



## **DWR-921**

### **4G LTE 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>7</b>
<b>Product Appearance</b> .....	<b>10</b>
Front Panel.....	10
Back Panel.....	12
<b>Delivery Package</b> .....	<b>13</b>
<b>Chapter 3. Installation and Connection</b> .....	<b>14</b>
<b>Before You Begin</b> .....	<b>14</b>
<b>Connecting to PC</b> .....	<b>15</b>
PC with Ethernet Adapter.....	15
Obtaining IP Address Automatically in OS Windows 7.....	16
PC with Wi-Fi Adapter.....	21
Configuring Wi-Fi Adapter in OS Windows 7.....	22
<b>Connecting to Web-based Interface</b> .....	<b>25</b>
<b>Web-based Interface Structure</b> .....	<b>27</b>
Summary Page.....	27
Home Page.....	29
Menu Sections.....	30
Notifications.....	31
<b>Chapter 4. Configuring via Web-based Interface</b> .....	<b>32</b>
<b>Initial Configuration Wizard</b> .....	<b>32</b>
Selecting Operation Mode.....	34
Creating LTE WAN Connection.....	37
Changing LAN IPv4 Address.....	38
Wi-Fi Client.....	39
Configuring Wired WAN Connection.....	41
<i>Static IPv4 Connection</i> .....	42
<i>Static IPv6 Connection</i> .....	43
<i>PPPoE, IPv6 PPPoE, PPPoE Dual Stack</i> .....	44
Configuring Wireless Network.....	45
Configuring LAN Ports for IPTV/VoIP.....	47
Changing Web-based Interface Password.....	49
<b>Connection of Multimedia Devices</b> .....	<b>51</b>
<b>Statistics</b> .....	<b>54</b>
Network Statistics.....	54
DHCP.....	55
Routing Table.....	56
Clients.....	57
Multicast Groups.....	58
Clients and Session.....	59

<b>Connections Setup</b> .....	<b>60</b>
WAN.....	60
<i>Creating Dynamic IPv4 or Static IPv4 WAN Connection</i> .....	62
<i>Creating Dynamic IPv6 or Static IPv6 WAN Connection</i> .....	67
<i>Creating PPPoE WAN Connection</i> .....	71
<i>Creating PPTP or L2TP WAN Connection</i> .....	76
<i>Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection</i> .....	80
<i>Creating LTE WAN Connection</i> .....	86
LAN.....	91
IPv4.....	91
IPv6.....	94
WAN Reservation.....	97
<b>Wi-Fi</b> .....	<b>99</b>
Basic Settings.....	99
Client Management.....	107
WPS.....	108
<i>Using WPS Function via Web-based Interface</i> .....	110
<i>Using WPS Function without Web-based Interface</i> .....	111
WMM.....	112
Client.....	115
Additional.....	117
MAC Filter.....	119
<b>LTE Modem</b> .....	<b>121</b>
Basic Settings.....	122
PIN.....	123
SMS.....	124
<b>Advanced</b> .....	<b>126</b>
VLAN.....	127
WAN Remapping.....	129
SNMP.....	130
DNS.....	133
DDNS.....	135
Ports Settings.....	137
Redirect.....	140
Routing.....	141
TR-069 Client.....	143
Remote Access.....	145
UPnP IGD.....	147
IGMP.....	148
ALG/Passthrough.....	149
IPsec.....	151
<b>Firewall</b> .....	<b>157</b>
IP Filter.....	157
Virtual Servers.....	161
DMZ.....	164
MAC Filter.....	165
URL Filter.....	167

<b>System</b> .....	<b>168</b>
Configuration.....	169
Firmware Update.....	171
<i>Local Update</i> .....	172
<i>Remote Update</i> .....	173
Log.....	174
Ping.....	176
Traceroute.....	178
Telnet.....	180
System Time.....	181
<b>Yandex.DNS</b> .....	<b>183</b>
Settings.....	183
Devices and Rules.....	185
<b>Chapter 5. Operation Guidelines</b> .....	<b>187</b>
<b>Safety Rules and Conditions</b> .....	<b>187</b>
<b>Wireless Installation Considerations</b> .....	<b>188</b>
<b>Chapter 6. Abbreviations and Acronyms</b> .....	<b>189</b>


# CHAPTER 1. INTRODUCTION

## Contents and Audience

This manual describes the router DWR-921 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 DWR-921 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 used in this manual.

## CHAPTER 2. OVERVIEW

### **General Information**

The DWR-921 device is a wireless router supporting 3G/LTE with a built-in switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

The router is equipped with a built-in LTE modem which provides 3G/4G mobile connection with fast downlink speeds of up to 150Mbps and uplink speeds up to 50Mbps.<sup>1</sup>

Also you are able to connect the wireless router DWR-921 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 DWR-921 device, you are able to quickly create a wireless network at home or in your office, which lets computers and mobile devices access the Internet virtually anywhere (within the operational range of your wireless network). The router can operate as a base station for connecting wireless devices of the standards 802.11b, 802.11g, and 802.11n (at the wireless connection rate up to 300Mbps).

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

Support of guest Wi-Fi network allows you to create a separate wireless network with individual security settings. 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 DWR-921 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.

In addition, the router supports IPsec and allows to create secure VPN tunnels.

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

You can configure the settings of the wireless router DWR-921 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 DWR-921 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.

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

---

<sup>1</sup> Data rates are theoretical. Data transfer rate depends on network capacity and signal strength.

## Specifications\*

Hardware	
<b>Processor</b>	<ul style="list-style-type: none"> <li>MT7620N (600MHz)</li> </ul>
<b>Flash</b>	<ul style="list-style-type: none"> <li>16MB, SPI</li> </ul>
<b>Interfaces</b>	<ul style="list-style-type: none"> <li>Slot for SIM card (mini-SIM)</li> <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>SIGNAL STRENGTH</li> <li>SMS</li> <li>LAN</li> <li>POWER</li> <li>2G/3G</li> <li>4G</li> <li>WLAN</li> </ul>
<b>Buttons</b>	<ul style="list-style-type: none"> <li>POWER ON/OFF button to power on/power off</li> <li>WPS button to 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>Two detachable LTE/3G antennas (3dBi gain)</li> <li>Two internal Wi-Fi antennas (3dBi gain)</li> </ul>
<b>MIMO</b>	<ul style="list-style-type: none"> <li>2 x 2</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>LTE</li> <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>PPTP/L2TP</li> </ul>
<b>Network functions</b>	<ul style="list-style-type: none"> <li>Support of IEEE 802.1X for Internet connection</li> <li>DHCP server/relay</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 IP routing</li> <li>Static IPv6 routing</li> <li>IGMP 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>LAN/WAN conversion</li> <li>Autonegotiation of speed, duplex mode, and flow control/Manual speed and duplex mode setup for each Ethernet port</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).

Software	
<b>Firewall functions</b>	<ul style="list-style-type: none"> <li>· Network Address Translation (NAT)</li> <li>· Stateful Packet Inspection (SPI)</li> <li>· IP filter</li> <li>· IPv6 filter</li> <li>· MAC filter</li> <li>· URL filter</li> <li>· DMZ</li> <li>· Prevention of ARP and DDoS attacks</li> <li>· Virtual servers</li> <li>· Built-in Yandex.DNS web content filtering service</li> </ul>
<b>VPN</b>	<ul style="list-style-type: none"> <li>· IPsec/PPTP/L2TP/PPPoE pass-through</li> <li>· IPsec tunnels</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li>· Local and remote access to settings through TELNET/WEB (HTTP/HTTPS)</li> <li>· Bilingual web-based interface for configuration and management (Russian/English)</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>· SNMP agent</li> </ul>

LTE Module Parameters	
<b>LTE connection rate<sup>2</sup></b>	<ul style="list-style-type: none"> <li>· Downlink: up to 150Mbps</li> <li>· Uplink: up to 50Mbps</li> </ul>
<b>Functions</b>	<ul style="list-style-type: none"> <li>· Auto connection to available type of supported network (4G/3G/2G)</li> <li>· Auto configuration of connection upon plugging in SIM card</li> <li>· Enabling/disabling PIN code check, changing PIN code</li> <li>· Sending/receiving/reading/removing SMS messages</li> </ul>

Wireless Module Parameters	
<b>Standards</b>	<ul style="list-style-type: none"> <li>· IEEE 802.11b/g/n</li> </ul>
<b>Frequency range</b>	<ul style="list-style-type: none"> <li>· 2400 ~ 2483.5MHz</li> </ul>
<b>Wireless connection security</b>	<ul style="list-style-type: none"> <li>· WEP</li> <li>· WPA/WPA2 (Personal/Enterprise)</li> <li>· MAC filter</li> <li>· WPS (PBC/PIN)</li> </ul>
<b>Advanced functions</b>	<ul style="list-style-type: none"> <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> </ul>
<b>Wireless connection rate</b>	<ul style="list-style-type: none"> <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: from 6.5 to 300Mbps (from MCS0 to MCS15)</li> </ul>

<sup>2</sup> Data rates are theoretical. Data transfer rate depends on network capacity and signal strength.



Wireless Module Parameters	
<b>Transmitter output power</b>  <i>The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country</i>	<ul style="list-style-type: none"> <li>· 15dBm</li> </ul>
<b>Receiver sensitivity</b>	<ul style="list-style-type: none"> <li>· 802.11b -86dBm at 11Mbps</li> <li>· 802.11g -81dBm at 54Mbps</li> <li>· 802.11n HT20 -71dBm at MCS15 HT40 -67dBm at MCS15</li> </ul>
<b>Modulation schemes</b>	<ul style="list-style-type: none"> <li>· 802.11b: DSSS, BPSK, QPSK, CCK</li> <li>· 802.11g: OFDM</li> <li>· 802.11n: OFDM</li> </ul>

Physical Parameters	
<b>Dimensions (L x W x H)</b>	<ul style="list-style-type: none"> <li>· 190 x 112 x 22 mm (7.5 x 4.4 x 0.9 in)</li> </ul>
<b>Weight</b>	<ul style="list-style-type: none"> <li>· 295 g (0.7 lb)</li> </ul>

Operating Environment	
<b>Power</b>	<ul style="list-style-type: none"> <li>· Output: 12V DC, 1A</li> </ul>
<b>Temperature</b>	<ul style="list-style-type: none"> <li>· Operating: from 0 to 40 °C</li> <li>· Storage: from -10 to 70 °C</li> </ul>
<b>Humidity</b>	<ul style="list-style-type: none"> <li>· Operating: from 10% to 90% (non-condensing)</li> <li>· Storage: from 0% to 95% (non-condensing)</li> </ul>

## Product Appearance

### Front Panel



Figure 1. Front panel view.

LED	Mode	Description
<b>SIGNAL STRENGTH</b>	<i>Solid green</i>	LTE WAN connection is on.
	<i>Solid red</i>	LTE WAN connection is off.
	<i>Blinking red</i>	No SIM card or failed to register in a mobile operator's network.
	<i>No light</i>	Searching for a mobile operator's network.
<b>SMS</b>	<i>Solid green</i>	An unread message (or messages).
	<i>No light</i>	No unread messages.
<b>LAN</b>	<i>Solid green</i>	The cable is connected to a port.
	<i>Blinking green</i>	Data transfer though one or several LAN ports.
	<i>No light</i>	The cable is not connected to a port.
<b>POWER</b>	<i>Solid green</i>	The router is powered on.
	<i>No light</i>	The router is powered off.
<b>2G/3G</b>	<i>Solid green</i>	2G/3G network registration is successfully done.
	<i>Blinking green</i>	Searching for a 2G/3G network.
	<i>No light</i>	No registration in a 2G/3G network.
<b>4G</b>	<i>Solid green</i>	4G network registration is successfully done.
	<i>Blinking green</i>	Searching for a 4G network.
	<i>No light</i>	No registration in a 4G network.

LED	Mode	Description
<b>WLAN</b>	<i>Solid green</i>	The router's WLAN is on.
	<i>Fast blinking green</i>	Data transfer though Wi-Fi network.
	<i>Slow blinking green</i>	Attempting to add a wireless device via the WPS function.
	<i>No light</i>	The router's WLAN is off.

The **RESET** and **WPS** buttons are located on the front panel of the router.

Button	Description
<b>RESET</b>	A button 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.
<b>WPS</b>	A button to set up a wireless connection (the WPS function). To use the WPS function: with the device turned on, push the button, and release. The <b>WLAN</b> LED should start blinking slowly.

## Back Panel



Figure 2. Back panel view.

Port	Description
<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>SIM Card</b>	A slot for SIM card (mini-SIM).
<b>12V=1A</b>	Power connector.
<b>POWER ON/OFF</b>	A button to turn the router on/off.

The device is also equipped with two external detachable LTE/3G antennas and two internal Wi-Fi antennas.

## ***Delivery Package***

The following should be included:

- Router DWR-921
- Power adapter DC 12V/1A
- Ethernet cable (CAT 5)
- Two detachable LTE/3G antennas
- “***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.

#### **Operating System**

Configuration of the wireless router supporting 3G/LTE with a built-in switch DWR-921 (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.

#### **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 802.11b, g, or n NIC (Wi-Fi adapter). In addition, you should specify the values of SSID, channel number and security settings defined in the web-based interface of the router for all these wireless workstations.

#### **SIM Card**

To connect to the Internet via mobile operators' networks, you should use an active SIM card. Then you will be able to configure a connection to the Internet<sup>3</sup>.

---

<sup>3</sup> Contact your operator to get information on the service coverage and fees.

## Connecting to PC

### PC with Ethernet Adapter

1. Insert a SIM card into the slot on the back panel of the router with the gold contacts facing downwards and gently push until it clicks.

**!** If you need to connect a SIM card or change it to another one when the router is powered on, power off the router, insert or change the SIM card, and power on the router.

2. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
3. 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.
4. Turn on the router by pressing the **POWER ON/OFF** button on its back panel.

Make sure that your Ethernet adapter is configured to obtain an IP address automatically (as DHCP client).

## Obtaining IP Address Automatically in 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.)

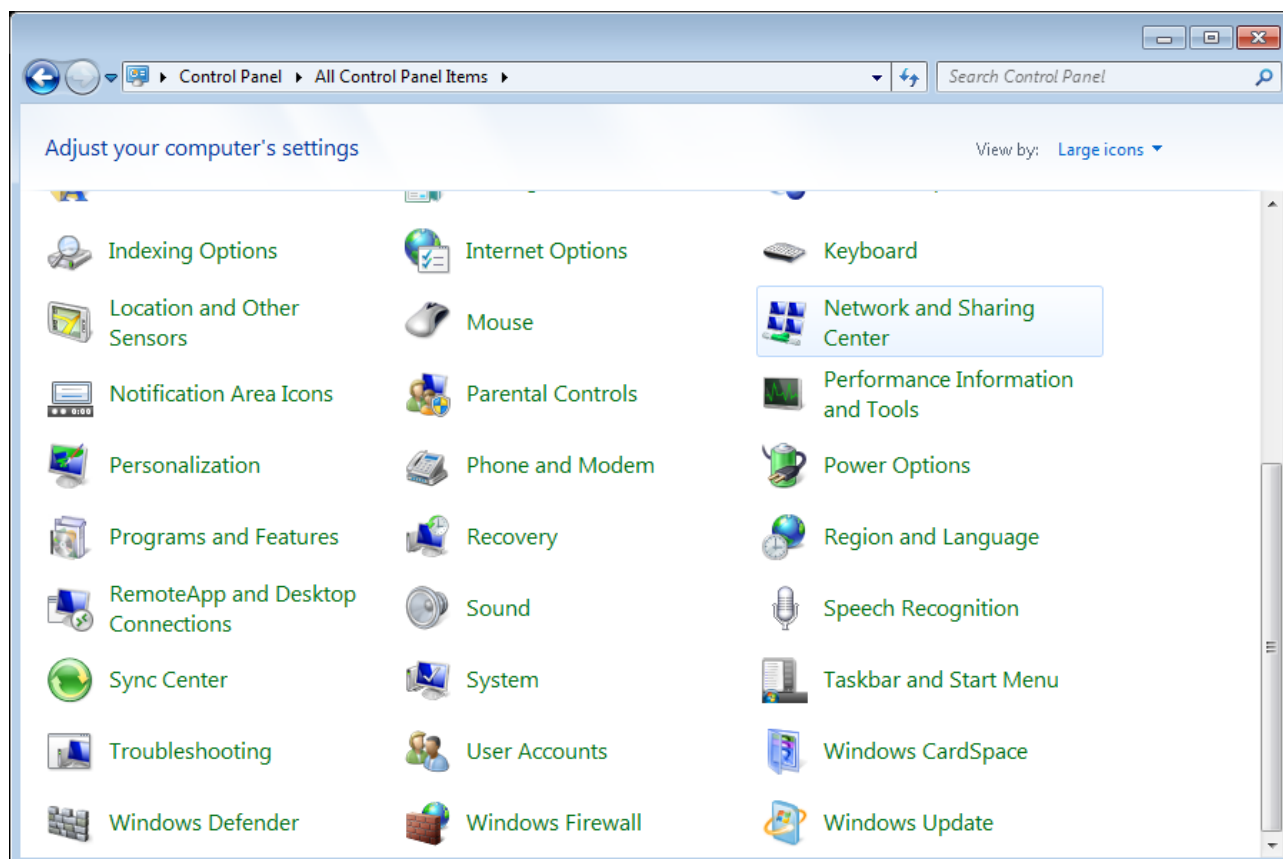


Figure 3. The **Control Panel** window.



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

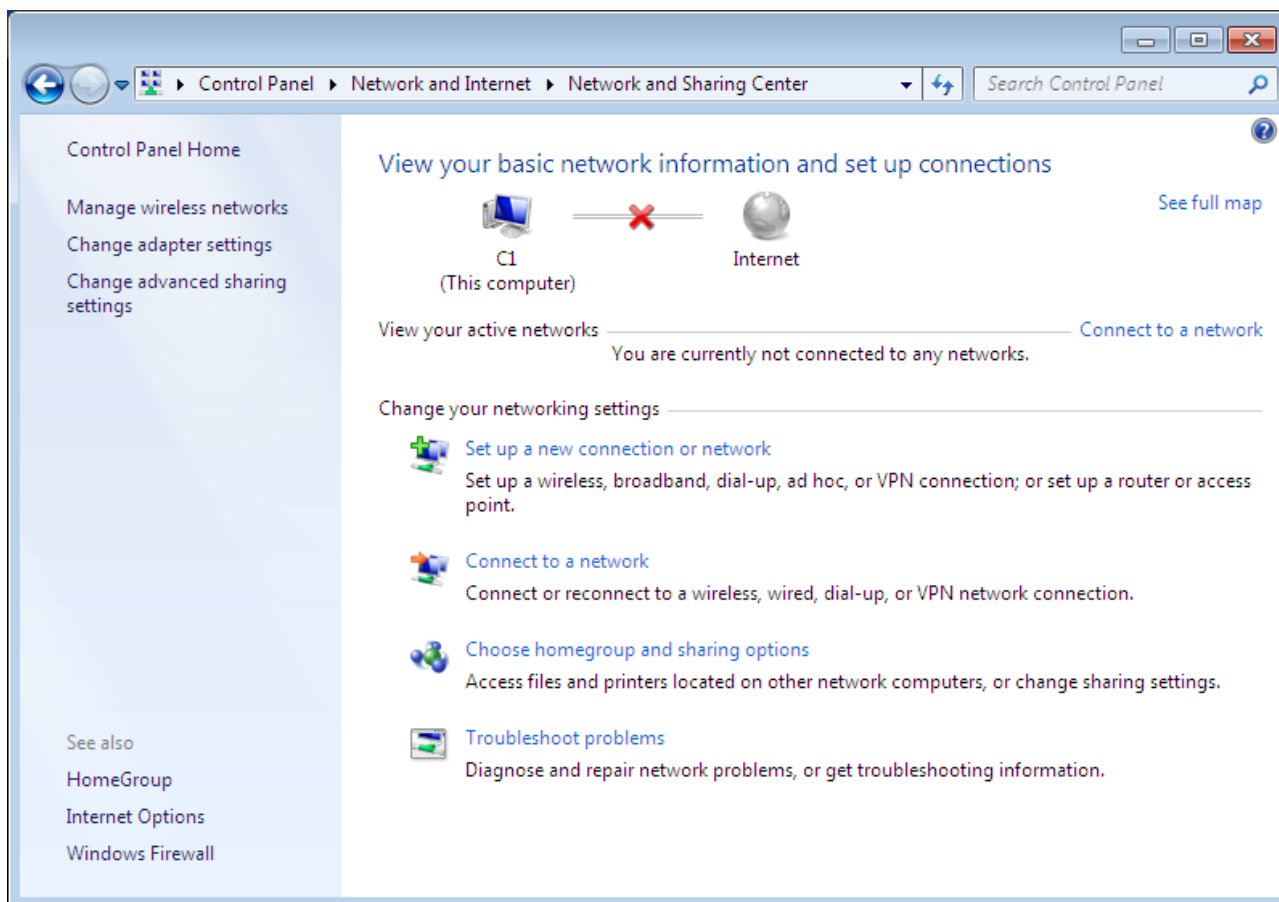


Figure 4. The **Network and Sharing Center** window.

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

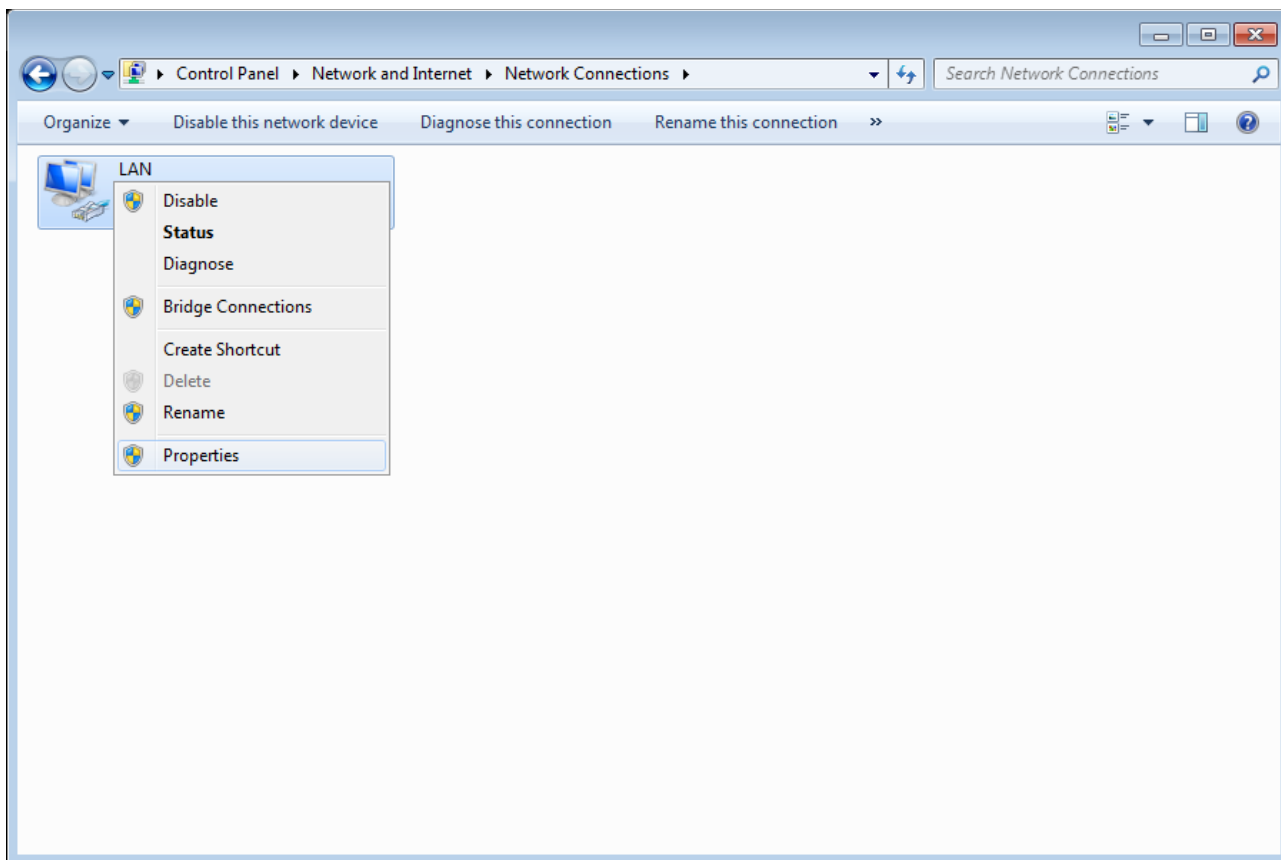


Figure 5. The **Network Connections** window.

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.

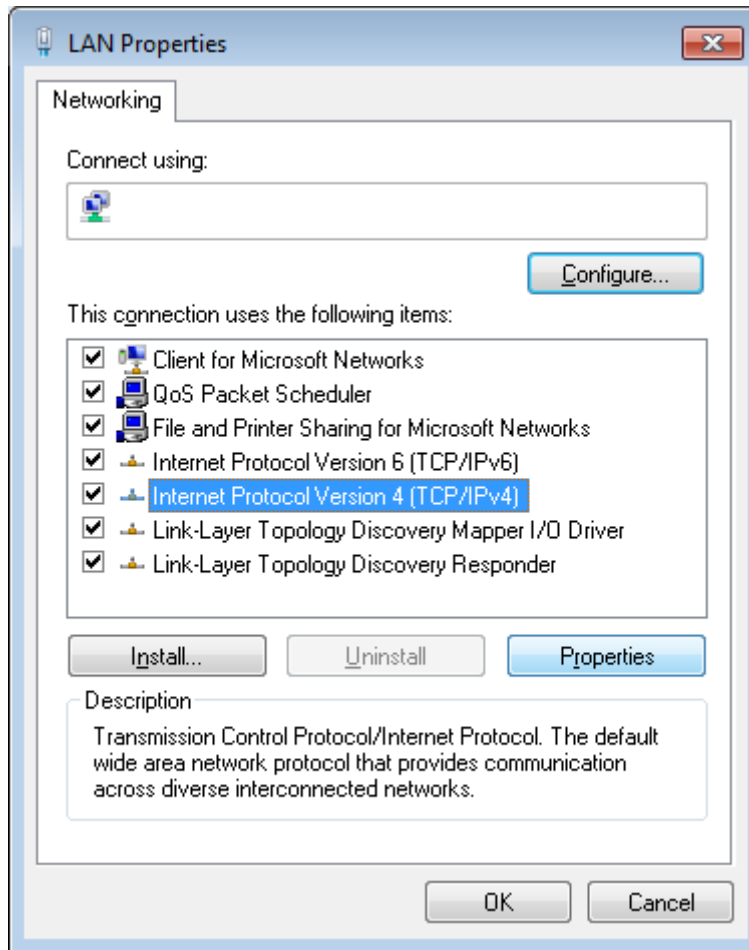


Figure 6. The **Local Area Connection Properties** window.

6. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. Click the **OK** button.

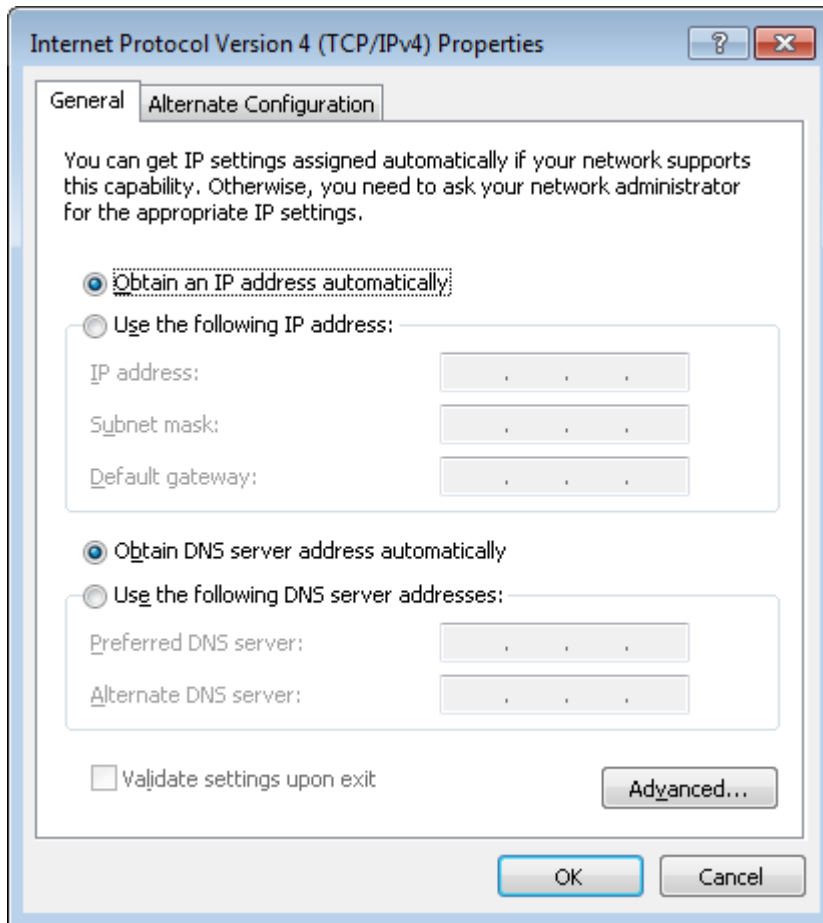


Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now your computer is configured to obtain an IP address automatically.

## PC with Wi-Fi Adapter

1. Insert a SIM card into the slot on the back panel of the router with the gold contacts facing downwards and gently push until it clicks.

**!** If you need to connect a SIM card or change it to another one when the router is powered on, power off the router, insert or change the SIM card, and power on the router.

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 ON/OFF** button on its back panel.
4. 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.

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

## Configuring Wi-Fi Adapter in 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.)

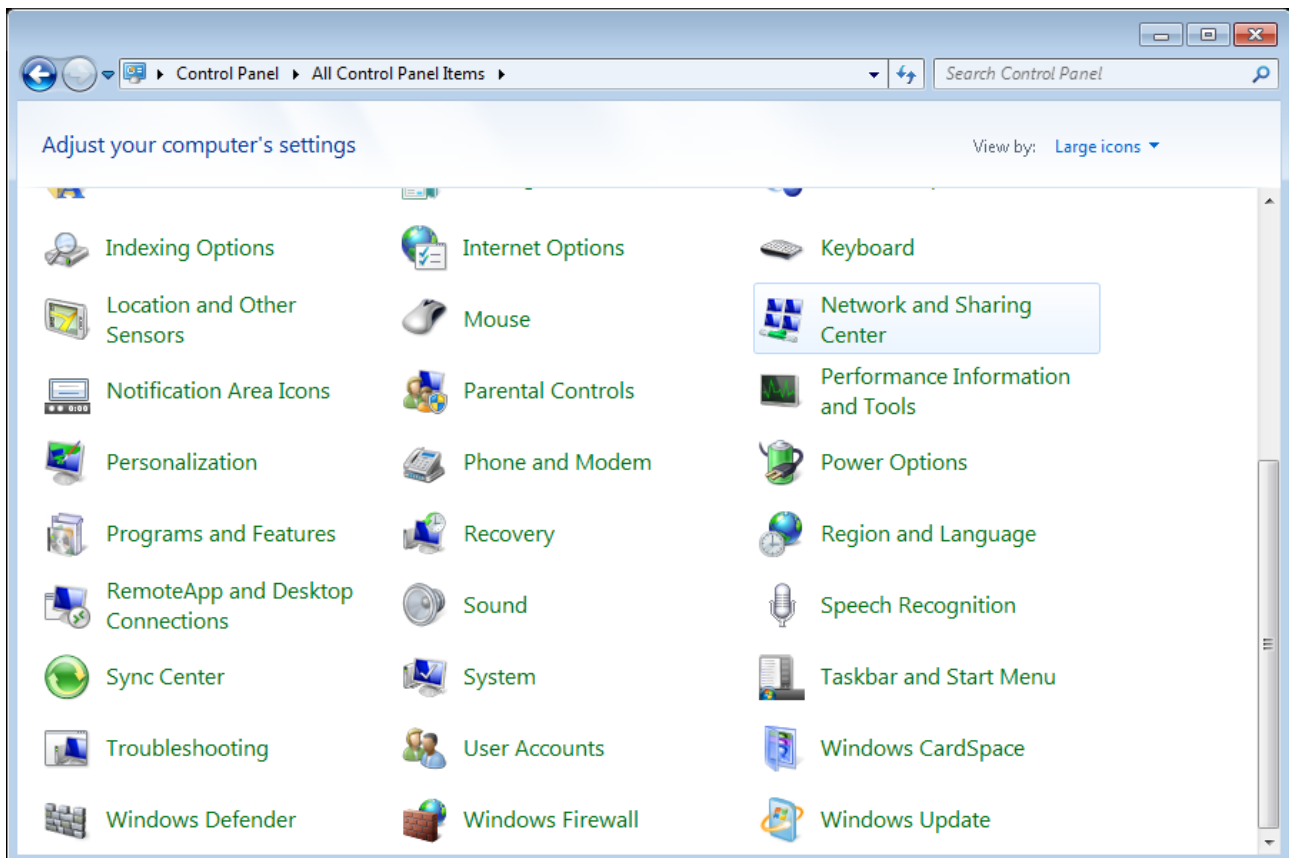


Figure 8. The **Control Panel** window.

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. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. Click the **OK** button.

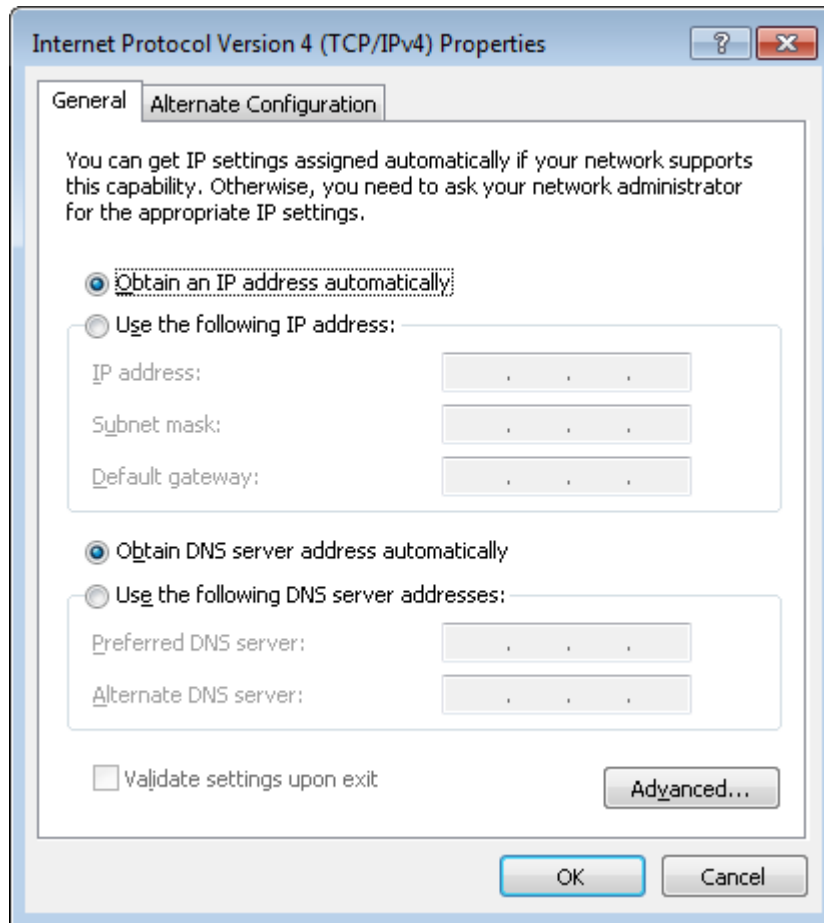


Figure 9. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

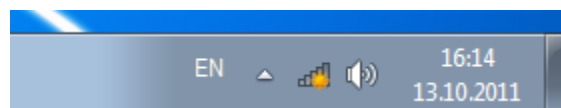


Figure 10. The notification area of the taskbar.

- In the opened **Wireless Network Connection** window, select the wireless network **DWR-921** and click the **Connect** button.

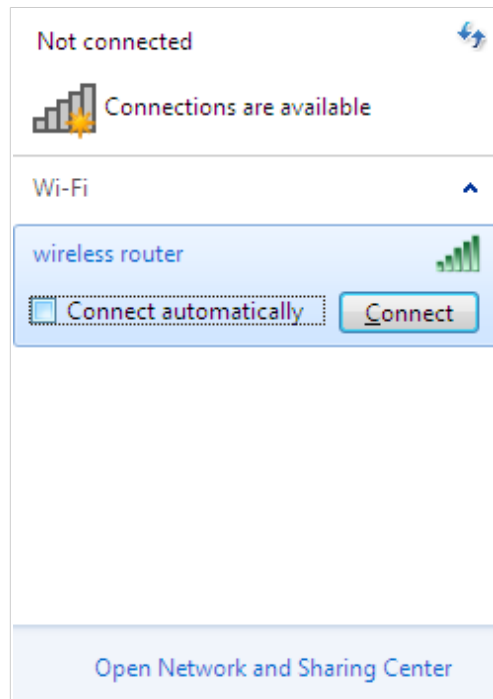


Figure 11. The list of available networks.

- 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.



## 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, DWR-921 with default settings cannot connect to the Internet. To get started, please set your own password used to access the web-based interface and, if needed, configure other settings recommended by your ISP.

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

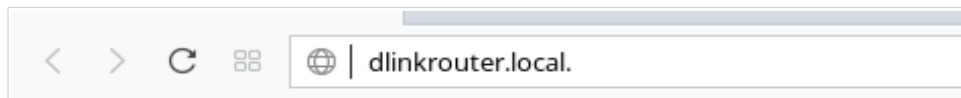


Figure 12. Connecting to the web-based interface of the DWR-921 device.

**!** 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 32).

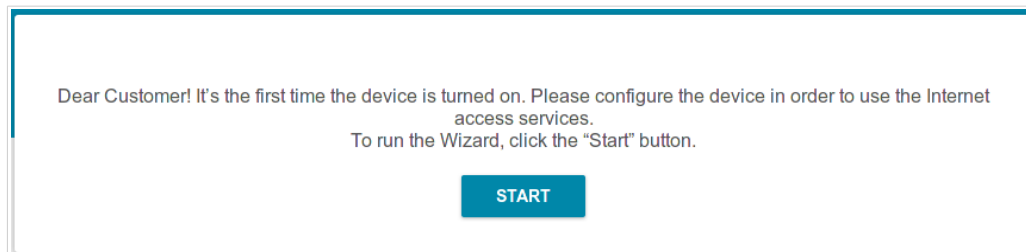
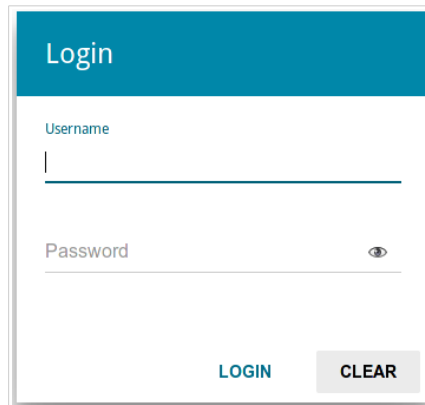


Figure 13. The page for running the Initial Configuration Wizard.

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.



The image shows a web-based login interface. At the top, there is a blue header with the word "Login" in white. Below the header, there are two input fields: "Username" and "Password". The "Username" field has a vertical cursor on the left. The "Password" field has a small eye icon to its right, indicating a toggle for password visibility. At the bottom of the form, there are two buttons: "LOGIN" in blue text and "CLEAR" in black text on a light gray background.

Figure 14. The login page.

## Web-based Interface Structure

### Summary Page

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

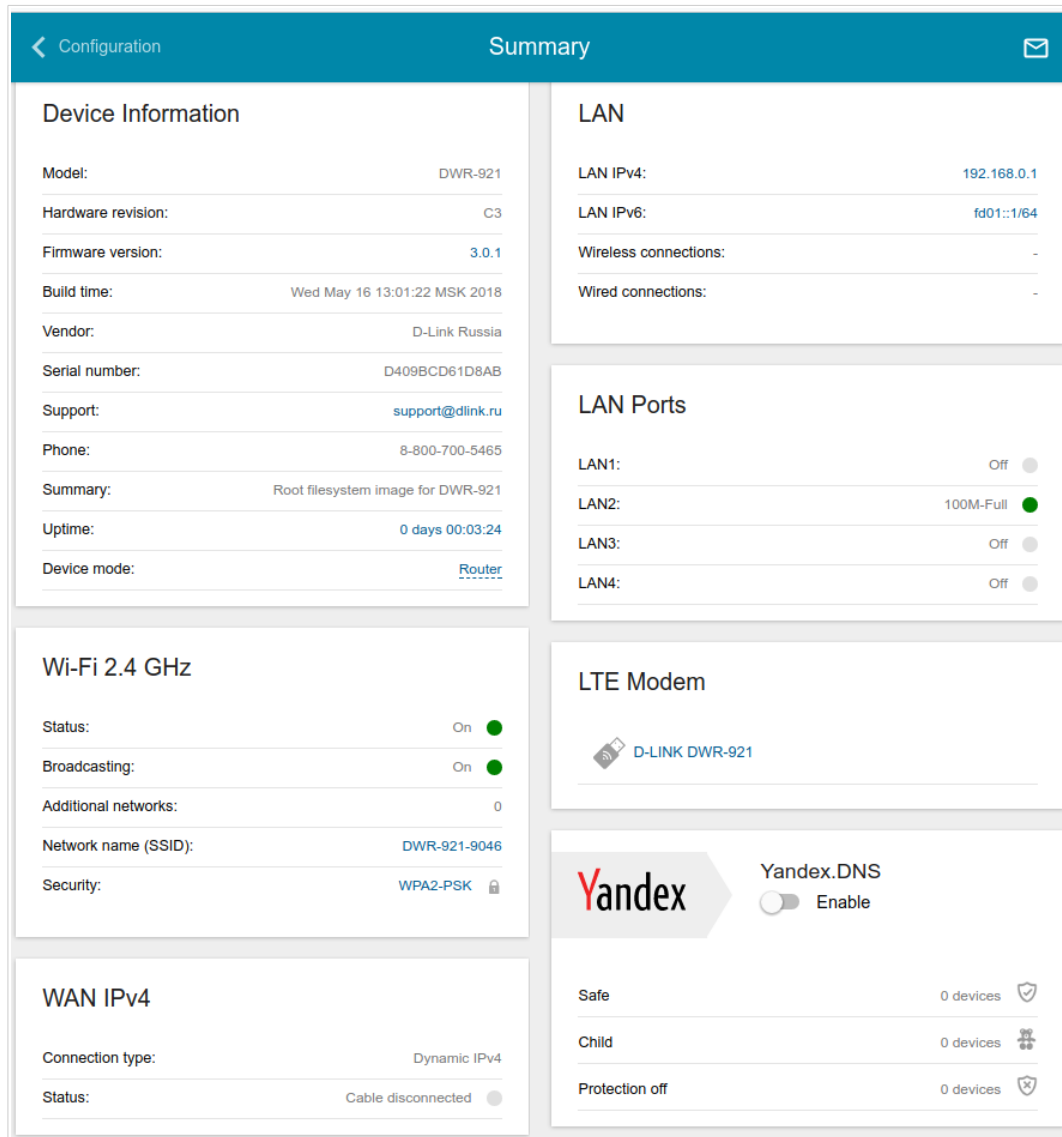


Figure 15. The summary page.

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 setup wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 32).

The **Wi-Fi 2.4 GHz** section displays 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 **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 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 **LTE Modem** section displays a name of a built-in LTE modem.

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.

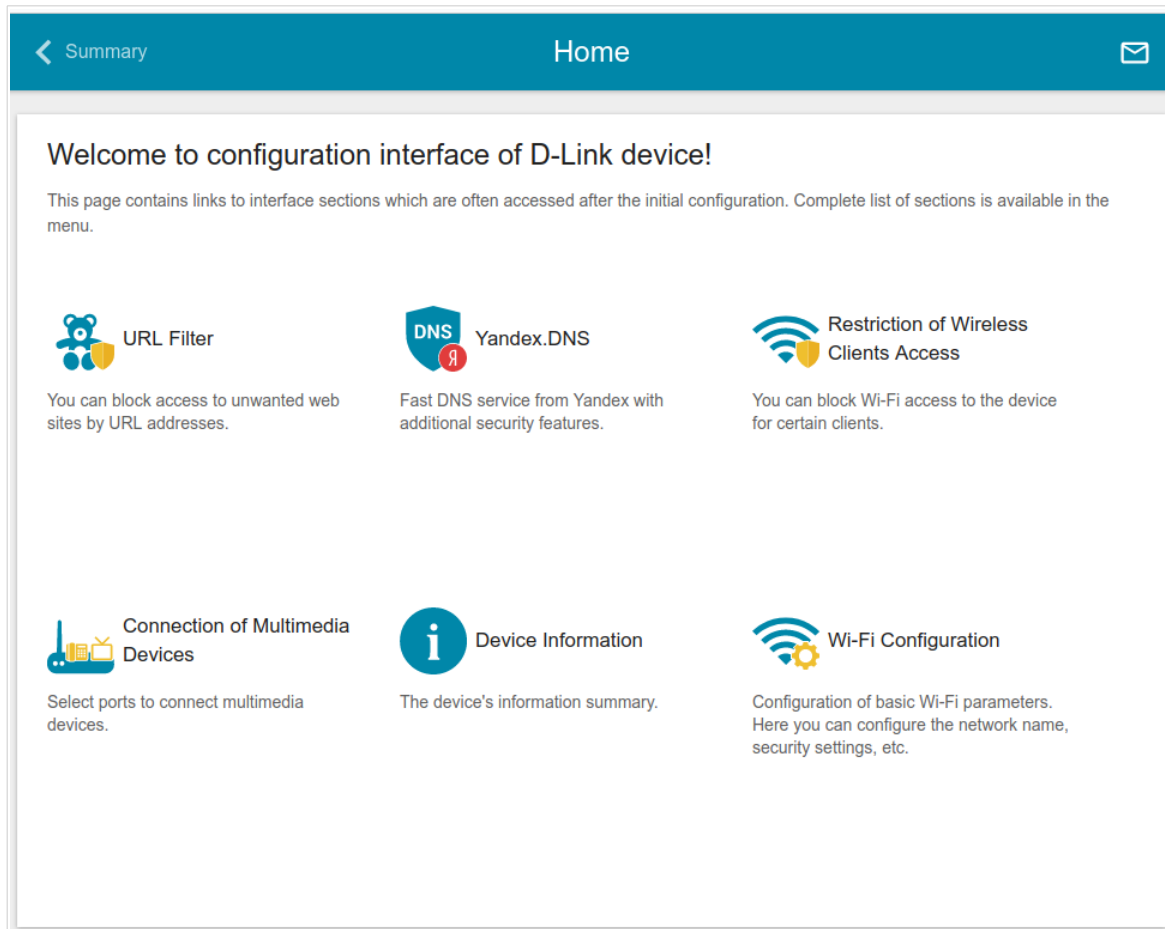


Figure 16. The **Home** page.

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 32).

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 54).

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 60).

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 99).

The pages of the **LTE Modem** section are designed for operating the built-in LTE modem (for the description of the pages, see the **LTE Modem** section, page 121).

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 126).

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 157).

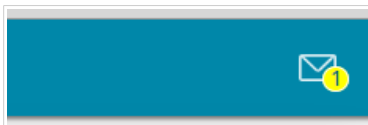
The pages of the **System** section provide functions for managing the internal system of the router (for the description of the pages, see the **System** section, page 168).

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 183).

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 17. 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.

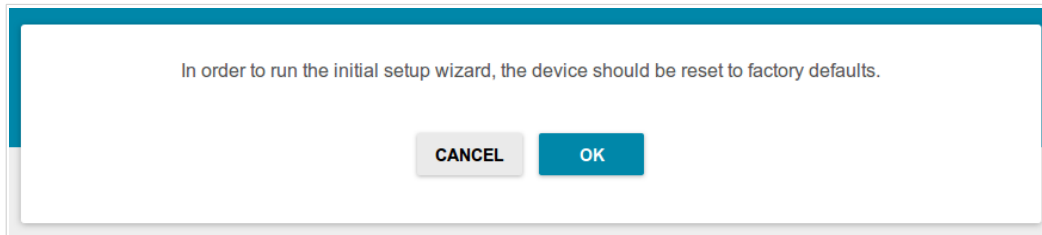


Figure 18. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network of DWR-921 (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

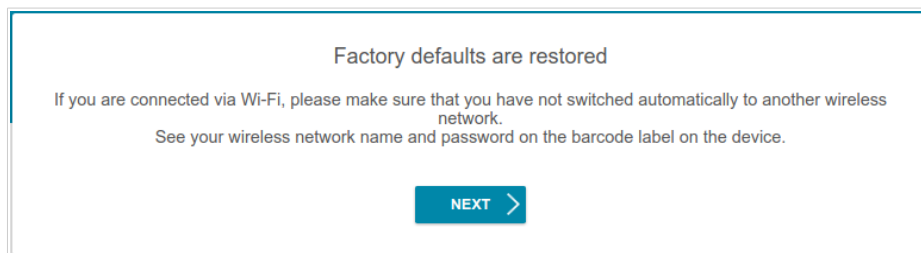


Figure 19. Checking connection to the wireless network.

Click the **START** button.

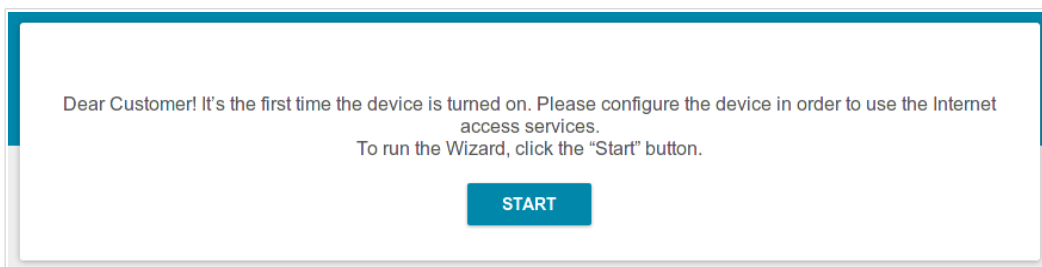


Figure 20. Starting the Wizard.

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.

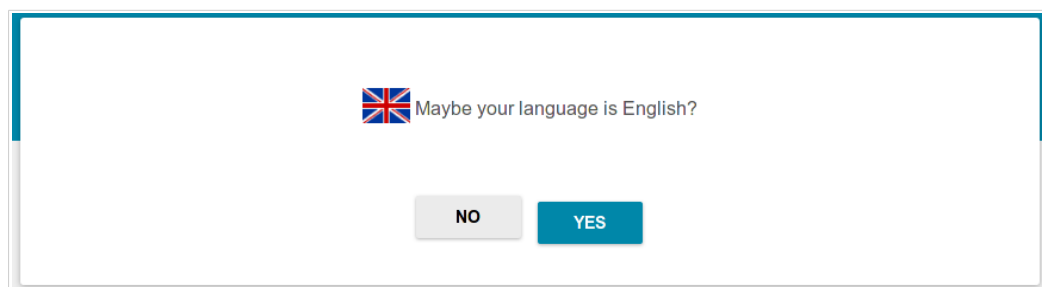


Figure 21. Selecting a language.



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 **Admin password** field and the name of the wireless network in the **Network name (SSID)** field. Then click the **APPLY** button.

Defaults

*In order to start up, please change several default settings.*

Admin password\*

ⓘ Password should be between 1 and 31 ASCII characters

Network name (SSID)\*

DWR-XXX-d8ac

← BACK APPLY

Figure 22. Changing the default settings.

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

## Selecting Operation Mode

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

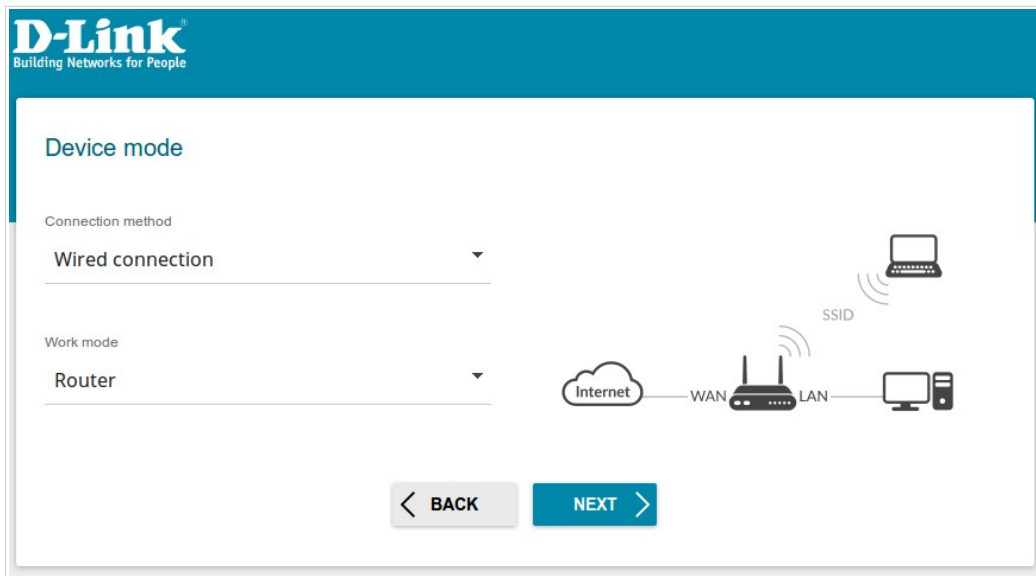


Figure 23. Selecting an operation mode. The **Router** mode.

In order to connect your device to the network of a 3G or LTE operator, on the **Device mode** page, from the **Connection method** list, select the **3G/LTE modem** value. In this mode you can configure an LTE WAN connection, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.

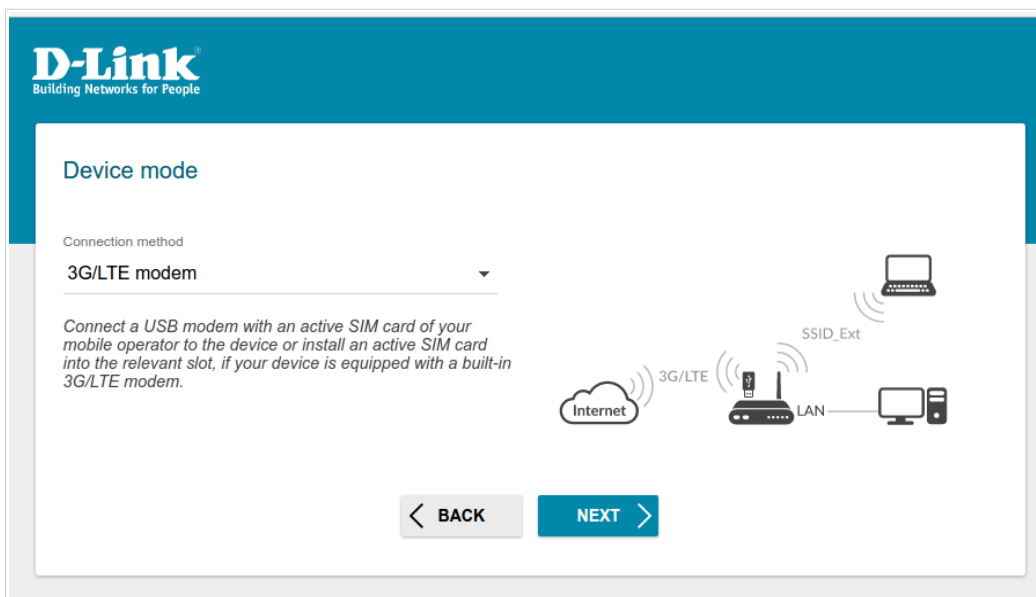


Figure 24. Selecting an operation mode. The **3G/LTE modem** mode.

In order to connect your device to a wireless ISP (WISP), on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **WISP Repeater** value. In this mode you can connect your device to another access point, configure a WAN connection, set your own settings for the wireless network, 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.

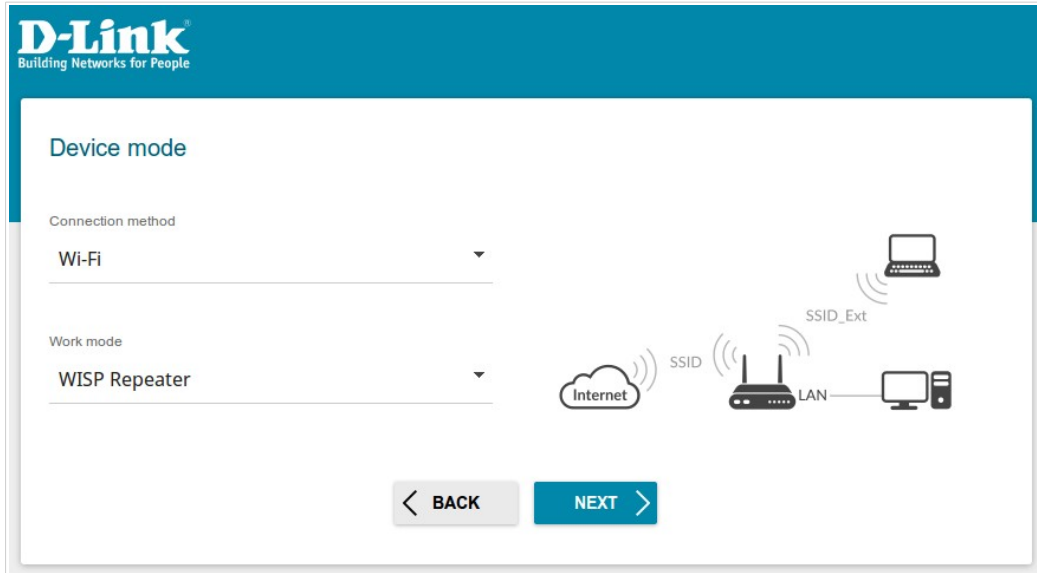


Figure 25. Selecting an operation mode. The **WISP Repeater** mode.

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

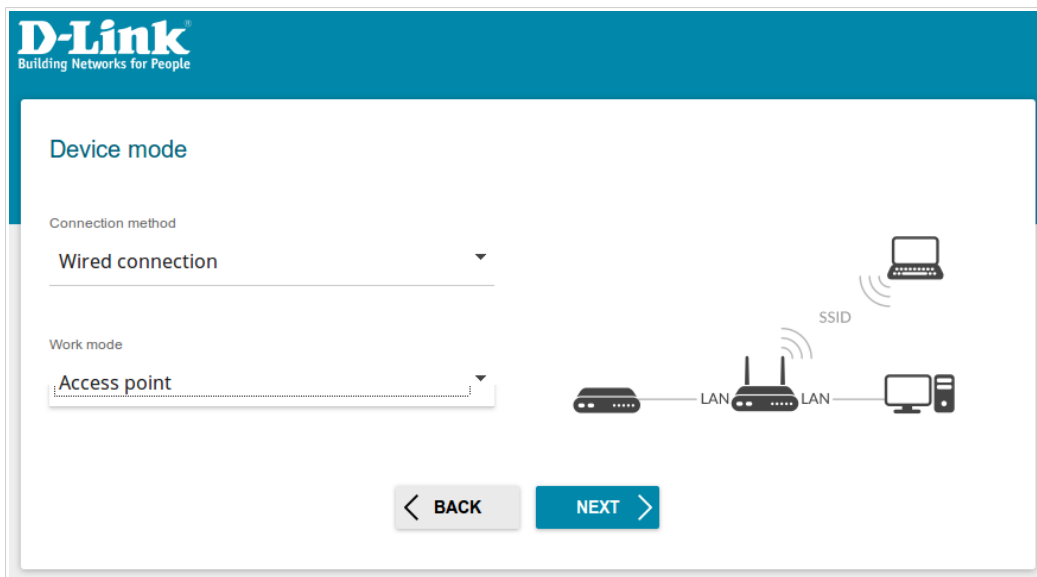


Figure 26. Selecting an operation mode. The **Access point** mode.

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

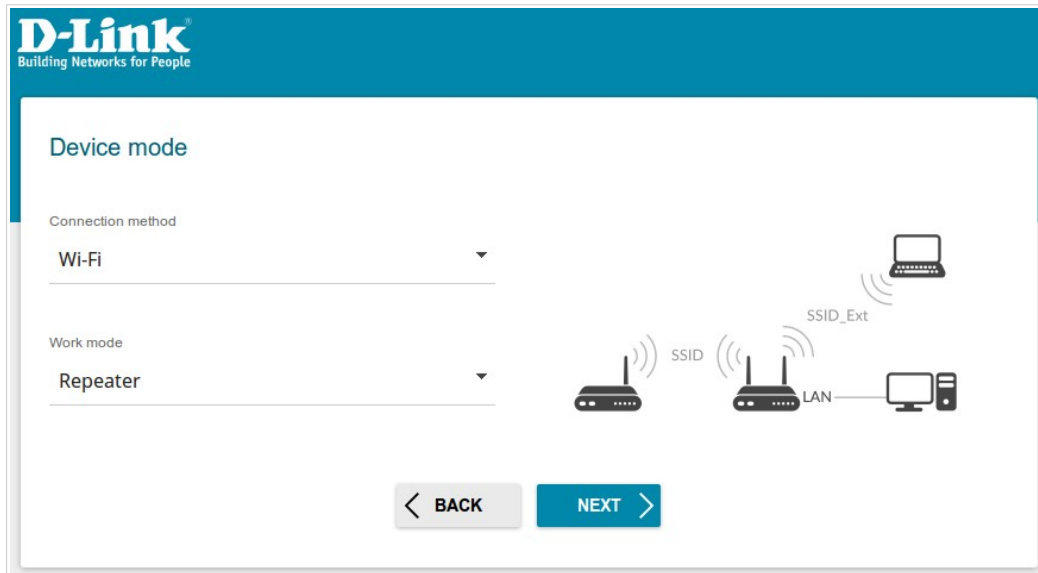


Figure 27. Selecting an operation mode. The **Repeater** mode.

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

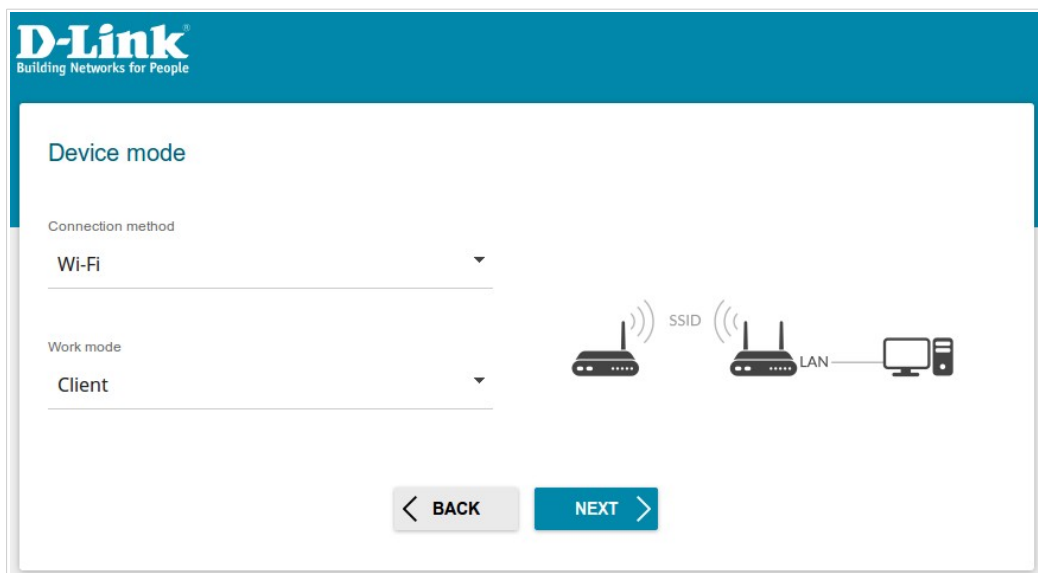


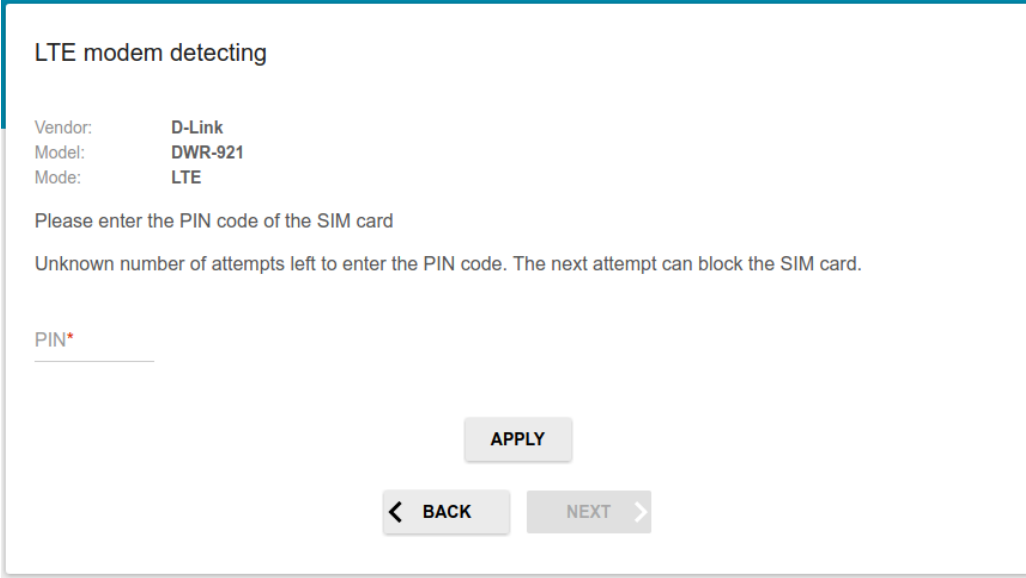
Figure 28. Selecting an operation mode. The **Client** mode.

When the operation mode is selected, click the **NEXT** button.

## Creating LTE WAN Connection

This configuration step is available for the **3G/LTE modem** mode.

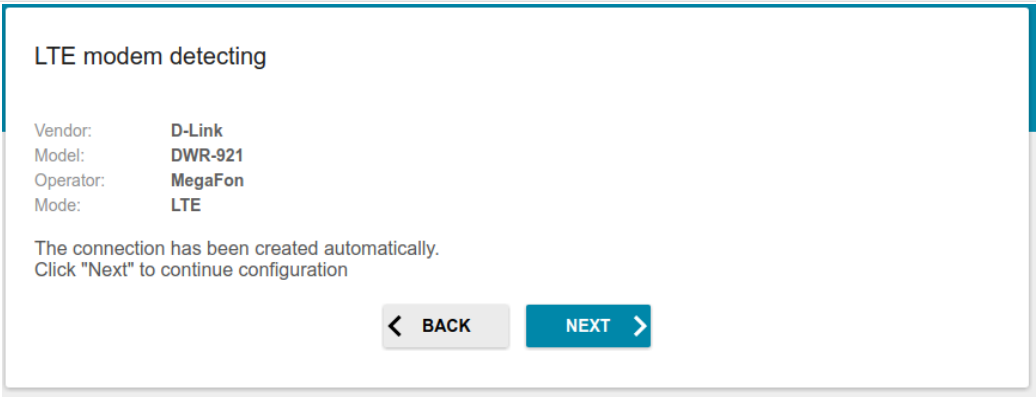
1. If the PIN code check is enabled for the SIM card inserted into the built-in modem, enter the PIN code in the **PIN** field and click the **APPLY** button.



The screenshot shows a web interface titled "LTE modem detecting". It displays the following information: Vendor: D-Link, Model: DWR-921, Mode: LTE. Below this, it asks the user to "Please enter the PIN code of the SIM card" and notes that an "Unknown number of attempts left to enter the PIN code. The next attempt can block the SIM card." There is a text input field labeled "PIN\*" and three buttons: "APPLY", "BACK", and "NEXT".

Figure 29. The page for entering the PIN code.

2. Please wait while the router automatically creates a WAN connection for your mobile operator.



The screenshot shows the same "LTE modem detecting" page. The information now includes: Vendor: D-Link, Model: DWR-921, Operator: MegaFon, Mode: LTE. A message states: "The connection has been created automatically. Click 'Next' to continue configuration". The "APPLY" button is no longer present, and the "NEXT" button is highlighted in blue.

Figure 30. The page for creating 3G/LTE connection.

3. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page. If the router failed to create a WAN connection automatically, click the **CONFIGURE MANUALLY** button. On the **Internet connection type** page, configure all needed settings and click the **NEXT** button.

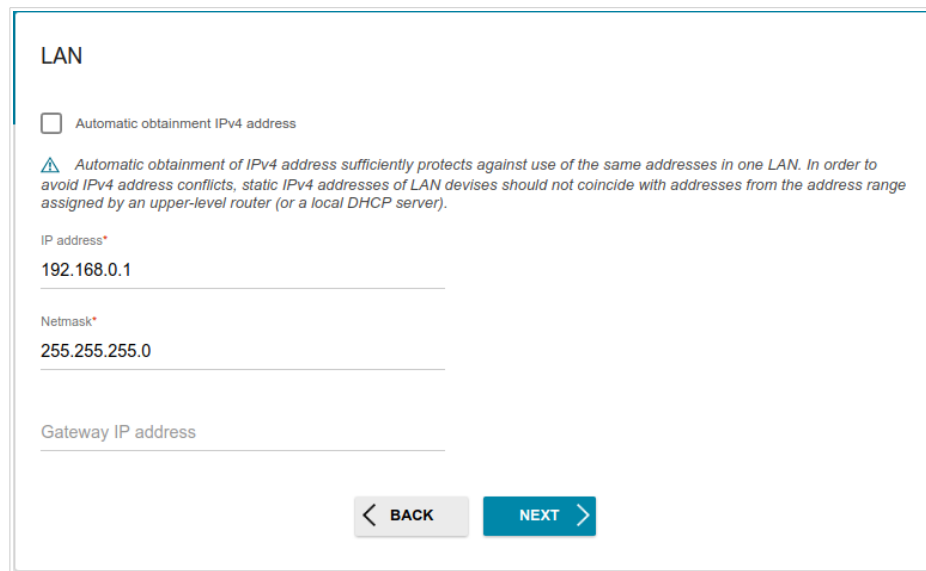
## Changing LAN IPv4 Address

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

1. Select the **Automatic obtainment of IPv4 address** to let DWR-921 automatically obtain the LAN IPv4 address.

**!** If the router obtains the LAN IPv4 address automatically, then after finishing the Wizard you can access the web-based interface using the domain name (by default, **dlinkrouter.local**) with a dot at the end.

If you want to manually assign the LAN IPv4 address for DWR-921, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address** and **Netmask** 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.



The screenshot shows a web interface titled "LAN". At the top, there is a checkbox labeled "Automatic obtainment IPv4 address" which is currently unchecked. Below this is a warning icon (a triangle with an exclamation mark) and a warning message: "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)." Below the warning, there are three input fields: "IP address\*" with the value "192.168.0.1", "Netmask\*" with the value "255.255.255.0", and "Gateway IP address" which is empty. At the bottom of the form, there are two buttons: a grey "BACK" button with a left arrow and a blue "NEXT" button with a right arrow.


Figure 31. The page for changing the LAN IPv4 address.


2. 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.

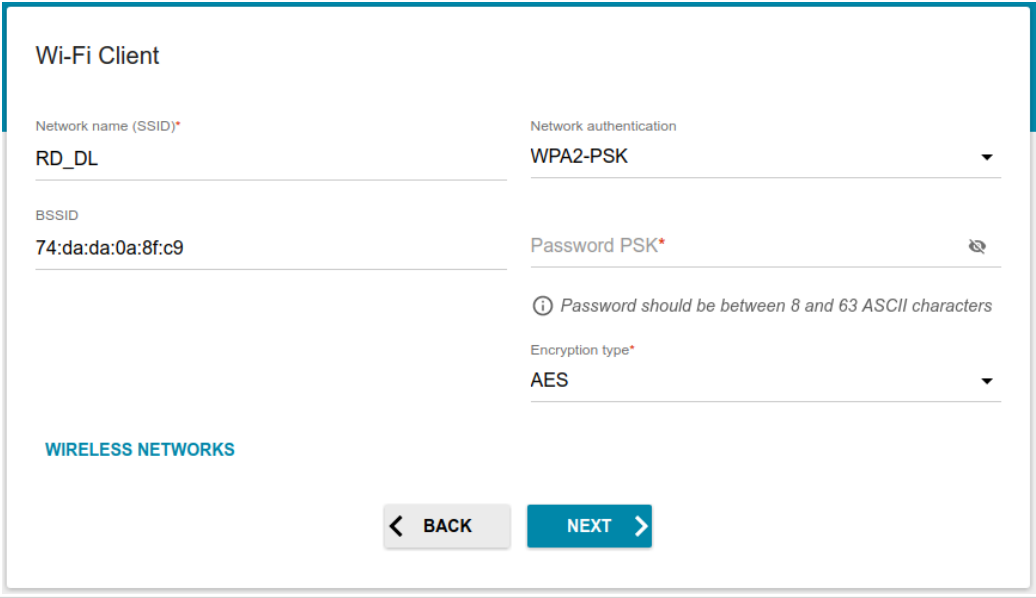


Figure 32. The page for configuring the Wi-Fi client.

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

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

Parameter	Description
<b>Enable encryption WEP</b>	<i>For <b>Open</b> authentication type only.</i> 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.

Parameter	Description
<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**, or **WPA-PSK/WPA2-PSK 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> .

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



## Configuring Wired 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, from the **Connection type** list, select the connection type used by your ISP and fill in the fields displayed on the page.
2. Specify the settings necessary for the connection of the selected type.
3. If your ISP uses MAC address binding, select the **Clone MAC address of your device** checkbox.
4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field.
5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

## Static IPv4 Connection

The screenshot shows a configuration page titled "Internet connection type". The "Connection type" dropdown menu is set to "Static IPv4". Below this, there is a descriptive sentence: "A connection of this type allows you to use a fixed IP address provided by your ISP." There are four input fields, each with a red asterisk indicating it is required: "IP address\*", "Netmask\*", "Gateway IP address\*", and "DNS IP address\*". Below these fields are two checkboxes: "Clone MAC address of your device" and "Use VLAN". A note below the checkboxes states: "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 bottom of the form are two buttons: a grey "BACK" button with a left arrow and a blue "NEXT" button with a right arrow.

Figure 33. The page for configuring Static IPv4 WAN connection.

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

## Static IPv6 Connection

Internet connection type

Connection type  
Static IPv6

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

IP address\*

Prefix\*

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

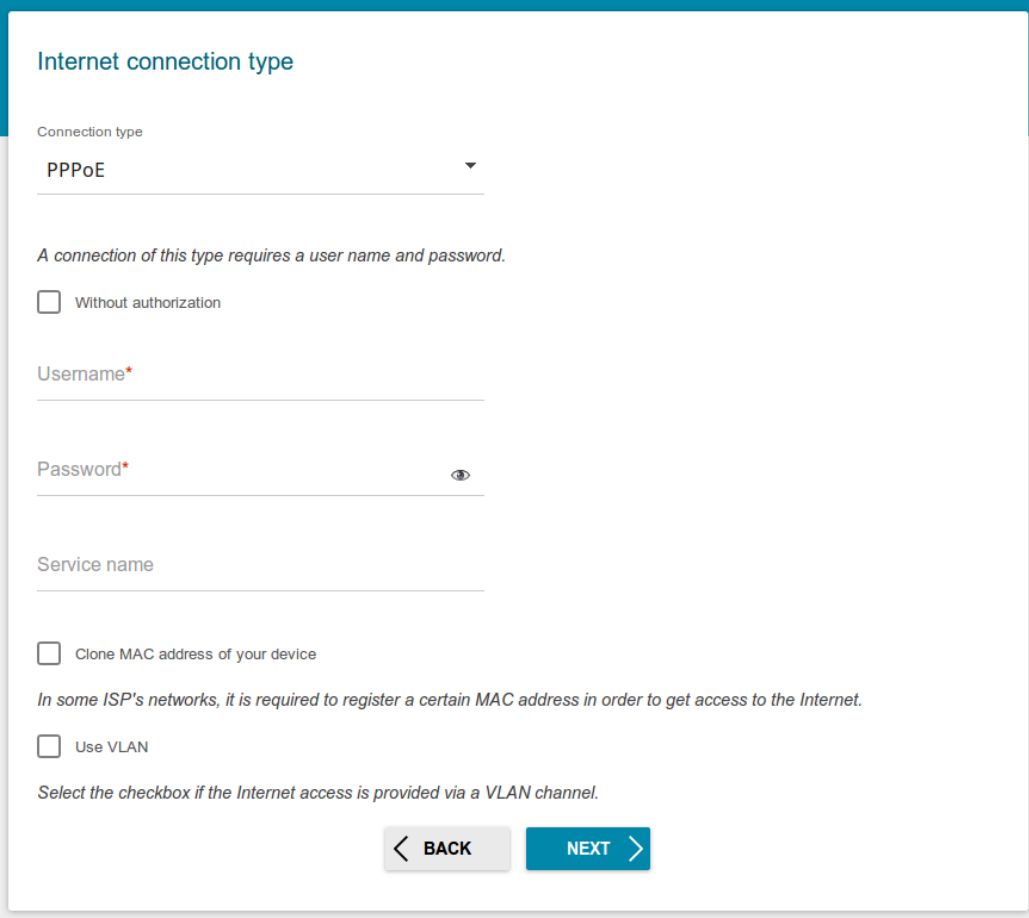
*i* Select the checkbox if the Internet access is provided via a VLAN channel.

[< BACK](#) [NEXT >](#)

Figure 34. The page for configuring Static IPv6 WAN connection.

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

## PPPoE, IPv6 PPPoE, PPPoE Dual Stack



The screenshot shows a web-based configuration interface for setting up an Internet connection. The title is "Internet connection type". Under "Connection type", a dropdown menu is set to "PPPoE". Below this, a note states: "A connection of this type requires a user name and password." There are two checkboxes: "Without authorization" (unchecked) and "Clone MAC address of your device" (unchecked). The "Clone MAC address" checkbox has a note: "In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet." Below these are input fields for "Username\*", "Password\*" (with a show/hide icon), and "Service name". At the bottom, there is a "Use VLAN" checkbox with a note: "Select the checkbox if the Internet access is provided via a VLAN channel." Navigation buttons for "BACK" and "NEXT" are at the bottom center.

Figure 35. 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.

## Configuring Wireless Network

This configuration step is available for the **3G/LTE modem, Router, Access point, WISP Repeater,** and **Repeater** modes.

1. On the **Wireless Network 2.4 GHz** page, in the **Network name** field, specify your own name for the wireless network or leave the value suggested by the router.
2. In the **Password** field, specify your own password for access to the wireless network or leave the value suggested by the router (WPS PIN of the device, see the barcode label).
3. 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\*

*The number of characters should not exceed 32*

Open network

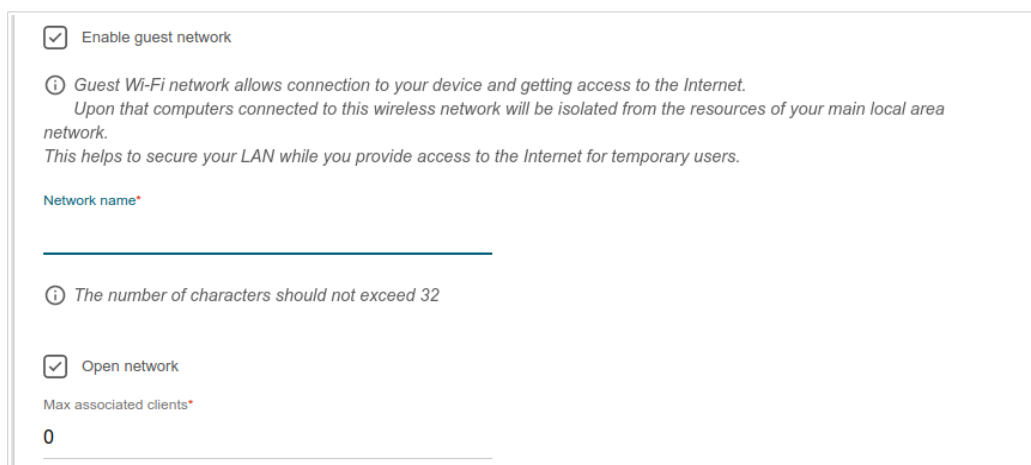
Password\*

*Password should be between 8 and 63 ASCII characters*

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

Figure 36. The page for configuring the wireless network.

4. If you want to create an additional wireless network isolated from your LAN, select the **Enable guest network** checkbox (available for the **3G/LTE modem**, **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\*

\_\_\_\_\_

*The number of characters should not exceed 32*

Open network

Max associated clients\*

0

Figure 37. The page for configuring the wireless network.

5. In the **Network name** field, specify your own name for the guest wireless network or leave the value suggested by the router.
6. 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.
7. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

## Configuring LAN Ports for IPTV/VoIP

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

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.*

4 3 LAN 2 1 Internet

Figure 38. The page for selecting a LAN port to connect an IPTV set-top box.

2. Select a free LAN port for connecting your set-top box.
3. If the IPTV service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.
4. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

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

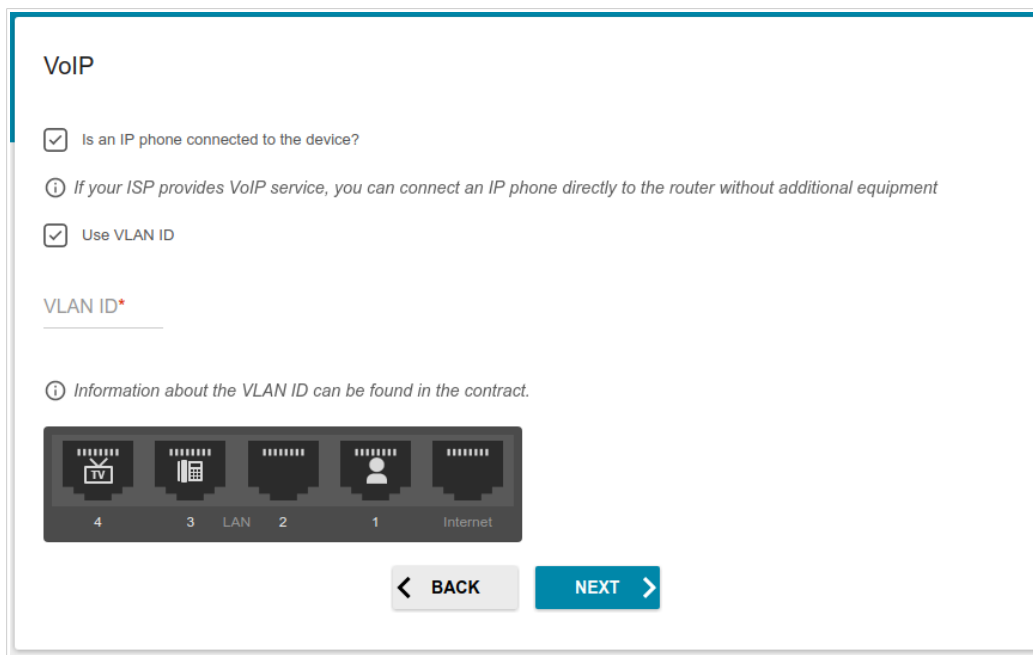


Figure 39. The page for selecting a LAN port to connect an VoIP phone.

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. 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>4</sup>

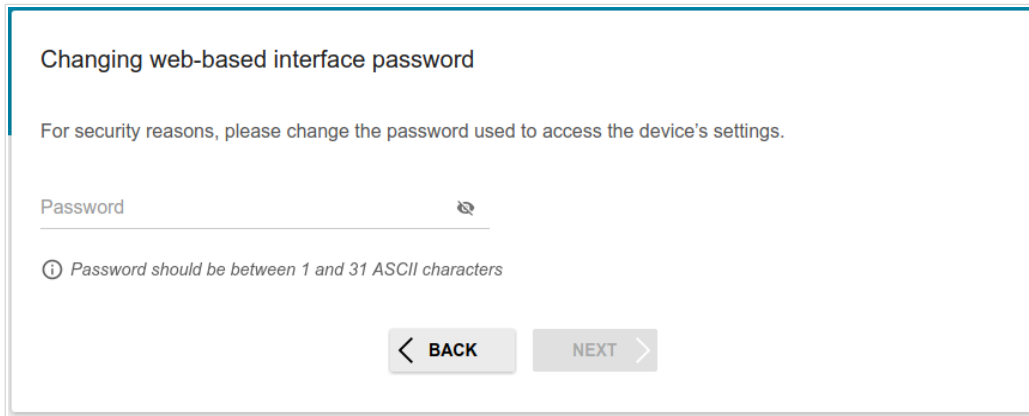


Figure 40. The page for changing the web-based interface password.

**!** 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.

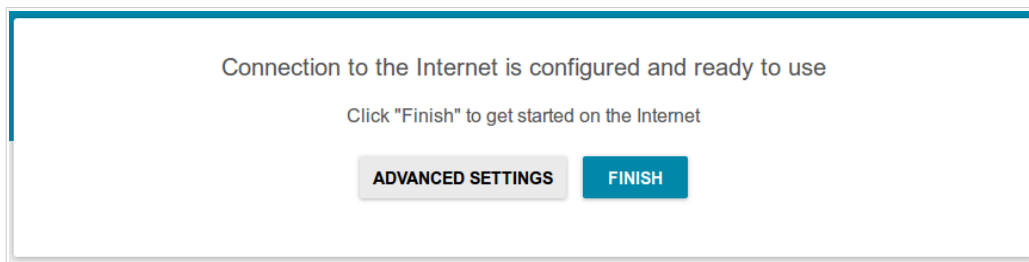
On the next page, check all specified settings.

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>4</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 41. 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 29).

## Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports or available wireless interfaces 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 DWR-921 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 or wireless interface 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.

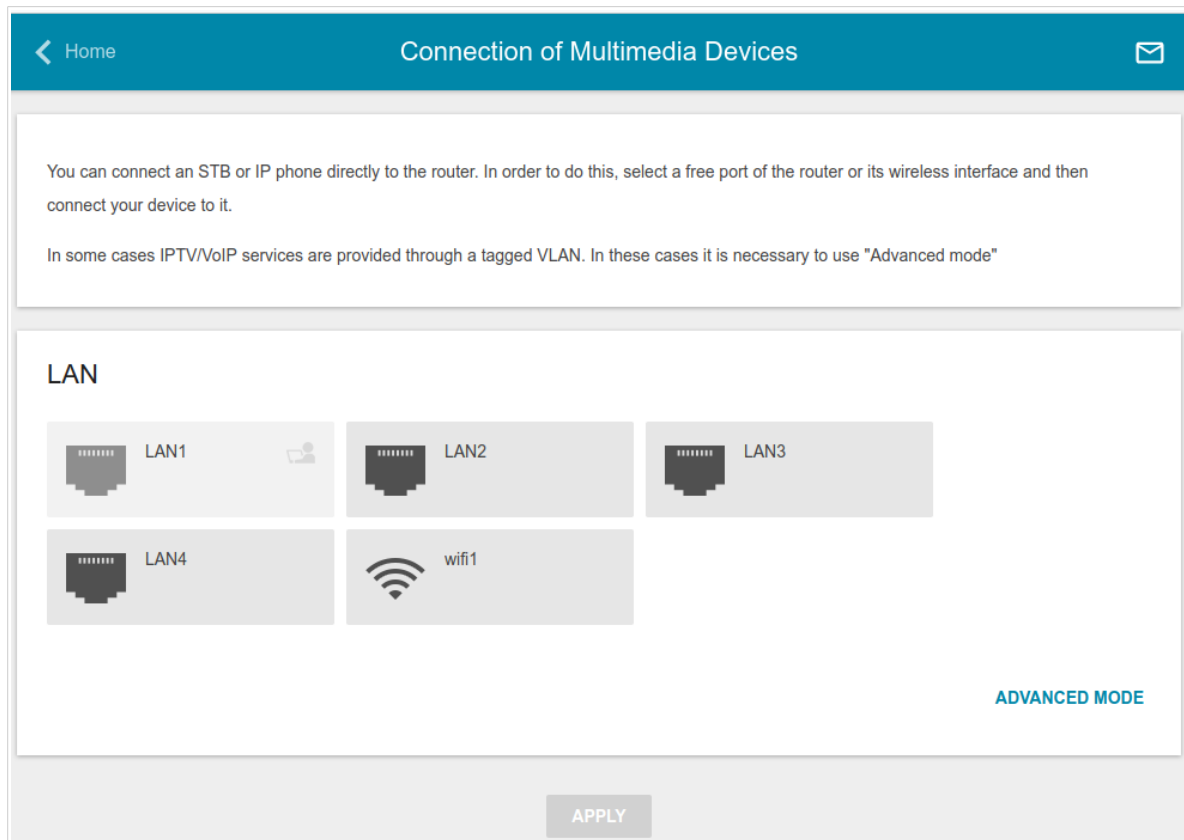


Figure 42. The Multimedia Devices Connection Wizard. The simple mode.

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

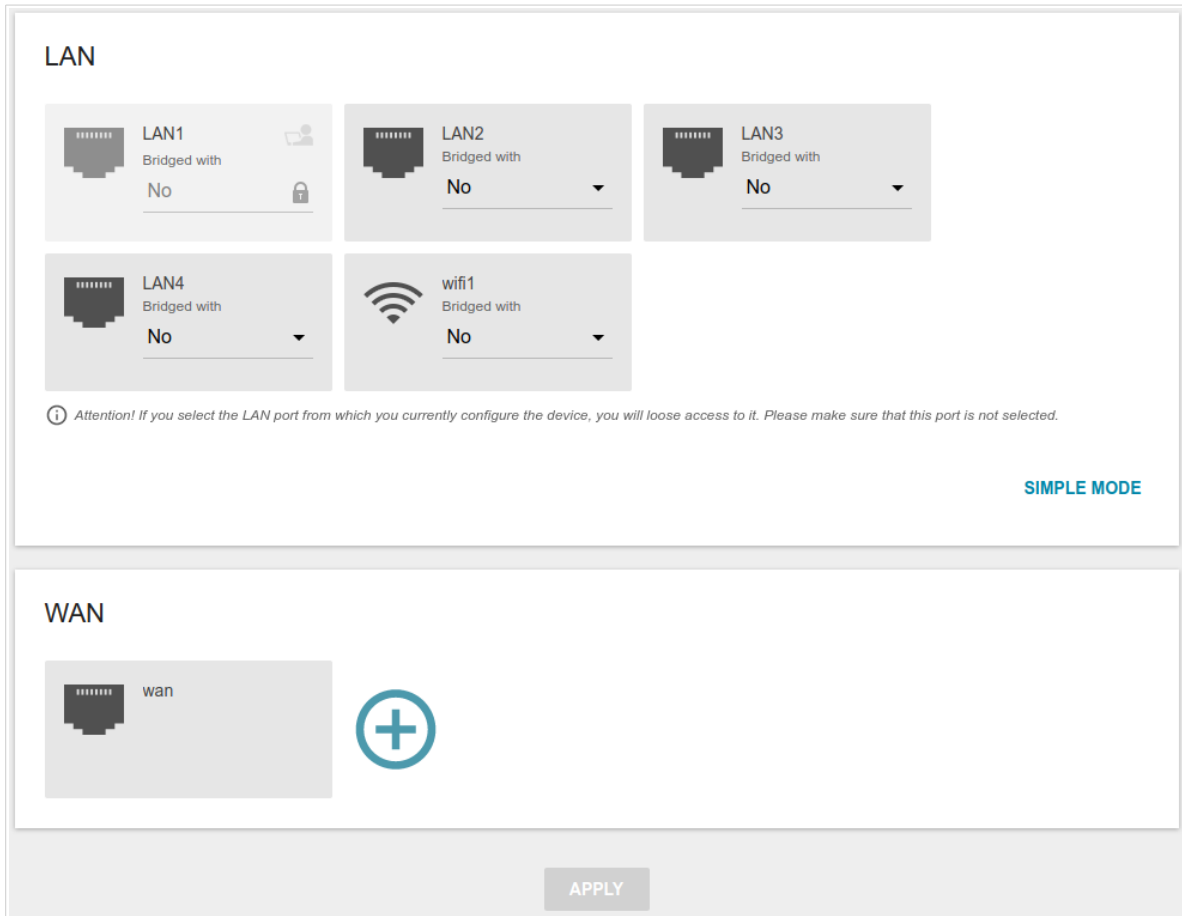


Figure 43. The Multimedia Devices Connection Wizard. The advanced mode.

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

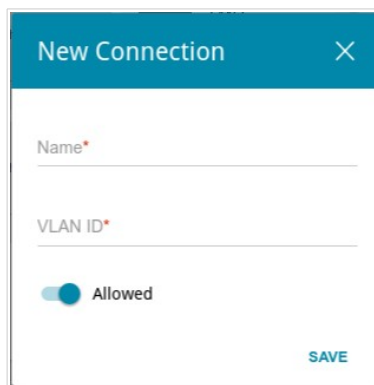



Figure 44. Adding a connection.

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 or wireless interface to which the additional device is connected, select the created connection. Click the **APPLY** button.

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

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

To deselect the port or wireless interface in the advanced mode, select the **No** value from the **Bridged with** drop-down list of the element corresponding to the needed LAN port or interface. Then in the **WAN** section, select the connection via VLAN which will not be used any longer and click the **REMOVE** 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 table
- data on devices connected to the router's network and its web-based interface
- addresses of active multicast groups
- active sessions.

## 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, gateway (if the connection is established), MAC address, and volume of data received and transmitted (with increase of the volume the units of measurement are changed automatically: byte, Kbyte, Mbyte, Gbyte).

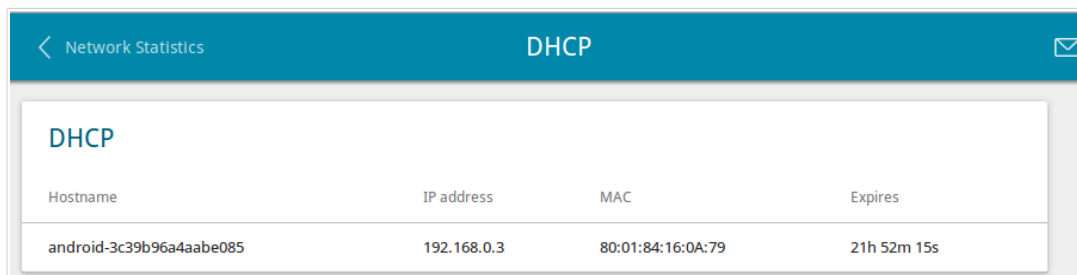
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 – 192.168.0.1 IPv6: fd01::1/64 – -	1.71 Mbyte / 3.58 Mbyte	0 / 0	-
WAN	-	-	-	-
WIFI	-	- / -	0 / 0	-

Figure 45. The **Statistics / Network Statistics** page.

To view 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, as well as the IP address expiration periods (the lease time).

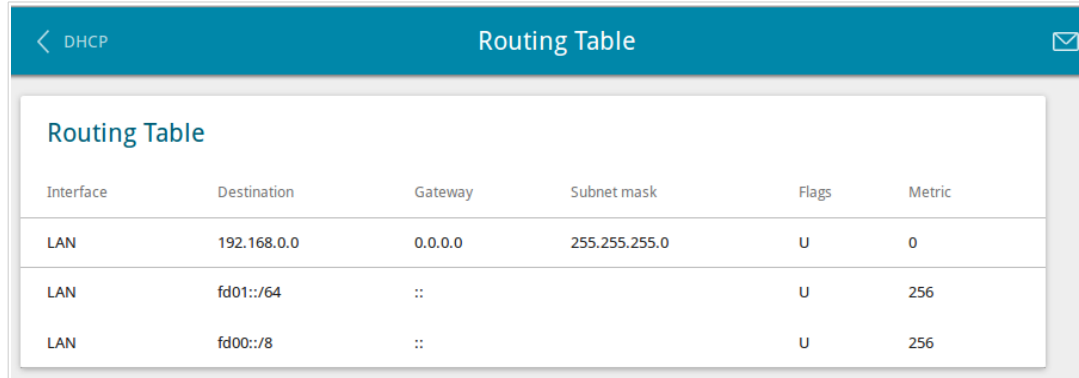


Hostname	IP address	MAC	Expires
android-3c39b96a4aabe085	192.168.0.3	80:01:84:16:0A:79	21h 52m 15s

Figure 46. The **Statistics / DHCP** page.

## Routing Table

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



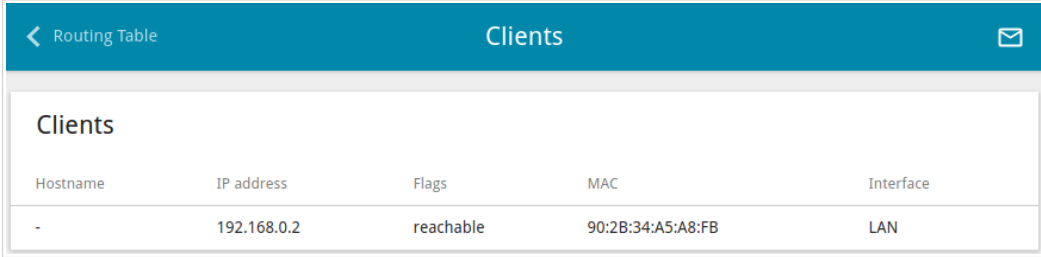
Interface	Destination	Gateway	Subnet mask	Flags	Metric
LAN	192.168.0.0	0.0.0.0	255.255.255.0	U	0
LAN	fd01::/64	::		U	256
LAN	fd00::/8	::		U	256

Figure 47. The **Statistics / Routing Table** page.



## Clients

On the **Statistics / Clients** page, you can view the list of devices connected to the local network of the router.



Hostname	IP address	Flags	MAC	Interface
-	192.168.0.2	reachable	90:2B:34:A5:A8:FB	LAN

*Figure 48. The **Statistics / Clients** 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.

## 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.

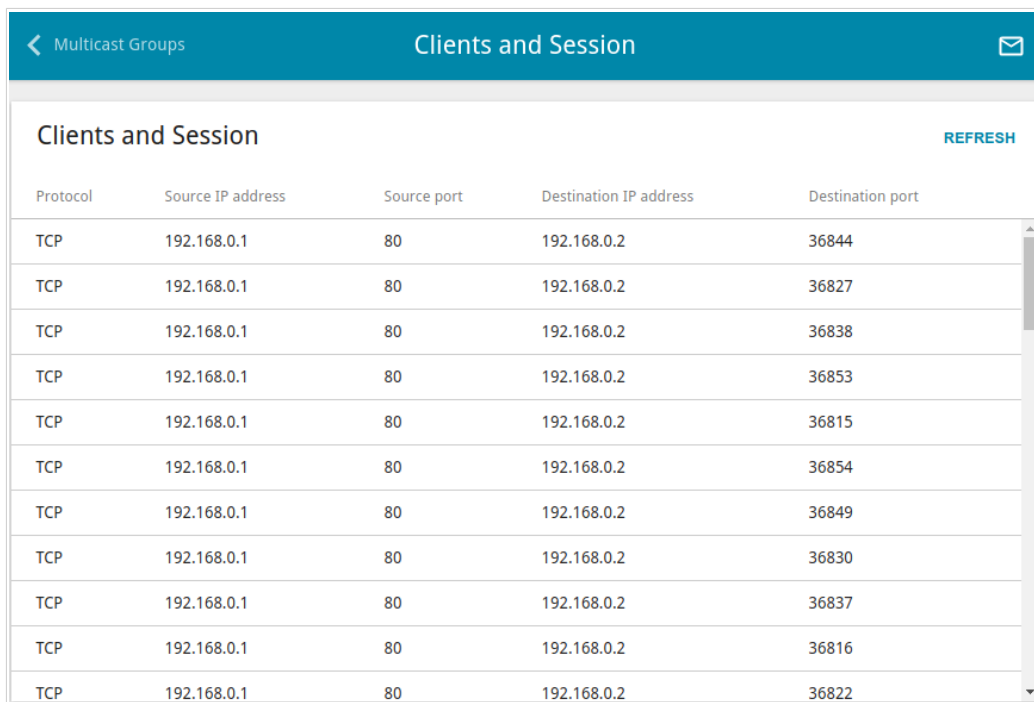
IPv4	
IP address	Interface
239.255.255.250	LAN

IPv6	
IP address	Interface

Figure 49. The **Statistics / Multicast Groups** page.

## Clients and Session

On the **Statistics / Clients and Session** page, you can view information on current sessions in the router's network. For each session the following data are displayed: the protocol for network packet transmission, the source IP address and port, and the destination IP address and port.



Protocol	Source IP address	Source port	Destination IP address	Destination port
TCP	192.168.0.1	80	192.168.0.2	36844
TCP	192.168.0.1	80	192.168.0.2	36827
TCP	192.168.0.1	80	192.168.0.2	36838
TCP	192.168.0.1	80	192.168.0.2	36853
TCP	192.168.0.1	80	192.168.0.2	36815
TCP	192.168.0.1	80	192.168.0.2	36854
TCP	192.168.0.1	80	192.168.0.2	36849
TCP	192.168.0.1	80	192.168.0.2	36830
TCP	192.168.0.1	80	192.168.0.2	36837
TCP	192.168.0.1	80	192.168.0.2	36816
TCP	192.168.0.1	80	192.168.0.2	36822

Figure 50. The **Statistics / Clients and Session** page.

To view the latest data on current sessions in the router's network, click the **REFRESH** button.

## 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.

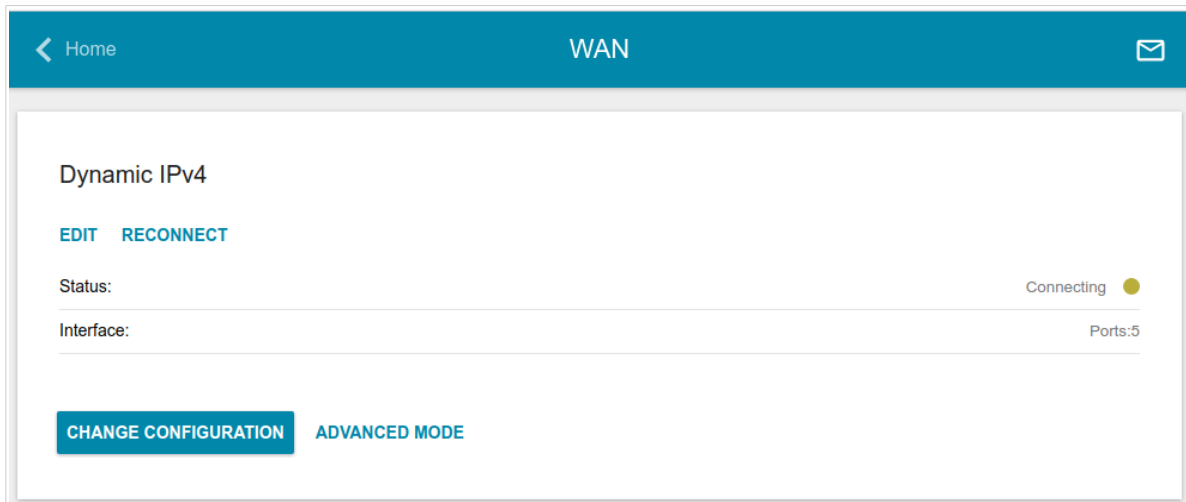


Figure 51. The **Connections Setup / WAN** page. The simplified mode.

To edit an existing connection, click the **EDIT** button. On the opened page, on the **Basic** tab, the mandatory settings of this connection will be displayed. To view all available settings of the WAN connection, go to the **All Settings** tab. 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.

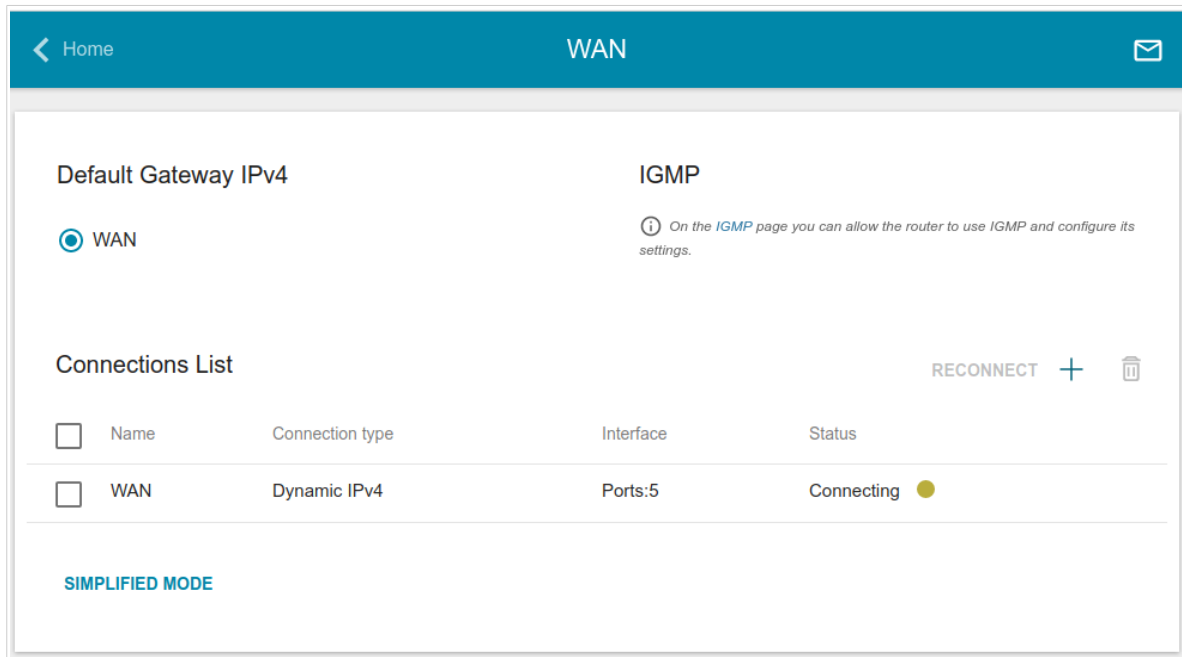



Figure 52. The **Connections Setup / WAN** page. The advanced mode.

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, on the **Basic** tab, the mandatory settings of this WAN connection will be displayed. To view all available settings of the WAN connection, go to the **All Settings** tab. 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 (  ). Also you can remove a connection on the editing page.

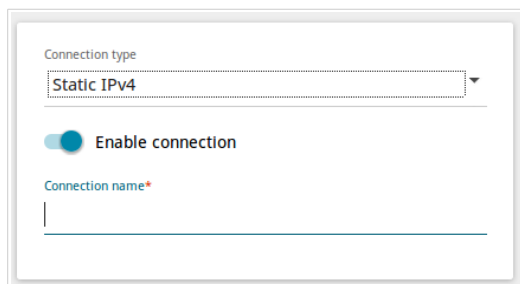
To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP** link (for the description of the page, see the **IGMP** section, page 148).

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, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.



The screenshot shows a web interface for creating a connection. At the top, there is a label 'Connection type' above a dropdown menu that has 'Static IPv4' selected. Below this is a toggle switch labeled 'Enable connection', which is currently turned on (indicated by a blue circle). At the bottom, there is a text input field labeled 'Connection name\*' which is currently empty.

Figure 53. The page for creating a new **Static IPv4** connection. Selecting a connection type.

Parameter	Description
<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>Connection name</b>	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.



Figure 54. 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.

The screenshot shows a configuration window titled "Authorization via 802.1x Protocol". At the top, there is a toggle switch labeled "Enable authorization via 802.1x protocol". Below this, the "Authentication method" is set to "EAP-MD5" with a lock icon. There are two input fields: "Login" and "Password", both with lock icons. The "Password" field has a dashed line below it, indicating a "Show" icon to toggle password visibility.

Figure 55. The page for creating a new **Static IPv4** connection. The **Authorization via 802.1x Protocol** section.


Parameter	Description
<b>Authorization via 802.1x Protocol</b>	
<b>Enable authorization via 802.1x protocol</b>	Move the switch to the right to allow authorization in the ISP's network via the 802.1x protocol.
<b>Authentication method</b>	Select a needed authentication method from the drop-down list.
<b>Login</b>	Enter the username provided by your ISP.
<b>Password</b>	Enter the password provided by your ISP. Click the <b>Show</b> icon (  ) to display the entered password.



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

Parameter	Description
<b>IPv4</b>	
<i>For <b>Static IPv4</b> type</i>	
<b>IP address</b>	Enter an IP address for this WAN connection.
<b>Netmask</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 server/ Secondary DNS server</b>	Enter addresses of the primary and secondary DNS servers in the relevant fields.
<i>For <b>Dynamic IPv4</b> 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 server</b> and <b>Secondary DNS server</b> fields are not available for editing.
<b>Primary DNS server/ Secondary DNS server</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>



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

Parameter	Description
<b>Miscellaneous</b>	
<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>Firewall</b>	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
<b>RIP</b>	Move the switch to the right to allow using RIP for this 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>Isolate connection</b>	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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

## Creating Dynamic IPv6 or Static IPv6 WAN Connection

On the connection creation page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.

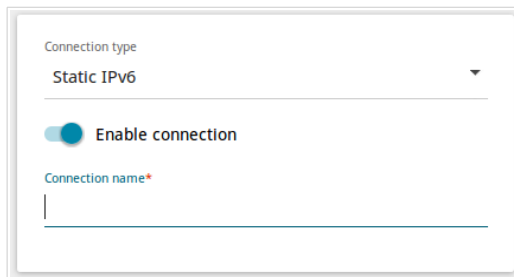


Figure 58. The page for creating a new **Static IPv6** connection. Selecting a connection type.

Parameter	Description
<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>Connection name</b>	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

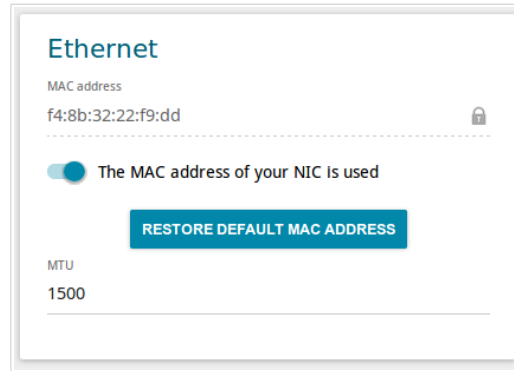


Figure 59. The page for creating a new **Static IPv6** connection. The **Ethernet** section.

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.

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

Parameter	Description
<b>IPv6</b>	
<i>For <b>Static IPv6</b> 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 <b>Dynamic IPv6</b> 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>Gateway by SLAAC</b>	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC ( <i>Stateless Address Autoconfiguration</i> ).
<b>Gateway IPv6 address</b>	The address of the IPv6 gateway. The field is available for editing, if the <b>Gateway by SLAAC</b> switch is moved to the left.
<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.



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

Parameter	Description
<b>Miscellaneous</b>	
<b>Firewall</b>	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
<b>RIP</b>	Move the switch to the right to allow using RIP for this 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>Isolate connection</b>	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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

## Creating PPPoE WAN Connection

On the connection creation page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.

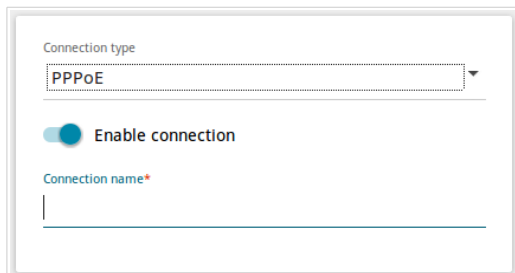


Figure 62. The page for creating a new **PPPoE** connection. Selecting a connection type.

Parameter	Description
<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>Connection name</b>	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

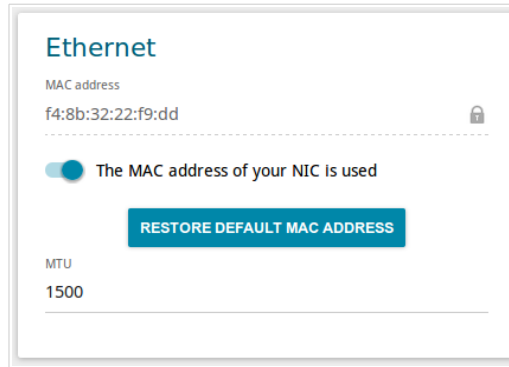


Figure 63. The page for creating a new **PPPoE** connection. The **Ethernet** section.

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.



Figure 64. 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.
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.

Parameter	Description
<b>Keep Alive</b>	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.
<b>Dial on demand</b>	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.
<b>Static IP address</b>	Fill in the field if you want to use a static IP address to access the Internet.
<b>PPP IP extension</b>	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on PPP connection debugging.

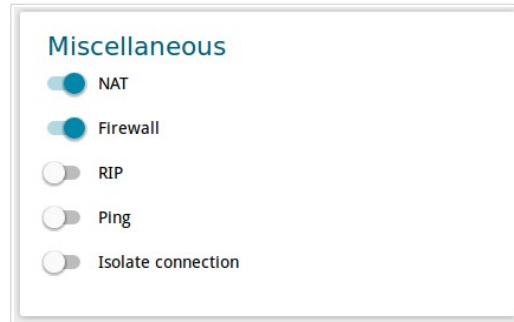


Figure 65. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.

Parameter	Description
<b>Miscellaneous</b>	
<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>Firewall</b>	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
<b>RIP</b>	Move the switch to the right to allow using RIP for this 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>Isolate connection</b>	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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

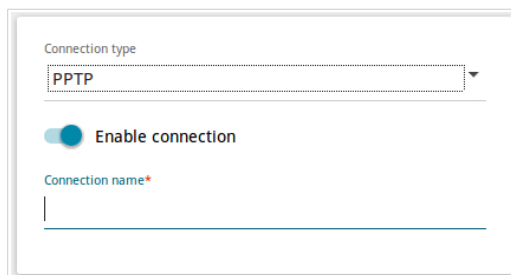
After clicking the button, the window for creating an additional connection opens.

If your ISP offers access to local services (e.g. audio and video resources), select the existing connection or select the **create a new connection** choice of the radio button. Then click the **OK** button. On the page displayed, specify the parameters for the connection of the Dynamic IPv4 or Static IPv4 type and click the **APPLY** button. Click the **BACK** button to specify other settings for the connection of the PPPoE type.

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 or L2TP WAN Connection

On the connection creation page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.



The screenshot shows a web interface for creating a connection. It features a dropdown menu labeled 'Connection type' with 'PPTP' selected. Below this is a toggle switch labeled 'Enable connection' which is currently turned on (indicated by a blue circle). At the bottom, there is a text input field labeled 'Connection name' with a red asterisk indicating it is a required field.


Figure 66. The page for creating a new **PPTP** connection. Selecting a connection type.

Parameter	Description
<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>Connection name</b>	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

**PPP**

Without authorization

Username\*

Password\*  

VPN server address\*

MTU\*  
1456

Authentication protocol  
AUTO ▼


Encryption protocol  
No encryption ▼

Keep Alive

LCP interval\*  
30

LCP fails\*  
3

Dial on demand

Maximum idle time (in seconds)  
0 

---


Extra options

Static IP address

PPP debug

Enable MPPC

Figure 67. 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.
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.

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>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>Extra options</b>	<p>Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional.</i></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>
<b>Enable MPPC</b>	<p><i>(Microsoft Point-to-Point Compression)</i> <i>For the PPTP type only.</i></p> <p>Move the switch to the right if it is necessary to use the data compression function in order to configure the connection.</p> <p>Move the switch to the left to disable the function.</p>

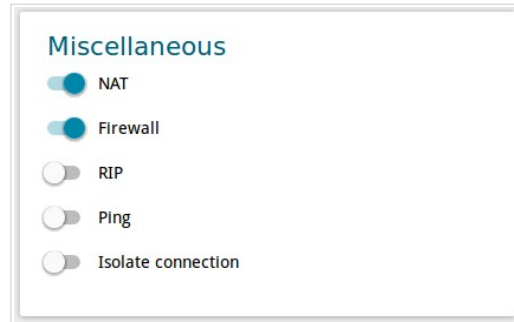


Figure 68. The page for creating a new **PPTP** connection. The **Miscellaneous** section.

Parameter	Description
<b>Miscellaneous</b>	
<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>Firewall</b>	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
<b>RIP</b>	Move the switch to the right to allow using RIP for this 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>Isolate connection</b>	If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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 the existing connection which will be used to access the PPTP/L2TP server or select the **create a new connection** choice of the radio 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.

Click the **OK** button.

## Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

On the connection creation page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.



The screenshot shows a configuration form with the following elements:

- A dropdown menu labeled "Connection type" with "PPPoE IPv6" selected.
- A toggle switch labeled "Enable connection" that is currently turned on (blue).
- A text input field labeled "Connection name\*" with a red asterisk indicating it is a required field.

Figure 69. The page for creating a new **PPPoE IPv6** connection. Selecting a connection type.

Parameter	Description
<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>Connection name</b>	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.



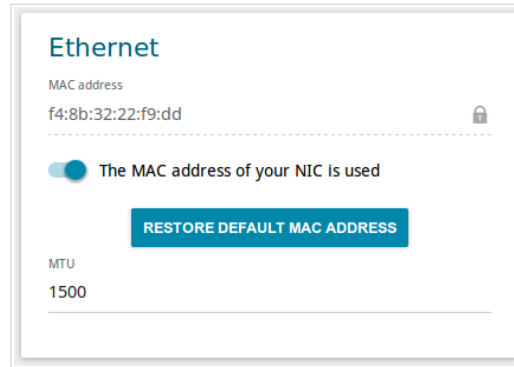


Figure 70. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.

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.

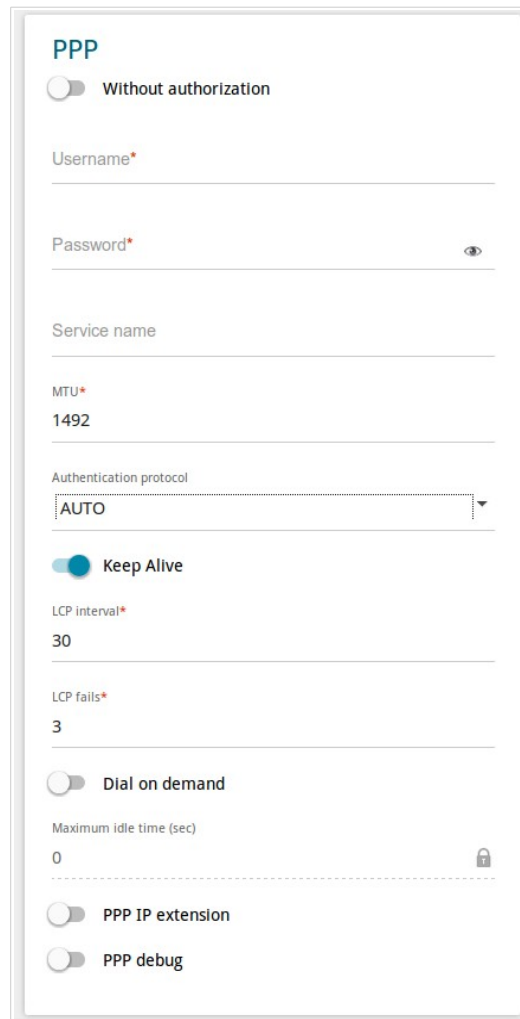


Figure 71. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.

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.
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.

Parameter	Description
<b>Keep Alive</b>	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.
<b>Dial on demand</b>	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.
<b>Static IP Address</b>	<i>For the <b>PPPoE Dual Stack</b> type only.</i> Fill in the field if you want to use a static IP address to access the Internet.
<b>PPP IP extension</b>	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on PPP connection debugging.

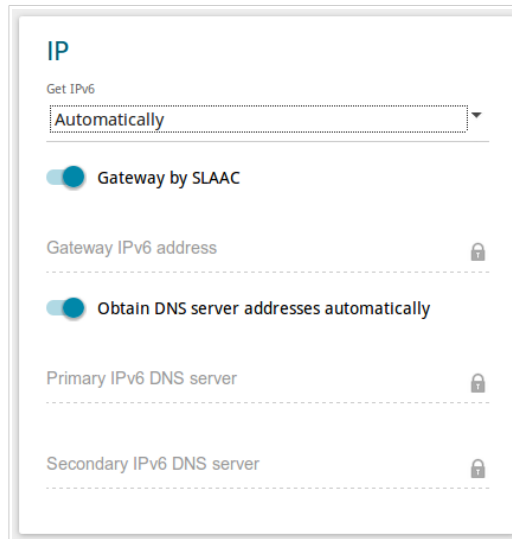


Figure 72. The page for creating a new PPPoE IPv6 connection. The IP section.

Parameter	Description
<b>IP</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>Gateway by SLAAC</b>	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC ( <i>Stateless Address Autoconfiguration</i> ).
<b>Gateway IPv6 address</b>	The address of the IPv6 gateway. The field is available for editing, if the <b>Gateway by SLAAC</b> switch is moved to the left.
<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.



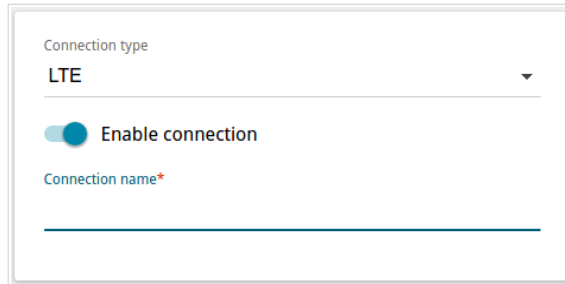
Figure 73. The page for creating a new **PPPoE IPv6** connection. The **Miscellaneous** section.

Parameter	Description
<b>Miscellaneous</b>	
<b>NAT</b>	<p><i>For the <b>PPPoE Dual Stack</b> type only.</i></p> <p>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.</p>
<b>Firewall</b>	<p>If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.</p>
<b>RIP</b>	<p>Move the switch to the right to allow using RIP for this connection.</p>
<b>Ping</b>	<p>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.</p>
<b>Isolate connection</b>	<p>If the switch is moved to the right, the router uses an alternate routing table for this connection. Enable this function only when your ISP requires this.</p>

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

## Creating LTE WAN Connection

If the PIN code check is enabled for the SIM card inserted into the built-in modem, then prior to creating an LTE WAN connection, go to the **LTE Modem** menu and enter the PIN code on the page displayed (see the *LTE Modem* section, page 121). Then on the connection creation page, go to the **All Settings** tab, select the relevant value from the **Connection Type** drop-down list, and specify the needed values.



The screenshot shows a web interface for creating a new LTE connection. It features a dropdown menu labeled 'Connection type' with 'LTE' selected. Below this is a toggle switch labeled 'Enable connection' which is currently turned on. At the bottom, there is a text input field labeled 'Connection name' with a red asterisk indicating it is required.

Figure 74. The page for creating a new **LTE** connection. Selecting a connection type.

Parameter	Description
<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>Connection name</b>	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

Figure 75. The page for creating a new **LTE** connection. The **USB Modem** section.


Parameter	Description
<b>USB Modem</b>	
<b>Mode</b>	The value of the field specifies the type of the network to which the router connects. Leave the <b>Auto</b> value to let the router connect automatically to an available type of network, or select a needed value from the drop-down list.
<b>APN</b>	An access point name.
<b>Without authorization</b>	Move the switch to the right if your operator does not require authorization.
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list.
<b>Username</b>	A username (login) to connect to the network of the operator.
<b>Password</b>	A password to connect to the network of the operator. Click the <b>Show</b> icon (  ) to display the entered password.

Figure 76. The page for creating a new **LTE** connection. The **IPv4** section.

Parameter	Description
<b>IPv4</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 server</b> and <b>Secondary DNS server</b> fields are not available for editing.
<b>Primary DNS server/ Secondary DNS server</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>



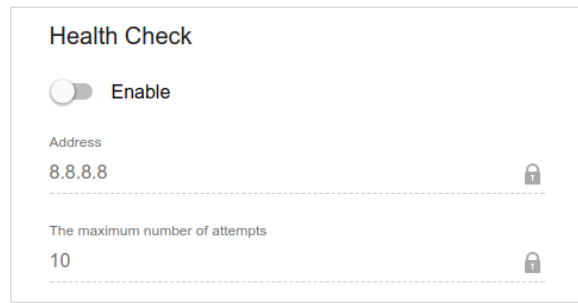


Figure 77. The page for creating a new **LTE** connection. The **Health Check** section.

Parameter	Description
<b>Health Check</b>	
<b>Enable</b>	The Health Check function allows the router to constantly check the LTE connection status by checking availability of a remote host. Move the switch to the right to enable the function. Move the switch to the left to disable the function.
<b>Address</b>	An IP address that the router will check for availability.
<b>The maximum number of attempts</b>	A number of messages that were sent to check the status of a remote host and left unanswered. By default, the value <b>10</b> is specified. If a remote host does not answer the specified number of messages, the <b>Connecting</b> value will be displayed in the <b>Status</b> field on the <b>Connections Setup / WAN</b> page.

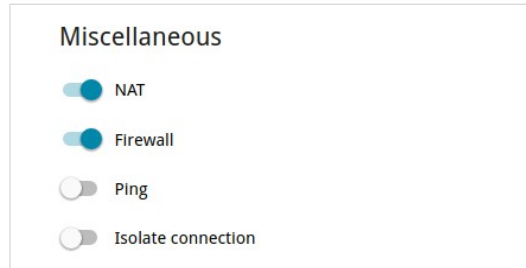


Figure 78. The page for creating a new **LTE** connection. The **Miscellaneous** section.

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

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 IPv4 address, configure the built-in DHCP server, or specify MAC address and IP address pairs.

Local IP Address

IP address\*  
192.168.0.1

Subnet mask\*  
255.255.255.0

Device domain name  
dlinkrouter.local

Figure 79. 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><i>For the <b>Access point, Repeater, and Client</b> modes only.</i></p> <p>Select the needed value from the drop-down list.</p> <p><b>Static:</b> the IP address, subnet mask, and the gateway IP address are assigned manually.</p> <p><b>Dynamic:</b> the router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.</p>
<b>IP address</b>	The IP address of the router in the local subnet. By default, the following value is specified: <b>192.168.0.1</b> .
<b>Subnet mask</b>	The mask of the local subnet. By default, the following value is specified: <b>255.255.255.0</b> .
<b>Gateway IP address</b>	<p><i>For the <b>Access point, Repeater, and Client</b> modes only.</i></p> <p>The gateway IP 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></p>
<b>Device domain name</b>	The name of the device assigned to its IP address in the local subnet.

Figure 80. 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>	<p>An operating mode of the router's DHCP server.</p> <p><b>Disable:</b> the router's DHCP server is disabled, clients' IP addresses are assigned manually.</p> <p><b>DHCP 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.</p> <p><b>DHCP 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> field is displayed on the tab.</p>
<b>Start IP</b>	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
<b>End IP</b>	The end IP address of the address pool 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.

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

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

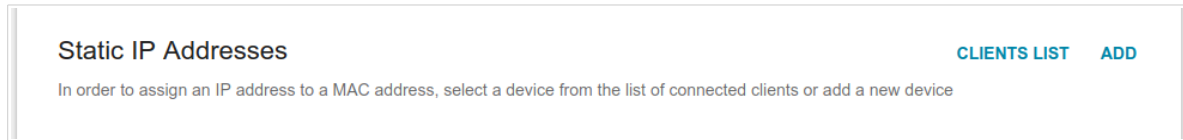




Figure 81. The section for creating MAC-IPv4 pairs.

To create a MAC-IPv4 pair, click the **ADD** button (  ). In the opened window, in the **IP address** field, enter an IPv4 address which will be assigned to the device from the LAN, then in the **MAC address** field, enter the MAC address of this device. In the **Hostname** field, specify a network name of the device for easier identification (*optional*). Click the **APPLY** button.

Also you can create a MAC-IPv4 pair for a device connected to the router's LAN at the moment. To do this, click the **CLIENTS LIST** button. In the opened window, select the relevant device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

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

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

## IPv6

Go to the **IPv6** tab to change IPv6 address of the router and configure IPv6 addresses assignment settings.

The screenshot shows a configuration window titled "Local IPv6 Address". It contains three main sections:
 

- Mode of local IPv6 address assignment:** A dropdown menu currently showing "Prefix delegation".
- IPv6 address:** A text input field containing "fd01::1" with a lock icon to its right.
- Prefix:** A text input field containing "64" with a lock icon to its right.

Figure 82. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.

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

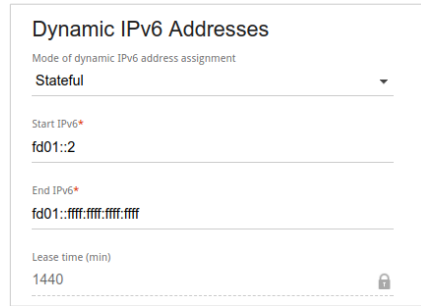


Figure 83. Configuring the local interface. The IPv6 tab. The **Dynamic IPv6 Addresses** section.

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> <p><b>Disable:</b> clients' IPv6 addresses are assigned manually.</p> <p><b>Stateful:</b> the built-in DHCPv6 server of the router allocates addresses from the range specified in the <b>Start IPv6</b> and <b>End IPv6</b> fields.</p> <p><b>Stateless:</b> clients themselves configure IPv6 addresses using the prefix.</p>
<b>Start IPv6</b>	The start IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
<b>End IPv6</b>	The end IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
<b>Lease Time</b>	The lifetime of IPv6 addresses provided to clients. The field is available for editing, if the <b>Static</b> value is selected from the <b>Mode of local IPv6 address assignment</b> list in the <b>Local IPv6 Address</b> section.

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

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

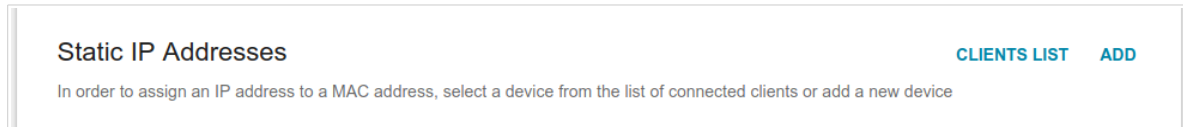




Figure 84. The section for creating MAC-IPv6 pairs.

To create a MAC-IPv6 pair, click the **ADD** button (  ). In the opened window, in the **IP address** field, enter an IPv6 address which will be assigned to the device from the LAN, then in the **MAC address** field, enter the MAC address of this device. In the **Hostname** field, specify a network name of the device for easier identification (*optional*). Click the **APPLY** button.

Also you can create a MAC-IPv6 pair for a device connected to the router's LAN at the moment. To do this, click the **CLIENTS LIST** button. In the opened window, select the relevant device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

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

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



## WAN Reservation

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

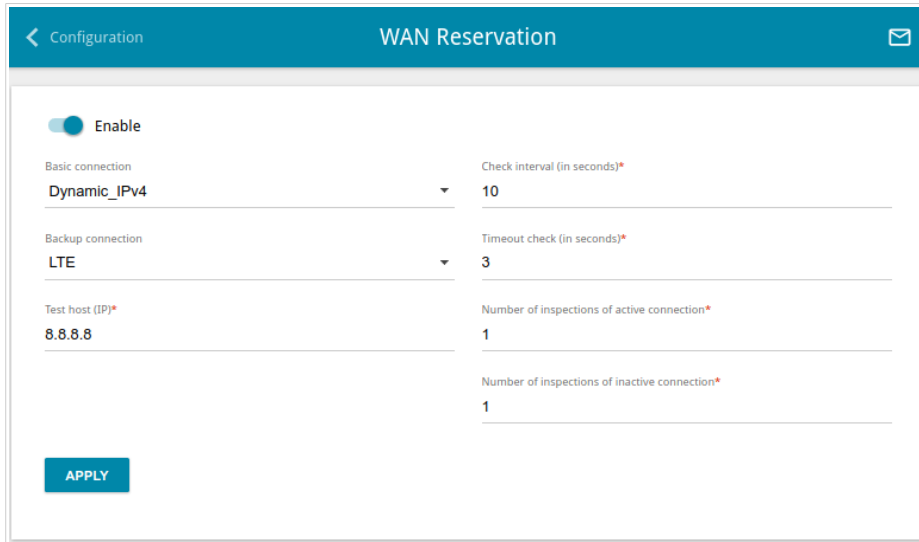


Figure 85. The **Connections Setup / WAN Reservation** page.

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

Parameter	Description
<b>Basic connection</b>	From the drop-down list, select a WAN connection which will be used as the main one.
<b>Backup connection</b>	From the drop-down list, select a WAN connection which will be used as the reserve one.
<b>Test host</b>	An IP address that the router will check for availability via ICMP ping mechanism.
<b>Check interval</b>	A time period (in seconds) between attempts to check the status of the main connection. By default, the value <b>10</b> is specified.
<b>Timeout check</b>	A time period (in seconds) for an attempt to check the status of the main connection. At the end of this period the router's internal system makes a decision to enable/disable the reserve channel. By default, the value <b>3</b> is specified.
<b>Number of inspections of active connection</b>	A number of requests that will be sent in order to analyze the status of the main connection when the connection is active (the router uses the main connection as a default gateway).

Parameter	Description
<b>Number of inspections of inactive connection</b>	A number of requests that will be sent in order to analyze the status of the main connection when the connection is inactive (the router uses the reserve connection as a default gateway).

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

## 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.

The screenshot shows the 'Basic Settings' page for the wireless LAN configuration. The page is divided into two main sections: 'General Settings' and 'Wi-Fi Network'. Below these, there is a 'Security Settings' section. At the bottom, there are two buttons: 'APPLY' and 'ADD WI-FI NETWORK'.

**General Settings**

- Enable Wireless
- Country: RUSSIAN FEDERATION
- Wireless mode: 802.11 B/G/N mixed
- Select channel automatically
- Channel: auto (channel 13)
- Enable periodic scanning
- Scanning period (in seconds): 60

**Wi-Fi Network**

- Network name (SSID)\*: DWR-XXX-d8ac
- Hide SSID
- Max associated clients\*: 0
- Broadcast wireless network
- Clients isolation

**Security Settings**

- Network authentication: WPA2-PSK
- Password PSK\*: [REDACTED]
- Encryption type\*: AES
- Group key update interval (in seconds)\*: 3600

Buttons: APPLY, ADD WI-FI NETWORK

Figure 86. Basic settings of the wireless LAN.

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

Parameter	Description
<b>Enable Wireless</b>	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left.
<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>Channel</b>	The wireless channel number. Left-click to open the window for selecting a channel (the action is available, when the <b>Select channel automatically</b> switch is moved to the left).
<b>Enable periodic scanning</b>	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.
<b>Scanning period</b>	Specify a period of time (in seconds) after which the router rescans channels.

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

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

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

The screenshot shows the 'Add Wi-Fi Network' configuration page. The page has a teal header with a back arrow, 'Basic Settings', 'Add Wi-Fi Network', and an envelope icon. The main content is split into two columns: 'Wi-Fi Network' and 'Security Settings'.  
**Wi-Fi Network**  
Network name (SSID)\*: DWR-921-d8ac.2  
*The number of characters should not exceed 32*  
 Hide SSID  
*Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point*  
Max associated clients\*: 0  
 Broadcast wireless network  
*Allows you to enable/disable broadcast of this SSID without disconnecting the wireless module of the router. Can be used with the mode "Wi-Fi Client"*  
 Clients isolation  
*Block traffic between devices connected to the access point*  
 Enable guest network  
*Enable the guest network in order to isolate Wi-Fi clients from the LAN network*  
**Security Settings**  
Network authentication: WPA2-PSK  
Password PSK\*: [masked]  
*Password should be between 8 and 63 ASCII characters*  
Encryption type\*: AES  
Group key update interval (in seconds)\*: 3600  
An **APPLY** button is at the bottom left.

Figure 87. Creating a wireless network.

Parameter	Description
<b>Wi-Fi Network</b>	
<b>Network name (SSID)</b>	A name for the wireless network. The name can consist of digits and Latin characters.
<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>Broadcast wireless network</b>	If the switch is moved to the left, devices cannot connect to the wireless network. Upon that the router can connect to another access point as a wireless client.
<b>Clients isolation</b>	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
<b>Enable guest network</b>	This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.

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

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

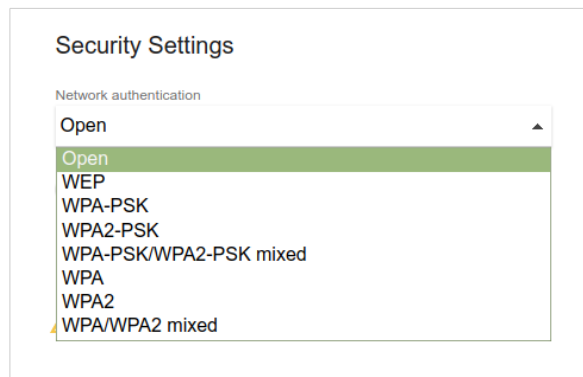


Figure 88. Network authentication types supported by the router.

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).
<b>WEP</b>	Authentication with with WEP encryption. This authentication type is not available when a mode supporting 802.11n 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.



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

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

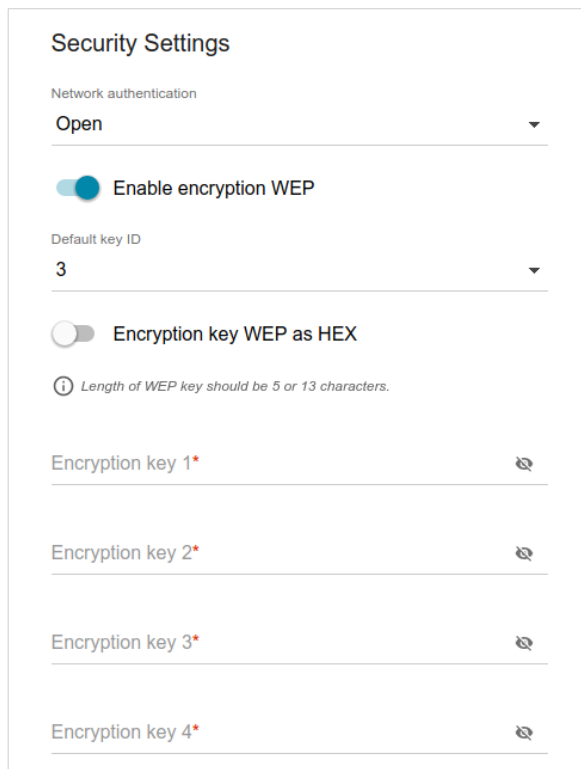



Figure 89. The **Open** value is selected from the **Network authentication** drop-down list.

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

Figure 90. 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>5</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> .
<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>5</sup> 0-9, A-Z, a-z, space, !"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~.

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


The screenshot shows the 'Security Settings' section of the router's web interface. It includes a 'Network authentication' dropdown menu currently set to 'WPA2'. Below it is a toggle switch for 'WPA2 Pre-authentication' which is currently turned off. There are several input fields: 'IP address RADIUS server\*' with the value '192.168.0.254', 'RADIUS server port\*' with the value '1812', 'RADIUS encryption key\*' with the value 'dlink', 'Encryption type\*' with a dropdown set to 'AES', and 'Group key update interval (in seconds)\*' with the value '3600'.

Figure 91. 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.
<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.

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.

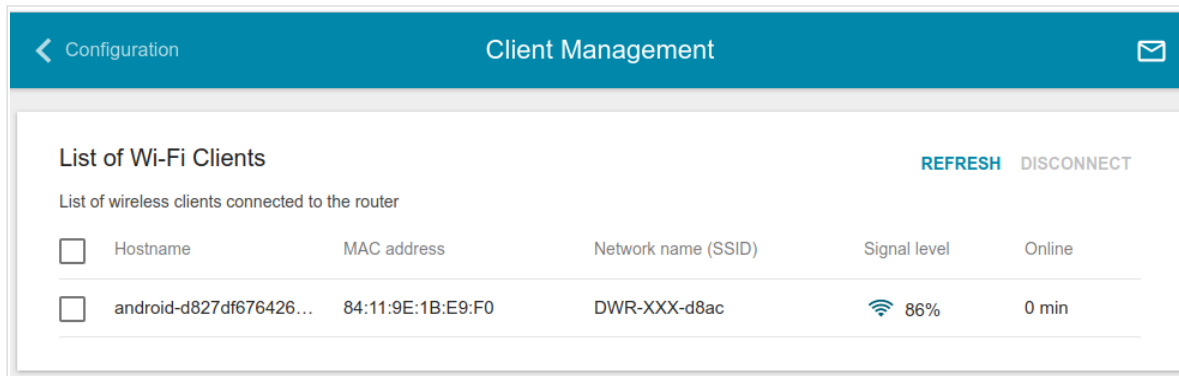


Figure 92. The page for managing the wireless clients.

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, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** with the **AES** encryption method. When other security settings are specified, controls of the **WPS** page are not available.

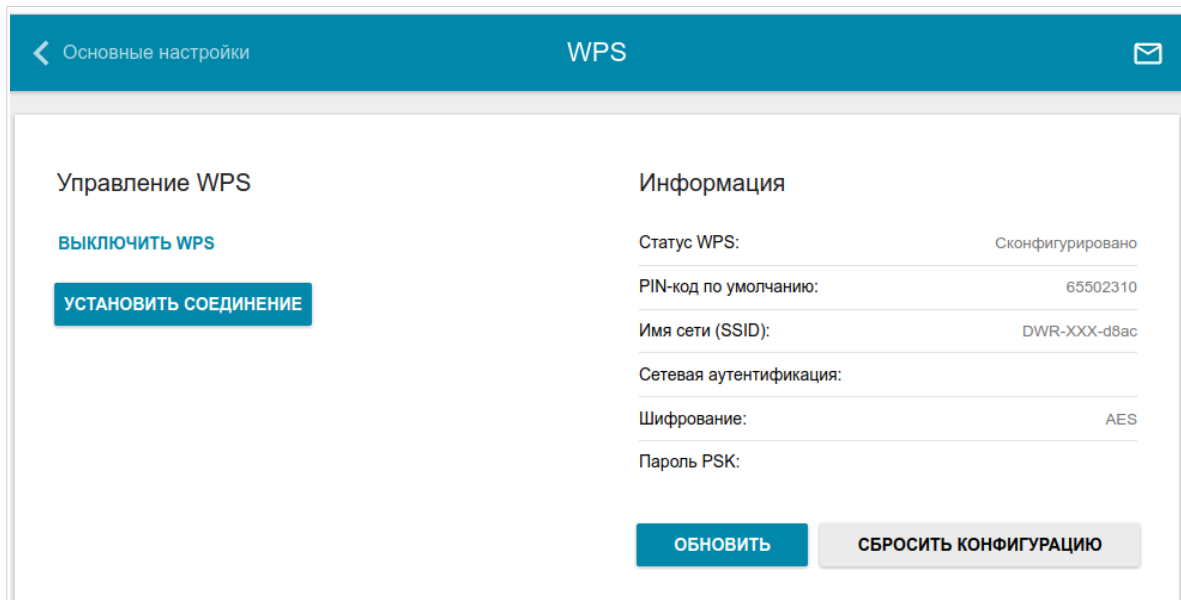


Figure 93. The page for configuring the WPS function.

To activate the WPS function, 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.
<b>RESET TO UNCONFIGURED</b>	Click the button to reset the parameters of the WPS function.

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

To connect to the basic wireless network via the 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. Click the **ENABLE WPS** button.
3. Save the settings and 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 and release. The **WLAN LED** will start blinking slowly.

## WMM

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

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

To enable the function, click the **ENABLE** button. Upon that the **Access Point** and **Station** sections are displayed on the page.

Access Point							Station					
AC	AIFSN	CWMin	CWMax	TXOP	ACM	ACK	AC	AIFSN	CWMin	CWMax	TXOP	ACM
BK	7	31	1023	0	off	off	BK	7	15	1023	0	off
BE	3	15	63	0	off	off	BE	3	15	1023	0	off
VI	1	7	15	94	off	off	VI	2	7	15	94	off
VO	1	3	7	47	off	off	VO	2	3	7	47	off

Figure 94. The page for configuring the WMM function.



All needed settings for the WMM function are specified in the device's system. It is recommended not to change the default values.



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.

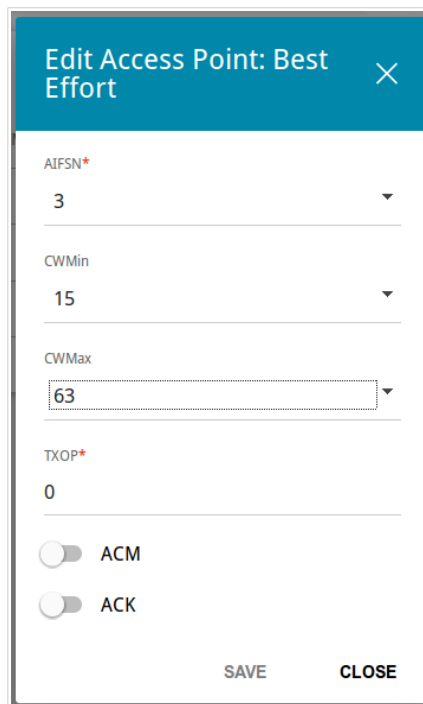


Figure 95. The window for changing parameters of the WMM function.

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.

Parameter	Description
<b>ACM</b>	<i>Admission Control Mandatory.</i> If the switch is moved to the right, the device cannot use the relevant Access Category.
<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.

To disable the WMM function, click the **DISABLE** 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.

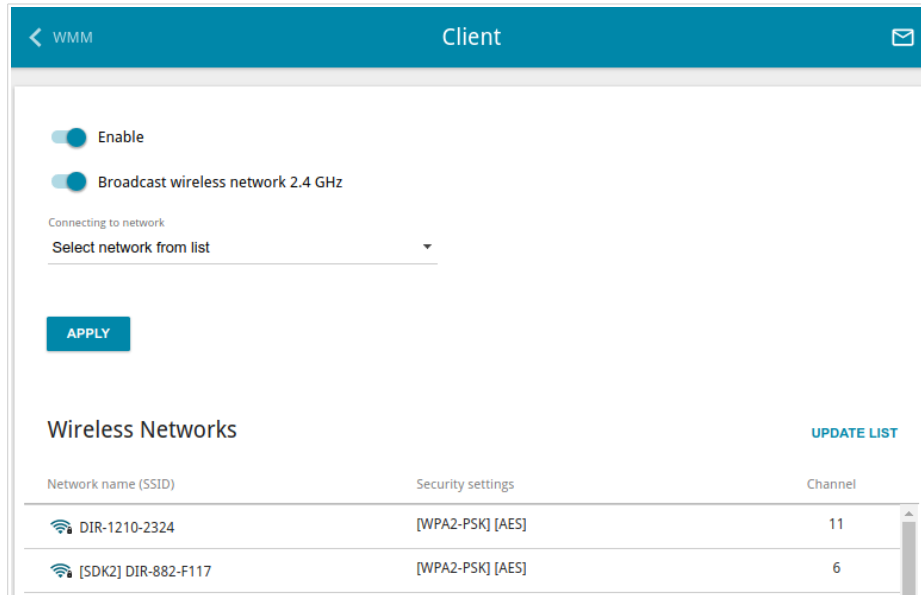


Figure 96. The page for configuring the client mode.

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</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>	<i>For <b>Open</b> authentication type only.</i> 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**, or **WPA-PSK/WPA2-PSK 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> .

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

Parameter	Description
<b>RADIUS server login</b>	The username of the account on the RADIUS server.
<b>RADIUS server password</b>	The password of the account on the RADIUS server.
<b>Encryption type</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> .

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

When connecting to a wireless access point, the wireless channel of DWR-921 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 **WLAN** interface.

## Additional

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

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

The screenshot shows the 'Additional' configuration page for the WLAN. The page has a teal header with 'Configuration' and 'Additional' labels. The settings are organized into two columns:

- Bandwidth:** 20/40MHz (dropdown menu)
- Beacon period (in milliseconds)\*:** 100
- TX power (in percent):** 100
- B/G protection:** Auto (dropdown menu)
- Short GI:** Enable (dropdown menu)
- Autonegotiation 20/40 (Coexistence):** Toggle switch (currently off)
- RTS threshold (in bytes)\*:** 2347
- Frag threshold (in bytes)\*:** 2346
- DTIM period (in beacon frames)\*:** 1
- Station Keep Alive (in seconds)\*:** 0
- Drop multicast:** Toggle switch (currently off)

An 'APPLY' button is located at the bottom left of the configuration area.

Figure 97. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
<b>Bandwidth</b>	The channel bandwidth for 802.11n standard. <b>20MHz:</b> 802.11n clients operate at 20MHz channels. <b>20/40MHz:</b> 802.11n clients operate at 20MHz or 40MHz channels.
<b>Autonegotiation 20/40 (Coexistence)</b>	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).
<b>TX power</b>	The transmit power (in percentage terms) of the router.

Parameter	Description
<b>B/G protection</b>	<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> <p><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).</p> <p><b>Always On:</b> The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</p> <p><b>Always Off:</b> The protection function is always disabled.</p>
<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> <p><b>Enable:</b> the router uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n standard (see the value of the <b>Wireless mode</b> drop-down list on the <b>Wi-Fi / Basic Settings</b> page).</p> <p><b>Disable:</b> the router uses the 800 ns standard guard interval.</p>
<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</b> page.</p>
<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 time period (in beacon frames) between sending a DTIM (a message notifying on broadcast or multicast transmission) and data 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 DWR-921.

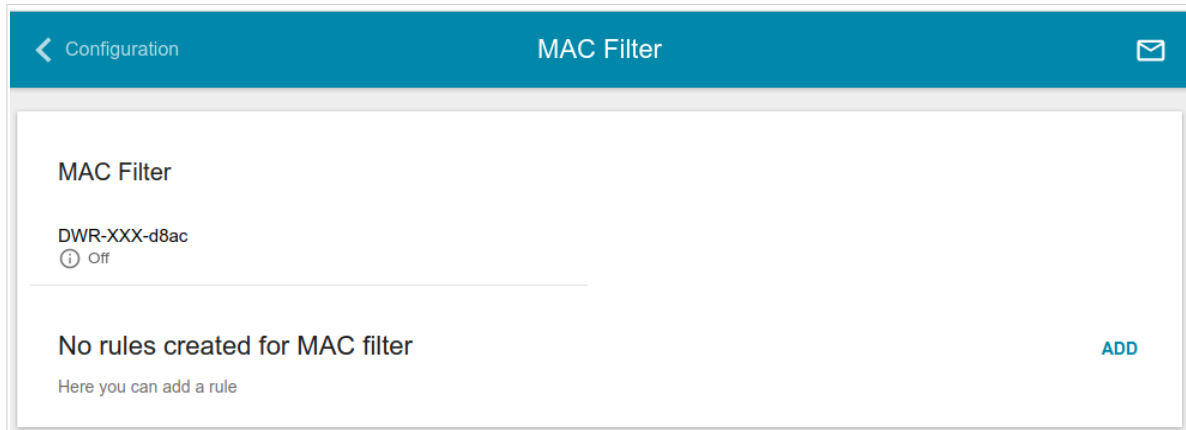


Figure 98. The page for configuring the MAC filter for the wireless network.

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 ( **+** ).

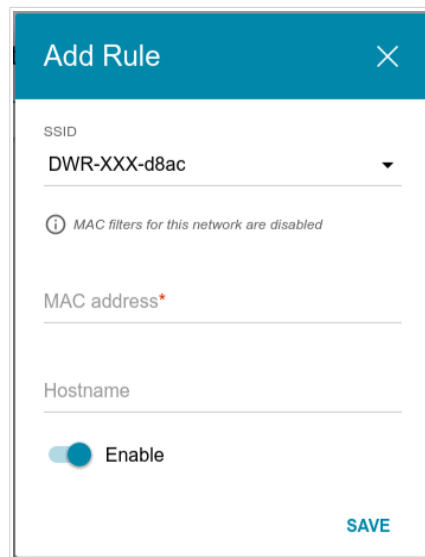



Figure 99. The window for adding a rule for the MAC filter.

You can specify the following parameters:

Parameter	Description
<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. 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, 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.



## LTE Modem

This menu is designed to operate the built-in LTE modem.

If the PIN code check for the SIM card inserted into the built-in modem is not disabled, the relevant notification will be displayed in the top right corner of the page.

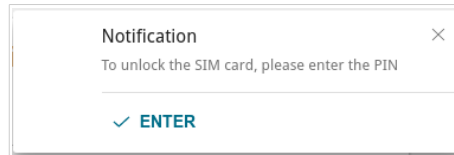


Figure 100. The notification on the PIN code check.

Click the **ENTER** button. When the **LTE Modem / PIN** page opens, enter the PIN code in the **Authorization** section. Click the **Show** icon (👁) to display the entered code. Then click the **APPLY** button.

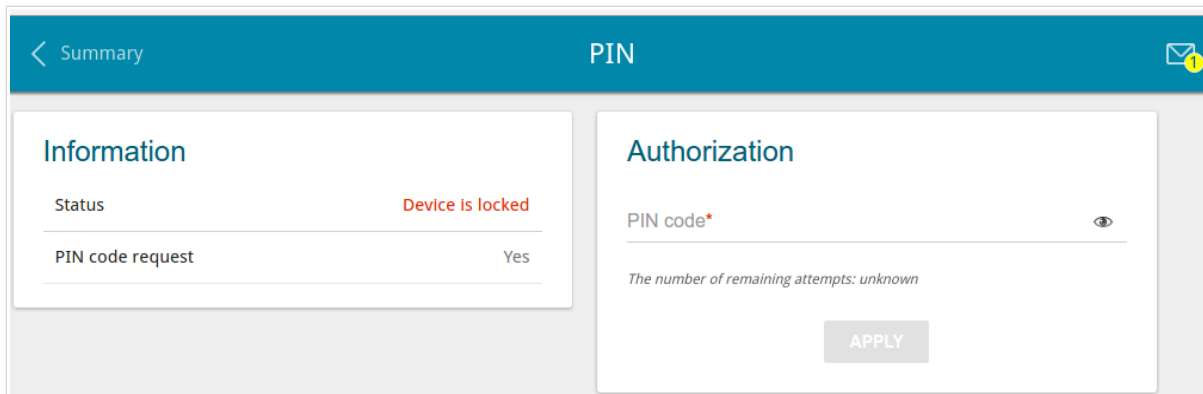


Figure 101. Entering the PIN code.

## Basic Settings

On the **LTE Modem / Basic Settings** page, you can view data on the built-in modem and enable/disable the function for automatic creation of LTE WAN connection.

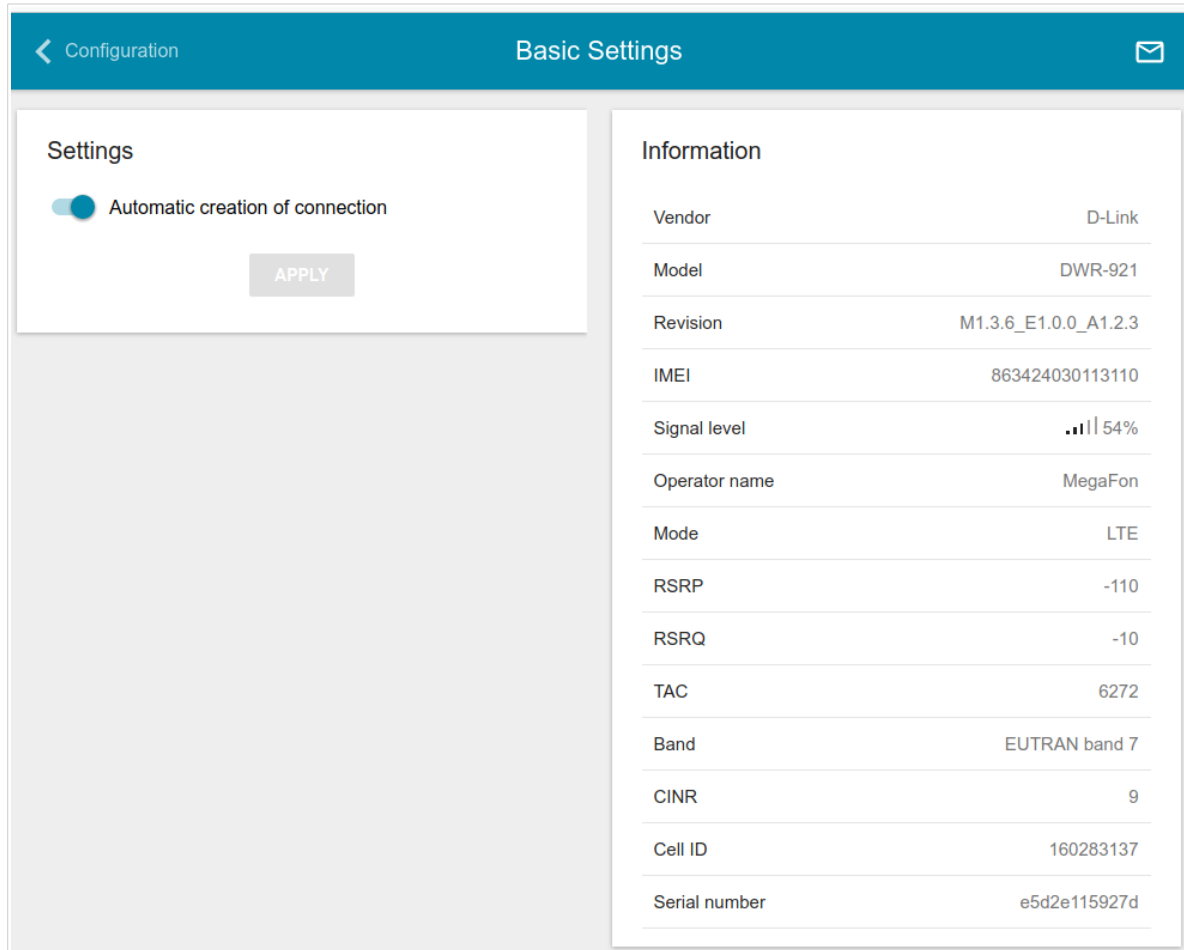


Figure 102. The **LTE Modem / Basic Settings** page.

If the **Automatic creation of connection** switch is moved to the right and the PIN code check for the SIM card inserted into the built-in modem is disabled, then an active WAN connection with the operator's settings will be automatically created when powering on the router. The connection will be displayed on the **Connections Setup / WAN** page.

If you don't want to use this function, move the **Automatic creation of connection** switch to the left and click the **APPLY** button.

The **Information** section displays detailed information on the built-in modem, a type of the network to which the modem is connected, the signal level, and other data.

## PIN

On the **LTE Modem / PIN** page, you can change the PIN code of the SIM card inserted into the built-in modem, disable or enable the check of the PIN code.

The current state of the SIM card inserted into the built-in modem is displayed in the **Status** field. If the PIN code is entered incorrectly or the PIN code is not entered when the PIN code check is enabled, the **Device is locked** value is displayed in the **Status** field. If the PIN code is entered correctly or the PIN check is disabled, the **Device is unlocked** value is displayed in the **Status** field.

If the PIN code check for the SIM card inserted into the built-in modem is not disabled, the **Yes** value is displayed in the **PIN code request** field. If the PIN check is disabled, the **No** value is displayed in the **PIN code request** field.

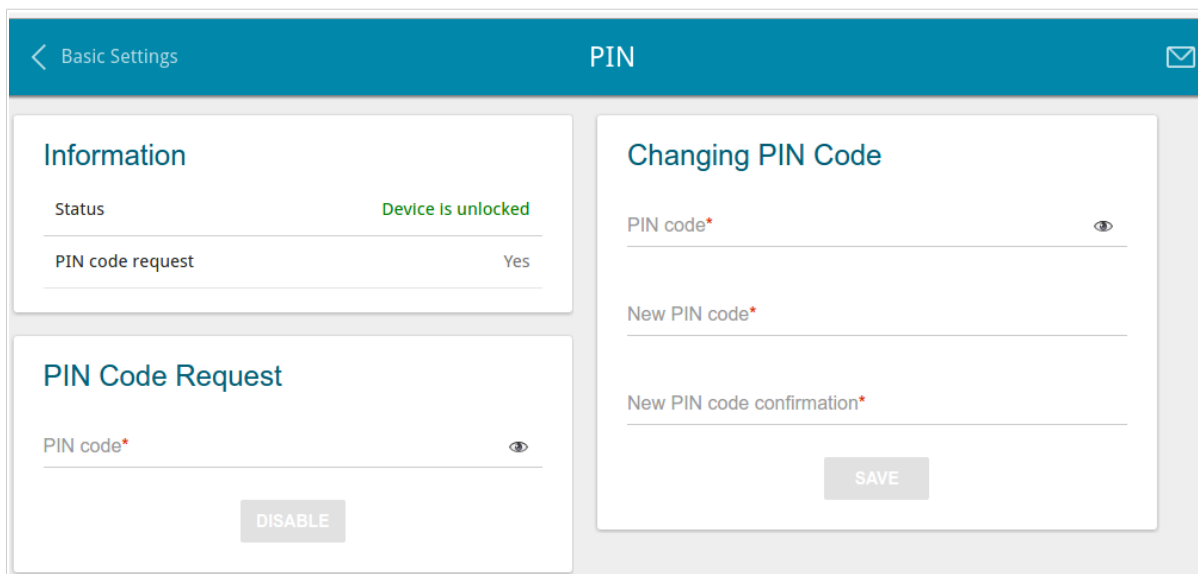


Figure 103. The **LTE Modem / PIN** page.

To disable the PIN code check, in the **PIN Code Request** section, enter the current PIN code in the **PIN code** field and click the **DISABLE** button (the button is displayed if the PIN code check is enabled).

To enable the PIN code check, in the **PIN Code Request** section, enter the PIN code used before disabling the check in the **PIN code** field and click the **ENABLE** button (the button is displayed if the PIN code check is disabled).

To change the PIN code, in the **Changing PIN Code** section, enter the current code in the **PIN code** field, then enter a new code in the **New PIN code** and **New PIN code confirmation** fields and click the **SAVE** button.

If upon one of the operations described above you have entered an incorrect value in the **PIN code** field three times (the number of remaining attempts is displayed on the page), the SIM card inserted into the built-in modem is blocked.

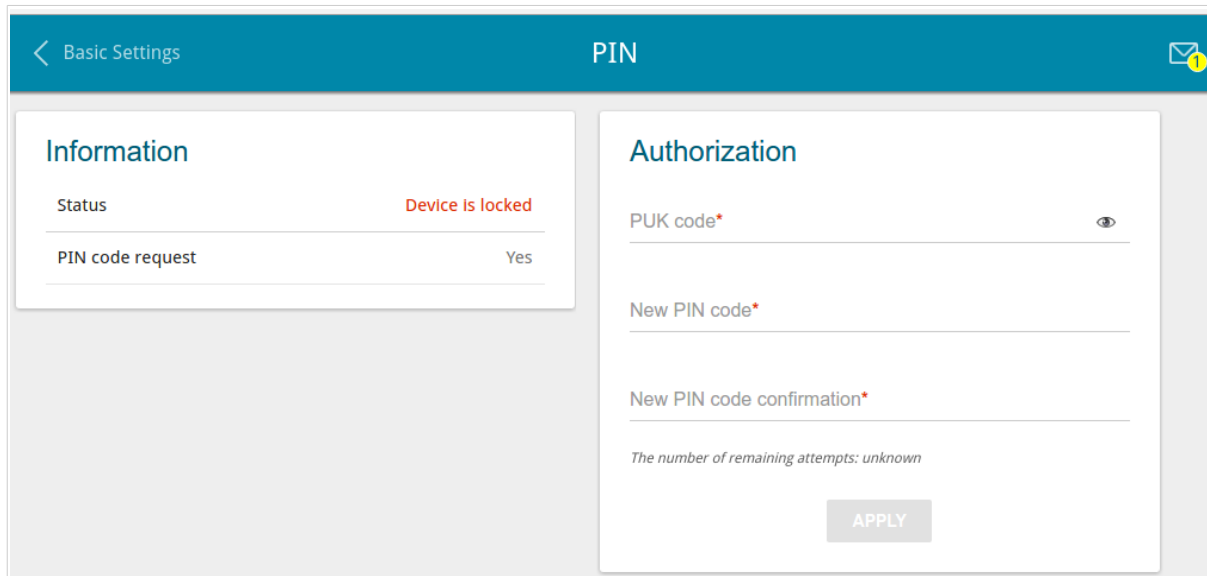


Figure 104. The **LTE Modem / PIN** page. The PUK code request.

For further use of the card, in the **Authorization** section, enter the PUK code in the relevant field, and then specify a new PIN code for your SIM card in the **New PIN code** and **New PIN code confirmation** field. Click the **APPLY** button.

## SMS

When a new text message is received, the relevant notification will be displayed in the top right corner of the page.

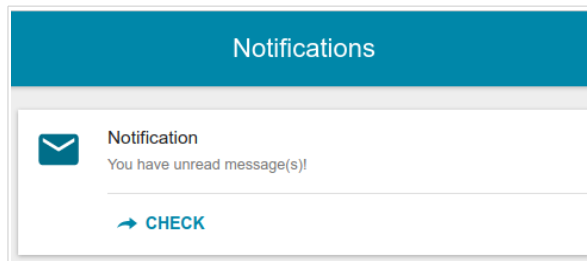


Figure 105. The notification on a new text message.

Click the **CHECK** button. After clicking the button, the **LTE Modem / SMS** page opens.

On the **LTE Modem / SMS** page, you can create and send a text message, view data on a number of messages and the memory state of the SIM card inserted into the built-in modem, and also view the history of sent and received messages stored in the memory of the SIM card.

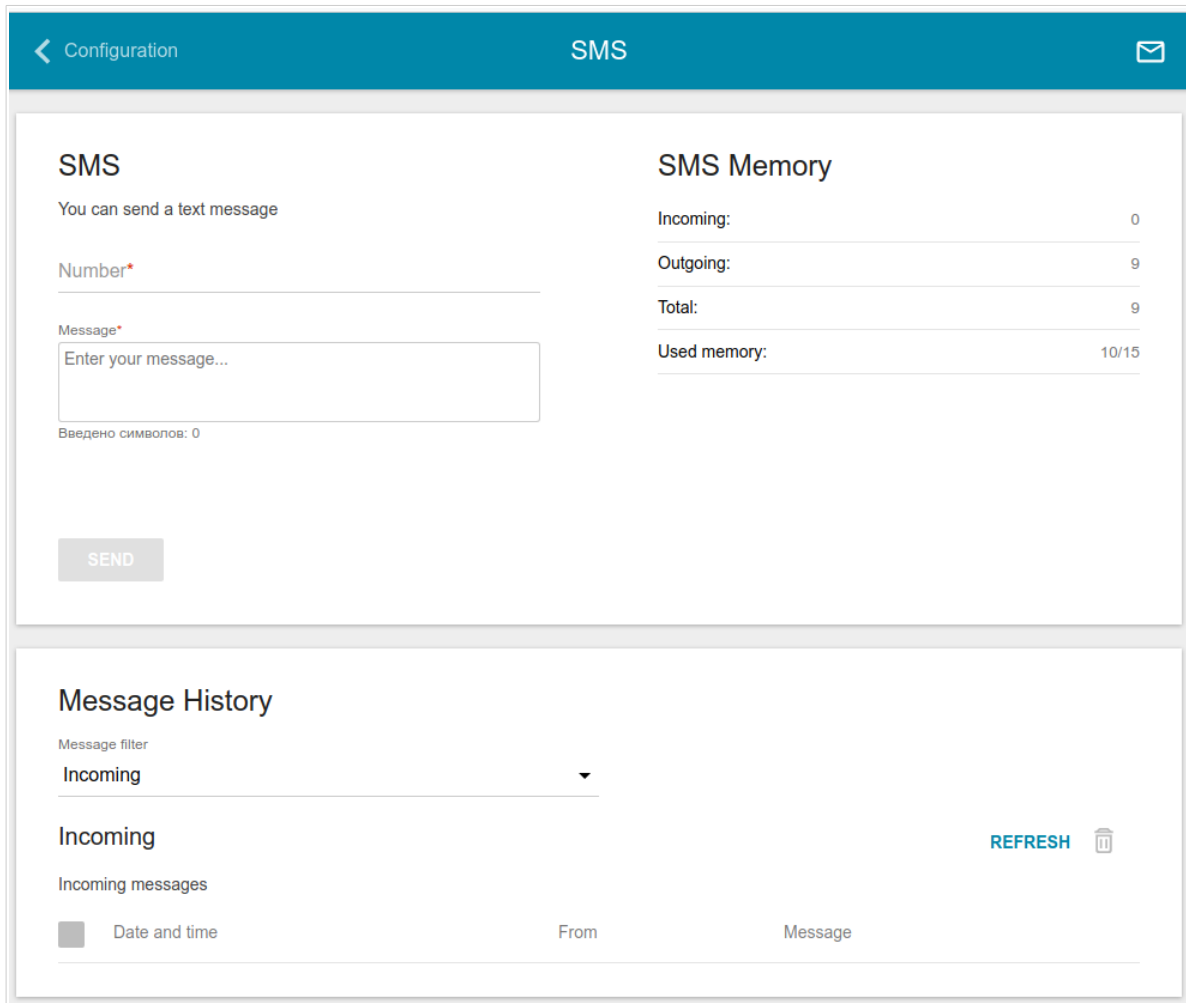


Figure 106. The **LTE Modem / SMS** page.

In the **SMS** section, you can create and send a text message. In the **Number** field, enter the recipient's phone number; in the **Message** field, enter the text of the message. Then click the **SEND** button.

In the **SMS Memory** section, you can view data on the number of messages and the state of the SIM card memory.

In the **Message History** section, you can read outgoing and incoming messages and remove messages from the memory of the SIM card.

To view all outgoing and incoming messages, select the relevant value from the **Message filter** drop-down list.

To view the latest data on sent and received messages, click the **REFRESH** button.

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

## ***Advanced***

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

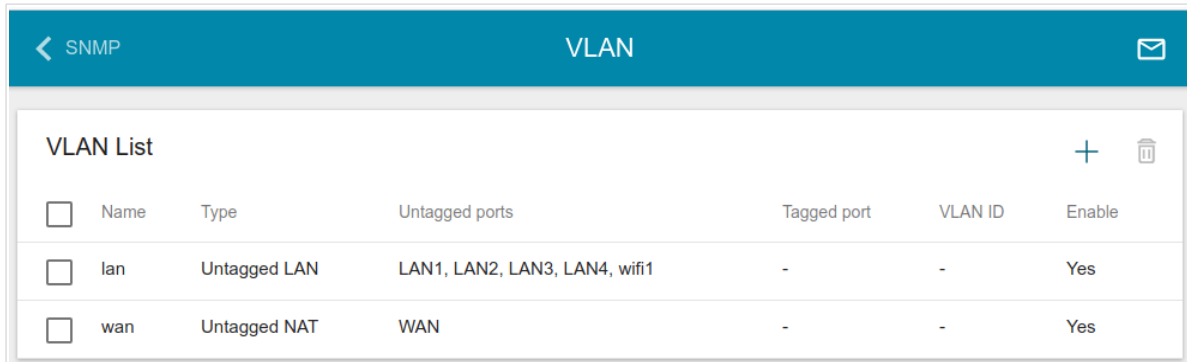
- create groups of ports for VLANs
- allow the router to connect to a private Ethernet line
- enable and configure the SNMP agent of the router
- add name servers
- configure a DDNS service
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the router
- configure notifications on the reason of the Internet connection failure
- define static routes
- configure TR-069 client
- create rules for remote access to the web-based interface
- enable the UPnP IGD protocol
- allow the router to use IGMP
- 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 create and edit groups of ports for virtual networks (VLANs).

By default, 2 groups are created in the router's system:

- **lan**: it includes ports 1-4. You cannot delete this group.
- **wan**: for the WAN interface; it includes the **WAN** port. You can edit or delete this group.

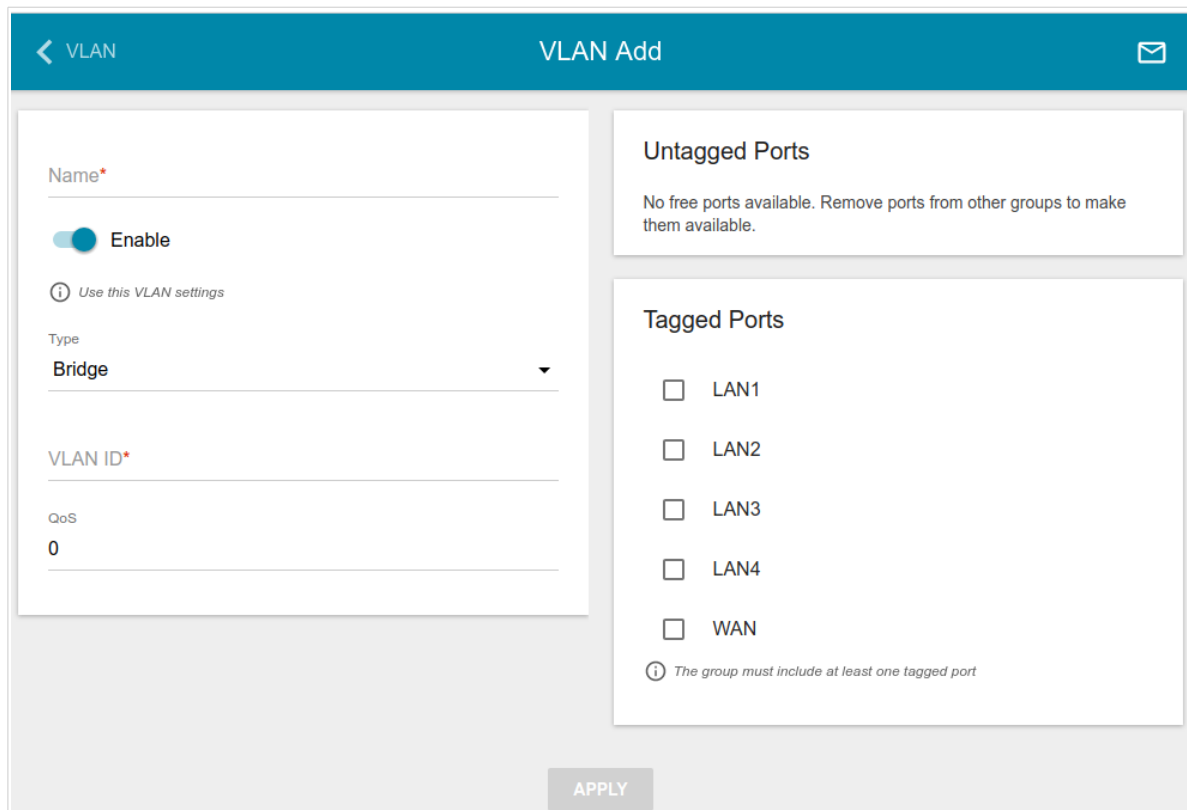


<input type="checkbox"/>	Name	Type	Untagged ports	Tagged port	VLAN ID	Enable
<input type="checkbox"/>	lan	Untagged LAN	LAN1, LAN2, LAN3, LAN4, wifi1	-	-	Yes
<input type="checkbox"/>	wan	Untagged NAT	WAN	-	-	Yes

Figure 107. The **Advanced / VLAN** page.

If you want to create a group including LAN ports of the router, first delete relevant records from the **lan** group on this page. To do this, select the **lan** group. On the opened page, in the **Untagged Ports** section, deselect the checkbox located to the left of the relevant port, and click the **APPLY** button.

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



**VLAN Add**

Name\*

Enable

Use this VLAN settings

Type  
Bridge

VLAN ID\*

QoS  
0

**Untagged Ports**  
No free ports available. Remove ports from other groups to make them available.

**Tagged Ports**

LAN1  
 LAN2  
 LAN3  
 LAN4  
 WAN

The group must include at least one tagged port

APPLY


Figure 108. The page for adding a group of ports for VLAN.

You can specify the following parameters:

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

Click the **APPLY** button.

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

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



## WAN Remapping

On the **Advanced / WAN Remapping** page, you can configure the router to connect to a private Ethernet line.

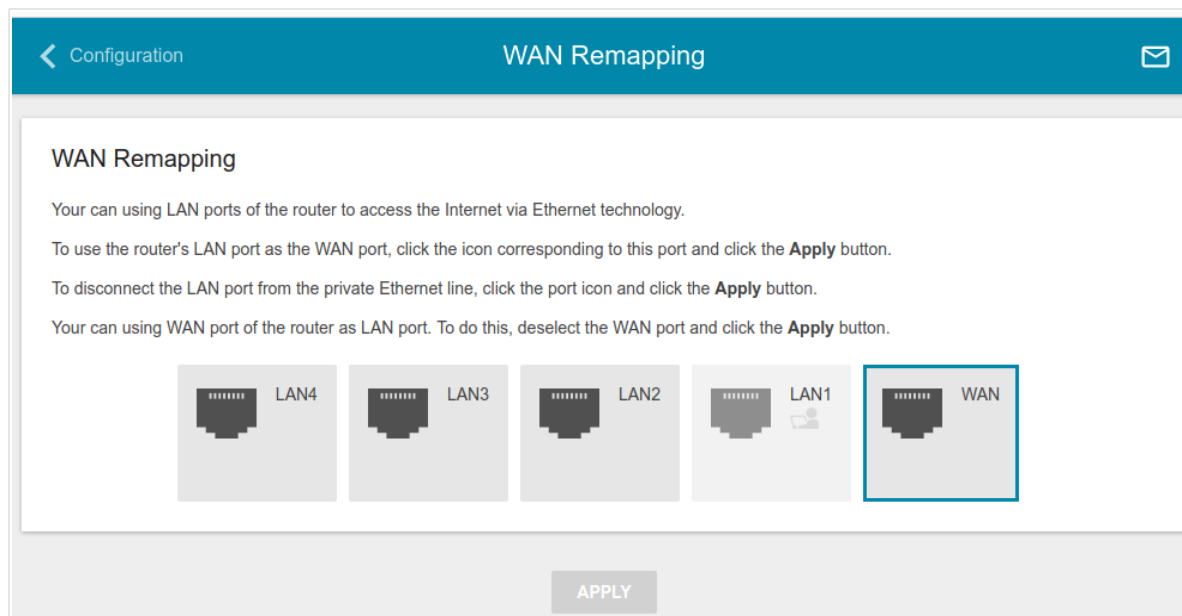


Figure 109. The **Advanced / WAN Remapping** page.

To use one of the router's LAN port as the WAN port, click the icon corresponding to this port and click the **APPLY** button. The port configured as the WAN port is highlighted in teal.

If in the future you need to disconnect the LAN port from the private Ethernet line, click the icon highlighted in teal and click the **APPLY** button.

To use the router's WAN port as a LAN port, click the icon corresponding to this port and click the **APPLY** button. The port configured as a LAN port is not highlighted.

If in the future you need to connect the WAN port to the private Ethernet line, click the icon corresponding to this port and click the **APPLY** button. The WAN port will be highlighted in teal again.

## SNMP

On the **Advanced / SNMP** page, you can enable and configure the SNMP agent of the router.

The SNMP agent is a service which sends data on the state and settings of the device where it is enabled to the SNMP manager (the network management system of your ISP or system administrator).

Figure 110. The **Advanced / SNMP** page.

In order to enable the SNMP agent, move the **SNMP service status** switch to the right. Then specify the needed parameters.

Parameter	Description
<b>Configuration</b>	
<b>Remote subnet</b>	The IP address of the remote subnet where the SNMP manager is located.
<b>Hostname</b>	A name of the router for identification in the SNMP manager.
<b>The contact information for the administrator</b>	Additional information used to contact the administrator of the router.
<b>System location</b>	Additional information used to locate the router.

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

In order to disable the SNMP agent, move the **SNMP service status** switch to the left and click the **APPLY** button.

If the SNMP manager operates over SNMPv2c, create a read-only community which will be used by the SNMP manager to get data on the device. To do this, in the **Communities** section, click the **ADD** button ( **+** ).

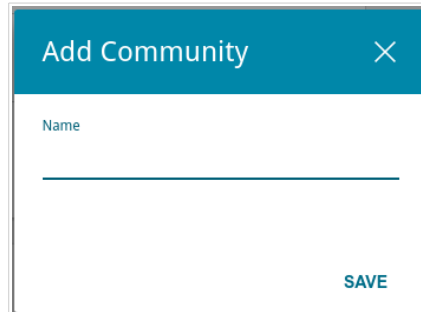



Figure 111. The window for adding a community.

In the opened window, specify the community name in the **Name** field and click the **SAVE** button.

To change a community name, select the relevant line in the table. In the opened window, specify the needed value of the **Name** field and click the **SAVE** button.

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

If the SNMP manager operates over SNMPv3, create a read-only user which will be used by the SNMP manager to get data on the device. To do this, in the **Users** section, click the **ADD** button ( **+** ).

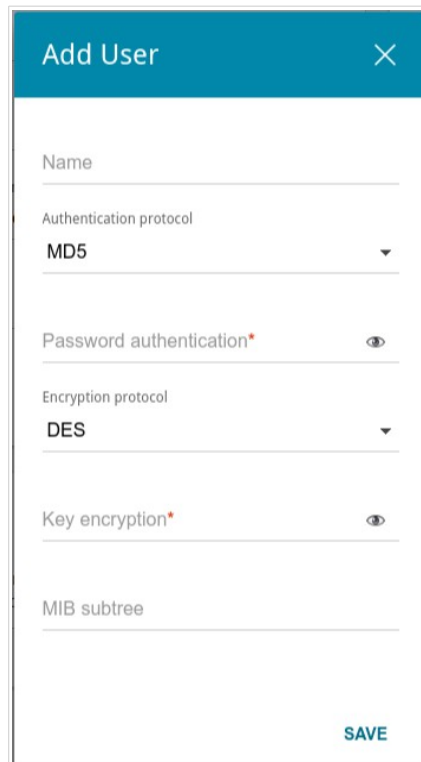



Figure 112. The window for adding a user.

In the opened window, specify the needed parameters:

Parameter	Description
<b>Name</b>	Specify a username for access from the SNMP manager.
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>None</b> value if authentication is not required.
<b>Authentication password</b>	Specify a password for user authentication from the SNMP manager. The field is displayed if the <b>MD5</b> or <b>SHA</b> value is selected from the <b>Authentication protocol</b> drop-down list.
<b>Encryption protocol</b>	Select a required encryption method from the drop-down list or leave the <b>None</b> value if encryption is not required. The list is displayed if the <b>MD5</b> or <b>SHA</b> value is selected from the <b>Authentication protocol</b> drop-down list.
<b>Encryption key</b>	Specify an encryption key for data exchange between the SNMP agent and SNMP manager. The field is displayed if the <b>DES</b> or <b>AES</b> value is selected from the <b>Encryption protocol</b> drop-down list.
<b>MIB subtree</b>	Specify a MIB element which will be available to the SNMP manager.

Click the **SAVE** button.

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

To remove a user, 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.

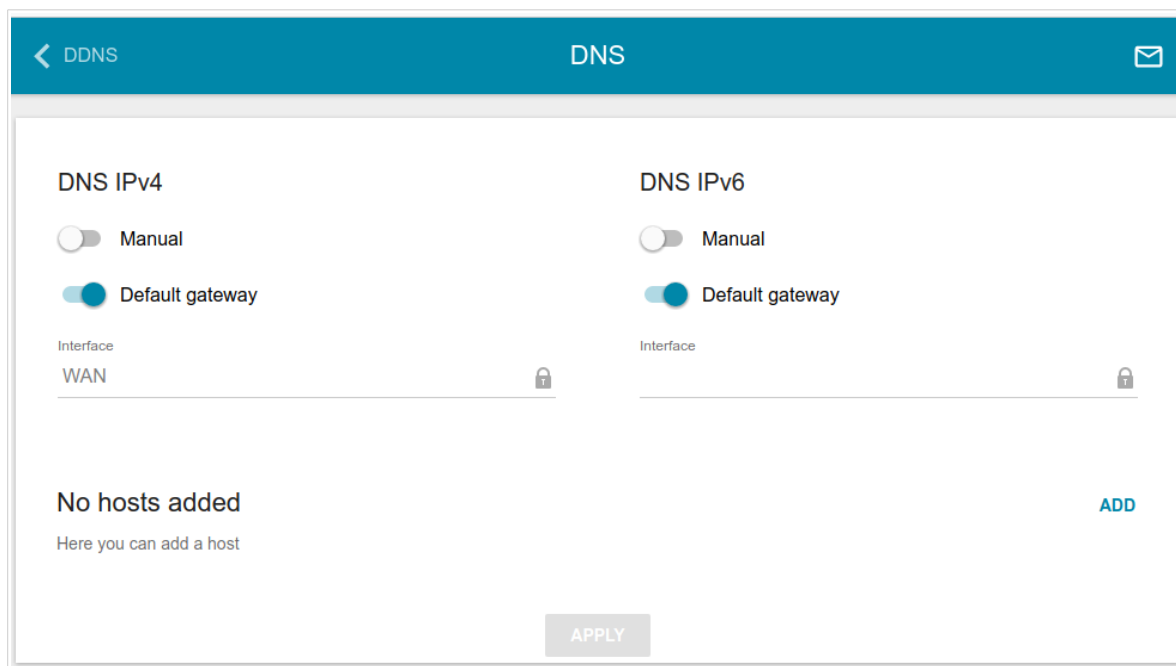


Figure 113. The **Advanced / DNS** page.

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.

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

If you want to configure automatic obtainment of DNS servers addresses, move the **Manual** switch to the left (use the **DNS IPv4** section for IPv4 and the **DNS IPv6** section for IPv6). Then move the **Default gateway** switch to the left and from the **Interface** drop-down list select a WAN connection which will be used to obtain addresses of DNS servers automatically. If you want the router to use the default WAN connection to obtain addresses of DNS servers, move the **Default gateway** switch to the right. Then click the **APPLY** button.

To specify a DNS server manually, move the **Manual** switch to the right (use the **DNS IPv4** section for IPv4 and the **DNS IPv6** section for IPv6). In the **Name Servers IPv4** or **Name Servers IPv6** section, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server. Then click the **APPLY** button.

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

If needed, you can add your own address resource record. To do this, click the **ADD** button (  ).

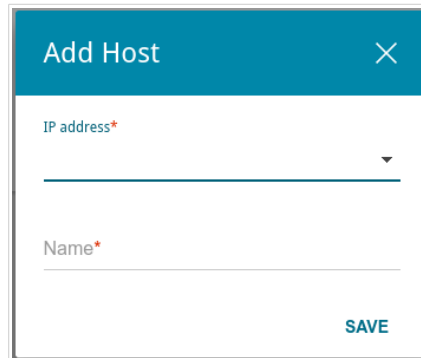



Figure 114. The window for adding a DNS record.

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

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

To remove a record, 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.

## DDNS

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

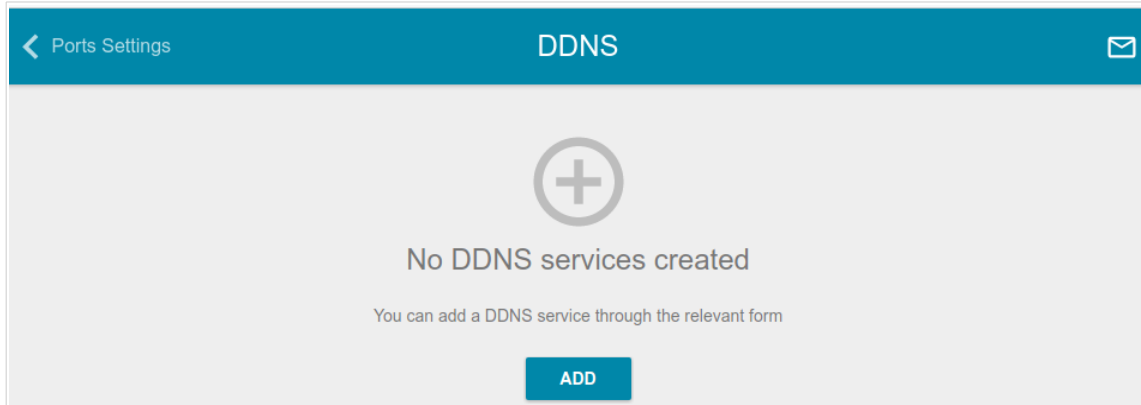


Figure 115. The **Advanced / DDNS** page.

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

 A screenshot of the 'Add DDNS' form. The page has a teal header with a back arrow, 'DDNS', 'Add DDNS', and an envelope icon. The form fields are: 'Hostname\*' (text input), 'Username\*' (text input), 'DDNS service\*' (drop-down menu with 'dns-master.ru' selected), 'Password\*' (password input with a 'Show' icon), and 'Update period (in minutes)\*' (text input). A teal 'SAVE' button is located at the bottom left.


Figure 116. The page for adding a DDNS service.

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

Parameter	Description
<b>Hostname</b>	The full domain name registered at your DDNS provider.
<b>DDNS service</b>	Select a DDNS provider from the drop-down list.
<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>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.

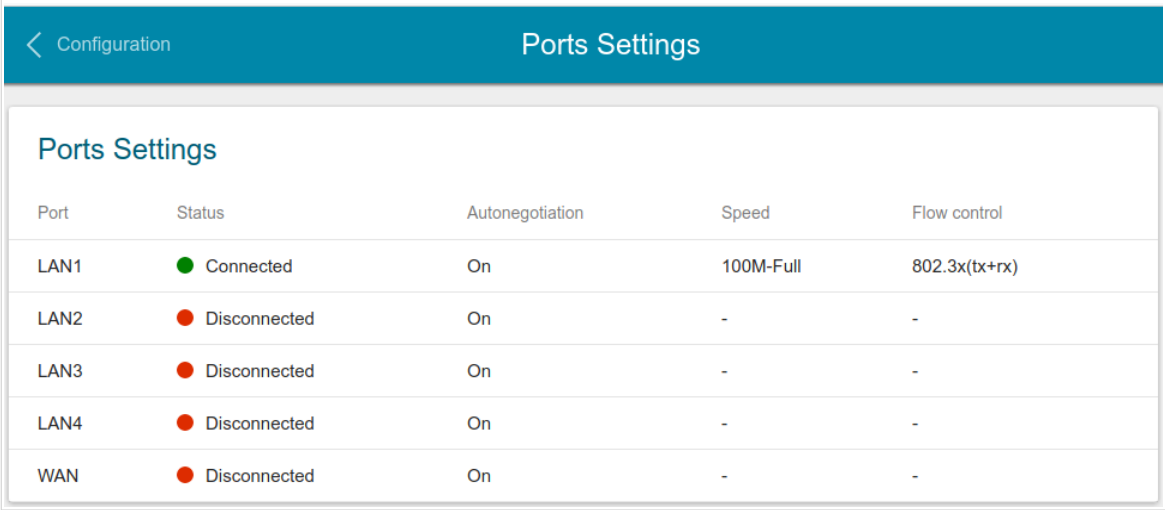
To edit parameters of the existing DDNS service, select the relevant line in the table. On the opened page, change the needed parameters and click the **SAVE** button.

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
LAN1	● Connected	On	100M-Full	802.3x(tx+rx)
LAN2	● Disconnected	On	-	-
LAN3	● Disconnected	On	-	-
LAN4	● Disconnected	On	-	-
WAN	● Disconnected	On	-	-

Figure 117. 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.

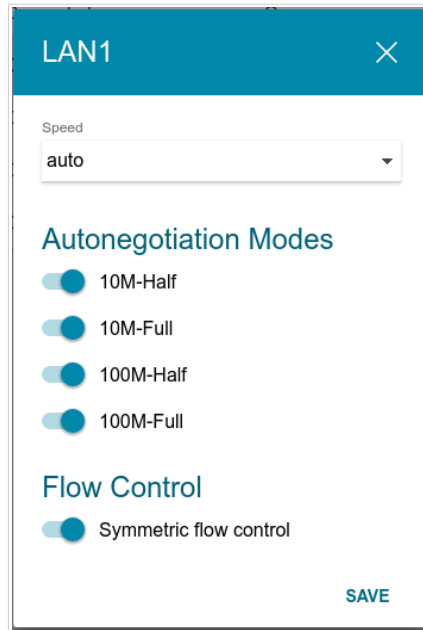


Figure 118. The window for changing the settings of the router's port.

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>
<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.

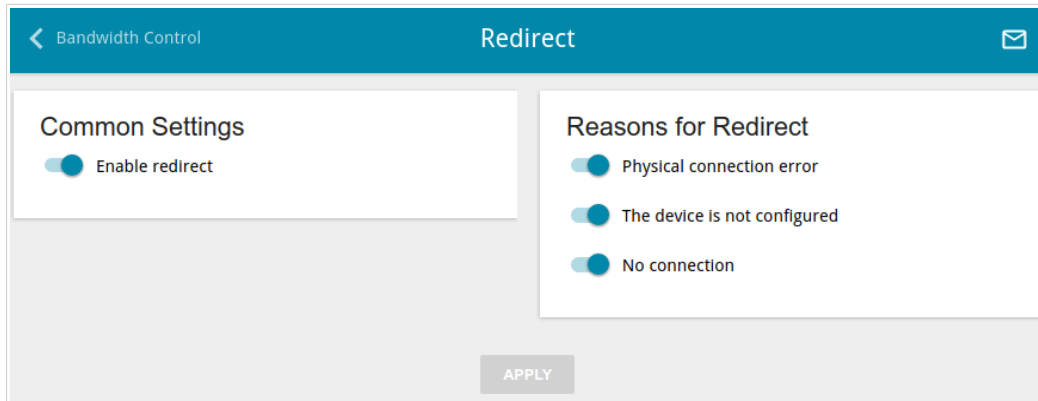


Figure 119. The **Advanced / Redirect** page.

To configure notifications, in the **Common Settings** section, move the **Enable redirect** switch to the right. 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>The device is not configured</b>	Notifications in case when the device works with default settings.
<b>No connection</b>	Notifications in case of problems of the default WAN connection (authorization error, the IPS's server does not respond, etc.).

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

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

## Routing

On the **Advanced / Routing** page, you can add static routes (routes for networks that are not connected directly to the device but are available through the interfaces of the device) into the system.

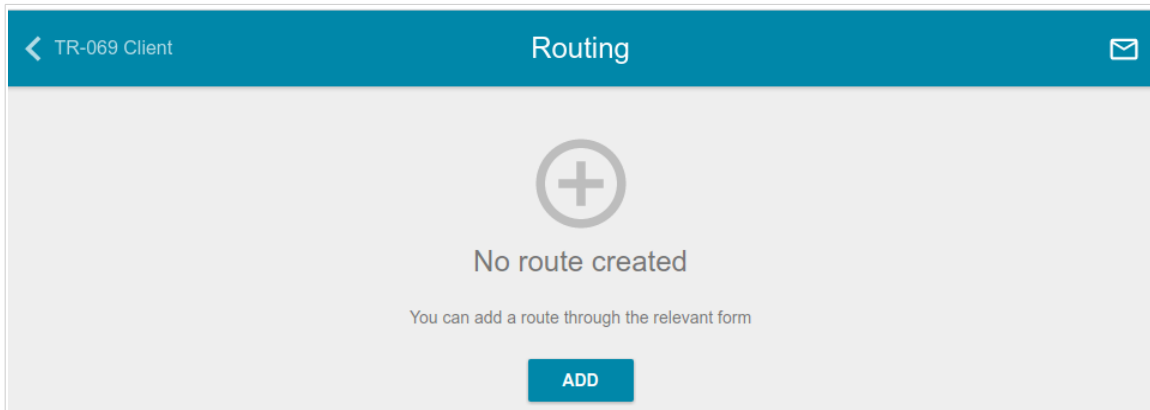


Figure 120. The **Advanced / Routing** page.

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

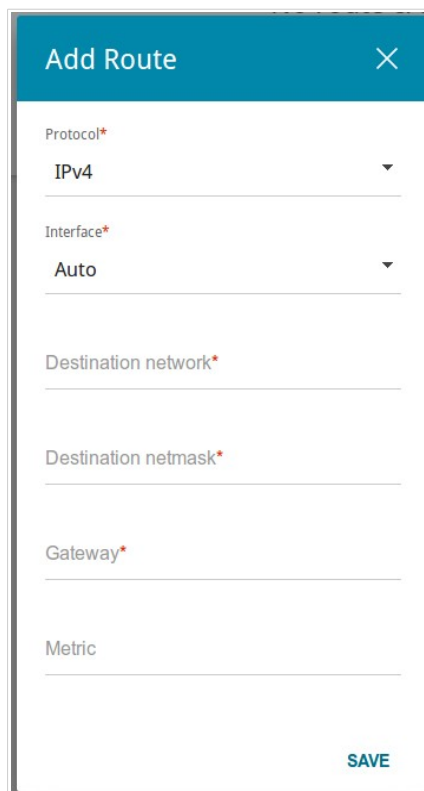
The screenshot shows a modal window titled 'Add Route' with a close button (X) in the top right corner. The form contains several input fields: 'Protocol\*' with a dropdown menu showing 'IPv4'; 'Interface\*' with a dropdown menu showing 'Auto'; 'Destination network\*'; 'Destination netmask\*'; 'Gateway\*'; and 'Metric'. A blue 'SAVE' button is located at the bottom right of the form.


Figure 121. The window for adding a new route.

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

Parameter	Description
<b>Protocol</b>	A protocol that the route will use.
<b>Interface</b>	From the drop-down list, select an interface through which the destination network can be accessed. If you have selected the <b>Auto</b> value, the router itself sets the interface on the basis of data on connected networks.
<b>Destination network</b>	A destination network to which this route is assigned. You can specify an IPv4 or IPv6 address. You can specify an IPv6 address ( <b>2001:db8:1234::1</b> ) or an IPv6 address with a prefix ( <b>2001:db8:1234::/64</b> ).
<b>Destination netmask</b>	<i>For IPv4 protocol only.</i> The destination 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>

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 122. The page for configuring the TR-069 client.

You can specify the following parameters:

Parameter	Description
<b>TR-069 Client</b>	
<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.
<b>Enable TR-069 client</b>	Move the switch to the right to enable the TR-069 client.
<b>Inform Settings</b>	
<b>Enable</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.

Parameter	Description
<b>Auto Configuration Server Settings</b>	
<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.
<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.
<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.



## 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.

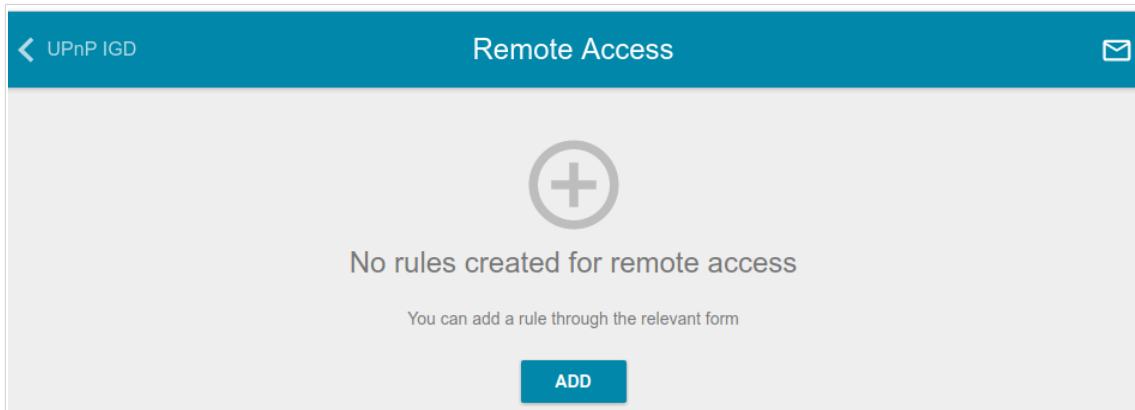


Figure 123. The **Advanced / Remote Access** page.

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

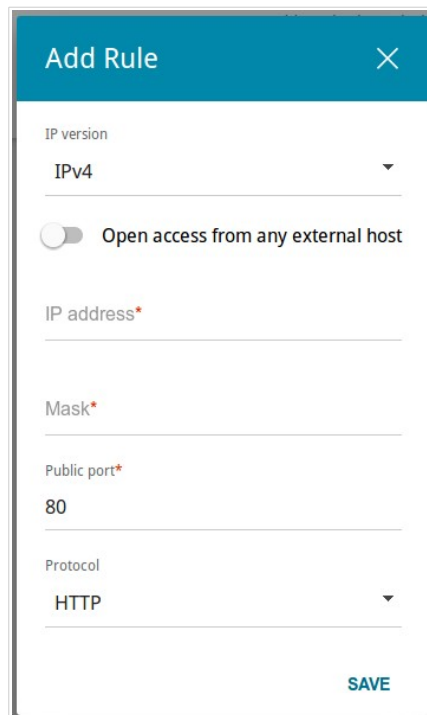


Figure 124. The window for adding a rule for remote management.


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

Parameter	Description
<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.

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

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

## 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.

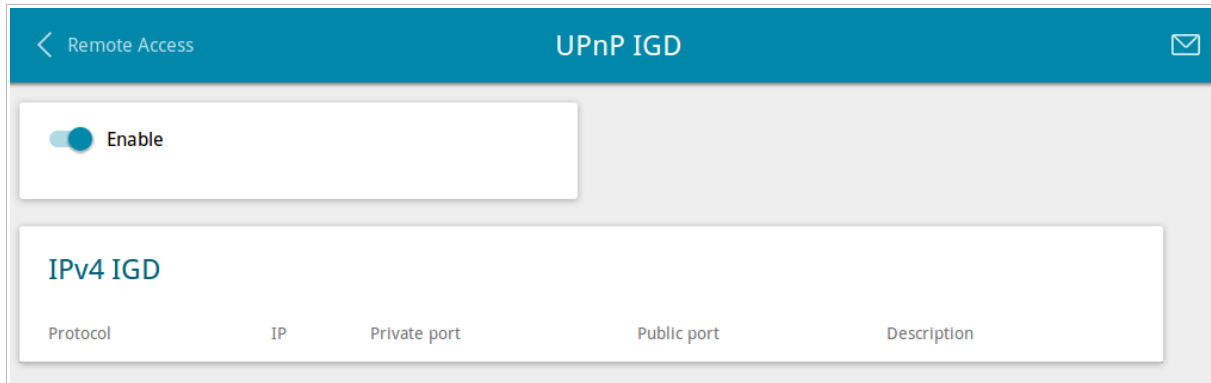


Figure 125. The **Advanced / UPnP IGD** page.

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 router's parameters configured automatically are displayed on the page:

Parameter	Description
<b>Protocol</b>	A protocol for network packet transmission.
<b>IP</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.

## IGMP

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

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

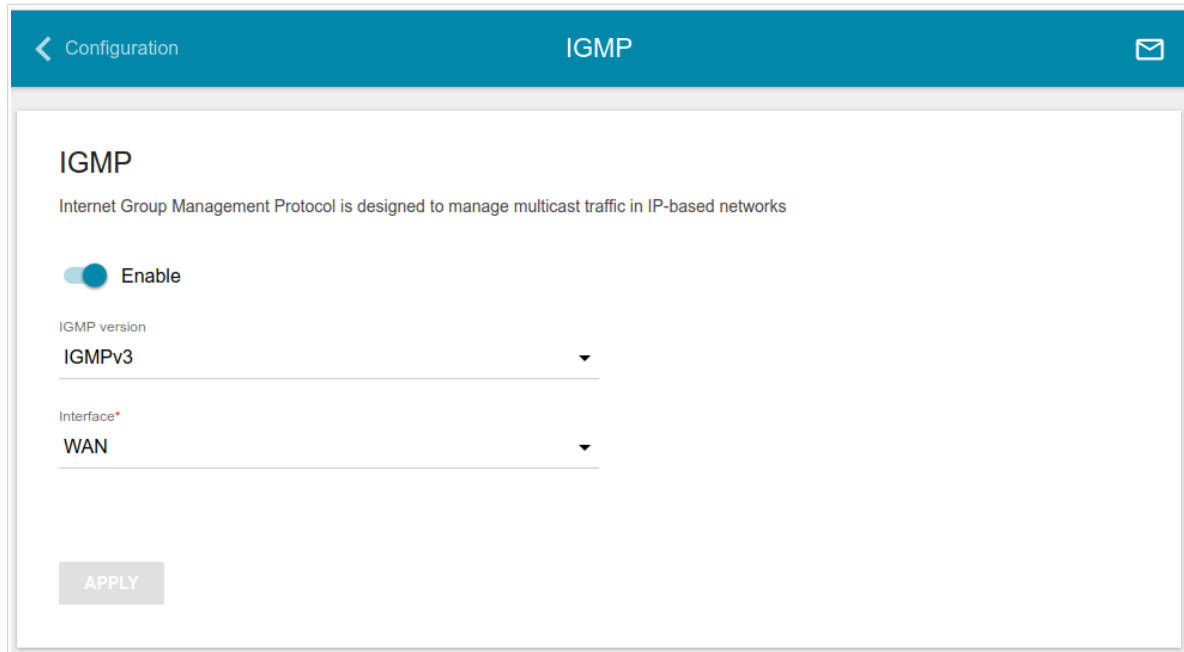


Figure 126. The **Advanced / IGMP** page.

The following elements are available on the page:

Parameter	Description
<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).

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.

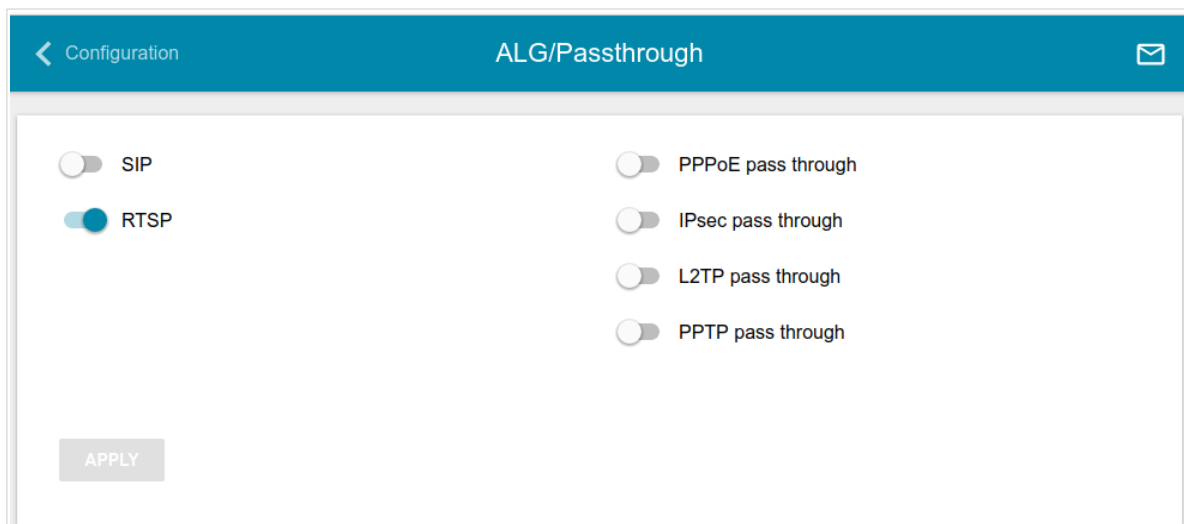


Figure 127. The **Advanced / ALG/Passthrough** page.

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.

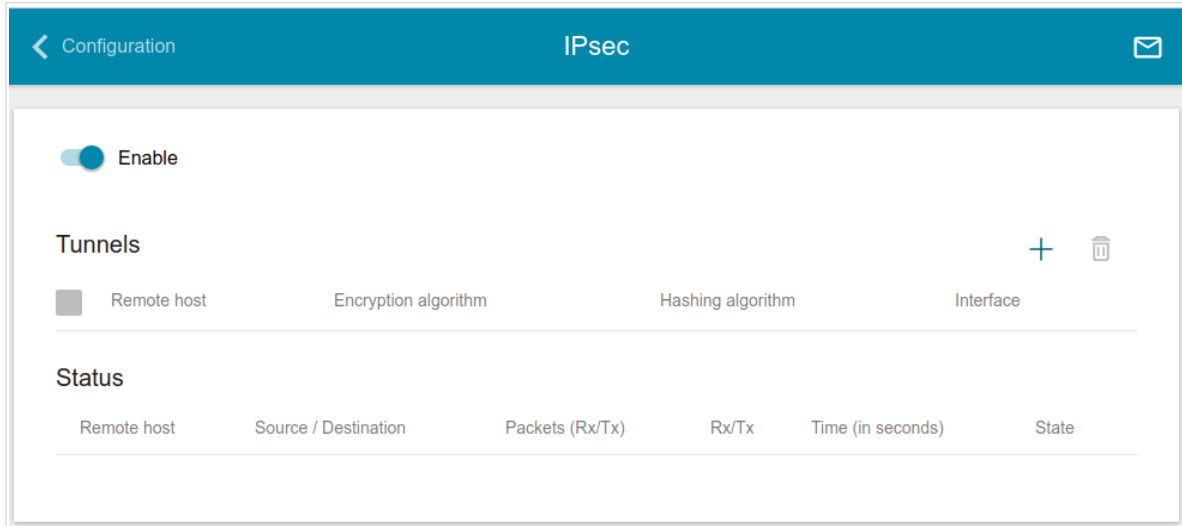



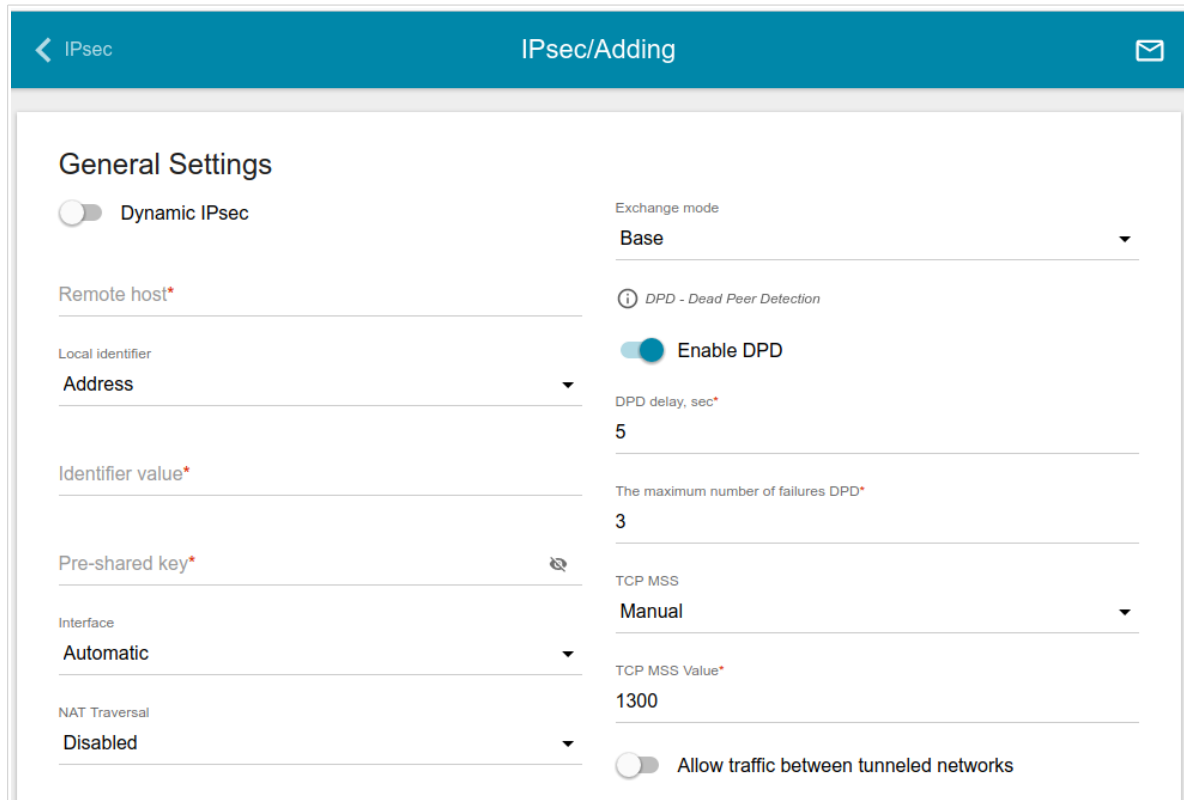
Figure 128. The **Advanced / IPsec** page.

To allow IPsec tunnels, move the **Enable** switch to the right. Upon that the **Tunnels** and **Status** sections are displayed on the page.

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

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 parameters:

- Dynamic IPsec:** A toggle switch currently turned off.
- Remote host\*:** A text input field.
- Local identifier:** A dropdown menu with 'Address' selected.
- Identifier value\*:** A text input field.
- Pre-shared key\*:** A text input field with a copy icon.
- Interface:** A dropdown menu with 'Automatic' selected.
- NAT Traversal:** A dropdown menu with 'Disabled' selected.
- Exchange mode:** A dropdown menu with 'Base' selected.
- DPD - Dead Peer Detection:** A section with an information icon, containing:
  - Enable DPD:** A toggle switch currently turned on.
  - DPD delay, sec\*:** A text input field with the value '5'.
  - The maximum number of failures DPD\*:** A text input field with the value '3'.
- TCP MSS:** A dropdown menu with 'Manual' selected.
- TCP MSS Value\*:** A text input field with the value '1300'.
- Allow traffic between tunneled networks:** A toggle switch currently turned off.

Figure 129. The page for adding an IPsec tunnel. The **General Settings** section.

You can specify the following parameters:

Parameter	Description
<b>General Settings</b>	
<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 tunnel only. Connection requests via this tunnel can be sent by a remote host only.
<b>Remote host</b>	A remote subnet VPN gateway IP address. The field is available, if the <b>Dynamic IPsec</b> switch is moved to the left.
<b>Local identifier</b>	Select an identification method for the local host (router) from the drop-down list: <b>Address:</b> The local host is identified by its IP address. <b>FQDN:</b> The local host is identified by its domain name. The value is unavailable, if the <b>Main</b> value is selected from the <b>Exchange mode</b> list.



Parameter	Description
<b>Identifier value</b>	Specify the local host identifier.
<b>Pre-shared key</b>	A key for mutual authentication of the parties.
<b>Interface</b>	Select a WAN connection through which the tunnel will pass. When the <b>Automatic</b> value is selected, the router uses the default WAN connection.
<b>NAT Traversal</b>	<p>The NAT Traversal function allows VPN traffic to pass through the NAT-enabled router.</p> <p>Select the <b>Disabled</b> value to disable the function.</p> <p>Select the <b>Enabled</b> value to enable the function if it is supported by a remote host.</p> <p>Select the <b>Force</b> value to make the function be always on, even if it is not supported by a remote host.</p>
<b>Exchange mode</b>	<p>Select the mode of negotiation from the drop-down list:</p> <p><b>Main:</b> The mode provides the most secure communication between the parties in the course of negotiation of the authentication procedures.</p> <p><b>Base:</b> The draft negotiation mode with preliminary authentication of a host.</p> <p><b>Aggressive:</b> The mode provides faster operation as it skips several stages of negotiation of the authentication procedures.</p>
<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 a 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 to the left, the <b>DPD delay</b> and <b>The maximum number of failures DPD</b> fields are not available for editing.
<b>DPD delay</b>	A time period (in seconds) between attempts to check the status of a remote host. By default, the value <b>5</b> is specified.
<b>The maximum number of failures DPD</b>	A number of DPD messages that were sent to check the status of a remote host and left unanswered. By default, the value <b>3</b> is specified. If a remote host does not answer the specified number of messages, the router breaks down the tunnel connection, removes the encryption keys, and tries to activate the connection.


Parameter	Description
<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 a remote host to the router.</p> <p>If the <b>Manual</b> value is selected, you can specify the parameter in the <b>TCP MSS Value</b> field.</p> <p>If the <b>Path MTU discovery</b> value is selected, the parameter will be configured automatically.</p>
<b>TCP MSS Value</b>	The maximum size (in bytes) of a non-fragmented packet. The field is available for editing when the <b>Manual</b> value is selected from the <b>TCP MSS</b> drop-down list.
<b>Allow traffic between tunneled networks</b>	Move the switch to the right to allow data exchange between subnets with which IPsec tunnels have been created.

The First Phase	The Second Phase
First phase encryption algorithm <b>DES</b>	Second phase encryption algorithm <b>DES</b>
Hashing algorithm <b>MD5</b>	Authentication algorithm <b>HMAC-MD5</b>
First phase DHgroup type <b>modp768</b>	<input checked="" type="checkbox"/> <b>Enable PFS</b>
IKE-SA lifetime* <b>28800</b>	Second phase PFSgroup type <b>modp768</b>
	IPsec-SA lifetime* <b>3600</b>

Figure 130. 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 encryption algorithm from the drop-down list.
<b>Hashing algorithm</b>	Select hashing algorithm from the drop-down list.
<b>First phase DHgroup type</b>	A Diffie-Hellman key group for Phase 1. 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 exceed the value specified in the <b>IPsec-SA lifetime</b> field. Specify <b>0</b> if you don't want to limit the lifetime of the keys.
<b>The Second Phase</b>	
<b>Second phase encryption algorithm</b>	Select encryption algorithm from the drop-down list.
<b>Authentication algorithm</b>	Select authentication algorithm 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 Phase 2. This option increases the security level of data transfer.
<b>Second phase PFSgroup type</b>	A Diffie-Hellman key group for Phase 2. Select a value from the drop-down list. The field is available, if the <b>Enable PFS</b> switch is moved to the right.

Parameter	Description
<b>IPsec-SA lifetime</b>	The lifetime of IPsec-SA keys in seconds. After the specified period it is required to renegotiate the keys. Specify <b>0</b> if you don't want to limit the lifetime of the keys.

If you need to specify IP addresses of local and remote subnets for creating a tunnel, click the **ADD** button (  ) in the **Tunneled Networks** section.

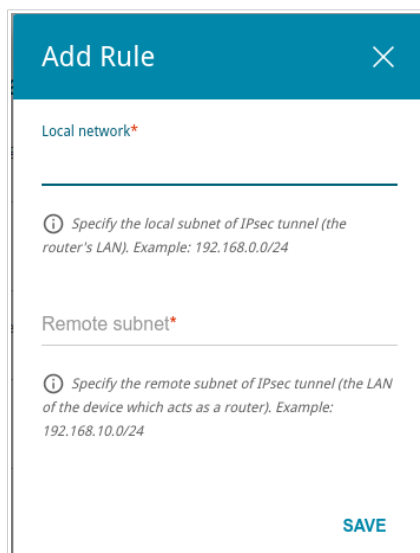



Figure 131. The page for adding an IPsec tunnel. The window for adding a tunneled network.

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.

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 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, move the **Enable** switch to the left.

## 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.

## IP Filter

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



Figure 132. The **Firewall / IP Filter** page.

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

Figure 133. 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.
<b>Name</b>	A name for the rule for easier identification. You can specify any name.
<b>Action</b>	Select an action for the rule. <b>Allow:</b> Allows packet transmission in accordance with the criteria specified by the rule. <b>Deny:</b> Denies packet transmission in accordance with the criteria specified by the rule.

Parameter	Description
<b>Protocol</b>	A protocol for network packet transmission. Select a value from the drop-down list.
<b>IP version</b>	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
<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>	The source host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the <b>End IPv4 address / End IPv6 address</b> field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
<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>	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the <b>End IPv4 address / End IPv6 address</b> field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
<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.

Parameter	Description
<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 edit a rule for IP filtering, select the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

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



## 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.

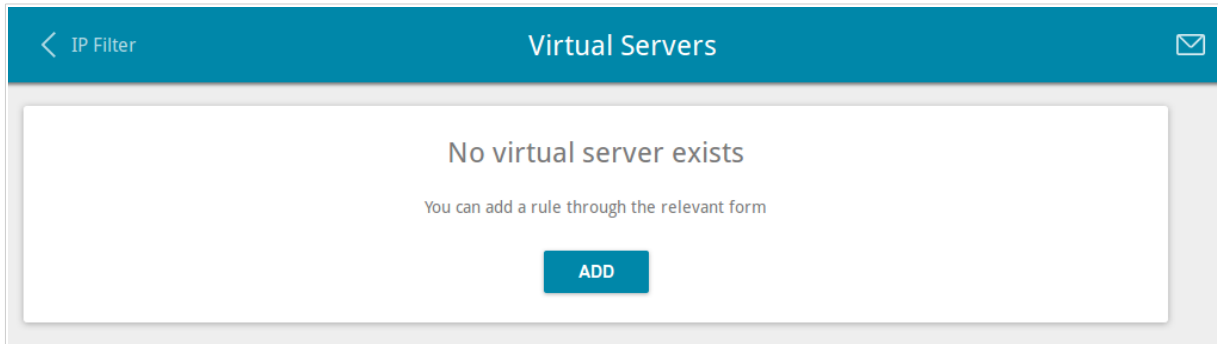


Figure 134. The **Firewall / Virtual Servers** page.

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

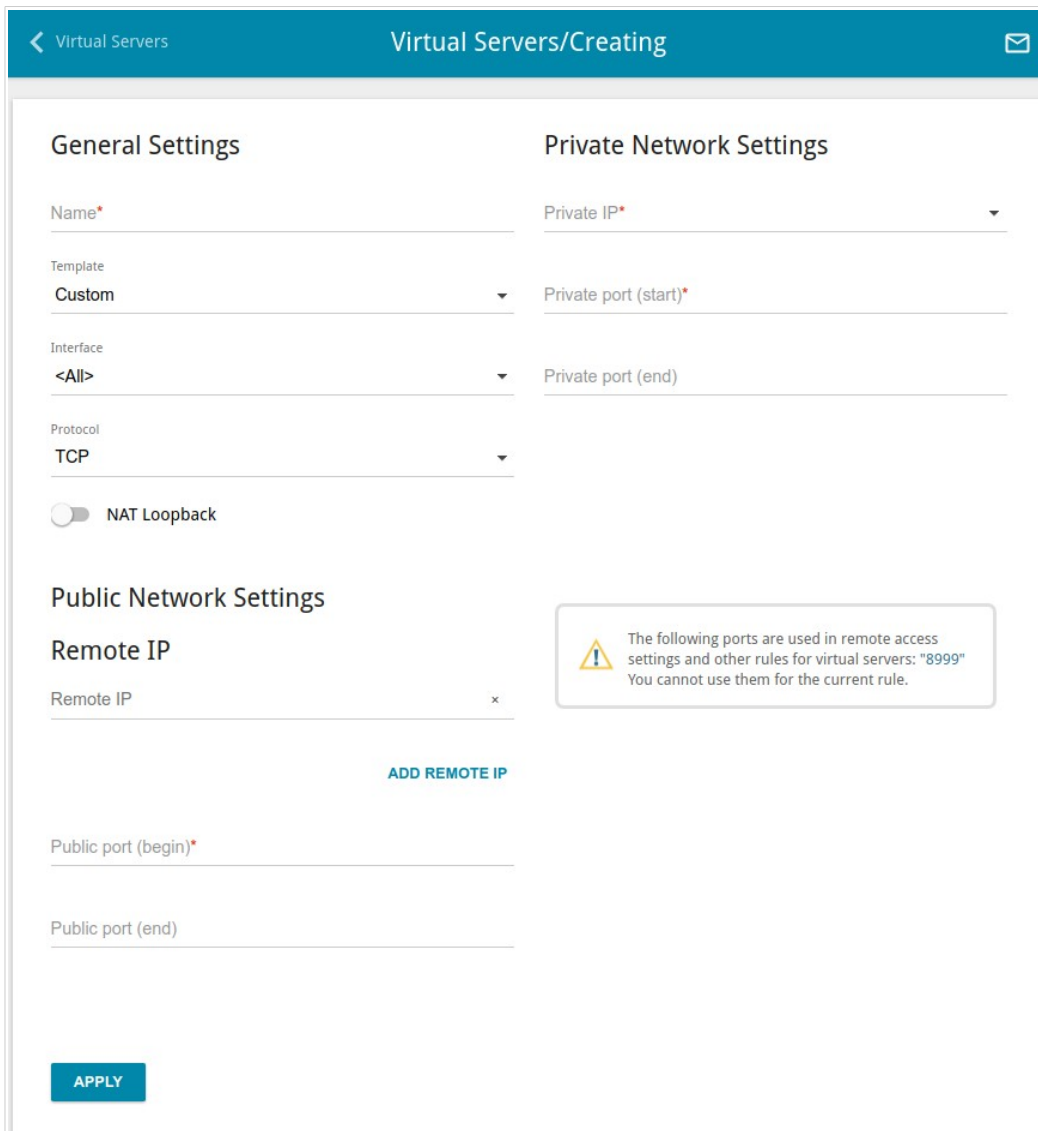



Figure 135. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
<b>General Settings</b>	
<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 (begin)/ Public port (end)</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. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the <b>Public port (begin)</b> field and leave the <b>Public port (end)</b> field blank.
<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 (start)/ Private port (end)</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> . Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the <b>Private port (start)</b> field and leave the <b>Private port (end)</b> field blank.

Click the **APPLY** button.

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

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

## 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.

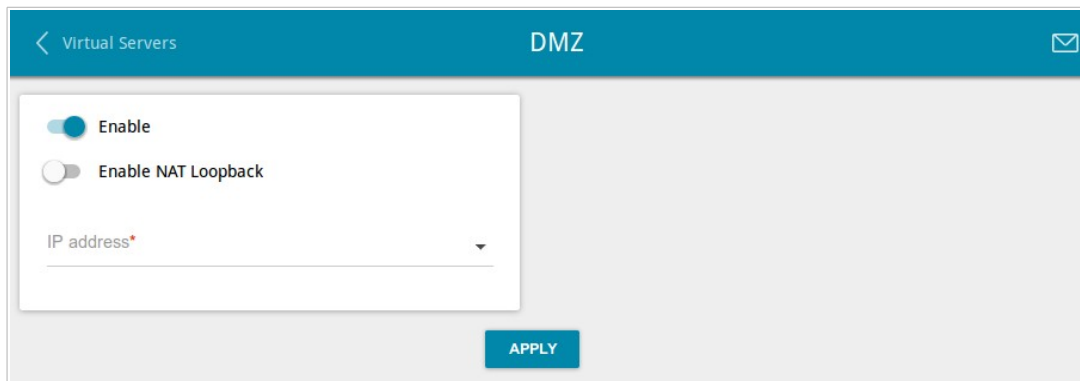


Figure 136. The **Firewall / DMZ** page.

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 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.

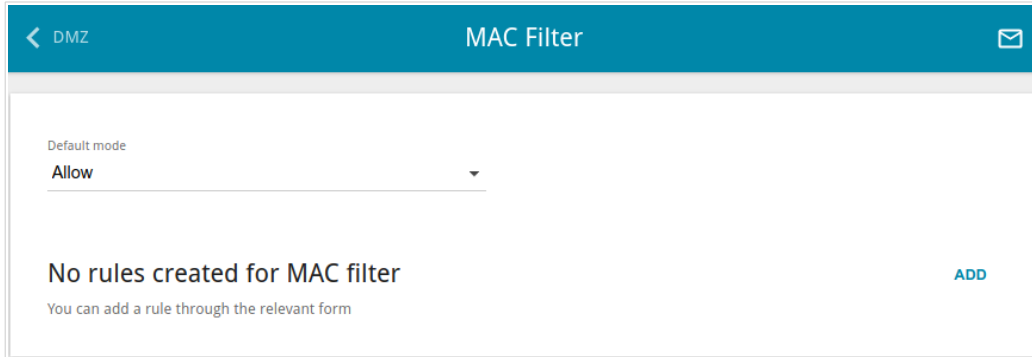


Figure 137. The **Firewall / MAC Filter** page.

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 ( **+** ).

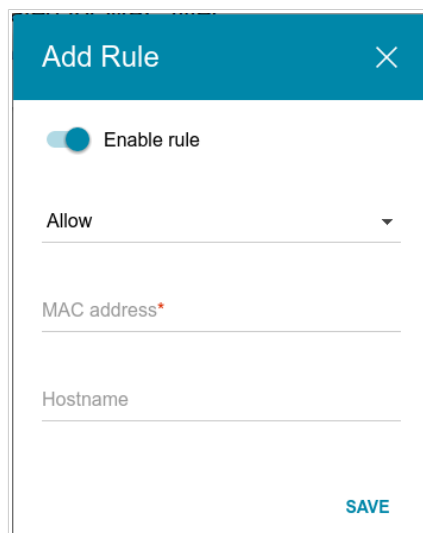



Figure 138. The window for adding a rule for the MAC filter.

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. <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. <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.
<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>Hostname</b>	The name of the device for easier identification. You can specify any name.

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

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

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

## URL Filter

On the **Firewall / URL Filter** page, you can specify restrictions on access to certain web sites.

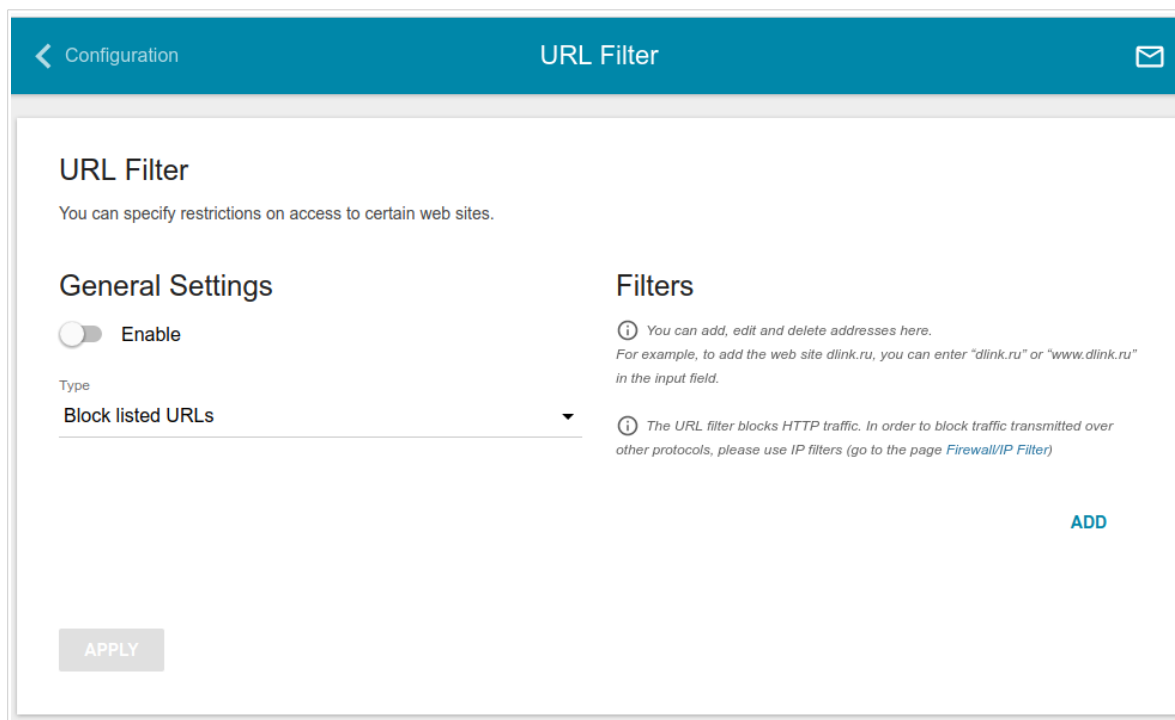


Figure 139. The **Firewall / URL Filter** page.

To enable the URL filter, in the **General Settings** section, move the **Enable** switch to the right, then select the needed mode from the **Type** drop-down list:

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

Click the **APPLY** button.

To specify URL addresses to which the selected filtering mode will be applied, in the **Filters** section, click the **ADD** button and enter a relevant address in the displayed line. Then click the **APPLY** button.

To remove an address from the list of URL addresses, click the **Delete** icon (✕) in the line of the relevant URL address. Then click the **APPLY** 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
- 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
- configure automatic synchronization of the system time or manually configure the date and time for the router.



## 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, 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.

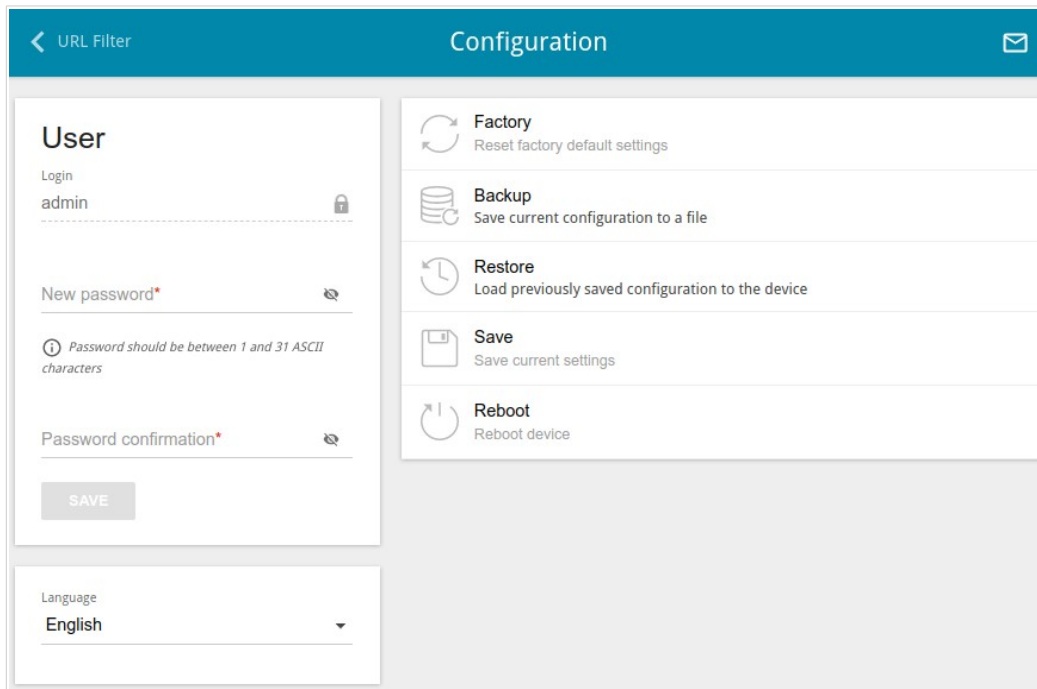


Figure 140. The **System / Configuration** page.

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>7</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>7</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>Front Panel</i> section, page 10).
<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.

## 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.

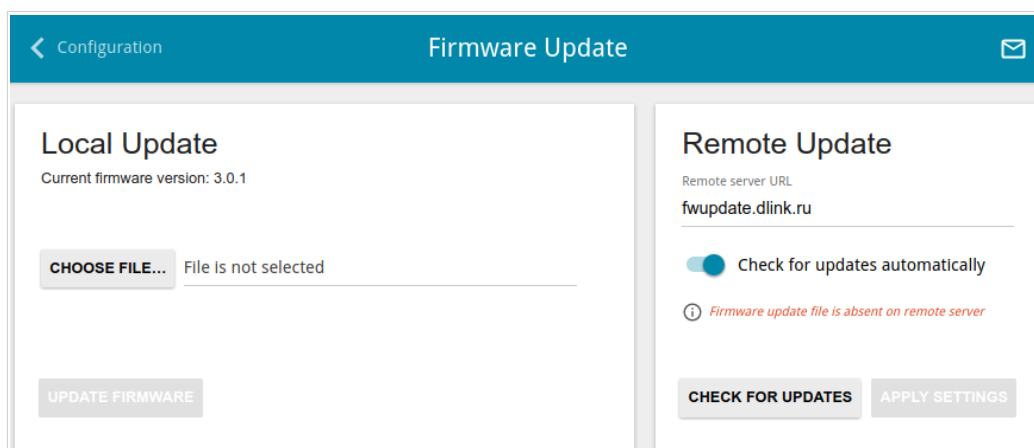


Figure 141. The **System / Firmware Update** page.

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

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

To enable the automatic check for firmware updates, in the **Remote Update** section, move the **Check for updates automatically** switch to the right and click the **APPLY SETTINGS** button. By default, in the **Remote server URL** field, the D-Link update server address (**fwupdate.dlink.ru**) is specified.

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. Click the **UPDATE FIRMWARE** button.
4. Wait until the router is rebooted (about one and a half or two minutes).
5. Log into the web-based interface using the login (**admin**) and the current password.

If after updating the firmware the router doesn't work correctly, please restore the factory default settings. To do this, click the **Factory** button on the **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.

## Log

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

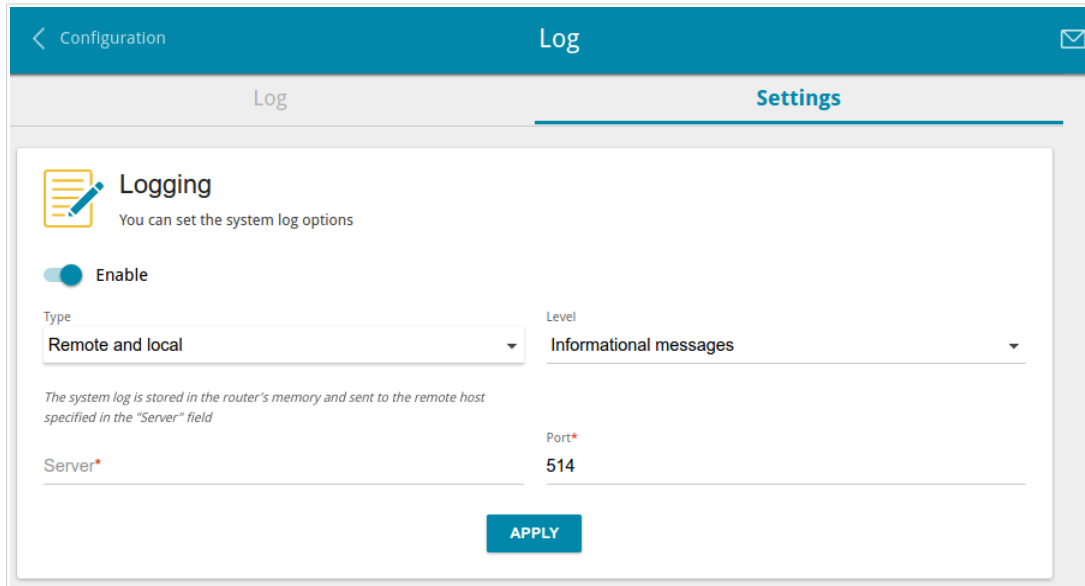


Figure 142. The **System / Log** page. The **Settings** tab.

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>Type</b>	Select a type of logging from the drop-down list. <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>Local and remote</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.

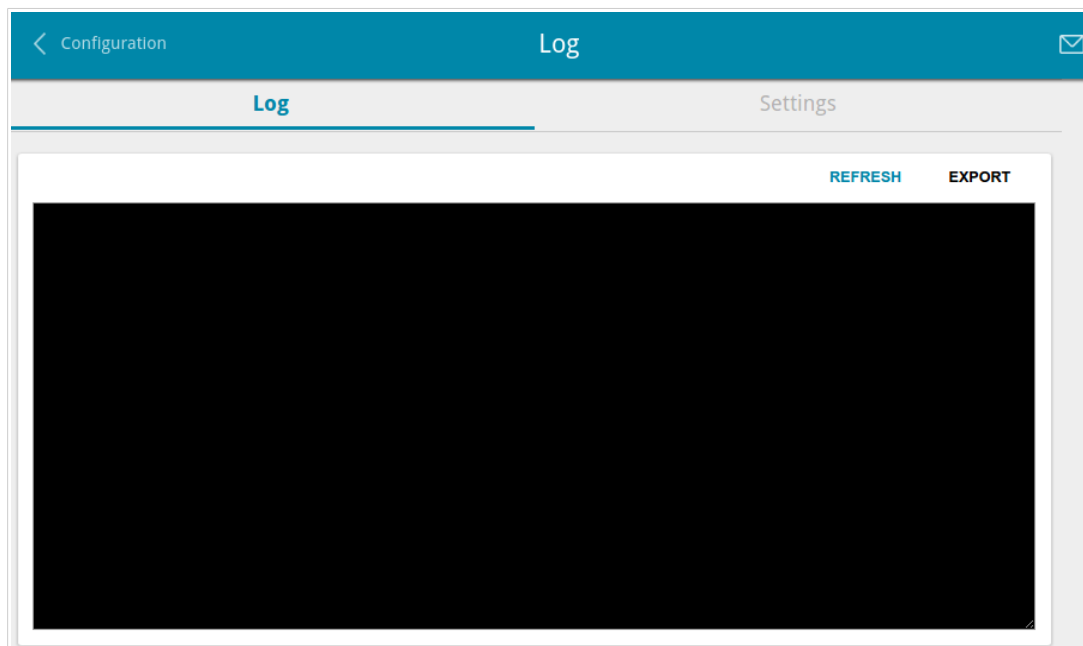


Figure 143. The **System / Log** page. The **Log** tab.

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.

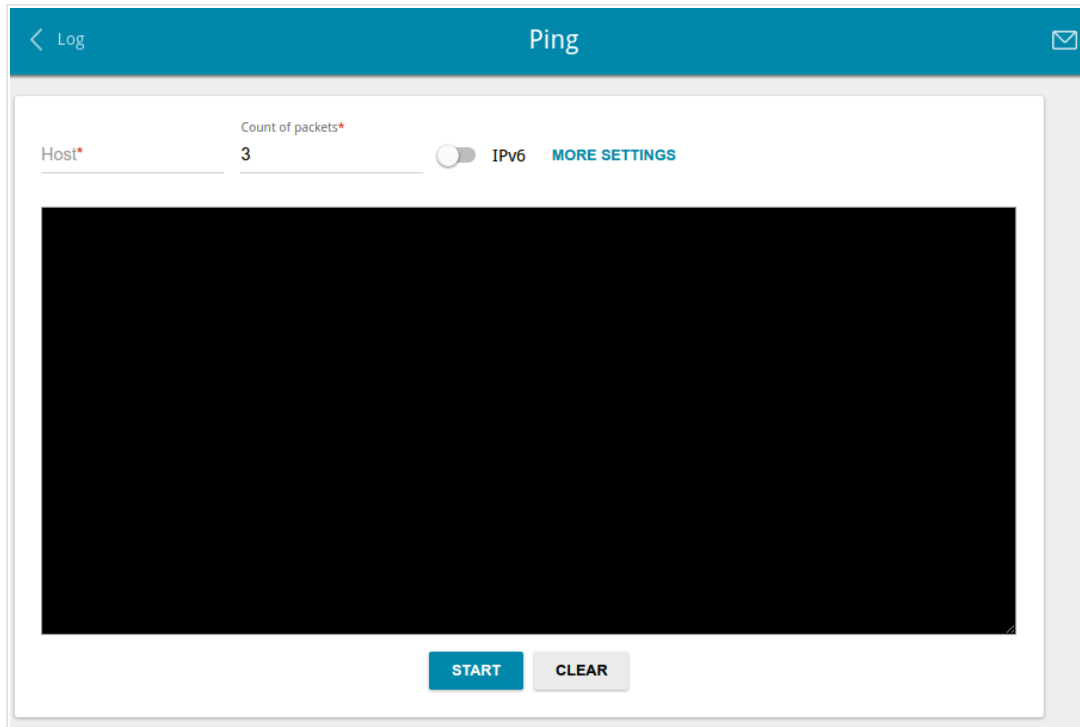


Figure 144. The **System / Ping** page.

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 **Count of packets** 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.

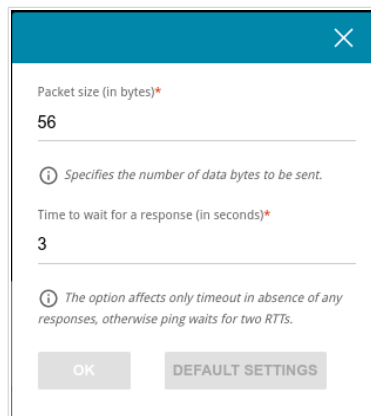


Figure 145. The **System / Ping** page. The additional settings window.

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

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



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

## Traceroute

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

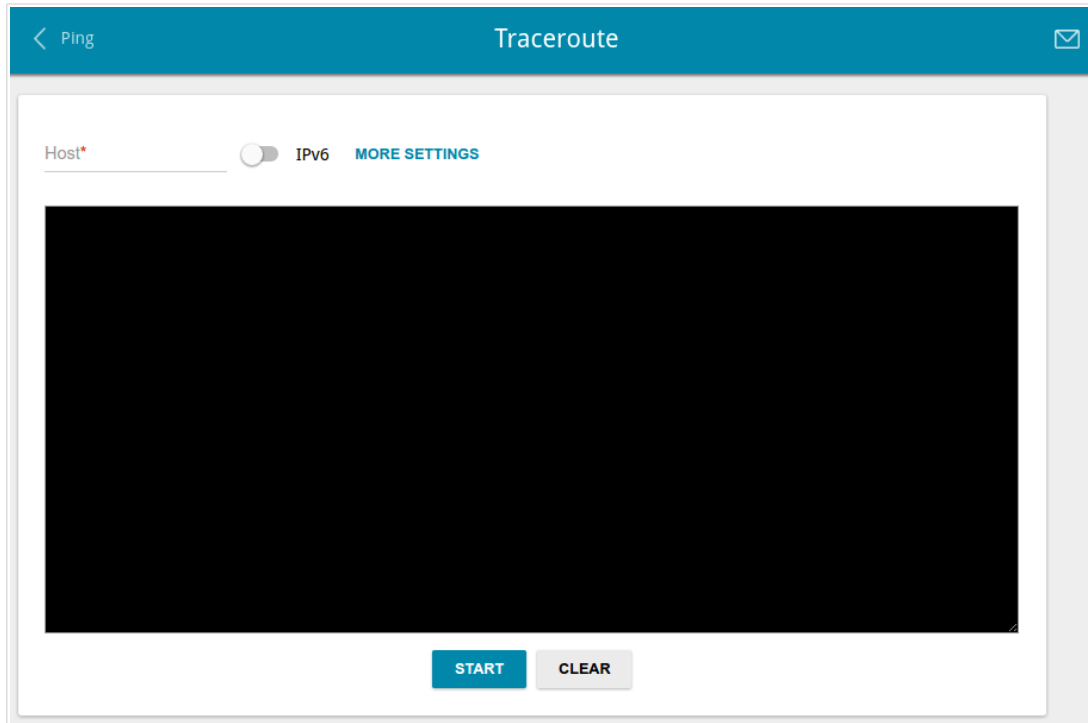


Figure 146. The **System / Traceroute** page.

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.

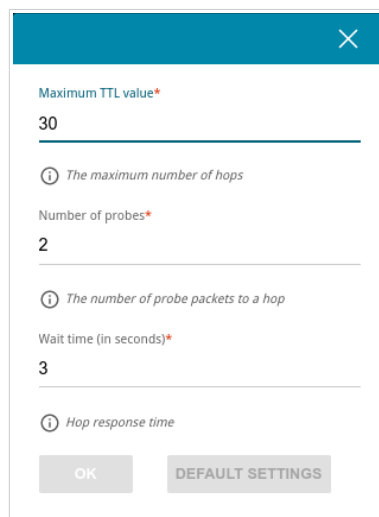


Figure 147. The **System / Traceroute** page. The additional settings window.

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 30.
<b>Number of probes</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.

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

## Telnet

On the **System / Telnet** page, you can enable or disable access to the device settings via TELNET from your LAN. Access via TELNET is disabled by default. It is automatically enabled after changing the default administrator password.

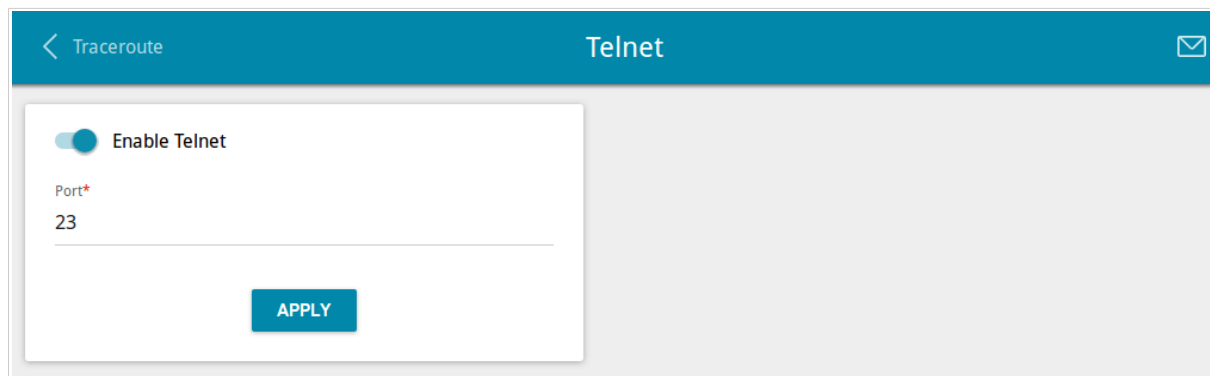


Figure 148. The **System / Telnet** page.

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

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

## 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.

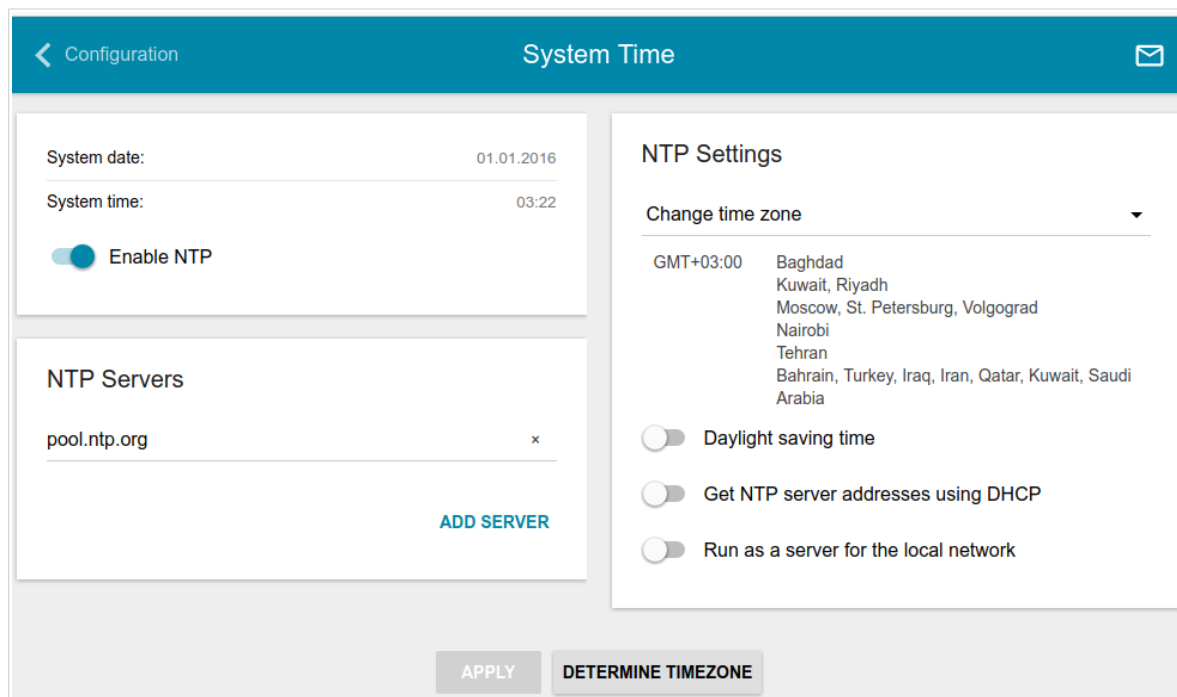


Figure 149. The **System / System Time** page.

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 **Change time zone** drop-down list in the **NTP Settings** section. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.
4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

To enable automatic adjustment for daylight saving time of the router, move the **Daylight saving time** switch to the right in the **NTP Settings** section and click the **APPLY** button.

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

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

 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).

## 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.

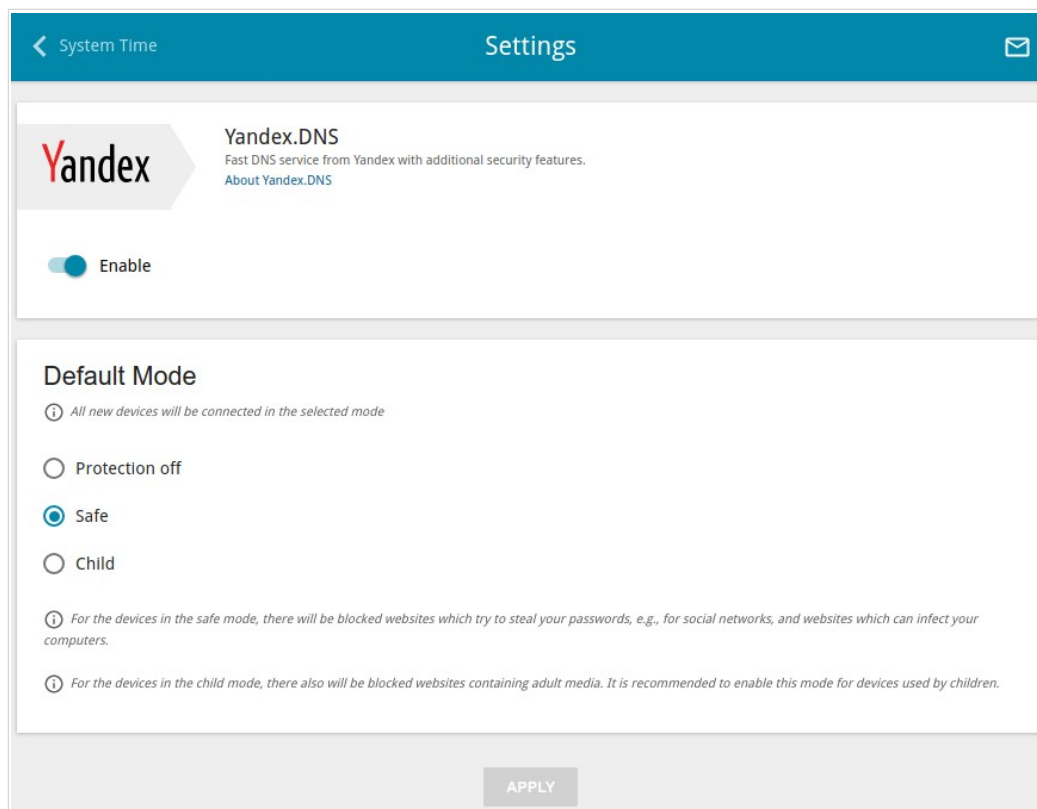


Figure 150. The **Yandex.DNS / Settings** page.

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.

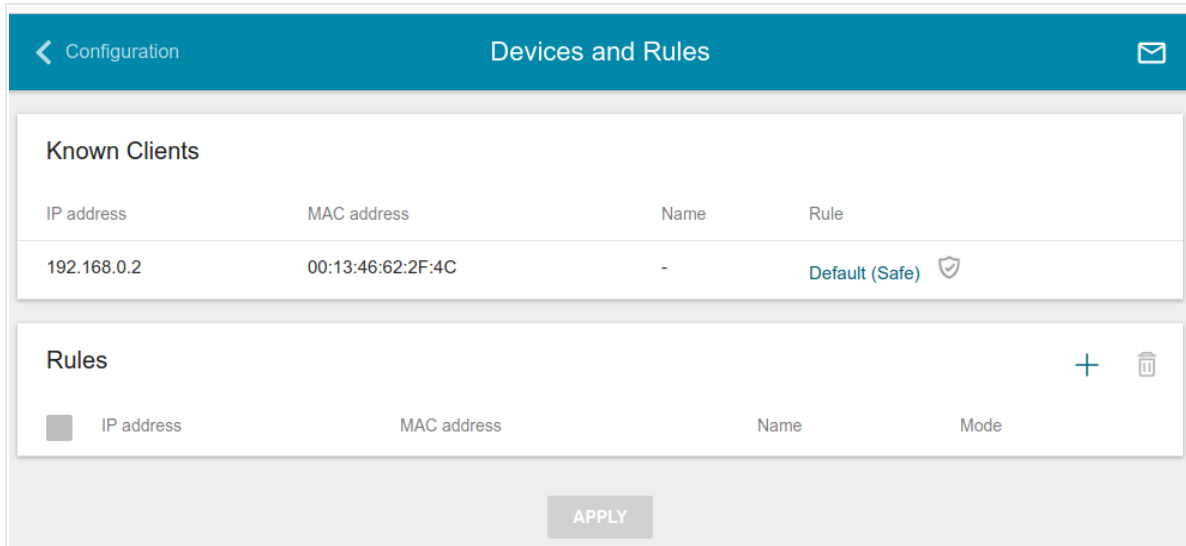


Figure 151. The **Yandex.DNS / Devices and Rules** page.

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<sup>8</sup> 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.

MAC address\*

IP address\*

Name

Protection off

Safe

Child

SAVE

Figure 152. Adding a new rule for the **Yandex.DNS** service.


<sup>8</sup> When a new rule for filtering is created, a MAC address and IP address pair is displayed on the **Connections Setup / LAN** page. The created pair will be deleted with the relevant rule.

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.
<b>IP address</b>	The IP address of a device from the router's LAN.
<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. <b>Protection off:</b> when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites. <b>Safe:</b> when this value is selected, the service blocks access to malicious and fraudulent web sites. <b>Child:</b> when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

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

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

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

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

## 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 DWR-921 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 DWR-921 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>ARP</b>	Address Resolution Protocol
<b>BSSID</b>	Basic Service Set Identifier
<b>CRC</b>	Cyclic Redundancy Check
<b>DDNS</b>	Dynamic Domain Name System
<b>DDoS</b>	Distributed Denial of Service
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DNS</b>	Domain Name System
<b>DTIM</b>	Delivery Traffic Indication Message
<b>GMT</b>	Greenwich Mean Time
<b>GSM</b>	Global System for Mobile Communications
<b>IGD</b>	Internet Gateway Device
<b>IGMP</b>	Internet Group Management Protocol
<b>IMEI</b>	International Mobile Equipment Identity
<b>IMSI</b>	International Mobile Subscriber Identity
<b>IP</b>	Internet Protocol
<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>LTE</b>	Long Term Evolution
<b>MAC</b>	Media Access Control
<b>MTU</b>	Maximum Transmission Unit
<b>NAT</b>	Network Address Translation

<b>NTP</b>	Network Time Protocol
<b>OFDM</b>	Orthogonal Frequency Division Multiplexing
<b>PBC</b>	Push Button Configuration
<b>PIN</b>	Personal Identification Number
<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>QoS</b>	Quality of Service
<b>RADIUS</b>	Remote Authentication in Dial-In User Service
<b>RIP</b>	Routing Information Protocol
<b>RTS</b>	Request To Send
<b>RTSP</b>	Real Time Streaming Protocol
<b>SIP</b>	Session Initiation Protocol
<b>SIM</b>	Subscriber Identification Module
<b>SMB</b>	Server Message Block
<b>SMS</b>	Short Message Service
<b>SSID</b>	Service Set Identifier
<b>TKIP</b>	Temporal Key Integrity Protocol
<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>WAN</b>	Wide Area Network
<b>WEP</b>	Wired Equivalent Privacy
<b>Wi-Fi</b>	Wireless Fidelity

<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