



## **DIR-822**

### **AC1200 Wave 2 MU-MIMO Wi-Fi EasyMesh Router**

## Contents

<b>Chapter 1. Introduction</b>	<b>5</b>
<b>Contents and Audience</b>	<b>5</b>
<b>Conventions</b>	<b>5</b>
<b>Document Structure</b>	<b>5</b>
<b>Chapter 2. Overview</b>	<b>6</b>
<b>General Information</b>	<b>6</b>
<b>Specifications</b>	<b>8</b>
<b>Product Appearance</b>	<b>14</b>
Upper Panel	14
Back and Bottom Panels	16
<b>Delivery Package</b>	<b>18</b>
<b>Chapter 3. Installation and Connection</b>	<b>19</b>
<b>Before You Begin</b>	<b>19</b>
<b>Connecting to PC</b>	<b>20</b>
PC with Ethernet Adapter	20
Obtaining IP Address Automatically (OS Windows 7)	21
Obtaining IP Address Automatically (OS Windows 10)	26
PC with Wi-Fi Adapter	30
Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 7)	31
Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 10)	34
<b>Connecting to Web-based Interface</b>	<b>37</b>
<b>Web-based Interface Structure</b>	<b>39</b>
Summary Page	39
Home Page	41
Menu Sections	42
Notifications	43
<b>Chapter 4. Configuring via Web-based Interface</b>	<b>44</b>
<b>Initial Configuration Wizard</b>	<b>44</b>
Selecting Operation Mode	46
Router	46
Access Point or Repeater	47
Mesh Network Main Device (Controller)	49
Mesh Network Subordinate Device (Agent)	51
Changing LAN IPv4 Address	52
Wi-Fi Client	53
Configuring WAN Connection	55
Static IPv4 Connection	56
Static IPv6 Connection	57
PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections	58
PPPoE + Static IP (PPPoE Dual Access) Connection	59
PPTP + Dynamic IP or L2TP + Dynamic IP Connection	60
PPTP + Static IP or L2TP + Static IP Connection	61
Configuring Wireless Network	62
Configuring LAN Ports for IPTV/VoIP	64
Changing Web-based Interface Password	66
<b>Connection of Multimedia Devices</b>	<b>68</b>

<b>Statistics</b> .....	<b>71</b>
Network Statistics.....	71
DHCP.....	72
Routing.....	73
Clients and Sessions.....	75
Port Statistics.....	76
Multicast Groups.....	77
IPsec Statistics.....	78
<b>Connections Setup</b> .....	<b>79</b>
WAN.....	79
<i>Creating Dynamic IPv4 or Static IPv4 WAN Connection</i> .....	81
<i>Creating Dynamic IPv6 or Static IPv6 WAN Connection</i> .....	84
<i>Creating PPPoE WAN Connection</i> .....	87
<i>Creating PPTP, L2TP, or L2TP over IPsec WAN Connection</i> .....	92
<i>Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection</i> .....	97
LAN.....	103
IPv4.....	103
IPv6.....	108
WAN Failover.....	111
<b>Wi-Fi</b> .....	<b>114</b>
Basic Settings.....	114
Client Management.....	125
WPS.....	126
<i>Using WPS Function via Web-based Interface</i> .....	128
<i>Using WPS Function without Web-based Interface</i> .....	129
WMM.....	130
Client.....	133
Client Shaping.....	135
Additional.....	137
MAC Filter.....	141
EasyMesh.....	144
<i>Connecting Subordinate Devices with Ethernet Cable</i> .....	145
<i>Connecting Subordinate Devices with Hardware Button</i> .....	145
<i>Connecting Subordinate Devices via Web-based Interface</i> .....	146
<b>Advanced</b> .....	<b>147</b>
VLAN.....	148
DNS.....	151
DDNS.....	153
Ports Settings.....	155
Redirect.....	158
Routing.....	159
TR-069 Client.....	161
UPnP IGD.....	163
UDPXY.....	164
IGMP/MLD.....	166
ALG/Passthrough.....	168
IPsec.....	170

<b>Firewall</b> .....	<b>178</b>
IP Filter.....	178
Virtual Servers.....	183
DMZ.....	187
MAC Filter.....	189
URL Filter.....	191
AdBlock.....	194
Remote Access.....	195
<b>System</b> .....	<b>197</b>
Configuration.....	198
Firmware Update.....	200
<i>Local Update</i> .....	202
<i>Remote Update</i> .....	203
Schedule.....	204
Log.....	208
Ping.....	211
Traceroute.....	213
Telnet/SSH.....	215
System Time.....	216
Auto Provision.....	219
<b>Yandex.DNS</b> .....	<b>221</b>
Settings.....	221
Devices and Rules.....	223
<b>SkyDNS</b> .....	<b>225</b>
Settings.....	226
Devices and Rules.....	228
<b>Chapter 5. Operation Guidelines</b> .....	<b>230</b>
<b>Safety Rules and Conditions</b> .....	<b>230</b>
<b>Wireless Installation Considerations</b> .....	<b>231</b>
<b>Chapter 6. Abbreviations and Acronyms</b> .....	<b>232</b>

# CHAPTER 1. INTRODUCTION

## Contents and Audience

This manual describes the router DIR-822 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.
<i>Before You Begin</i>	A reference to a chapter or section of this manual.
<i>“Quick Installation Guide”</i>	A reference to a document.
<b>Change</b>	A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.).
<b>192.168.0.1</b>	Data that you should enter in the specified field.
 <u>Information</u>	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-822 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-822 device is a wireless dual band 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-822 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-822 device, you are able to quickly create a high-speed 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). Simultaneous activity of 2.4GHz band and 5GHz band allows performing a wide range of tasks. The router can operate as a base station for connecting wireless devices of the standards 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac (at the wireless connection rate up to 1167Mbps<sup>1</sup>).

The router supports multiple functions for the wireless interface: several security standards (WEP, WPA/WPA2/WPA3), MAC address filtering, WPS, WMM.

In addition, the device is equipped with a button for switching the Wi-Fi network off/on. If needed, for example, when you leave home, you can easily switch the router's WLAN by pressing the button, and devices connected to the LAN ports of the router will stay online.

The EasyMesh function is D-Link implementation of mesh networks designed to quickly connect several<sup>2</sup> devices into one transport network, for example, when it's required to provide high-quality Wi-Fi coverage without dead zones in living units of complicated planning or it's needed to create a large temporary Wi-Fi network for an outdoor event.

Multi-user MIMO technology allows to distribute the router's resources to let multiple wireless clients use the Wi-Fi network efficiently, keeping high rates for HD media streaming, lag-free gaming, and fast transfer of large files.

Transmit Beamforming technology allows to flexibly change the antennas' radiation pattern and to redistribute the signal directly to wireless devices connected to the router.

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 wireless router DIR-822 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.

The SSH protocol support provides more secure remote configuration and management of the router due to encryption of all transmitted traffic, including passwords.

In addition, the router supports IPsec and allows to create secure VPN tunnels. Support of the IKEv2 protocol allows to provide simplified message exchange and use asymmetric authentication engine upon configuration of an IPsec tunnel.

<sup>1</sup> Up to 300Mbps for 2.4GHz and up to 867Mbps for 5GHz.

<sup>2</sup> Up to 6 devices.

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

The router also supports the SkyDNS web content filtering service, which provides more settings and opportunities for safer Internet experience for home users of all ages and for professional activities of corporate users.

Now the schedules are also implemented; they can be applied to the rules and settings of the firewall and used to reboot the router at the specified time or every specified time period and to enable/disable the wireless network and the Wi-Fi filter.

The new ad blocking function effectively blocks advertisements which appear during web surfing.

You can configure the settings of the wireless router DIR-822 via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

The configuration wizard allows you to quickly switch DIR-822 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-822 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	
<b>Processor</b>	<ul style="list-style-type: none"> <li>· RTL8197FH-VG5 (1GHz)</li> </ul>
<b>RAM</b>	<ul style="list-style-type: none"> <li>· 128MB, DDR2, built in processor</li> </ul>
<b>Flash</b>	<ul style="list-style-type: none"> <li>· 128MB, SPI NAND</li> </ul>
<b>Interfaces</b>	<ul style="list-style-type: none"> <li>· 10/100BASE-TX WAN port</li> <li>· 4 10/100BASE-TX LAN ports</li> </ul>
<b>LEDs</b>	<ul style="list-style-type: none"> <li>· Power</li> <li>· Internet</li> <li>· 4 LAN LEDs</li> <li>· WLAN 2.4G</li> <li>· WLAN 5G</li> <li>· WPS</li> </ul>
<b>Buttons</b>	<ul style="list-style-type: none"> <li>· POWER button to power on/power off</li> <li>· WIFI button to enable/disable wireless network</li> <li>· WPS button to connect mesh network devices and set up wireless connection</li> <li>· RESET button to restore factory default settings</li> </ul>
<b>Antenna</b>	<ul style="list-style-type: none"> <li>· Four external non-detachable antennas (5dBi gain)</li> </ul>
<b>MIMO</b>	<ul style="list-style-type: none"> <li>· 2 x 2, MU-MIMO</li> </ul>
<b>Power connector</b>	<ul style="list-style-type: none"> <li>· Power input connector (DC)</li> </ul>

Software	
<b>WAN connection types</b>	<ul style="list-style-type: none"> <li>· PPPoE</li> <li>· IPv6 PPPoE</li> <li>· PPPoE Dual Stack</li> <li>· Static IPv4 / Dynamic IPv4</li> <li>· Static IPv6 / Dynamic IPv6</li> <li>· PPPoE + Static IP (PPPoE Dual Access)</li> <li>· PPPoE + Dynamic IP (PPPoE Dual Access)</li> <li>· PPTP/L2TP + Static IP</li> <li>· PPTP/L2TP + Dynamic IP</li> </ul>

\* The device features are subject to change without notice. For the latest versions of the firmware and relevant documentation, visit [www.dlink.ru](http://www.dlink.ru).

<b>Software</b>	
<b>Network functions</b>	<ul style="list-style-type: none"> <li>· DHCP server/relay</li> <li>· Advanced configuration of built-in DHCP server</li> <li>· Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation</li> <li>· Automatic obtainment of LAN IP address (for access point/repeater/client modes)</li> <li>· DNS relay</li> <li>· Dynamic DNS</li> <li>· Static IPv4/IPv6 routing</li> <li>· IGMP/MLD Proxy</li> <li>· RIP</li> <li>· Support of UPnP IGD</li> <li>· Support of VLAN</li> <li>· WAN ping respond</li> <li>· Support of SIP ALG</li> <li>· Support of RTSP</li> <li>· WAN failover</li> <li>· Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port</li> <li>· Built-in UDPXY application</li> </ul>
<b>Firewall functions</b>	<ul style="list-style-type: none"> <li>· Network Address Translation (NAT)</li> <li>· Stateful Packet Inspection (SPI)</li> <li>· IPv4/IPv6 filter</li> <li>· MAC filter</li> <li>· URL filter</li> <li>· Ad blocking function</li> <li>· DMZ</li> <li>· Virtual servers</li> <li>· Built-in Yandex.DNS web content filtering service</li> <li>· Built-in SkyDNS web content filtering service</li> </ul>
<b>VPN</b>	<ul style="list-style-type: none"> <li>· IPsec/PPTP/L2TP/PPPoE pass-through</li> <li>· PPTP/L2TP tunnels</li> <li>· L2TP over IPsec</li> <li>· IPsec tunnels Transport/Tunnel mode IKEv1/IKEv2 support DES encryption NAT Traversal Support of DPD (Keep-alive for VPN tunnels)</li> </ul>
<b>Management and monitoring</b>	<ul style="list-style-type: none"> <li>· Local and remote access to settings through SSH/TELNET/WEB (HTTP/HTTPS)</li> <li>· Bilingual web-based interface for configuration and management (Russian/English)</li> <li>· Support of D-Link Assistant application for Android and iPhone smartphones</li> <li>· Notification on connection problems and auto redirect to settings</li> <li>· Firmware update via web-based interface</li> <li>· Automatic notification on new firmware version</li> <li>· Saving/restoring configuration to/from file</li> <li>· Support of logging to remote host</li> <li>· Automatic synchronization of system time with NTP server and manual time/date setup</li> <li>· Ping utility</li> <li>· Traceroute utility</li> <li>· TR-069 client</li> <li>· Schedules for rules and settings of firewall, automatic reboot, and enabling/disabling wireless network and Wi-Fi filter</li> <li>· Automatic upload of configuration file from ISP's server (Auto Provision)</li> </ul>

<b>Wireless Module Parameters</b>	
<b>Standards</b>	<ul style="list-style-type: none"> <li>· IEEE 802.11ac Wave 2</li> <li>· IEEE 802.11a/b/g/n</li> <li>· IEEE 802.11k/v</li> <li>· IEEE 802.11w</li> </ul>
<b>Frequency range</b>  <i>The frequency range depends upon the radio frequency regulations applied in your country</i>	<ul style="list-style-type: none"> <li>· 2400 ~ 2483.5MHz</li> <li>· 5150 ~ 5350MHz</li> <li>· 5650 ~ 5850MHz</li> </ul>
<b>Wireless connection security</b>	<ul style="list-style-type: none"> <li>· WEP</li> <li>· WPA/WPA2 (Personal/Enterprise)</li> <li>· WPA3 (Personal)</li> <li>· MAC filter</li> <li>· WPS (PBC/PIN)</li> </ul>
<b>Advanced functions</b>	<ul style="list-style-type: none"> <li>· EasyMesh function</li> <li>· Support of client mode</li> <li>· WMM (Wi-Fi QoS)</li> <li>· Information on connected Wi-Fi clients</li> <li>· Advanced settings</li> <li>· Guest Wi-Fi / support of MBSSID</li> <li>· Rate limitation for wireless network/separate MAC addresses</li> <li>· Periodic scan of channels, automatic switch to least loaded channel</li> <li>· Support of 5GHz TX Beamforming</li> <li>· Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence)</li> <li>· Support of STBC</li> </ul>
<b>Wireless connection rate</b>	<ul style="list-style-type: none"> <li>· IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54Mbps</li> <li>· IEEE 802.11b: 1, 2, 5.5, and 11Mbps</li> <li>· IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps</li> <li>· IEEE 802.11n (2.4GHz): from 6.5 to 300Mbps (MCS0–MCS15)</li> <li>· IEEE 802.11n (5GHz): from 6.5 to 300Mbps (from MCS0 to MCS15)</li> <li>· IEEE 802.11ac (5GHz): from 6.5 to 867Mbps (from MCS0 to MCS9)</li> </ul>

## Wireless Module Parameters

### Transmitter output power

*The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country*

- 802.11a (typical at room temperature 25 °C)  
14dBm at 6, 9, 12, 18, 24Mbps  
13dBm at 36Mbps  
12.5dBm at 48Mbps  
12dBm at 54Mbps
- 802.11b (typical at room temperature 25 °C)  
15dBm at 1, 2, 5.5, 11Mbps
- 802.11g (typical at room temperature 25 °C)  
15dBm at 6, 9, 12, 18, 24, 36, 48, 54Mbps
- 802.11n (typical at room temperature 25 °C)  
2.4GHz, HT20  
15dBm at MCS0~7  
2.4GHz, HT40  
15dBm at MCS0~7  
5GHz, HT20  
14dBm at MCS0~4  
13dBm at MCS5  
12.5dBm at MCS6  
12dBm at MCS7  
5GHz, HT40  
14dBm at MCS0~2  
13dBm at MCS3~4  
12.5dBm at MCS5~6  
12dBm at MCS7
- 802.11ac (typical at room temperature 25 °C)  
VHT20  
14dBm at MCS0~4  
13dBm at MCS5  
12dBm at MCS6  
11dBm at MCS7/8  
VHT40  
14dBm at MCS0~2  
13dBm at MCS3~4  
12dBm at MCS5~6  
11dBm at MCS7/8/9  
VHT80  
14dBm at MCS0~4  
13dBm at MCS5~6  
12dBm at MCS7  
11dBm at MCS8/9

### Receiver sensitivity

- 802.11a (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C)  
-82dBm at 6Mbps  
-81dBm at 9Mbps  
-79dBm at 12Mbps  
-77dBm at 18Mbps  
-74dBm at 24Mbps  
-70dBm at 36Mbps  
-66dBm at 48Mbps  
-65dBm at 54Mbps
- 802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C)  
-80dBm at 1Mbps  
-80dBm at 2Mbps  
-76dBm at 5.5Mbps  
-76dBm at 11Mbps

**Wireless Module Parameters**

	<ul style="list-style-type: none"> <li>· 802.11g (typical at PER &lt; 10% (1000-byte PDUs) at room temperature 25 °C)                         <ul style="list-style-type: none"> <li>-82dBm at 6Mbps</li> <li>-81dBm at 9Mbps</li> <li>-79dBm at 12Mbps</li> <li>-77dBm at 18Mbps</li> <li>-74dBm at 24Mbps</li> <li>-70dBm at 36Mbps</li> <li>-66dBm at 48Mbps</li> <li>-65dBm at 54Mbps</li> </ul> </li>   <li>· 802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C)                         <ul style="list-style-type: none"> <li>2.4GHz, HT20                                 <ul style="list-style-type: none"> <li>-82dBm at MCS0</li> <li>-79dBm at MCS1</li> <li>-77dBm at MCS2</li> <li>-74dBm at MCS3</li> <li>-70dBm at MCS4</li> <li>-66dBm at MCS5</li> <li>-65dBm at MCS6</li> <li>-64dBm at MCS7</li> </ul> </li> <li>2.4GHz, HT40                                 <ul style="list-style-type: none"> <li>-79dBm at MCS0</li> <li>-76dBm at MCS1</li> <li>-74dBm at MCS2</li> <li>-71dBm at MCS3</li> <li>-67dBm at MCS4</li> <li>-63dBm at MCS5</li> <li>-62dBm at MCS6</li> <li>-61dBm at MCS7</li> </ul> </li> <li>5GHz, HT20                                 <ul style="list-style-type: none"> <li>-82dBm at MCS0</li> <li>-79dBm at MCS1</li> <li>-77dBm at MCS2</li> <li>-74dBm at MCS3</li> <li>-70dBm at MCS4</li> <li>-66dBm at MCS5</li> <li>-65dBm at MCS6</li> <li>-64dBm at MCS7</li> </ul> </li> <li>5GHz, HT40                                 <ul style="list-style-type: none"> <li>-79dBm at MCS0</li> <li>-76dBm at MCS1</li> <li>-74dBm at MCS2</li> <li>-71dBm at MCS3</li> <li>-67dBm at MCS4</li> <li>-63dBm at MCS5</li> <li>-62dBm at MCS6</li> <li>-61dBm at MCS7</li> </ul> </li> </ul> </li>   <li>· 802.11ac (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C)                         <ul style="list-style-type: none"> <li>VHT20                                 <ul style="list-style-type: none"> <li>-82dBm at MCS0</li> <li>-79dBm at MCS1</li> <li>-77dBm at MCS2</li> <li>-74dBm at MCS3</li> <li>-70dBm at MCS4</li> <li>-66dBm at MCS5</li> <li>-65dBm at MCS6</li> <li>-64dBm at MCS7</li> <li>-56dBm at MCS8</li> </ul> </li> </ul> </li> </ul>
--	--

Wireless Module Parameters	
	VHT40 -79dBm at MCS0 -76dBm at MCS1 -74dBm at MCS2 -71dBm at MCS3 -67dBm at MCS4 -63dBm at MCS5 -62dBm at MCS6 -61dBm at MCS7 -56dBm at MCS8 -54dBm at MCS9 VHT80 -76dBm at MCS0 -73dBm at MCS1 -71dBm at MCS2 -68dBm at MCS3 -64dBm at MCS4 -60dBm at MCS5 -59dBm at MCS6 -58dBm at MCS7 -53dBm at MCS8 -51dBm at MCS9
<b>Modulation schemes</b>	<ul style="list-style-type: none"> <li>· 802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM</li> <li>· 802.11b: DQPSK, DBPSK, DSSS, CCK</li> <li>· 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM</li> <li>· 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM</li> <li>· 802.11ac: BPSK, QPSK, 16QAM, 64QAM, up to 256QAM with OFDM</li> </ul>

Physical Parameters	
<b>Dimensions (L x W x H)</b>	· 205 x 136 x 33 mm (8.07 x 5.35 x 1.3 in)
<b>Weight</b>	· 285 g (0.63 lb)

Operating Environment	
<b>Power</b>	· Output: 12V DC, 1A
<b>Temperature</b>	<ul style="list-style-type: none"> <li>· Operating: from 0 to 40 °C</li> <li>· Storage: from -20 to 65 °C</li> </ul>
<b>Humidity</b>	<ul style="list-style-type: none"> <li>· Operating: from 10% to 90% (non-condensing)</li> <li>· Storage: from 5% to 95% (non-condensing)</li> </ul>

## Product Appearance

### Upper Panel



Figure 1. Upper panel view.

LED	Mode	Description
Power	<i>Solid green</i>	The router is powered on.
	<i>No light</i>	The router is powered off.
Internet	<i>Solid green</i>	The WAN cable is connected to the port.
	<i>Blinking green</i>	Data transfer through the WAN port.
	<i>No light</i>	The WAN cable is not connected.

LED	Mode	Description
<b>LAN 1-4</b>	<i>Solid green</i>	A device (computer) is connected to the relevant port, the connection is on.
	<i>Blinking green</i>	Data transfer through the relevant LAN port. When the router is being loaded, the LEDs are blinking one at a time. When the firmware is being upgraded, the LEDs are blinking two at a time.
	<i>No light</i>	The cable is not connected to the relevant port.
<b>WLAN 2.4G WLAN 5G</b>	<i>Solid green</i>	The router's WLAN of the relevant band is on.
	<i>Blinking green</i>	Data transfer through the Wi-Fi network of the relevant band.
	<i>No light</i>	The router's WLAN of the relevant band is off.
<b>WPS</b>	<i>Blinking green</i>	Attempting to connect mesh network devices or add a wireless device via the WPS function.
	<i>No light</i>	The WPS function is not in use.

In case the **Power** LED is solid green, and the **Internet**, **LAN**, and **WPS** LEDs are fast blinking green at the same time, the device is in the emergency mode. Power the device off and on. If the device is loaded in the emergency mode again, restore the factory default settings via the hardware **RESET** button.

## Back and Bottom Panels



Figure 2. Back panel view.

Port	Description
<b>WIFI</b>	A button to enable/disable wireless network. To disable the router's wireless network: with the device turned on, press the button and release. The <b>WLAN 2.4G</b> and <b>WLAN 5G</b> LEDs should turn off.
<b>WPS</b>	A button to connect mesh network devices or set up wireless connection (the WPS function). To connect mesh network devices: with the device turned on and factory default settings or with the EasyMesh function enabled in the router settings, push the button, hold it for 2 seconds, and release. To use the WPS function: push the button, hold it for 2 seconds, and release.
<b>LAN 1-4</b>	4 Ethernet ports to connect computers or network devices.
<b>WAN</b>	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).
<b>POWER</b>	A button to turn the router on/off.

Also, the power connector is located on the back panel of the router.

The **RESET** button located on the bottom panel of the router is designed to restore the factory default settings. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.

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

## ***Delivery Package***

The following should be included:

- Router DIR-822
- Power adapter DC 12V/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](http://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 dual band router with a built-in 4-port switch DIR-822 (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 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 802.11a, b, g, n, or ac 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.
3. Turn on the router by pressing the **POWER** button on its back panel.

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.)

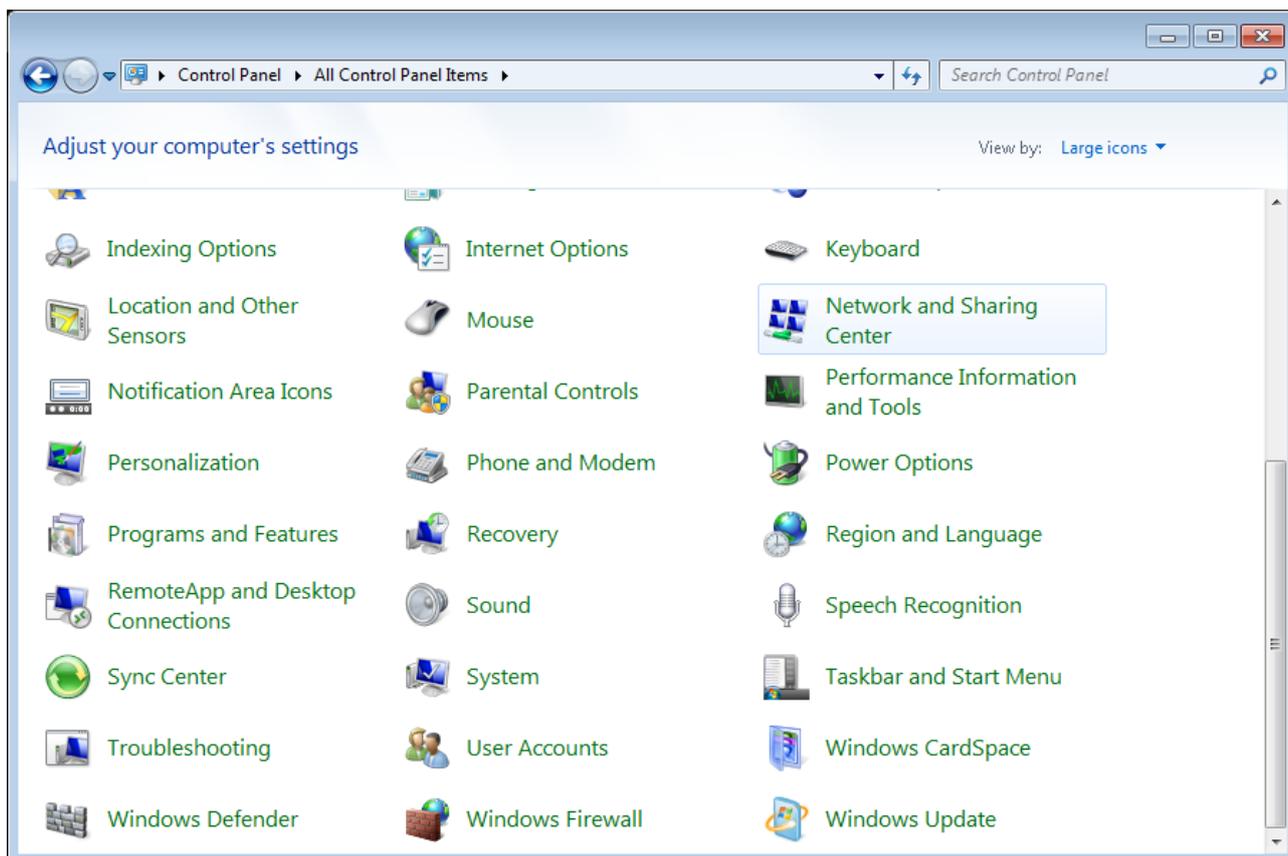


Figure 3. The **Control Panel** window.

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

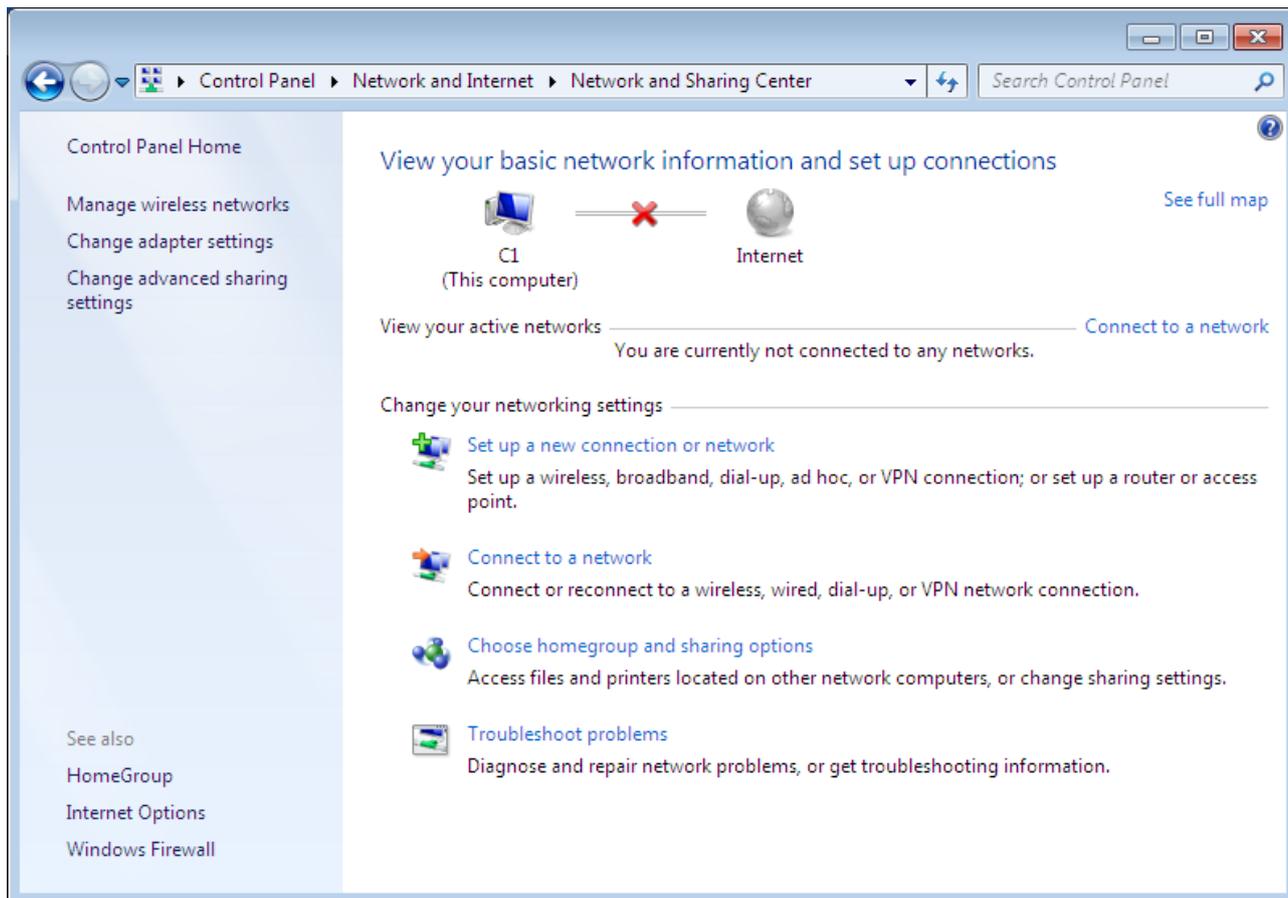


Figure 4. The **Network and Sharing Center** window.

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

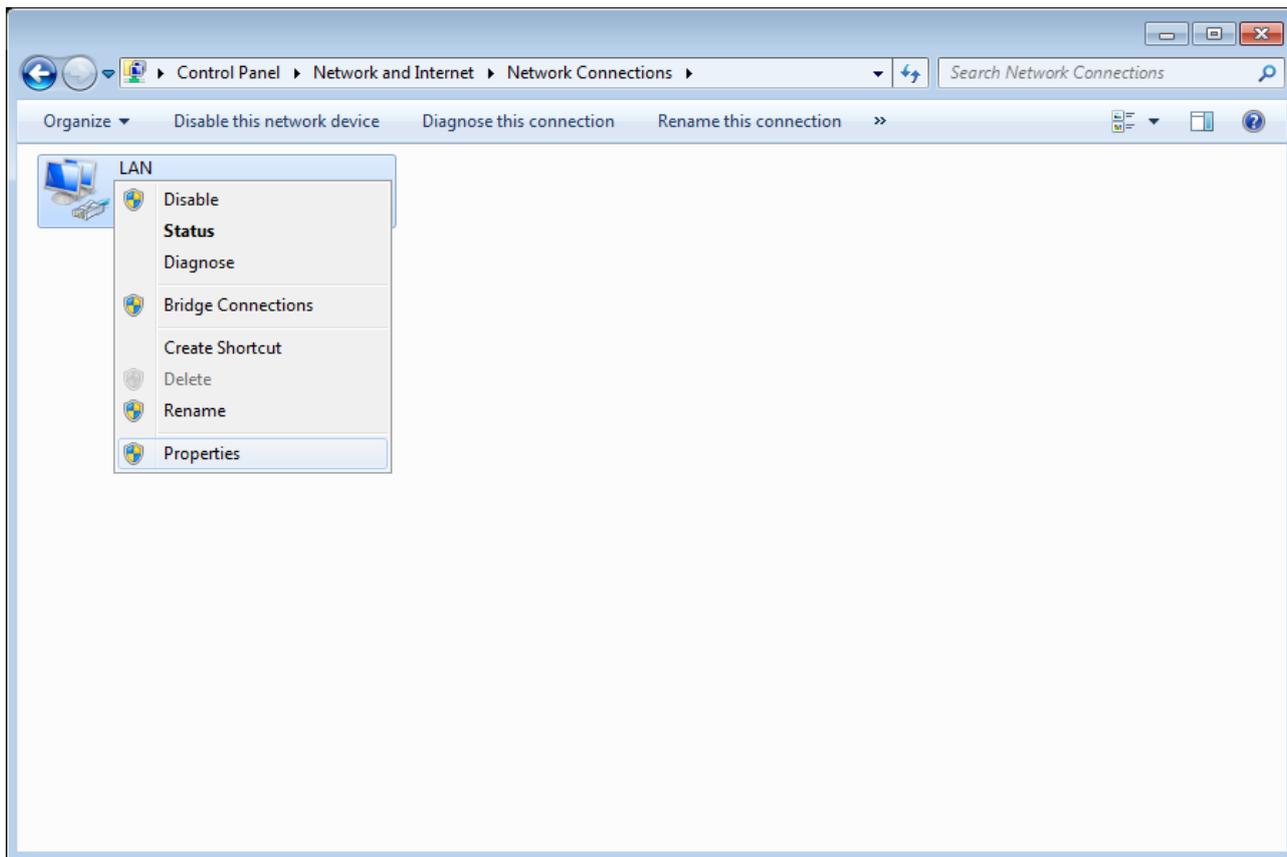


Figure 5. The **Network Connections** window.

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.

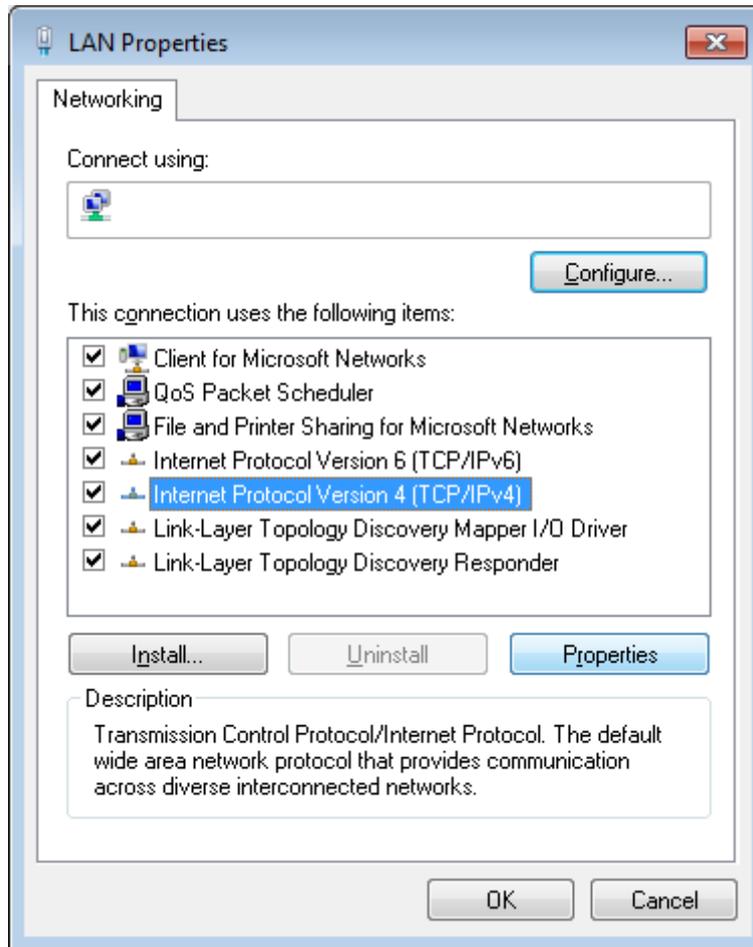


Figure 6. The **Local Area Connection Properties** window.

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.

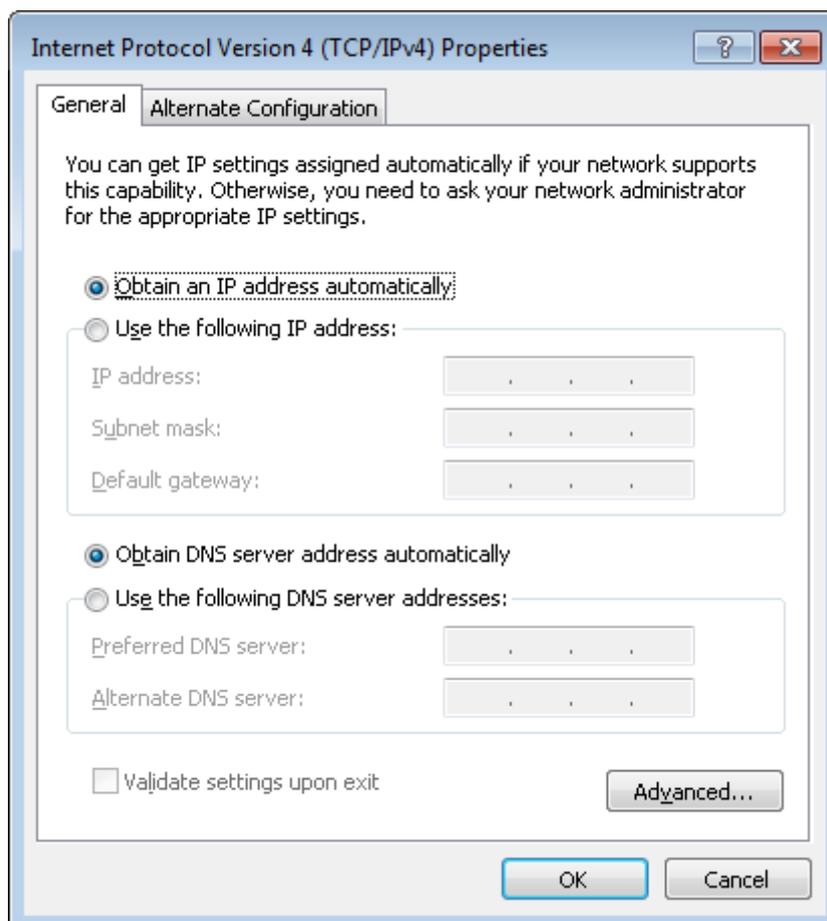
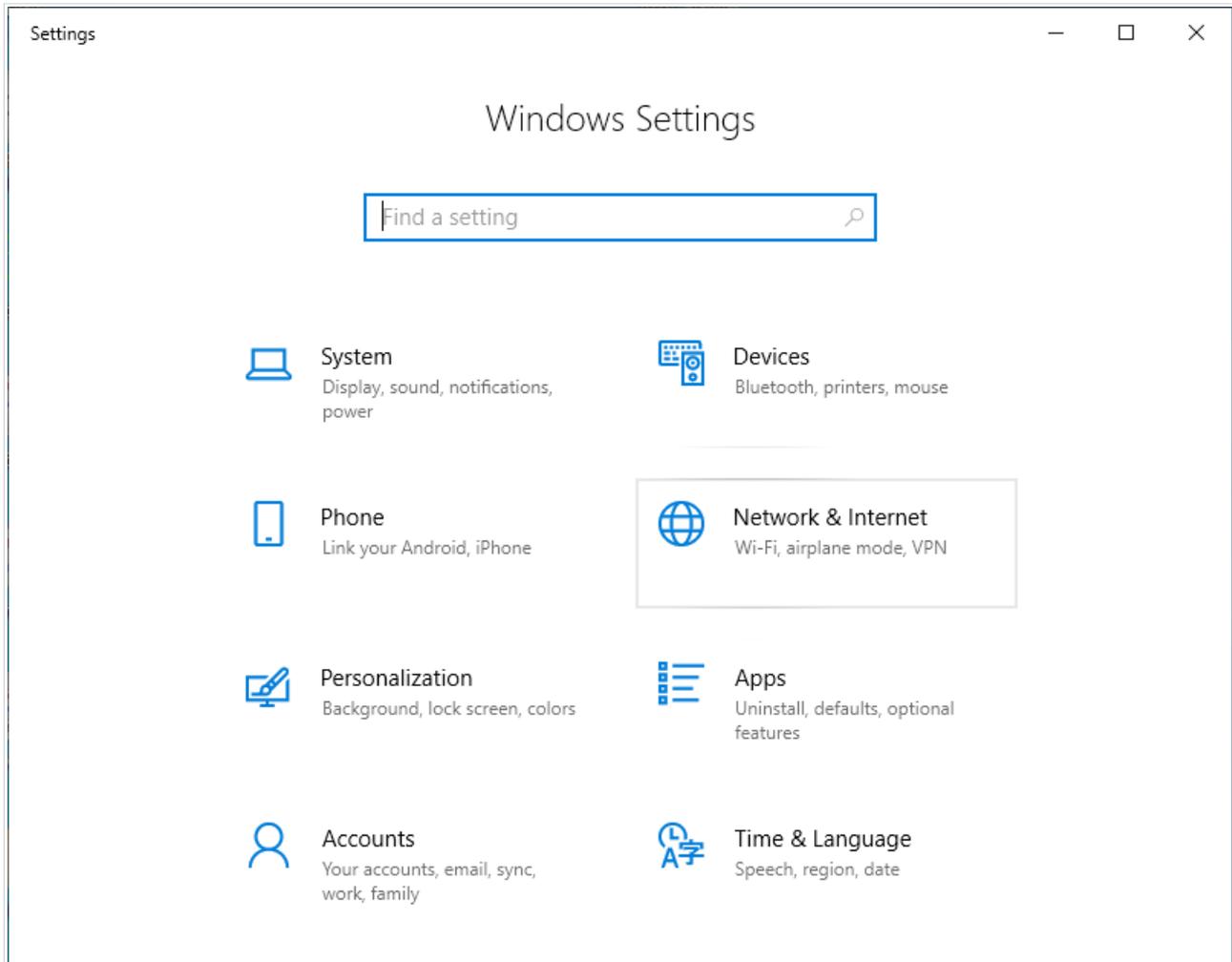


Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

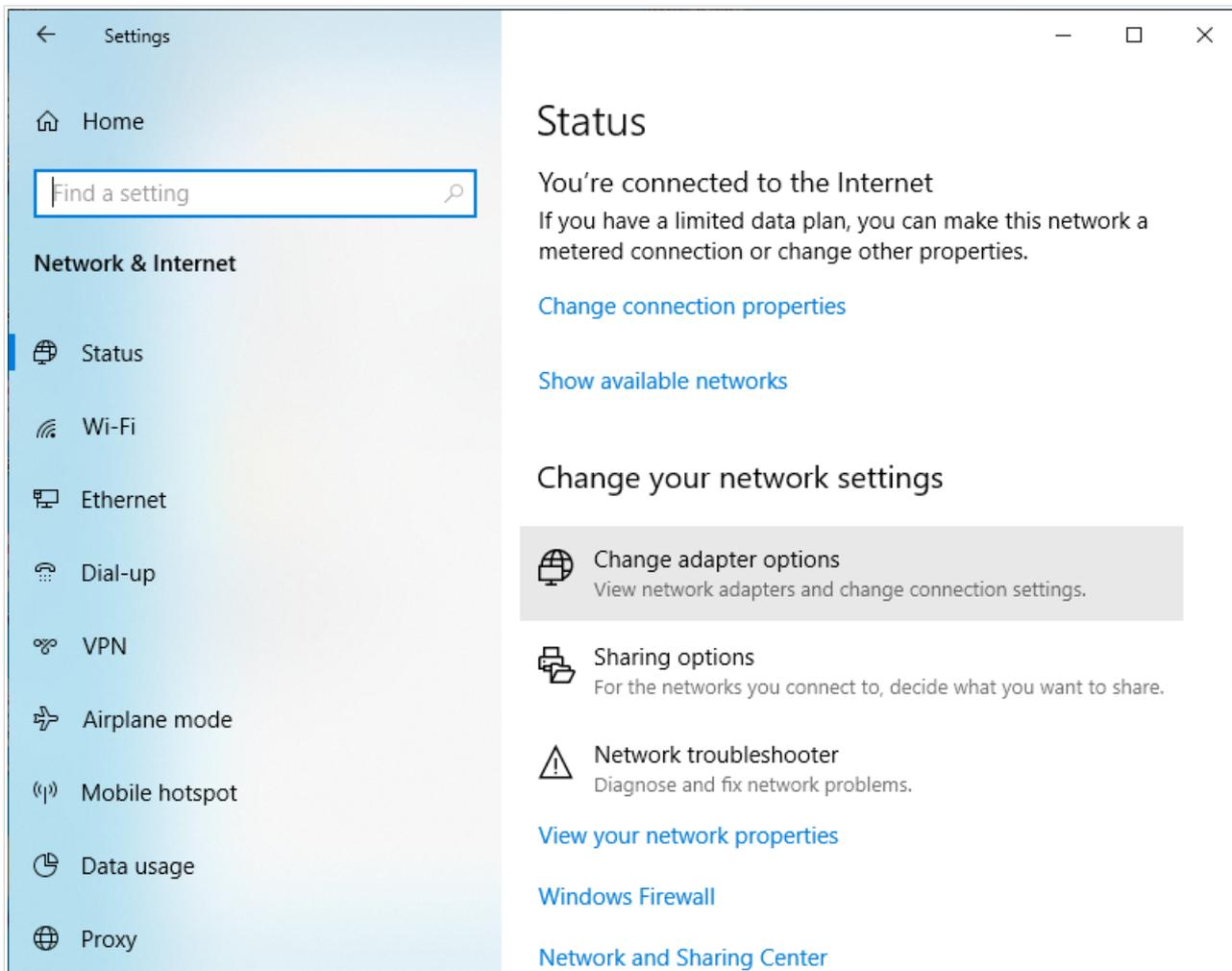


Figure 9. The **Network & Internet** window.

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

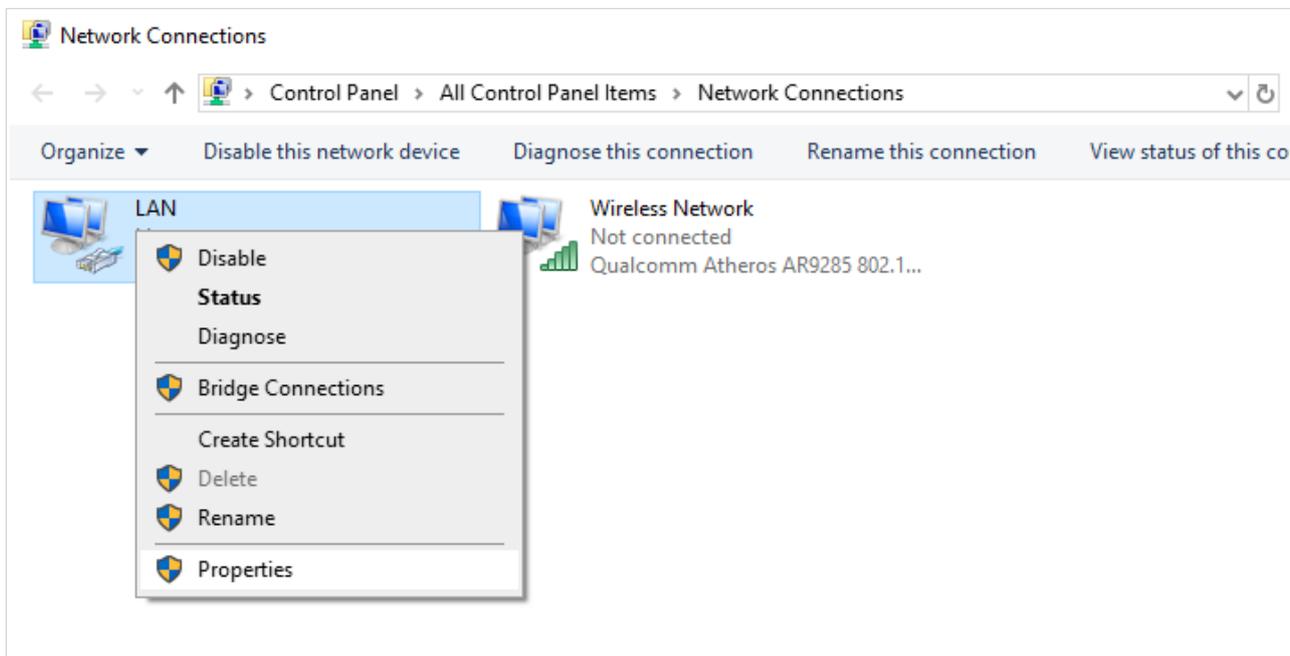


Figure 10. The **Network Connections** window.

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.

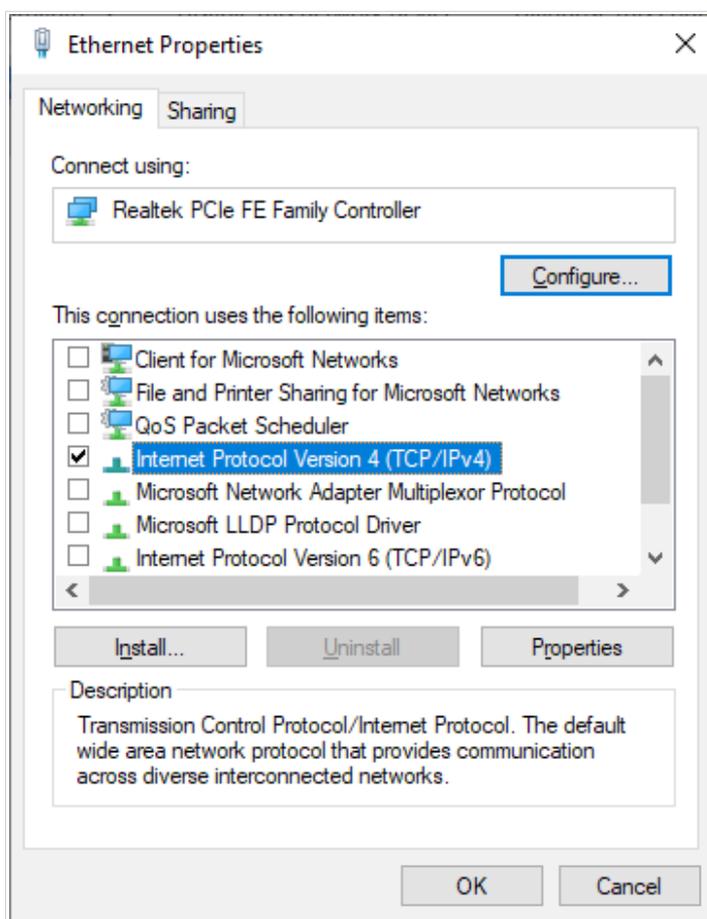


Figure 11. The local area connection properties window.

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.

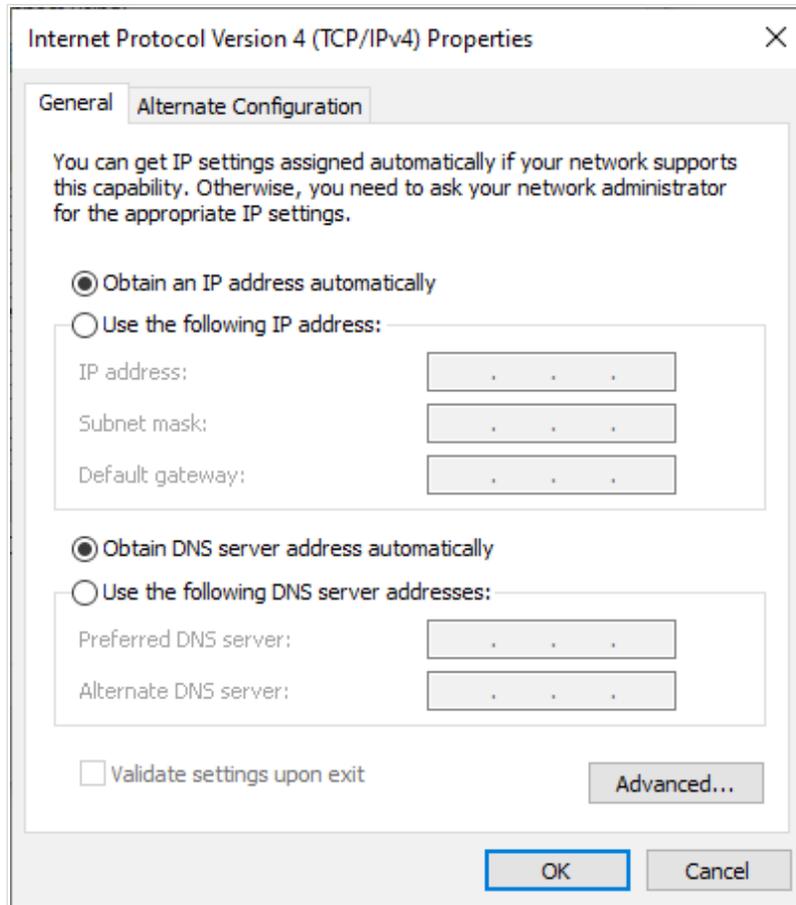


Figure 12. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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. Turn on the router by pressing the **POWER** button on its back panel.
3. 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.)

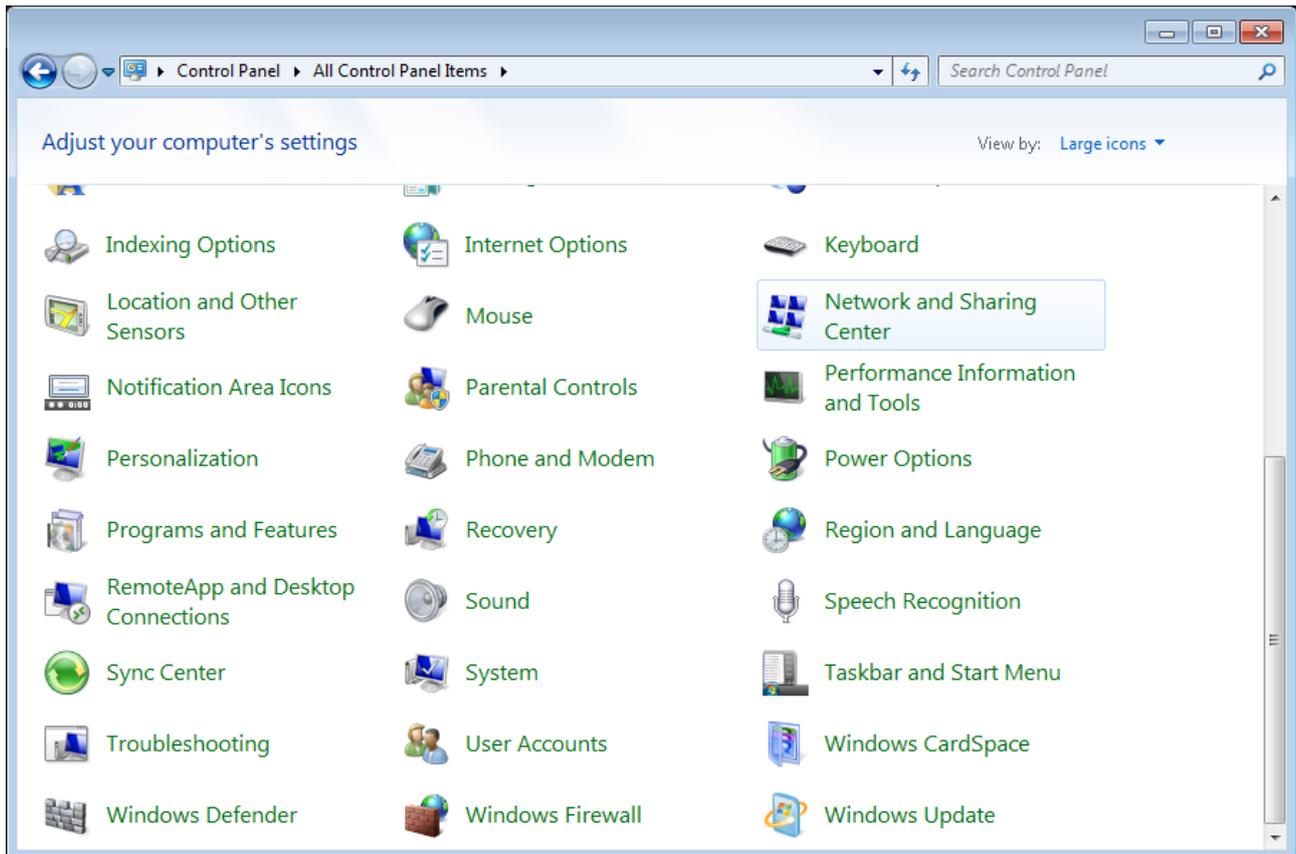


Figure 13. The **Control Panel** window.

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.

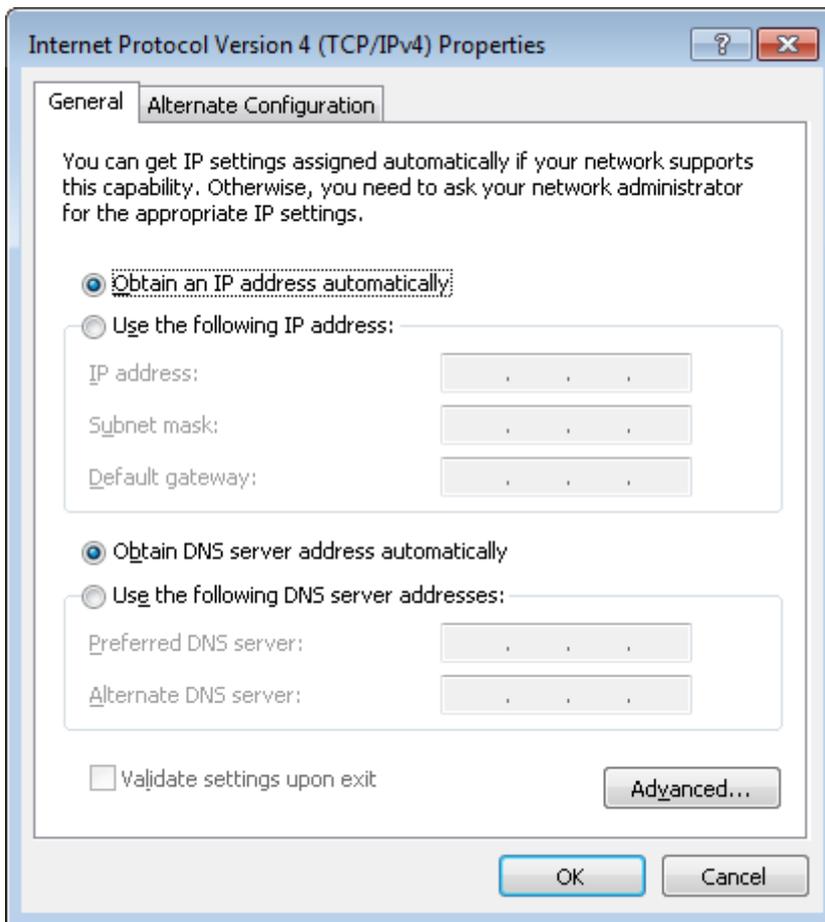


Figure 14. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

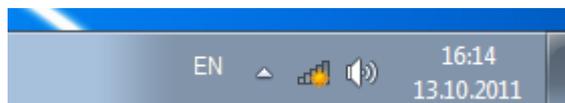


Figure 15. The notification area of the taskbar.

- In the opened **Wireless Network Connection** window, select the wireless network **DIR-822** (for operating in the 2.4GHz band) or **DIR-822-5G** (for operating in the 5GHz band) and click the **Connect** button.

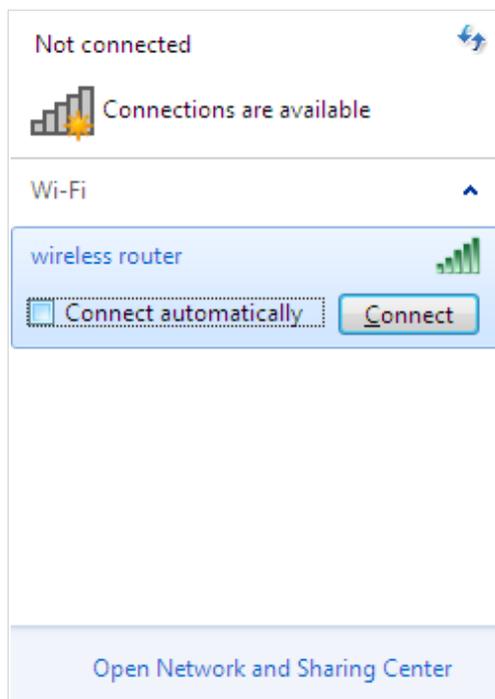


Figure 16. The list of available networks.

- 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.
- 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.

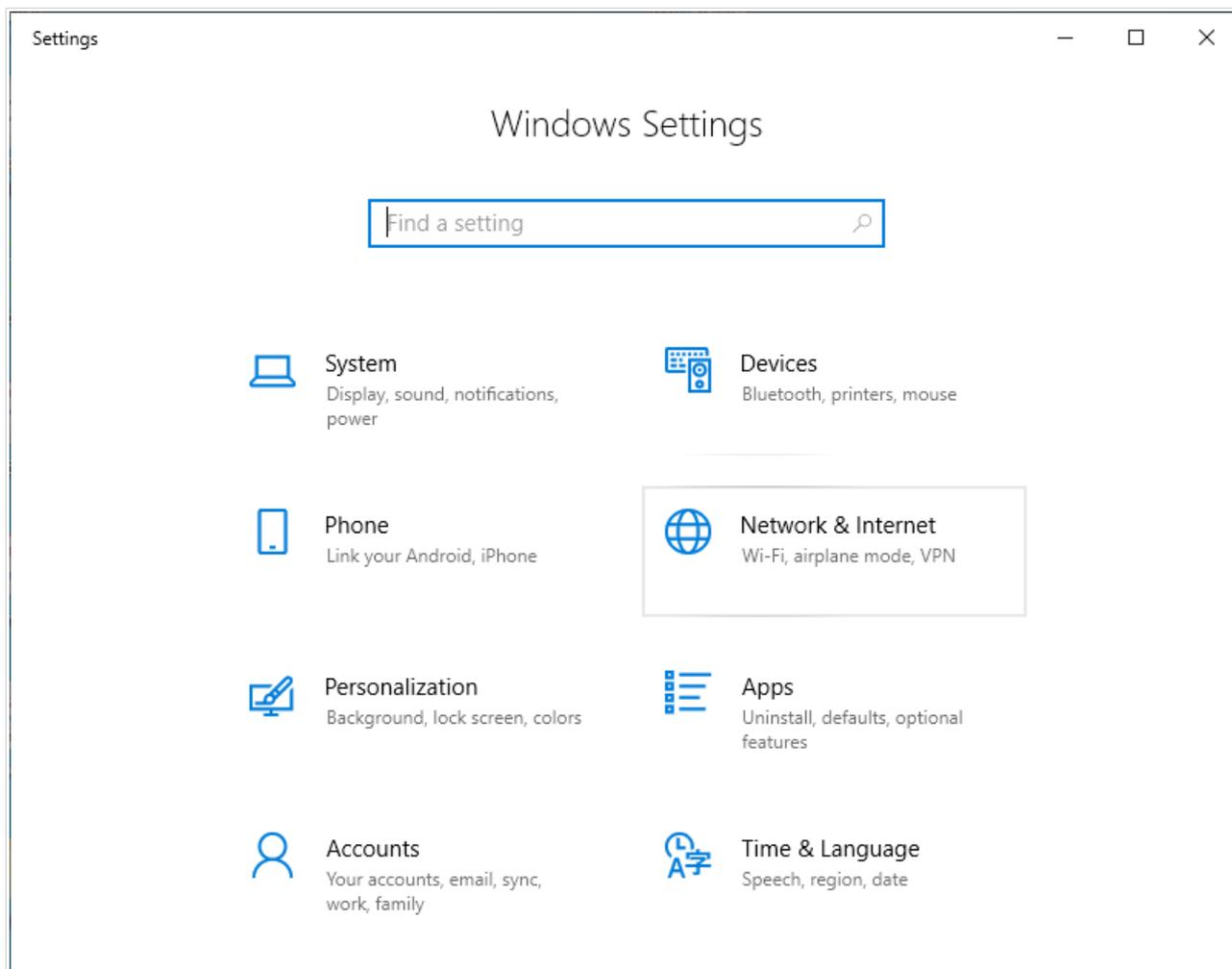


Figure 17. The **Windows Settings** window.

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.

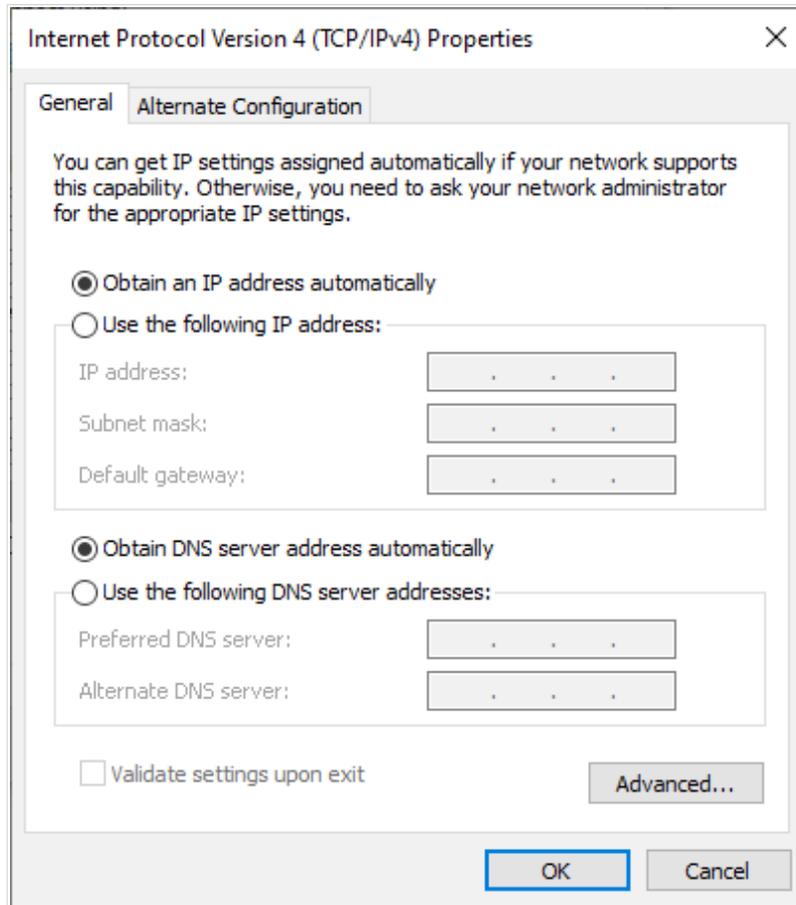


Figure 18. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

- In the opened **Wireless Network Connection** window, select the wireless network **DIR-822** (for operating in the 2.4GHz band) or **DIR-822-5G** (for operating in the 5GHz band) and click the **Connect** button.

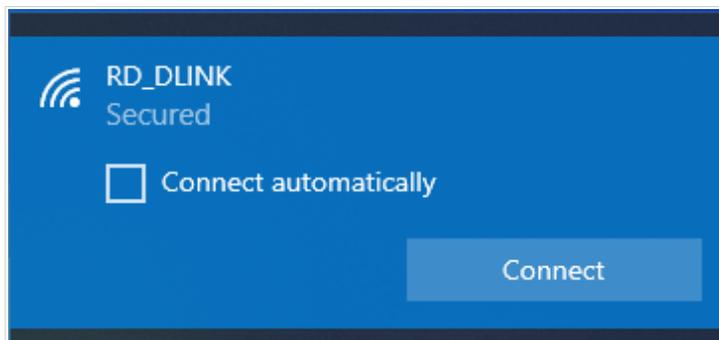


Figure 20. The list of available networks.

- 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.
- Allow or forbid your PC to be discoverable by other devices on this network (**Yes / No**).

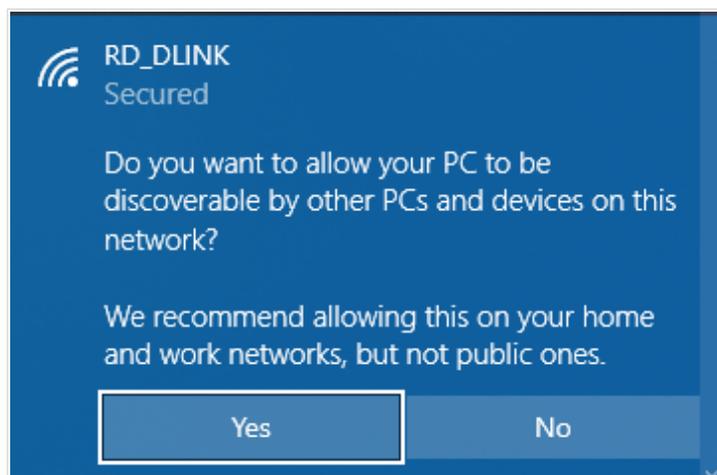


Figure 21. PC discovery settings.

- 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-822 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 19). 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-822 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 Initial Configuration Wizard opens (see the **Initial Configuration Wizard** section, page 44).

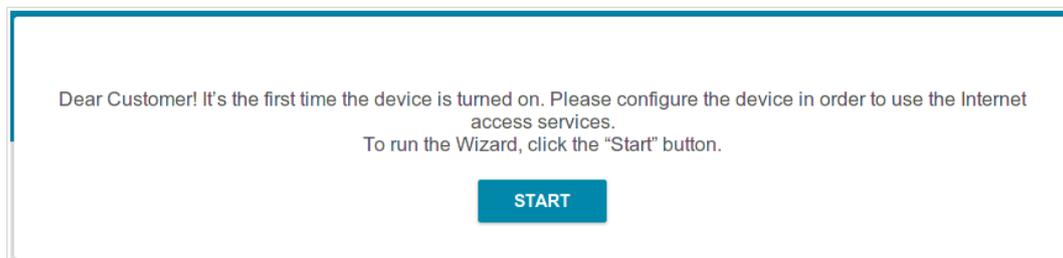


Figure 23. The page for running the Initial Configuration Wizard.

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.

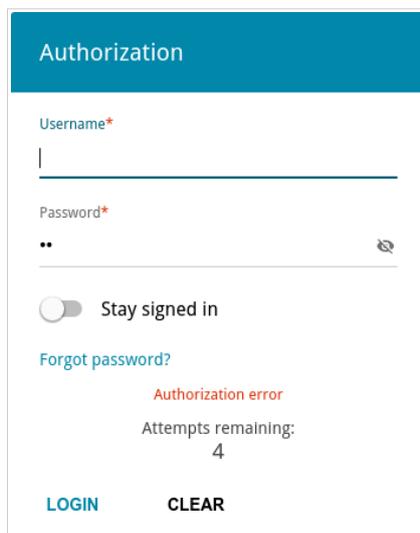


Figure 24. The login page.

In order not to log out, move the **Stay signed in** switch to the right. After closing the web browser or rebooting the device, you need to enter the username and the password again.

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

### Summary Page

On the **Summary** page, detailed information on the device state is displayed.

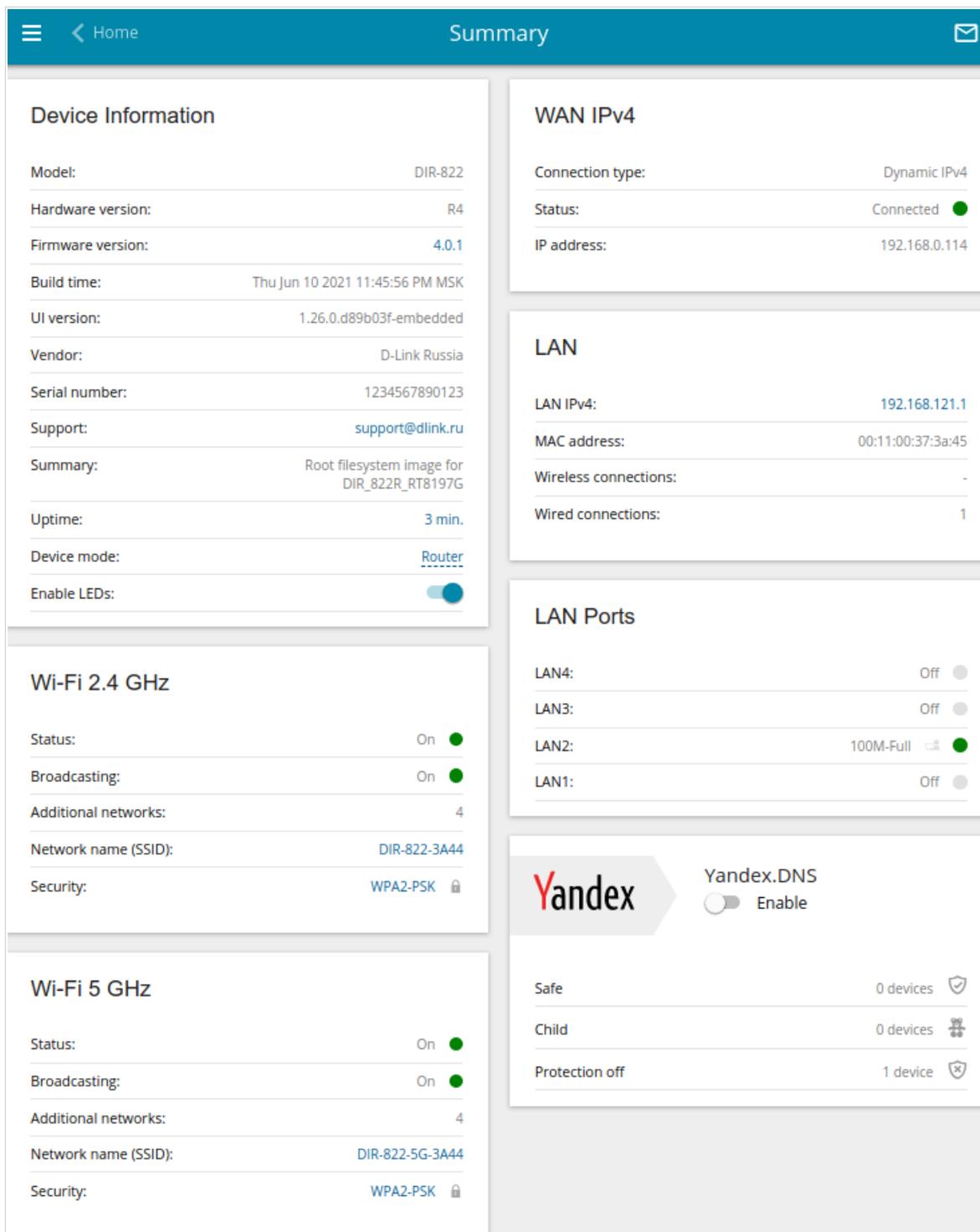


Figure 25. The summary page.

The **Device Information** section displays the model and hardware version of the router, the firmware version, and other data.

To contact the technical support group (to send an e-mail), left-click the support e-mail address. After clicking the line, the e-mail client window for sending a new letter to the specified address opens.

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **Initial Configuration Wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 44).

If needed, you can disable the LEDs of the device. To do this, move the **Enable LEDs** switch to the left. In order to enable the LEDs, move the switch to the right and reboot the device.

The **Wi-Fi 2.4 GHz** and **Wi-Fi 5 GHz** sections display data on the state of the device's wireless network, its name and the authentication type, and availability of an additional wireless network in the relevant band.

In the **WAN** section, data on the type and status of the existing WAN connection are displayed.

In the **LAN** section, the IPv4 and IPv6 address of the router, the LAN MAC address, and the number of wired and wireless clients of the device are displayed.

The **LAN Ports** section displays the state of the device's LAN ports and data transfer mode of active ports.

The **Yandex.DNS** section displays the Yandex.DNS service state and operation mode. To enable the Yandex.DNS service, move the **Enable** switch to the right. If needed, change the operation mode of the service.

## Home Page

The **Home** page displays links to the most frequently used pages with device's settings.

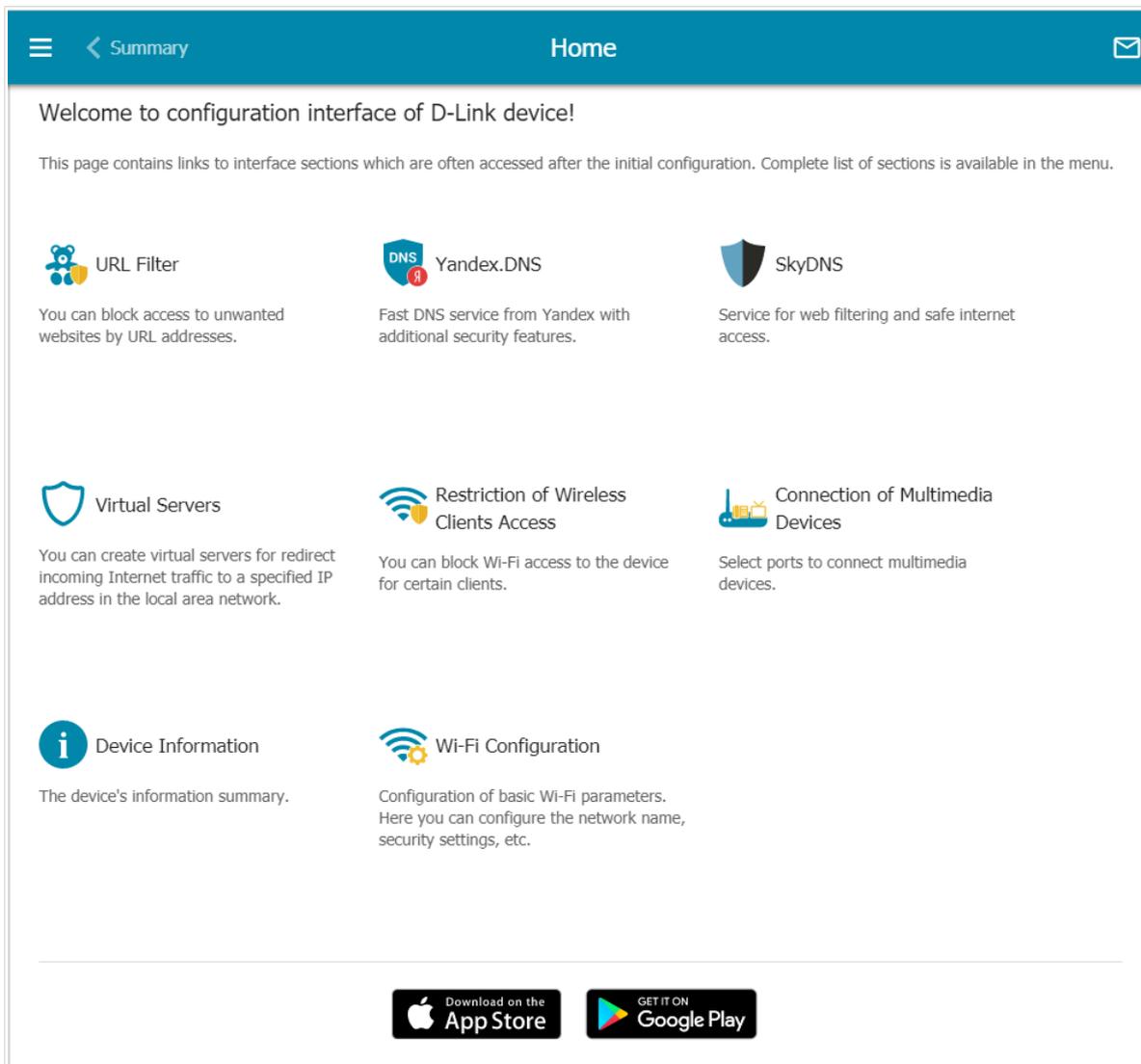


Figure 26. The **Home** page.

Other settings of the router are available in the menu in the left part of the page.

## Menu Sections

To configure the router use the menu in the left part of the page.

In the **Initial Configuration** section you can run the Initial Configuration 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 **Initial Configuration Wizard** section, page 44).

The pages of the **Statistics** section display data on the current state of the router (for the description of the pages, see the **Statistics** section, page 71).

The pages of the **Connections Setup** section are designed for configuring basic parameters of the LAN interface of the router and creating a connection to the Internet (for the description of the pages, see the **Connections Setup** section, page 79).

The pages of the **Wi-Fi** section are designed for specifying all needed settings of the router's wireless network (for the description of the pages, see the **Wi-Fi** section, page 114).

The pages of the **Advanced** section are designed for configuring additional parameters of the router (for the description of the pages, see the **Advanced** section, page 147).

The pages of the **Firewall** section are designed for configuring the firewall of the router (for the description of the pages, see the **Firewall** section, page 178).

The pages of the **System** section provide functions for managing the internal system of the router (for the description of the pages, see the **System** section, page 197).

The pages of the **Yandex.DNS** section are designed for configuring the Yandex.DNS web content filtering service (for the description of the pages, see the **Yandex.DNS** section, page 221).

The pages of the **SkyDNS** section are designed for configuring the SkyDNS web content filtering service (for the description of the pages, see the **SkyDNS** section, page 225).

To exit the web-based interface, click the **Logout** line of the menu.

## Notifications

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



*Figure 27. 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

### Initial Configuration Wizard

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

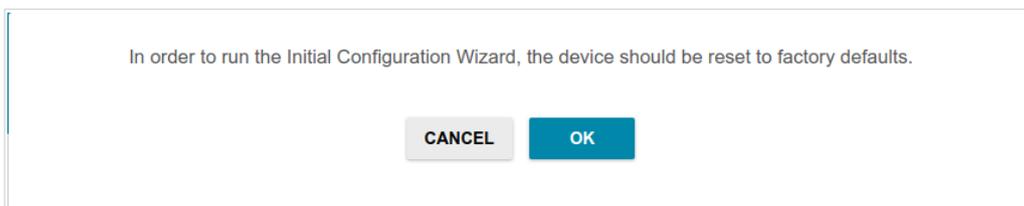


Figure 28. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network of DIR-822 (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

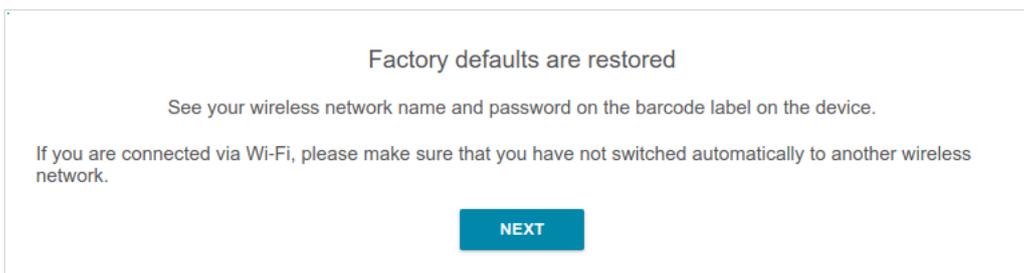


Figure 29. Checking connection to the wireless network.

Click the **START** button.

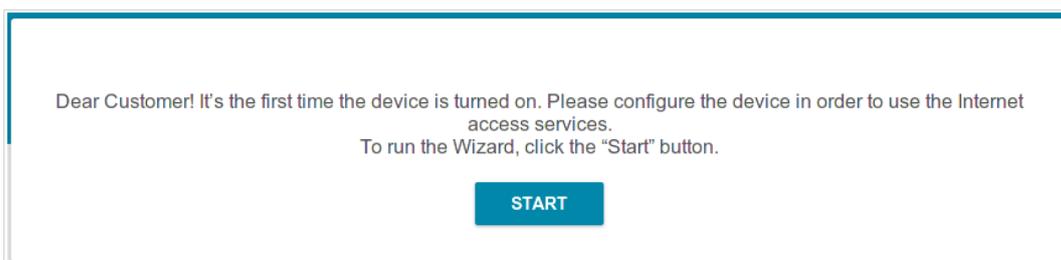


Figure 30. Starting the Wizard.

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

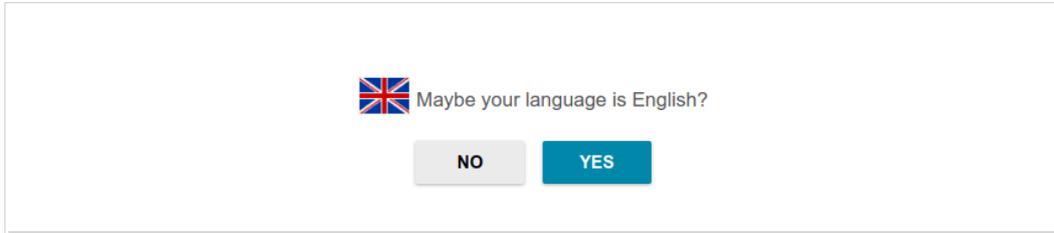


Figure 31. Selecting a language.

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** and the name of the wireless network in the 2.4GHz and 5GHz bands in the **Network name 2.4 GHz (SSID)** and **Network name 5 GHz (SSID)** fields correspondingly. Then click the **APPLY** button.

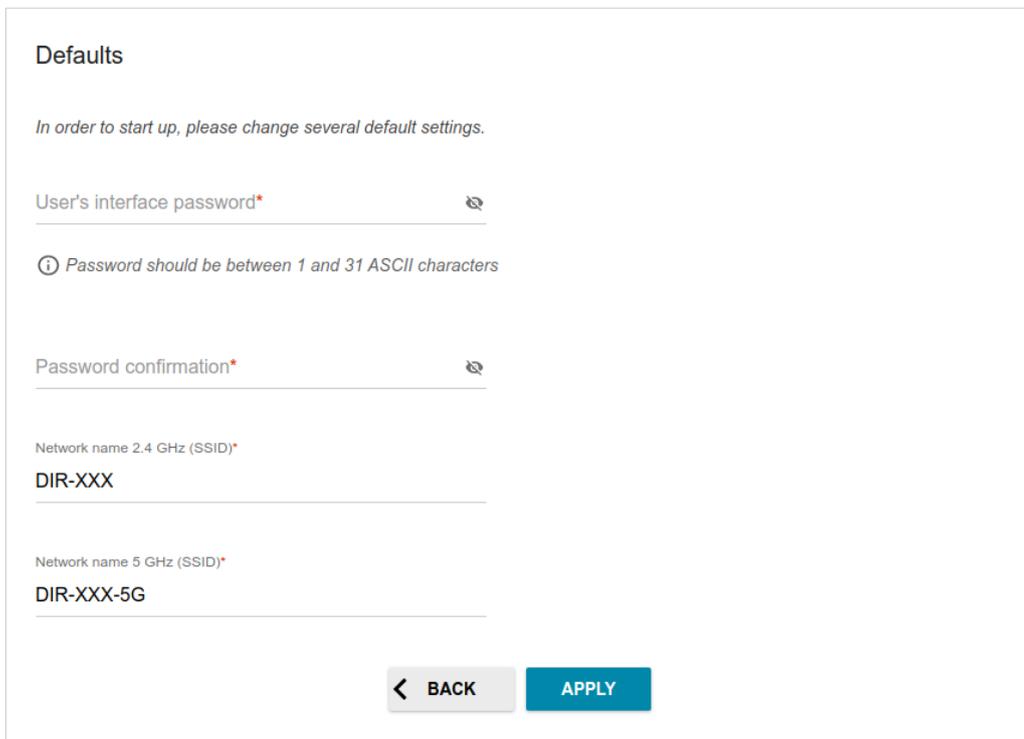


Figure 32. Changing the default settings.

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 **Autonomous** 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 in the 2.4GHz and 5GHz bands, 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.

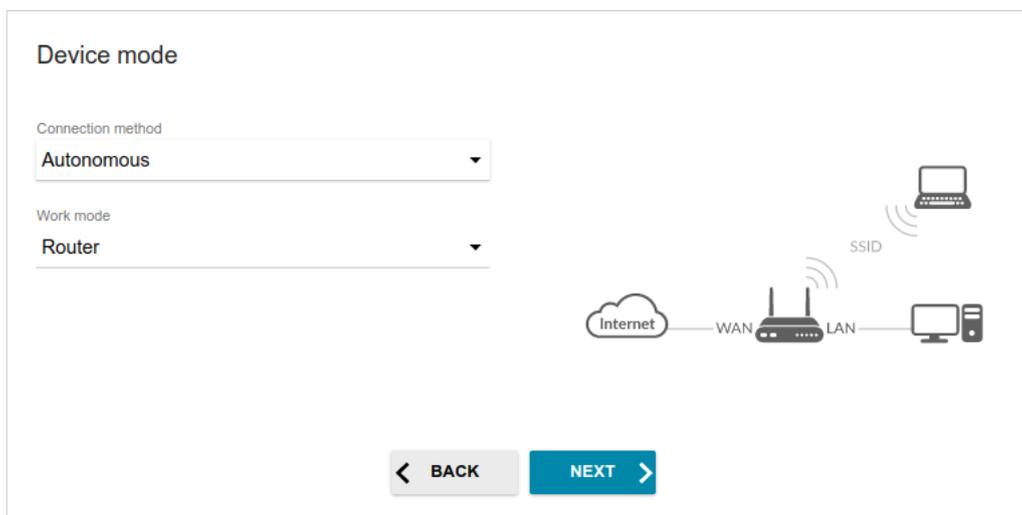


Figure 33. Selecting an operation mode. The **Router** mode.

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

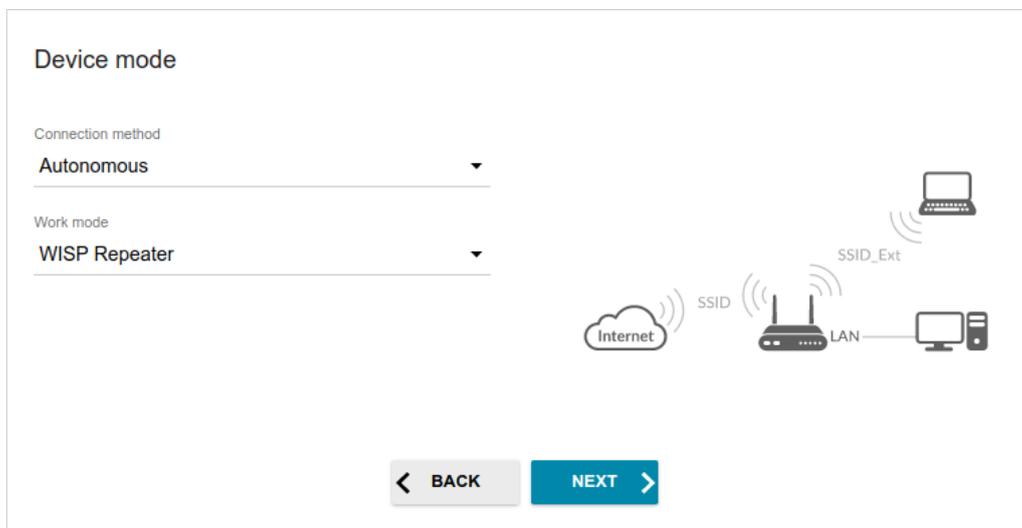


Figure 34. Selecting an operation mode. The **WISP Repeater** mode.

## 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 **Autonomous** 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 in the 2.4GHz and 5GHz bands and set your own password for access to the web-based interface of the device.

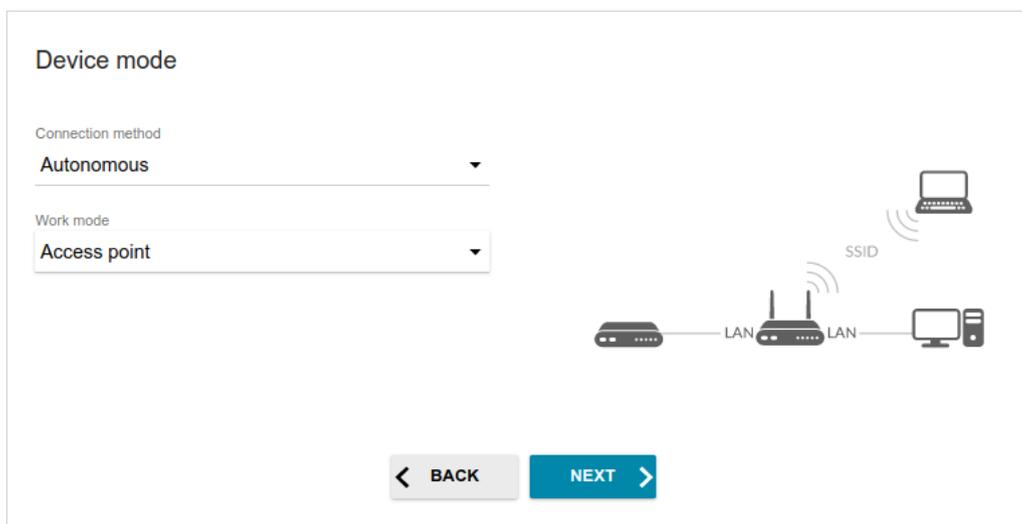


Figure 35. Selecting an operation mode. The **Access point** mode.

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 **Autonomous** 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 in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

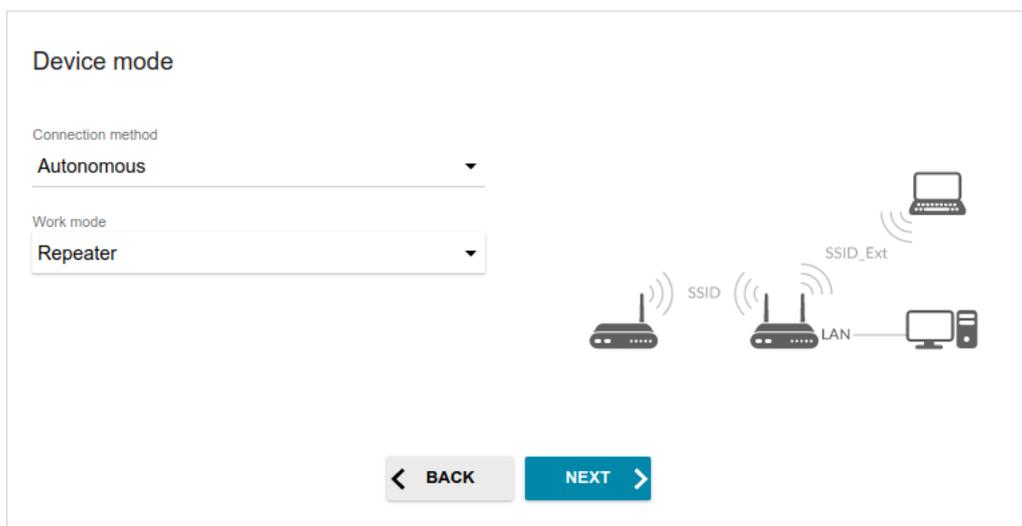


Figure 36. Selecting an operation mode. The **Repeater** mode.

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 **Autonomous** 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.

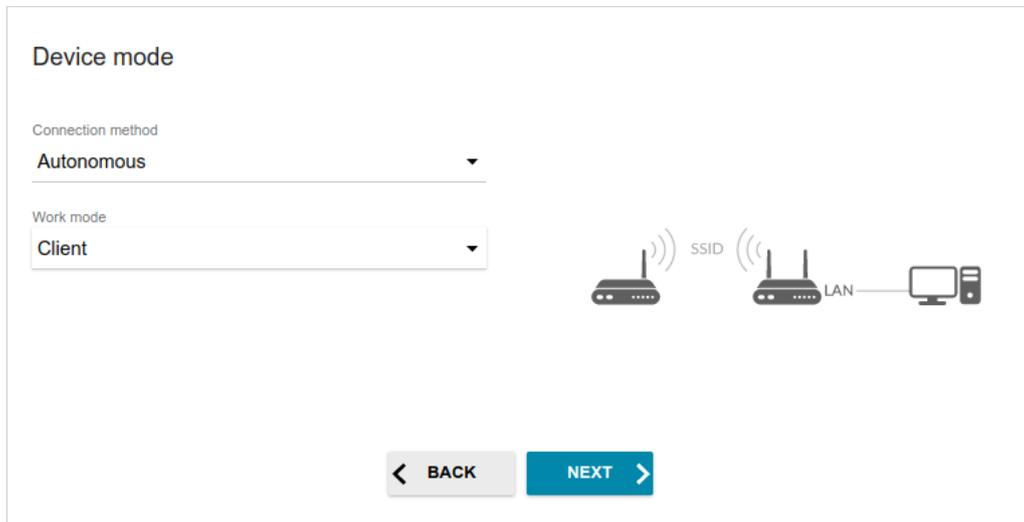


Figure 37. Selecting an operation mode. The **Client** mode.

## Mesh Network Main Device (Controller)

In order to configure DIR-822 as a main device of your mesh network, from the **Connection method** list, select the **EasyMesh** value. Then from the **Device role** list, select the **Controller** value. From the **Backhaul band** list, select the band where your mesh network operates.

**!** The EasyMesh function cannot operate in both bands simultaneously. Select one of the bands (2.4GHz or 5GHz) for all devices of the configured network.

You can connect Agent devices with factory defaults to the main mesh network device via the hardware **WPS** button. To do this, on the main device, in the **Backhaul band** drop-down list, select the **5 GHz** option and complete the configuration of the main device via the Wizard. Then press the hardware WPS button on both devices, hold it for 2 seconds, and release. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.

In order to connect your main device to a wired ISP, 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 in the 2.4GHz and 5GHz bands, 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.

The screenshot shows a configuration page titled "Device mode". It contains four dropdown menus: "Connection method" set to "EasyMesh", "Device role" set to "Controller", "Work mode" set to "Router", and "Backhaul band" set to "5 GHz". Below these is an information icon and text: "The backhaul band should be the same for the Controller device and all Agent devices". Further down, there are two paragraphs of explanatory text: "The EasyMesh function is designed to connect devices in one network. The connection can be wired or wireless." and "The Controller device in the mesh network is equivalent to a router in a usual network. One network can contain only one Controller device. If you already have such a device in your network, configure the present device to act as Agent." At the bottom left, there is a warning icon and text: "When Agent devices with factory defaults connect to the mesh network via the hardware button, they obtain the wireless settings and the administrator's password of the Controller." At the bottom center, there are two buttons: "BACK" and "NEXT". To the right of the form is a network diagram showing a central "Controller" router connected to an "Internet" cloud via a "LAN" port. The router has two other "LAN" ports connected to a "Mesh" cloud and a laptop. The router also has an "SSID" and "Mesh SSID" label with wireless signal icons.

Figure 38. Configuring the EasyMesh function for the main device. The **Router** mode.

In order to connect your main device to a wireless ISP (WISP), from the **Work mode** list, select the **WISP Repeater** value. In this mode you can connect your device to another access point, configure a WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

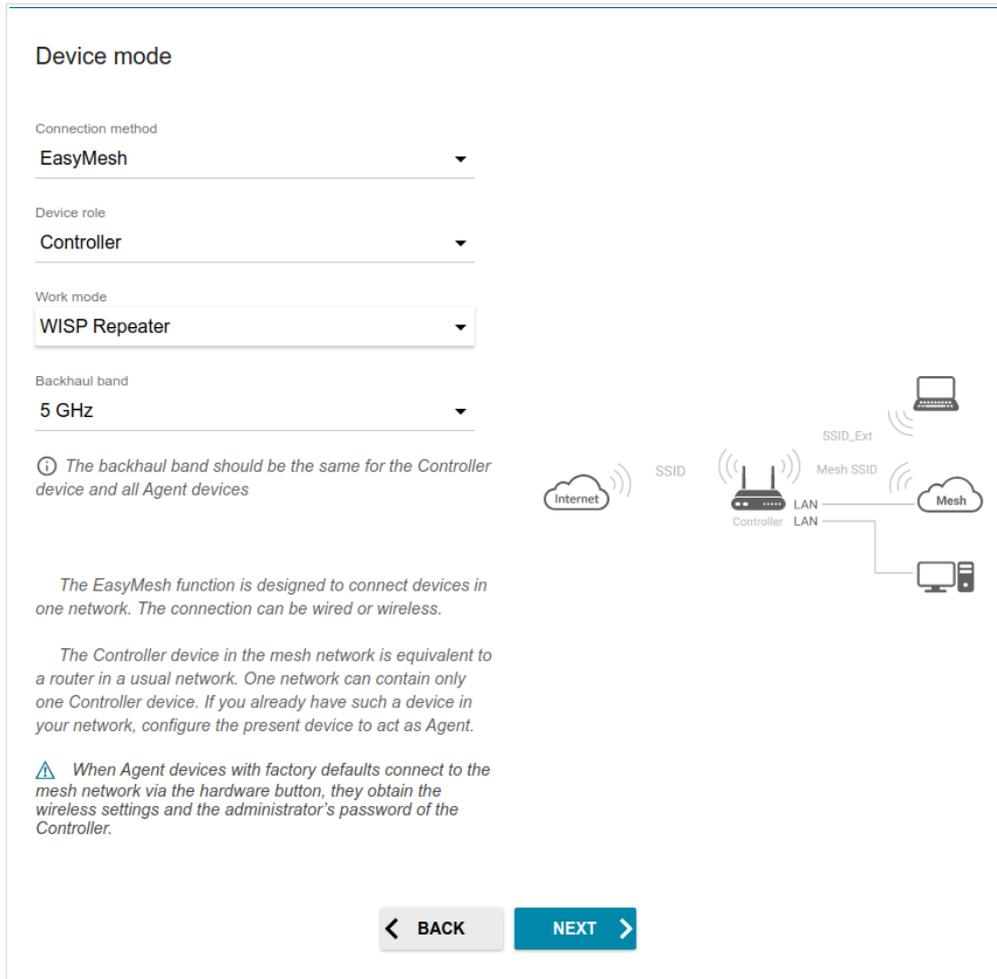


Figure 39. Configuring the EasyMesh function for a main device. The **WISP Repeater** mode.

## Mesh Network Subordinate Device (Agent)

In order to configure DIR-822 as a subordinate device of your mesh network, from the **Connection method** list, select the **EasyMesh** value. Then from the **Device role** list, select the **Agent** value. From the **Backhaul band** list, select the band where your main device (in the Controller role) operates.

Then a subordinate device is configured in the access point mode. In this mode you can change the LAN IP address, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

### Device mode

Connection method  
**EasyMesh**

Device role  
**Agent**

Backhaul band  
**5 GHz**

*The backhaul band should be the same for the Controller device and all Agent devices*

*The EasyMesh function is designed to connect devices in one network. The connection can be wired or wireless.*

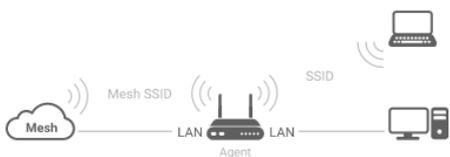
*When the settings are applied, simultaneously click the "Connect" button in the EasyMesh section (or the hardware WPS button) on the Agent device and on the Controller device (or on two Agent devices) in order to transfer data from one device to another.*

*If needed, disconnect the Agent device from the Controller device (or another Agent device) and move it to its permanent worksite.*

**1**



**2**



**< BACK**   **NEXT >**

Figure 40. Configuring the EasyMesh function for a subordinate device.

## 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-822 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-822, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Subnet mask**, **DNS IP address**, **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.

LAN

Automatic obtainment of IPv4 address

**!** Automatic obtainment of IPv4 address sufficiently protects against use of the same addresses in one LAN. In order to avoid IPv4 address conflicts, static IPv4 addresses of LAN devices should not coincide with addresses from the address range assigned by an upper-level router (or a local DHCP server).

IP address\*

192.168.0.1

Subnet mask\*

255.255.255.0

Gateway IP address

DNS IP address\*

8.8.8.8

Hostname\*

dlinkap18c6.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, dlinkap12ab.local./)

**< BACK** **NEXT >**

Figure 41. 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.

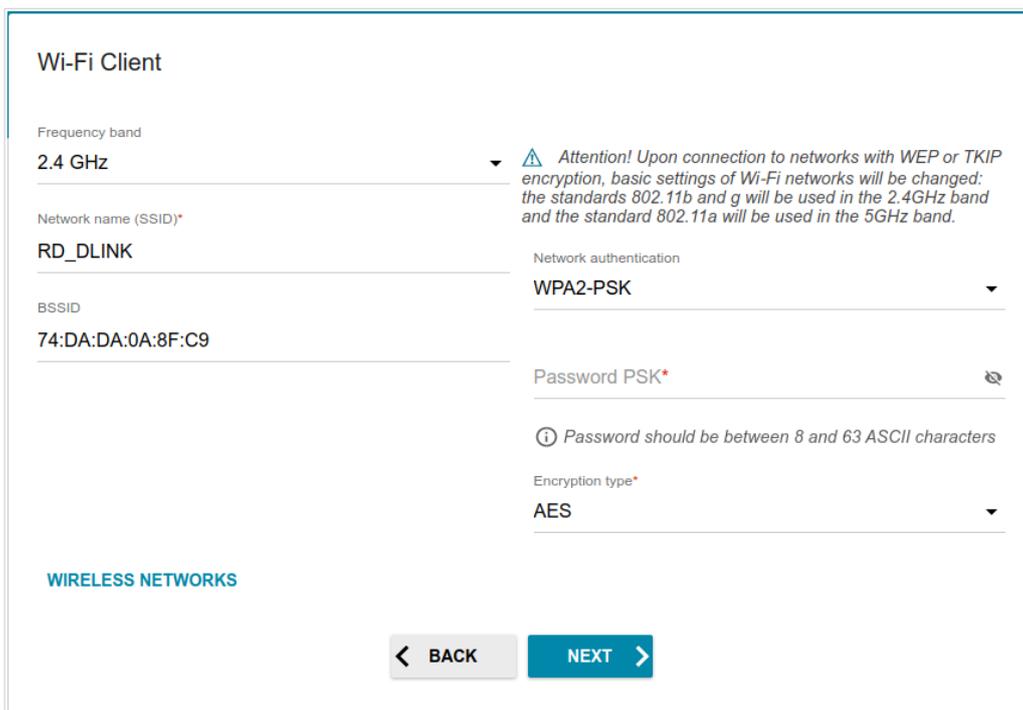


Figure 42. The page for configuring the Wi-Fi client.

If you connect to a hidden network, select the band where the hidden network operates from the **Frequency band** list and enter the network name in 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
<b>Enable encryption WEP</b>	<i>For <b>Open</b> authentication type only.</i> The checkbox activating WEP encryption. When the checkbox is selected, the <b>Default key ID</b> drop-down list, the <b>Encryption key WEP as HEX</b> checkbox, and four <b>Encryption key</b> fields are displayed on the page.
<b>Default key ID</b>	The number of the key (from first to fourth) which will be used for WEP encryption.

Parameter	Description
<b>Encryption key WEP as HEX</b>	Select the checkbox to set a hexadecimal number as a key for encryption.
<b>Encryption key (1-4)</b>	Keys for WEP encryption. The router uses the key selected from the <b>Default key ID</b> drop-down list. It is required to specify all the fields. Click the <b>Show</b> icon (👁) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK mixed**, **WPA3-SAE**, or **WPA2-PSK/WPA3-SAE mixed** authentication type is selected, the following fields are displayed:

Parameter	Description
<b>Password PSK</b>	A password for WPA encryption. Click the <b>Show</b> icon (👁) to display the entered password.
<b>Encryption type</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> . <i>TKIP and TKIP+AES encryption types are not available for WPA3-SAE and WPA2-PSK/WPA3-SAE mixed authentication types.</i>

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 for the **Router** mode only) 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 (available for the **Router** mode only).
4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field (available for the **Router** mode only).
5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

## Static IPv4 Connection

Internet connection type

Connection type  
Static IPv4

*i* A connection of this type allows you to use a fixed IP address provided by your ISP.

**SCAN** Network scan for connection type and parameters detection

IP address\*

Subnet mask\*

Gateway IP address\*

DNS IP address\*

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

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

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

Ping

**< BACK** **NEXT >**

Figure 43. 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

Internet connection type

Connection type  
Static IPv6

*ⓘ A connection of this type allows you to use a fixed IP address provided by your ISP.*

**SCAN** Network scan for connection type and parameters detection

IP address\*

Prefix\*

Gateway IP address\*

DNS IP 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.*

Ping

**< BACK** **NEXT >**

Figure 44. 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

The screenshot shows a configuration page titled "Internet connection type". At the top, there is a dropdown menu labeled "Connection type" with "PPPoE" selected. Below this is an information icon and a note: "A connection of this type requires a user name and password." There is a "SCAN" button with the text "Network scan for connection type and parameters detection". A checkbox labeled "Without authorization" is present. Below these are input fields for "Username\*" and "Password\*" (with a "Show" icon). A "Service name" field is also present. At the bottom, there are several checkboxes: "Clone MAC address of your device", "Use VLAN", and "Ping". Each of these has an information icon and a note: "In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet." and "Select the checkbox if the Internet access is provided via a VLAN channel." At the very bottom are "BACK" and "NEXT" buttons.

Figure 45. 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

The screenshot shows a web interface for configuring a WAN connection. The title is "Internet connection type". Below it, a dropdown menu is set to "PPPoE + Static IP (PPPoE Dual Access)". An information icon (i) is followed by the text: "A connection of this type requires a user name, password, and a fixed IP address provided by your ISP." There is a "SCAN" button with the text "Network scan for connection type and parameters detection" next to it. Below that is a checkbox labeled "Without authorization". The form contains several input fields: "Username\*", "Password\*" (with a show/hide icon), "Service name", "IP address\*", "Subnet mask\*", "Gateway IP address\*", and "DNS IP address\*".

Figure 46. 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

The screenshot shows a configuration page titled "Internet connection type". At the top, there is a dropdown menu for "Connection type" with "PPTP + Dynamic IP" selected. Below this is an information icon and a note: "PPTP and L2TP are methods for implementing virtual private networks." There is a "SCAN" button followed by the text "Network scan for connection type and parameters detection". A checkbox labeled "Without authorization" is present. Below these are three input fields: "Username\*", "Password\*" (with a "Show" icon), and "VPN server address\*". At the bottom, there are several checkboxes: "Clone MAC address of your device", "Use VLAN", "Use IGMP" (checked), and "Ping". Each checkbox has an associated information icon and a note. The "Use IGMP" note states: "Internet Group Management Protocol is designed to manage multicast traffic in IP-based networks." At the very bottom, there are "BACK" and "NEXT" navigation buttons.

Figure 47. 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

The screenshot shows a web interface for configuring a PPTP + Static IP WAN connection. The title is "Internet connection type". Below the title, there is a dropdown menu for "Connection type" with "PPTP + Static IP" selected. A help icon and text state: "PPTP and L2TP are methods for implementing virtual private networks." There is a "SCAN" button with the text "Network scan for connection type and parameters detection". Below that is a checkbox labeled "Without authorization". The form contains several text input fields, each with a red asterisk indicating it is required: "Username\*", "Password\*" (with a show/hide icon), "VPN server address\*", "IP address\*", "Subnet mask\*", "Gateway IP address\*", and "DNS IP address\*".

Figure 48. 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 in the 2.4GHz band 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.

Wireless Network 2.4 GHz

Enable

Broadcast wireless network 2.4 GHz

*Disabling broadcast does not influence the ability to connect to another Wi-Fi network as a client.*

Network name\*

my wi-fi

Open network

Password\*

.....

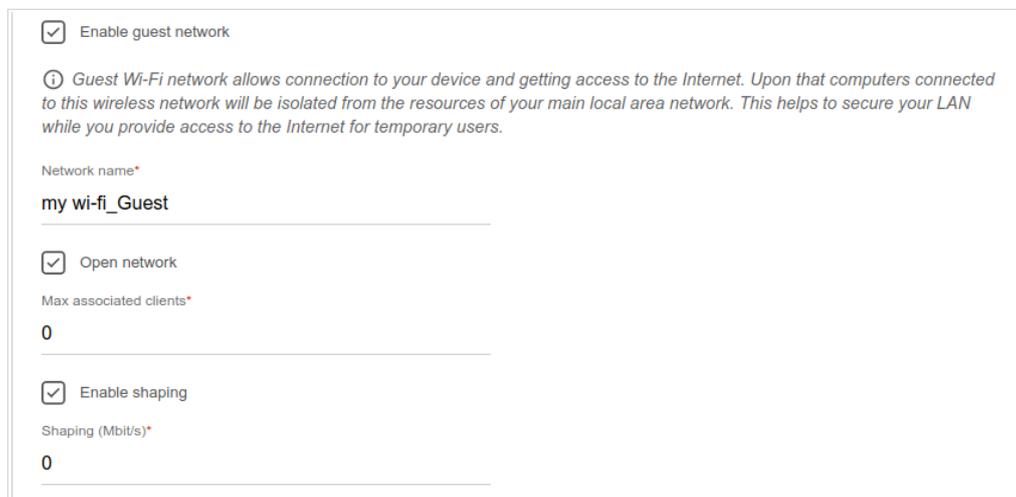
*Password should be between 8 and 63 ASCII characters*

**USE** *Use the same parameters as on the root access point.*

**RESTORE** *You can restore network name and security that was set before applying factory settings.*

Figure 49. The page for configuring the wireless network.

5. If you want to create an additional wireless network isolated from your LAN in the 2.4GHz band, select the **Enable guest network** checkbox (available for the **Router** and **WISP Repeater** modes only).



Enable guest network

ⓘ Guest Wi-Fi network allows connection to your device and getting access to the Internet. Upon that computers connected to this wireless network will be isolated from the resources of your main local area network. This helps to secure your LAN while you provide access to the Internet for temporary users.

Network name\*

my wi-fi\_Guest

Open network

Max associated clients\*

0

Enable shaping

Shaping (Mbit/s)\*

0

Figure 50. 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.
10. On the **Wireless Network 5 GHz** page, specify needed settings for the wireless network in the 5GHz band and click the **NEXT** button.

## 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.

IPTV

Is an STB connected to the device?

*ⓘ If your ISP provides IPTV service, you can connect an STB directly to the router without additional equipment*

Use VLAN ID

VLAN ID\*

*ⓘ Information about the VLAN ID can be found in the contract.*

LAN4 LAN3 LAN2 LAN1 WAN

Figure 51. 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.

VoIP

Is an IP phone connected to the device?

*ⓘ If your ISP provides VoIP service, you can connect an IP phone directly to the router without additional equipment*

Use VLAN ID

VLAN ID\*

*ⓘ Information about the VLAN ID can be found in the contract.*

LAN4 LAN3 LAN2 LAN1 WAN

[← BACK](#) [NEXT →](#)

Figure 52. 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.<sup>3</sup>

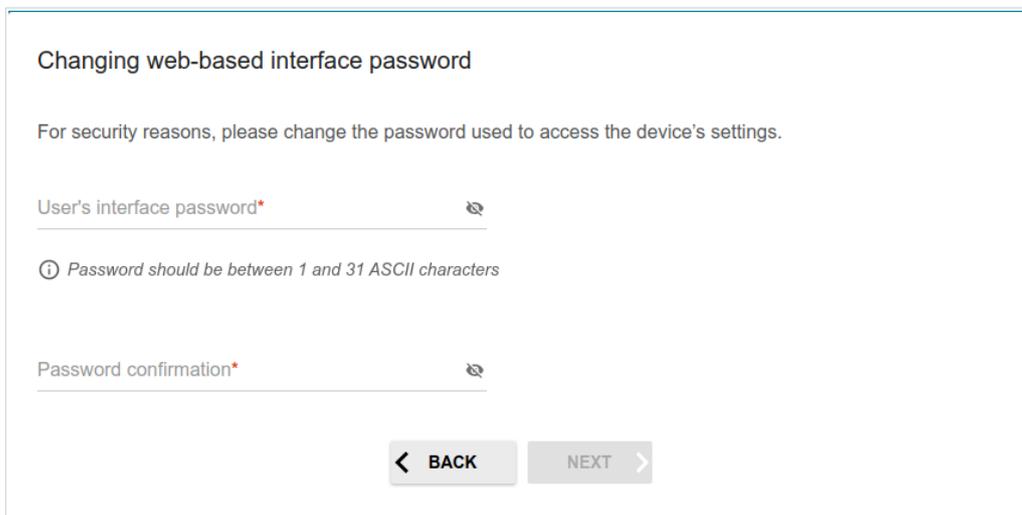


Figure 53. The page for changing the web-based interface password.



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 **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.

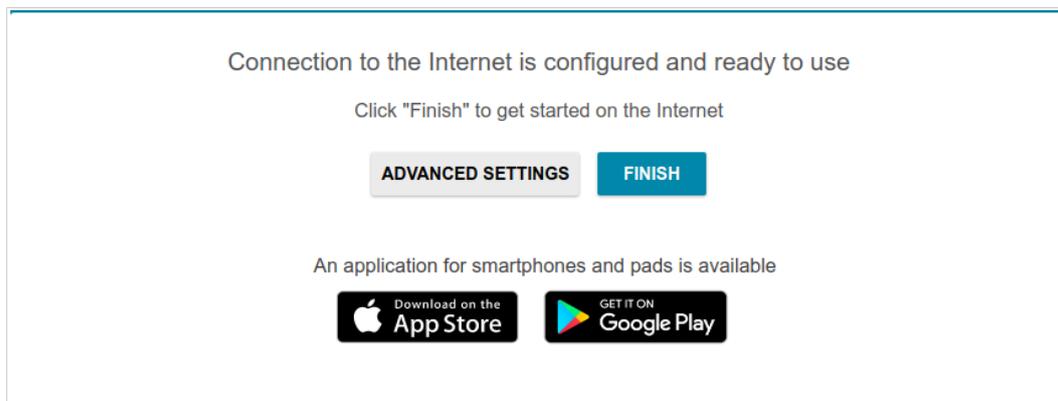
On the next page, check all specified settings.

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.

<sup>3</sup> 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 54. 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 (the phone number will be displayed on the page after several attempts of checking the connection).

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 41).

## Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports of the router for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DIR-822 in order to use these devices.

To start the Wizard, on the **Home** page, select the **Connection of Multimedia Devices** section. If you need to select a port in order to use an additional device, left-click the relevant element in the **LAN** section (the selected element will be marked with a frame). Then click the **APPLY** button.

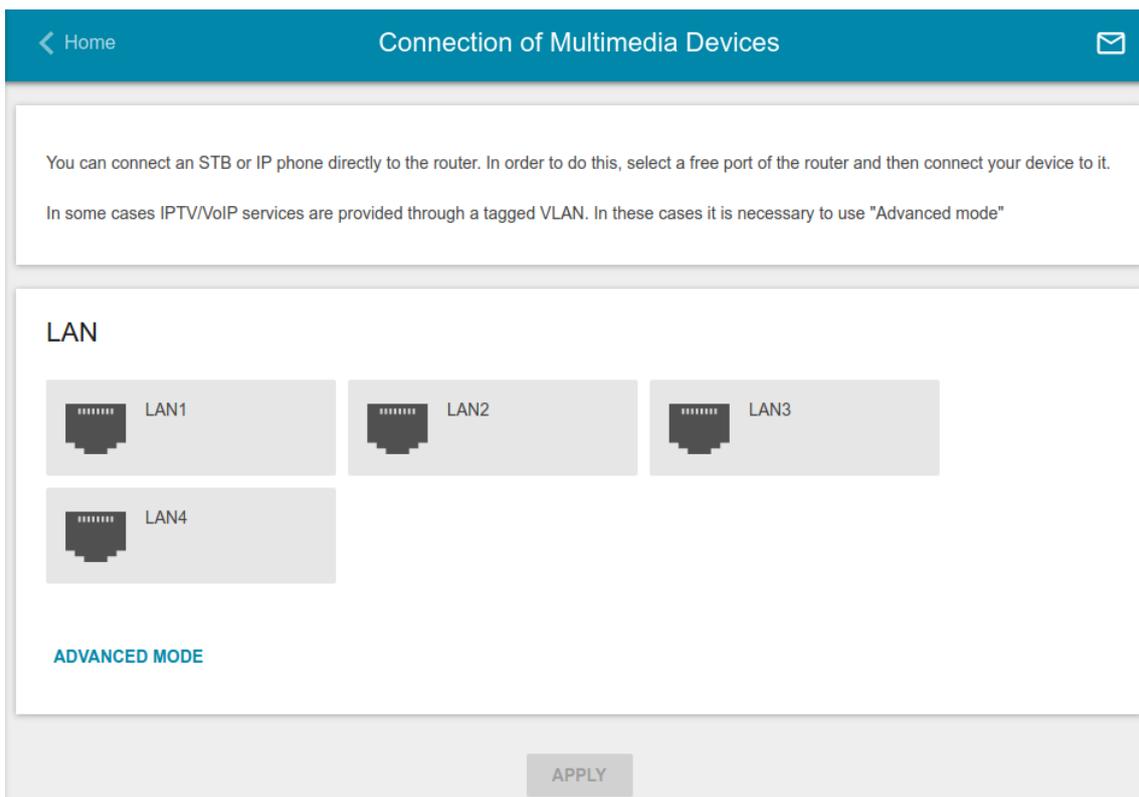


Figure 55. The Multimedia Devices Connection Wizard. The simplified mode.

If you need to configure a connection via VLAN, click the **ADVANCED MODE** button.

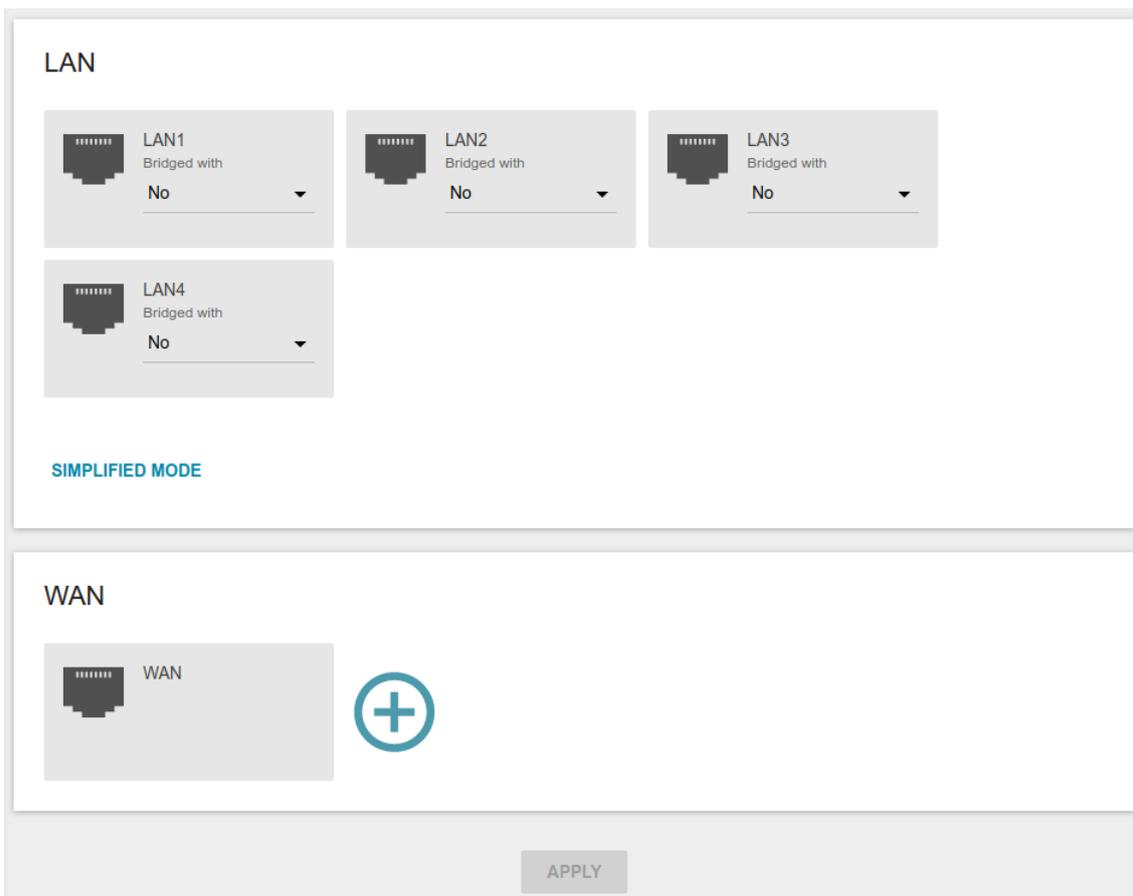


Figure 56. The Multimedia Devices Connection Wizard. The advanced mode.

In the **WAN** section, click the **Add** icon (  ).

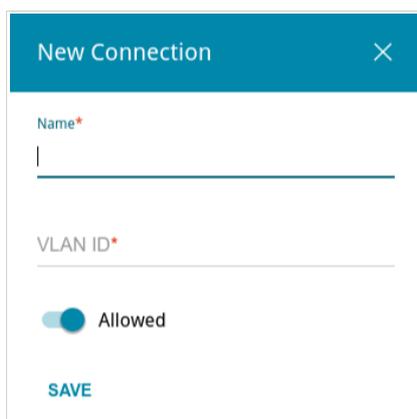


Figure 57. Adding a connection.

In the opened window, specify a name of the connection for easier identification in the **Name** field (you can specify any name). Specify the VLAN ID provided by your ISP and click the **SAVE** button.

Then in the **LAN** section, from the **Bridged with** drop-down list of the element corresponding to the LAN port to which the additional device is connected, select the created connection. Click the **APPLY** button.



The selected port cannot use the default connection to access the Internet.

To deselect the port in the simplified mode, left-click the selected element (the frame will disappear) and click the **APPLY** button.

To deselect the port in the advanced mode, select the **No** value from the **Bridged with** drop-down list of the element corresponding to the needed LAN port. Then in the **WAN** section, select the connection via VLAN which will not be used any longer and click the **DELETE** button. Then click the **APPLY** button.

## Statistics

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

- network statistics
- IP addresses leased by the DHCP server
- the routing rules and routing tables
- data on devices connected to the router's network and its web-based interface, and information on current sessions of these devices
- statistics for traffic passing through ports of the router
- addresses of active multicast groups
- statistics for IPsec connections.

### Network Statistics

On the **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).

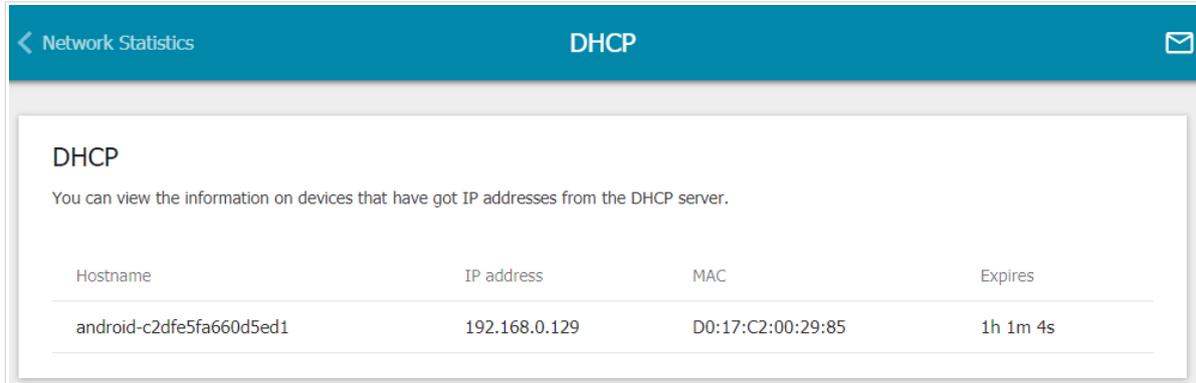
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 – 192.168.0.1	3.54 Mbyte / 31.22 Mbyte	0 / 0	-
statip_93	IPv4: 192.168.161.189/24 – 192.168.161.1	71.30 Mbyte / 96.19 Mbyte	0 / 0	22 h., 19 min
WIFI_2.4GHZ	-	408.27 Kbyte / 655.96 Kbyte	1 / 0	-
WIFI_5GHZ	-	- / -	0 / 0	-

Figure 58. The **Statistics / Network Statistics** page.

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

## DHCP

The **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.

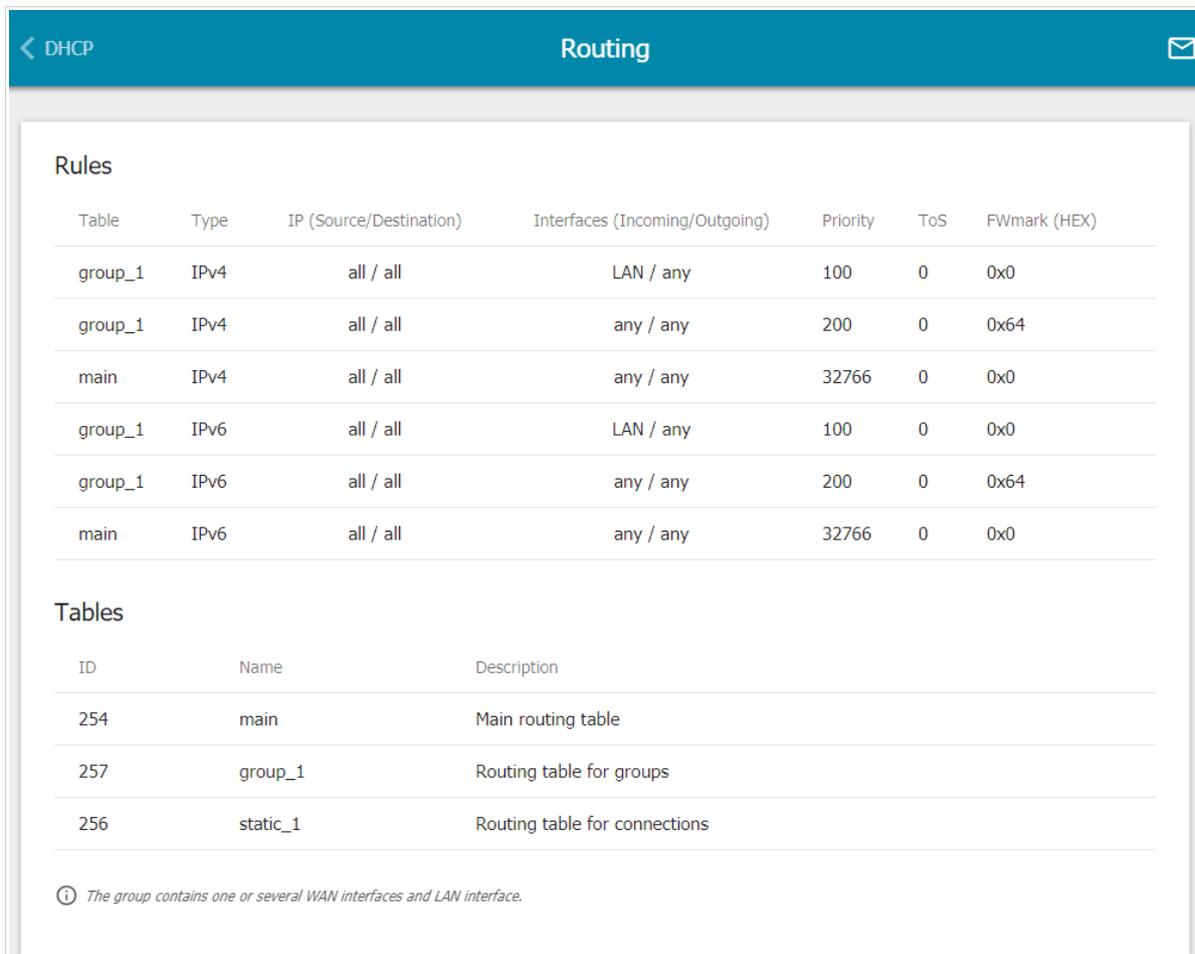


Hostname	IP address	MAC	Expires
android-c2dfe5fa660d5ed1	192.168.0.129	D0:17:C2:00:29:85	1h 1m 4s

Figure 59. The **Statistics / DHCP** page.

## Routing

The **Statistics / Routing** page displays the routing rules and routing tables.



**Rules**

Table	Type	IP (Source/Destination)	Interfaces (Incoming/Outgoing)	Priority	ToS	FWmark (HEX)
group_1	IPv4	all / all	LAN / any	100	0	0x0
group_1	IPv4	all / all	any / any	200	0	0x64
main	IPv4	all / all	any / any	32766	0	0x0
group_1	IPv6	all / all	LAN / any	100	0	0x0
group_1	IPv6	all / all	any / any	200	0	0x64
main	IPv6	all / all	any / any	32766	0	0x0

**Tables**

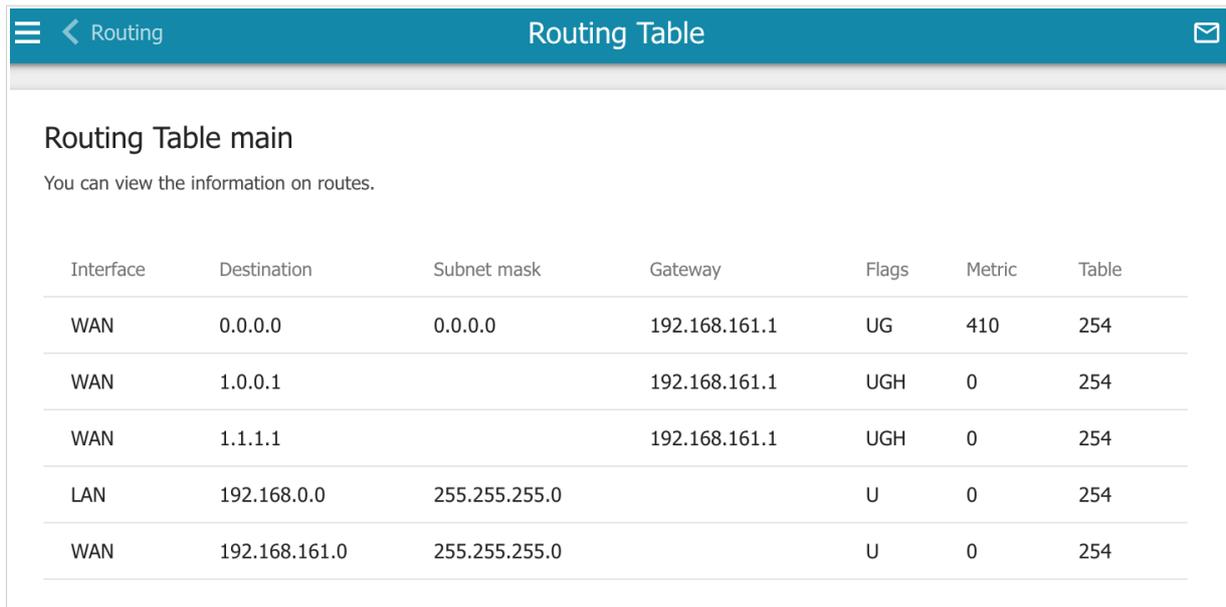
ID	Name	Description
254	main	Main routing table
257	group_1	Routing table for groups
256	static_1	Routing table for connections

ⓘ The group contains one or several WAN interfaces and LAN interface.

Figure 60. The **Statistics / Routing** page.

The **Rules** section displays routing rules, their corresponding routing tables, incoming and outgoing interfaces, priority levels, and other data.

The **Tables** section displays the list of routing tables stored in the device's memory. To view detailed information on routes, left-click the relevant line in the table.



**Routing Table main**  
You can view the information on routes.

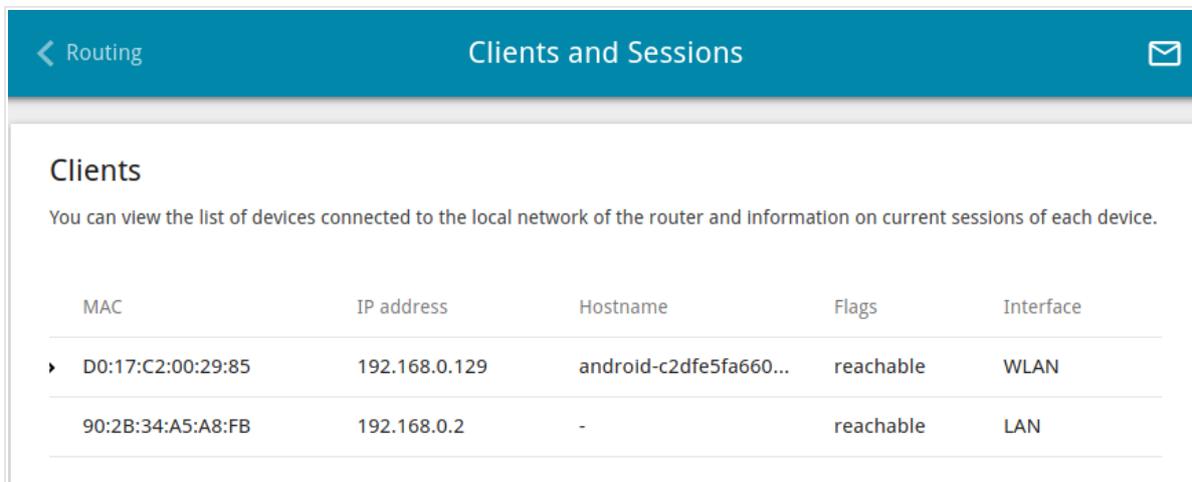
Interface	Destination	Subnet mask	Gateway	Flags	Metric	Table
WAN	0.0.0.0	0.0.0.0	192.168.161.1	UG	410	254
WAN	1.0.0.1		192.168.161.1	UGH	0	254
WAN	1.1.1.1		192.168.161.1	UGH	0	254
LAN	192.168.0.0	255.255.255.0		U	0	254
WAN	192.168.161.0	255.255.255.0		U	0	254

Figure 61. The routing table page.

The opened page displays the information on routes in the selected routing table. The table contains destination IP addresses, gateways, subnet masks, and other data.

## Clients and Sessions

On the **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.



MAC	IP address	Hostname	Flags	Interface
▶ D0:17:C2:00:29:85	192.168.0.129	android-c2dfe5fa660...	reachable	WLAN
90:2B:34:A5:A8:FB	192.168.0.2	-	reachable	LAN

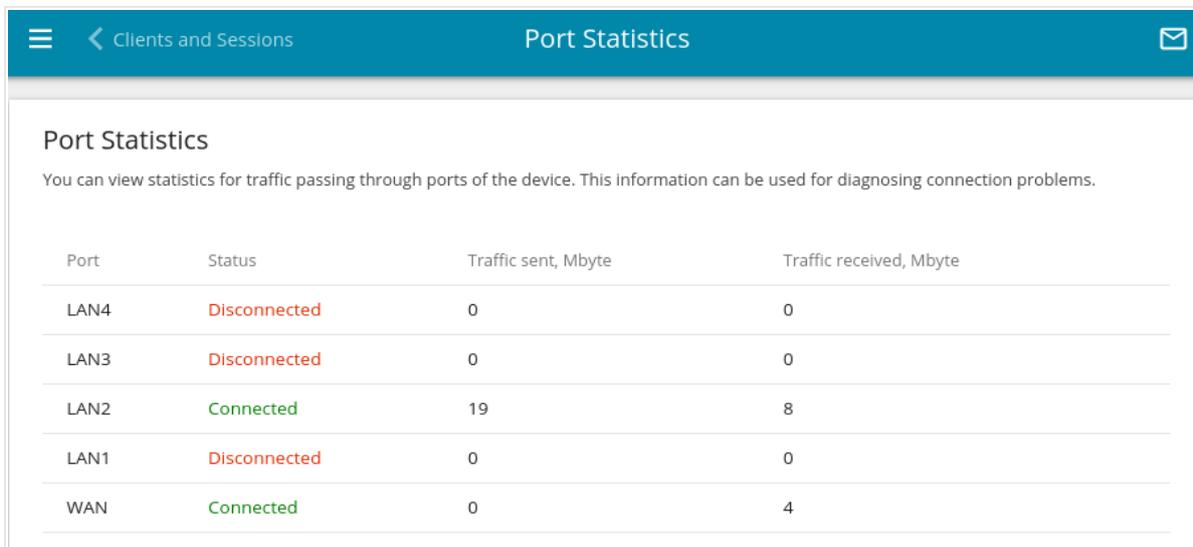
Figure 62. The **Statistics / Clients and Sessions** page.

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.

## Port Statistics

On the **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.



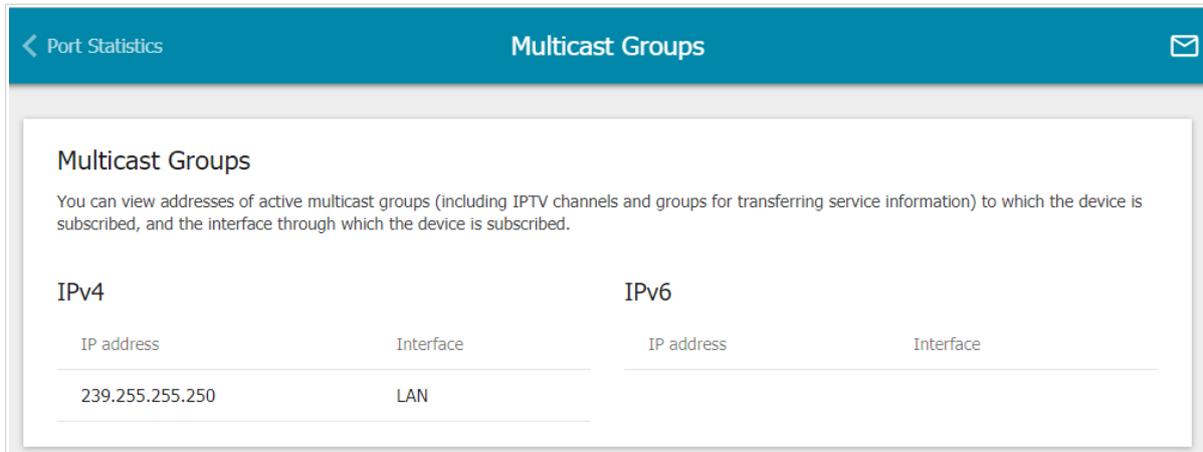
Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte
LAN4	Disconnected	0	0
LAN3	Disconnected	0	0
LAN2	Connected	19	8
LAN1	Disconnected	0	0
WAN	Connected	0	4

Figure 63. The **Statistics / Port Statistics** page.

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

## Multicast Groups

The **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.



IPv4		IPv6	
IP address	Interface	IP address	Interface
239.255.255.250	LAN		

Figure 64. The **Statistics / Multicast Groups** page.

## IPsec Statistics

On the **Statistics / IPsec Statistics** page, you can view statistics for IPsec tunnels of the router. For each tunnel 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), remote host address or domain name, connection type, and number of packets and volume of data received and transmitted.



The screenshot shows a web interface for 'IPsec Statistics'. The page has a teal header with a menu icon, a back arrow, and the text 'Multicast Groups'. The main content area is titled 'IPsec Statistics' and includes a sub-header 'IPsec Statistics' and a note: 'You can view statistics for IPsec connections.' Below this is a table with the following data:

Name	Remote host	Packets sent / Packets received	Traffic sent / Traffic received	Connection type
ipsec_52	192.168.161.189	- / -	- / -	IPv4

Figure 65. The **Statistics / IPsec Statistics** page.

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

## Connections Setup

In this menu you can configure basic parameters of the router's local area network and configure connection to the Internet (a WAN connection).

### WAN

On the **Connections Setup / 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.

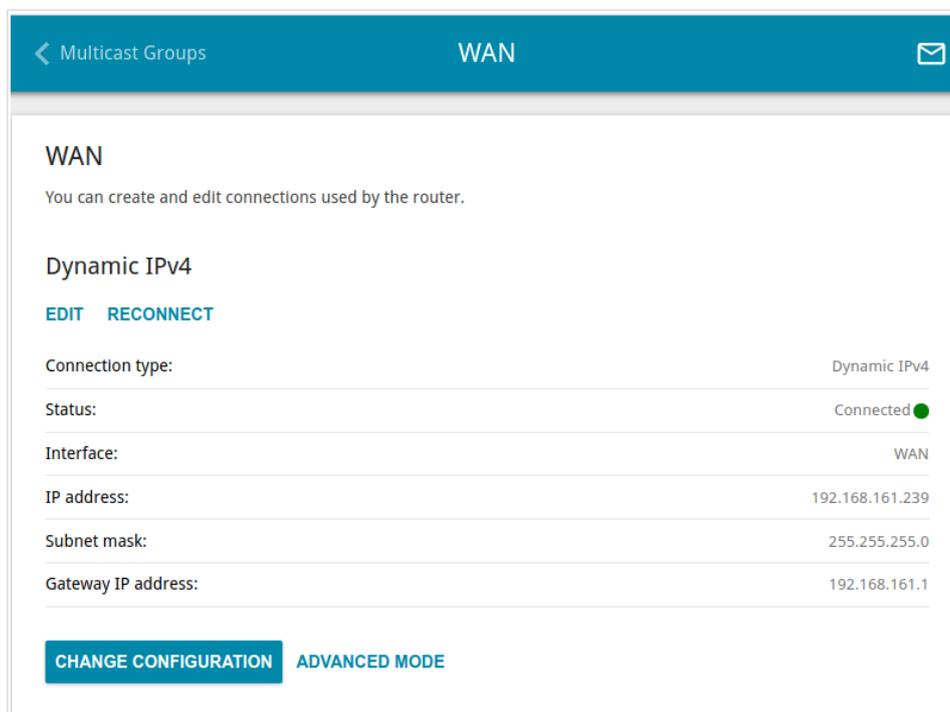


Figure 66. The **Connections Setup / WAN** page. The simplified mode.

To edit an existing connection, click the **EDIT** button. On the opened page, 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 **Connections Setup / WAN** page is automatically displayed in the advanced mode.

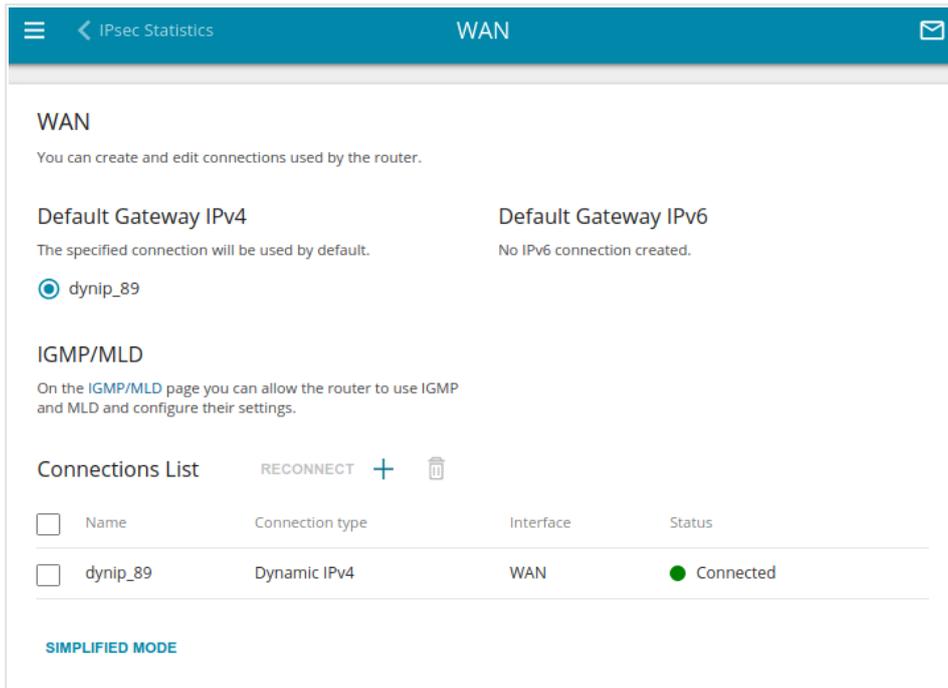


Figure 67. The **Connections Setup / WAN** page. The advanced mode.

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. On the opened page, 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/MLD** link (for the description of the page, see the **IGMP/MLD** section, page 166).

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.

The screenshot shows the 'General Settings' section of a web interface. It contains the following elements:

- Connection type:** A dropdown menu with 'Static IPv4' selected.
- Interface:** A dropdown menu with 'WAN' selected.
- Connection name\*:** A text input field containing 'statip'.
- Enable connection:** A toggle switch that is turned on (blue).
- NAT:** A toggle switch that is turned on (blue). Below it is a note: 'The network address translation function. It is recommended not to disable unless your ISP requires it.'
- Ping:** A toggle switch that is turned off (grey).
- RIP:** A toggle switch that is turned off (grey). Below it is a note: 'WAN Ping Respond allows the device to respond to ping requests from the external network.'

Figure 68. The page for creating a new **Static IPv4** connection. The **General Settings** section.

Parameter	Description
<b>General Settings</b>	
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	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.
<b>Ping</b>	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.
<b>RIP</b>	Move the switch to the right to allow using RIP for this connection.

**Ethernet**

MAC address\*

BC:0F:9A:6D:36:4C

---

Clone MAC address of your NIC  
(90:2B:34:A5:A8:FB)

**RESTORE DEFAULT MAC ADDRESS**

MTU\*

1500

Figure 69. The page for creating a new **Static IPv4** connection. The **Ethernet** section.

Parameter	Description
<b>Ethernet</b>	
<b>MAC address</b>	<p>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.</p> <p>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 <b>Clone MAC address of your NIC</b> switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the router's MAC address, click the <b>RESTORE DEFAULT MAC ADDRESS</b> button (the button is available when the switch is moved to the right).</p>
<b>MTU</b>	The maximum size of units transmitted by the interface.

**IPv4**

IP address\*  
192.168.161.224

---

Subnet mask\*  
255.255.255.0

---

Gateway IP address\*  
192.168.161.1

---

Primary DNS\*  
1.1.1.1

---

Secondary DNS  
1.0.0.1

---

ⓘ If the connection is created for the IPTV service only and no data on IP addressing is given by your ISP, then you can set the following values: IP address = 1.0.0.1, Netmask = 255.255.255.252, Gateway IP address = 1.0.0.2, Primary DNS server = 1.0.0.2

Figure 70. The page for creating a new **Static IPv4** connection. The **IPv4** section.

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

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.

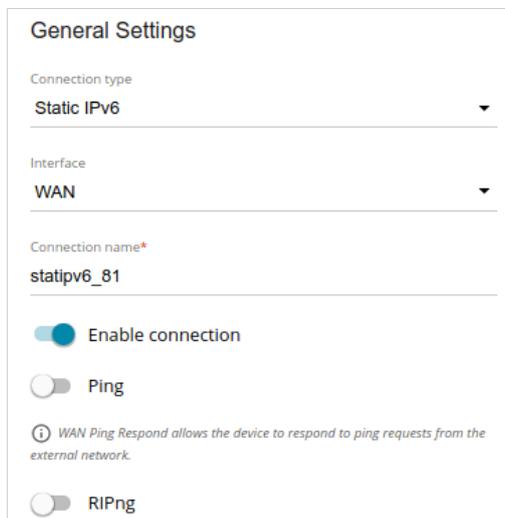


Figure 71. The page for creating a new **Static IPv6** connection. The **General Settings** section.

Parameter	Description
<b>General Settings</b>	
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>Ping</b>	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.
<b>RIPng</b>	Move the switch to the right to allow using RIPng for this connection.

**Ethernet**

MAC address\*

BC:0F:9A:6D:36:4C

---

Clone MAC address of your NIC  
(90:2B:34:A5:A8:FB)

**RESTORE DEFAULT MAC ADDRESS**

MTU\*

1500

Figure 72. The page for creating a new **Static IPv6** connection. The **Ethernet** section.

Parameter	Description
<b>Ethernet</b>	
<b>MAC address</b>	<p>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.</p> <p>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 <b>Clone MAC address of your NIC</b> switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the router's MAC address, click the <b>RESTORE DEFAULT MAC ADDRESS</b> button (the button is available when the switch is moved to the right).</p>
<b>MTU</b>	The maximum size of units transmitted by the interface.

**IPv6**

IPv6 address\*

---

Prefix\*

---

Gateway IPv6 address\*

---

Primary IPv6 DNS server\*

---

Secondary IPv6 DNS server

---

Figure 73. The page for creating a new **Static IPv6** connection. The **IPv6** section.

Parameter	Description
<b>IPv6</b>	
<i>For Static IPv6 type</i>	
<b>IPv6 address</b>	Enter an IPv6 address for this WAN connection.
<b>Prefix</b>	The length of the subnet prefix. The value <b>64</b> is used usually.
<b>Gateway IPv6 address</b>	Enter an IPv6 address of the gateway used by this WAN connection.
<b>Primary IPv6 DNS server / Secondary IPv6 DNS server</b>	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
<i>For Dynamic IPv6 type</i>	
<b>Get IPv6</b>	Select a method for IPv6 address assignment from the drop-down list or leave the <b>Automatically</b> value.
<b>Enable prefix delegation</b>	Move the switch to the right if it is necessary that the router requests a prefix to configure IPv6 addresses for the local network from a delegating router.
<b>Obtain DNS server addresses automatically</b>	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the <b>Primary IPv6 DNS server</b> and <b>Secondary IPv6 DNS server</b> fields are not available for editing.
<b>Primary IPv6 DNS server / Secondary IPv6 DNS server</b>	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.

The screenshot shows the 'General Settings' section of a web interface. It contains the following elements:

- Connection type:** A dropdown menu with 'PPPoE' selected.
- Interface:** A dropdown menu with 'WAN' selected.
- Connection name\*:** A text input field containing 'pppoe'.
- Enable connection:** A toggle switch that is turned on (blue).
- NAT:** A toggle switch that is turned on (blue). Below it is an information icon and text: 'The network address translation function. It is recommended not to disable unless your ISP requires it.'
- Ping:** A toggle switch that is turned off (grey).
- RIP:** A toggle switch that is turned off (grey). Below it is an information icon and text: 'WAN Ping Respond allows the device to respond to ping requests from the external network.'

Figure 74. The page for creating a new PPPoE connection. The **General Settings** section.

Parameter	Description
<b>General Settings</b>	
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	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.
<b>Ping</b>	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.
<b>RIP</b>	Move the switch to the right to allow using RIP for this connection.

**Ethernet**

MAC address\*

BC:0F:9A:6D:36:4C

---

Clone MAC address of your NIC  
 (90:2B:34:A5:A8:FB)

**RESTORE DEFAULT MAC ADDRESS**

MTU\*

1500

Figure 75. The page for creating a new PPPoE connection. The **Ethernet** section.

Parameter	Description
<b>Ethernet</b>	
<b>MAC address</b>	<p>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.</p> <p>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 <b>Clone MAC address of your NIC</b> switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the router's MAC address, click the <b>RESTORE DEFAULT MAC ADDRESS</b> button (the button is available when the switch is moved to the right).</p>
<b>MTU</b>	The maximum size of units transmitted by the interface.

**PPP**

Without authorization

Username\*

---

Password\* 🔍

---

Service name

---

MTU\*

1492

---

Encryption protocol

No encryption ▼

---

Authentication protocol

AUTO ▼

---

Keep Alive

LCP interval\*

30

---

LCP fails\*

3

---

Dial on demand

Maximum idle time (in seconds) 🔒

---

Static IP address

---

PPP debug

Figure 76. The page for creating a new **PPPoE** connection. The **PPP** section.

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

Parameter	Description
<b>Encryption protocol</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encryption</b>: MPPE encryption is not applied.</li> <li>• <b>MPPE 40 128 bit</b>: MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit</b>: MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit</b>: MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MS-CHAP</b>, <b>MS-CHAPV2</b>, or <b>AUTO</b> value is selected from the <b>Authentication protocol</b> drop-down list.</p>
<b>Authentication protocol</b>	<p>Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.</p>
<b>Keep Alive</b>	<p>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 <b>LCP interval</b> and <b>LCP fails</b> fields are available. Specify the required values.</p>
<b>Dial on demand</b>	<p>Move the switch to the right if you want the router to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.</p>
<b>Static IP address</b>	<p>Fill in the field if you want to use a static IP address to access the Internet.</p>
<b>PPP debug</b>	<p>Move the switch to the right if you want to log all data on PPP connection debugging.</p>

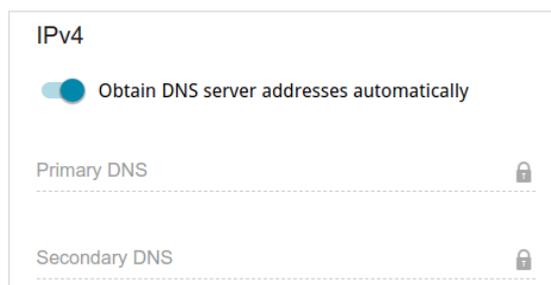


Figure 77. The page for creating a new **PPPoE** connection. The **IPv4** section.

Parameter	Description
<b>Obtain DNS server addresses automatically</b>	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the <b>Primary DNS</b> and <b>Secondary DNS</b> fields are not available for editing.
<b>Primary DNS / Secondary DNS</b>	Enter addresses of the primary and secondary DNS servers in the relevant fields.

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 **Connections Setup / WAN** page opens.

## Creating PPTP, L2TP, or L2TP over IPsec 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.

The screenshot shows the 'General Settings' section of a web interface. It includes a dropdown menu for 'Connection type' with 'PPTP' selected. Below it is a text input field for 'Connection name\*' containing 'pptp'. There are three toggle switches: 'Enable connection' (checked), 'NAT' (checked), and 'Ping' (unchecked). Informational icons and text are present for the NAT and Ping options.

Figure 78. The page for creating a new PPTP connection. The **General Settings** section.

Parameter	Description
<b>General Settings</b>	
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	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.
<b>Ping</b>	<i>For the PPTP and L2TP types only.</i> 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.

**PPP**

Without authorization

Username\*

Password\* 

VPN server address\*

MTU\*  
1456

Encryption protocol  
No encryption ▼

Authentication protocol  
AUTO ▼

Keep Alive

LCP interval\*  
30

LCP fails\*  
3

Dial on demand

Maximum idle time (in seconds) 

Static IP address

PPP debug

Figure 79. The page for creating a new PPTP connection. The PPP section.

Parameter	Description
<b>PPP</b>	
<b>Without authorization</b>	Move the switch to the right if you don't need to enter a username and password to access the Internet.
<b>Username</b>	A username (login) to access the Internet.
<b>Password</b>	A password to access the Internet. Click the <b>Show</b> icon (  ) to display the entered password.
<b>VPN server address</b>	The IP or URL address of the PPTP or L2TP authentication server.
<b>MTU</b>	The maximum size of units transmitted by the interface.

Parameter	Description
<b>Encryption protocol</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encryption</b>: MPPE encryption is not applied.</li> <li>• <b>MPPE 40 128 bit</b>: MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit</b>: MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit</b>: MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MS-CHAP</b>, <b>MS-CHAPV2</b>, or <b>AUTO</b> value is selected from the <b>Authentication protocol</b> drop-down list.</p>
<b>Authentication protocol</b>	<p>Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.</p>
<b>Keep Alive</b>	<p>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 <b>LCP interval</b> and <b>LCP fails</b> fields are available. Specify the required values.</p>
<b>Dial on demand</b>	<p>Move the switch to the right if you want the router to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.</p>
<b>Static IP address</b>	<p>Fill in the field if you want to use a static IP address to access the Internet.</p>
<b>PPP debug</b>	<p>Move the switch to the right if you want to log all data on PPP connection debugging.</p>

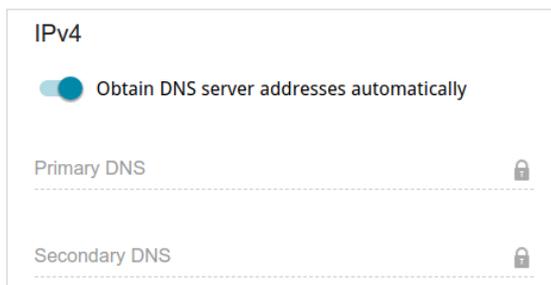


Figure 80. The page for creating a new **PPTP** connection. The **IPv4** section.

Parameter	Description
<b>Obtain DNS server addresses automatically</b>	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the <b>Primary DNS</b> and <b>Secondary DNS</b> fields are not available for editing.
<b>Primary DNS / Secondary DNS</b>	Enter addresses of the primary and secondary DNS servers in the relevant fields.

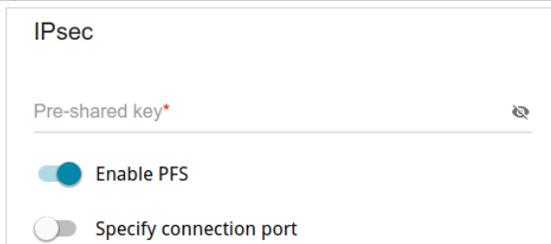


Figure 81. The page for creating a new **L2TP over IPsec** connection. The **IPsec** section.

**!** Setting for both parties which establish the tunnel should be the same.

Parameter	Description
<b>IPsec (for the L2TP over IPsec type)</b>	
<b>Pre-shared key</b>	A key for mutual authentication of the parties. Click the <b>Show</b> icon (  ) to display the entered key.
<b>Enable PFS</b>	Move the switch to the right to enable the PFS option ( <i>Perfect Forward Secrecy</i> ). If the switch is moved to the right, a new encryption key exchange will be used upon establishing the IPsec tunnel. This option enhances the security level of data transfer, but increases the load on DIR-822.
<b>Specify connection port</b>	Move the switch to the right to change the port used for data exchange with the other party enter the needed value in the <b>Port</b> filed displayed. By default, the value <b>1701</b> is specified.

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.

After creating a connection of the L2TP over IPsec type, on the **Advanced / IPsec** page, in the **Status** section, the current state of the IPsec tunnel is displayed.

## 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.

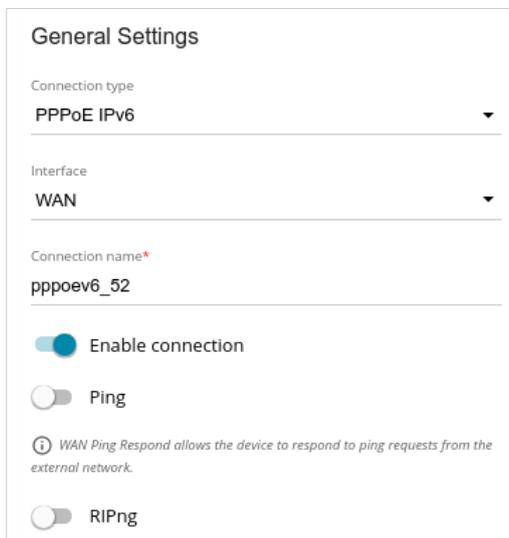


Figure 82. The page for creating a new **PPPoE IPv6** connection. The **General Settings** section.

Parameter	Description
<b>General Settings</b>	
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	<i>For the <b>PPPoE Dual Stack</b> type only.</i> If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
<b>Ping</b>	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.
<b>RIP</b>	<i>For the <b>PPPoE Dual Stack</b> type only.</i> Move the switch to the right to allow using RIP for this connection.
<b>RIPng</b>	Move the switch to the right to allow using RIPng for this connection.

**Ethernet**

MAC address\*

BC:0F:9A:6D:36:4C

---

Clone MAC address of your NIC  
 (90:2B:34:A5:A8:FB)

**RESTORE DEFAULT MAC ADDRESS**

MTU\*

1500

Figure 83. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.

Parameter	Description
<b>Ethernet</b>	
<b>MAC address</b>	<p>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.</p> <p>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 <b>Clone MAC address of your NIC</b> switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the router's MAC address, click the <b>RESTORE DEFAULT MAC ADDRESS</b> button (the button is available when the switch is moved to the right).</p>
<b>MTU</b>	The maximum size of units transmitted by the interface.

**PPP**

Without authorization

---

Username\*

---

Password\* 🔍

---

Service name

---

MTU\*

1492

---

Encryption protocol

No encryption ▼

---

Authentication protocol

AUTO ▼

---

Keep Alive

LCP interval\*

30

---

LCP fails\*

3

---

Static IP address

---

PPP debug

Figure 84. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.

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

Parameter	Description
<b>Encryption protocol</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encryption:</b> MPPE encryption is not applied.</li> <li>• <b>MPPE 40 128 bit:</b> MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit:</b> MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit:</b> MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MS-CHAP</b>, <b>MS-CHAPV2</b>, or <b>AUTO</b> value is selected from the <b>Authentication protocol</b> drop-down list.</p>
<b>Authentication protocol</b>	<p>Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.</p>
<b>Keep Alive</b>	<p>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 <b>LCP interval</b> and <b>LCP fails</b> fields are available. Specify the required values.</p>
<b>Static IP address</b>	<p>Fill in the field if you want to use a static IP address to access the Internet.</p>
<b>PPP debug</b>	<p>Move the switch to the right if you want to log all data on PPP connection debugging.</p>

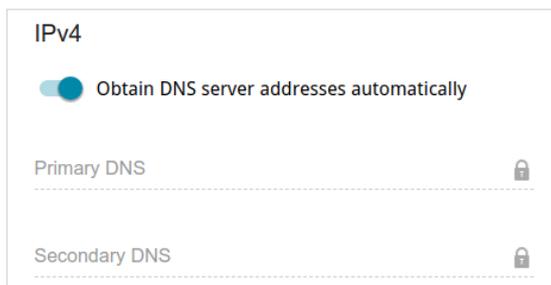


Figure 85. The page for creating a new PPPoE Dual Stack connection. The IPv4 section.

Parameter	Description
<b>IPv4 (for the PPPoE Dual Stack type)</b>	
<b>Obtain DNS server addresses automatically</b>	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the <b>Primary DNS</b> and <b>Secondary DNS</b> fields are not available for editing.
<b>Primary DNS / Secondary DNS</b>	Enter addresses of the primary and secondary DNS servers in the relevant fields.

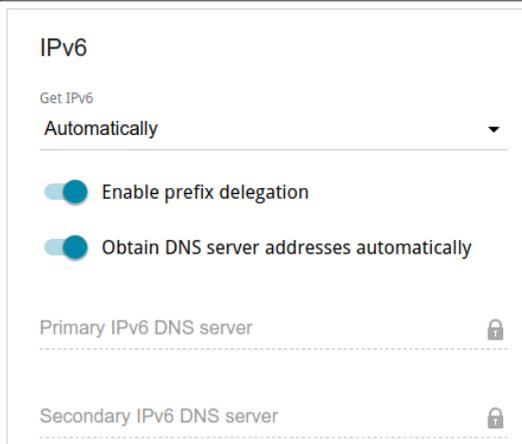


Figure 86. The page for creating a new PPPoE Pv6 connection. The IPv6 section.

Parameter	Description
<b>IPv6</b>	
<b>Get IPv6</b>	Select a method for IPv6 address assignment from the drop-down list or leave the <b>Automatically</b> value.
<b>Enable prefix delegation</b>	Move the switch to the right if it is necessary that the router requests a prefix to configure IPv6 addresses for the local network from a delegating router.
<b>Obtain DNS server addresses automatically</b>	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the <b>Primary IPv6 DNS server</b> and <b>Secondary IPv6 DNS server</b> fields are not available for editing.

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

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

## LAN

To configure the router's local interface, go to the **Connections Setup / LAN** page.

### IPv4

Go to the **IPv4** tab to change the IPv4 address of the router, configure the built-in DHCP server, specify MAC address and IPv4 address pairs, or add own DNS records.

Local IP Address

IP address\*  
192.168.0.1

---

Mask\*  
255.255.255.0

---

Hostname  
dlinkrouter.local

---

ⓘ 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 87. Configuring the local interface. The **IPv4** tab. The **Local IP Address** section.

Parameter	Description
<b>Local IP Address</b>	
<b>Mode of local IP address assignment</b>	<p>Available if the <b>Access point</b>, <b>Repeater</b>, or <b>Client</b> mode was selected in the <i>Initial Configuration Wizard</i>.</p> <p>Select the needed value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Static</b>: The IPv4 address, subnet mask, and the gateway IP address are assigned manually.</li> <li>• <b>Dynamic</b>: The router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.</li> </ul>
<b>IP address</b>	The IPv4 address of the router in the local subnet. By default, the following value is specified: <b>192.168.0.1</b> .
<b>Mask</b>	The mask of the local subnet. By default, the following value is specified: <b>255.255.255.0</b> .

Parameter	Description
<b>Gateway IP address</b>	Available if the <b>Access point, Repeater, or Client</b> mode was selected in the <i>Initial Configuration Wizard</i> . 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). <i>Optional</i> .
<b>Hostname</b>	The name of the device assigned to its IPv4 address in the local subnet.

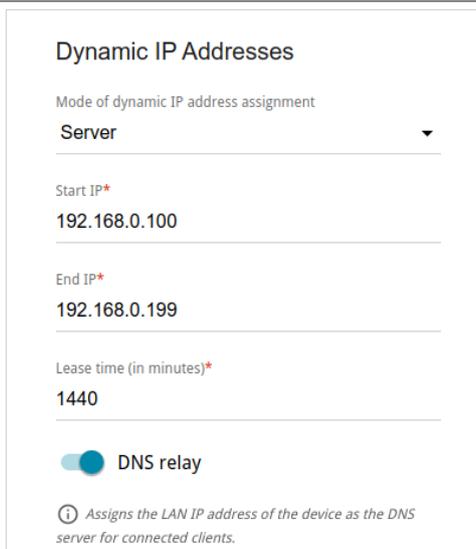


Figure 88. Configuring the local interface. The IPv4 tab. The Dynamic IP Addresses section.

Parameter	Description
<b>Dynamic IP Addresses</b>	
<b>Mode of dynamic IP address assignment</b>	An operating mode of the router's DHCP server. <ul style="list-style-type: none"> <li>• <b>Disable</b>: The router's DHCP server is disabled, clients' IP addresses are assigned manually.</li> <li>• <b>Server</b>: The router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the <b>Start IP</b>, <b>End IP</b>, <b>Lease time</b> fields and the <b>DNS relay</b> switch are displayed on the tab. Also when this value is selected, the <b>DHCP Options</b>, <b>Static IP Addresses</b>, and <b>Hosts</b> sections are displayed on the tab.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>Relay</b>: An external DHCP server is used to assign IP addresses to clients. When this value is selected, the <b>External DHCP server IP</b>, <b>Option 82 Circuit ID</b>, <b>Option 82 Remote ID</b>, and <b>Option 82 Subscriber ID</b> fields are displayed on the tab. <i>Available if the <b>Router</b> or <b>WISP Repeater</b> mode was selected in the Initial Configuration Wizard.</i></li> </ul>
<b>Start IP</b>	The start IP address of the address range used by the DHCP server to distribute IP addresses to clients.
<b>End IP</b>	The end IP address of the address range used by the DHCP server to distribute IP addresses to clients.
<b>Lease time</b>	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.
<b>DNS relay</b>	<p>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.</p> <p>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 <b>Advanced / DNS</b> page as the DNS server address.</p>
<b>External DHCP server IP</b>	The IP address of the external DHCP server which assigns IP addresses to the router's clients.
<b>Option 82 Circuit ID</b> <b>Option 82 Remote ID</b> <b>Option 82 Subscriber ID</b>	The value of the relevant field of DHCP option 82. Do not fill in the fields unless your ISP or the administrator of the external DHCP server provided these values.

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 89. Configuring the local interface. The IPv4 tab. The section for configuring DHCP options.

To do this, click the **ADD** button (  ).

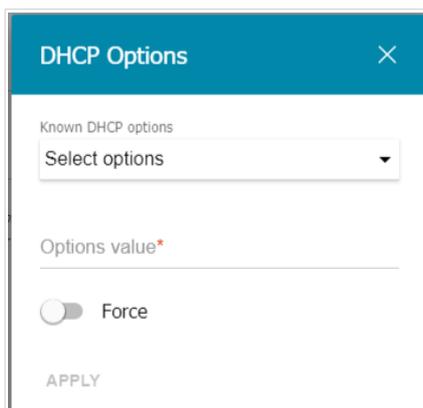


Figure 90. Configuring the local interface. The IPv4 tab. The window for configuring a DHCP option.

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

Parameter	Description
<b>Known DHCP options</b>	From the drop-down list, select an option which you want to configure.
<b>Options value</b>	Specify the value for the selected option.
<b>Force</b>	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.

If needed, you can add your own address resource records. To do this, click the **ADD** button (  ) in the **Hosts** section (available if the **Router** or **WISP Repeater** mode was selected in the *Initial Configuration Wizard*).

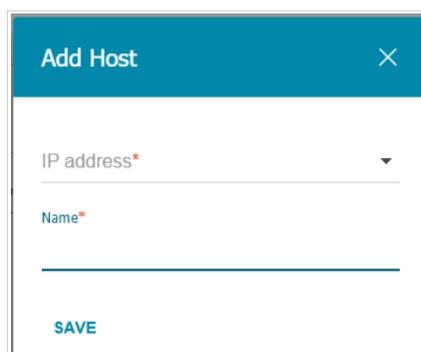


Figure 91. Configuring the local interface. The **IPv4** tab. The window for adding a DNS record.

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 IPv4 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 IPv4 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.

## IPv6

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

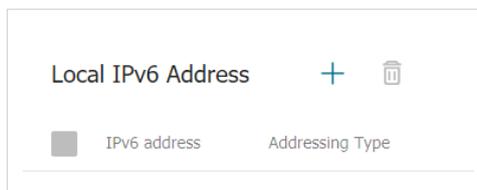


Figure 92. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.

To add an IPv6 address of the router, click the **ADD** button ( **+** ). To change the IPv6 address of the router, select it in the table.

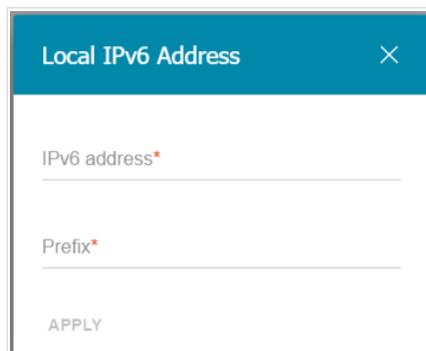


Figure 93. Configuring the local interface. The **IPv6** tab. The window for adding an IPv6 address.

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

Parameter	Description
<b>Local IPv6 Address</b>	
<b>IPv6 address</b>	The IPv6 address of the router in the local subnet.
<b>Prefix</b>	The length of the prefix subnet.
<b>Gateway IPv6 address</b>	<i>Available if the <b>Access point, Repeater, or Client</b> mode was selected in the Initial Configuration Wizard.</i> The gateway IPv6 address which is used by the router to connect to the Internet (e.g., for synchronizing the system time with an NTP server). <i>Optional.</i>

Click the **APPLY** button.

To remove the IPv6 address, 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 the IPv6 address in the editing window.

In the **Dynamic IPv6 Addresses** section, you can configure IPv6 addresses assignment settings.

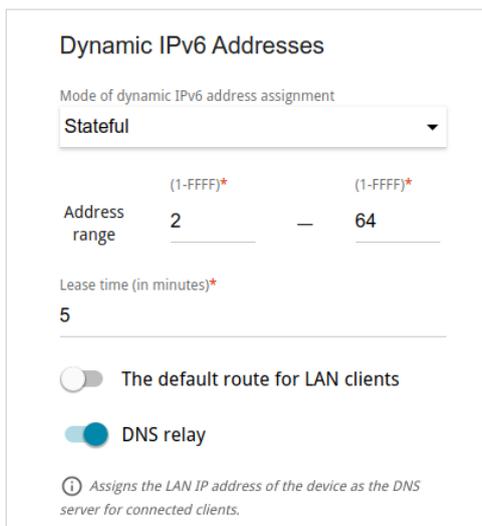


Figure 94. Configuring the local interface. The IPv6 tab. The **Dynamic IPv6 Addresses** section.

Parameter	Description
<b>Dynamic IPv6 Addresses</b>	
<b>Mode of dynamic IPv6 address assignment</b>	<p>Select the needed value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>: Clients' IPv6 addresses are assigned manually.</li> <li>• <b>Stateful</b>: The built-in DHCPv6 server of the router allocates addresses from the range specified in the <b>Address range</b> fields. Also when this value is selected, the <b>Static IP Addresses</b> and <b>Hosts</b> sections are displayed on the tab.</li> <li>• <b>Stateless</b>: Clients themselves configure IPv6 addresses using the prefix.</li> </ul>
<b>Address range</b>	The start and the end values for the latest hexet (16 bit) of the range of IPv6 addresses which the DHCPv6 server distributes to clients.
<b>Lease time</b>	The lifetime of IPv6 addresses provided to clients.
<b>The default route for LAN clients</b>	Move the switch to the right to let the clients, that received IPv6 addresses or configured them using the prefix, use the router as the default IPv6 route.
<b>DNS relay</b>	<p>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.</p> <p>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 <b>Advanced / DNS</b> page as the DNS server address.</p>

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

If needed, you can add your own address resource records. To do this, click the **ADD** button (  ) in the **Hosts** section (available if the **Router** or **WISP Repeater** mode was selected in the *Initial Configuration Wizard*).

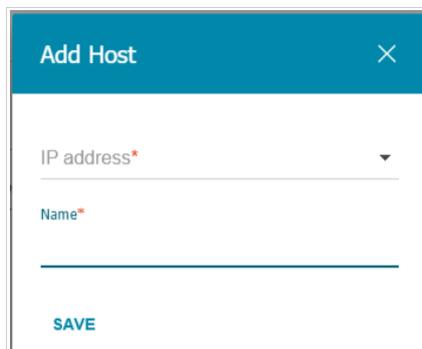


Figure 95. Configuring the local interface. The **IPv6** tab. The window for adding a DNS record.

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 IPv6 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 IPv6 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.

## WAN Failover

On the **Connections Setup / 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.

**WAN Failover**

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.

Enable

**Connections IPv4**  
The list of available connections on order of priority.

Connection	Check with ping
ppoe_46	On
statip_81	On

**Check with ping**

Interval between checks (in seconds)\*  
30

Waiting for response (in seconds)\*  
1

Number of attempts\*  
3

*Number of ping requests to the specified hosts*

**Hosts**

8.8.8.8	x
77.88.55.55	x
94.100.180.200	x

[ADD HOST](#)

**APPLY**

Figure 96. The **Connections Setup / WAN Failover** page.

To activate the backup function, create several WAN connections. After that go to the **Connections Setup / WAN Failover** page, move the **Enable** switch to the right.

In the **Connections IPv4** section, the existing IPv4 connections are displayed in order of their priority. The first connection on the list serves as the main connection, the others are backup connections.

To change the priority of a connection, left-click the relevant line in the table.

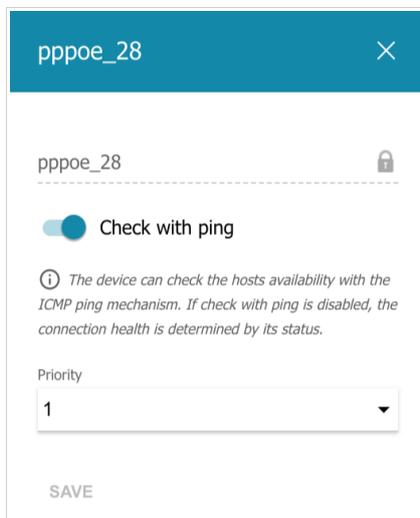


Figure 97. The window for changing the priority of a connection.

In the opened window, specify the needed parameters.

Parameter	Description
<b>Check with ping</b>	Move the switch to the right to let the router use ICMP ping mechanism for checking the connection. Move the switch to the left to let the router check only the status of the connection (may be useful for unstable connections).
<b>Priority</b>	The priority level of the connection. Level <b>1</b> is for the main connection, the others are backup connections. Select the required value from the drop-down list.

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

In the **Check with ping** section, specify settings of checking the connection using ICMP ping mechanism.

Parameter	Description
<b>Check with ping</b>	
<b>Interval between checks</b>	<p>A time period (in seconds) between regular checks of the hosts' availability. By default, the value <b>30</b> is specified. The value of this field should be higher than product of <b>Waiting for response</b> and <b>Number of attempts</b> fields values.</p> <p>Several ping requests are sent to check the hosts. After a successful attempt the router keeps using the main connection. After several failed attempts the next connection from the list is enabled.</p>
<b>Waiting for response</b>	A time period (in seconds) allocated for a response to one ping request.
<b>Number of attempts</b>	A number of failed attempts to check the health of a connection after which the next connection from the list is enabled.
<b>Hosts</b>	<p>External IP addresses that the router will check for availability via ICMP ping mechanism.</p> <p>Click the <b>ADD HOST</b> button, and in the line displayed, enter an IP address or leave values suggested by the router.</p> <p>To remove an IP address from the list, click the <b>Delete</b> icon (✕) in the line of the address.</p>

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

## Wi-Fi

In this menu you can specify all needed settings for your wireless network.

### Basic Settings

In the **Wi-Fi / Basic Settings** section, you can change basic parameters for the wireless interface of the router and configure the basic and additional wireless networks. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

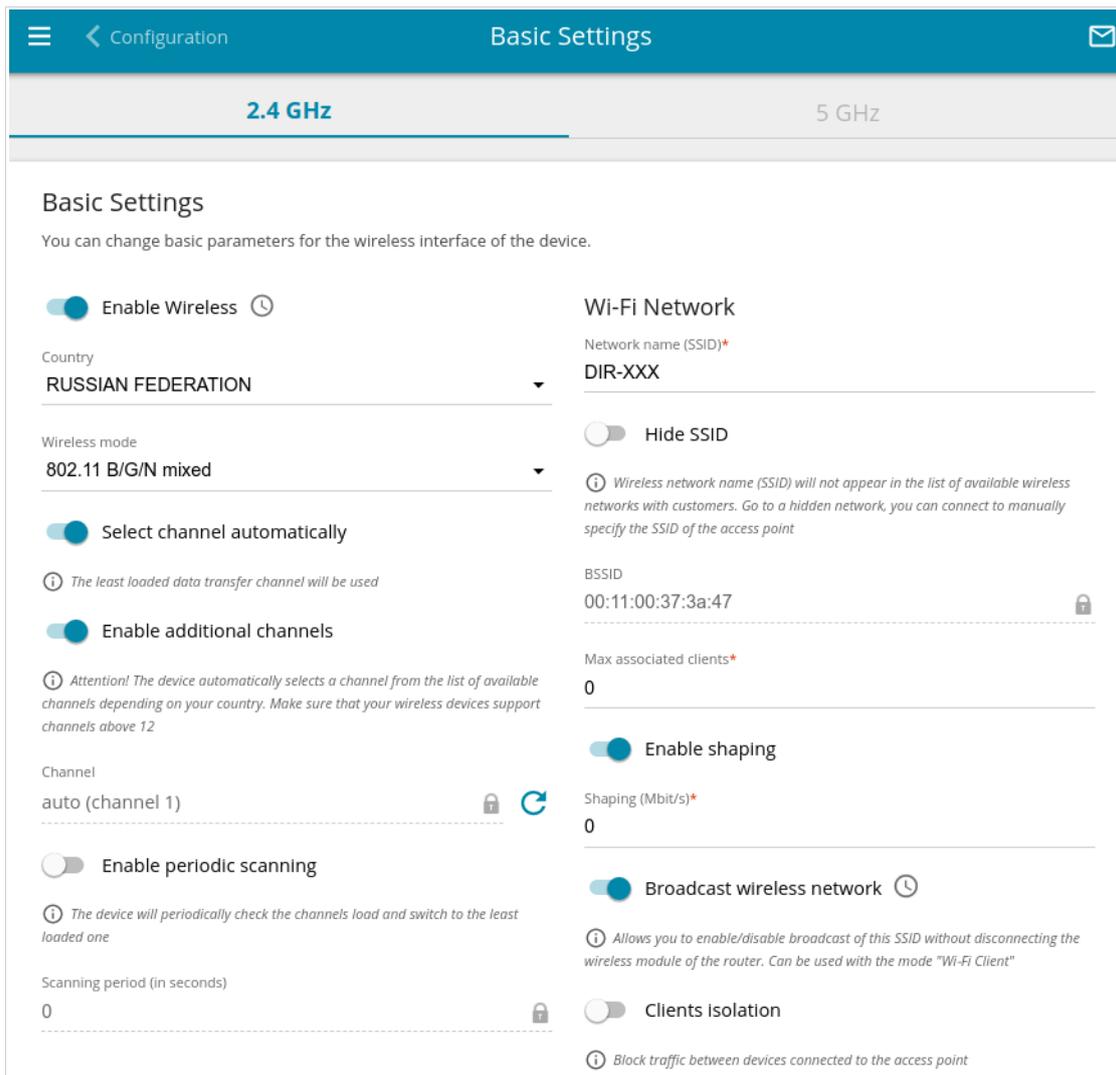


Figure 98. Basic settings of the wireless LAN in the 2.4GHz band.

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

Parameter	Description
<b>Enable Wireless</b>	<p>To enable Wi-Fi connection, move the switch to the right.</p> <p>To disable Wi-Fi connection, move the switch to the left.</p> <p>To enable/disable Wi-Fi connection on a schedule, click the <b>Set schedule</b> icon (🕒). In the opened window, from the <b>Rule</b> drop-down list, select the <b>Create rule</b> value to create a new schedule (see the <i>Schedule</i> section, page 204) or select the <b>Select an existing one</b> value to use the existing one. Existing schedules are displayed in the <b>Rule name</b> drop-down list.</p> <p>To enable Wi-Fi connection at the time specified in the schedule and disable it at the other time, select the <b>Enable wireless connection</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button.</p> <p>To disable Wi-Fi connection at the time specified in the schedule and enable it at the other time, select the <b>Disable wireless connection</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button.</p> <p>To change or delete the schedule, click the <b>Edit schedule</b> icon (🕒). In the opened window, change the parameters and click the <b>SAVE</b> button or click the <b>DELETE FROM SCHEDULE</b> button.</p>
<b>Country</b>	The country you are in. Select a value from the drop-down list.
<b>Wireless mode</b>	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.
<b>Select channel automatically</b>	Move the switch to the right to let the router itself choose the channel with the least interference.
<b>Enable additional channels</b>	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 – in the 2.4 GHz band, the 100th and higher – in the 5 GHz band), move the switch to the right.

Parameter	Description
<b>Channel</b>	<p>The wireless channel number.</p> <p>To select a channel manually, left-click; in the opened window, select a channel and click the <b>SAVE</b> button. The action is available, when the <b>Select channel automatically</b> switch is moved to the left.</p> <p>To make the router select the currently least loaded channel, click the <b>Refresh</b> icon (). The icon is displayed, when the <b>Select channel automatically</b> switch is moved to the right.</p>
<b>Enable periodic scanning</b>	<p>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 <b>Scanning period</b> field is available for editing.</p>
<b>Scanning period</b>	<p>Specify a period of time (in seconds) after which the router rescans channels.</p>

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.

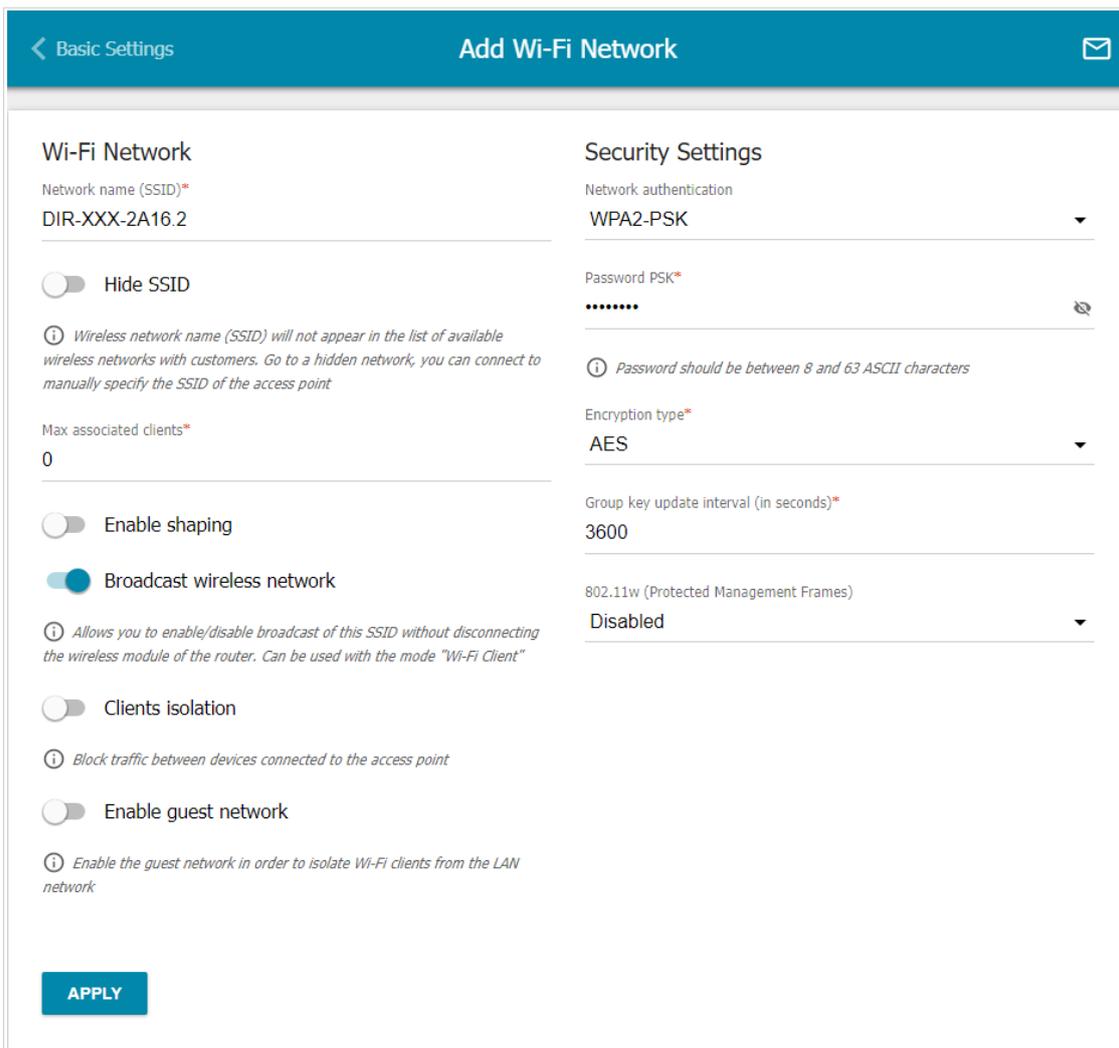


Figure 99. Creating a wireless network.

Parameter	Description
<b>Wi-Fi Network</b>	
<b>Network name (SSID)</b>	A name for the wireless network.
<b>Hide SSID</b>	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.
<b>BSSID</b>	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.
<b>Max associated clients</b>	The maximum number of devices connected to the wireless network. When the value <b>0</b> is specified, the device does not limit the number of connected clients.
<b>Enable shaping</b>	<p>Move the switch to the right to limit the maximum bandwidth of the wireless network. In the <b>Shaping</b> field displayed, specify the maximum value of speed (Mbps).</p> <p>Move the switch to the left not to limit the maximum bandwidth.</p>

Parameter	Description
<p><b>Broadcast wireless network</b></p>	<p>If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DIR-822 can connect to another access point as a wireless client.</p> <p>To enable/disable broadcasting on a schedule, click the <b>Set schedule</b> icon (🕒). In the opened window, from the <b>Rule</b> drop-down list, select the <b>Create rule</b> value to create a new (see the <i>Schedule</i> section, page 204) or select the <b>Select an existing one</b> value to use the existing one. Existing schedules are displayed in the <b>Rule name</b> drop-down list.</p> <p>To enable broadcasting at the time specified in the schedule and disable it at the other time, select the <b>Enable wireless network broadcasting</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button. When the wireless connection is disabled, the device will not be able to enable broadcasting of this wireless network on schedule.</p> <p>To disable broadcasting at the time specified in the schedule and enable it at the other time, select the <b>Disable wireless network broadcasting</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button.</p> <p>To change or delete the schedule, click the <b>Edit schedule</b> icon (🕒). In the opened window, change the parameters and click the <b>SAVE</b> button or click the <b>DELETE FROM SCHEDULE</b> button.</p> <p>If you created an additional network, you can configure, change or delete a schedule for each network. To do this, click the button in the line of the network.</p>
<p><b>Clients isolation</b></p>	<p>Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.</p>
<p><b>Enable guest network</b></p>	<p>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.</p>

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

By default, the **WPA2-PSK** network authentication type of both bands of the wireless network is specified. WPS PIN from the barcode label is used as the network key.

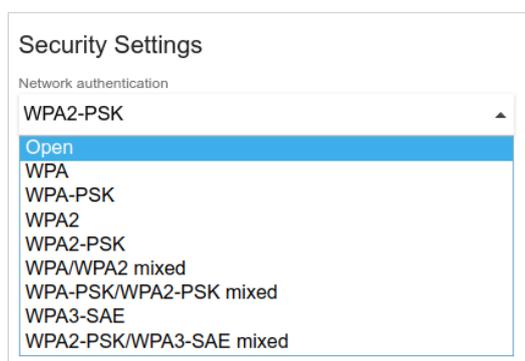


Figure 100. Network authentication types supported by the router.

The router supports the following authentication types:

Authentication type	Description
<b>Open</b>	Open authentication (with WEP encryption for wireless network modes not supporting 802.11n or 802.11ac devices).
<b>WEP</b>	Authentication with a shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n or 802.11ac devices is selected from the <b>Wireless mode</b> drop-down list on the <b>Wi-Fi / Basic Settings</b> page.
<b>WPA</b>	WPA-based authentication using a RADIUS server.
<b>WPA-PSK</b>	WPA-based authentication using a PSK.
<b>WPA2</b>	WPA2-based authentication using a RADIUS server.
<b>WPA2-PSK</b>	WPA2-based authentication using a PSK.
<b>WPA/WPA2 mixed</b>	A mixed type of authentication. When this value is selected, devices using the <b>WPA</b> authentication type and devices using the <b>WPA2</b> authentication type can connect to the wireless network.
<b>WPA-PSK/WPA2-PSK mixed</b>	A mixed type of authentication. When this value is selected, devices using the <b>WPA-PSK</b> authentication type and devices using the <b>WPA2-PSK</b> authentication type can connect to the wireless network.
<b>WPA3-SAE</b>	WPA3-based authentication using a PSK and SAE method.
<b>WPA2-PSK/WPA3-SAE mixed</b>	A mixed type of authentication. When this value is selected, devices using the <b>WPA2-PSK</b> authentication type and devices using the <b>WPA3-SAE</b> 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 or 802.11ac):

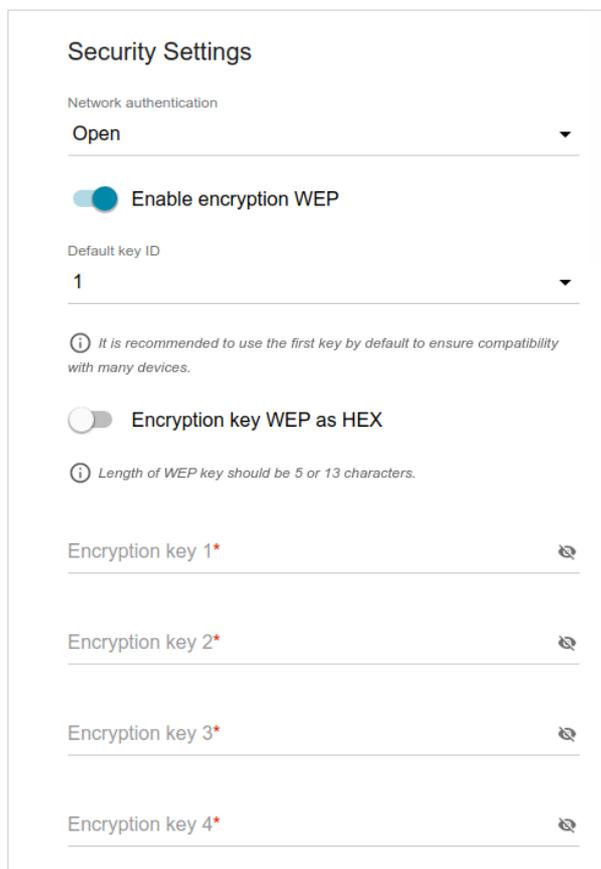


Figure 101. The **Open** value is selected from the **Network authentication** drop-down list.

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

When the **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK mixed**, **WPA3-SAE**, or **WPA2-PSK/WPA3-SAE mixed** value is selected, the following fields are displayed on the page:

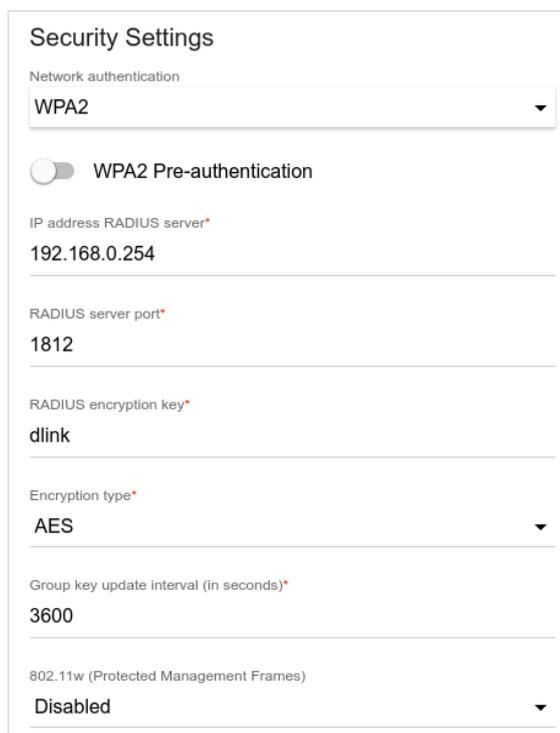
Figure 102. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.

Parameter	Description
<b>Password PSK</b>	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. <sup>4</sup> Click the <b>Show</b> icon (👁) to display the entered password.
<b>Encryption type</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> . <i><b>TKIP</b> and <b>TKIP+AES</b> encryption types are not available for <b>WPA3-SAE</b> and <b>WPA2-PSK/WPA3-SAE mixed</b> authentication types.</i>
<b>Group key update interval</b>	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value <b>0</b> is specified for this field, the key is not renewed.

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

Parameter	Description
<b>802.11w (Protected Management Frames)</b>	<p>For <b>WPA2-PSK</b>, <b>WPA3-SAE</b>, and <b>WPA2-PSK/WPA3-SAE mixed</b> authentication types only.</p> <p>Protected Management Frames help to improve packet privacy protection for wireless data transmission. Select a value for the wireless network from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Protected Management Frames are not used.</li> <li>• <b>Optional:</b> Protected Management Frames are optional.</li> <li>• <b>Required:</b> Protected Management Frames are required. When this value is selected, devices not supporting the 802.11w standard cannot connect to the wireless network.</li> </ul> <p>The default value cannot be changed for <b>WPA3-SAE</b> and <b>WPA2-PSK/WPA3-SAE mixed</b> authentication types.</p>

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the following settings are displayed on the page:



Security Settings

Network authentication  
WPA2

WPA2 Pre-authentication

IP address RADIUS server\*  
192.168.0.254

RADIUS server port\*  
1812

RADIUS encryption key\*  
dlink

Encryption type\*  
AES

Group key update interval (in seconds)\*  
3600

802.11w (Protected Management Frames)  
Disabled

Figure 103. The **WPA2** value is selected from the **Network authentication** drop-down list.

Parameter	Description
<b>WPA2 Pre-authentication</b>	Move the switch to the right to activate preliminary authentication (displayed only for the <b>WPA2</b> and <b>WPA/WPA2 mixed</b> authentication types).
<b>IP address RADIUS server</b>	The IP address of the RADIUS server.

Parameter	Description
<b>RADIUS server port</b>	A port of the RADIUS server.
<b>RADIUS encryption key</b>	The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings).
<b>Encryption type</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> .
<b>Group key update interval</b>	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value <b>0</b> is specified for this field, the key is not renewed.
<b>802.11w (Protected Management Frames)</b>	<p><i>For <b>WPA2</b> authentication type only.</i></p> <p>Protected Management Frames help to improve packet privacy protection for wireless data transmission. Select a value for the wireless network from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> Protected Management Frames are not used.</li> <li>• <b>Optional:</b> Protected Management Frames are optional.</li> <li>• <b>Required:</b> Protected Management Frames are required. When this value is selected, devices not supporting the 802.11w standard cannot connect to the wireless network.</li> </ul>

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.

## Client Management

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

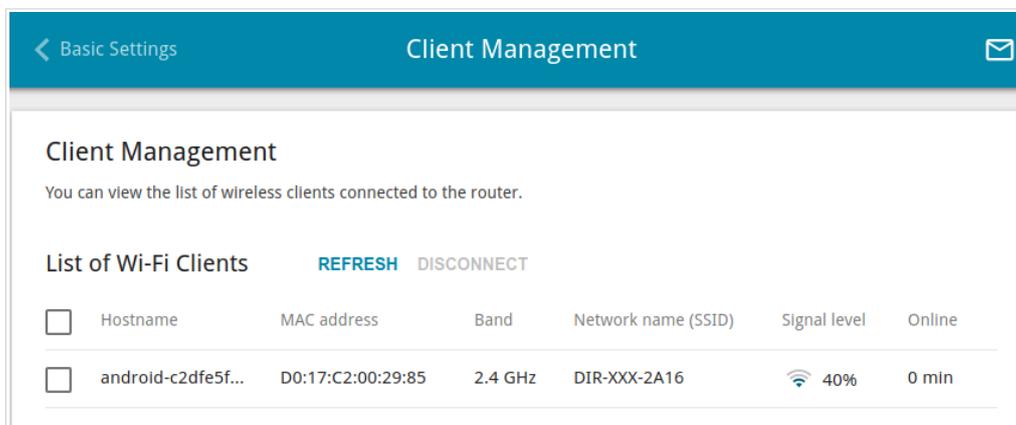


Figure 104. The page for managing the wireless clients.

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

## WPS

On the **Wi-Fi / WPS** page, you can enable the function for configuration of the WLAN and select a method for connection to the WLAN.

The WPS function helps to configure the protected 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 on the tab of the relevant band are not available.

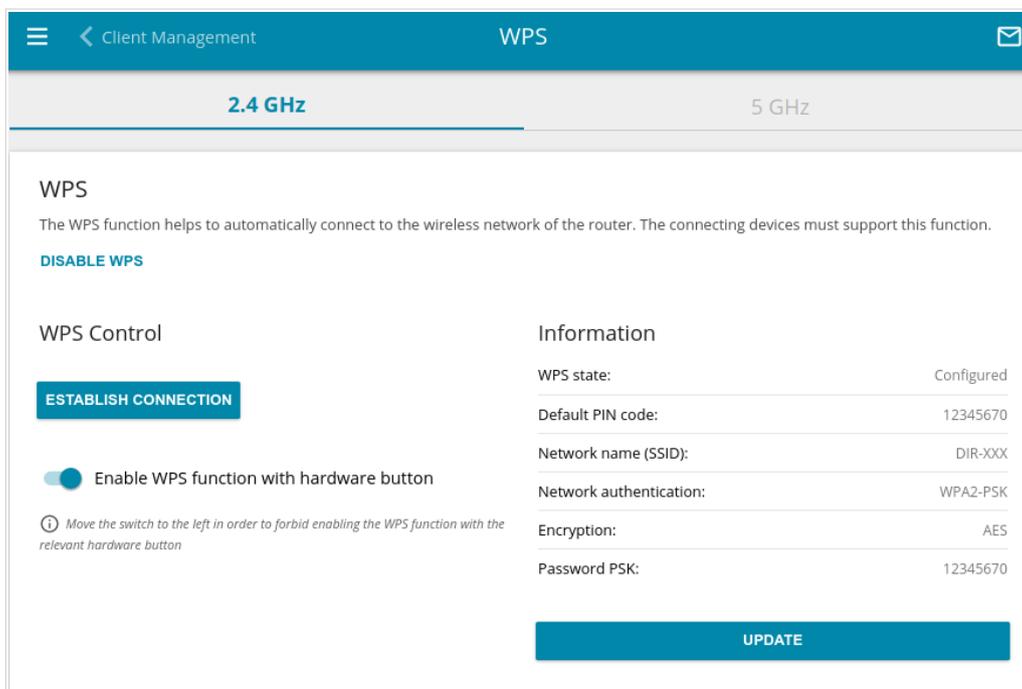


Figure 105. The page for configuring the WPS function.

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

To activate the WPS function via the hardware button, move the **Enable Wi-Fi when WPS function is activated with hardware button** switch to the right on the tabs of both bands. Then, with the device turned on, push the button, hold it for 2 seconds, and release. The **WPS** LED should start blinking. In addition, upon pressing the button, the wireless interfaces of the device are enabled if they were disabled before.

If you want to disable activating the WPS function via the hardware button, on the tabs of both bands, move the **Enable Wi-Fi when WPS function is activated 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, on the tab of the relevant band, click the **ENABLE WPS** button.

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

Parameter	Description
<b>WPS state</b>	The state of the WPS function: <ul style="list-style-type: none"> <li>• <b>Configured</b> (all needed settings are specified; these settings will be used upon establishing the wireless connection)</li> <li>• <b>Unconfigured</b> (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).</li> </ul>
<b>Default PIN code</b>	The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function.
<b>Network name (SSID)</b>	The name of the router's wireless network.
<b>Network authentication</b>	The network authentication type specified for the wireless network.
<b>Encryption</b>	The encryption type specified for the wireless network.
<b>Password PSK</b>	The encryption password specified for the wireless network.
<b>UPDATE</b>	Click the button to update the data on the page.

## ***Using WPS Function via Web-based Interface***

To connect to the basic wireless network via the PIN method of 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. In the opened window, select the **PIN** value from the **WPS method** drop-down list.
4. Select the PIN method in the software of the wireless device that you want to connect to the router's WLAN.
5. Click the relevant button in the software of the wireless device that you want to connect to the WLAN.
6. Right after that, enter the PIN code specified on the cover of the wireless device or in its software in the **PIN code** field.
7. Click the **CONNECT** button in the web-based interface of the router.

To connect to the basic wireless network via the PBC method of 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. In the opened window, select the **PBC** value from the **WPS method** drop-down list.
4. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
5. 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.
6. 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 Wi-Fi when WPS function is activated with hardware button** switch is moved to the right on the tabs of both bands.
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** 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** button of the router, hold it for 2 seconds, and release. The **WPS** LED should start blinking.

## WMM

On the **Wi-Fi / WMM** page, you can enable the Wi-Fi Multimedia function. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

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 drop-down list in the **Work mode** section 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.

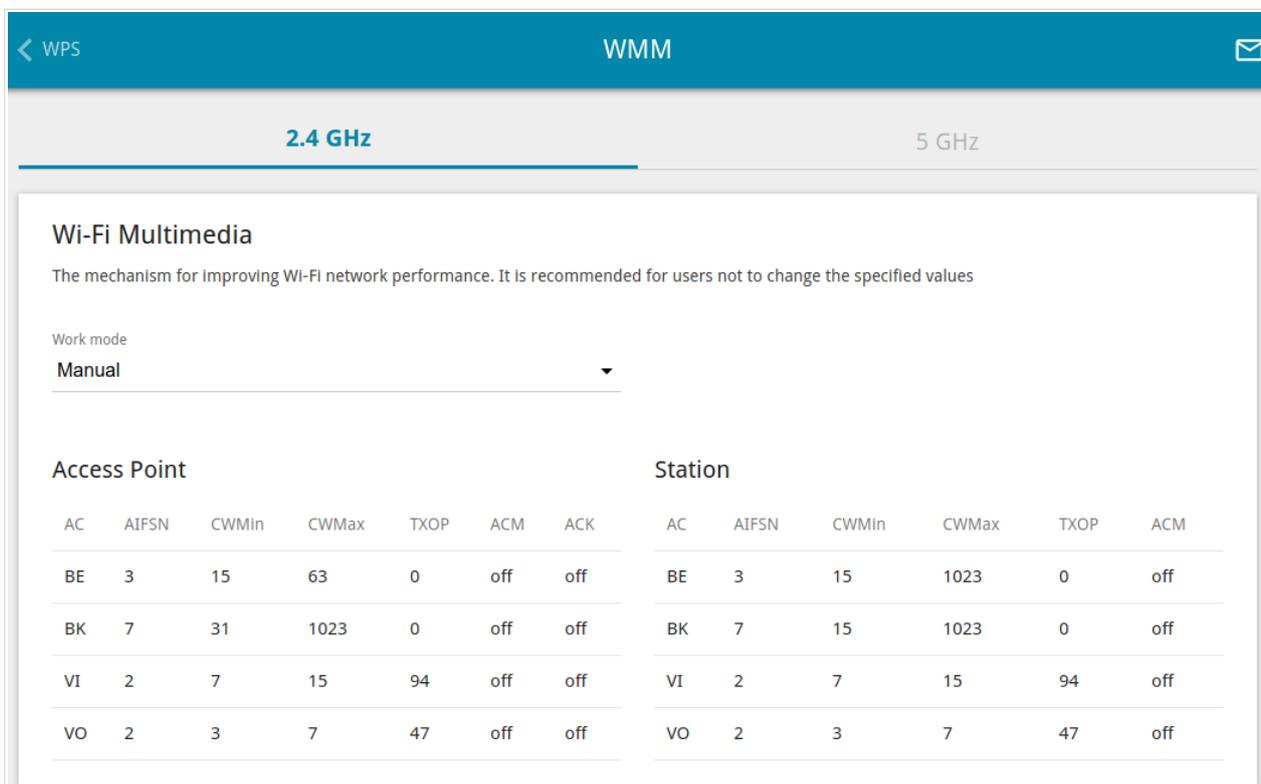


Figure 106. The page for configuring the WMM function.

**!** 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.

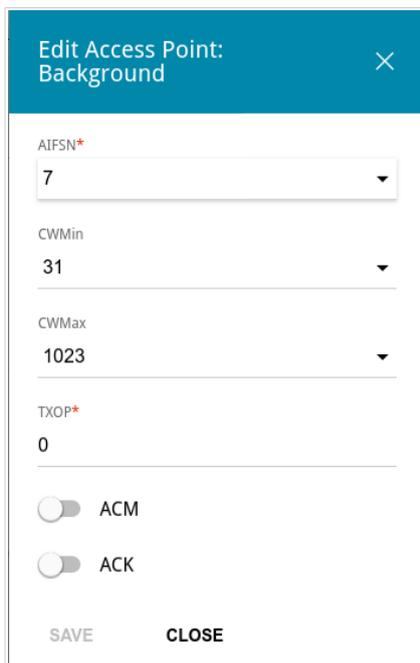


Figure 107. The window for changing parameters of the WMM function.

Parameter	Description
<b>AIFSN</b>	<i>Arbitrary Inter-Frame Space Number.</i> This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
<b>CWMin / CWMax</b>	<i>Contention Window Minimum/Contention Window Maximum.</i> Both fields influence time delays for the relevant Access Category. The <b>CWMax</b> field value should not be lower, than the <b>CWMin</b> field value. The lower the difference between the <b>CWMax</b> field value and the <b>CWMin</b> field value, the higher is the Access Category priority.
<b>TXOP</b>	<i>Transmission Opportunity.</i> The higher the value, the higher is the Access Category priority.
<b>ACM</b>	<i>Admission Control Mandatory.</i> If the switch is moved to the right, the device cannot use the relevant Access Category.

Parameter	Description
<b>ACK</b>	<i>Acknowledgment.</i> Answering response requests while transmitting. Displayed only in the <b>Access Point</b> 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 **Wi-Fi / Client** page, you can configure the router as a client to connect to a wireless access point or to a WISP. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

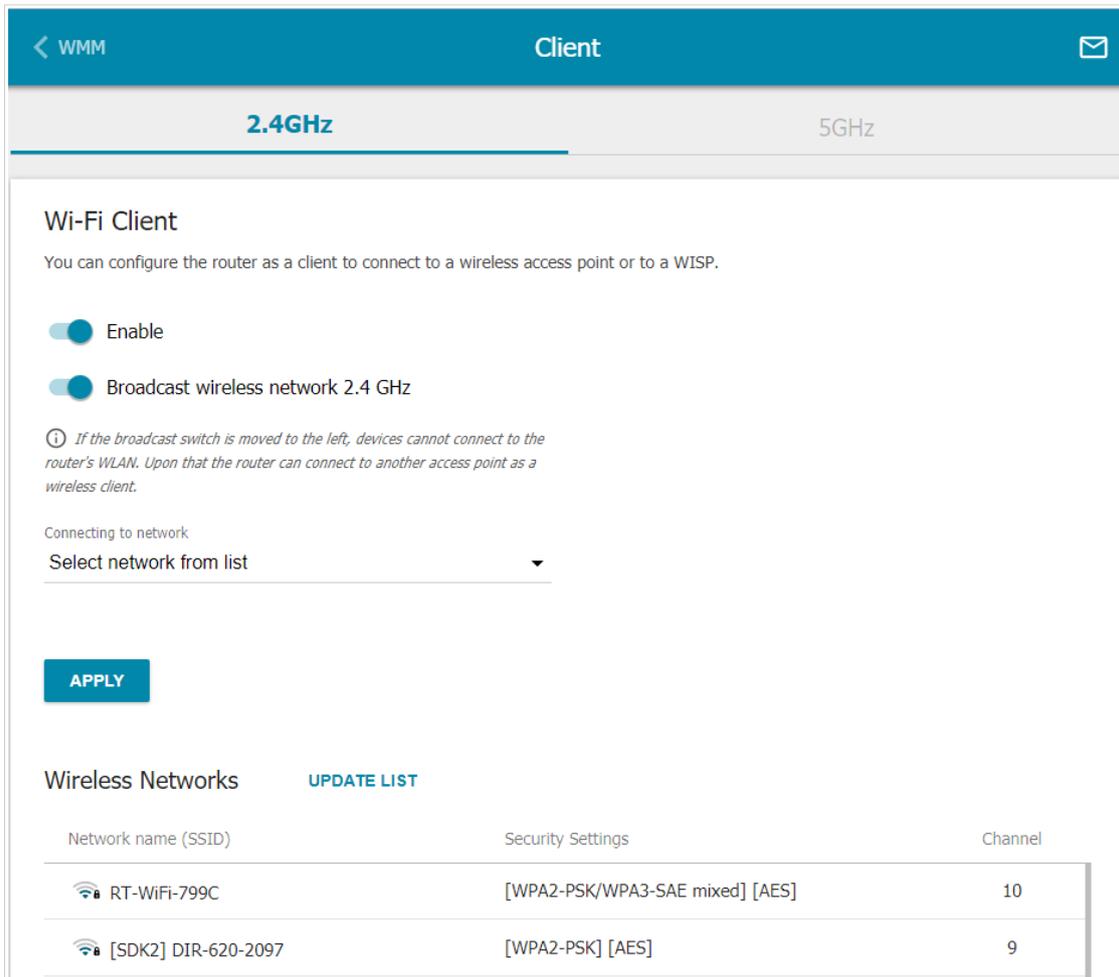


Figure 108. The page for configuring the client mode.

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
<b>Broadcast wireless network 2.4 GHz / Broadcast wireless network 5 GHz</b>	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.
<b>Connecting to network</b>	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. Enter the name of the network 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
<b>Enable encryption WEP</b>	For <b>Open</b> authentication type only. To activate WEP encryption, move the switch to the right. Upon that the <b>Default key ID</b> drop-down list, the <b>Encryption key WEP as HEX</b> switch, and four <b>Encryption key</b> fields are displayed on the page.
<b>Default key ID</b>	The number of the key (from first to fourth) which will be used for WEP encryption.
<b>Encryption key WEP as HEX</b>	Move the switch to the right to set a hexadecimal number as a key for encryption.
<b>Encryption key (1-4)</b>	Keys for WEP encryption. The router uses the key selected from the <b>Default key ID</b> drop-down list. It is required to specify all the fields. Click the <b>Show</b> icon (👁) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK mixed**, **WPA3-SAE**, or **WPA2-PSK/WPA3-SAE mixed** authentication type is selected, the following fields are displayed:

Parameter	Description
<b>Password PSK</b>	A password for WPA encryption. Click the <b>Show</b> icon (👁) to display the entered key.
<b>Encryption type</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> . <i>TKIP and TKIP+AES encryption types are not available for WPA3-SAE and WPA2-PSK/WPA3-SAE mixed authentication types.</i>

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

When connecting to a wireless access point, the wireless channel of DIR-822 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\_2GHz** interface in the 2.4GHz band or for the **WiFiClient\_5GHz** interface in the 5GHz band.

## Client Shaping

On the **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.

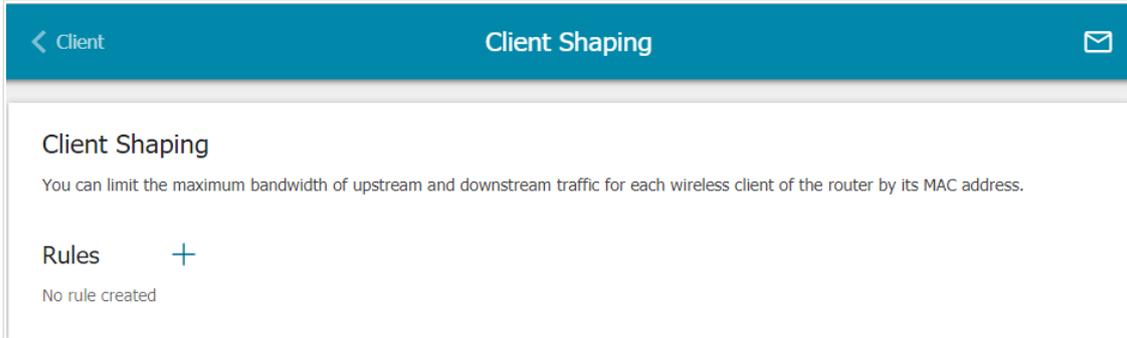


Figure 109. The **Wi-Fi / Client Shaping** page.

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 110. The window for setting up rate limit.

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

Parameter	Description
<b>Frequency band</b>	From the drop-down list, select a band of the wireless network.
<b>SSID</b>	A wireless network to which the rule will be applied. Select the needed value from the drop-down list.
<b>Enabled</b>	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.
<b>MAC address</b>	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).
<b>Upload</b>	
<b>Maximum rate</b>	Specify the maximum value of the upstream traffic rate (Mbps) or move the <b>Not limited</b> switch to the right not to limit the maximum bandwidth of upstream traffic.
<b>Download</b>	
<b>Maximum rate</b>	Specify the maximum value of the downstream traffic rate (Mbps) or move the <b>Not limited</b> 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 **Wi-Fi / Additional** section, you can define additional parameters for the WLAN of the router. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

**!** Changing parameters presented on this page may negatively affect your WLAN!

The screenshot shows the 'Additional' settings page for the 2.4 GHz band. The page is titled 'Wi-Fi Additional Settings' and includes a sub-header 'You can define additional parameters for the WLAN of the router.' The settings are organized into two columns. The left column includes: Bandwidth (Auto), Autonegotiation 20/40 (Coexistence) (disabled), TX power (in percent) (100), Drop multicast (disabled), Adaptivity mode (disabled), and STBC (enabled). The right column includes: B/G protection (Auto), Short GI (Enable), Beacon period (in milliseconds)\* (100), RTS threshold (in bytes)\* (2347), Frag threshold (in bytes)\* (2346), DTIM period (in beacon frames)\* (1), and Station Keep Alive (in seconds)\* (0). An 'APPLY' button is located at the bottom left of the settings area.

Figure 111. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
<b>Bandwidth</b>	<p>The channel bandwidth for 802.11n standard in the 2.4GHz band (the <b>2.4 GHz</b> tab).</p> <ul style="list-style-type: none"> <li>• <b>20 MHz</b>: 802.11n clients operate at 20MHz channels.</li> <li>• <b>20/40 MHz</b>: 802.11n clients operate at 20MHz or 40MHz channels.</li> <li>• <b>Auto</b>: The router automatically chooses the most suitable channel bandwidth for 802.11n clients.</li> </ul> <p>The channel bandwidth for 802.11n and 802.11ac standards in 5GHz band (the <b>5 GHz</b> tab).</p> <ul style="list-style-type: none"> <li>• <b>20 MHz</b>: 802.11n and 802.11ac clients operate at 20MHz channels.</li> <li>• <b>20/40 MHz</b>: 802.11n and 802.11ac clients operate at 20MHz or 40MHz channels.</li> <li>• <b>20/40/80 MHz</b>: 802.11ac clients operate at 20MHz, 40MHz, or 80MHz channels.</li> <li>• <b>Auto</b>: The router automatically chooses the most suitable channel bandwidth for 802.11n and 802.11ac clients.</li> </ul>
<b>Autonegotiation 20/40 (Coexistence)</b>	<p><i>Available on the <b>2.4 GHz</b> tab.</i></p> <p>Move the switch to the right to let the router to automatically choose the most suitable channel bandwidth (20MHz or 40MHz) for the connected devices (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the <b>20/40 MHz</b> or <b>Auto</b> value is selected from the <b>Bandwidth</b> drop-down list.</p>
<b>TX power</b>	<p>The transmit power (in percentage terms) of the router.</p>
<b>Enable DFS</b>	<p><i>Available on the <b>5 GHz</b> tab.</i></p> <p>Move the switch to the right to enable the DFS (<i>Dynamic Frequency Selection</i>) mechanism. Upon that the router uses the channels at which radars and other mobile or stationary radio systems can operate, but switches to other channels if these devices require this. In order to use the DFS mechanism, the automatic channel selection should be enabled (on the <b>Wi-Fi / Basic Settings</b> page).</p> <p>Move the switch to the left not to let the router use the channels at which radars and other mobile or stationary radio systems can operate.</p>

Parameter	Description
<b>Drop multicast</b>	<p>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 <b>Advanced / IGMP/MLD</b> page. If the switch is moved to the right, the device will not be available by the domain name for Wi-Fi clients.</p>
<b>Enable TX Beamforming</b>	<p><i>Available on the <b>5 GHz</b> tab.</i></p> <p>TX Beamforming is the signal processing/directing technique which helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation.</p> <p>Move the switch to the right to improve the signal quality.</p>
<b>Adaptivity mode</b>	<p>Move the switch to the right to let the router switch from the channels at which radars and other mobile or stationary radio systems operate in case it interferes with these devices. Such a setting can slow down the router's WLAN.</p> <p>In order to use the adaptivity mode, the automatic channel selection should be enabled (on the <b>Wi-Fi / Basic Settings</b> page).</p>
<b>Reduce power on OFDM modulation</b>	<p><i>Available on the <b>5 GHz</b> tab.</i></p> <p>Move the switch to the right to lower service signals strength for improving the quality of their transmission. Use the setting in case of problems with connecting wireless clients to the router.</p>
<b>STBC</b>	<p>The STBC (<i>Space-time block coding</i>) technique allows increasing data transfer reliability even for portable devices equipped with poor antennas (smartphones, pads, etc.) due to using several data streams and processing several versions or received data.</p> <p>Move the switch to the right if you need to use the STBC technique.</p>
<b>B/G protection</b>	<p><i>Available on the <b>2.4 GHz</b> tab.</i></p> <p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Auto:</b> 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).</li> <li>• <b>Always On:</b> The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</li> <li>• <b>Always Off:</b> The protection function is always disabled.</li> </ul>

Parameter	Description
<b>Short GI</b>	<p>Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices.</p> <ul style="list-style-type: none"> <li>• <b>Enable:</b> 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 <b>Wireless mode</b> drop-down list on the <b>Wi-Fi / Basic Settings</b> page).</li> <li>• <b>Disable:</b> The router uses the 800 ns standard guard interval.</li> </ul>
<b>Beacon period</b>	<p>The time interval (in milliseconds) between packets sent to synchronize the wireless network.</p>
<b>RTS threshold</b>	<p>The minimum size (in bytes) of a packet for which an RTS frame is transmitted.</p>
<b>Frag threshold</b>	<p>The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).</p>
<b>DTIM period</b>	<p>The number of beacon frames between sending DTIM messages (messages notifying on broadcast or multicast transmission).</p>
<b>Station Keep Alive</b>	<p>The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value <b>0</b> is specified, the checking is disabled.</p>

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

## MAC Filter

On the **Wi-Fi / MAC Filter** page, you can define a set of MAC addresses of devices which will be allowed to access the WLAN, or define 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-822.

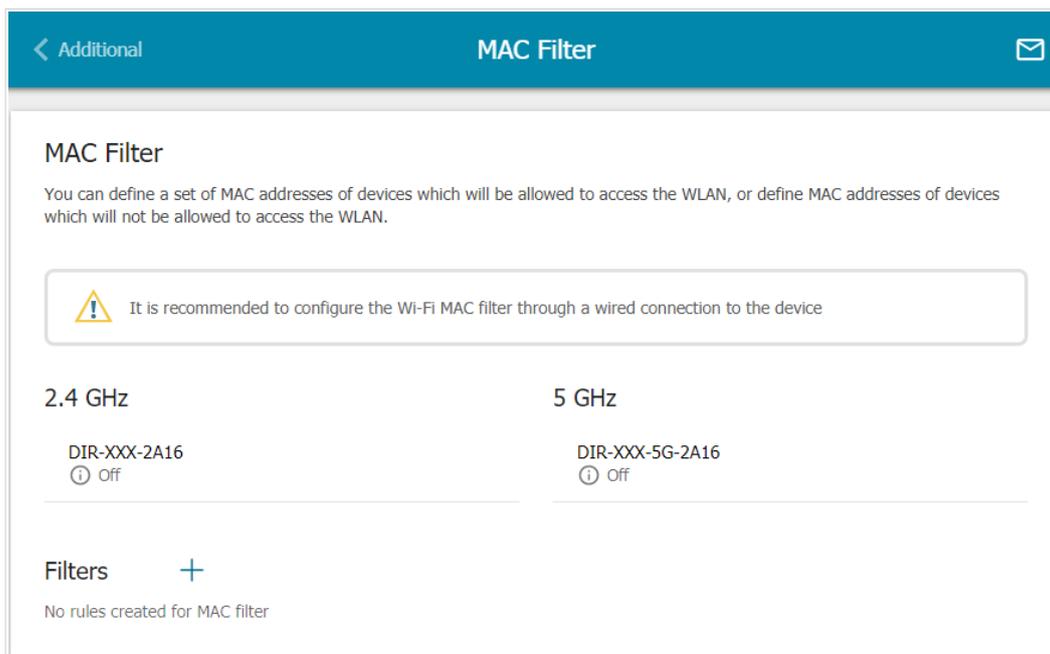


Figure 112. The page for configuring the MAC filter for the wireless network.

By default, the Wi-Fi MAC filter is disabled.

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 ( **+** ).

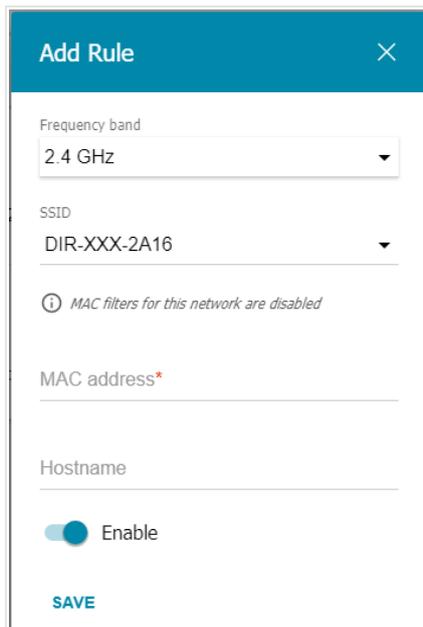


Figure 113. The window for adding a rule for the MAC filter.

You can specify the following parameters:

Parameter	Description
<b>Frequency band</b>	From the drop-down list, select a band of the wireless network.
<b>SSID</b>	A wireless network to which the rule will be applied. Select the needed value from the drop-down list.
<b>MAC address</b>	In the field, enter the MAC address to which the selected filtering mode will be applied.
<b>Hostname</b>	The name of the device for easier identification ( <i>optional</i> ). You can specify any name.
<b>Enable</b>	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, in the section corresponding to the band (**2.4 GHz** or **5 GHz**), left-click the line of the wireless network. In the opened window, move the **Enable MAC filter** switch to the right. Upon that the **MAC filter restrict mode** drop-down list will be displayed. Select the **Allow** value from the 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.

To set a schedule for the MAC filter rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 204) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the MAC filter rule at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the MAC filter rule at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

To change or delete the schedule for a rule, click the **Edit schedule** icon (🕒) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

## EasyMesh

On the **Wi-Fi / EasyMesh** page, you can enable the EasyMesh function. This function is designed to quickly connect several devices into one transport network for providing high-quality Wi-Fi coverage in living units of complicated planning or for creating a large temporary Wi-Fi network for an outdoor event.

A mesh network consists of a main device (the Controller role) and subordinate devices (the Agent role).<sup>5</sup> Devices connect to each other via wireless or wired connection. The Controller device enables connection and configuration of other devices of the mesh network, controls the data flow and the roaming of clients between devices in this network. Agents execute commands from the Controller device and serve as Wi-Fi access points for subordinate devices.

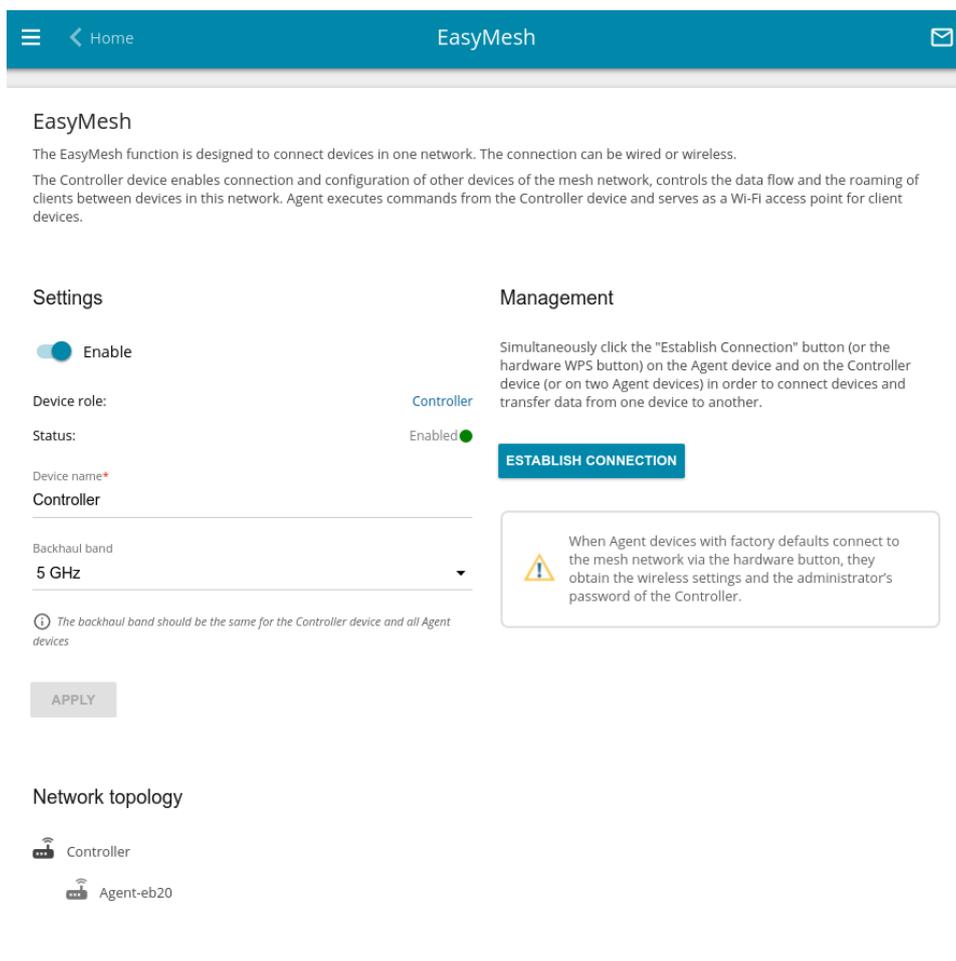


Figure 114. The **Wi-Fi / EasyMesh** page.

To activate the EasyMesh function, in the **Settings** section, move the **Enable** switch to the right. The following fields are available on the page:

Parameter	Description
<b>Device role</b>	The current role of the device in the mesh network.

<sup>5</sup> At present, you can connect up to 6 D-Link devices with EasyMesh support: 1 in the Controller role and 5 in the Agent role.

Parameter	Description
<b>Status</b>	<p>The current status of the mesh network.</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The mesh network is enabled and configured.</li> <li>• <b>Waiting:</b> Establishing connection and exchanging parameters between the main and subordinate devices.</li> <li>• <b>Disabled:</b> The mesh network is disabled.</li> </ul>
<b>Device name</b>	The name of the device for easier identification. You can specify any name.
<b>Backhaul band</b>	The band in which the mesh network operates. Select one of the bands (2.4GHz or 5GHz) for all devices of the configured network.

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

To configure DIR-822 as the main or subordinate device of the mesh network, go to the **Setup Wizard** section (see the *Initial Configuration Wizard* section, page 44), from the **Connection method** list, select the **EasyMesh** value. Then from the **Device Role** list, select the required value.

To complete your mesh network configuration, connect subordinate devices to the main device.

### **Connecting Subordinate Devices with Ethernet Cable**

To connect a subordinate device with an Ethernet cable, follow the next steps:

1. Connect an Ethernet cable between any of the LAN ports of the main and subordinate device.
2. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.
3. Make sure that the connection is established. To do this, in the web-based interface of the main device, on the **Wi-Fi / EasyMesh** page, in the **Network topology** section, check the information on the connected devices.

### **Connecting Subordinate Devices with Hardware Button**

To connect a subordinate device with the hardware **WPS** button, follow the next steps:

1. Simultaneously press the hardware **WPS** button on the cover of the main and the subordinate device (or two subordinate devices, if one of them has previously been connected to the mesh network), hold it for 2 seconds, and release.

**!** Do not press the button on more than two devices simultaneously. When Agent devices with factory defaults connect to the mesh network via the hardware button, the 5 GHz backhaul band should be selected on the main device.

2. The **WPS** LED of DIR-822 should start blinking. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.

3. Make sure the connection is successful. To do this, in the web-based interface of the main device, on the **Wi-Fi / EasyMesh** page, in the **Network topology** section, check the information on the connected devices.

### Connecting Subordinate Devices via Web-based Interface

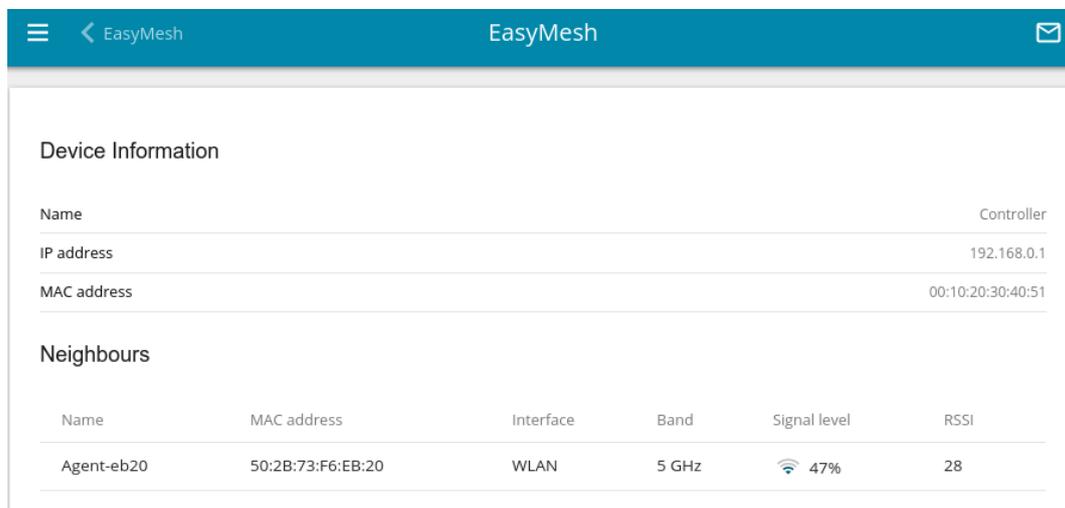
To connect a subordinate device with the **ESTABLISH CONNECTION** button in the web-based interface, follow the next steps:

1. Simultaneously press the **ESTABLISH CONNECTION** button in the web-based interface the main and the subordinate device (or two subordinate devices, if one of them has previously been connected to the mesh network).

**!** Do not press the button on more than two devices simultaneously.

2. The DIR-822 **WPS** LED should start blinking. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.
3. Make sure the connection is successful. To do this, in the web-based interface of the main device, on the **Wi-Fi / EasyMesh** page, in the **Network topology** section, check the information on the connected devices.

To view detailed data on a mesh network device, click the line corresponding to this device in the **Network topology** section.



The screenshot shows the EasyMesh web interface. At the top, there is a teal header with a menu icon, a back arrow, the text 'EasyMesh', and a mail icon. Below the header, the page is divided into two sections: 'Device Information' and 'Neighbours'.

**Device Information**

Name	Controller
IP address	192.168.0.1
MAC address	00:10:20:30:40:51

**Neighbours**

Name	MAC address	Interface	Band	Signal level	RSSI
Agent-eb20	50:2B:73:F6:EB:20	WLAN	5 GHz	47%	28

Figure 115. The device information page.

## ***Advanced***

In this menu you can configure advanced settings of the router:

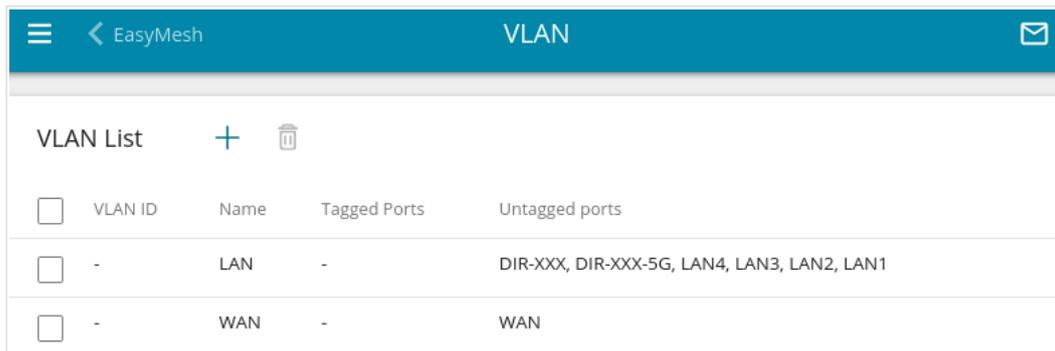
- create or edit VLANs
- add name servers
- configure a DDNS service
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the router
- configure notifications on the reason of the Internet connection failure
- define static routes
- configure TR-069 client
- enable the UPnP IGD protocol
- enable the built-in UDPXY application for the router
- allow the router to use IGMP and MLD
- allow the router to use RTSP, enable the SIP ALG, the PPPoE/PPTP/L2TP/IPsec pass through functions for the router
- configure VPN tunnels based on IPsec protocol.

## VLAN

On the **Advanced / 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.



<input type="checkbox"/>	VLAN ID	Name	Tagged Ports	Untagged ports
<input type="checkbox"/>	-	LAN	-	DIR-XXX, DIR-XXX-5G, LAN4, LAN3, LAN2, LAN1
<input type="checkbox"/>	-	WAN	-	WAN

Figure 116. The **Advanced / 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, from the **Type** drop-down list of the element corresponding to the relevant LAN port or Wi-Fi network, select the **Excluded** value and click the **APPLY** button.

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

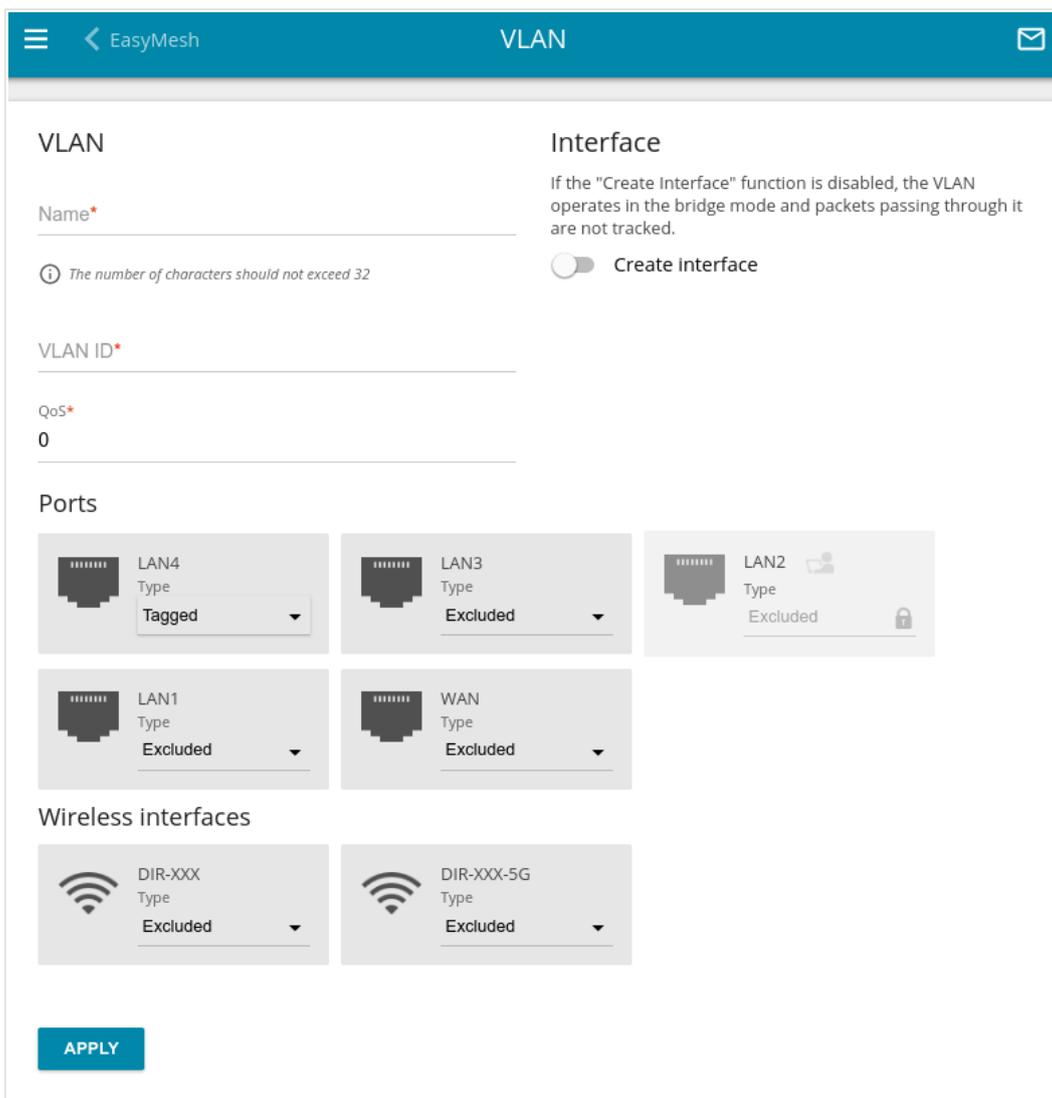


Figure 117. The page for adding a VLAN.

You can specify the following parameters:

Parameter	Description
<b>Name</b>	A name for the VLAN for easier identification.
<b>VLAN ID</b>	An identifier of the VLAN.
<b>QoS</b>	A priority tag for the transmitted traffic.
<b>Create interface</b>	<p>Move the switch to the right to create an interface that can be used for creating WAN connections. Upon that the VLAN should include the WAN port.</p> <p>Move the switch to the left for the VLAN to work in the bridge mode. This mode is mostly used to connect IPTV set-top boxes.</p>

Parameter	Description
<p style="text-align: center;"><b>Ports</b></p>	<p>Select a type for each port included in the VLAN.</p> <ul style="list-style-type: none"> <li>• <b>Untagged</b>: Untagged traffic will be transmitted through the specified port.</li> <li>• <b>Tagged</b>: Tagged traffic will be transmitted through the specified port. If at least one port of this type is included to the VLAN, it is required to fill in the <b>VLAN ID</b> and <b>QoS</b> fields.</li> </ul> <p>Leave the <b>Excluded</b> value for the ports not included in the VLAN.</p>
<p style="text-align: center;"><b>Wireless interfaces</b></p>	<p>Select the <b>Untagged</b> value for each Wi-Fi interface included in the VLAN.</p> <p>Leave the <b>Excluded</b> value for the Wi-Fi interfaces not included in the VLAN.</p>

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 **Advanced / DNS** page, you can add DNS servers to the system.

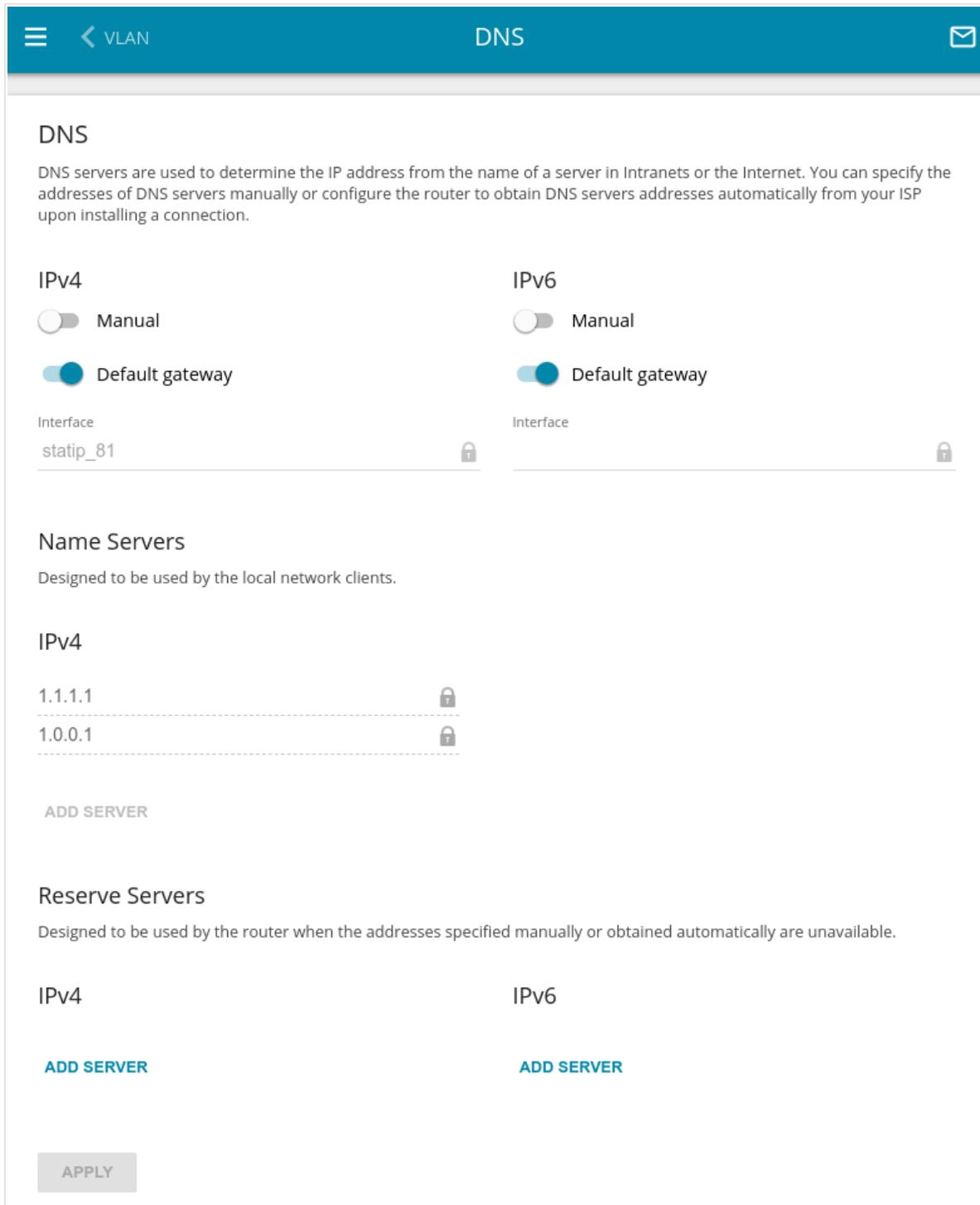


Figure 118. The **Advanced / DNS** page.

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. Also here you can specify addresses of reserve DNS servers which the router can use if the addresses specified manually or obtained automatically are unavailable.



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.

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 specify a reserve DNS server, in the **Reserve 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.

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

## DDNS

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

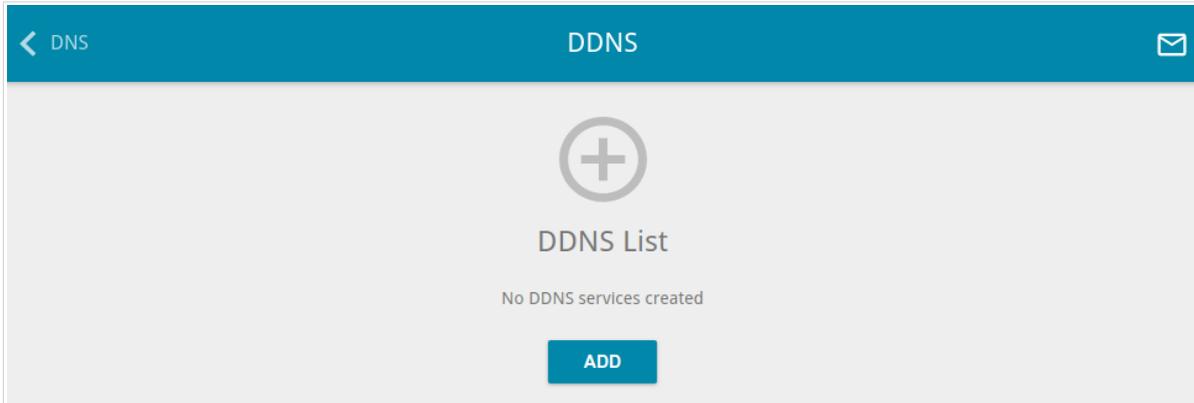


Figure 119. The **Advanced / DDNS** page.

To add a new DDNS service, click the **ADD** button ( **+** ).

Figure 120. The page for adding a DDNS service.

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

Parameter	Description
<b>Enable</b>	Move the switch to the right to enable DDNS. Move the switch to the left to disable DDNS.
<b>Hostname</b>	Enter the full domain name registered at your DDNS provider. If you want to use another domain name of this DDNS provider, click the <b>ADD HOST</b> button, and in the line displayed, enter the needed value. To remove a domain name, click the <b>Delete</b> icon (✕) in the line of the name.
<b>DDNS service</b>	Select the DDNS provider from the drop-down list. If your provider is not in the list, select the <b>Custom provider</b> value and fill in the fields displayed on the page. Specify the DDNS provider name in the <b>Name</b> field, the domain name of the provider's server in the <b>Server</b> field, and the location of settings in the <b>Path</b> field.
<b>Username</b>	The username to authorize for your DDNS provider.
<b>Password</b>	The password to authorize for your DDNS provider. Click the <b>Show</b> icon (👁) to display the entered password.
<b>Interface</b>	From the drop-down list, select a WAN connection which will be used for DDNS, or leave the <b>Default gateway</b> value.
<b>Update period</b>	An interval (in minutes) between sending data on the router's external IP address to the relevant DDNS service.

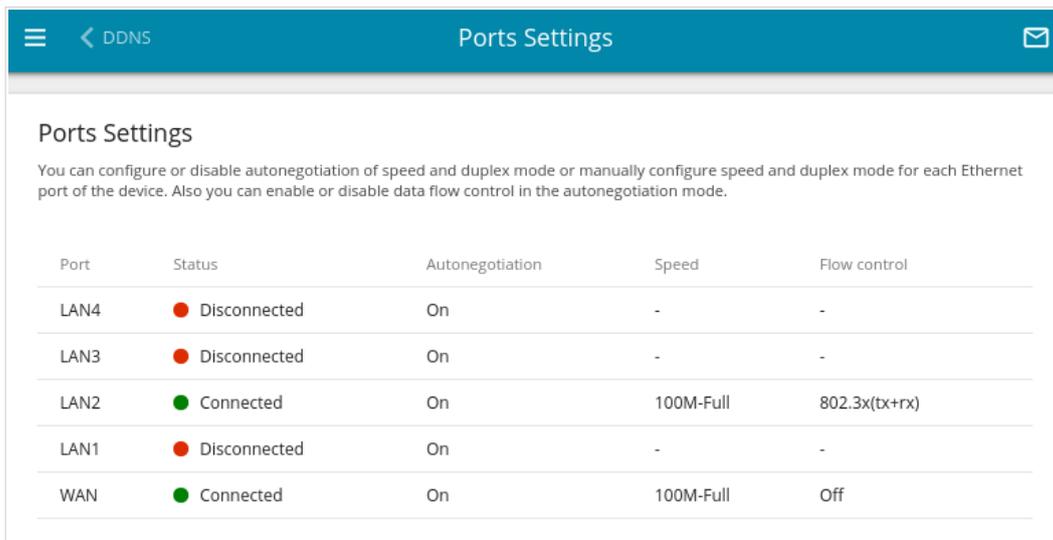
After specifying the needed parameters, click the **SAVE** button.

To edit parameters of the existing DDNS service, select the relevant line in the table. On the opened page, change the needed parameters and click the **SAVE** button.

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

## Ports Settings

On the **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.



Port	Status	Autonegotiation	Speed	Flow control
LAN4	● Disconnected	On	-	-
LAN3	● Disconnected	On	-	-
LAN2	● Connected	On	100M-Full	802.3x(tx+rx)
LAN1	● Disconnected	On	-	-
WAN	● Connected	On	100M-Full	Off

Figure 121. The **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.

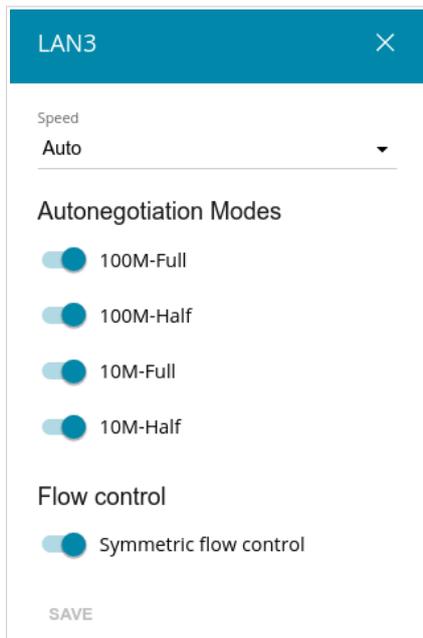


Figure 122. The window for changing the settings of the router's port.

In the opened window, specify the needed parameters:

Parameter	Description
<p><b>Speed</b></p>	<p>Data transfer mode.</p> <p>Select the <b>Auto</b> value to enable autonegotiation. When this value is selected, the <b>Autonegotiation Modes</b> and <b>Flow control</b> sections are displayed.</p> <p>Select the <b>10M-Half</b>, <b>10M-Full</b>, <b>100M-Half</b>, or <b>100M-Full</b> value to manually configure speed and duplex mode for the selected port.</p> <ul style="list-style-type: none"> <li>• <b>10M-Half:</b> 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.</li> <li>• <b>10M-Full:</b> 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.</li> <li>• <b>100M-Half:</b> 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.</li> <li>• <b>100M-Full:</b> 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.</li> </ul>
Parameter	Description
<p><b>Autonegotiation Modes</b></p>	
<p>To enable the needed data transfer modes, move relevant switches to the right.</p>	

Parameter	Description
<b>Flow control</b>	
<b>Symmetric flow control</b>	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 **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.

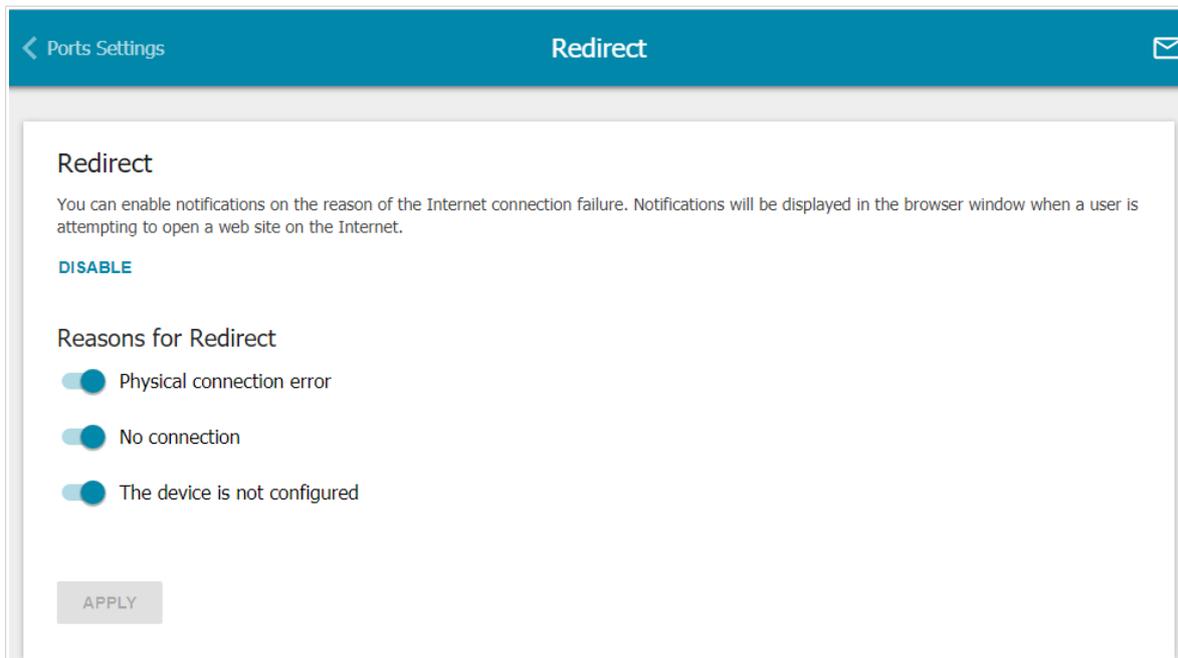


Figure 123. The **Advanced / Redirect** page.

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

Parameter	Description
<b>Reasons for Redirect</b>	
<b>Physical connection error</b>	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).
<b>No connection</b>	Notifications in case of problems of the default WAN connection (authorization error, the IPS's server does not respond, etc.).
<b>The device is not configured</b>	Notifications in case when the device works with default settings.

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

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

## Routing

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

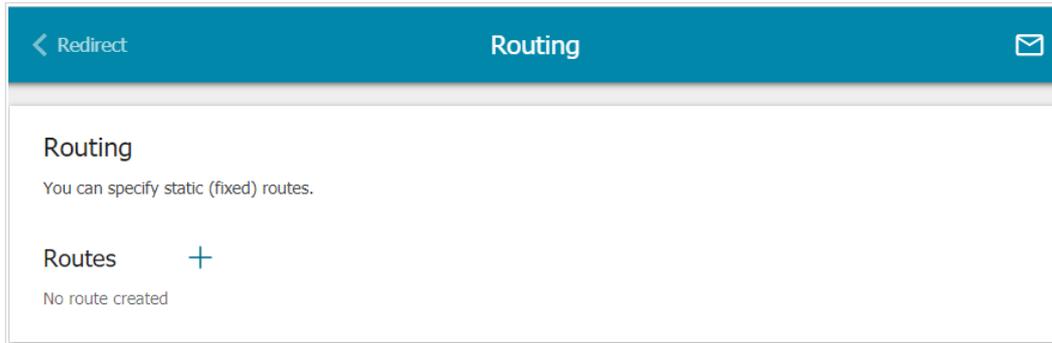


Figure 124. The **Advanced / Routing** page.

To specify a new route, click the **ADD** button ( **+** ).

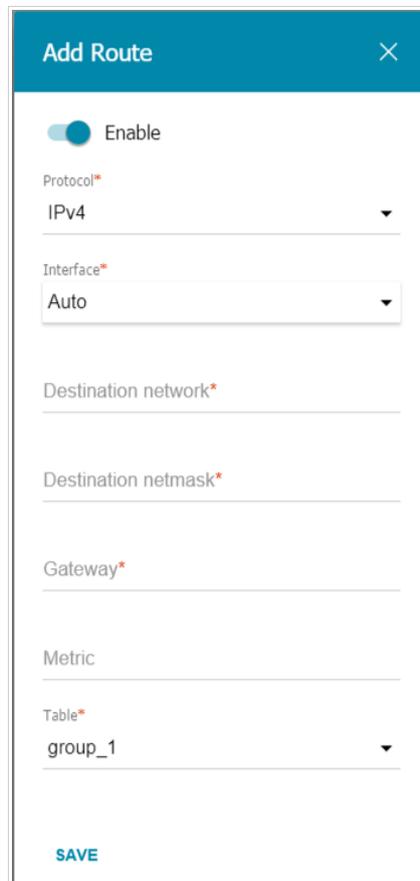


Figure 125. The window for adding a new route.

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

Parameter	Description
<b>Enable</b>	Move the switch to the right to enable the route. Move the switch to the left to disable the route.
<b>Protocol</b>	An IP version.
<b>Interface</b>	From the drop-down list, select an interface (connection) through which the device will communicate with the remote network. If you have selected the <b>Auto</b> value, the router itself sets the interface according to the data on the existing dynamic routes.
<b>Destination network</b>	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 <b>2001:db8:1234::1</b> , the format of a subnet IPv6 address is <b>2001:db8:1234::/64</b> .
<b>Destination netmask</b>	<i>For IPv4 protocol only.</i> The remote network mask.
<b>Gateway</b>	An IP address through which the destination network can be accessed.
<b>Metric</b>	A metric for the route. The lower the value, the higher is the route priority. <i>Optional.</i>
<b>Table</b>	From the drop-down list, select a routing table for the route. <ul style="list-style-type: none"> <li><b>group_1</b> table is used to route user traffic.</li> <li><b>main</b> table is used to route management traffic from internal system services of the router.</li> </ul>

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 (  ).

## TR-069 Client

On the **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 126. The page for configuring the TR-069 client.

You can specify the following parameters:

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

Parameter	Description
<b>Inform Settings</b>	
<b>On</b>	Move the switch to the right so the router may send reports (data on the device and network statistics) to the ACS.
<b>Interval</b>	Specify the time period (in seconds) between sending reports.
<b>Auto Configuration Server Settings</b>	
<b>Get URL address via DHCP</b>	If the switch is moved to the right, the router obtains the URL address of the ACS upon establishing the <b>Dynamic IP</b> type connection. If you need to specify the URL address manually, move the switch to the left and enter the needed value in the <b>URL address</b> field.
<b>URL address</b>	The URL address of the ACS provided by the ISP.
<b>Username</b>	The username to connect to the ACS.
<b>Password</b>	The password to connect to the ACS. Click the <b>Show</b> icon (🔍) to display the entered password.
<b>Connection Request Settings</b>	
<b>Username</b>	The username used by the ACS to transfer a connection request to the router.
<b>Password</b>	The password used by the ACS. Click the <b>Show</b> icon (🔍) to display the entered password.
<b>Request port</b>	The port used by the ACS. By default, the port <b>8999</b> is specified.
<b>Request path</b>	The path used by the ACS.

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

## UPnP IGD

On the **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.

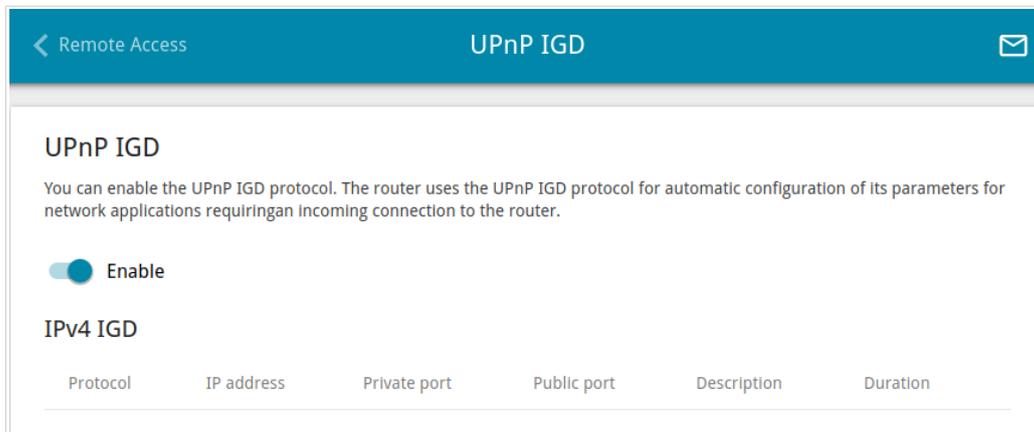


Figure 127. The **Advanced / UPnP IGD** page.

If you want to manually specify all parameters needed for network applications, move the **Enable** switch to the left. Then go to the **Firewall / Virtual Servers** page and specify needed settings. If you want to enable the UPnP IGD protocol in the router, move the **Enable** switch to the right. When the protocol is enabled, the following parameters of the router are displayed on the page:

Parameter	Description
<b>Protocol</b>	A protocol for network packet transmission.
<b>IP address</b>	The IP address of a client from the local area network.
<b>Private port</b>	A port of a client's IP address to which traffic is directed from a public port of the router.
<b>Public port</b>	A public port of the router from which traffic is directed to a client's IP address.
<b>Description</b>	Information transmitted by a client's network application.
<b>Duration</b>	The time period during which the UPnP IGD protocol has been used.

## UDPXY

On the **Advanced / UDPXY** page, you can allow the router to use the built-in UDPXY application. The UDPXY application transforms UDP traffic into HTTP traffic. This application allows devices which cannot receive UDP streams to access stream video.

Figure 128. The **Advanced / UDPXY** page.

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

Upon that the following fields are displayed on the page:

Parameter	Description
<b>Port</b>	The port of the router which the UDPXY application uses.
<b>Maximum client number</b>	Maximum number of devices from the router's LAN which will be served by the application.
<b>Buffer size for incoming data</b>	Size of intermediate buffer for received data. By default, the minimum acceptable value is specified.
<b>Buffer size for data transferred to client</b>	Size of intermediate buffer for transmitted data. By default, the minimum acceptable value is specified.
<b>WAN interface</b>	From the drop-down list, select a WAN connection which will be used for operation with streaming video.

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

To access the status page of the application, click the **Status** link.

**udpxy status:**

Server Process ID	Accepting clients on	Multicast address	Active clients
2443	192.168.0.1:4022	202.254.1.2	0

**Available HTTP requests:**

Request template	Function
<code>http://address:port/udp/mcast_addr:mport/</code>	Relay multicast traffic from mcast_addr:mport
<code>http://address:port/status/</code>	Display udpxy status
<code>http://address:port/restart/</code>	Restart udpxy

udpxy v. 1.0 (Build 23) standard - [Thu Jan 1 00:31:30 1970]  
udpxy and udpexec are Copyright (C) 2008-2013 Pavel V. Cherenkov and licensed under GNU GPLv3

Figure 129. The UDPXY application status page.

## IGMP/MLD

On the **Advanced / IGMP/MLD** page, you can allow the router to use IGMP and MLD and specify needed settings.

IGMP and MLD are used for managing multicast traffic (transferring data to a group of destinations) in IPv4 and IPv6 networks correspondingly. These protocols allow using network resources for some applications, e.g., for streaming video, more efficiently.

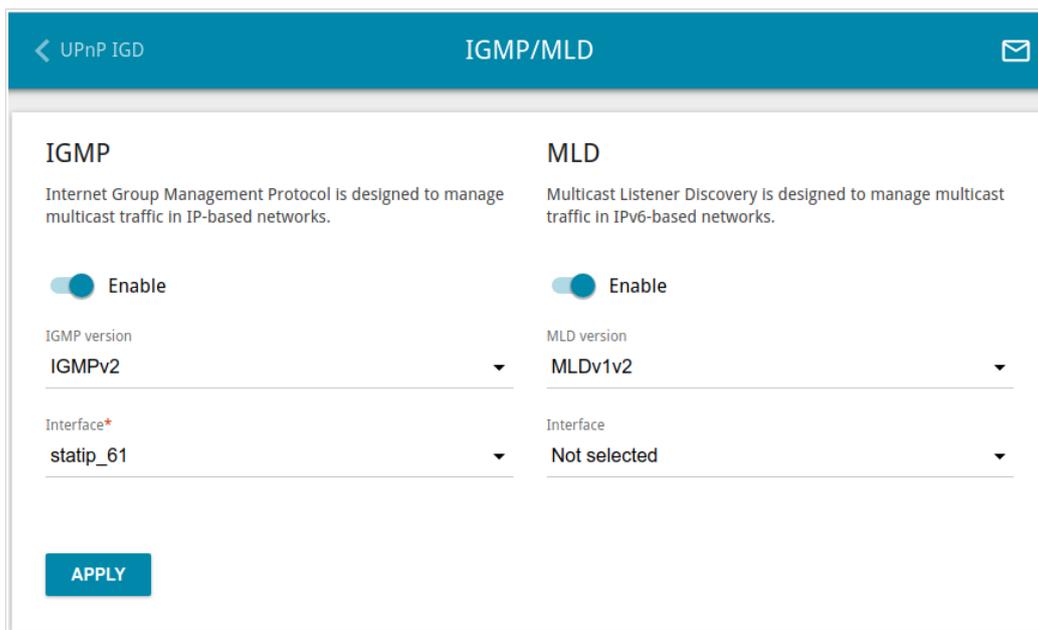


Figure 130. The **Advanced / IGMP/MLD** page.

The following elements are available on the page:

Parameter	Description
<b>IGMP</b>	
<b>Enable</b>	Move the switch to the right to enable IGMP.
<b>IGMP version</b>	Select a version of IGMP from the drop-down list.
<b>Interface</b>	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).

Parameter	Description
<b>MLD</b>	
<b>Enable</b>	Move the switch to the right to enable MLD.
<b>MLD version</b>	Select a version of MLD from the drop-down list.
<b>Interface</b>	From the drop-down list, select a connection of the Dynamic IPv6 or Static IPv6 type for which you need to allow multicast traffic (e.g. streaming video).

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

## ALG/Passthrough

On the **Advanced / ALG/Passthrough** page, you can allow the router to use RTSP, enable the SIP ALG and PPPoE/PPTP/L2TP/IPsec pass through functions.

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.

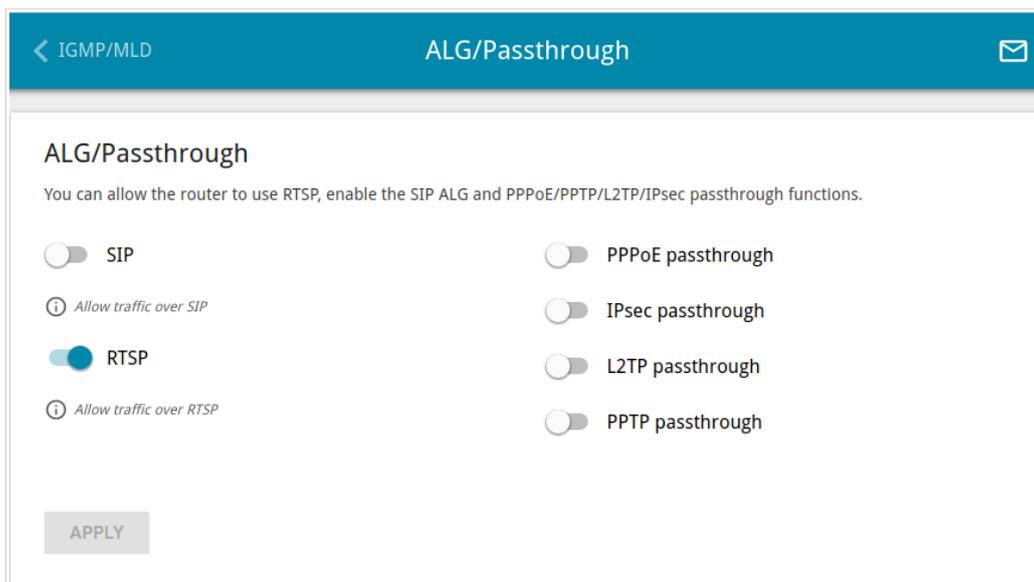


Figure 131. The **Advanced / ALG/Passthrough** page.

The following elements are available on the page:

Parameter	Description
<b>SIP</b>	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. <sup>6</sup>
<b>RTSP</b>	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.
<b>PPPoE pass through</b>	Move the switch to the right to enable the PPPoE pass through function.
<b>IPsec pass through</b>	Move the switch to the right to enable the IPsec pass through function.
<b>L2TP pass through</b>	Move the switch to the right to enable the L2TP pass through function.
<b>PPTP pass through</b>	Move the switch to the right to enable the PPTP pass through function.

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

<sup>6</sup> On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **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).

## IPsec

On the **Advanced / IPsec** page, you can configure VPN tunnels based on IPsec protocol. IPsec is a protocol suite for securing IP communications.

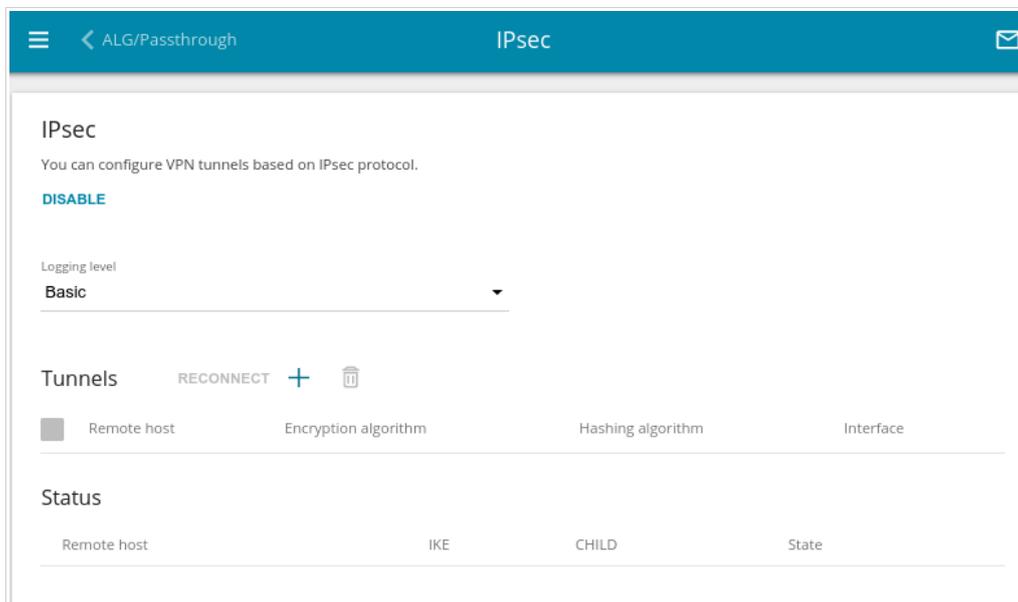


Figure 132. The **Advanced / IPsec** page.

To allow IPsec tunnels, click the **ENABLE** button. Upon that the **Tunnels** and **Status** sections and the **Logging level** drop-down list are displayed on the page.

In the **Status** section, the current state of an existing tunnel is displayed.

From the **Logging level** drop-down list, select a detail level of messages recorded to the system log or leave the value specified by default. The **Basic** value is recommended to establish an IPsec tunnel faster. To view the log, go to the **System / Log** page (see the **Log** section, page 208).

To create a new tunnel, click the **ADD** button (  ) in the **Tunnels** section.



Setting for both devices which establish the tunnel should be the same.

The screenshot shows the 'IPsec/Adding' configuration page. The 'General Settings' section includes the following fields and options:

- Enable:** A toggle switch that is currently turned on (blue).
- Name\*:** A text input field containing 'ipsec\_15'.
- IP version:** A dropdown menu set to 'IPv4'.
- Dynamic IPsec:** A toggle switch that is currently turned off (grey).
- Type:** A dropdown menu set to 'Address'.
- Remote host\*:** An empty text input field.
- Remote Identifier:** An empty text input field.
- Remote port:** An empty text input field.
- Pre-shared key\*:** A text input field with a copy icon on the right.
- Local WAN:** A dropdown menu set to 'Default gateway'.
- Local identifier:** An empty text input field.
- Local port:** An empty text input field.
- NAT Traversal:** A dropdown menu set to 'Enabled'.
- Mode:** A dropdown menu set to 'TUNNEL'.
- Enable DPD:** A toggle switch that is currently turned on (blue).
- DPD - Dead Peer Detection:** A sub-section containing:
  - DPD delay (in seconds)\*:** A text input field containing '30'.
  - DPD timeout (in seconds)\*:** A text input field containing '120'.
  - TCP MSS:** A dropdown menu set to 'Path MTU discovery'.
- Allow traffic from IPsec to router:** A toggle switch that is currently turned on (blue).

Figure 133. The page for adding an IPsec tunnel. The **General Settings** section.

You can specify the following parameters:

Parameter	Description
<b>General Settings</b>	
<b>Enable</b>	Move the switch to the right to enable the tunnel. Move the switch to the left to disable the tunnel.

Parameter	Description
<b>Name</b>	A name for the tunnel for easier identification. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout. <sup>7</sup>
<b>IP version</b>	An IP version.
<b>Dynamic IPsec</b>	Move the switch to the right to allow a remote host with any public IP address to connect to the router via IPsec protocol. Such a setting can be specified for one IPsec tunnel only. Connection requests via this tunnel can be sent by a remote host only.
<b>Type</b>	Select an identification method for the remote host (router) from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Address</b>: The remote host is identified by its IP address.</li> <li>• <b>FQDN</b>: The remote host is identified by its domain name.</li> </ul> The drop-down list is displayed if the <b>Dynamic IPsec</b> switch is moved to the left.
<b>Remote host</b>	Enter the remote subnet VPN gateway IP address if the <b>Address</b> value is selected from the <b>Type</b> drop-down list. Enter the remote subnet VPN gateway domain name if the <b>FQDN</b> value is selected from the <b>Type</b> drop-down list. The field is available for editing if the <b>Dynamic IPsec</b> switch is moved to the left.
<b>Remote identifier</b>	A remote host identifier to establish connection over IPsec with particular hosts only. To establish connection, DIR-822 remote identifier value should correspond to the local identifier value specified in the settings of the remote host. Use an IP address, domain name, or certificate CN. <i>Optional.</i>
<b>Remote port</b>	A port of the remote host, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If the field is left blank and the network address translation (NAT) function is used for the connection, port 4500 is used.
<b>Pre-shared key</b>	A PSK key for mutual authentication of the parties. Click the <b>Show</b> icon (🔑) to display the entered key.

<sup>7</sup> 0-9, A-Z, a-z, space, !"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~.

Parameter	Description
<b>Local WAN</b>	<p>A WAN connection through which the tunnel will pass. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Interface:</b> When this value is selected, the <b>Interface</b> drop-down list is displayed. Select an existing WAN connection from the list.</li> <li>• <b>Default gateway:</b> When this value is selected, the router uses the default WAN connection.</li> </ul>
<b>Local identifier</b>	<p>A local identifier of the router to establish connection over IPsec with particular hosts only. To establish connection, DIR-822 local identifier value should correspond to the remote identifier value specified in the settings of the remote host. Use an IP address, domain name, or certificate CN. <i>Optional.</i></p>
<b>Local port</b>	<p>A port of the router, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If the field is left blank and the network address translation (NAT) function is used for the connection, port 4500 is used.</p>
<b>NAT Traversal</b>	<p>The NAT Traversal function allows VPN traffic to pass through the NAT-enabled device. DIR-822 allows to forcibly encapsulate VPN traffic in UDP packets for passing through a remote device regardless of whether it supports address translation.</p> <p>If you need to enable forced encapsulation of VPN traffic, select the <b>Enabled</b> value.</p> <p>If you need to disable forced encapsulation of VPN traffic, select the <b>Disabled</b> value.</p>
<b>Mode</b>	<p>An operation mode of the IPsec tunnel. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>TUNNEL:</b> As a rule, it is used to create a secure connection to remote networks. In this mode, the source IP packet is fully encrypted and added to a new IP packet and data transfer is based on the header of the new IP packet.</li> <li>• <b>TRANSPORT:</b> As a rule, it is used to encrypt data stream within one network. In this mode, only the content of the source IP packet is encrypted, its header remains unchanged and data transfer is based on the source header.</li> </ul>
<b>Allow traffic from IPsec to router</b>	<p>Move the switch to the left to deny access to your router from the remote subnet via IPsec. The switch is displayed when the <b>TUNNEL</b> value is selected from the <b>Mode</b> drop-down list.</p>

Parameter	Description
<b>Enable DPD</b>	Move the switch to the right to enable using DPD protocol for this tunnel. Such a setting allows to check the status of the remote host: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD messages to the remote host. If the switch is moved to the left, the <b>DPD delay</b> and <b>DPD timeout</b> fields are not available for editing.
<b>DPD delay</b>	A time period (in seconds) between DPD messages. By default, the value <b>30</b> is specified.
<b>DPD timeout</b>	A waiting period for the response to a DPD message (in seconds). If the host does not answer in the specified time, the router breaks down the tunnel connection, updates information on it, and tries to reestablish the connection. By default, the value <b>120</b> is specified.
<b>TCP MSS</b>	<p><i>Maximum Segment Size of a TCP packet.</i> This parameter influences the size of a TCP packet which will be sent from the remote host to the router.</p> <p>If the <b>Manual</b> value is selected, you can specify the value of this parameter for each subnet of the tunnel in the <b>MTU</b> field. The field is displayed in the window for adding a subnet in the <b>Tunneled Networks</b> section.</p> <p>If the <b>Path MTU discovery</b> value is selected, the parameter will be configured automatically for all created subnets.</p>

The First Phase	The Second Phase
First phase encryption algorithm <b>DES</b>	Second phase encryption algorithm <b>DES</b>
Encryption mode <b>CBC</b>	Encryption mode <b>CBC</b>
Hashing algorithm <b>MD5</b>	Hashing algorithm <b>MD5</b>
Size of hash <b>96</b>	Size of hash <b>96</b>
Hashing mode <b>HMAC</b>	Hashing mode <b>HMAC</b>
First phase DHgroup type <b>MODP768</b>	<input checked="" type="checkbox"/> Enable PFS
IKE-SA lifetime* <b>10800</b>	Second phase DHgroup type <b>MODP768</b>
<input type="checkbox"/> Aggressive Mode	IPsec-SA lifetime* <b>3600</b>
IKE version <b>1</b>	

Figure 134. The page for adding an IPsec tunnel. **The First Phase / The Second Phase** sections.

Parameter	Description
<b>The First Phase</b>	
<b>First phase encryption algorithm</b>	Select an available encryption algorithm from the drop-down list.
<b>Encryption mode</b>	Select an encryption mode from the drop-down list.
<b>Hashing algorithm</b>	Select a hashing algorithm from the drop-down list.
<b>Size of hash</b>	The length of the hash in bits.
<b>Hashing mode</b>	Select a hashing mode from the drop-down list.
<b>First phase DHgroup type</b>	A Diffie-Hellman key group for the First Phase. Select a value from the drop-down list.
<b>IKE-SA lifetime</b>	The lifetime of IKE-SA keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should be greater than the value specified in the <b>IPsec-SA lifetime</b> field.
<b>Aggressive Mode</b>	Move the switch to the right to enable the aggressive mode for mutual authentication of the parties. Such a setting accelerates the connection establishment, but reduces its security.

Parameter	Description
<b>IKE version</b>	IKE ( <i>Internet Key Exchange</i> ) is a protocol of keys exchange between two hosts of VPN connections. Select a version of the protocol from the drop-down list.
<b>The Second Phase</b>	
<b>Second phase encryption algorithm</b>	Select an available encryption algorithm from the drop-down list.
<b>Encryption mode</b>	Select an encryption mode from the drop-down list.
<b>Hashing algorithm</b>	Select a hashing algorithm from the drop-down list.
<b>Size of hash</b>	The length of the hash in bits.
<b>Hashing mode</b>	Select a hashing mode from the drop-down list.
<b>Enable PFS</b>	Move the switch to the right to enable the PFS option ( <i>Perfect Forward Secrecy</i> ). If the switch is moved to the right, a new encryption key exchange will be used for the Second Phase. This option enhances the security level of data transfer, but increases the load on DIR-822.
<b>Second phase DHgroup type</b>	A Diffie-Hellman key group for the Second Phase. Select a value from the drop-down list. The drop-down list is available if the <b>Enable PFS</b> switch is moved to the right.
<b>IPsec-SA lifetime</b>	The lifetime of the Second Phase keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should be greater than zero.

To specify IP addresses of local and remote subnets for this tunnel, click the **ADD** button (  ) in the **Tunneled Networks** section.

If the IPsec tunnel operates over IKEv1 (**1** is selected from the **IKE version** list in the **The First Phase** section), you can create only one subnet.

If the IPsec tunnel operates over IKEv2 (**2** is selected from the **IKE version** list in the **The First Phase** section), you can create several subnets.

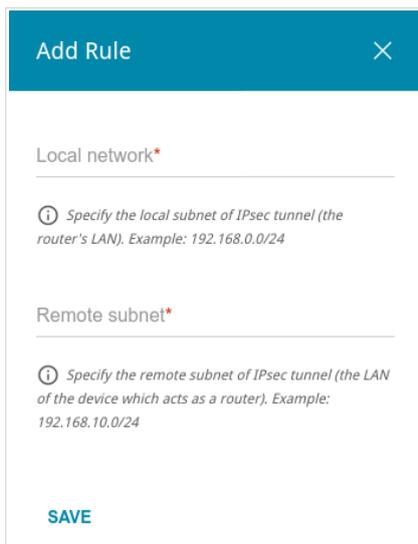


Figure 135. The page for adding an IPsec tunnel. The window for adding a tunneled network.

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

Parameter	Description
<b>Local network</b>	A local subnet IP address and mask.
<b>Remote subnet</b>	A remote subnet IP address and mask.
<b>MTU</b>	The maximum size (in bytes) of a non-fragmented packet. The field is displayed when the <b>Manual</b> value is selected from the <b>TCP MSS</b> drop-down list in the <b>General Settings</b> section.

To edit fields in the **Tunneled Networks** section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

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

After configuring all needed settings for the IPsec tunnel, click the **APPLY** button.

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

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

To disable VPN tunnels based on IPsec protocol, click the **DISABLE** button.

## Firewall

In this menu you can configure the firewall of the router:

- add rules for IP filtering
- create virtual servers
- define a DMZ
- configure the MAC filter
- specify restrictions on access to certain web sites
- enable the function of blocking advertisements
- create rules for remote access to the web-based interface.

### IP Filter

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

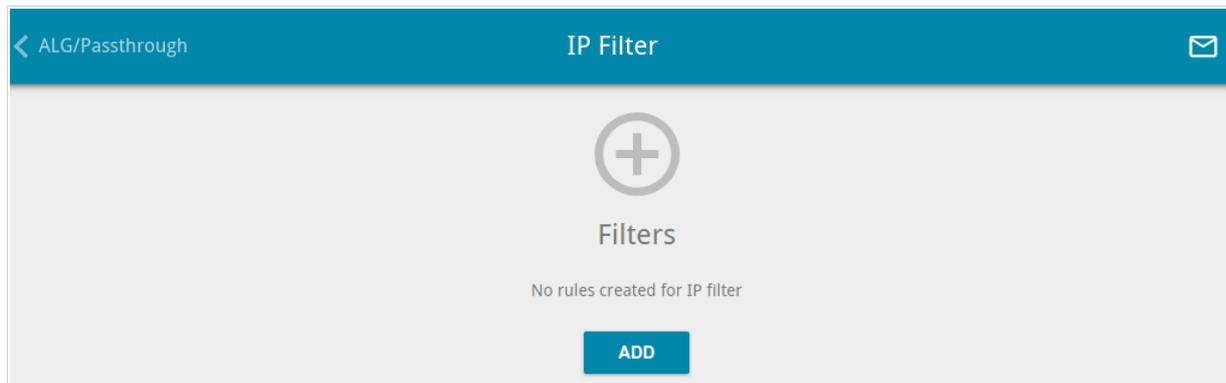


Figure 136. The **Firewall / IP Filter** page.

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

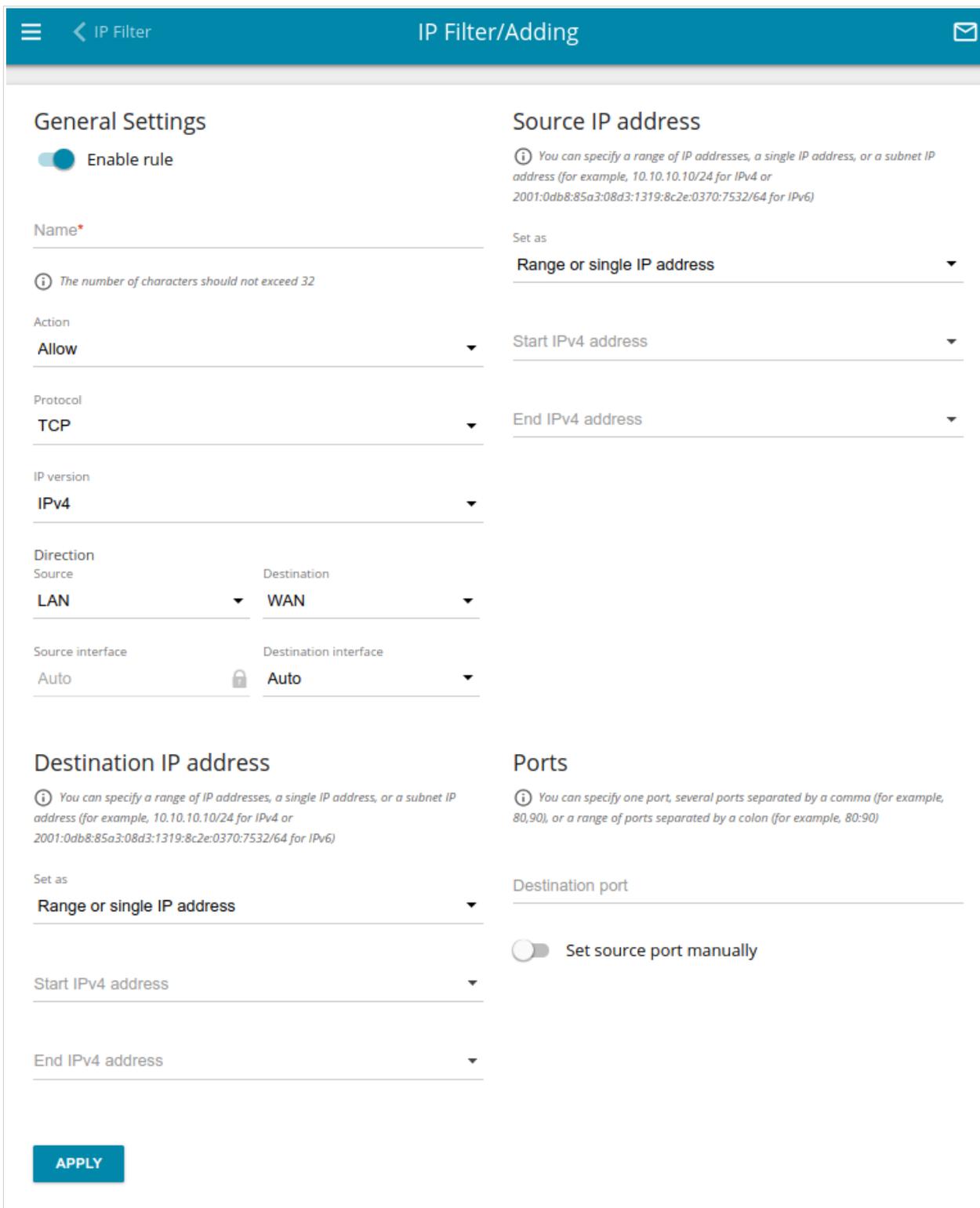


Figure 137. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
<b>General Settings</b>	
<b>Enable rule</b>	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.

Parameter	Description
<p><b>Name</b></p>	<p>A name for the rule for easier identification. You can specify any name.</p>
<p><b>Action</b></p>	<p>Select an action for the rule.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>: Allows packet transmission in accordance with the criteria specified by the rule.</li> <li>• <b>Deny</b>: Denies packet transmission in accordance with the criteria specified by the rule.</li> </ul>
<p><b>Protocol</b></p>	<p>A protocol for network packet transmission. Select a value from the drop-down list.</p>
<p><b>IP version</b></p>	<p>An IP version to which the rule will be applied. Select the relevant value from the drop-down list.</p>
<p><b>Direction</b></p>	<p>The direction of network packet transmission to which the rule will be applied. Select the source of the packet direction from the <b>Source</b> drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>WAN</b>: The rule will be applied to the packets transmitted from the external network.</li> <li>• <b>LAN</b>: The rule will be applied to the packets transmitted from the local network.</li> <li>• <b>IPsec</b>: The rule will be applied to the packets transmitted from the IPsec tunnel (<i>available if an IPsec tunnel has been created on the device</i>).</li> </ul> <p>Select the destination of the packet direction from the <b>Destination</b> drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Router</b>: The rule will be applied to the packets transmitted to DIR-822.</li> <li>• <b>WAN</b>: The rule will be applied to the packets transmitted to the external network.</li> <li>• <b>LAN</b>: The rule will be applied to the packets transmitted to the local network.</li> <li>• <b>IPsec</b>: The rule will be applied to the packets transmitted to the IPsec tunnel (<i>available if an IPsec tunnel has been created on the device</i>).</li> </ul> <p>From the <b>Source interface</b> and <b>Destination interface</b> drop-down lists, select source and destination interfaces for which the rule will be applied. Leave the <b>Auto</b> values to apply the rule to all created WAN interfaces.</p>

Parameter	Description
<b>Source IP Address</b>	
<b>Set as</b>	Select the needed value from the drop-down list.
<b>Start IPv4 address / Start IPv6 address</b>	<p>The source host start IPv4 or IPv6 address.</p> <p>If it is necessary to specify a single address, leave the <b>End IPv4 address / End IPv6 address</b> field blank.</p> <p>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).</p>
<b>End IPv4 address / End IPv6 address</b>	The source host end IPv4 or IPv6 address.
<b>Subnet IPv4 address / Subnet IPv6 address</b>	The source subnet IPv4 or IPv6 address. The field is displayed when the <b>Subnet</b> value is selected from the <b>Set as</b> drop-down list.
<b>Destination IP Address</b>	
<b>Set as</b>	Select the needed value from the drop-down list.
<b>Start IPv4 address / Start IPv6 address</b>	<p>The destination host start IPv4 or IPv6 address.</p> <p>If it is necessary to specify a single address, leave the <b>End IPv4 address / End IPv6 address</b> field blank.</p> <p>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).</p>
<b>End IPv4 address / End IPv6 address</b>	The destination host end IPv4 or IPv6 address.
<b>Subnet IPv4 address / Subnet IPv6 address</b>	The destination subnet IPv4 or IPv6 address. The field is displayed when the <b>Subnet</b> value is selected from the <b>Set as</b> drop-down list.
<b>Ports</b>	
<b>Destination port</b>	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.
<b>Set source port manually</b>	Move the switch to the right to specify a port of the source IP address manually. Upon that the <b>Source port</b> field is displayed.
<b>Source port</b>	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 set a schedule for the IP filter rule, click the **Set schedule** icon (  ) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 204) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the IP filter rule at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the IP filter rule at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

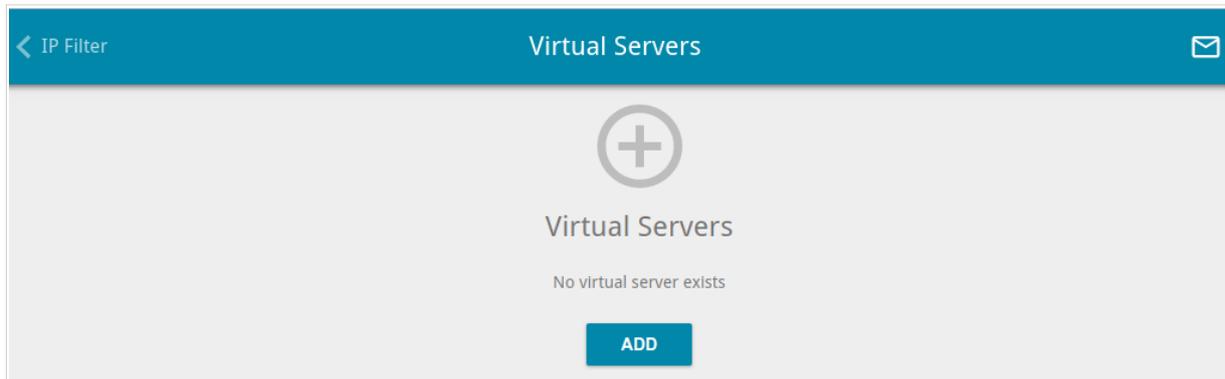
To edit a rule, select the relevant line in the table. In the opened window, change the needed parameters and click the **APPLY** button.

To change or delete the schedule for a rule, click the **Edit schedule** icon (  ) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** 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.

## Virtual Servers

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



*Figure 138. The Firewall / Virtual Servers page.*

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

Figure 139. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
<b>General Settings</b>	
<b>Enable</b>	Move the switch to the right to enable the server. Move the switch to the left to disable the server.

Parameter	Description
<b>Name</b>	A name for the virtual server for easier identification. You can specify any name.
<b>Template</b>	Select a virtual server template from the drop-down list, or select <b>Custom</b> to specify all parameters of the new virtual server manually.
<b>Interface</b>	A WAN connection to which this virtual server will be assigned.
<b>Protocol</b>	A protocol that will be used by the new virtual server. Select a value from the drop-down list.
<b>NAT Loopback</b>	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).
<b>Public Network Settings</b>	
<b>Remote IP</b>	Enter the IP address of the server from the external network. To add one more IP address, click the <b>ADD REMOTE IP</b> button and enter the address in the displayed line. To remove the IP address, click the <b>Delete</b> icon (✕) in the line of the address.
<b>Public port</b>	A port of the router from which traffic is directed to the IP address specified in the <b>Private IP</b> field in the <b>Private Network Settings</b> section. You can specify one port or several ports separated by a comma.
<b>Private Network Settings</b>	
<b>Private IP</b>	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).
<b>Private port</b>	A port of the IP address specified in the <b>Private IP</b> field to which traffic is directed from the <b>Public port</b> . You can specify one port or several ports separated by a comma.

Click the **APPLY** button.

To set a schedule for a virtual server, click the **Set schedule** icon (🕒) in the line corresponding to this server. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 204) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the virtual server at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the virtual server at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** 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 change or delete the schedule for a server, click the **Edit schedule** icon (  ) in the line corresponding to this server. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** 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.

## 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 **Firewall / DMZ** page, you can specify the IP address of the DMZ host.

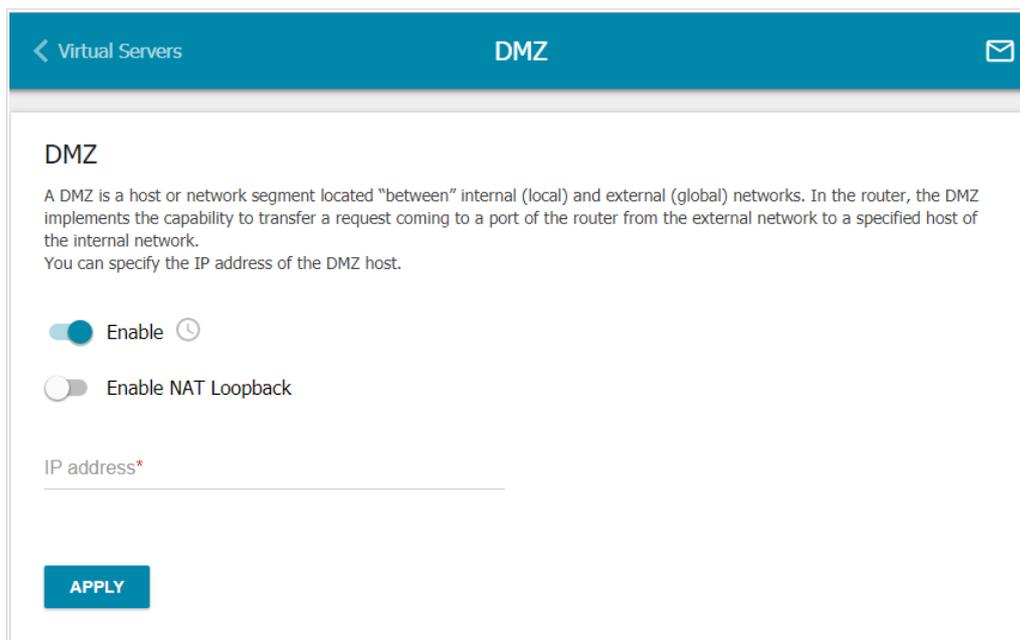


Figure 140. The **Firewall / DMZ** page.

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 **Firewall / DMZ** page.

To set a schedule for the DMZ, click the **Set schedule** icon (  ). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 204) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the DMZ for the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the DMZ for the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

To change or delete the schedule for the DMZ, click the **Edit schedule** icon (  ). In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

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

## MAC Filter

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

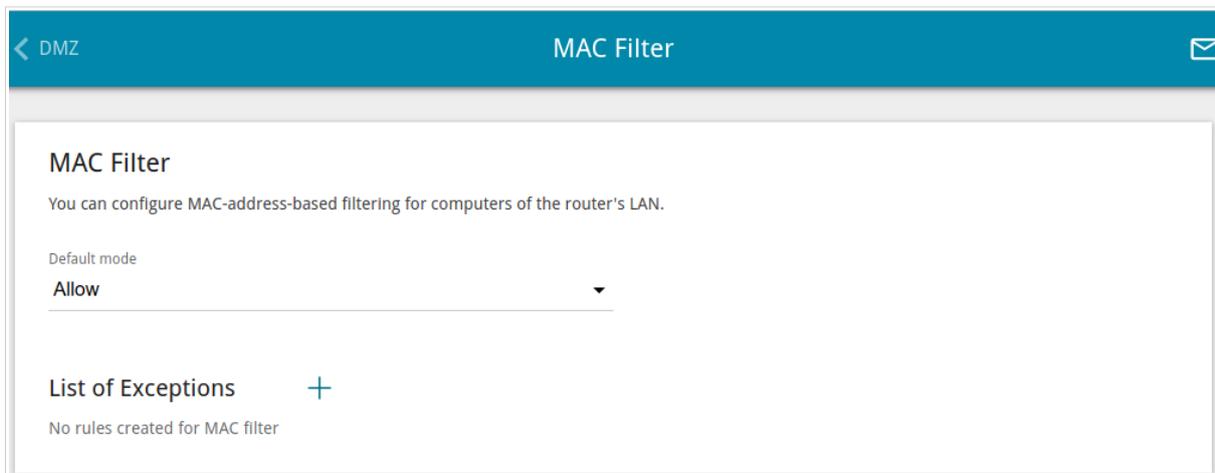


Figure 141. The **Firewall / MAC Filter** page.

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 ( **+** ).

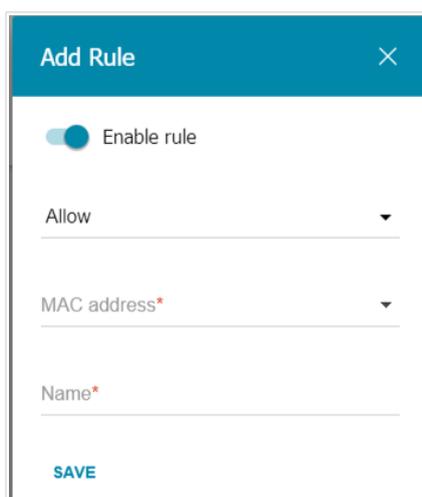


Figure 142. The window for adding a rule for the MAC filter.

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

Parameter	Description
<b>Enable rule</b>	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
<b>Action</b>	Select an action for the rule. <ul style="list-style-type: none"> <li>• <b>Deny</b>: Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices.</li> <li>• <b>Allow</b>: 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.</li> </ul>
<b>MAC address</b>	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).
<b>Name</b>	The name of the device for easier identification. You can specify any name.

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

To set a schedule for the MAC filter rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 204) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the MAC filter rule at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the MAC filter rule at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and 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 change or delete the schedule for a rule, click the **Edit schedule** icon (🕒) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** 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.

## URL Filter

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

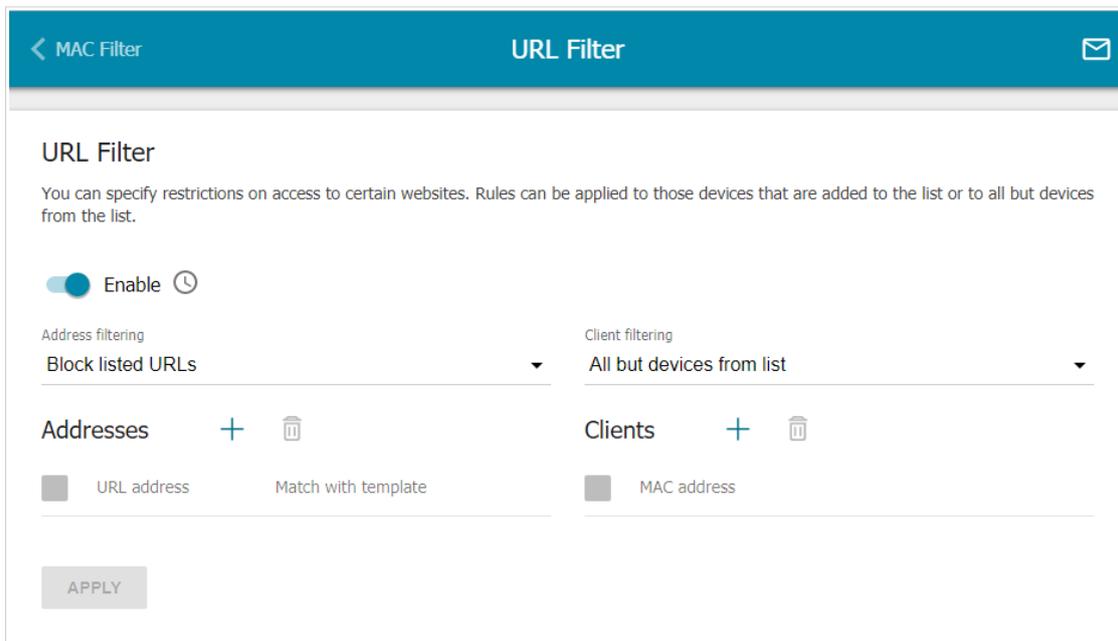


Figure 143. The **Firewall / URL Filter** page.

To enable the URL 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
<b>URL address</b>	A URL address, a part of URL address, or a keyword.
<b>Match with template</b>	<p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Full</b>: The request address should exactly match the value specified in the field above.</li> <li>• <b>Begin</b>: The request address should begin with the value specified in the field above.</li> <li>• <b>End</b>: The request address should end with the value specified in the field above.</li> <li>• <b>Partly</b>: The request address should contain the value specified in the field above in any part of it.</li> </ul>

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 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) and click the **SAVE** button.

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

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

To set a schedule for the URL filter, click the **Set schedule** icon (  ). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 204) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the URL filter for the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the URL filter for the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

To change or delete the schedule for URL filter, click the **Edit schedule** icon (  ) in the **URL Filter** section. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

## AdBlock

On the **Firewall / AdBlock** page, you can enable the function of blocking advertisements which appear during web surfing.

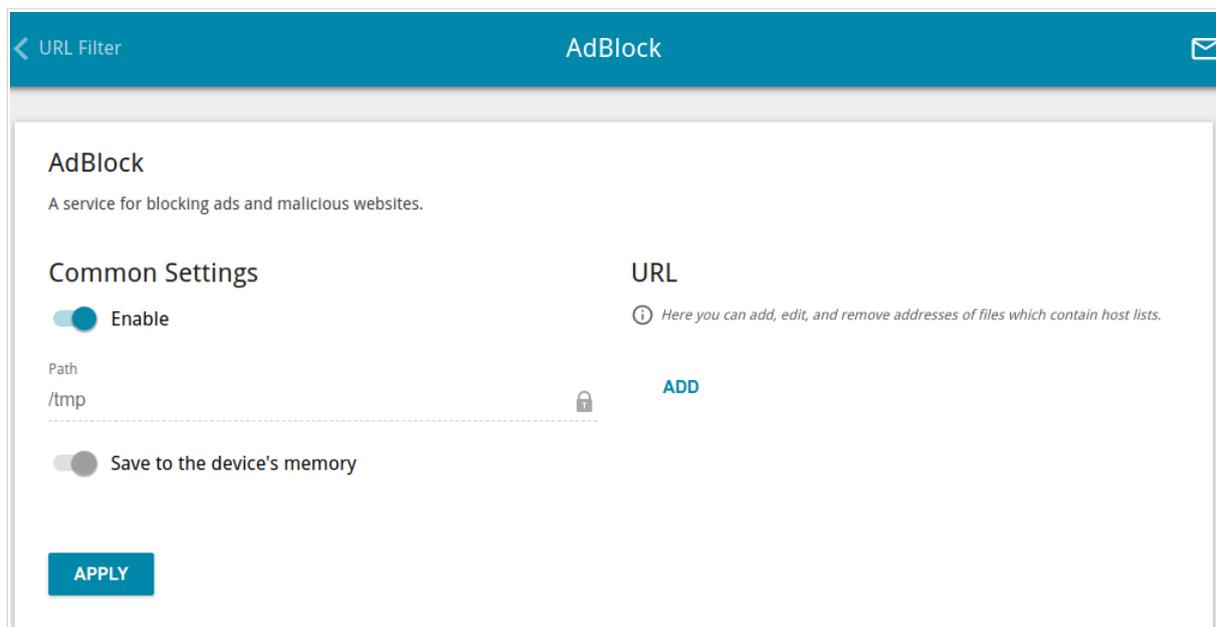


Figure 144. The **Firewall / AdBlock** page.

To enable the advertisements blocking function, in the **Common Settings** section, move the **Enable** switch to the right. Then in the **URL** section, click the **ADD** button and in the line displayed, enter a URL address of a file containing the list of advertising web sites which should be blocked. Click the **APPLY** button and wait while the file is being loaded to the device's memory.



Files saved to the device's memory are updated upon every reboot of the router or its or firmware update. In case the file is not available at that moment, the list of web sites to be blocked will not be received.

If you don't want to use a file for blocking advertisements any longer, click the **Delete** icon (✕) in the line of the URL address of the relevant file. Then click the **APPLY** button.

To disable the advertisements blocking function, move the **Enable** switch to the left and click the **APPLY** button.

## Remote Access

On the **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.

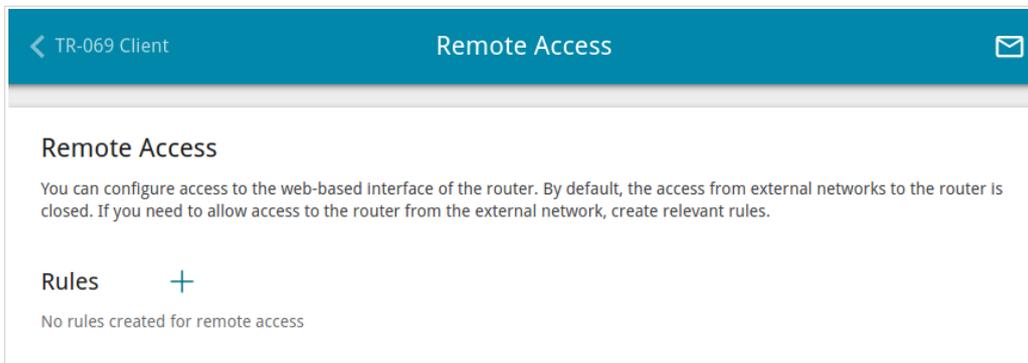


Figure 145. The **Advanced / Remote Access** page.

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

The screenshot shows a modal window titled 'Add Rule' with a close button (X) in the top right corner. The form contains several fields: 'Name\*' (text input), 'Interface' (dropdown menu with 'Automatic' selected), 'IP version' (dropdown menu with 'IPv4' selected), a toggle switch for 'Open access from any external host' (currently off), 'IP address\*' (text input), 'Mask\*' (text input), 'Public port\*' (text input with '80' entered), and 'Protocol' (dropdown menu with 'HTTP' selected). At the bottom of the form is a 'SAVE' button.

Figure 146. The window for adding a rule for remote management.

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

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

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

To set a schedule for the remote access rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 204) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the rule for remote access at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the rule for remote access at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and 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 change or delete the schedule for a rule, click the **Edit schedule** icon (🕒) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** 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 (🗑️).

## System

In this menu you can do the following:

- change the password used to access the router's settings
- restore the factory default settings
- create a backup of the router's configuration
- restore the router's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the router
- change the web-based interface language
- update the firmware of the router
- configure automatic notification on new firmware version
- enable/disable Wi-Fi connection and the Wi-Fi filter, configure automatic reboot of the device on a schedule, and set a schedule for different rules and settings of the firewall
- view the system log; configure sending the system log to a remote host
- check availability of a host on the Internet through the web-based interface of the router
- trace the route to a host
- allow or forbid access to the router via TELNET and SSH
- configure automatic synchronization of the system time or manually configure the date and time for the router
- enable the Auto Provision function.

## Configuration

On the **System / Configuration** 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 and SSH, 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, or change the web-based interface language.

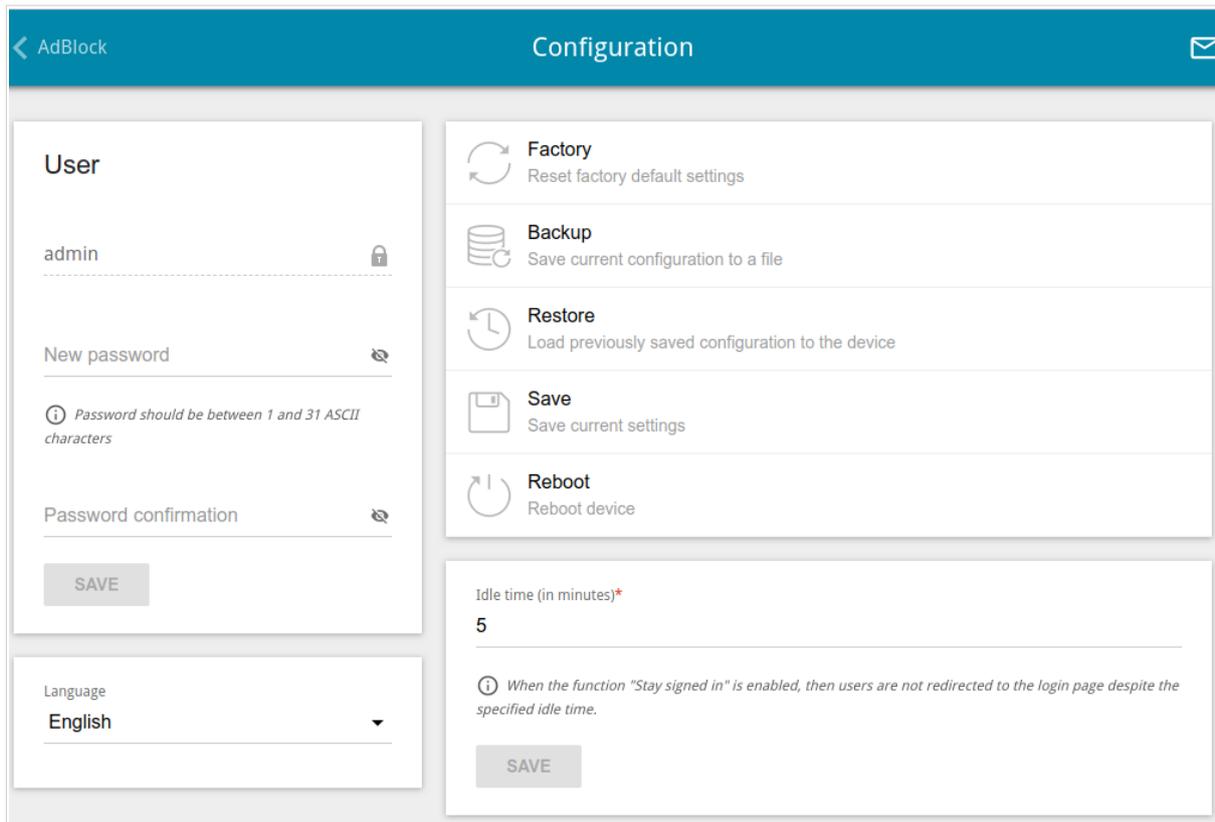


Figure 147. The **System / Configuration** page.

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.<sup>8</sup> 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 **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.

<sup>8</sup> 0-9, A-Z, a-z, space, !"#%&'()\*+,-./:;<=>?@[\\]^\_`{|}~.

The following buttons are also available on the page:

Control	Description
<b>Factory</b>	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware <b>RESET</b> button (see the <i>Back and Bottom Panels</i> section, page 16).
<b>Backup</b>	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.
<b>Restore</b>	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.
<b>Save</b>	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.
<b>Reboot</b>	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.

## Firmware Update

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

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

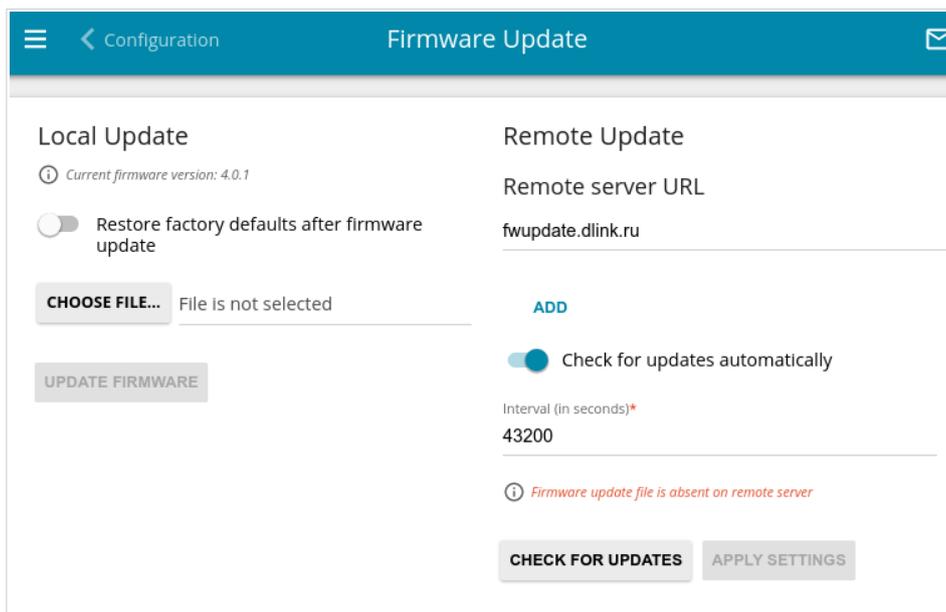


Figure 148. The **System / Firmware Update** page.

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 Initial Configuration Wizard and the **Static** value is selected from the **Mode of local IP address assignment** list on the **Connections Setup / LAN** 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. In the **Interval** field, specify the time period (in seconds) between checks or leave the value specified by default (**43200**).

By default, in the **Remote server URL** field, the D-Link update server address (**fwupdate.dlink.ru**) is specified. To add one more address, click the **ADD** button and enter the address in the displayed line. To remove the address, click the **Delete** icon ( **x** ) in the line of the address.

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](http://www.dlink.ru).
2. Click the **CHOOSE FILE** button in the **Local Update** section on the **System / Firmware Update** page to locate the new firmware file.
3. If you want to restore the factory default settings immediately after updating the firmware, move the **Restore factory defaults after firmware update** switch to the right.
4. Click the **UPDATE FIRMWARE** button.
5. Wait until the router is rebooted (about one and a half or two minutes).
6. 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 **System / Configuration** 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 **System / 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 **System / Configuration** page. Wait until the router is rebooted.

## Schedule

On the **System / Schedule** page, you can enable/disable Wi-Fi connection and the Wi-Fi filter, configure automatic reboot of the device on a schedule, and set a schedule for different rules and settings of the firewall.

**!** Before creating a schedule you need to configure automatic synchronization of the system time with a time server on the Internet(see the **System Time** section, page 216).

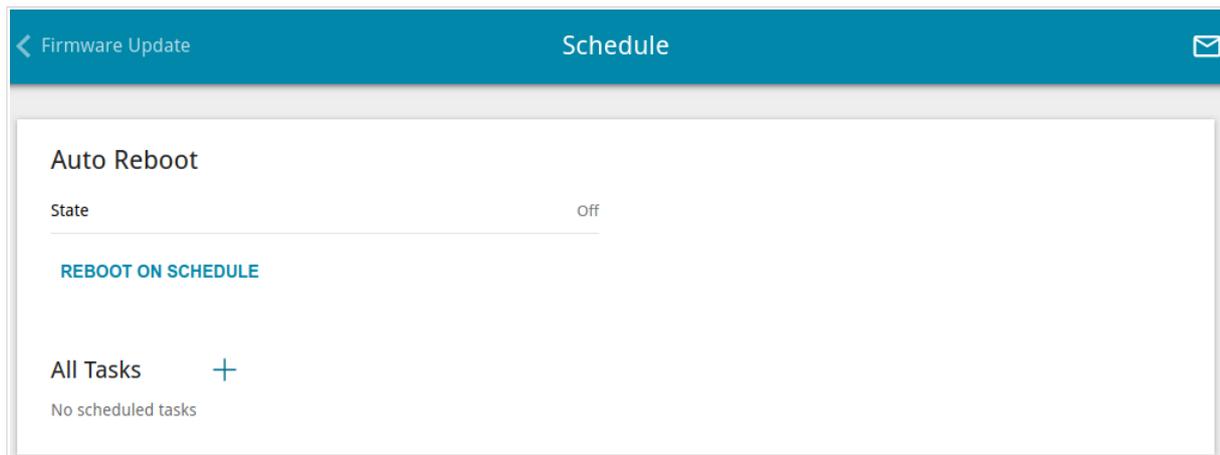


Figure 149. The **System / Schedule** page.

To configure automatic reboot of the device on a schedule, click the **REBOOT ON SCHEDULE** button in the **Auto Reboot** section.

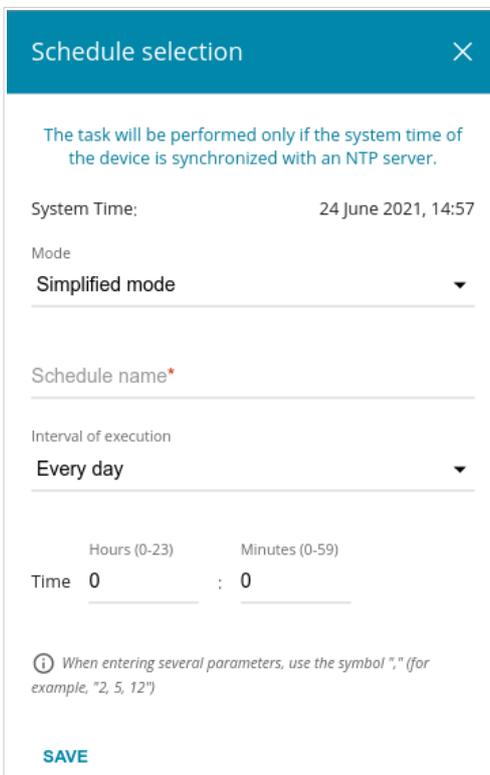


Figure 150. The window for configuring automatic reboot on a schedule.

In the opened window, in the **System Time** field, the system time of the device is displayed. You can select the **Simplified mode** value from the **Mode** drop-down list and specify the following parameters:

Parameter	Description
<b>Simplified mode</b>	
<b>Schedule name</b>	Specify a schedule name for easier identification. You can specify any name.
<b>Interval of execution</b>	Specify the time period for the device's reboot. <ul style="list-style-type: none"> <li>• <b>Every day</b>: When this value is selected, the <b>Time</b> field is displayed in the section.</li> <li>• <b>Every week</b>: When this value is selected, the names of days of the week and the <b>Time</b> field are displayed in the section.</li> <li>• <b>Every month</b>: When this value is selected, the <b>Day of month</b> and <b>Time</b> fields are displayed in the section.</li> </ul>
<b>Time</b>	Specify the time for the device's reboot.
<b>Days of week</b>	Select a day or days of the week when the device will be automatically rebooted. To do this, select the checkbox located to the left of the relevant value.
<b>Day of month</b>	Specify a day of the month. You can specify one value or several values separated by a comma.

In the advanced mode, you can specify more parameters for the schedule using a cron expression. To do this, select the **Advanced mode** value from the **Mode** drop-down list and specify the needed values in the fields displayed. You can specify one value or several values separated by a comma. You can use the character \* (asterisk) to specify the entire range of possible values. Upon that the **Schedule** field will be filled in automatically. In the **Schedule name** field, specify a schedule name for easier identification (you can specify any name).

Click the **SAVE** button.

To edit the automatic reboot schedule, click the **EDIT** button in the **Auto Reboot** section. In the opened window, change the needed parameters and click the **SAVE** button.

To disable automatic reboot of the device on a schedule, click the **EDIT** button in the **Auto Reboot** section. In the opened window, click the **DISABLE** button.

To set a schedule for a task which will be applied to a rule or setting of the firewall or will enable/disable Wi-Fi connection or Wi-Fi filter, click the **ADD** button ( **+** ) in the **All Tasks** section.

Figure 151. The window for adding a schedule for a task.

In the opened window, in the **System Time** field, the system time of the device is displayed. You can select the simplified mode of the schedule. To do this, select the **Simplified mode** value from the **Mode** drop-down list and specify the following parameters:

Parameter	Description
<b>Perform task on schedule</b>	Move the switch to the right to enable the schedule. Move the switch to the left to disable the schedule.
<b>Simplified mode</b>	
<b>Schedule name</b>	Specify a schedule name for easier identification. You can specify any name.

Parameter	Description
<b>Interval of execution</b>	Specify the time period for performing a task. <ul style="list-style-type: none"> <li>• <b>Every minute.</b></li> <li>• <b>Every hour:</b> When this value is selected, the <b>Time</b> field is displayed in the section.</li> <li>• <b>Every day:</b> When this value is selected, the <b>Time</b> field is displayed in the section.</li> <li>• <b>Every week:</b> When this value is selected, the names of days of the week and the <b>Time</b> field are displayed in the section.</li> <li>• <b>Every month:</b> When this value is selected, the <b>Day of month</b> and <b>Time</b> fields are displayed in the section.</li> </ul>
<b>Duration</b>	Specify the interval during which the task will be performing.
<b>Time</b>	Specify the time when the task should start running.
<b>Days of week</b>	Select a day or days of the week when the task will be performing. To do this, select the checkbox located to the left of the relevant value.
<b>Day of month</b>	Specify a day of the month. You can specify one value or several values separated by a comma.

In the advanced mode, you can specify more parameters for the schedule using a cron expression. To do this, select the **Advanced mode** value from the **Mode** drop-down list and specify the needed values in the fields displayed. You can specify one value or several values separated by a comma. You can use the character \* (asterisk) to specify the entire range of possible values. Upon that the **Schedule** field will be filled in automatically. In the **Schedule name** field, specify a schedule name for easier identification (you can specify any name).

You can also use the calendar mode to configure the schedule. To do this, select the **Calendar mode** value from the **Mode** drop-down list. In the **Schedule name** field, specify a schedule name for easier identification (you can specify any name). In the table, select cells corresponding to needed hours and days of the week. To deselect a cell, left-click it once again. To deselect all cells and select others, click the **RESET** button and select new cells.

Click the **SAVE** button.

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

To remove a schedule, in the **All Tasks** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (.

To assign a created schedule to a task which will be applied to a rule or setting of the firewall or will enable/disable Wi-Fi connection or Wi-Fi filter, go to the relevant page of the web-based interface of the device.

## Log

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

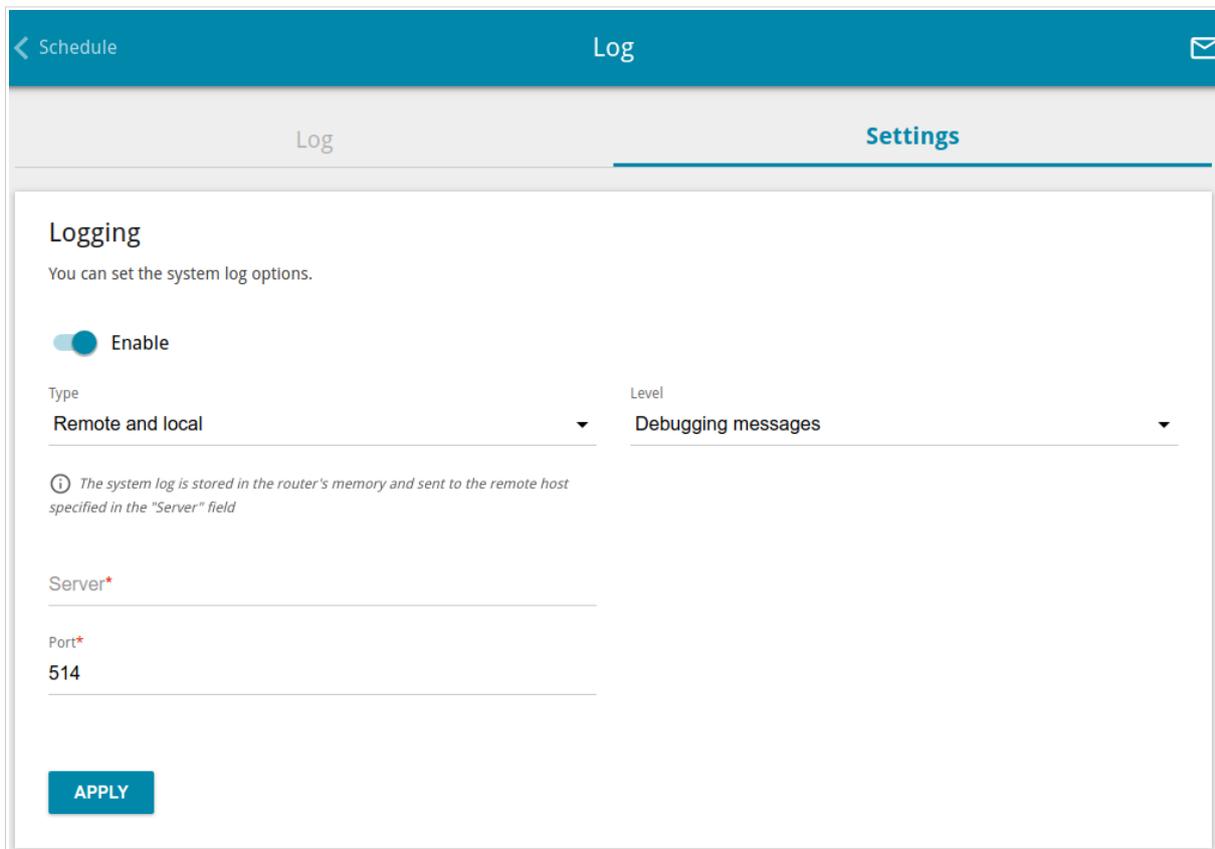


Figure 152. The **System / Log** page. The **Settings** tab.

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
<b>Logging</b>	
<b>Type</b>	<p>Select a type of logging from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Local:</b> The system log is stored in the router's memory. When this value is selected, the <b>Server</b> and <b>Port</b> fields are not displayed.</li> <li>• <b>Remote:</b> The system log is sent to the remote host specified in the <b>Server</b> field.</li> <li>• <b>Remote and local:</b> The system log is stored in the router's memory and sent to the remote host specified in the <b>Server</b> field.</li> </ul>
<b>Level</b>	Select a type of messages and alerts/notifications to be logged.
<b>Server</b>	The IP or URL address of the host from the local or global network, to which the system log will be sent.
<b>Port</b>	A port of the host specified in the <b>Server</b> field. By default, the value <b>514</b> 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.

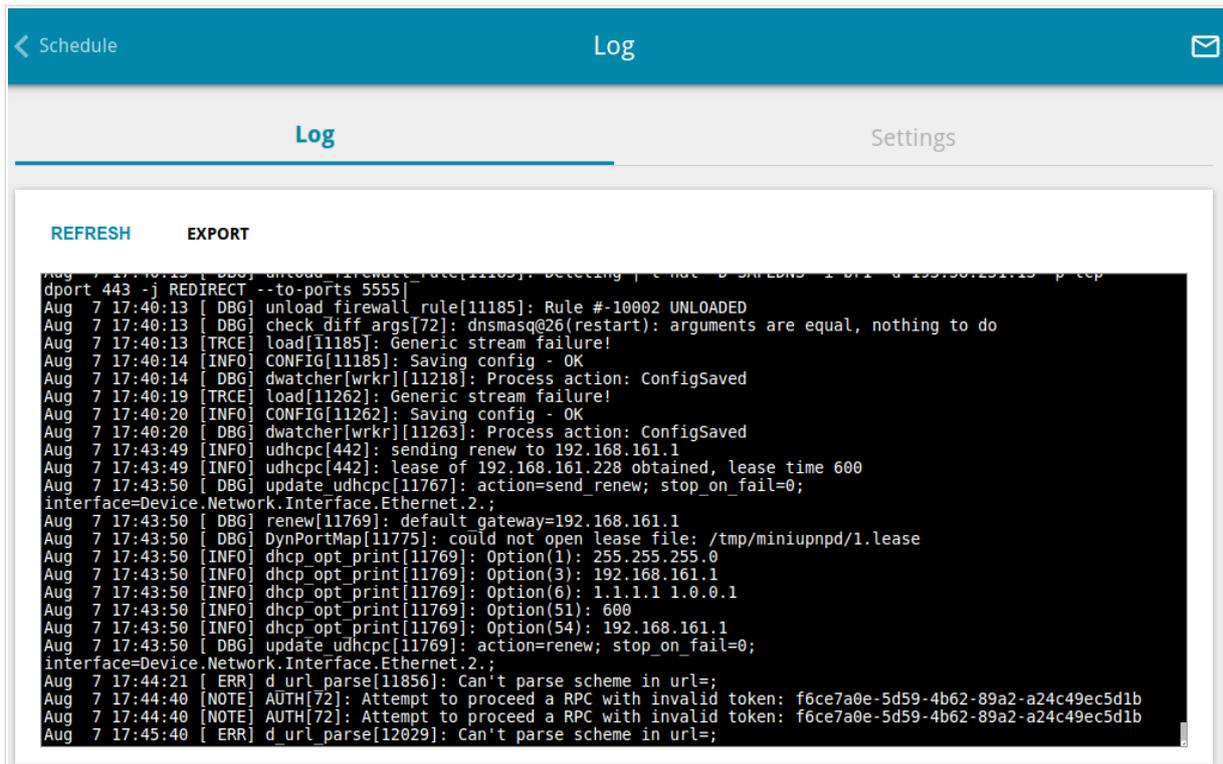


Figure 153. The System / Log page. The Log tab.

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.

## Ping

On the **System / 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.

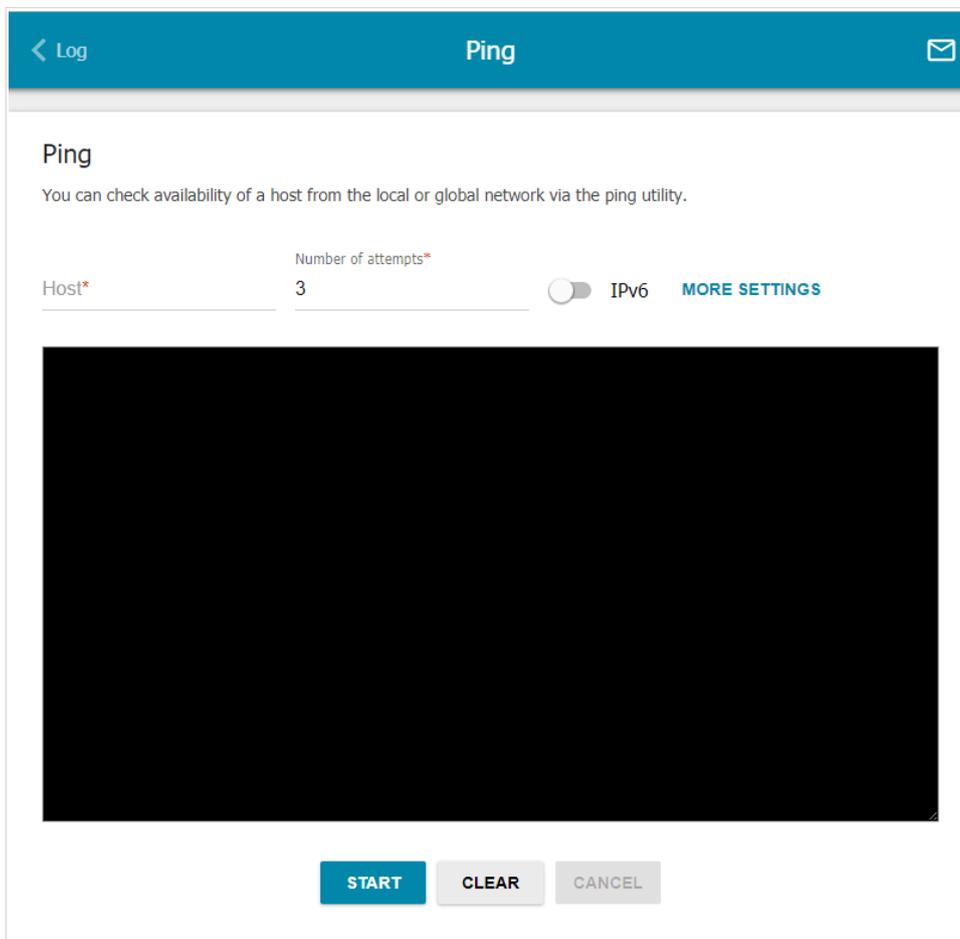


Figure 154. The **System / Ping** page.

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.

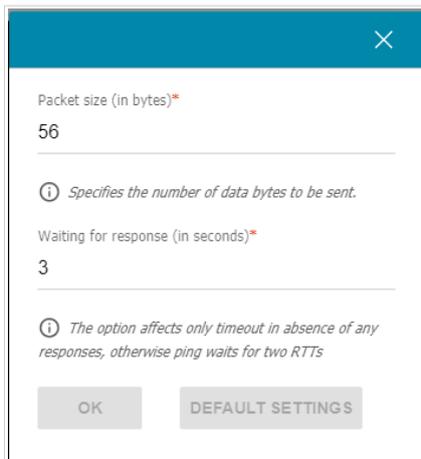


Figure 155. The **System / Ping** page. The additional settings window.

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.

If you need to interrupt the check, click the **CANCEL** button (the button is available from the moment the check starts).

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

## Traceroute

On the **System / Traceroute** page, you can determine the route of data transfer to a host via the traceroute utility.

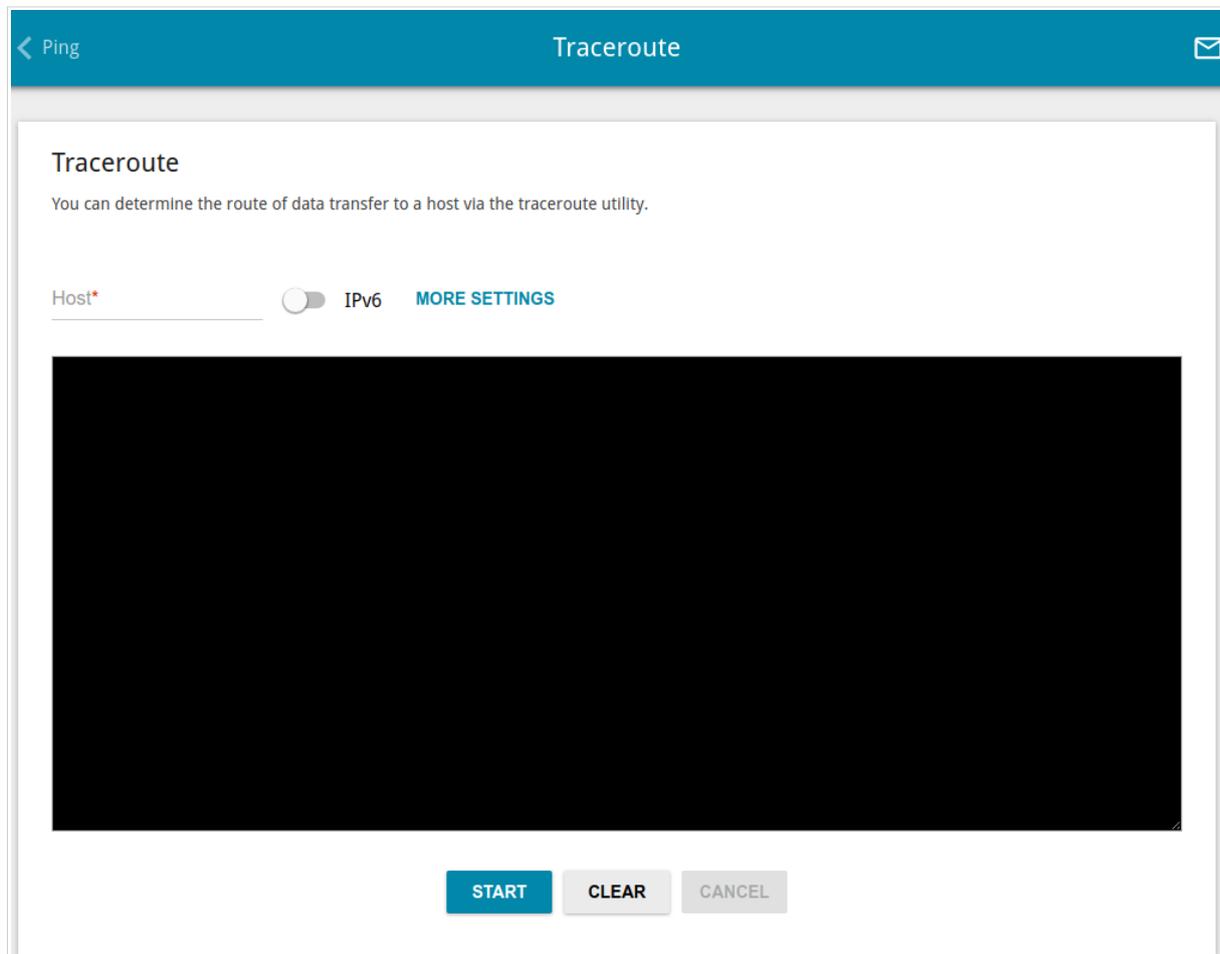


Figure 156. The **System / Traceroute** page.

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.

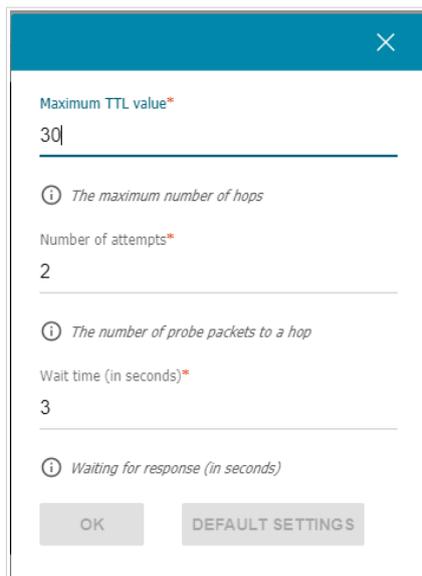


Figure 157. The **System / Traceroute** page. The additional settings window.

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

Parameter	Description
<b>Maximum TTL value</b>	Specify the TTL ( <i>Time to live</i> ) parameter value. The default value is <b>30</b> .
<b>Number of attempts</b>	The number of attempts to hit an intermediate host.
<b>Wait time</b>	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.

If you need to interrupt the check, click the **CANCEL** button (the button is available from the moment the check starts).

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

## Telnet/SSH

On the **System / Telnet/SSH** page, you can enable or disable access to the device settings via TELNET and/or SSH from your LAN. By default, access is disabled.

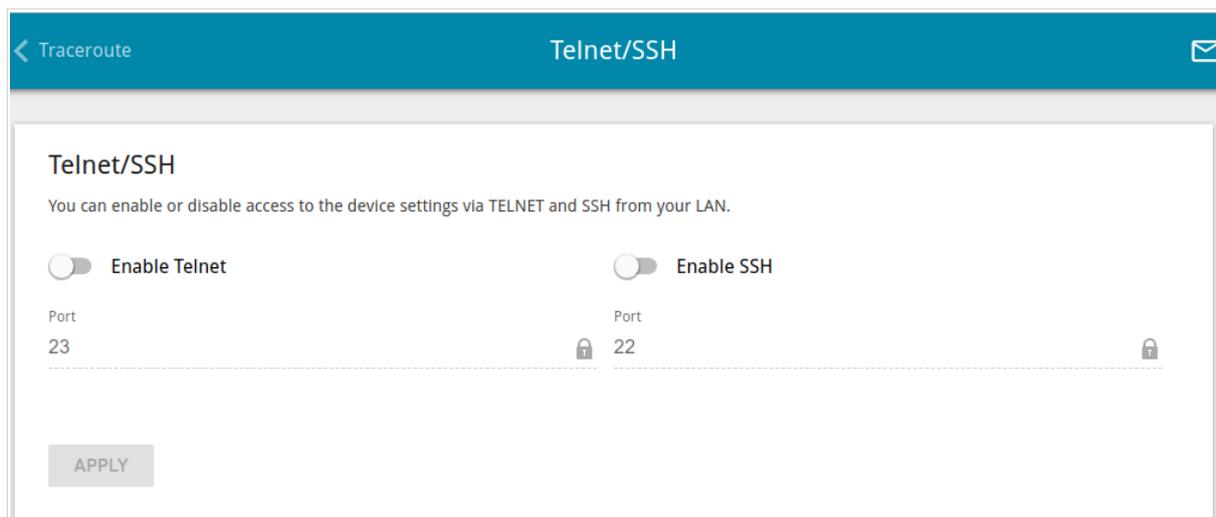


Figure 158. The **System / Telnet/SSH** page.

To enable access via TELNET and/or SSH, move the **Enable Telnet** switch and/or **Enable SSH** 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 for Telnet and the port **22** is specified for SSH). Then click the **APPLY** button.

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

## System Time

On the **System / 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.

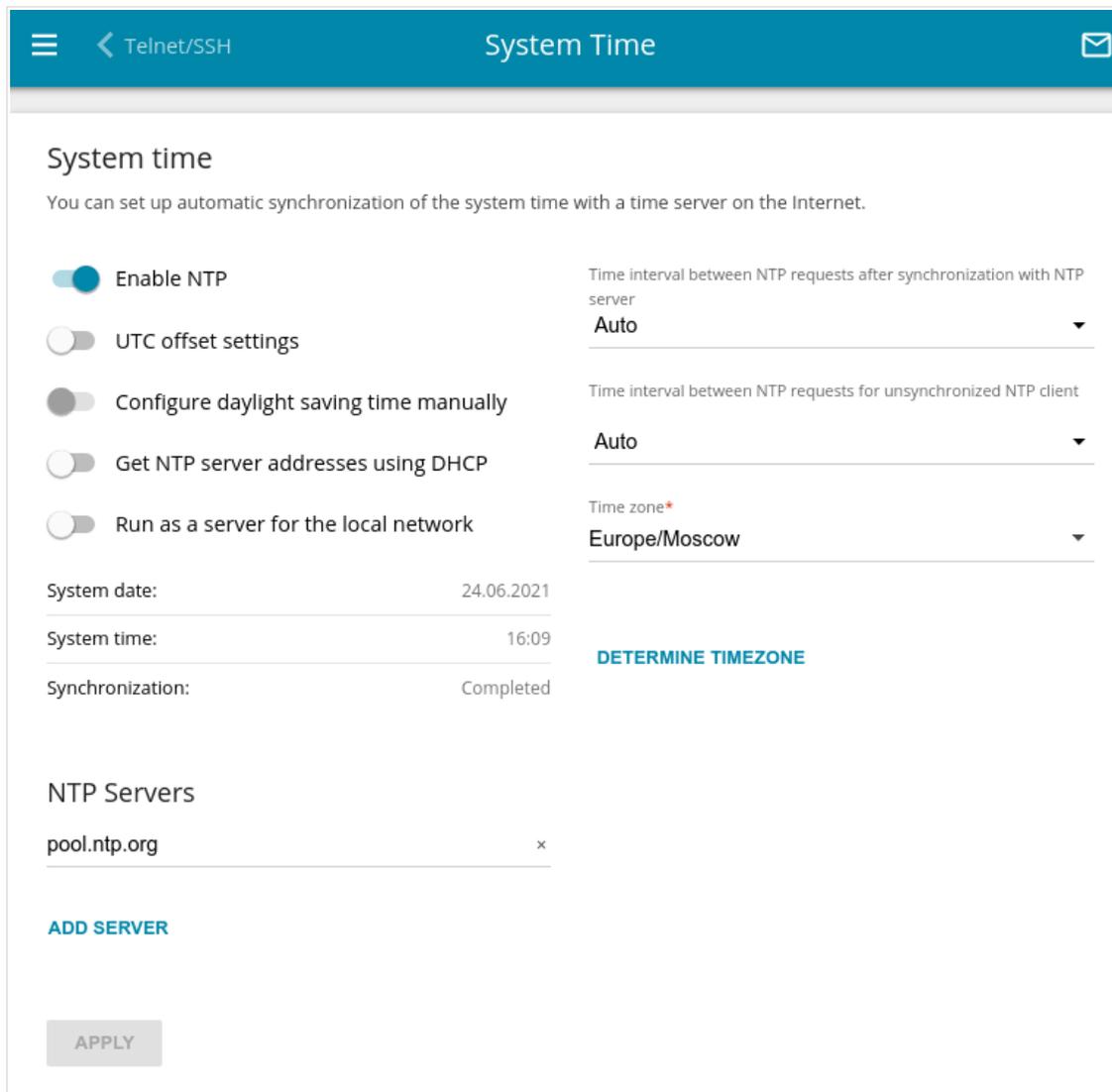


Figure 159. The **System / System Time** page.

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 up 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 **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 and the **Completed** value will be displayed in the **Synchronization** field.

Additional settings are also available on the page:

Parameter	Description
<b>UTC offset settings</b>	Move the switch to the right to set the UTC ( <i>Coordinated Universal Time</i> ) offset for the router clock manually. In the <b>UTC offset</b> field displayed, specify the required offset time (in minutes).
<b>Configure daylight saving time manually</b>	Move the switch to the right to configure settings for daylight saving time for the router clock manually. In the <b>Daylight Saving Time</b> section displayed, specify the required offset time for daylight saving time (in minutes), and specify the needed values in the <b>Beginning of daylight saving time</b> and <b>End of daylight saving time</b> sections.
<b>Get NTP server addresses using DHCP</b>	Move the switch to the right if NTP servers addresses are provided by your ISP. Contact your ISP to clarify if this setting needs to be enabled.  If the switch is moved to the right, the <b>NTP Servers</b> section is not displayed.
<b>Run as a server for the local network</b>	Move the switch to the right to allow connected devices to use the IP address of the router in the local subnet as a time server.
<b>Time interval between NTP requests after synchronization with NTP server</b>	From the drop-down list, select a time period (in seconds) after which a request to update the system time will be sent to the NTP server or leave the <b>Auto</b> value.
<b>Time interval between NTP requests for unsynchronized NTP client</b>	A time period (in seconds) after which a request to synchronize the system time will be sent to the NTP server. Select the needed value from the drop-down list. <ul style="list-style-type: none"> <li>• <b>Auto</b>: The time period is defined automatically.</li> <li>• <b>Manual</b>: The time period is defined in accordance with the value specified in the <b>Interval value</b> field.</li> </ul>
<b>Interval value</b>	Specify the time period (in seconds). The minimum acceptable value is 3.

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



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).

## Auto Provision

On the **System / Auto Provision** page, you can enable the Auto Provision function.

The Auto Provision function allows your ISP to manage the device's settings remotely: DIR-822 connects to the ISP's server, compares the current configuration file with the configuration file stored on this server, and updates its settings if the files are different.

Figure 160. The page for configuring the Auto Provision function.

You can specify the following parameters:

Parameter	Description
<b>Enable Auto Provision</b>	Move the switch to the right to enable the Auto Provision function. Move the switch to the left to disable the Auto Provision function.
<b>Use BOOTP option</b>	If the switch is moved to the right, the parameters of your ISP's server (the address, the location of the configuration file, and the protocol) are automatically specified using DHCP options 66 and 67. Upon that a connection of the Dynamic IPv4 type should be configured on the <b>Connections Setup / WAN</b> page. If the switch is moved to the left, the parameters of your ISP's server should be specified manually.
<b>Autoconfiguration server address</b>	The IP or URL address of your ISP's server where the configuration file is stored.
<b>File name</b>	The location of the configuration file on the ISP's server.

Parameter	Description
<b>File check period</b>	A time period (in seconds) between attempts to compare the current configuration file with the configuration file on the ISP's server.
<b>Protocol type</b>	A protocol for communication with the ISP's server where the configuration file is stored.

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

If you need to check manually if the current configuration file corresponds to the configuration file on the ISP's server, click the **CHECK STATUS** button. The check result will be displayed in the **Status** field. If the files are different, the device's settings will be updated.

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

**!** The Yandex.DNS service is unavailable when the SkyDNS service is enabled.

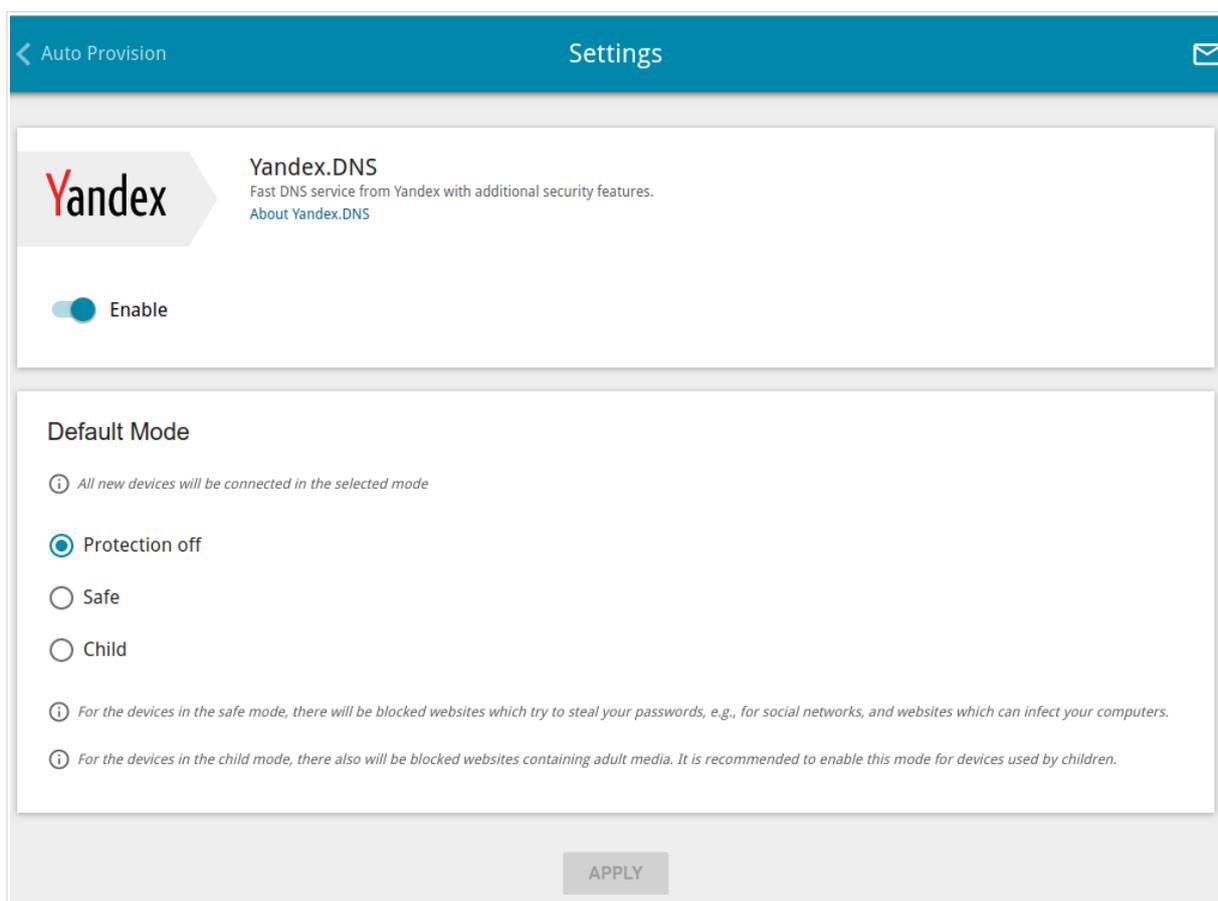


Figure 161. The **Yandex.DNS / Settings** page.

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

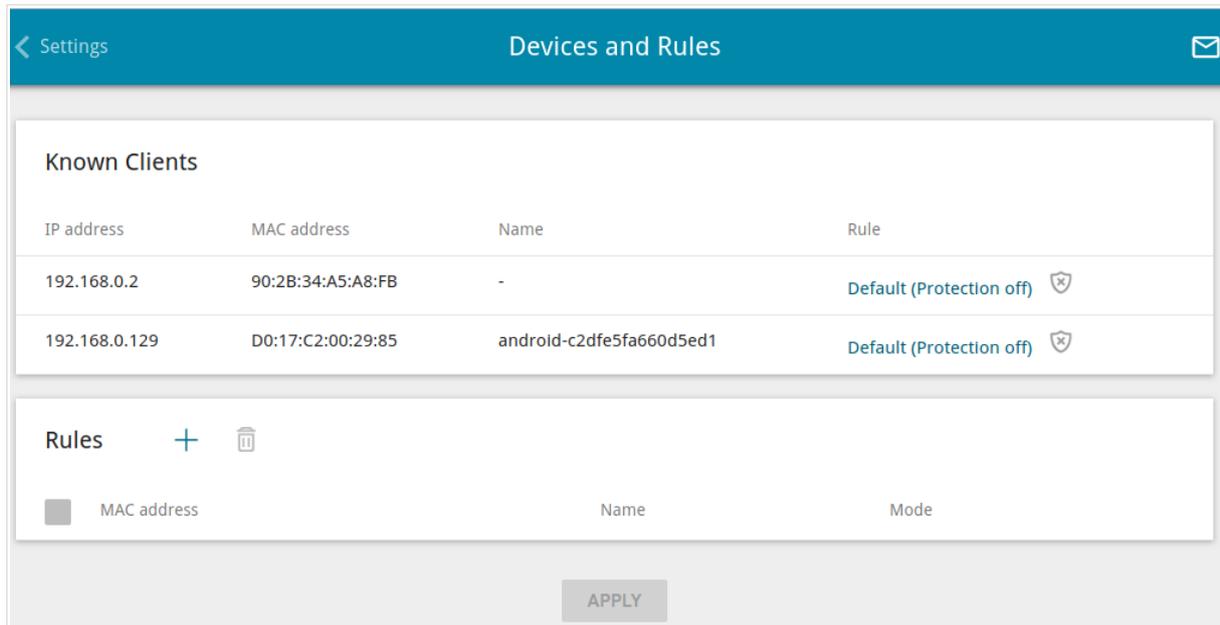


Figure 162. The **Yandex.DNS / Devices and Rules** page.

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.

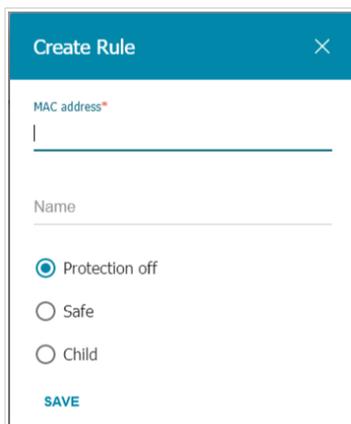


Figure 163. Adding a new rule for the **Yandex.DNS** service.

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

Parameter	Description
<b>MAC address</b>	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).
<b>Name</b>	Enter a name for the rule for easier identification. <i>Optional</i> .
<b>Mode</b>	Select an operating mode of the Yandex.DNS service for this rule. <ul style="list-style-type: none"> <li>• <b>Protection off:</b> When this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites.</li> <li>• <b>Safe:</b> When this value is selected, the service blocks access to malicious and fraudulent web sites.</li> <li>• <b>Child:</b> When this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.</li> </ul>

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.

## ***SkyDNS***

This menu is designed to configure the SkyDNS service.

SkyDNS is a web content filtering service which provides protection against malicious web sites for devices connected to the router's network, and also allows to configure filtering, block access to adult web sites, and use search engines safely. In order to use the service, first register an account on the SkyDNS service web site.

## Settings

On the **SkyDNS / Settings** page, you can enable the SkyDNS service and specify settings for its operation.

**!** The SkyDNS service is unavailable when the Yandex.DNS service is enabled.

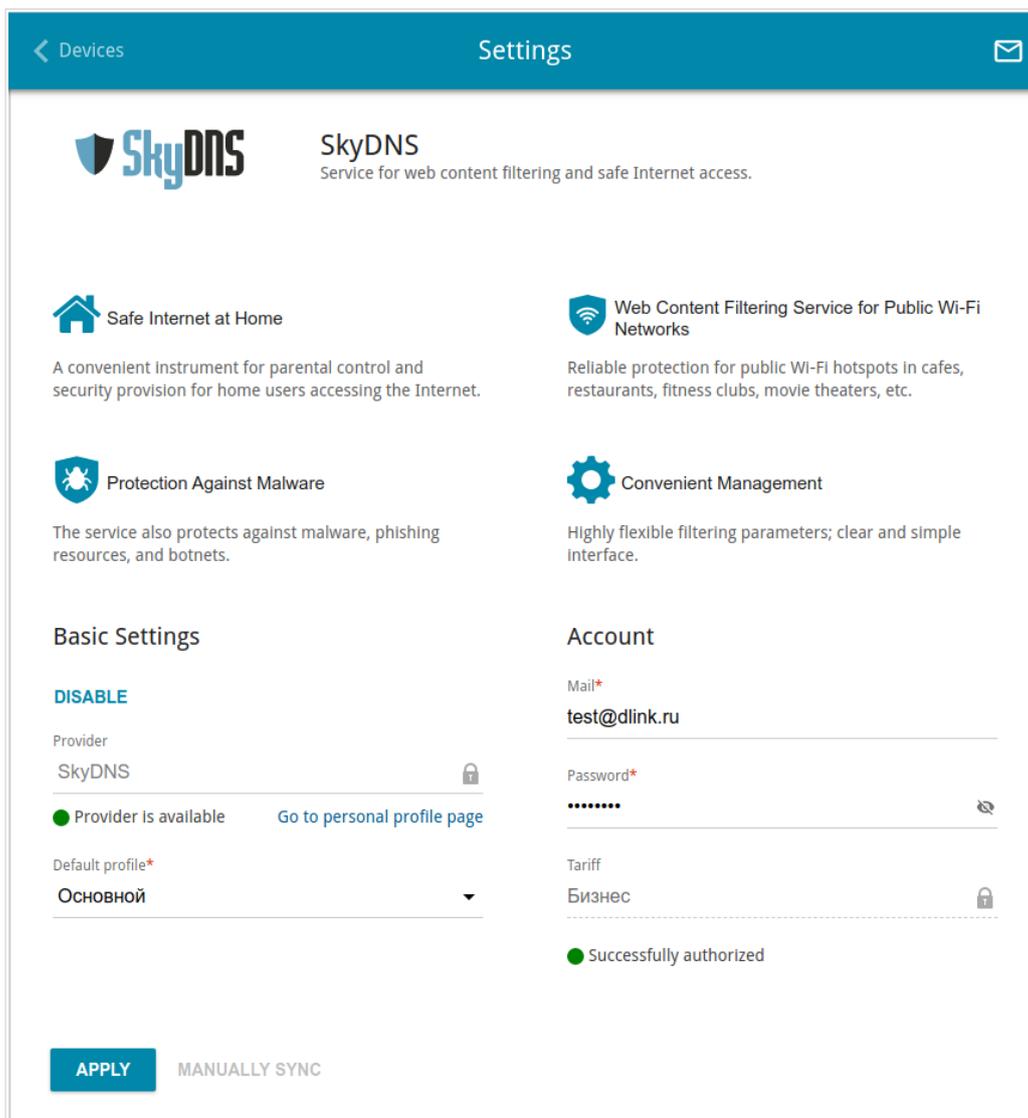


Figure 164. The **SkyDNS / Settings** page.

To enable the SkyDNS service, click the **ENABLE** button. Then in the **Mail** and **Password** fields, enter the account data (the e-mail address and the password correspondingly) specified upon registration on the SkyDNS service web site. Click the **APPLY** button. The account data (authorization status, the tariff used) and the **Default profile** drop-down list will be displayed on the page. If needed, from the **Default profile** list, select another filtering profile which will be used for all devices of your LAN and click the **APPLY** button again.

The default filtering profile will be applied to all devices newly connected to the router's network.

To change the parameters of your account on the SkyDNS service web site, click the **Go to personal profile page** link.

By default, the account parameters are automatically synchronized with the SkyDNS service web site once an hour. To start synchronization manually, click the **MANUALLY SYNC** button.

To use another account, specify its data in the **Mail** and **Password** fields and click the **APPLY** button.

To disable the SkyDNS service, click the **DISABLE** button.

## Devices and Rules

On the **SkyDNS / Devices and Rules** page, you can assign a specific filtering profile to a device connected to the router's network.

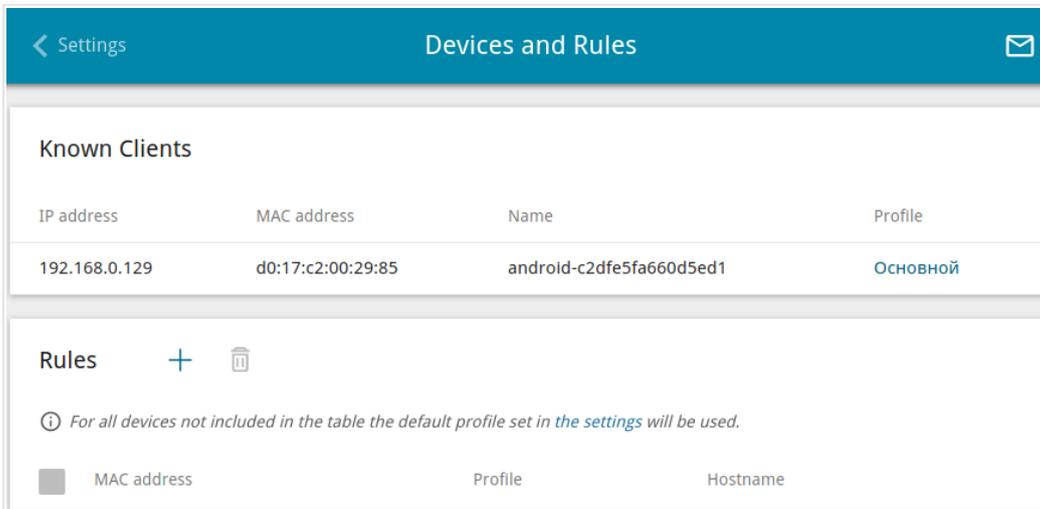


Figure 165. The **SkyDNS / Devices and Rules** page.

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

To assign a specific filtering profile for a device, click the **ADD** button ( **+** ) in the **Rules** section or left-click the name of the filtering profile in the line of the device for which a profile should be assigned in the **Known Clients** section.

Adding

MAC address\*

Profile\*  
Основной

Hostname

SAVE

Figure 166. The **SkyDNS / Devices and Rules** page. The window for adding a rule.

In the opened window, specify the following parameters:

Parameter	Description
<b>MAC address</b>	The MAC address of a device from the router's LAN to which the specified filtering profile 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).
<b>Profile</b>	Select the filtering profile which will be used for the device with the specified MAC address from the drop-down list.
<b>Hostname</b>	Enter a name for the rule for easier identification. <i>Optional.</i>

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 (  ).

## 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-822 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-822 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 is not in use.

## CHAPTER 6. ABBREVIATIONS AND ACRONYMS

<b>3G</b>	Third Generation
<b>AC</b>	Access Category
<b>AES</b>	Advanced Encryption Standard
<b>AP</b>	Access Point
<b>ARP</b>	Address Resolution Protocol
<b>BPSK</b>	Binary Phase-shift Keying
<b>BSSID</b>	Basic Service Set Identifier
<b>CCK</b>	Complementary Code Keying
<b>CHAP</b>	Challenge Handshake Authentication Protocol
<b>DBSK</b>	Differential Binary Phase-shift Keying
<b>DDNS</b>	Dynamic Domain Name System
<b>DDoS</b>	Distributed Denial of Service
<b>DES</b>	Data Encryption Standard
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DMZ</b>	DeMilitarized Zone
<b>DNS</b>	Domain Name System
<b>DPD</b>	Dead Peer Detection
<b>DQPSK</b>	Differential Quadrature Phase-shift Keying
<b>DSL</b>	Digital Subscriber Line
<b>DSSS</b>	Direct-sequence Spread Spectrum
<b>DTIM</b>	Delivery Traffic Indication Message
<b>EoGRE</b>	Ethernet over Generic Routing Encapsulation
<b>GMT</b>	Greenwich Mean Time
<b>GRE</b>	Generic Routing Encapsulation
<b>GSM</b>	Global System for Mobile Communications
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure

<b>ICMP</b>	Internet Control Message Protocol
<b>ID</b>	Identifier
<b>IGD</b>	Internet Gateway Device
<b>IGMP</b>	Internet Group Management Protocol
<b>IKE</b>	Internet Key Exchange
<b>IMEI</b>	International Mobile Equipment Identity
<b>IMSI</b>	International Mobile Subscriber Identity
<b>IP</b>	Internet Protocol
<b>IPTV</b>	Internet Protocol Television
<b>IPsec</b>	Internet Protocol Security
<b>ISP</b>	Internet Service Provider
<b>L2TP</b>	Layer 2 Tunneling Protocol
<b>LAN</b>	Local Area Network
<b>LCP</b>	Link Control Protocol
<b>LED</b>	Light-emitting diode
<b>LTE</b>	Long Term Evolution
<b>MAC</b>	Media Access Control
<b>MBSSID</b>	Multiple Basic Service Set Identifier
<b>MIB</b>	Management Information Base
<b>MIMO</b>	Multiple Input Multiple Output
<b>MPPE</b>	Microsoft Point-to-Point Encryption
<b>MS-CHAP</b>	Microsoft Challenge Handshake Authentication Protocol
<b>MTU</b>	Maximum Transmission Unit
<b>NAT</b>	Network Address Translation
<b>NIC</b>	Network Interface Controller
<b>NTP</b>	Network Time Protocol
<b>OFDM</b>	Orthogonal Frequency Division Multiplexing
<b>PAP</b>	Password Authentication Protocol

<b>PBC</b>	Push Button Configuration
<b>PFS</b>	Perfect Forward Secrecy
<b>PIN</b>	Personal Identification Number
<b>PoE</b>	Power over Ethernet
<b>PPP</b>	Point-to-Point Protocol
<b>pppd</b>	Point-to-Point Protocol Daemon
<b>PPPoE</b>	Point-to-point protocol over Ethernet
<b>PPTP</b>	Point-to-point tunneling protocol
<b>PSK</b>	Pre-shared key
<b>PUK</b>	PIN Unlock Key
<b>QAM</b>	Quadrature Amplitude Modulation
<b>QoS</b>	Quality of Service
<b>QPSK</b>	Quadrature Phase-shift Keying
<b>RADIUS</b>	Remote Authentication in Dial-In User Service
<b>RIP</b>	Routing Information Protocol
<b>RIPng</b>	Next Generation Routing Information Protocol
<b>RTS</b>	Request To Send
<b>RTSP</b>	Real Time Streaming Protocol
<b>SA</b>	Security Association
<b>SAE</b>	Simultaneous Authentication of Equals
<b>SIM</b>	Subscriber Identification Module
<b>SIP</b>	Session Initiation Protocol
<b>SMB</b>	Server Message Block
<b>SNMP</b>	Simple Network Management Protocol
<b>SSH</b>	Secure Shell
<b>SSID</b>	Service Set Identifier
<b>STBC</b>	Space-time block coding
<b>TCP</b>	Transmission Control Protocol

<b>TKIP</b>	Temporal Key Integrity Protocol
<b>UAM</b>	Universal Access Method
<b>UDP</b>	User Datagram Protocol
<b>UPnP</b>	Universal Plug and Play
<b>URL</b>	Uniform Resource Locator
<b>USB</b>	Universal Serial Bus
<b>VLAN</b>	Virtual Local Area Network
<b>VPN</b>	Virtual Private Network
<b>VRID</b>	Virtual Router Identifier
<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>WAN</b>	Wide Area Network
<b>WEP</b>	Wired Equivalent Privacy
<b>Wi-Fi</b>	Wireless Fidelity
<b>WISP</b>	Wireless Internet Service Provider
<b>WLAN</b>	Wireless Local Area Network
<b>WMM</b>	Wi-Fi Multimedia
<b>WPA</b>	Wi-Fi Protected Access
<b>WPS</b>	Wi-Fi Protected Setup