enter the new PIN code.

Click **Apply** to apply the changes.



2/3G Modem Information Settings

Serial Number	30013051100035
IMEI	355189036250928
RSSI	-85 dBm



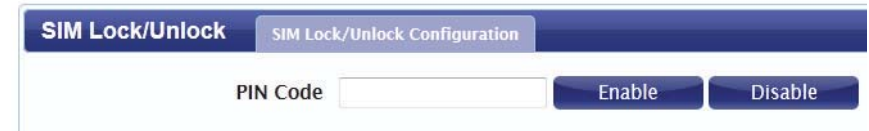
2/3G Modem Information Settings

Network Type Auto Change

SIM

This section allows you to turn SIM lock on or off for the SIM card which is currently inserted into the router.

PIN Code: Enter the PIN code for the SIM card. Click **Enable** to turn on SIM lock, or click **Disable** to turn off SIM lock.



The screenshot shows a web interface for SIM lock configuration. It features a dark blue header with two tabs: "SIM Lock/Unlock" (selected) and "SIM Lock/Unlock Configuration". Below the header, there is a label "PIN Code" followed by a text input field. To the right of the input field are two buttons: "Enable" and "Disable".

PLMN

This page allows you to view available Public Land Mobile Networks (PLMN). This page can also be used to select a preferred network when you are roaming outside of your home network.

Mode: Select **Automatic** to allow the router to automatically connect to the first available network when roaming. Select **Manual** to choose your preferred roaming network from the list below.

If you have selected Manual mode, click on the preferred network to select it, and then click the **Update** button to select that network as the preferred network. Click **Query** to refresh the list of available networks.

Note: You will need to manually disconnect the current mobile data service before selecting a network using PLMN. Please refer to “Connection” on page 18 for further information on how to do this.

The screenshot shows a web interface for PLMN configuration. At the top, there's a tab labeled 'PLMN' and a sub-tab '2/3G Modem'. Below this, there's a 'Mode' dropdown menu currently set to 'Automatic'. Underneath, there's a table with the following columns: 'Status', 'PLMN number', 'Operator Name', and 'Access Technology'. Below the table, it says 'Total Num: 0'. At the bottom right, there are two buttons: 'Update' and 'Query'.

Network

The **Network** pages allow you to check the current status of your Local Area Network (LAN), and make changes to LAN settings.



Wi-Fi

This section allows you to configure the IP settings for your wireless network.

IPv4

IP Address: Enter the IPv4 address for your Wi-Fi network. If you change this address, you will need to enter the new address in your web browser's address bar in order to access the web-based configuration utility.

IP Subnet Mask: Enter the IPv4 subnet mask for your Wi-Fi network.

Click **Apply** to save the current configuration.



The image shows the 'Wi-Fi' configuration page with the 'IPv4' tab selected. It contains two input fields: 'IP Address' with the value '192.168.0.1' and 'IP Subnet Mask' with the value '255.255.255.0'. An 'Apply' button is located at the bottom right.

IPv6

IPv6 Address: Enter the IPv6 address for your Wi-Fi network.

Prefix for LAN: Enter the prefix to be used to delegate IPv6 addresses to the LAN.

RA Autonomous: Check the box to set the router announcement mode to autonomous.

RA On-Link: Check the box to enable router announcement on-link

Click **Apply** to save the current configuration.



The image shows the 'Wi-Fi' configuration page with the 'IPv6' tab selected. It contains two input fields: 'IPv6 Address' with the value 'fc00::1' and 'Prefix for LAN' with the value 'fc00::/64'. Below these are two checked checkboxes: 'RA Autonomous' and 'RA On-Link'. An 'Apply' button is located at the bottom right.

DNS NAME

DNS Device Name: Enter your router's DNS device name in the field provided.

Click **Apply** to save the current configuration.



The image shows the 'Wi-Fi' configuration page with the 'DNS Name' tab selected. It contains one input field: 'DNS Device Name' with the value '192.168.0.1'. An 'Apply' button is located at the bottom right.

DHCP

The DWR-830 has a built-in DHCP server which can assign IP addresses to connected clients. This section allows you to configure the DHCP settings.

DHCP SERVER

DHCP Mode: Select the desired DHCP mode from the drop down menu:

None - Turns off DHCP functionality

Server - The router will act as a DHCP server and assign IP addresses to connected devices.

Relay - The router will act as a relay between DHCP clients and a DHCP server on another subnet.

Start IP: Enter the starting address for the DHCP pool.

End IP: Enter the ending address for the DHCP pool.

Lease Time: Enter the lease time (in minutes) for assigned IP addresses.

Relay IP: If you selected Relay above, enter the IP address of the DHCP server to be relayed.

Metric Number: Enter the metric number to be used for the DHCP server.

Click **Apply** to save the current configuration.

The screenshot shows the 'DHCP' configuration page with the 'DHCP Server' tab selected. The 'DHCP Mode' is set to 'Server'. The 'Start IP' is 192.168.0.100, 'End IP' is 192.168.0.199, 'Lease Time' is 1440, 'Relay IP' is 0.0.0.0, and 'Metric Number' is 30. An 'Apply' button is at the bottom right.

DHCP	
DHCP Server	DNS Server
DHCP Mode	Server
Start IP	192.168.0.100
End IP	192.168.0.199
Lease Time	1440
Relay IP	0.0.0.0
Metric Number	30

Apply

DNS SERVER

First/Second/Third DNS Server: Select **None** from the drop-down menus if you do not wish to specify a first, second, or third DNS server. Select **User Define** to specify a DNS server, and enter the address of the server in the field provided.

Click **Apply** to save the current configuration.

The screenshot shows the 'DNS Server' configuration page with the 'DNS Server' tab selected. The 'First DNS Server', 'Second DNS Server', and 'Third DNS Server' are all set to 'None'. An 'Apply' button is at the bottom right.

DHCP	
DHCP Server	DNS Server
First DNS Server	None
Second DNS Server	None
Third DNS Server	None

Apply

NTP SERVER

First/Second/Third NTP Server: Select **None** from the drop-down menus if you do not wish to specify a first, second, or third Network Time Protocol server. Select **From ISP** to use the automatic settings supplied by your ISP, or select **User Define** to specify an NTP server, and enter the address of the server in the field provided.

Click **Apply** to save the current configuration.

DHCP

DHCP Server

DNS Server

NTP Server

Static DHCP

Leased Hosts

First NTP Server

None

0.0.0.0

Second NTP Server

None

0.0.0.0

Third NTP Server

None

0.0.0.0

Apply

STATIC DHCP

Use this option to specify a DHCP address reservation to a particular device or machine based on MAC address. To add a new reservation, click **Add**.

MAC Address: Enter the MAC address of the device or machine for which you wish to make the DHCP reservation.

IP Address: Enter the IP address that you wish to reserve. This address must be within the DHCP address pool.

Click **OK** to save the reservation.

DHCP

DHCP Server

DNS Server

NTP Server

Static DHCP

Leased Hosts

10

per page

1

page

#

MAC Address

IP Address

1

00:00:00:00:00:00

192.168.0.0

Total Num : 1

Add

OK

Apply

LEASED HOSTS

This table shows the details of clients currently receiving a DHCP address from the DHCP server. Click **Refresh** to update the table.

DHCP

DHCP Server

DNS Server

NTP Server

Static DHCP

Leased Hosts

10

per page

0

page

#

Host Name

MAC Address

IP Address

Remaining Time

1

07869PCWIN7E

C8:D3:A3:03:43:86

192.168.0.100

23:49:05

Total Num : 1

Refresh

DHCPv6

This section allows you to configure your router’s DHCP server for the IPv6 protocol. To edit any of the fields under this tab, click on the field that you wish to edit, and a text box will appear. Click **OK** at the bottom of each section to save that particular rule or configuration.

OPTIONS

- DUID-LLT:** Displays the router’s DHCP Unique Identifier.
- Enable:** Check the box to enable the router to operate as a DHCPv6 server and issue DHCPv6 IP addresses to requesting clients.
- DNS Mode:** Select the preferred Domain Name Server (DNS) mode from the drop down menu. Select **Manual** to manually enter DNS information. Select **Proxy** to use a proxy server to resolve the DNS information.
- DNS Server:** If you selected Manual above, select whether you want to use **None**, **From ISP**, or **User Defined** for your domain name server. Enter the address of your DNS in the field provided.
- Domain Name:** Enter the DNS search path for your domain. From the drop-down menu on the left, select **Y** to activate the setting, or **N** to deactivate it.
- NTP Server:** Select **IP Address** from the drop-down menu and enter the IP address of an NTP server which will provide IPv6 Network Time Protocol information to IPv6 hosts.

DHCPv6

Options

Address Pool

Particular Client

Client Assigned Address

Client Delegated Prefix

DUID-LLT

00:01:00:01:c7:94:0e:82:00:0c:e7:0b:01:02

Enable

☒

DNS Mode

Manual

Type

DNS Server

None

None

DNS Server

None

None

Total Num : 3

OK

Active

DNS Search Path

N

N

Domain Name

N

Total Num : 3

OK

Type

NTP Server

None

None

NTP Server

None

None

Total Num : 3

OK

SIP Server: Select **Y(es)** or **N(o)** as the status of the SIP server function.
Enter the address of a Session Information Protocol (SIP) server.

SIP Domain: Select **Y(es)** or **N(o)** as the status of the SIP domain name function. Enter the SIP domain name for the rule.

NIS Server: Select **Y(es)** or **N(o)** as the status of the NIS server function.
Enter the address of a Network Information Service (NIS) server.

NIS Domain: Select **Y(es)** or **N(o)** as the status of the NIS domain name function. Enter the NIS domain name for the rule.

NIS+ Server: Select **Y(es)** or **N(o)** as the status of the NIS+ server function.
Enter the address of a Network Information Service Plus (NIS+) server.

NIS+ Domain: Select **Y(es)** or **N(o)** as the status of the NIS+ domain name function. Enter the NIS+ domain name for the rule.

Refresh Time: Enter the amount of time a DHCP client should wait before refreshing DHCP information with the DHCP server.

Allow Rapid Commit: Check this option to allow a two-method exchange method for faster configuration as defined by the rapid commit protocol.

Preference: Enter an integer to represent the preference level for the advertisement message

Active	SIP Server
<input type="button" value="N"/>	<input type="text"/>
N	::
N	::
Total Num : 3	
<input type="button" value="OK"/>	

Active	SIP Domain Name
<input type="button" value="N"/>	<input type="text"/>
N	
N	
Total Num : 3	
<input type="button" value="OK"/>	

Active	Server Address
<input type="button" value="N"/>	<input type="text"/>
N	::
N	::
Total Num : 3	
<input type="button" value="OK"/>	

Active	Domain Name
<input type="button" value="N"/>	<input type="text"/>
N	
N	
Total Num : 3	
<input type="button" value="OK"/>	

Active	Server Address
<input type="button" value="N"/>	<input type="text"/>
N	::
N	::
Total Num : 3	
<input type="button" value="OK"/>	

Active	Domain Name
<input type="button" value="N"/>	<input type="text"/>
N	
N	
Total Num : 3	
<input type="button" value="OK"/>	

Refresh Time

Allow Rapid Commit ☒

Preference

ADDRESS POOL

This tab allows you to specify address ranges for the DHCPv6 address pool. These addresses will be assigned to DHCPv6 clients that request an IPv6 address from the DHCP server.

Active: Check the box to activate the address pool rule.

Start Address: Enter the starting IPv6 address for the pool range.

End Address: Enter the ending IPv6 address for the pool range.

Preferred Lifetime: Enter the preferred lifetime for addresses in the DHCP pool.

Valid Lifetime: Enter the valid lifetime for addresses in the DHCP pool. This value should be larger than the preferred lifetime.

Click **OK** to save the DHCP address pool rule. Click **Apply** to save the current settings.

The screenshot shows the 'DHCPv6' configuration window with the 'Address Pool' tab selected. It contains a table with columns: Active, Start Address, End Address, Preferred Lifetime, and Valid Lifetime. The first row is active (checkbox checked) and has values for all fields. Below the table, it says 'Total Num : 4'. There are 'OK' and 'Apply' buttons at the bottom right.

Active	Start Address	End Address	Preferred Lifetime	Valid Lifetime
<input checked="" type="checkbox"/>	0	0
N	0	0
N	0	0
N	0	0

Total Num : 4

OK Apply

PARTICULAR CLIENT

Active: Check the box to activate the rule.

DUID-LLT: Enter the DHCP Unique Identifier (DUID) for the rule.

Security: Check the box to enable security on this rule. Enter the ID, Realm and Key for security using the DUID.

Click **OK** to save the current configuration.

The screenshot shows the 'DHCPv6' configuration window with the 'Particular Client' tab selected. It contains a table with columns: #, Active, DUID-LLT, Enable, ID, Security (Realm, Key). The first row is active (checkbox checked) and has values for all fields. Below the table, it says 'Total Num : 8'. There are 'OK' and 'Apply' buttons at the bottom right.

#	Active	DUID-LLT	Enable	ID	Security	
					Realm	Key
1	<input checked="" type="checkbox"/>	...	<input checked="" type="checkbox"/>	0		
2	N		N	0		
3	N		N	0		
4	N		N	0		
5	N		N	0		
6	N		N	0		
7	N		N	0		
8	N		N	0		

Total Num : 8

OK Apply

CLIENT ASSIGNED ADDRESS

- Active:** Check the box to activate the rule.
- Client #:** Enter a number to identify the client.
- Address:** Enter the address to be assigned.
- Preferred Lifetime:** Enter the preferred lifetime for the address to be assigned.
- Valid Lifetime:** Enter the valid lifetime for the address to be assigned.

Click **OK** to save the current rule.

Active	Client #	Address	Preferred Lifetime	Valid Lifetime
<input type="checkbox"/>	0	::	0	0
N	0	::	0	0
N	0	::	0	0
N	0	::	0	0

CLIENT DELEGATED PREFIX

- Active:** Check the box to activate the rule.
- Client #:** Enter a number to identify the client.
- Prefix:** Enter the prefix to be delegated.
- Preferred Lifetime:** Enter the preferred lifetime for the prefix to be assigned.
- Valid Lifetime:** Enter the valid lifetime for the prefix to be assigned.

Click **OK** to save the current rule.

DHCPv6					
Options Address Pool Particular Client Client Assigned Address Client Delegated Prefix					
Active	Client #	Prefix	Preferred Lifetime	Valid Lifetime	
<input type="checkbox"/>	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
N	0	::/128	0	0	
Total Num : 16					
					OK
					Apply

NAT

This section allows you to configure functions related to Network Address Translation (NAT) such as port triggering.

PORT TRIGGER

Use this option to have inbound traffic automatically forwarded to a dynamic address on the LAN when triggered by outbound traffic. To add a new port triggering rule, click **Add**.

Active: Check the box to activate this rule.

Name: Specify a name to identify the rule.

Trigger Protocol: Select **TCP** or **UDP** as the protocol for the trigger ports from the drop-down menu.

Trigger Port: Enter the starting and ending trigger port for the rule.

Open Protocol: Select **TCP** or **UDP** as the protocol for the ports to be opened from the drop-down menu.

Open Port(s): Enter the starting and ending ports to be opened when the trigger occurs.

Delete: Click the **Delete** icon to delete the rule.

Click **OK** to save the rule. Click **Apply** to apply the current rules and return to the Network page.

#	Active	Name	Trigger Protocol	Trigger Port(s)		Open Protocol	Open Port(s)		
				Start Port	End Port		Start Port	End Port	
1	<input checked="" type="checkbox"/>		TCP			TCP			

Total Num : 1

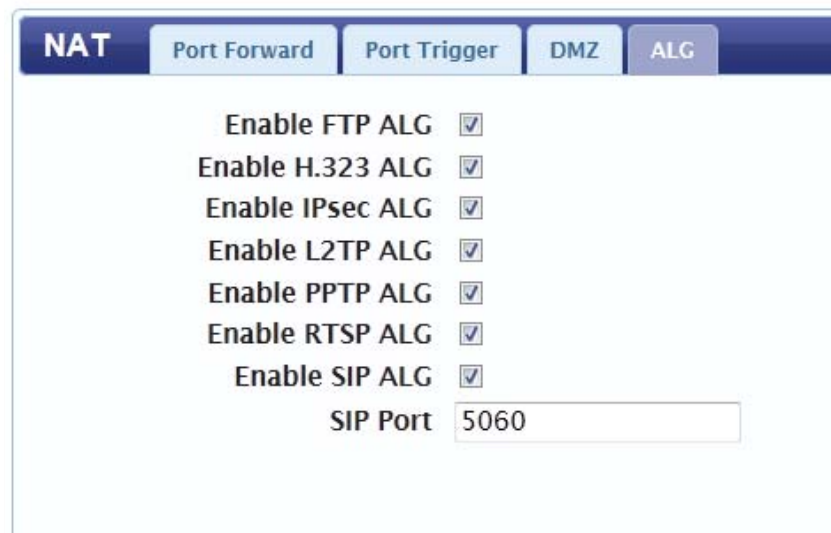
Add **OK** **Apply**

ALG

Application Level Gateways (ALG) allow certain applications to augment a network's firewall or NAT. This section enables you to enable various ALGs as required by specific applications. To enable an ALG, check the box next to the name of the rule.

SIP Port: Enter the Session Initiation Protocol (SIP) port required by your applications.

Click **Apply** to save the settings and return to the Network page.



The screenshot shows the NAT configuration interface with the ALG tab selected. The interface includes a header with tabs for NAT, Port Forward, Port Trigger, DMZ, and ALG. Below the tabs, there is a list of ALG options, each with a checkbox. The 'SIP Port' field is set to 5060.

ALG	Enabled
Enable FTP ALG	<input checked="" type="checkbox"/>
Enable H.323 ALG	<input checked="" type="checkbox"/>
Enable IPsec ALG	<input checked="" type="checkbox"/>
Enable L2TP ALG	<input checked="" type="checkbox"/>
Enable PPTP ALG	<input checked="" type="checkbox"/>
Enable RTSP ALG	<input checked="" type="checkbox"/>
Enable SIP ALG	<input checked="" type="checkbox"/>

SIP Port:

NAT 64

NAT 64 allows you to configure Network Address Translation for the IPv6 protocol.

Enable: Check the box to enable the NAT64 function.

Virtual IPv4 Pool: Enter the IPv4 address to be used for the virtual IPv4 address pool.

NAT64 Prefix: Enter the IPv6 prefix you wish to add, and select a prefix length from the drop-down menu. Click **OK** to save the rule.

Click **OK** to save the current configuration.

The screenshot shows the NAT64 configuration window with the following settings:

- Enable:** ☐ (unchecked)
- Virtual IPv4 Pool:** 192.168.255.1 / 24
- NAT64 Prefix:** 64:ff9b::
- Prefix Length:** 96
- Total Num:** 1
- Buttons:** OK, Apply

SMS

The DWR-830 can send and receive SMS text messages through the mobile network’s SMS function. In this section you can check the SIM card’s inbox and outbox, as well as send new messages.

New Message

Send To: Enter the phone number that you wish to send the message to

Messages: Enter the body of the message to be sent.

Click **Apply** to save the current configuration.



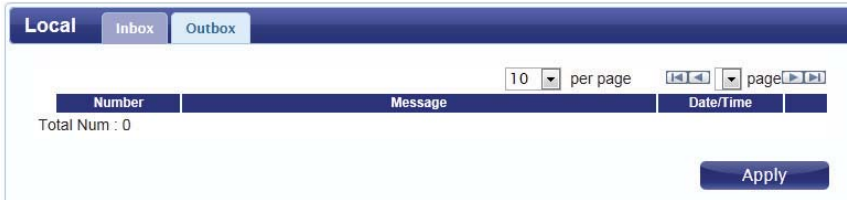
Local

INBOX

This tab shows a summary of SMS messages in the inbox.

OUTBOX

This tab shows a summary of messages in the outbox which are yet to be sent.



Wi-Fi

The **Wi-Fi** pages allow you to check the current status of your Wi-Fi network, and make changes to Wi-Fi settings.

Basic

This section allows you to configure your Wi-Fi network and specify the wireless security method to be used to secure your network.

Enable Check the box to enable the Wi-Fi function.

Mode: Select the desired 802.11 wireless mode from the drop-down menu. You should make your selection based on the standards supported by the wireless clients which will be connecting to your network.

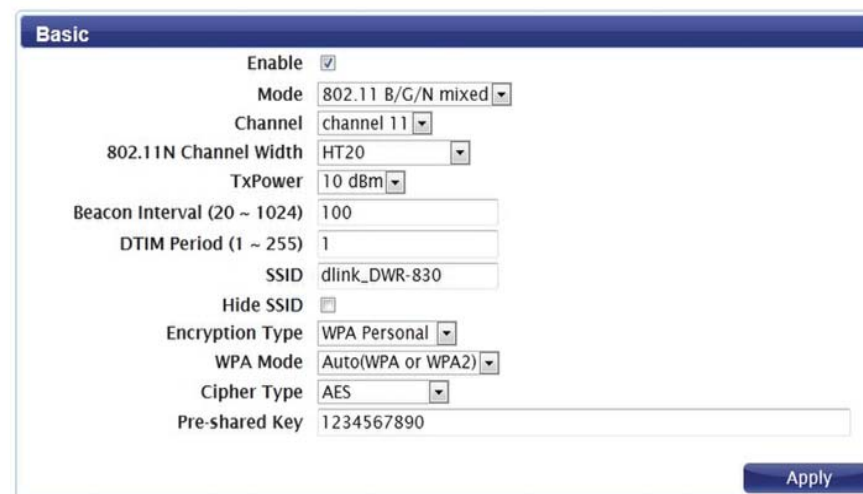
Channel: To have the router automatically select the optimal wireless channel, select **Auto** from the drop-down menu. If you wish to select a particular channel, select it from the drop-down menu.

802.11N If you are using the 802.11n standard, you can

Channel Width: manually select the channel width which best suits your network environment.

TxPower: Select the desired transmission power from the drop-down menu.

Beacon Interval: The beacon interval determines how often information about the wireless network is broadcast. It is recommended that you do not adjust this setting unless instructed to do so.



The screenshot shows the 'Basic' configuration window for the Wi-Fi network. The 'Enable' checkbox is checked. The 'Mode' is set to '802.11 B/G/N mixed'. The 'Channel' is set to 'channel 11'. The '802.11N Channel Width' is set to 'HT20'. The 'TxPower' is set to '10 dBm'. The 'Beacon Interval (20 ~ 1024)' is set to '100'. The 'DTIM Period (1 ~ 255)' is set to '1'. The 'SSID' is 'dlink_DWR-830'. The 'Hide SSID' checkbox is unchecked. The 'Encryption Type' is 'WPA Personal'. The 'WPA Mode' is 'Auto(WPA or WPA2)'. The 'Cipher Type' is 'AES'. The 'Pre-shared Key' is '1234567890'. An 'Apply' button is at the bottom right.

Basic	
Enable	<input checked="" type="checkbox"/>
Mode	802.11 B/G/N mixed
Channel	channel 11
802.11N Channel Width	HT20
TxPower	10 dBm
Beacon Interval (20 ~ 1024)	100
DTIM Period (1 ~ 255)	1
SSID	dlink_DWR-830
Hide SSID	<input type="checkbox"/>
Encryption Type	WPA Personal
WPA Mode	Auto(WPA or WPA2)
Cipher Type	AES
Pre-shared Key	1234567890
<input type="button" value="Apply"/>	

DTIM Period: The Delivery Traffic Indication Message broadcasts information about buffered data to clients that are currently in low-power mode. Enter the desired DTIM period as a number of beacon intervals.

SSID: Enter the SSID (network name) to identify your wireless network.

Hide SSID: Check the box to hide the SSID of your network. If the SSID is hidden, wireless clients must manually enter it in order to connect to your network.

Encryption Type: Select the wireless encryption method that you wish to use from the drop-down menu. Depending on the method that you select, you may need to configure additional settings. For more information regarding wireless encryption and how to configure it, please refer to “Wireless Security” on page 46. If you do not wish to enable wireless security, select **None** from the drop-down menu.

Click **Apply** to save the current settings.

The screenshot shows the 'Basic' configuration page for a wireless network. The settings are as follows:

- Enable:** ☒
- Mode:** 802.11 B/G/N mixed
- Channel:** channel 11
- 802.11N Channel Width:** HT20
- TxPower:** 10 dBm
- Beacon Interval (20 ~ 1024):** 100
- DTIM Period (1 ~ 255):** 1
- SSID:** dlink_DWR-830
- Hide SSID:** ☐
- Encryption Type:** WPA Personal
- WPA Mode:** Auto(WPA or WPA2)
- Cipher Type:** AES
- Pre-shared Key:** 1234567890

An **Apply** button is located at the bottom right of the configuration area.

Wireless Security

It is recommended that you enable wireless security on your router in order to protect your wireless network from unauthorized access. You should select a wireless security protocol that is compatible with the wireless clients which will be accessing your network.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is an older wireless security standard, which although providing more protection than no security at all, has some weaknesses which could make it vulnerable to intrusion. It is recommended that you only use WEP if your wireless clients do not support Wi-Fi Protected Access (WPA). WEP is not supported by the 802.11n standard, and therefore you will not be able to achieve 802.11n speeds if using WEP.

Encryption Type: Select **WEP** from the drop-down menu.

Authentication Method: Select the desired authentication method from the drop-down menu:

- Auto** - The router will automatically determine the authentication method based on the client that is connecting to it.
- Open System** - Clients do not require authentication in order to associate with the router. The encryption key will be used to encrypt data packets sent over the network.
- Shared** - The encryption key is used for authentication as well as to encrypt data packets.

WEP Encryption Length: Select the length of the encryption key to be used.

- Length: 64-bit** - A 64-bit key comprises a string of 10 hexadecimal characters, or 5 ASCII characters.
- 128-bit** - A 128-bit key comprises a string of 26 hexadecimal characters, or 13 ASCII characters.

Key 1-4: You can predetermine up to 4 WEP keys. Select the WEP key you wish to use by clicking on the radio buttons next to the keys. Select whether you wish to use **HEX** or **ASCII** characters in your key using the drop-down menu. Enter the desired key in the field provided. Click **Apply** to save the current settings.

Encryption Type	WEP	
Authentication Method	OPEN SYSTEM	
WEP Encryption Length	64-bit	
<input checked="" type="radio"/> Key 1	HEX	●●●●●●●●●●
<input type="radio"/> Key 2	HEX	●●●●●●●●●●
<input type="radio"/> Key 3	HEX	●●●●●●●●●●
<input type="radio"/> Key 4	HEX	●●●●●●●●●●

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a newer and more secure encryption protocol which makes significant improvements over WEP. There are two versions of WPA; the original WPA, and the newer WPA2.

Encryption Type: Select **WPA Personal** from the drop-down menu.

WPA Mode: Select the desired authentication method from the drop-down menu:
Auto (WPA or WPA2) - The router will automatically determine the version of WPA to be used based on the client that is connecting to it.
WPA - Clients will only be able to associate with the router using the WPA standard.
WPA2 - Clients will only be able to associate with the router using the WPA2 standard. Clients which do not support WPA2 will not be able to associate with the router.

Cipher Type: Select the desired cipher type from the drop-down menu:
TKIP - This cipher is used by the WPA standard.
AES - A newer cipher used by the WPA2 standard. Use of this cipher type is required in order to achieve 802.11 speeds.

Pre-Shared Key The pre-shared key is the password which clients will require in order to connect to your network. Enter a password of between 8 and 63 characters in length.

Click **Apply** to save the current settings

Encryption Type	WPA Personal ▼
WPA Mode	Auto(WPA or WPA2) ▼
Cipher Type	TKIP and AES ▼
Pre-shared Key	1234567890

WLAN Authentication and Privacy Infrastructure (WAPI)

WLAN Authentication and Privacy Infrastructure (WAPI) is a wireless security standard which is implemented in China. You should only use this protocol if your wireless clients do not support any of the other security methods provided by the DWR-830.

Encryption Type: Select **WAPI Personal** from the drop-down menu.

WAPI Pre-Shared Select whether your key should use **ASCII** or **HEX** characters
Key: using the drop down menu. Enter your desired key in the field provided.

Click **Apply** to save the current settings.

Encryption Type

WAPI Personal ▼

WAPI Pre-Shared Key

ASCII ▼

1234567890

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) enables you to quickly and securely add compatible devices to your wireless network.

Enable: Check the box to enable the Wi-Fi Protected Setup feature.

Configure State: Select whether you wish to **Configure** or **Unconfigure** the WPS function using the radio buttons.

Configure Method: Select the WPS method that you wish to use. If your device supports Push Button Connection (PBC), simply select this option and click **Apply** to start the connection process. You will then have 120 seconds to press the WPS button on your wireless device in order to initiate the connection. If your device does not support PBC, you can select the PIN method and continue to the next step.

Current PIN: A PIN is a unique number that can be used to add the router to an existing network or to create a new network.

Generate PIN: For extra security, a new PIN can be generated. Click **Generate** to create a new PIN. The current PIN will be shown in the field next to **Current PIN**. This PIN can be used by wireless clients to join your network using the PIN method.

Enrollee PIN: If the device you are trying to add to the network was provided with a PIN number, select this option and enter the device's PIN in the field.

Click **Apply** to commence the connection process.

The image shows a web-based configuration interface for WPS. At the top is a blue header bar with the text "WPS". Below the header, there are several settings: "Enable" with a checked checkbox, "Configure State" with two radio buttons (selected: "Unconfigure", unselected: "Configure"), and "Configure Method" with a dropdown menu set to "PIN". Under the "PIN" method, there are two options: "Current PIN:" with a text field containing "30332409" and a "Generate Pin" button, and "Enrollee PIN:" with an empty text field. At the bottom right of the form is a blue "Apply" button.

MAC Filter

The MAC filtering option allows you to allow or deny access to wireless clients based on their MAC address.

Enable MAC Address Filter: Check the box to enable the MAC filtering feature.

Mode: Select the filtering mode from the drop-down menu. You can choose to **Deny Listed Stations** access to your network, or **Allow Listed Stations** access.

LISTED STATIONS TABLE

To add a new filtering rule, click **Add**.

Active: Check the box to activate the rule.

Name: Enter a name to identify the machine or station which will be filtered.

MAC Address: Enter the MAC address of the machine or station which you wish to filter.

Delete: Click the **Delete** icon to delete the rule from the table.

Click **OK** to save the current rule and add it to the table.
Click **Apply** to save all changes and return to the Wi-Fi page.

MAC Filter

Enable MAC Address Filter

☒

Mode


Deny listed stations

10

per page

1

page

#	Active	Name	MAC Address	
1	<input checked="" type="checkbox"/>		00:00:00:00:00:00	

Total Num : 1

Add

OK

Apply

Station Lists

The Station List tab shows a list of all wireless clients currently connected to your wireless network.

Station Lists

10 per page 1 page

#	MAC Address
1	c8:d3:a3:03:43:86

Total Num : 1

Advanced

IPv4

The IPv4 routing table lists all current routing rules. Click **Add** to add a new routing rule.

Destination IP: Enter the destination IP address for your route.

Destination Mask: Enter the destination mask for your route.

Next Hop Type: Select **Interface** or **IP Address** as the hop type from the drop-down menu.

Next Hop Interface: Select either **LAN** or **WAN** as the next hop interface from the drop-down menu.

Metric: The metric will determine your route selection process. Enter a metric between 1 and 255 in the field provided.

Click **Apply** to save the routing rule.



The Static Route configuration interface shows a tabbed view with 'Static Route' selected. It includes a table with columns for '#', 'Destination IP', 'Destination Mask', 'Next Hop', and 'Metric'. The table is currently empty, and the 'Total Num' is 0. There are pagination controls showing '10 per page' and an 'Add' button.



The Route Editor configuration interface shows a tabbed view with 'IPv4' selected. It contains fields for 'Destination IP', 'Destination Mask', 'Next Hop Type' (a dropdown menu set to 'Interface'), 'Next Hop Interface' (a dropdown menu set to 'LAN'), and 'Metric (1 ~ 255)'. An 'Apply' button is located at the bottom right.

IPv6

The IPv6 routing table lists all current routing rules. Click **Add** to add a new routing rule.

Active: Check the box to activate the rule.

Destination Prefix: Enter the destination IPv6 address prefix for your route.

Route Type: Select **Directly Attached**, **Recursive**, or **Fully Specified** from the drop-down menu.

Output Interface: Select either **LAN** or **WAN** as the next hop interface from the drop-down menu.

Next Hop Address: Enter the next hop IPv6 address.

Metric: The metric will determine your route selection process. Enter a metric between 1 and 255 in the field provided.

Delete Icon: Click the **Delete** icon to delete this rule.

Click **OK** to save the routing rule. Click **Apply** to save the current configuration.

The screenshot shows the 'Static Route' configuration window with the 'IPv6' tab selected. At the top, there are tabs for 'IPv4' and 'IPv6'. Below the tabs, there is a table with columns: '#', 'Active', 'Destination Prefix', 'Route Type', 'Output Interface', 'NextHop Address', and 'Metric'. The table contains one row with the following values: '# 1', 'Active' (checked), 'Destination Prefix' (empty), 'Route Type' (Directly Attached), 'Output Interface' (LAN), 'NextHop Address' (empty), and 'Metric' (empty). To the right of the table, there is a 'Total Num : 1' label. At the bottom right, there are 'Add', 'OK', and 'Apply' buttons. The 'Add' button is disabled. The 'OK' button is enabled. The 'Apply' button is enabled.

#	Active	Destination Prefix	Route Type	Output Interface	NextHop Address	Metric
1	<input checked="" type="checkbox"/>		Directly Attached	LAN	::	

Total Num : 1

Add OK Apply

RIP

The Routing Information Protocol (RIP) uses metrics to prevent routing loops from being propagated. Use this section to configure your router’s RIP settings.

SETTING

Enable: Check the box to enable RIP. The table will show details of your RIP settings.

LAN

Direction: Select the desired direction in which to apply RIP. Select **RX/TX** to apply RIP in both inbound and outbound directions, **RX** for inbound only, and **TX** for outbound only.

Version: Select the RIP version that you wish to use from the drop-down menu.

Authentication: Select the desired authentication type from the drop-down menu.

WAN

Direction: Select the desired direction in which to apply RIP. Select **RX/TX** to apply RIP in both inbound and outbound directions, **RX** for inbound only, and **TX** for outbound only.

Version: Select the RIP version that you wish to use from the drop-down menu.

Authentication: Select the desired authentication type from the drop-down menu.

Click **Apply** to save the current configuration.

RIP

Setting

LAN

WAN

Enable

☒

Redistribute

Active	Type	Metric (0~16)
Y	static route	7

Total Num : 1

OK

Apply

RIP

Setting

LAN

WAN

Direction

RX/TX

Version

RIP-2M

Authentication

None

Apply

RIP

Setting

LAN

WAN

Direction

RX/TX

Version

RIP-2M

Authentication

None

Apply

LAN IPv6 RA

This tab allows to you customize what information is sent in the router's advertisement packets.

IsRouter: Select the router advertisement flag status.

AdvSend Advertisements: Check this box to have the router send advertisements.

Unicast Only: Check the box to have the router advertise unicast addresses only.

MaxRtrAdvInterval: Enter the maximum advertisement interval.

MinRtrAdvInterval: Enter the minimum advertisement interval.

AdvManagedFlag: Check the box to advertise that hosts should use managed protocol.

AdvOtherConfigFlag: Check the box to advertise that hosts should use an alternative configuration.

AdvLinkMTU: Enter the Maximum Transmission Unit size for advertisements.

AdvReachableTime: Enter the amount of time for which the router should consider a neighbor reachable after receiving a reachability confirmation.

AdvRetransTimer: Enter the amount of time that the host should wait before retransmitting a solicitation message.

AdvCurHopLimit: Enter the recommended hop limit which the router will transmit in datagrams sent.

The screenshot shows the 'Router Advertisement' configuration window with the following settings:

Setting	Value
IsRouter	Auto
AdvSendAdvertisements	<input checked="" type="checkbox"/>
Unicast Only	<input type="checkbox"/>
MaxRtrAdvInterval	600
MinRtrAdvInterval	198
AdvManagedFlag	<input type="checkbox"/>
AdvOtherConfigFlag	<input checked="" type="checkbox"/>
AdvLinkMTU	0
AdvReachableTime	0
AdvRetransTimer	0
AdvCurHopLimit	64
AdvDefaultLifetime	1800
AdvDefaultPreference	Medium
AdvSourceLLAddress	<input checked="" type="checkbox"/>

An 'Apply' button is located at the bottom right of the window.

AdvDefaultLifetime: Enter the default lifetime of router advertisements.

AdvDefault Preference: From the drop-down menu, select the default preferability of the address as a default router address.

AdvSource LLAddress: Check the box to allow the advertisement of the source link-local address.

Click **Apply** to save the current configuration.

PREFIX

Use this tab to customize the prefixes for router advertisements. Click **Add** to add a new prefix.

On-Link: Check to specify an on-link flag.

Autonomous: Check to specify an autonomous flag.

Valid Lifetime: Enter the amount of time for which the prefix will remain valid for on-link determination.

Preferred Lifetime: Enter the amount of time for which a prefix generated by stateless autoconfiguration will remain valid for on-link determination.

Prefix: Enter the name of the prefix.

Prefix Length: Enter the length of the prefix.

Delete Icon: Click the icon to delete the prefix rule.

Click **OK** to save the prefix rule. Click **Apply** to save the current configuration.

AdvDefaultLifetime: 1800
 AdvDefaultPreference: Medium
 AdvSourceLLAddress: ☒

Apply

#	On-Link	Autonomous	Valid Lifetime	Preferred Lifetime	Prefix	Prefix Length	
1	<input type="checkbox"/>	<input type="checkbox"/>					

Total Num : 1

Add OK

Apply

DNS CONFIGURATION

Use this tab to specify how the router delivers DNS information using router advertisements.

DNSSL: Enter the domain name of the DNS search list to be included in the advertisement.

Domain Name of DNS Search List: Enter the advertisement lifetime for the domain name.

Click the **Delete** icon to delete the DNS rule.

Click **OK** to save the current rule. Click **Apply** to save the current configuration.

Router Advertisement

SettingPrefixDNS Configuration

DNS ModeProxy

10per page1page

#	Domain Names of DNS Search List	Lifetime
1		

Total Num : 1

AddOK

Apply

IPv6 Multicast

This section allows you to configure your router to receive multicast streams over the IPv6 protocol.

- Enable:

Check the box to enable the router to receive IPv6 multicast streams.
- Source Preference:

Enter the source preference in the field provided.
- Source Metric:

Enter the source metric to be used in the field provided.
- Candidate RP:

Check the box to allow this router to be a candidate rendezvous point (RP).
- Candidate Bootstrap Router:

Check the box to allow this router to be a candidate bootstrap router.
- Group Prefix:

To add a group prefix, click on an available prefix in the group prefix table. Check the box to activate the prefix rule, and enter the desired prefix in the field provided.

Click **OK** to save the current configuration. Click **Apply** to save the current configuration.

PIM-SM

Options

Enable

☐

Source Preference

1024

Source Metric

1024

Candidate RP

☒

Candidate Bootstrap Router

☒

Active

Prefix

☐

FF00::/128

N

FF00::/128

N

FF00::/128

N

FF00::/128

Total Num :

4

OK

Apply

Security

The Security tab allows you to configure your router’s firewall settings and enable features to protect your network from outside intrusions and malicious attacks.

Firewall

IP Filter

Click **Add** to add a new filtering rule.

Active: Check the box to activate the IP filter rule.

Source IP: Enter the source IP address to be filtered.

Source From Port: Enter the starting port on the source IP.

Source To Port: Enter the ending port on the source IP.

Destination IP: Enter the destination IP address to be filtered.

Destination From Port: Enter the starting port of the destination IP.

Destination To Port: Enter the ending port of the destination IP.

Protocol: Select the protocol for the IP filter rule.

Delete: Click the icon to delete the IP filtering rule.

Click **OK** to save the filtering rule. Click **Apply** to save the current configuration.



IPv6 Filter

Click **Add** to add a new filtering rule.

Active: Check the box to activate the IP filter rule.

Source IP: Enter the source IP address to be filtered.

Source Port: Enter the port for the source IP.

Destination IP: Enter the destination IP address to be filtered.

Destination Port: Enter the port on the destination IP.

Protocol: Select the protocol for the IP filter rule.

Delete: Click the icon to delete the IP filtering rule.

Click **OK** to save the current filtering rule. Click **Apply** to save the current configuration.

The screenshot shows the 'IPv6 Filter' configuration window. At the top, there are tabs for 'Firewall', 'IP Filter', 'IPv6 Filter', 'MAC Filter', 'DDOS', and 'Content Filter'. The 'IPv6 Filter' tab is selected. Below the tabs, there is a table with columns: '#', 'Active', 'Source IP', 'Source Port', 'Destination IP', 'Destination Port', and 'Protocol'. The table contains one row with the following values: '#1', a checked 'Active' box, empty 'Source IP' and 'Source Port' fields (with '0' in the 'Source Port' field), empty 'Destination IP' and 'Destination Port' fields (with '0' in the 'Destination Port' field), and 'TCP' in the 'Protocol' dropdown. To the right of the table, there are 'Add' and 'OK' buttons. Below the table, it says 'Total Num : 1'. At the bottom right, there is an 'Apply' button.

MAC Filter

The MAC filter lets you to allow or deny access to your wireless network based on a client's MAC address.

Click **Add** to add a new MAC filtering rule.

Blacklist/Whitelist: Select **Blacklist** to deny access to only the MAC addresses listed below. Select **Whitelist** to allow access to only the MAC addresses listed below.

Active: Check the box to activate the MAC filter rule.

Source MAC: Enter the MAC address of the machine or device which you wish to filter packets coming from.

Destination MAC: Enter the MAC address of the machine you wish to filter packets.

Day: Check the box for each day that you wish to activate the MAC filtering rule.

Start Time: Enter the starting time at which you wish to activate the MAC filtering rule each day.

End Time: Enter the ending time at which you wish to deactivate the MAC filtering rule each day.

Delete: Click the icon to delete this MAC filtering rule.

Click **OK** to add the current rule to the rules list. Click **Apply** to save the current configuration.

The screenshot shows the 'Firewall' configuration page with the 'MAC Filter' tab selected. Below the tab, there is a dropdown menu set to 'Blacklist/Whitelist' with 'Blacklist' selected. A table lists the configured rules. The first rule is active and has a source MAC address entered. The table includes columns for days of the week (Mon-Sun) and start/end times. At the bottom right, there are 'Add', 'OK', and 'Apply' buttons.

#	Active	Source MAC	Destination MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	
1	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	<input type="button" value="Delete"/>

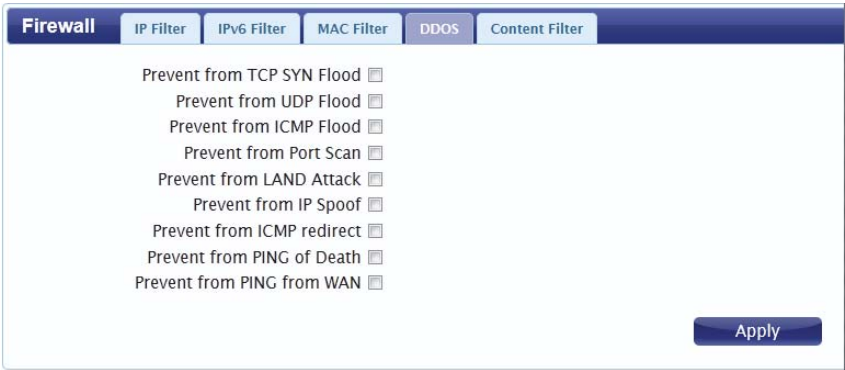
Total Num : 1

DDOS

This section allows you to enable various security features to protect against Denial of Service (DoS) attacks.

DoS Prevention Check the box next to the rule to enable prevention against **Filters:** that specific kind of DoS attack.

Click **Apply** to save the current configuration.



URL Filter

The content filter allows you to allow or deny access to specific URLs.

Enable URL Filter: Check the box to enable URL filtering.

Blacklist/Whitelist: Select **Blacklist** to deny access to only URLs listed in the rule table. Select **Whitelist** to allow access to only URLs listed in the rule list.

Active: Check the box to activate the URL filtering rule.

URL: Enter the URL that you wish to allow or deny access to. If you enter a domain name, all URLs under this domain will be allowed or denied access.

Delete: Click the icon to delete the rule.

Click **Add** to save the rule and add it to the rule table. Click **Apply** to save the current configuration.

The screenshot shows the 'Content Filter' configuration page under the 'Firewall' tab. The 'Enable URL Filter' checkbox is checked. Below it, the 'Blacklist/Whitelist' dropdown is set to 'Blacklist'. A table with one row shows a rule with 'Active' checked and an empty 'URL' field. The 'Total Num' is 1. 'Add', 'OK', and 'Apply' buttons are visible.

#	Active	URL
1	<input checked="" type="checkbox"/>	

Total Num : 1

Buttons: Add, OK, Apply

Application

This tab allows you to configure the router’s administrative functions, such as time & date, remote access, and firmware. You can also access the system log.

About

This tab shows the router’s basic information.

About

Device Name

DWR-730 Configuration Manager

FW Version

V2.00_CN

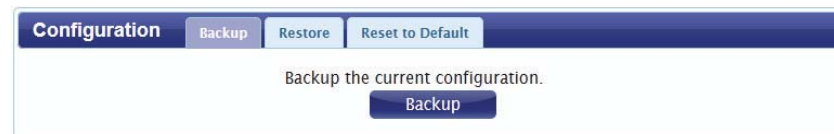
IMEI

355189036250928

Configuration

BACKUP

Click **Backup** to save the router's current configuration to a file on your computer. You will then be prompted with a "save file" dialogue, where you can choose where to save the configuration file.



RESTORE

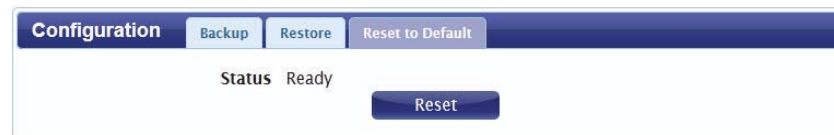
Click **Browse** to locate a previously saved configuration file on your computer. Once you have located the file, click **Restore** to configure the router according to the selected configuration file.



RESET TO DEFAULT

Click **Reset** to restore the router's settings to the factory defaults.

Important: All settings stored on the router will be lost following a factory reset.



Firmware Upgrade

You can upgrade the firmware of the router here. Make sure the firmware file you want to use is on the local hard drive of the computer. Please check your local D-Link support site or **<http://support.dlink.com>** for firmware updates and language packs.

Click **Browse** to locate a previously downloaded firmware file on your computer. Once the file has been located, click **Update** to carry out the firmware upgrade process.

A screenshot of a web-based firmware upgrade interface. It features a blue header bar with the text "Firmware Upgrade". Below the header, there is a "File name" label followed by a text input field and a "Browse..." button. Underneath, the "Status" is displayed as "Ready". In the bottom right corner, there is a blue "Update" button.

Firmware Upgrade	
File name	<input type="text"/> Browse...
Status	Ready
<div>Update</div>	

Important: All current settings will be restored to their factory defaults following a firmware upgrade.

Standby Mode

This section allows you to configure the router's automatic power-saving modes.

Enable Auto Power Saving: Check the box to enable the automatic power saving features.

Enter Standby Mode: Enter the number of minutes after which the router will enter standby mode if no activity is detected.

Enter Hibernate Mode: Enter the number of minutes after which the router will enter hibernate mode if no activity is detected.

Auto Power Off: Enter the number of minutes after which the router will shut down if no activity is detected.

Click **Apply** to save the current configuration.



The screenshot shows a configuration window titled "Standby Mode". It contains three settings: "Enable Auto Power Saving" with a checked checkbox, "Enter Standby Mode (minutes)" with a text box containing "5", and "Enter Hibernate Mode (minutes)" with a text box containing "5". Below these is "Auto Power Off (minutes)" with a text box containing "120". An "Apply" button is located at the bottom right of the window.

Standby Mode	
Enable Auto Power Saving	<input checked="" type="checkbox"/>
Enter Standby Mode (minutes)	5
Enter Hibernate Mode (minutes)	5
Auto Power Off (minutes)	120

Apply

Password

This page lets you change the configuration interface passwords for the Administrator (Admin) and User accounts.

Select the user to change password: Select whether you wish to change the password for the admin or user account from the drop down menu.

Old Password: Enter the existing password for this account.

New Password: Enter the new password for this account.

Retype New Password: Type the new password again to confirm.

Click **Apply** to save the current configuration.

A screenshot of a web-based configuration interface titled "Password". It contains a dropdown menu labeled "Select the user to change password" with "admin" selected. Below this are three text input fields labeled "Old password", "New password", and "Retype new password". An "Apply" button is located in the bottom right corner of the form area.

Password	
Select the user to change password	admin ▼
Old password	<input type="password"/>
New password	<input type="password"/>
Retype new password	<input type="password"/>
<input type="button" value="Apply"/>	

Date and Time

This page lets you set the time and date for your router, and also configure automatic time synchronization and daylight savings time.

DATE

Current System Time: Displays the current time and date according to the router's system clock.

Mode: Select **Manual** to manually set the time and date, or select **Get from Time Server** to have the router automatically synchronize the time with a Network Time Protocol (NTP) server.

New Time: If you selected Manual mode, enter the current time.

New Date: If you selected Manual mode, enter the current date.

Time Protocol: If you selected Get time From Server, select the desired time protocol from the drop-down menu.

Time Server Address 1-4: Enter up to four NTP server addresses which will be used to synchronize the router's system time and date.

Click **Apply** to save the current settings.

The screenshot shows the 'Date and Time' configuration page. The 'Date' tab is active. The 'Current System Time' is 'Mon Jun 10 15:45:41 2013'. The 'Mode' is set to 'Manual'. The 'New Time (hh:mm:ss)' is '15 : 45 : 41'. The 'New Date (mm-dd-yyyy)' is '6 / 10 / 2013'. There is an 'Apply' button at the bottom right.

The screenshot shows the 'Date and Time' configuration page. The 'Date' tab is active. The 'Current System Time' is 'Mon Jun 10 15:45:41 2013'. The 'Mode' is set to 'Get from Time Server'. The 'Time Protocol' is set to 'NTP (RFC-1305)'. There are four 'Time Server Address' fields, all containing '1.my.pool.ntp.org', '2.my.pool.ntp.org', '3.my.pool.ntp.org', and '4.my.pool.ntp.org' respectively. There is an 'Apply' button at the bottom right.

TIME ZONE

Time Zone: Select your time zone from the drop-down menu.

Enable Daylight Saving: Check the box to enable automatic adjustment for daylight saving.

Start Date: Enter the details of the starting date and time for daylight saving time in your region.

End Date: Enter the details of the ending date and time for daylight saving time in your region.

Click **Apply** to save the current settings.



The screenshot shows a configuration window titled "Date and Time" with two tabs: "Date" and "Time Zone". The "Time Zone" tab is active, displaying a dropdown menu for "Time Zone" set to "(GMT+08:00) Kuala Lumpur, Singapore". Below this is a checkbox for "Enable Daylight Saving" which is checked. The "Start Date" section has three dropdowns: "First", "Sunday", and "April", followed by a numeric input "2" and the text "o'clock". The "End Date" section has three dropdowns: "Last", "Sunday", and "October", followed by a numeric input "2" and the text "o'clock". An "Apply" button is located at the bottom right of the window.

Language

Language: Select your preferred language from the drop-down menu.

Click **Apply** to save the current configuration.

A screenshot of a web-based configuration interface for language settings. It features a blue header bar with the word "Language" in white. Below the header, the word "Language" is followed by a text input field containing "English" and a small downward-pointing arrow icon. To the right of the input field is a blue button with the word "Apply" in white.

Language English

System Log

The system log displays a record of all events which occur while the router is running.

LOG SETTING

Enable Log: Check the box to enable the router’s log-keeping function.

Click **Apply** to save the current configuration.

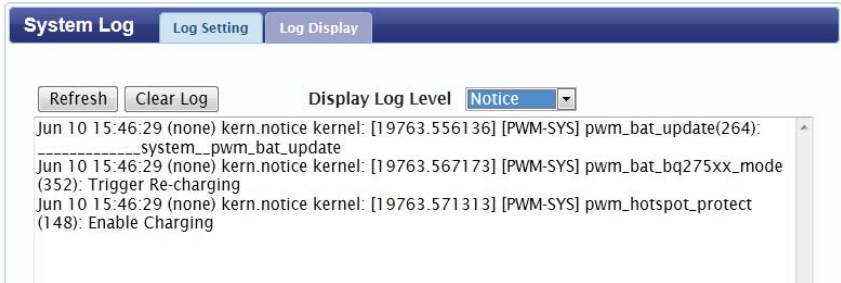


LOG DISPLAY

Refresh: Click to update the log display.

Clear Log: Click to clear all log entries.

Display Log Level: Select the level of log event which you wish to view from the drop-down menu.



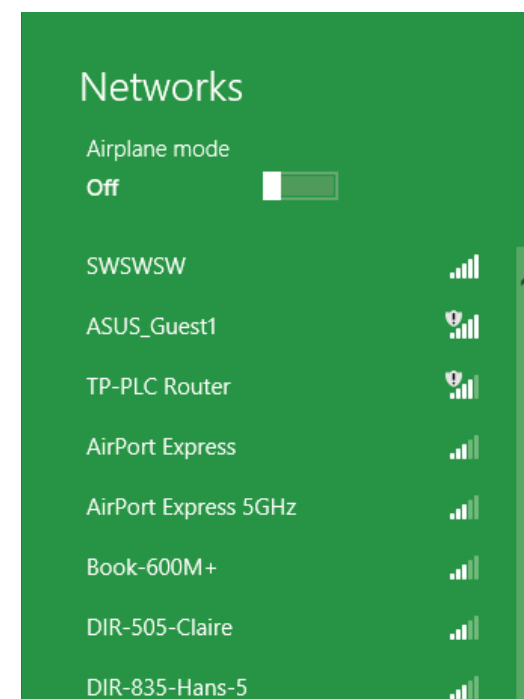
Connecting to a Wireless Network Using Windows 8

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

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

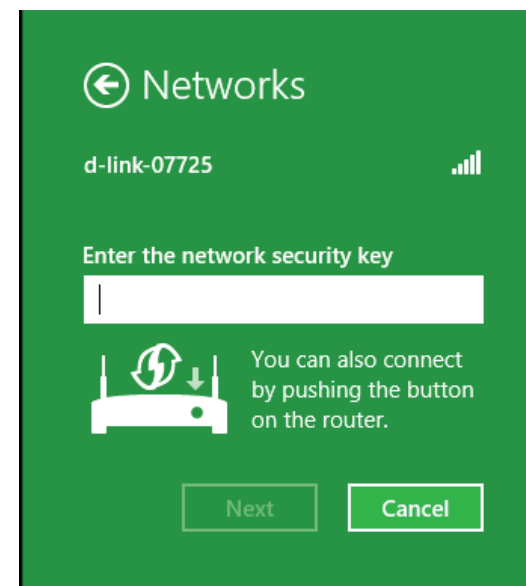


Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.

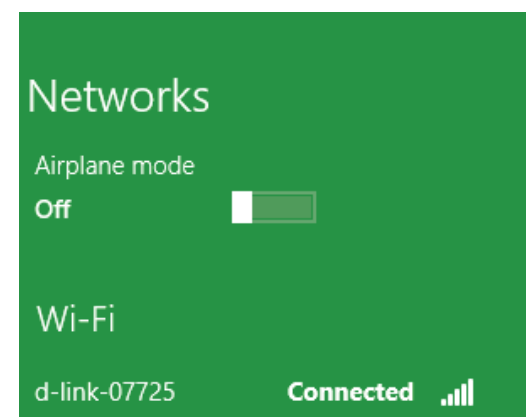


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click Next.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router at this point to enable the WPS function.



When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



Connecting to a Wireless Network Using Windows 7

Windows 7 users may use the built-in wireless utility to connect to a wireless network. 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 7 utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility. You can also click on the wireless icon in your system tray (lower-right corner).

The utility will display any available wireless networks in your area.



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

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to “Networking Basics” on page 90 for more information.



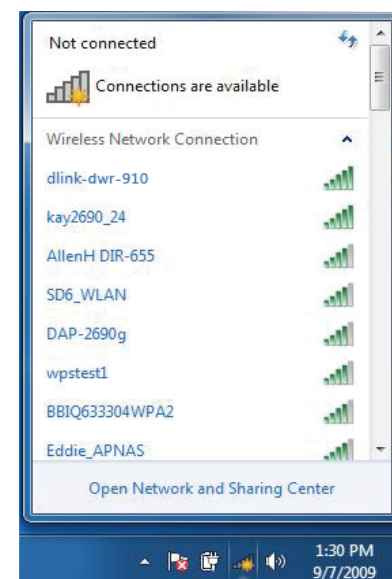
Configuring Wireless Security

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

1. Click on the wireless icon in your system tray (lower-right corner).



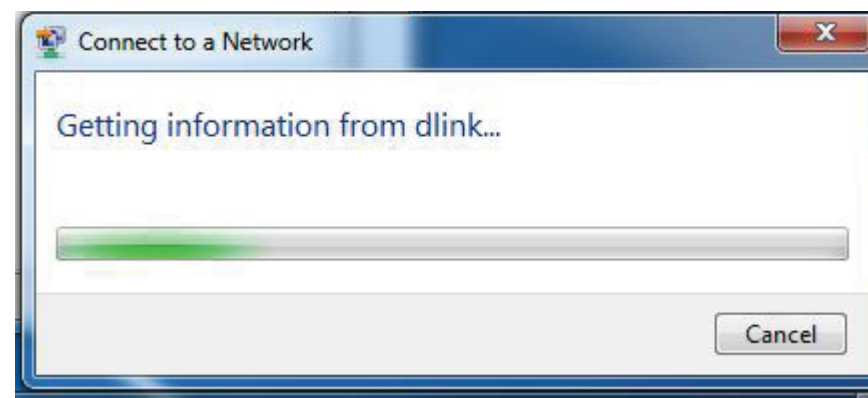
2. The utility will display any available wireless networks in your area.



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



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



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

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.



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 "Networking Basics" on page 90 for more information.



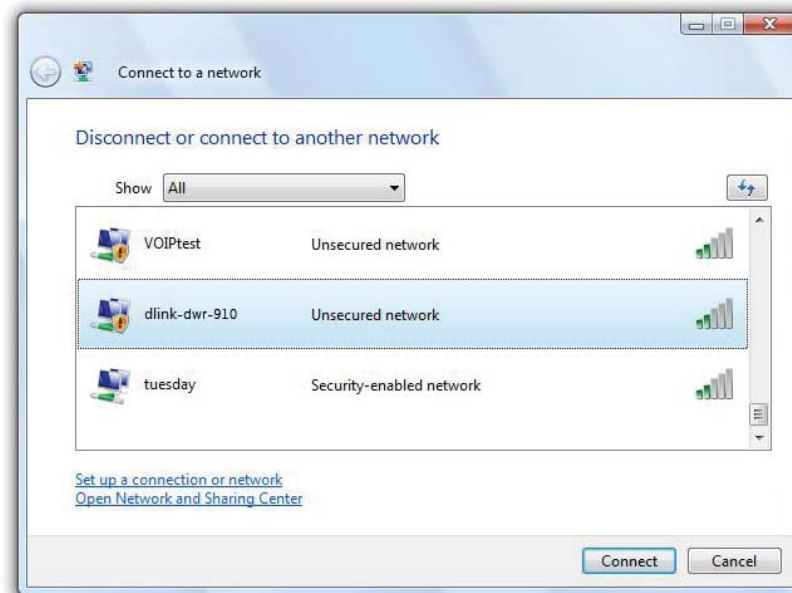
Configuring Wireless Security

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

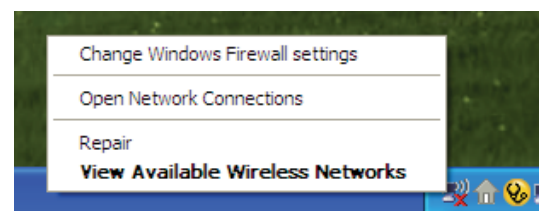
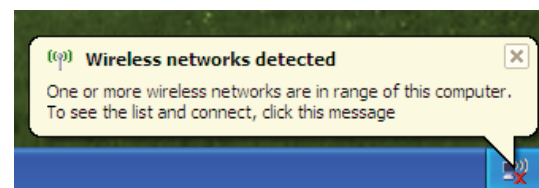
Using Windows® XP

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.

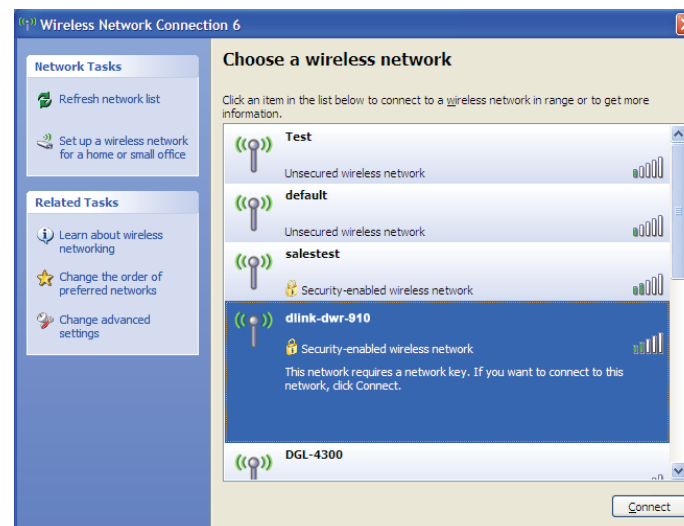
or

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.

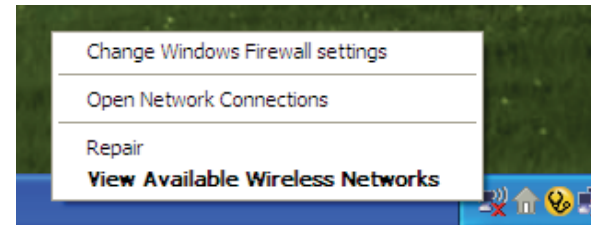
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Networking Basics" on page 90 for more information.



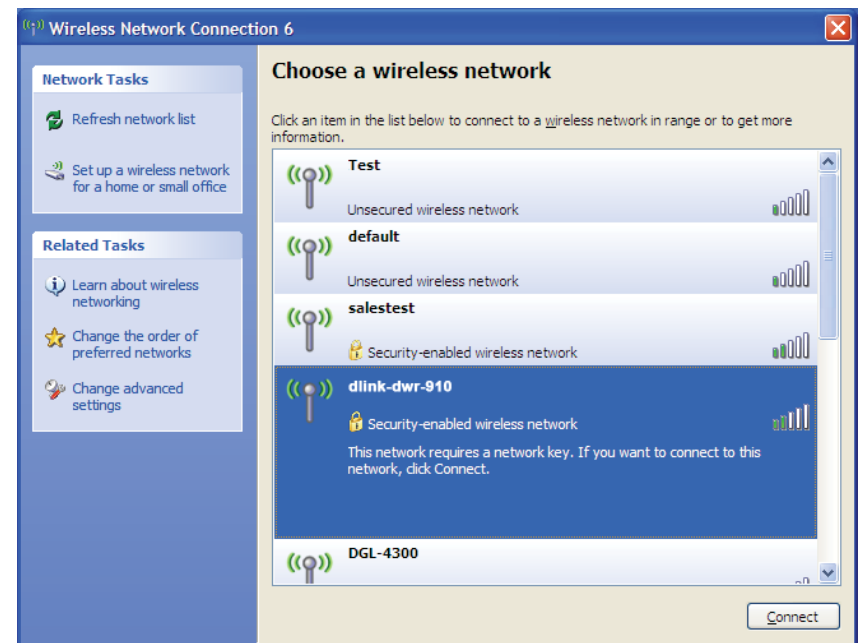
Configure WEP

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**.

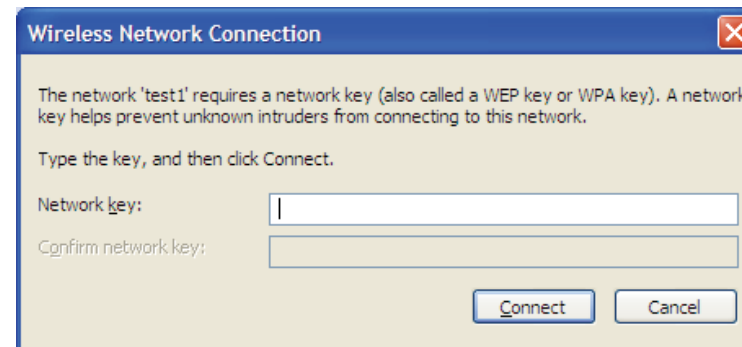


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

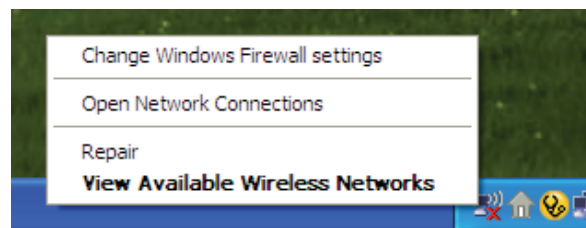
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



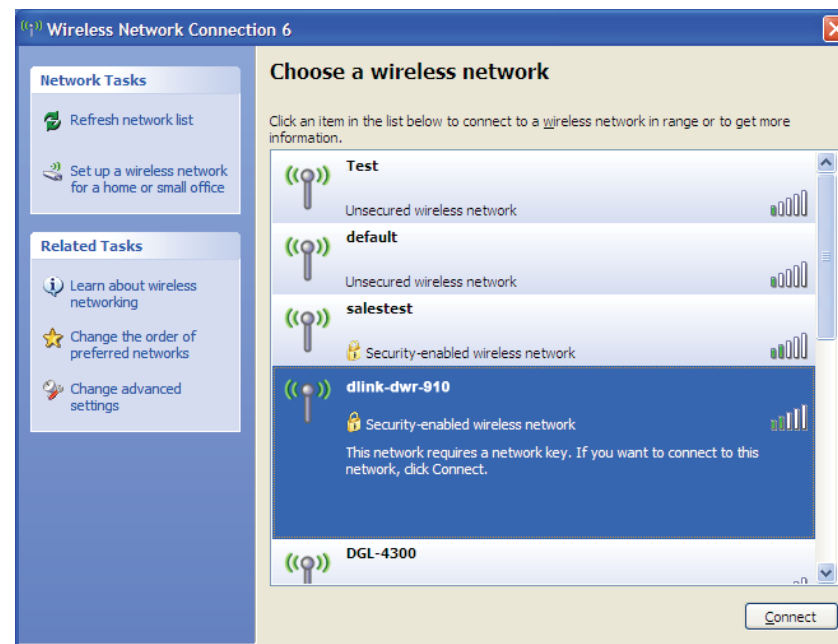
Configure WPA-PSK

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**.

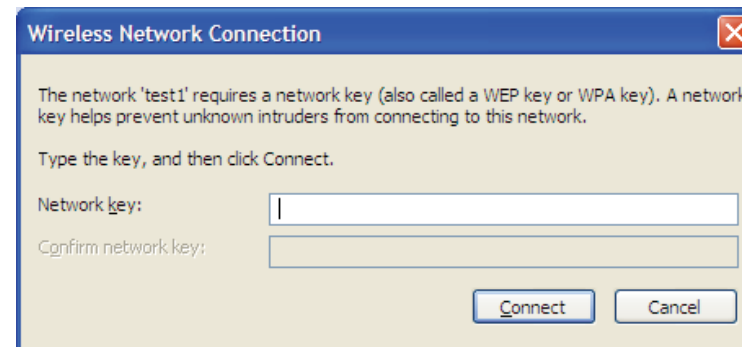


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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-830. Read the following descriptions if you are having problems.

1. Why can't I access the web-based configuration utility?

When entering the IP address of your 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.

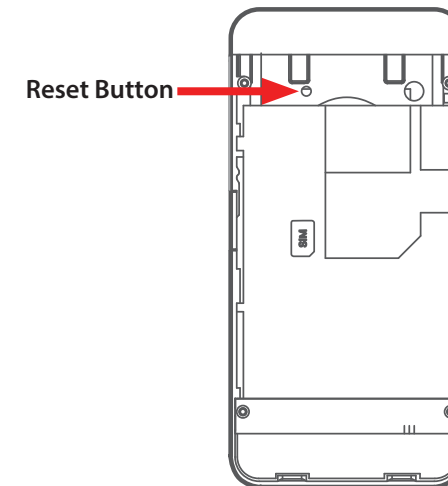
- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 8 or higher, Chrome 19.0, Firefox 12.0, or Safari 4.0.
- If attempting to connect wirelessly, ensure that the wireless icon on the OLED display is showing. Also, ensure that you are connected to the correct SSID for your mobile router.
- Make sure that the computer you are using is not connected to any other devices (such as routers or switches) which might have the same IP address as the DWR-830, as this may cause an IP address conflict. If you have a conflict, temporarily unplug any other devices from your computer while you configure the DWR-830. You can also change the IP address of the DWR-830 in the Network section of the configuration utility. Please refer to "Wi-Fi" on page 33 for further information on changing the IP address. You may also need to renew your computer's IP address configuration. To do this, start the Command utility: Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows Vista users type **cmd** in the **Start Search** box.) This will bring up a black screen with white text. At the command prompt, type **ipconfig /release** and wait for the process to be completed. Next, type **ipconfig /renew** which will renew your computer's IP address configuration.
- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, 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 **Default Level** 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 re-open it.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Please note that this process will change all your settings back to the factory defaults.

To reset the router, first remove the back cover of the router to expose the battery. Using a paperclip or similar object, press and hold the reset button, which is located inside the hole to the upper-left of the SIM card slot (see diagram). The DWR-830 will restore the factory default settings. Wait about 30 seconds for the router to restart before you attempt to reconnect to it. The default IP address is 192.168.0.1, and the default username is **admin** and the password should be left blank.



Networking Basics

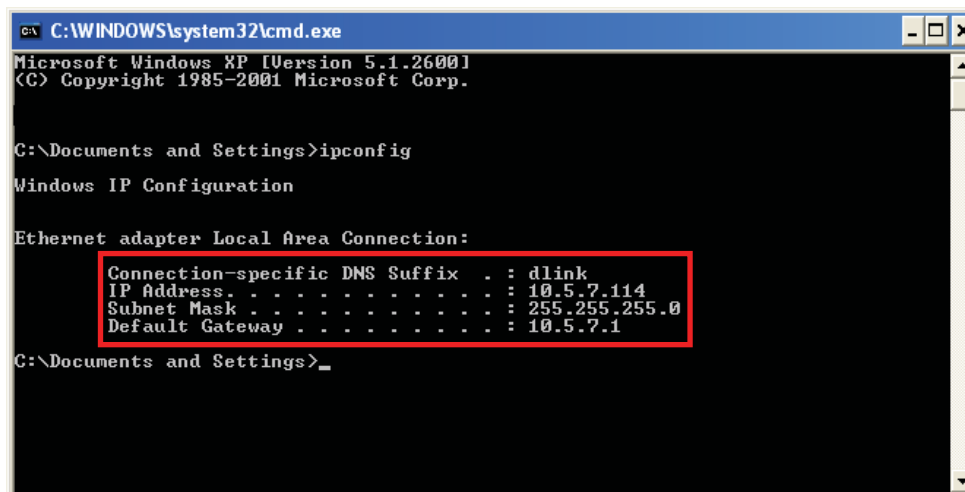
Check your IP address

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.



```
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>
```

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.

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® 8 Click on **Start > Control Panel > Network and Internet Connections > Network Connections > Configure your Internet Protocol (IP) settings.**

Windows® 7 Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**

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.**

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

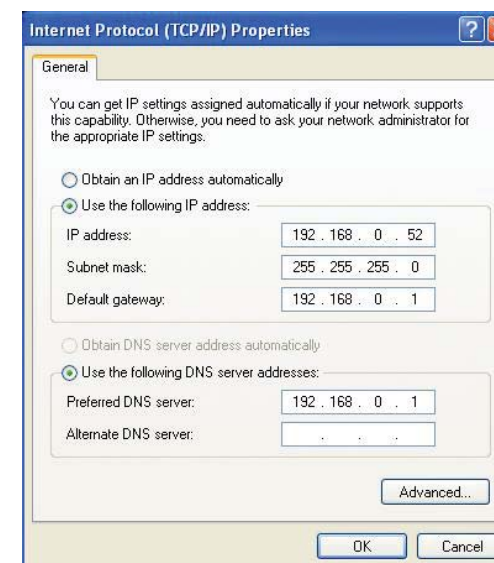
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

Radio Frequency Bands

- HSUPA/HSPDA/UMTS: 900/2100 MHz or 850/1900 MHz (Option)
- EDGE/GPRS/GSM: 850/900/1800/1900 MHz
- Power Class 3 (+23 dBm)

Cellular Access

- DC-HSPA+
 - Downlink: 42 Mbps
 - Uplink: 11 Mbps

Wi-Fi Access Point

- 802.11n (150 Mbps compatible)
- 802.11g (54 Mbps)
- 802.11b (11 Mbps)

Antenna

- One internal antenna

USB Interface

- micro USB port

USIM Slot

- Standard 6-pin SIM card interface

Status Indicators

- OLED display

Storage

- microSD card slot

Wireless Security

- 64/128-bit WEP (Wired Equivalent Privacy)
- WPA & WPA2 (Wi-Fi Protected Access)
- WAPI (WLAN Authentication and Privacy Infrastructure)

Firewall

- Network Address Translation (NAT)

Dimensions (L x W x H)

- 100.3 x 49.35 x 14.13 mm (3.95 x 1.94 x 0.56 inches)

Weight

- 90 g (3.17 ounces)

Operating Temperature

- -10 to 40 °C (14 to 104 °F)

Certifications

- FCC/CE

Warnings and Declarations

Specific Absorption Rate (SAR)

This mobile device is a radio transmitter and receiver. It is not designed to exceed the limits for exposure to radio waves recommended by international guidelines. These guidelines were developed by the independent scientific organization ICNIRP and include safety margins designed to assure the protection of all persons, regardless of age and health.

The guidelines use a unit of measurement known as the Specific Absorption Rate, or SAR.

The SAR limit for mobile devices is 2 W/kg and the highest SAR value for this device when tested complied with this limit.

To comply with radiofrequency radiation (RF) exposure guidelines during body worn operation, this device must be used with a minimum of 0.5 cm separation from the body.

Failure to observe these instructions could result in your RF exposure exceeding the relevant guideline limits.

1. CAUTION : RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

2. The product shall only be connected to a USB interface of version USB2.0

3. The adapter shall be installed near the equipment and shall be easily accessible.

Only can use adapter as below: Adapter brand name: AMIGO

Adapter model: AMS47-0501000FV

I/P:100-240V,50/60Hz,0.2A,O/P 5V,1.0A

The plug considered as disconnect device of adapter

4. The device could be used with a separation distance of 0.5cm to the human body.

The device complies with the essential requirements of Article 3 of the R&TTE 1999/5/EC Directive, if used for its intended use and that the following standards have been applied:

1. Health (Article 3.1(a) of the R&TTE Directive)

- EN62311 :2008/EN62209-2 :2010

- EN62479 :2010

2. Safety (Article 3.1(a) of the R&TTE Directive)

Applied Standard(s):

- EN 60950-1:2006+A11:2009+A1:2010+A12:2011

3. Electromagnetic compatibility (Article 3.1 (b) of the R&TTE Directive)

Applied Standard(s):

- EN 301 489-1 V1.9.2/-7 V1.3.1/-17 V2.2.1/-24 V1.5.1

4. Radio frequency spectrum usage (Article 3.2 of the R&TTE Directive)

Applied Standard(s):

- EN 301 511 V9.0.2

- EN 301908-1/-2 V5.2.1

- EN 300328 V1.8.1

All the reports of the applied standards have the Positive Opinion of Notified Body:

PHONEIX TESTLAB, Königswinkel 10 D-32825 Blomberg, Germany

Identification mark: **0700** (Notified Body) **C**

CE 0700

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.

RF Exposure Information (SAR)

This device meets the government's requirements for exposure to radio waves.

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

The exposure standard for wireless devices employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit set by the FCC is 1.6W/kg. *Tests for SAR are conducted using standard operating positions accepted by the FCC with the device transmitting at its highest certified power level in all tested frequency bands. Although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. This is because the device is designed to operate at multiple power levels so as to use only the power required to reach the network. In general, the closer you are to a wireless base station antenna, the lower the power output.

During SAR testing, this device is set to transmit at its highest certified power level in all tested frequency bands, and placed in positions that simulate RF exposure in usage near the body with the separation of 0.5cm. the highest SAR value as reported to the FCC is 0.86 W/kg

The FCC has granted an Equipment Authorization for this device with all reported SAR levels evaluated as in compliance with the FCC RF exposure guidelines. SAR information on this device is on file with the FCC and can be found under the Display Grant section of www.fcc.gov/oet/ea/fccid after searching on FCC ID: KA2WR830A1.

This device has been tested and meets the FCC RF exposure guidelines.