



User Manual

AC1200 Wi-Fi Router

DIR-822

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	DescRIPngtion
1.00	November 02, 2020	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.

Apple®, Apple logo®, Safari®, iPhone®, iPad®, iPod touch® and Macintosh® are trademarks of Apple Inc., registered in the U.S. and other countries. App Store™ is a service mark of Apple Inc.

Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.

Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

Copyright © 2020 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

Product Overview.....	1	Connected Clients	22
Package Contents.....	1	Settings	23
System Requirements	2	Wizard	23
Introduction	3	Internet.....	23
Features.....	4	WAN	23
Hardware Overview	5	VLAN.....	56
LED Indicators	5	DNS	58
Back Panel	6	WAN Failover	59
Installation	7	Wireless network.....	60
Before you Begin.....	7	Network.....	63
Wireless Installation Considerations.....	8	IPv4	63
Hardware Setup	9	IPv6	67
Completing Setup	12	Functions	69
Setup Wizard	13	Firewall	69
Router Mode.....	14	Wi-Fi	75
AP Mode.....	15	Client management	75
Repeater Mode	15	WPS.....	76
Client Mode.....	16	WMM	78
WISP Repeater Mode	16	Client	79
Mobile Internet Mode	17	Client Shaping.....	81
Advanced Settings	18	Additional 2.4 GHz.....	83
Default Settings.....	18	Additional 5 GHz	85
Configuration.....	19	MAC Filter	87
Home	20	Roaming.....	89
Internet.....	20	Advanced.....	91
DIR-822	21	UPnP IGD.....	91
		Remote Access.....	92

TR-069 Client	96	Tips.....	134
Static Route	98	Wireless Modes.....	135
Dynamic DNS	100	Networking Basics	136
IPsec.....	102	Check your IP address.....	136
Ports Settings	107	Statically Assign an IP address	137
Redirect	108	Technical Specifications	138
IGMP/MLD	109	Regulatory Statements	139
ALG/Passthrough	110		
Management.....	111		
System Time.....	111		
System Log	112		
Administration	113		
Telnet/SSH.....	114		
Yandex.DNS	115		
Firmware Update	117		
Schedule	118		
Statistics	120		
Network Statistics	120		
Port Statistics.....	121		
Routing	122		
DHCP	123		
Multicast Groups.....	124		
Diagnostics	125		
Ping.....	125		
Traceroute	126		
Troubleshooting	127		
Wireless Basics	131		
What is Wireless?	132		

Package Contents



DIR-822



Ethernet Cable



Power Adapter



Warranty Documents



Quick Installation Guide

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

Note: Using a power supply with a different voltage rating than the one included with the DIR-822 will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based cable or DSL modem • IEEE 802.11 ac/n/g/b/a wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	Computer with the following: • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter Browser Requirements: • Internet Explorer 10 or higher • Firefox 44 or higher • Safari 8 or higher • Chrome 48 or higher • Edge 20.10240 or higher Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

The D-Link DIR-822 is a wireless IEEE 802.11ac compliant device that delivers up to 3x faster speeds than 802.11n while staying backward compatible with 802.11n/g/b/a devices. This means you can connect the DIR-822 to a cable or DSL modem and provide high-speed Internet access to multiple computers, game consoles, and media players. You can create a protected wireless network to share photos, files, music, videos, printers, and network storage. Powered by 802.11ac technology and equipped with four external antennas, this router provides superior wireless coverage for larger homes and offices, or for users running bandwidth-intensive applications. The DIR-822 also includes a 4-port 10/100 Ethernet switch that connects to wired devices for uninterrupted video calling and faster file transfers.

The DIR-822 supports the latest wireless protection features to help prevent unauthorized access, be it from over a wireless network or the Internet. Support for WPA, WPA2 and WPA3 standards ensure that you will be able to use the best possible encryption regardless of your client devices. In addition, this router is equipped with a dual-active firewall (SPI and NAT) to prevent potential attacks over the Internet.

Features

- **Superior Wireless Networking** - The DIR-822 provides up to 300 Mbps wireless connection in 2.4 GHz band, and up to 867 Mbps¹ wireless connection in 5 GHz with other 802.11ac and 802.11n wireless clients. This capability rivals wired connections, allowing users to participate in real-time activities online, such as HD video communication, online gaming, and use mobile devices from anywhere in your home while still offering full 802.11n/g/b backward compatibility.
- **IPv6 Support** - The DIR-822 fully supports IPv6 and includes support for a variety of IPv6 connection types including: SLAAC/DHCPv6, Static IPv6, IPv6 PPPoE, IPv6 Dual Stack, and IPv6 LAN.
- **Advanced Firewall Features** - The web-based user interface displays a number of advanced network management features. Easily apply parental control based on MAC addresses and schedules.
- **Encrypted Multiple/Concurrent Sessions** - The DIR-822 can pass through VPN sessions. It supports multiple and concurrent IPsec and PPTP sessions, so users behind the DIR-822 can access corporate networks through encrypted channels.
- **User-friendly Setup Wizard** - Through its easy-to-use wizard, the DIR-822 lets you quickly switch itself to one of the following modes: router (for connection to a wired or wireless ISP), access point, repeater, or client, and then configure all needed setting for operation in the selected mode in several simple steps.

¹ Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11g, 802.11n and 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Hardware Overview

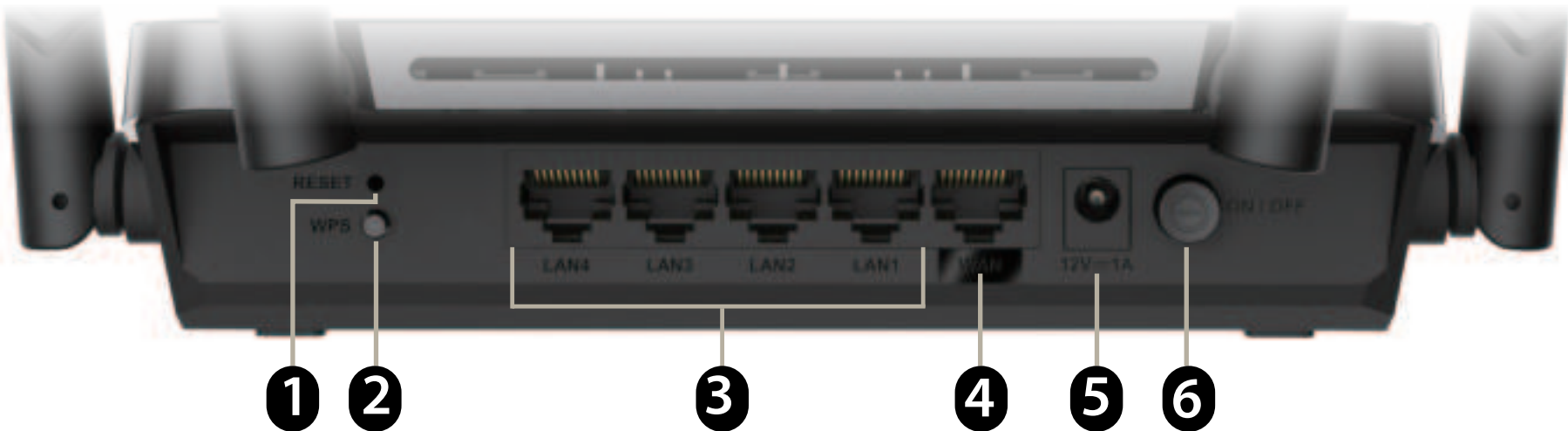
LED Indicators



1	Power LED	A solid light indicates a proper connection to the power supply.
2	Internet LED	A solid light indicates a cable is connected on the Internet port. If the LED is blinking fast, the device is loading. If the LED is blinking slow, a firmware update is in progress.
3	2.4 GHz Wireless LED	A solid light indicates the 2.4 GHz wireless band is enabled. If the light is blinking, data transmission is in progress.
4	5 GHz Wireless LED	A solid light indicates the 5 GHz wireless band is enabled. If the light is blinking, data transmission is in progress.

Hardware Overview

Back Panel



1	Reset Button	Insert a paperclip in the hole, wait for 10 seconds, and release to reset the router to default settings.
2	WPS Button	Press to start the WPS process and automatically create an encrypted connection to a WPS client. Press for several seconds to switch on/off Wi-Fi.
3	LAN Ports (1- 4)	Connect Ethernet devices such as computers, switches, storage (NAS) devices, and game consoles.
4	Internet Port	Using an Ethernet cable, connect your broadband modem to this port.
5	Power Connector	Connector for the supplied power adapter.
6	Power Button	Press the power button to power the device on or off.

Installation

This section will walk you through the installation of the DIR-822.

Before you Begin

- Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, attic, or garage.
- Configure the router with the computer that was last connected directly to your Internet connection. Verify that it is connected to the Internet before connecting additional devices.
- If your ISP provided you with a modem/router combo, you will need to set it to “bridge” mode so the router can work properly. Please contact your ISP or refer to the user manual for your modem/router device.
- If connecting to a DSL modem, make sure to have your DSL service information provided by your Internet Service Provider handy. This information is likely to include your DSL account's Username and Password. Your ISP may also supply you with additional WAN configuration settings which might be necessary to establish a connection.
- If you are connecting a considerable amount of networking equipment, it may be a good idea to take the time to label each cable or take a picture of your existing setup before making any changes.
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoET, BroadJump, or EnterNet 300 from your computer or you will not be able to connect to the Internet.

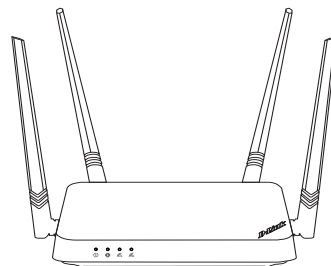
Wireless Installation Considerations

The D-Link wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

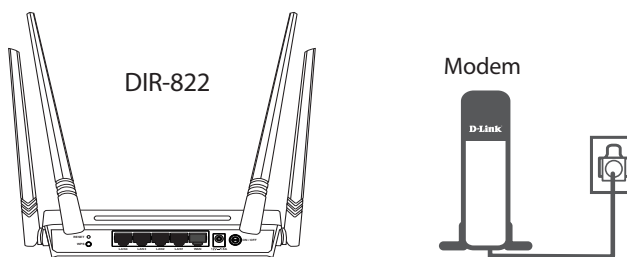
1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Hardware Setup

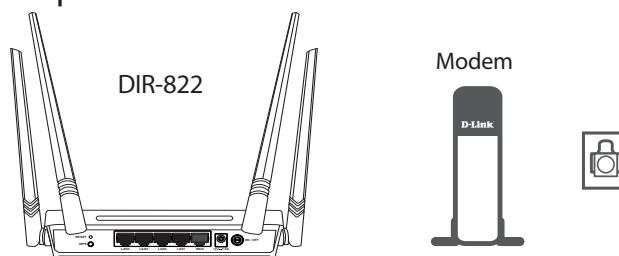
1. The DIR-822 is designed to give you the fastest, most stable network connection possible. In order to maximize performance, fully extend the antennas to provide optimal wireless coverage. Keep the router in an open area for better wireless coverage.



2. Position your DIR-822 near your Internet-connected modem. Place it in an open area for better wireless coverage.



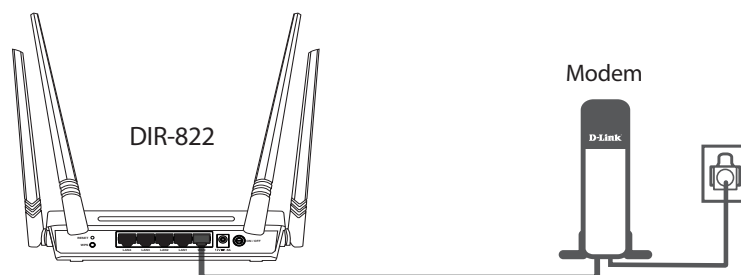
3. Turn off and unplug the power and Ethernet cable to your cable or DSL broadband modem. This is required. In some cases, you may need to turn it off for up to five minutes.



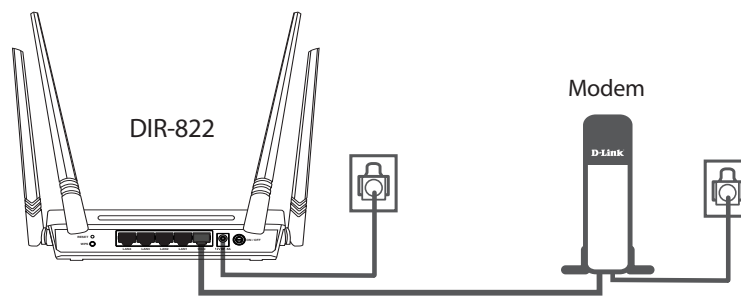
4. Use the included Ethernet cable to connect your modem to the yellow port labeled **INTERNET** on the router.



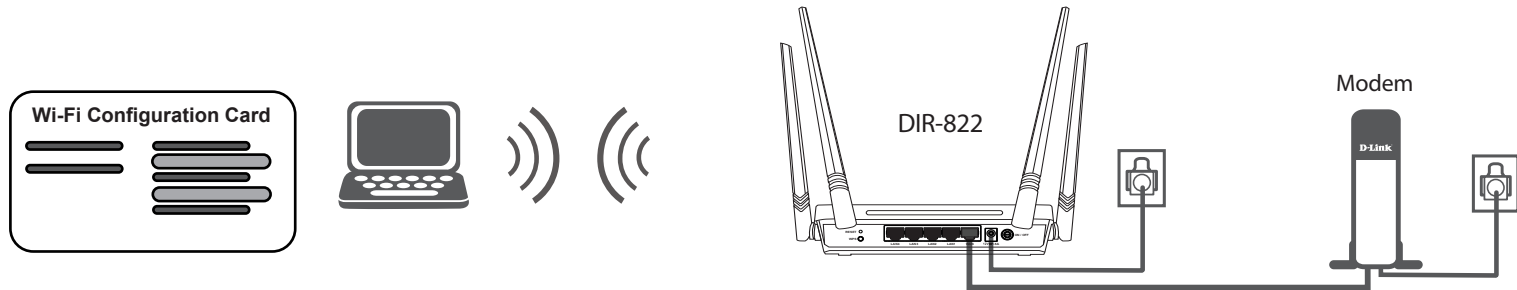
5. Turn on or plug your modem back in and wait approximately one minute before proceeding onward.



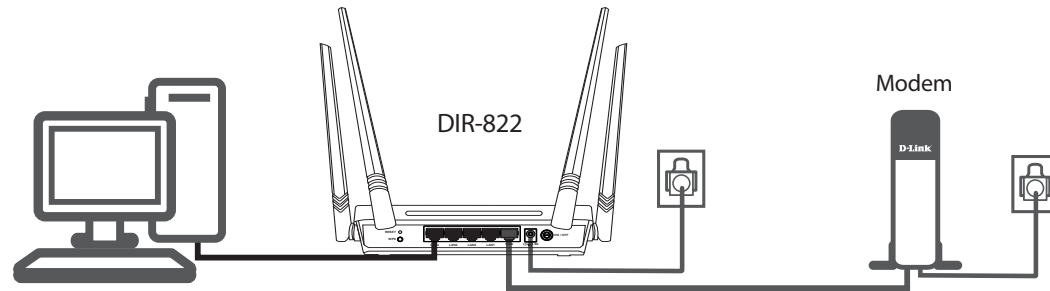
6. Connect the supplied power adapter to the router and a power outlet, press the power button, and wait approximately one minute until the Power LED indicator on the front of the device changes to solid blue.



7. **If you are configuring the DIR-822 wirelessly from a PC**, connect to a Wi-Fi network printed on the included Wi-Fi Configuration Card. You can also find the Wi-Fi network names and passwords printed on the label attached to the bottom your router.



If you are configuring the DIR-822 from a PC with a wired Ethernet connection, plug one end of an Ethernet cable into the port labeled 1 on the back of the router, and the other end into the Ethernet port on your computer.



8. Proceed to **Completing Setup** on page **12** in order to complete setup to connect to the Internet.

Completing Setup

There are several different ways you can configure your router to connect to the Internet and connect to your clients:

- **D-Link Setup Wizard** - This wizard will launch when you log into the router for the first time.
Refer to **Setup Wizard** on page **13**.
- **Manual Setup** - Log in to the router and manually configure your router.
Refer to **Configuration** on page **19**.

Setup Wizard

If this is your first time installing the router, open your web browser and enter **http://dlinkrouter.local/** in the address bar. Alternatively, enter the IP address of the router (default: **http://192.168.0.1**).

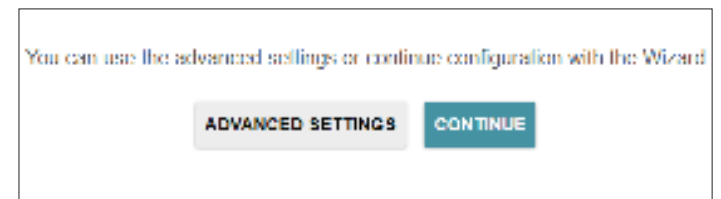
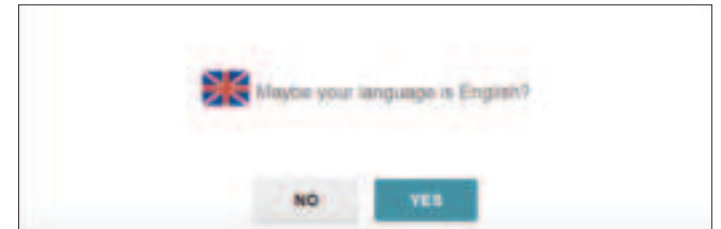
The wizard is designed to guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

Click **Start** to continue.



To start the full setup wizard, click **Continue** and see page 14.

To skip the wizard and directly configure the router from default DHCP WAN configuration, click **Advanced Settings**.



The DIR-822 can operate in six different modes:

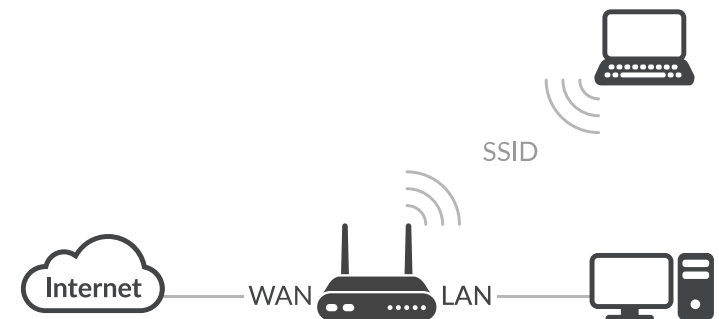
- Router Mode
- Access Point Mode
- Client Mode
- Repeater Mode
- WISP Repeater Mode
- Mobile Internet Mode



Router Mode

In Router Mode, the DIR-822 connects to your cable modem, DSL modem, or other Internet source and shares your Internet connection with your devices both wirelessly and over a wired LAN connection, providing Internet access for an entire home or office. Router Mode is suitable for most wired home Internet connections.

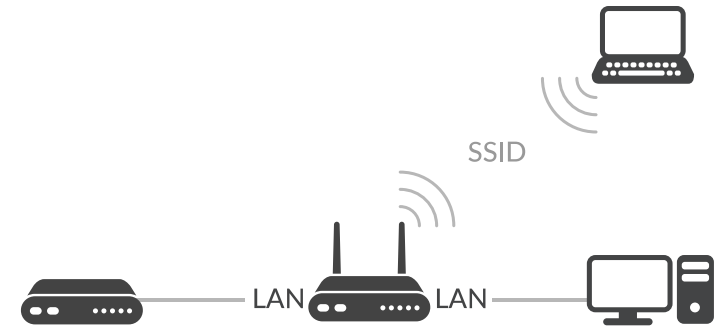
Follow the on-screen instructions to complete router mode setup.



AP Mode

In Access Point Mode, the DIR-822 connects your wireless devices together, but does not provide routing functionality. This can be useful if you already have an existing Internet router that does not have built-in wireless capabilities. You can also use this to create a private wireless network without Internet access so that your devices can connect to one another without being exposed to the Internet or other computers.

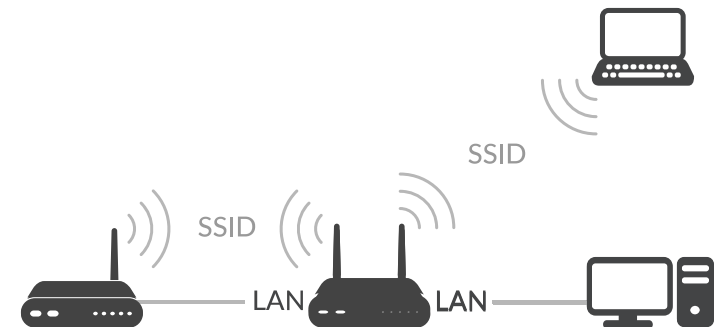
Follow the on-screen instructions to complete setup.



Repeater Mode

In Repeater Mode, the DIR-822 extends the range of an existing wireless network. You can use this to extend the coverage of an existing wireless router to provide better signal for parts of your home or office that may have poor reception. Additionally, you can use this mode to connect a wired device to a wireless network, which can be useful for devices that do not have a built-in wireless card, such as some smart TVs, game consoles, or DVRs.

Follow the on-screen instructions to complete setup.



Client Mode

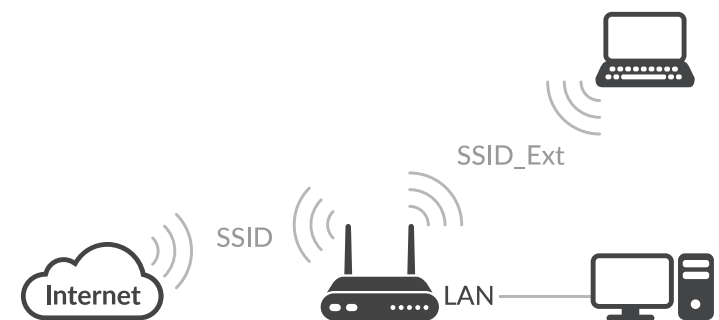
In client mode, the DIR-822 connects to a wireless hotspot or existing wireless network and lets you share access to that network with your devices, much like a wireless bridge. This mode is similar to Router mode, but instead of connecting to a cable or DSL modem as your Internet source, the DIR-822 connects to a Wi-Fi hotspot and shares that connection with your devices. You can use this mode to connect one or several wired devices to a wireless network, which can be useful for devices that do not have a built-in wireless card, such as some smart TVs, game consoles, or DVRs. Additionally, it can provide an added layer of isolation when connecting to public hotspots by hiding your computers and devices from other devices on the network, and keeping them in your own private network.



Follow the on-screen instructions to complete setup.

WISP Repeater Mode

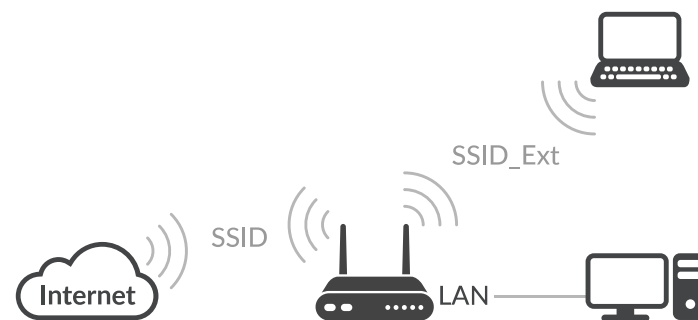
In WISP mode, the DIR-822 can be used as a gateway for a Wireless Internet Service Provider's (WISP) Wi-Fi-compatible network. This allows you to extend your provider's Internet access to every corner of your home. Alternatively, this mode can be used to extend an existing wireless network while keeping your LAN behind a NAT firewall. This mode is similar to the Router mode, but instead of connecting to a cable or DSL modem as your Internet source, the DIR-822 connects to the ISP's Wi-Fi network and shares that connection with your devices. Additionally, it can provide an added layer of isolation when connecting to a public network by hiding your computers and devices from other devices on the network, and keeping them in your own private network.



Follow the on-screen instructions to complete setup.

Mobile Internet Mode

In Mobile Internet mode you can configure a 3G/LTE WAN connection, set your own settings for the wireless network in the 2.4 GHz and 5 GHz bands, and set your own password for access to the web-based interface of the device. In order to connect your device to a wireless ISP (WISP), on the Device mode page, from the Connection method list, select the Wi-Fi value. Then from the Work mode list select the WISP Repeater value. In this mode you can connect your device to another access point, configure a WAN connection, set your own settings for the wireless network in the 2.4 GHz and 5 GHz bands, and set your own password for access to the web-based interface of the device.



Follow the on-screen instructions to complete setup.

Advanced Settings

Default Settings

These settings allow advanced users to quickly setup the router with a default IPv4 DHCP WAN and a simple SSID. Once configured, the user is taken directly to the full UI and can configure the router according to **Configuration** on page 19.

Defaults

- User's interface Password:

Enter a new password for the administrator account. You will need to enter this password whenever you configure the router using a web browser.
- Password Confirmation:

Confirm your new password for the administrator account.
- Network name 2.4 GHz (SSID):

Create a name for your 2.4 GHz wireless network using up to 32 characters.
- Network name 5 GHz (SSID):

Create a name for your 5 GHz wireless network using up to 32 characters.

Click **Apply** to proceed to the router according to **Configuration** on page 19.



Configuration

To access the configuration utility, open a web-browser such as Internet Explorer and enter **http://dlinkrouter.local/** or you may also connect by typing the IP address of the router (by default this is **http://192.168.0.1**) in the address bar.

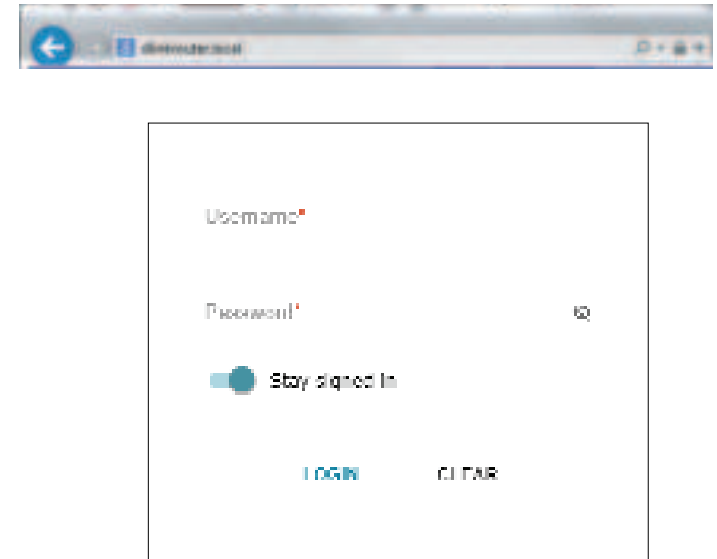
If you have already followed the setup wizard or changed the default settings, the login page opens. Enter the username (default username is: **admin**) and the admin password you entered during the wizard. Click **Login** to proceed.

Note: If you cannot remember your password and cannot log in, press the reset button on the bottom of the device for longer than 10 seconds to restore the router to its default settings.

The router's home page will open displaying its current connection status.

The navigation bar at the top of the page has quick access to Settings and Management functions. You may quickly jump back to the Home page at any time.

Note: The system will automatically log out after a period of inactivity. In order to not be logged out, switch the Stay signed in option in the login screen.

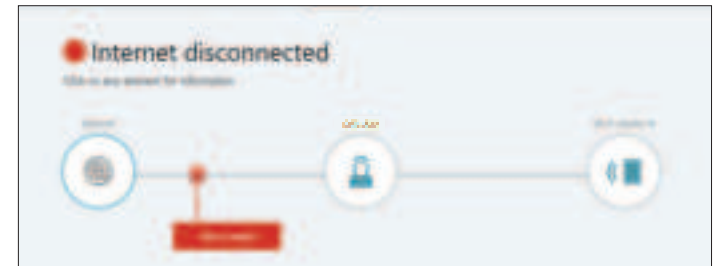
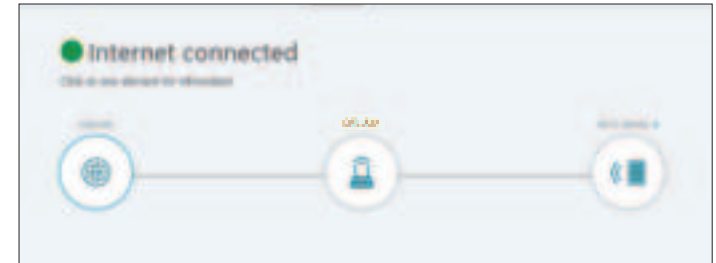


Home

The Home page displays the current status of the router in the form of an interactive diagram. You can click each icon at the bottom of the screen to display information about each part of the network. The menu bar at the top of the page will allow you to quickly navigate to other pages.

The Home page displays whether or not the router is currently connected to the Internet. If it is disconnected, click on repair to go to the Internet - WAN Configuration page to change your Internet configuration and reconnect to the Internet.

To reconfigure the Internet settings, click on **Edit** or **Change Configuration**. For more information refer to **Internet** on page 23.



Internet

To bring up more details about your Internet connection, click on the **Internet** icon. Click **IPv4** or **IPv6** to see details of the IPv4 connection and IPv6 connection respectively.

To reconfigure the Internet settings, refer to **Internet** on page 23.



DIR-822

Click on the **DIR-822** icon to view details about the router and its wireless settings.

Here you can see the router's current Wi-Fi network name and password, as well as the router's MAC address, IPv4 address, and IPv6 address.

To reconfigure the network settings, either click **Go to settings** on the lower left, or click on **Settings** in the navigation bar and then **Network** on the menu that appears. Refer to **Network** on page 63 for more information.

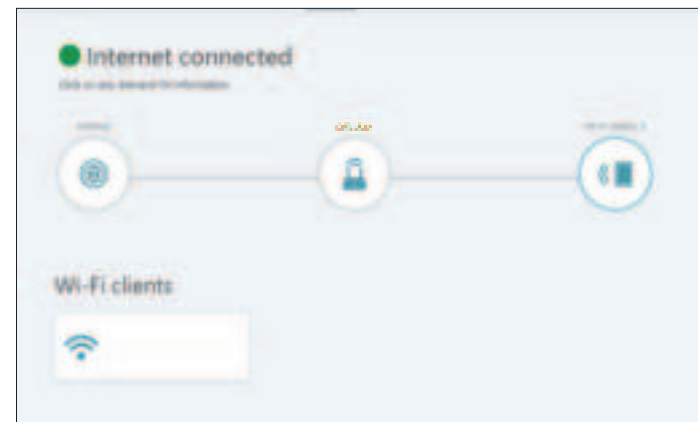
To reconfigure the wireless settings, either click **Go to settings**, on the lower right, or click **Settings** in the navigation bar and then **Wireless** on the menu that appears. Refer to **Wireless network** on page 60 for more information.



Connected Clients

Click on the **Connected Clients** icon to view details about wireless clients connected to the router.

On this page you can see all the clients currently connected to the router. Such devices are marked by the colored Wi-Fi logo.



Settings Wizard

In the Settings menu on the bar on the top of the page, click **Wizard** to open the setup wizard. This is the same wizard that appears when you start the router for the first time. Refer to **Setup Wizard** on page **13** for details. Note that activating the wizard will reset the router to factory defaults.

Internet

In the Settings menu on the bar on the top of the page, click **Internet** to see the Internet configuration options.

WAN

The **WAN** contains information about your current Internet connection settings.

Edit: Click here to be taken to **WAN/AddingWAN/Adding** on page **24**. Note that edit allows editing of connection specific settings and does not allow you to change the connection type. Edit allows you to change settings without losing your current active connection.

Reconnect: Click here to re-initialize the active WAN connection.

Change Configuration: Click here to be taken to **WAN/AddingWAN/Adding** on page **24**. Note that **Change Configuration** will allow you to change your connection type and may disrupt active connections.

Advanced Mode: Click here to see a list of Internet WAN connections and their status. You can add, delete or re-initialize a connection.



WAN/Adding

This section allows you to configure your WAN interface in detail.

Under **General Settings**, you will see the following:

Connection Type: Select your connection type from drop-down menu:

For **Dynamic IPv4** refer to page **25**.

For **Static IPv4** refer to page **27**.

For **Dynamic IPv6** refer to page **29**.

For **Static IPv6** refer to page **31**.

For **PPPoE** refer to page **33**.

For **PPPoE IPv6** refer to page **37**.

For **PPPoE Dual Stack** refer to page **41**.

For **PPTP** refer to page **45**.

For **L2TP** refer to page **48**.

For **Mobile Internet** refer to page **60**.

Note: this option can only be edited in the **WAN/Adding** mode.

Click **Apply** when you are done.

Dynamic IPv4

Select **Dynamic IPv4** to obtain IPv4 address information automatically from your Internet Service Provider (ISP).

General Settings

Connection Type: Select your connection type.

Interface: Select your connection interface.

Connection Name: Enter name for your connection.

Enable Toggle this switch to enable the connection. This is enabled by default.

Connection: Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

RIPng: Toggle this switch to enable Routing Information Protocol (RIPng). This setting is disabled by default.

ARP Proxy: Toggle this switch to enable ARP Proxy. This setting is disabled by default.

[illegible]

Dynamic IPv4 (cont)

Ethernet

MAC address: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can edit that address manually here.

Clone MAC address of your NIC: Toggle this switch to clone the MAC address of the device you are using to access the web UI. Note that no two MAC address within the same subnet can be the same.

Restore Default MAC Address: Click here to restore your router's default MAC address.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1500.

IPv4

Obtain DNS server addresses automatically: Toggle this switch to enable DNS information to be acquired automatically through DHCP. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Vendor ID: Specify a custom vendor ID. (Optional)

Hostname: Specify a hostname here. This will be the name of your router when viewed from networking tools.

Click **Apply** when you are done.

Static IPv4

Select **Static IP** if your IP information is provided by your Internet Service Provider (ISP). Choose Basic configuration or All Settings.

General Settings

Connection Type: Select your connection type.

Interface: Select your connection interface.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

RIPng: Toggle this switch to enable Routing Information Protocol (RIPng). This setting is disabled by default.

ARP Proxy: Toggle this switch to enable ARP Proxy. This setting is disabled by default.

The screenshot displays the configuration interface for Static IPv4. It is divided into two main sections: 'General Settings' and 'IPv4'.
 In the 'General Settings' section, there are dropdown menus for 'Connection type' (set to 'Static IPv4') and 'Interface' (set to 'WAN'). Below these is a 'Connection name' field. A series of toggle switches are shown: 'Enable connection' (checked), 'NAT' (checked), 'Ping' (unchecked), 'ARP' (unchecked), and 'ARP Proxy' (unchecked).
 The 'IPv4' section contains fields for 'IP address', 'Subnet mask', 'Gateway IP address', 'Primary DNS', and 'Secondary DNS'. A note below these fields states: 'If the connection is connected to the Internet, you can enable the following: IPv4 address (1 to 255), Subnet mask (255.255.255.0 to 255.0.0.0), Gateway IP address (1 to 255), Primary DNS (1 to 255), Secondary DNS (1 to 255)'.
 At the bottom, there is an 'Ethernet' section with a 'MAC address' field (showing '00:0B:73:FE:00:04') and a toggle for 'Clone MAC address of peer MAC' (checked, showing '0C:40:8D:8F:C3:21').

Static IPv4 (cont)

Ethernet

MAC address: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can edit that address manually here.

Clone MAC address of your NIC: Toggle this switch to clone the MAC address of the device you are using to access the web UI. Note that no two MAC address within the same subnet can be the same.

Restore Default MAC Address: Click here to restore your router's default MAC address.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1500.

IPv4

IP address: Specify the IP address provided by your ISP.

Netmask: Specify the subnet mask provided by your ISP.

Gateway IP address: Specify the default gateway address provided by your ISP.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP.

Click **Apply** when you are done.

Dynamic IPv6

Select **Dynamic IPv6** to obtain IPv6 address information automatically from your Internet Service Provider (ISP).

General Settings

Connection Type: Select your connection type.

Interface: Select your connection interface.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

RIPng: Toggle this switch to enable Routing Information Protocol (RIP) for IPv6. This setting is disabled by default.

ARP Proxy: Toggle this switch to enable ARP Proxy. This setting is disabled by default.



Dynamic IPv6 (cont)

Ethernet

MAC address: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can edit that address manually here.

Clone MAC address of your NIC: Toggle this switch to clone the MAC address of the device you are using to access the web UI. Note that no two MAC address within the same subnet can be the same.

Restore Default MAC Address: Click here to restore your router's default MAC address.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1500.

IPv6

Get IPv6: Choose **Automatically, IPv6 by DHCPv6** or **by SLAAC** according to the type of IPv6 is used by your ISP. The default setting is Automatically.

Enable prefix delegation: Enable prefix delegation. This setting is enabled by default.

Obtain DNS server addresses automatically: Obtain DNS server addresses automatically. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Click **Apply** when you are done.

Static IPv6

Select **Static IP** if your IPv6 information is provided by your Internet Service Provider (ISP).

General Settings

Connection Type: Select your connection type.

Interface: Select your connection interface.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

RIPng: Toggle this switch to enable Routing Information Protocol (RIP) for IPv6. This setting is disabled by default.

ARP Proxy: Toggle this switch to enable ARP Proxy. This setting is disabled by default.

The screenshot shows the configuration interface for Static IPv6. It includes fields for connection type, interface, connection name, and various protocol toggles (Enable connection, Ping, RIPng, ARP Proxy). It also features an Ethernet section with a MAC address field and a clone MAC address option, and an MTU field at the bottom.

Static IPv6 (cont)

Ethernet

MAC address: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can edit that address manually here.

Clone MAC address of your NIC: Toggle this switch to clone the MAC address of the device you are using to access the web UI. Note that no two MAC address within the same subnet can be the same.

Restore Default MAC Address: Click here to restore your router's default MAC address.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1500.

IPv6

IPv6 address: Specify the IPv6 address provided by your ISP.

Prefix: Specify the prefix provided by your ISP.

Gateway IPv6 address: Specify the default gateway address provided by your ISP.

Primary IPv6 DNS server: Specify the primary DNS server IP address assigned by your ISP.

Secondary IPv6 DNS server: Specify the secondary DNS server IP address assigned by your ISP.

Click **Apply** when you are done.

PPPoE

Select **PPPoE** if your ISP provides and requires you to enter a PPPoE username and password in order to connect to the Internet.

General Settings

Connection Type: Select your connection type.

Interface: Select your connection interface.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

RIPng: Toggle this switch to enable Routing Information Protocol (RIPng). This setting is disabled by default.

ARP Proxy: Toggle this switch to enable ARP Proxy. This setting is disabled by default.

The screenshot displays the 'General Settings' and 'PPP' configuration sections of the D-Link DIR-822 web interface. In the 'General Settings' section, 'Connection Type' is set to 'PPPoE', 'Interface' is 'Ethernet', and 'Connection Name' is 'internet_12'. The 'Enable connection' switch is turned on. In the 'PPP' section, 'Authentication' is set to 'Without authentication', 'Username' and 'Password' fields are present, and 'Encryption' is set to 'No encryption'. The 'Dial on demand' switch is also turned on. Other visible settings include 'NAT' (enabled), 'Ping' (disabled), 'RIPng' (disabled), and 'ARP Proxy' (disabled).

PPPoE (cont)

Ethernet

MAC address: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can edit that address manually here.

Clone MAC address of your NIC: Toggle this switch to clone the MAC address of the device you are using to access the web UI. Note that no two MAC address within the same subnet can be the same.

Restore Default MAC Address: Click here to restore your router's default MAC address.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1500.

PPP

Without authorization: Enable this setting to connect without a username and password. This configuration is uncommon and is disabled by default.

Username: If **Without authorization** is disabled, specify the PPP username provided by your ISP.

Password: If **Without authorization** is disabled, specify the PPP password provided by your ISP.

Service name: Specify the ISP service name (optional).

PPPoE (cont)

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1492.

Encryption protocol: Choose from **No encryption**, **MPPE 40 128 bit**, **MPPE 40 bit**, or **MPPE 128 bit**. **No encryption** is selected by default.

Authentication protocol: Choose from **AUTO**, **PAP**, **CHAP**, **MS-CHAP**, or **MS-CHAPv2**. **AUTO** is selected by default.

Keep alive: Toggle this switch to maintain your connection when no activity is detected.

LCP interval: If you have enabled **Keep alive**, specify the LCP Echo frequency in seconds. The default setting is 30.

LCP fails: If you have enabled **Keep alive**, specify the maximum number of LCP fails before the connection is dropped.

Dial on demand: Enable this option to automatically dial a PPPoE connection when data flow is detected.

Maximum idle time: If you have enabled **Dial on demand**, specify a maximum idle time in seconds before the connection will be dropped.

Extra options: Specify extra options if required by your ISP.

Static IP address: Specify the IP address provided by your ISP.

PPP debug: Toggle this switch to enable PPP debug, this setting is disabled by default.

PPPoE (cont)

IPv4

Obtain DNS server addresses automatically: Toggle this switch to enable DNS information to be acquired automatically through DHCP. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

PPPoE IPv6 (cont)

Ethernet

MAC address: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can edit that address manually here.

Clone MAC address of your NIC: Toggle this switch to clone the MAC address of the device you are using to access the web UI. Note that no two MAC address within the same subnet can be the same.

Restore Default MAC Address: Click here to restore your router's default MAC address.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1500.

PPP

Without authorization: Enable this setting to connect without a username and password. This configuration is uncommon and is disabled by default.

Username: If **Without authorization** is disabled, specify the PPP username provided by your ISP.

Password: If **Without authorization** is disabled, specify the PPP password provided by your ISP.

Service name: Specify the ISP service name (optional).

PPPoE IPv6 (cont)

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1492.

Encryption protocol: Choose from **No encryption**, **MPPE 40 128 bit**, **MPPE 40 bit**, or **MPPE 128 bit**. **No encryption** is selected by default.

Authentication protocol: Choose from **AUTO**, **PAP**, **CHAP**, **MS-CHAP**, or **MS-CHAPv2**. **AUTO** is selected by default.

Keep alive: Toggle this switch to maintain your connection when no activity is detected.

LCP interval: If you have enabled **Keep alive**, specify the LCP Echo frequency in seconds. The default setting is 30.

LCP fails: If you have enabled **Keep alive**, specify the maximum number of LCP fails before the connection is dropped.

Dial on demand: Enable this option to automatically dial a PPPoE connection when data flow is detected.

Maximum idle time: If you have enabled **Dial on demand**, specify a maximum idle time in seconds before the connection will be dropped.

Extra options: Specify extra options if required by your ISP.

Static IP address: Specify the IP address provided by your ISP.

PPP debug: Toggle this switch to enable PPP debug, this setting is disabled by default.

PPPoE IPv6 (cont)

IPv6

Get IPv6: Choose **Automatically, IPv6 by DHCPv6** or **by SLAAC** according to the type of IPv6 is used by your ISP. The default setting is Automatically.

Enable prefix delegation: Enable prefix delegation. This setting is enabled by default.

Obtain DNS server addresses automatically: Obtain DNS server addresses automatically. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Click **Apply** when you are done.

PPPoE Dual Stack

Select **PPPoE Dual Stack** if your ISP provides and requires you to enter a PPPoE username and password in order to connect to the Internet and supports adding IPv6 access to PPP for IPv4.

General Settings

Connection Type: Select your connection type.

Interface: Select your connection interface.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

RIPng: Toggle this switch to enable Routing Information Protocol (RIPng). This setting is disabled by default.

RIPngg: Toggle this switch to enable Routing Information Protocol (RIPng) for IPv6. This setting is disabled by default.

ARP Proxy: Toggle this switch to enable ARP Proxy. This setting is disabled by default.

[illegible]

PPPoE Dual Stack (cont)

Ethernet

MAC address: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can edit that address manually here.

Clone MAC address of your NIC: Toggle this switch to clone the MAC address of the device you are using to access the web UI. Note that no two MAC address within the same subnet can be the same.

Restore Default MAC Address: Click here to restore your router's default MAC address.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1500.

PPP

Without authorization: Enable this setting to connect without a username and password. This configuration is uncommon and is disabled by default.

Username: If **Without authorization** is disabled, specify the PPP username provided by your ISP.

Password: If **Without authorization** is disabled, specify the PPP password provided by your ISP.

Service name: Specify the ISP service name (optional).

PPPoE Dual Stack (cont)

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1492.

Encryption protocol: Choose from **No encryption**, **MPPE 40 128 bit**, **MPPE 40 bit**, or **MPPE 128 bit**. **No encryption** is selected by default.

Authentication protocol: Choose from **AUTO**, **PAP**, **CHAP**, **MS-CHAP**, or **MS-CHAPv2**. **AUTO** is selected by default.

Keep alive: Toggle this switch to maintain your connection when no activity is detected.

LCP interval: If you have enabled **Keep alive**, specify the LCP Echo frequency in seconds. The default setting is 30.

LCP fails: If you have enabled **Keep alive**, specify the maximum number of LCP fails before the connection is dropped.

Dial on demand: Enable this option to automatically dial a PPPoE connection when data flow is detected.

Maximum idle time: If you have enabled **Dial on demand**, specify a maximum idle time in seconds before the connection will be dropped.

Extra options: Specify extra options if required by your ISP.

Static IP address: Specify the IP address provided by your ISP.

PPP debug: Toggle this switch to enable PPP debug, this setting is disabled by default.

PPPoE Dual Stack (cont)

IPv4

Obtain DNS server addresses automatically: Toggle this switch to enable DNS information to be acquired automatically through DHCP. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

IPv6

Get IPv6: Choose **Automatically**, **IPv6 by DHCPv6** or **by SLAAC** according to the type of IPv6 is used by your ISP. The default setting is Automatically.

Enable prefix delegation: Enable prefix delegation. This setting is enabled by default.

Obtain DNS server addresses automatically: Obtain DNS server addresses automatically. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Click **Apply** when you are done.

PPTP

Choose **PPTP** (Point-to-Point-Tunneling Protocol) if your Internet Service Provider (ISP) uses a PPTP connection. Your ISP will provide you with a username and password.

General Settings

Connection Type: Select your connection type.

Interface: Select your connection interface.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

The screenshot shows the 'General Settings' tab for a PPTP connection. On the left, under 'General Settings', there are fields for 'Connection Name' (containing 'PPTP'), 'Interface' (set to 'WAN'), and a section with three toggle switches: 'Enable connection' (checked), 'NAT' (checked), and 'Ping' (unchecked). On the right, under the 'PPTP' section, there are fields for 'Username' and 'Password', a dropdown for 'LCP protocol' (set to 'No compression'), a dropdown for 'Authentication protocol' (set to 'PPTP'), a checked 'Keep alive' toggle, a 'PPTP server' dropdown (set to 'All'), and a 'Server' field (set to '1'). Below these are fields for 'Maximum idle time in seconds' (set to '30') and 'Idle timeout' (set to '30'). At the bottom, there is a 'WAN ping' section with a checked 'WAN ping' toggle, a 'IPv4' section with a checked 'Obtain IPv4 address automatically' toggle, and fields for 'Primary DNS' and 'Secondary DNS'. An 'APPLY' button is at the bottom left.

PPTP (cont)

PPP

Username: If **Without authorization** is disabled, specify the PPP username provided by your ISP.

Password: If **Without authorization** is disabled, specify the PPP password provided by your ISP.

VPN Server address: Specify the VPN server address provided by your ISP.

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1456.

Encryption protocol: Choose **No Encryption**, **MPPE 40 125 bit**, **MPPE 40 bit**, or **MPPE 128 bit**.

Authentication protocol: Choose from **AUTO**, **PAP**, **CHAP**, **MS-CHAP**, or **MS-CHAPv2**. **AUTO** is selected by default.

Keep alive: Toggle this switch to maintain your connection when no activity is detected.

LCP interval: If you have enabled **Keep alive**, specify the LCP Echo frequency in seconds. The default setting is 30.

LCP fails: If you have enabled **Keep alive**, specify the maximum number of LCP fails before the connection is dropped.

Dial on demand: Enable this option to automatically dial a PPPoE connection when data flow is detected.

PPTP (cont)

Maximum idle time: If you have enabled **Dial on demand**, specify a maximum idle time in seconds before the connection will be dropped.

Extra options: Specify extra options if required by your ISP.

Static IP address: Specify the IP address provided by your ISP.

PPP debug: Toggle this switch to enable PPP debug. This feature is disabled by default.

IPv4

Obtain DNS server addresses automatically: Toggle this switch to enable DNS information to be acquired automatically through DHCP. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Click **Apply** when you are done.

L2TP

Choose **L2TP** (Layer 2 Tunneling Protocol) if your Internet Service Provider (ISP) uses a L2TP connection. Your ISP will provide you with a username and password.

General Settings

Connection Type: Select your connection type.

Connection Name: Enter name for your connection.

Enable Toggle this switch to enable the connection. This is enabled by default.

Connection: Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

PPP

Without authorization: Enable this setting to connect without a username and password. This configuration is uncommon and is disabled by default.

Username: If **Without authorization** is disabled, specify the PPP username provided by your ISP.

Password: If **Without authorization** is disabled, specify the PPP password provided by your ISP.

VPN Server address: Specify the VPN server address provided by your ISP.

[illegible]

L2TP (cont)

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1456.

Encryption protocol: Choose **No Encryption**, **MPPE 40 125 bit**, **MPPE 40 bit**, or **MPPE 128 bit**.

Authentication protocol: Choose from **AUTO**, **PAP**, **CHAP**, **MS-CHAP**, or **MS-CHAPv2**. **AUTO** is selected by default.

Keep alive: Toggle this switch to maintain your connection when no activity is detected.

LCP interval: If you have enabled **Keep alive**, specify the LCP Echo frequency in seconds. The default setting is 30.

LCP fails: If you have enabled **Keep alive**, specify the maximum number of LCP fails before the connection is dropped.

Dial on demand: Enable this option to automatically dial a PPPoE connection when data flow is detected.

Maximum idle time: If you have enabled **Dial on demand**, specify a maximum idle time in seconds before the connection will be dropped.

Extra options: Specify extra options if required by your ISP.

Static IP address: Specify the IP address provided by your ISP.

PPP debug: Toggle this switch to enable PPP debug. This feature is disabled by default.

L2TP (cont)

IPv4

Obtain DNS server addresses automatically: Toggle this switch to enable DNS information to be acquired automatically through DHCP. This setting is enabled by default.

Primary DNS server: Specify the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS server: Specify the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Click **Apply** when you are done.

L2TP over IPsec

Choose **L2TP** (Layer 2 Tunneling Protocol) if your Internet Service Provider (ISP) uses a L2TP connection. Your ISP will provide you with a username and password.

General Settings

Connection Type: Select your connection type.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

IPsec

Pre-shared key: Enter your pre-shared key for your connection.

Enable PFS: Enable PFS for your connection.

Specify connection port: Enter the connection port for your connection.

The screenshot shows the configuration page for L2TP over IPsec. It is organized into two columns. The left column, titled 'General Settings', contains a dropdown for 'Connection Type' (set to L2TP over IPsec), a text field for 'Connection Name', a toggle for 'Enable connection' (checked), a toggle for 'NAT' (checked), and a text field for 'Pre-shared key'. The right column, titled 'IPsec', contains a toggle for 'Enable PFS' (checked), a dropdown for 'Specify connection port' (set to 500), and a section for 'IPsec policies'. This section includes a list of policies with columns for 'Policy Name', 'Policy ID', and 'Status'. At the bottom of the page is an 'APPLY' button.

PPP

Without authorization: Enable this setting to connect without a username and password. This configuration is uncommon and is disabled by default.

Username: If **Without authorization** is disabled, specify the PPP username provided by your ISP.

Password: If **Without authorization** is disabled, specify the PPP password provided by your ISP.

VPN Server address: Specify the VPN server address provided by your ISP.

Mobile Internet

Select **Mobile Internet** if you are using a mobile connection to connect to the Internet.

General Settings

Connection Type: Select your connection type.

Connection Name: Enter name for your connection.

Enable Connection: Toggle this switch to enable the connection. This is enabled by default. Disabling this feature may disable your Internet connection.

NAT: Toggle this switch to enable Network Address Translation (NAT). This setting is enabled by default.

Ping: Toggle this switch to enable WAN Ping. This setting is disabled by default.

Modem settings

Mode: Choose from **AUTO, 3G / 4G, 2G / 3G, 4G, 3G** or **2G**. **AUTO** is selected by default.

APN: Enter Access Point Name for your device

Dial number: Specify the Dial number provided by your Service Provider.

Without authorization: Enable this setting to connect without a username and password. This configuration is uncommon and is disabled by default.

Authentication protocol: If **Without authorization** is disabled, choose from **PAP** or **CHAP**. **PAP** is selected by default.

Username: If **Without authorization** is disabled, specify the PPP username provided by your ISP.

Password: If **Without authorization** is disabled, specify the PPP password provided by your ISP.

Use as interface: Enable this option to use the connection to communicate to the modem, but not to access the Internet.

Type: Choose from **IPv4**, **IPv6** or **Dual**. **IPv4** is selected by default.

PPP

MTU: Specify the Maximum Transmission Unit of your Internet connection. You may need to change the MTU for optimal performance with your ISP. The default setting is 1370.

Keep alive: Toggle this switch to maintain your connection when no activity is detected.

LCP interval: If you have enabled **Keep alive**, specify the LCP Echo frequency in seconds. The default setting is 30.

LCP fails: If you have enabled **Keep alive**, specify the maximum number of LCP fails before the connection is dropped.

Dial on demand: Enable this option to automatically dial a PPPoE connection when data flow is detected.

Maximum idle time: If you have enabled **Dial on demand**, specify a maximum idle time in seconds before the connection will be dropped.

PPP debug: Toggle this switch to enable PPP debug. This feature is disabled by default.

Health Check

Enable: Enable to check the connection status using the ping command

Modem IP address verification: Toggle the switch to enable the router to request for update of the IP addresses of the actual connections assigned to the modem in case the modem's IP address changes

The maximum number of attempts: The maximum number of attempts the ping command will execute before stopping.

Timeout (in seconds): The maximum response time for one attempt

Addresses: Click **ADD** to add addresses to ping.

Click **Apply** when you are done.

VLAN

VLAN tagging allows for services such as TRIPngle-Play to be used, and divides a network into segments that can only be accessed by other devices in the same VLAN.

In the Settings menu on the bar on the top of the page, click **Internet**, then click the **VLAN** link.

Click on any VLAN to configure it. Refer to **VLAN Add/Edit** on page 57 for configuration instructions.



VLAN List

Add: Click here to add a new VLAN. Refer to **VLAN Add/Edit on page 57**

Delete: Click here to delete the selected VLAN.

VLAN ID: Indicates the VLAN ID to which the tagged ports belong.

Name: This column indicates the name of the VLAN.

Tagged port: This column indicates the tagged ports belonging to the VLAN.

Untagged Ports: This column indicates the untagged ports belonging to the VLAN.

VLAN Add/Edit

Name: Specify a name for the VLAN.

VLAN ID: Specify the VLAN ID.

QoS: Enter a Quality of Service level.

Interface

Create interface: If the "Create Interface" function is disabled, the VLAN operates in the bridge mode and packets passing through it are not tracked.

Untagged Ports

Untagged Ports: If you have chosen to edit an existing untagged connection, or if you have chosen to add a bridge connection, select the untagged ports to be included in the VLAN.

Note: Ports can only belong to one VLAN at a time, and may need to be freed from other VLANs before changing this setting.

Tagged Ports

VLAN ID: If you have chosen to edit an existing tagged connection, or if you have chosen to add a bridge connection, select the tagged ports to be included in the VLAN.

Click **Apply** when you are done.

The screenshot shows the 'VLAN' configuration page. At the top, there's a 'Name' field with a red asterisk, followed by a 'VLAN ID' field with a red asterisk, and a 'QoS' field. Below these is the 'Interface' section, which includes a 'Create interface' checkbox (checked) and a 'Link to interface' button. The 'Ports' section contains a grid of port configuration cards for LAN1, LAN2, LAN3, LAN4, LAN5, and LAN6. Each card shows the port name, a 'Type' dropdown menu, and a 'Status' indicator. Below the ports is the 'Wireless interfaces' section with similar cards for WLAN1 and WLAN2. At the bottom right, there is a blue 'Apply' button.

DNS

Domain Name System (DNS) servers convert URLs into IP addresses to make it easier to navigate the internet. This screen allows you to manually configure DNS servers if required by your ISP or if a custom configuration is needed

DNS IPv4/IPv6

Manual: Enable this to specify name servers manually under **Name Server IPv4/IPv6**.

Default Gateway: If the **Manual** switch is set to disabled, apply below Interface setting as default.

Interface: Select the interface to which your DNS settings will apply.

Name Servers IPv4/IPv6

IP address: If **Manual** is set as enabled, specify one or more IP addresses for DNS name servers.

Add Server: Click here to add an additional server.

Reserve servers IPv4/IPv6

Add Server: Click here to add Reserve servers.

Click **Apply** when you are done.



WAN Failover

WAN Failover allows the device to switch to another WAN or Internet connection in the event that the primary connection becomes unavailable.

Enable: Toggle to enable WAN Failover.

Connections IPv4

Connection: Select your primary internet connection from the list.

Status of checking: Switch to enable or disable status checking.

Checking availability of hosts

Check interval: Specify the frequency to check your connection in seconds. The default setting is 10 seconds.

Timeout check: Specify the amount of time in seconds the device will wait before considering a ping to have timed out.

Number of checks: Specify the number of consecutive checks before switching.

Test hosts

ADD HOST: Click here to add additional test host IPs. Specify a test host IP address the router will use to determine the status of the connection. The default setting is 8.8.8.8, which is the public Google DNS.

Click **Apply** when you are done.

The screenshot shows the 'WAN Reservation' configuration page. At the top, there is a toggle switch labeled 'Enable' which is currently turned on. Below this, there is a section titled 'Connections IPv4' with a list of connections. The 'WAN_1' connection is selected. To the right of this section, there is a 'Checking availability of hosts' section. It includes a 'Check interval' field set to '10', a 'Timeout check' field set to '1000', and a 'Number of checks' field set to '3'. Below these fields, there is a 'Test hosts' section with three input fields: '8.8.8.8', '77.88.88.88', and '88.100.100.200'. Each field has a small 'x' icon to its right. At the bottom right of the page, there is an 'ADD HOST' button. At the bottom left, there is an 'APPLY' button.

Wireless network

From this page you can configure your wireless network settings. There are two tabs for 2.4 GHz and 5 GHz. 802.11n/g/b operate on 2.4 GHz, while 802.11ac/n/a operates over 5 GHz. 2.4 GHz and 5 GHz networks are configured independently.

General Settings

- Enable Wireless:** Toggle this switch to enable wireless access. To enable/disable Wi-Fi connection on a schedule, click the Set schedule button (🕒). In the opened window, you can create a new schedule (see the Schedule section Simplified mode on page 119page 118).
- Wireless mode:** Select a wireless mode from the list.
- Select channel automatically:** Toggle this switch to enable to allow the router to automatically select an operating channel.
- Enable additional channels:** Toggle this switch to enable higher channels.
 - Channel:** If **Select channel automatically** is disabled, select the channel your router will use.
- Enable periodic scanning:** Toggle this switch to periodically scan for an optimal channel.



Wireless network (cont)

Scanning period: If **Enable periodic scanning** is enabled, specify the amount of time in seconds between scans.

Wi-Fi Network

Network name (SSID): Specify the desire SSID for your wireless network. All devices must connect to this SSID.

Hide SSID: Toggle this switch to prevent SSID broadcasting. Clients will still need to enter the correct SSID to connect to your network.

BSSID: Enter the Basic service set identifiers (BSSID) is used in your network.

Max Associated Clients: Specify the maximum number of clients that can be connected at one time. Enter 0 for unlimited clients. The default setting is 0.

Enable shaping: Toggle this switch to enable shaping. This setting is disabled by default.

Shaping (Mbits/s): If **Enable shaping** is set to enable, specify the shaping threshold in Mbits/second.

Broadcast wireless network: Toggle this switch to disable broadcasting of a wireless network. This is useful if the router is being configured as a Wi-Fi client. This setting is enabled by default.

Clients isolation: Toggle this switch to prevent Wi-Fi clients from interacting with each other.

Security Settings

Network authentication: Select **Open, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 mixed, WPA-PSK/WPA2-PSK mixed, WPA3-SAE, or WPA2-PSK/WPA3-SAE mixed**. The default and recommended setting is WPA2-PSK.

Wireless network (cont)

If you have selected **WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK mixed, WPA3-SAE, or WPA2-PSK/WPA3-SAE mixed**:

Password: Specify a wireless password. Each device connecting to your network must enter this password.

Encryption type: Select an encryption type.

Group key update interval: Specify an update interval in seconds. The default setting is 604800.

If you have selected **WPA, WPA2, or WPA/WPA2 mixed**

WPA2 Pre-authentication: Toggle this switch to enable WPA pre-authentication.

IP address RADIUS server: Specify the IP address of the RADIUS authentication server.

RADIUS server port: Specify the port of the RADIUS authentication software.

RADIUS encryption key: Specify the RADIUS encryption key.

Encryption type: Select the encryption type. As of this writing, only AES is supported.

Group key update interval: Specify an update interval in seconds. The default setting is 604800.

Click **Apply** when you are done.

Click **ADD WI-FI NETWORK** to create an additional wireless network. If you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN, enable guest network in its settings.

Network

This section will allow you to change the local network settings of the router and to configure the DHCP settings. In the Settings menu on the bar on the top of the page, click **Network**. Click **IPv4** and **IPv6** to configure their respective settings.

IPv4

Local IP Address

IP Address: Specify the IP address of the router. The default IP address is **192.168.0.1**.

If you change the IP address, once you click **Apply** you will need to enter the new IP address in your browser to access the configuration utility.

Mask: Specify the subnet mask of the router. The default subnet mask is **255.255.255.0**.

Hostname: Specify the device domain name and URL to access the management utility. The default URL is **http://dlinkrouter.local/**

Gateway IP Address: *For Access Point, Repeater, and Client modes only.* Specify the gateway IP address which is used by the router to connect to the internet. (Optional)



IPv4 (cont)

Dynamic IP Addresses

Mode of Dynamic IP address assignment: Select **Disable**, **Server**, or **Relay**. The default setting is **Server**.
Select **Static** to assign the IPv4 address, subnet mask, and the gateway IP address manually or **Dynamic** to automatically obtains these parameters from the LAN DHCP server or another router.

Start IP: If **DHCP server** has been selected, specify the starting IP address in the DHCP server pool.

End IP: If **DHCP server** has been selected, specify the end IP address in the DHCP server pool.

Lease Time: If **DHCP server** has been selected, specify the lease time in minutes for DHCP-issued IP addresses.

DNS Relay: Disable to transfer the DNS server information from your ISP to your computers. If enabled, your computers will use the router for a DNS server.

ARP Proxy: Enable for the router to use its MAC address to respond to ARP requests sent to devices in its LAN.
Disable for the router to use its MAC addresses of devices in its LAN to respond to ARP requests sent to these devices.

IPv4 (cont)

DHCP Options

Known DHCP options: Select DHCP option.

Options value: Enter the DHCP option value.

Force: Enable the force function for this DHCP option.



Static IP Addresses

Clients list: Click this button to select a current host to add to the table of reserved static IP address. See **Clients List** below.

Add: Click this button to manually reserve a local IP address.

Delete: Click this button to delete a selected reserved IP address.

IP address: Indicates the reserved static IP.

MAC address: Indicates the MAC address for which the IP is reserved.

Hostname: Indicates the hostname of the client for which the IP is reserved.

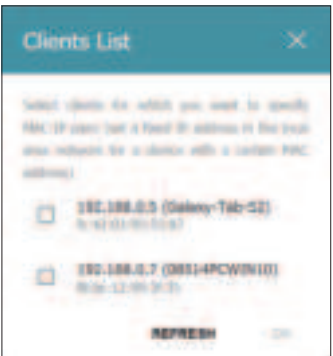
Click **Apply** when you are done.

KNOWN CLIENTS

Clients list: Click the corresponding client(s) on this list to automatically add their information to the Static IP Addresses list.

Refresh: Click here to refresh the connected clients list.

Click **OK** to save changes or click the X in the upper right hand corner to cancel changes.



Add/Static IP Addresses

IP address: Specify the IP address you wish to reserve for the given client.

MAC address: Specify the MAC address of the client for which the IP address is reserved.

Hostname: Specify the Hostname of the client for which the IP address is reserved.

Lease time (in minutes): Specify the lease time of the client for which the IP is reserved.

Click **Apply** to save changes or click the X in the upper right hand corner to cancel changes.



The screenshot shows a web-based configuration form titled "Static IP" in a teal header bar. The form contains four input fields: "IP address" with a red exclamation mark icon, "MAC address" with a red exclamation mark icon and a minus sign on the right, "Hostname", and "Lease time (in minutes)". An "Apply" button is located in the bottom right corner of the form area.

IPv6

Local IPv6 Address

IPv6 Address: The IPv6 address.

Addressing Type: Addressing Type of the IPv6 address.

Add Local IPv6 Address IP Addresses

IPv6 Address: Enter IPv6 address.

Prefix: Specify the IPv6 prefix of the address. The default prefix is **64**.

Dynamic IPv6 Addresses

Mode of Dynamic IPv6 address assignment: Select **Disable**, **Stateful**, or **Stateless**.

Address range If **Stateful** has been selected, specify the starting and end IP address range in the DHCP server pool.

Lease Time: If **Stateful** or **Stateless** has been selected, specify the lease time in minutes for dynamic IPv6 addresses.

Click **Apply** when you are done.

*If **Stateful** is selected then the following options will be available.*



Local IPv6 Address

IPv6 address*

Prefix*

APPLY

If **Stateful** is selected then the following options will be available.

KNOWN CLIENTS

Clients list: Click the corresponding client(s) on this list to automatically add their information to the Static IP Addresses list.

Refresh: Click here to refresh the connected clients list.

Click **OK** to save changes or click the X in the upper right hand corner to cancel changes.



Add/Static IP Addresses

IP address: Specify the IP address you wish to reserve for the given client.

MAC address: Specify the MAC address of the client for which the IP address is reserved.

Hostname: Specify the Hostname of the client for which the IP address is reserved.

Lease time (in minutes): Specify the lease time of the client for which the IP is reserved.

Click **Apply** to save changes or click the X in the upper right hand corner to cancel changes.



Functions

Firewall

IP Filter

The IP Filters page manages LAN users' access to the Internet. It is possible to permit access to the Internet for specified IP addresses within your LAN or to restrict access for specified IP addresses. You can also define filters for port access.

The currently defined IP filters are displayed in the table. You may define up to 16 IP filtering rules. If you wish to remove a rule, click the corresponding check box to select it and then click **Delete**. If you wish to create a new rule, click the **Add** button.

Filters

Add: Click here to add a new filter to the firewall. For details, see **IP Filter Create/Edit** on **page 70**.

Delete: If you have a selected one or more filters, click this button to delete the selected filter(s).

No: Indicates the number of the filter.

Name: Indicates the name of the filter.

State: Indicates whether the is enabled or disabled.

Action: Indicates the action taken when the filter is triggered.

IP version: Indicate to which IP version the filter applies.



Filters							
☐	IP	Name	State	Action	IP version	Protocol	[Name: Firewall] [10.0]
☐							[Name: Firewall] [10.0]
☐	IPv4	Filter	Enabled	Allow	TCP	TCP	[192.168.0.0 - 192.168.0.255] : [1 - 65535] [192.168.0.0 - 192.168.0.255] [1]

IP Filter Create/Edit

Protocol: Indicates to which protocol(s) the filter applies.

[Source IP address] Indicates the IP address range and port(s) to which the filter applies.

To enable schedule on a filter, click the Set schedule button (🕒). In the opened window, you can create a new schedule (see the Schedule section Simplified mode on page 119page 118)

General Settings

Enable rule: Toggle this switch to enable the rule.

Name: Specify a name for the rule. This name is for reference only and does not affect functionality.

Action: Choose the action to be taken when the rule is triggered. Choose **Allow** or **Deny**.

Protocol: Choose which protocol to which the rule will apply. Choose from **TCP/UDP, TCP, UDP, ICMP, or <All>**

IP version: Choose if the rule should apply to **IPv4** or **IPv6**.

Direction: Choose the direction to be taken when the rule is triggered. Choose from **LAN to WAN, WAN to LAN** or **LAN to Router**.

Destination IP Address

Set as: Choose **Range or single IP address** to enter a specific IP address or ranges for the destination filter. Choose **Subnet** to specify a subnet only.

General Settings

☒ Enable rule

Name:

☒ The number of connections allowed per hour of IP

Action: **Allow**

Protocol: **TCP**

IP version: **IPv4**

Direction: **LAN to WAN**

Source IP address

☒ You can specify a range of IP addresses, a single IP address, or a subnet of IP address (for example, 192.168.1.1/24 or 192.168.1.1/24). You can also specify a range of IP addresses (for example, 192.168.1.1-192.168.1.255).

Set as: **Range or single IP address**

Start IP address:

End IP address:

Destination IP address

☒ You can specify a range of IP addresses, a single IP address, or a subnet of IP address (for example, 192.168.1.1/24 or 192.168.1.1/24). You can also specify a range of IP addresses (for example, 192.168.1.1-192.168.1.255).

Set as: **Range or single IP address**

Start IP address:

End IP address:

Ports

☒ You can specify a range of ports, a single port, or a range of ports separated by a comma (for example, 8080-8090).

Set as: **Set source port manually**

Destination port:

Apply

Start/End IPv4/IPv6 address: If you have selected **Range or single IP address**, specify an IP address range for the destination filter. To enter a single address, use only the **Start IPv4/IPv6 address** field and leave the **End IPv4/IPv6 address** field blank.

Subnet IPv4/IPv6 address: If you have selected **Subnet**, specify the destination subnet to filter.

Source IP Address

Set as: Choose **Range or single IP address** to enter a specific IP address or ranges for the source filter. Choose **Subnet** to specify a subnet only.

Start/End IPv4/IPv6 address: If you have selected **Range or single IP address**, specify an IP address range for the source filter. To specify a single address, use only the **Start IPv4/IPv6 address** field and leave the **End IPv4/IPv6 address** field blank.

Subnet IPv4/IPv6 address: If you have selected **Subnet**, enter the source subnet to filter.

Ports

Destination port: Specify the destination port or ports to which the filter will apply. Specify multiple ports by separating them with commas. Specify port ranges by separating the beginning and end of the range with a colon.

Set source port manually: Toggle this switch to specify source ports to which the filter will apply.

Source port: If **Set source port manually** has been enabled, specify the source port to which the filter will apply. Specify multiple ports by separating them with commas. Specify port ranges by separating the beginning and end of the range with a colon.

Click **Apply** when you are done.

DMZ

This Demilitarized Zone (DMZ) feature directly exposes the client to the Internet, and is not recommended in ordinary situations.

Enable: Toggle this switch to enable the DMZ feature.

Enable NAT Loopback: Toggle this switch to enable NAT Loopback. NAT Loopback allows LAN devices to connect directly to the DMZ host by using the WAN IP address.

IP Address: If DMZ is enabled, specify the IP address of the DMZ host.

Click **Apply** when you are done.



MAC Filter

The MAC filter is used to restrict or allow certain types of Ethernet Frames through the gateway based on their source or destination MAC address. These filters are helpful in securing or restricting traffic on your local network.

The currently defined MAC filters are displayed in the table. You may define up to 32 MAC filtering rules. If you wish to remove a rule, click the corresponding check box to select it and then click **Delete**. If you wish to create a new rule, click the **Add** button.

Default Mode: Select **Allow** to allow all traffic except from MAC addresses in the **List of exceptions** with the **Deny** action. Select **Deny** to allow all traffic except from MAC addresses in the **List of exceptions** with the **Allow** action.

To enable schedule on a filter, click the Set schedule button (⌚). In the opened window, you can create a new schedule (see the Schedule section Simplified mode on page 119page 118).

Click (+) to add a new filter to the firewall.

If you have a selected one or more filters, click (🗑) to delete the selected filter(s).



List of exceptions

No: If DMZ is enabled, specify the IP address of the DMZ host.

State: Indicates the number of the filter.

Action: Indicates the action taken when the filter is triggered.

MAC address: Indicates the MAC address to which the filter applies.

Name: Indicates the hostname of the device to which the filter applies.

MAC Filter (cont)

Add Rule

Enable rule: Switch to enable/disable rule.

Allow/Deny: Choose the action to be taken when the rule is triggered. Choose **Allow** or **Deny**.

MAC address: Specify the MAC address of the host to which the filter will apply. This field is mandatory.

Name: Specify the hostname of the host to which the filter will apply. This field is optional.

Click **Save** when you are done, or click the **X** to cancel.



The screenshot shows a 'Add Rule' dialog box with a teal header and a close button (X) in the top right corner. Inside the dialog, there is a toggle switch labeled 'Enable rule' which is currently turned on. Below this, there are three input fields: 'Action' with a dropdown menu showing a minus sign, 'MAC address' with a dropdown menu showing a minus sign, and 'Name' with a red asterisk indicating it is mandatory. At the bottom right of the dialog, there is a blue 'Save' button.

Wi-Fi Client management

The Client Management page displays a list of currently connected Wi-Fi devices. You can view detailed information about these devices or force them to disconnect from your network.



List of Wi-Fi Clients

Refresh: Click here to refresh the connected clients list.

Disconnect: Click here to disconnect the selected client(s) from your network. Note that this only disconnects the client, it does not prevent the client from reconnecting.

Hostname: Indicates the hostname of the connected client.

MAC address: Indicates the MAC address of the connected client.

Band: Indicates the band over which the client is connected.

Network name (SSID): Indicates the SSID to which the client is connected.

Signal Level: Indicates signal strength as a percentage.

Online: Indicates the time online in minutes.

Last RX rate: Indicates the last recorded transmission rate in Mbps.

Rx/Tx: Indicates total bytes received or transmitted this session.

A screenshot of a modal window showing detailed information for a selected client. The modal has a title bar with a close button. The content is organized into two columns. The left column lists various attributes: Hostname, MAC address, Band, Network name (SSID), Signal level, Online time, Last RX rate, and Rx/Tx. The right column displays the corresponding values for these attributes. For example, the MAC address is '08:00:27:00:00:00' and the Signal level is '100%'. The 'Online' status is indicated by a green dot and the text 'Online'. The 'Last RX rate' is '100.00 Mbps'.

WPS

The Wi-Fi Protected Setup page allows you to create a wireless connection between your router and a device automatically by simply pushing a button. WPS for 2.5 GHz and 5 GHz are configured separately by clicking the corresponding buttons for 2.5 GHz and 5 GHz.

WPS Control

Enable/Disable: Click this button to toggle WPS. For security reasons, WPS is enabled by default.

Establish connection: Click this button to launch the **Establish Connection** menu, described below.

Enable Wi-Fi when WPS function is activated with hardware button: Move the switch to the left in order to forbid the router to enable Wi-Fi/WPS when the WPS function is activated with the relevant hardware button.

Establish Connection

WPS Method Choose **PBC** (Push Button Connection).

Connect: Click here to initiate the pairing process.

Information

WPS state: Shows whether it is configured or not.

Network name (SSID): Indicates the SSID to which the client is connected.



WPS (cont)

Network authentication: Indicates the type of authentication used on the network.

Encryption: Indicates the encryption used by the authentication method.

Password PSK: Indicates the password of the network.

Update: Click this button to refresh the page.

WMM

WMM (Wi-Fi Multimedia) is a QoS (Quality of Service) system for improving the quality of video and voice applications on your wireless network.

Wi-Fi Multimedia 2.4 GHz/ 5 GHz

Work mode: Select **Auto** or **Manual**. The default and recommended setting is **Auto**. If you select **Manual**, you will be prompted for detailed configuration. This setting is intended for advanced users only and is not recommended for most users.

Access Point/Station

If **Work mode** has been set to **Manual**, you can click on each row to configure advanced QoS settings for that connection type.



Client

Client mode allows you to configure your router as a client on another wireless network. This would be useful to setup the router as a wireless repeater or connect to a WISP.

Enable: Toggle this switch to enable your router to act as a Wi-Fi client.

Broadcast wireless network 2.4/5 GHz: Toggle these switches to enable or disable your router's wireless APs.

Connecting to network: Choose **Select network from list** or **Connect to hidden network**. If you choose **Select network from list**, select the network you wish to connect to and enter any necessary security information as prompted. If you choose **Connect to hidden network**, enter the Wi-Fi information below.



Client (cont)

If you selected **Connect to hidden network**:

Network name (SSID): Specify the network name used by the hidden network. This must be specified correctly to connect.

BSSID: Specify the BSSID.

Network authentication: Select the network authentication used by the hidden network. This must be specified correctly to connect.

Password PSK: Specify the password or PSK used by the hidden network. This must be specified correctly to connect.

Encryption type: Specify the encryption type used by the hidden network. This must be specified correctly to connect.

Click **Apply** when you are done.



The screenshot shows a web interface for configuring a hidden network connection. It includes the following fields and options:

- Connect to hidden network:** A toggle switch that is currently turned on.
- Network name (SSID):** A text input field containing the value "2.4 GHz".
- BSSID:** A text input field that is currently empty.
- Network authentication:** A dropdown menu with "WPA2-PSK" selected.
- Password PSK:** A text input field containing the value "12345678".
- Encryption type:** A dropdown menu with "AES" selected.
- Apply:** A blue button at the bottom of the form.

Client Shaping

Client shaping allows you to impose speed limits on clients to ensure that bandwidth is not being monopolized by a single Wi-Fi client.

Client Shaping

Add: Click this button to add a new client shaping rule. You will be taken to the **Add Rule** dialogue, described below.

Delete: Click this button to delete the selected rule(s).

MAC address: Indicates the MAC address of the Wi-Fi client to which the rule applies.

Maximum upload rate: Indicates the maximum upload rate for the given client in megabits per second.

Maximum download rate: Indicates the maximum download rate for the given client in megabits per second.

Enabled: Indicates if the rule is enabled.



Add/Edit Rule

Frequency band: Select the frequency band for this rule.

SSID: Select the SSID for this rule.

Enabled: Toggle this switch to enable the rule.

MAC address: Specify the MAC address of the Wi-Fi client to which the rule will apply.



Client Shaping (cont)

Upload/Download

Not limited: Toggle this switch to disable the limit for the corresponding transfer type.

Maximum rate: If **Not limited** is disabled, specify a maximum transfer rate in megabits per second.

Click **Save** when you are done.

Additional 2.4 GHz

The additional screen allows you to configure details of your router's Wi-Fi settings. These are advanced settings and should not be needed for normal usage. 2.4 GHz and 5 GHz Wi-Fi are configured separately by clicking on the corresponding tab.

Bandwidth: Specify the channel bandwidth. Choose from **Auto**, **20 MHz** or **20/40 MHz**.

Autonegotiation 20/40 (Coexistence): 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Choose from **Auto**, **Always On** or **Always Off**.

TX Power (in percent): Specify the routers transmission power in percentage. Choose from **100**, **75**, **50**, **25**, **10**.



Drop multicast: Toggle to enable or disable.

Adaptivity mode: Toggle to enable or disable.

Reduce power on OFDM: If 5 GHz is selected. Toggle to enable or disable.

STBC: Toggle to enable or disable.

Enable 802.11k: Toggle to enable or disable.

B/G protection: Choose from **Auto**, **Always On** or **Always Off**.

Short GI: Choose from **Enable** or **Disable**.

- Beacon Period (in milliseconds):** Specify the time interval (in milliseconds) between packets sent to synchronize the wireless network. The default setting is 100ms.
- RTS threshold (in bytes):** Specify the minimum size (in bites) of a packet for which an RTS frame is transmitted. The default size is 2347 bytes and the standard range is 256-2346 bytes.
- Frag threshold (in bytes):** Specify in bytes the maximum frame size for a non-fragmented packet. The default size is 2346.
- DTIM period (in beacon frames):** Specify how often (by the number of beacon frames) that DTIM is transmitted. By default this is set to 1.
- Station Keep Alive (in seconds):** Specify the time interval (in seconds) between keep alive checks of wireless devices from your WLAN.

Additional 5 GHz

- Bandwidth:** Specify the channel bandwidth. Choose from **Auto**, **20 MHz**, **20/40 MHz** or **20/40/80 MHz**.
- TX Power (in percent):** Specify the routers transmission power in percentage. Choose from **100**, **75**, **50**, **25**, **10**.
- Enable DFS:** Toggle to enable or disable.
- Drop multicast:** Toggle to enable or disable.
- Enable TX Beamforming:** Toggle to enable or disable.
- Adaptivity mode:** Toggle to enable or disable.
- Reduce power on OFDM:** Toggle to enable or disable.
- STBC:** Toggle to enable or disable.
- Enable 802.11k:** Toggle to enable or disable.
- Short GI:** Choose from **Enable** or **Disable**.
- Beacon Period (in milliseconds):** Specify the time interval (in milliseconds) between packets sent to synchronize the wireless network. The default setting is 100ms.
- RTS threshold (in bytes):** Specify the minimum size (in bites) of a packet for which an RTS frame is transmitted. The default size is 2347 bytes and the standard range is 256-2346 bytes.
- Frag threshold (in bytes):** Specify in bytes the maximum frame size for a non-frgmented packet. The default size is 2346.



DTIM period (in beacon frames): Specify how often (by the number of beacon frames) that DTIM is transmitted. By default this is set to 1.

Station Keep Alive (in seconds): Specify the time interval (in seconds) between keep alive checks of wireless devices from your WLAN.

MAC Filter

On the Wi-Fi/MAC Filter page, you can define a set of MAC addresses of devices which will be allowed to access the WLAN, or define a set of MAC addresses of devices which will not be allowed to access the WLAN.

To Enable or Disable MAC Filter for a specific SSID, click on the SSID name listed below each Wi-Fi band.

- Enable MAC Filter:** Toggle this switch to enable MAC filter. When this option is activated, you can create rules for filtering by MAC addresses.
- MAC filter restrict mode:** Choose either allow or deny to enable/disable connection only for specified MAC addresses.

To add a rule, click on the **add** button.

Frequency Band: Choose which frequency band you want the rule to apply to.

SSID: Choose which SSID you want the rule to apply to.

MAC Address: Specify the MAC address of the device.

Hostname: Specify hostname of the device (optional).

Enable Rule: Toggle this switch to enable or disable the rule.



Once a filter has been defined, page will display the list of filters below. To edit a filter, click directly on the corresponding row.

MAC Address: MAC address of device.

Hostname: Hostname of device.

SSID: Name of wireless network.

Band: Frequency band.

Enabled: Current status of filter.

To delete a filter, select the corresponding check box then click on the delete symbol.

To enable MAC Filter on a schedule, click the Set schedule button (📅). In the opened window, you can create a new schedule (see the Schedule section Simplified mode on page 119page 118).

Roaming

On the Roaming page you can enable the smart adjustment function of Wi-Fi clients.

To enable this function, click on **Enable**.



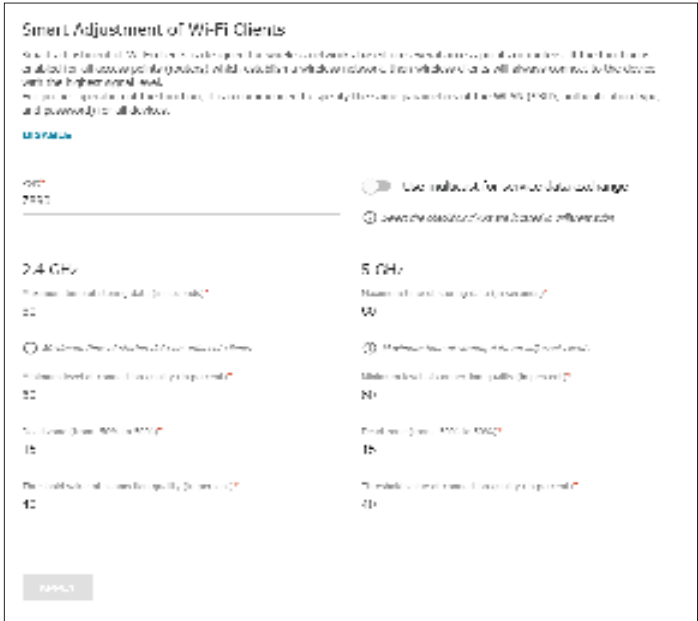
Port: Port number.

Use Multicast for Service Data Exchange: Toggle this switch to enable. Once enabled, multicast TTL, multicast group address needs to be specified.

Threshold value of connection quality: Toggle this switch to enable threshold value of connection quality.

Multicast TTL: Specify the TTL (Time to live) parameter value. The recommended value is 4.

Multicast group address: Specify the address of the multicast group (from the subnet 239.255.0.0/16).



2.4 GHz and 5 GHz specify the following options:

- Maximum time of storing data (in seconds):** Specify in seconds the maximum time of storing data on adjacent clients.
- Minimum level of connection quality:** Specify in percentage the connection quality.
- Dead zone:** Specify in percentage the dead zone (from -50% to 50%).
- Threshold value of connection quality (in percent):** Specify in percentage of threshold value of connection quality.

Click **Apply** when finished.

Advanced

UPnP IGD

UPnP IGD (Universal Plug and Play Internet Gateway Device) is a protocol that allows ports to automatically be mapped between your devices behind your NAT and the Internet.



Enable: Toggle this switch to enable or disable UPnP. If it is enabled, a table will appear indicating active UPnP connections.

IPv4 IGD

Protocol: Indicates the protocol used by the UPnP connection.

IP: Indicates the internal IP used by the UPnP connection.

Private Port: Indicates the internal port used by the used by the UPnP connection.

Public port: Indicates the port exposed to the internet used by the UPnP connection.

Description: Indicates the description of the protocol used by the UPnP connection.

Duration: Indicates the duration of the UPnP connection.

Remote Access

Remote access allows you to access the web GUI from WAN. By default, the access from external networks to the router is disabled for security reasons. If you need to allow access to the router from external networks, create relevant rules.

Remote Access

Add: Click here to add a new rule, described below.

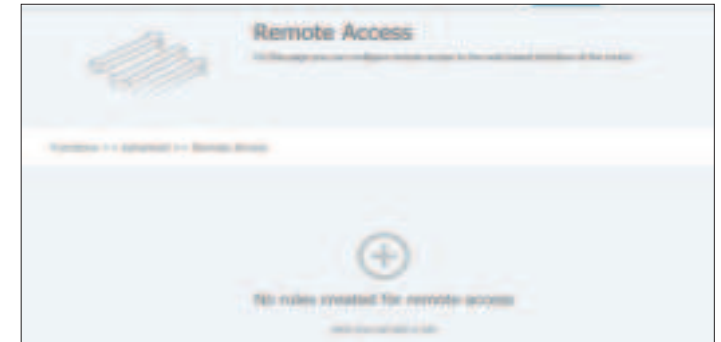
Delete: Click here to delete a selected rule.

IP address: Indicates the IP address permitted to access the GUI.

Mask: Indicates the subnet mask of the IP address permitted to access the GUI.

Public Port: Indicates the public port over which the IP address is permitted to access the GUI.

Protocol: Indicates the protocol used to access the GUI.



Add Rule

IP Version: Select **IPv4** or **IPv6**.

Open access: Toggle this switch to enable any remote host to access the GUI. This is not recommended.

IP address: Specify the IP address of the remote host allowed to access the GUI.



Remote Access (cont)

Mask: Specify the subnet mask of the remote host allowed to access the GUI.

Public Port: Specify the port over which the remote host will access the GUI.

Protocol: Choose **HTTP, HTTPS, FTP, TELNET, SMB** or **SSH** as the protocol for remote access.

Click **Save** when you are done.

Virtual Servers

Virtual Servers allows you to redirect incoming Internet traffic to a specified IP address in the local area network.

Click on **ADD** to create a new virtual server and specify the below parameters.

General Settings

Enable: Toggle this switch to enable or disable Virtual Servers.

Name: Specify a name for the virtual server.

Template: Choose a template for the virtual server to pre-populate some fields, or choose **Custom** to configure all fields manually.

Interface: Select an interface from the drop-down menu, or select **<All>**.

Protocol: Select a protocol from the drop-down menu to which the rule will apply.

NAT Loopback: Toggle this switch to enable NAT loopback.

Public Network Settings Remote IP

Remote IP: Specify the remote IP to which the rule will apply.

Add Remote IP: Click this button to add additional remote IP fields.

Public port: Specify the remote IP to which the rule will apply.

Private Network Settings

Private IP: Specify the IP address on your local network to which the rule will forward.

Private Port (start/end): Specify a start and an end port to which the rule will apply. If you wish to specify a single port, specify a start port only.

Click **Apply** when you are done.

TR-069 Client

On the TR-069 Client page, you can configure the router for communication with a remote Auto Configuration Server (ACS). The TR-069 client is used for remote monitoring and management of the device.

TR-069 Client

Interface: Select the interface over which the client should operate.

Enable TR-069 client: Toggle this switch to enable or disable TR-069.

Auto Configuration Server Settings

Get URL address via DHCP: Toggle this switch to enable or disable getting the URL address via DHCP.

URL address: Specify the URL of your ISP's ACS.

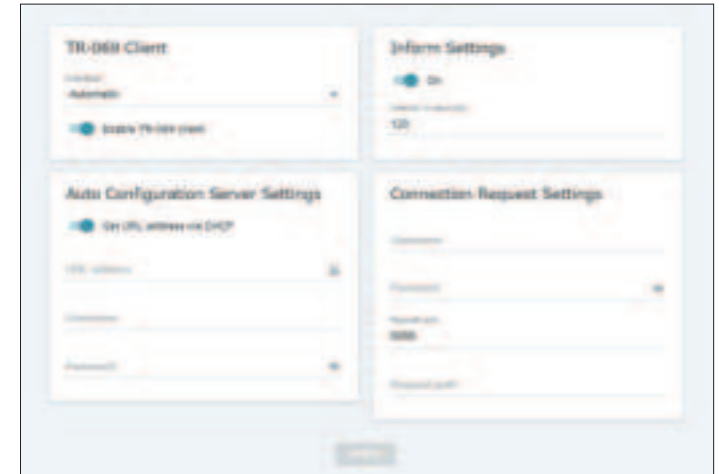
Username: Specify the username for your ISP's ACS.

Password: Specify the password for your ISP's ACS.

Inform Settings

Enable: Toggle this switch to enable active contact with your ISP's ACS.

Interval: Specify the interval in seconds for each inform packet.



TR-069 Client (cont)

Connection Request Settings

Username: Specify the username here.

Password: Specify the password here.

Request Port: Specify the request port here.

Request Path: Specify the request path here.

Click **Apply** when you are done.

Static Route

Once connected to the Internet, your router automatically builds routing tables that determine where traffic should be sent. Static routes can override this process, allowing traffic to be directed to a specific client or location.

Routing Configuration

Add: Click this button to add a new static route.

Delete: Click this button to delete the selected route(s).

Destination network: Indicates the IP address of the destination network.

Gateway: Indicates the gateway traversed by the static route.

Interface: Indicates the interface traversed by the static route.

Metric: Indicates the metric of the static route.

Accessibility: Indicates the current status of the route.

Add Route

Protocol: Choose the protocol used by the static route.

Interface: Choose the interface used by the static route.

Destination network: Specify the IP address of the destination.

Destination netmask: Specify the netmask used by the destination IP.



Static Route (cont)

Gateway: Specify the gateway used by the static route.

Metric: Specify a metric between 1 and 255.

Table: Select a route table for the static route.

Click **Save** when you are done.

Dynamic DNS

Dynamic Domain Name Service allows your router to associate an easy-to-remember domain name such as [YourDomainName].com with the regularly changing IP address assigned by your Internet Service provider. This feature is helpful when running a virtual server.

DDNS List

Add: Click this button to add a new DDNS service, described below.

Delete: Click this button to delete the selected DDNS service(s).

Hostname: Indicates the hostname of the DDNS service.

DDNS service: Indicates the name of the DDNS service.

Username: Indicates the username used with the DDNS service.

Update period: Indicates the update period in minutes of the DDNS service.



Add DDNS

Hostname: Specify the assigned hostname used by your DDNS service. If you want to use another domain name of this DDNS provider, click the **ADD HOST** button and enter the needed value in the line displayed.

DDNS service: Select the DDNS service you are using.
If your provider is not in the list, select the Custom provider value and fill in the fields displayed on the page. Specify the DDNS provider name in the Name field, the domain name of the provider's server in the Server field, and the location of settings in the Path field.

Username: Specify the username for your DDNS service.

Password: Specify the password for your DDNS service.

Update period: Specify the update period in minutes.

Click **Save** when you are done.

IPsec

The router's IPsec function allows the router to act as an IPsec client, allowing connected devices behind the router to use the tunnel without being individually configured.

Enable: Toggle this switch to enable the IPsec client functionality.

Logging level: Select the Logging level of the IPsec client. Basic is recommended to establish faster IPsec tunnel. To view the log, go to the Management/System Log on page **112**.

Tunnels

Add: Click here to add a new IPsec client, described in **IPsec/Adding** on page **104**.

Delete: Click this button to delete the selected tunnel(s).

Remote host: Indicates the remote host of the tunnel.

Encryption algorithm: Indicates the encryption algorithm used by the tunnel.



IPsec (cont)

Hashing algorithm: Indicated the hashing algorithm used by the tunnel.

Interface: Indicates the interface over which the tunnel operates.

Status

Remote host: Indicates the status of the remote host of the tunnel.

IKE: Indicates Internet Key Exchange.

CHILD: Indicates any security association negotiated via IKE SA.

State: Indicates tunnel status.

IPsec/Adding

Enable: Toggle this switch to enable Dynamic IPsec.

General Settings

IP version: Choose IP version.

Dynamic IPsec: Enable or disable dynamic IPsec.

Type: Choose type of address.

Remote Host: Enter IP address of remote host. If Dynamic IPsec is enabled, this field will be disabled.

Identifier value: Specify from the drop down list either **IP address** or **fqdn** as local identifier

Pre-shared key: Specify a pre-shared key.

Local WAN: Specify from drop down list either **Default gateway** or **Interface**.

NAT Traversal: Specify from drop down list **Disabled** or **Enabled**.

Type: Specify from down list **TUNNEL** or **TRANSPORT**.

Enable DPD: Toggle this switch to enable/disable Dead Peer Detection.

DPD delay: Specify in seconds DPD delay.

DPD time out, sec: Specify maximum seconds of DPD timeouts.

TCP MSS: Specify from drop down list either Manual or Path MTU Discovery.

The First Phase

Encryption Mode: Choose the encryption mode.

First phase encryption algorithm: Choose the encryption algorithm for first phase.

Hashing mode: Choose the hashing mode for First Phase from drop down list.

Size of hash: Choose the value for the size of hash.

Hashing algorithm: Choose the hashing algorithm for first phase from drop down list.

First phase DHgroup type: Specify DHgroup type for First Phase from the drop down list.

IKE-SA lifetime: Specify a valid value between 60 seconds and 86400 seconds.

IKE version: Specify the IKE version.

The Second Phase

Encryption Algorithm: Specify from drop down list the encryption algorithm for Second Phase.

Second phase encryption algorithm: Specify from drop down list the authentication algorithm for First Phase.

Hashing mode: Choose the hashing mode for First Phase from drop down list.

Size of hash: Choose the value for the size of hash.

Hashing Algorithm: Specify from drop down list the authentication algorithm for Second Phase.

Enable PFS: Toggle this switch to enable Perfect Forward Secrecy for second phase.

Second phase DHgroup type: Specify DHgroup type for Second Phase from drop down list.

IPsec-SA lifetime: Specify valid value in seconds.

Tunneled Networks

Add: Click to add rule to apply to IPsec tunnel.

Delete: Click to delete rule.

Local Network: Specify/shows the local subnet of IPsec tunnel.

Remote Subnet: Specify/shows the remote subnet of IPsec tunnel.

Click **Apply** when finished.

Ports Settings

The Ports Settings page allows you to configure or disable autonegotiation of speed and duplex mode or manually configure speed and duplex mode for each Ethernet port of the router.

Ports Settings

Port: Indicates port number.

Status: Indicates current status of port.

Autonegotiation: Indicates whether autonegotiation is on/off.

Speed: Indicates port speed.

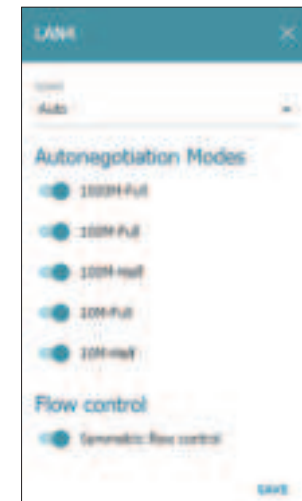
Flow Control: Indicates whether symmetric flow control is on/off.

To configure a port, click on the corresponding port you wish to configure.

Speed: Specify from drop down list port speed.

Autonegotiation Modes: Toggle this switch to enable/disable autonegotiation modes.

Flow Control: Toggle this switch to enable/disable symmetric flow control.



Redirect

The Redirect page allows to enable or disable notifications for when Internet connection has failed.

Common Setting

ENABLE/DISABLE: Click this button to enable/disable failure notifications in the browser window.

Redirect

You can enable or disable notifications in the case of the Internet connection failure. Notifications will be displayed in the browser window when a warning message is displayed on the screen.

ENABLE

Reasons for Redirect

☒ Physical connection error

☒ No connection

☒ The device is not configured

APPLY

Reasons for Redirect

The below options will only appear if redirect is enabled.

Physical Connection Error: Toggle this switch to enable notification if connection failure is due to physical error.

No Connection: Toggle this switch to enable notification if connection failure to due no connection detected.

The Device is not Configured: Toggle this switch to enable notification if connection failure due to device not configured.

IGMP/MLD

The IGMP/MLD page allows you to manage multicast traffic in IP-based networks.

IGMP

Enable/Disable: Toggle this switch to enable/disable IGMP.

IGMP version: Choose from drop down list which IGMP version to use.

Interface: Choose from drop down list which interface to apply to.

Click **APPLY** when finished.

MLD

Enable/Disable: Toggle this switch to enable/disable MLD.

MLD version: Choose from drop down list which MLD version to use.

Interface: Choose from drop down list which interface to apply to.

Click **APPLY** when finished.



The screenshot shows a web interface for configuring IGMP and MLD. It is divided into two main sections: IGMP and MLD. Each section has a toggle switch for 'Enable/Disable', a dropdown menu for 'Version', and another dropdown menu for 'Interface'. At the bottom of the IGMP section is an 'APPLY' button.

IGMP	MLD
☒ Enable	☒ Enable
IGMP version: v2	MLD version: v2
Interface: vlan10	Interface: vlan10
APPLY	

ALG/Passthrough

The ALG/Passthrough page allows you to configure the router to use RTSP, enable the SIP ALG and PPPoE/PPTP/L2TP/IPsec passthrough functions.

Toggle this switch to enable/disable the following:

SIP

RTSP

PPPoE passthrough

IPsec passthrough

L2TP passthrough

PPTP passthrough

Click **APPLY** when finished.



Management

System Time

System Time allows you to configure date and time to be synchronized with a public time server on the Internet or set manually.

System Time

Enable NTP: Toggle this switch to enable/disable NTP.

Get NTP server addresses using DHCP: Toggle this switch to enable/disable getting NTP server addresses using DHCP.

Run as a server for the local network: Toggle this switch to enable/disable running as a server for the local network.

System Date: Displays device's current system date.

System Time: Displays router's current system Time.

Enable/Disable: Toggle this switch to enable/disable NTP.

Main time zone: Select the main time zone manually.
To set the time zone in accordance with the settings of your operating system or portable device, click **DETERMINE TIMEZONE**.



NTP Servers

Displays default public time server. Click on 'x' to delete.

Click **ADD SERVER** to add a new public time server.

System Log

The System Log page displays diagnostic information that run in the background to monitor the health of your device if enabled.

Log

Refresh: Click to refresh log for new updates.

Export: Click to export log as text file.

Settings

Enable/Disable: Toggle this switch to enable/disable logging function.

Type: Choose from drop down list type of diagnostics to log.

Level: Choose from drop down list level of diagnostics to log.

Click **APPLY** when finished.



Administration

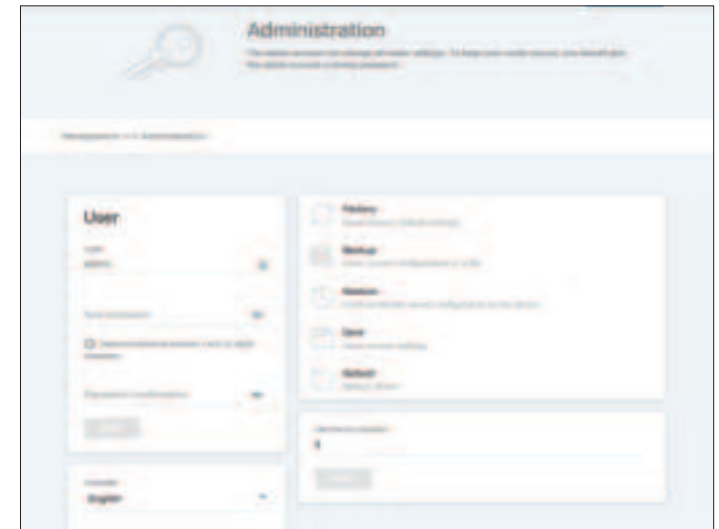
The Administration page allows you to change router settings.

User

Login: Username to login to router's configuration UI as the administrator. This cannot be changed.

Password: Specify new password. Password needs to be between 1 - 31 ASCII characters. Confirm password again below.

Click **SAVE** when finished.



Language: Choose router UI language from drop down list.

Factory: Click to reset router to factory default settings.

Backup: Click to save current configuration to a file.

Restore: Click to load previously saved configuration file to the device.

Save: Click to save current settings.

Reboot: Click to reboot device.

Idle Time: Specify a period of inactivity (in minutes) after which the device will log you out.

Telnet/SSH

The Telnet page allows you to enable or disable access to the device settings via TELNET from your LAN.



Enable/Disable Telnet: Toggle this switch to enable Telnet.

Port: Specify port number for Telnet access.

Enable/Disable SSH: Toggle this switch to enable SSH.

Port: Specify port number for SSH access.

Click **APPLY** when finished.

Yandex.DNS

Yandex.DNS is a web content filtering service which provides the DNS server, protects a computer against malicious web sites, and blocks access to adult web sites.

Enable: Toggle this switch to enable or disable Yandex.DNS.

Default Mode

Protection off: When selected, the DNS server has no restrictions on access to unsafe web sites.

Safe: For the devices in safe mode, it will block websites that try to steal your passwords.

Child: For the devices in child mode, it will block websites containing adult media. It is recommended to enable this mode for devices used by children.



Click **APPLY** when finished.

The selected filtering mode will be applied to all devices connected to the router's network.

Known Clients

IP address: Indicates the IP address of the client.

MAC address: Indicates the MAC address of the client.

Name: Indicates the name of the client.

Rule: Indicates the Yandex rule applied to the client.

Known Clients			
IP Address	MAC Address	Name	Rule
192.168.1.100	08:00:27:00:00:00	AndroidPhone 0	Default (NoAccessAll)
Rules			
☐ MAC address			
Name			
Rule			
APPLY			

Create Rule

MAC address: Specify the MAC address of the device.

Name: Specify the name of the device.

Rule: Specify the rule to apply.

Click **Save** when you are done.

Click **APPLY** when finished.

Create Rule

MAC address

Name

☒ ProtectionOff

☐ Soft

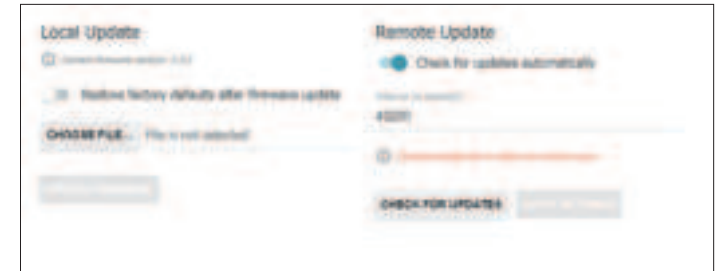
☐ Hard

SAVE

Firmware Update

The Firmware Update page allows you to upgrade firmware manually or you can configure the router to check for updates automatically.

Do not turn off the router before the firmware upgrade is completed. This may cause the device to malfunction.



Local Update

Choose File: Click to select firmware file to update.

Click on **Update Firmware** when ready.

Remote Update

Enable/Disable: Toggle this switch to check for updates automatically.

Interval (in seconds): Specify the interval to check for firmware updates.

Click on **CHECK FOR UPDATES** to check for the latest firmware available from the remote server.

Click on **APPLY SETTINGS** when finished.

Schedule

The schedule page allows you to enable/disable Wi-Fi connection and configure automatic reboot of the device on a schedule, and set a schedule for different filter rules.

Auto Reboot

State: Shows the state of the auto reboot function.

Click on **REBOOT ON SCHEDULE** to add a auto reboot schedule.



All Tasks

Status: Shows the status of the schedule.

State: Shows the state of the schedule.

Schedule: Shows the schedule.

Duration: Shows the duration of the schedule.

Tasks: Shows if tasks will be performed as part of the schedule.

Click (+) when to add a schedule or (-) to delete selected schedule.

Simplified mode

Interval of execution: Specify the time period for the device's reboot.
 Every day: When this value is selected, the Time field is displayed in the section.
 Every week: When this value is selected, the names of days of the week and the Time field are displayed in the section.
 Every month: When this value is selected, the Day of month and Time fields are displayed in the section.

Time: Specify the time for the device's reboot.

Duration: Specify the duration of this schedule.

Click on **SAVE** when finished.

Advanced mode

Minutes: Specify the time to the minute (0-59).

Hours: Specify the time to the hour (0-23).

Day of month: Specify the time to the day of month (1-31).

Month: Specify the time to the month (1-12).

Days of week: Specify the time to the day of the week (0-6).

Schedule: Displays the schedule.

Duration: Specify the duration of this schedule.

Click on **SAVE** when finished.

Statistics

Network Statistics

Network Statistics provides you with various statistics about data transmitted and received through the Internet.

Network Statistics

Name: Name of connection.

IP - Gateway: IP Address and Gateway

Rx/Tx: Receive and Transmit volume

Rx/Tx Errors Number of Rx/Tx errors.

Duration Duration of connection.

Click on the connection to view further details of the connection.



WAN	
Status	WAN
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MAC	88:88:88:88:88:88
Rx/Tx	1000000 / 1000000
Rx/Tx Errors	0 / 0
Duration	0 / 0

Port Statistics

The Port Statistics Page displays statistics of traffic passing through the router by ports.

Port Statistics

Port: The name of port.

Status: Current status of the port.

Traffic sent Amount of traffic sent in Mbyte.

Traffic received Amount of traffic received in Mbyte.

Click on the port to view the full list of counters for the port.



Routing

The Routing page displays information on routing tables and rules.

Rules

Table: Table of traffic rules.

Type: Type of connection type.

IP (Source/Destination): IP addresses.

Interfaces (Incoming/Outgoing): Traffic interfaces.

Priority: QoS traffic priority.

ToS: Type of service.

FWmark (HEX): Hexadecimal FWmark and FWmark mask for Linux Advanced Routing and Traffic Control.

Rules						
Table	Type	IP (Source/Destination)	Interfaces (Incoming/Outgoing)	Priority	ToS	FWmark (HEX)
example1	IPsec	all / all	eth0 / eth0	100	0	0x0
group1	IPsec	all / all	eth0 / eth0	200	0	0x0
rule1	IPsec	all / all	eth0 / eth0	30000	0	0x0
example2	IPsec	all / all	eth0 / eth0	100	0	0x0
group2	IPsec	all / all	eth0 / eth0	200	0	0x0
rule2	IPsec	all / all	eth0 / eth0	30000	0	0x0
Tables						
001	main	Routing table				
004	main	Routing table				
007	group 1	Routing table for group 1				
008	group 2	Routing table for group 2				

Tables

ID: ID of the table.

Name: Name of the table.

Description: Descriptions of the routing table.

Click on the routing table to view detailed data for the routing table.

DHCP

The DHCP page displays information on computers that have received IP addresses from the DHCP of the router.

DHCP

- Hostname:** Hostname of connected device.
- IP Address:** IP address from connected device.
- MAC:** MAC address of connected device.
- Expires:** IP address expiration date (lease time).



Multicast Groups

This page displays addresses and the interface of active multicast group to which the device is subscribed.

IPv4

IP Address: IP address of active IPv4 multicast group.

Interface: Interface of active IPv4 mutlicast group.

IPv6

IP Address: IP address of active IPv6 multicast group.

Interface: Interface of active IPv6 mutlicast group.



Diagnostics Ping

The Ping page allows you to manually check availability of a host from the local or global network.

Host: Address of host.

Count of Packets: Number of packets to send.

IPv6: Toggle this switch to check through IPv6 protocol.

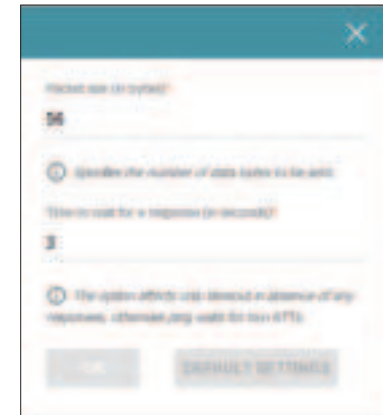
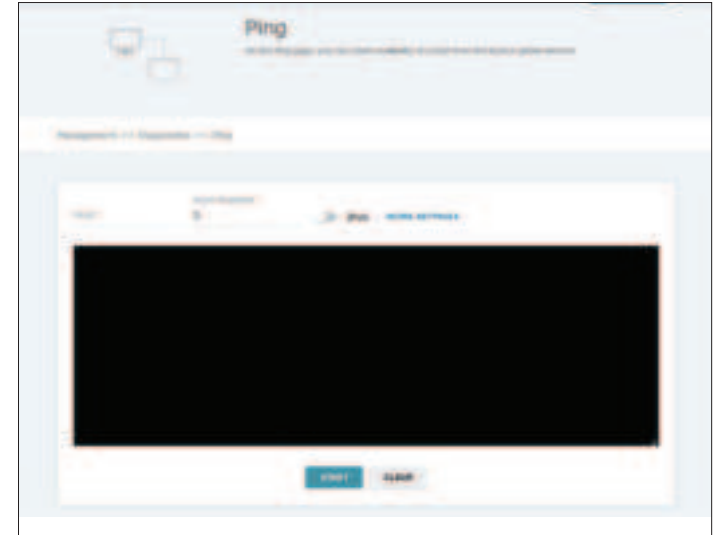
MORE SETTINGS

Packet Size: Number of data bytes to send.

Wait Time: Time to wait for a response in seconds.

Click **OK** to save or **DEFAULT SETTINGS** to reset back to default configuration.

Click **START** to begin Ping Test or **CLEAR** to clear the results.



Traceroute

The Traceroute page allows you to determine the route of data transfer to a host.

Host: Address of the host.

IPv6: Toggle this switch to check the IPv6 protocol.

MORE SETTINGS

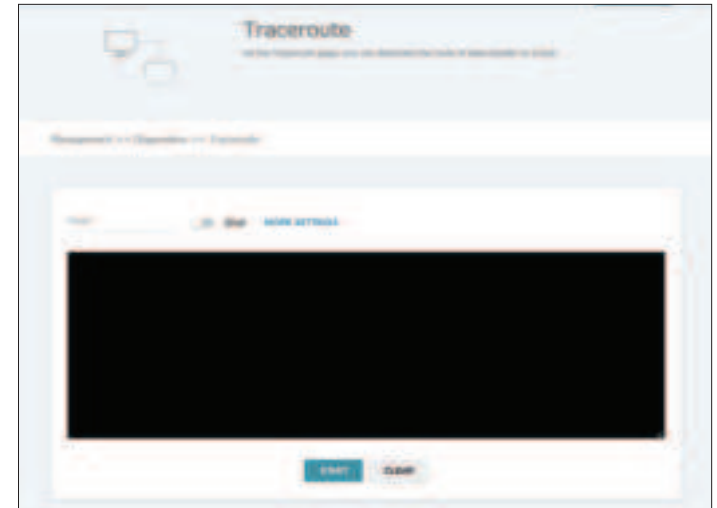
Maximum TTL value: Maximum number of hops.

Number of probes: Number of probe packets to a hop.

Wait Time: Hop response time in seconds.

Click **OK** to save or **DEFAULT SETTINGS** to reset back to default configuration.

Click **START** to begin Traceroute or **CLEAR** to clear the results.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-822. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to these examples.

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

When entering the IP address of the D-Link router (**192.168.0.1** for example), you are not connecting to a website, nor do you 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 10 or higher
 - Firefox 44 or higher
 - Safari 8 or higher
 - Chrome 48 or higher
 - Edge 20.10240 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable, or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as 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 button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

To reset the router, locate the reset button (hole) on the bottom panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait 60 seconds or more to access the router. The default IP address is **192.168.0.1**. When you login, the wizard should start automatically.

3. Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1492

Pinging yahoo.com [66.94.209.101] with 1492 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.209.101:
    Packets: Sent = 4, Received = 0, Loss = 4 (100% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.209.101] with 1472 bytes of data:

Reply from 66.94.209.101: bytes=1472 time=93ms TTL=62
Reply from 66.94.209.101: bytes=1472 time=187ms TTL=62
Reply from 66.94.209.101: bytes=1472 time=125ms TTL=62
Reply from 66.94.209.101: bytes=1472 time=203ms TTL=62

Ping statistics for 66.94.209.101:
    Packets: Sent = 4, Received = 4, Loss = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 93ms, Maximum = 203ms, Average = 102ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, let's say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with ($1452+28=1480$).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (previously specified). Click **Login** to enter the web configuration page for the device.
- In the **Settings** menu on the bar at the top of the page, click on Internet and then go to the **WAN** page. From there click on **Edit** and go to the **All Settings** tab.
- To change the MTU, enter the number in the MTU field and click **Apply** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home Uses/Benefits

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

Small Office and Home Office Uses/Benefits

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

Where is wireless used?

Wireless technology is expanding everywhere, not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link USB adapter with your laptop, you can access the hotspot to connect to the Internet from remote locations like: airports, hotels, coffee shops, libraries, restaurants, and convention centers.

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

Tips

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

Centralize your router or access point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-hoc** – Directly connecting to another computer for peer-to-peer communication using wireless network adapters on each computer, such as two or more DIR-822 wireless network USB adapters.

An Infrastructure network contains an access point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-hoc network contains only clients, such as laptops with wireless USB adapters. All the adapters must be in Ad-hoc mode to communicate.

Networking Basics

Check your IP address

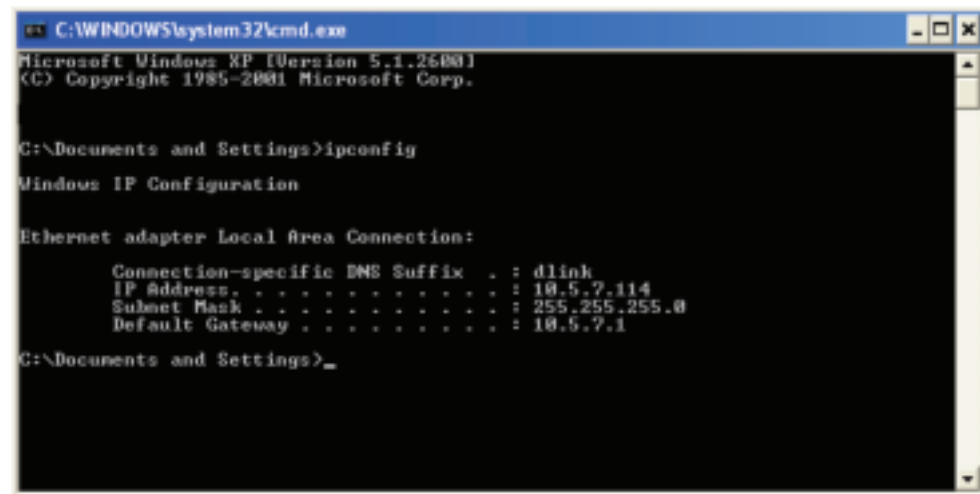
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start** > **Run**. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type *cmd* in the **Start Search** box.)

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . . : 10.5.7.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>
```

Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

Windows® 10 - Click on **Start > Windows System > Control Panel > Network and Internet > Network and Sharing Center**.

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

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

Windows® XP - Click on **Start > Control Panel > Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places > Properties**.

Step 2

Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

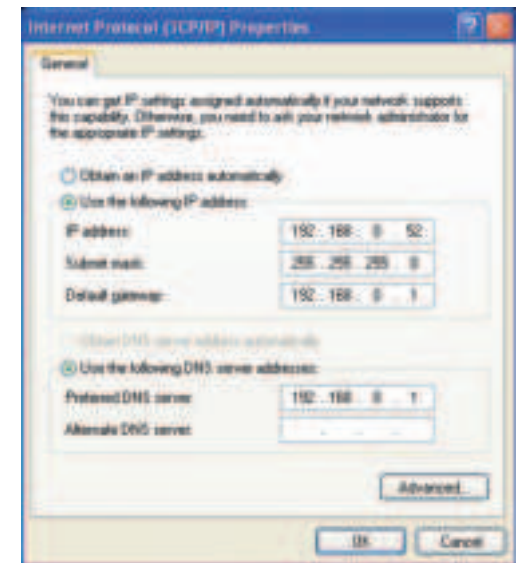
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 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

Device Interfaces

- Wireless Interface (2.4 GHz): IEEE 802.11n/g/b
- Wireless Interface (5 GHz): IEEE 802.11 ac/n/a
- Four 10/100 Mbps LAN ports
- One 10/100 Mbps WAN port

Antenna Types

- Four external antennas

Standards

- IEEE 802.11ac^{1,2,3}
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u

Security

- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise
- WPA3
- Wi-Fi Protected Setup (WPS) PBC

Power

- Input: 100 to 240 V AC, 50/60 Hz

- Output: 12 V DC, 1 A

Temperature

- Operating: 0 to 40 °C (32 to 104 °F)
- Storage: -20 to 65 °C (-4 to 149 °F)

Humidity

- Operating: 10% to 90% maximum, non-condensing
- Storage: 5% to 95% maximum, non-condensing

Certifications

- FCC
- CE

Dimensions & Weight

- 181 x 132.5 x 47.71 mm (7.13 x 5.22 x 1.88 in)
- 304.8 g (0.67 lbs)

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

2 Frequency Range varies depending on country's regulation.

3 The DIR-822 does not include 5.25-5.35 GHz & 5.47-5.725 GHz in some regions.

Regulatory Statements

Federal Communication Commission Interference Statement

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

Non-modifications Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Caution:

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 and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Note

The country code selection is for non-USA models only and is not available to all USA models. Per FCC regulations, all WiFi product marketed in the USA must be fixed to USA operational channels only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 44 cm between the radiator and your body.

Innovation, Science and Economic Development Canada (ISED) Statement:

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Radiation Exposure Statement

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

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

以下警語適用台灣地區

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在5.25-5.35 GHz頻帶內操作之無線資訊傳輸設備，限於室內使用。

電磁波曝露量MPE標準值(MPE) 1 mW/cm²，送測產品實值為 0.77 mW/cm²



	Frequency Band(s) Frequenzband Fréquence bande(s) Bandas de Frecuencia Frequenza/e Frequentie(s)	Max. Output Power (EIRP) Max. Output Power Consommation d'énergie max. Potencia máxima de Salida Potenza max. Output Max. Output Power
5 G	5.15 – 5.25 GHz	200 mW
	5.25 – 5.35 GHz	200 mW
	5.47 – 5.725 GHz	1 W
2.4 G	2.4 – 2.4835 GHz	100 mW

European Community Declaration of Conformity:

Česky [Czech]	Tímto D-Link Corporation prohlašuje, že tento produkt, jeho příslušenství a software jsou v souladu se směrnicí 2014/53/EU. Celý text ES prohlášení o shodě vydaného EU a o firmwaru produktu lze stáhnout na stránkách k produktu www.dlink.com .
Dansk [Danish]	D-Link Corporation erklærer herved, at dette produkt, tilbehør og software er i overensstemmelse med direktiv 2014/53/EU. Den fulde tekst i EU-overensstemmelseserklæringen og produktfirmware kan wnloades fra produktsiden hos www.dlink.com .
Deutsch [German]	Hiermit erklärt die D-Link Corporation, dass dieses Produkt, das Zubehör und die Software der Richtlinie 2014/53/EU entsprechen. Der vollständige Text der Konformitätserklärung der Europäischen Gemeinschaft sowie die Firmware zum Produkt stehen Ihnen zum Herunterladen von der Produktseite im Internet auf www.dlink.com zur Verfügung.
Eesti [Estonian]	Käesolevaga kinnitab D-Link Corporation, et see toode, tarvikud ja tarkvara on kooskõlas direktiiviga 2014/53/EL. Euroopa Liidu vastavusdeklaratsiooni täistekst ja toote püsivara on allalaadimiseks saadaval tootelehel www.dlink.com .
English	Hereby, D-Link Corporation, declares that this product, accessories, and software are in compliance with directive 2014/53/EU. The full text of the EU Declaration of Conformity and product firmware are available for download from the product page at www.dlink.com
Español [Spanish]	Por la presente, D-Link Corporation declara que este producto, accesorios y software cumplen con las directivas 2014/53/UE. El texto completo de la declaración de conformidad de la UE y el firmware del producto están disponibles y se pueden descargar desde la página del producto en www.dlink.com .
Ελληνική [Greek]	Με την παρούσα, η D-Link Corporation δηλώνει ότι αυτό το προϊόν, τα αξεσουάρ και το λογισμικό συμμορφώνονται με την Οδηγία 2014/53/ΕΕ. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ και το υλικολογισμικό του προϊόντος είναι διαθέσιμα για λήψη από τη σελίδα του προϊόντος στην τοποθεσία www.dlink.com .
Français [French]	Par les présentes, D-Link Corporation déclare que ce produit, ces accessoires et ce logiciel sont conformes aux directives 2014/53/UE. Le texte complet de la déclaration de conformité de l'UE et le microprogramme du produit sont disponibles au téléchargement sur la page des produits à www.dlink.com .
Italiano [Italian]	Con la presente, D-Link Corporation dichiara che questo prodotto, i relativi accessori e il software sono conformi alla direttiva 2014/53/UE. Il testo completo della dichiarazione di conformità UE e il firmware del prodotto sono disponibili per il download dalla pagina del prodotto su www.dlink.com .

Latviski [Latvian]	Ar šo uzņēmums D-Link Corporation apliecina, ka šis produkts, piederumi un programmatūra atbilst direktīvai 2014/53/ES. ES atbilstības deklarācijas pilno tekstu un produkta aparātprogrammatūru var lejupielādēt attiecīgā produkta lapā vietnē www.dlink.com .
Lietuvių [Lithuanian]	Šiuo dokumentu „D-Link Corporation“ pareiškia, kad šis gaminys, priedai ir programinė įranga atitinka direktyvą 2014/53/ES. Visą ES atitikties deklaracijos tekstą ir gaminio programinę aparatinę įrangą galima atsisiųsti iš gaminio puslapio adresu www.dlink.com .
Nederlands [Dutch]	Hierbij verklaart D-Link Corporation dat dit product, accessoires en software voldoen aan de richtlijnen 2014/53/EU. De volledige tekst van de EU conformiteitsverklaring en productfirmware is beschikbaar voor download van de productpagina op www.dlink.com .
Malti [Maltese]	Bil-preżenti, D-Link Corporation tiddikjara li dan il-prodott, l-aċċessorji, u s-software huma konformi mad-Direttiva 2014/53/UE. Tista' tniżżel it-test sħiħ tad-dikjarazzjoni ta' konformità tal-UE u l-firmware tal-prodott mill-paġna tal-prodott fuq www.dlink.com .
Magyar [Hungarian]	Ezennel a D-Link Corporation kijelenti, hogy a jelen termék, annak tartozékai és szoftvere megfelelnek a 2014/53/EU sz. rendeletnek rendelkezéseinek. Az EU Megfelelőségi nyilatkozat teljes szövege és a termék firmware a termék oldaláról tölthető le a www.dlink.com címen.
Polski [Polish]	D-Link Corporation niniejszym oświadcza, że ten produkt, akcesoria oraz oprogramowanie są zgodne z dyrektywami 2014/53/EU. Pełen tekst deklaracji zgodności UE oraz oprogramowanie sprzętowe do produktu można pobrać na stronie produktu w witrynie www.dlink.com .
Português [Portuguese]	Desta forma, a D-Link Corporation declara que este produto, os acessórios e o software estão em conformidade com a diretiva 2014/53/UE. O texto completo da declaração de conformidade da UE e do firmware
Slovensko[Slovenian]	Podjetje D-Link Corporation s tem izjavlja, da so ta izdelek, dodatna oprema in programnska oprema skladni z direktivami 2014/53/EU. Celotno besedilo izjave o skladnosti EU in vdelana programska oprema sta na voljo za prenos na strani izdelka na www.dlink.com .
Slovensky [Slovak]	Spoločnosť D-Link týmto vyhlasuje, že tento produkt, príslušenstvo a softvér sú v súlade so smernicou 214/53/EÚ. Úplné znenie vyhlásenia EÚ o zhode a firmvéri produktu sú k dispozícii na prevzatie zo stránky produktu www.dlink.com .
Suomi [Finnish]	D-Link Corporation täten vakuuttaa, että tämä tuote, lisävarusteet ja ohjelmisto ovat direktiivin 2014/53/EU vaatimusten mukaisia. Täydellinen EU-vaatimustenmukaisuusvakuutus samoin kuin tuotteen laiteohjelmisto ovat ladattavissa osoitteesta www.dlink.com .

Svenska[Swedish]	D-Link Corporation försäkrar härmed att denna produkt, tillbehör och programvara överensstämmer med direktiv 2014/53/EU. Hela texten med EU-försäkran om överensstämmelse och produkt-firmware kan hämtas från produktsidan på www.dlink.com .
Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara, fylgihlutir og hugbúnaður eru í samræmi við tilskipun 2014/53/EB. Sækja má ESB-samræmisýfirlýsinguna í heild sinni og fastbúnað vörunnar af vefsíðu vörunnar á www.dlink.com .
Norsk [Norwegian]	Herved erklærer D-Link Corporation at dette produktet, tilbehøret og programvaren er i samsvar med direktivet 2014/53/EU. Den fullstendige teksten i EU-erklæring om samsvar og produktets fastvare er tilgjengelig for nedlasting fra produktsiden på www.dlink.com .

Warning Statement:

The power outlet should be near the device and easily accessible.

NOTICE OF WIRELESS RADIO LAN USAGE IN THE EUROPEAN COMMUNITY (FOR WIRELESS PRODUCT ONLY):

- This device is restricted to indoor use when operated in the European Community using channels in the 5.15-5.35 GHz band to reduce the potential for interference.
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries. This equipment may be operated in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, and CY.

Usage Notes:

- To remain in conformance with European National spectrum usage regulations, frequency and channel limitations will be applied on the products according to the country where the equipment will be deployed.
- This device is restricted from functioning in Ad-hoc mode while operating in 5 GHz. Ad-hoc mode is direct peer-to-peer communication between two client devices without an Access Point.
- Access points will support DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) functionality as required when operating in 5 GHz band within the EU.
- Please refer to the product manual or datasheet to check whether your product uses 2.4 GHz and/or 5 GHz wireless.

HINWEIS ZUR VERWENDUNG VON DRAHTLOS-NETZWERK (WLAN) IN DER EUROPÄISCHEN GEMEINSCHAFT (NUR FÜR EIN DRAHTLOSES PRODUKT)

- Der Betrieb dieses Geräts in der Europäischen Gemeinschaft bei Nutzung von Kanälen im 5,15-5,35 GHz Frequenzband ist ausschließlich auf Innenräume beschränkt, um das Interferenzpotential zu reduzieren.
- Bei diesem Gerät handelt es sich um ein zum Einsatz in allen EU-Mitgliedsstaaten und in EFTA-Ländern - ausgenommen Frankreich. Der Betrieb dieses Geräts ist in den folgenden Ländern erlaubt: AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebrauchshinweise:

- Um den in Europa geltenden nationalen Vorschriften zum Nutzen des Funkspektrums weiterhin zu entsprechen, werden Frequenz und Kanalbeschränkungen, dem jeweiligen Land, in dem das Gerät zum Einsatz kommt, entsprechend, auf die Produkte angewandt.
- Die Funktionalität im Ad-hoc-Modus bei Betrieb auf 5 GHz ist für dieses Gerät eingeschränkt. Bei dem Ad-hoc-Modus handelt es sich um eine Peer-to-Peer-Kommunikation zwischen zwei Client-Geräten ohne einen Access Point.
- Access Points unterstützen die Funktionen DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) wie erforderlich bei Betrieb auf 5 GHz innerhalb der EU.
- Bitte schlagen Sie im Handbuch oder Datenblatt nach, ob Ihr Gerät eine 2,4 GHz und / oder 5 GHz Verbindung nutzt.

AVIS CONCERNANT L'UTILISATION DE LA RADIO SANS FIL LAN DANS LA COMMUNAUTÉ EUROPÉENNE (UNIQUEMENT POUR LES PRODUITS SANS FIL)

- Cet appareil est limité à un usage intérieur lorsqu'il est utilisé dans la Communauté européenne sur les canaux de la bande de 5,15 à 5,35 GHz afin de réduire les risques d'interférences.
- Cet appareil est un système de transmission à large bande (émetteur-récepteur) de 2,4 GHz, destiné à être utilisé dans tous les États-membres de l'UE et les pays de l'AELE. Cet équipement peut être utilisé dans les pays suivants : AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notes d'utilisation:

- Pour rester en conformité avec la réglementation nationale européenne en matière d'utilisation du spectre, des limites de fréquence et de canal seront appliquées aux produits selon le pays où l'équipement sera déployé.
- Cet appareil ne peut pas utiliser le mode Ad-hoc lorsqu'il fonctionne dans la bande de 5 GHz. Le mode Adhoc fournit une communication directe pair à pair entre deux périphériques clients sans point d'accès.
- Les points d'accès prendront en charge les fonctionnalités DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control) au besoin lors du fonctionnement dans la bande de 5 GHz au sein de l'UE.
- Merci de vous référer au guide d'utilisation ou de la fiche technique afin de vérifier si votre produit utilise 2.4 GHz et/ou 5 GHz sans fil.

AVISO DE USO DE LA LAN DE RADIO INALÁMBRICA EN LA COMUNIDAD EUROPEA (SOLO PARA EL PRODUCTO INALÁMBRICO)

- El uso de este dispositivo está restringido a interiores cuando funciona en la Comunidad Europea utilizando canales en la banda de 5,15-5,35 GHz, para reducir la posibilidad de interferencias.
- Este dispositivo es un sistema de transmisión (transceptor) de banda ancha de 2,4 GHz, pensado para su uso en todos los estados miembros de la UE y en los países de la AELC. Este equipo se puede utilizar en AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notas de uso:

- Para seguir cumpliendo las normas europeas de uso del espectro nacional, se aplicarán limitaciones de frecuencia y canal en los productos en función del país en el que se pondrá en funcionamiento el equipo.
- Este dispositivo tiene restringido el funcionamiento en modo Ad-hoc mientras funcione a 5 GHz. El modo Ad-hoc es la comunicación directa de igual a igual entre dos dispositivos cliente sin un punto de acceso.
- Los puntos de acceso admitirán la funcionalidad DFS (Selección de frecuencia dinámica) y TPC (Control de la potencia de transmisión) si es necesario cuando funcionan a 5 GHz dentro de la UE.
- Por favor compruebe el manual o la ficha de producto para comprobar si el producto utiliza las bandas inalámbricas de 2.4 GHz y/o la de 5 GHz.

AVVISO PER L'USO DI LAN RADIO WIRELESS NELLA COMUNITÀ EUROPEA (SOLO PER PRODOTTI WIRELESS)

- Nella Comunità europea, l'uso di questo dispositivo è limitato esclusivamente agli ambienti interni sui canali compresi nella banda da 5,15 a 5,35 GHz al fine di ridurre potenziali interferenze. Questo dispositivo è un sistema di trasmissione a banda larga a 2,4 GHz (ricetrasmittente), destinato all'uso in tutti gli stati membri dell'Unione europea e nei paesi EFTA.
- Questo dispositivo può essere utilizzato in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Note per l'uso

- Al fine di mantenere la conformità alle normative nazionali europee per l'uso dello spettro di frequenze, saranno applicate limitazioni sulle frequenze e sui canali per il prodotto in conformità alle normative del paese in cui il dispositivo viene utilizzato.
- Questo dispositivo non può essere attivato in modalità Ad-hoc durante il funzionamento a 5 GHz. La modalità Ad-hoc è una comunicazione diretta peer-to-peer fra due dispositivi client senza un punto di accesso.
- I punti di accesso supportano le funzionalità DFS (Dynamic Frequency Selection) e TPC (Transmit Power Control) richieste per operare a 5 GHz nell'Unione europea.
- Ti invitiamo a fare riferimento al manuale del prodotto o alla scheda tecnica per verificare se il tuo prodotto utilizza le frequenze 2,4 GHz e/o 5 GHz.

KENNISGEVING VAN DRAADLOOS RADIO LAN-GEBRUIK IN DE EUROPESE GEMEENSCHAP (ALLEEN VOOR DRAADLOOS PRODUCT)

- Dit toestel is beperkt tot gebruik binnenshuis wanneer het wordt gebruikt in de Europese Gemeenschap gebruik makend van kanalen in de 5.15-5.35 GHz band om de kans op interferentie te beperken.
- Dit toestel is een 2.4 GHz breedband transmissiesysteem (transceiver) dat bedoeld is voor gebruik in alle EU lidstaten en EFTA landen. Deze uitrusting mag gebruikt worden in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebruiksaanwijzingen:

- Om de gebruiksvoorschriften van het Europese Nationale spectrum na te leven, zullen frequentie- en kanaalbeperkingen worden toegepast op de producten volgens het land waar de uitrusting gebruikt zal worden.
- Dit toestel kan niet functioneren in Ad-hoc mode wanneer het gebruikt wordt in 5 GHz. Ad-hoc mode is directe peer-to-peer communicatie tussen twee klantenapparaten zonder een toegangspunt.
- Toegangspunten ondersteunen DFS (Dynamic Frequency Selection) en TPC (Transmit Power Control) functionaliteit zoals vereist bij gebruik in 5 GHz binnen de EU.
- Raadpleeg de handleiding of de datasheet om te controleren of uw product gebruik maakt van 2.4 GHz en/of 5 GHz.

SAFETY INSTRUCTIONS

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product user instructions for more details.

- Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e. touching grounded bare metal) before touching the product.
- Do not attempt to service the product and never disassemble the product. For some products with a user replaceable battery, please read and follow the instructions in the user manual.
- Do not spill food or liquid on your product and never push any objects into the openings of your product.
- Do not use this product near water, areas with high humidity, or condensation unless the product is specifically rated for outdoor application.
- Keep the product away from radiators and other heat sources.
- Always unplug the product from mains power before cleaning and use a dry lint free cloth only.

SICHERHEITSVORSCHRIFTEN

Die folgenden allgemeinen Sicherheitsvorschriften dienen als Hilfe zur Gewährleistung Ihrer eigenen Sicherheit und zum Schutz Ihres Produkts. Weitere Details finden Sie in den Benutzeranleitungen zum Produkt.

- Statische Elektrizität kann elektronischen Komponenten schaden. Um Schäden durch statische Aufladung zu vermeiden, leiten Sie elektrostatische Ladungen von Ihrem Körper ab, (z. B. durch Berühren eines geerdeten blanken Metallteils), bevor Sie das Produkt berühren.
- Unterlassen Sie jeden Versuch, das Produkt zu warten, und versuchen Sie nicht, es in seine Bestandteile zu zerlegen. Für einige Produkte mit austauschbaren Akkus lesen Sie bitte das Benutzerhandbuch und befolgen Sie die dort beschriebenen Anleitungen.
- Vermeiden Sie, dass Speisen oder Flüssigkeiten auf Ihr Produkt gelangen, und stecken Sie keine Gegenstände in die Gehäuseschlitze oder -öffnungen Ihres Produkts.
- Verwenden Sie dieses Produkt nicht in unmittelbarer Nähe von Wasser und nicht in Bereichen mit hoher Luftfeuchtigkeit oder Kondensation, es sei denn, es ist speziell zur Nutzung in Außenbereichen vorgesehen und eingestuft.
- Halten Sie das Produkt von Heizkörpern und anderen Quellen fern, die Wärme erzeugen.
- Trennen Sie das Produkt immer von der Stromzufuhr, bevor Sie es reinigen und verwenden Sie dazu ausschließlich ein trockenes fusselfreies Tuch.

CONSIGNES DE SÉCURITÉ

Les consignes générales de sécurité ci-après sont fournies afin d'assurer votre sécurité personnelle et de protéger le produit d'éventuels dommages. Veuillez consulter les consignes d'utilisation du produit pour plus de détails.

- L'électricité statique peut endommager les composants électroniques. Déchargez l'électricité statique de votre corps (en touchant un objet en métal relié à la terre par exemple) avant de toucher le produit.
- N'essayez pas d'intervenir sur le produit et ne le démontez jamais. Pour certains produits contenant une batterie remplaçable par l'utilisateur, veuillez lire et suivre les consignes contenues dans le manuel d'utilisation.
- Ne renversez pas d'aliments ou de liquide sur le produit et n'insérez jamais d'objets dans les orifices.
- N'utilisez pas ce produit à proximité d'un point d'eau, de zones très humides ou de condensation sauf si le produit a été spécifiquement conçu pour une application extérieure.
- Éloignez le produit des radiateurs et autres sources de chaleur.
- Débranchez toujours le produit de l'alimentation avant de le nettoyer et utilisez uniquement un chiffon sec non pelucheux.

INSTRUCCIONES DE SEGURIDAD

Las siguientes directrices de seguridad general se facilitan para ayudarle a garantizar su propia seguridad personal y para proteger el producto frente a posibles daños. No olvide consultar las instrucciones del usuario del producto para obtener más información.

- La electricidad estática puede resultar nociva para los componentes electrónicos. Descargue la electricidad estática de su cuerpo (p. ej., tocando algún metal sin revestimiento conectado a tierra) antes de tocar el producto.
- No intente realizar el mantenimiento del producto ni lo desmonte nunca. Para algunos productos con batería reemplazable por el usuario, lea y siga las instrucciones del manual de usuario.
- No derrame comida o líquidos sobre el producto y nunca deje que caigan objetos en las aberturas del mismo.
- No utilice este producto cerca del agua, en zonas con humedad o condensación elevadas a menos que el producto esté clasificado específicamente para aplicación en exteriores.
- Mantenga el producto alejado de los radiadores y de otras fuentes de calor.
- Desenchufe siempre el producto de la alimentación de red antes de limpiarlo y utilice solo un paño seco sin pelusa.

ISTRUZIONI PER LA SICUREZZA

Le seguenti linee guida sulla sicurezza sono fornite per contribuire a garantire la sicurezza personale degli utenti e a proteggere il prodotto da potenziali danni. Per maggiori dettagli, consultare le istruzioni per l'utente del prodotto.

- L'elettricità statica può essere pericolosa per i componenti elettronici. Scaricare l'elettricità statica dal corpo (ad esempio toccando una parte metallica collegata a terra) prima di toccare il prodotto.
- Non cercare di riparare il prodotto e non smontarlo mai. Per alcuni prodotti dotati di batteria sostituibile dall'utente, leggere e seguire le istruzioni riportate nel manuale dell'utente.
- Non versare cibi o liquidi sul prodotto e non spingere mai alcun oggetto nelle aperture del prodotto.
- Non usare questo prodotto vicino all'acqua, in aree con elevato grado di umidità o soggette a condensa a meno che il prodotto non sia specificatamente approvato per uso in ambienti esterni.
- Tenere il prodotto lontano da caloriferi e altre fonti di calore.
- Scollegare sempre il prodotto dalla presa elettrica prima di pulirlo e usare solo un panno asciutto che non lasci filacce.

VEILIGHEIDSGEGEGENSTANDEN

De volgende algemene veiligheidsinformatie werd verstrekt om uw eigen persoonlijke veiligheid te waarborgen en uw product te beschermen tegen mogelijke schade. Denk eraan om de gebruikersinstructies van het product te raadplegen voor meer informatie.

- Statische elektriciteit kan schadelijk zijn voor elektronische componenten. Ontlaad de statische elektriciteit van uw lichaam (d.w.z. het aanraken van geaard bloot metaal) voordat u het product aanraakt.
- U mag nooit proberen het product te onderhouden en u mag het product nooit demonteren. Voor sommige producten met door de gebruiker te vervangen batterij, dient u de instructies in de gebruikershandleiding te lezen en te volgen.
- Mors geen voedsel of vloeistof op uw product en u mag nooit voorwerpen in de openingen van uw product duwen.
- Gebruik dit product niet in de buurt van water, gebieden met hoge vochtigheid of condensatie, tenzij het product specifiek geclassificeerd is voor gebruik buitenshuis.
- Houd het product uit de buurt van radiators en andere warmtebronnen.
- U dient het product steeds los te koppelen van de stroom voordat u het reinigt en gebruik uitsluitend een droge pluisvrije doek.

Disposing of and Recycling Your Product

ENGLISH

EN



This symbol on the product or packaging means that according to local laws and regulations this product should not be disposed of in household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will accept products for free. By recycling the product and its packaging in this manner you help to conserve the environment and protect human health.

D-Link and the Environment

At D-Link, we understand and are committed to reducing any impact our operations and products may have on the environment. To minimise this impact D-Link designs and builds its products to be as environmentally friendly as possible, by using recyclable, low toxic materials in both products and packaging.

D-Link recommends that you always switch off or unplug your D-Link products when they are not in use. By doing so you will help to save energy and reduce CO2 emissions.

To learn more about our environmentally responsible products and packaging please visit www.dlinkgreen.com.

DEUTSCH

DE



Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde entsprechend amtlich ausgewiesenen Sammelstelle, sobald das Produkt das Ende seiner Nutzungsdauer erreicht hat. Für die Annahme solcher Produkte erheben einige dieser Stellen keine Gebühren. Durch ein auf diese Weise durchgeführtes Recycling des Produkts und seiner Verpackung helfen Sie, die Umwelt zu schonen und die menschliche Gesundheit zu schützen.

D-Link und die Umwelt

D-Link ist sich den möglichen Auswirkungen seiner Geschäftstätigkeiten und seiner Produkte auf die Umwelt bewusst und fühlt sich verpflichtet, diese entsprechend zu mindern. Zu diesem Zweck entwickelt und stellt D-Link seine Produkte mit dem Ziel größtmöglicher Umweltfreundlichkeit her und verwendet wiederverwertbare, schadstoffarme Materialien bei Produktherstellung und Verpackung.

D-Link empfiehlt, Ihre Produkte von D-Link, wenn nicht in Gebrauch, immer auszuschalten oder vom Netz zu nehmen. Auf diese Weise helfen Sie, Energie zu sparen und CO2-Emissionen zu reduzieren.

Wenn Sie mehr über unsere umweltgerechten Produkte und Verpackungen wissen möchten, finden Sie entsprechende Informationen im Internet unter www.dlinkgreen.com.

FRANÇAIS**FR**

Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et réglementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront vos produits gratuitement. En recyclant le produit et son emballage de cette manière, vous aidez à préserver l'environnement et à protéger la santé de l'homme.

D-Link et l'environnement

Chez D-Link, nous sommes conscients de l'impact de nos opérations et produits sur l'environnement et nous engageons à le réduire. Pour limiter cet impact, D-Link conçoit et fabrique ses produits de manière aussi écologique que possible, en utilisant des matériaux recyclables et faiblement toxiques, tant dans ses produits que ses emballages.

D-Link recommande de toujours éteindre ou débrancher vos produits D-Link lorsque vous ne les utilisez pas. Vous réaliserez ainsi des économies d'énergie et réduirez vos émissions de CO2.

Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le www.dlinkgreen.com.

ESPAÑOL**ES**

Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida útil; algunos de ellos aceptan recogerlos de forma gratuita. Al reciclar el producto y su embalaje de esta forma, contribuye a preservar el medio ambiente y a proteger la salud de los seres humanos.

D-Link y el medio ambiente

En D-Link, comprendemos y estamos comprometidos con la reducción del impacto que puedan tener nuestras actividades y nuestros productos en el medio ambiente. Para reducir este impacto, D-Link diseña y fabrica sus productos para que sean lo más ecológicos posible, utilizando materiales reciclables y de baja toxicidad tanto en los productos como en el embalaje.

D-Link recomienda apagar o desenchufar los productos D-Link cuando no se estén utilizando. Al hacerlo, contribuirá a ahorrar energía y a reducir las emisiones de CO2.

Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio www.dlinkgreen.com.

ITALIANO**IT**

La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto di raccolta indicato dalle autorità locali. Alcuni questi punti di raccolta accettano gratuitamente i prodotti da riciclare. Scegliendo di riciclare il prodotto e il relativo imballaggio, si contribuirà a preservare l'ambiente e a salvaguardare la salute umana.

D-Link e l'ambiente

D-Link cerca da sempre di ridurre l'impatto ambientale dei propri stabilimenti e dei propri prodotti. Allo scopo di ridurre al minimo tale impatto, D-Link progetta e realizza i propri prodotti in modo che rispettino il più possibile l'ambiente, utilizzando materiali riciclabili a basso tasso di tossicità sia per i prodotti che per gli imballaggi.

D-Link raccomanda di spegnere sempre i prodotti D-Link o di scollegarne la spina quando non vengono utilizzati. In questo modo si contribuirà a risparmiare energia e a ridurre le emissioni di anidride carbonica.

Per ulteriori informazioni sui prodotti e sugli imballaggi D-Link a ridotto impatto ambientale, visitate il sito all'indirizzo **www.dlinkgreen.com**.

NEDERLANDS**NL**

Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te brengen dat hiertoe werd aangeduid door uw plaatselijke autoriteiten, sommige autoriteiten accepteren producten zonder dat u hiervoor dient te betalen. Door het product en de verpakking op deze manier te recyclen helpt u het milieu en de gezondheid van de mens te beschermen.

D-Link en het milieu

Bij D-Link spannen we ons in om de impact van onze handelingen en producten op het milieu te beperken. Om deze impact te beperken, ontwerpt en bouwt D-Link zijn producten zo milieuvriendelijk mogelijk, door het gebruik van recycleerbare producten met lage toxiciteit in product en verpakking.

D-Link raadt aan om steeds uw D-Link producten uit te schakelen of uit de stekker te halen wanneer u ze niet gebruikt. Door dit te doen bespaart u energie en beperkt u de CO₂-emissies.

Breng een bezoek aan **www.dlinkgreen.com** voor meer informatie over onze milieuverantwoorde producten en verpakkingen.

POLSKI**PL**

Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie do tego celu podmioty przyjmą takie produkty nieodpłatnie, dlatego prosimy dostarczyć go do punktu zbiórki wskazanego przez lokalne władze. Poprzez proces recyklingu i dzięki takiemu postępowaniu z produktem oraz jego opakowaniem, pomogą Państwo chronić środowisko naturalne i dbać o ludzkie zdrowie.

D-Link i środowisko

D-Link podchodzimy w sposób świadomy do ochrony otoczenia oraz jesteśmy zaangażowani w zmniejszanie wpływu naszych działań i produktów na środowisko naturalne. W celu zminimalizowania takiego wpływu firma D-Link konstruuje i wytwarza swoje produkty w taki sposób, aby były one jak najbardziej przyjazne środowisku, stosując do tych celów materiały nadające się do powtórnego wykorzystania, charakteryzujące się małą toksycznością zarówno w przypadku samych produktów jak i opakowań.

Firma D-Link zaleca, aby Państwo zawsze prawidłowo wyłączali z użytku swoje produkty D-Link, gdy nie są one wykorzystywane. Postępując w ten sposób pozwalają Państwo oszczędzać energię i zmniejszać emisje CO₂.

Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną Internetową www.dlinkgreen.com.

ČESKY**CZ**

Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odnese jej prosím na sběrné místo určené místními úřady k tomuto účelu. Někteří sběrná místa přijímají výrobky zdarma. Recyklací výrobku i obalu pomáháte chránit životní prostředí i lidské zdraví.

D-Link a životní prostředí

Ve společnosti D-Link jsme si vědomi vlivu našich provozů a výrobků na životní prostředí a snažíme se o minimalizaci těchto vlivů. Proto své výrobky navrhujeme a vyrábíme tak, aby byly co nejekologičtější, a ve výrobcích i obalech používáme recyklovatelné a nízkotoxické materiály.

Společnost D-Link doporučuje, abyste své výrobky značky D-Link vypnuli nebo vytáhli ze zásuvky vždy, když je nepoužíváte. Pomůžete tak šetřit energii a snížit emise CO₂.

Více informací o našich ekologických výrobcích a obalech najdete na adrese www.dlinkgreen.com.

MAGYAR**HU**

Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által kijelölt gyűjtőhelyre. A termékek egyes helyeken ingyen elhelyezhetők. A termék és a csomagolás újrahasznosításával segíti védeni a környezetet és az emberek egészségét.

A D-Link és a környezet

A D-Linknél megértjük és elköteleztük magunkat a műveleteink és termékeink környezetre gyakorolt hatásainak csökkentésére. Az ezen hatás csökkentése érdekében a D-Link a lehető leginkább környezetbarát termékeket tervez és gyárt azért, hogy újrahasznosítható, alacsony károsanyag-tartalmú termékeket gyárt és csomagolásokat alkalmaz.

A D-Link azt javasolja, hogy mindig kapcsolja ki vagy húzza ki a D-Link termékeket a tápforrásból, ha nem használja azokat. Ezzel segít az energia megtakarításában és a széndioxid kibocsátásának csökkentésében.

Környezetbarát termékeinkről és csomagolásainkról további információkat a www.dlinkgreen.com weboldalon tudhat meg.

NORSK**NO**

Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet. For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO2-utslipp.

For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til www.dlinkgreen.com.

DANSK**DK**



Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.

D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO₂-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på www.dlinkgreen.com.

SUOMI

FI



Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittelemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta www.dlinkgreen.com.

SVENSKA

SE



Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar www.dlinkgreen.com.

PORTUGUÊS

PT



Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando materiais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO₂.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite www.dlinkgreen.com.