D-Link®

DIR-615

Wireless N300 Router

Contents

CHAPTER 1.   INTRODUCTION

Contents and Audience

This manual describes the router DIR-615 and explains how to configure and operate it.

This manual is intended for users familiar with basic networking concepts, who create an in-home local area network, and system administrators, who install and configure networks in offices.

Conventions

Example	Description
text	The body text of the manual.
Before You Begin	A reference to a chapter or section of this manual.
"Quick Installation Guide"	A reference to a document.
Change	A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.).
`192.168.0.1`	Data that you should enter in the specified field.
❗ Information	An important note.

Document Structure

Chapter 1 describes the purpose and structure of the document.

Chapter 2 gives an overview of the router's hardware and software features, describes its appearance and the package contents.

Chapter 3 explains how to install the router DIR-615 and configure a PC in order to access its web-based interface.

Chapter 4 describes all pages of the web-based interface in detail.

Chapter 5 includes safety instructions and tips for networking.

Chapter 6 introduces abbreviations and acronyms most commonly used in User Manuals for D-Link customer premises equipment.

CHAPTER 2.   OVERVIEW

General Information

The DIR-615 device is a wireless router with a built-in 4-port switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

You are able to connect the wireless router DIR-615 to a cable or DSL modem or to a private Ethernet line and use a high-speed Internet connection to successfully fulfill a wide range of professional tasks. The built-in 4-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network.

Using the DIR-615 device, you are able to quickly create a wireless network at home or in your office, which lets computers and mobile devices access the Internet virtually anywhere (within the operational range of your wireless network). The router can operate as a base station for connecting wireless devices of the standards 802.11b, 802.11g, and 802.11n (at the rate up to 300Mbps).

The router supports multiple functions for the wireless interface: several security standards (WEP, WPA/WPA2), MAC address filtering, WPS, WMM.

Support of guest Wi-Fi network allows you to create a separate wireless network with individual security settings and maximum rate limitation. Devices connected to the guest network will be able to access the Internet, but will be isolated from the devices and resources of the router's LAN.

The built-in 4-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network.

The wireless router DIR-615 includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

Built-in Yandex.DNS service protects against malicious and fraudulent web sites and helps to block access to adult content on children's devices.

You can configure the settings of the wireless router DIR-615 via the user-friendly web-based interface (the interface is available in several languages).

The configuration wizard allows you to quickly switch DIR-615 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.

Also DIR-615 supports configuration and management via mobile application for Android and iPhone smartphones.

You can simply update the firmware: the router itself finds approved firmware on D-Link update server and notifies when ready to install it.

*Specifications**

Hardware	
Processor	· RTL8196E (400MHz)
RAM	· 32MB, DDR SDRAM
Flash	· 4MB, SPI
Interfaces	· 10/100BASE-TX WAN port · 4 10/100BASE-TX LAN ports
LEDs	· Internet · WLAN / WPS · Power
Buttons	· WPS/RESET button to set up wireless connection and restore factory default settings
Antenna	· Two external non-detachable antennas (5dBi gain)
MIMO	· 2 x 2
Power connector	· Power input connector (DC)

Software	
WAN connection types	· PPPoE · IPv6 PPPoE · PPPoE Dual Stack · Static IPv4 / Dynamic IPv4 · Static IPv6 / Dynamic IPv6 · PPPoE + Static IP (PPPoE Dual Access) · PPPoE + Dynamic IP (PPPoE Dual Access) · PPTP/L2TP + Static IP · PPTP/L2TP + Dynamic IP
Network functions	· DHCP server/relay · Advanced configuration of built-in DHCP server · Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation · Automatic obtainment of LAN IP address (for access point/repeater/client modes) · DNS relay · Dynamic DNS · Static IPv4/IPv6 routing · IGMP Proxy · Support of UPnP IGD · Support of VLAN · WAN ping respond · Support of SIP ALG · Support of RTSP · WAN failover · Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port · Setup of maximum TX rate for each port of the router

---

* The device features are subject to change without notice. For the latest versions of the firmware and relevant documentation, visit www.dlink.ru.

Software

Firewall functions	· Network Address Translation (NAT) · Stateful Packet Inspection (SPI) · IPv4/IPv6 filter · MAC filter · URL filter · DMZ · Prevention of ARP and DDoS attacks · Virtual servers · Built-in Yandex.DNS web content filtering service
VPN	· IPsec/PPTP/L2TP/PPPoE pass-through · PPTP/L2TP tunnels
Management and monitoring	· Local and remote access to settings through TELNET/WEB (HTTP/HTTPS) · Multilingual web-based interface for configuration and management · Support of D-Link Assistant application for Android and iPhone smartphones · Notification on connection problems and auto redirect to settings · Firmware update via web-based interface · Automatic notification on new firmware version · Saving/restoring configuration to/from file · Support of logging to remote host · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility · TR-069 client · Automatic reboot on schedule

Wireless Module Parameters

Standards	· IEEE 802.11b/g/n
Frequency range *The frequency range depends upon the radio frequency regulations applied in your country*	· 2400 ~ 2483.5MHz
Wireless connection security	· WEP · WPA/WPA2 (Personal/Enterprise) · MAC filter · WPS (PBC)
Advanced functions	· Support of client mode · WMM (Wi-Fi QoS) · Information on connected Wi-Fi clients · Advanced settings · Guest Wi-Fi / support of MBSSID · Rate limitation for wireless network/separate MAC addresses · Periodic scan of channels, automatic switch to least loaded channel · Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence)
Wireless connection rate	· IEEE 802.11b: 1, 2, 5.5, and 11Mbps · IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11n: from 6.5 to 300Mbps (from MCS0 to MCS15)
Transmitter output power *The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country*	· 802.11b (typical at room temperature 25 °C) 15dBm at 1, 2, 5.5, 11Mbps

Wireless Module Parameters	
Receiver sensitivity	· 802.11n (typical at PER = 10% at room temperature 25 °C) HT20 -74dBm at MCS7/15 HT40 -71.5dBm at MCS7/15
Modulation schemes	· 802.11b: DQPSK, DBPSK, and CCK · 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM · 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM

Physical Parameters	
Dimensions (L x W x H)	· 158 x 131 x 36 mm (6.2 x 5.2 x 1.4 in)

Operating Environment	
Power	· Output: 5V DC, 1A
Temperature	· Operating: from 0 to 40 °C · Storage: from -20 to 65 °C
Humidity	· Operating: from 10% to 90% (non-condensing) · Storage: from 5% to 90% (non-condensing)

Product Appearance

Upper Panel

Figure 1. Upper panel view.

LED	Mode	Description
Internet	*Solid blue*	The default WAN connection is on.
	Fast blinking blue	The router is being loaded.
	Slow blinking blue	The firmware is being updated.
	No light	• There are no WAN connections created, or • the default WAN connection is off, or • the WAN cable is not connected.
WLAN / WPS	*Solid blue*	The router's WLAN is on.
	Fast blinking blue	Data transfer through the Wi-Fi network.
	Slow blinking blue	Attempting to add a wireless device via the WPS function.
	No light	The router's WLAN is off.

LED	Mode	Description
Power	*Solid blue*	The router is powered on.
	No light	The router is powered off.

Back Panel

Figure 2. Back panel view.

Name	Description
5V	Power connector.
LAN 1-4	4 Ethernet ports to connect computers or network devices.
WAN	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).
WPS/RESET	A button to set up a wireless connection (the WPS function) and to restore the factory default settings. To use the WPS function: with the device turned on, push the button and release. The **WLAN / WPS** LED should start blinking slowly. To restore the factory defaults: with the device turned on, push the button, hold it for 10 seconds, and then release the button.

The device is also equipped with two external non-detachable Wi-Fi antennas.

Delivery Package

The following should be included:

- Router DIR-615
- Power adapter DC 5V/1A
- Ethernet cable
- "*Quick Installation Guide*" (brochure).

The "*User Manual*" and "*Quick Installation Guide*" documents are available on D-Link website (see www.dlink.ru).

> ❗ Using a power supply with a different voltage rating than the one included will cause damage and void the warranty for this product.

CHAPTER 3.   INSTALLATION AND CONNECTION

Before You Begin

Please, read this manual prior to installing the device. Make sure that you have all the necessary information and equipment.

Computer or Mobile Device

Configuration of the wireless router DIR-615 with a built-in 4-port switch (hereinafter referred to as "the router") is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

Also you can use D-Link Assistant application for Android or iPhone mobile devices (smartphones or tablets).

PC Web Browser

The following PC web browsers are recommended:

- Apple Safari 8 and later
- Google Chrome 48 and later
- Microsoft Internet Explorer 10 and later
- Microsoft Edge 20.10240 and later
- Mozilla Firefox 44 and later
- Opera 35 and later.

For successful operation, JavaScript should be enabled on the web browser. Make sure that JavaScript has not been disabled by other software (such as virus protection or web user security packages) running on your computer.

Wired or Wireless NIC (Ethernet or Wi-Fi Adapter)

Any computer that uses the router should be equipped with an Ethernet or Wi-Fi adapter (NIC). If your computer is not equipped with such a device, install an Ethernet or Wi-Fi adapter prior to using the router.

Wireless Connection

Wireless workstations from your network should be equipped with a wireless 802.11b, g, or n NIC (Wi-Fi adapter). In addition, you should specify the values of SSID, channel number and security settings defined in the web-based interface of the router for all these wireless workstations.

Connecting to PC

PC with Ethernet Adapter

1. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.

2. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.

Then make sure that your PC is configured to obtain an IP address automatically (as DHCP client).

Obtaining IP Address Automatically (OS Windows 7)

1. Click the **Start** button and proceed to the **Control Panel** window.

2. Select the **Network and Sharing Center** section. (If the Control Panel has the category view (the **Category** value is selected from the **View by** drop-down list in the top right corner of the window), choose the **View network status and tasks** line under the **Network and Internet** section.)
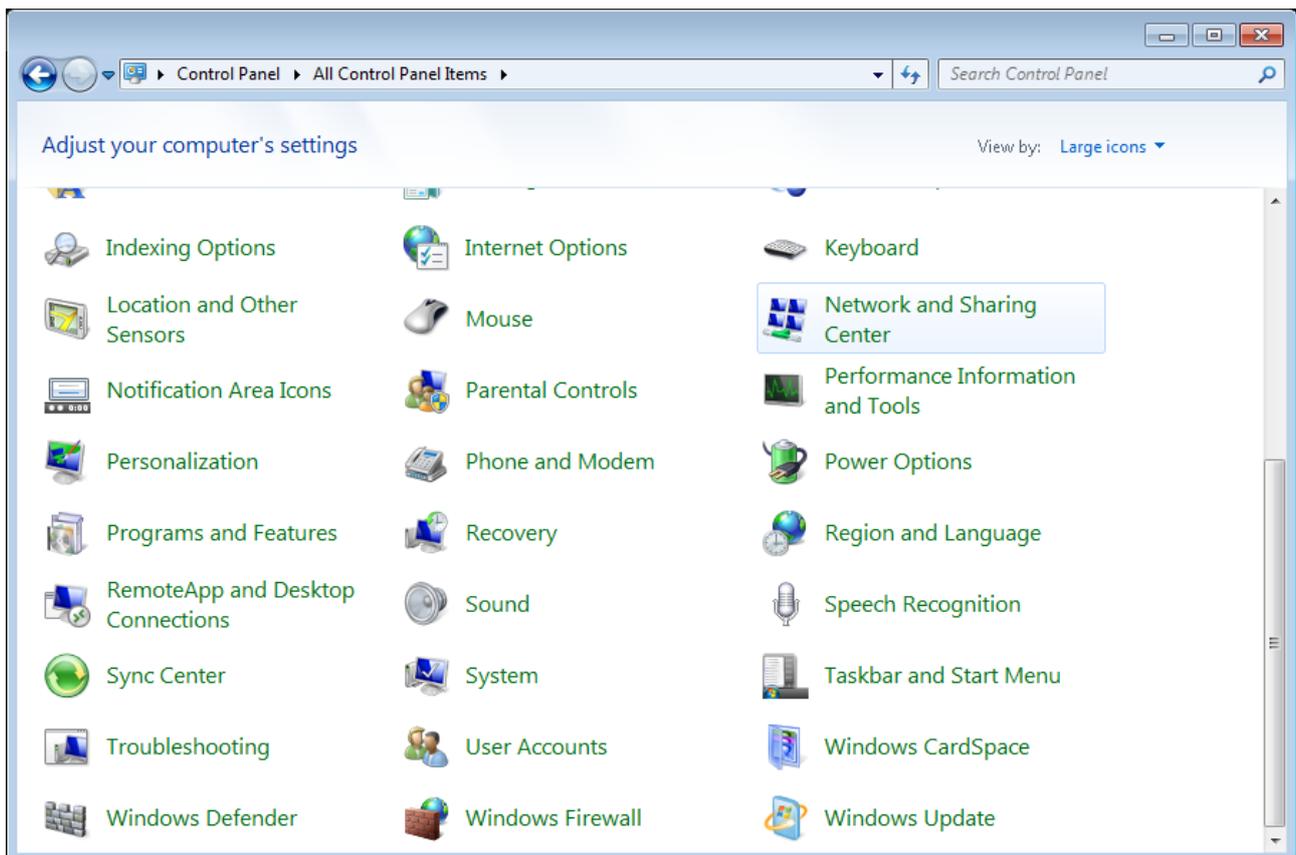
Figure 3. The Control Panel window.

3. In the menu located on the left part of the window, select the **Change adapter settings** line.
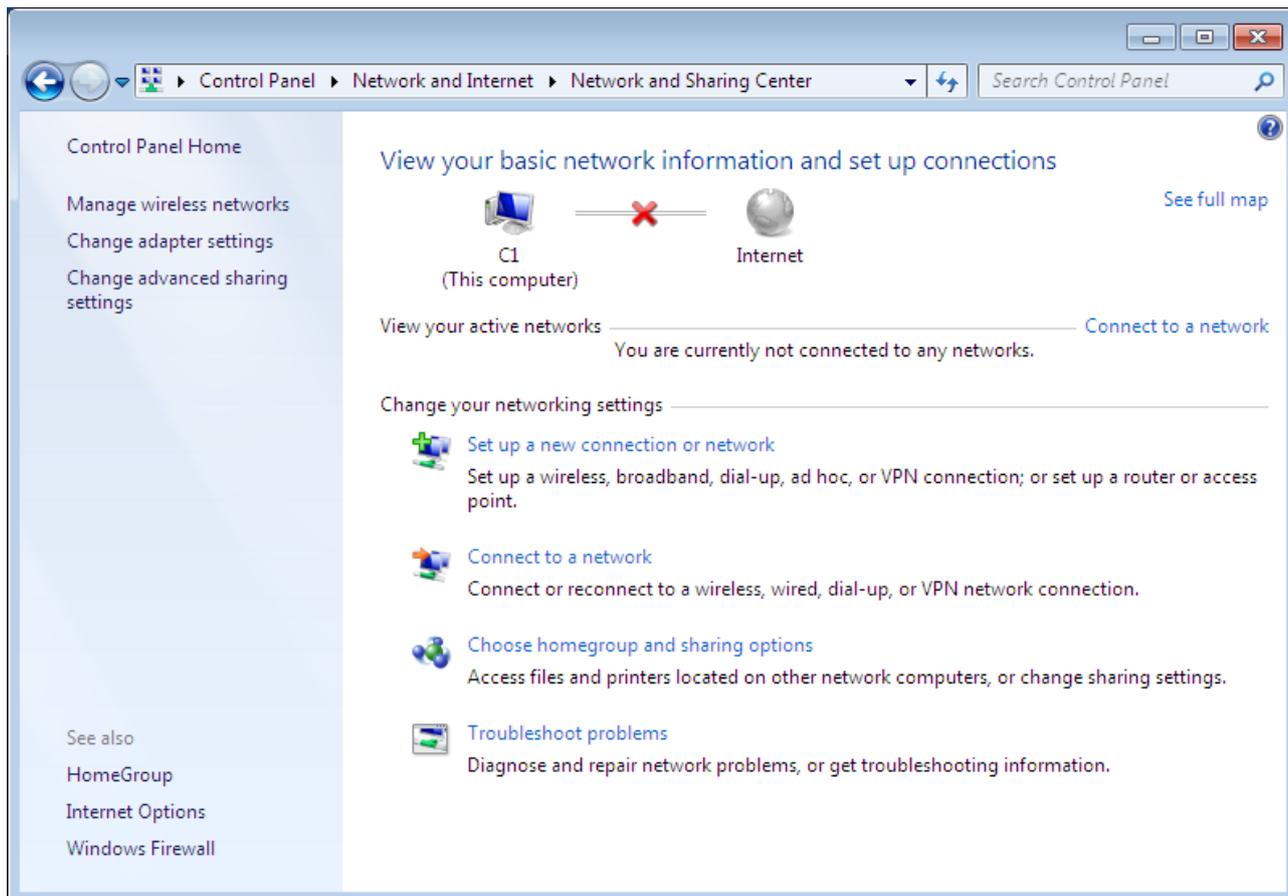
Figure 4. The Network and Sharing Center window.

4. In the opened window, right-click the relevant **Local Area Connection** icon and select the **Properties** line in the menu displayed.
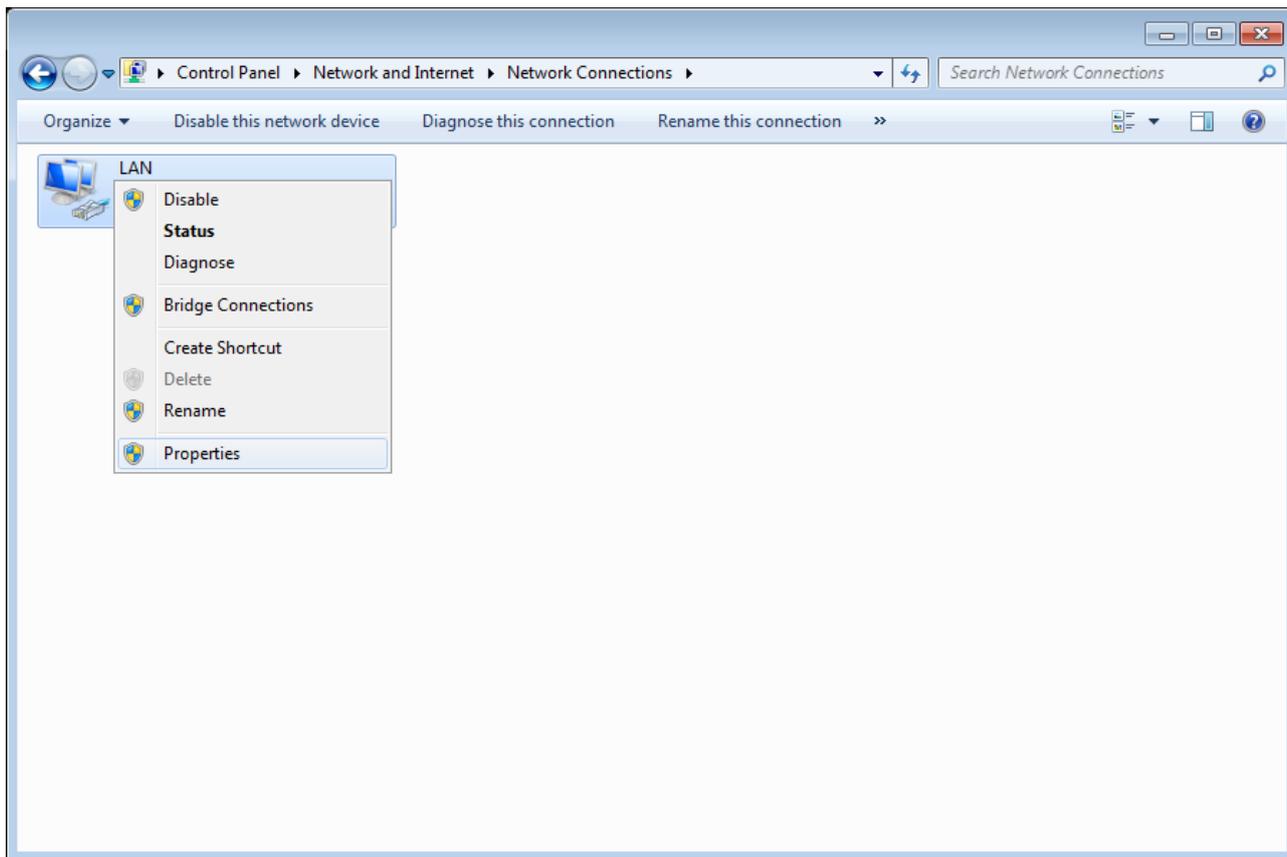
*Figure 5. The **Network Connections** window.*

5. In the **Local Area Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.

*Figure 6. The **Local Area Connection Properties** window.*

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.
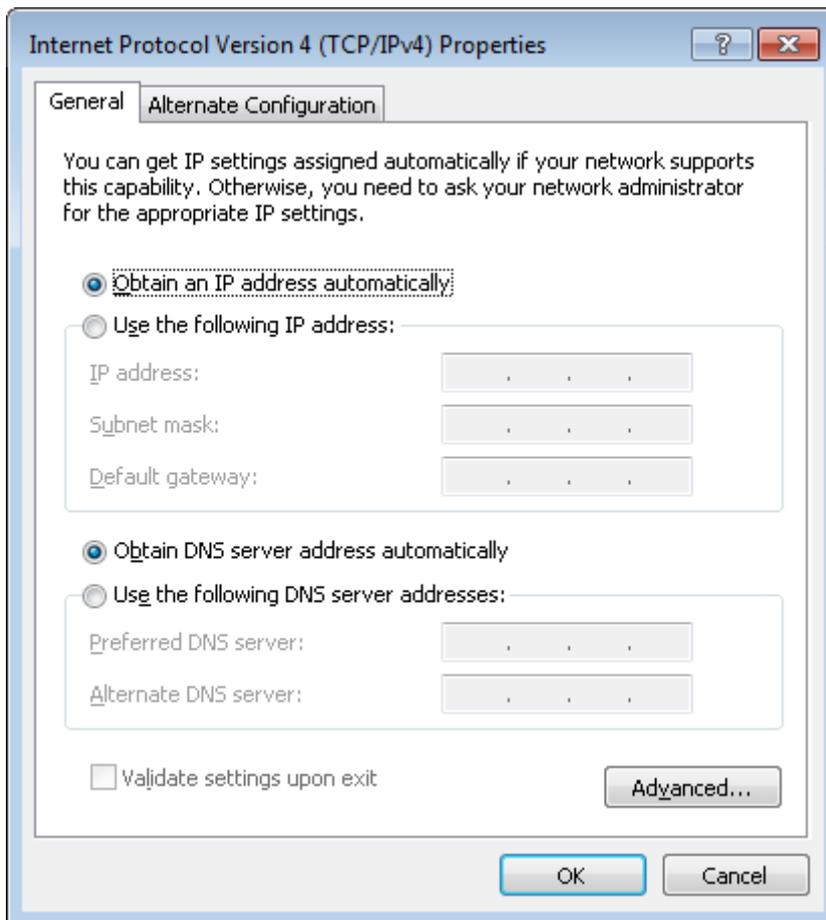
*Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

7. Click the **OK** button in the connection properties window.

Obtaining IP Address Automatically (OS Windows 10)

1. Click the **Start** button and proceed to the **Settings** window.
2. Select the **Network & Internet** section.

*Figure 8. The **Windows Settings** window.*

3. In the **Change your network settings** section, select the **Change adapter options** line.
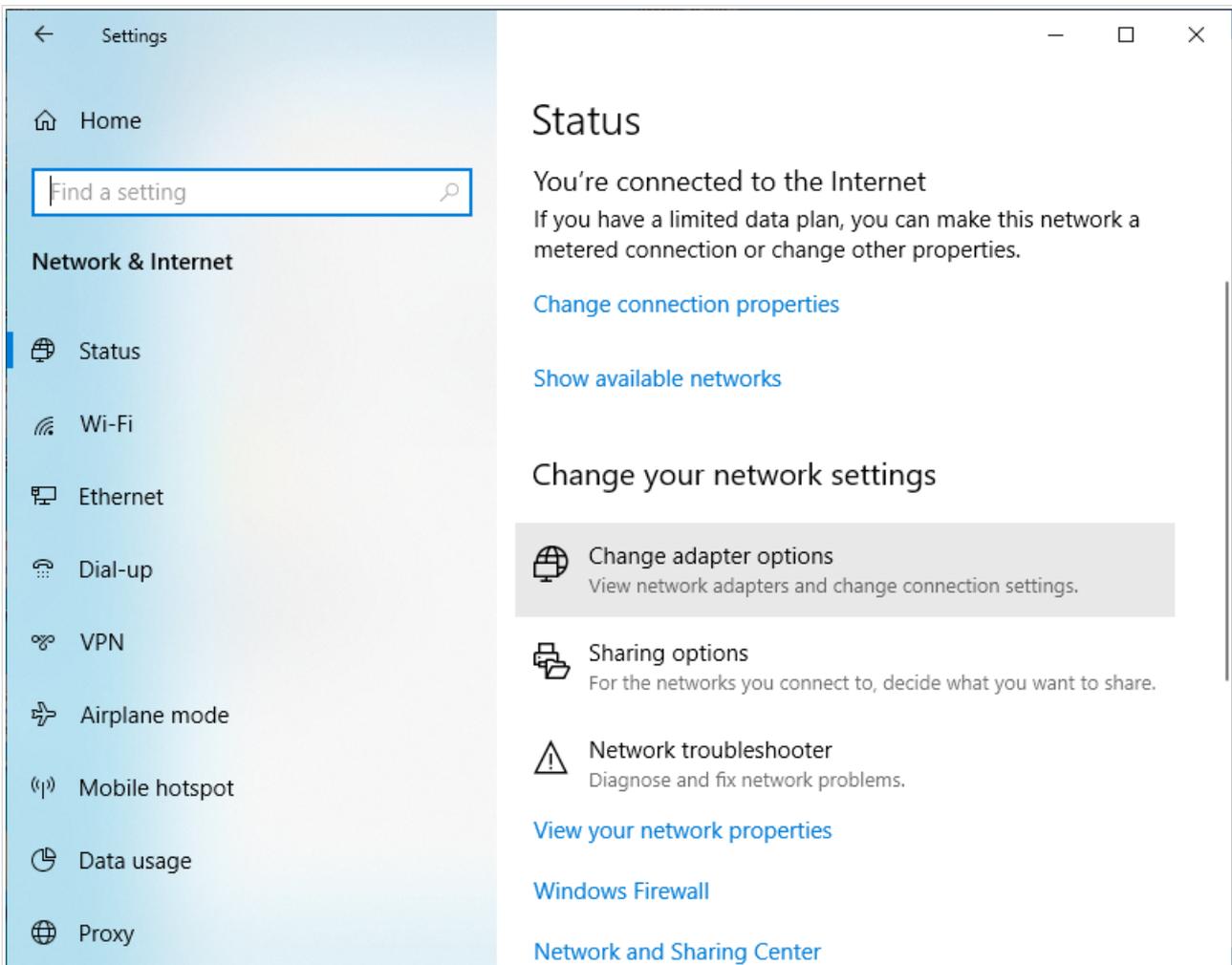
*Figure 9. The **Network & Internet** window.*

4. In the opened window, right-click the relevant **Local Area Connection** icon and select the **Properties** line in the menu displayed.
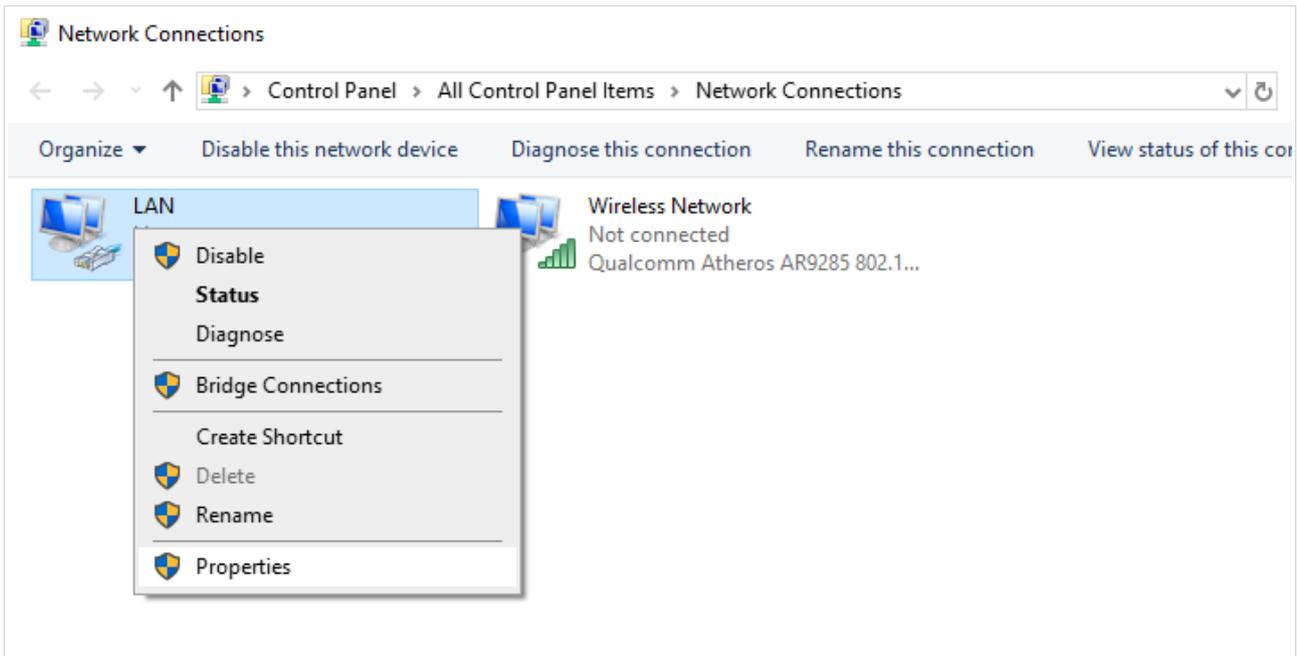
*Figure 10. The **Network Connections** window.*

5. In the **Local Area Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.

Figure 11. The local area connection properties window.

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.
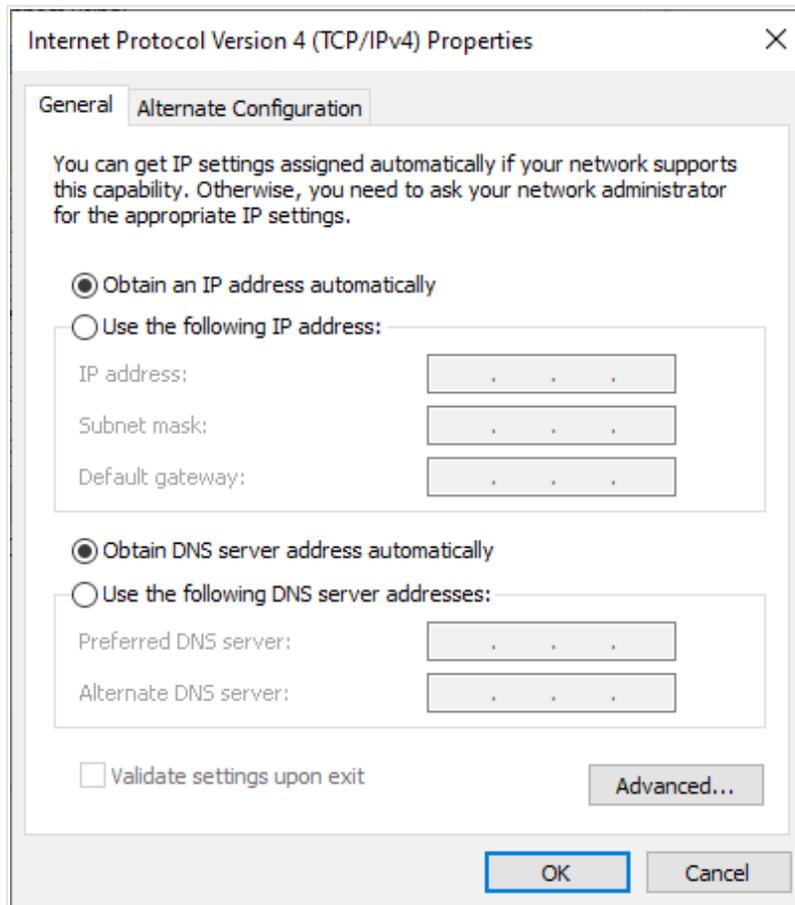
*Figure 12. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

7. Click the **Close** button in the connection properties window.

PC with Wi-Fi Adapter

1. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.

2. Make sure that your Wi-Fi adapter is on. As a rule, modern notebooks with built-in wireless NICs are equipped with a button or switch that turns on/off the wireless adapter (refer to your PC documents). If your PC is equipped with a pluggable wireless NIC, install the software provided with your Wi-Fi adapter.

Then make sure that your Wi-Fi adapter is configured to obtain an IP address automatically (as DHCP client).

Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 7)

1. Click the **Start** button and proceed to the **Control Panel** window.

2. Select the **Network and Sharing Center** section. (If the Control Panel has the category view (the **Category** value is selected from the **View by** drop-down list in the top right corner of the window), choose the **View network status and tasks** line under the **Network and Internet** section.)
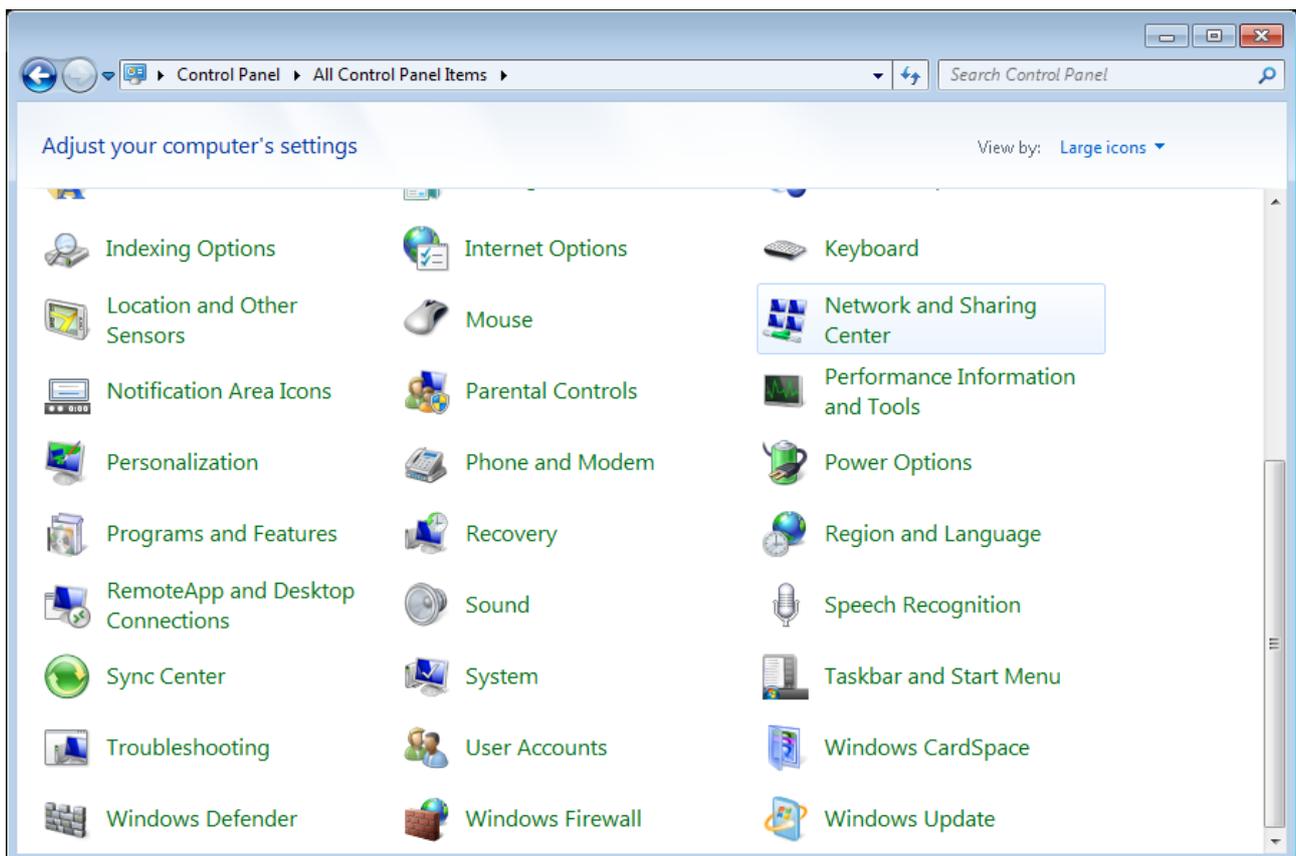
*Figure 13. The **Control Panel** window.*

3. In the menu located on the left part of the window, select the **Change adapter settings** line.

4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.

5. In the **Wireless Network Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.
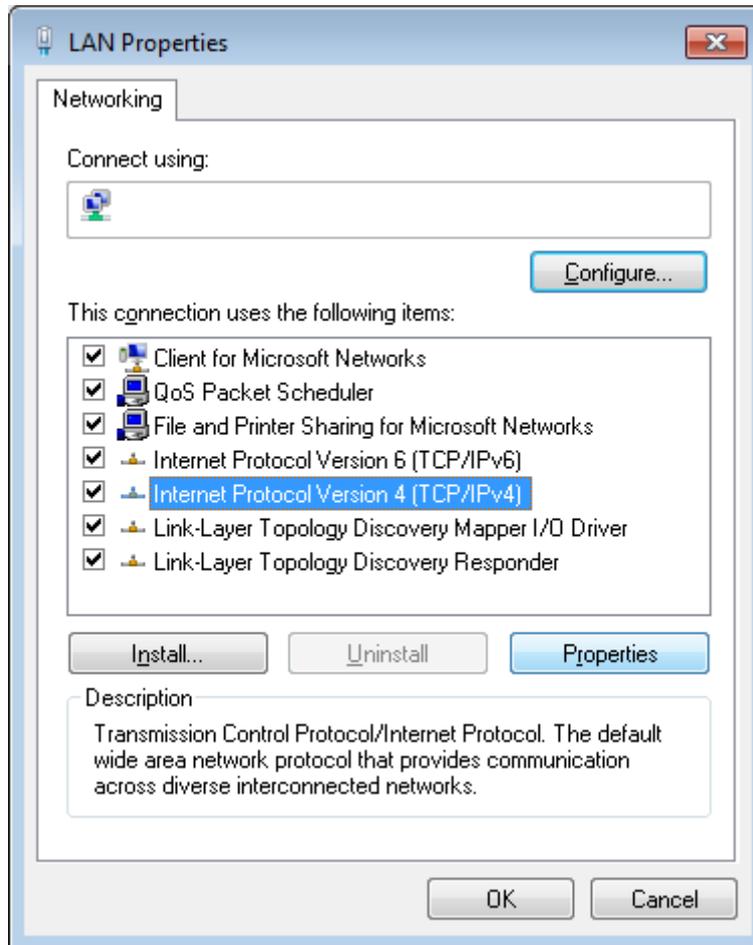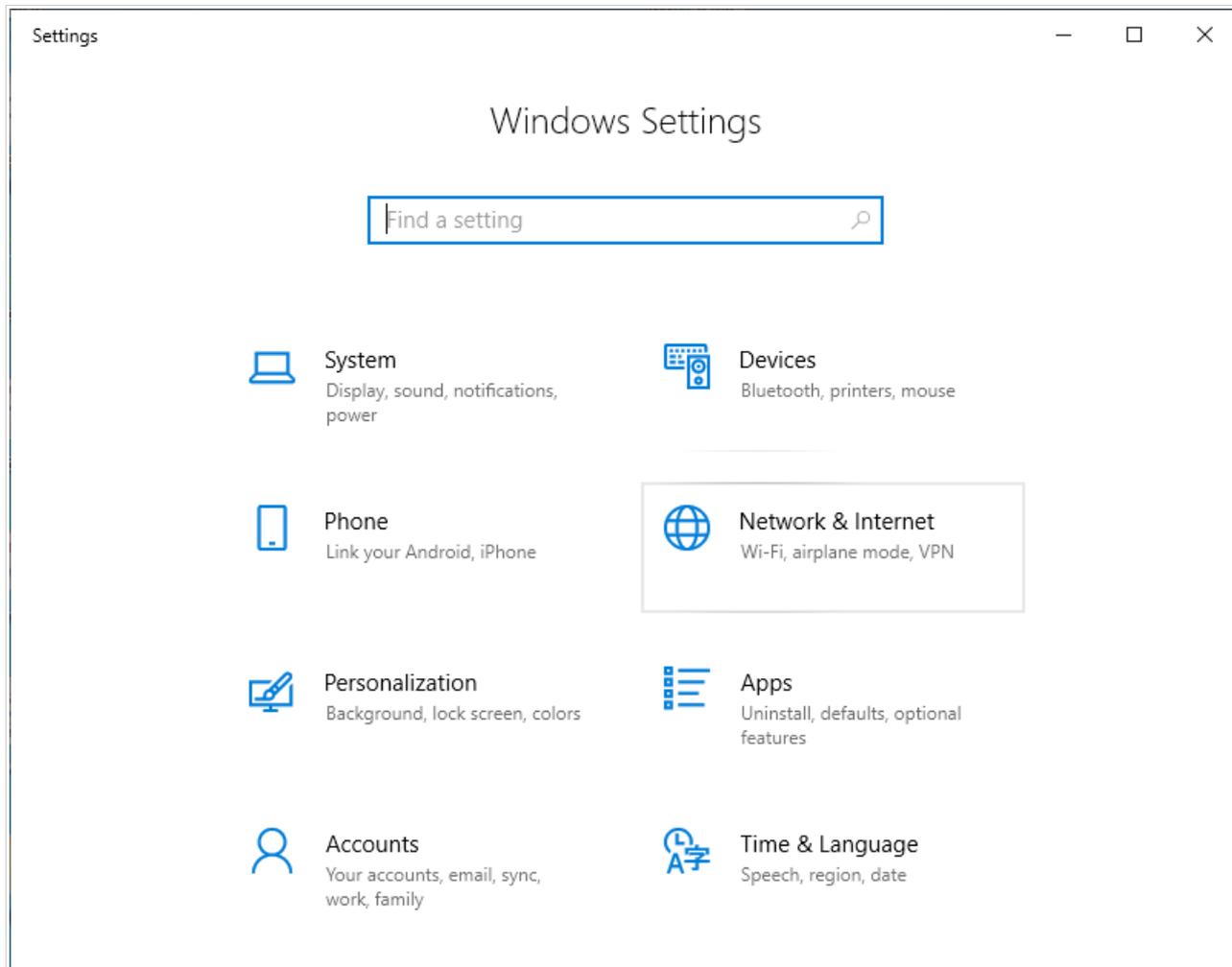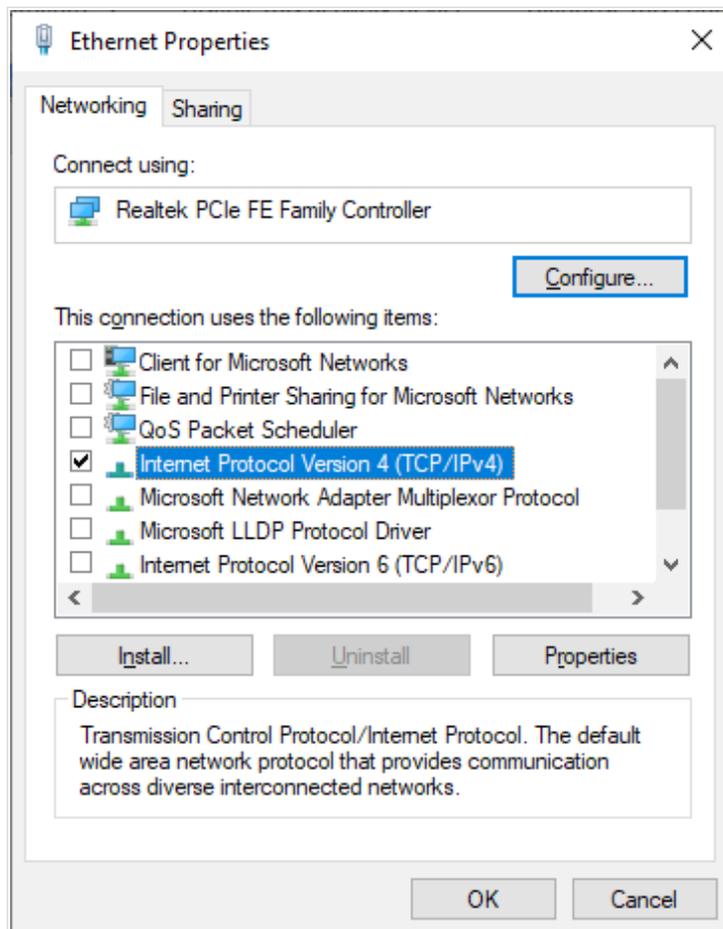
6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.

*Figure 14. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

7. Click the **OK** button in the connection properties window.

8. To open the list of available wireless networks, select the icon of the wireless network connection and click the **Connect To** button or left-click the network icon in the notification area located on the right side of the taskbar.

Figure 15. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network `DIR-615` and click the **Connect** button.

Figure 16. The list of available networks.

10. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **OK** button.

11. Wait for about 20-30 seconds. After the connection is established, the network icon will be displayed as the signal level scale.

> ❗ If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings of the router you will need to reconfigure the wireless connection using the newly specified settings.

Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 10)

1. Click the **Start** button and proceed to the **Settings** window.
2. Select the **Network & Internet** section.
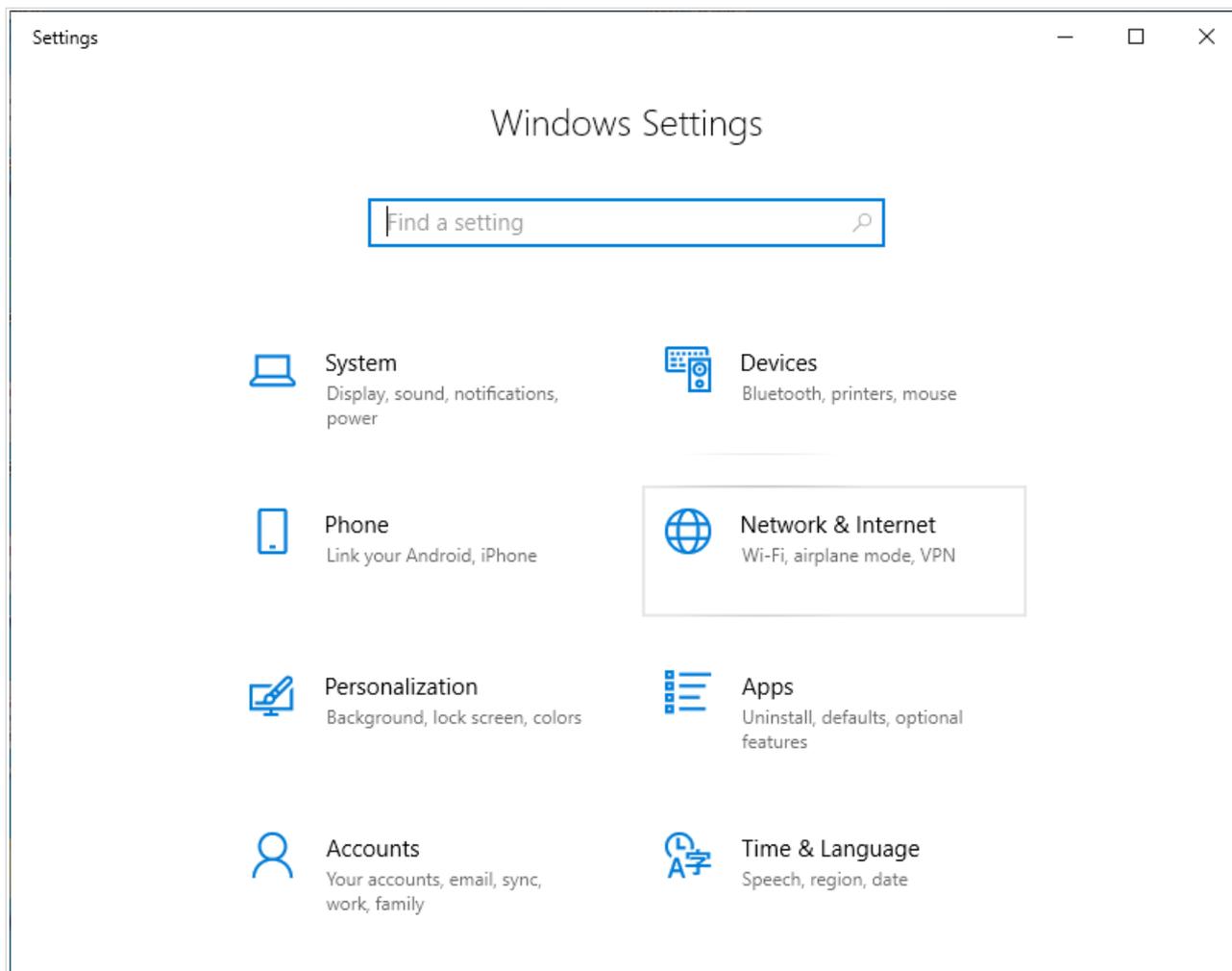
*Figure 17. The **Windows Settings** window.*

3. In the **Change your network settings** section, select the **Change adapter options** line.

4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.

5. In the **Wireless Network Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.
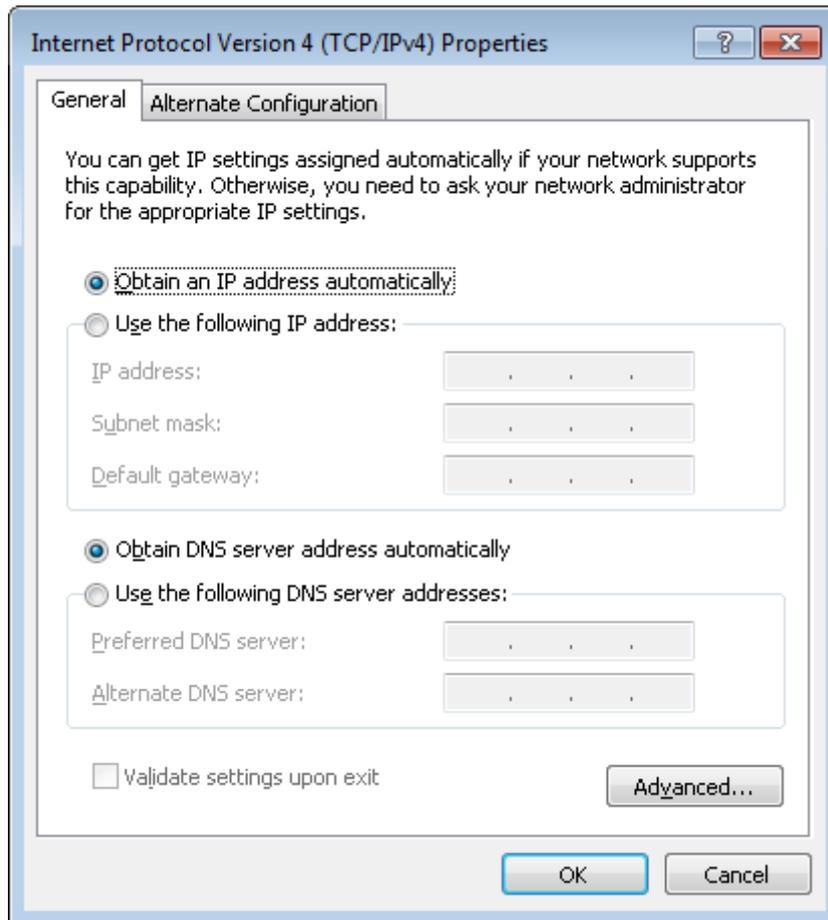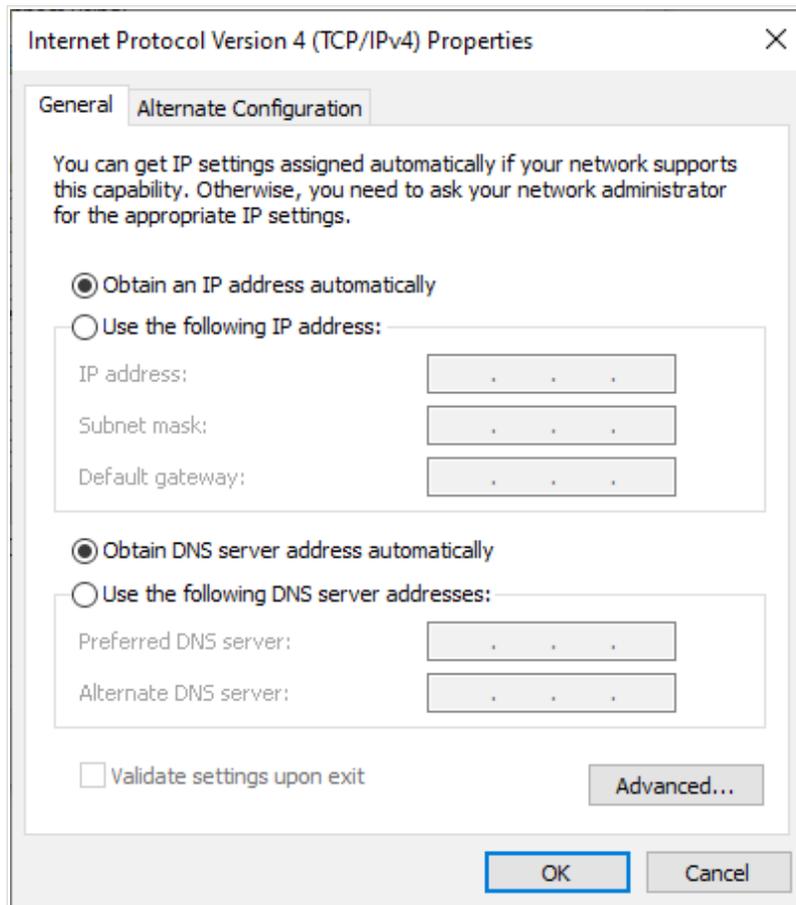

*Figure 18. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

7. Click the **Close** button in the connection properties window.

8. To open the list of available wireless networks, select the icon of the wireless network connection and click the **Connect To** button or left-click the network icon in the notification area located on the right side of the taskbar.

Figure 19. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network **DIR-615** and click the **Connect** button.
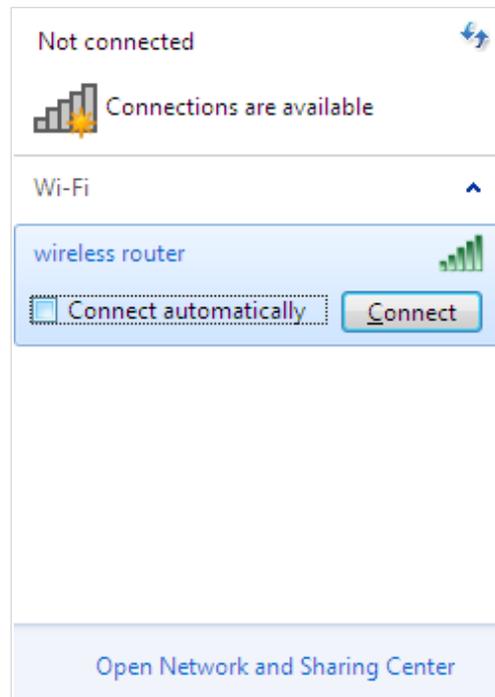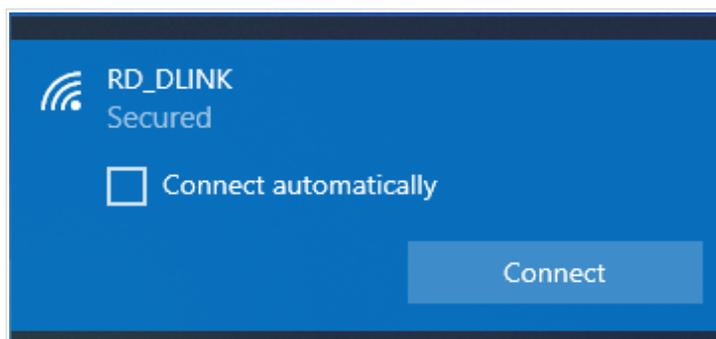

Figure 20. The list of available networks.

10. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **Next** button.

11. Allow or forbid your PC to be discoverable by other devices on this network (**Yes / No**).
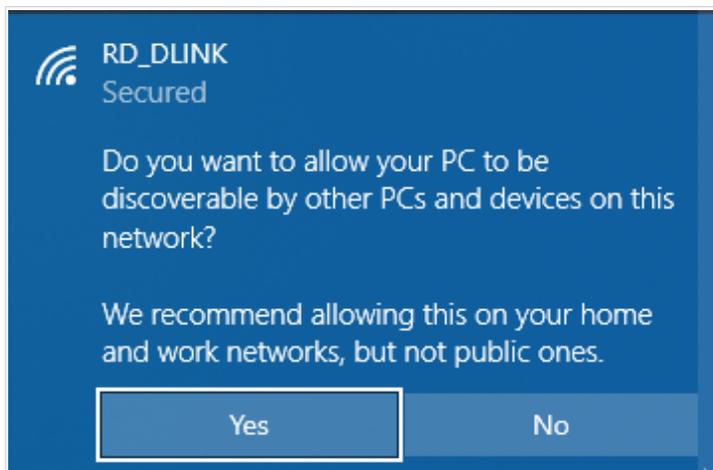
Figure 21. PC discovery settings.

12. Wait for about 20-30 seconds. After the connection is established, the network icon will be displayed as a dot with curved lines indicating the signal level.

! If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings of the router you will need to reconfigure the wireless connection using the newly specified settings.

Connecting to Web-based Interface

When you have configured your computer, you can access the web-based interface and configure needed parameters (create a WAN connection, change the parameters of the wireless network, specify the settings of the firewall, etc.).

> **!** For security reasons, DIR-615 with default settings cannot connect to the Internet. To get started, please set your own password used to access the web-based interface and, if needed, configure other settings recommended by your ISP.

Start a web browser (see the ***Before You Begin*** section, page 14). In the address bar of the web browser, enter the domain name of the router (by default, `dlinkrouter.local`) with a dot at the end and press the **Enter** key. Also you can enter the IP address of the device (by default, `192.168.0.1`).

Figure 22. Connecting to the web-based interface of the DIR-615 device.

> **!** If the error "*The page cannot be displayed*" (or "*Unable to display the page*"/"*Could not connect to remote server*") occurs upon connecting to the web-based interface of the router, make sure that you have properly connected the router to your computer.

If the device has not been configured previously or the default settings have been restored, after access to the web-based interface the Setup Wizard opens (see the ***Setup Wizard*** section, page 38).

Dear Customer! It's the first time the device is turned on. Please configure the device in order to use the Internet access services. To run the Wizard, click the "Start" button.

START
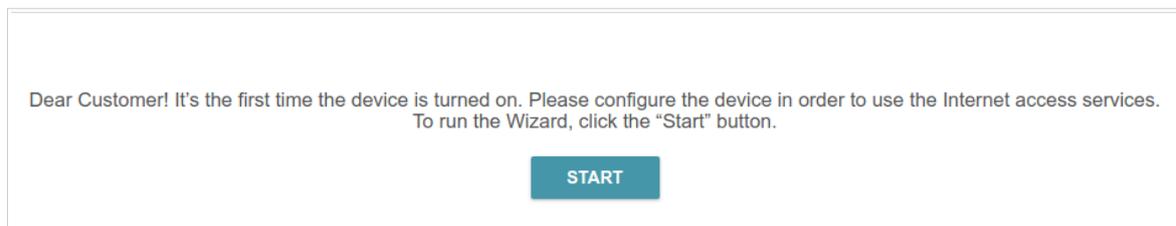
Figure 23. The page for running the Setup Wizard.

If you configured the device previously, after access to the web-based interface the login page opens. Enter the username (`admin`) in the **Username** field and the password you specified in the **Password** field, then click the **LOGIN** button.
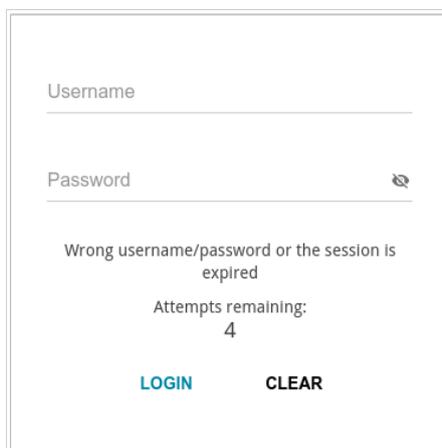
Figure 24. The login page.

If you enter a wrong password several times, the web-based interface will be blocked for a while. Please wait for one minute and reenter the password you specified.

Web-based Interface Structure

Home Page

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

The page displays whether or not the router is currently connected to the Internet. If it is disconnected, click the sign **Click to repair** to go to the **Settings / Internet / WAN** page (for the description of the page, see the *WAN* section, page 59), or click **Internet disconnected** to run the Setup Wizard (for the description of the Wizard, see the *Setup Wizard* section, page 38).
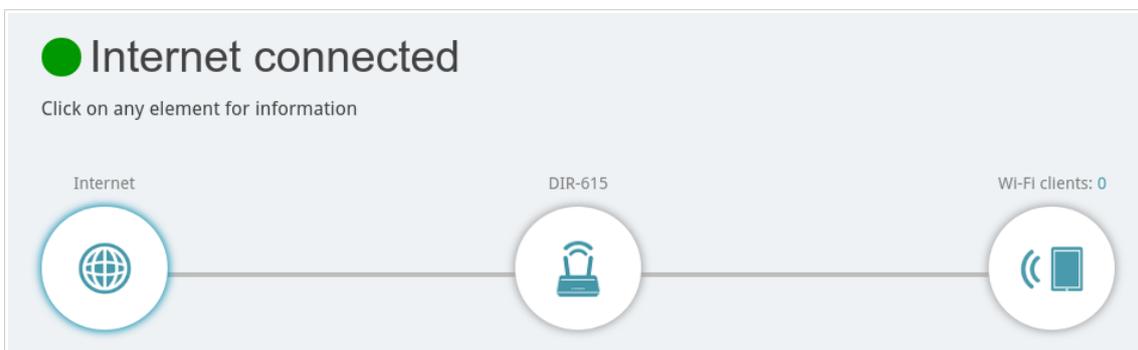
*Figure 25. The **Home** page. The device is connected to the Internet.*
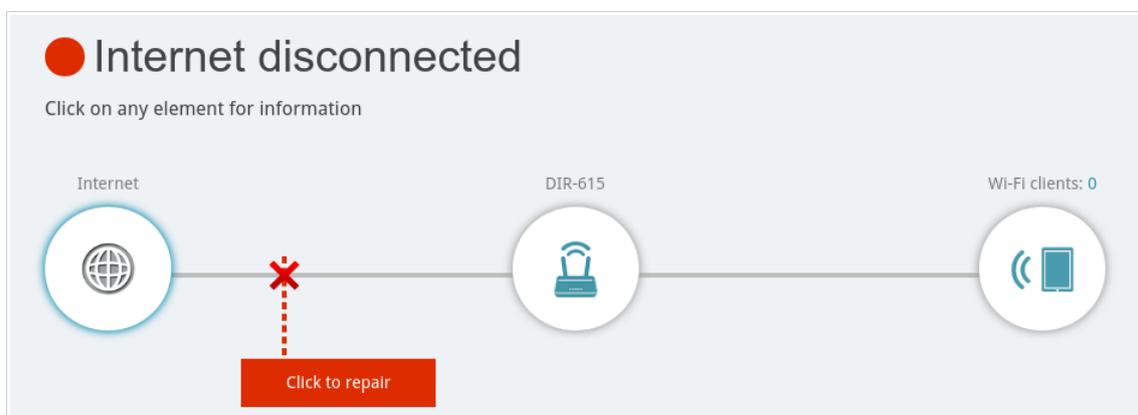
*Figure 26. The **Home** page. The device is not connected to the Internet.*

Internet Section

Click the **Internet** icon to view more details about your Internet connection.

*Figure 27. The **Home** page. The **Internet** section.*

Click **IPv4** or **IPv6** to display details of the IPv4 connection and IPv6 connection respectively.

To reconfigure the Internet settings, click **Go to settings**. Upon that the **Settings / Internet / WAN** page opens (for the description of the page, see the *WAN* section, page 59).

DIR-615 Section

Click the **DIR-615** icon to view details about the router and its wireless settings.

*Figure 28. The **Home** page. The **DIR-615** section.*

Here you can see the router's current Wi-Fi network name, the password (click **Show** (👁) to display it), 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 **Settings** (at the top of the page) and then **Network** on the menu that appears (for the description of the page, see the ***Settings / Network*** section, page 94).

To reconfigure the wireless settings, either click **Go to settings** on the lower right, or click **Settings** (at the top of the page) and then **Wireless Network** on the menu that appears (for the description of the page, see the ***Settings / Wireless Network*** section, page 87).

Wi-Fi Clients Section

Click the **Wi-Fi clients** icon to view details about wireless clients connected to the router.
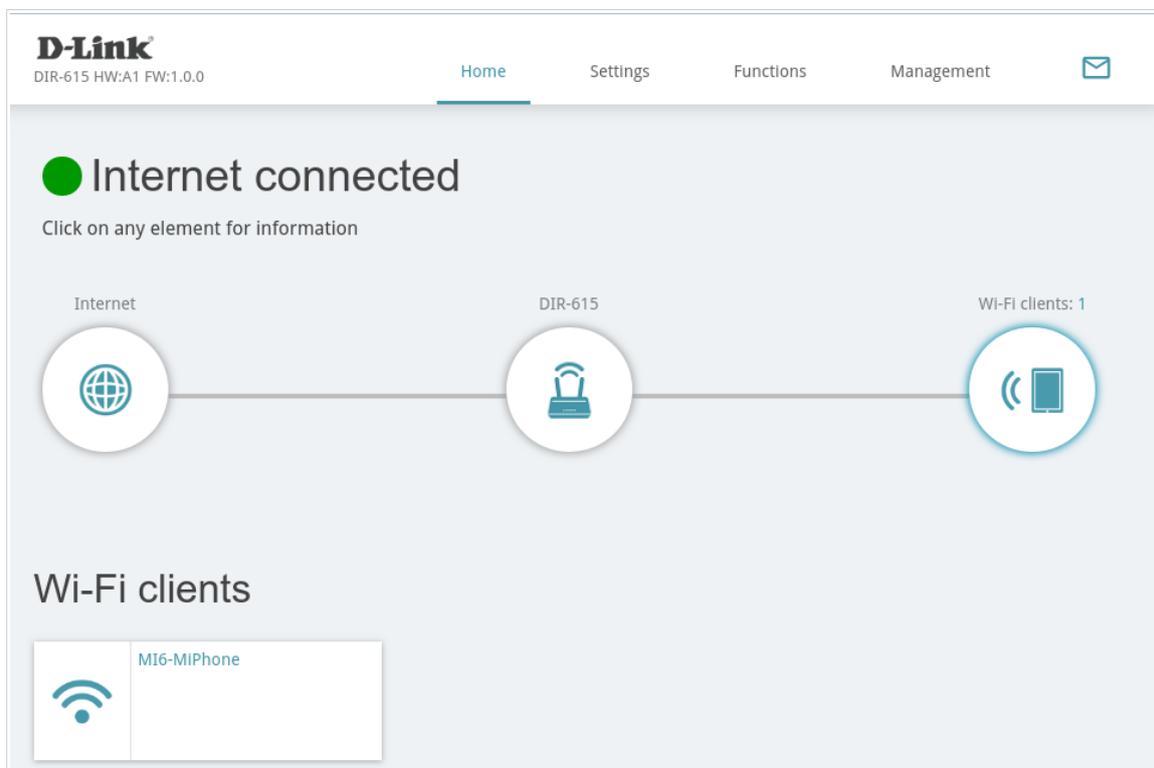
*Figure 29. The **Home** page. The **Wi-Fi clients** section.*

Here you can see all wireless clients currently connected to the router. Such devices are marked by the **Connected** icon ( ).

Menu Sections

To configure the router use the menu bar in the top part of the page.

The **Settings** section provides you with the most essential settings.

On the **Setup Wizard** page you can run the Setup Wizard. The Wizard allows you to configure the router for operation in the needed mode and specify all parameters necessary for getting started (for the description of the Wizard, see the *Setup Wizard* section, page 38).

On the **Internet / WAN** page you can create a connection to the Internet or reconfigure existing connections (for the description of the page, see the *WAN* section, page 59).

On the **WAN Failover** page you can enable and configure the WAN backup function (for the description of the page, see the *Settings / WAN Failover* section, page 85).

On the **Wireless network** page you can configure the basic and additional wireless networks (for the description of the page, see the *Settings / Wireless Network* section, page 87).

On the **Network** page you can configure basic parameters of the LAN interface of the router (for the description of the page, see the *Settings / Network* section, page 94).

The pages of the **Functions / Firewall** subsection are designed for configuring the firewall of the router (for the description of the pages, see the *Functions / Firewall* section, page 102).

The pages of the **Functions / Wi-Fi** subsection are designed for specifying all other settings of the router's wireless network (for the description of the pages, see the *Functions / Wi-Fi* section, page 112).

The pages of the **Functions / Advanced** subsection are designed for configuring additional parameters of the router (for the description of the pages, see the *Functions / Advanced* section, page 127).

The pages of the **Management** section provide functions for managing the internal system of the router (for the description of the pages, see the *Management* section, page 146). And the pages of the **Management / Statistics** subsection display data on the current state of the router (for the description of the pages, see the *Statistics* section, page 161). Also the pages of the **Management / Yandex.DNS** subsection are designed for configuring the Yandex.DNS web content filtering service (for the description of the pages, see the *Yandex.DNS* section, page 154).

Notifications

The router's web-based interface displays notifications in the top right part of the page.

Figure 30. The web-based interface notifications.

Click the icon displaying the number of notifications to view the complete list and click the relevant button.

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Setup Wizard

To start the Setup Wizard, go to the **Settings / Setup Wizard** section. On the opened page, click the **OK** button and wait until the factory default settings are restored.

In order to run the Initial Configuration Wizard, the device should be reset to factory defaults.

CANCEL   OK
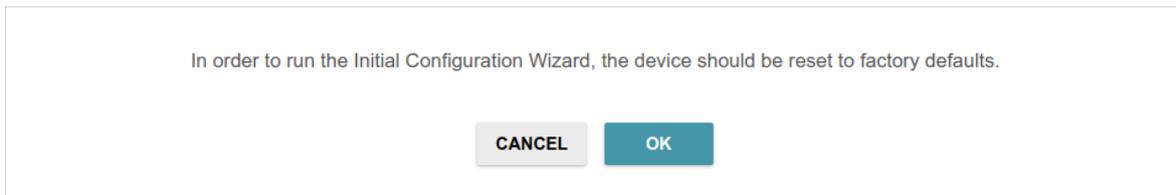
Figure 31. Restoring the default settings in the Wizard.

Click the **START** button.

Dear Customer! It's the first time the device is turned on. Please configure the device in order to use the Internet access services. To run the Wizard, click the "Start" button.
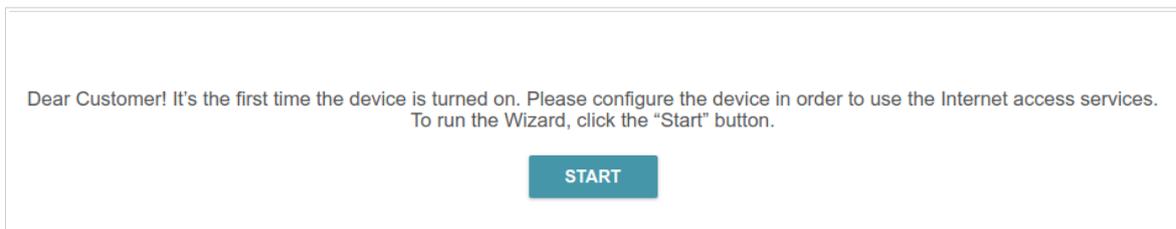
START

Figure 32. Starting the Wizard.

On the opened page, click **YES** in order to leave the current language of the web-based interface or click **NO** to select another language.

Maybe your language is English?

NO   YES
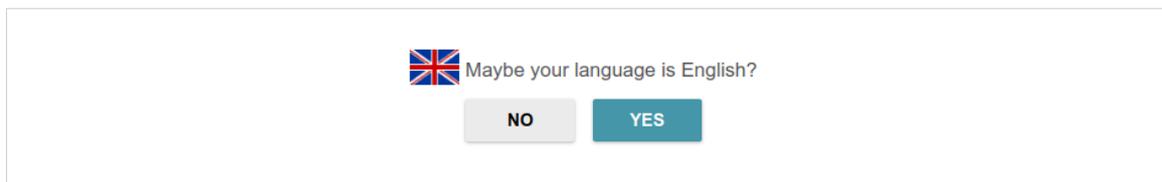
Figure 33. Selecting a language.

You can finish the wizard earlier and go to the menu of the web-based interface. To do this, click the **ADVANCED SETTINGS** button. On the opened page, change the default settings: specify the administrator password in the **User's interface password** and **Password confirmation** fields and the name of the wireless network in the **Network name (SSID)** field. Then click the **APPLY** button.
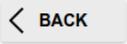
Figure 34. Changing the default settings.

To continue the configuration of the router via the Wizard, click the **CONTINUE** button.

Selecting Operation Mode

Select the needed operation mode and click the **NEXT** button.

Router

In order to connect your device to a wired ISP, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Router** value. In this mode you can configure a WAN connection, set your own settings for the wireless network, configure LAN ports to connect an STB or VoIP phone, and set your own password for access to the web-based interface of the device.
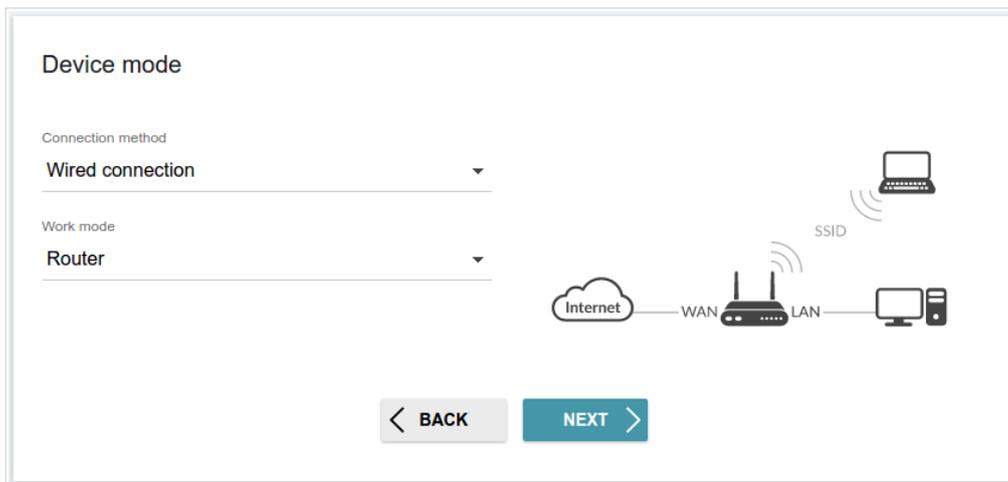
*Figure 35. Selecting an operation mode. The **Router** mode.*

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, and set your own password for access to the web-based interface of the device.
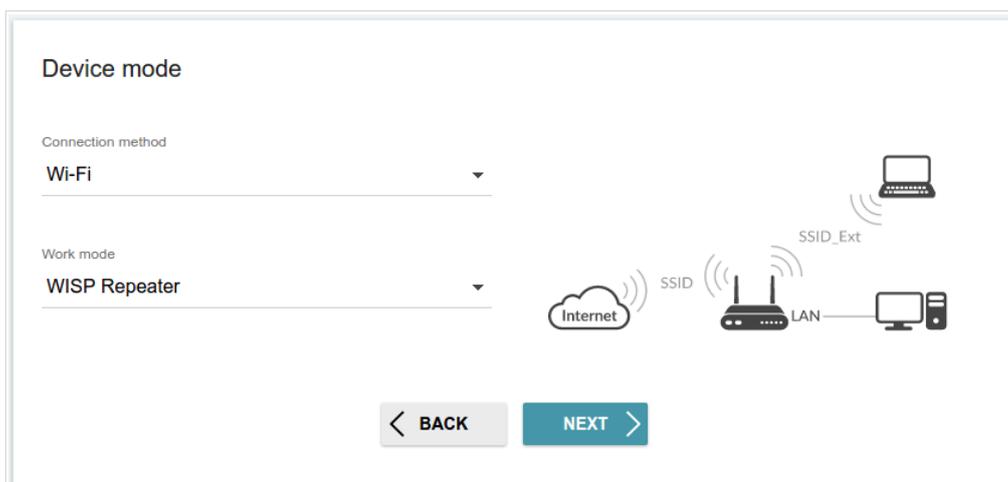
*Figure 36. Selecting an operation mode. The **WISP Repeater** mode.*

Access Point or Repeater

In order to connect your device to a wired router for adding a wireless network to the existing local network, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Access point** value. In this mode you can change the LAN IP address, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.

*Figure 37. Selecting an operation mode. The **Access point** mode.*

In order to connect your device to a wireless router for extending the range of the existing wireless network, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **Repeater** value. In this mode you can change the LAN IP address, connect your device to another access point, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.

*Figure 38. Selecting an operation mode. The **Repeater** mode.*

In order to let wired PCs connected to your device access the network of a wireless router, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **Client** value. In this mode you can change the LAN IP address, connect your device to another access point, and set your own password for access to the web-based interface of the device.
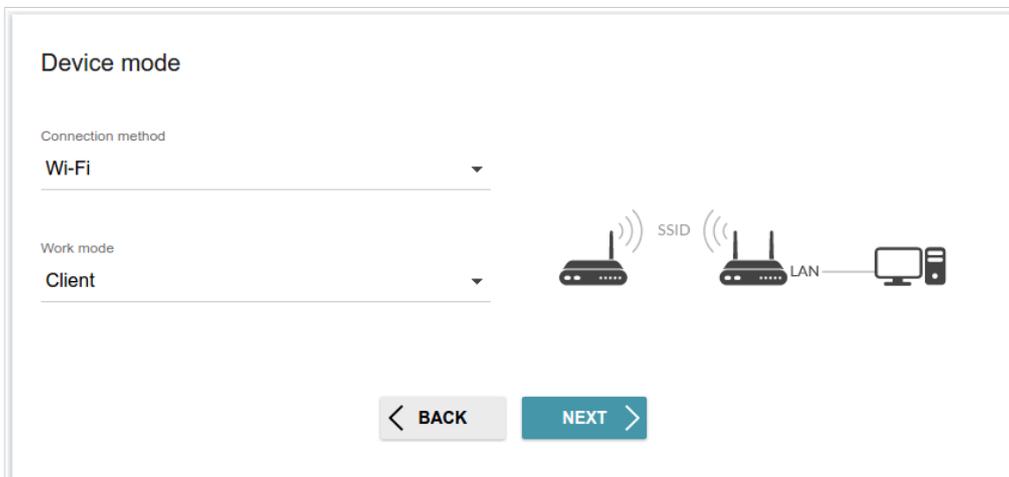
*Figure 39. Selecting an operation mode. The **Client** mode.*

Changing LAN IPv4 Address

This configuration step is available for the **Access point**, **Repeater**, and **Client** modes.

1. Select the **Automatic obtainment of IPv4 address** to let DIR-615 automatically obtain the LAN IPv4 address.

2. In the **Hostname** field, you should specify a domain name of the router using which you can access the web-based interface after finishing the Wizard. Enter a new domain name of the router ending with `.local` or leave the value suggested by the router.

> **!** In order to access the web-based interface using the domain name, in the address bar of the web browser, enter the name of the router with a dot at the end.

If you want to manually assign the LAN IPv4 address for DIR-615, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Subnet mask**, **Hostname** fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.

Figure 40. The page for changing the LAN IPv4 address.

3. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Wi-Fi Client

This configuration step is available for the **WISP Repeater**, **Repeater**, and **Client** modes.

1. On the **Wi-Fi Client** page, click the **WIRELESS NETWORKS** button and select the network to which you want to connect in the opened window. When you select a network, the **Network name (SSID)** and **BSSID** fields are filled in automatically.

If you cannot find the needed network in the list, click the **UPDATE LIST** icon (⟳).

2. If a password is needed to connect to the selected network, fill in the relevant field. Click the **Show** icon (👁) to display the entered password.
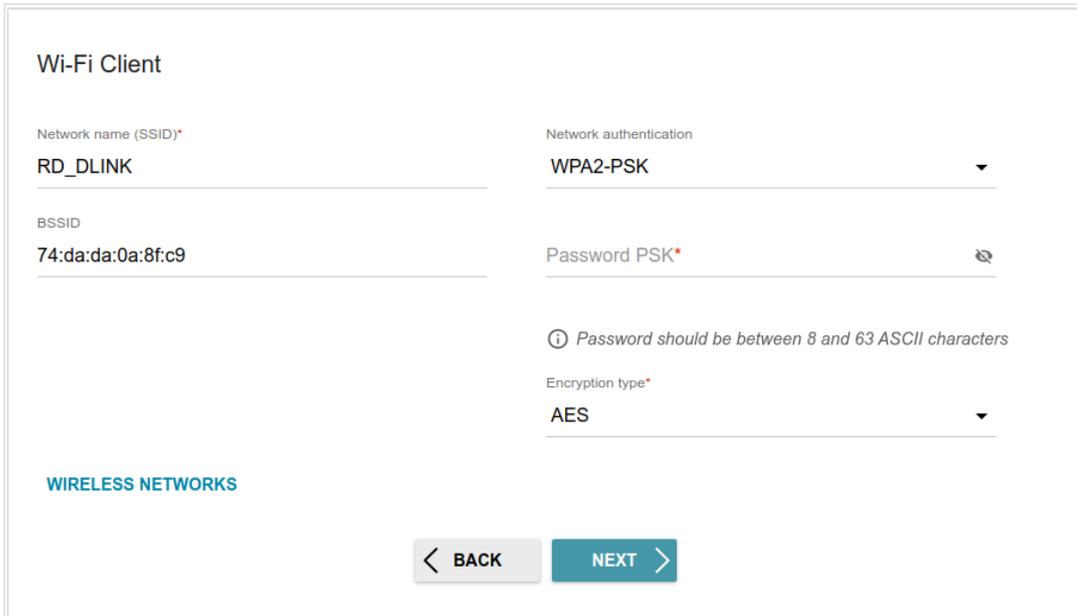
Figure 41. The page for configuring the Wi-Fi client.

If you connect to a hidden network, enter the network name to the **Network name (SSID)** field. Then select a needed value from the **Network authentication** list and then, if needed, enter the password in the relevant field.

When the **Open** or **WEP** authentication type is selected, the following settings are displayed on the page:

Parameter	Description
Enable encryption WEP	*For **Open** authentication type only.* The checkbox activating WEP encryption. When the checkbox is selected, the **Default key ID** drop-down list, the **Encryption key WEP as HEX** checkbox, and four **Encryption key** fields are displayed on the page.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.

Parameter	Description
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields. Click the **Show** icon ( ) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** authentication type is selected, the following fields are displayed:

Parameter	Description
Password PSK	A password for WPA encryption. Click the **Show** icon ( ) to display the entered password.
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.

3. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Configuring WAN Connection

This configuration step is available for the **Router** and **WISP Repeater** modes.

> ❗ You should configure your WAN connection in accordance with data provided by your Internet service provider (ISP). Make sure that you have obtained all necessary information prior to configuring your connection. Otherwise contact your ISP.

1. On the **Internet connection type** page, click the **SCAN** button (available only for the **Router** mode) to automatically specify the connection type used by your ISP or manually select the needed value from the **Connection type** list.

2. Specify the settings necessary for the connection of the selected type.

3. If your ISP uses MAC address binding, select the **Clone MAC address of your device** checkbox.

4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field.

5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Static IPv4 Connection

Figure 42. The page for configuring Static IPv4 WAN connection.

Fill in the following fields: **IP address**, **Subnet mask**, **Gateway IP address**, and **DNS IP address**.

Static IPv6 Connection

Figure 43. The page for configuring Static IPv6 WAN connection.

Fill in the following fields: **IP address**, **Prefix**, **Gateway IP address**, and **DNS IP address**.

PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections

Figure 44. The page for configuring PPPoE WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon ( ) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

PPPoE + Static IP (PPPoE Dual Access) Connection

Figure 45. The page for configuring PPPoE + Static IP (PPPoE Dual Access) WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon ( ) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

Also fill in the following fields: **IP address**, **Subnet mask**, **Gateway IP address**, and **DNS IP address**.

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

Internet connection type

Connection type
PPTP + Dynamic IP ▼

ⓘ *PPTP and L2TP are methods for implementing virtual private networks.*

SCAN
Network scan for connection type and parameters detection

☐ Without authorization

Username*

Password*   👁

VPN server address*

☐ Clone MAC address of your device
ⓘ *In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet.*

☐ Use VLAN
ⓘ *Select the checkbox if the Internet access is provided via a VLAN channel.*

☑ Use IGMP
ⓘ *Internet Group Management Protocol is designed to manage multicast traffic in IP-based networks.*

☐ Ping

‹ **BACK**   **NEXT** ›

Figure 46. The page for configuring PPTP + Dynamic IP WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (👁) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

PPTP + Static IP or L2TP + Static IP Connection

Figure 47. The page for configuring PPTP + Static IP WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon ( ) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

Also fill in the following fields: **IP address**, **Subnet mask**, **Gateway IP address**, and **DNS IP address**.

Configuring Wireless Network

This configuration step is available for the **Router**, **Access point**, **WISP Repeater**, and **Repeater** modes.

1. On the **Wireless Network 2.4 GHz** page, in the **Network name** field, specify your own name for the wireless network or leave the value suggested by the router.

2. In the **Password** field, specify your own password for access to the wireless network or leave the value suggested by the router (WPS PIN of the device, see the barcode label).

3. If the router is used as a Wi-Fi client, you can specify the same parameters of the wireless network as specified for the network to which you are connecting. To do this, click the **USE** button (available for the **WISP Repeater** and **Repeater** modes only).

4. You can restore the parameters of the wireless network specified before resetting to factory defaults. To do this, click the **RESTORE** button.

Figure 48. The page for configuring the wireless network.

5. If you want to create an additional wireless network isolated from your LAN, select the **Enable guest network** checkbox (available for the **Router** and **WISP Repeater** modes only).
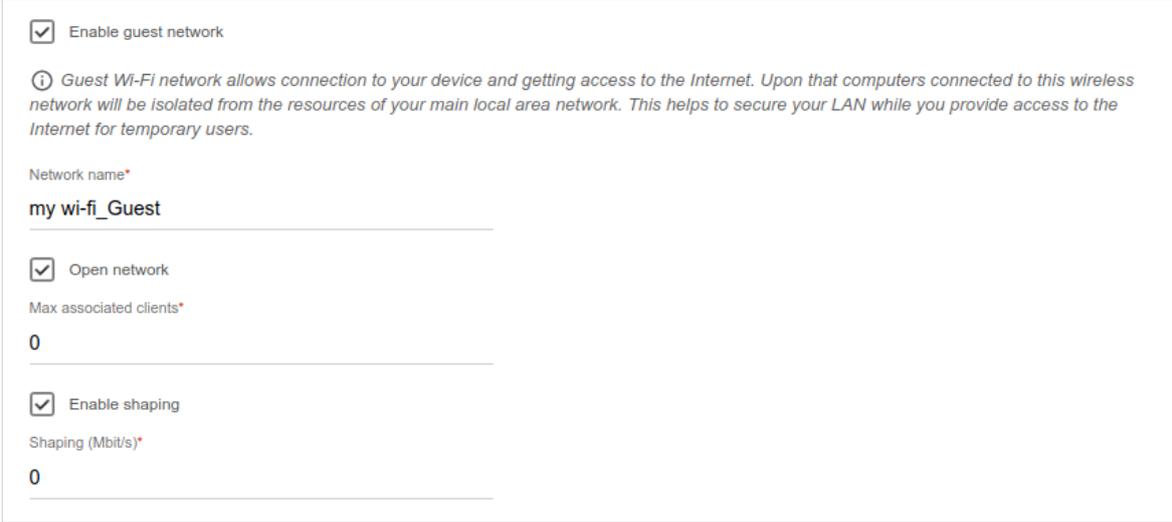
Figure 49. The page for configuring the wireless network.

6. In the **Network name** field, specify your own name for the guest wireless network or leave the value suggested by the router.

7. If you want to create a password for access to the guest wireless network, deselect the **Open network** checkbox and fill in the **Password** field.

8. If you want to limit the bandwidth of the guest wireless network, select the **Enable shaping** checkbox and fill in the **Shaping** field.

9. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

Configuring LAN Ports for IPTV/VoIP

This configuration step is available for the **Router** mode.

1. On the **IPTV** page, select the **Is an STB connected to the device** checkbox.

Figure 50. The page for selecting a LAN port to connect an IPTV set-top box.

2. Select a free LAN port for connecting your set-top box.

3. If the IPTV service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.

4. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

5. On the **VoIP** page, select the **Is an IP phone connected to the device** checkbox.

Figure 51. The page for selecting a LAN port to connect an VoIP phone.

6. Select a free LAN port for connecting your IP phone.

7. If the VoIP service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.

8. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **User's interface password** and **Password confirmation** fields. You may set any password except `admin`. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[1]
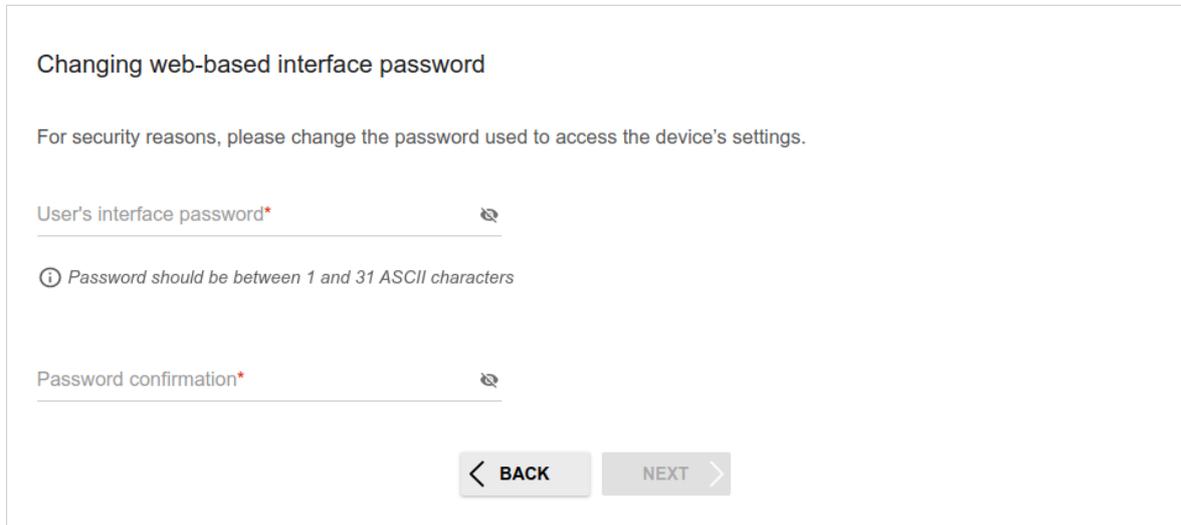
Figure 52. The page for changing the web-based interface password.

> ⚠ Remember or write down the new password for the administrator account. In case of losing the new password, you can access the settings of the router only after restoring the factory default settings via the hardware **WPS/RESET** button. This procedure wipes out all settings that you have configured for your router.

Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

On the next page, check all specified settings.

Also you can save a text file with parameters set by the Wizard to your PC. To do this, click the **SAVE CONFIGURATION FILE** button and follow the dialog box appeared.

To finish the Wizard, click the **APPLY** button. The router will apply settings and reboot. Click the **BACK** button to specify other settings.

---

1 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

If the Wizard has configured a WAN connection, after clicking the **APPLY** button, the page for checking the Internet availability opens.
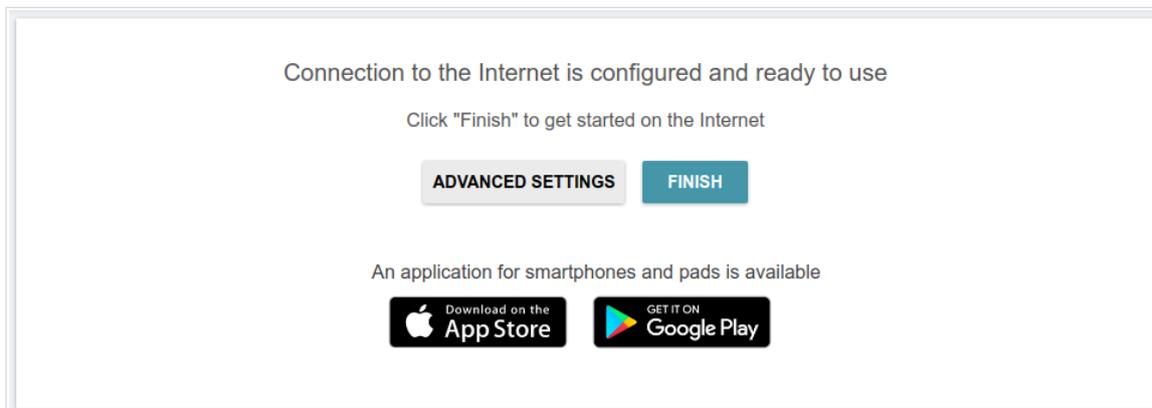
Figure 53. Checking the Internet availability.

If the router has been successfully connected to the Internet, click the **FINISH** button.

If problems appeared when connecting to the Internet, click the **CHECK AGAIN** button to recheck the state of the WAN connection.

If problems of connection have not been solved, contact the technical support of your ISP (as a rule, the technical support phone is provided with the agreement) or the D-Link technical support.

To specify other settings, click the **ADVANCED SETTINGS** button. After clicking the **ADVANCED SETTINGS** button, the **Home** page opens (see the *Home Page* section, page 32).

Settings / Internet

WAN

On the **Settings / Internet / WAN** page, you can create and edit connections used by the router.

By default, a **Dynamic IPv4** connection is configured in the system. It is assigned to the **WAN** port of the router.

Figure 54. The Settings / Internet / WAN page. The simplified mode.

To edit an existing connection, click the **EDIT** button. Change the needed parameters and click the **APPLY** button.

To disconnect a connection and establish it again, click the **RECONNECT** button.

To remove an existing connection and create a new one, click the **CHANGE CONFIGURATION** button. Upon that the connection creation page opens.

To create several WAN connections, go to the advanced mode. To do this, click the **ADVANCED MODE** button.

> ! When connections of some types are created, the **Settings / Internet / WAN** page is automatically displayed in the advanced mode.

WAN

You can create and edit connections used by the router.

Default Gateway IPv4

The specified connection will be used by default.

Default Gateway IPv6

No IPv6 connection created.

⦿ dynamic_Internet

IGMP

On the IGMP page you can allow the router to use IGMP and configure its settings.

Connections List RECONNECT ＋ 🗑

☐	Name	Connection type	Interface	Status
☐	dynamic_Internet	Dynamic IPv4	Internet	● Connected

SIMPLIFIED MODE

*Figure 55. The **Settings / Internet / WAN** page. The advanced mode.*

To create a new connection, click the **ADD** button (＋) in the **Connections List** section. Upon that the connection creation page opens.

To edit an existing connection, in the **Connections List** section, left-click the relevant line in the table. Change the needed parameters and click the **APPLY** button.

To disconnect a connection and establish it again, select the checkbox located to the left of the relevant line in the table and click the **RECONNECT** button.

To remove a connection, in the **Connections List** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑).

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP** link (for the description of the page, see the *IGMP* section, page 143).

To use one of existing WAN connections as the default IPv4 or IPv6 connection, in the **Default Gateway** section, select the choice of the radio button which corresponds to this connection.

To return to the simplified mode, click the **SIMPLIFIED MODE** button (the button is unavailable if several WAN connections are created).

Creating Dynamic IPv4 or Static IPv4 WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

*Figure 56. The page for creating a new **Static IPv4** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.

Parameter	Description
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

Ethernet

MAC address*

58:D5:6E:9B:02:AA

◯ Clone MAC address of your NIC
(00:13:46:62:2F:4C)

RESTORE DEFAULT MAC ADDRESS

MTU*

1500

*Figure 57. The page for creating a new **Static IPv4** connection. The **Ethernet** section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.

*Figure 58. The page for creating a new **Static IPv4** connection. The **IPv4** section.*

Parameter	Description
IPv4	
*For **Static IPv4** type*	
IP address	Enter an IP address for this WAN connection.
Subnet mask	Enter a subnet mask for this WAN connection.
Gateway IP address	Enter an IP address of the gateway used by this WAN connection.
Primary DNS / Secondary DNS	Enter addresses of the primary and secondary DNS servers in the relevant fields.
*For **Dynamic IPv4** type*	
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the **Primary DNS** and **Secondary DNS** fields are not available for editing.
Primary DNS / Secondary DNS	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. *Optional*.
Hostname	A name of the router specified by your ISP. *Optional*.

When all needed settings are configured, click the **APPLY** button.

Creating Dynamic IPv6 or Static IPv6 WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

*Figure 59. The page for creating a new **Static IPv6** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

Parameter	Description
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

Ethernet

MAC address*
58:D5:6E:9B:02:AA

⊙ Clone MAC address of your NIC
(00:13:46:62:2F:4C)

RESTORE DEFAULT MAC ADDRESS

MTU*
1500

*Figure 60. The page for creating a new **Static IPv6** connection. The **Ethernet** section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.

*Figure 61. The page for creating a new **Static IPv6** connection. The **IPv6** section.*

Parameter	Description
IPv6	
*For **Static IPv6** type*	
IPv6 address	Enter an IPv6 address for this WAN connection.
Prefix	The length of the subnet prefix. The value **64** is used usually.
Gateway IPv6 address	Enter an IPv6 address of the gateway used by this WAN connection.
Primary IPv6 DNS server / Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
*For **Dynamic IPv6** type*	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (*Stateless Address Autoconfiguration*).
Gateway IPv6 address	The address of the IPv6 gateway. The field is available for editing if the **Gateway by SLAAC** switch is moved to the left.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.

Parameter	Description
Primary IPv6 DNS server / Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.

When all needed settings are configured, click the **APPLY** button.

Creating PPPoE WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

*Figure 62. The page for creating a new **PPPoE** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.

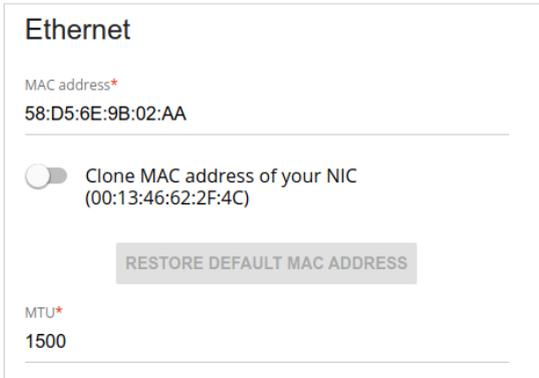| Parameter	Description
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

*Figure 63. The page for creating a new **PPPoE** connection. The **Ethernet** section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.

*Figure 64. The page for creating a new **PPPoE** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the **Show** icon (👁) to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.

Parameter	Description
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

When all needed settings are configured, click the **APPLY** button. In the simplified mode, after clicking the button, the window for creating an additional connection opens.

If your ISP offers access to local services (e.g. audio and video resources), click the **CREATE CONNECTION** button. On the page displayed, specify the parameters for the connection of the Dynamic IPv4 or Static IPv4 type and click the **APPLY** button.

If you do not need to create an additional connection, click the **SKIP** button. In this case, the **Settings / Internet / WAN** page opens.

Creating PPTP or L2TP WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

*Figure 65. The page for creating a new **PPTP** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.

Parameter	Description
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

*Figure 66. The page for creating a new **PPTP** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.

Parameter	Description
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the **Show** icon (👁) to display the entered password.
VPN server address	The IP or URL address of the PPTP or L2TP authentication server.
MTU	The maximum size of units transmitted by the interface.
Encryption protocol	Select a method of MPPE encryption. • **No encryption**: MPPE encryption is not applied. • **MPPE 40 128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied. • **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied. • **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the **MS-CHAP, MS-CHAPv2**, or **AUTO** value is selected from the **Authentication protocol** drop-down list.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Extra options	Advanced options of the pppd daemon which need to be specified for this connection. *Optional*.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.
Enable MPPC	*(Microsoft Point-to-Point Compression)* *For the **PPTP** type only*. Move the switch to the right if it is necessary to use the data compression function in order to configure the connection. Move the switch to the left to disable the function.

When all needed settings are configured, click the **APPLY** button.

After clicking the button, the window for additional configuration of the connection opens.

If you want to use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select an existing connection which will be used to access the PPTP/L2TP server and click the **CONTINUE** button; or select the **create a new connection** choice of the radio button and click the **CREATE CONNECTION** button.

If you have already configured the connection to the Internet and you want to use this WAN connection only to connect to the virtual private network, select the **to the virtual private network** choice of the radio button and click the **CONTINUE** button.

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

*Figure 67. The page for creating a new **PPPoE IPv6** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	*For the **PPPoE Dual Stack** type only.* If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.

Parameter	Description
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

*Figure 68. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.*

Parameter	Description
Ethernet	
MAC address	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, move the **Clone MAC address of your NIC** switch to the right. When the switch is moved to the right, the field is unavailable for editing. To set the router's MAC address, click the **RESTORE DEFAULT MAC ADDRESS** button (the button is available when the switch is moved to the right).
MTU	The maximum size of units transmitted by the interface.

*Figure 69. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the **Show** icon (👁) to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.

Parameter	Description
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

*Figure 70. The page for creating a new **PPPoE Pv6** connection. The **IPv6** section.*

Parameter	Description
IPv6	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (*Stateless Address Autoconfiguration*).
Gateway IPv6 address	The address of the IPv6 gateway. The field is available for editing if the **Gateway by SLAAC** switch is moved to the left.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.
Primary IPv6 DNS server / Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.

When all needed settings are configured, click the **APPLY** button.

VLAN

On the **Settings / Internet / VLAN** page, you can edit existing and create new virtual networks (VLAN), e.g., for distinguishing traffic or specifying additional WAN interfaces.

By default, 2 VLANs are created in the router's system.

- **lan**: For the LAN interface, it includes LAN ports and Wi-Fi networks. You cannot delete this VLAN.

- **wan**: For the WAN interface; it includes the **WAN** port. You can edit or delete this VLAN.

	Name	Type	Untagged ports	Tagged port	VLAN ID	Enable
☐	lan	Untagged LAN	LAN1, LAN2, LAN3, LAN4, wifi1	-	-	Yes
☐	wan	Untagged NAT	WAN	-	-	Yes

*Figure 71. The **Settings / Internet / VLAN** page.*

In order to add untagged LAN ports or available Wi-Fi networks to an existing or new VLAN, first you need to exclude them from the **lan** network on this page. To do this, select the **lan** line. On the opened page, in the **Untagged Ports** section, deselect the checkbox located to the left of the relevant element, and click the **APPLY** button.

To create a new VLAN, click the **ADD** button (+).

Figure 72. The page for adding a VLAN.

You can specify the following parameters:

Parameter	Description
Name	A name for the VLAN for easier identification.
Enable	Move the switch to the right to allow using this VLAN.
Type	The type of the VLAN. • **Untagged NAT**. The VLAN of this type is an external connection with address translation. It is mostly used to transmit untagged traffic. When this value is selected, the **VLAN ID** field and the **Tagged Ports** section are not displayed. Only one VLAN of this type can exist in the system. • **Tagged NAT**. The VLAN of this type is an external connection with address translation. It is mostly used to connect to the Internet. Later the network which identifier is specified in the **VLAN ID** field is used as an interface to create a WAN connection (on the **Settings / Internet / WAN** page). When this value is selected, the **Untagged Ports** section is not displayed. • **Bridge**. The VLAN of this type is a transparent connection between an internal port and an external connection. It is mostly used to connect IPTV set-top boxes.
VLAN ID	An identifier of the VLAN.
Untagged Ports	The section includes the ports and Wi-Fi networks that can be added to the VLAN. To add an element, select the checkbox located to the left of it. To remove an element, deselect the checkbox located to the left of it.
Tagged Ports	Select an available value to assign it to this VLAN. To do this, select the checkbox located to the left of the relevant port.

Click the **APPLY** button.

To edit an existing VLAN, select the relevant line in the table. On the page displayed, change the parameters and click the **APPLY** button.

To remove an existing VLAN, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑).

DNS

On the **Settings / Internet / DNS** page, you can add DNS servers to the system.
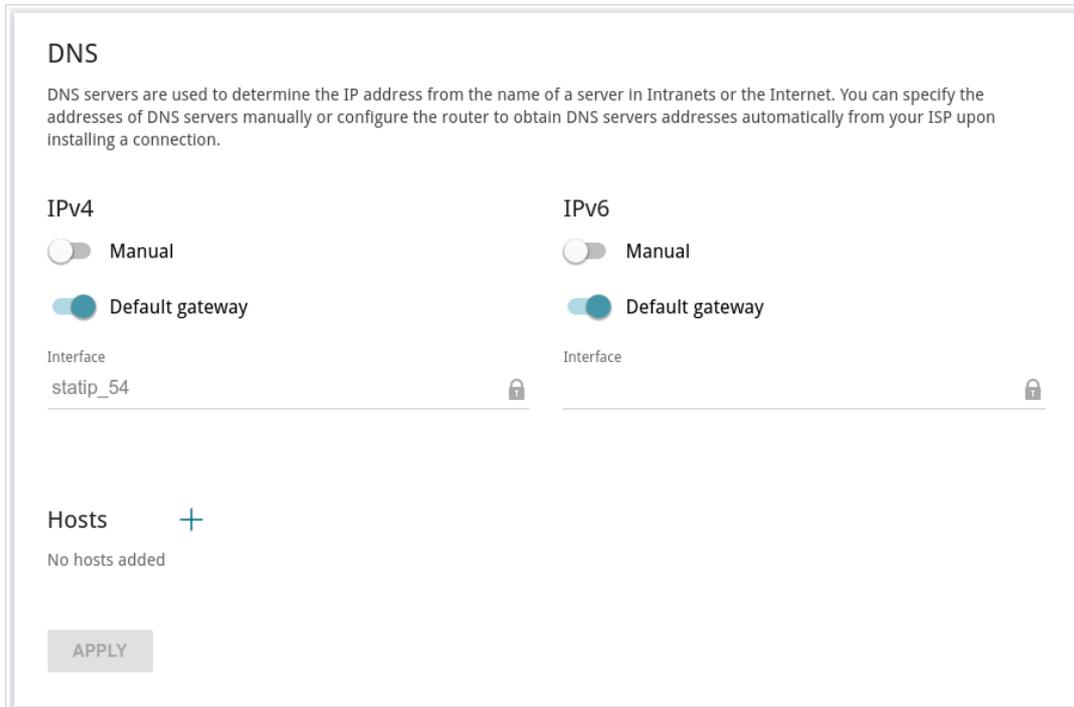
*Figure 73. The **Settings / Internet / DNS** page.*

DNS servers are used to determine the IP address from the name of a server in Intranets or the Internet (as a rule, they are specified by an ISP or assigned by a network administrator).

You can specify the addresses of DNS servers manually on this page or configure the router to obtain DNS servers addresses automatically from your ISP upon installing a connection.

> ! When you use the built-in DHCP server, the network parameters (including DNS servers) are distributed to clients automatically.

Specify needed settings for IPv4 in the **IPv4** section and for IPv6 in the **IPv6** section.

If you want to configure automatic obtainment of DNS servers addresses, move the **Manual** switch to the left. Then move the **Default gateway** switch to the left and from the **Interface** drop-down list select a WAN connection which will be used to obtain addresses of DNS servers automatically. If you want the router to use the default WAN connection to obtain addresses of DNS servers, move the **Default gateway** switch to the right. Then click the **APPLY** button.

To specify a DNS server manually, move the **Manual** switch to the right. In the **Name Servers** section of the relevant IP version, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server.

To remove a DNS server from the page, click the **Delete** icon (×) in the line of the address and then click the **APPLY** button.

If needed, you can add your own address resource record. To do this, click the **ADD** button (+) in the **Hosts** section.
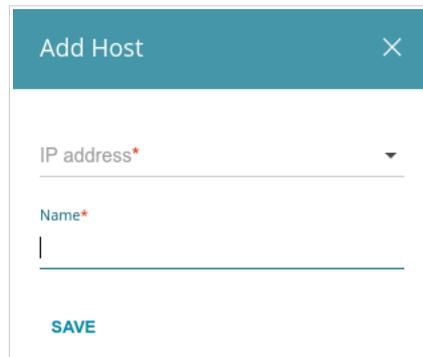
Figure 74. The window for adding a DNS record.

In the **IP address** field, specify a host from the internal or external network. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IP address from the drop-down list (the field will be filled in automatically). In the **Name** field, specify the domain name to which the specified IP address will correspond. Click the **SAVE** button.

To edit an existing record, in the **Hosts** section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a record, in the **Hosts** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑).

After completing the work with records, click the **APPLY** button.

Settings / WAN Failover

On the **Settings / WAN Failover** page, you can enable the WAN backup function, which provides you with uninterrupted access to the Internet. When your main connection breaks down, the router activates the backup connection; and when the main channel is recovered, the router switches to it and disconnects the reserve one.

*Figure 75. The **Settings / WAN Failover** page.*

To activate the backup function, create the main and the reserve WAN connections. After that go to the **Settings / WAN Failover** page, move the **Enable** switch to the right, and specify the needed values in the fields displayed on the page.

Parameter	Description
Basic connection	From the drop-down list, select a WAN connection which will be used as the main one.
Backup connection	From the drop-down list, select a WAN connection which will be used as the reserve one.
Test host	An IP address that the router will check for availability via ICMP ping mechanism.
Interval between checks	A time period (in seconds) between attempts to check the status of the main connection. By default, the value `10` is specified.

Parameter	Description
Timeout check	A time period (in seconds) for an attempt to check the status of the main connection. At the end of this period the router's internal system makes a decision to enable/disable the reserve channel. By default, the value **3** is specified.
Number of inspections of active connection	A number of requests that will be sent in order to analyze the status of the main connection when the connection is active (the router uses the main connection as a default gateway).
Number of inspections of inactive connection	A number of requests that will be sent in order to analyze the status of the main connection when the connection is inactive (the router uses the reserve connection as a default gateway).

When all needed settings are configured, click the **APPLY** button.

Settings / Wireless Network

On the **Settings / Wireless Network** page, you can change basic parameters for the wireless interface of the router and configure the basic and additional wireless networks.

Figure 76. Basic settings of the wireless LAN.

In the **Basic Settings** section, the following parameters are available:

Parameter	Description
Enable Wireless	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left.
Wireless mode	Operating mode of the wireless network of the router. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
Select channel automatically	Move the switch to the right to let the router itself choose the channel with the least interference.

Parameter	Description
Enable additional channels	If the switch is moved to the left, the device automatically selects one of available standard channels. To use additional channels (the 12th and 13th), move the switch to the right.
Channel	The wireless channel number. To select a channel manually, left-click; in the opened window, select a channel and click the **SAVE** button. The action is available, when the **Select channel automatically** switch is moved to the left. To make the router select the currently least loaded channel, click the **Refresh** icon (C). The icon is displayed, when the **Select channel automatically** switch is moved to the right.
Enable periodic scanning	Move the switch to the right to let the router search for a free channel in certain periods of time. When the switch is moved to the right, the **Scanning period** field is available for editing.
Scanning period	Specify a period of time (in seconds) after which the router rescans channels.

When you have configured the parameters, click the **APPLY** button.

To edit the settings of the basic wireless network, in the **Wi-Fi Network** section, change the needed parameters and click the **APPLY** button.

Also you can create an additional wireless network. To do this, click the **ADD WI-FI NETWORK** button. On the opened page, specify the relevant parameters.

Figure 77. Creating a wireless network.

Parameter	Description
Wi-Fi Network	
Network name (SSID)	A name for the wireless network.
Hide SSID	If the switch is moved to the right, other users cannot see your Wi-Fi network. It is recommended not to hide the network in order to simplify initial configuration of the wireless network.
BSSID	The unique identifier for this wireless network. You cannot change the value of this parameter, it is determined in the device's internal settings. The field is displayed in the settings of the existing wireless network.
Max associated clients	The maximum number of devices connected to the wireless network. When the value **0** is specified, the device does not limit the number of connected clients.

Parameter	Description
Enable shaping	Move the switch to the right to limit the maximum bandwidth of the wireless network. In the **Shaping** field displayed, specify the maximum value of speed (Mbps). Move the switch to the left not to limit the maximum bandwidth.
Broadcast wireless network	If the switch is moved to the left, devices cannot connect to the wireless network. Upon that the router can connect to another access point as a wireless client.
Clients isolation	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
Enable guest network	This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.

In the **Security Settings** section, you can change security settings of the wireless network.

By default, the **WPA2-PSK** network authentication type of the wireless network is specified. WPS PIN from the barcode label is used as the network key.
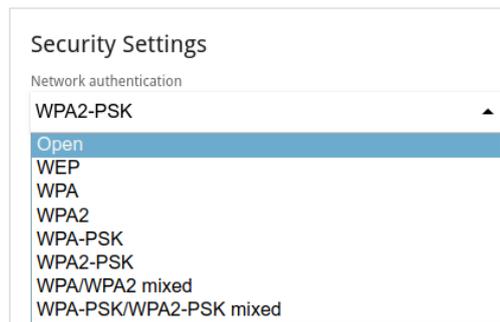
Figure 78. Network authentication types supported by the router.

The router supports the following authentication types:

Authentication type	Description
Open	Open authentication (with WEP encryption for wireless network modes not supporting 802.11n devices).
WEP	Authentication with a shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n devices is selected from the **Wireless mode** drop-down list on the **Settings / Wireless Network** page.
WPA	WPA-based authentication using a RADIUS server.
WPA-PSK	WPA-based authentication using a PSK.
WPA2	WPA2-based authentication using a RADIUS server.

Authentication type	Description
WPA2-PSK	WPA2-based authentication using a PSK.
WPA/WPA2 mixed	A mixed type of authentication. When this value is selected, devices using the **WPA** authentication type and devices using the **WPA2** authentication type can connect to the wireless network.
WPA-PSK/WPA2-PSK mixed	A mixed type of authentication. When this value is selected, devices using the **WPA-PSK** authentication type and devices using the **WPA2-PSK** authentication type can connect to the wireless network.

! The **WPA**, **WPA2**, and **WPA/WPA2 mixed** authentication types require a RADIUS server.

When the **Open** or **WEP** value is selected, the following settings are displayed on the page (unavailable for the wireless network operating modes which support the standard 802.11n):

*Figure 79. The **Open** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
Enable encryption WEP	*For* **Open** *authentication type only.* To activate WEP encryption, move the switch to the right. Upon that the **Default key ID** drop-down list, the **Encryption key WEP as HEX** switch, and four **Encryption key** fields are displayed on the page.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields. Click the **Show** icon (👁) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the following fields are displayed on the page:
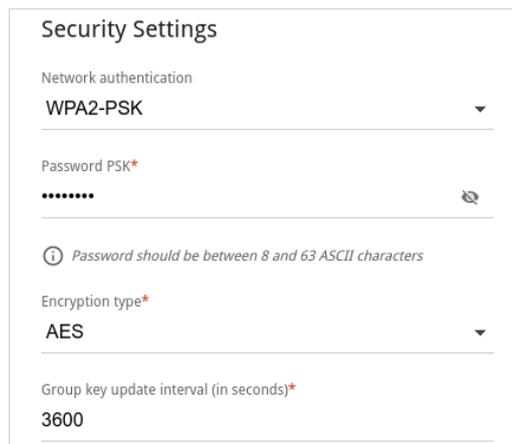
Figure 80. The **WPA2-PSK** *value is selected from the* **Network authentication** *drop-down list.*

Parameter	Description
Password PSK	A password for WPA encryption. The password can contain digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[2] Click the **Show** icon (👁) to display the entered password.
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed.

---

2   0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the following settings are displayed on the page:
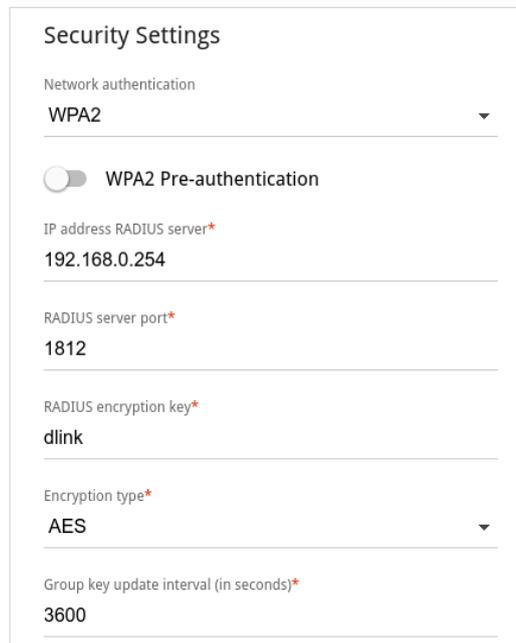
*Figure 81. The **WPA2** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
WPA2 Pre-authentication	Move the switch to the right to activate preliminary authentication (displayed only for the **WPA2** and **WPA/WPA2 mixed** authentication types).
IP address RADIUS server	The IP address of the RADIUS server.
RADIUS server port	A port of the RADIUS server.
RADIUS encryption key	The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings).
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed.

When you have configured the parameters, click the **APPLY** button.

To edit the basic or additional wireless network, left-click the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove the additional network, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑). Then click the **APPLY** button.

Settings / Network

To configure the router's local interface, go to the **Settings / Network** page.

IPv4

Go to the **IPv4** tab to change IPv4 address, configure the built-in DHCP server, or specify MAC address and IP address pairs.

```
Local IP Address

IP address*
192.168.0.1

Mask*
255.255.255.0

Hostname
dlinkrouter.local

(i)  Specify a domain name ending with .local. In order to access the web-
     based interface using the domain name, enter this name with a dot and
     slash at the end in the address bar of the web browser (for example,
     dlinkrouter.local./)
```

*Figure 82. Configuring the local interface. The **IPv4** tab. The **Local IP Address** section.*

Parameter	Description
Local IP Address	
Mode of local IP address assignment	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Setup Wizard.* Select the needed value from the drop-down list. • **Static**: The IPv4 address, subnet mask, and the gateway IP address are assigned manually. • **Dynamic**: The router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.
IP address	The IPv4 address of the router in the local subnet. By default, the following value is specified: `192.168.0.1`.
Mask	The mask of the local subnet. By default, the following value is specified: `255.255.255.0`.
Gateway IP address	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Setup Wizard.* The gateway IPv4 address which is used by the router to connect to the Internet (e.g., for synchronizing the system time with an NTP server). *Optional*.

Parameter	Description
Hostname	The name of the device assigned to its IPv4 address in the local subnet. For Wi-Fi clients, the device is not available by the domain name, if multicasting is disabled in the additional settings of Wi-Fi.

*Figure 83. Configuring the local interface. The **IPv4** tab. The **Dynamic IP Addresses** section.*

Parameter	Description
Dynamic IP Addresses	
Mode of dynamic IP address assignment	An operating mode of the router's DHCP server. • **Disable**: The router's DHCP server is disabled, clients' IP addresses are assigned manually. • **DHCP server**: The router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the **Start IP**, **End IP**, **Lease time** fields and the **DNS relay** switch are displayed on the tab. Also when this value is selected, the **DHCP Options** and **Static IP Addresses** sections are displayed on the tab. • **DHCP relay**: An external DHCP server is used to assign IP addresses to clients. When this value is selected, the **External DHCP server IP** and **Option 82 Remote ID** fields are displayed on the tab. *Available if the **Router** or **WISP Repeater** mode was selected in the Setup Wizard.*
Start IP	The start IP address of the address range used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address range used by the DHCP server to distribute IP addresses to clients.

Parameter	Description
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
DNS relay	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the **Settings / Internet / DNS** page as the DNS server address.
External DHCP server IP	The IP address of the external DHCP server which assigns IP addresses to the router's clients. To specify several IP addresses, click the **ADD** button, and in the line displayed, enter an IP address. To remove the IP address, click the **Delete** icon (×) in the line of the address.
Option 82 Remote ID	The value of the Remote ID field of DHCP option 82 in accordance with RFC3046. Do not fill in the field unless your ISP or the administrator of the external DHCP server provided this value.

When all needed settings are configured, click the **APPLY** button.

In the **DHCP Options** section, you can change default values for some options of DHCP protocol (IP address, subnet mask, DNS servers) or specify additional parameters which the built-in DHCP server should send to clients to configure the local network.
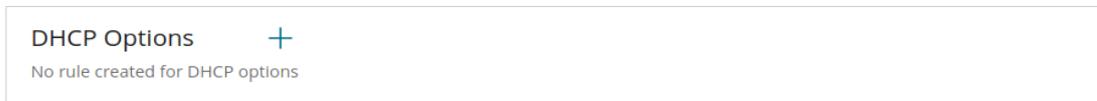
*Figure 84. Configuring the local interface. The **IPv4** tab. The section for configuring DHCP options.*

To do this, click the **ADD** button (+).
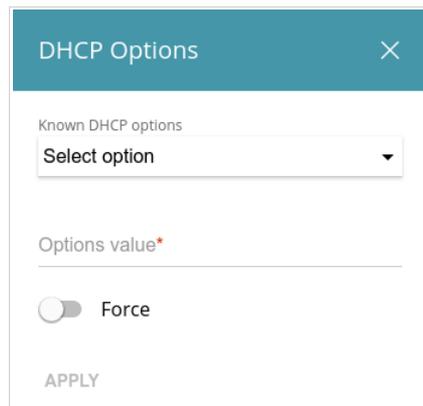
*Figure 85. Configuring the local interface. The **IPv4** tab. The window for configuring a DHCP option.*

In the opened window, you can specify the following parameters:

Parameter	Description
Known DHCP options	From the drop-down list, select an option which you want to configure.
Options value	Specify the value for the selected option.
Force	Move the switch to the right to let the DHCP server send the selected option regardless of the client's request. Move the switch to the left to let the DHCP server send the selected option only when the client requests it.

After specifying the needed parameters, click the **APPLY** button.

To edit the parameters of an option, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **APPLY** button.

To remove the value of an option, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑). Then click the **APPLY** button.

In the **Static IP Addresses** section, you can specify MAC address and IPv4 address pairs (set a fixed IPv4 address in the local area network for a device with a certain MAC address). The router assigns IPv4 addresses in accordance with the specified pairs only when the DHCP server is enabled (in the **Dynamic IP Addresses** section, the **DHCP server** value is selected from the **Mode of dynamic IP address assignment** drop-down list).

Static IP Addresses   KNOWN CLIENTS   +
In order to assign an IP address to a MAC address, select a device from the list of connected clients or add a new device

*Figure 86. Configuring the local interface. The **IPv4** tab. The section for creating MAC-IPv4 pairs.*

To create a MAC-IPv4 pair, click the **ADD** button (+). In the opened window, fill in the **MAC address** field. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant MAC address from the drop-down list (the field will be filled in automatically). Then in the **IP address** field, enter an IPv4 address which will be assigned to the device with the specified MAC address. In the **Hostname** field, specify a network name of the device for easier identification (*optional*). Click the **APPLY** button.

To create MAC-IPv4 pairs for the devices connected to the router at the moment, click the **KNOWN CLIENTS** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

To edit the settings for an existing MAC-IPv4 pair, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **APPLY** button.

To remove a MAC-IPv4 pair, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑). Then click the **APPLY** button. Also you can remove a pair in the editing window.

IPv6

Go to the **IPv6** tab to change or add the IPv6 address of the router, configure IPv6 addresses assignment settings, or specify MAC address and IPv6 address pairs.

*Figure 87. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.*

Parameter	Description
Local IPv6 Address	
Mode of local IPv6 address assignment	Select the needed value from the drop-down list. • **Static**: An IPv6 address and a prefix are specified manually. • **Prefix delegation**: The router requests a prefix to configure an IPv6 address from a delegating router.
IPv6 address	The IPv6 address of the router in the local subnet. By default, the following value is specified: `fd01::1`. The field is available for editing if the **Static** value is selected from the **Mode of local IPv6 address assignment** drop-down list.
Prefix length	The length of the prefix subnet. By default, the value `64` is specified. The field is available for editing if the **Static** value is selected from the **Mode of local IPv6 address assignment** drop-down list.

*Figure 88. Configuring the local interface. The **IPv6** tab. The **Dynamic IPv6 Addresses** section.*

Parameter	Description
Dynamic IPv6 Addresses	
Mode of dynamic IPv6 address assignment	Select the needed value from the drop-down list. • **Disable**: Clients' IPv6 addresses are assigned manually. • **Stateful**: The built-in DHCPv6 server of the router allocates addresses from the range specified in the **Start IPv6** and **End IPv6** fields. Also when this value is selected, the **Static IP Addresses** section is displayed on the tab. • **Stateless**: Clients themselves configure IPv6 addresses using the prefix.
Start IPv6	The start IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
End IPv6	The end IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
Lease time	The lifetime of IPv6 addresses provided to clients. The field is available for editing if the **Static** value is selected from the **Mode of local IPv6 address assignment** list in the **Local IPv6 Address** section.
DNS relay	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the **Settings / Internet / DNS** page as the DNS server address.

When all needed settings are configured, click the **APPLY** button.

In the **Static IP Addresses** section, you can specify MAC address and IPv6 address pairs (set a fixed IPv6 address in the local area network for a device with a certain MAC address). The router assigns IPv6 addresses in accordance with the specified pairs only when the **Stateful** value is selected from the **Mode of dynamic IPv6 address assignment** drop-down list in the **Dynamic IPv6 Addresses** section.

Static IP Addresses   KNOWN CLIENTS   +

In order to assign an IP address to a MAC address, select a device from the list of connected clients or add a new device
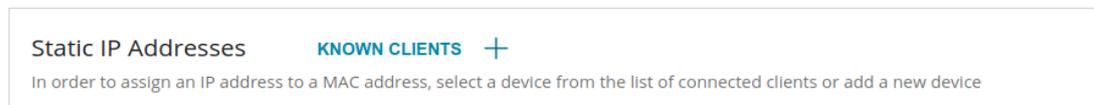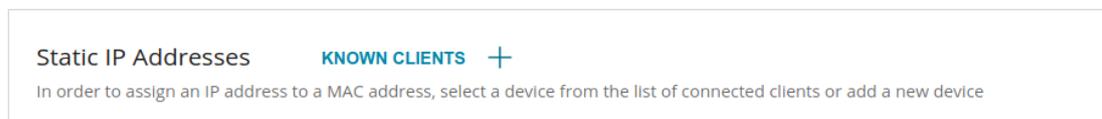
*Figure 89. Configuring the local interface. The **IPv6** tab. The section for creating MAC-IPv6 pairs.*

To create a MAC-IPv6 pair, click the **ADD** button (+). In the opened window, fill in the **MAC address** field. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant MAC address from the drop-down list (the field will be filled in automatically). Then in the **IP address** field, enter an IPv6 address which will be assigned to the device with the specified MAC address. In the **Hostname** field, specify a network name of the device for easier identification (*optional*). Click the **APPLY** button.

To create MAC-IPv6 pairs for the devices connected to the router at the moment, click the **KNOWN CLIENTS** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

To edit the settings for an existing MAC-IPv6 pair, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **APPLY** button.

To remove a MAC-IPv6 pair, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑). Then click the **APPLY** button. Also you can remove a pair in the editing window.

Functions / Firewall

IP Filter

On the **Functions / Firewall / IP Filter** page, you can create new rules for filtering IP packets and edit or remove existing rules.
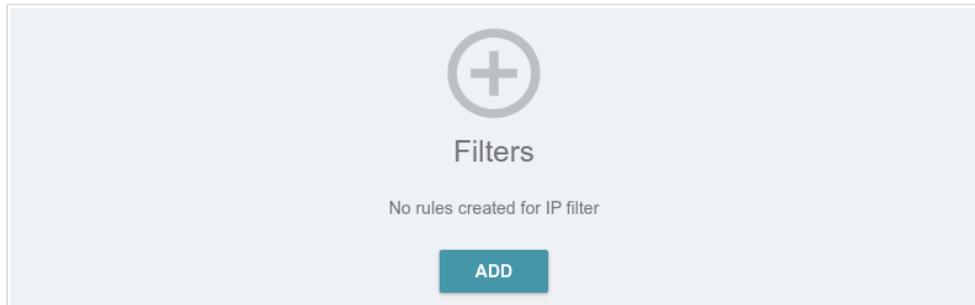
*Figure 90. The **Functions / Firewall / IP Filter** page.*

To create a new rule, click the **ADD** button (＋).

Figure 91. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
General Settings	
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Name	Enter a name for the rule for easier identification.
Action	Select an action for the rule. • **Allow**: Allows packet transmission in accordance with the criteria specified by the rule. • **Deny**: Denies packet transmission in accordance with the criteria specified by the rule.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Source IP address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The source host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the **End IPv4 address / End IPv6 address** field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The source host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The source subnet IPv4 or IPv6 address. The field is displayed when the **Subnet** value is selected from the **Set as** drop-down list.
Destination IP address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the **End IPv4 address / End IPv6 address** field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).

Parameter	Description
End IPv4 address / End IPv6 address	The destination host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The destination subnet IPv4 or IPv6 address. The field is displayed when the **Subnet** value is selected from the **Set as** drop-down list.
Ports	
Destination port	A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.
Set source port manually	Move the switch to the right to specify a port of the source IP address manually. Upon that the **Source port** field is displayed.
Source port	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

Click the **APPLY** button.

To edit a rule, select the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button (🗑). Also you can remove a rule in the editing window.

DMZ

A DMZ is a host or network segment located "between" internal (local) and external (global) networks. In the router, the DMZ implements the capability to transfer a request coming to a port of the router from the external network to a specified host of the internal network.

On the **Functions / Firewall / DMZ** page, you can specify the IP address of the DMZ host.
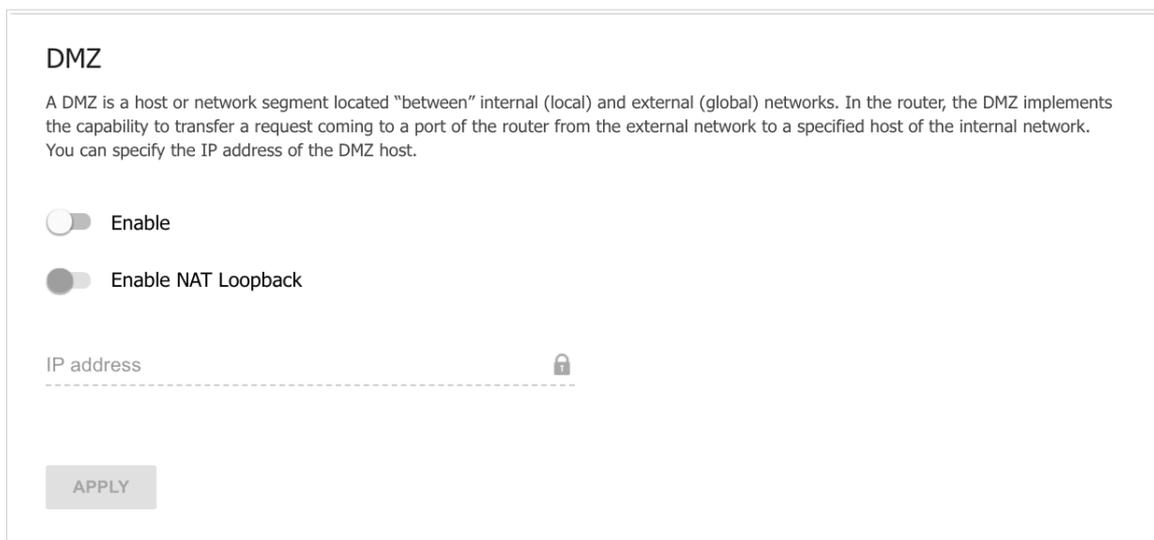
*Figure 92. The **Functions / Firewall / DMZ** page.*

To enable the DMZ, move the **Enable** switch to the right.

Enter the IP address of a host from your network in the **IP address** field. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).

Move the **Enable NAT Loopback** switch to the right in order to let the users of the router's LAN access the DMZ host using the external IP address of the router or its DDNS name (if a DDNS service is configured). Users from the external network access the router using the same address (or DDNS name).

Click the **APPLY** button.

Note that when the DMZ is enabled, all traffic coming to a port of the WAN interface of the router is directed to the same port of the specified IP address. Also note that virtual servers have higher priority than the DMZ host. In other words, if there has been created a virtual server that directs traffic from external port 80 to a port of the device from the router's local network, then entering `http://router_WAN_IP` in the address bar, users of the external network are directed to the specified port and IP address configured for the virtual server, but not to port 80 of the device with the IP address specified on the **Functions / Firewall / DMZ** page.

To disable the DMZ, move the **Enable** switch to the left and click the **APPLY** button.

MAC Filter

On the **Functions / Firewall / MAC Filter** page, you can configure MAC-address-based filtering for computers of the router's LAN.

MAC Filter

You can configure MAC-address-based filtering for computers of the router's LAN.

Default mode
Allow

List of Exceptions +

No rules created for MAC filter
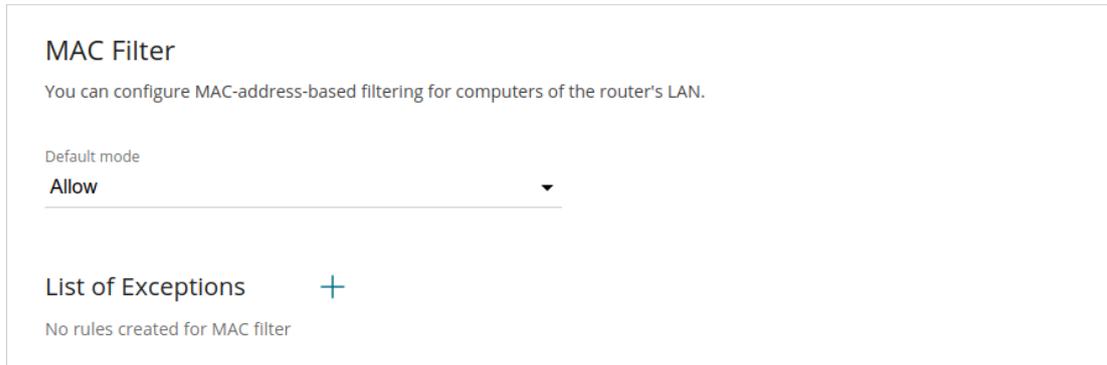
*Figure 93. The **Functions / Firewall / MAC Filter** page.*

Select the needed action from the drop-down list in the **Default mode** section to configure filtering for all devices of the router's network:

- **Allow**: Allows access to the router's network and to the Internet for devices (the value is specified by default);

- **Deny**: Blocks access to the router's network for devices.

> ! You can use the **Deny** mode only if an active rule which allows access to the device's network is created on the page.

To create a rule (specify a MAC address of a device for which the specified filtering mode will be applied), click the **ADD** button (+).

Add Rule   ✕

⬤ Enable rule

Allow

MAC address*

Hostname

SAVE
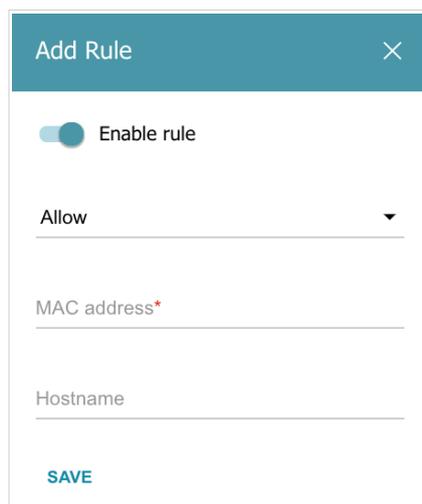
Figure 94. The window for adding a rule for the MAC filter.

In the opened window, you can specify the following parameters:

Parameter	Description
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. • **Deny**: Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices. • **Allow**: Allows access to the router's network and to the Internet for the device with the specified MAC address even if the default mode denies access for all devices.
MAC address	The MAC address of a device from the router's LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Hostname	The name of the device for easier identification (*optional*). You can specify any name.

After specifying the needed parameters, click the **SAVE** button.

To edit a rule, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button (🗑). Also you can remove a rule in the editing window.

Websites Filter

On the **Function / Firewall / Websites Filter** page, you can specify restrictions on access to certain web sites and define devices to which the specified restrictions will be applied.

*Figure 95. The **Function / Firewall / Websites Filter** page.*

To enable the filter, move the **Enable** switch to the right, then select a mode from the **Address filtering** drop-down list:

- **Block listed URLs**: When this value is selected, the router blocks access to all web sites specified in the **Addresses** section;
- **Block all URLs except listed**: When this value is selected, the router allows access to web sites specified in the **Addresses** section and blocks access to all other web sites.

To specify URL addresses to which the selected filtering mode will be applied, in the **Addresses** section, click the **ADD** button (✚). In the opened window, you can specify the following parameters:

Parameter	Description
URL address	A URL address, a part of URL address, or a keyword.
Match with template	Select a value from the drop-down list. • **Full**: The request address should exactly match the value specified in the field above. • **Begin**: The request address should begin with the value specified in the field above. • **End**: The request address should end with the value specified in the field above. • **Partly**: The request address should contain the value specified in the field above in any part of it.

Click the **SAVE** button.

To remove a URL address from the list, select the checkbox located to the left of the relevant address in the table and click the **DELETE** button (🗑). Also you can remove an address in the editing window.

To define devices to which the specified restrictions will be applied, select a needed value from the **Client filtering** drop-down list.

- **Devices from list**: When this value is selected, the router applies restrictions only to the devices specified in the **Clients** section;

- **All but devices from the list**: When this value is selected, the router does not apply restrictions to the devices specified in the **Clients** section, but applies restrictions to other devices.

To add a client to the list, in the **Clients** section, click the **ADD** button (➕). In the opened window, in the **MAC address** field, enter the MAC address of the device from the LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically). Then specify a name of the device for easier identification in the **Name** field and click the **SAVE** button.

To remove a client from the list, select the checkbox located to the left of the relevant rule in the table and click the **DELETE** button (🗑). Also you can remove a client in the editing window.

After completing configuration of the filter, click the **APPLY** button.

DoS Protection

On the **Functions / Firewall / DoS Protection** page, you can configure protection against DoS attacks of different types.

DoS (*Denial of Service*) attacks are network attacks during which the router and devices connected to it are flooded with more requests than they can handle, which leads to significant reduce of performance or even their malfunction.

*Figure 96. The **Functions / Firewall / DoS Protection** page.*

To enable protection against DoS attacks, move the **Enable** switch to the right. Upon that the **Per-source IP Flood** and **Other Settings** sections are displayed on the page.

In the **Per-source IP Flood** section you can enable protection against main types of DoS attacks.

Parameter	Description
TCP/SYN	Enables protection against a flood with connection requests (TCP packets with the SYN flag).
TCP/FIN	Enables protection against a flood with requests for connection termination (TCP packets with the FIN flag).
UDP	Enables protection against a flood with UDP packets.
ICMP	Enables protection against a flood with ICMP packets.

Move the relevant switches to the right. In the **threshold** field corresponding to the switch, specify the maximum number of packets which arrive from one IP address within one second. The value of the field should be greater than zero (for example, `200`). Then, in the **Other Settings** section, move the **Block source IP** switch to the right, and in the **Block time** field, specify the time period (in seconds) during which the source IP address will be blocked. For example, you can specify `120`. When the threshold value is exceeded, the source of packets will be blocked for the specified time period.

In the **Other Settings** section, you can activate additional protection methods.

Parameter	Description
TCP/UDP port scan	Blocks the source of TCP or UDP packets which check the ports state if the router receives more than 200 requests per second from one IP address. The source of packets will be blocked during the time period specified in the **Block time** field (the field is displayed if the **Block source IP** switch is moved to the right). If the switch is moved to the right, the **High sensitivity** switch is displayed on the page. Activate the setting to let the router block the source if it sends more than 10 requests per second.
IP Land	Blocks TCP packets with the SYN flag in which the source IP address and port coincides with the destination IP address and port.
IP Spoof	Block packets in which the source IP address coincides with the router's LAN IP address.
IP TearDrop	Blocks fragmented IP packets if errors can occur upon assembling these packets.
TCP scan	Blocks TCP packets with invalid flags.
TCP/SYN with data	Blocks TCP packets with the SYN flag if they are fragmented or contain data.
UDP Bomb	Blocks UDP packets if they contain incorrect service data.
Block source IP	Move the switch to the right to block the sources of packets protection against which is activated in the **Other Settings** section for a certain time period. Then, in the **Block time** field displayed, specify the needed value (in seconds).

After specifying the needed parameters, click the **APPLY** button.

Functions / Wi-Fi

Client Management

On the **Functions / Wi-Fi / Client Management** page, you can view the list of wireless clients connected to the router.

Client Management

You can view the list of wireless clients connected to the router.

	Hostname	MAC address	Network name (SSID)	Signal level	Online
☐					
☐	MI6-MiPhone	50:8F:4C:E3:9E:50	DIR-XXX	🛜 69%	5 min

List of Wi-Fi Clients   REFRESH   DISCONNECT

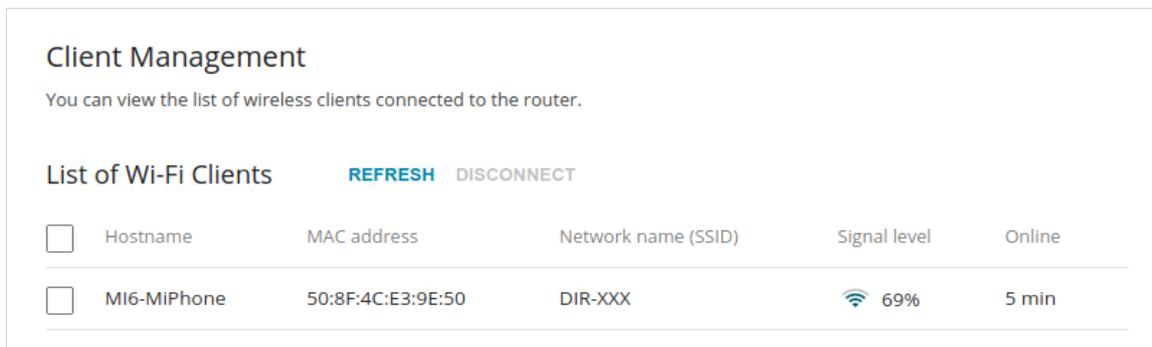*Figure 97. The page for managing the wireless clients.*

If you want to disconnect a wireless device from your WLAN, select the checkbox in the line containing the MAC address of this device and click the **DISCONNECT** button.

To view the latest data on the devices connected to the WLAN, click the **REFRESH** button.

To view data on a connected device, left-click the line containing the MAC address of this device.

WPS

On the **Functions / Wi-Fi / WPS** page, you can enable the function for configuration of the WLAN.

The WPS function helps to configure the wireless network automatically. Devices connecting to the wireless network via the WPS function must support the WPS function.

> ! The WPS function allows adding devices only to the basic wireless network of the router.

> ! Before using the function you need to configure one of the following authentication types: **Open** with no encryption, **WPA2-PSK** or **WPA-PSK/WPA2-PSK mixed** with the **AES** encryption method. When other security settings are specified, controls of the **WPS** page are not available.

Figure 98. The page for configuring the WPS function.

You can activate the WPS function via the web-based interface or the hardware **WPS/RESET** button on the cover of the device.

To activate the WPS function via the hardware button, move the **Enable WPS function with hardware button** switch to the right. Then, with the device turned on, push the **WPS/RESET** button and release it. The **WLAN / WPS** LED should start blinking slowly. In addition, upon pushing the button, the wireless interface of the device is enabled if it was disabled before.

If you want to disable activating the WPS function via the hardware button, move the **Enable WPS function with hardware button** switch to the left and make sure that the WPS function is not activated via the web-based interface.

To activate the WPS function via the web-based interface, click the **ENABLE WPS** button.

When the WPS function is enabled, the **Information** section is available on the page.

Parameter	Description
WPS state	The state of the WPS function: • **Configured** (all needed settings are specified; these settings will be used upon establishing the wireless connection) • **Unconfigured** (after activating the WPS function, the SSID and the encryption key will be configured automatically, the network authentication type will be changed to WPA2-PSK).
Network name (SSID)	The name of the router's wireless network.
Network authentication	The network authentication type specified for the wireless network.
Encryption	The encryption type specified for the wireless network.
Password PSK	The encryption password specified for the wireless network.
UPDATE	Click the button to update the data on the page.
RESET TO UNCONFIGURED	Click the button to reset the parameters of the WPS function.

Using WPS Function via Web-based Interface

To connect to the basic wireless network via the WPS function, follow the next steps:

1. Click the **ENABLE WPS** button.

2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.

3. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.

4. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.

5. Right after that, click the **CONNECT** button in the web-based interface of the router.

Using WPS Function without Web-based Interface

You can use the WPS function without accessing the web-based interface of the router. To do this, you need to configure the following router's settings:

1. Specify relevant security settings for the wireless network of the router.

2. Make sure that the **Enable WPS function with hardware button** switch is moved to the right.

3. Click the **ENABLE WPS** button.

4. Close the web-based interface (click the **Logout** line of the menu).

Later you will be able to add wireless devices to the WLAN by pressing the **WPS/RESET** button of the router.

1. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.

2. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.

3. Press the **WPS/RESET** button of the router and release. The **WLAN / WPS** LED will start blinking slowly.

WMM

On the **Functions / Wi-Fi / WMM** page, you can enable the Wi-Fi Multimedia function.

The WMM function implements the QoS features for Wi-Fi networks. It helps to improve the quality of data transfer over Wi-Fi networks by prioritizing different types of traffic.

Select the needed action from the **Work mode** drop-down list to configure the WMM function:

- **Auto**: the settings of the WMM function are configured automatically (the value is specified by default).
- **Manual**: the settings of the WMM function are configured manually. When this value is selected, the **Access Point** and **Station** sections are displayed on the page.
- **Disabled**: The WMM function is disabled.

Wi-Fi Multimedia

The mechanism for improving Wi-Fi network performance. It is recommended for users not to change the specified values

Work mode

Manual

Access Point

AC	AIFSN	CWMin	CWMax	TXOP	ACM	ACK
BK	7	31	1023	0	off	off
BE	3	15	63	0	off	off
VI	1	7	15	94	off	off
VO	1	3	7	47	off	off

Station

AC	AIFSN	CWMin	CWMax	TXOP	ACM
BK	7	15	1023	0	off
BE	3	15	1023	0	off
VI	2	7	15	94	off
VO	2	3	7	47	off

Figure 99. The page for configuring the WMM function.

! All needed settings for the WMM function are specified in the device's system. Changing parameters manually may negatively affect your WLAN!

The WMM function allows assigning priorities for four Access Categories (AC):

- **BK** (*Background*), low priority traffic (print jobs, file downloads, etc.).
- **BE** (*Best Effort*), traffic from legacy devices or devices/applications that do not support QoS.
- **VI** (*Video*).
- **VO** (*Voice*).

Parameters of the Access Categories are defined for both the router itself (in the **Access Point** section) and wireless devices connected to it (in the **Station** section).

To edit the parameters of an Access Category, left-click the relevant line. In the opened window, change the needed parameters.

Figure 100. The window for changing parameters of the WMM function.

Parameter	Description
AIFSN	*Arbitrary Inter-Frame Space Number*. This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
CWMin / CWMax	*Contention Window Minimum/Contention Window Maximum*. Both fields influence time delays for the relevant Access Category. The **CWMax** field value should not be lower, than the **CWMin** field value. The lower the difference between the **CWMax** field value and the **CWMin** field value, the higher is the Access Category priority.
TXOP	*Transmission Opportunity*. The higher the value, the higher is the Access Category priority.
ACM	*Admission Control Mandatory*. If the switch is moved to the right, the device cannot use the relevant Access Category.
ACK	*Acknowledgment*. Answering response requests while transmitting. Displayed only in the **Access Point** section. If the switch is moved to the left, the router answers requests. If the switch is moved to the right, the router does not answer requests.

Click the **SAVE** button.

Client

On the **Functions / Wi-Fi / Client** page, you can configure the router as a client to connect to a wireless access point or to a WISP.

Figure 101. The page for configuring the client mode.

To configure the router as a client, move the **Enable** switch to the right. Upon that the following fields are displayed on the page:

Parameter	Description
Broadcast wireless network 2.4 GHz	If the switch is moved to the left, devices cannot connect to the router's WLAN. Upon that the router can connect to another access point as a wireless client.
Connecting to network	A method for connecting to another access point.

In the **Wireless Networks** section, the list of available wireless networks is displayed. To view the latest data on available wireless networks, click the **UPDATE LIST** button.

To connect to a wireless network from the list, select the needed network. Move the **Network options** switch to the right to view more detailed information on the network to which the router connects. If a password is required, enter it in the relevant field. Click the **CONNECT** button.

To connect to a hidden network, select the **Connect to hidden network** value from the **Connecting to network** drop-down list. Then enter the network name in the **Network name (SSID)** field. If needed, fill in the **BSSID** field. Then select the needed type of authentication from the **Network authentication** drop-down list.

When the **Open** or **WEP** authentication type is selected, the following settings are displayed on the page:

Parameter	Description
Enable encryption WEP	*For **Open** authentication type only.* To activate WEP encryption, move the switch to the right. Upon that the **Default key ID** drop-down list, the **Encryption key WEP as HEX** switch, and four **Encryption key** fields are displayed on the page.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields. Click the **Show** icon ( ) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** authentication type is selected, the following fields are displayed:

Parameter	Description
Password PSK	A password for WPA encryption. Click the **Show** icon ( ) to display the entered password.
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.

When you have configured the parameters, click the **APPLY** button.

When connecting to a wireless access point, the wireless channel of DIR-615 will switch to the channel of the access point to which you have connected.

In addition, the **Connection Information** section in which you can view the connection status and the network basic parameters is displayed.

If you want to connect to the WISP network, after configuring the device as a client, you need to create a WAN connection with relevant parameters for the **WiFiClient** interface.

Client Shaping

On the **Functions / Wi-Fi / Client Shaping** page, you can limit the maximum bandwidth of upstream and downstream traffic for each wireless client of the router by its MAC address.
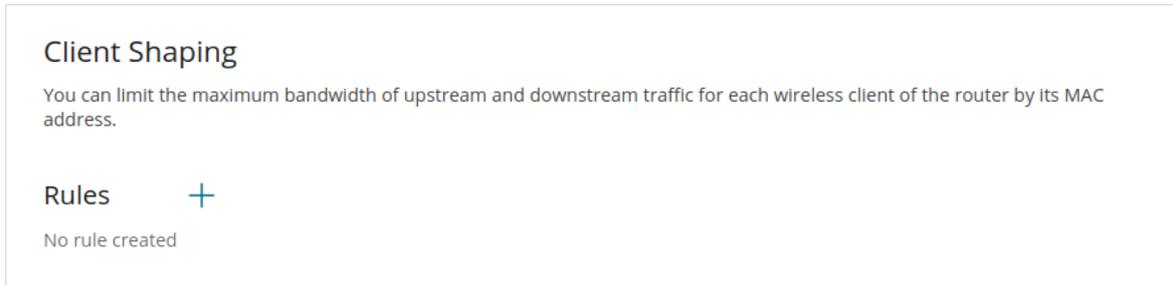

*Figure 102. The **Functions / Wi-Fi / Client Shaping** page.*

If you want to limit the maximum bandwidth of traffic for the router's wireless client, create a relevant rule. To do this, click the **ADD** button (+).
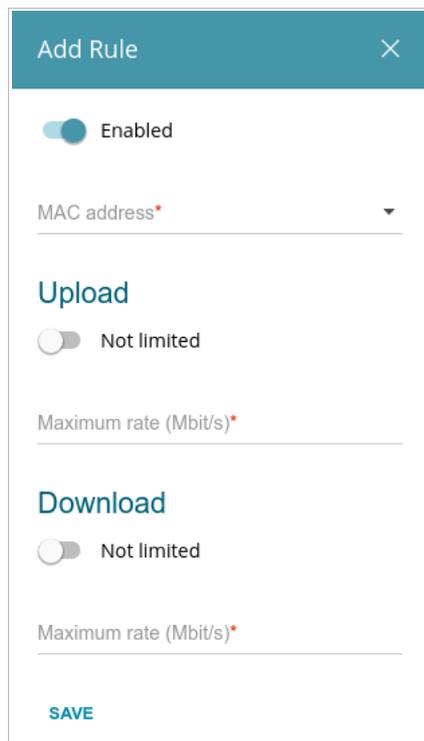

Figure 103. The window for setting up rate limit.

In the opened window, you can specify the following parameters:

Parameter	Description
Enabled	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.
MAC address	In the field, enter the MAC address to which the rule will be applied. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Upload	
Maximum rate	Specify the maximum value of the upstream traffic rate (Mbps) or move the **Not limited** switch to the right not to limit the maximum bandwidth of upstream traffic.
Download	
Maximum rate	Specify the maximum value of the downstream traffic rate (Mbps) or move the **Not limited** switch to the right not to limit the maximum bandwidth of downstream traffic.

After specifying the needed parameters, click the **SAVE** button.

To edit a rule, left-click the relevant rule. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ( ).

Additional

On page of the **Functions / Wi-Fi / Additional** section, you can define additional parameters for the WLAN of the router.

> ! <u>Changing parameters presented on this page may negatively affect your WLAN!</u>

Figure 104. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	The channel bandwidth for 802.11n standard. • **20 MHz**: 802.11n clients operate at 20MHz channels. • **20/40 MHz**: 802.11n clients operate at 20MHz or 40MHz channels.

Parameter	Description
Autonegotiation 20/40 (Coexistence)	Move the switch to the right to let the router automatically choose the channel bandwidth (20MHz or 40MHz) depending on availability of other APs within its operational range (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the **20/40 MHz** value is selected from the **Bandwidth** drop-down list.
TX power	The transmit power (in percentage terms) of the router.
Drop multicast	Move the switch to the right to disable multicasting for the router's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected on the **Functions / Advanced / IGMP** page.
Adaptivity mode	Move the switch to the right to prevent your wireless network from interfering with radars and other mobile or stationary radio systems. Such a setting can slow down the router's WLAN.
B/G protection	The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Select a value from the drop-down list. • **Auto**: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices). • **Always On**: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network). • **Always Off**: The protection function is always disabled.
Short GI	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices. • **Enable**: The router uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n and 802.11ac standards (see the value of the **Wireless mode** drop-down list on the **Settings / Wireless Network** page). • **Disable**: The router uses the 800 ns standard guard interval.

Parameter	Description
Method of channel auto select	A method of automatic channel selection. • **BSS (by signal level)** (*Basic Service Set*): When this value is selected, the router analyzes the signal levels of the neighboring wireless networks and selects a channel with the minimum value of the total level of interference from these networks. • **FA & CCA (by volume of data transmitted)** (*False Alarm and Clear Channel Assessment*): When this value is selected, the router analyzes the volume of data transmitted in the neighboring wireless networks and selects a channel with the minimum value of the total number of packets transmitted in these networks upon scanning them.
Beacon period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS threshold	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
Frag threshold	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).
DTIM period	The number of beacon frames between sending DTIM messages (messages notifying on broadcast or multicast transmission).
Station Keep Alive	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value **0** is specified, the checking is disabled.

When you have configured the parameters, click the **APPLY** button.

MAC Filter

On the **Functions / 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 MAC addresses of devices which will not be allowed to access the WLAN.

> **!** It is recommended to configure the Wi-Fi MAC filter through a wired connection to DIR-615.

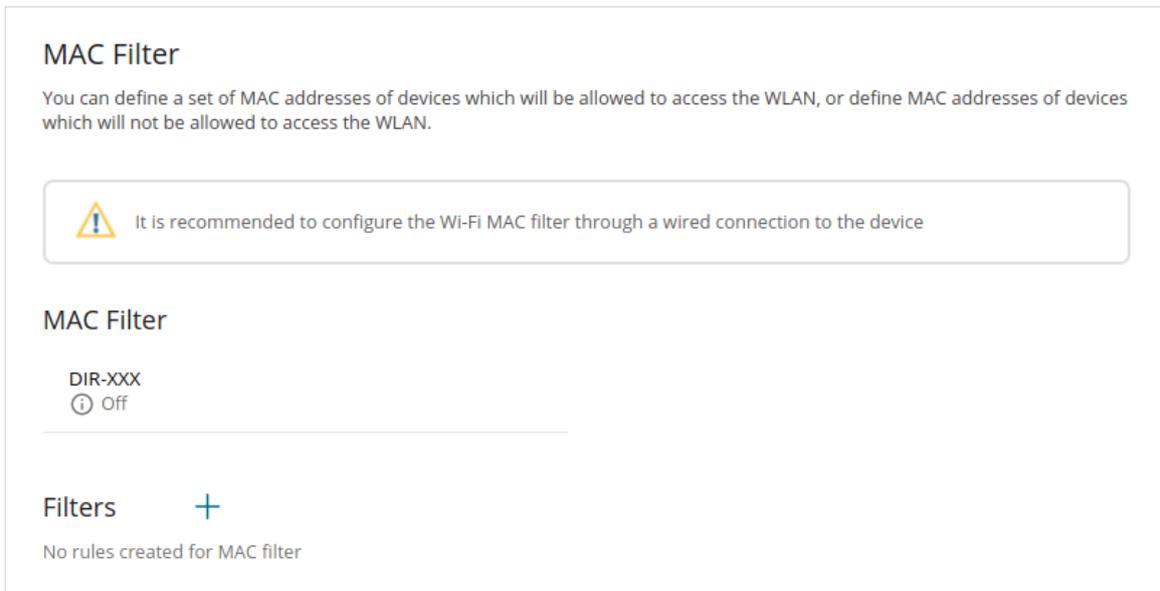

Figure 105. The page for configuring the MAC filter for the wireless network.

By default, the Wi-Fi MAC filter is not configured.

To configure the MAC filter, first you need to create rules (specify MAC addresses of devices for which the specified filtering modes will be applied). To do this, click the **ADD** button (+).
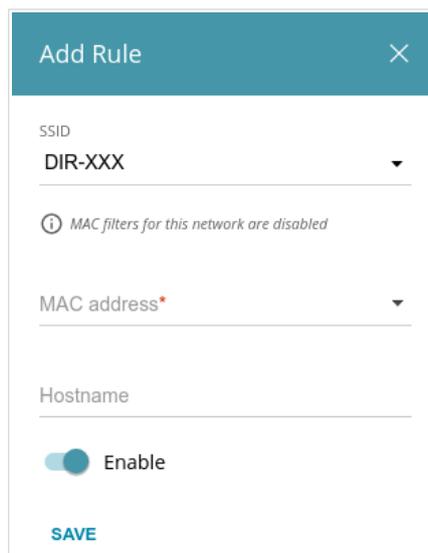

Figure 106. The window for adding a rule for the MAC filter.

You can specify the following parameters:

Parameter	Description
SSID	A wireless network to which the rule will be applied. Select the needed value from the drop-down list.
MAC address	In the field, enter the MAC address of the device to which the selected filtering mode will be applied. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Hostname	The name of the device for easier identification (*optional*). You can specify any name.
Enable	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.

When you have configured the parameters, click the **SAVE** button.

To edit the parameters of the existing rule, in the **Filters** section, left-click the needed rule. In the opened window, change the settings and click the **SAVE** button.

To remove the rule from the page, in the **Filters** section, select the checkbox located to the left of the relevant rule and click the **DELETE** button ( ).

After creating the rules you need to configure the filtering modes.

To open the basic or additional wireless network for the devices which MAC addresses are specified on this page and to close the wireless network for all other devices, left-click the line of the wireless network. In the opened window, move the **Enable MAC filter** switch to the right. Select the **Allow** value from the **MAC filter restrict mode** drop-down list and click the **SAVE** button.

To close the wireless network for the devices which MAC addresses are specified on this page, select the **Deny** value from the **MAC filter restrict mode** drop-down list and click the **SAVE** button.

Functions / Advanced

UPnP IGD

On the **Functions / Advanced / UPnP IGD** page, you can enable the UPnP IGD protocol. The router uses the UPnP IGD protocol for automatic configuration of its parameters for network applications requiring an incoming connection to the router.
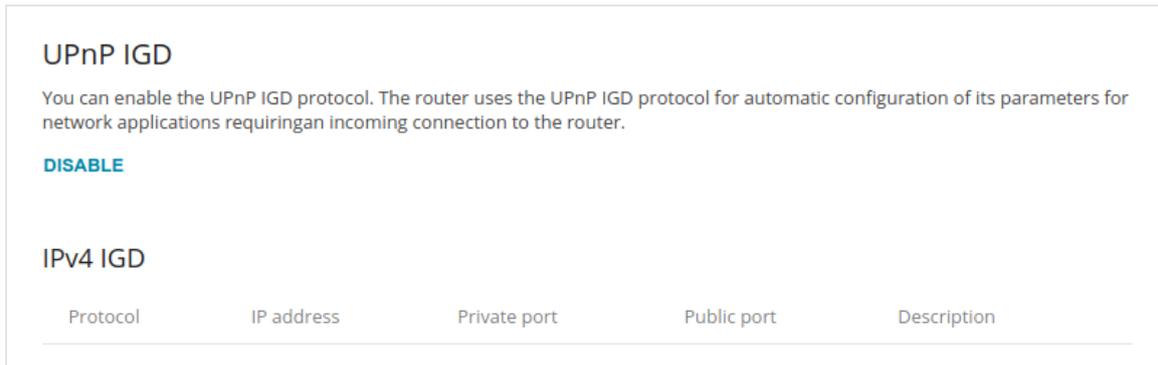

*Figure 107. The **Functions / Advanced / UPnP IGD** page.*

If you want to manually specify all parameters needed for network applications, click the **DISABLE** button. Then go to the **Functions / Advanced / Virtual Servers** page and specify needed settings.

If you want to enable the UPnP IGD protocol in the router, click the **ENABLE** button.

When the protocol is enabled, the router's parameters configured automatically are displayed on the page:

Parameter	Description
Protocol	A protocol for network packet transmission.
IP address	The IP address of a client from the local area network.
Private port	A port of a client's IP address to which traffic is directed from a public port of the router.
Public port	A public port of the router from which traffic is directed to a client's IP address.
Description	Information transmitted by a client's network application.

Remote Access

On the **Functions / Advanced / Remote Access** page, you can configure access to the web-based interface of the router. By default, the access from external networks to the router is closed. If you need to allow access to the router from the external network, create relevant rules.
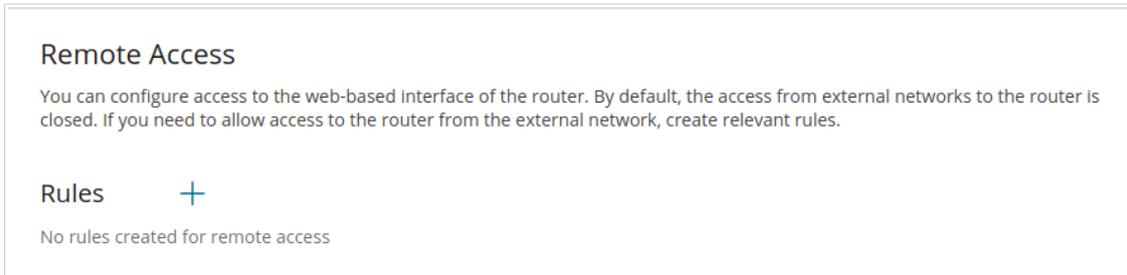

*Figure 108. The **Functions / Advanced / Remote Access** page.*

To create a new rule, click the **ADD** button (✛).

Figure 109. The window for adding a rule for remote management.

In the opened window, you can specify the following parameters:

Parameter	Description
Name	A name for the rule for easier identification. You can specify any name.

Parameter	Description
Interface	From the drop-down list, select an interface (WAN connection) through which remote access to the router will operate. Leave the **Automatic** value to allow remote access to operate through all created WAN connections.
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Open access from any external host	Move the switch to the right to allow access to the router for any host. Upon that the **IP address** and **Mask** fields are not displayed.
IP address	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.
Mask	*For the IPv4-based network only.* The mask of the subnet.
Public port	*For the IPv4-based network only.* An external port of the router. You can specify only one port.
Protocol	The protocol available for remote management of the router.

After specifying the needed parameters, click the **SAVE** button.

To edit a rule for remote access, left-click the relevant rule. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule for remote access, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑).

Virtual Servers

On the **Functions / Advanced / Virtual Servers** page, you can create virtual servers for redirecting incoming Internet traffic to a specified IP address in the local area network.
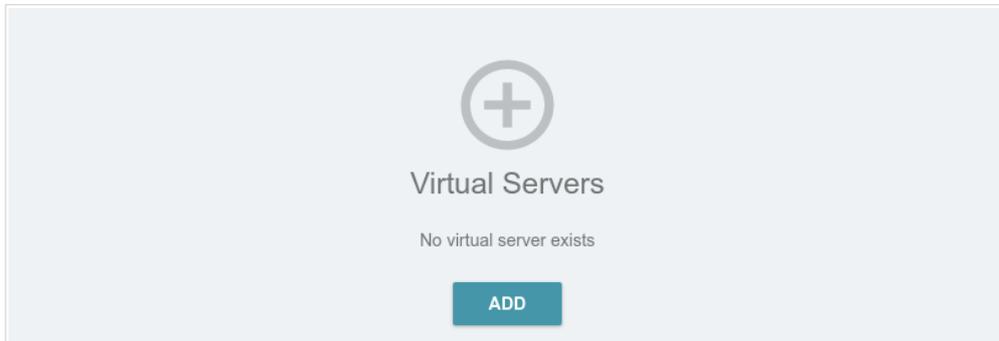

*Figure 110. The **Functions / Advanced / Virtual Servers** page.*

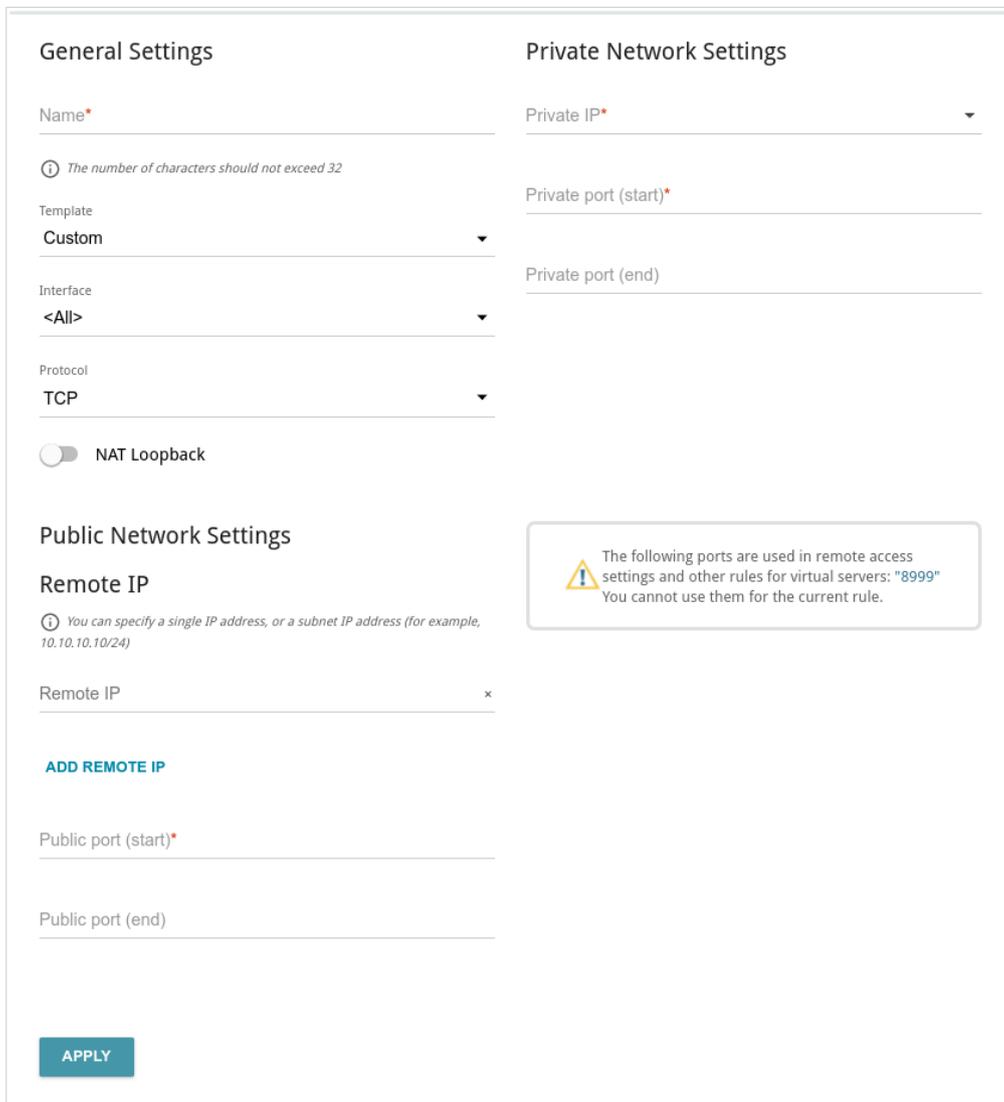To create a new virtual server, click the **ADD** button ( ).

Figure 111. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
General Settings	
Name	A name for the virtual server for easier identification. You can specify any name.
Template	Select a virtual server template from the drop-down list, or select **Custom** to specify all parameters of the new virtual server manually.
Interface	A WAN connection to which this virtual server will be assigned.
Protocol	A protocol that will be used by the new virtual server. Select a value from the drop-down list.
NAT Loopback	Move the switch to the right in order to let the users of the router's LAN access the local server using the external IP address of the router or its DDNS name (if a DDNS service is configured). Users from the external network access the router using the same address (or DDNS name).
Public Network Settings	
Remote IP	Enter the IP address of the server from the external network. To add one more IP address, click the **ADD REMOTE IP** button and enter the address in the displayed line. To remove the IP address, click the **Delete** icon (✖) in the line of the address.
Public port (start) / Public port (end)	A port of the router from which traffic is directed to the IP address specified in the **Private IP** field in the **Private Network Settings** section. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the **Public port (start)** field and leave the **Public port (end)** field blank.
Private Network Settings	
Private IP	The IP address of the server from the local area network. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).
Private port (start) / Private port (end)	A port of the IP address specified in the **Private IP** field to which traffic is directed from the **Public port**. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the **Private port (start)** field and leave the **Private port (end)** field blank.

Click the **APPLY** button.

To edit the parameters of an existing server, select the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove a server, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button (🗑). Also you can remove a server on the editing page.

TR-069 Client

On the **Functions / Advanced / 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.

Figure 112. The page for configuring the TR-069 client.

You can specify the following parameters:

Parameter	Description
TR-069 Client	
Enable TR-069 client	Move the switch to the right to enable the TR-069 client.
Interface	The interface which the router uses for communication with the ACS. Leave the **Automatic** value to let the device select the interface basing on the routing table or select another value if required by your ISP.

Parameter	Description
Inform Settings	
On	Move the switch to the right so the router may send reports (data on the device and network statistics) to the ACS.
Interval	Specify the time period (in seconds) between sending reports.
Auto Configuration Server Settings	
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS. Click the **Show** icon (👁) to display the entered password.
Connection Request Settings	
Username	The username used by the ACS to transfer a connection request to the router.
Password	The password used by the ACS. Click the **Show** icon (👁) to display the entered password.
Request port	The port used by the ACS. By default, the port `8999` is specified.
Request path	The path used by the ACS.

When you have configured the parameters, click the **APPLY** button.

Static Route

On the **Functions / Advanced / Static Route** page, you can specify static (fixed) routes.

Routing

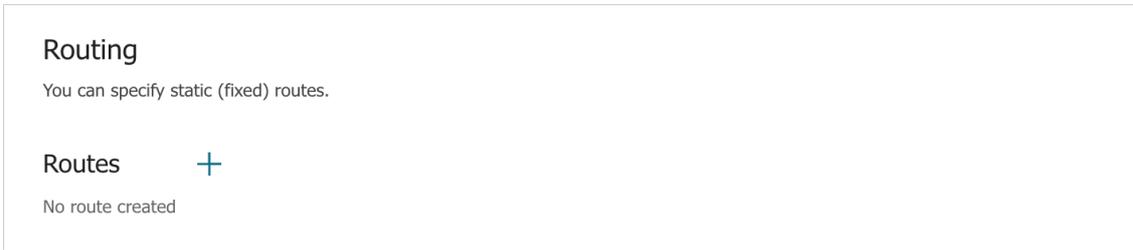You can specify static (fixed) routes.

Routes ➕

No route created

*Figure 113. The **Functions / Advanced / Static Route** page.*

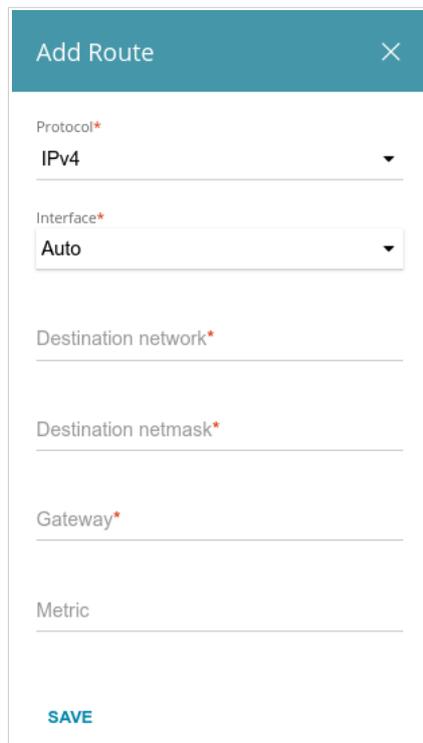To specify a new route, click the **ADD** button (➕) in the **Routes** section.

Add Route ✕

Protocol*
IPv4 ▾

Interface*
Auto ▾

Destination network*

Destination netmask*

Gateway*

Metric

SAVE

Figure 114. The window for adding a new route.

In the opened window, you can specify the following parameters:

Parameter	Description
Protocol	An IP version.
Interface	From the drop-down list, select an interface (connection) through which the device will communicate with the remote network. If you have selected the **Auto** value, the router itself sets the interface according to the data on the existing dynamic routes.
Destination network	A remote network which can be accessed with help of this route. You can specify an IPv4 or IPv6 address. The format of a host IPv6 address is `2001:db8:1234::1`, the format of a subnet IPv6 address is `2001:db8:1234::/64`.
Destination netmask	*For IPv4 protocol only.* The remote network mask.
Gateway	An IP address through which the destination network can be accessed.
Metric	A metric for the route. The lower the value, the higher is the route priority. *Optional*.

After specifying the needed parameters, click the **SAVE** button.

To edit an existing route, select a relevant line of the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove an existing route, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑).

Dynamic DNS

On the **Functions / Advanced / Dynamic DNS** page, you can define parameters of the DDNS service, which allows associating a domain name with dynamic IP addresses.
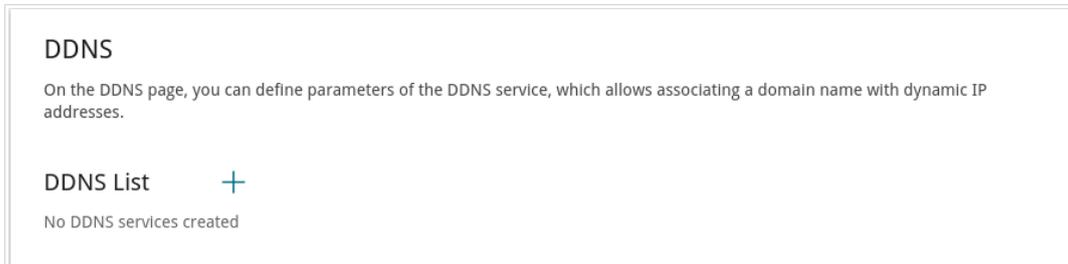
DDNS

On the DDNS page, you can define parameters of the DDNS service, which allows associating a domain name with dynamic IP addresses.

DDNS List ✛

No DDNS services created

*Figure 115. The **Functions / Advanced / Dynamic DNS** page.*

To configure needed settings for the router, click the **ADD** button (✛).

Hostname*

ⓘ *You must specify a fully qualified domain name. For example, example.com*

DDNS service*
DynDNS.com ▾

Username*

Password* 👁

Update period (in minutes)*

SAVE

Figure 116. The page for adding a DDNS service.

On the opened page, you can specify the following parameters:

| Parameter	Description
Hostname	The full domain name registered at your DDNS provider.
DDNS service	Select a DDNS provider from the drop-down list.
Username	The username to authorize for your DDNS provider.
Password	The password to authorize for your DDNS provider. Click the **Show** icon (👁) to display the entered password.
Update period	An interval (in minutes) between sending data on the router's external IP address to the relevant DDNS service.

After specifying the needed parameters, click the **SAVE** button.

To specify other parameters for a DDNS service, select the relevant line in the table. On the opened page, change the needed parameters and click the **SAVE** button.

To remove settings for a DDNS service, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (🗑).
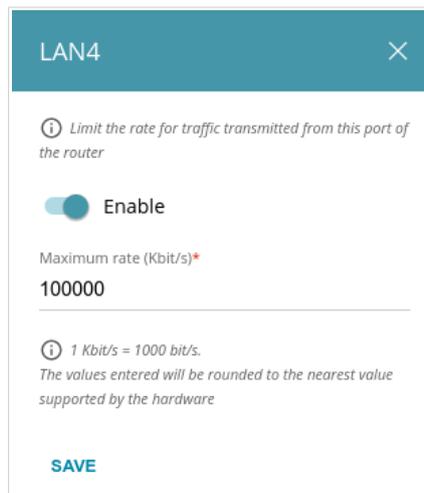
Bandwidth Control

On the **Functions / Advanced / Bandwidth Control** page, you can setup the rate limit for traffic transmitted from every port of the router.
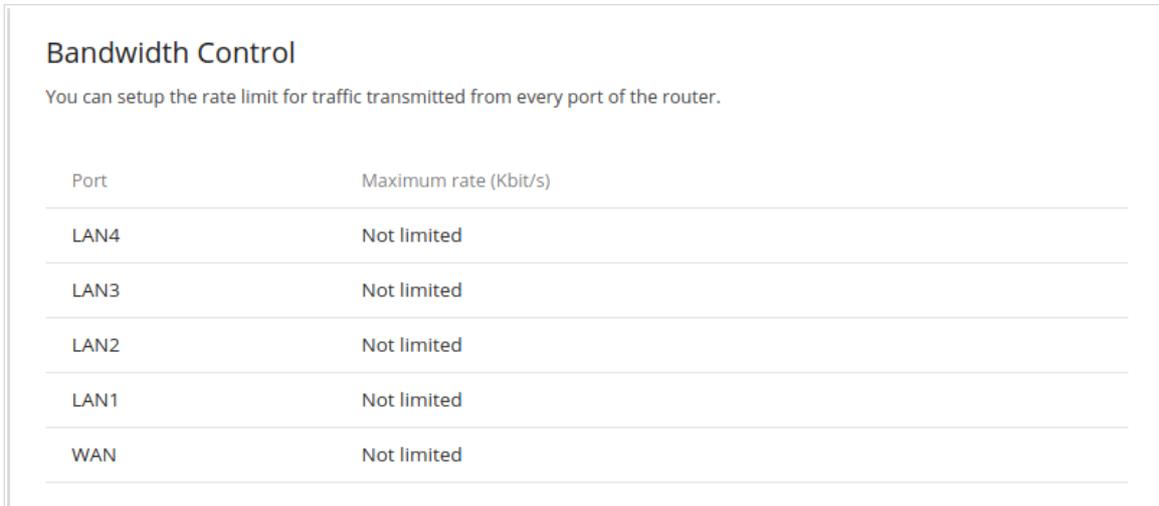
*Figure 117. The **Functions / Advanced / Bandwidth Control** page.*

By default, the rate is not limited. If you want to limit the rate for traffic transmitted from a port, select the line corresponding to this port.

*Figure 118. The window for setting up rate limit.*

In the opened window, move the **Enable** switch to the right and enter the maximum value of the transmitted traffic rate for this port in the **Maximum rate** field. Then click the **SAVE** button.

If you want to remove the rate limit for this port, move the **Enable** switch to the left and click the **SAVE** button.

Ports Settings

On the **Functions / Advanced / Ports Settings** page, you can configure or disable autonegotiation of speed and duplex mode or manually configure speed and duplex mode for each Ethernet port of the router.

Also you can enable or disable data flow control in the autonegotiation mode. This function is used for equal load balancing in ISPs' networks. Contact your ISP to clarify if this function needs to be enabled.

Ports Settings

You can configure or disable autonegotiation of speed and duplex mode or manually configure speed and duplex mode for each Ethernet port of the device. Also you can enable or disable data flow control in the autonegotiation mode.
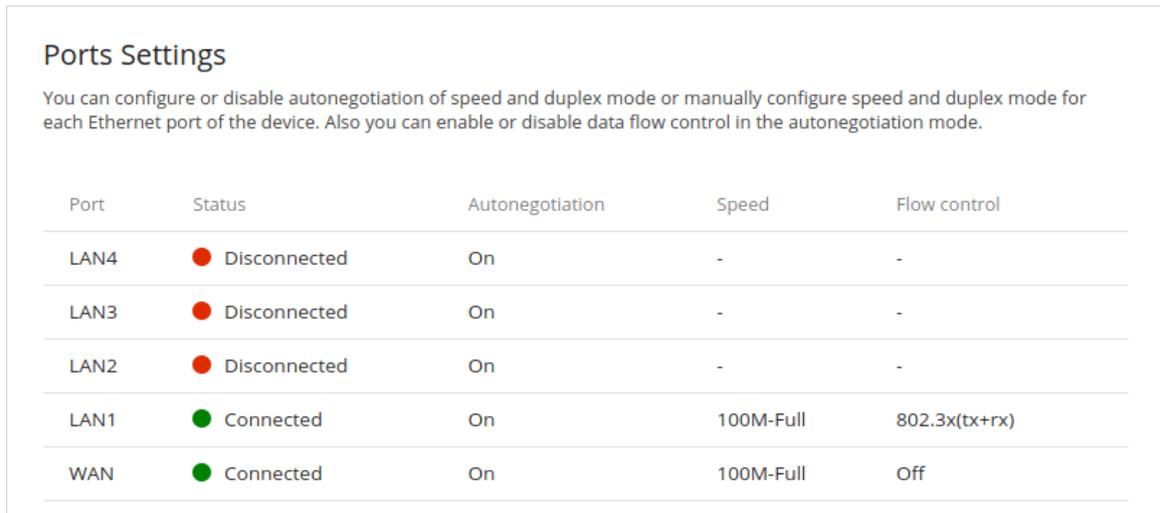
Port	Status	Autonegotiation	Speed	Flow control
LAN4	● Disconnected	On	-	-
LAN3	● Disconnected	On	-	-
LAN2	● Disconnected	On	-	-
LAN1	● Connected	On	100M-Full	802.3x(tx+rx)
WAN	● Connected	On	100M-Full	Off

*Figure 119. The **Functions / Advanced / Ports Settings** page.*

In order to configure autonegotiation or configure speed and duplex mode manually for an Ethernet port, select it in the table.

> ! Autonegotiation should be enabled for both devices connected to each other.

> ! When autonegotiation is disabled, speed and duplex mode settings for both devices connected to each other should be the same.
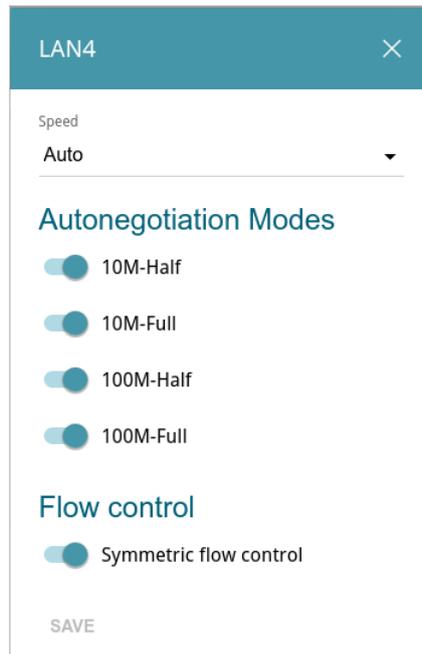
Figure 120. The window for changing the settings of the router's port.

In the opened window, specify the needed parameters:

Parameter	Description
Speed	Data transfer mode. Select the **Auto** value to enable autonegotiation. When this value is selected, the **Autonegotiation Modes** and **Flow control** sections are displayed. Select the **10M-Half**, **10M-Full**, **100M-Half**, or **100M-Full** value to manually configure speed and duplex mode for the selected port: **10M-Half**: Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 10Mbps. **10M-Full:** Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 10Mbps. **100M-Half:** Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 100Mbps. **100M-Full:** Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 100Mbps.

Parameter	Description
Autonegotiation Modes	
To enable the needed data transfer modes, move relevant switches to the right.	
Flow control	
Symmetric flow control	Move the switch to the right to enable the flow control function for the port. Move the switch to the left to disable the flow control function for the port.

After specifying the needed parameters, click the **SAVE** button.

If in the future you need to edit the parameters of the router's port, select the port in the table. In the opened window, change the needed parameters and click the **SAVE** button.

Redirect

On the **Functions / Advanced / Redirect** page, you can enable notifications on the reason of the Internet connection failure. Notifications will be displayed in the browser window when a user is attempting to open a web site on the Internet.
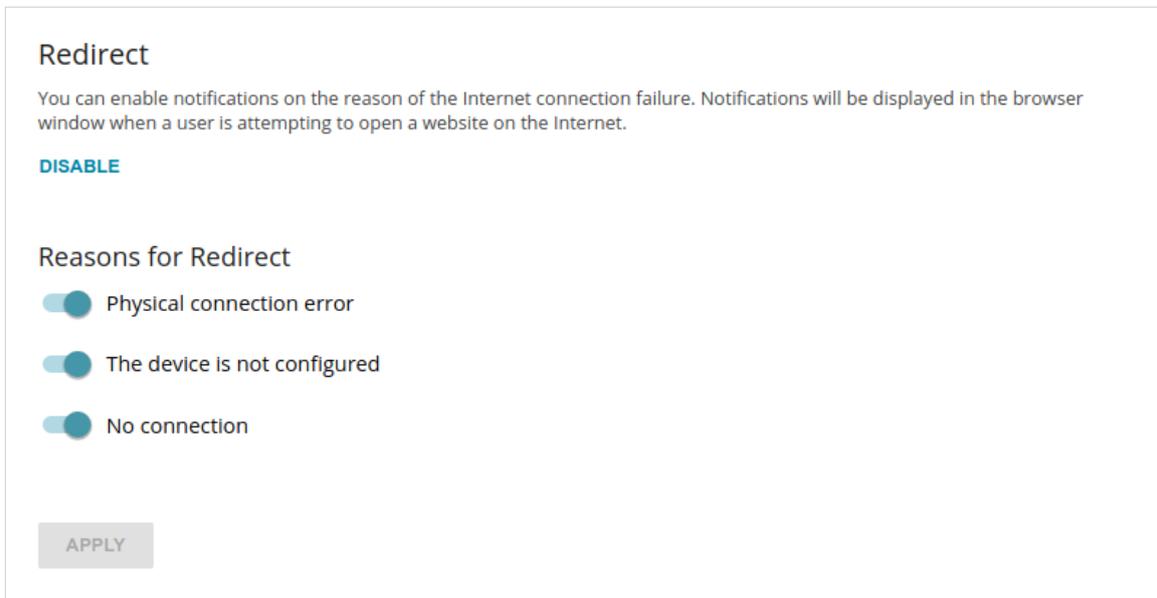

*Figure 121. The **Functions / Advanced / Redirect** page.*

To configure notifications, click the **ENABLE** button. Then, in the **Reasons for Redirect** section, move the needed switches to the right.

Parameter	Description
Reasons for Redirect	
Physical connection error	Notifications in case of physical connection problems (the ISP's cable is not connected, an additional device needed to access the Internet is not connected).
The device is not configured	Notifications in case when the device works with default settings.
No connection	Notifications in case of problems of the default WAN connection (authorization error, the IPS's server does not respond, etc.).

When you have configured the parameters, click the **APPLY** button.

To disable notifications, click the **DISABLE** button.

IGMP

On the **Functions / Advanced / IGMP** page, you can allow the router to use IGMP.

IGMP is used for managing multicast traffic (transferring data to a group of destinations). This protocol allows using network resources for some applications, e.g., for streaming video, more efficiently.

*Figure 122. The **Functions / Advanced / IGMP** page.*

The following elements are available on the page:

Parameter	Description
Enable	Move the switch to the right to enable IGMP.
IGMP version	Select a version of IGMP from the drop-down list.
Interface	From the drop-down list, select a connection of the Dynamic IPv4 or Static IPv4 type for which you need to allow multicast traffic (e.g. streaming video).
Set the address of outgoing IGMP packets equal to 0.0.0.0	Move the switch to the right if you want all outgoing IGMP packets to have the IP address 0.0.0.0.

After specifying the needed parameters, click the **APPLY** button.

ALG/Passthrough

On the **Functions / Advanced / ALG/Passthrough** page, you can allow the router to use RTSP, enable the SIP ALG and PPPoE/PPTP/L2TP/IPsec pass through functions, and assign a higher priority for a specific type of traffic.

Assigning a higher priority for a specific type of traffic allows you to allocate the router's resources for online games or IPTV services, service packet transmission, or management of the router.

SIP is used for creating, modifying, and terminating communication sessions. This protocol allows telephone calls via the Internet.

RTSP is used for real-time streaming multimedia data delivery. This protocol allows some applications to receive streaming audio/video from the Internet.

The PPPoE pass through function allows PPPoE clients of computers from your LAN to connect to the Internet through connections of the router.

The PPTP pass through, L2TP pass through and IPsec pass through functions allow VPN PPTP, L2TP and IPsec traffic to pass through the router so that clients from your LAN can establish relevant connections with remote networks.
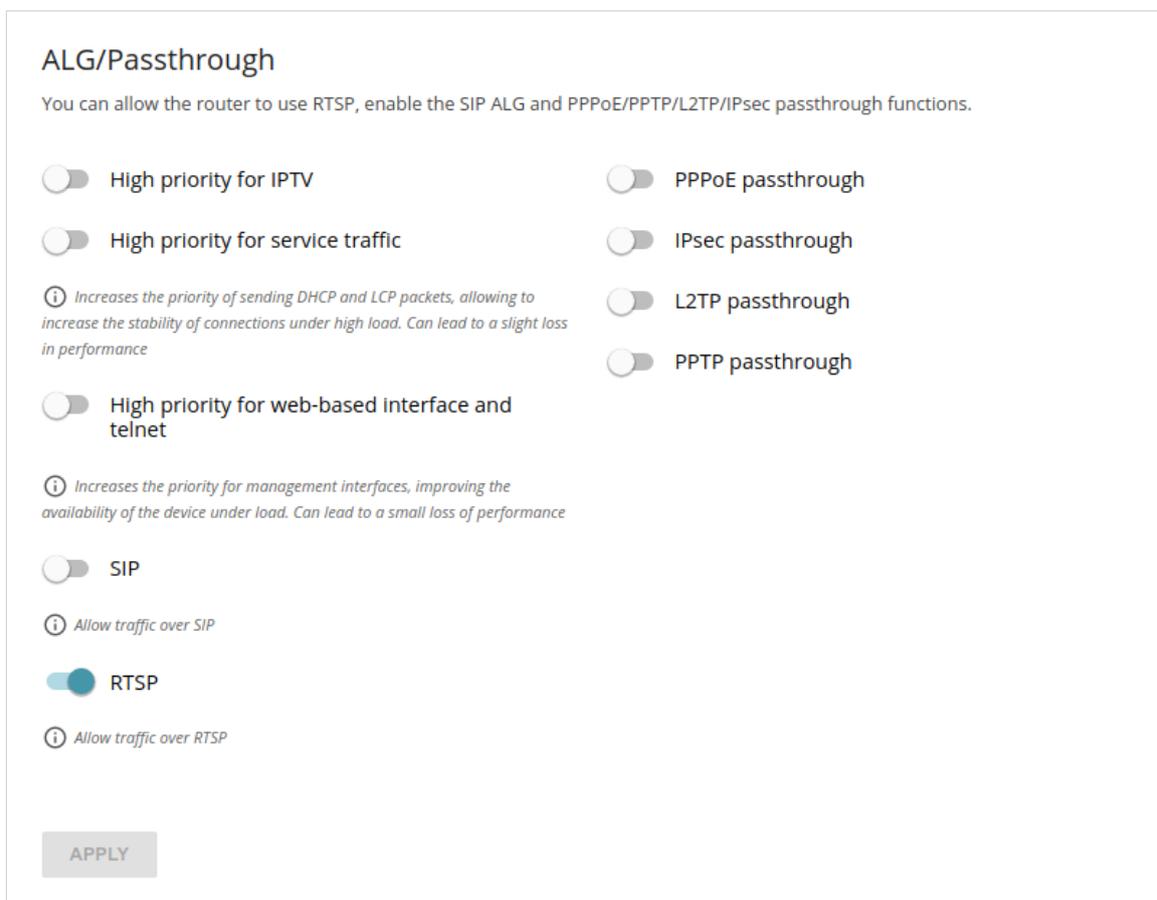

*Figure 123. The **Functions / Advanced / ALG/Passthrough** page.*

The following elements are available on the page:

Parameter	Description
High priority for IPTV	Move the switch to the right to assign a higher priority for IPTV traffic. Move the switch to the left so that online games traffic could have a higher priority.
High priority for service traffic	Move the switch to the right to assign a higher priority for passing LCP and DHCP packets. Such a setting allows keeping a persistent Internet connection at high load. It can lead to a small loss of performance.
High priority for web interface and telnet	Move the switch to the right to assign a higher priority for packets related to Telnet and web-based management of the router at high load. It can lead to a small loss of performance.
SIP	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled router.[3]
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.

After specifying the needed parameters, click the **APPLY** button.

---

3 On the **Settings / Internet / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Functions / Advanced / ALG/Passthrough** page, connect an Ethernet cable between a LAN port of the router and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

Management

System Time

On the **Management / System Time** page, you can manually set the time and date of the router or configure automatic synchronization of the system time with a time server on the Internet.

*Figure 124. The **Management / System Time** page.*

To set the system time manually, follow the next steps:

1. Move the **Enable NTP** switch to the left.

2. In the **Time Settings** section, specify needed values. To specify the time set on your PC or portable device, click the **SET LOCAL TIME** button.

3. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

To enable automatic synchronization with a time server, follow the next steps:

1. Move the **Enable NTP** switch to the right.

2. Specify the needed NTP server or leave the value specified by default in the **NTP Servers** section. If you need to specify several servers, click the **ADD SERVER** button.

3. Select your time zone from the **Main time zone** drop-down list. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.

4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

To enable the router to automatically adjust to daylight saving time, move the **Daylight saving time** switch to the right. From the **Daylight saving time zone** drop-down list, select the time zone that will be used during summer time and specify the needed values in the **Beginning of daylight saving time** and **End of daylight saving time** sections. Click the **APPLY** button.

In some cases NTP servers addresses are provided by your ISP. In this case, you need to move the **Get NTP server addresses using DHCP** switch to the right and click the **APPLY** button. Contact your ISP to clarify if this setting needs to be enabled. If the **Get NTP server addresses using DHCP** switch is moved to the right, the **NTP Servers** section is not displayed.

To allow connected devices to use the IP address of the router in the local subnet as a time server, move the **Run as a server for the local network** switch to the right and click the **APPLY** button.

By default, the system is configured to automatically determine the system time synchronization interval. Upon that the **Specify update period automatically** switch is moved to the right. To configure the synchronization interval of the system time manually, move the **Specify update period automatically** switch to the left, and in the **Update period** field, specify the needed value (in minutes).

> ! When the router is powered off or rebooted, the system time is reset to the default value. If you have set automatic synchronization for the system time, the internal clock of the device will be configured after connecting to the Internet. If you have set the system time manually, you need to set the time and date again (see above).

System Log

On the **Management / System Log** page, you can set the system log options and configure sending the system log to a remote host.

*Figure 125. The **Management / System Log** page. The **Settings** tab.*

To enable logging of the system events, go to the **Settings** tab and move the **Enable** switch to the right. Then specify the needed parameters.

Parameter	Description
Logging	
Type	Select a type of logging from the drop-down list. • **Local**: The system log is stored in the router's memory. When this value is selected, the **Server** and **Port** fields are not displayed. • **Remote**: The system log is sent to the remote host specified in the **Server** field. • **Remote and local**: The system log is stored in the router's memory and sent to the remote host specified in the **Server** field.
Level	Select a type of messages and alerts/notifications to be logged.
Server	The IP or URL address of the host from the local or global network, to which the system log will be sent.
Port	A port of the host specified in the **Server** field. By default, the value `514` is specified.

After specifying the needed parameters, click the **APPLY** button.

To disable logging of the system events, move the **Enable** switch to the left and click the **APPLY** button.
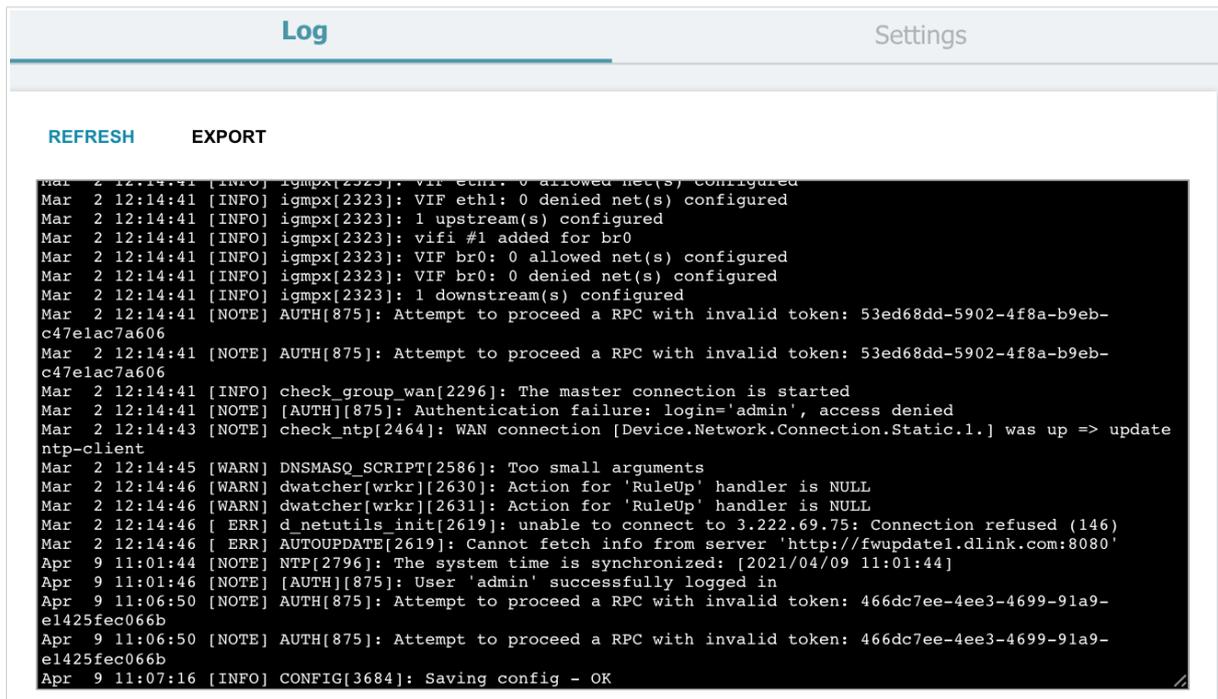
To view the system log, go to the **Log** tab.

Figure 126. The *Management / System Log* page. The *Log* tab.

To view the latest system events, click the **REFRESH** button.

To save the system log to your PC, click the **EXPORT** button. The file will be stored in the download location of your web browser.

Administration

On the **Management / Administration** page, you can change the password for the administrator account used to access the web-based interface of the router and to access the device settings via TELNET, restore the factory defaults, backup the current configuration, restore the router's configuration from a previously created file, save the changed settings to the non-volatile memory, reboot the device, change the web-based interface language, or configure automatic reboot of the device on a schedule.

*Figure 127. The **Management / Administration** page.*

In order to change the password for the administrator account, in the **User** section, enter a new password in the **New password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[4] Click the **Show** icon ( ) to display the entered values. Then click the **SAVE** button.

> ! Remember or write down the new password for the administrator account. In case of losing the new password, you can access the settings of the router only after restoring the factory default settings via the hardware **WPS/RESET** button. This procedure wipes out all settings that you have configured for your router.

To change the web-based interface language, select the needed value from the **Language** drop-down list.

---

4   0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

The following buttons are also available on the page:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware **WPS/RESET** button (see the *Back Panel* section, page 12).
Backup	Click the button to save the configuration (all settings of the router) to your PC. The configuration backup will be stored in the download location of your web browser.
Restore	Click the button and follow the dialog box appeared to select a previously saved configuration file (all settings of the router) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The router saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

In the **Idle time** field specify a period of inactivity (in minutes) after which the router completes the session of the interface. By default, the value **5** is specified. Then click the **SAVE** button.

To configure automatic reboot of the device on a schedule, in the **Automatic Reboot** section, move the **Enable** switch to the right and specify the time period for the device's reboot (in seconds) in the **Period** field. Click the **SAVE** button.

To disable automatic reboot of the device on a schedule, in the **Automatic Reboot** section, move the **Enable** switch to the left and click the **SAVE** button.

Telnet

On the **Management / Telnet** page, you can enable or disable access to the device settings via TELNET from your LAN. Access via TELNET is disabled by default.
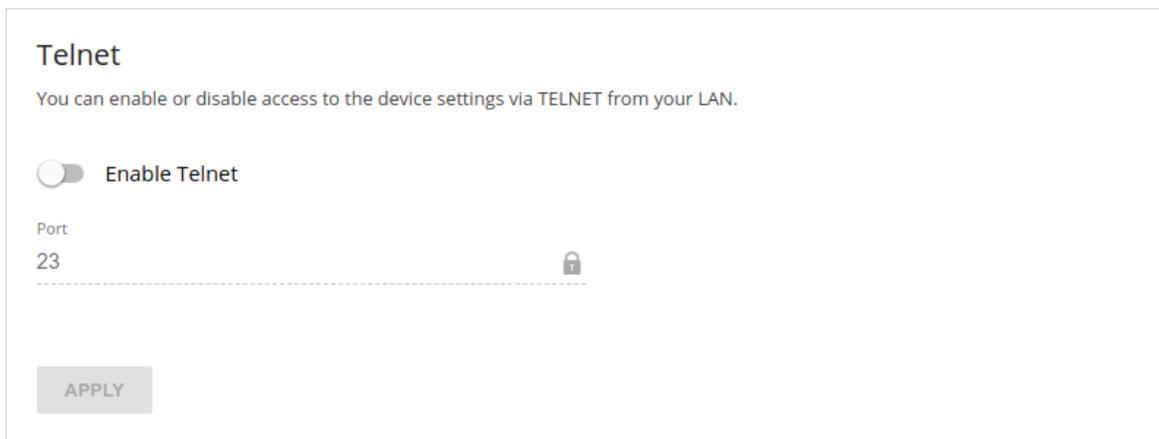

*Figure 128. The **Management / Telnet** page.*

To enable access via TELNET, move the **Enable Telnet** switch to the right. In the **Port** field, enter the number of the router's port through which access will be allowed (by default, the port `23` is specified). Then click the **APPLY** button.

To disable access via TELNET again, move the **Enable Telnet** switch to the left and click the **APPLY** button.
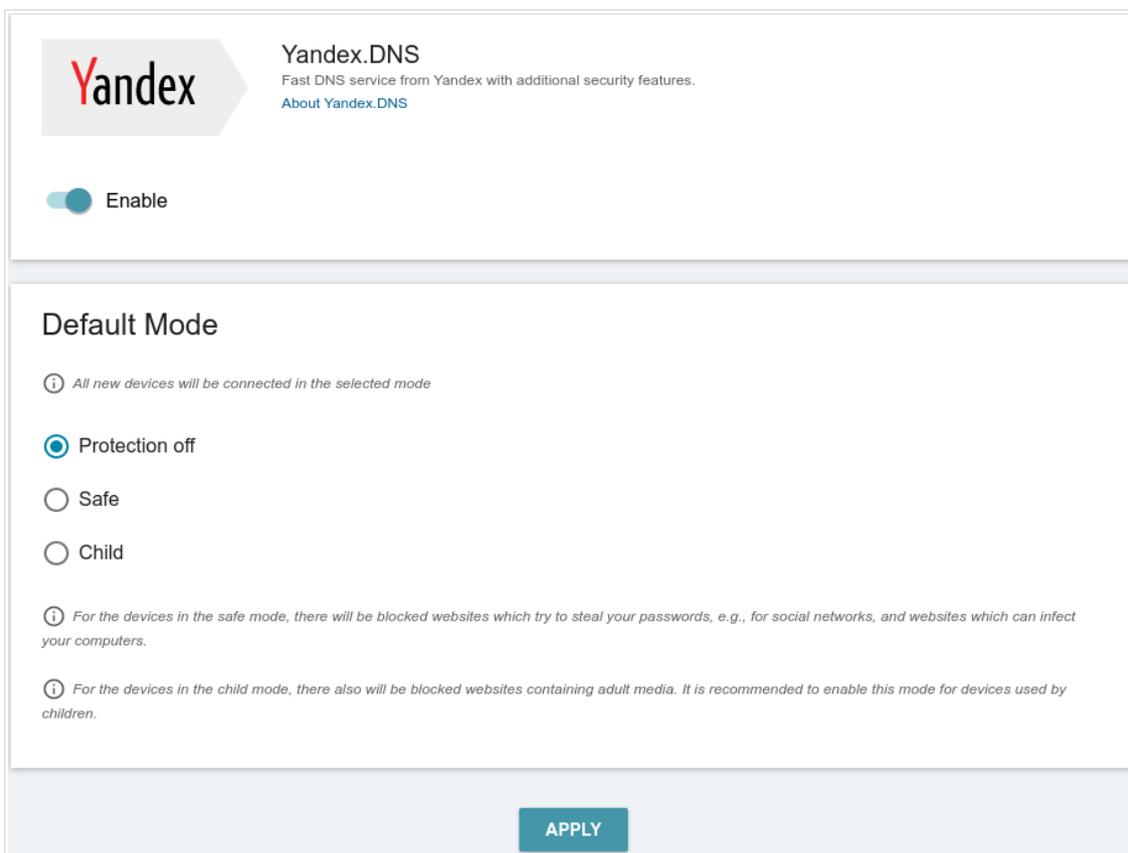
Yandex.DNS

This menu is designed to configure the Yandex.DNS service.

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.

Settings

On the **Management / Yandex.DNS / Settings** page, you can enable the Yandex.DNS service and configure its operating mode.

*Figure 129. The **Management / Yandex.DNS / Settings** page.*

To get detailed information on the service, click the **About Yandex.DNS** link.

To enable the Yandex.DNS service, move the **Enable** switch to the right.

When the service is enabled, the **Default Mode** section is displayed on the page. Select the needed choice of the radio button to configure filtering for all devices of the router's network:

- **Protection off**: When this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites;

- **Safe**: When this value is selected, the service blocks access to malicious and fraudulent web sites;

- **Child**: When this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

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

After specifying all needed parameters, click the **APPLY** button.

To disable the Yandex.DNS service, move the **Enable** switch to the left and click the **APPLY** button.

Devices and Rules

On the **Management / Yandex.DNS / Devices and Rules** page, you can specify a filtering mode for each device separately.
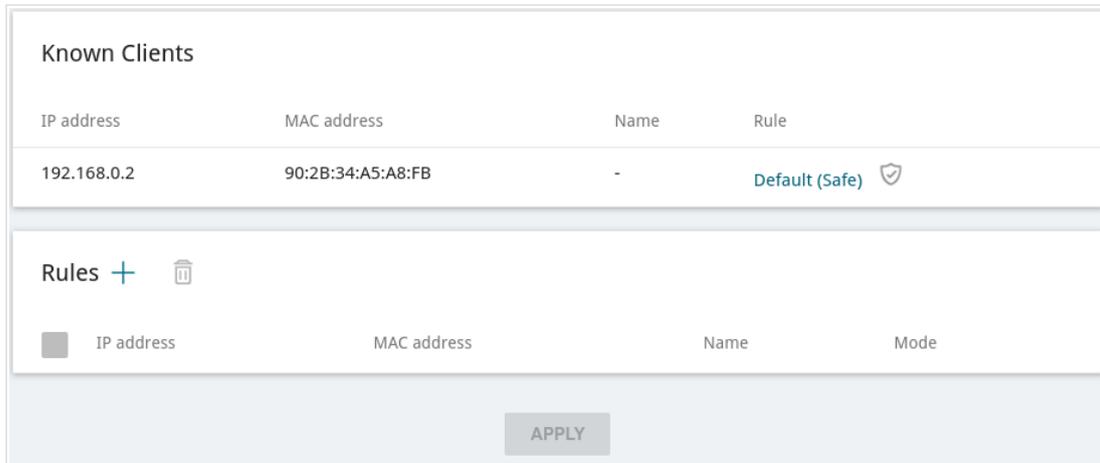

*Figure 130. The **Management / Yandex.DNS / Devices and Rules** page.*

In the **Known Clients** section, the devices connected to the local network of the router at the moment and their relevant filtering mode are displayed.

To create a new filtering rule for a device, click the **ADD** button (+) in the **Rules** section, or left-click the name of the filtering mode in the line of the device for which a rule should be created in the **Known Clients** section.
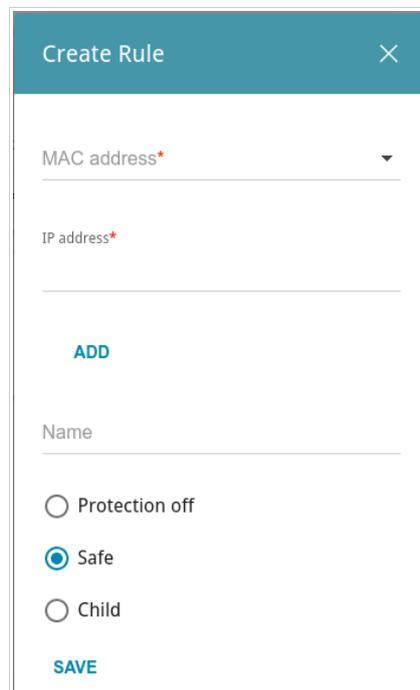

Figure 131. Adding a new rule for the Yandex.DNS service.

In the opened window, you can specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the router's LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
IP address	The IP address of a device from the router's LAN. To assign several fixed IP addresses to a device with a certain MAC address, click the **ADD** button, and in the line displayed, enter an IP address. A device of your LAN can have one IPv4 address and several IPv6 addresses. To remove the IP address, click the **Delete** icon (✕) in the line of the address.
Name	Enter a name for the rule for easier identification. *Optional*.
Mode	Select an operating mode of the Yandex.DNS service for this rule. • **Protection off**: When this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites. • **Safe**: When this value is selected, the service blocks access to malicious and fraudulent web sites. • **Child**: When this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

After specifying the needed parameters, click the **SAVE** button.

To edit a rule for filtering, select a relevant line of the table, in the opened window, change the needed values and click the **SAVE** button.

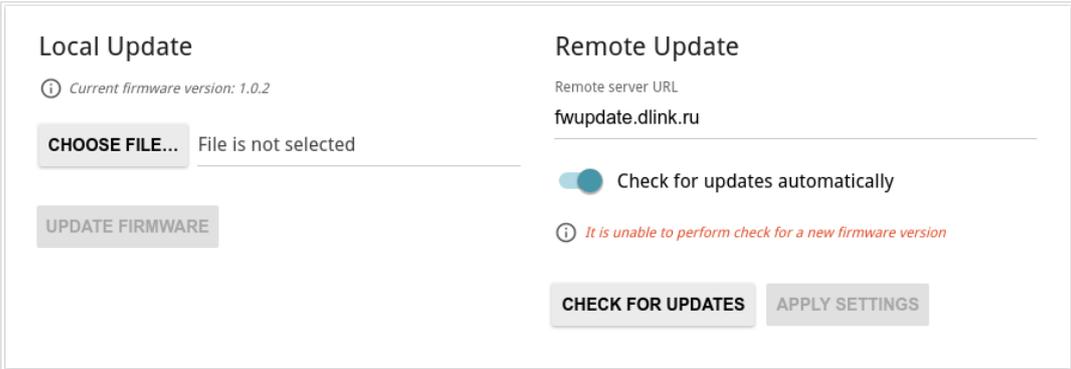To remove a rule for filtering, select the checkbox located to the left of the relevant rule and click the **DELETE** button (🗑). Also you can remove a rule in the editing window.

After completing the work with rules, click the **APPLY** button.

Firmware Update

On the **Management / Firmware Update** page, you can update the firmware of the router and configure the automatic check for updates of the router's firmware.

> **!** <u>Update the firmware only when the router is connected to your PC via a wired connection.</u>

*Figure 132. The **Management / Firmware Update** page.*

The current version of the router's firmware is displayed in the **Current firmware version** field.

By default, the automatic check for the router's firmware updates is enabled. If the **Access point**, **Repeater**, or **Client** mode was selected in the Setup Wizard, and the **Static** value is selected from the **Mode of local IP address assignment** list on the **Settings / Network** page, the **Gateway IP address** field should also be filled in on order to realize automatic check.

If a firmware update is available, a notification will be displayed in the top right corner of the page.

To disable the automatic check for firmware updates, in the **Remote Update** section, move the **Check for updates automatically** switch to the left and click the **APPLY SETTINGS** button.

To enable the automatic check for firmware updates, in the **Remote Update** section, move the **Check for updates automatically** switch to the right and click the **APPLY SETTINGS** button.

You can update the firmware of the router locally (from the hard drive of your PC) or remotely (from the update server).

Local Update

! Attention! Do not turn off the router before the firmware update is completed. This may cause the device breakdown.

To update the firmware of the router locally, follow the next steps:

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **CHOOSE FILE** button in the **Local Update** section on the **Management / Firmware Update** page to locate the new firmware file.
3. Click the **UPDATE FIRMWARE** button.
4. Wait until the router is rebooted (about one and a half or two minutes).
5. Log into the web-based interface using the login (`admin`) and the current password.

If after updating the firmware the router doesn't work correctly, please restore the factory default settings. To do this, click the **Factory** button on the **Management / Administration** page. Wait until the router is rebooted.

Remote Update

> **!** Attention! Do not turn off the router before the firmware update is completed. This may cause the device breakdown.

To update the firmware of the router remotely, follow the next steps:

1. On the **Management / Firmware Update** page, in the **Remote Update** section, click the **CHECK FOR UPDATES** button to check if a newer firmware version exists.

2. Click the **UPDATE FIRMWARE** button (the button is displayed if a newer version of the firmware is available).

3. Wait until the router is rebooted (about one and a half or two minutes).

4. Log into the web-based interface using the login (`admin`) and the current password.

If after updating the firmware the router doesn't work correctly, please restore the factory default settings. To do this, click the **Factory** button on the **Management / Administration** page. Wait until the router is rebooted.

Statistics

The pages of this section display data on the current state of the router.

Network Statistics

On the **Management / Statistics / Network Statistics** page, you can view statistics for all connections existing in the system (WAN connections, LAN, WLAN). For each connection the following data are displayed: name and state (when the connection is on, its name is highlighted in green, when the connection is off, its name is highlighted in red), IP address and subnet mask, and volume of data received and transmitted (with increase of the volume the units of measurement are changed automatically: byte, Kbyte, Mbyte, Gbyte).
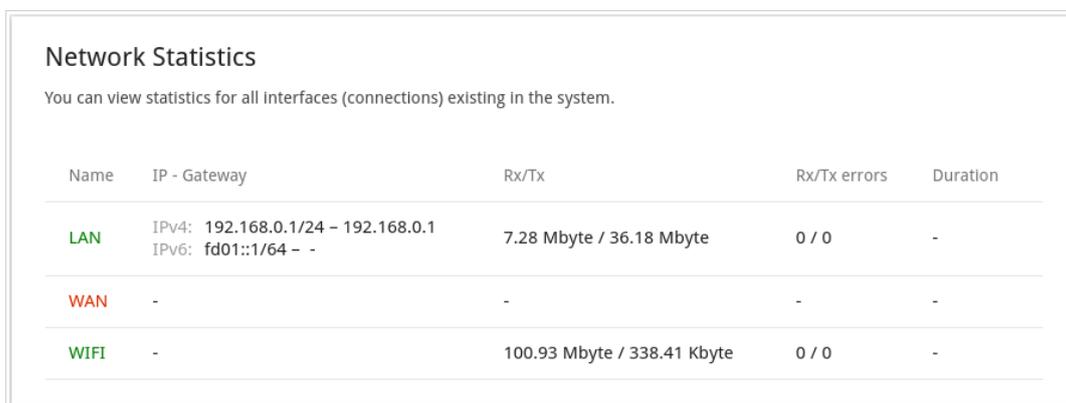
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 – 192.168.0.1 IPv6: fd01::1/64 – -	7.28 Mbyte / 36.18 Mbyte	0 / 0	-
WAN	-	-	-	-
WIFI	-	100.93 Mbyte / 338.41 Kbyte	0 / 0	-

*Figure 133. The **Management / Statistics / Network Statistics** page.*

To view detailed data on a connection, click the line corresponding to this connection.

Port Statistics

On the **Management / Statistics / Port Statistics** page, you can view statistics for traffic passing through ports of the router. The information shown on the page can be used for diagnosing connection problems.

*Figure 134. The **Management / Statistics / Port Statistics** page.*

To view the full list of counters for a port, click the line corresponding to this port.

Routing Table

The **Management / Statistics / Routing Table** page displays the information on routes. The table contains destination IP addresses, gateways, subnet masks, and other data.

Interface	Destination	Subnet mask	Gateway	Flags	Metric
LAN	224.0.0.252	255.255.255.255	0.0.0.0	UH	0
LAN	239.255.255.250	255.255.255.255	0.0.0.0	UH	0
LAN	224.0.0.251	255.255.255.255	0.0.0.0	UH	0
statip_13	192.168.161.0	255.255.255.0	0.0.0.0	U	0
LAN	192.168.0.0	255.255.255.0	0.0.0.0	U	0
statip_13	0.0.0.0	0.0.0.0	192.168.161.1	UG	100
LAN	fd01::/64		::	U	256
LAN	fd00::/8		::	U	256
LAN	fe80::28f4:4ff:fe81:c3d9/128		fe80::28f4:4ff:fe81:c3d9	U	0

*Figure 135. The **Management / Statistics / Routing Table** page.*

DHCP

The **Management / Statistics / DHCP** page displays the information on computers that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the device.

*Figure 136. The **Management / Statistics / DHCP** page.*

Clients and Sessions

On the **Management / Statistics / Clients and Sessions** page, you can view the list of devices connected to the local network of the router and information on current sessions of each device.

*Figure 137. The **Management / Statistics / Clients and Sessions** page.*

For each device the following data are displayed: the IP address, the MAC address, and the network interface to which the device is connected.

To view the information on current sessions of a device, select this device in the table. On the opened page, the following data for each session of the selected device will be displayed: the protocol for network packet transmission, the source IP address and port, and the destination IP address and port.

Multicast Groups

The **Management / Statistics / Multicast Groups** page displays addresses of active multicast groups (including IPTV channels and groups for transferring service information) to which the device is subscribed, and the interface through which the device is subscribed.

*Figure 138. The **Management / Statistics / Multicast Groups** page.*

Diagnostics

Ping

On the **Management / Diagnostics / Ping** page, you can check availability of a host from the local or global network via the Ping utility.

The Ping utility sends echo requests to a specified host and receives echo replies.

*Figure 139. The **Management / Diagnostics / Ping** page.*

To check availability of a host, enter the IP address or name of this host in the **Host** field and specify a number of requests that will be sent in order to check its availability in the **Number of attempts** field. If availability check should be performed with IPv6, move the **IPv6** switch to the right.

To specify additional settings, click the **MORE SETTINGS** button.
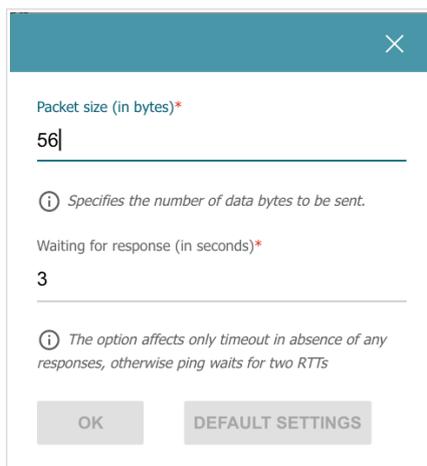
*Figure 140. The **Management / Diagnostics / Ping** page. The additional settings window.*

In the opened window, in the **Packet size** field, specify the volume of data sent in a request. In the **Waiting for response** field, specify the response waiting period in seconds. To restore the default field values, click the **DEFAULT SETTINGS** button.

After specifying the additional parameters, click the **OK** button.

To run the check, click the **START** button. After a while, the results will be displayed on the page.

To remove the check result from the page, click the **CLEAR** button.

Traceroute

On the **Management / Diagnostics / Traceroute** page, you can determine the route of data transfer to a host via the traceroute utility.
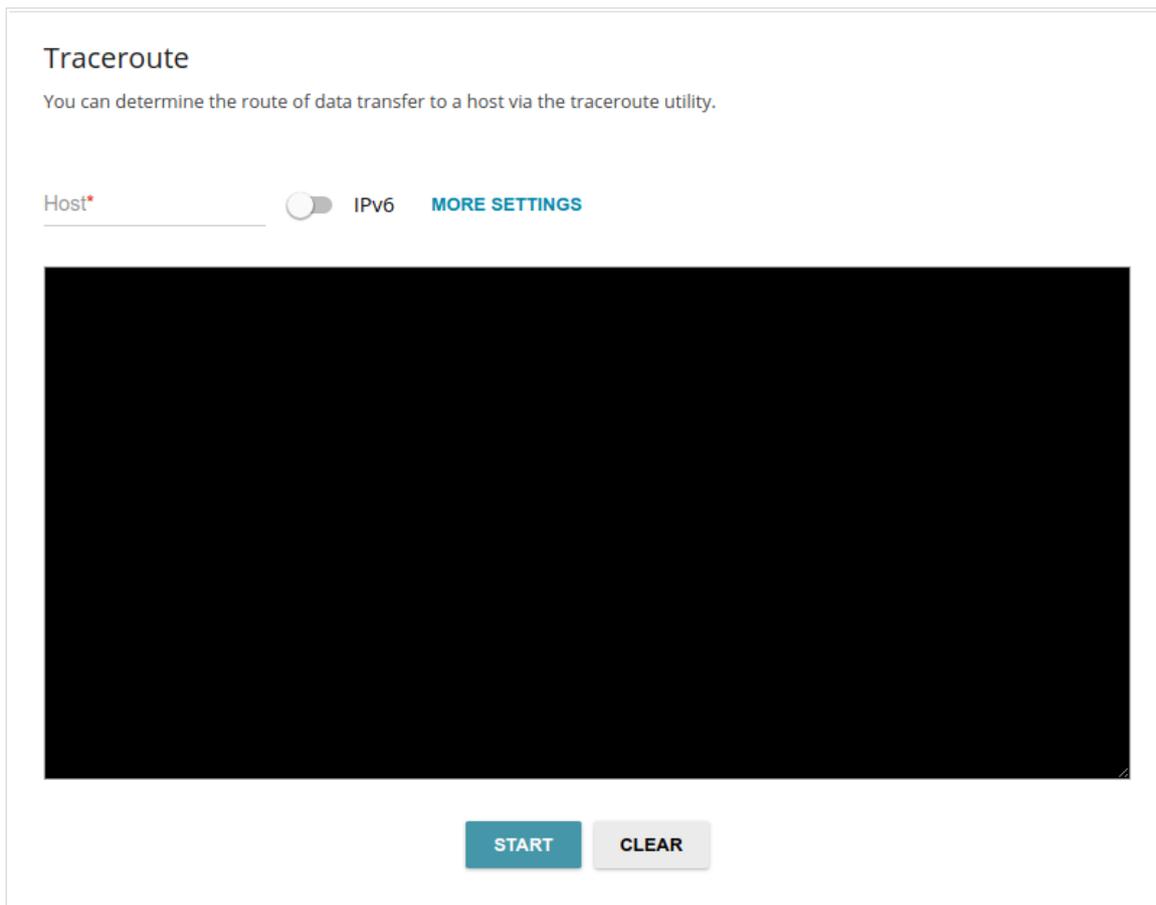
*Figure 141. The **Management / Diagnostics / Traceroute** page.*

To determine the route, enter the name or IP address of a host in the **Host** field. If the route should be determined using IPv6, move the **IPv6** switch to the right.

To specify additional settings, click the **MORE SETTINGS** button.

*Figure 142. The **Management / Diagnostics / Traceroute** page. The additional settings window.*

In the opened window, you can specify the following parameters:

Parameter	Description
Maximum TTL value	Specify the TTL (*Time to live*) parameter value. The default value is `30`.
Number of attempts	The number of attempts to hit an intermediate host.
Wait time	A period of waiting for an intermediate host response.

To restore the default field values, click the **DEFAULT SETTINGS** button.

After specifying the additional parameters, click the **OK** button.

To run the check, click the **START** button. After a while, the results will be displayed on the page.

To remove the check result from the page, click the **CLEAR** button.

CHAPTER 5. OPERATION GUIDELINES

Safety Rules and Conditions

Please carefully read this section before installation and connection of the device. Make sure that the power adapter and cables are not damaged. The device should be used only as intended in accordance with the documents.

The device is intended for use in dry, clean, dust-free, and well ventilated areas with normal humidity away from strong heat sources. Do not use the device outdoors or in the areas with high humidity. Do not place foreign objects on the device. Do not obstruct the ventilation openings of the device. The environmental temperature near the device and the temperature inside the device's cover should be within the range from 0 °C to +40 °C.

Only use the power adapter supplied with the device. Do not plug in the adapter, if its case or cable are damaged. Plug the adapter only into working electrical outlets with parameters indicated on the adapter.

Do not open the cover of the device! Unplug the device before dusting and cleaning. Use a damp cloth to clean the device. Do not use liquid/aerosol cleaners or magnetic/static cleaning devices. Prevent moisture getting into the device or the power adapter.

The service life of the device is 2 years.

Wireless Installation Considerations

The DIR-615 device lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, 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 noise in your home or office. To maximize your wireless range, follow the guidelines below.

1. Keep the number of walls and ceilings between the DIR-615 device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).

2. Be aware of the direct line between network devices. Place your devices so that the signal travels 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 your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls 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 router 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 equipment (wireless devices 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. Note, that the base transmits a signal even if the phone in not in use.

CHAPTER 6.   ABBREVIATIONS AND ACRONYMS

3G	Third Generation
AC	Access Category
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BPSK	Binary Phase-shift Keying
BSSID	Basic Service Set Identifier
CCK	Complementary Code Keying
DBSK	Differential Binary Phase-shift Keying
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DPD	Dead Peer Detection
DQPSK	Differential Quadrature Phase-shift Keying
DSL	Digital Subscriber Line
DSSS	Direct-sequence Spread Spectrum
DTIM	Delivery Traffic Indication Message
GMT	Greenwich Mean Time
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ID	Identifier
IGD	Internet Gateway Device

IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPTV	Internet Protocol Television
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light-emitting diode
LTE	Long Term Evolution
MAC	Media Access Control
MBSSID	Multiple Basic Service Set Identifier
MIB	Management Information Base
MIMO	Multiple Input Multiple Output
MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Controller
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PBC	Push Button Configuration
PFS	Perfect Forward Secrecy
PIN	Personal Identification Number
PoE	Power over Ethernet

PPP	Point-to-Point Protocol
pppd	Point-to-Point Protocol Daemon
PPPoE	Point-to-point protocol over Ethernet
PPTP	Point-to-point tunneling protocol
PSK	Pre-shared key
PUK	PIN Unlock Key
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-shift Keying
RADIUS	Remote Authentication in Dial-In User Service
RIP	Routing Information Protocol
RIPng	Next Generation Routing Information Protocol
RTS	Request To Send
RTSP	Real Time Streaming Protocol
SA	Security Association
SAE	Simultaneous Authentication of Equals
SIM	Subscriber Identification Module
SIP	Session Initiation Protocol
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
STBC	Space-time block coding
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator

USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup