User Manual

DWR-953

Wireless AC1200 4G LTE Router with Gigabit Ethernet Ports

January 2023

Contents

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DWR-953 and explains how to configure and operate it.

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

Conventions

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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the router DWR-953 and configure a PC in order to access its web-based interface.

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

Chapter 5 includes safety instructions and tips for networking.

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

CHAPTER 2. OVERVIEW

General Information

The DWR-953 device is a wireless dual band gigabit 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 of up to 50Mbps.[1]

Also you are able to connect the wireless router DWR-953 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-953 device, you are able to quickly create a high-speed wireless network at home or in your office, which lets computers and mobile devices access the Internet virtually anywhere (within the operational range of your wireless network). Simultaneous activity of 2.4GHz band and 5GHz band allows performing a wide range of tasks. The router can operate as a base station for connecting wireless devices of the standards 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac (at the wireless connection rate up to 1167Mbps[2]).

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

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

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

Smart adjustment of Wi-Fi clients is useful for networks based on several D-Link access points or routers – when the smart adjustment function is configured on each of them, a client always connects to the access point (router) with the highest signal level.

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

The wireless router DWR-953 includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

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

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

1 Data rates are theoretical. Data transfer rate depends on network capacity and signal strength.
2 Up to 300Mbps for 2.4GHz and up to 867Mbps for 5GHz.

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

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

You can configure the settings of the wireless router DWR-953 via the user-friendly web-based interface (the interface is available in several languages).

The configuration wizard allows you to quickly switch DWR-953 to one of the following modes: router (for connection to a wired or wireless ISP), access point, repeater, or client, and then configure all needed setting for operation in the selected mode in several simple steps.

Also DWR-953 supports configuration and management via mobile application for Android and iPhone smartphones.

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

*Specifications**

Hardware	
Processor	· RTL8685PB (1GHz)
RAM	· 128MB, DDR2, built in processor
Flash	· 16MB, SPI
Built-in modem	· BroadMobi BM806U-E1
Interfaces	· Slot for SIM card (mini-SIM) · 10/100/1000BASE-T WAN port · 4 10/100/1000BASE-T LAN ports
LEDs	· POWER · INTERNET · 5GHz · 2.4GHz · 4G · 2G/3G · LAN · WAN · SMS · SIGNAL STRENGTH
Buttons	· ON/OFF button to power on/power off · RESET button to restore factory default settings · WPS button to set up wireless connection · WLAN button to enable/disable wireless network
Antenna	· Two detachable LTE/3G antennas (3dBi gain) · Two internal Wi-Fi antennas for 2.4GHz band (3dBi gain) · Two internal Wi-Fi antennas for 5GHz band (3dBi gain)
MIMO	· 2 x 2
Power connector	· Power input connector (DC)

Software	
WAN connection types	· Mobile Internet · PPPoE · IPv6 PPPoE · PPPoE Dual Stack · Static IPv4 / Dynamic IPv4 · Static IPv6 / Dynamic IPv6 · PPPoE + Static IP · PPPoE + Dynamic IP · PPTP/L2TP + Static IP · PPTP/L2TP + Dynamic IP

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

Software	
Network functions	· DHCP server/relay · Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation · Automatic obtainment of LAN IP address (for access point/repeater/client modes) · DNS relay · Dynamic DNS · Static IPv4/IPv6 routing · IGMP Proxy · RIP · Support of UPnP · Support of VLAN · WAN ping respond · Support of SIP ALG · Support of RTSP · WAN failover · LAN/WAN conversion · Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port · Built-in UDPXY application · Equal load distribution while using several WAN connections (traffic balancing)
Firewall functions	· Network Address Translation (NAT) · Stateful Packet Inspection (SPI) · IPv4/IPv6 filter · MAC filter · URL filter · DMZ · Virtual servers · Built-in SkyDNS web content filtering service
VPN	· IPsec/PPTP/L2TP/PPPoE pass-through · PPTP/L2TP servers · PPTP/L2TP tunnels · L2TP over IPsec · GRE/EoGRE/EoIP tunnels · IPsec tunnels Transport/Tunnel mode IKEv1/IKEv2 support DES encryption NAT Traversal Support of DPD (Keep-alive for VPN tunnels)
Management and monitoring	· Local and remote access to settings through SSH/TELNET/WEB (HTTP/HTTPS) · Multilingual web-based interface for configuration and management · Support of D-Link Assistant application for Android and iPhone smartphones · Notification on connection problems and auto redirect to settings · Firmware update via web-based interface · Automatic notification on new firmware version · Saving/restoring configuration to/from file · Support of logging to remote host · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility · TR-069 client · Schedules for rules and settings of firewall, automatic reboot, limitation of wireless client maximum bandwidth, and enabling/disabling wireless network and Wi-Fi filter · Automatic upload of configuration file from ISP's server (Auto Provision) · Configuration of action for hardware buttons

LTE Module Parameters	
LTE connection rate[3]	· Downlink: up to 150Mbps · Uplink: up to 50Mbps
Supported frequencies[4]	· Power Class 3 · LTE Band: TX / RX B1: 1920~1980MHz / 2110~2170MHz B2: 1850~1910MHz / 1930~1990MHz B3: 1710~1785MHz / 1805~1880MHz B5: 824~849MHz / 869~894MHz B7: 2500~2570MHz / 2620~2690MHz B8: 880~915MHz / 925~960MHz B20: 832~862MHz / 791~821MHz B38: 2570~2620MHz / 2570~2620MHz B40: 2300~2400MHz / 2300~2400MHz · UMTS B1/2/3/5/8 (2100/1900/1800/850/900MHz) · GSM/GPRS 850/900/1800/1900MHz
Functions	· Auto connection to available type of supported network (4G/3G/2G) · Auto configuration of connection upon plugging in SIM card · Enabling/disabling PIN code check, changing PIN code · Sending/receiving/reading/removing SMS messages · Support of USSD requests (*For DWR-953 with the built-in modem FW version M1.4.4_E1.0.3_A1.1.8. See the data on the modem FW version in the web-based interface of the router, on the "LTE Modem" page.*)

Wireless Module Parameters	
Standards	· IEEE 802.11n/ac · IEEE 802.11b/g/n · IEEE 802.11k/v · IEEE 802.11w
Frequency range *The frequency range depends upon the radio frequency regulations applied in your country*	· 2400 ~ 2483.5MHz · 5150 ~ 5350MHz · 5650 ~ 5850MHz
Wireless connection security	· WEP · WPA/WPA2 (Personal/Enterprise) · WPA3 (Personal) · MAC filter · WPS (PBC/PIN)
Advanced functions	· Support of client mode · WMM (Wi-Fi QoS) · Information on connected Wi-Fi clients · Advanced settings · Smart adjustment of Wi-Fi clients · Guest Wi-Fi / support of MBSSID · Rate limitation for wireless network/separate MAC addresses · Periodic scan of channels, automatic switch to least loaded channel · Support of 2.4GHz/5GHz TX Beamforming · Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence) · Support of STBC

3 Data rates are theoretical. Data transfer rate depends on network capacity and signal strength.

4 Supported frequency bands are dependent on regional variants.

Wireless Module Parameters	
Wireless connection rate	· IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11b: 1, 2, 5.5, and 11Mbps · IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11n (2.4GHz/5GHz): from 6.5 to 300Mbps (from MCS0 to MCS15) · IEEE 802.11ac (5GHz): from 6.5 to 867Mbps (from MCS0 to MCS9)
Transmitter output power *The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country*	· 802.11b 15dBm (+/-1.5dB) · 802.11g 12dBm (+/-1.5dB) · 802.11n HT20 12dBm (+/-1.5dB) HT40 12dBm (+/-1.5dB) · 802.11ac 14dBm
Receiver sensitivity	· 802.11b -76dBm at 11Mbps · 802.11g -65dBm at 54Mbps · 802.11n HT20 -64dBm at MCS7/15 HT40 -61dBm at MCS7/15 · 802.11ac VHT20 -56dBm at MCS8 VHT40 -53dBm at MCS9 VHT80 -51dBm at MCS9
Modulation schemes	· 802.11b: DSSS/BPSK/QPSK/CCK · 802.11g: OFDM/DSSS/BPSK/QPSK/CCK · 802.11n: BPSK/QPSK/16 QAM/64 QAM/DBPSK/DQPSK/CCK · 802.11ac: BPSK/QPSK/16 QAM/64 QAM/256 QAM

Physical Parameters	
Dimensions (L x W x H)	· 170 x 80 x 180 mm (6.7 x 3.2 x 7.1 in)
Weight	· 400 g (0.88 lb)

Operating Environment	
Power	· Output: 12V DC, 1.5A
Temperature	· Operating: from 0 to 40 °C · Storage: from -10 to 70 °C
Humidity	· Operating: from 10% to 90% (non-condensing) · Storage: from 0% to 95% (non-condensing)

Product Appearance

Front Panel

Figure 1. Front panel view.

LED	Mode	Description
POWER	*Solid green*	The router is powered on.
	Blinking green	The firmware is being updated.
	No light	The router is powered off.
INTERNET	*Solid red*	There are no WAN connections created or the default WAN connection is off.
	Solid green	The default WAN connection is on.
	No light	The WAN cable is not connected or the SIM card is blocked.
5GHz **2.4GHz**	*Solid green*	The router's WLAN of the relevant band is on.
	Fast blinking green	Data transfer through the Wi-Fi network of the relevant band.
	Slow blinking green	Attempting to add a wireless device via the WPS function.
	No light	The router's WLAN of the relevant band is off.
4G	*Solid green*	4G network registration is successfully done.
	Blinking green	Searching for a 4G network.
	No light	No registration in a 4G network.

LED	Mode	Description
2G/3G	*Solid green*	2G/3G network registration is successfully done.
	Blinking green	Searching for a 2G/3G network.
	No light	No registration in a 2G/3G network.
LAN	*Solid green*	The cable is connected to a LAN port.
	Blinking green	Data transfer through one or several LAN ports.
	No light	The cable is not connected to a LAN port.
WAN	*Solid green*	The cable is connected to the WAN port.
	Blinking green	Data transfer through the WAN port.
	No light	The cable is not connected to the WAN port.
SMS	*Solid green*	An unread message (or messages).
	No light	No unread messages.
SIGNAL STRENGTH	*Solid green*	Poor signal strength.  Fair signal strength.  Good signal strength.  Excellent signal strength. 
	Blinking green	Searching for a mobile operator network.
	No light	The SIM card is not installed or is blocked.

In case the **POWER**, **5GHz**, **2.4GHz**, **4G**, **2G/3G**, **SMS**, and **SIGNAL STRENGTH** LEDs are fast blinking green at the same time, the device is in the emergency mode. Power the device off and on. If the device is loaded in the emergency mode again, restore the factory default settings via the hardware **RESET** button.

Left Side Panel

Figure 2. Left side panel view.

Name	Description
RESET	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.
WPS	A button to quickly add wireless devices to the router's WLAN (the WPS function). To use the WPS function: with the device turned on, press the button and release.
WLAN	A button to enable/disable wireless network. To disable the router's wireless network: with the device turned on, press the button and release. The **2.4GHz** and **5GHz** LEDs should turn off.

Right Side Panel

Figure 3. Right side panel view.

Name	Description
ON/OFF	A button to turn the router on/off.

A slot for SIM card (mini-SIM) is also located on the right side panel of the router.

Back Panel

Figure 4. Back panel view.

Port	Description
12V=1.5A	Power connector.
WAN	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).
LAN 1-4	4 Ethernet ports to connect computers or network devices.

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

Delivery Package

The following should be included:

- Router DWR-953
- Power adapter DC 12V/1.5A
- Ethernet cable
- 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).

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

CHAPTER 3. INSTALLATION AND CONNECTION

Before You Begin

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

Computer or Mobile Device

Configuration of the wireless dual band gigabit router with 3G/LTE support DWR-953 (hereinafter referred to as "the router") is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

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

PC Web Browser

The following web browsers are recommended:

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

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

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

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

Wireless Connection

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

SIM Card

To connect to 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.[5]

5 Contact your operator to get information on the service coverage and fees.

Connecting to PC

PC with Ethernet Adapter

1. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
2. ***To connect via built-in LTE modem***: insert a SIM card into the slot on the right side panel of the router with the gold contacts facing towards the front of the device 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.

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 **ON/OFF** button on its right side panel.

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

Obtaining IP Address Automatically (OS Windows 7)

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

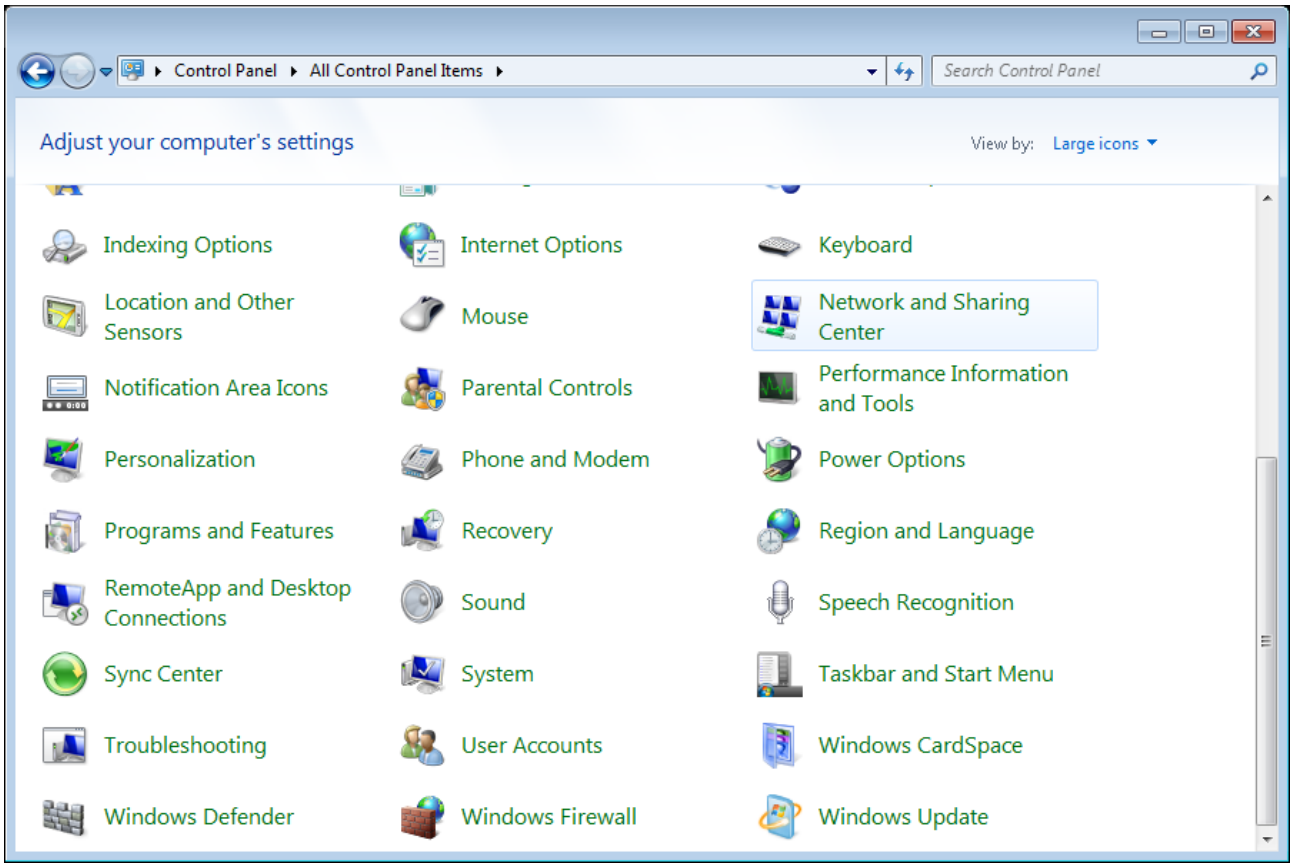

*Figure 5. The **Control Panel** window.*

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

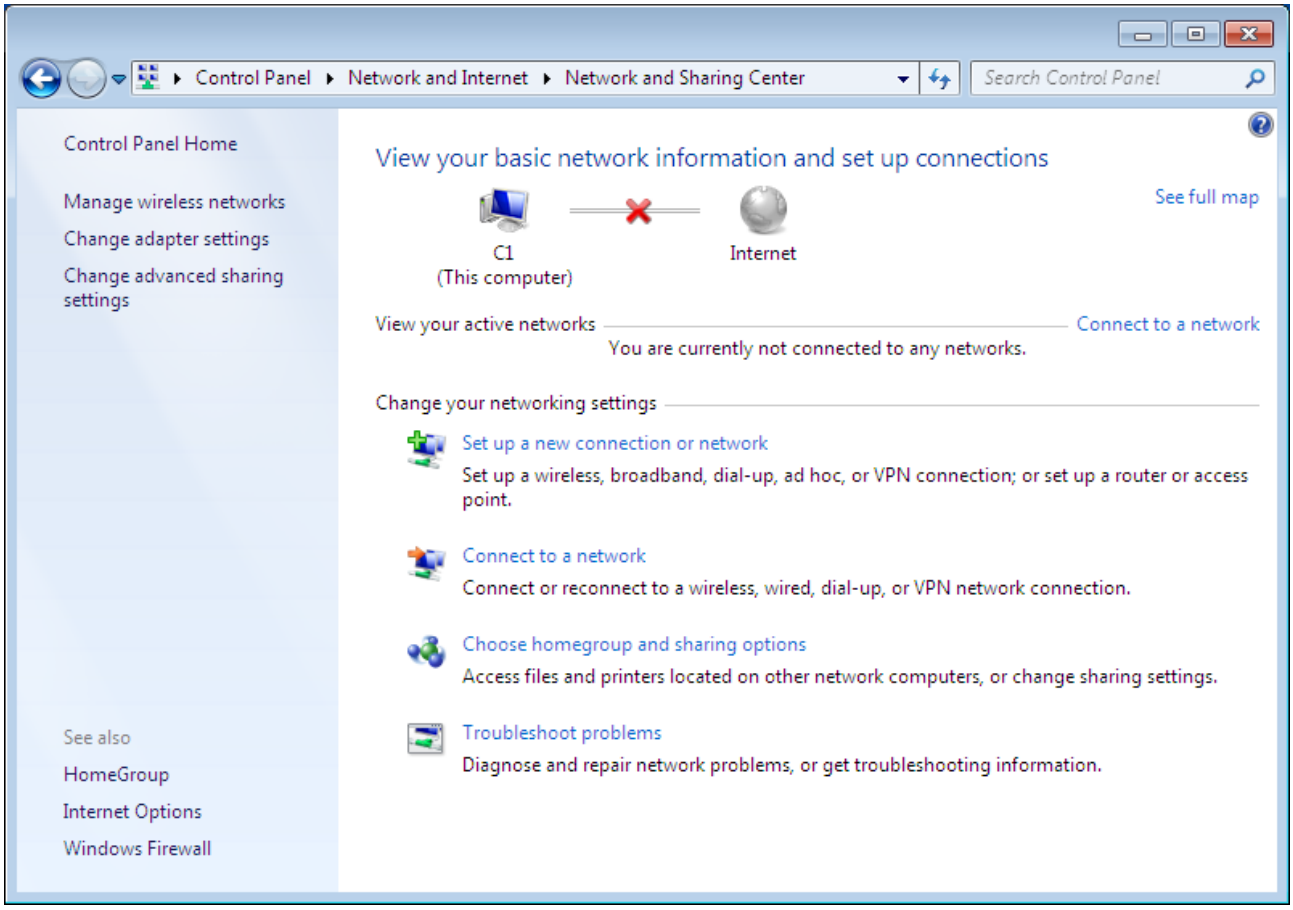

*Figure 6. The **Network and Sharing Center** window.*

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

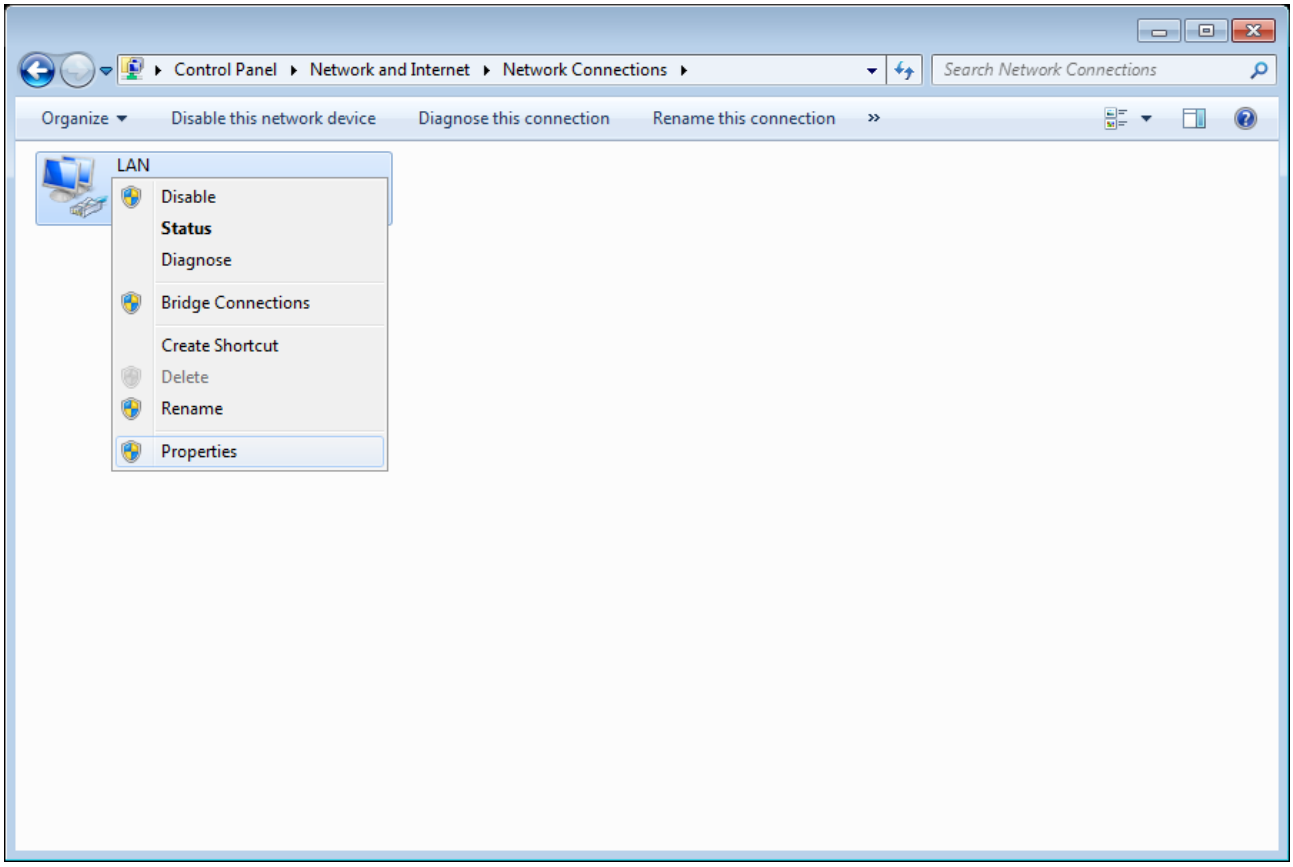

*Figure 7. The **Network Connections** window.*

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.

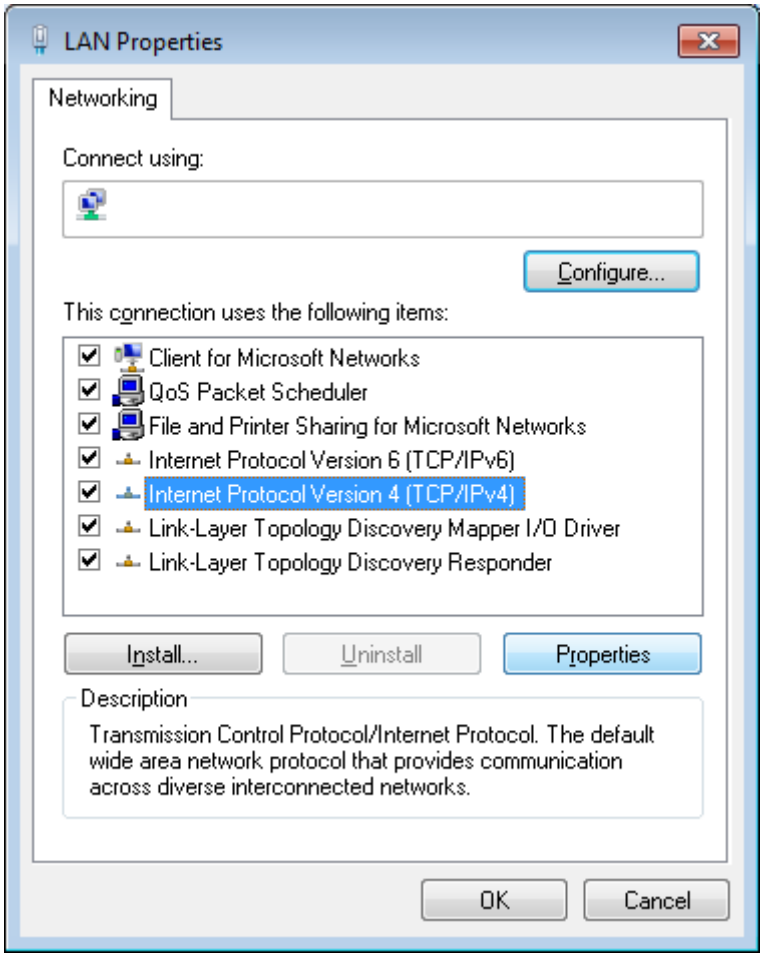

*Figure 8. The **Local Area Connection Properties** window.*

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

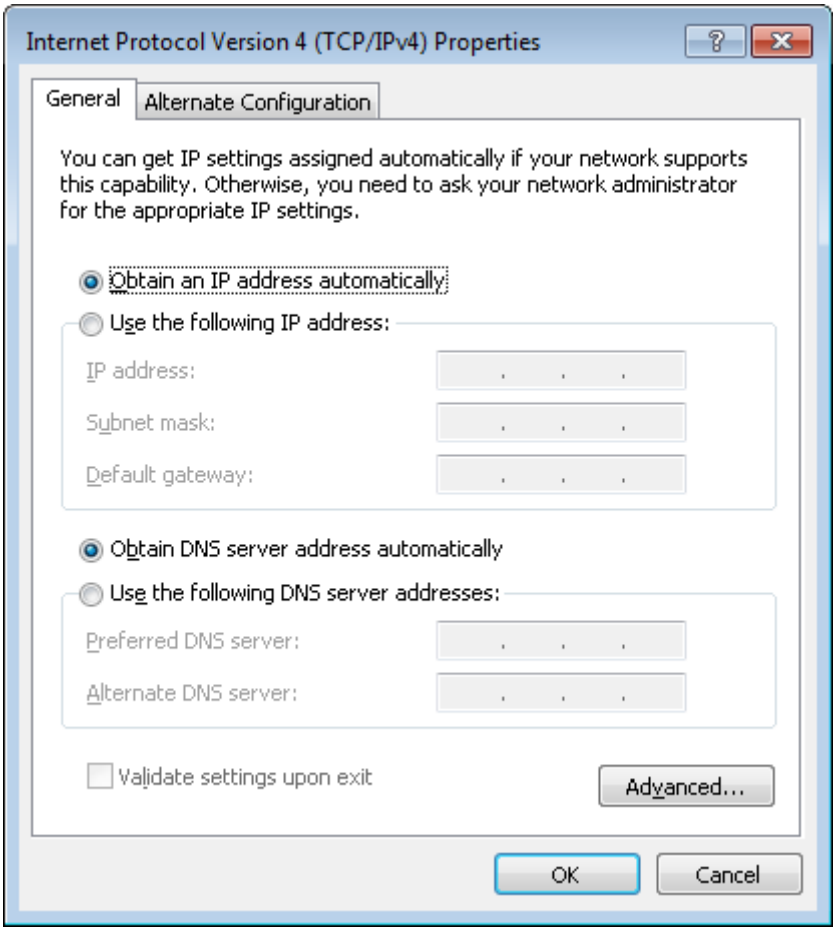

*Figure 9. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

Obtaining IP Address Automatically (OS Windows 10)

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

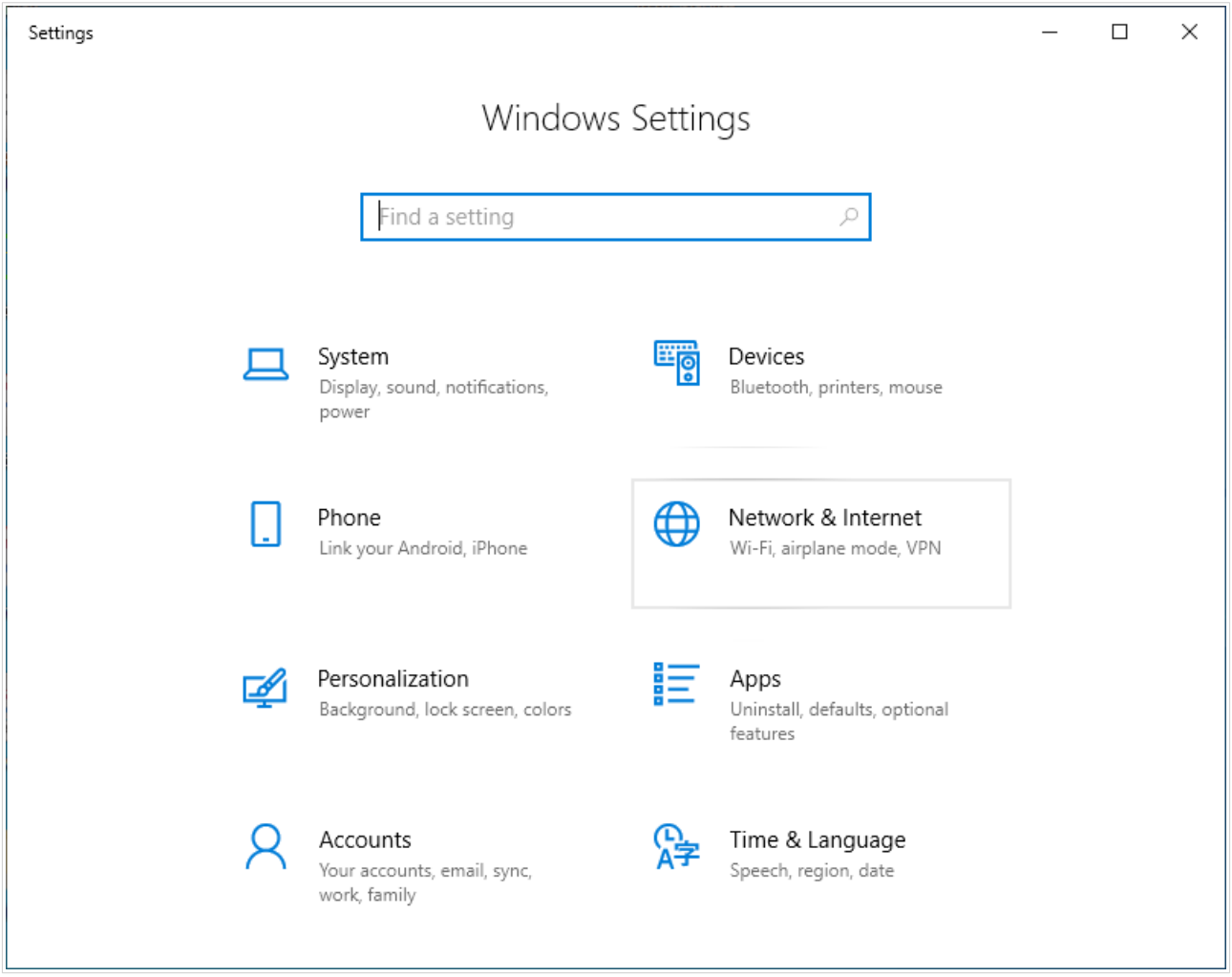

*Figure 10. The **Windows Settings** window.*

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

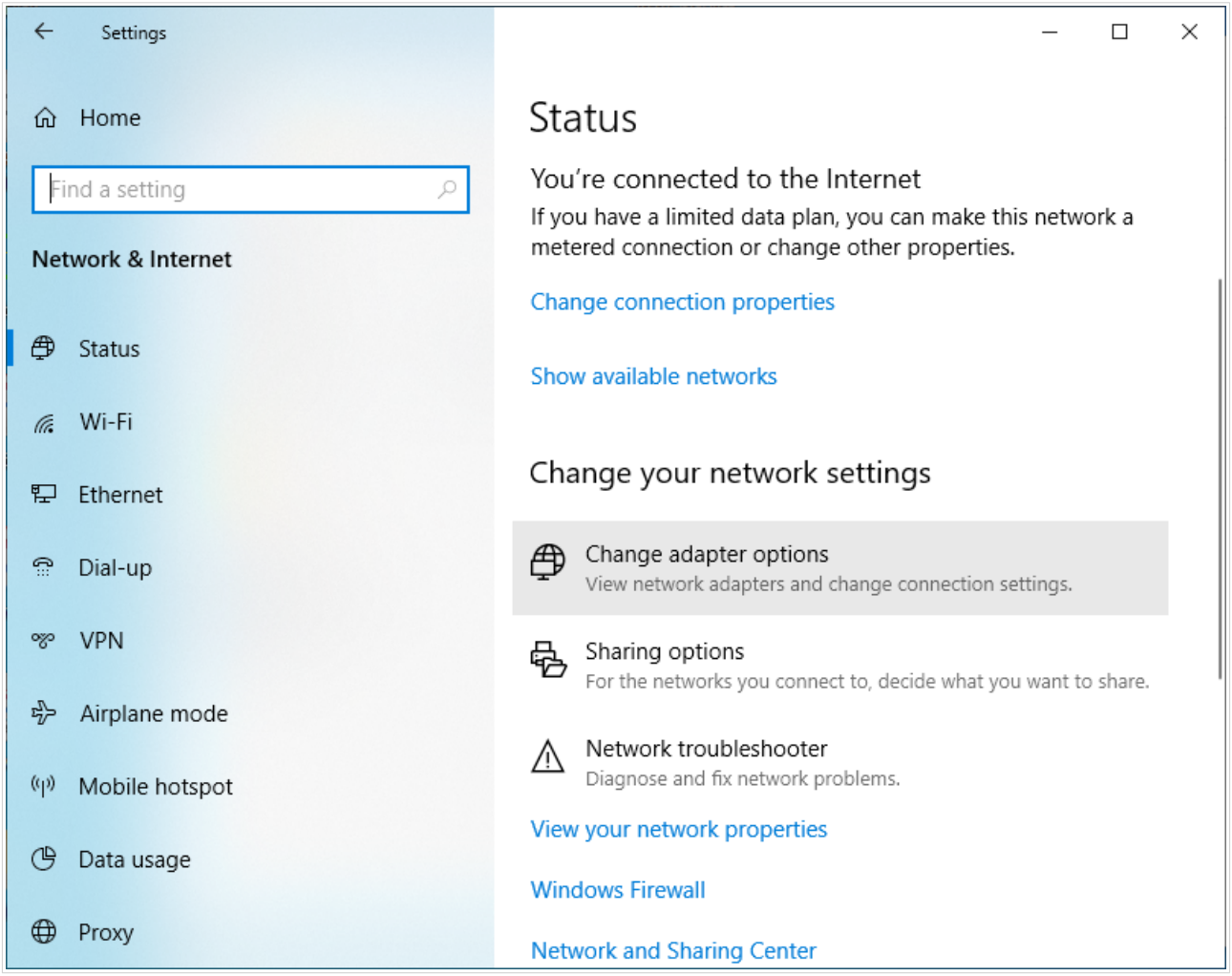

*Figure 11. The **Network & Internet** window.*

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

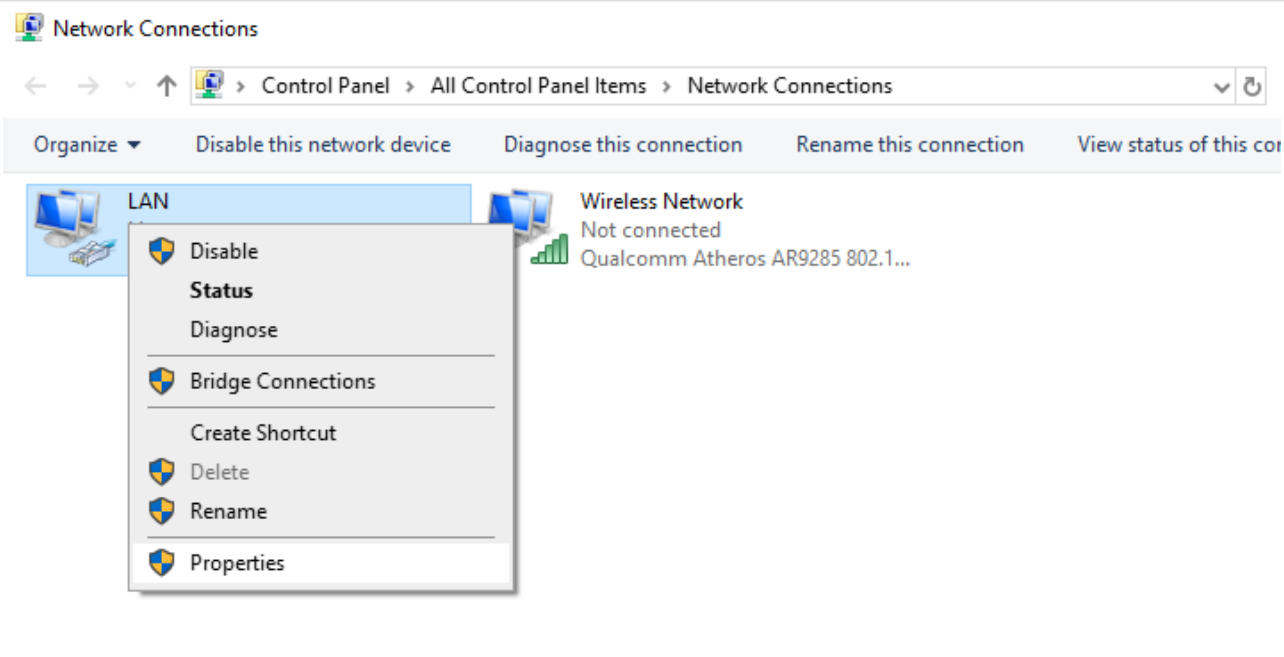

*Figure 12. The **Network Connections** window.*

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.

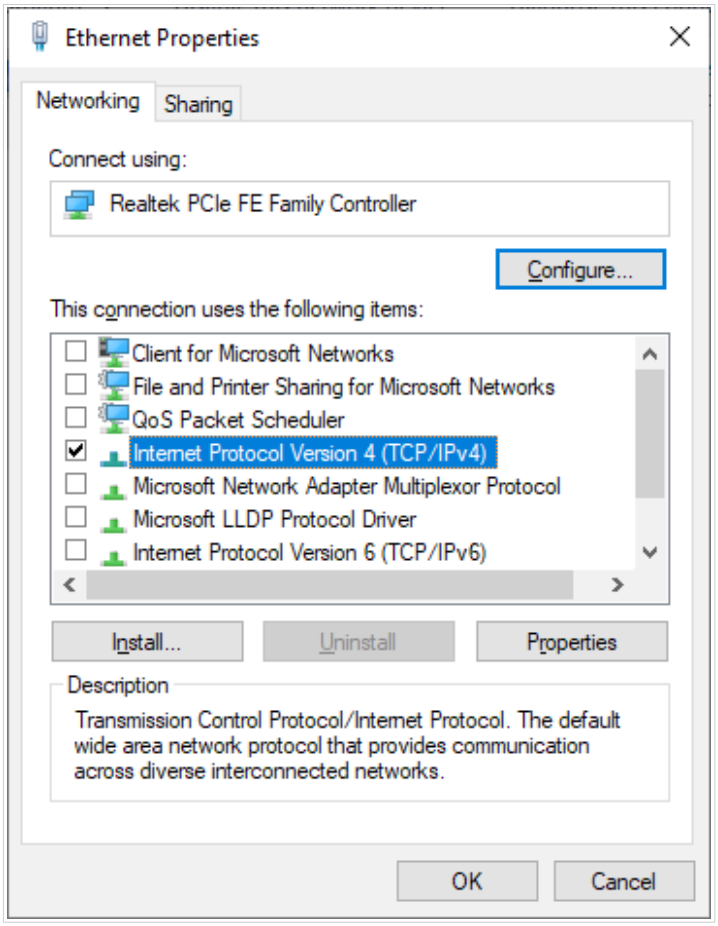

Figure 13. The local area connection properties window.

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

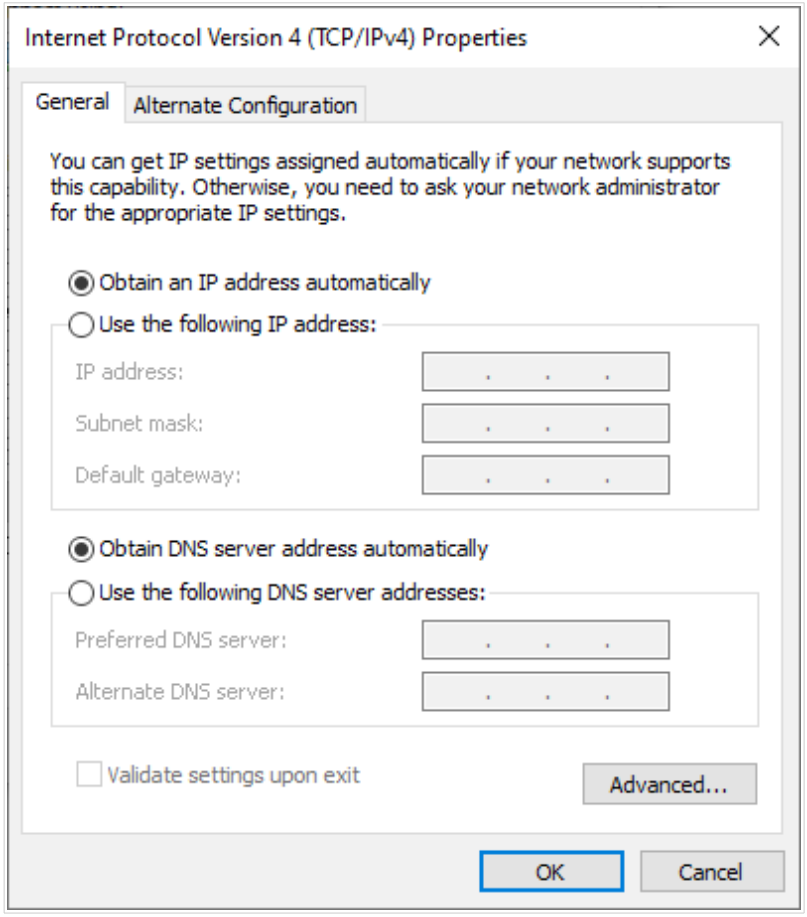

*Figure 14. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

PC with Wi-Fi Adapter

1. ***To connect via built-in LTE modem***: insert a SIM card into the slot on the right side panel of the router with the gold contacts facing towards the front of the device 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 **ON/OFF** button on its right side 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.

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

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

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

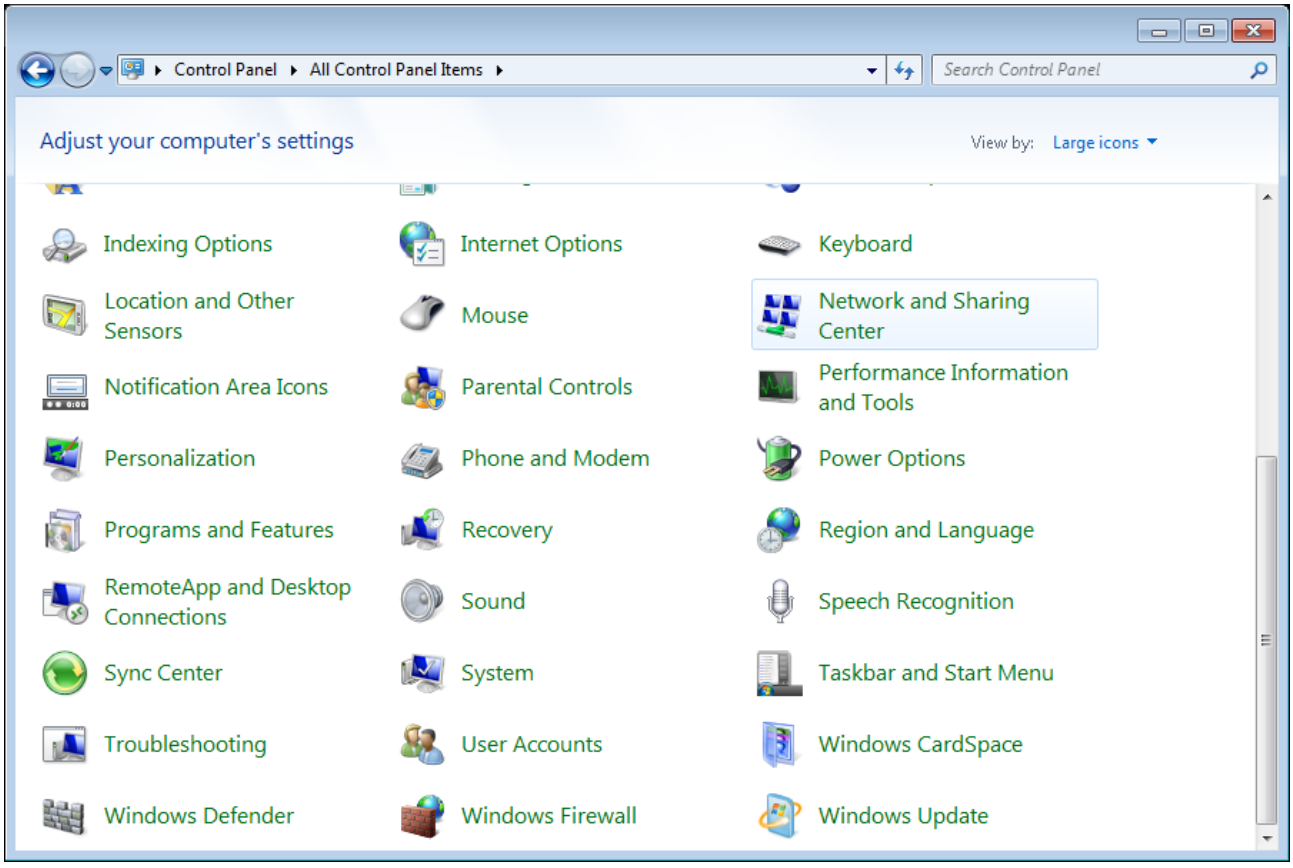

*Figure 15. The **Control Panel** window.*

3. In the menu located on the left part of the window, select the **Change adapter settings** line.
4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.
5. In the **Wireless Network Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.

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

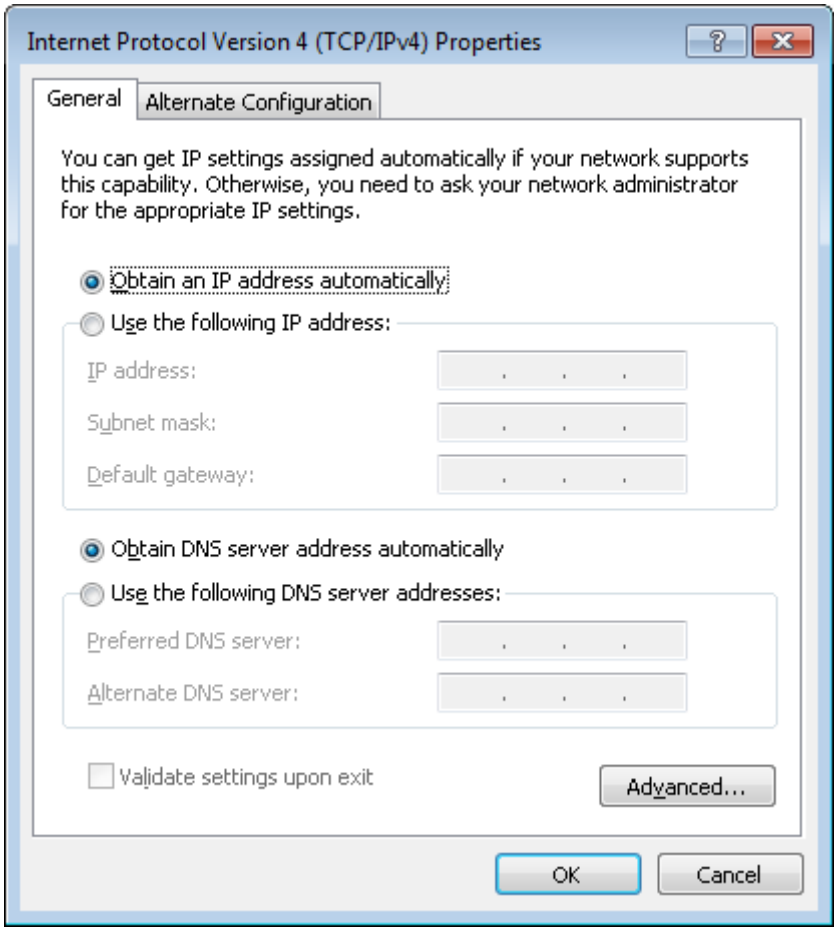

*Figure 16. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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.

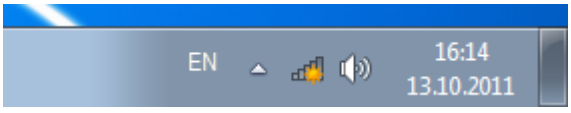

Figure 17. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network **DWR-953** (for operating in the 2.4GHz band) or **DWR-953-5G** (for operating in the 5GHz band) and click the **Connect** button.

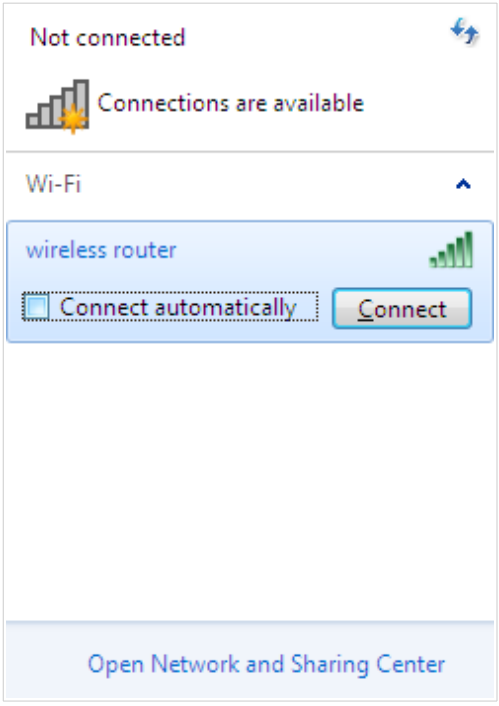

Figure 18. The list of available networks.

10. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **OK** button.
11. Wait for about 20-30 seconds. After the connection is established, the network icon will be displayed as the signal level scale.

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

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

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

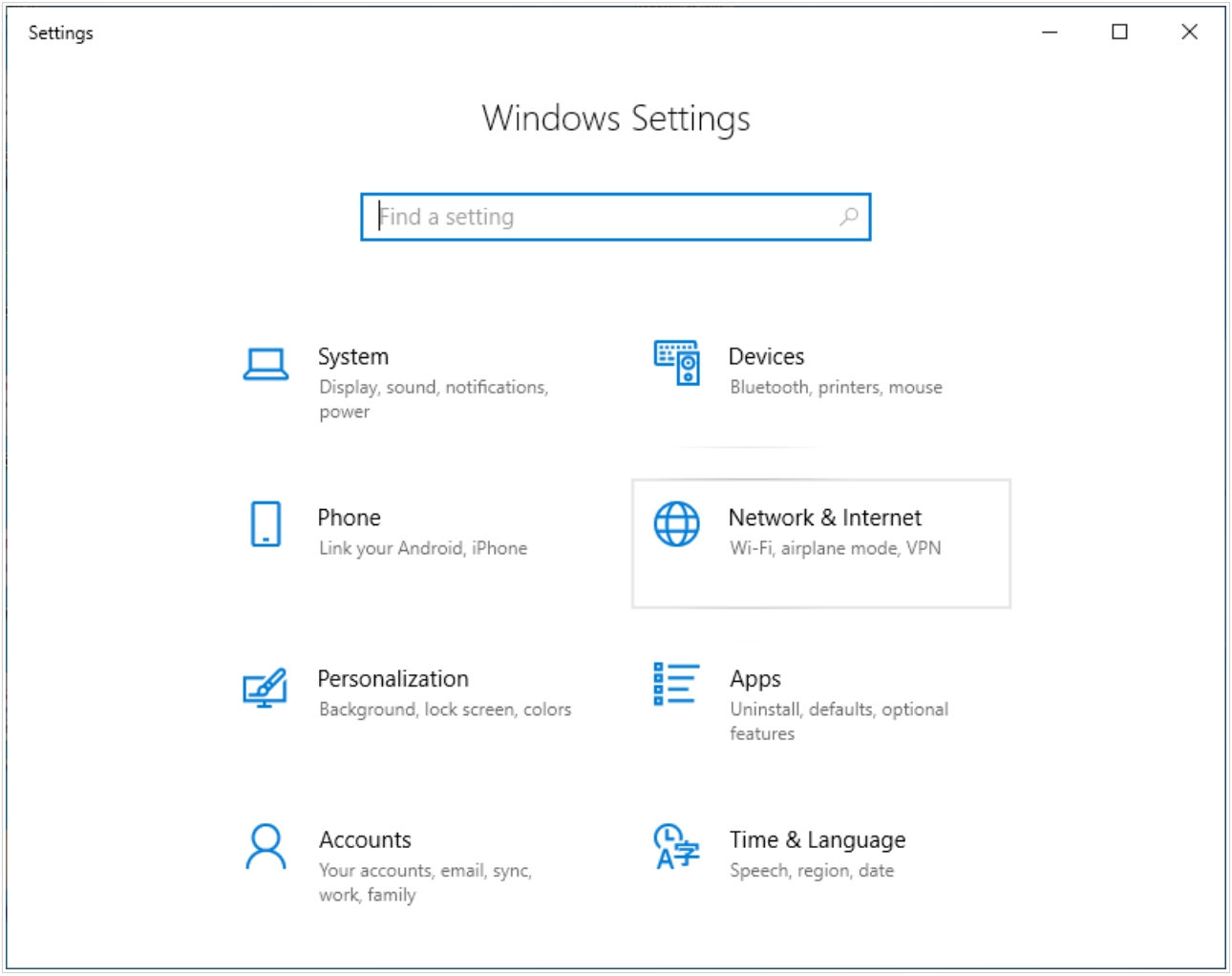

*Figure 19. The **Windows Settings** window.*

3. In the **Change your network settings** section, select the **Change adapter options** line.
4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.
5. In the **Wireless Network Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.

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

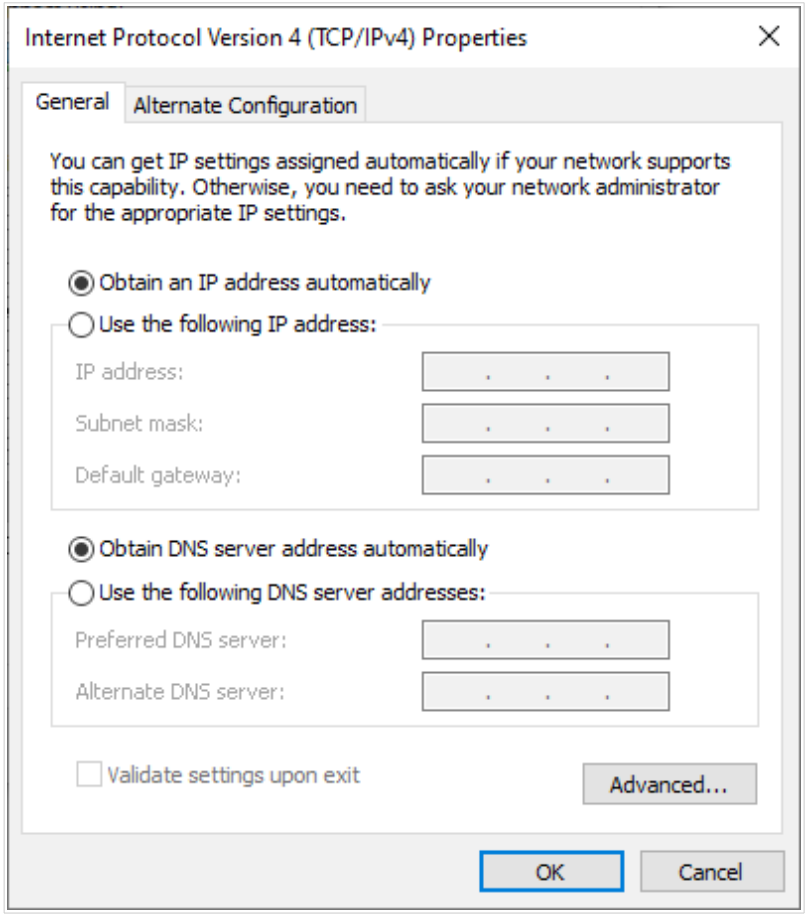

*Figure 20. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

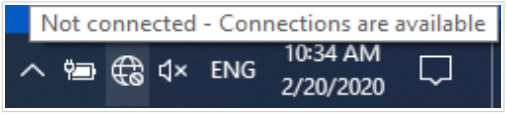

Figure 21. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network **DWR-953** (for operating in the 2.4GHz band) or **DWR-953-5G** (for operating in the 5GHz band) and click the **Connect** button.

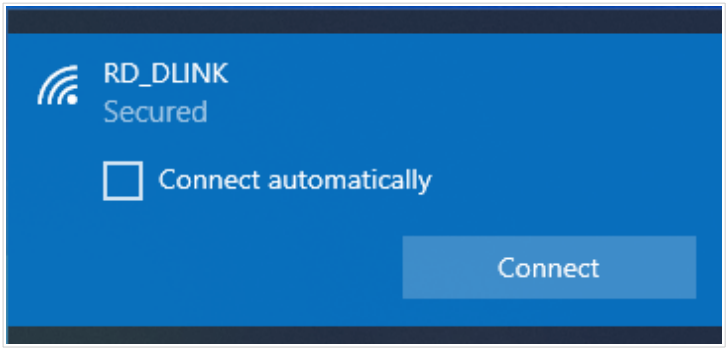

Figure 22. The list of available networks.

10. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **Next** button.
11. Allow or forbid your PC to be discoverable by other devices on this network (**Yes / No**).

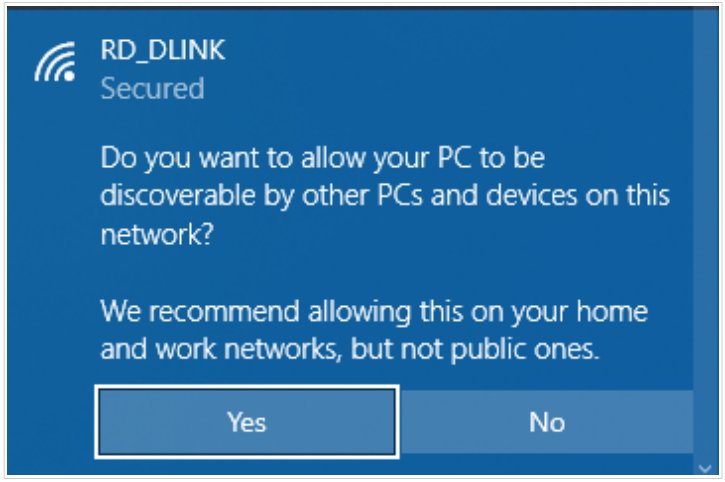

Figure 23. PC discovery settings.

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

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

Connecting to Web-based Interface

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

> **!** Clients connected to the router with default settings do not have access to the Internet. To get started, please set your own password for access to the web-based interface and change the WLAN name (SSID); then, if needed, configure other settings recommended by your ISP.

Start a web browser (see the ***Before You Begin*** section, page 18). 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 24. Connecting to the web-based interface of the DWR-953 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 43).

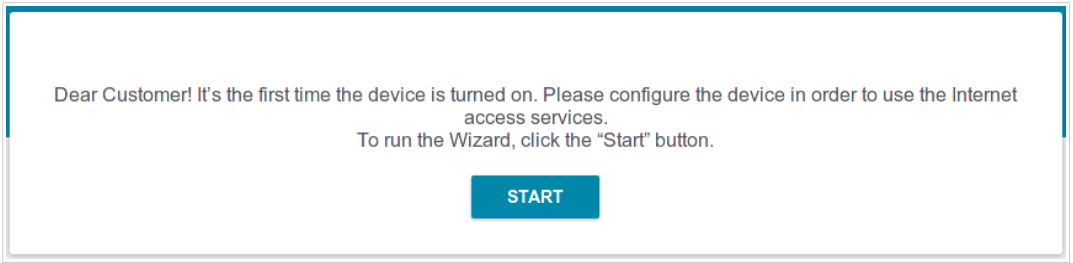

Figure 25. The page for running the Initial Configuration Wizard.

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

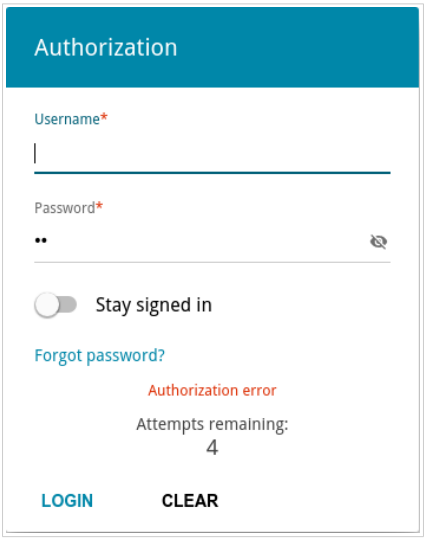

Figure 26. The login page.

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

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

Web-based Interface Structure

Summary Page

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

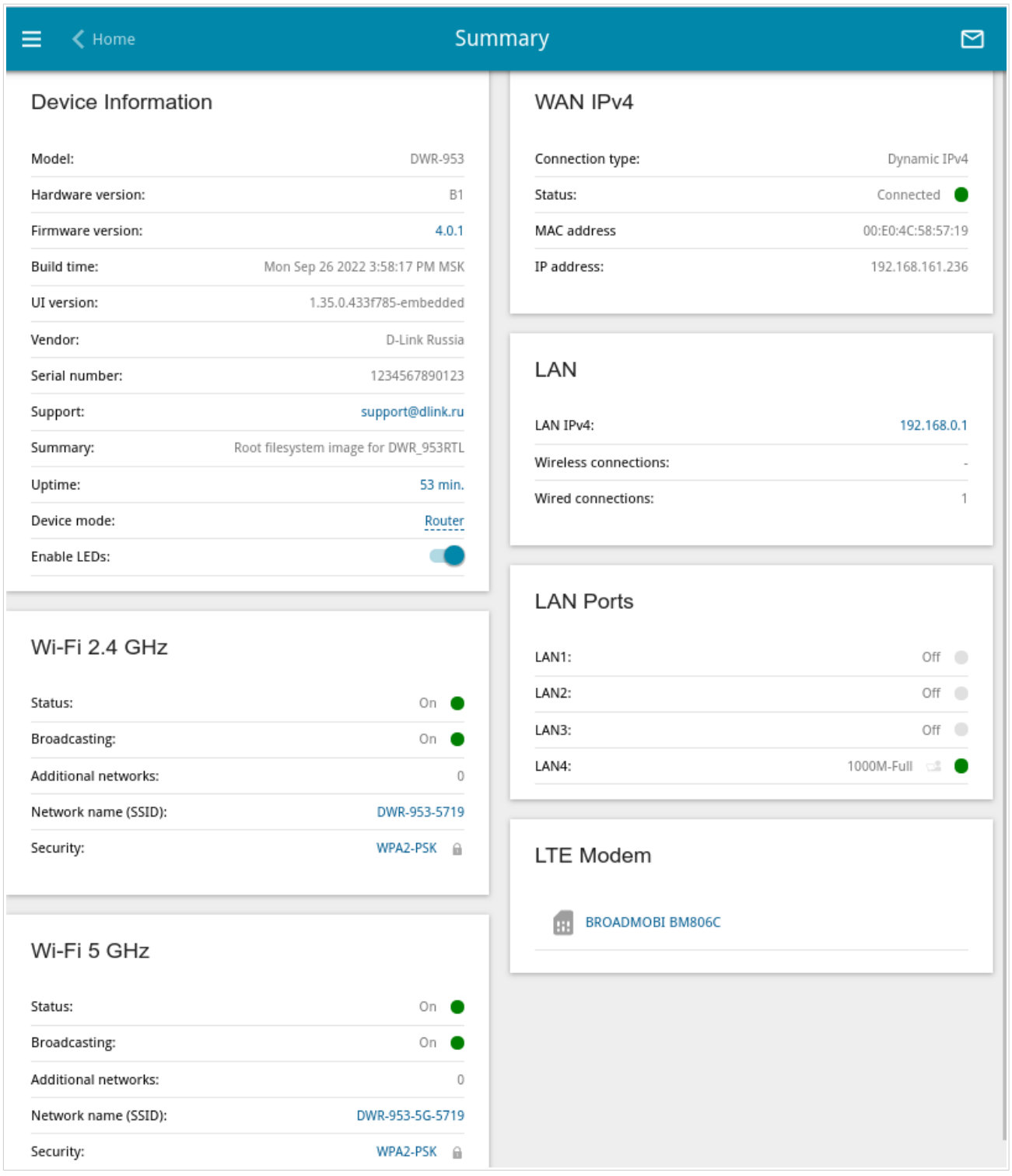

Figure 27. The summary page.

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

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

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **Initial Configuration Wizard** link (for the detailed description of the Wizard, see the ***Initial Configuration Wizard*** section, page 43).

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

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

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

In the **LAN** section, the IPv4 and IPv6 address of the router, 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.

Home Page

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

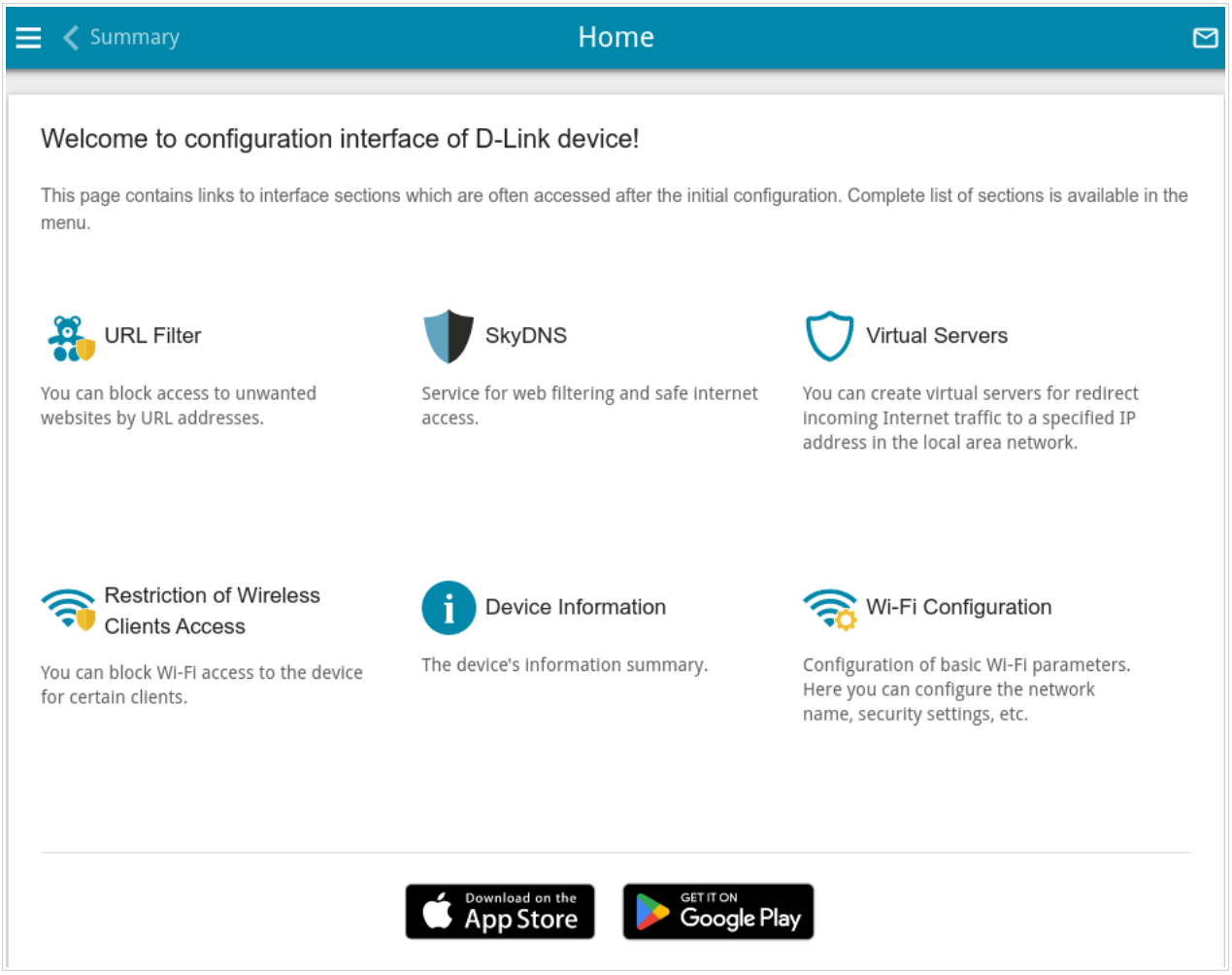

*Figure 28. The **Home** page.*

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 43).

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 66).

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 75).

The pages of the **VPN** section are designed for configuring VPN connections based on IPsec/GRE/EoGRE/EoIP protocols and creating a PPTP or L2TP server and accounts for access to it (for the description of the pages, see the ***VPN*** section, page 121).

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 143).

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 176).

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 184).

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 208).

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 227).

The pages of the **SkyDNS** section are designed for configuring the SkyDNS web content filtering service (for the description of the pages, see the ***SkyDNS*** section, page 254).

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.

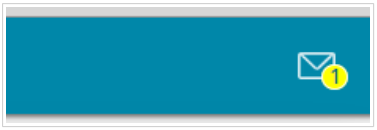

Figure 29. The web-based interface notifications.

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.

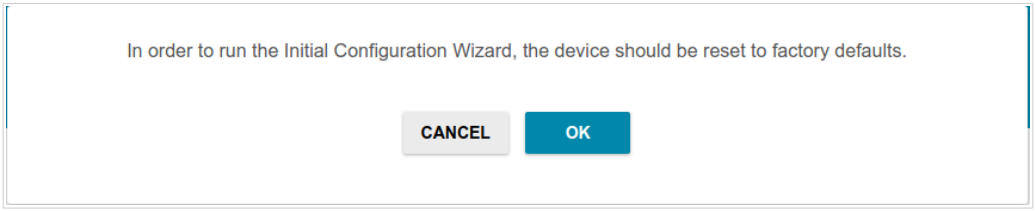

Figure 30. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network **DWR-953** (for operating in the 2.4GHz band) or **DWR-953-5G** (for operating in the 5GHz band) and click the **NEXT** button.

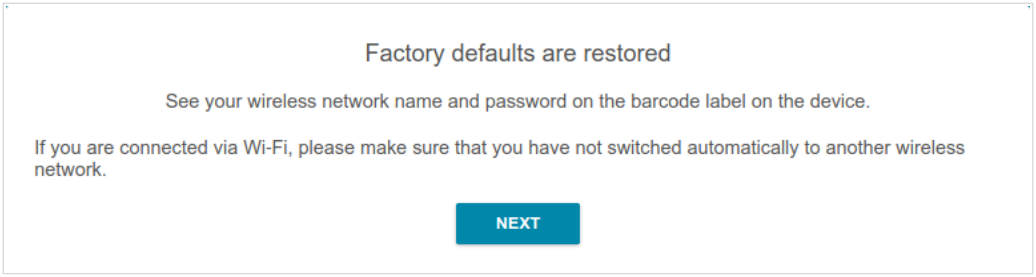

Figure 31. Checking connection to the wireless network.

Click the **START** button.

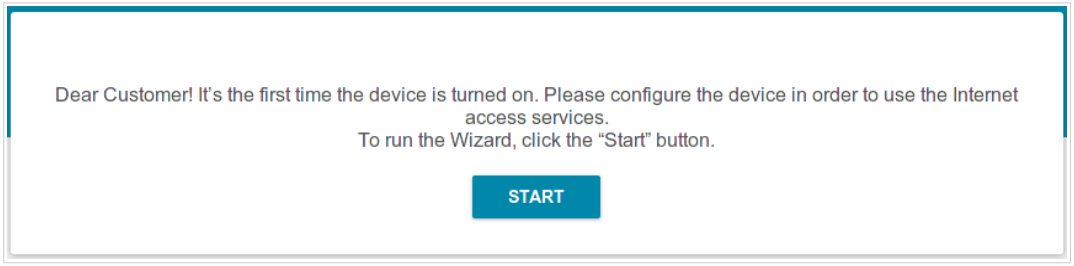

Figure 32. Starting the Wizard.

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

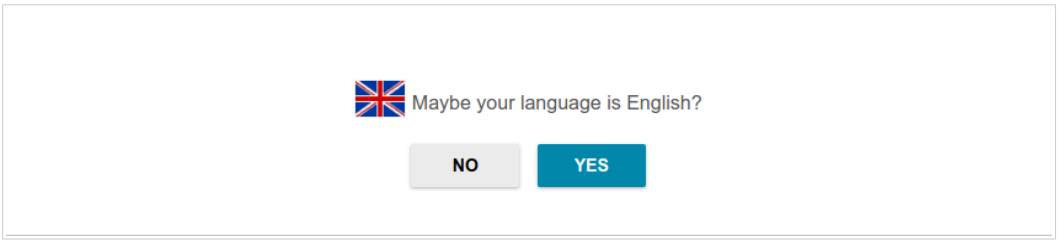

Figure 33. Selecting a language.

You can finish the wizard earlier and go to the menu of the web-based interface. To do this, click the **ADVANCED SETTINGS** button. On the opened page, change the default settings: specify the administrator password in the **User's interface password** and **Password confirmation** and the name of the wireless network in the 2.4GHz and 5GHz bands in the **Network name 2.4 GHz (SSID)** and **Network name 5 GHz (SSID)** fields correspondingly. Then click the **APPLY** button.

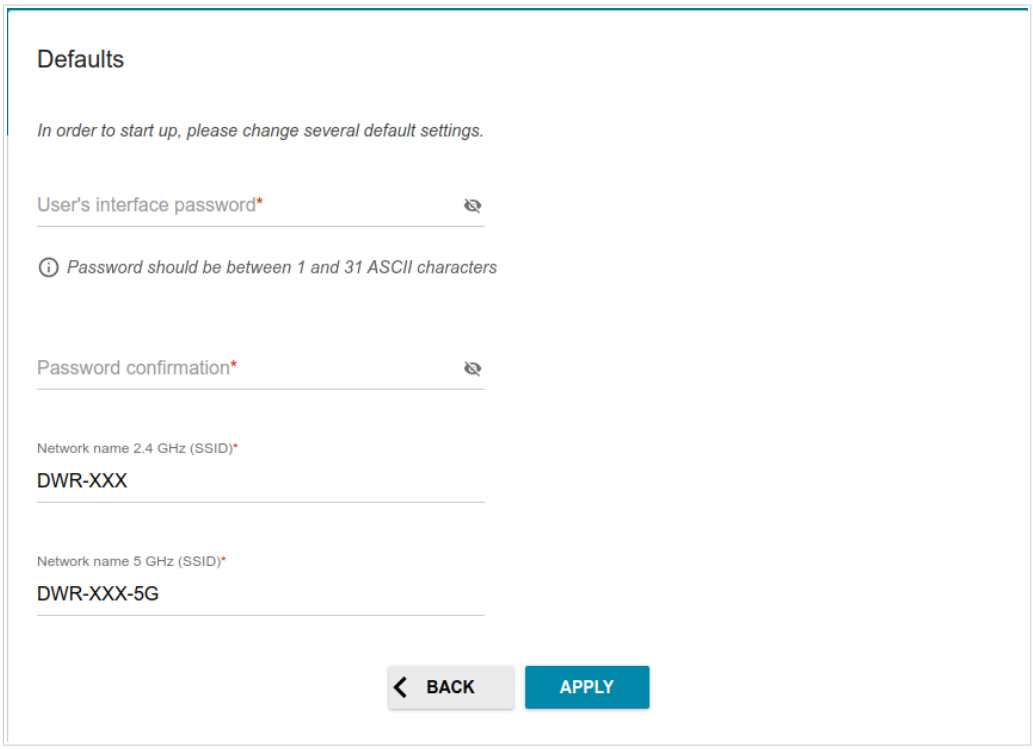

Figure 34. Changing the default settings.

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

Selecting Operation Mode

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

Router

In order to connect your device to a private Ethernet line, on the **Device mode** page, from the **Connection method** list, select the **Ethernet** value. Then from the **Work mode** list, select the **Router** value. In this mode you can configure one of the router's LAN port as the WAN port, configure a WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, configure LAN ports to connect an STB or VoIP phone, and set your own password for access to the web-based interface of the device.

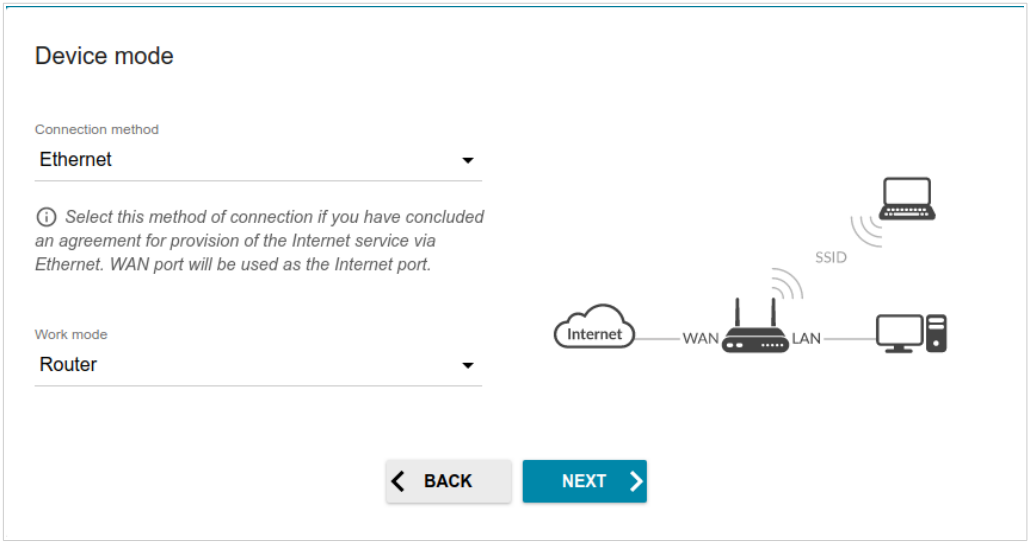

*Figure 35. Selecting an operation mode. The **Router** mode.*

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 **Mobile Internet** value. In this mode you can configure a 3G/LTE WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

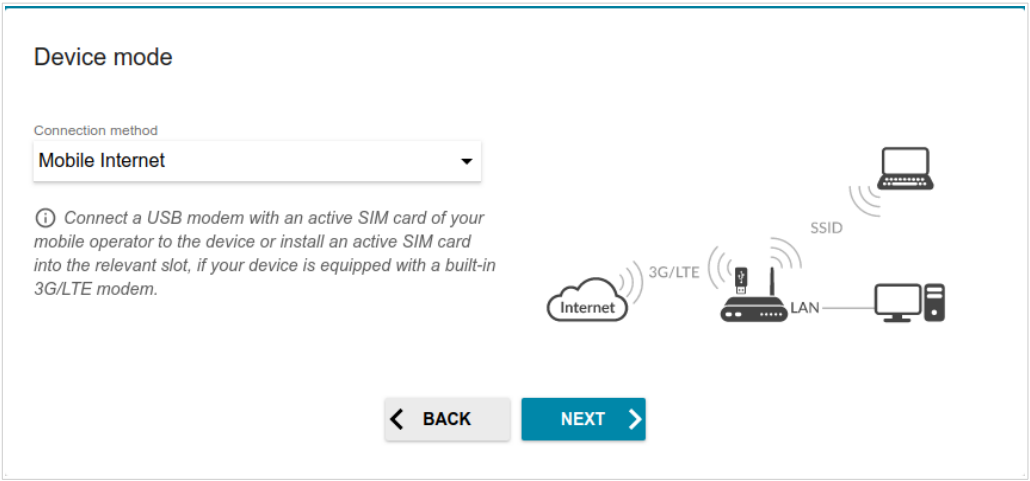

*Figure 36. Selecting an operation mode. The **Mobile Internet** mode.*

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

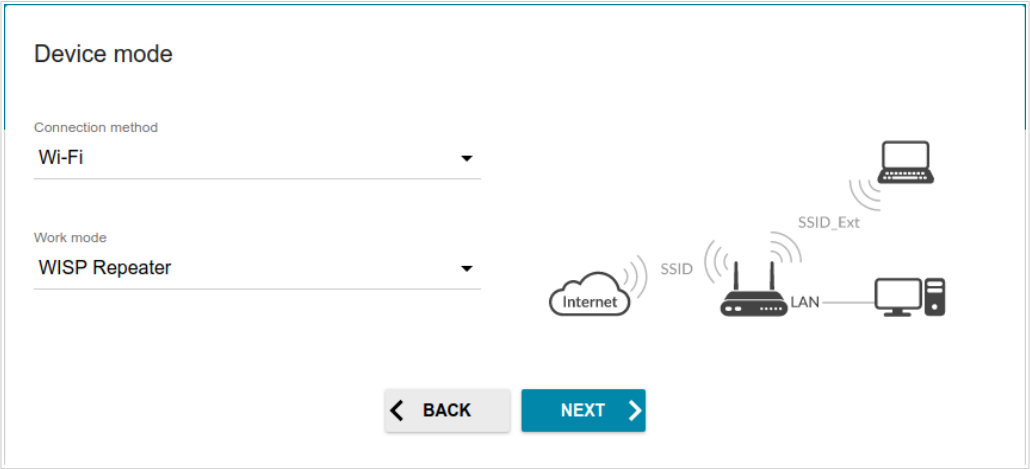

*Figure 37. Selecting an operation mode. The **WISP Repeater** mode.*

Access Point or Repeater

In order to connect your device to a wired router for adding a wireless network to the existing local network, on the **Device mode** page, from the **Connection method** list, select the **Ethernet** value. Then from the **Work mode** list select the **Access point** value. In this mode you can change the LAN IP address, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

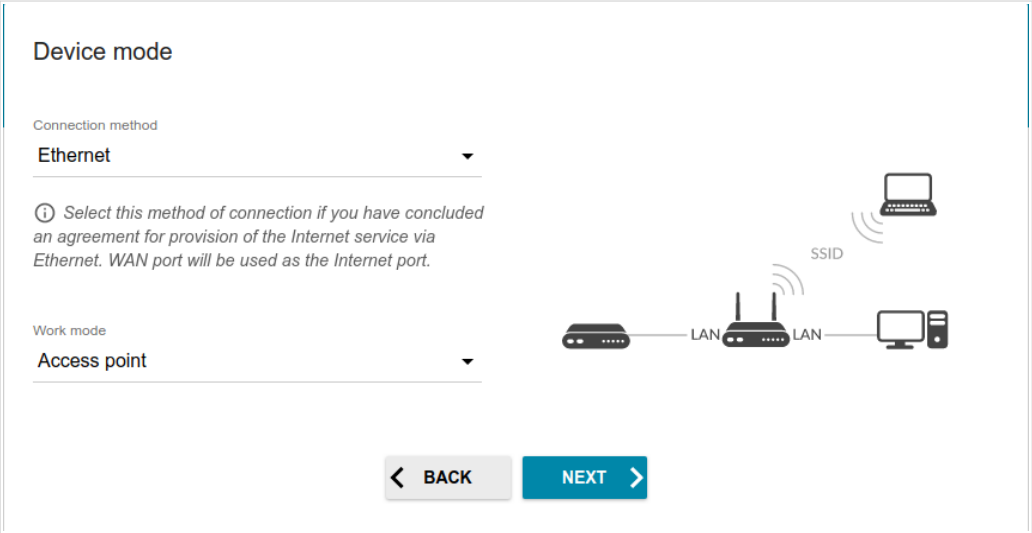

*Figure 38. Selecting an operation mode. The **Access point** mode.*

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

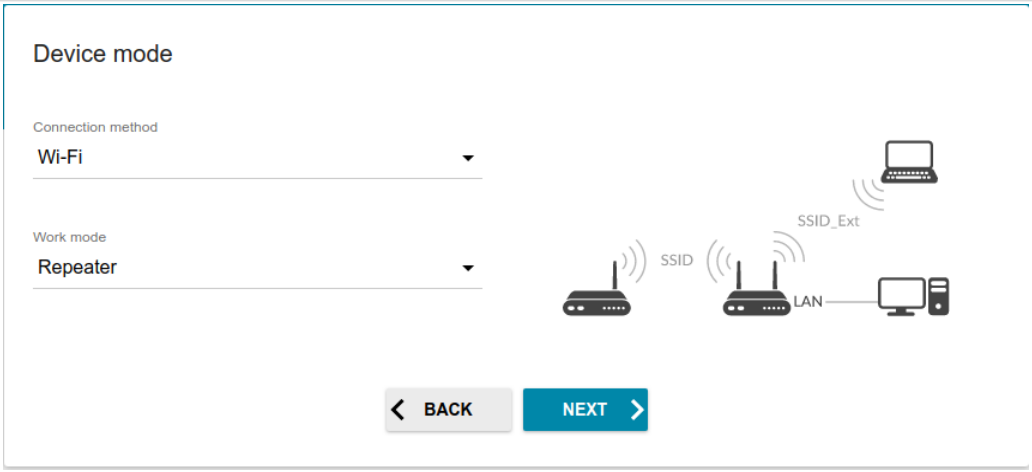

*Figure 39. Selecting an operation mode. The **Repeater** mode.*

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.

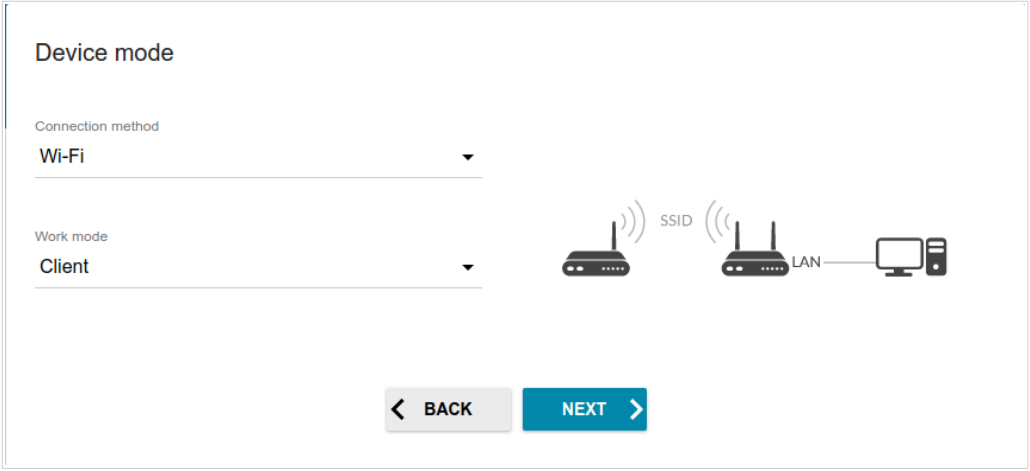

*Figure 40. Selecting an operation mode. The **Client** mode.*

Creating LTE WAN Connection

This configuration step is available for the **Mobile Internet** 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.

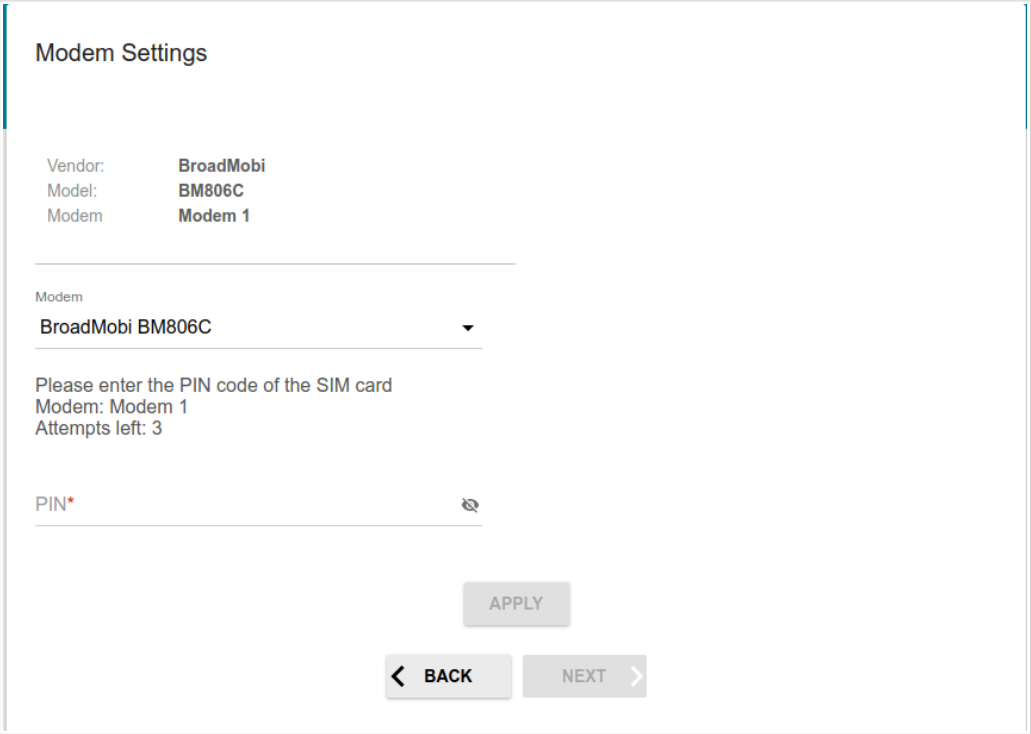

Figure 41. The page for entering the PIN code.

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

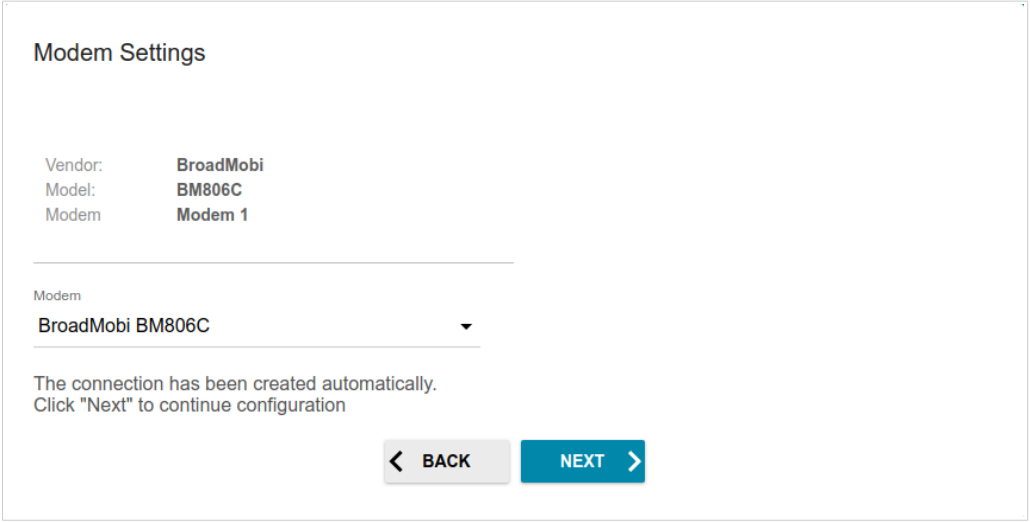

Figure 42. The page for creating LTE connection.

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 **Modem Settings** page, configure all needed settings and click the **NEXT** button.

Configuring LAN Port as WAN Port

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

1. On the **Device connection** page, select a free LAN port which will be used as the WAN port.

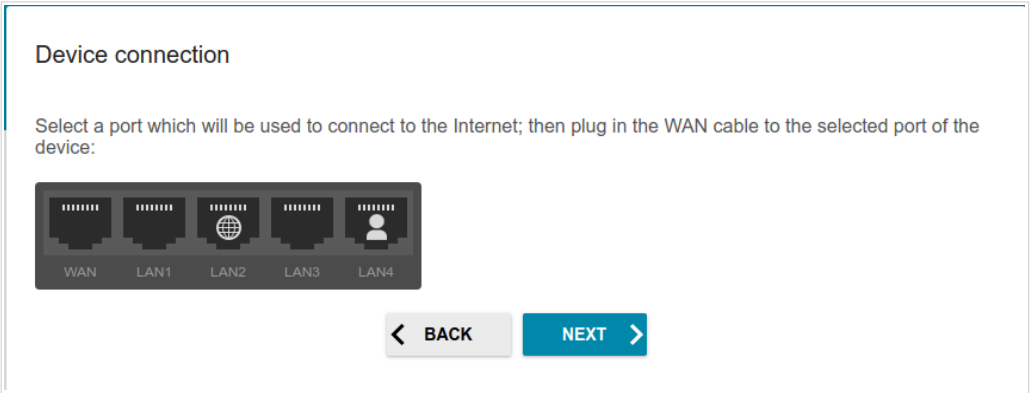

Figure 43. The page for configuring a LAN port as the WAN port.

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

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-953 automatically obtain the LAN IPv4 address.
2. In the **Hostname** field, you should specify a domain name of the router using which you can access the web-based interface after finishing the Wizard. Enter a new domain name of the router ending with `.local` or leave the value suggested by the router.

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

If you want to manually assign the LAN IPv4 address for DWR-953, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Subnet mask**, **DNS IP address, Hostname** fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.

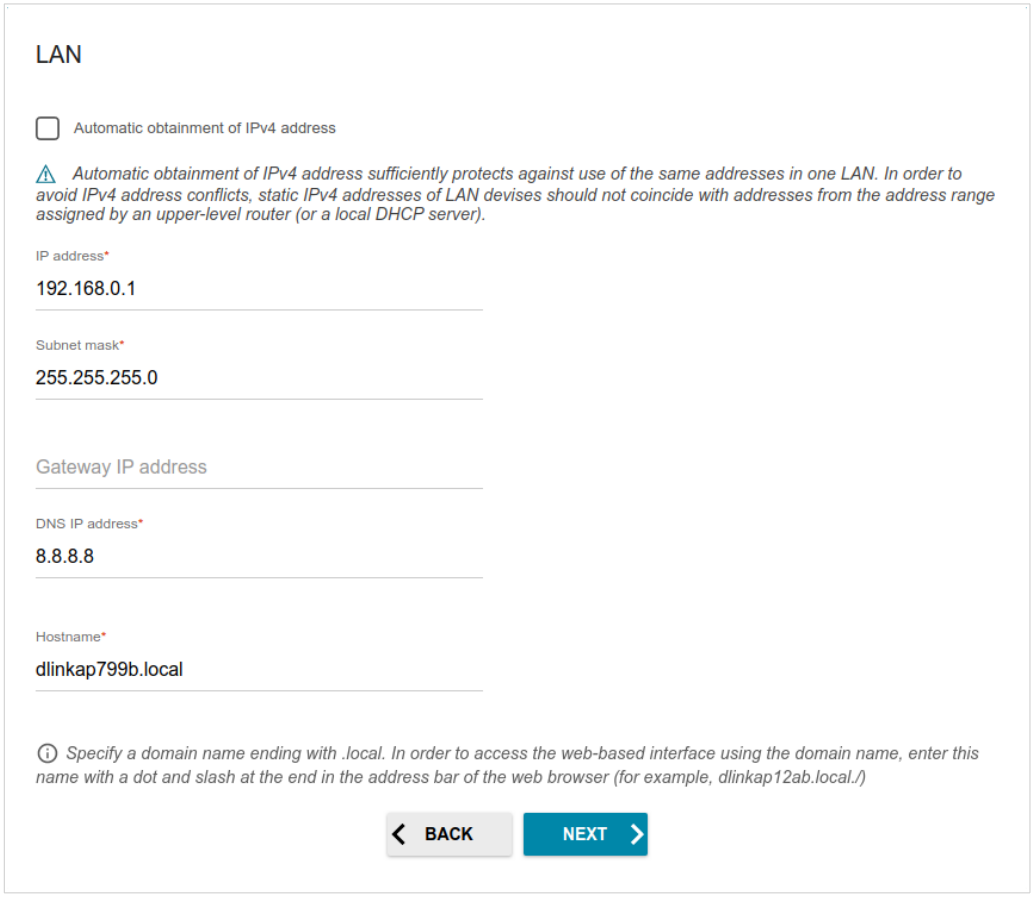

Figure 44. The page for changing the LAN IPv4 address.

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

Wi-Fi Client

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

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

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

2. If a password is needed to connect to the selected network, fill in the relevant field. Click the **Show** icon ( ) to display the entered password.

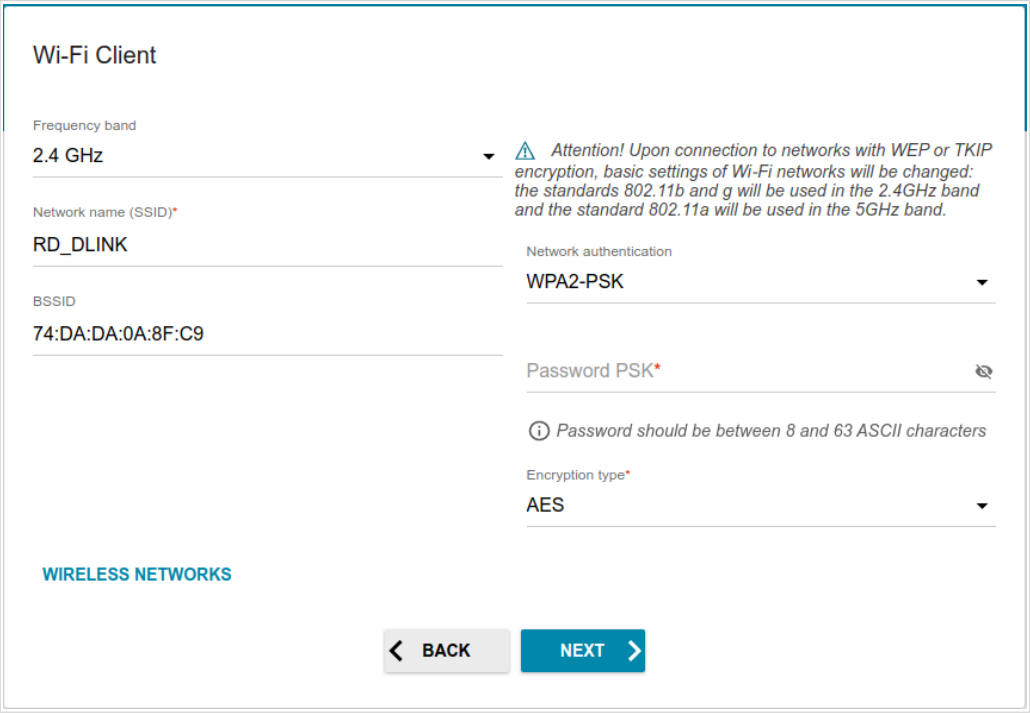

Figure 45. The page for configuring the Wi-Fi client.

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

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

Parameter	Description
Enable encryption WEP	*For **Open** authentication type only.* The checkbox activating WEP encryption. When the checkbox is selected, the **Default key ID** drop-down list, the **Encryption key WEP as HEX** checkbox, and four **Encryption key** fields are displayed on the page.

Parameter	Description
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields. Click the **Show** icon ( ) to display the entered key.

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

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

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, click the **SCAN** button (available for the **Router** mode only) to automatically specify the connection type used by your ISP or manually select the needed value from the **Connection type** list.
2. Specify the settings necessary for the connection of the selected type.
3. If a particular MAC address was registered by your ISP upon concluding the agreement, from the **MAC address assignment method** drop-down list (available for the **Router** mode only), select the **Manual** value and enter this address in the **MAC address** field. Choose the **Clone MAC address of your device** value to place the MAC address of your network interface card in the field, or leave the **Default MAC address** value to place the router's WAN interface MAC address in the field.
4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field (available for the **Router** mode only).
5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Static IPv4 Connection

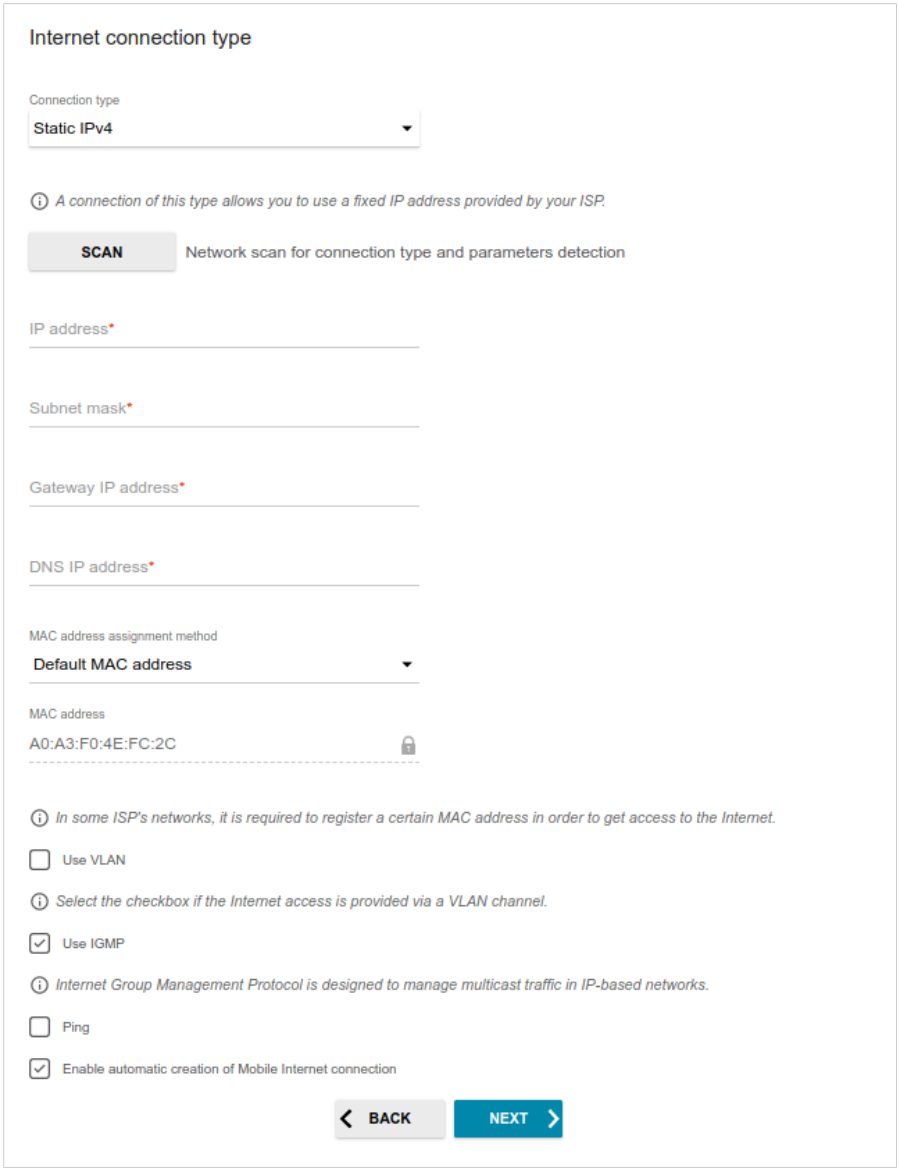

Figure 46. The page for configuring Static IPv4 WAN connection.

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

Static IPv6 Connection

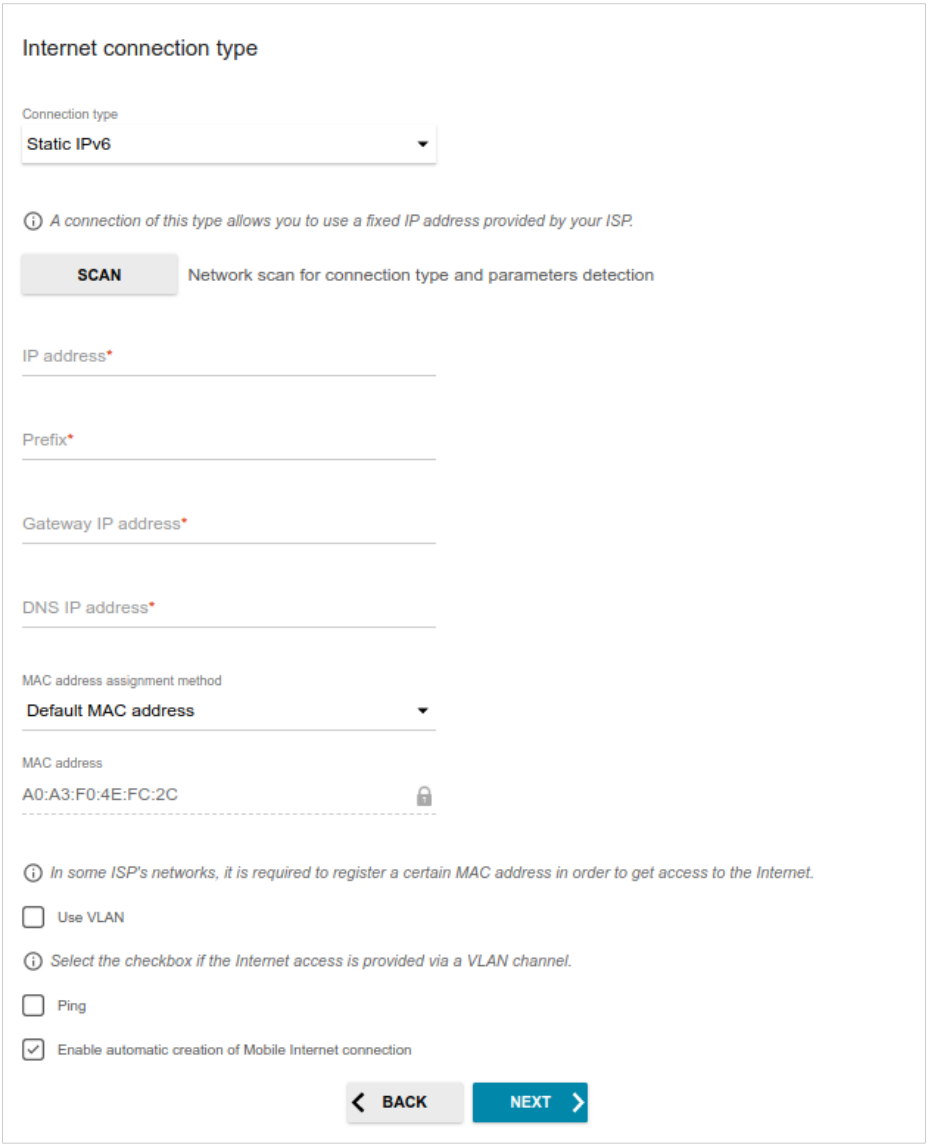

Figure 47. The page for configuring Static IPv6 WAN connection.

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

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

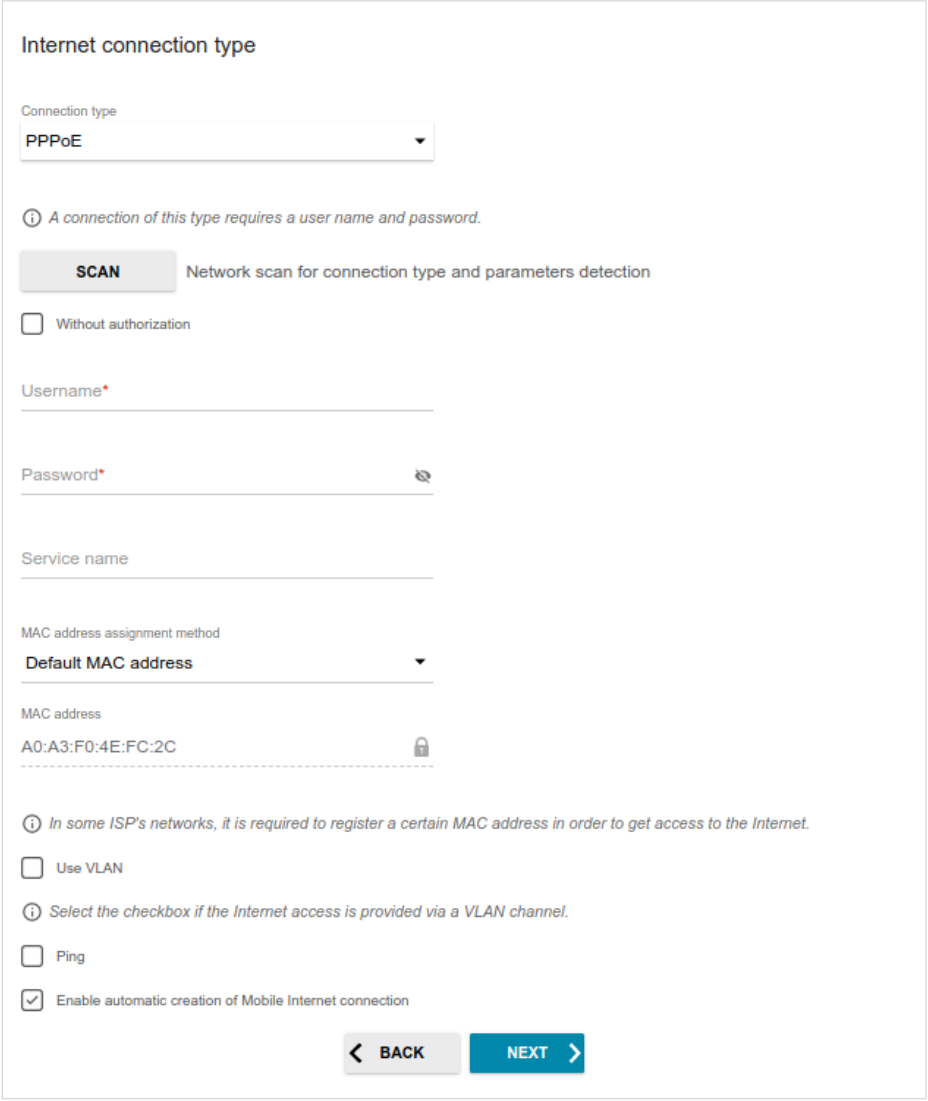

Figure 48. The page for configuring PPPoE WAN connection.

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

PPPoE + Static IP (PPPoE Dual Access) Connection

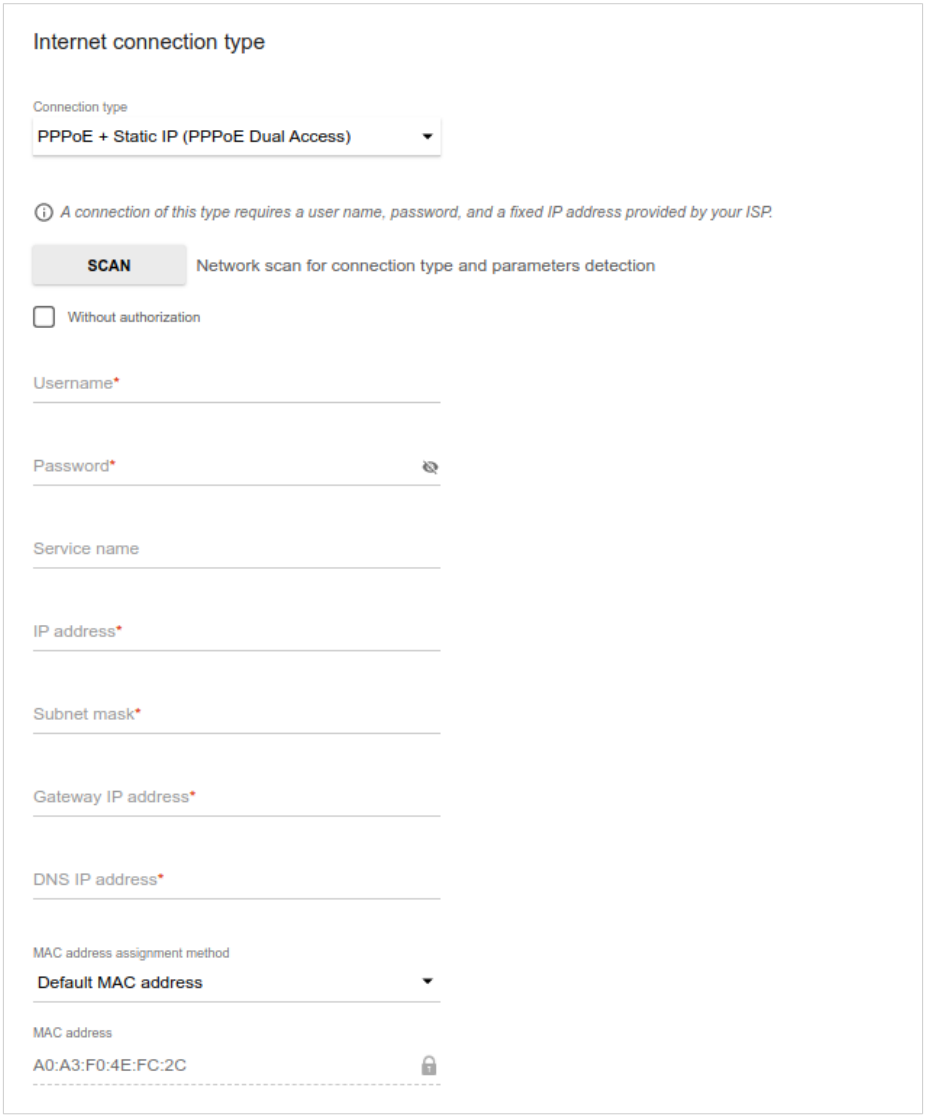

Figure 49. The page for configuring PPPoE + Static IP (PPPoE Dual Access) WAN connection.

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

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

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

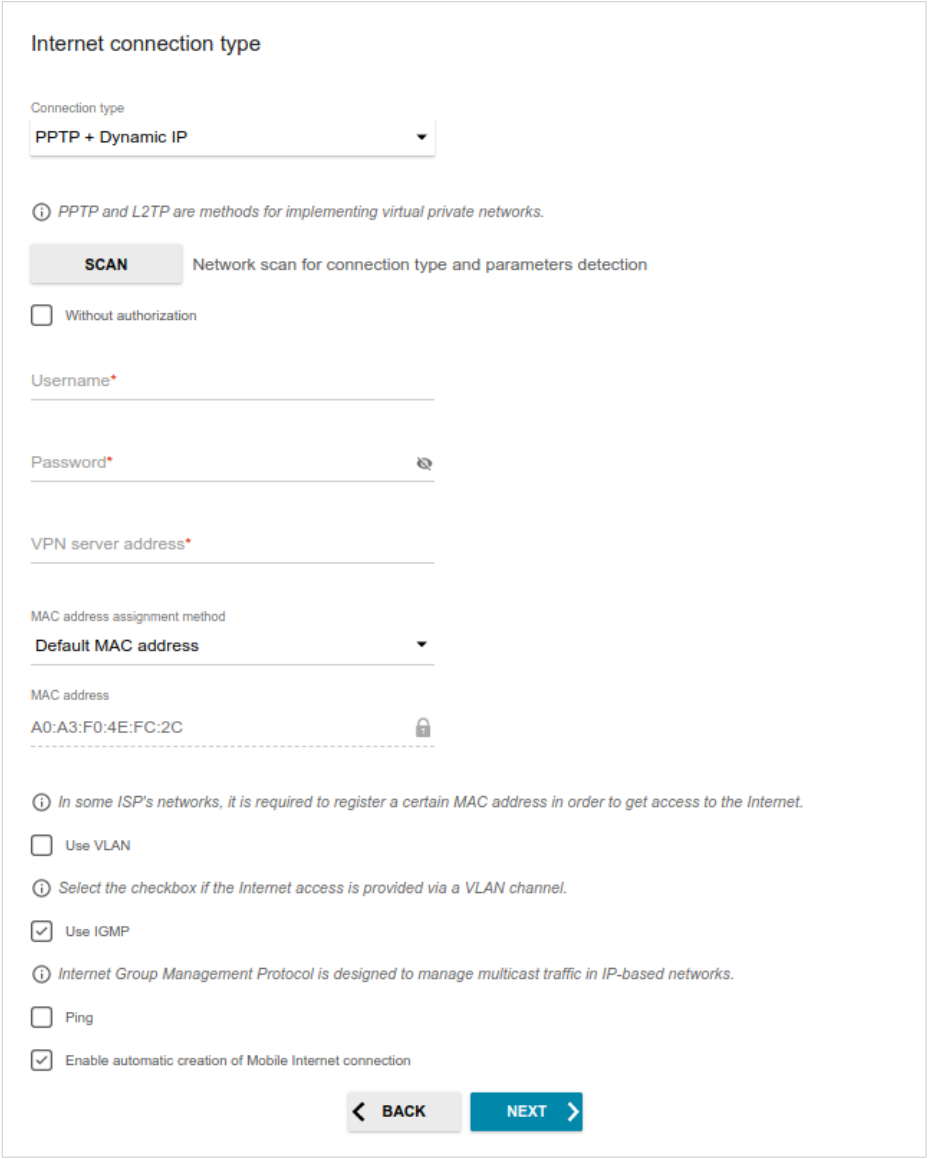

Figure 50. The page for configuring PPTP + Dynamic IP WAN connection.

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

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

PPTP + Static IP or L2TP + Static IP Connection

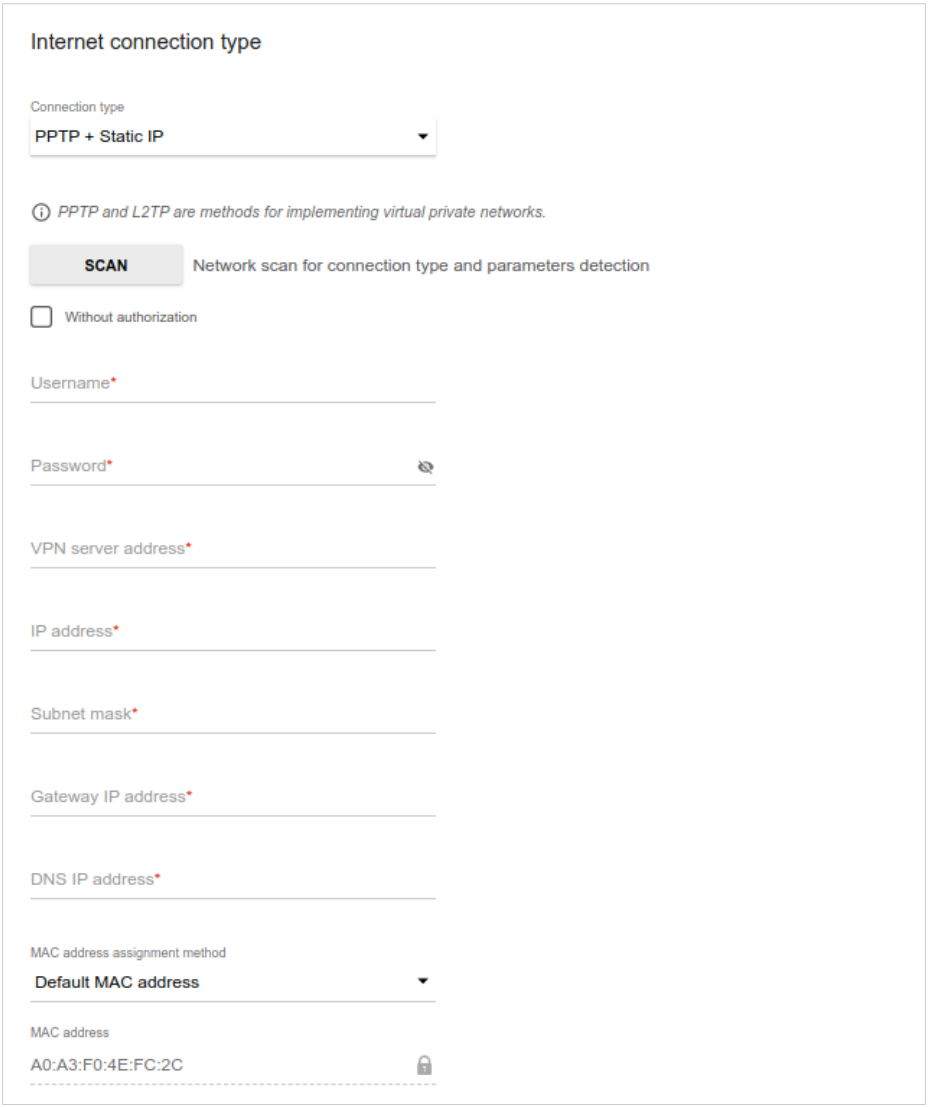

Figure 51. The page for configuring PPTP + Static IP WAN connection.

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

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

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

Configuring Wireless Network

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

1. On the **Wireless Network 2.4 GHz** page, in the **Network name** field, specify your own name for the wireless network in the 2.4GHz band or leave the value suggested by the router.
2. In the **Password** field, specify your own password for access to the wireless network or leave the value suggested by the router (WPS PIN of the device, see the barcode label).
3. If the router is used as a Wi-Fi client, you can specify the same parameters of the wireless network as specified for the network to which you are connecting. To do this, click the **USE** button (available for the **WISP Repeater** and **Repeater** modes only).
4. You can restore the parameters of the wireless network specified before resetting to factory defaults. To do this, click the **RESTORE** button.

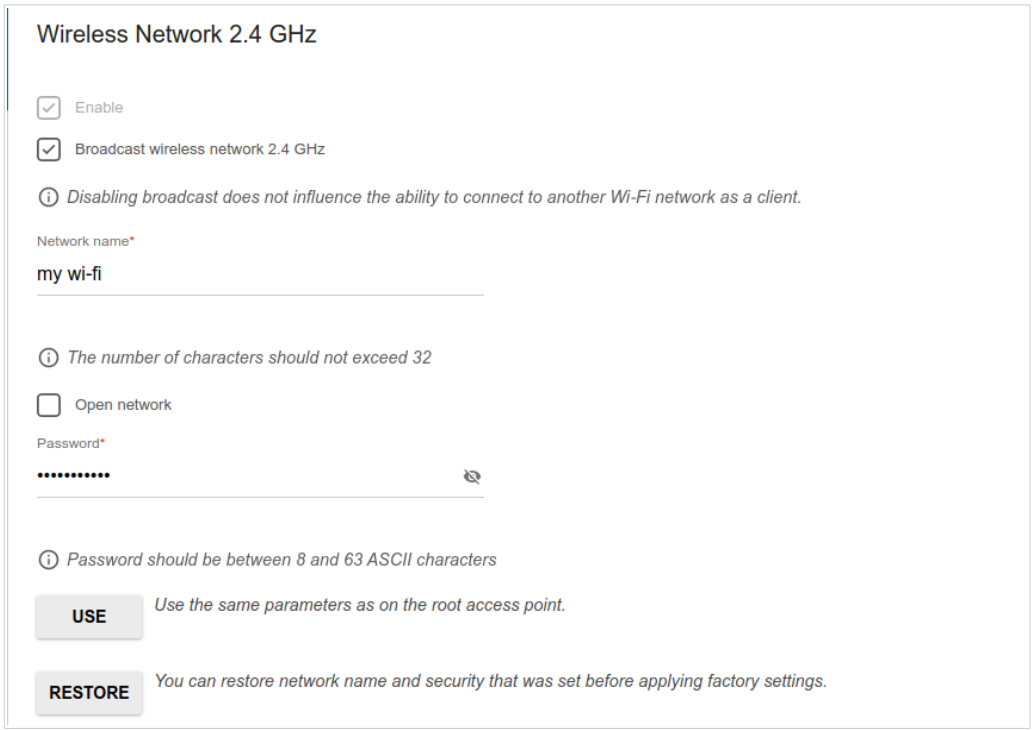

Figure 52. The page for configuring the wireless network.

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

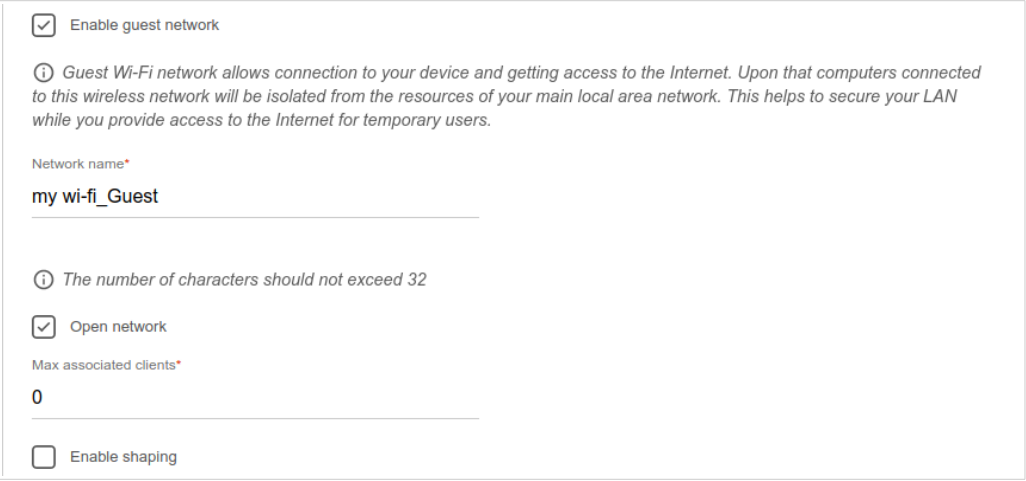

Figure 53. The page for configuring the wireless network.

6. In the **Network name** field, specify your own name for the guest wireless network or leave the value suggested by the router.
7. If you want to create a password for access to the guest wireless network, deselect the **Open network** checkbox and fill in the **Password** field.
8. If you want to limit the bandwidth of the guest wireless network, select the **Enable shaping** checkbox and fill in the **Shaping** field.
9. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.
10. On the **Wireless Network 5 GHz** page, specify needed settings for the wireless network in the 5GHz band and click the **NEXT** button.

Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **User's interface password** and **Password confirmation** fields. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[6]

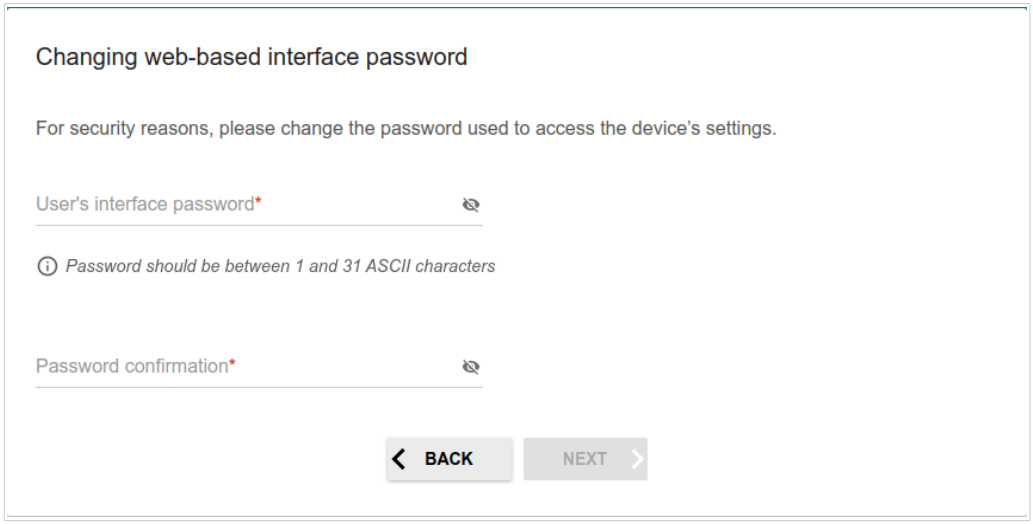

Figure 54. The page for changing the web-based interface password.

! 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.

6 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.

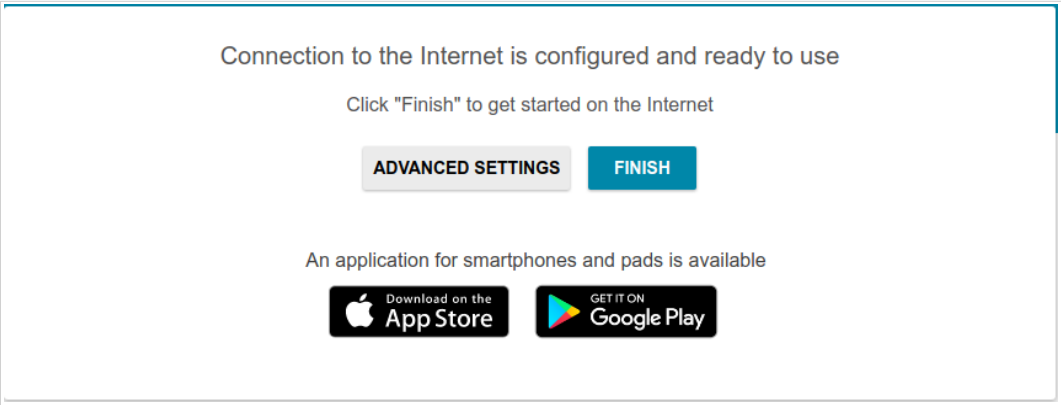

Figure 55. Checking the Internet availability.

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 40).

Statistics

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

- network statistics
- IP addresses leased by the DHCP server
- the routing rules and routing tables
- data on devices connected to the router's network and its web-based interface, and information on current sessions of these devices
- statistics for traffic passing through ports of the router
- addresses of active multicast groups
- statistics for IPsec tunnels of the router
- the list of clients connected to the PPTP or L2TP server of the router.

Network Statistics

On the **Statistics / Network Statistics** page, you can view statistics for all connections existing in the system (WAN connections, LAN, WLAN). For each connection the following data are displayed: name and state (when the connection is on, its name is highlighted in green, when the connection is off, its name is highlighted in red), IP address and subnet mask, and volume of data received and transmitted (with increase of the volume the units of measurement are changed automatically: byte, Kbyte, Mbyte, Gbyte).

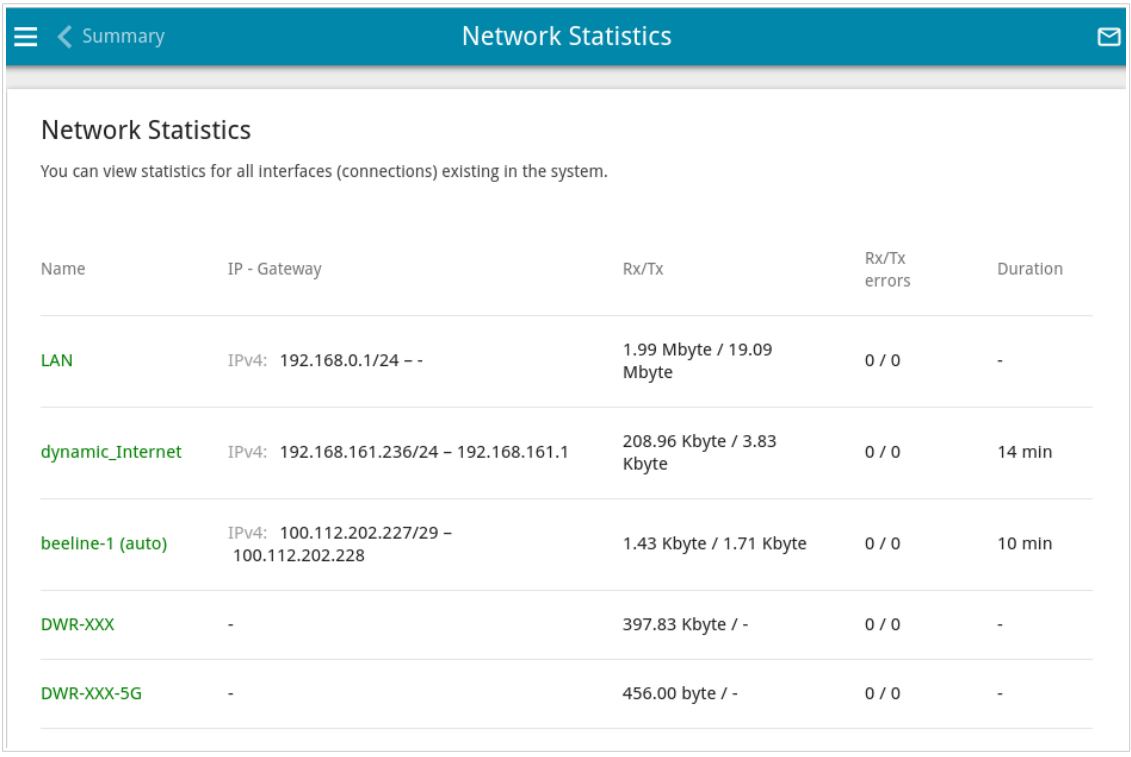

*Figure 56. The **Statistics / Network Statistics** page.*

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

DHCP

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

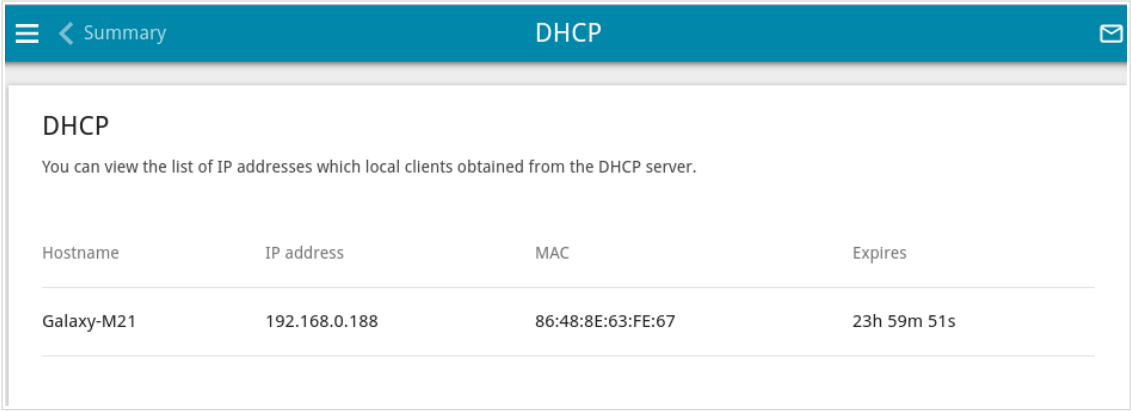

*Figure 57. The **Statistics / DHCP** page.*

Routing

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

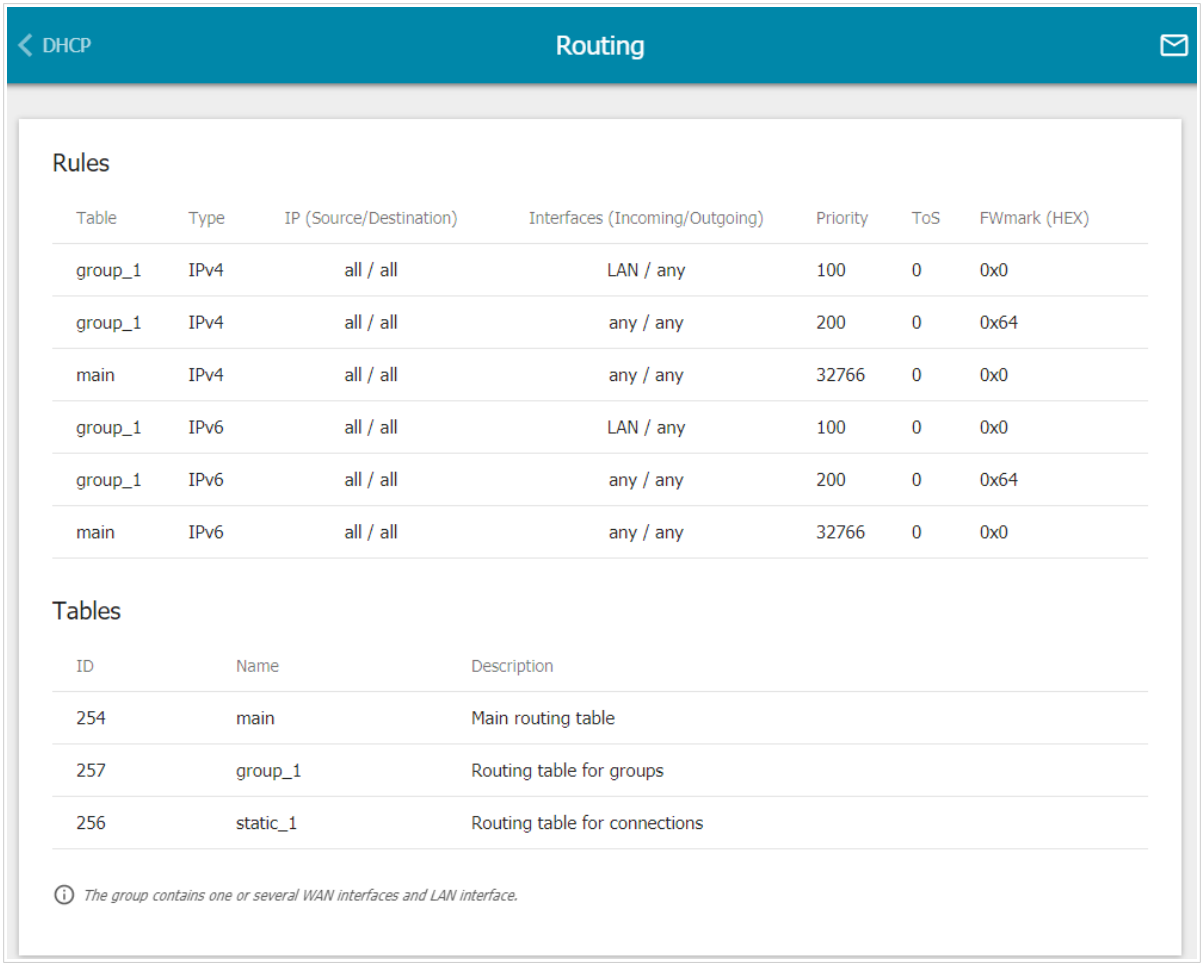

*Figure 58. The **Statistics / Routing** page.*

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

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

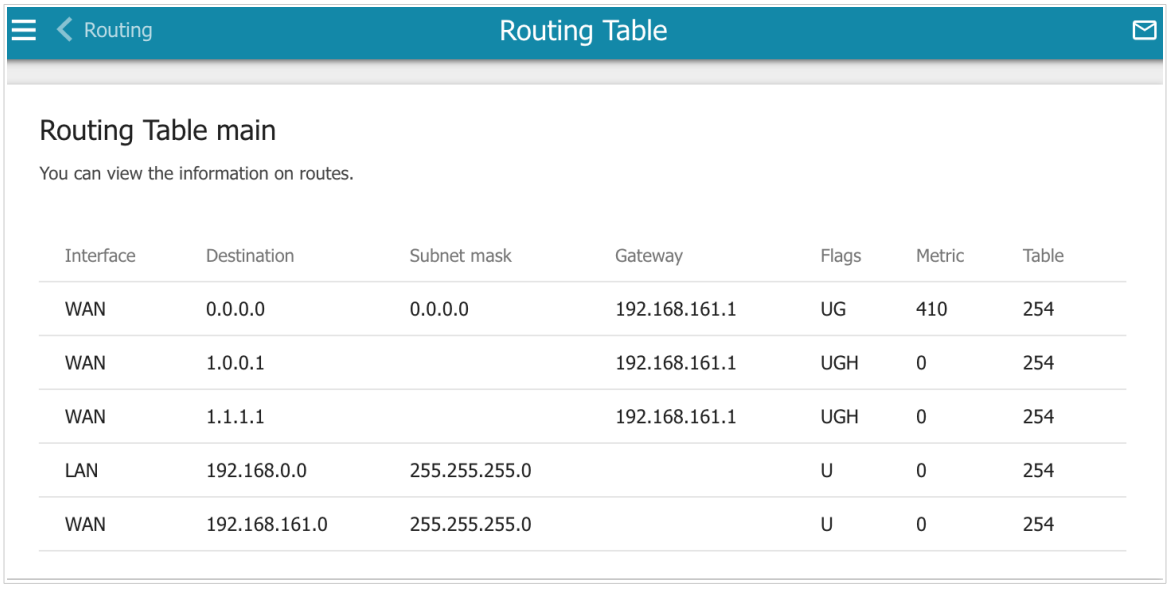

Figure 59. The routing table page.

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

Clients and Sessions

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

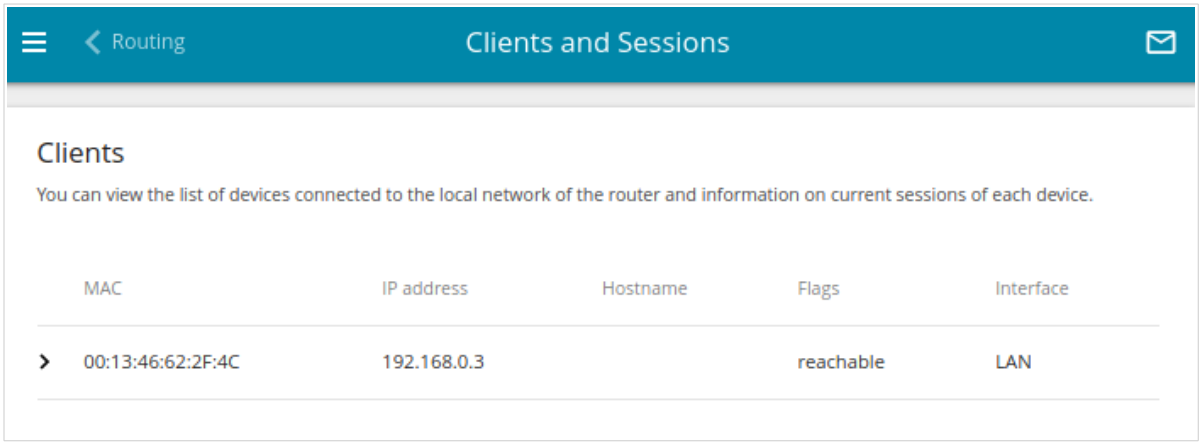

*Figure 60. The **Statistics / Clients and Sessions** page.*

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

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

Port Statistics

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

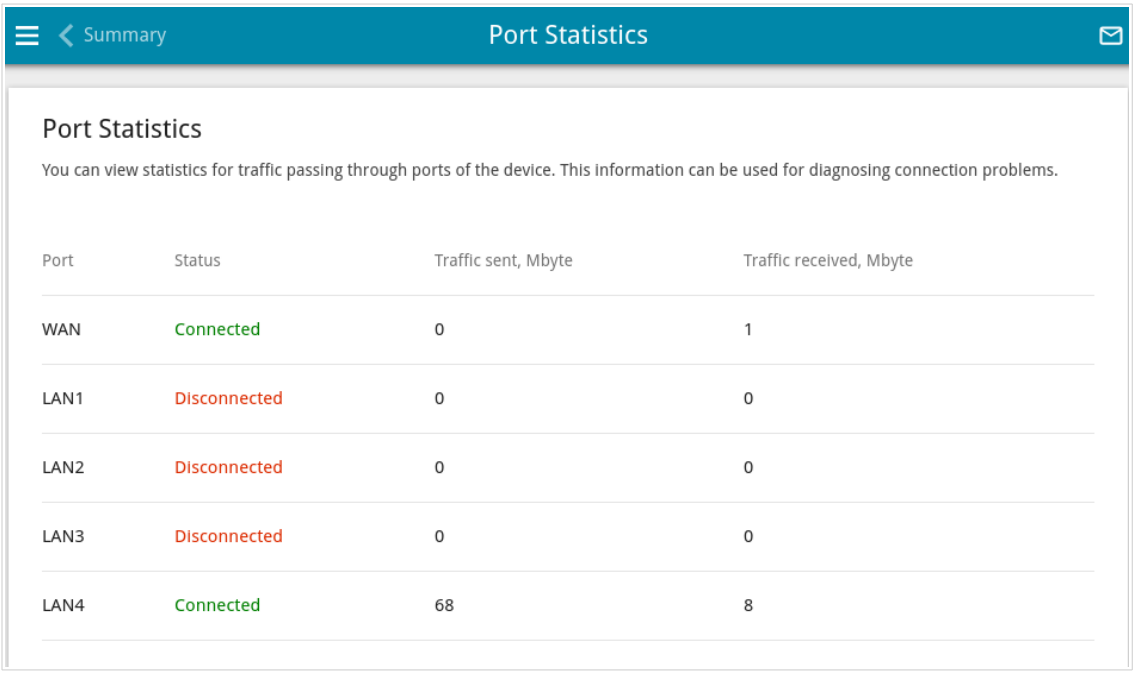

*Figure 61. The **Statistics / Port Statistics** page.*

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

Multicast Groups

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

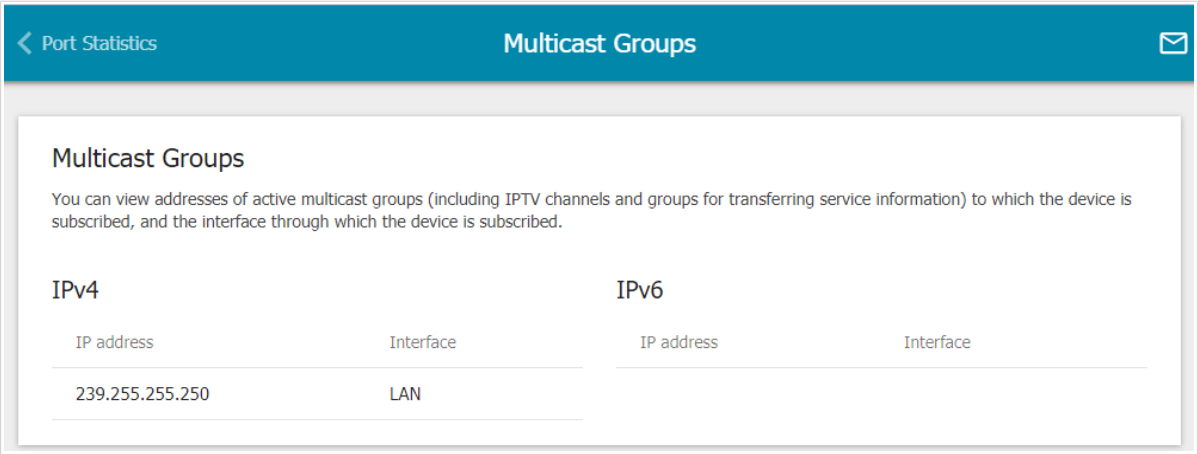

*Figure 62. The **Statistics / Multicast Groups** page.*

IPsec Statistics

On the **Statistics / IPsec Statistics** page, you can view statistics for IPsec tunnels of the router. For each tunnel the following data are displayed: name and state (when the connection is on, its name is highlighted in green, when the connection is off, its name is highlighted in red), remote host address or domain name, operation mode and connection type, and number of packets and volume of data received and transmitted.

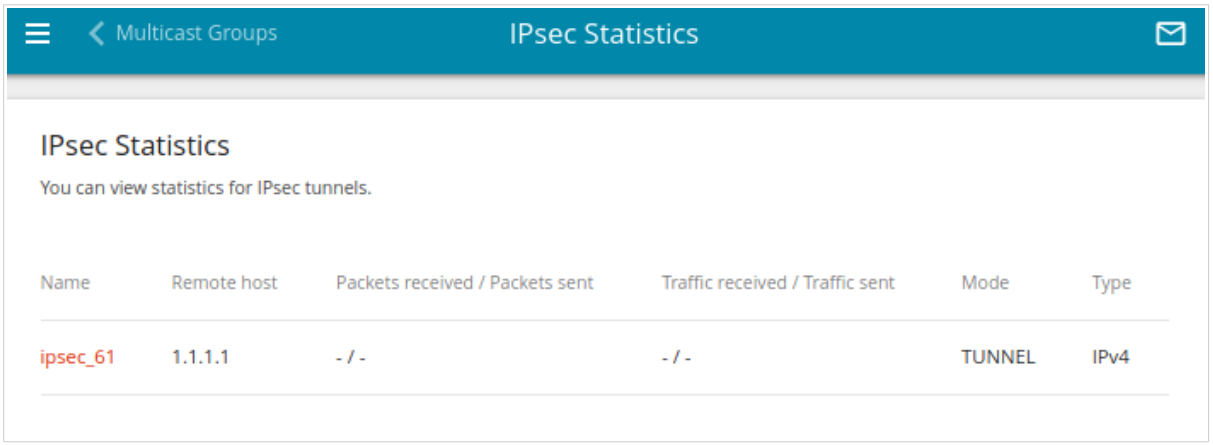

*Figure 63. The **Statistics / IPsec Statistics** page.*

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

VPN Statistics

On the **Statistics / VPN Statistics** page, you can view the list of clients connected to the PPTP or L2TP server of the router.

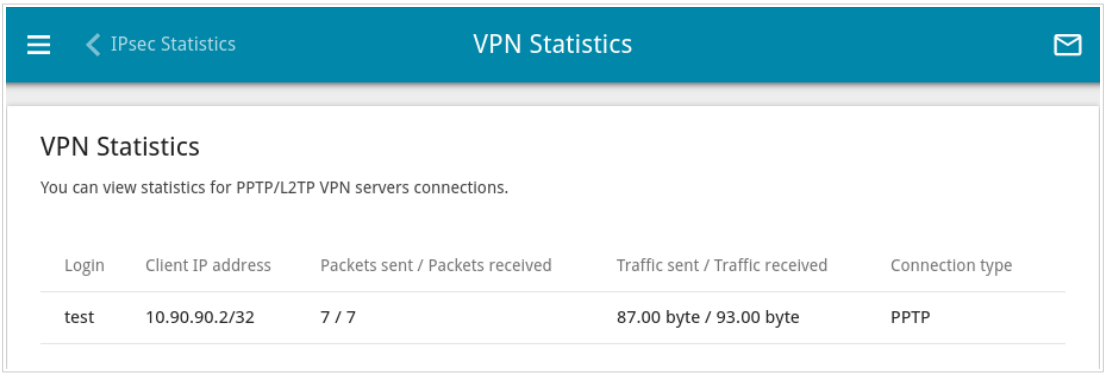

*Figure 64. The **Statistics / VPN Statistics** page.*

For each VPN client the following data are displayed: the unique IP address, username, connection type, and number of packets and volume of data received and transmitted.

To view detailed data on a connected VPN client, click the line corresponding to this client.

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.

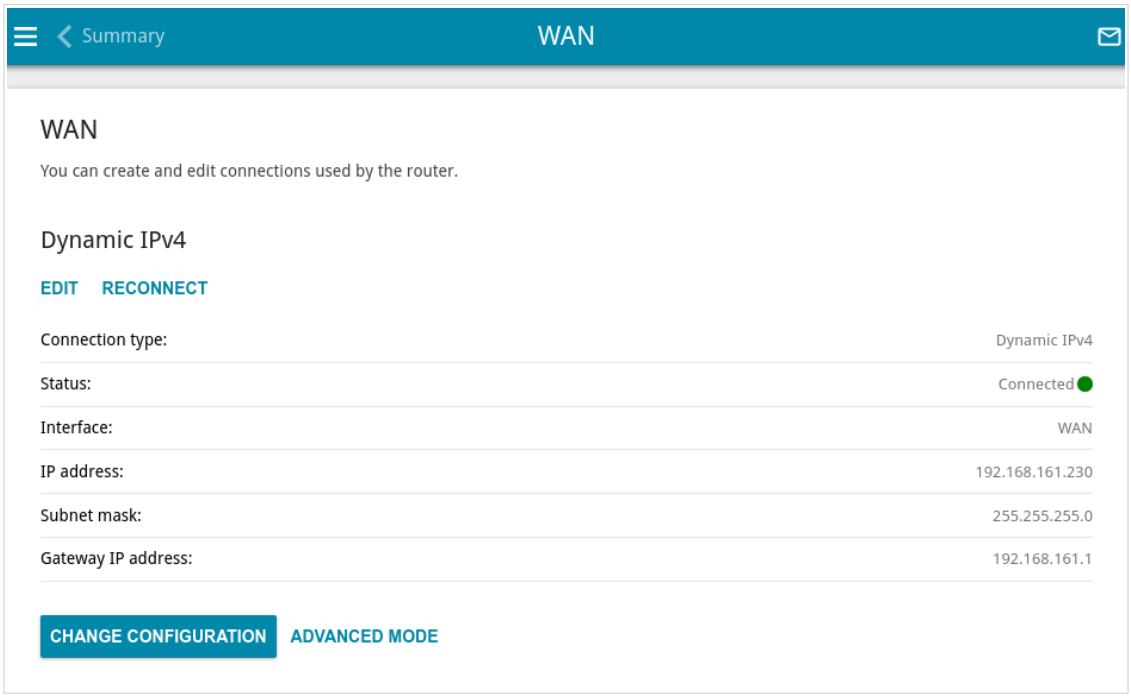

*Figure 65. The **Connections Setup / WAN** page. The simplified mode.*

To edit an existing connection, click the **EDIT** button. On the opened page, change the needed parameters and click the **APPLY** button.

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

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

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

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

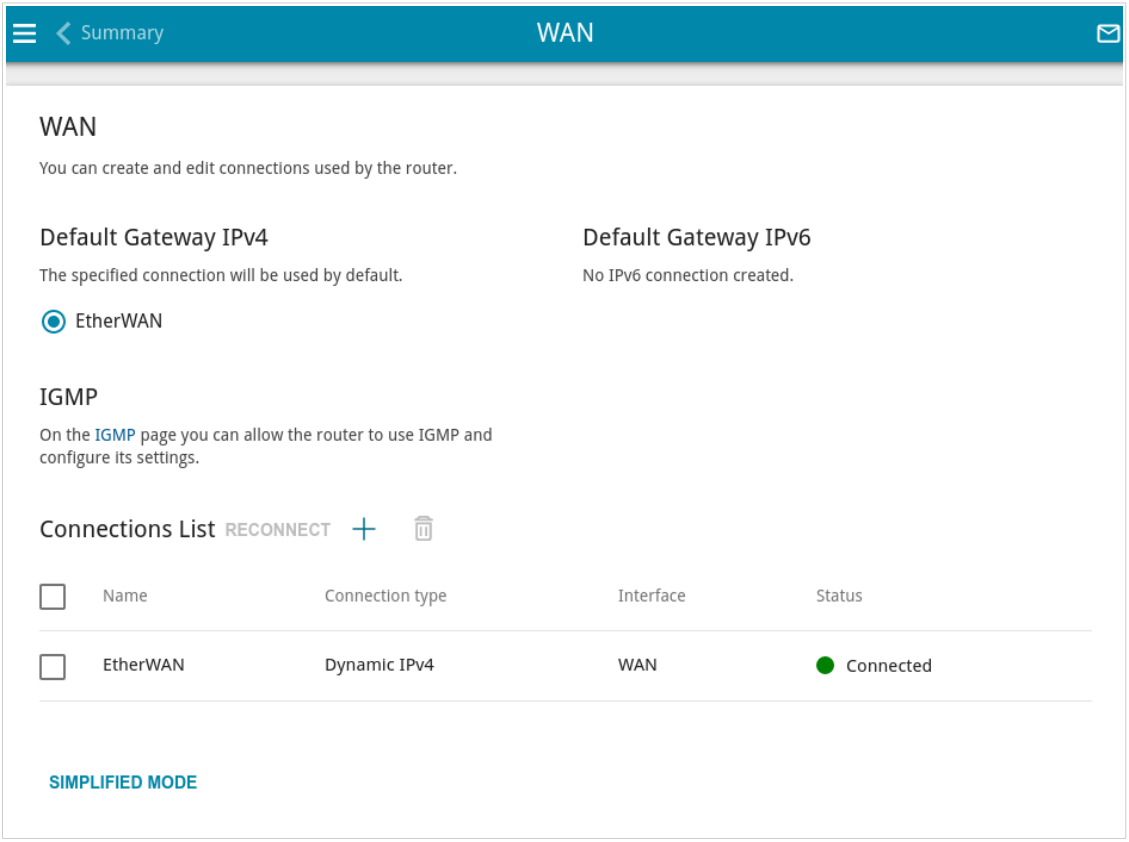

*Figure 66. The **Connections Setup / WAN** page. The advanced mode.*

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

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

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

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

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP** link (for the description of the page, see the ***IGMP*** section, page 205).

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

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

Creating Dynamic IPv4 or Static IPv4 WAN Connection

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

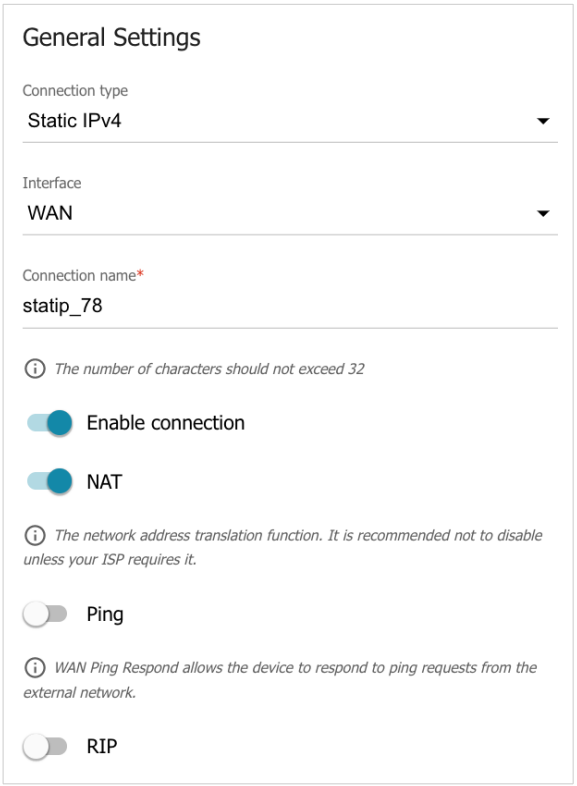

*Figure 67. The page for creating a new **Static IPv4** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.

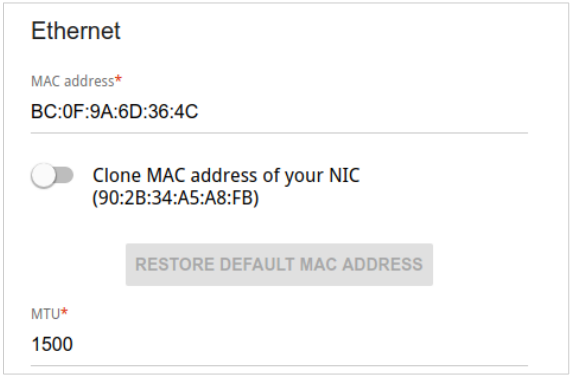

*Figure 68. The page for creating a new **Static IPv4** connection. The **Ethernet** section.*

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

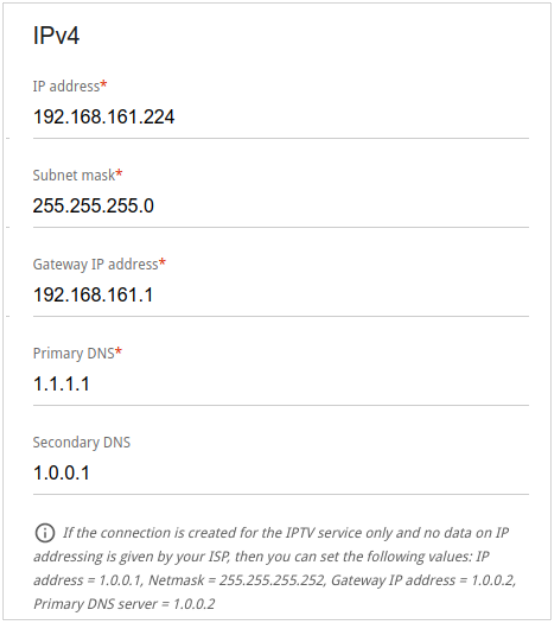

*Figure 69. The page for creating a new **Static IPv4** connection. The **IPv4** section.*

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

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

Creating Dynamic IPv6 or Static IPv6 WAN Connection

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

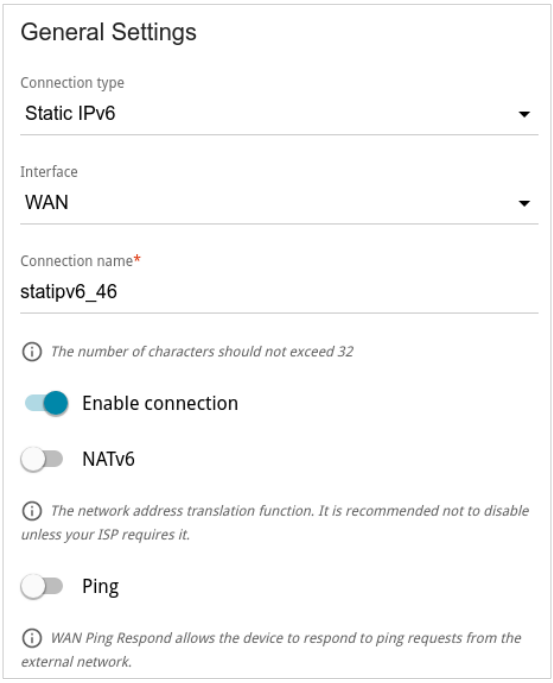

*Figure 70. The page for creating a new **Static IPv6** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NATv6	If the switch is moved to the right, the network address translation function for IPv6 is enabled. Do not disable the function unless your ISP requires this.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

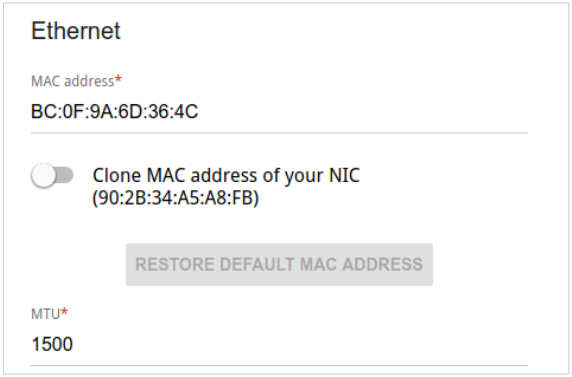

*Figure 71. The page for creating a new **Static IPv6** connection. The **Ethernet** section.*

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

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

Parameter	Description
IPv6	
*For **Static IPv6** type*	
IPv6 address	Enter an IPv6 address for this WAN connection.
Prefix	The length of the subnet prefix. The value **64** is used usually.
Gateway IPv6 address	Enter an IPv6 address of the gateway used by this WAN connection.
Primary IPv6 DNS server / Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
*For **Dynamic IPv6** type*	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.
Enable prefix delegation	From the drop-down list, select the mode of a prefix request from a delegating DHCPv6 server to configure a range of IPv6 addresses for the local network. • **None**: The mode without prefix request. • **Auto**: The mode with the ability to request a prefix. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is not mandatory to establish the connection. • **Force**: The mode with forced prefix request. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is mandatory to establish the connection.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.
Primary IPv6 DNS server / Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.

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

Creating PPPoE WAN Connection

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

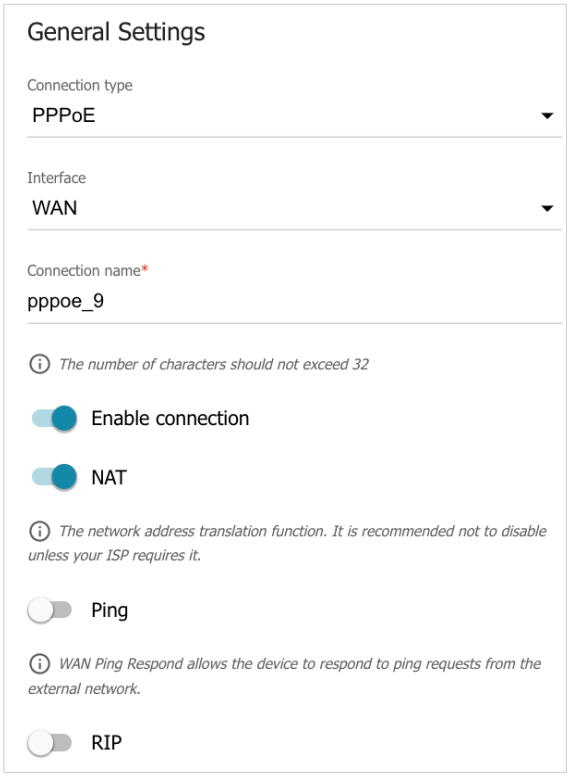

*Figure 73. The page for creating a new **PPPoE** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.

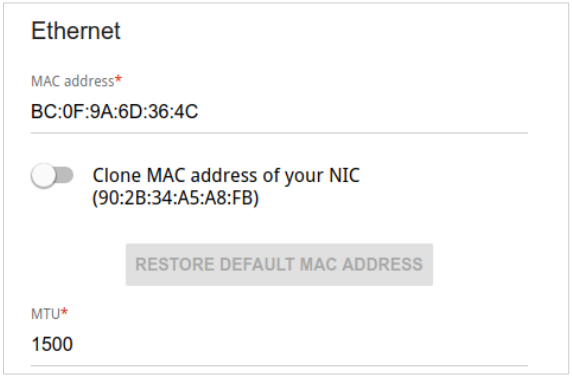

*Figure 74. The page for creating a new **PPPoE** connection. The **Ethernet** section.*

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

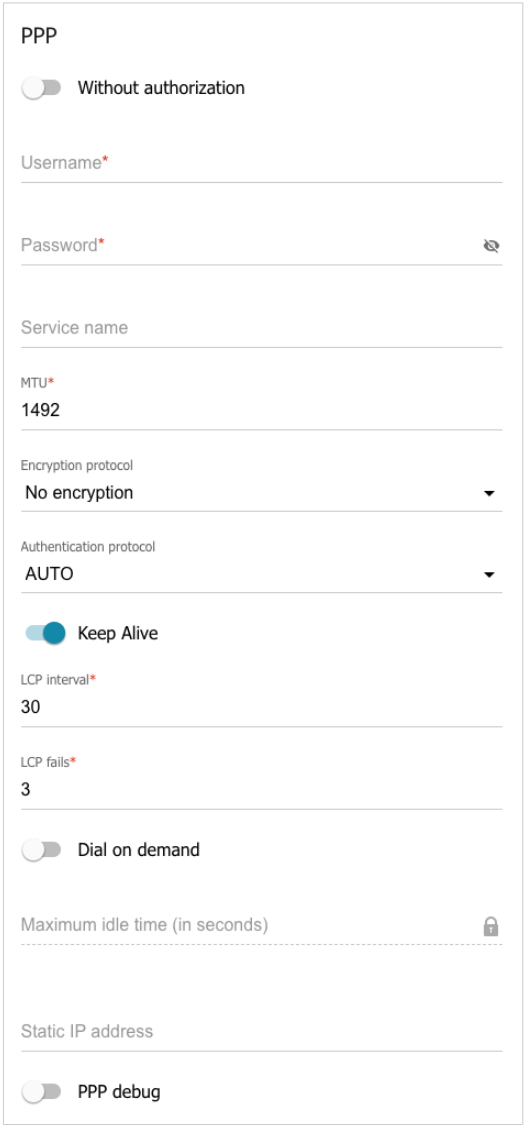

*Figure 75. The page for creating a new **PPPoE** connection. The **PPP** section.*

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

Parameter	Description
Encryption protocol	Select a method of MPPE encryption. • **No encryption**: MPPE encryption is not applied. • **MPPE 40 128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied. • **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied. • **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the **MS-CHAP, MS-CHAPv2**, or **AUTO** value is selected from the **Authentication protocol** drop-down list.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

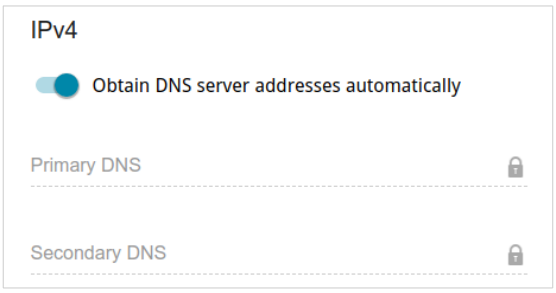

*Figure 76. The page for creating a new **PPPoE** connection. The **IPv4** section.*

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

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

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

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

Creating PPTP, L2TP, or L2TP over IPsec WAN Connection

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

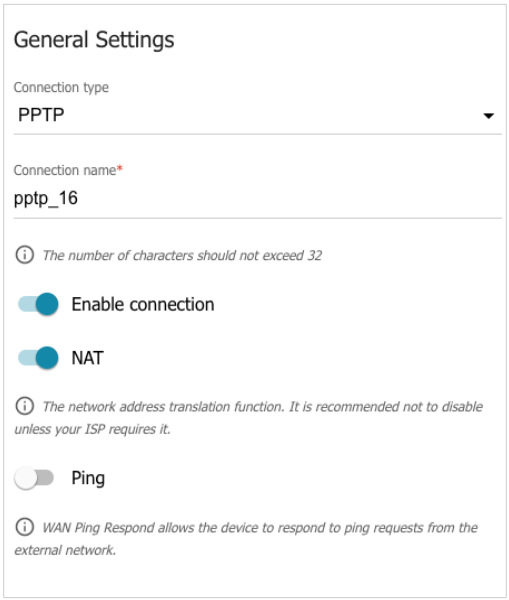

*Figure 77. The page for creating a new **PPTP** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Ping	*For the **PPTP** and **L2TP** types only.* 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.

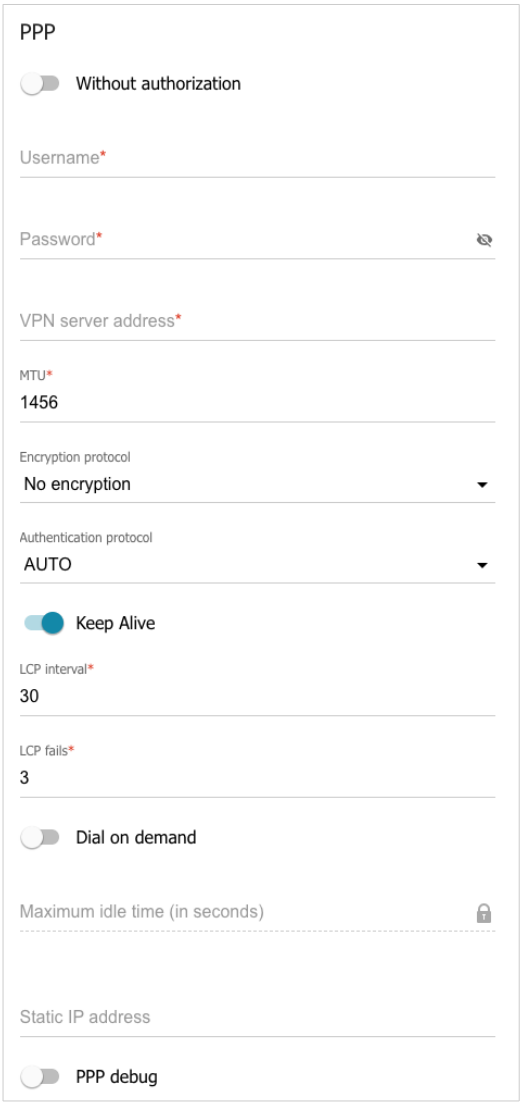

*Figure 78. The page for creating a new **PPTP** connection. The **PPP** section.*

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

Parameter	Description
Encryption protocol	Select a method of MPPE encryption. • **No encryption**: MPPE encryption is not applied. • **MPPE 40 128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied. • **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied. • **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the **MS-CHAP**, **MS-CHAPv2**, or **AUTO** value is selected from the **Authentication protocol** drop-down list.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

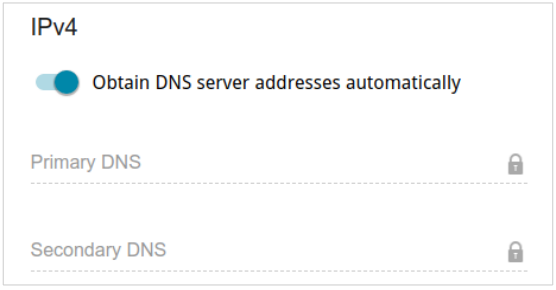

*Figure 79. The page for creating a new **PPTP** connection. The **IPv4** section.*

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

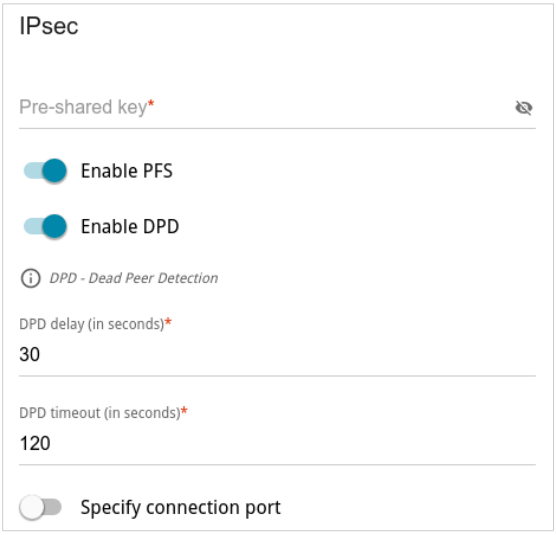

*Figure 80. The page for creating a new **L2TP over IPsec** connection. The **IPsec** section.*

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

Parameter	Description
IPsec *(for the **L2TP over IPsec** type)*	
Pre-shared key	A key for mutual authentication of the parties. Click the **Show** icon ( ) to display the entered key.
Enable PFS	Move the switch to the right to enable the PFS option (*Perfect Forward Secrecy*). If the switch is moved to the right, a new encryption key exchange will be used upon establishing the IPsec tunnel. This option enhances the security level of data transfer, but increases the load on DWR-953.
Enable DPD	Move the switch to the right to enable using DPD protocol for this tunnel. Such a setting allows to check the status of the remote host: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD messages to the remote host. If the switch is moved to to the left, the **DPD delay** and **DPD timeout** fields are not available for editing.
DPD delay	A time period (in seconds) between DPD messages. By default, the value `30` is specified.
DPD timeout	A waiting period for the response to a DPD message (in seconds). If the host does not answer in the specified time, the router breaks down the tunnel connection, updates information on it, and tries to reestablish the connection. By default, the value `120` is specified.
Specify connection port	Move the switch to the right to change the port used for data exchange with the other party enter the needed value in the **Port** field displayed. By default, the value `1701` is specified.

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

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

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

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

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

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

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

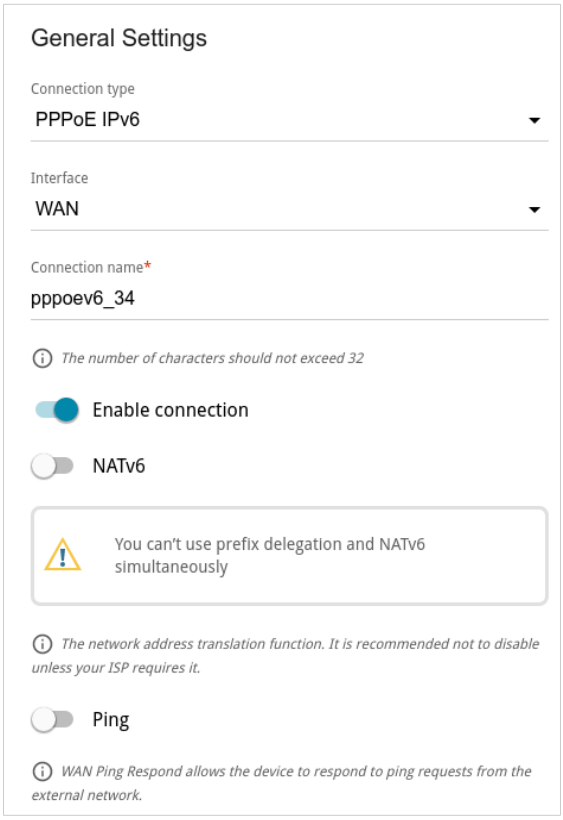

*Figure 81. The page for creating a new **PPPoE IPv6** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	*For the **PPPoE Dual Stack** type only.* If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
NATv6	If the switch is moved to the right, the network address translation function for IPv6 is enabled. Do not disable the function unless your ISP requires this.

Parameter	Description
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
RIP	*For the **PPPoE Dual Stack** type only.* Move the switch to the right to allow using RIP for this connection.

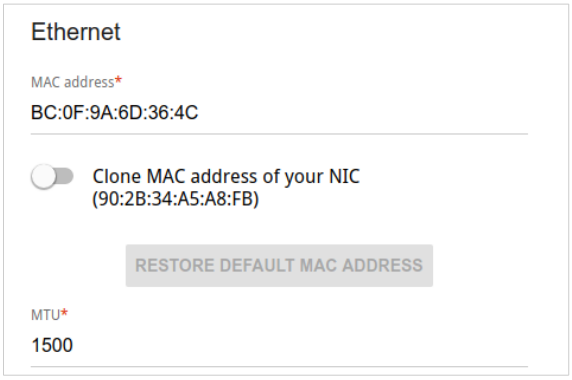

*Figure 82. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.*

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

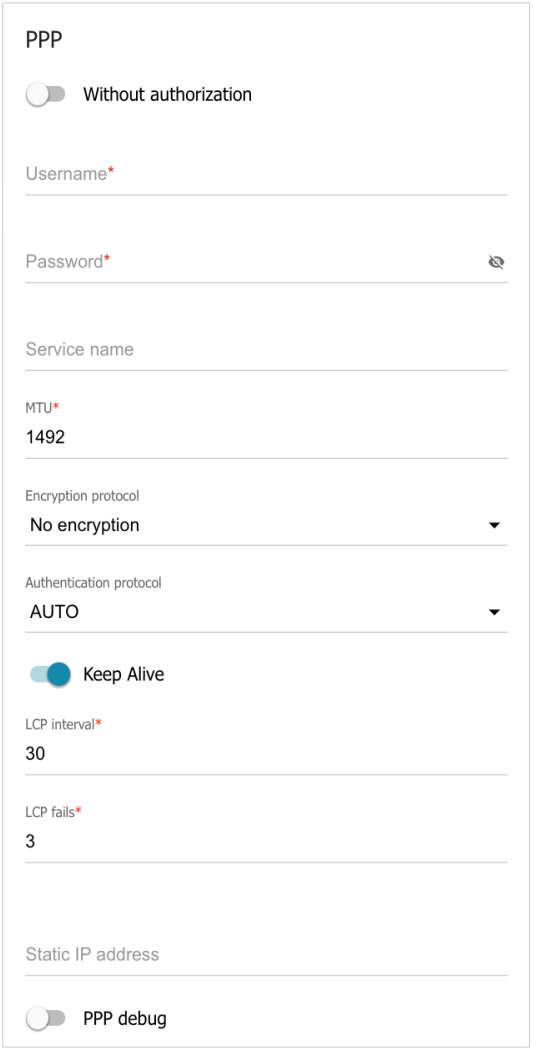

*Figure 83. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.*

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

Parameter	Description
Encryption protocol	Select a method of MPPE encryption. • **No encryption**: MPPE encryption is not applied. • **MPPE 40 128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied. • **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied. • **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the **MS-CHAP**, **MS-CHAPv2**, or **AUTO** value is selected from the **Authentication protocol** drop-down list.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

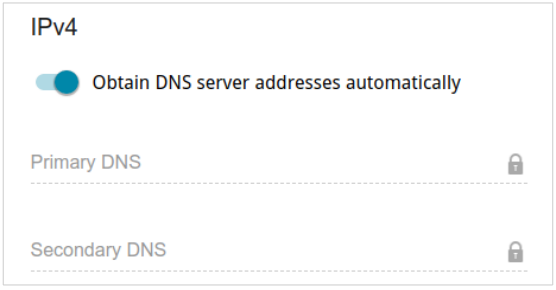

*Figure 84. The page for creating a new **PPPoE Dual Stack** connection. The **IPv4** section.*

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

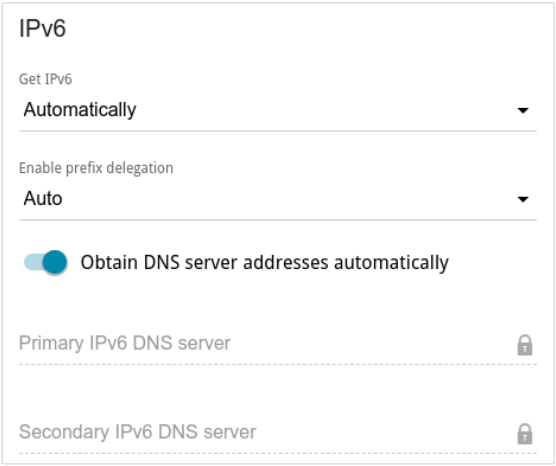

*Figure 85. The page for creating a new **PPPoE Pv6** connection. The **IPv6** section.*

Parameter	Description
IPv6	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.

Parameter	Description
Enable prefix delegation	From the drop-down list, select the mode of a prefix request from a delegating DHCPv6 server to configure a range of IPv6 addresses for the local network. • **None**: The mode without prefix request. • **Auto**: The mode with the ability to request a prefix. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is not mandatory to establish the connection. • **Force**: The mode with forced prefix request. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is mandatory to establish the connection.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.
Primary IPv6 DNS server / Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.

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

Creating Mobile Internet WAN Connection

If the PIN code check is enabled for the SIM card inserted into the built-in LTE modem, for correct operation of the mobile WAN connection click the **ENTER PIN** button in the notification in the top right corner of the page and enter the PIN code in the window displayed. Then on the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

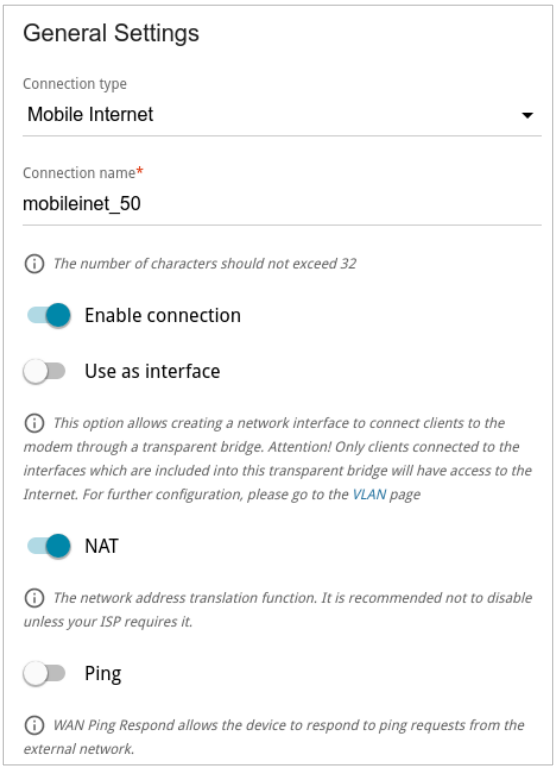

*Figure 86. The page for creating a new **Mobile Internet** connection. The **General Settings** section.*

Parameter	Description
General Settings	
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Use as interface	Move the switch to the right in order to create a network interface for this connection, for example, to combine several interfaces into a transparent connection.
NAT	If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this. The switch is displayed when the **IPv4** or **Dual** value is selected from the **Type** drop-down list in the **Modem Settings** section.

Parameter	Description
NATv6	If the switch is moved to the right, the network address translation function for IPv6 is enabled. Do not disable the function unless your ISP requires this. The switch is displayed when the **IPv6** or **Dual** value is selected from the **Type** drop-down list in the **Modem Settings** section.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

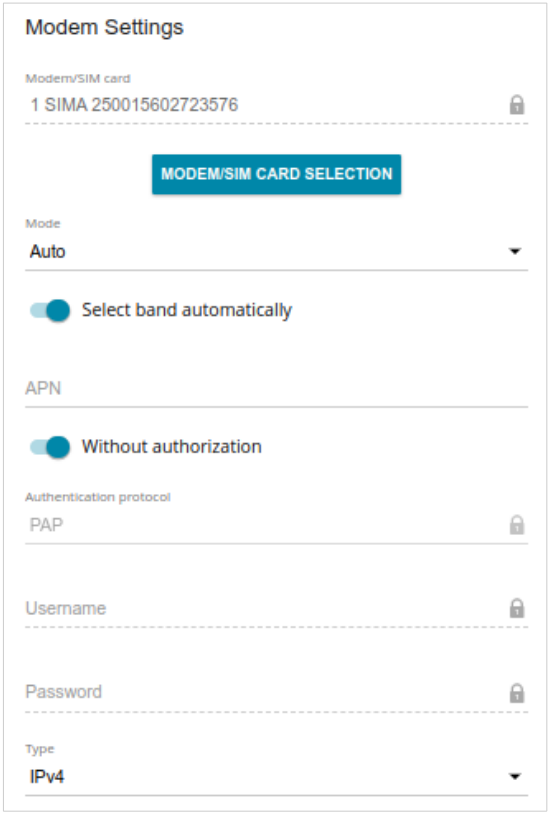

*Figure 87. The page for creating a new **Mobile Internet** connection. The **Modem Settings** section.*

Parameter	Description
Modem Settings	
MODEM/SIM CARD SELECTION	Click the button in order to assign the connection to the SIM card of the built-in LTE modem.
Mode	The value of the field specifies the type of the network to which the router connects. Leave the **Auto** value to let the router connect automatically to an available type of network, or select a needed value from the drop-down list.

Parameter	Description
Select band automatically	If the switch is moved to the right, the frequency band configuration is performed automatically. If you need to configure the frequency band manually, move the switch to the left. Upon that available bands for the type of network selected from the **Mode** list are displayed on the page. To disable the needed bands, move relevant switches to the left. Contact your operator to clarify the information on used bands. *The switch is displayed after assigning the connection to the connected SIM card.*
APN	An access point name.
Without authorization	Move the switch to the right if your operator does not require authorization.
Authentication protocol	Select a required authentication method from the drop-down list.
Username	A username (login) to connect to the network of the operator.
Password	A password to connect to the network of the operator. Click the **Show** icon ( ) to display the entered password.
Type	An IP version which will be used by this connection. Select the **IPv4**, **IPv6**, or **Dual** value from the drop-down list.

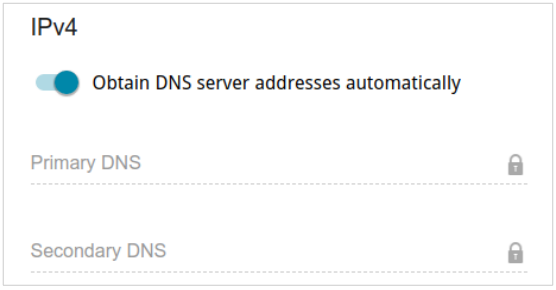

*Figure 88. The page for creating a new **Mobile Internet** connection. The **IPv4** section.*

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

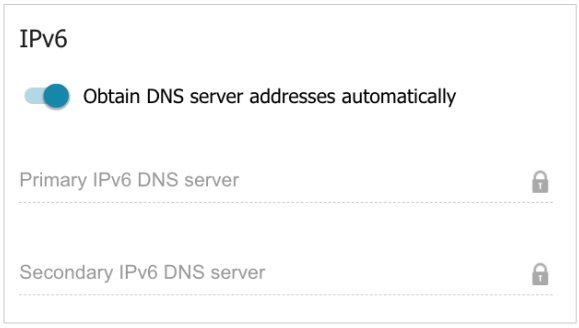

*Figure 89. The page for creating a new **Mobile Internet** connection. The **IPv6** section.*

Parameter	Description
IPv6 *(for the **Dual** and **IPv6** types)*	
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.
Primary IPv6 DNS server / Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.

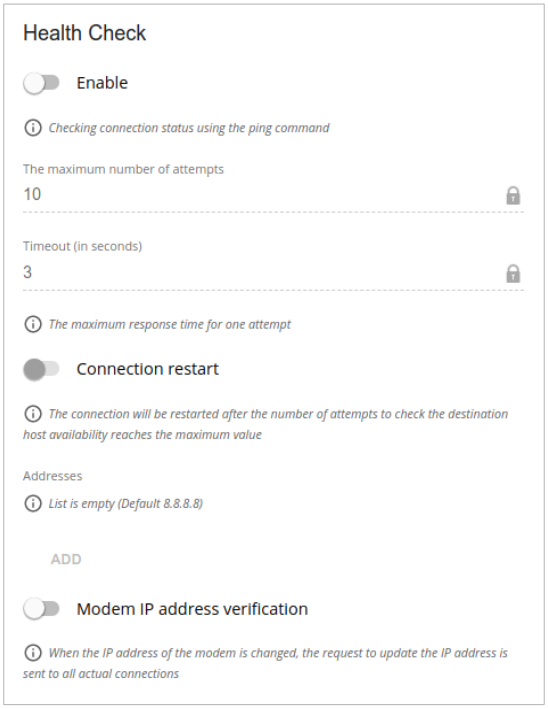

*Figure 90. The page for creating a new **Mobile Internet** connection. The **Health Check** section.*

Parameter	Description
Health Check	
Enable	Move the switch to the right to check the connection health using the ICMP ping mechanism.

Parameter	Description
The maximum number of attempts	A number of requests to check the health of the connection. By default, the value `10` is specified. Several ping requests are sent to check the hosts. After several failed attempts the connection status is changed until a successful attempt is made.
Timeout	A time period (in seconds) allocated for a respond to one ping request. By default, the value `3` is specified.
Connection restart	Move the switch to the right to reestablish connection if the maximum number of ping requests fails.
Addresses	IP addresses from the external network that the router will check for availability via ICMP ping mechanism. By default, the router checks the IP address 8.8.8.8. Click the **ADD** button, and in the line displayed, enter an IP address or leave value suggested by the router. You can add several addresses. To remove an IP address from the list, click the **Delete** button ( ) in the line of the address.
Modem IP address verification	Move the switch to the right to let the router request the actual IP address from the modem in case modem's IP address changes before expiration of the previous one.

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

LAN

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

IPv4

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

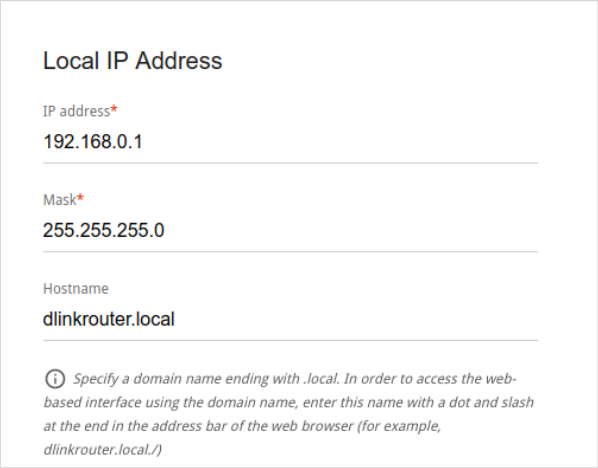

*Figure 91. Configuring the local interface. The **IPv4** tab. The **Local IP Address** section.*

Parameter	Description
Local IP Address	
Mode of local IP address assignment	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Initial Configuration Wizard.* Select the needed value from the drop-down list. • **Static**: The IPv4 address, subnet mask, and the gateway IP address are assigned manually. • **Dynamic**: The router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects. When this value is selected, the controls of the **Dynamic IP Addresses** section are not available. Also when this value is selected, the **Obtain DNS server addresses automatically** switch is displayed on the tab.
IP address	The IPv4 address of the router in the local subnet. By default, the following value is specified: `192.168.0.1`.
Mask	The mask of the local subnet. By default, the following value is specified: `255.255.255.0`.

Parameter	Description
Gateway IP address	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Initial Configuration Wizard.* The gateway IPv4 address which is used by the router to connect to the Internet (e.g., for synchronizing the system time with an NTP server). *Optional*.
Hostname	The name of the device assigned to its IPv4 address in the local subnet.
Obtain DNS server addresses automatically	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Initial Configuration Wizard.* Move the switch to the right to configure automatic assignment of DNS server IPv4 addresses. Upon that the **DNS IP address** field is not available for editing.
DNS IP address	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Initial Configuration Wizard.* If needed, specify a DNS server IPv4 address for the selected mode of local IP address assignment. If you want to specify several DNS servers, click the **ADD** button, and in the line displayed, enter the IPv4 address. To remove the address, click the **Delete** button ( ) in the line of the address. The DNS servers specified on this page will have higher priority than the servers specified on the **Advanced / DNS** page.

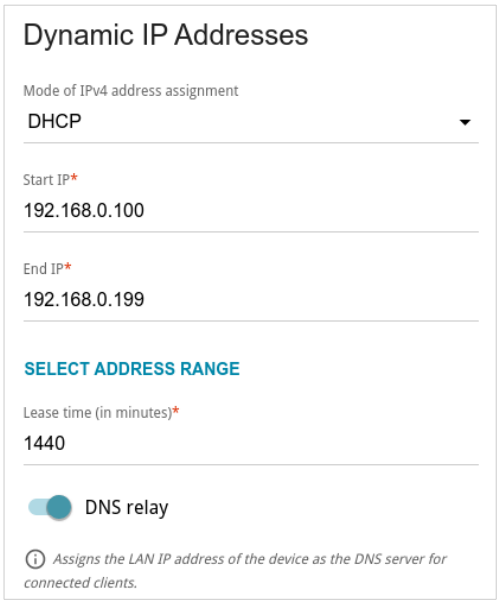

*Figure 92. Configuring the local interface. The **IPv4** tab. The **Dynamic IP Addresses** section.*

Parameter	Description
Dynamic IP Addresses	
Mode of IPv4 address assignment	An operating mode of the router's DHCP server. • **Disable**: The router's DHCP server is disabled, clients' IP addresses are assigned manually. • **DHCP**: The router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the **Start IP**, **End IP**, **Lease time** fields, the **SELECT ADDRESS RANGE** button, and the **DNS relay** switch are displayed on the tab. Also when this value is selected, the **DHCP Options**, **Static IP Addresses**, and **Hosts** sections are displayed on the tab. • **Relay**: An external DHCP server is used to assign IP addresses to clients. When this value is selected, the **External DHCP server IP**, **Option 82 Circuit ID**, **Option 82 Remote ID**, and **Option 82 Subscriber ID** fields are displayed on the tab. *Available if the **Router**, **WISP Repeater**, or **Mobile Internet** mode was selected in the Initial Configuration Wizard.*
Start IP	The start IP address of the address range used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address range used by the DHCP server to distribute IP addresses to clients.
SELECT ADDRESS RANGE	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the **SAVE** button to automatically fill in the **Start IP** and **End IP** fields.
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
DNS relay	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the **Advanced / DNS** page as the DNS server address.

Parameter	Description
External DHCP server IP	The IPv4 address of the external DHCP server which assigns IPv4 addresses to the router's clients. To specify several IPv4 addresses, click the **ADD** button, and in the line displayed, enter an IPv4 address. To remove the IPv4 address, click the **Delete** button ( ) in the line of the address.
Option 82 Circuit ID **Option 82 Remote ID** **Option 82 Subscriber ID**	The value of the relevant field of DHCP option 82. Do not fill in the fields unless your ISP or the administrator of the external DHCP server provided these values.

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

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

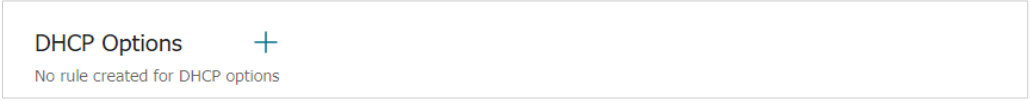

*Figure 93. Configuring the local interface. The **IPv4** tab. The section for configuring DHCP options.*

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

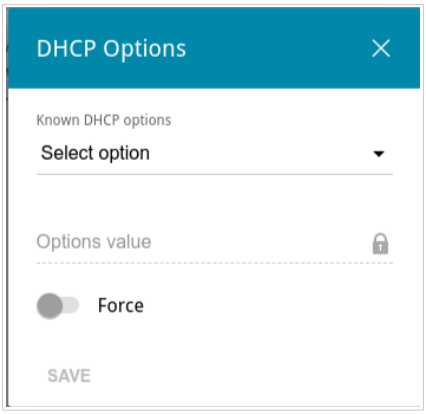

*Figure 94. Configuring the local interface. The **IPv4** tab. The window for configuring a DHCP option.*

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

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

Parameter	Description
Force	Move the switch to the right to let the DHCP server send the selected option regardless of the client's request. Move the switch to the left to let the DHCP server send the selected option only when the client requests it.

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

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

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

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

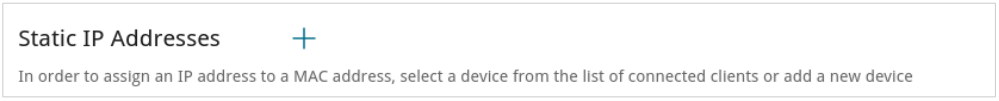

*Figure 95. Configuring the local interface. The **IPv4** tab. The section for creating MAC-IPv4 pairs.*

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

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

If needed, you can add your own address resource records. To do this, click the **ADD** button (+) in the **Hosts** section (*available if in the* ***Dynamic IP Addresses*** *section the* ***DHCP*** *value is selected from the* ***Mode of IPv4 address assignment*** *drop-down list*).

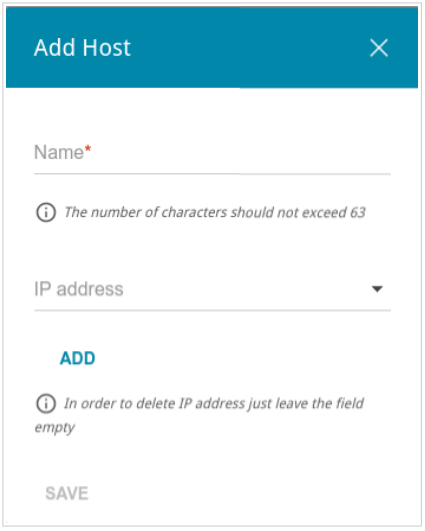

Figure 96. Configuring the local interface. The ***IPv4*** *tab. The window for adding a DNS record.*

In the **Name** field, specify the domain or domain name to which the specified IPv4 address will correspond. In the **IP address** field, specify a host from the internal or external network. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 address from the drop-down list (the field will be filled in automatically). To specify several IP addresses, click the **ADD** button. Click the **SAVE** button.

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

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

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

IPv6

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

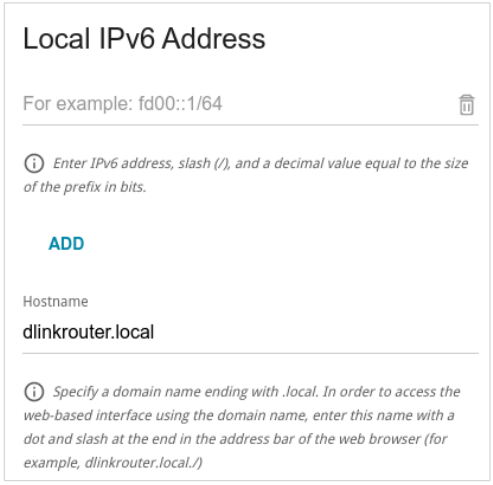

*Figure 97. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.*

To add an IPv6 address of the router, click the **ADD** button. In the line displayed, enter an IPv6 address and then a slash followed by a decimal value of the prefix length. To change an IPv6 address of the router, edit the corresponding line.

To remove an IPv6 address, click the **DELETE** ( ) button in the corresponding line of the table. Then click the **APPLY** button.

Also you can specify the following parameters:

Parameter	Description
Local IPv6 Address	
Gateway IPv6 address	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Initial Configuration Wizard.* The gateway IPv6 address which is used by the router to connect to the Internet (e.g., for synchronizing the system time with an NTP server). *Optional*.
Hostname	The name of the device assigned to its IPv6 address in the local subnet.

Parameter	Description
DNS IP address	*Available if the **Access point**, **Repeater**, or **Client** mode was selected in the Initial Configuration Wizard.* If needed, specify a DNS server IPv6 address. If you want to specify several DNS servers, click the **ADD** button, and in the line displayed, enter the IPv6 address. To remove the address, click the **Delete** button ( ) in the line of the address. The DNS servers specified on this page will have higher priority than the servers specified on the **Advanced / DNS** page.

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

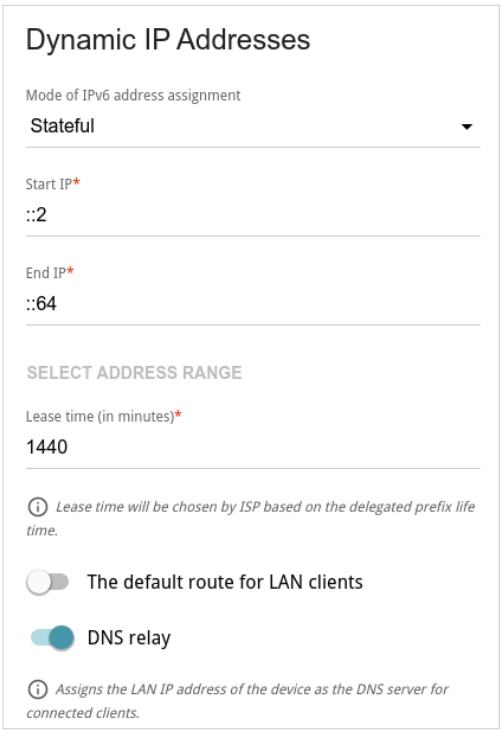

*Figure 98. Configuring the local interface. The **IPv6** tab. The **Dynamic IP Addresses** section.*

Parameter	Description
Dynamic IP Addresses	
Mode of IPv6 address assignment	Select the needed value from the drop-down list. • **Disable**: Clients' IPv6 addresses are assigned manually. • **Stateless:** Clients themselves configure IPv6 addresses using the prefix. • **Stateful**: The built-in DHCPv6 server of the router allocates addresses from the range specified in the **Start IP** and **End IP** fields. Also when this value is selected, the **Static IP Addresses** and **Hosts** sections are displayed on the tab. • **Relay**: An external DHCP server is used to assign IPv6 addresses to clients. When this value is selected, the **External DHCP server IP** field is displayed on the tab. *Available if the **Router**, **WISP Repeater**, or **Mobile Internet** mode was selected in the Initial Configuration Wizard.*
Start IP / End IP	The start and the end values for the latest hextet (16 bit) of the range of IPv6 addresses which the DHCPv6 server distributes to clients.
SELECT ADDRESS RANGE	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the **SAVE** button to automatically fill in the **Start IP** and **End IP** fields.
Lease time	The lifetime of IPv6 addresses provided to clients.
The default route for LAN clients	Move the switch to the right to let the clients, that received IPv6 addresses or configured them using the prefix, use the router as the default IPv6 route.
DNS relay	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the **Advanced / DNS** page as the DNS server address.
External DHCP server IP	The IPv6 address of the external DHCP server which assigns IPv6 addresses to the router's clients. To specify several IPv6 addresses, click the **ADD** button, and in the line displayed, enter an IPv6 address. To remove the IPv6 address, click the **Delete** button ( ) in the line of the address.

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

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

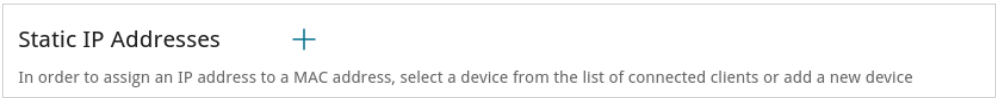

*Figure 99. Configuring the local interface. The **IPv6** tab. The section for creating MAC-IPv6 pairs.*

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

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

If needed, you can add your own address resource records. To do this, click the **ADD** button ( ) in the **Hosts** section (*available if in the **Dynamic IP Addresses** section the **Stateful** value is selected from the **Mode of IPv6 address assignment** drop-down list*).

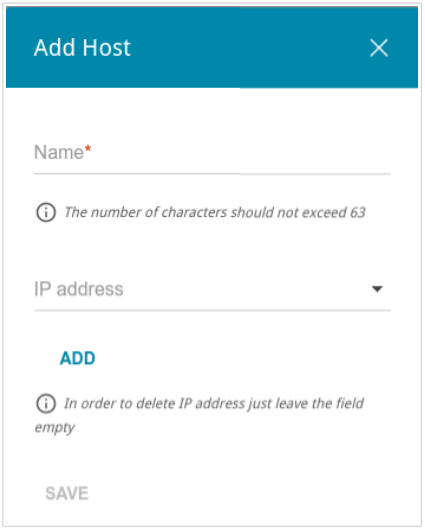

*Figure 100. Configuring the local interface. The **IPv6** tab. The window for adding a DNS record.*

In the **Name** field, specify the domain or domain name to which the specified IPv6 address will correspond. In the **IP address** field, specify a host from the internal or external network. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv6 address from the drop-down list (the field will be filled in automatically). To specify several IP addresses, click the **ADD** button. Click the **SAVE** button.

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

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

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

WAN Failover

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

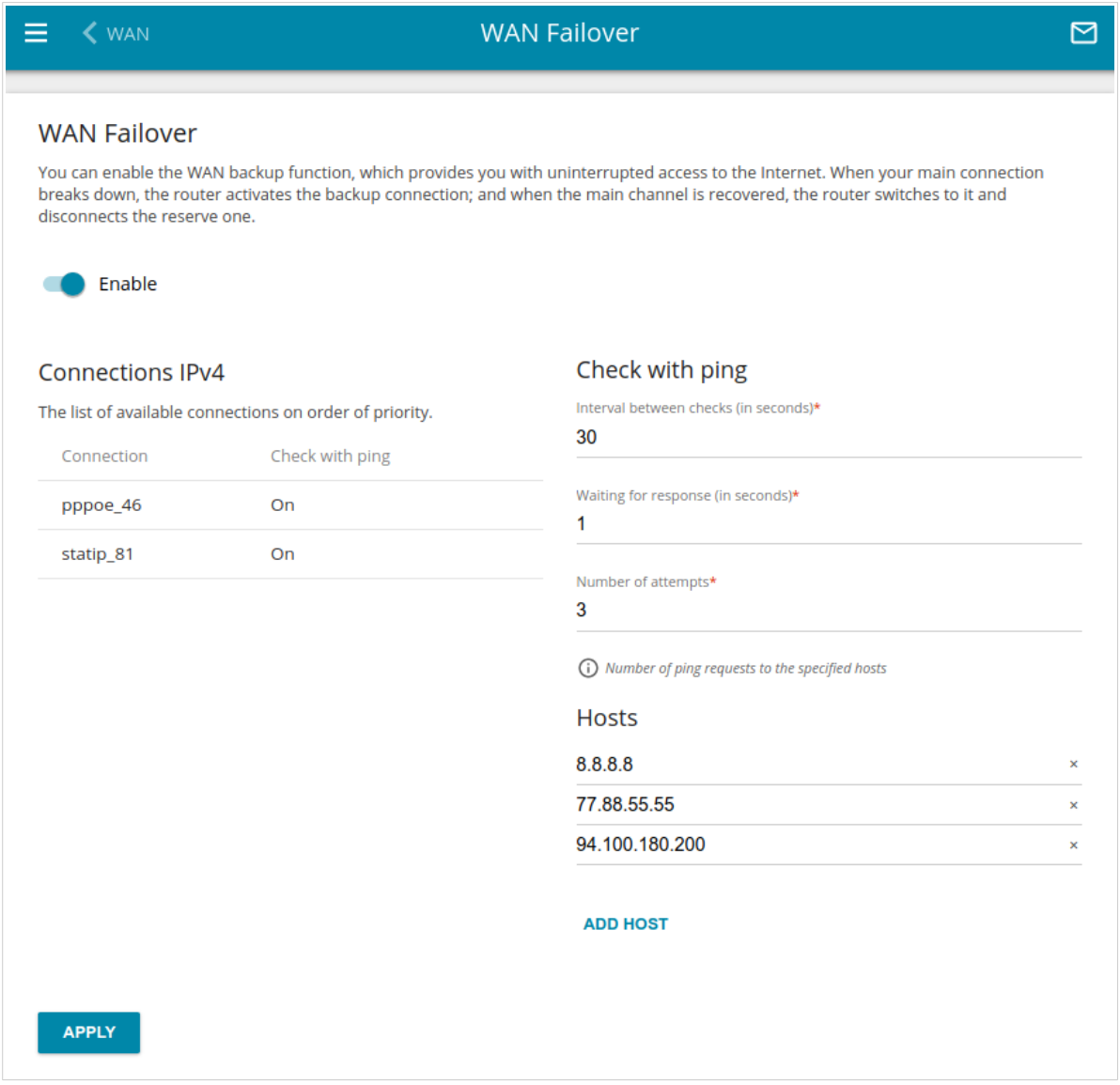

*Figure 101. The **Connections Setup / WAN Failover** page.*

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

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

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

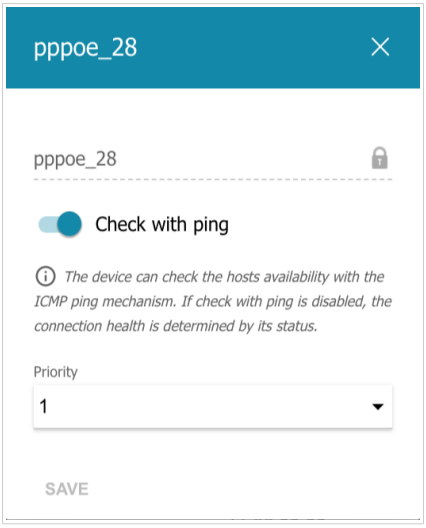

Figure 102. The window for changing the priority of a connection.

In the opened window, specify the needed parameters.

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

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

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

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

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

Auto Configuration of 3G/LTE

On the **Connections Setup / Auto Configuration of 3G/LTE** page, you can enable the function for automatic creation of a mobile WAN connection upon powering the router on.

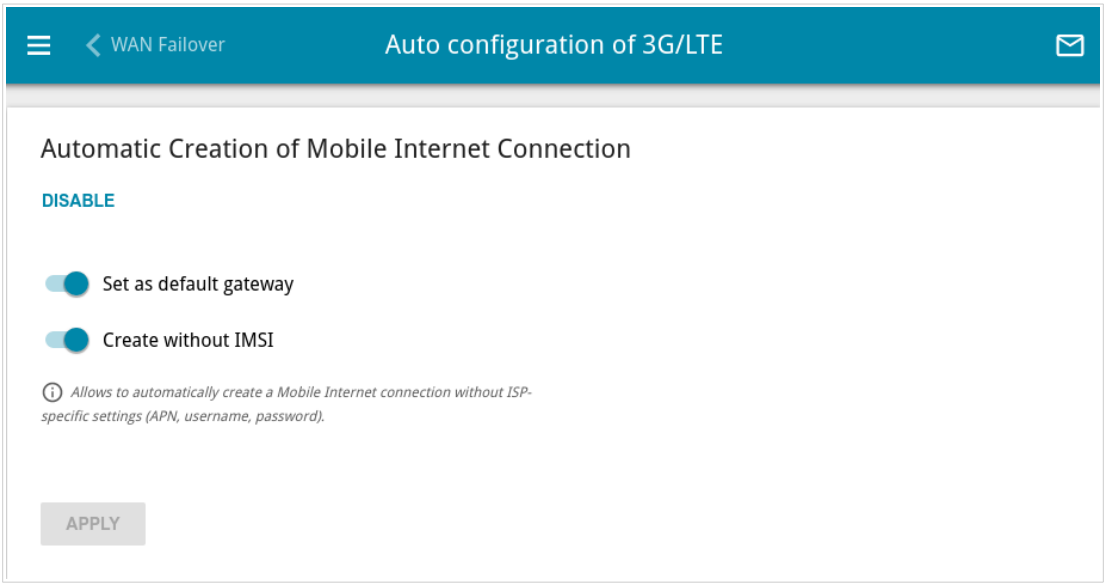

*Figure 103. The **Connections Setup / Auto Configuration of 3G/LTE** page.*

If you want to enable the function for automatic creation of a mobile WAN connection, click the **ENABLE** button. If needed, change the settings on this page.

Parameter	Description
Set as default gateway	Move the switch to the right to allow the router to use an automatically created mobile WAN connection as the default connection. Move the switch to the left if you want the router to continue using the existing default connection when automatically creating a mobile WAN connection.
Create without IMSI	Move the switch to the right to enable automatic creation of a mobile WAN connection without the operator's settings. This setting will be useful if the code stored in the SIM card is unavailable. Move the switch to the left to disable automatic creation of a mobile WAN connection without the operator's settings.

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

If the PIN code check for the SIM card inserted into the built-in LTE 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 want to disable the function for automatic creation of a mobile WAN connection, click the **DISABLE** button.

Traffic Balancing

On the **Connections Setup / Traffic Balancing** page, you can enable the traffic balancing function. This function enables equal load balancing on the router and increases maximum bandwidth of your Internet connection while using several WAN connections (for example, if access to the Internet is provided by several ISPs).

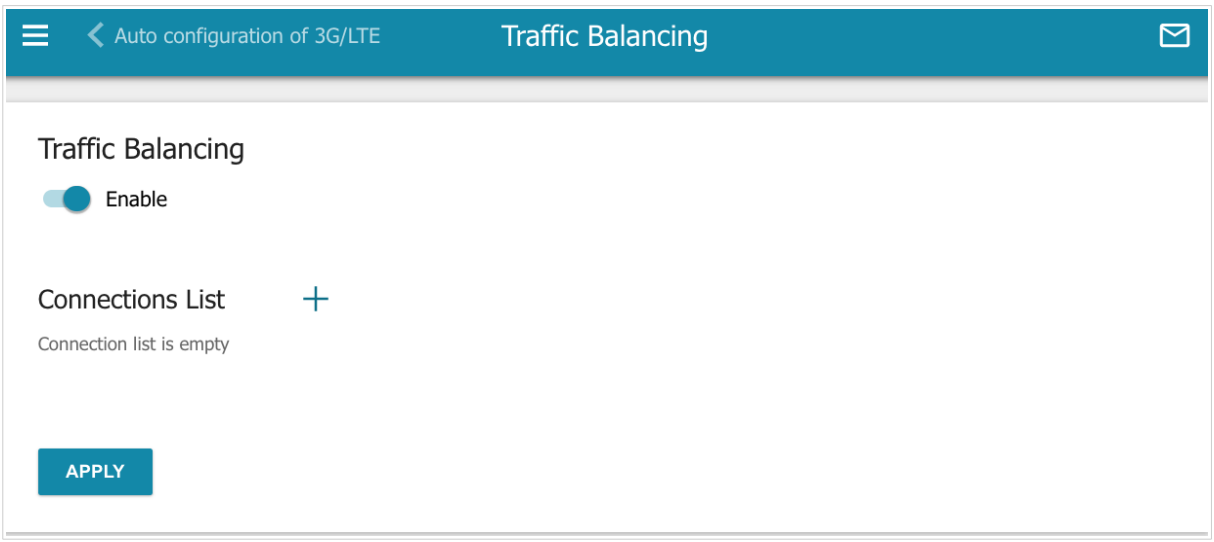

*Figure 104. The **Connections Setup / Traffic Balancing** page.*

To enable the traffic balancing function, move the **Enable** switch to the right. Then add connections to the page among which traffic will be balanced. To do this, click the **ADD** button (+) in the **Connections List** section.

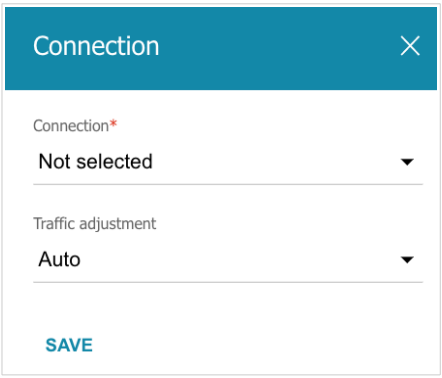

Figure 105. The window for adding a new connection to the page.

In the opened window, specify the needed parameters.

Parameter	Description
Connection	From the drop-down list, select a WAN connection to which traffic balancing will be applied.
Traffic adjustment	Select a value from the drop-down list. • **Auto**: Traffic is equally divided among connections with the same setting. • **Manual**: Traffic is equally divided among connections in accordance with the value specified in the **Weight** field.
Weight	Specify the percentage of traffic which will pass through the connection.

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

To edit the setting for an added connection, in the **Connections List** section, select the relevant line in the table. In the opened window, change the value and click the **SAVE** button.

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

After specifying the needed parameters, click the **APPLY** button. Upon that the **Status** field is displayed on the page.

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

VPN

In this menu you can configure VPN connections based on IPsec/GRE/EoGRE/EoIP protocols and create a PPTP or L2TP server and accounts for access to it.

IPsec

On the **VPN / IPsec** page, you can configure VPN tunnels based on IPsec protocol.

IPsec is a protocol suite for securing IP communications.

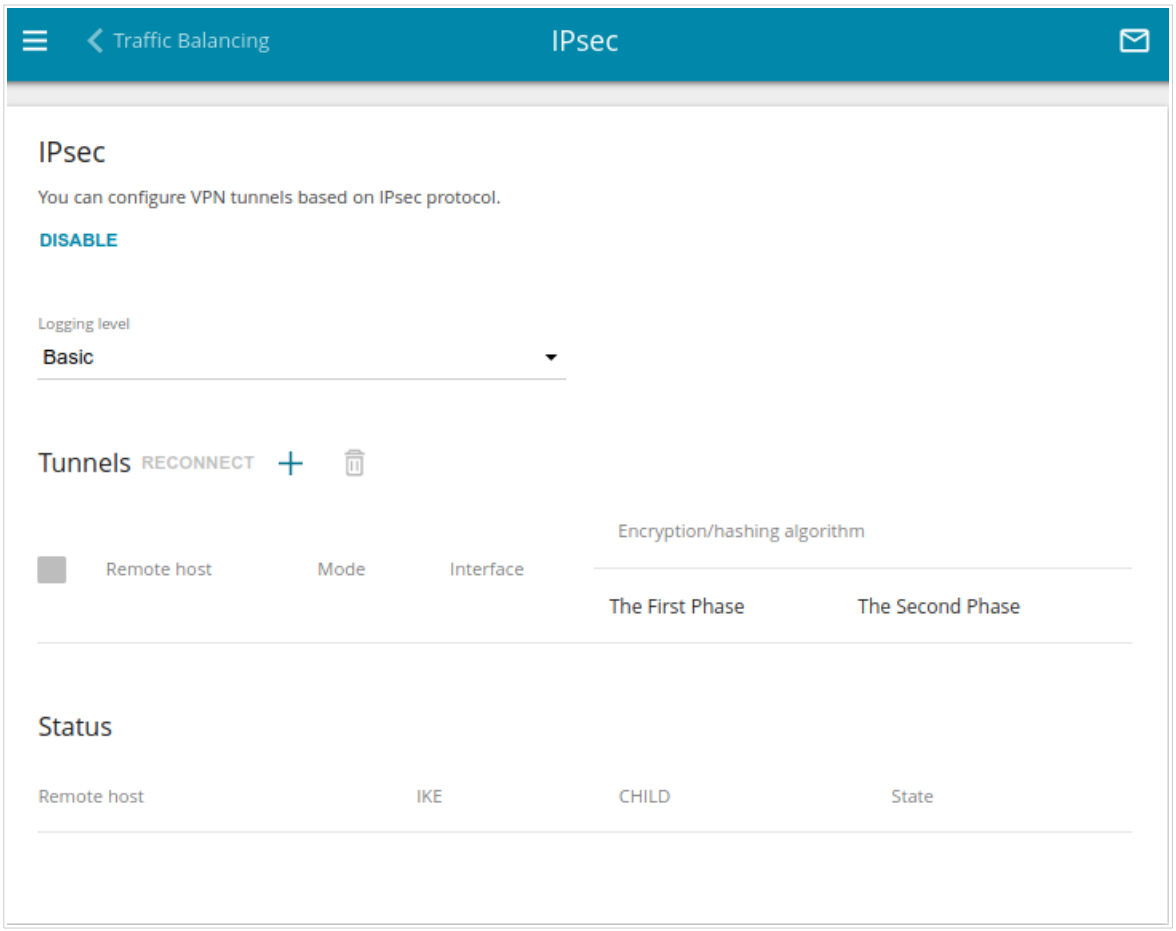

*Figure 106. The **VPN / IPsec** page.*

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

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

From the **Logging level** drop-down list, select a detail level of messages recorded to the system log or leave the value specified by default. The **Basic** value is recommended to establish an IPsec tunnel faster. To view the log, go to the **System / Log** page (see the ***Log*** section, page 241).

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.

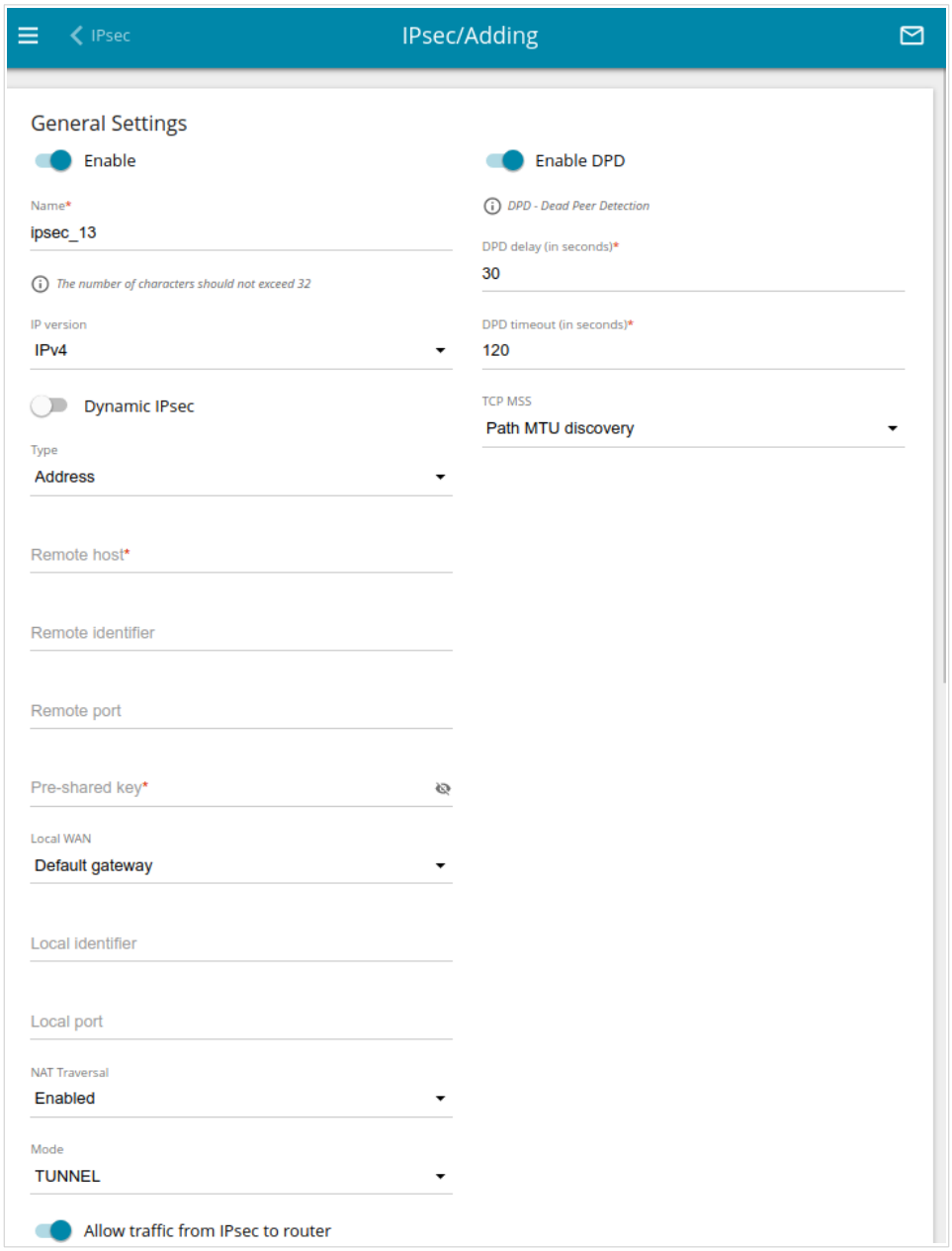

*Figure 107. The page for adding an IPsec tunnel. The **General Settings** section.*

You can specify the following parameters:

Parameter	Description
General Settings	
Enable	Move the switch to the right to enable the tunnel. Move the switch to the left to disable the tunnel.

Parameter	Description
Name	A name for the tunnel for easier identification. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[7]
IP version	An IP version.
Dynamic IPsec	Move the switch to the right to allow a remote host with any public IP address to connect to the router via IPsec protocol. Such a setting can be specified for one IPsec tunnel only. Connection requests via this tunnel can be sent by a remote host only.
Type	Select an identification method for the remote host (router) from the drop-down list: • **Address**: The remote host is identified by its IP address. • **FQDN**: The remote host is identified by its domain name. The drop-down list is displayed if the **Dynamic IPsec** switch is moved to the left.
Remote host	Enter the remote subnet VPN gateway IP address if the **Address** value is selected from the **Type** drop-down list. Enter the remote subnet VPN gateway domain name if the **FQDN** value is selected from the **Type** drop-down list. The field is available for editing if the **Dynamic IPsec** switch is moved to the left.
Remote identifier	A remote host identifier to establish connection over IPsec with particular hosts only. To establish connection, DWR-953 remote identifier value should correspond to the local identifier value specified in the settings of the remote host. Use an IP address of a host or subnet, the value `%any` (all IP addresses), a domain name, or certificate CN. By default, the value specified in the **Remote host** field is used.
Remote port	A port of the remote host, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If the field is left blank and the network address translation (NAT) function is used for the connection, port 4500 is used.
Pre-shared key	A PSK key for mutual authentication of the parties. Click the **Show** icon ( ) to display the entered key.

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

Parameter	Description
Local WAN	A WAN connection through which the tunnel will pass. Select a value from the drop-down list. • **Interface**: When this value is selected, the **Interface** drop-down list is displayed. Select an existing WAN connection from the list. • **Default gateway**: When this value is selected, the router uses the default WAN connection.
Local identifier	A local identifier of the router to establish connection over IPsec with particular hosts only. To establish connection, DWR-953 local identifier value should correspond to the remote identifier value specified in the settings of the remote host. Use an IP address, domain name, or certificate CN. *Optional.*
Local port	A port of the router, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If the field is left blank and the network address translation (NAT) function is used for the connection, port 4500 is used.
NAT Traversal	The NAT Traversal function allows VPN traffic to pass through the NAT-enabled device. DWR-953 allows to forcibly encapsulate VPN traffic in UDP packets for passing through a remote device regardless of whether it supports address translation. If you need to enable forced encapsulation of VPN traffic, select the **Enabled** value. If you need to disable forced encapsulation of VPN traffic, select the **Disabled** value.
Mode	An operation mode of the IPsec tunnel. Select a value from the drop-down list. • **TUNNEL**: As a rule, it is used to create a secure connection to remote networks. In this mode, the source IP packet is fully encrypted and added to a new IP packet and data transfer is based on the header of the new IP packet. • **TRANSPORT**: As a rule, it is used to encrypt data stream within one network. In this mode, only the content of the source IP packet is encrypted, its header remains unchanged and data transfer is based on the source header.
Allow traffic from IPsec to router	Move the switch to the left to deny access to your router from the remote subnet via IPsec. The switch is displayed when the **TUNNEL** value is selected from the **Mode** drop-down list.

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

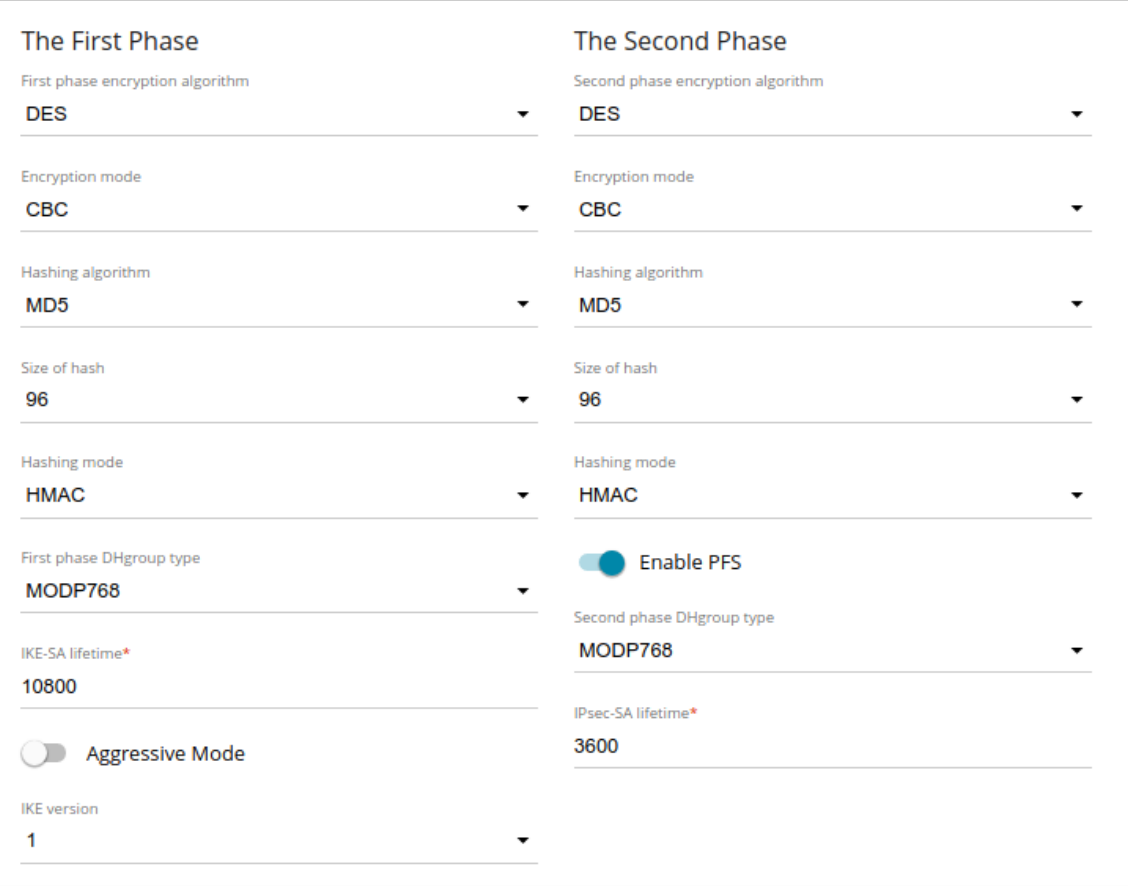

*Figure 108. The page for adding an IPsec tunnel. **The First Phase / The Second Phase** sections.*

Parameter	Description
The First Phase	
First phase encryption algorithm	Select an available encryption algorithm from the drop-down list.
Encryption mode	Select an encryption mode from the drop-down list.
Hashing algorithm	Select a hashing algorithm from the drop-down list.
Size of hash	The length of the hash in bits.
Hashing mode	Select a hashing mode from the drop-down list.
First phase DHgroup type	A Diffie-Hellman key group for the First Phase. Select a value from the drop-down list.
IKE-SA lifetime	The lifetime of IKE-SA keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should be greater than the value specified in the **IPsec-SA lifetime** field.

Parameter	Description
Aggressive Mode	Move the switch to the right to enable the aggressive mode for mutual authentication of the parties. Such a setting accelerates the connection establishment, but reduces its security.
IKE version	IKE (*Internet Key Exchange*) is a protocol of keys exchange between two hosts of VPN connections. Select a version of the protocol from the drop-down list.
The Second Phase	
Second phase encryption algorithm	Select an available encryption algorithm from the drop-down list.
Encryption mode	Select an encryption mode from the drop-down list.
Hashing algorithm	Select a hashing algorithm from the drop-down list.
Size of hash	The length of the hash in bits.
Hashing mode	Select a hashing mode from the drop-down list.
Enable PFS	Move the switch to the right to enable the PFS option (*Perfect Forward Secrecy*). If the switch is moved to the right, a new encryption key exchange will be used for the Second Phase. This option enhances the security level of data transfer, but increases the load on DWR-953.
Second phase DHgroup type	A Diffie-Hellman key group for the Second Phase. Select a value from the drop-down list. The drop-down list is available if the **Enable PFS** switch is moved to the right.
IPsec-SA lifetime	The lifetime of the Second Phase keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should be greater than zero.

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

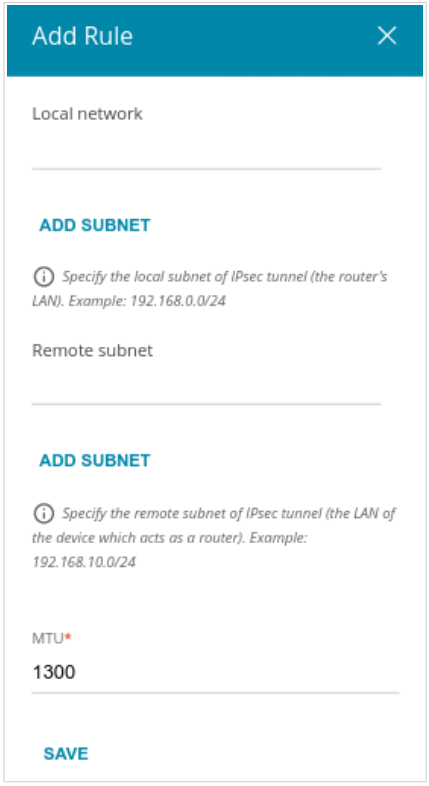

Figure 109. The page for adding an IPsec tunnel. The window for adding a tunneled network.

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

Parameter	Description
Local network	A local subnet IP address and mask. To add one more subnet, click the **ADD SUBNET** button and enter the subnet address in the displayed line (available if **2** is selected from the **IKE version** list in the **The First Phase** section). To remove the subnet, click the **Delete** icon (×) in the line of the subnet address.
Remote subnet	A remote subnet IP address and mask. To add one more subnet, click the **ADD SUBNET** button and enter the subnet address in the displayed line (available if **2** is selected from the **IKE version** list in the **The First Phase** section). To remove the subnet, click the **Delete** icon (×) in the line of the subnet address.
MTU	The maximum size (in bytes) of a non-fragmented packet. The field is displayed when the **Manual** value is selected from the **TCP MSS** drop-down list in the **General Settings** section.

Click the **SAVE** button.

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

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

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

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

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

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

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

GRE

On the **VPN / GRE** page, you can configure VPN tunnels based on GRE protocol.

GRE (*Generic Routing Encapsulation*) is a protocol for tunneling network packets, which enables you to create unprotected VPN tunnels.

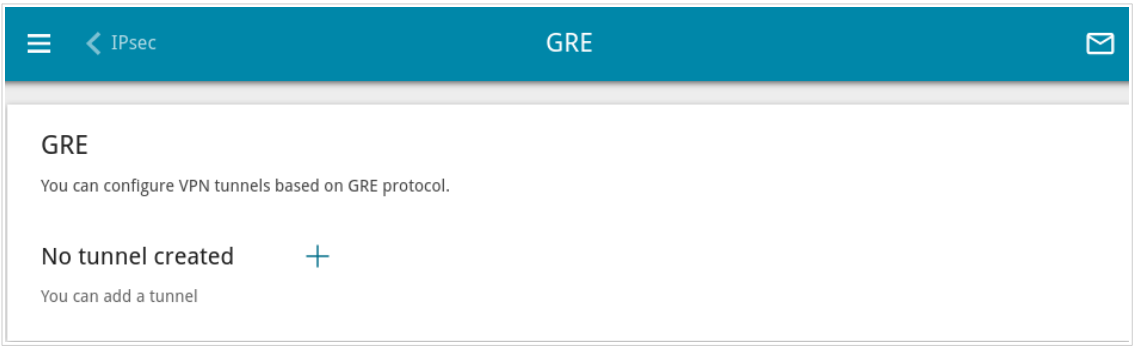

*Figure 110. The **VPN / GRE** page.*

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

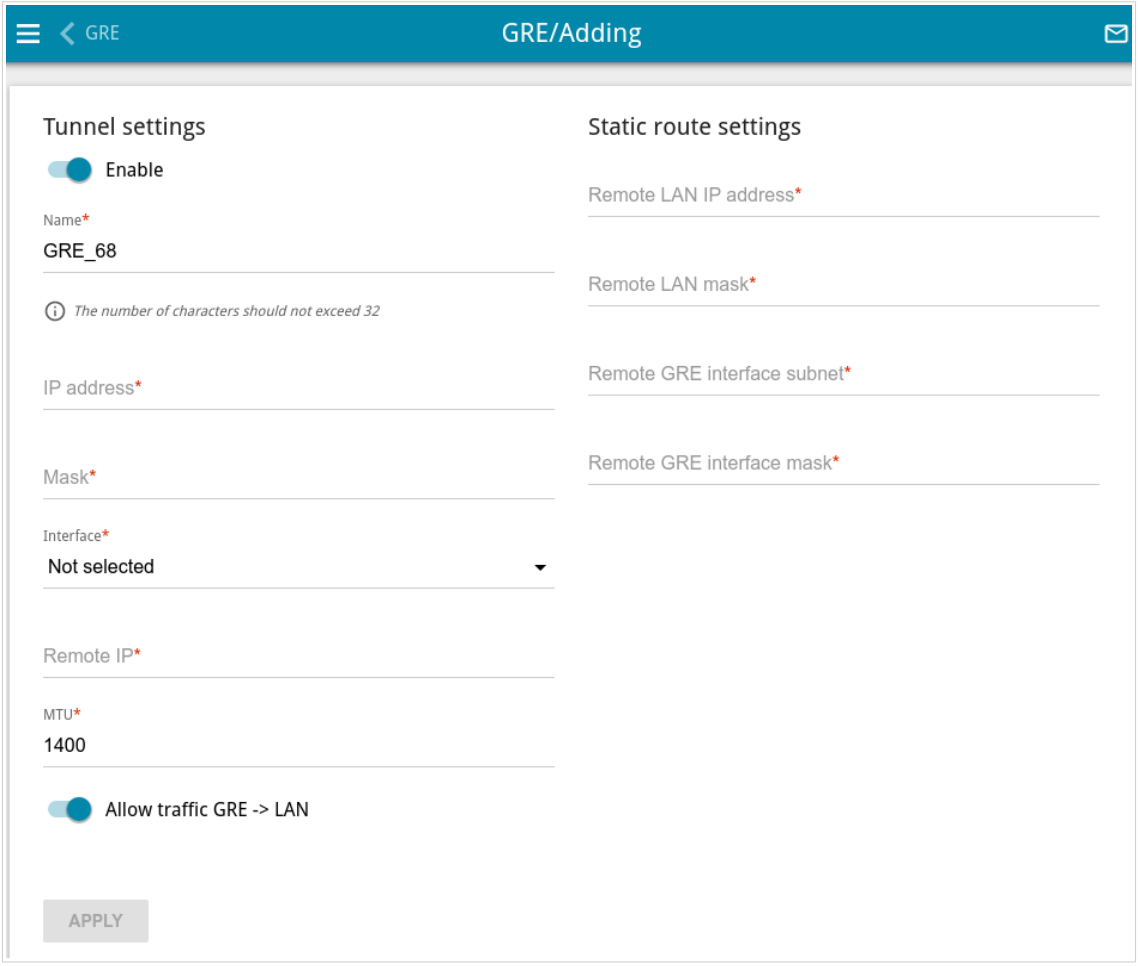

Figure 111. The page for adding a GRE tunnel.

You can specify the following parameters:

Parameter	Description
Tunnel settings	
Enable	Move the switch to the right to enable the GRE tunnel. Move the switch to the left to disable the GRE tunnel.
Name	A name of the tunnel for easier identification. You can specify any name.
IP address	The IP address of the GRE tunnel interface.
Mask	The mask of the subnet.
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the **Default gateway** value to use the default WAN connection.
Remote IP	Enter the IP address of the remote subnet VPN gateway.
MTU	The maximum size of units transmitted from the remote host to the router.
Allow traffic GRE → LAN	Move the switch to the right to allow GRE tunnel users access devices in the remote local subnet.
Static route settings	
Remote LAN IP address	The IP address of the remote local subnet.
Remote LAN mask	The mask of the remote local subnet.
Remote GRE interface subnet	The subnet of the remote GRE interface.
Remote GRE interface mask	The mask of the remote GRE interface.

After configuring all needed settings, 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 ( ).

PPTP/L2TP Servers

On the **VPN / PPTP/L2TP Servers** page, you can enable the PPTP or L2TP VPN server. To configure the PPTP or L2TP server, go to the relevant tab.

PPTP and L2TP help to establish a secure connection creating a tunnel in the standard insecure network.

Before creating the PPTP or L2TP server, it is required to create user accounts (see the ***VPN Users*** section, page 137).

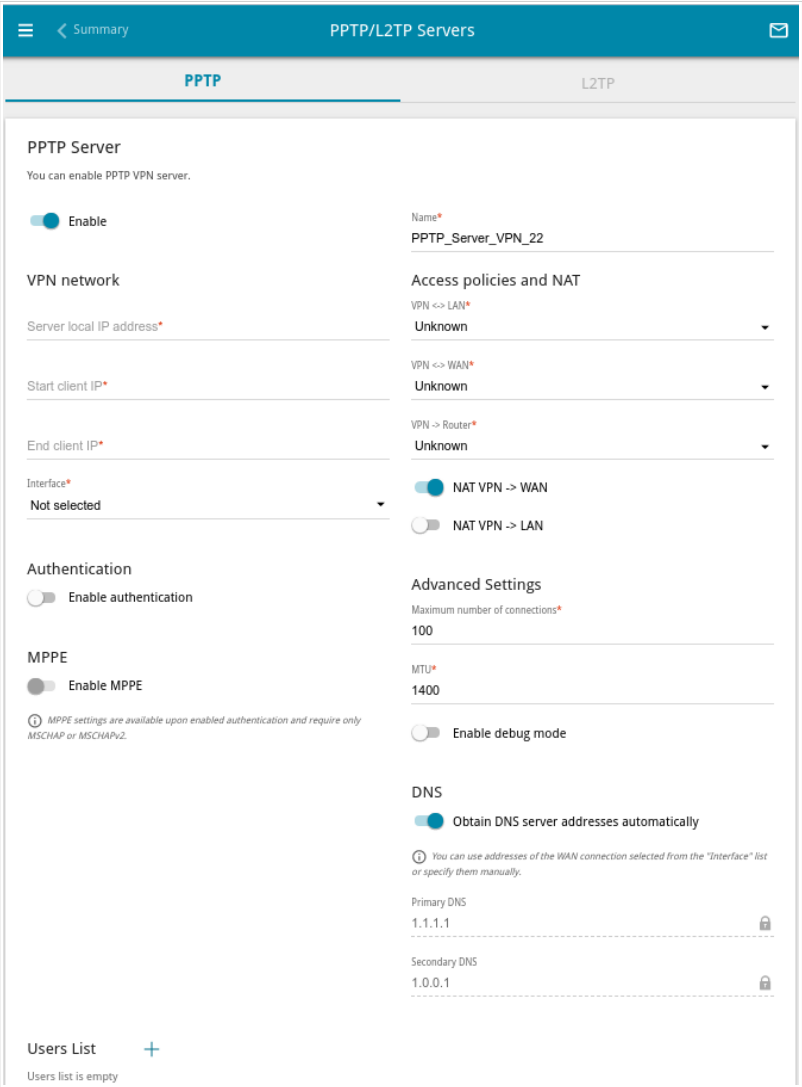

*Figure 112. The **VPN / PPTP/L2TP Servers** page.*

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

You can specify the following parameters:

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

Parameter	Description
VPN network	
Server local IP address	The IP address of the VPN server.
Start client IP	The start IP address of the address range for VPN server's clients.
End client IP	The end IP address of the address range for VPN server's clients.
Interface	Select a WAN connection through which this VPN server will be available. If the **Default gateway** value is selected, the router uses the default WAN connection.
Access policies and NAT	
VPN ↔ LAN	Select a value from the drop-down list. • **Allow**: VPN server's clients can access the router's local network; clients from the router's local network can access the VPN server's network. • **Deny**: VPN server's clients cannot access the router's local network; clients from the router's local network cannot access the VPN server's network.
VPN ↔ WAN	Select a value from the drop-down list. • **Allow**: VPN server's clients can access the external network; clients from the external network can access the VPN server's network. • **Deny**: VPN server's clients cannot access the external network; clients from the external network cannot access the VPN server's network.
VPN → Router	Select a value from the drop-down list. • **Allow**: VPN server's clients can access the router. • **Deny**: VPN server's clients cannot access the router.
NAT VPN → WAN	If the switch is moved to the right, the network address translation function between the VPN server's interface and the external network interface is enabled.
NAT VPN → LAN	If the switch is moved to the right, the network address translation function between the VPN server's interface and the local network interface is enabled.

Parameter	Description
Authentication	
Enable authentication	Move the switch to the right to enable authentication. Upon that the **Multiple sessions**, **CHAP**, **MSCHAP**, **MSCHAPv2**, and **PAP** lists are displayed on the page.
Multiple sessions	The mode of connection for the users listed in the **Users List** section. Select a value from the drop-down list. • **Allow**: Several users with the same user account are allowed to connect. • **Only new connections**: If there are several users with the same user account, only new users are allowed to connect. • **Only old connections**: If there are several users with the same user account, new users are not allowed to connect.
CHAP **MSCHAP** **MSCHAPv2** **PAP**	*Challenge Handshake Authentication Protocol.* *Microsoft Challenge Handshake Authentication Protocol.* *Password Authentication Protocol.* Select the needed action from the drop-down list for the relevant protocol. • **Auto**: Enable automatic client authentication over this protocol. • **Refuse**: Disable client authentication over this protocol. • **Require**: Require client authentication over this protocol.
MPPE	
Enable MPPE	Move the switch to the right to enable MPPE encryption. MPPE encryption can be applied only if the **Require** value is selected from the **MSCHAP** or **MSCHAPv2** drop-down list.
MPPE40 **MPPE128**	MPPE encryption with a 40-bit or 128-bit key is applied. Select the needed action from the drop-down list. • **Auto**: Allow clients to connect to the VPN server automatically with MPPE encryption. • **Refuse**: Restrict clients from connecting to the VPN server with MPPE encryption. • **Require**: Allow clients to connect to the VPN server only with MPPE encryption.

Parameter	Description
Advanced Settings	
Maximum number of connections	*Available on the **PPTP** tab.* The maximum number of devices allowed to connect to the PPTP server.
Port	*Available on the **L2TP** tab.* The port of L2TP server. By default, the value `1701` is specified.
MTU	The maximum size of units transmitted by the interface.
Enable debug mode	Move the switch to the right if you want to log all data on this VPN server debugging.
DNS	
Obtain DNS server addresses automatically	Move the switch to the right to let VPN server's clients obtain DNS server addresses of the WAN connection which is selected from the **Interface** list. Upon that the **Primary DNS** and **Secondary DNS** fields are not available for editing.
Primary DNS/ Secondary DNS	Enter addresses of the primary and secondary DNS servers in the relevant fields.

If you want to specify the list of accounts to provide access to this server, click the **ADD** (+) button in the **Users List** section.

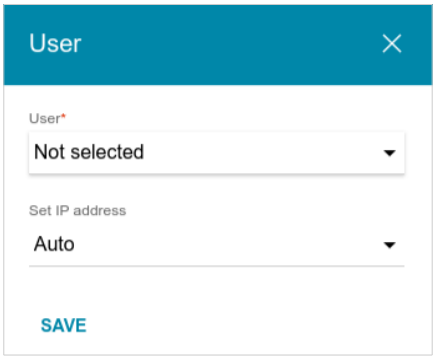

Figure 113. A window for adding a user.

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

Parameter	Description
User	Select a user account to allow access.
Set IP address	The mode of IP address assignment. Select a value from the drop-down list. • **Auto**: The IP address is assigned to the user automatically. • **Single IP**: The IP address is assigned to the user manually. When this value is selected, the **IP address** field is displayed.
IP address	Specify an IP address from the range specified in the **Start client IP** and **End client IP** fields.

Click the **SAVE** button.

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

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

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

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

VPN Users

On the **VPN / VPN Users** page, you can create user accounts to provide authorized access to a PPTP or L2TP server.

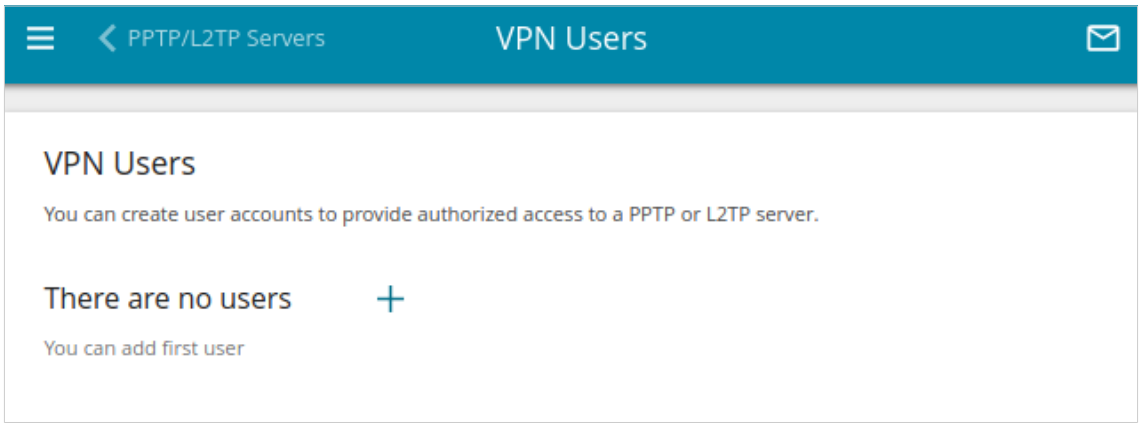

*Figure 114. The **VPN / VPN Users** page.*

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

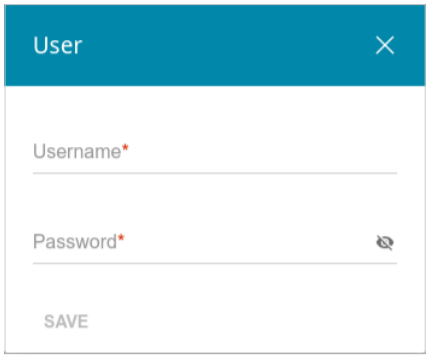

Figure 115. The window for adding a user.

In the opened window, in the **Username** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[8] Click the **Show** icon ( ) to display the entered key.

Click the **SAVE** button.

To view passwords of all user accounts, move the **Show password** switch to the right.

To edit the parameters of an account, select the relevant line in the table. In the opened window, enter a new value in the relevant field, and then click the **SAVE** button.

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

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

EoGRE

On the **VPN / EoGRE** page, you can configure VPN tunnels based on EoGRE technology.

EoGRE (*Ethernet over GRE*) technology allows transferring traffic through VPN tunnels in heterogeneous networks, encapsulating Ethernet packets with the help of GRE protocol and transferring them over a network which uses a network protocol of another level.

*Figure 116. The **VPN / EoGRE** page.*

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

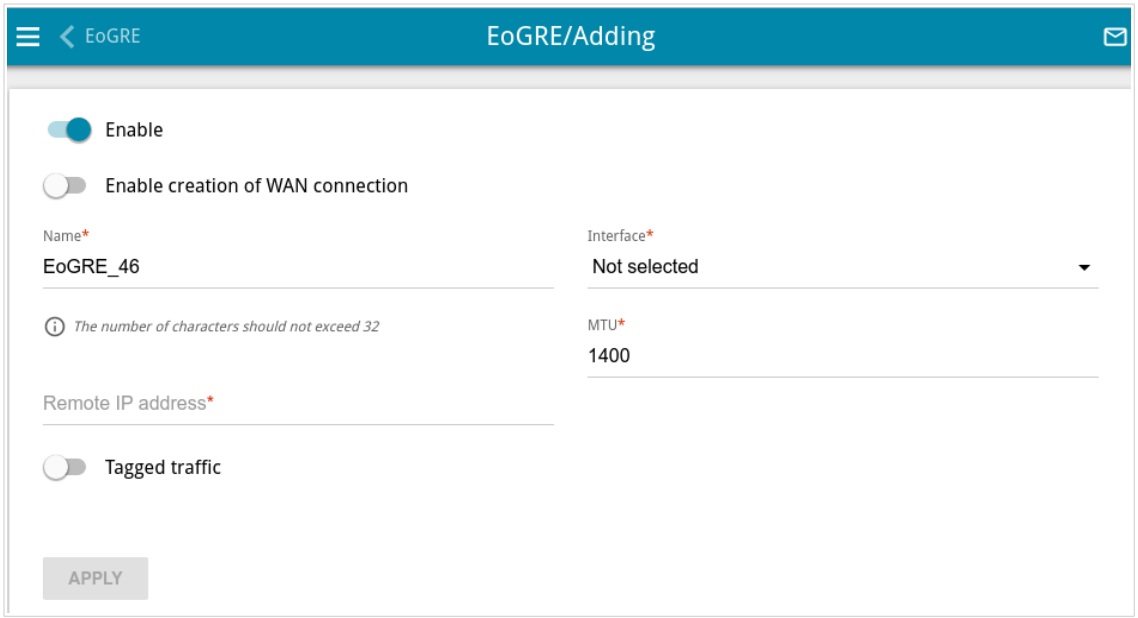

Figure 117. The page for adding an EoGRE tunnel.

You can specify the following parameters:

Parameter	Description
Enable	Move the switch to the right to enable the EoGRE tunnel. Move the switch to the left to disable the EoGRE tunnel.

Parameter	Description
Enable creation of WAN connection	Move the switch to the right to use the EoGRE tunnel as an interface for creating a WAN connection. For further configuration, you need to create a VLAN which will include the EoGRE interface (see the ***VLAN*** section, page 185), and then create a WAN connection which will be assigned to the interface of this VLAN (see the ***WAN*** section, page 75). Move the switch to the left if creating a WAN connection is not required.
Name	A name of the tunnel for easier identification. You can specify any name.
Remote IP address	Enter the IP address of the remote subnet VPN gateway.
Tagged traffic	Move the switch to the right to assign a tag (VLAN ID) to EoGRE traffic and specify the needed value in the **VLAN ID** field displayed.
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the **Default gateway** value to use the default WAN connection.
MTU	The maximum size of units transmitted by the interface.

After configuring all needed settings, 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 ( ).

VPN tunnels using EoGRE technology will appear in the **EoGRE interfaces** section on the **Advanced / VLAN** page and will be automatically removed from this section after the tunnel is deleted from the current page.

EoIP

On the **VPN / EoIP** page, you can configure VPN tunnels based on EoIP technology.

EoIP (*Ethernet over IP*) technology allows creating an Ethernet tunnel between two routers via connections which can transmit IP packets (e.g., IPIP, PPTP connections).

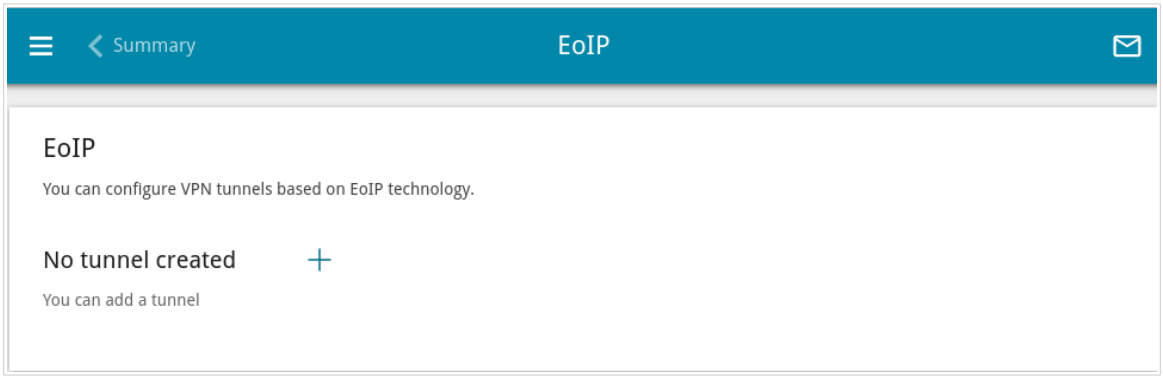

*Figure 118. The **VPN / EoIP** page.*

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

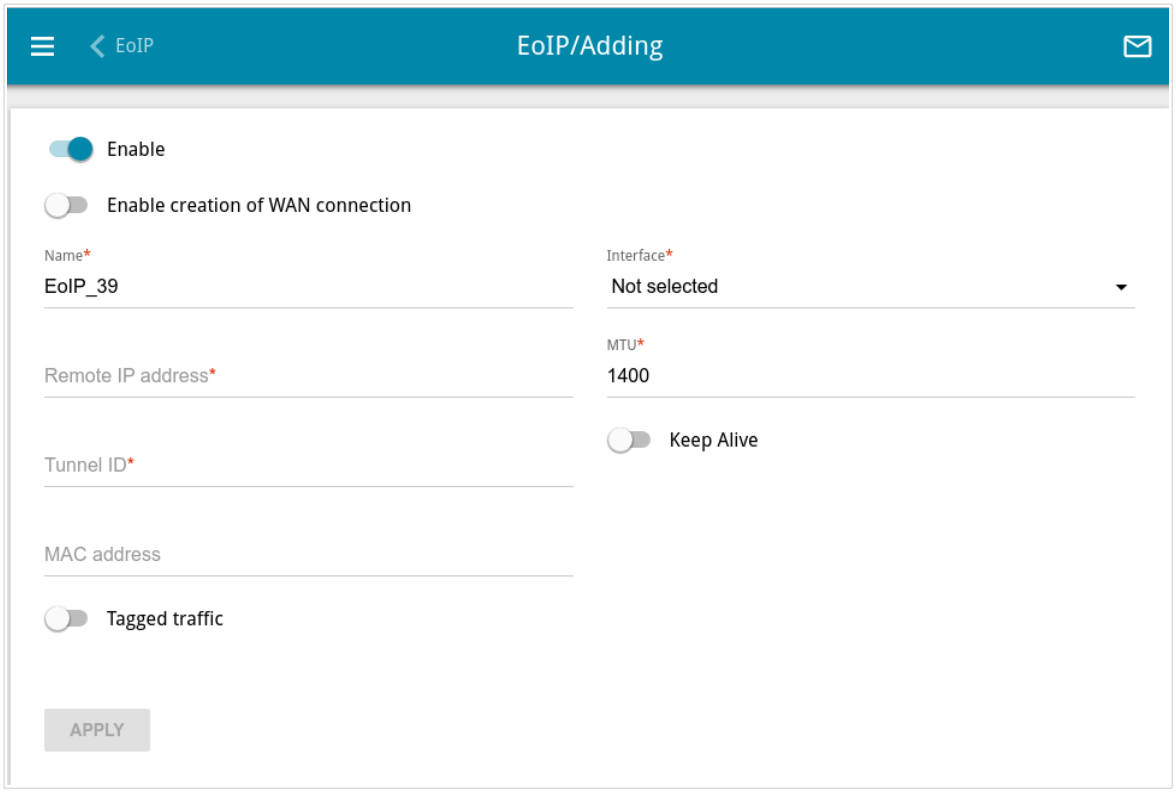

Figure 119. The page for adding an EoIP tunnel.

You can specify the following parameters:

Parameter	Description
Enable	Move the switch to the right to enable the EoIP tunnel. Move the switch to the left to disable the EoIP tunnel.
Enable creation of WAN connection	Move the switch to the right to use the EoIP tunnel as an interface for creating a WAN connection. For further configuration, you need to create a VLAN which will include the EoIP interface (see the ***VLAN*** section, page 185), and then create a WAN connection which will be assigned to the interface of this VLAN (see the ***WAN*** section, page 75). Move the switch to the left if creating a WAN connection is not required.
Name	A name of the tunnel for easier identification. You can specify any name.
Remote IP address	Enter the IP address of the remote subnet VPN gateway.
Tunnel ID	Specify a unique identifier of the tunnel. The value for both parties which establish the tunnel should be the same.
MAC address	A MAC address assigned to the EoIP tunnel interface. *Optional.* If the field is blank, the MAC address is assigned automatically.
Tagged traffic	Move the switch to the right to assign a tag (VLAN ID) to EoIP traffic and specify the needed value in the **Tag ID** field displayed.
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the **Default gateway** value to use the default WAN connection.
MTU	The maximum size of units transmitted by the interface.
Keep Alive	Move the switch to the right to let the router detect the state of the tunnel on the other end. In the **Interval** and **Attempts** fields displayed, specify the required values. The router sends several check requests. If after several failed attempts the connection on the other end of the tunnel is inactive, the tunnel will be disabled. Upon that it will be enabled automatically when the other end tries to establish the connection.
Interval	A time period (in seconds) allocated for one request to check the state of the tunnel on the other end. By default, the value **5** is specified.

Parameter	Description
Attempts	A number of failed attempts to check the state of the tunnel on the other end after which the tunnel is disabled. By default, the value **5** is specified.

After configuring all needed settings, 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 ( ).

VPN tunnels using EoIP technology will appear in the **EoIP interfaces** section on the **Advanced / VLAN** page and will be automatically removed from this section after the tunnel is deleted from the current page.

Wi-Fi

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

Basic Settings

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

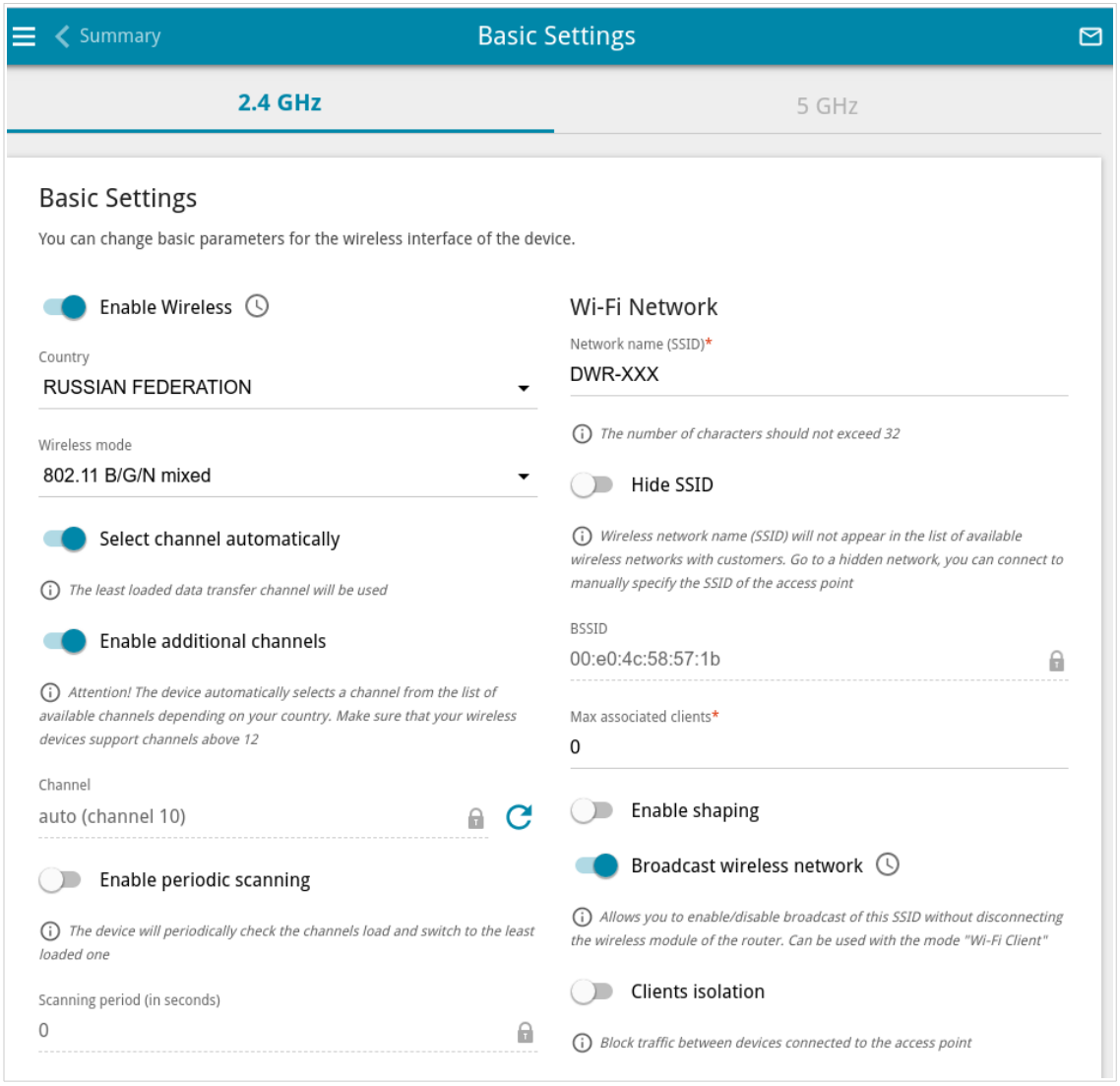

Figure 120. Basic settings of the wireless LAN in the 2.4GHz band.

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

Parameter	Description
Enable Wireless	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left. To enable/disable Wi-Fi connection on a schedule, click the **Set schedule** icon ( ). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list. To enable Wi-Fi connection at the time specified in the schedule and disable it at the other time, select the **Enable wireless connection** value from the **Action** drop-down list and click the **SAVE** button. To disable Wi-Fi connection at the time specified in the schedule and enable it at the other time, select the **Disable wireless connection** value from the **Action** drop-down list and click the **SAVE** button. To change or delete the schedule, click the **Edit schedule** icon ( ). In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.
Country	The country you are in. Select a value from the drop-down list.
Wireless mode	Operating mode of the wireless network of the router. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
Select channel automatically	Move the switch to the right to let the router itself choose the channel with the least interference.
Enable additional channels	If the switch is moved to the left, the device automatically selects one of available standard channels. To use additional channels (the 12th and 13th – in the 2.4 GHz band, the 100th and higher – in the 5 GHz band), move the switch to the right.

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

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

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

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

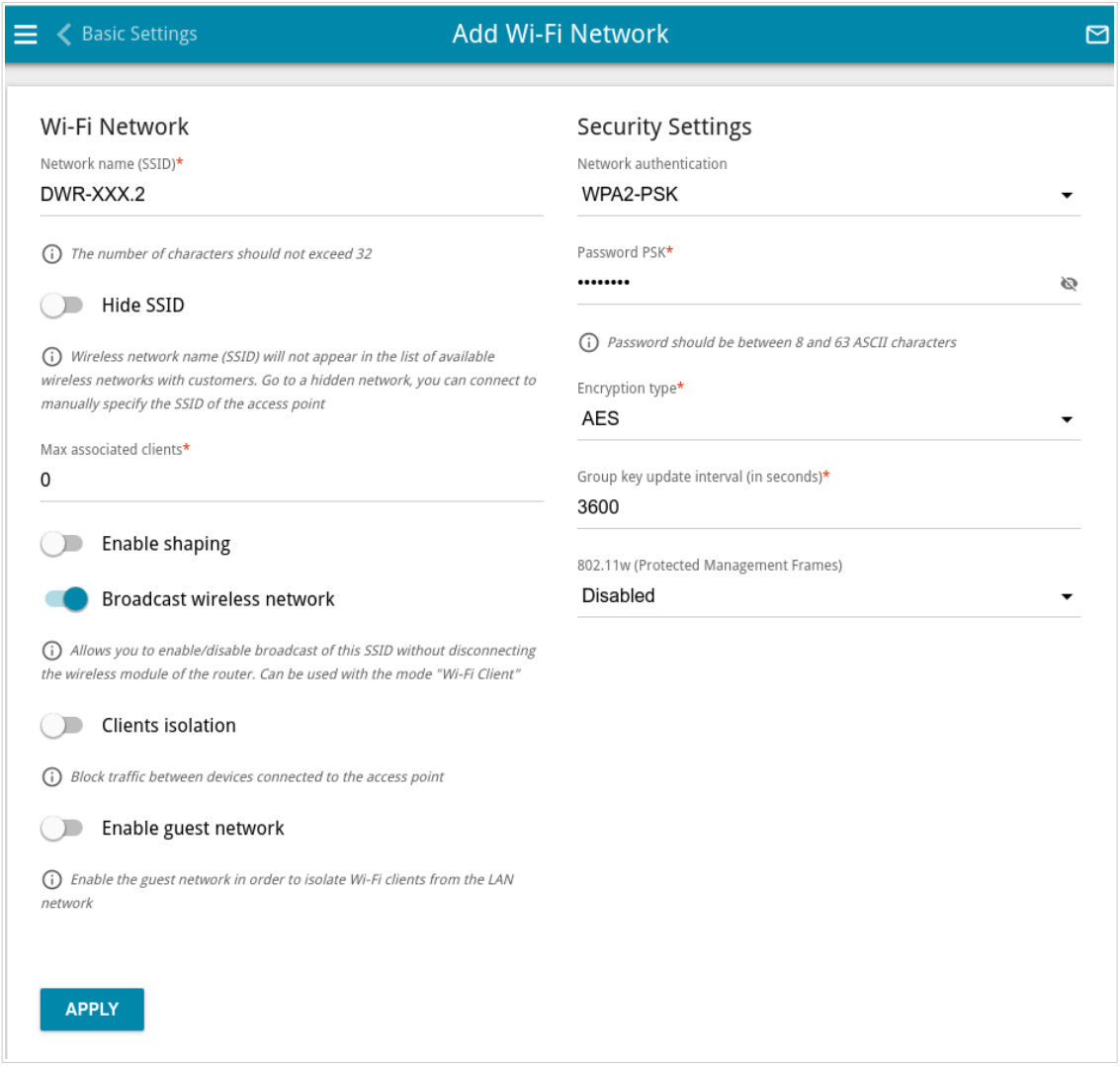

Figure 121. Creating a wireless network.

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

Parameter	Description
Enable shaping	Move the switch to the right to limit the maximum bandwidth of the wireless network. In the **Shaping** field displayed, specify the maximum value of speed (Mbps). Move the switch to the left not to limit the maximum bandwidth.
Broadcast wireless network	If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DWR-953 can connect to another access point as a wireless client. To enable/disable broadcasting on a schedule, click the **Set schedule** icon ( ). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list. To enable broadcasting at the time specified in the schedule and disable it at the other time, select the **Enable wireless network broadcasting** value from the **Action** drop-down list and click the **SAVE** button. When the wireless connection is disabled, the device will not be able to enable broadcasting of this wireless network on schedule. To disable broadcasting at the time specified in the schedule and enable it at the other time, select the **Disable wireless network broadcasting** value from the **Action** drop-down list and click the **SAVE** button. To change or delete the schedule, click the **Edit schedule** icon ( ). In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button. If you created an additional network, you can configure, change or delete a schedule for each network. To do this, click the button in the line of the network.
Clients isolation	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
Enable guest network	This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.

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

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

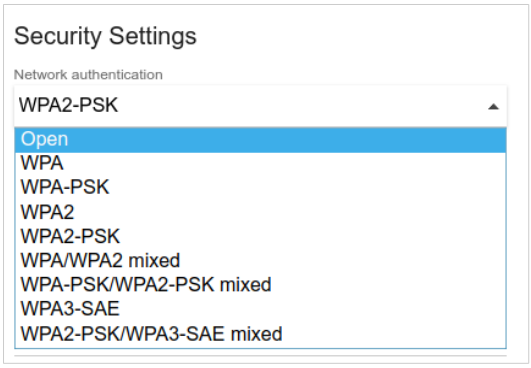

Figure 122. Network authentication types supported by the router.

The router supports the following authentication types:

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

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

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

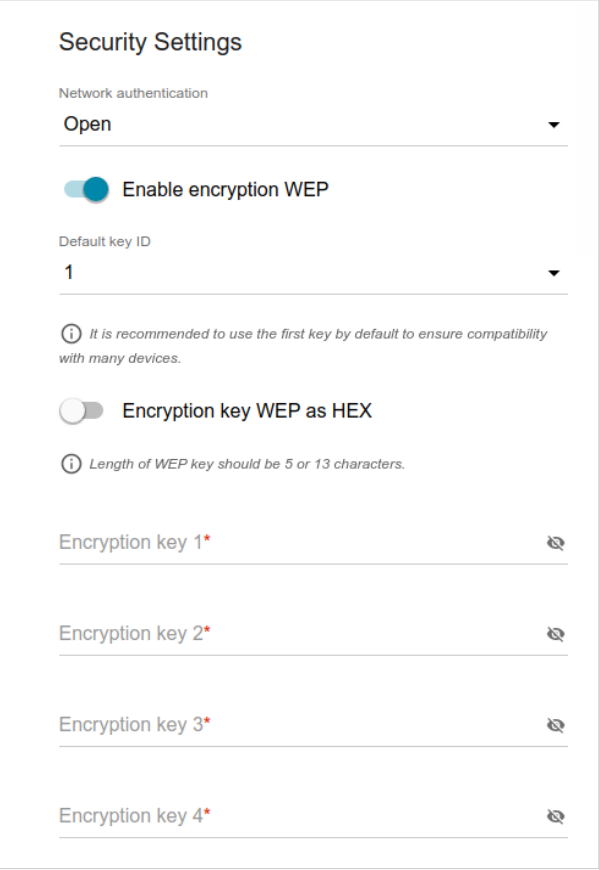

*Figure 123. The **Open** value is selected from the **Network authentication** drop-down list.*

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

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

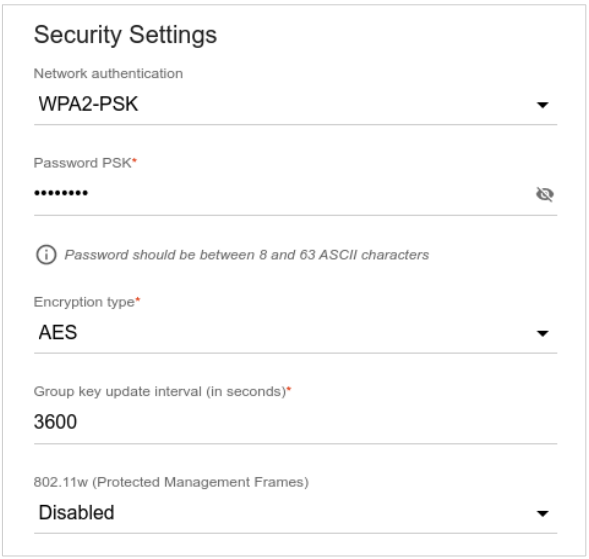

*Figure 124. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
Password PSK	A password for WPA encryption. The password can contain digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[9] Click the **Show** icon ( ) to display the entered password.
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**. ***TKIP*** *and* ***TKIP+AES*** *encryption types are not available for* ***WPA3-SAE*** *and* ***WPA2-PSK/WPA3-SAE mixed*** *authentication types.*
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value `0` is specified for this field, the key is not renewed.

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

Parameter	Description
802.11w (Protected Management Frames)	*For **WPA2-PSK**, **WPA3-SAE**, and **WPA2-PSK/WPA3-SAE mixed** authentication types only.* Protected Management Frames help to improve packet privacy protection for wireless data transmission. Select a value for the wireless network from the drop-down list. • **Disabled**: Protected Management Frames are not used. • **Optional**: Protected Management Frames are optional. • **Required**: Protected Management Frames are required. When this value is selected, devices not supporting the 802.11w standard cannot connect to the wireless network. The default value cannot be changed for **WPA3-SAE** and **WPA2-PSK/WPA3-SAE mixed** authentication types.

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

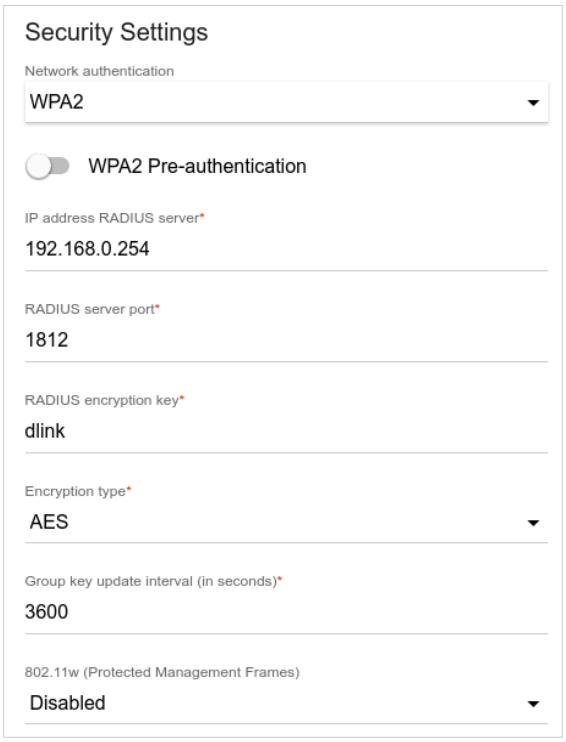

*Figure 125. The **WPA2** value is selected from the **Network authentication** drop-down list.*

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

Parameter	Description
RADIUS server port	A port of the RADIUS server.
RADIUS encryption key	The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings).
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value `0` is specified for this field, the key is not renewed.
802.11w (Protected Management Frames)	*For **WPA2** authentication type only.* Protected Management Frames help to improve packet privacy protection for wireless data transmission. Select a value for the wireless network from the drop-down list. • **Disabled**: Protected Management Frames are not used. • **Optional**: Protected Management Frames are optional. • **Required**: Protected Management Frames are required. When this value is selected, devices not supporting the 802.11w standard cannot connect to the wireless network.

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.

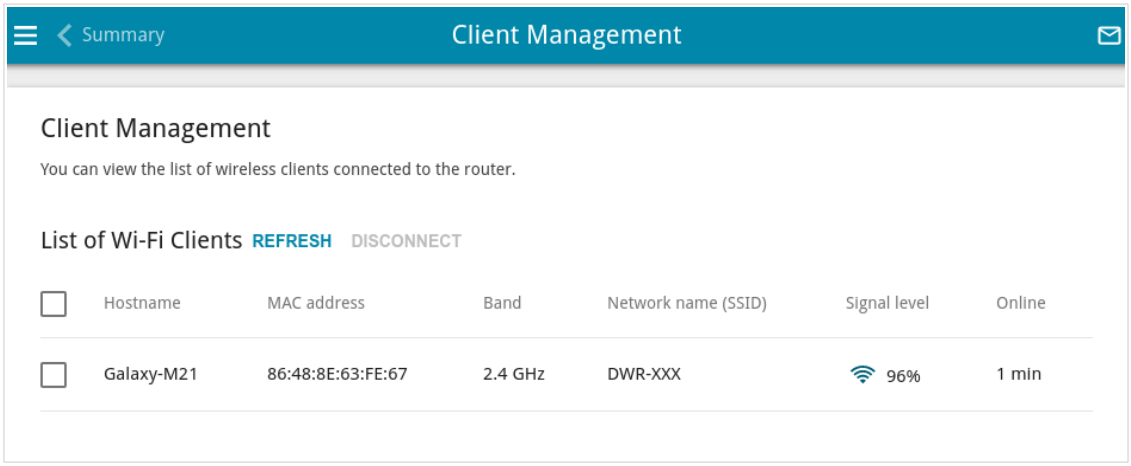

Figure 126. The page for managing the wireless clients.

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

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

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

WPS

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

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

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

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

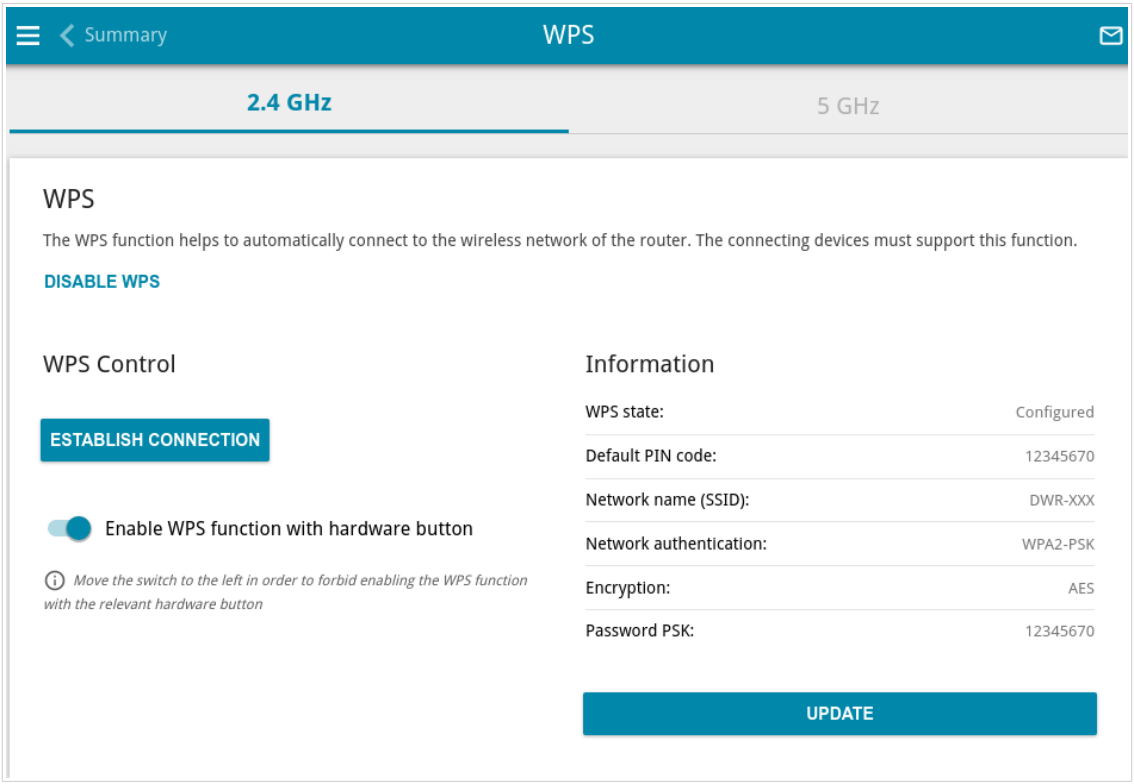

Figure 127. The page for configuring the WPS function.

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

To activate the WPS function via the hardware button, move the **Enable WPS function with hardware button** switch to the right on the tabs of both bands. Then, with the device turned on, press the **WPS** button and release. The **2.4GHz** and **5GHz** LEDs should start blinking slowly. In addition, upon pressing the button, the wireless interfaces of the device are enabled if they were disabled before.

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

To activate the WPS function via the web-based interface, 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
WPS state	The state of the WPS function: • **Configured** (all needed settings are specified; these settings will be used upon establishing the wireless connection) • **Unconfigured** (after activating the WPS function, the SSID and the encryption key will be configured automatically, the network authentication type will be changed to WPA2-PSK).
Default PIN code	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.
Network name (SSID)	The name of the router's wireless network.
Network authentication	The network authentication type specified for the wireless network.
Encryption	The encryption type specified for the wireless network.
Password PSK	The encryption password specified for the wireless network.
UPDATE	Click the button to update the data on the page.

Using WPS Function via Web-based Interface

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

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

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

1. Click the **ENABLE WPS** button.
2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.
3. In the opened window, select the **PBC** value from the **WPS method** drop-down list.
4. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
5. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
6. Right after that, click the **CONNECT** button in the web-based interface of the router.

Using WPS Function without Web-based Interface

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

1. Specify relevant security settings for the wireless network of the router.
2. Make sure that the **Enable WPS function with hardware button** switch is moved to the right on the tabs of both bands.
3. Click the **ENABLE WPS** button.
4. Close the web-based interface (click the **Logout** line of the menu).

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

1. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
2. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
3. Press the **WPS** button of the router and release. The **2.4GHz** and **5GHz** LEDs will start blinking slowly.

WMM

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

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

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

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

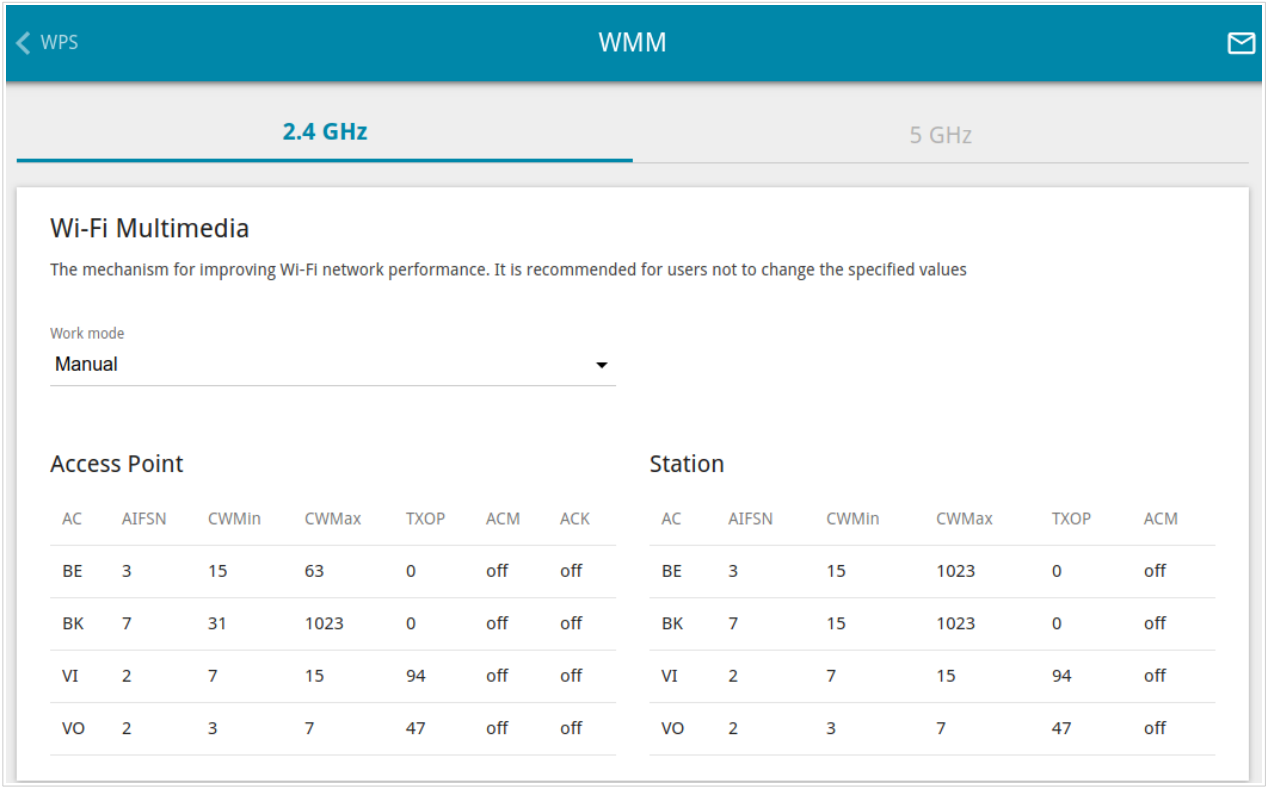

Figure 128. The page for configuring the WMM function.

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

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

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

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

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

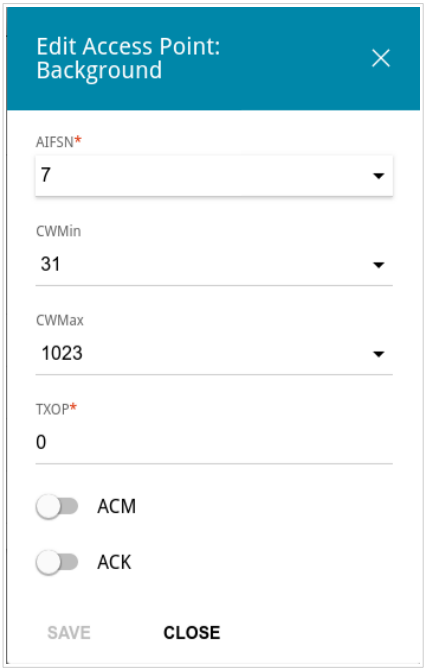

Figure 129. The window for changing parameters of the WMM function.

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

Parameter	Description
ACK	*Acknowledgment*. Answering response requests while transmitting. Displayed only in the **Access Point** section. If the switch is moved to the left, the router answers requests. If the switch is moved to the right, the router does not answer requests.

Click the **SAVE** button.

Client

On the **Wi-Fi / Client** page, you can configure the router as a client to connect to a wireless access point or to a WISP. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

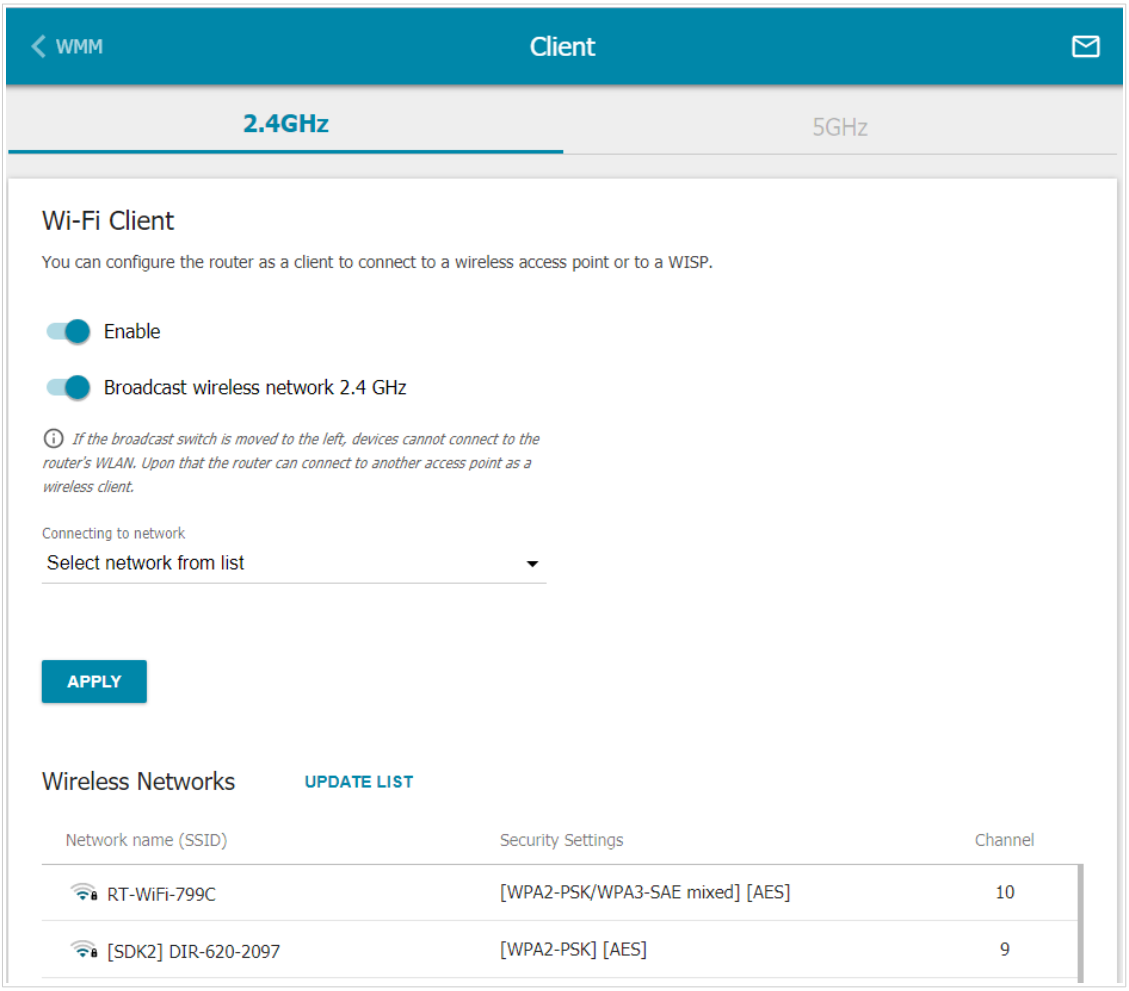

Figure 130. The page for configuring the client mode.

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

Parameter	Description
Broadcast wireless network 2.4 GHz / Broadcast wireless network 5 GHz	If the switch is moved to the left, devices cannot connect to the router's WLAN. Upon that the router can connect to another access point as a wireless client.
Connecting to network	A method for connecting to another access point.

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

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

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

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

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

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

When connecting to a wireless access point, the wireless channel of DWR-953 will switch to the channel of the access point to which you have connected.

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

If you want to connect to the WISP network, after configuring the device as a client, you need to create a WAN connection with relevant parameters for the **WiFiClient_2GHz** interface in the 2.4GHz band or for the **WiFiClient_5GHz** interface in the 5GHz band.

Client Shaping

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

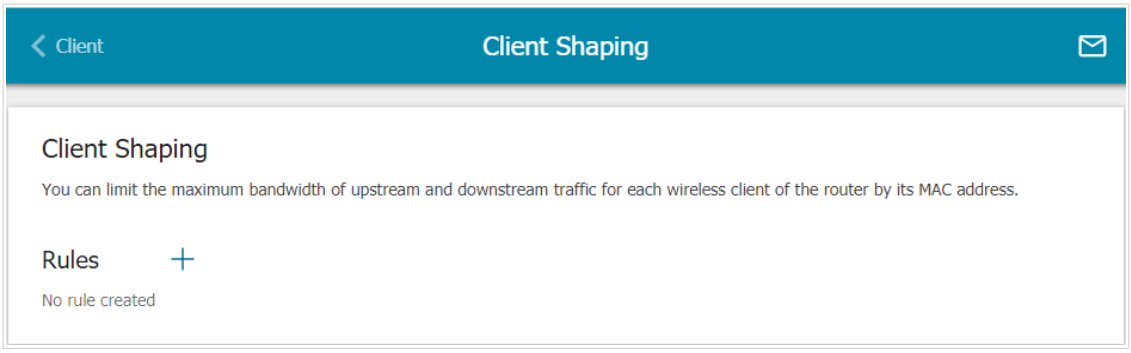

*Figure 131. The **Wi-Fi / Client Shaping** page.*

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

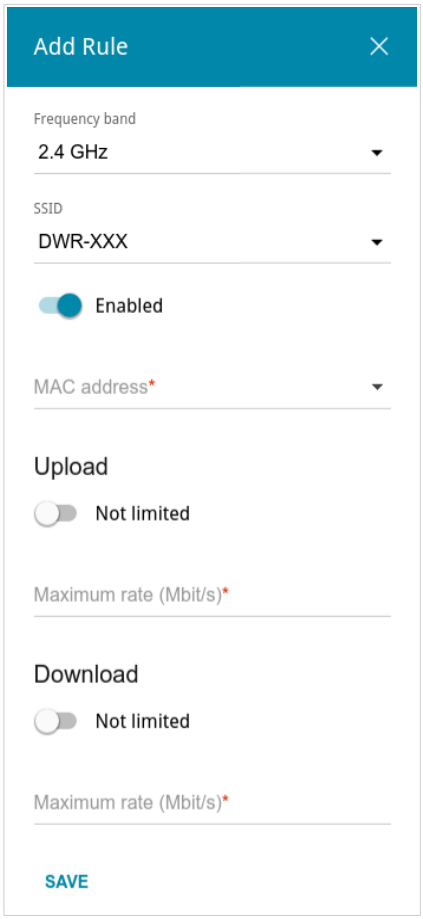

Figure 132. The window for setting up rate limit.

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

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

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

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

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

To set a schedule for the bandwidth limitation rule, click the **Set schedule** icon ( ) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

Additional

On page of the **Wi-Fi / Additional** section, you can define additional parameters for the WLAN of the router. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

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

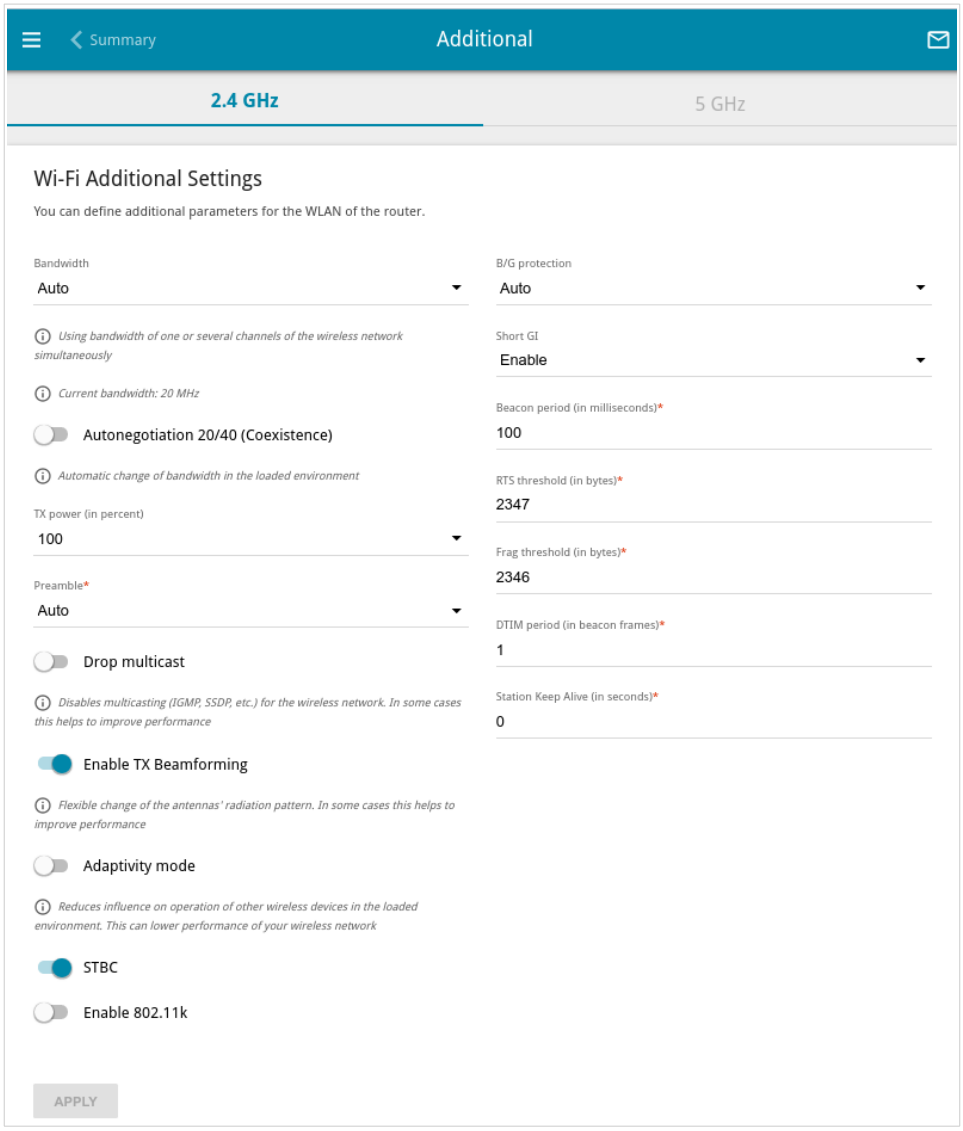

Figure 133. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	The channel bandwidth for 802.11n standard in the 2.4GHz band (the **2.4 GHz** tab). • **20 MHz**: 802.11n clients operate at 20MHz channels. • **20/40 MHz**: 802.11n clients operate at 20MHz or 40MHz channels. • **Auto**: The router automatically chooses the most suitable channel bandwidth for 802.11n clients. The channel bandwidth for 802.11n and 802.11ac standards in 5GHz band (the **5 GHz** tab). • **20 MHz**: 802.11n and 802.11ac clients operate at 20MHz channels. • **20/40 MHz**: 802.11n and 802.11ac clients operate at 20MHz or 40MHz channels. • **20/40/80 MHz**: 802.11ac clients operate at 20MHz, 40MHz, or 80MHz channels. • **Auto**: The router automatically chooses the most suitable channel bandwidth for 802.11n and 802.11ac clients.
Autonegotiation 20/40 (Coexistence)	*Available on the **2.4 GHz** tab.* Move the switch to the right to let the router automatically choose the most suitable channel bandwidth (20MHz or 40MHz) for the connected devices (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the **20/40 MHz** or **Auto** value is selected from the **Bandwidth** drop-down list.
TX power	The transmit power (in percentage terms) of the router.
Preamble	This parameter defines the length of the CRC block sent by the router when communicating to wireless devices. Select the needed value from the drop-down list. • **Auto**: The length of the block is defined automatically. • **Long**: The long block. • **Short**: The short block (this value is recommended for networks with high-volume traffic).

Parameter	Description
Enable DFS	*Available on the **5 GHz** tab.* Move the switch to the right to enable the DFS (*Dynamic Frequency Selection*) mechanism. Upon that the router uses the channels at which radars and other mobile or stationary radio systems can operate, but switches to other channels if these devices require this. In order to use the DFS mechanism, the automatic channel selection should be enabled (on the **Wi-Fi / Basic Settings** page). Move the switch to the left not to let the router use the channels at which radars and other mobile or stationary radio systems can operate.
Drop multicast	Move the switch to the right to disable multicasting for the router's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected on the **Advanced / IGMP** page.
Enable TX Beamforming	TX Beamforming is the signal processing/directing technique which helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation. Move the switch to the right to improve the signal quality.
Adaptivity mode	Move the switch to the right to let the router switch from the channels at which radars and other mobile or stationary radio systems operate in case it interferes with these devices. Such a setting can slow down the router's WLAN. In order to use the adaptivity mode, the automatic channel selection should be enabled (on the **Wi-Fi / Basic Settings** page).
Reduce power on OFDM modulation	*Available on the **5 GHz** tab.* Move the switch to the right to lower service signals strength for improving the quality of their transmission. Use the setting in case of problems with connecting wireless clients to the router.
STBC	The STBC (*Space-time block coding*) technique allows increasing data transfer reliability even for portable devices equipped with poor antennas (smartphones, pads, etc.) due to using several data streams and processing several versions or received data. Move the switch to the right if you need to use the STBC technique.

Parameter	Description
Enable 802.11k	802.11k standard allows faster roaming of clients between access points within the same network. Clients supporting 802.11k standard can request a list of neighbor access points with their signal levels and Wi-Fi channel numbers. The device does not need to probe all of the available channels, but selects an access point to roam to from the list. Move the switch to the right if you need to use 802.11k standard.
Enable 802.11v	802.11v roaming allows improving the wireless client load balancing. If the wireless access point supports 802.11v standard, then with a large number of devices connected to this point, a request may be sent to some clients to switch to a less loaded point with the same network parameters or to transfer from a loaded band to a freer band (in case the SSID and security settings are the same in both frequency bands) to improve operation of each client. The request is advisory, upon that the device does not forcibly disconnect clients. Move the switch to the right if you need to use 802.11v standard. The switch is displayed if the **Enable 802.11k** switch is moved to the right.
B/G protection	*Available on the **2.4 GHz** tab.* The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Select a value from the drop-down list. • **Auto**: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices). • **Always On**: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network). • **Always Off**: The protection function is always disabled.

Parameter	Description
Short GI	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices. • **Enable**: The router uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n and 802.11ac standards (see the value of the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page). • **Disable**: The router uses the 800 ns standard guard interval.
Beacon period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS threshold	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
Frag threshold	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).
DTIM period	The number of beacon frames between sending DTIM messages (messages notifying on broadcast or multicast transmission).
Station Keep Alive	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value **0** is specified, the checking is disabled.

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

MAC Filter

On the **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-953.

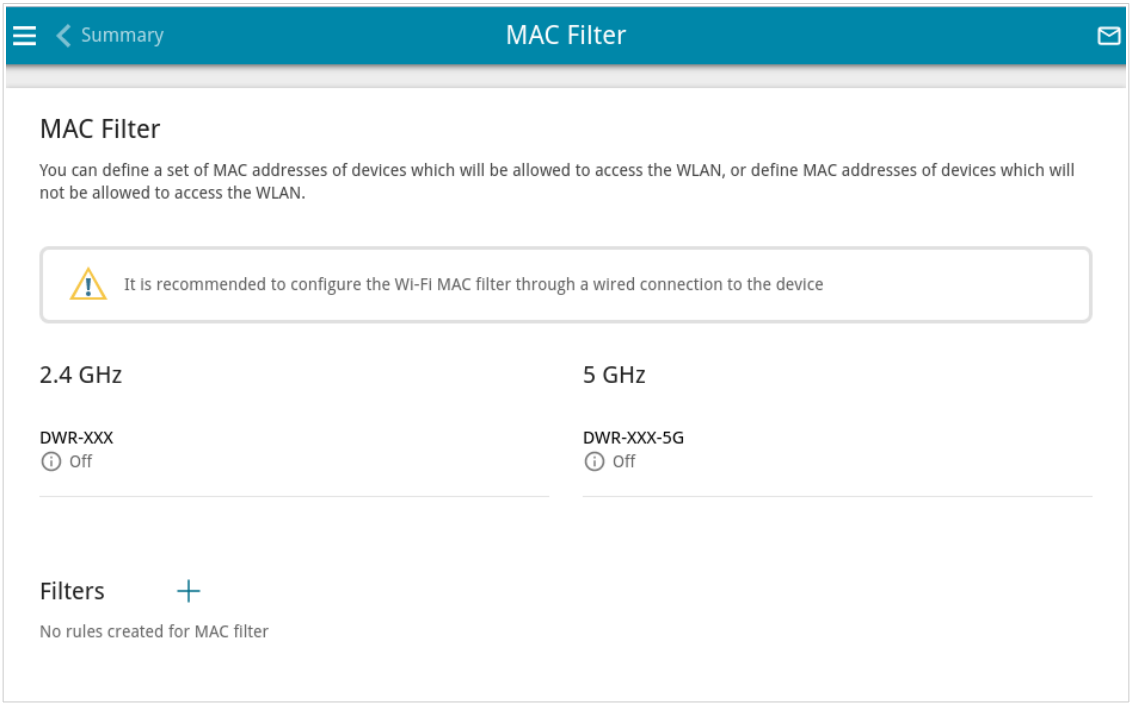

Figure 134. The page for configuring the MAC filter for the wireless network.

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 (+).

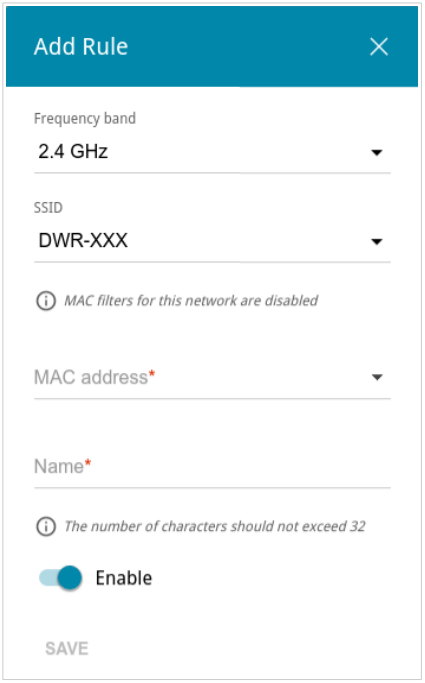

Figure 135. The window for adding a rule for the MAC filter.

You can specify the following parameters:

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

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

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

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

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

To open the basic or additional wireless network for the devices which MAC addresses are specified on this page and to close the wireless network for all other devices, in the section corresponding to the band (**2.4 GHz** or **5 GHz**), left-click the line of the wireless network. In the opened window, move the **Enable MAC filter** switch to the right. Upon that the **MAC filter restrict mode** drop-down list will be displayed. Select the **Allow** value from the drop-down list and click the **SAVE** button.

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

To set a schedule for the MAC filter rule, click the **Set schedule** icon ( ) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

Roaming

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

This function is designed for wireless networks based on several access points or routers. If the function is enabled for all access points (routers) which establish a wireless network, then wireless clients will always connect to the device with the highest signal level.

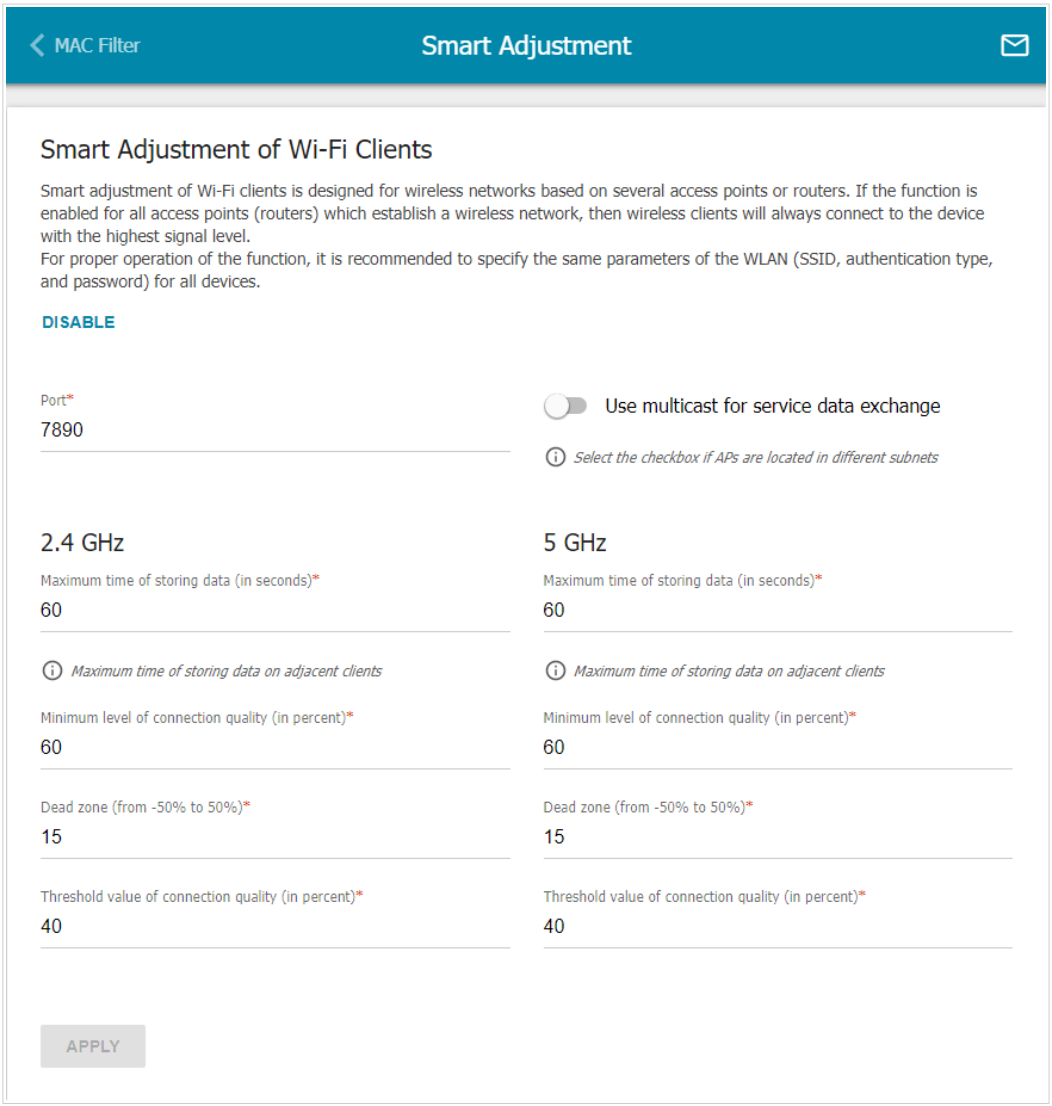

*Figure 136. The **Wi-Fi / Roaming** page.*

To enable the function, click the **ENABLE** button. Upon that the following settings are available on the page.

Parameter	Description
Port	The number of the port used for data exchange between access points (routers).
Use multicast for service data exchange	Move the switch to the right in order to use multicast traffic for service data exchange between access points (routers). This setting is needed if the devices which support the smart adjustment function are located in different subnets. If the switch is moved to the right, the **Multicast TTL** and **Multicast group address** fields are displayed on the page. If the switch is moved to the left, broadcast traffic is used for service data exchange.
Multicast TTL	Specify the TTL (*Time to live*) parameter value.
Multicast group address	Specify the address of the multicast group (from the subnet 239.255.0.0/16).
2.4 GHz / 5 GHz	
Maximum time of storing data	The maximum time period (in seconds) during which the access point (router) stores data on the signal strength of the client located on its coverage area.
Minimum level of connection quality	The signal strength upon which the access point (router) starts scanning other devices in order to find a device with a higher signal level.
Dead zone	This parameter is used for calculation of the signal strength upon which the smart adjustment function goes off. If the signal strength provided by another device is less than the sum of the **Minimum level of connection quality** field value and the **Dead zone** field value, then the client disconnects from the access point (router). You can specify the values from `-50%` to `+50%`.
Threshold value of connection quality	The signal strength upon which the access point (router) disconnects the client from its wireless network regardless of the signal levels of other devices. This value should not be greater than the value specified in the field **Minimum level of connection quality**.

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

To disable the function of smart adjustment of Wi-Fi clients, click the **DISABLE** 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 LTE modem is not disabled, the relevant notification will be displayed in the top right corner of the page.

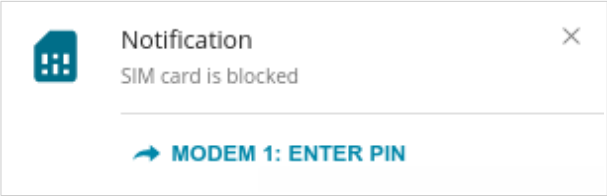

Figure 137. The notification on the PIN code check.

Click the **ENTER PIN** button and enter the PIN code in the **PIN input** window. Click the **Show** icon ( ) to display the entered code. Then click the **APPLY** button.

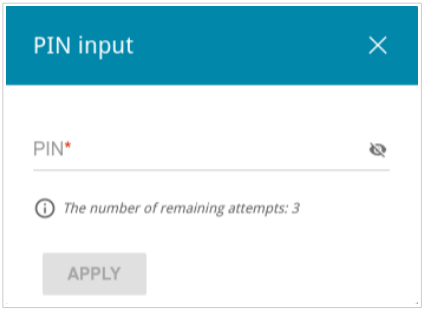

Figure 138. The window for entering the PIN code.

Basic Settings

On the **LTE Modem / Modem 1 / Basic Settings** page, you can view data on the built-in LTE modem, change the PIN code of the SIM card inserted into the LTE modem, and disable or enable the check of the PIN code.

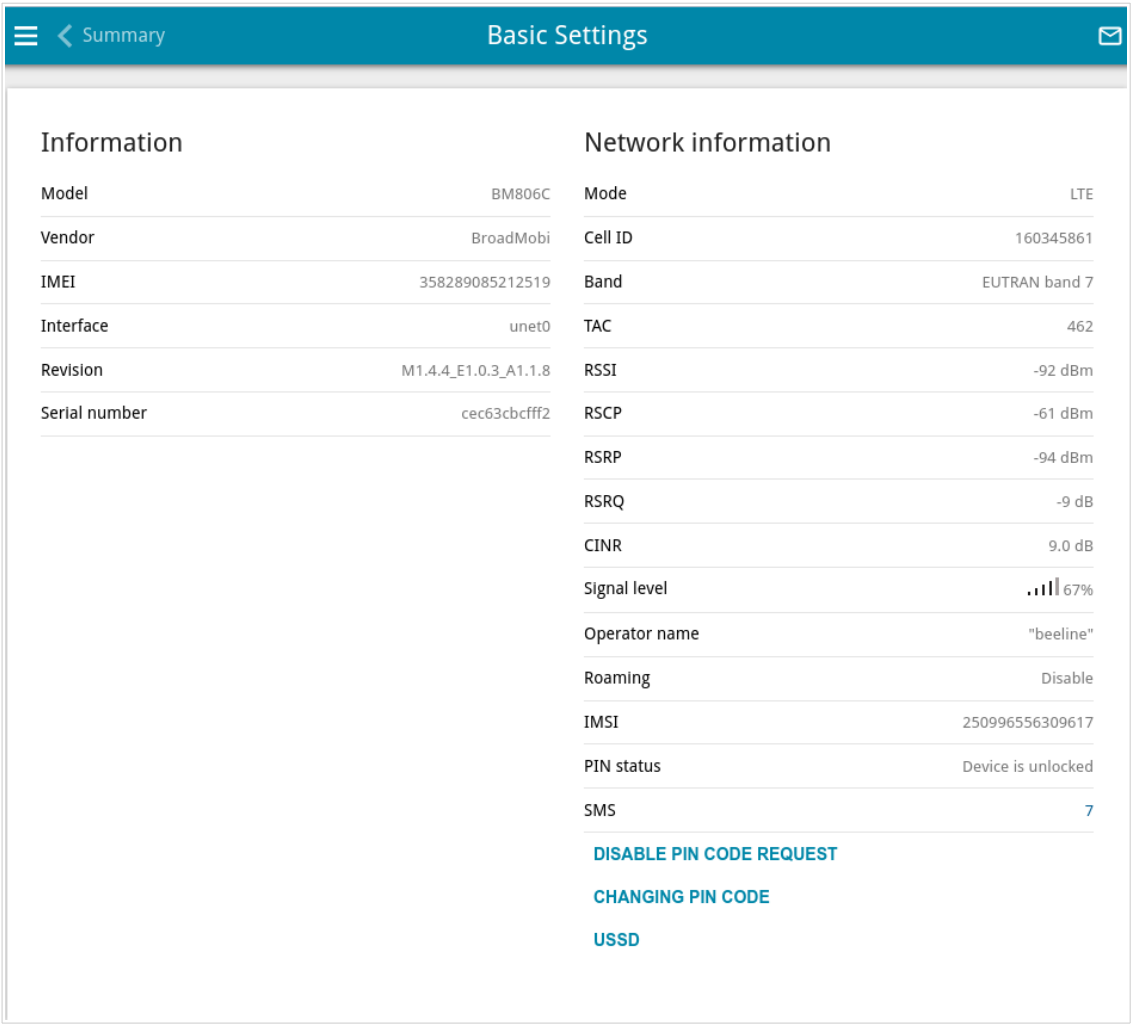

*Figure 139. The **LTE Modem / Modem 1 / Basic Settings** page.*

If the PIN code check for the SIM card of the LTE 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.

The following data are displayed on the page:

Parameter	Description
Information	
Model	The alphanumeric code of the model of the LTE modem.
Vendor	The manufacturer of the LTE modem.
IMEI	*International Mobile Equipment Identity* The code stored in the memory of the LTE modem.
Interface	The network interface name.
Revision	The revision of the firmware of the LTE modem.
Serial number	The unique identifier assigned to the device by its manufacturer.
Network information	
Mode	A type of the network to which the LTE modem is connected.
Cell ID	Unique number to identify the Base Transceiver Station.
Band	The frequency band of the LTE modem.
TAC	Tracking Area Code.
RSSI	*Received Signal Strength Indicator* The strength of the signal received by the LTE modem.
RSCP	*Received Signal Code Power* The average power of the signal received by the LTE modem.
RSRP	*Reference Signal Received Power* The average power of the reference signals received by the LTE modem.
RSRQ	*Reference Signal Received Quality* The quality of the reference signals received by the LTE modem.
CINR	*Carrier to Interference + Noise Ratio* The ratio of the effective signal received by the LTE modem to noise and interference level.
Signal level	The signal level at the input of the LTE modem's receiver. The zero signal level shows that you are out of the coverage area of the selected operator's network.

Parameter	Description
Operator name	The name of the mobile operator proving the service.
Roaming	Roaming mode status of the SIM card inserted into the LTE modem.
IMSI	*International Mobile Subscriber Identity* The code stored in the SIM card inserted into the LTE modem.
PIN status	PIN code request status of the SIM card inserted into the LTE modem.
SMS	The number of text messages stored in the memory of the SIM card inserted into the LTE modem. Click the number of text messages in the line to go to **LTE Modem / Modem 1 / SMS** page.

If the PIN code check for the SIM card inserted into the LTE modem is not disabled, the **PIN INPUT** button is displayed on the page.

To disable the PIN code check, click the **DISABLE PIN CODE REQUEST** button (the button is displayed if the PIN code check is enabled). In the opened window, enter the current PIN code in the **PIN code** field and click the **DISABLE** button.

To enable the PIN code check, click the **ENABLE PIN CODE REQUEST** button (the button is displayed if the PIN code check is disabled). In the opened window, enter the PIN code used before disabling the check in the **PIN code** field and click the **ENABLE** button.

To change the PIN code, click the **CHANGING PIN CODE** button (the button is displayed if the PIN code check is enabled). In the opened window, 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 in the PIN input window), the SIM card inserted into the LTE modem is blocked.

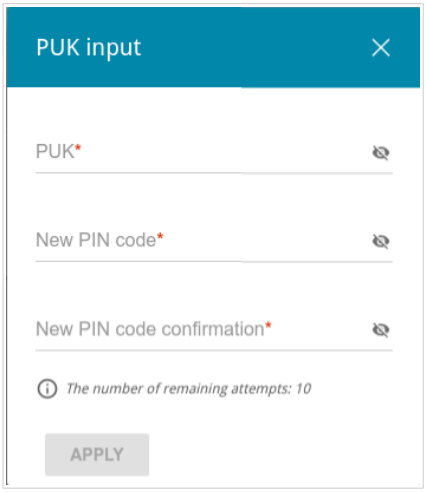

*Figure 140. The **LTE Modem / Modem 1 / Basic Settings** page. The window for PUK code input.*

For further use of the card, click the **PUK INPUT** button, 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** fields. Click the **Show** icon ( ) to display the entered values. Click the **APPLY** button.

Click the **USSD** button to go to the **LTE Modem / Modem 1 / USSD** page.

SMS

When a new text message is received, the relevant notification will be displayed in the top right corner of the page. Click the **CHECK** button. After clicking the button, the **LTE Modem / Modem 1 / SMS** page opens.

On the **LTE Modem / Modem 1 / SMS** page, you can create and send a text message and also view the history and status of sent and received messages stored in the memory of the SIM card.

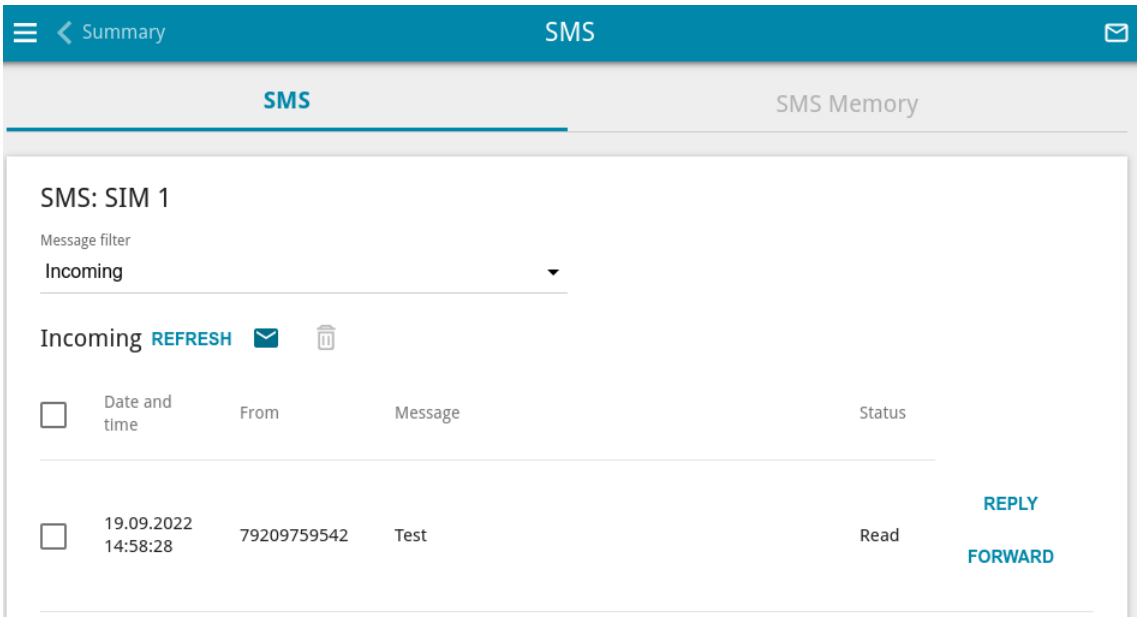

*Figure 141. The **LTE Modem / Modem 1 / SMS** page. The **SMS** tab.*

To view all outgoing and incoming messages on the **SMS** tab, 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 create and send a text message, click the **New message** button ( ).

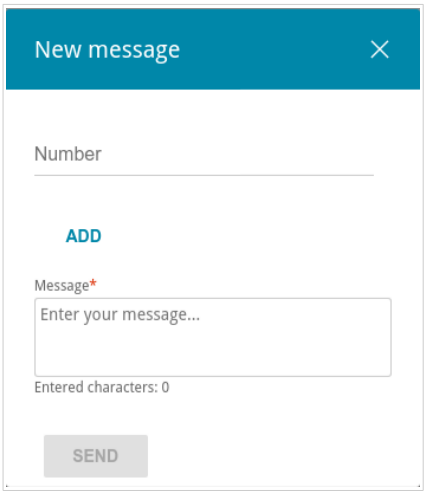

Figure 142. The window for creating a new text message.

In the **Number** field, enter the recipient's phone number. If you need to send the text message to several recipients, click the **ADD** button, and in the line displayed, enter a phone number. Enter the text of the message in the **Message** field and click the **SEND** button.

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

To reply to an incoming message, click the **REPLY** button in the line corresponding to the message.

To forward an incoming message, click the **FORWARD** button in the line corresponding to the message.

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

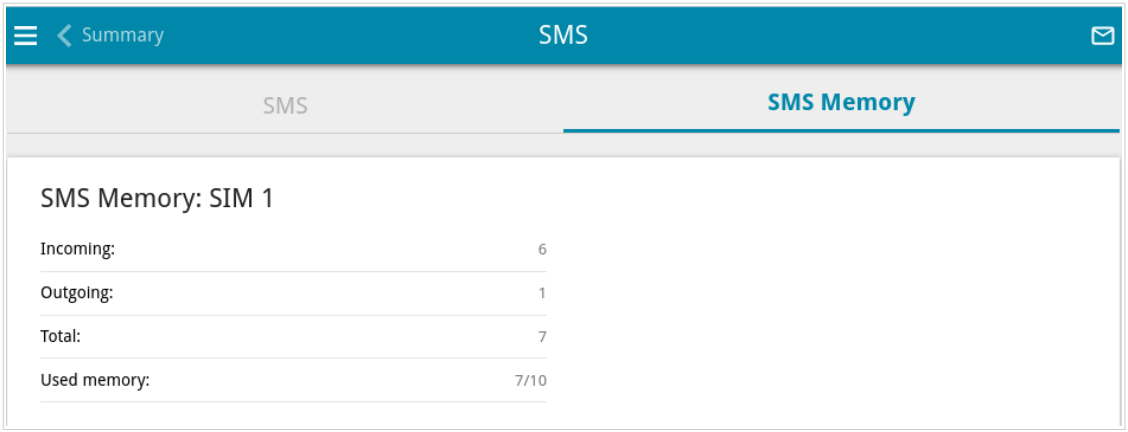

*Figure 143. The **LTE Modem / Modem 1 / SMS** page. The **SMS Memory** tab.*

USSD

On the **LTE Modem / Modem 1 / USSD** page, you can send a USSD command for the SIM card.[10]

USSD (*Unstructured Supplementary Service Data*) is a technology which provides real-time message exchange between a subscriber and a mobile operator's special application. USSD commands are often used to check the SIM card balance, receive data on the rate plan or service packets, etc.

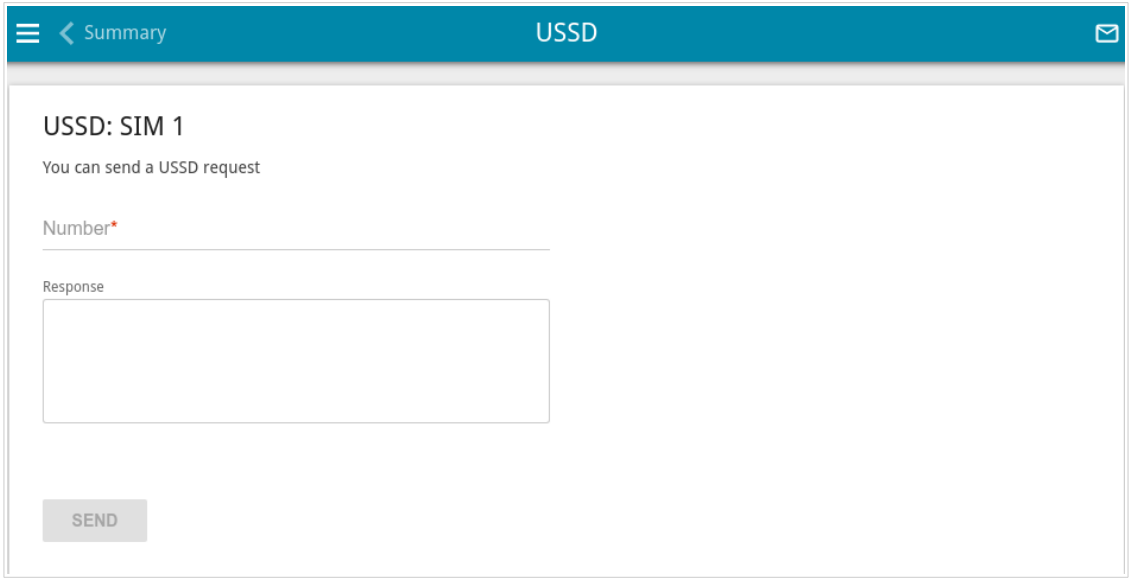

*Figure 144. The **LTE Modem / Modem 1 / USSD** page.*

In the **Number** field, enter a USSD command and click the **SEND** button. After a while, the results will be displayed in the **Response** field.

10 Contact your operator to get information on USSD commands and their functions.

Advanced

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

- create or edit VLANs
- allow the router to connect to a private Ethernet line
- add name servers
- configure a DDNS service
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the router
- configure notifications on the reason of the Internet connection failure
- define static routes
- configure TR-069 client
- enable the UPnP function
- enable the built-in UDPXY application for the router
- 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.

VLAN

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

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

- **LAN**: For the LAN interface, it includes the LAN port and Wi-Fi networks. You cannot delete this VLAN.
- **WAN**: For the WAN interface; it includes the **WAN** port. You can edit or delete this VLAN.

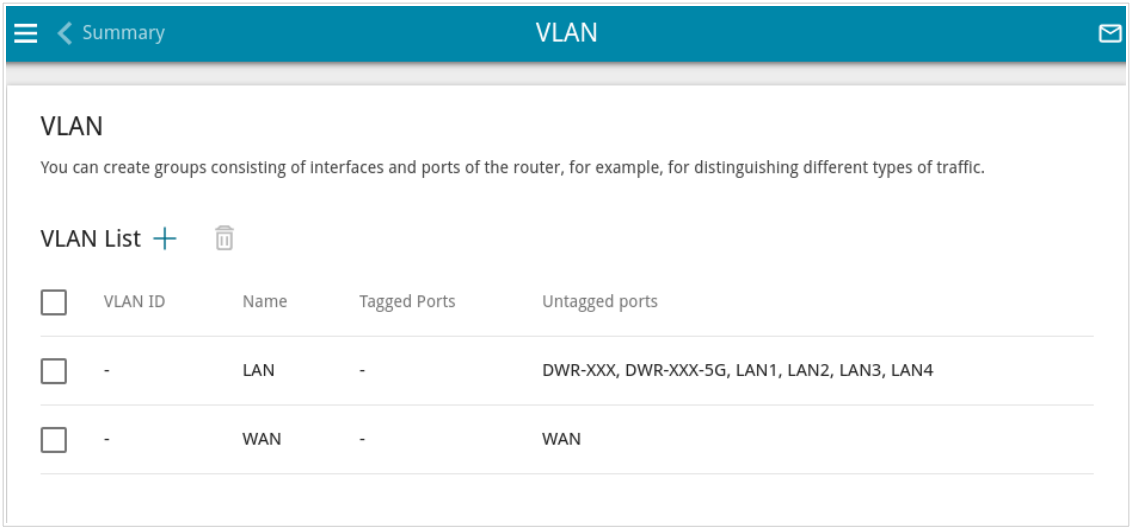

*Figure 145. The **Advanced / VLAN** page.*

In order to add an untagged LAN port or available Wi-Fi networks to an existing or new VLAN, first you need to exclude them from the **LAN** network on this page. To do this, select the **LAN** line. On the opened page, from the **Type** drop-down list of the element corresponding to the LAN port or Wi-Fi network, select the **Excluded** value and click the **APPLY** button.

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

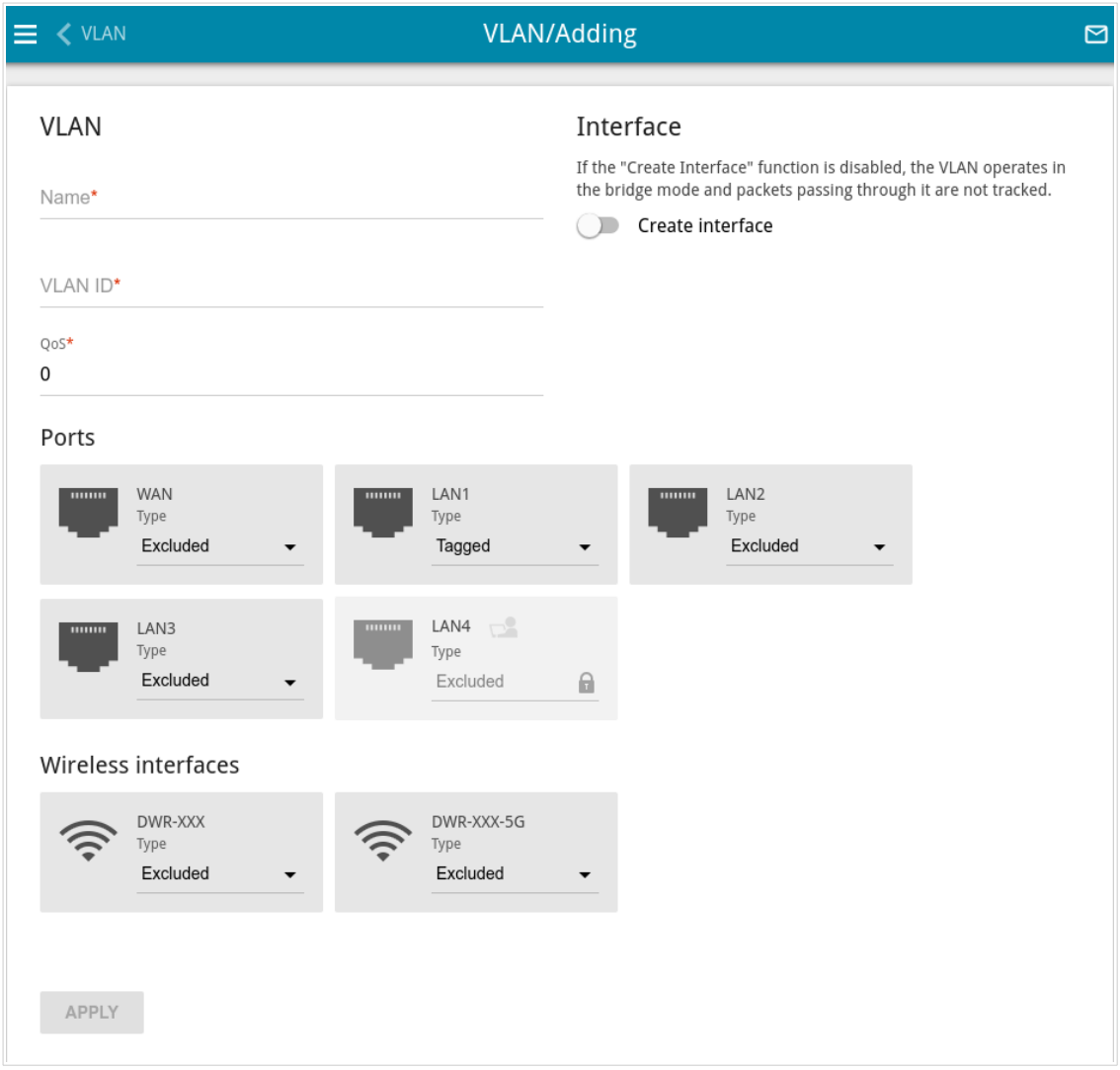

Figure 146. The page for adding a VLAN.

You can specify the following parameters:

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

Parameter	Description
Ports	Select a type for each port included in the VLAN. • **Untagged**: Untagged traffic will be transmitted through the specified port. • **Tagged**: Tagged traffic will be transmitted through the specified port. If at least one port of this type is included to the VLAN, it is required to fill in the **VLAN ID** and **QoS** fields. Leave the **Excluded** value for the ports not included in the VLAN.
Wireless interfaces	Select the **Untagged** value for each Wi-Fi interface included in the VLAN. Leave the **Excluded** value for the Wi-Fi interfaces not included in the VLAN.

Click the **APPLY** button.

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

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

WAN Remapping

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

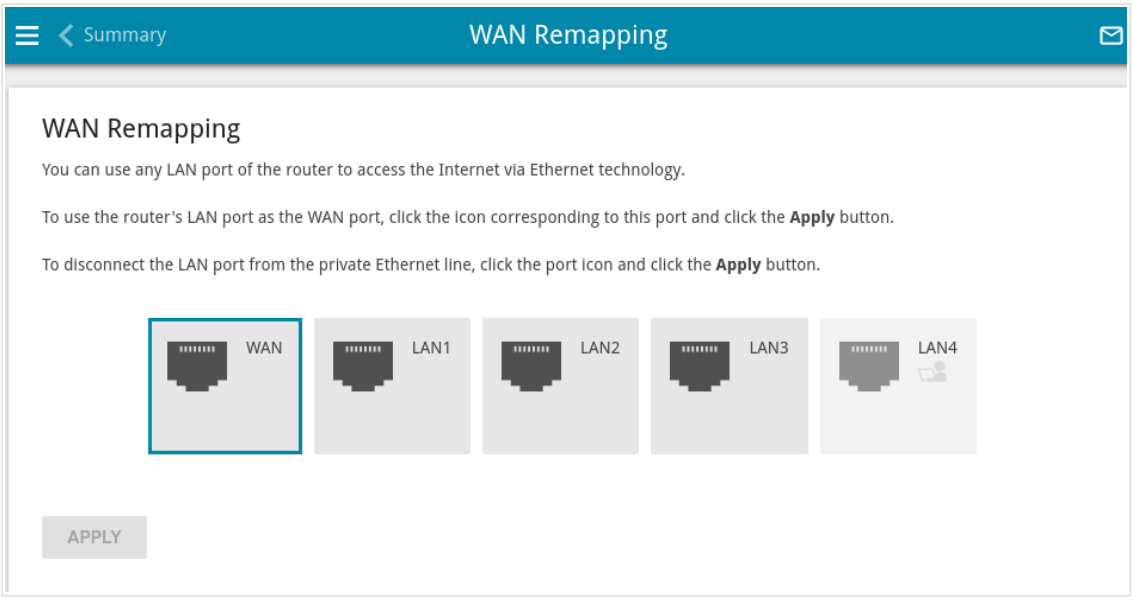

*Figure 147. The **Advanced / WAN Remapping** page.*

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.

DNS

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

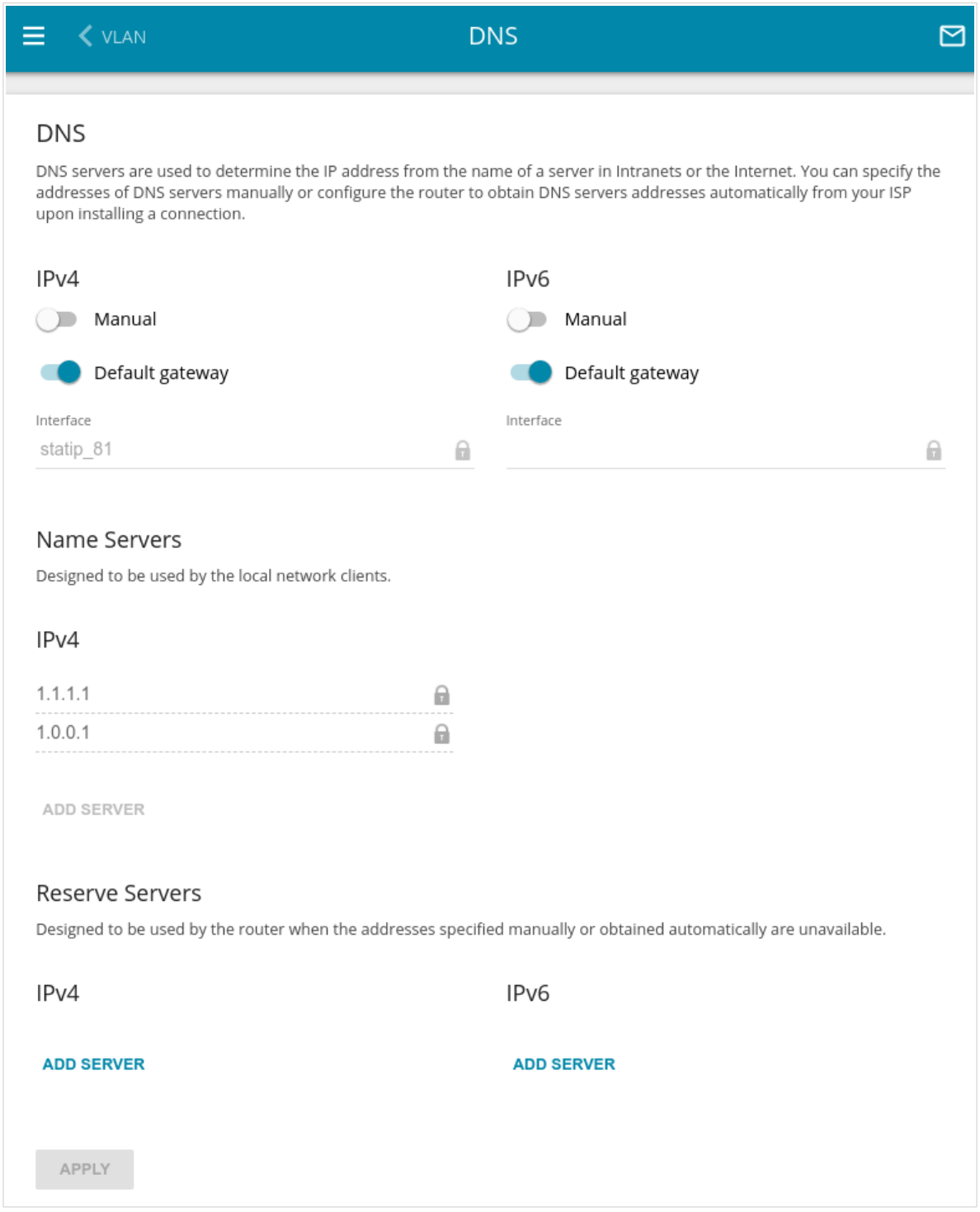

*Figure 148. The **Advanced / DNS** page.*

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

You can specify the addresses of DNS servers manually on this page or configure the router to obtain DNS servers addresses automatically from your ISP upon installing a connection. Also here you can specify addresses of reserve DNS servers which the router can use if the addresses specified manually or obtained automatically are unavailable.

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

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

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

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

To specify a reserve DNS server, in the **Reserve Servers** section of the relevant IP version, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server.

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

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

DDNS

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

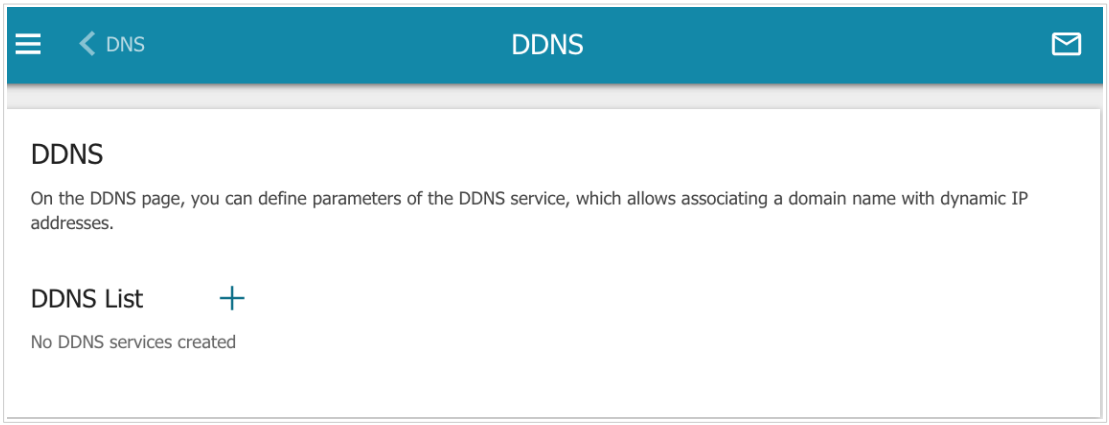

*Figure 149. The **Advanced / DDNS** page.*

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

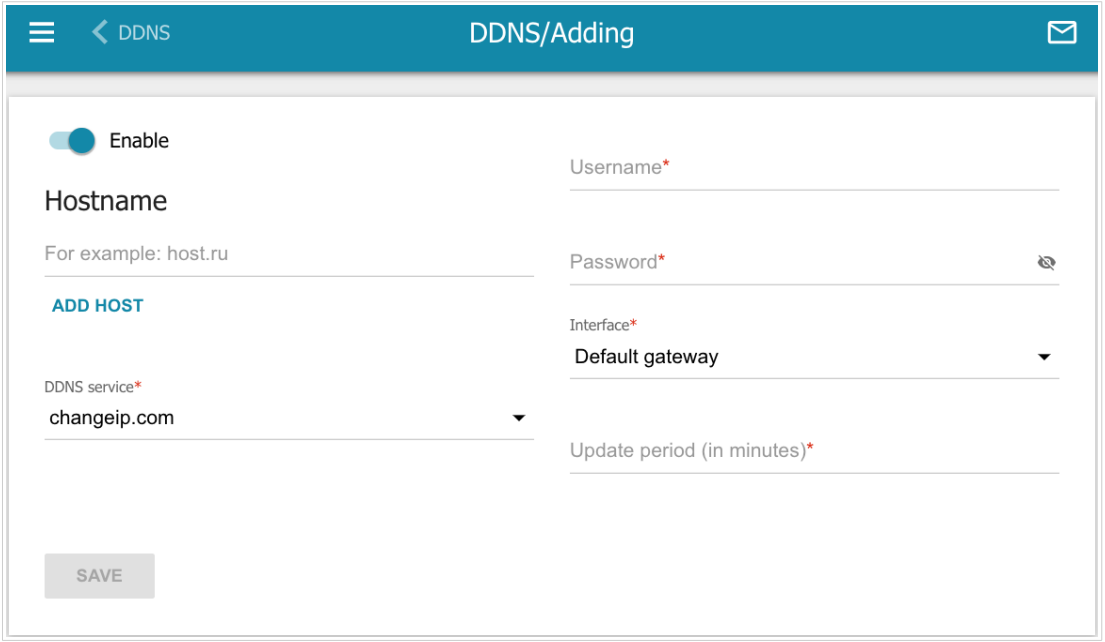

Figure 150. The page for adding a DDNS service.

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

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

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

To 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.

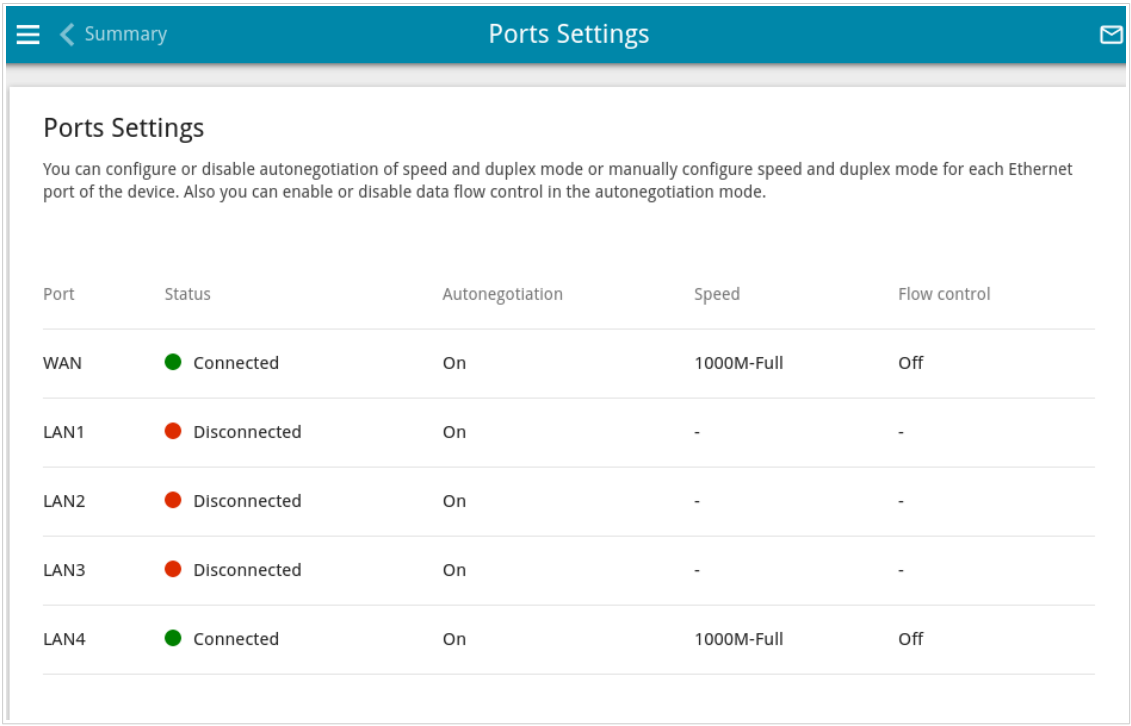

*Figure 151. The **Advanced / Ports Settings** page.*

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.

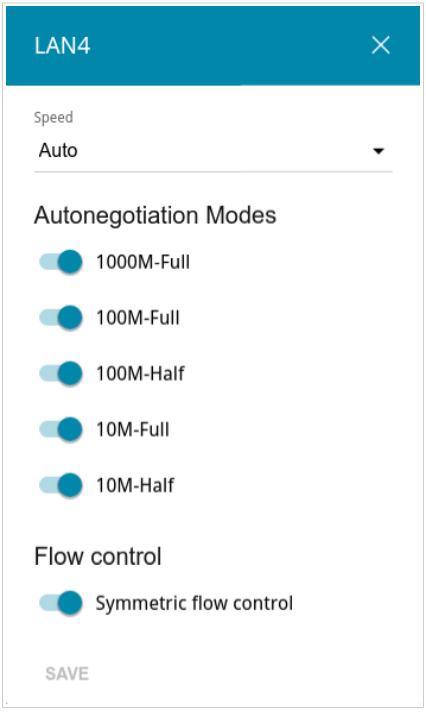

Figure 152. The window for changing the settings of the router's port.

In the opened window, specify the needed parameters:

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

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

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

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

Redirect

On the **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.

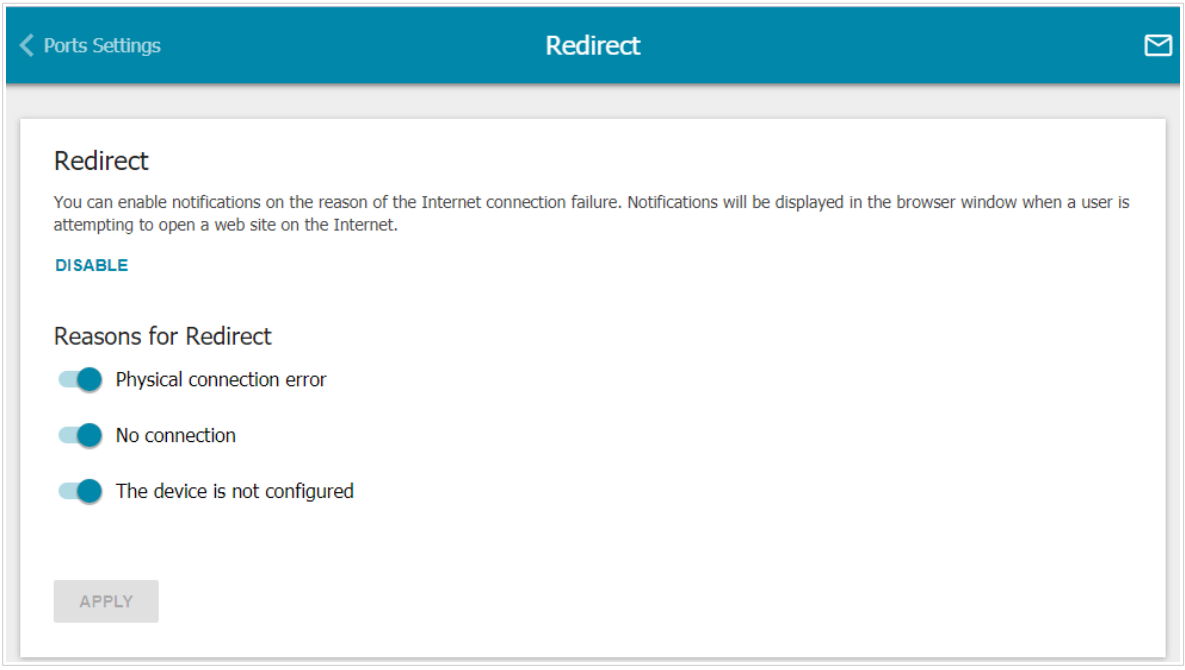

*Figure 153. The **Advanced / Redirect** page.*

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

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

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

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

Routing

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

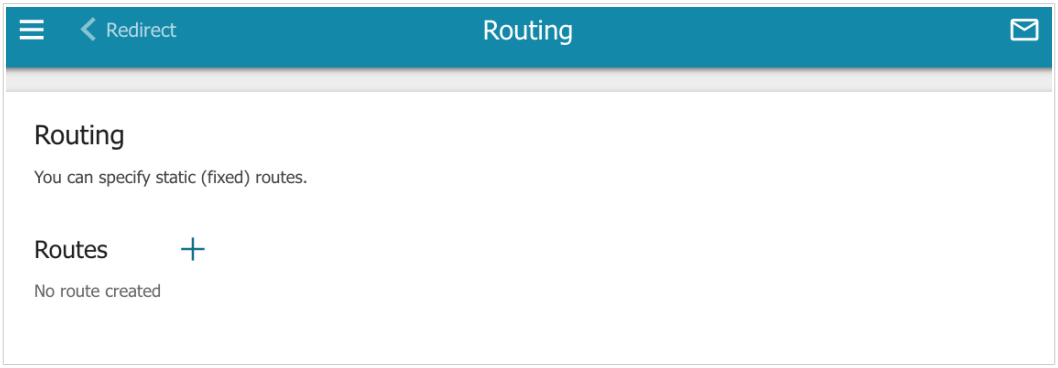

*Figure 154. The **Advanced / Routing** page.*

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

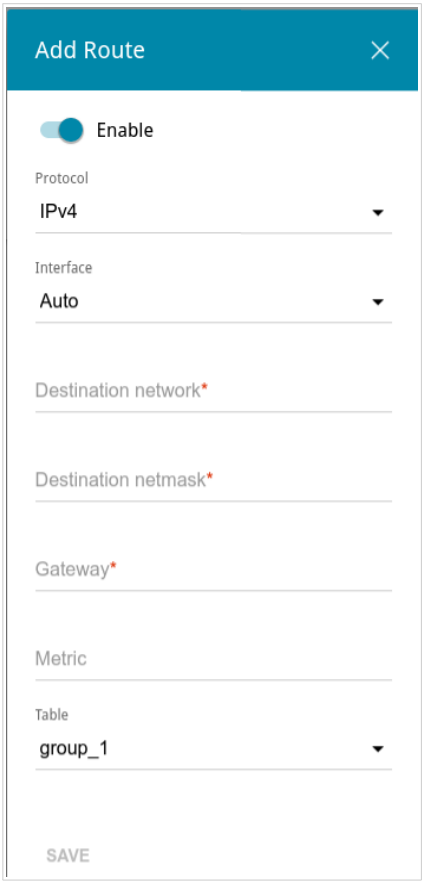

Figure 155. The window for adding a new route.

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

Parameter	Description
Enable	Move the switch to the right to enable the route. Move the switch to the left to disable the route.
Protocol	An IP version.
Interface	From the drop-down list, select an interface (connection) through which the device will communicate with the remote network. If you have selected the **Auto** value, the router itself sets the interface according to the data on the existing dynamic routes.
Destination network	A remote network which can be accessed with help of this route. You can specify an IPv4 or IPv6 address. The format of a host IPv6 address is `2001:db8:1234::1`, the format of a subnet IPv6 address is `2001:db8:1234::/64`.
Destination netmask	*For IPv4 protocol only.* The remote network mask.
Gateway	An IP address through which the destination network can be accessed.
Metric	A metric for the route. The lower the value, the higher is the route priority. *Optional*.
Table	From the drop-down list, select a routing table for the route. • **group_1** table is used to route user traffic. • **main** table is used to route management traffic from internal system services of the router.

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.

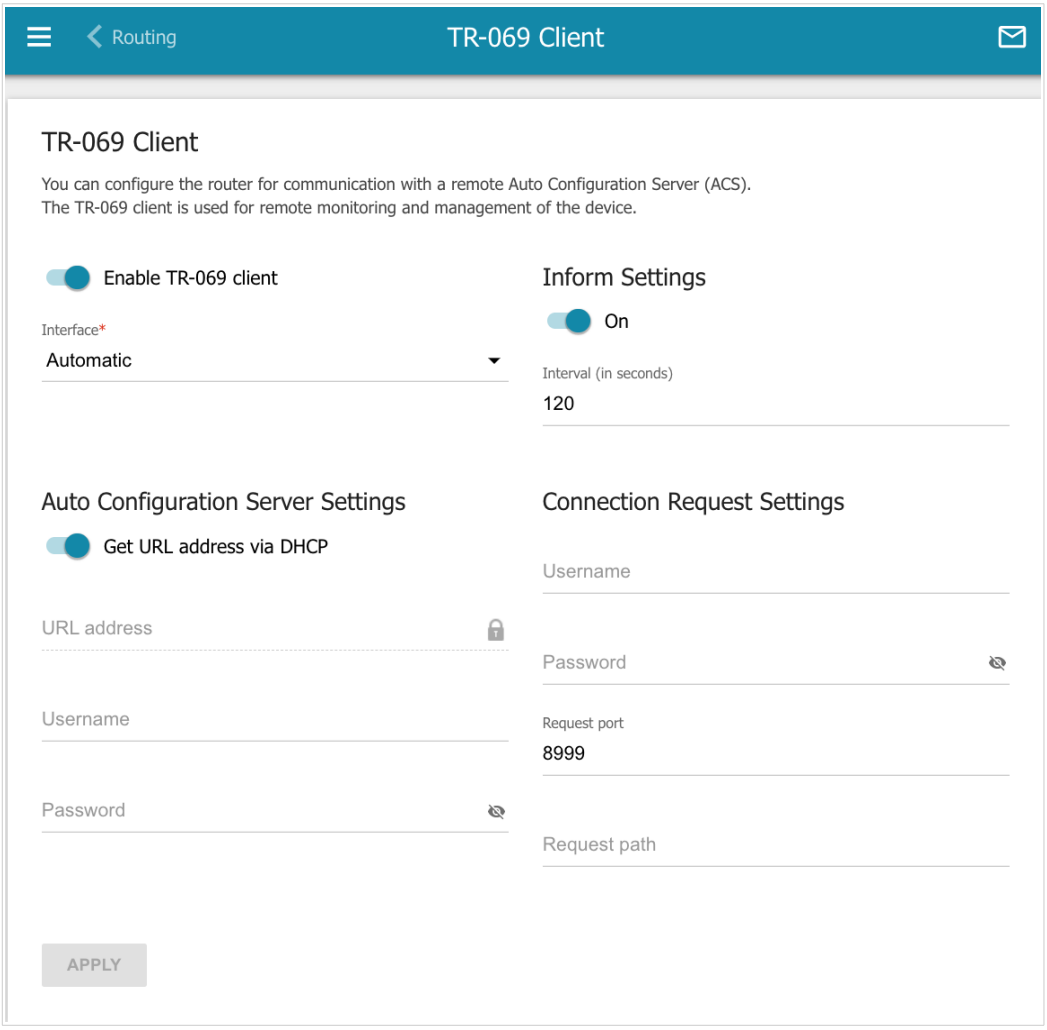

Figure 156. The page for configuring the TR-069 client.

You can specify the following parameters:

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

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

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

UPnP

On the **Advanced / UPnP** page, you can enable the UPnP function. The UPnP function allows to automatically create port forwarding rules for applications in the router's LAN requiring a connection from an external network.

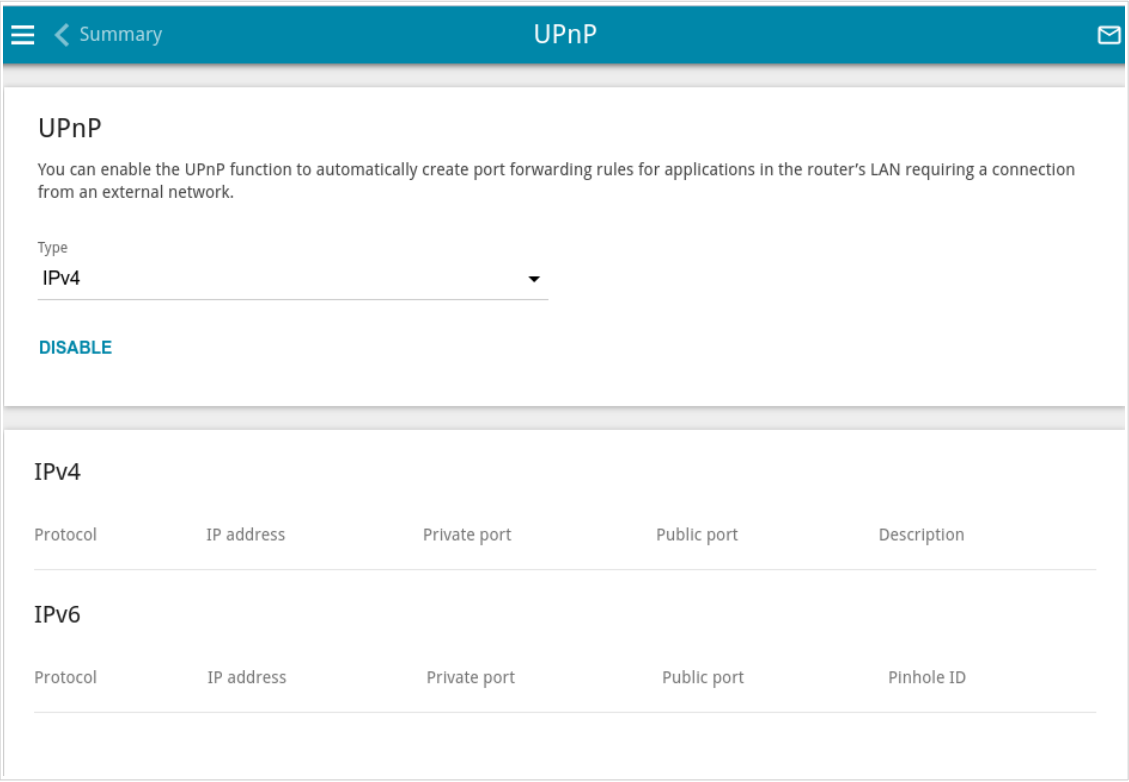

*Figure 157. The **Advanced / UPnP** page.*

By default, the UPnP function is enabled. You can also manually add port forwarding rules for network applications on the **Firewall / Virtual Servers** page. From the **Type** drop-down list, select the WAN connection type through which the function will operate.

- **IPv4**: When this value is selected, port forwarding rules will operate only through the IPv4 connection.
- **Dual**: When this value is selected, port forwarding rules will operate through IPv4 and IPv6 connections.

Port forwarding rules will be automatically created only in case the router's default WAN connection uses a public IP address.

When the function is enabled, the following parameters of the router are displayed on the page:

Parameter	Description
IPv4 / IPv6	
Protocol	A protocol for network packet transmission.
IP address	The IP address of a client from the local area network.

Parameter	Description
Private port	A port of a client's IP address to which traffic is directed from a public port of the router.
Public port	A public port of the router from which traffic is directed to a client's IP address.
Description	*For **IPv4** only.* Information transmitted by a client's network application.
Pinhole ID	*For **IPv6** only.* An identifier of the rule created for an incoming connection to the router.

If you want to disable the UPnP function, click the **DISABLE** button.

UDPXY

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

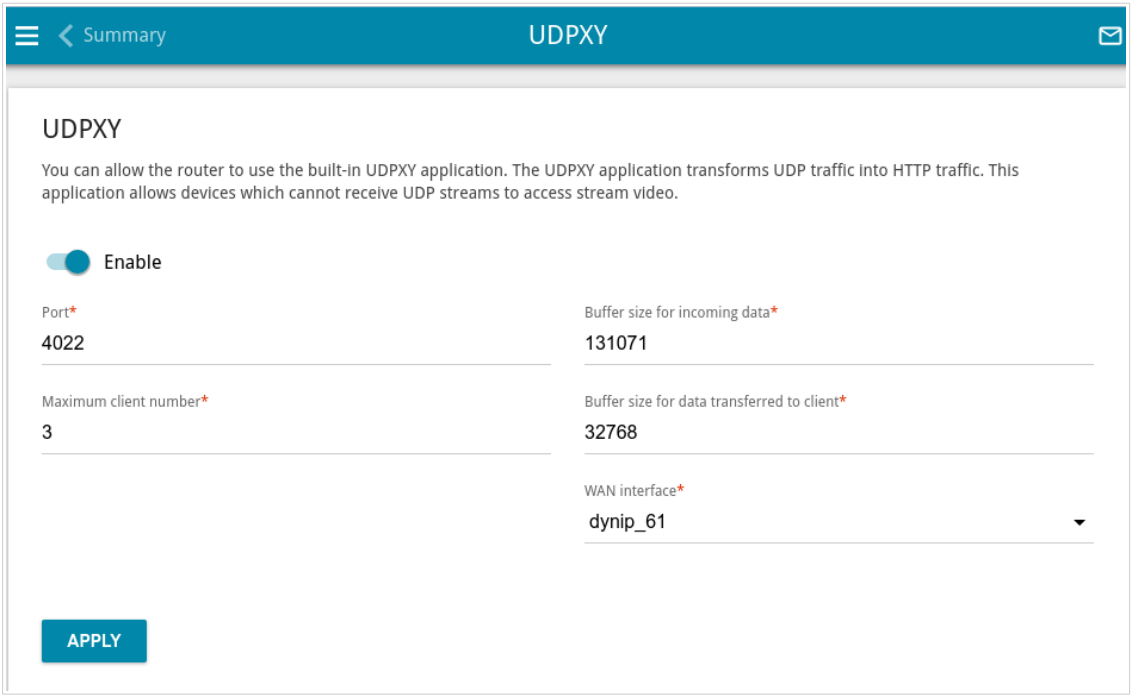

*Figure 158. The **Advanced / UDPXY** page.*

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

Upon that the following fields are displayed on the page:

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

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

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

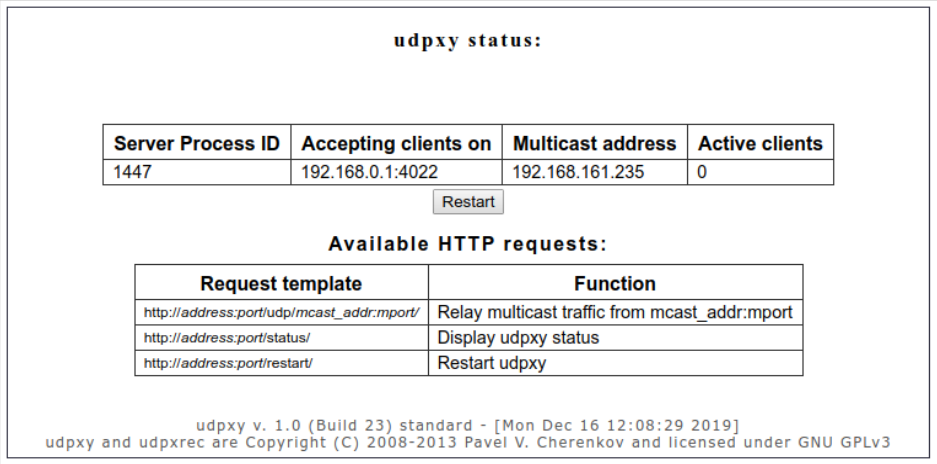

Figure 159. The UDPXY application status page.

IGMP

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

IGMP is used for managing multicast traffic (transferring data to a group of destinations) in IPv4 and networks. This protocol allows using network resources for some applications, e.g., for streaming video, more efficiently.

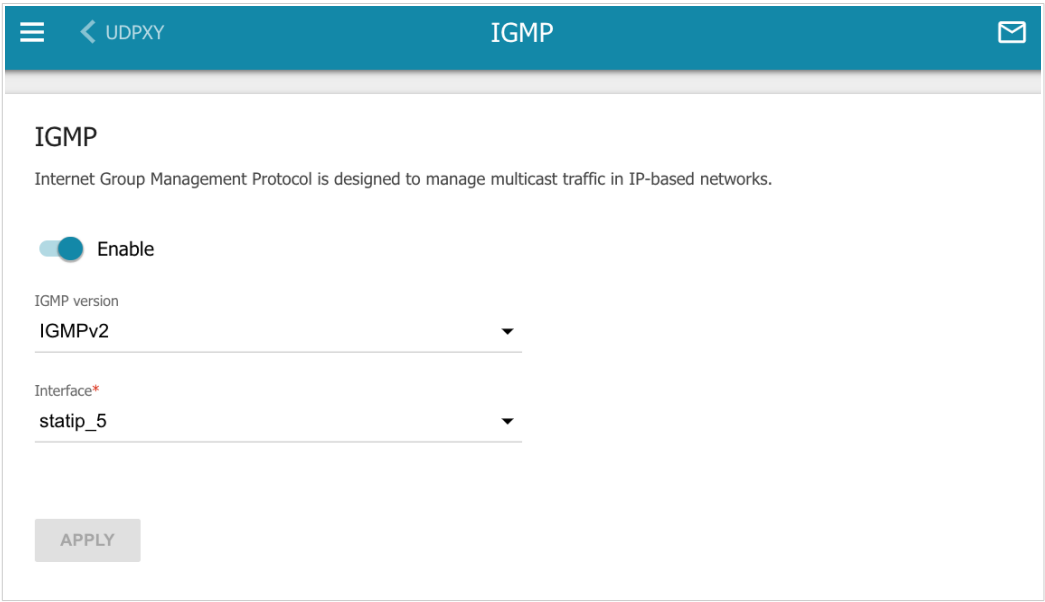

*Figure 160. The **Advanced / IGMP** page.*

The following elements are available on the page:

Parameter	Description
IGMP	
Enable	Move the switch to the right to enable IGMP.
IGMP version	Select a version of IGMP from the drop-down list.
Interface	From the drop-down list, select a connection of the Dynamic IPv4 or Static IPv4 type for which you need to allow multicast traffic (e.g. streaming video).

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.

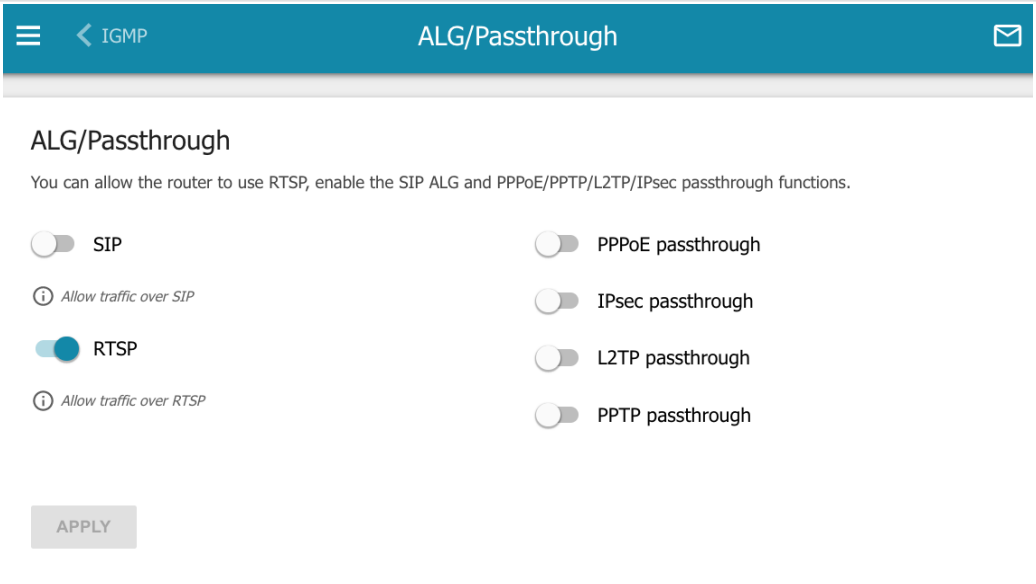

*Figure 161. The **Advanced / ALG/Passthrough** page.*

The following elements are available on the page:

Parameter	Description
SIP	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled router.[11]
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.

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

11 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 the 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).

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
- create rules for remote access to the web-based interface.

IP Filter

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

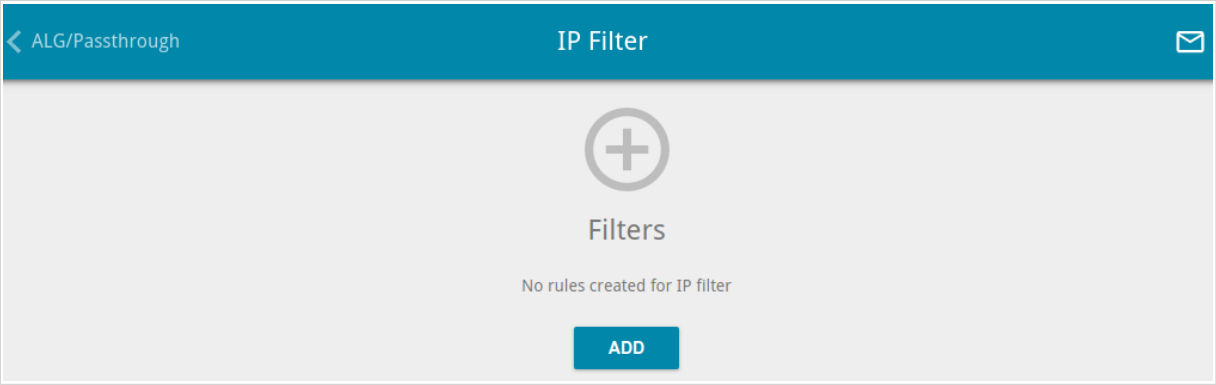

*Figure 162. The **Firewall / IP Filter** page.*

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

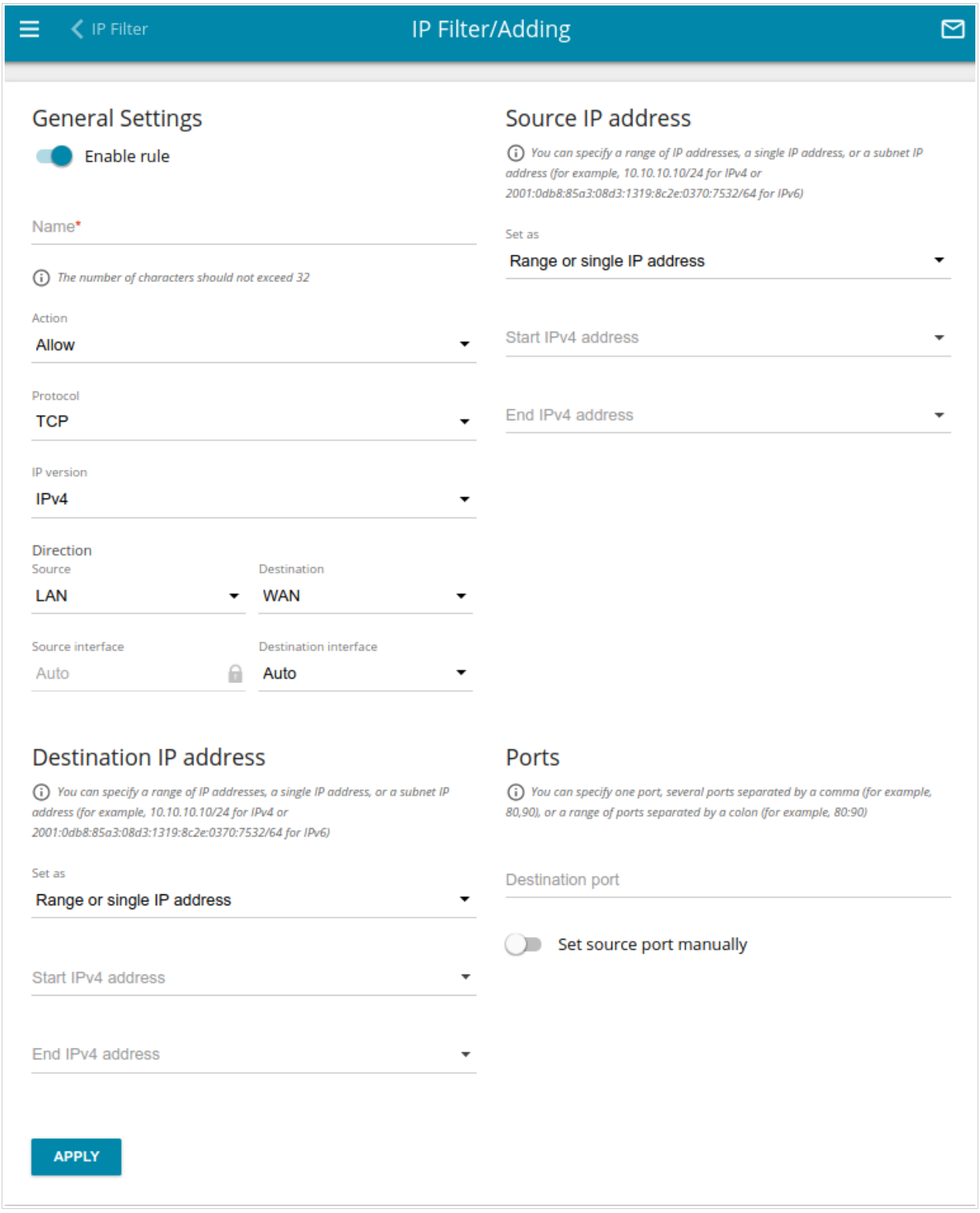

Figure 163. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
General Settings	
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Name	A name for the rule for easier identification. You can specify any name.
Action	Select an action for the rule. • **Allow**: Allows packet transmission in accordance with the criteria specified by the rule. • **Deny**: Denies packet transmission in accordance with the criteria specified by the rule.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Direction	The direction of network packet transmission to which the rule will be applied. Select the source of the packet direction from the **Source** drop-down list. • **WAN**: The rule will be applied to the packets transmitted from the external network. • **LAN**: The rule will be applied to the packets transmitted from the local network. • **GRE**: The rule will be applied to the packets transmitted from the GRE tunnel (*available if a GRE tunnel has been created on the device*). • **IPsec**: The rule will be applied to the packets transmitted from the IPsec tunnel (*available if an IPsec tunnel has been created on the device*). • **PPTP Server**: The rule will be applied to the packets transmitted from the PPTP server (*available if a PPTP server has been created on the device*). • **L2TP Server**: The rule will be applied to the packets transmitted from the L2TP server (*available if an L2TP server has been created on the device*).

Parameter	Description
	Select the destination of the packet direction from the **Destination** drop-down list. • **Router**: The rule will be applied to the packets transmitted to DWR-953. • **WAN**: The rule will be applied to the packets transmitted to the external network. • **LAN**: The rule will be applied to the packets transmitted to the local network. • **GRE**: The rule will be applied to the packets transmitted to the GRE tunnel (*available if a GRE tunnel has been created on the device*). • **IPsec**: The rule will be applied to the packets transmitted to the IPsec tunnel (*available if an IPsec tunnel has been created on the device*). • **PPTP Server**: The rule will be applied to the packets transmitted to the PPTP server (*available if a PPTP server has been created on the device*). • **L2TP Server**: The rule will be applied to the packets transmitted to the L2TP server (*available if an L2TP server has been created on the device*). From the **Source interface** and **Destination interface** drop-down lists, select source and destination interfaces for which the rule will be applied. Leave the **Auto** values to apply the rule to all created WAN interfaces.
Source IP address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The source host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the **End IPv4 address / End IPv6 address** field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The source host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The source subnet IPv4 or IPv6 address. The field is displayed when the **Subnet** value is selected from the **Set as** drop-down list.
Destination IP address	

Parameter	Description
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the **End IPv4 address / End IPv6 address** field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The destination host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The destination subnet IPv4 or IPv6 address. The field is displayed when the **Subnet** value is selected from the **Set as** drop-down list.
Ports	
Destination port	A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.
Set source port manually	Move the switch to the right to specify a port of the source IP address manually. Upon that the **Source port** field is displayed.
Source port	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

Click the **APPLY** button.

To set a schedule for the IP filter rule, click the **Set schedule** icon ( ) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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

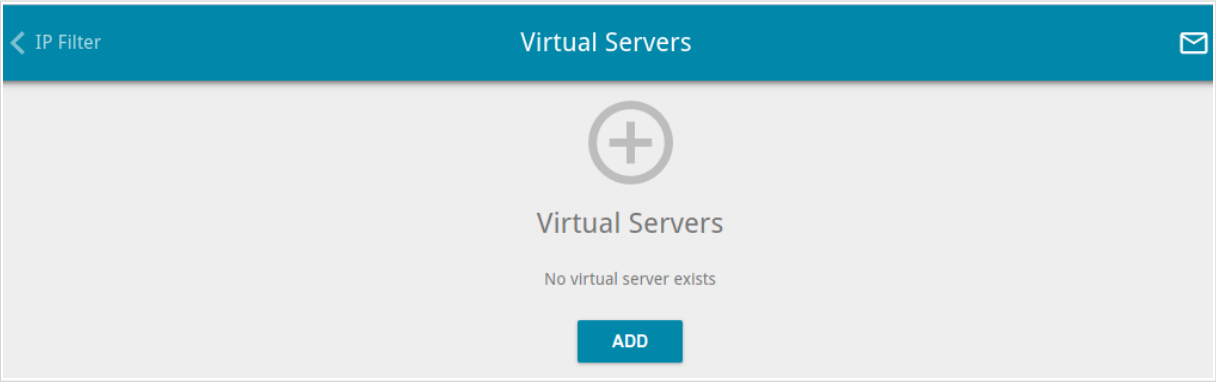

*Figure 164. The **Firewall / Virtual Servers** page.*

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

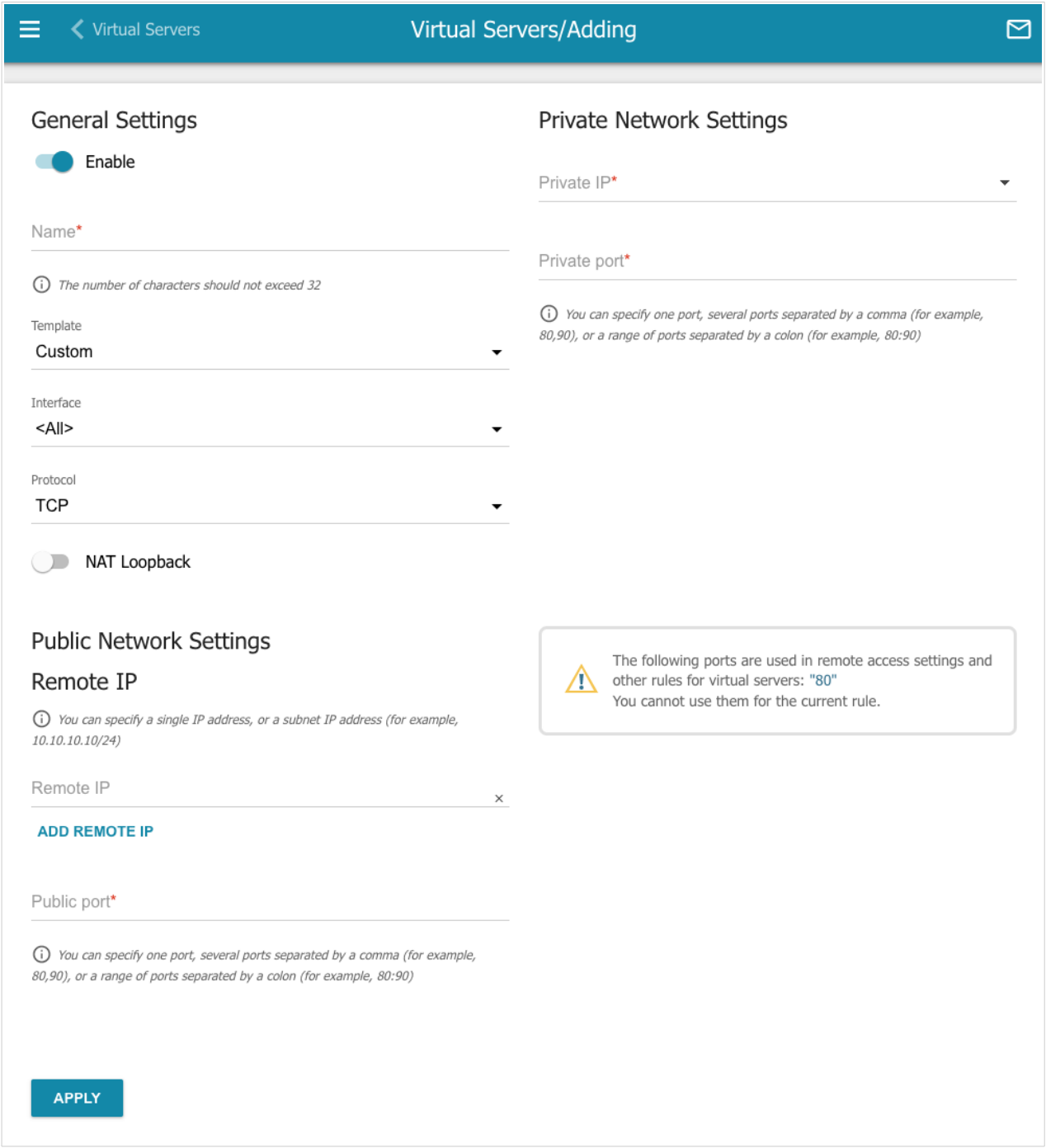

Figure 165. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
General Settings	
Enable	Move the switch to the right to enable the server. Move the switch to the left to disable the server.
Name	A name for the virtual server for easier identification. You can specify any name.

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

Click the **APPLY** button.

To set a schedule for a virtual server, click the **Set schedule** icon ( ) in the line corresponding to this server. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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

DMZ

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

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

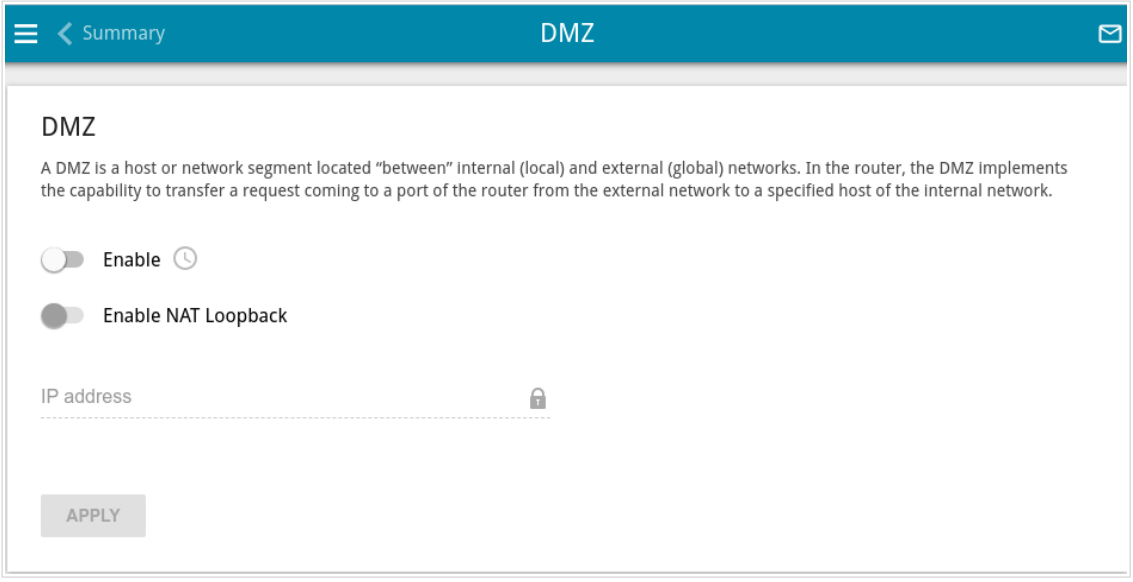

*Figure 166. The **Firewall / DMZ** page.*

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

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

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

Click the **APPLY** button.

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

To set a schedule for the DMZ, click the **Set schedule** icon ( ). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

MAC Filter

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

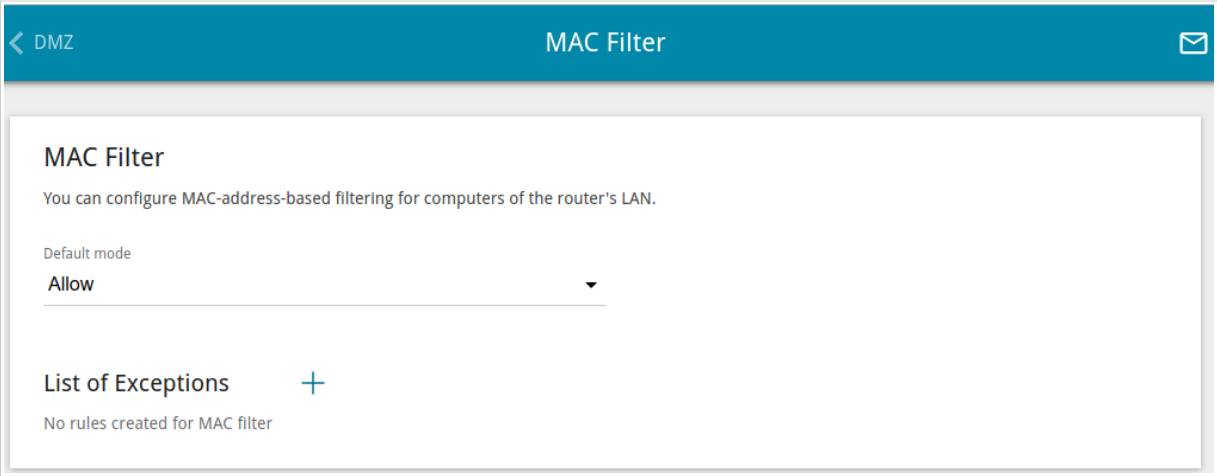

*Figure 167. The **Firewall / MAC Filter** page.*

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 (**+**).

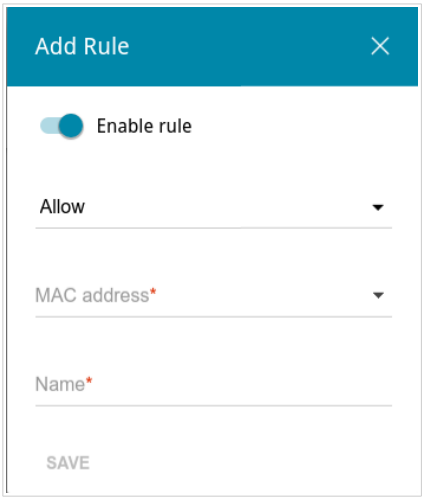

Figure 168. The window for adding a rule for the MAC filter.

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

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

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

To set a schedule for the MAC filter rule, click the **Set schedule** icon ( ) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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

URL Filter

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

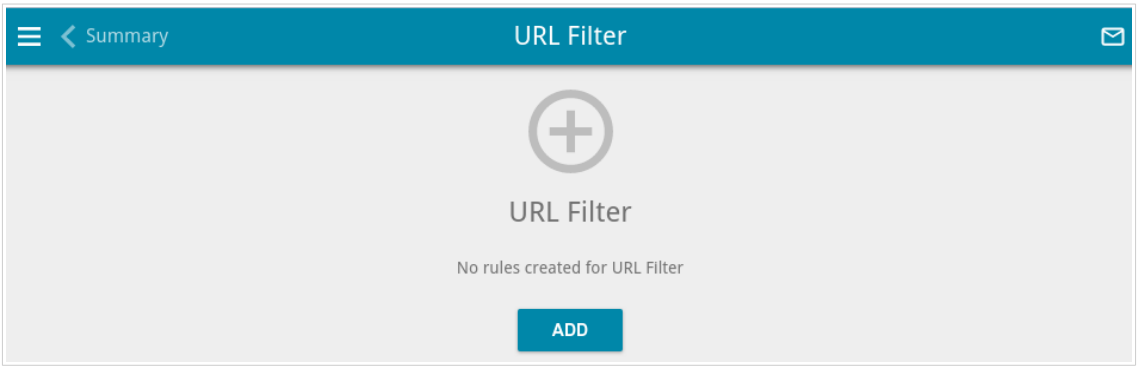

*Figure 169. The **Firewall / URL Filter** page.*

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

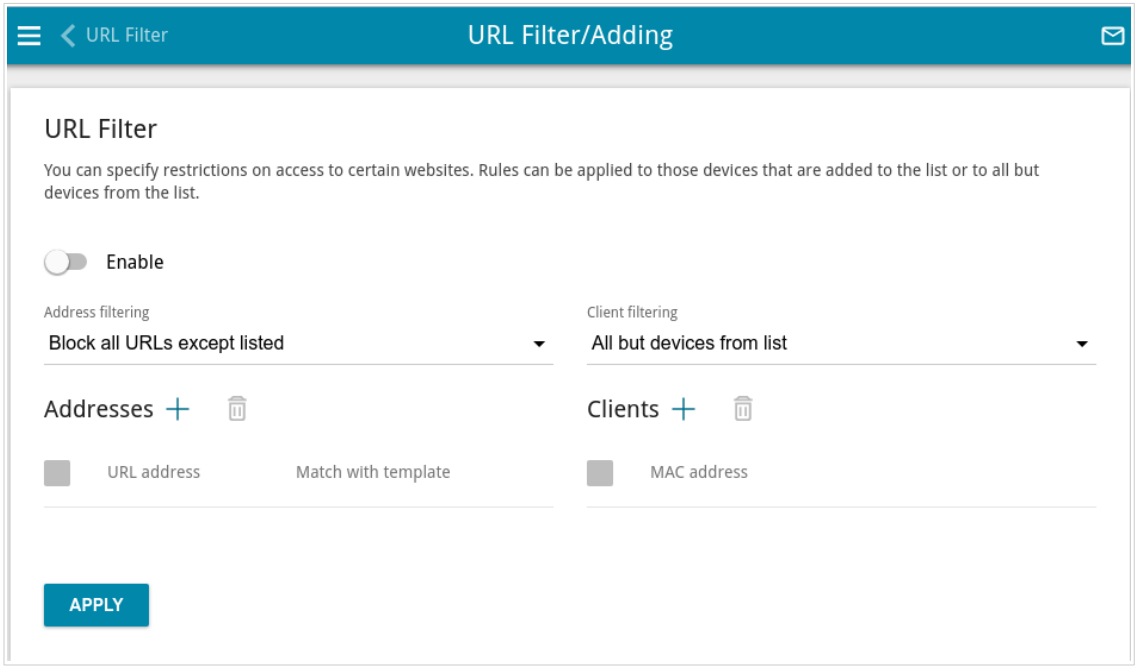

Figure 170. The page for adding a rule for URL filter.

On the opened page, move the **Enable** switch to the right to enable the rule, then select a mode from the **Address filtering** drop-down list.

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

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

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

Click the **SAVE** button.

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

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

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

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

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

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

To set a schedule for the URL filter rule, click the **Set schedule** icon ( ) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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

Remote Access

On the **Firewall / 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.

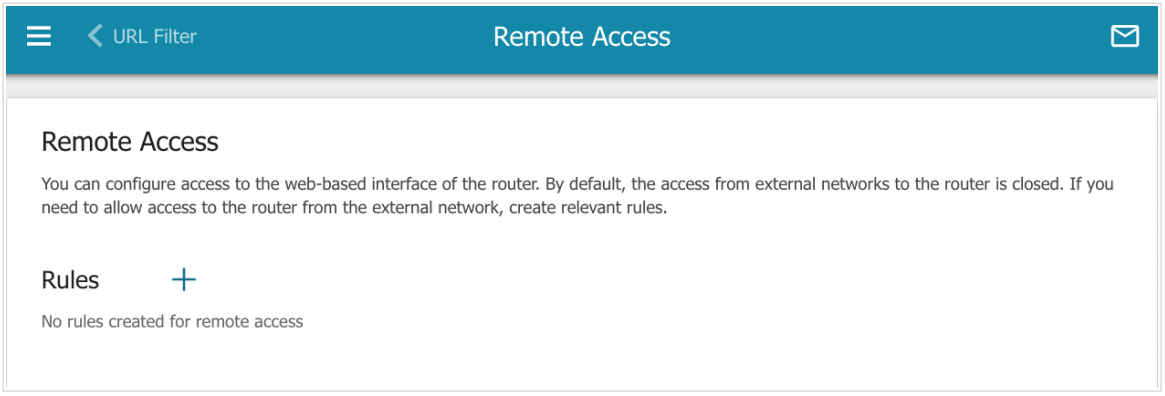

*Figure 171. The **Firewall / Remote Access** page.*

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

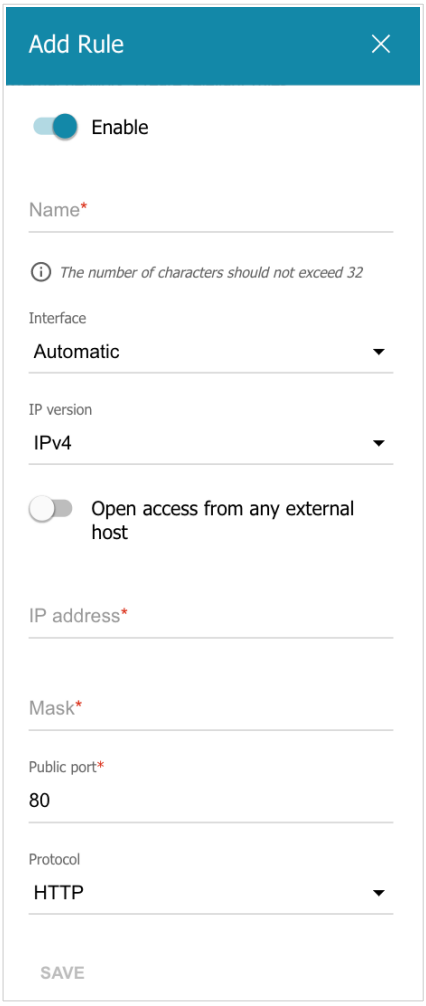

Figure 172. The window for adding a rule for remote management.

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

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

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

To set a schedule for the remote access rule, click the **Set schedule** icon ( ) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the ***Schedule*** section, page 236) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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

System

In this menu you can do the following:

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

Configuration

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

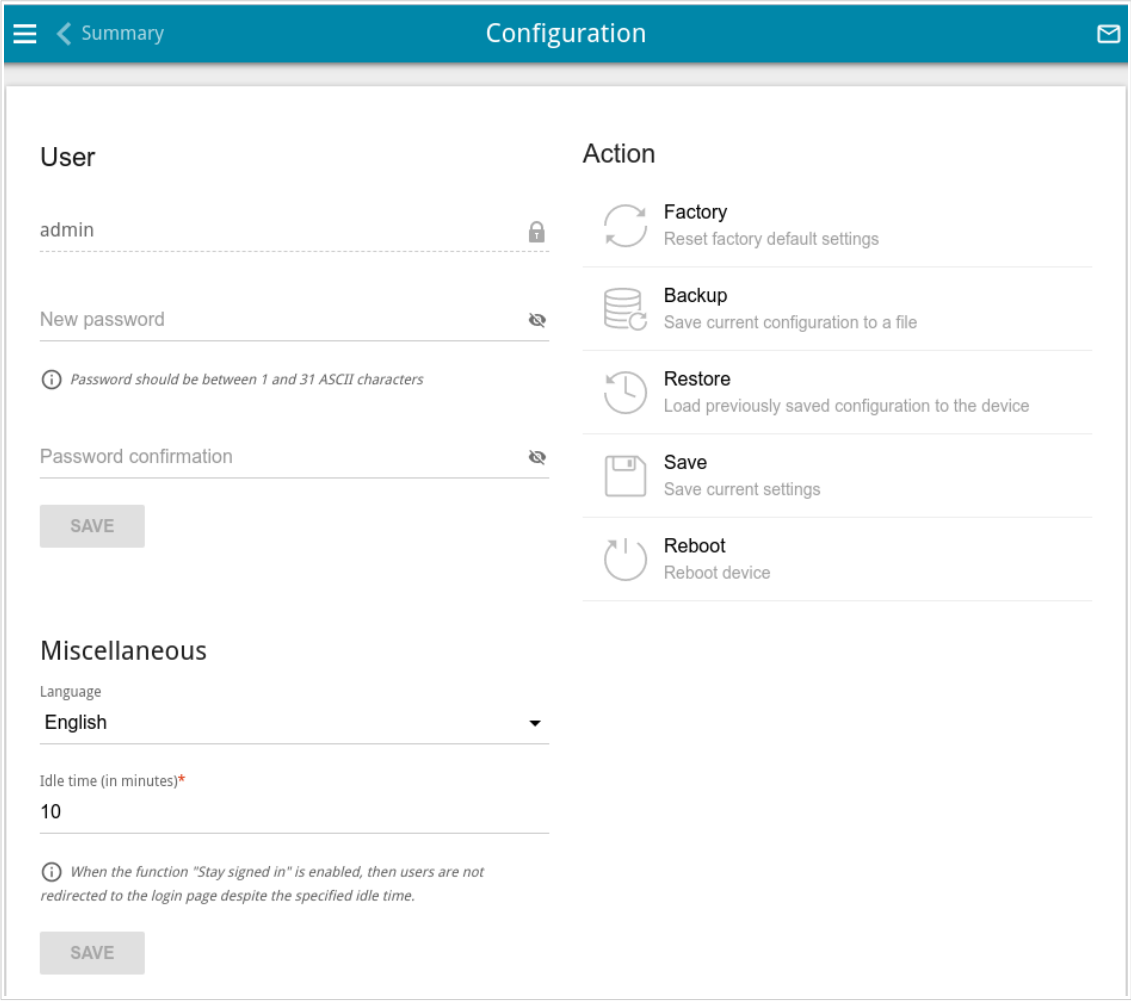

*Figure 173. The **System / Configuration** page.*

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.[12] 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.

12 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

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

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

In the **Action** section, the following buttons are available:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware **RESET** button (see the ***Left Side Panel*** section, page 14).
Backup	Click the button to save the configuration (all settings of the router) to your PC. The configuration backup will be stored in the download location of your web browser.
Restore	Click the button and follow the dialog box appeared to select a previously saved configuration file (all settings of the router) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The router saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

Buttons Configuration

On the **System / Buttons Configuration** page, you can edit or add commands for the **RESET**, **WLAN**, and **WPS** hardware buttons.

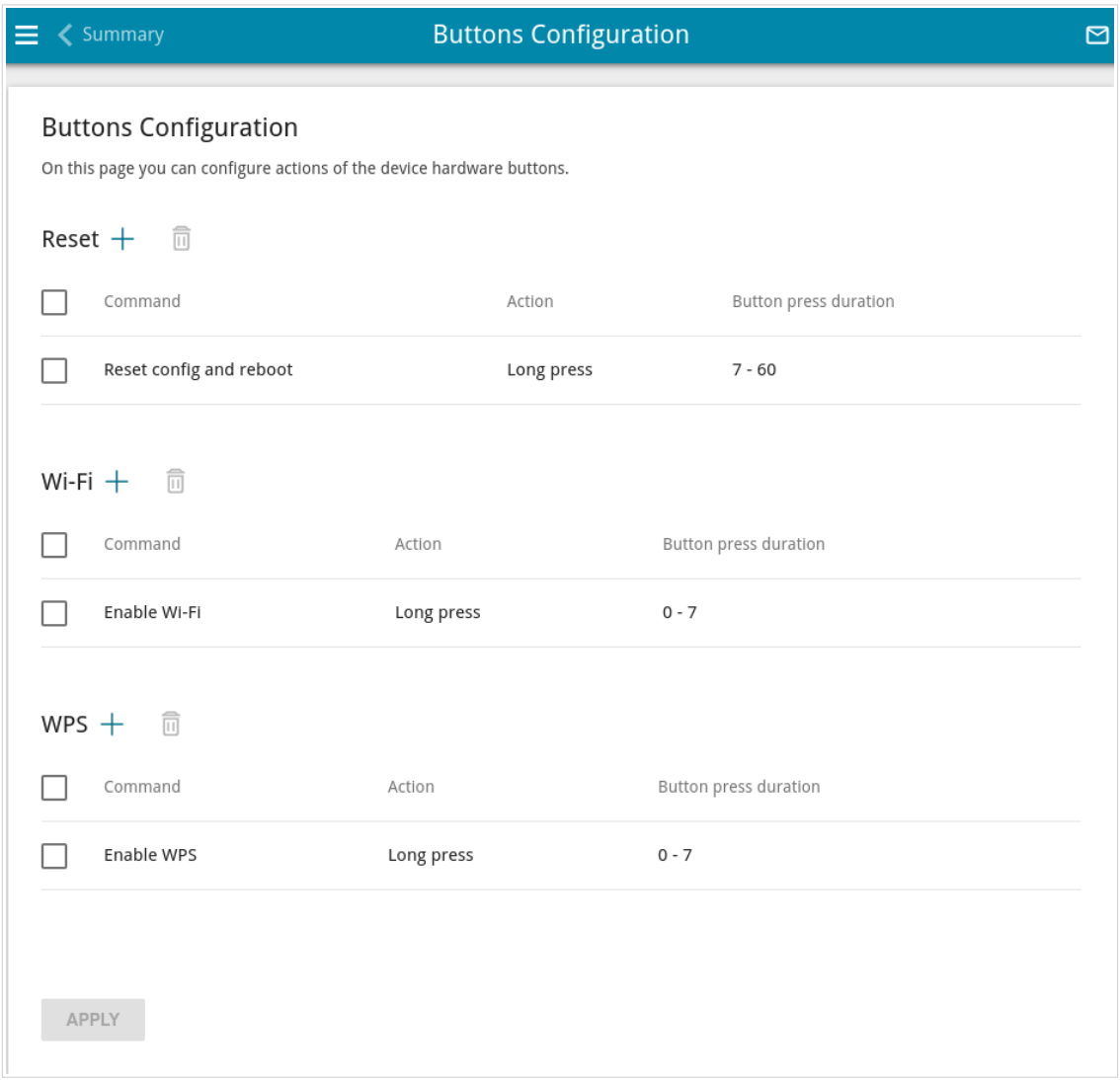

*Figure 174. The **System / Buttons Configuration** page.*

The page displays commands assigned to the buttons by default (for the description of the buttons actions with the commands assigned by default, see the ***Product Appearance*** section, page 12). You can edit or delete them.

To add a command for a button, click the **ADD** button (+) in the relevant section.

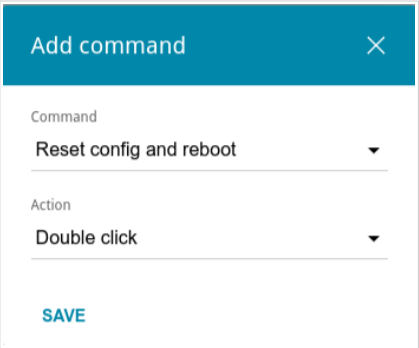

Figure 175. The window for adding a command.

In the opened window, specify the following parameters:

Control	Description
Reset / Wi-Fi / WPS	
Command	From the drop-down list, select a command.
Action	From the drop-down list, select an action for the command. • **Single click**: One short press of the button lasting less than one second. • **Double click**: Two short presses of the button. • **Long press**: Pressing of the button for several seconds. When this value is selected, the **Button press duration** section is displayed.
Button press duration	Specify a period of time (in seconds) within which you should hold the button to perform the specified action. You can specify values from **2** to **60**.

Click the **SAVE** button.

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

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

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

Firmware Update

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

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

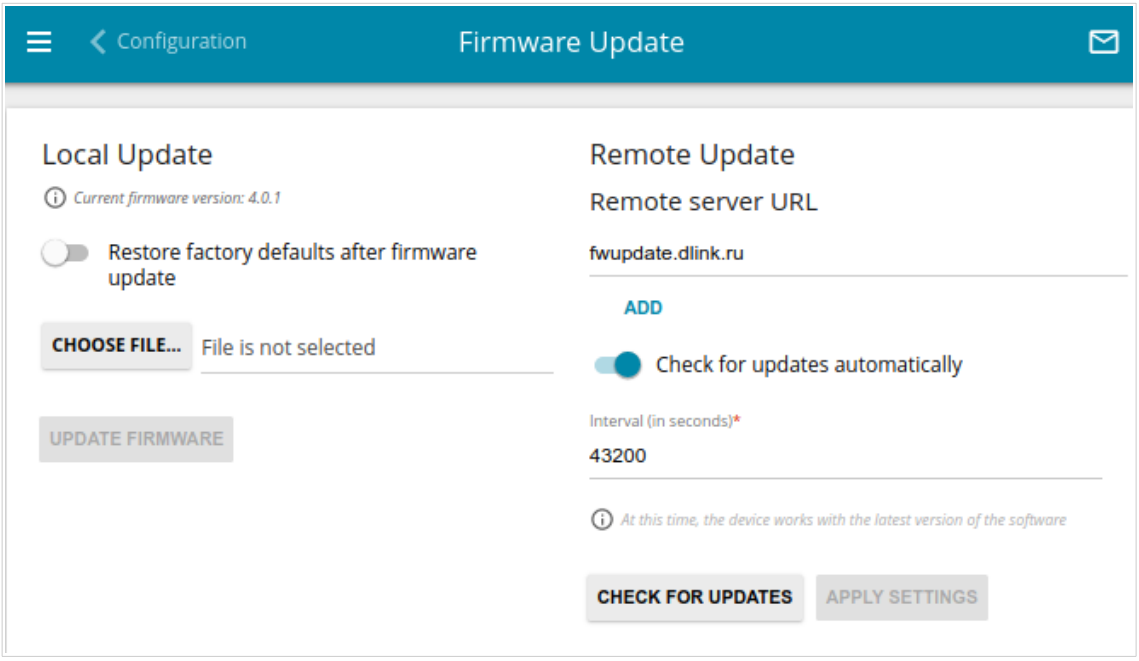

*Figure 176. The **System / Firmware Update** page.*

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

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

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

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

To enable the automatic check for firmware updates, in the **Remote Update** section, move the **Check for updates automatically** switch to the right. In the **Interval** field, specify the time period (in seconds) between checks or leave the value specified by default (`43200`).

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

Click the **APPLY SETTINGS** button.

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

Local Update

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

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

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **CHOOSE FILE** button in the **Local Update** section on the **System / Firmware Update** page to locate the new firmware file.
3. If you want to restore the factory default settings immediately after updating the firmware, move the **Restore factory defaults after firmware update** switch to the right.
4. Click the **UPDATE FIRMWARE** button.
5. Wait until the router is rebooted (about one and a half or two minutes).
6. Log into the web-based interface using the login (`admin`) and the current password.

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

Remote Update

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

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

1. On the **System / Firmware Update** page, in the **Remote Update** section, click the **CHECK FOR UPDATES** button to check if a newer firmware version exists.
2. Click the **UPDATE FIRMWARE** button (the button is displayed if a newer version of the firmware is available).
3. Wait until the router is rebooted (about one and a half or two minutes).
4. Log into the web-based interface using the login (`admin`) and the current password.

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

Schedule

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

Before creating a schedule you need to configure automatic synchronization of the system time with a time server on the Internet (see the ***System Time*** section, page 249).

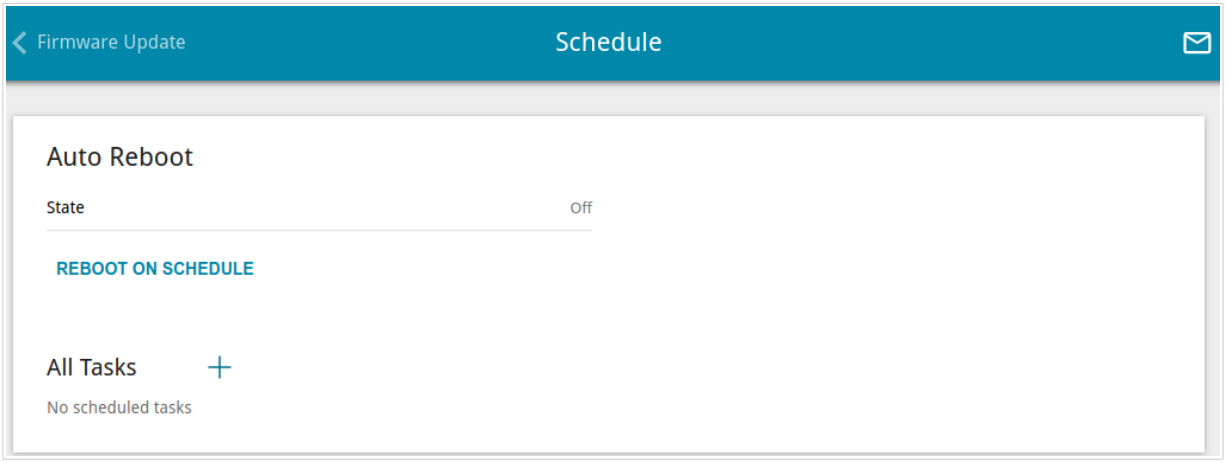

*Figure 177. The **System / Schedule** page.*

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

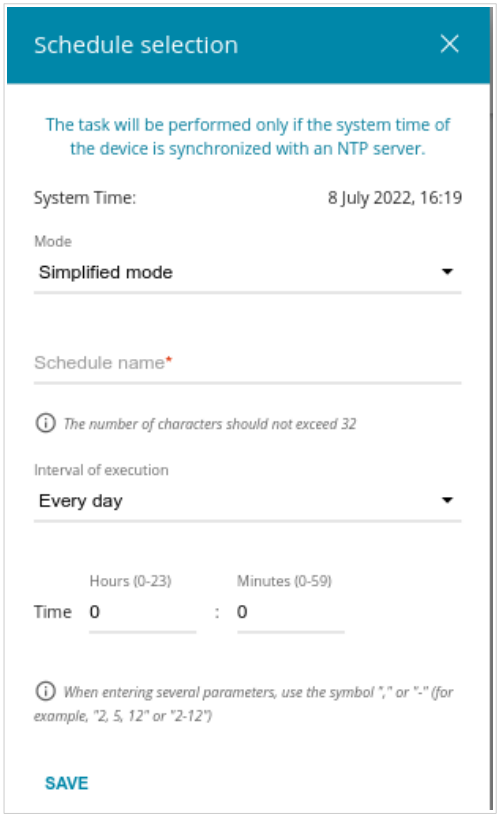

Figure 178. The window for configuring automatic reboot on a schedule.

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

Parameter	Description
Simplified mode	
Schedule name	Specify a schedule name for easier identification. You can specify any name.
Interval of execution	Specify the time period for the device's reboot. • **Every day**: When this value is selected, the **Time** field is displayed in the section. • **Every week**: When this value is selected, the names of days of the week and the **Time** field are displayed in the section. • **Every month**: When this value is selected, the **Day of month** and **Time** fields are displayed in the section.
Time	Specify the time for the device's reboot.
Days of week	Select a day or days of the week when the device will be automatically rebooted. To do this, select the checkbox located to the left of the relevant value.
Day of month	Specify a day of the month. You can specify one value or several values separated by a comma.

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

Click the **SAVE** button.

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

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

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

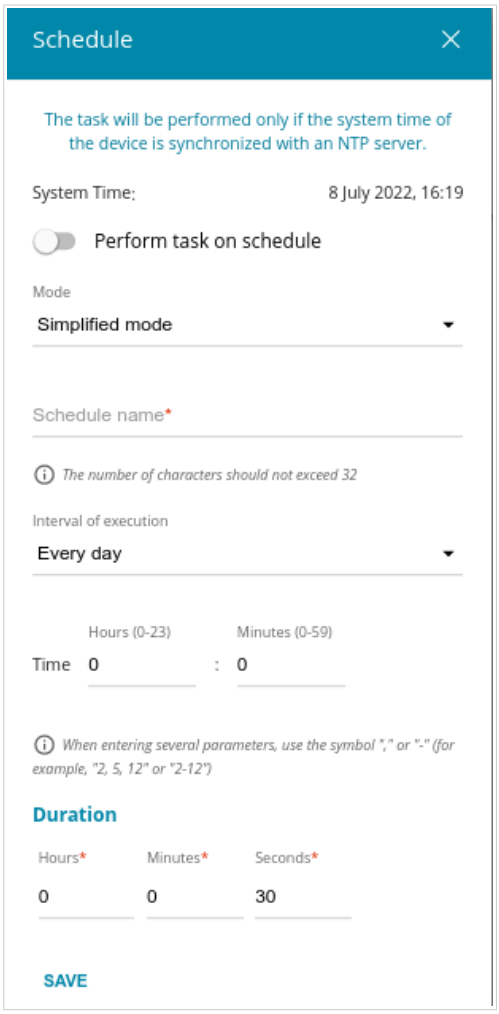

Figure 179. The window for adding a schedule for a task.

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

Parameter	Description
Perform task on schedule	Move the switch to the right to enable the schedule. Move the switch to the left to disable the schedule.

Parameter	Description
Simplified mode	
Schedule name	Specify a schedule name for easier identification. You can specify any name.
Interval of execution	Specify the time period for performing a task. • **Every minute**. • **Every hour**: When this value is selected, the **Time** field is displayed in the section. • **Every day**: When this value is selected, the **Time** field is displayed in the section. • **Every week**: When this value is selected, the names of days of the week and the **Time** field are displayed in the section. • **Every month**: When this value is selected, the **Day of month** and **Time** fields are displayed in the section.
Duration	Specify the interval during which the task will be performing.
Time	Specify the time when the task should start running.
Days of week	Select a day or days of the week when the task will be performing. To do this, select the checkbox located to the left of the relevant value.
Day of month	Specify a day of the month. You can specify one value or several values separated by a comma.

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

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

Click the **SAVE** button.

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

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

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

Log

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

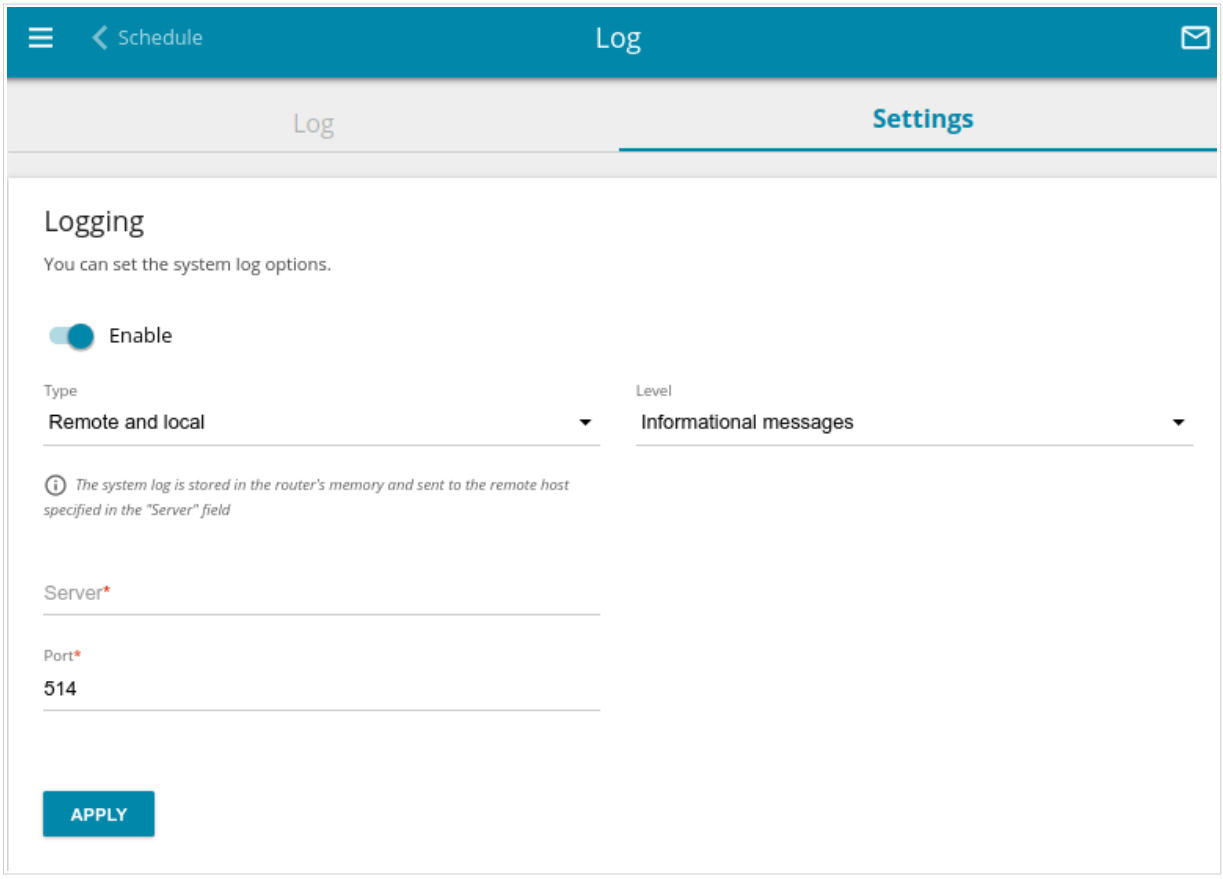

*Figure 180. The **System / Log** page. The **Settings** tab.*

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

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

To disable logging of the system events, move the **Enable** switch to the left and click the **APPLY** button.

To view the system log, go to the **Log** tab.

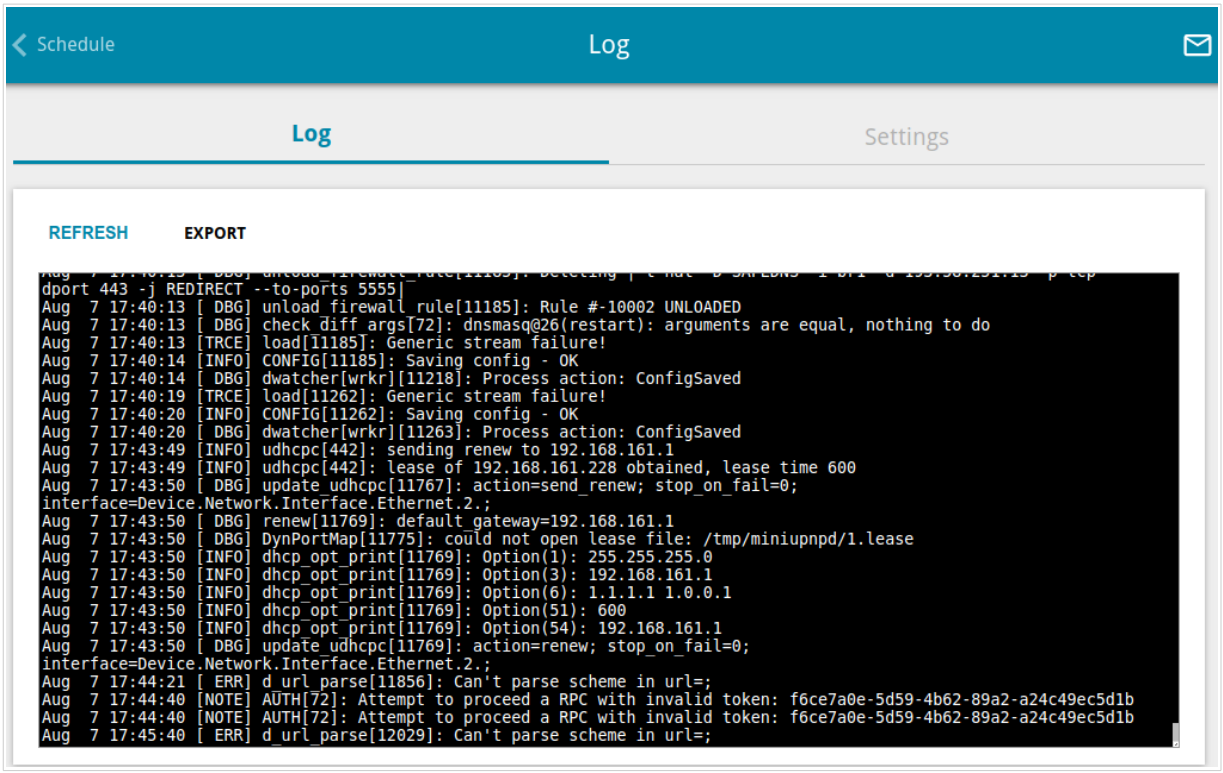

*Figure 181. The **System / Log** page. The **Log** tab.*

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.

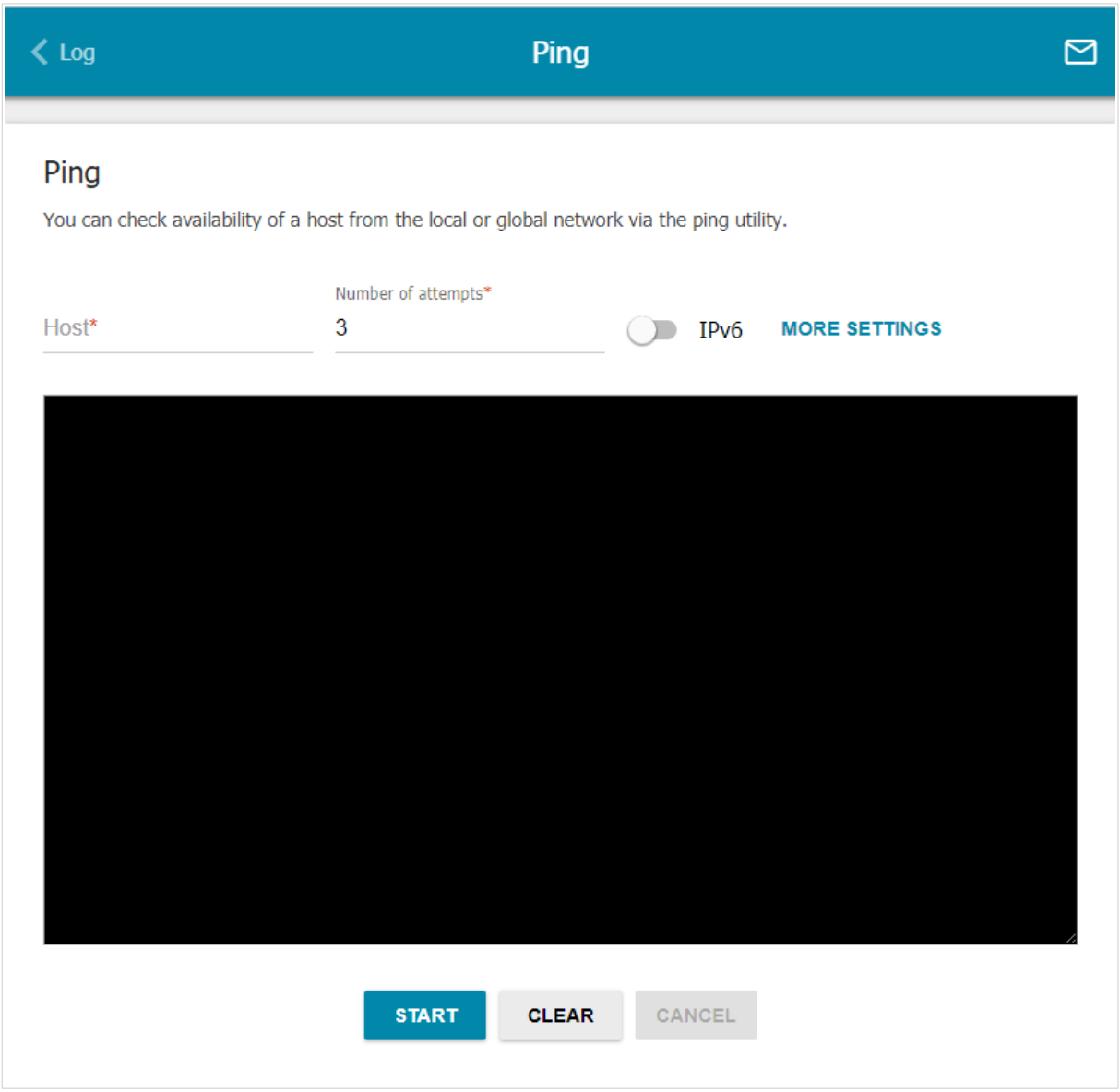

*Figure 182. The **System / Ping** page.*

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

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

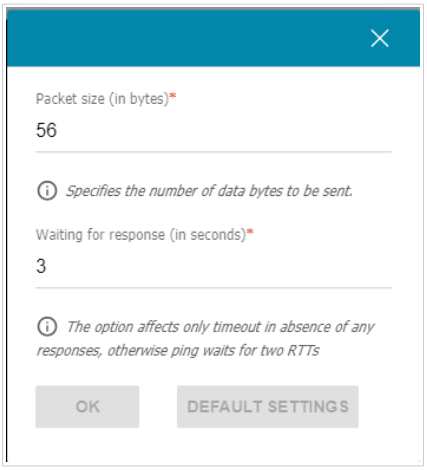

*Figure 183. The **System / Ping** page. The additional settings window.*

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

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

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

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

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

Traceroute

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

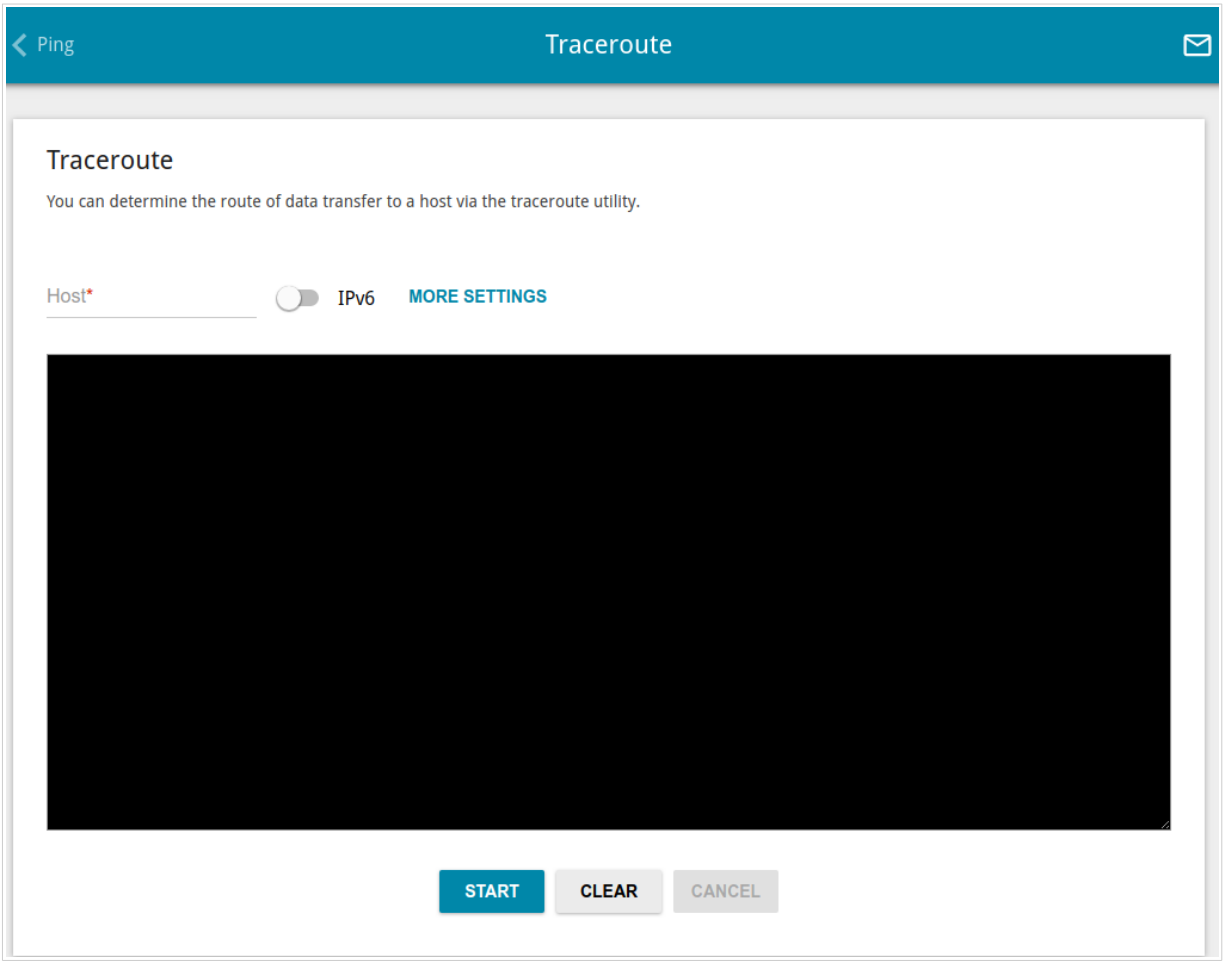

*Figure 184. The **System / Traceroute** page.*

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.

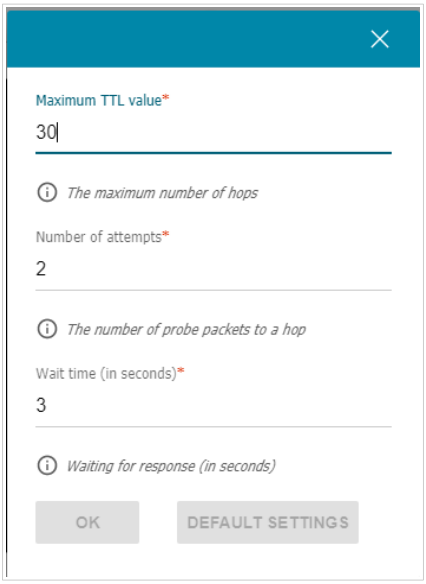

*Figure 185. The **System / Traceroute** page. The additional settings window.*

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

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

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

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

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

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

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

Telnet/SSH

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

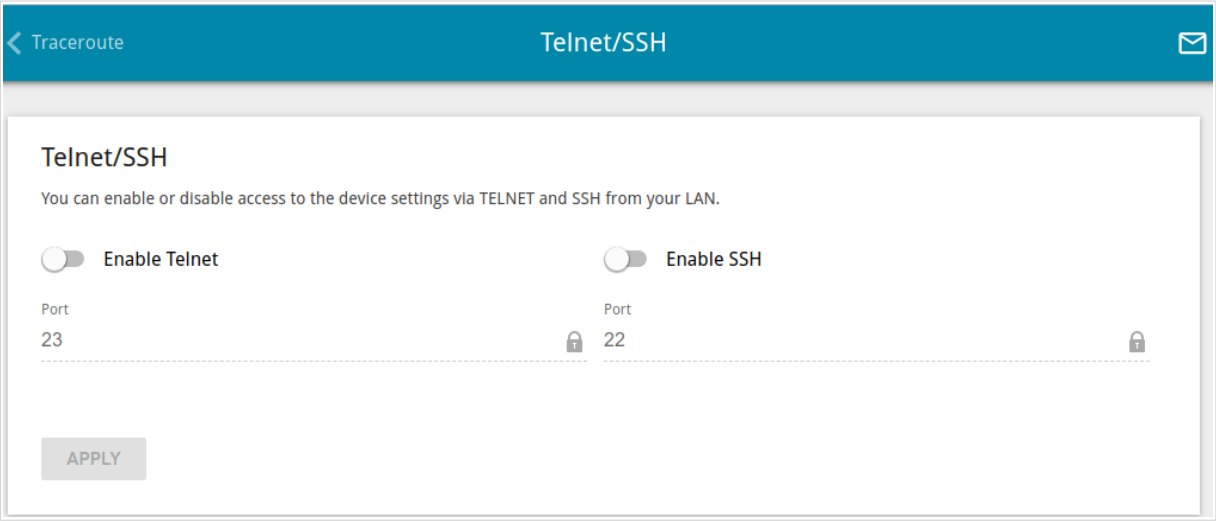

*Figure 186. The **System / Telnet/SSH** page.*

To enable access via TELNET and/or SSH, move the **Enable Telnet** switch and/or **Enable SSH** switch to the right. In the **Port** field, enter the number of the router's port through which access will be allowed (by default, the port `23` is specified for Telnet and the port `22` is specified for SSH). Then click the **APPLY** button.

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

System Time

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

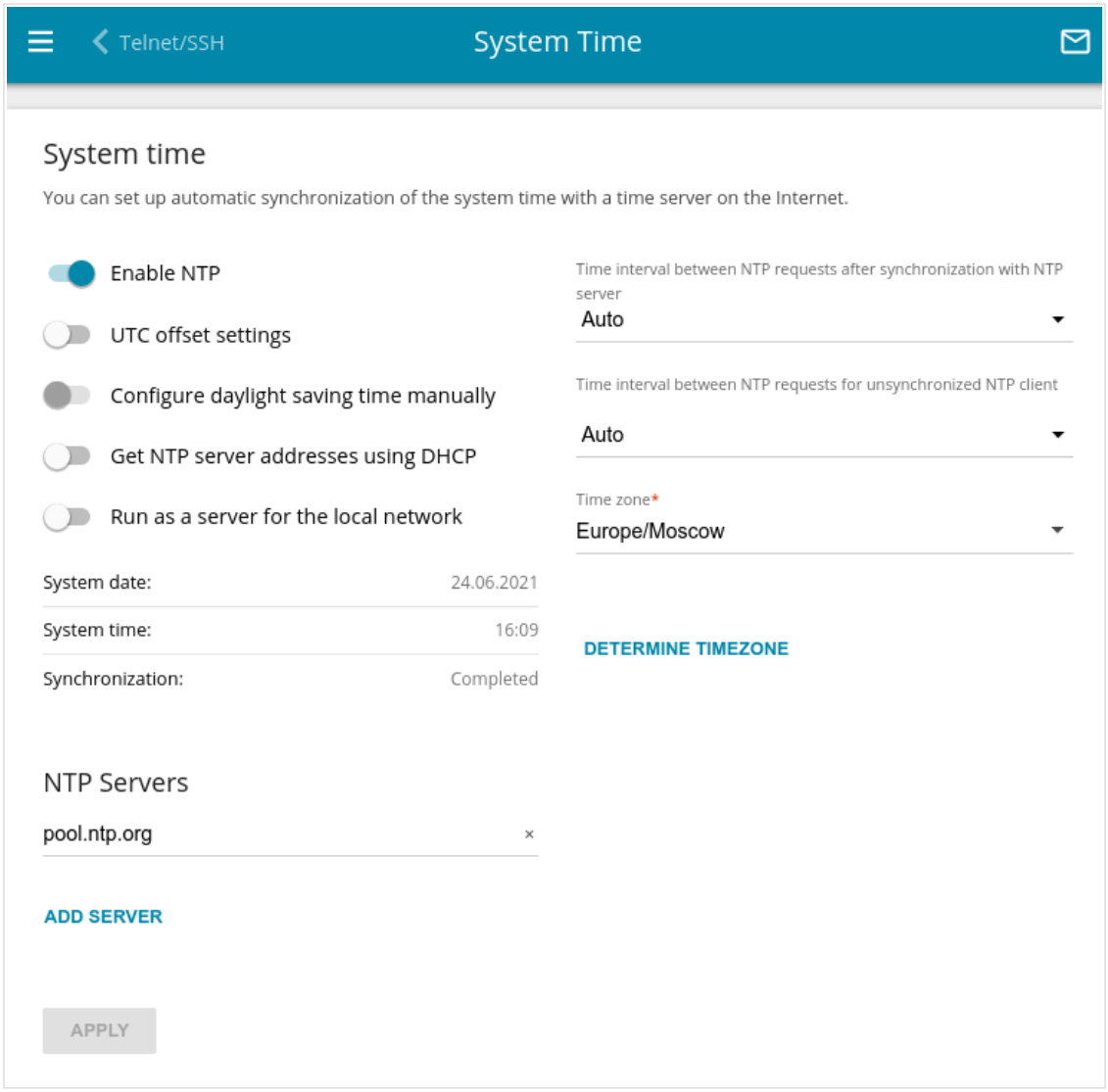

*Figure 187. The **System / System Time** page.*

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

1. Move the **Enable NTP** switch to the left.
2. In the **Time Settings** section, specify needed values. To specify the time set up your PC or portable device, click the **SET LOCAL TIME** button.
3. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

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

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

3. Select your time zone from the **Time zone** drop-down list. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.
4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically. In case of successful synchronization with the NTP server, the **Completed** value will be displayed in the **Synchronization** field.

If the router failed to get data from the server, the **Failed** value will be displayed in the **Synchronization** field. Upon that the creation date and time of the router's current firmware version is specified.

Additional settings are also available on the page:

Parameter	Description
UTC offset settings	Move the switch to the right to set the UTC (*Coordinated Universal Time*) offset for the router clock manually. In the **UTC offset** field displayed, specify the required offset time (in minutes).
Configure daylight saving time manually	Move the switch to the right to configure settings for daylight saving time for the router clock manually. In the **Daylight Saving Time** section displayed, specify the required offset time for daylight saving time (in minutes), and specify the needed values in the **Beginning of daylight saving time** and **End of daylight saving time** sections.
Get NTP server addresses using DHCP	Move the switch to the right if NTP servers addresses are provided by your ISP. Contact your ISP to clarify if this setting needs to be enabled. If the switch is moved to the right, the **NTP Servers** section is not displayed.
Run as a server for the local network	Move the switch to the right to allow connected devices to use the IP address of the router in the local subnet as a time server.
Time interval between NTP requests after synchronization with NTP server	From the drop-down list, select a time period (in seconds) after which a request to update the system time will be sent to the NTP server or leave the **Auto** value.
Time interval between NTP requests for unsynchronized NTP client	A time period (in seconds) after which a request to synchronize the system time will be sent to the NTP server. Select the needed value from the drop-down list. • **Auto**: The time period is defined automatically. • **Manual**: The time period is defined in accordance with the value specified in the **Interval value** field.
Interval value	Specify the time period (in seconds). The minimum acceptable value is 3.

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

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

Auto Provision

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

The Auto Provision function allows your ISP to manage the device's settings remotely: DWR-953 connects to the ISP's server, compares the current configuration file with the configuration file stored on this server, and updates its settings if the files are different.

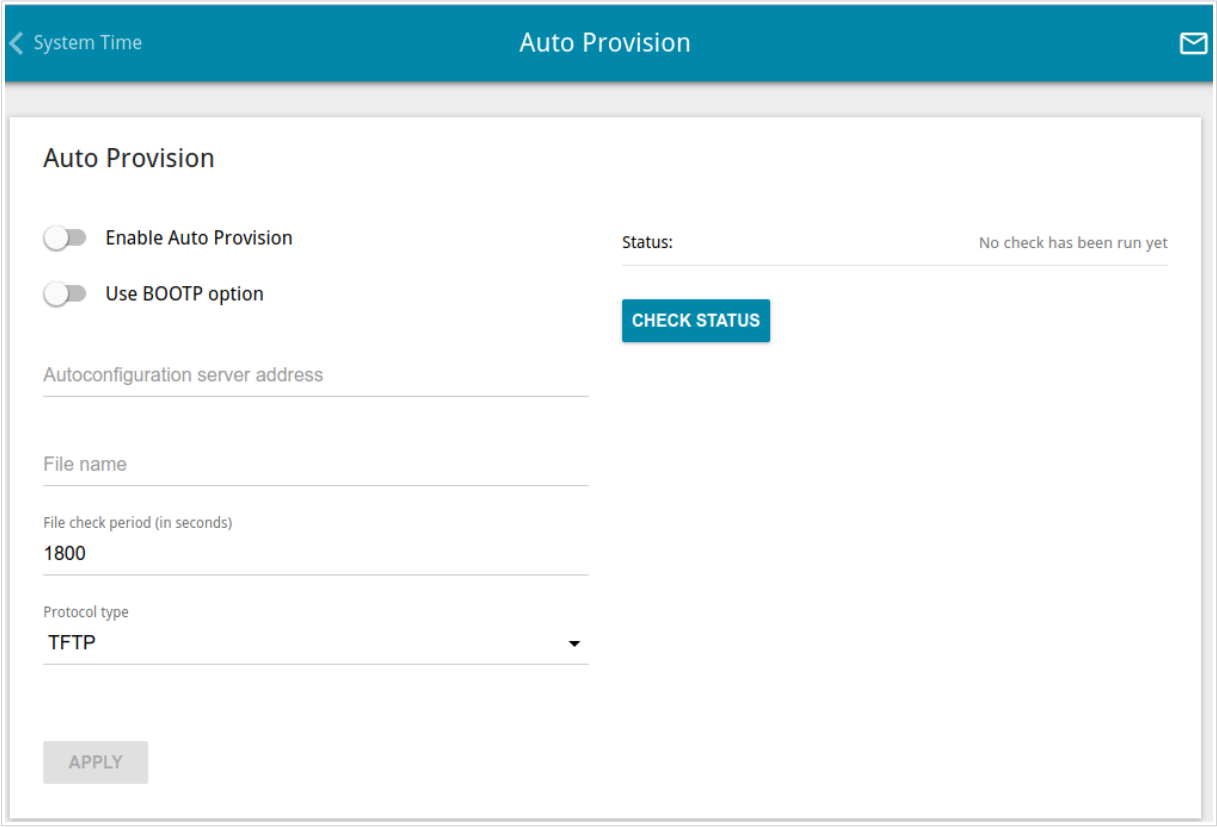

Figure 188. The page for configuring the Auto Provision function.

You can specify the following parameters:

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

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

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

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

SkyDNS

This menu is designed to configure the SkyDNS service.

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

Settings

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

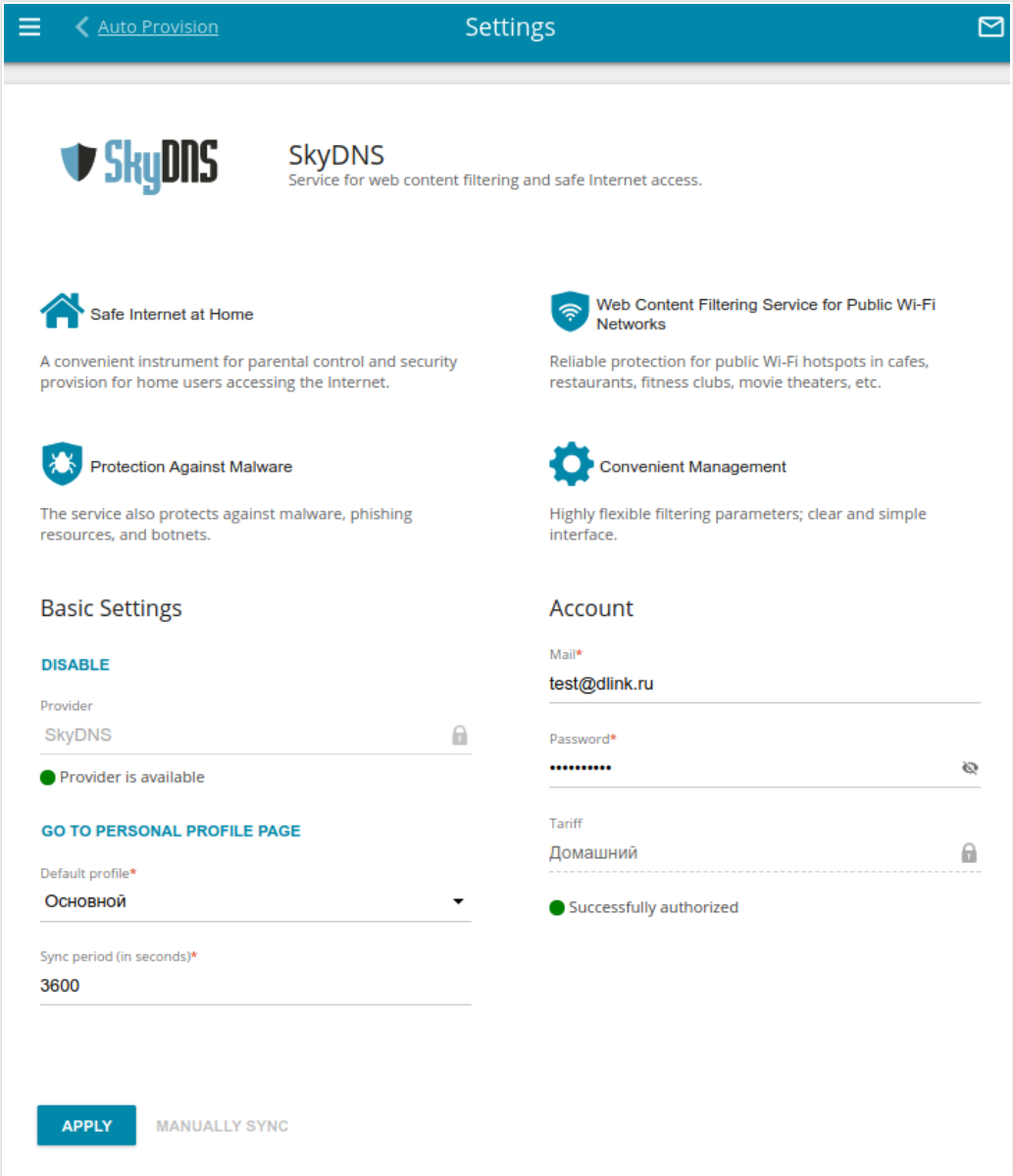

*Figure 189. The **SkyDNS / Settings** page.*

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

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

To change the parameters of your account on the SkyDNS service web site, click the **GO TO PERSONAL PROFILE PAGE** button.

By default, the account parameters are automatically synchronized with the SkyDNS service web site once an hour (3600 seconds). To change the automatic synchronization period, specify another value in the **Sync period** field and click the **APPLY** button. To start synchronization manually, click the **MANUALLY SYNC** button.

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

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

Devices and Rules

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

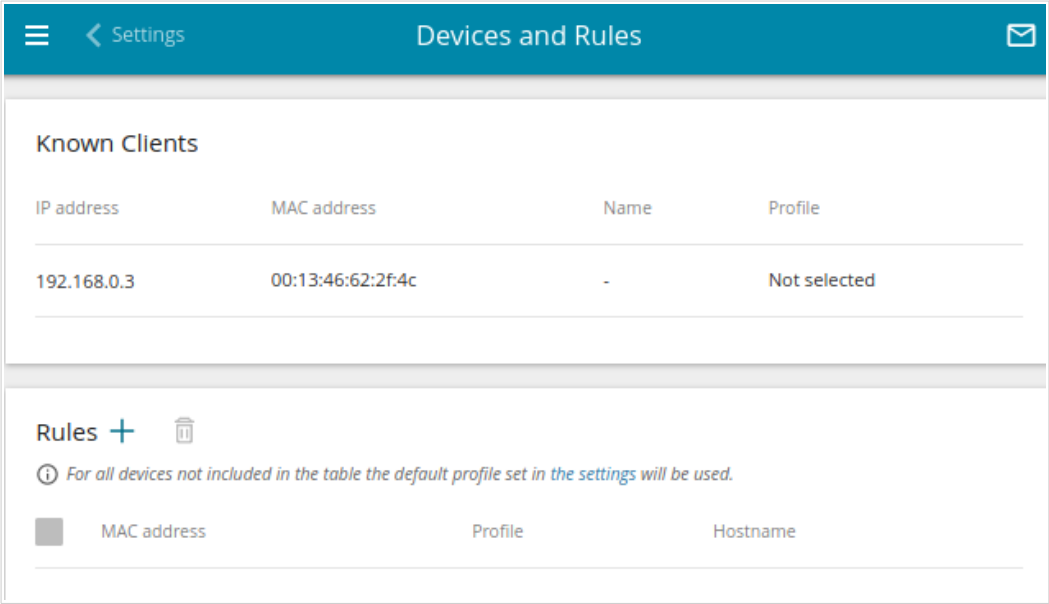

*Figure 190. The **SkyDNS / Devices and Rules** page.*

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

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

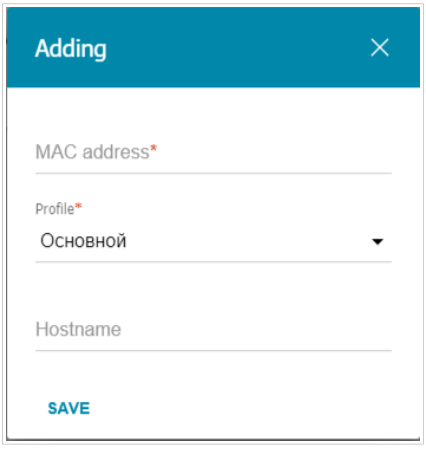

*Figure 191. The **SkyDNS / Devices and Rules** page. The window for adding a rule.*

In the opened window, specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the router's LAN to which the specified filtering profile will be applied. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Profile	Select the filtering profile which will be used for the device with the specified MAC address from the drop-down list.
Hostname	Enter a name for the rule for easier identification. *Optional*.

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

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

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

CHAPTER 5. OPERATION GUIDELINES

Safety Rules and Conditions

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

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

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

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

The service life of the device is 2 years.

Wireless Installation Considerations

The DWR-953 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-953 device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).
2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone in not in use.

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

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

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

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

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