D-Link®

DIR-X1860

AX1800 Wi-Fi 6 EasyMesh Gigabit Router

Contents

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DIR-X1860 and explains how to configure and operate it.

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

Conventions

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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the router DIR-X1860 and configure a PC in order to access its web-based interface.

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

Chapter 5 includes safety instructions and tips for networking.

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

CHAPTER 2.   OVERVIEW

General Information

The DIR-X1860 device is a wireless dual band gigabit router with a built-in 3-port switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

You are able to connect the wireless router DIR-X1860 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 3-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network.

You can use any Ethernet port of the router as LAN or WAN port. The new-generation firmware supports assigning several WAN ports, for example, in order to configure the primary and backup WAN connection of different ISPs.

Support of Wi-Fi 6 (802.11ax) standard provides faster speeds, greater capacity, and less network congestion for high-performance device-dense environments. It ensures connection of more devices and prevents weakening wireless connectivity by wall obstruction and interference from other appliances.

Using the DIR-X1860 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, 802.11ac, and 802.11ax (at the wireless connection rate up to 1775Mbps[1]).

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

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

The Band Steering technology simplifies connection to the network and optimizes further operation for the wireless clients. You can configure the wireless network with one name for both bands, so the clients automatically choose the preferred band when they are connecting or when the network conditions change.

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

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

---

1   Up to 574Mbps for 2.4GHz and up to 1201Mbps for 5GHz.
2   Up to 6 devices.

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. Devices connected to the guest network will be able to access the Internet, but will be isolated from the devices and resources of the router's LAN.

The wireless router DIR-X1860 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.

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

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

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

You can configure the settings of the wireless router DIR-X1860 via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

The configuration wizard allows you to quickly switch DIR-X1860 to one of the following modes: router (for connection to a wired or wireless ISP), access point, repeater, or client, and then configure all needed setting for operation in the selected mode in several simple steps.

Also DIR-X1860 supports configuration and management via mobile application for Android 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	· MT7621AT (880MHz, dual core)
RAM	· 256MB, DDR3L SDRAM
Flash	· 128MB, NAND
Interfaces	· 10/100/1000BASE-T WAN port · 3 10/100/1000BASE-T LAN ports
LEDs	· Power · Internet · WLAN 2.4G · WLAN 5G
Buttons	· POWER button to power on/power off · RESET button to restore factory default settings · WPS button to connect mesh network devices, set up wireless connection, and enable/disable wireless network
Antenna	· Two external non-detachable antennas for 2.4GHz band (5dBi gain) · Two external non-detachable antennas for 5GHz band (5dBi gain)
MIMO	· 2 x 2, MU-MIMO
Power connector	· Power input connector (DC)

Software	
WAN connection types	· PPPoE · IPv6 PPPoE · PPPoE Dual Stack · Static IPv4 / Dynamic IPv4 · Static IPv6 / Dynamic IPv6 · PPPoE + Static IP (PPPoE Dual Access) · PPPoE + Dynamic IP (PPPoE Dual Access) · PPTP/L2TP + Static IP · PPTP/L2TP + Dynamic IP · L2TP Dual Stack · 6in4 · 6to4 · 6rd

---

* 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 · Advanced configuration of built-in DHCP server · Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation · Automatic obtainment of LAN IP address (for access point/repeater/client modes) · DNS relay · Dynamic DNS · Static IPv4/IPv6 routing · IGMP/MLD Proxy · RIP · Support of UPnP · Support of VLAN · WAN ping respond · Support of SIP ALG · Support of RTSP · WAN failover · LAN/WAN conversion · Multi-WAN support · 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) · Support of VRRP · Port mirroring · Wake-on-LAN support
Firewall functions	· Network Address Translation (NAT) · Stateful Packet Inspection (SPI) · IPv4/IPv6 filter · MAC filter · URL filter · Ad blocking function · 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 client
	· GRE/EoGRE/EoIP/IPIP 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) · Bilingual web-based interface for configuration and management (Russian/English) · Support of D-Link Assistant application for Android 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 · SNMP agent · Schedules for rules and settings of firewall, automatic reboot, 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

Wireless Module Parameters	
Standards	· IEEE 802.11ax · IEEE 802.11ac Wave 2 · IEEE 802.11a/b/g/n
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	· EasyMesh function · 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 · 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 · CoovaChilli authentication portal · Support of OFDMA technology · Support of TWT technology · Support of Band Steering · Support of Airtime Fairness
Wireless connection rate[3]	· 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 (MCS0–MCS15) · IEEE 802.11ac (5GHz): from 6.5 to 867Mbps · IEEE 802.11ax (2.4GHz): from 6.5 to 574Mbps · IEEE 802.11ax (5GHz): from 6.5 to 1201Mbps
Transmitter output power *The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country*	· Less than 20dBm (100mW)

---

3   Maximum wireless signal rate is derived from IEEE standard 802.11ax and 802.11ac specifications. In order to get the rate of 574Mbps in the 2.4GHz band, a Wi-Fi client should support 802.11ax, HE40 mode with MIMO 2x2, and 1024-QAM modulation. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Wireless Module Parameters	
Receiver sensitivity	· 802.11a (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -92dBm at 6Mbps -90dBm at 9Mbps -89dBm at 12Mbps -87dBm at 18Mbps -84dBm at 24Mbps -80dBm at 36Mbps -76dBm at 48Mbps -74dBm at 54Mbps · 802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C) -96dBm at 1Mbps -94dBm at 2Mbps -91dBm at 5.5Mbps -88dBm at 11Mbps · 802.11g (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -92dBm at 6Mbps -90dBm at 9Mbps -89dBm at 12Mbps -87dBm at 18Mbps -84dBm at 24Mbps -80dBm at 36Mbps -77dBm at 48Mbps -75dBm at 54Mbps · 802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) 2.4GHz, HT20 -92dBm at MCS0/8 -89dBm at MCS1/9 -87dBm at MCS2/10 -84dBm at MCS3/11 -80dBm at MCS4/12 -76dBm at MCS5/13 -75dBm at MCS6/14 -73dBm at MCS7/15 2.4GHz, HT40 -89dBm at MCS0/8 -86dBm at MCS1/9 -83dBm at MCS2/10 -80dBm at MCS3/11 -78dBm at MCS4/12 -74dBm at MCS5/13 -72dBm at MCS6/14 -70dBm at MCS7/15 5GHz, HT20 -92dBm at MCS0/8 -89dBm at MCS1/9 -86dBm at MCS2/10 -83dBm at MCS3/11 -79dBm at MCS4/12 -76dBm at MCS5/13 -74dBm at MCS6/14 -72dBm at MCS7/15

Wireless Module Parameters

	5GHz, HT40 -88dBm at MCS0/8 -85dBm at MCS1/9 -83dBm at MCS2/10 -80dBm at MCS3/11 -76dBm at MCS4/12 -72dBm at MCS5/13 -70dBm at MCS6/14 -68dBm at MCS7/15 · 802.11ac (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) VHT20 -91dBm at MCS0 -89dBm at MCS1 -87dBm at MCS2 -84dBm at MCS3 -80dBm at MCS4 -76dBm at MCS5 -74dBm at MCS6 -72dBm at MCS7 -68dBm at MCS8 VHT40 -90dBm at MCS0 -86dBm at MCS1 -84dBm at MCS2 -81dBm at MCS3 -77dBm at MCS4 -73dBm at MCS5 -72dBm at MCS6 -70dBm at MCS7 -67dBm at MCS8 -65dBm at MCS9 VHT80 -86dBm at MCS0 -83dBm at MCS1 -81dBm at MCS2 -78dBm at MCS3 -74dBm at MCS4 -70dBm at MCS5 -68dBm at MCS6 -66dBm at MCS7 -63dBm at MCS8 -61dBm at MCS9 · 802.11ax (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) 2.4GHz, HE20 -90dBm at HE0 -89dBm at HE1 -85dBm at HE2 -83dBm at HE3 -80dBm at HE4 -78dBm at HE5 -76dBm at HE6 -73dBm at HE7 -72dBm at HE8 -68dBm at HE9 -64dBm at HE10 -61dBm at HE11

Wireless Module Parameters

	2.4GHz, HE40
	-90dBm at HE0
	-88dBm at HE1
	-85dBm at HE2
	-83dBm at HE3
	-80dBm at HE4
	-76dBm at HE5
	-74dBm at HE6
	-72dBm at HE7
	-69dBm at HE8
	-67dBm at HE9
	-64dBm at HE10
	-61dBm at HE11
	5GHz, HE20
	-89dBm at HE0
	-88dBm at HE1
	-86dBm at HE2
	-83dBm at HE3
	-80dBm at HE4
	-78dBm at HE5
	-76dBm at HE6
	-74dBm at HE7
	-70dBm at HE8
	-68dBm at HE9
	-65dBm at HE10
	-63dBm at HE11
	5GHz, HE40
	-88dBm at HE0
	-86dBm at HE1
	-84dBm at HE2
	-81dBm at HE3
	-78dBm at HE4
	-74dBm at HE5
	-73dBm at HE6
	-71dBm at HE7
	-67dBm at HE8
	-65dBm at HE9
	-62dBm at HE10
	-60dBm at HE11
	5GHz, HE80
	-84dBm at HE0
	-81dBm at HE1
	-79dBm at HE2
	-75dBm at HE3
	-73dBm at HE4
	-71dBm at HE5
	-70dBm at HE6
	-68dBm at HE7
	-63dBm at HE8
	-61dBm at HE9
	-59dBm at HE10
	-56dBm at HE11

Physical Parameters

Dimensions (L x W x H)	· 174 x 139 x 60 mm (6.85 x 5.47 x 2.36 in)
Weight	· 280 g (0.62 lb)

Operating Environment	
Power	· Output: 12V DC, 1A
Temperature	· Operating: from 0 to 40 °C · Storage: from -20 to 65 °C
Humidity	· Operating: from 10% to 90% (non-condensing) · Storage: from 5% to 95% (non-condensing)

Product Appearance

Upper Panel

Figure 1. Upper panel view.

LED	Mode	Description
Power	*Solid orange*	The router is being loaded.
	Solid white	The router is powered on.
	Blinking white	The firmware is being updated.
	No light	The router is powered off.

LED	Mode	Description
Internet	*Solid white*	The default WAN connection is on.
	Solid orange	• The default WAN connection is off, or • there are no WAN connections created.
	No light	• The router is powered off, or • the device is configured as an access point or repeater.
WLAN 2.4G **WLAN 5G**	*Solid white*	The router's WLAN of the relevant band is on.
	Fast blinking white	Data transfer through the Wi-Fi network of the relevant band.
	Slow blinking white	When attempting to connect a mesh network device in the Controller role or add a wireless device via the hardware **WPS** button, both LEDs are blinking. When attempting to connect mesh network devices in the Agent role or add a wireless device via the web-based interface, the LED of the band selected in the settings of the EasyMesh or WPS function is blinking.
	No light	The router's WLAN of the relevant band is off.

Back Panel

Figure 2. Back panel view.

Port	Description
LAN 1-3	3 Ethernet ports to connect computers or network devices.
INTERNET	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).
DC IN 12V=1A	Power connector.
POWER	A button to turn the router on/off.

Port	Description
WPS	A button to connect mesh network devices, set up wireless connection (the WPS function), and enable/disable the wireless network. To connect mesh network devices: with the device turned on and factory default settings or with the EasyMesh function enabled in the router settings, press the button, hold it for 2 seconds, and release. To use the WPS function: with the device turned on, press the button, hold it for 2 seconds, and release. The **WLAN 2.4G** and **WLAN 5G** LEDs should start blinking. To disable the router's wireless network: with the device turned on, press the button, hold for 10 seconds, and release. The **WLAN 2.4G** and **WLAN 5G** LEDs should turn off.
RESET	A button to restore the factory defaults. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.

In case the **Power** and **Internet** LEDs are blinking orange 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.

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

Delivery Package

The following should be included:

- Router DIR-X1860

- Power adapter DC 12V/1A

- Ethernet cable

- "*Quick Installation Guide*" (brochure).

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

> **!** 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 a built-in 3-port switch DIR-X1860 (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 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, ac, or ax NIC (Wi-Fi adapter). In addition, you should specify the values of SSID, channel number and security settings defined in the web-based interface of the router for all these wireless workstations.

Connecting to Mobile Device with D-Link Assistant Application

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

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

3. Make sure that the Wi-Fi connection on your mobile device is on. To switch it on, go to the mobile device settings.

4. In the list of available wireless networks on your mobile device, select the wireless network `DIR-X1860` (for operating in the 2.4GHz band) or `DIR-X1860-5G` (for operating in the 5GHz band).

5. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) as the password and connect to the wireless network of DIR-X1860.

6. Launch D-Link Assistant application on your mobile device. The application is available for Android smartphones in Google Play.

D-Link Assistant for Android

7. Make sure that the application correctly identified the router to which you connect.

8. In the application interface, select the **Advanced Settings** menu option to go through the Initial Configuration Wizard or finish the Wizard earlier and go the configuration menu (for the description of the configuration pages, see the relevant section of the ***Configuring via Web-based Interface*** chapter).

> **!** As 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.

If you changed the administrator password via the web-based interface, when DIR-X1860 is accessed with the application the next time, click the **ENTER LOGIN/PASSWORD** button. Enter the username (`admin`) and the password you specified.

Connecting to PC

PC with Ethernet Adapter

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

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

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

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

Obtaining IP Address Automatically (OS Windows 7)

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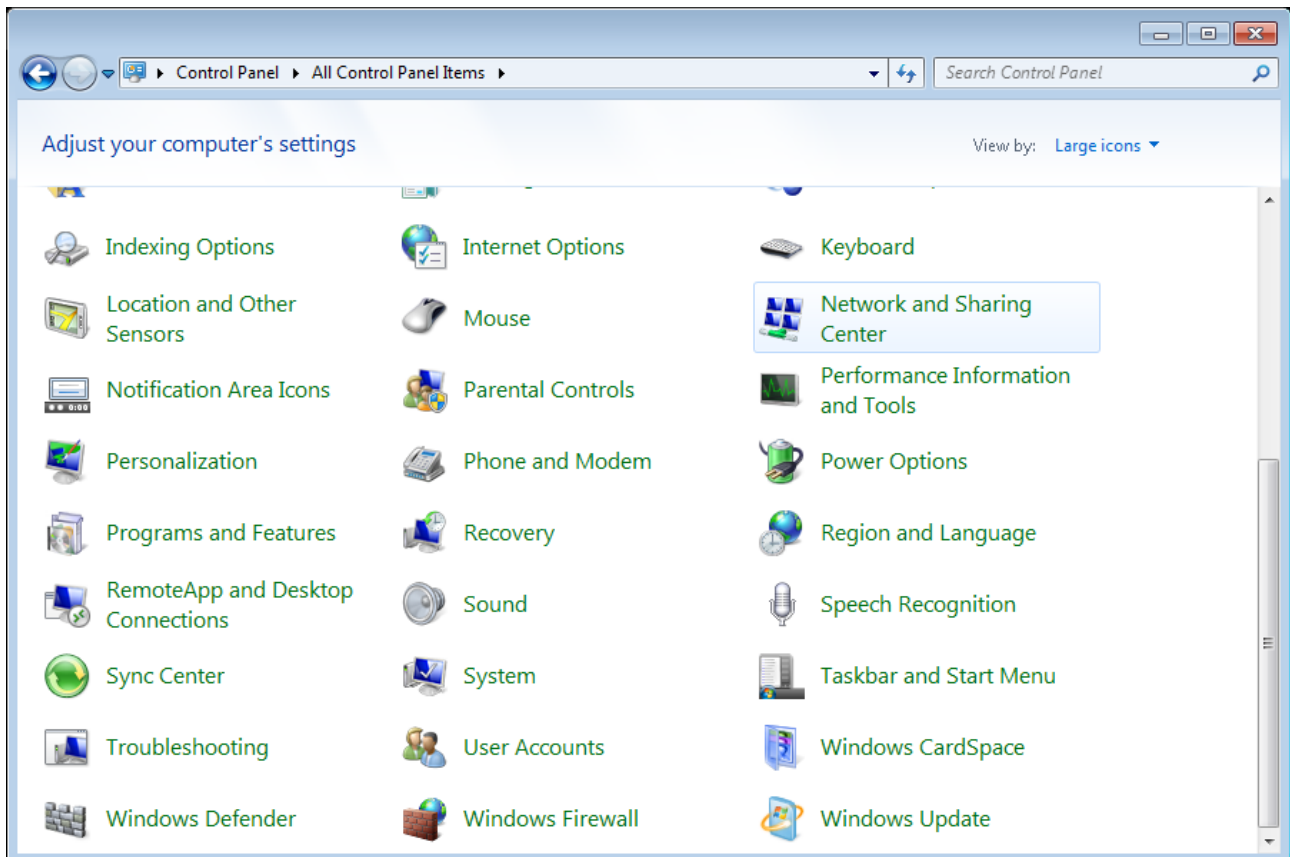

*Figure 3. The **Control Panel** window.*

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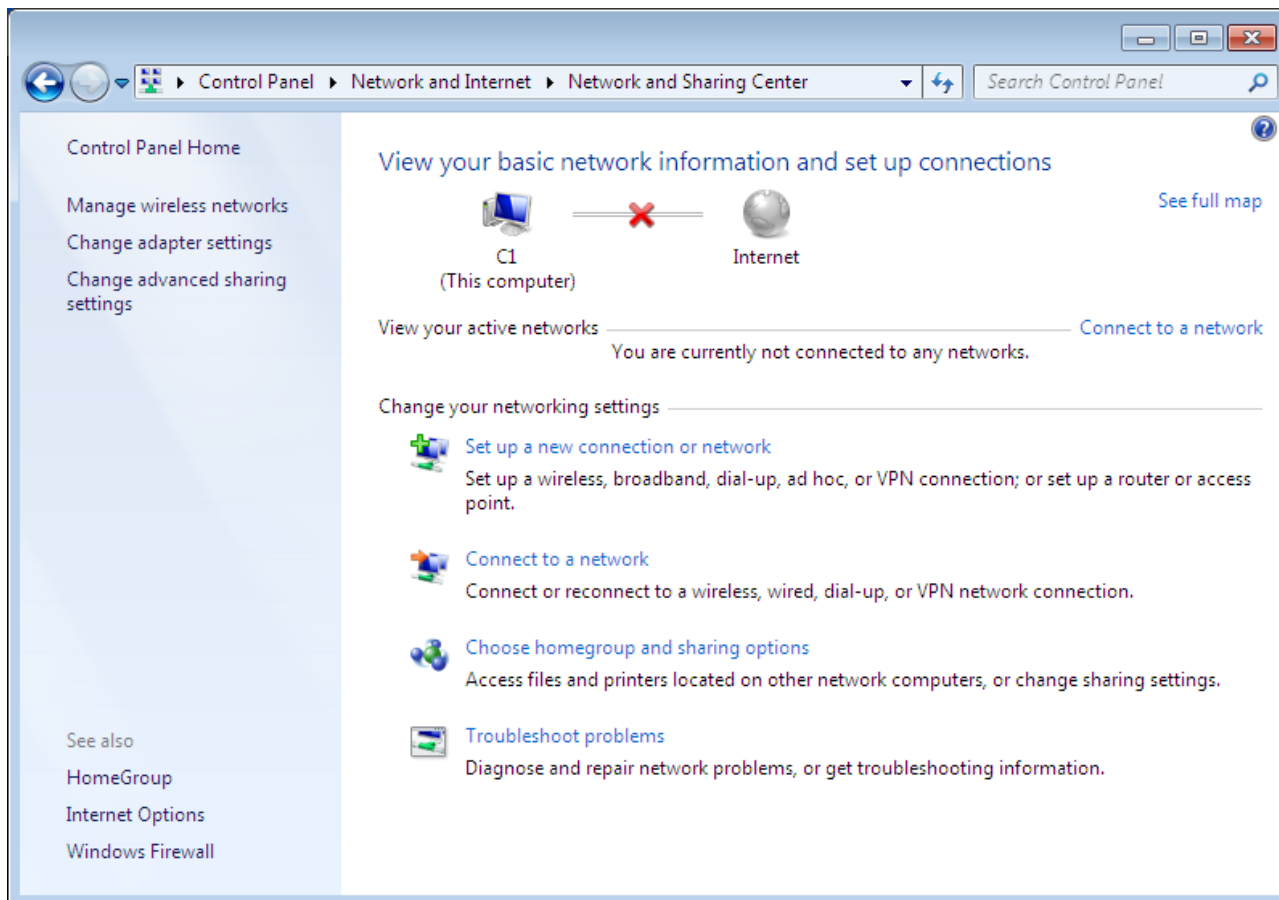

*Figure 4. The **Network and Sharing Center** window.*

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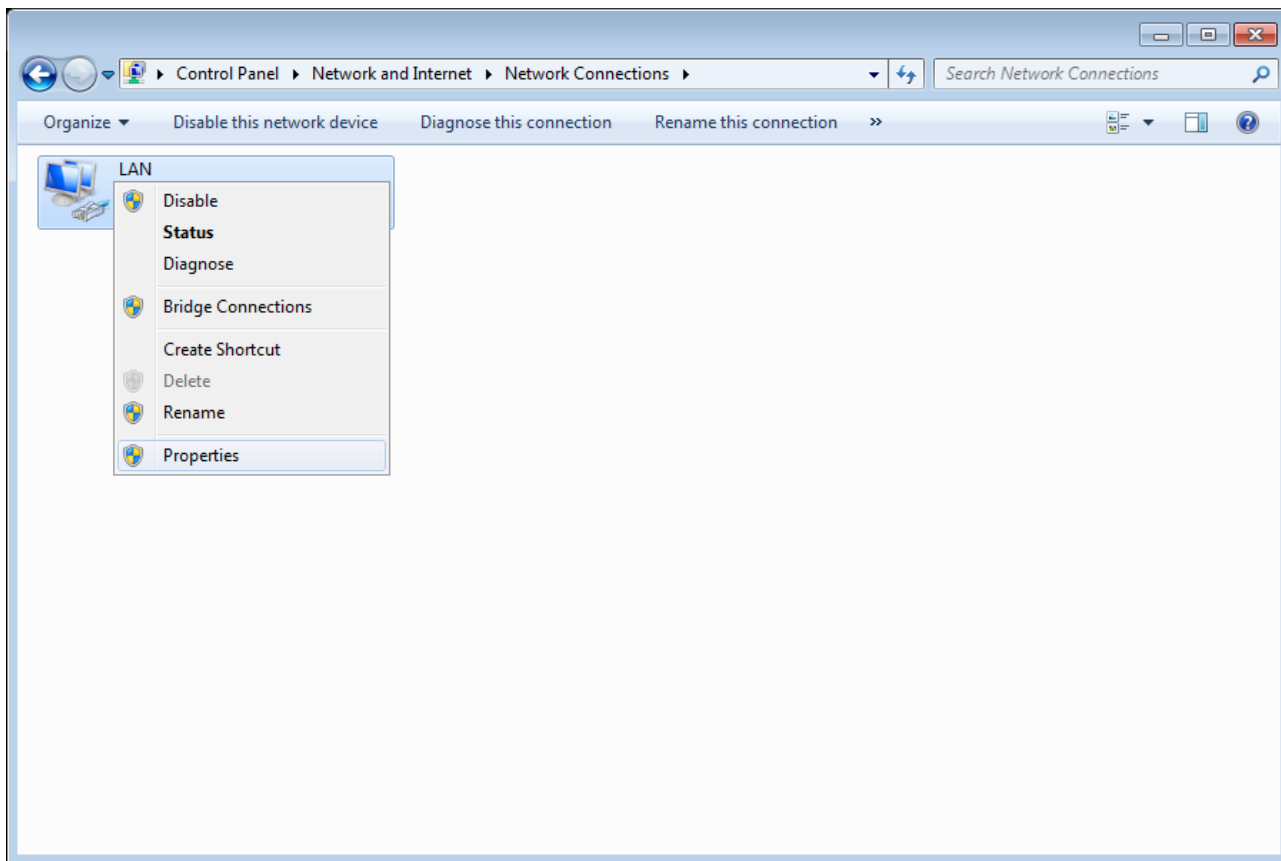

*Figure 5. The **Network Connections** window.*

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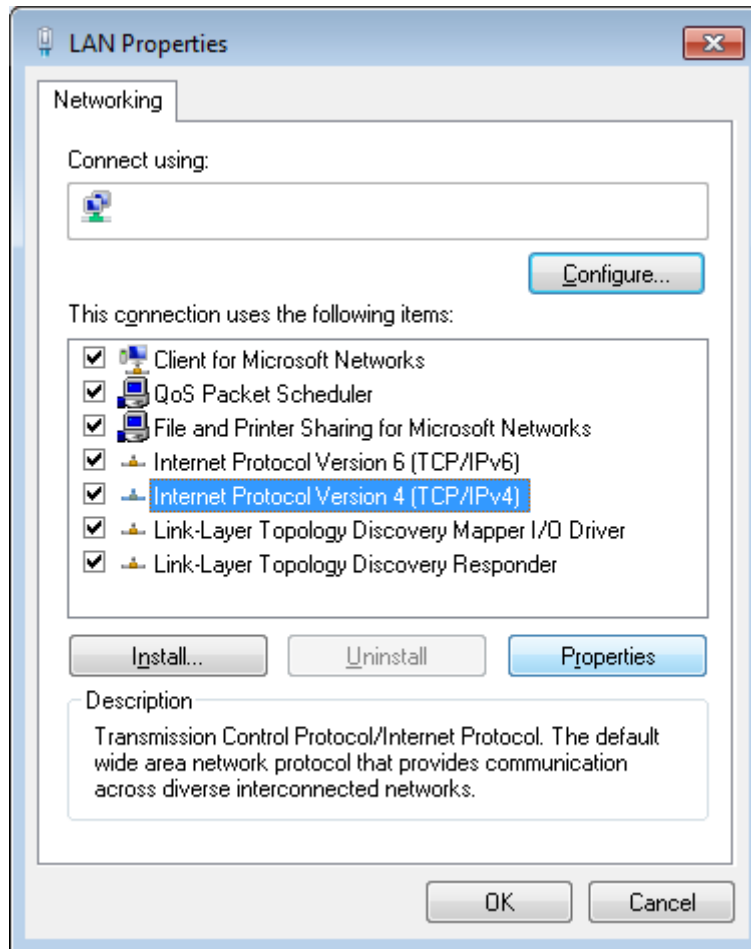

*Figure 6. The **Local Area Connection Properties** window.*

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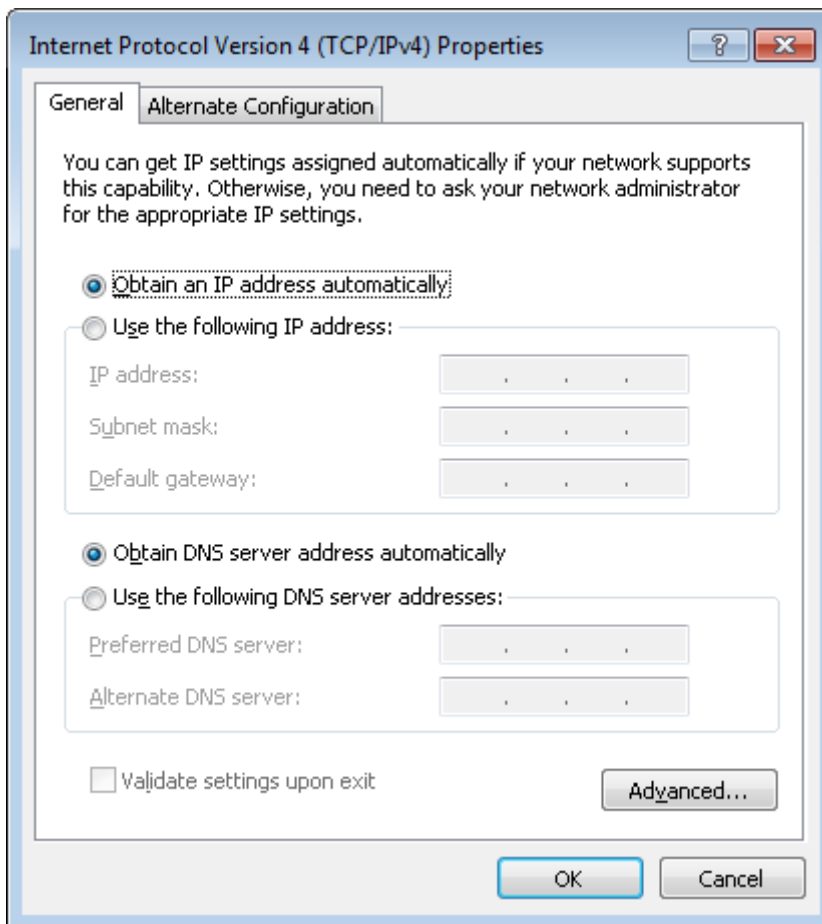

*Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

Obtaining IP Address Automatically (OS Windows 10)

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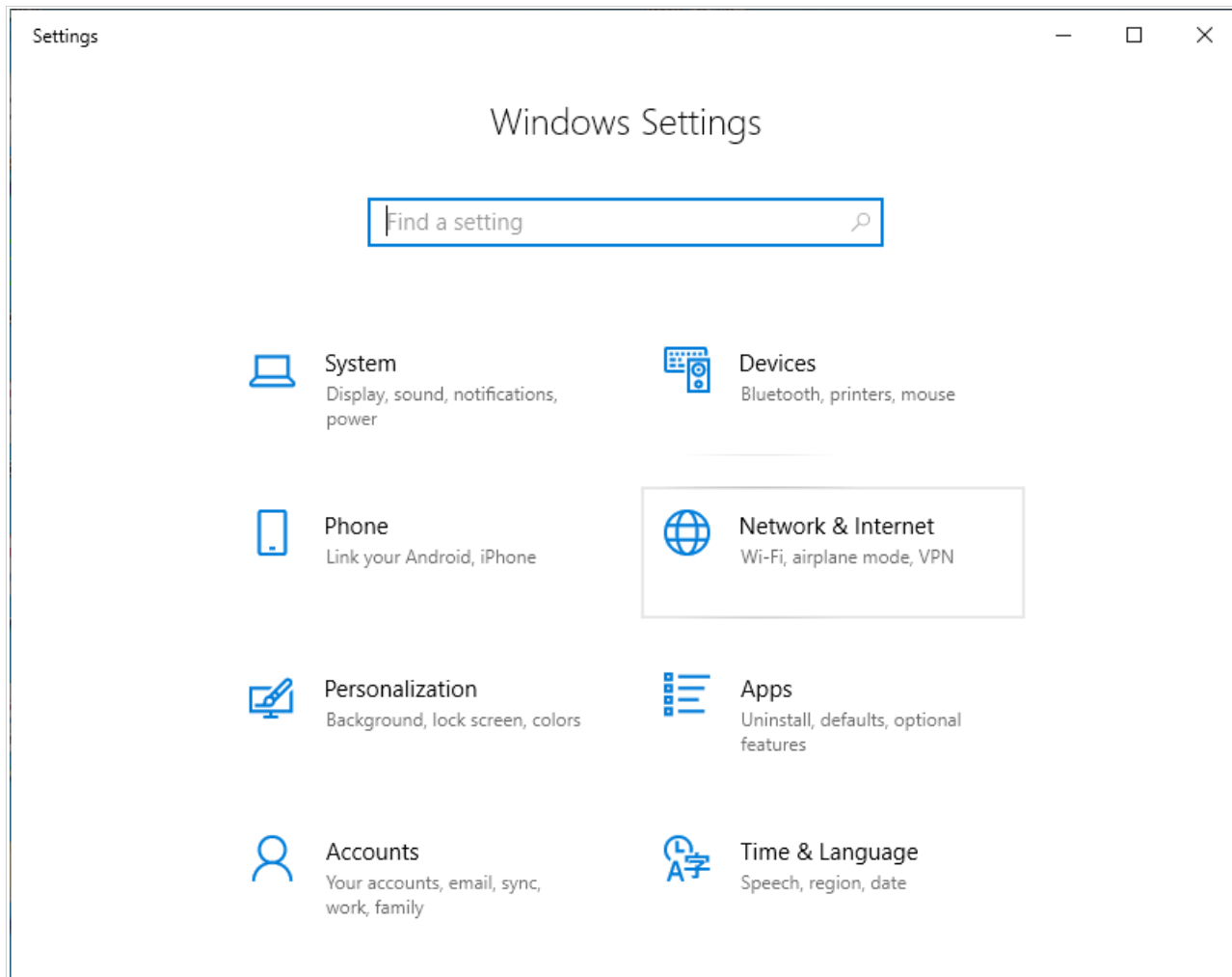
2. Select the **Network & Internet** section.

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

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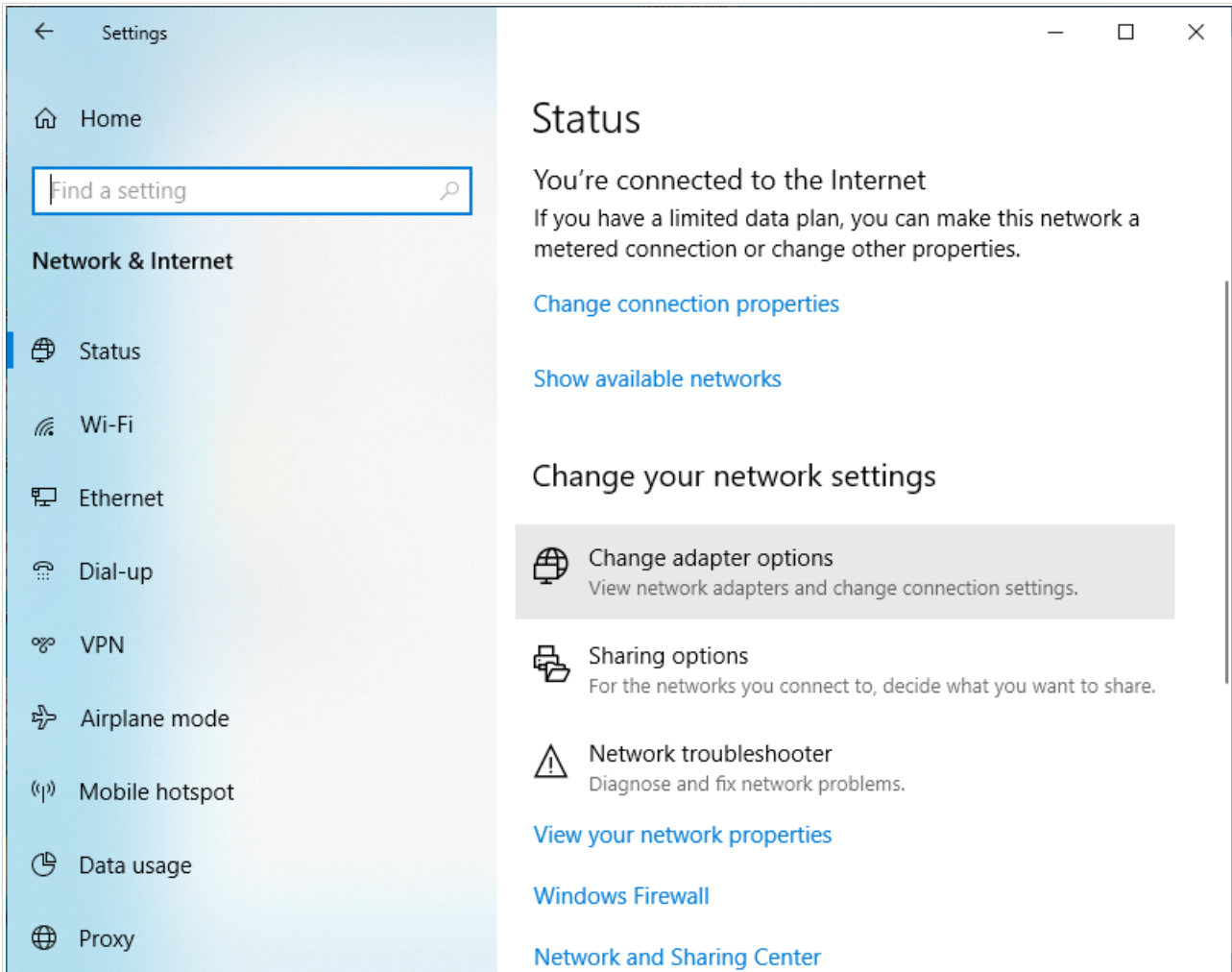

*Figure 9. The **Network & Internet** window.*

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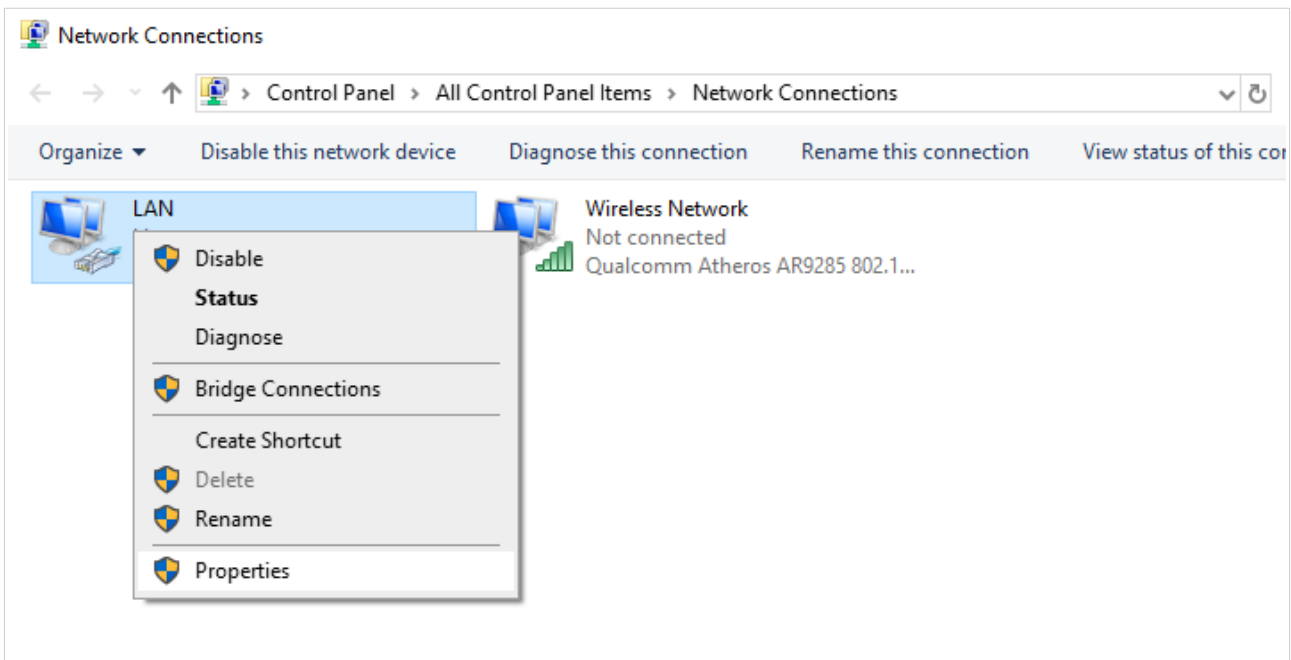

*Figure 10. The **Network Connections** window.*

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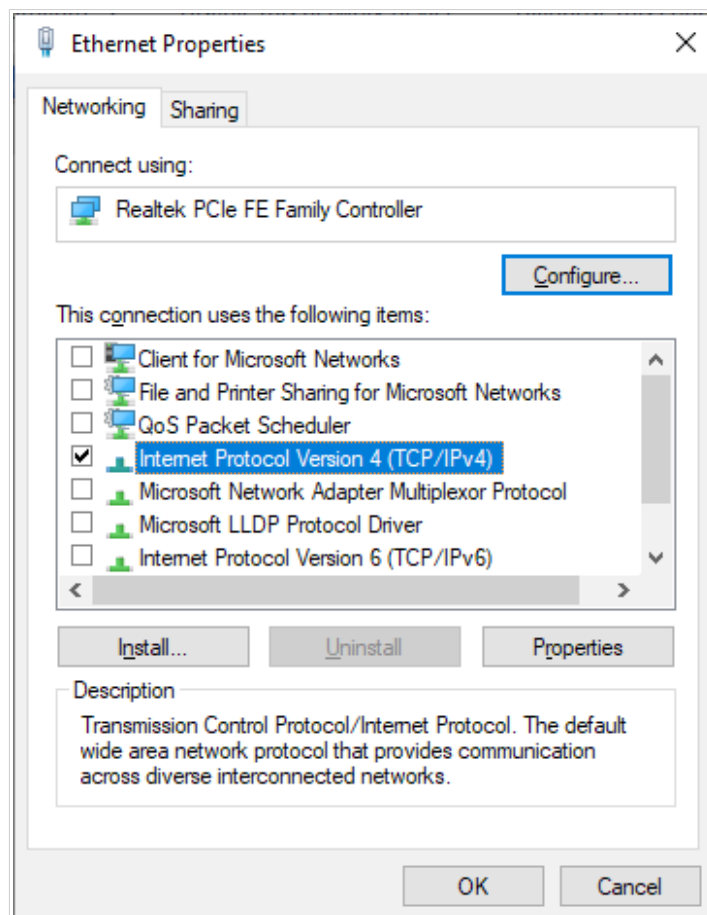

Figure 11. The local area connection properties window.

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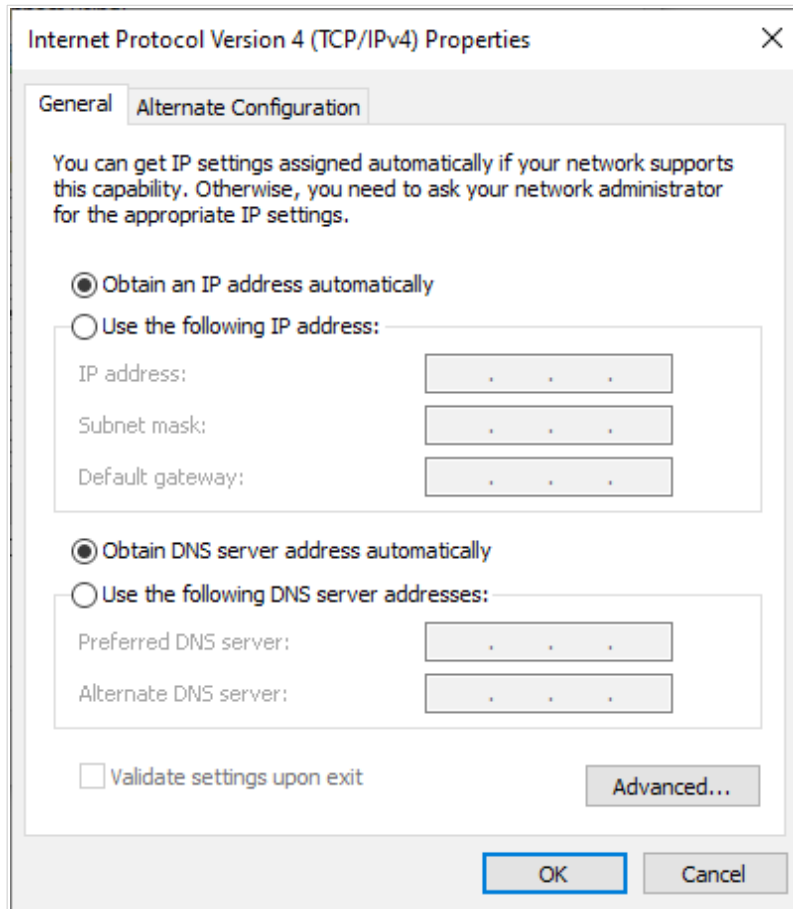

*Figure 12. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

PC with Wi-Fi Adapter

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

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

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

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

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

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

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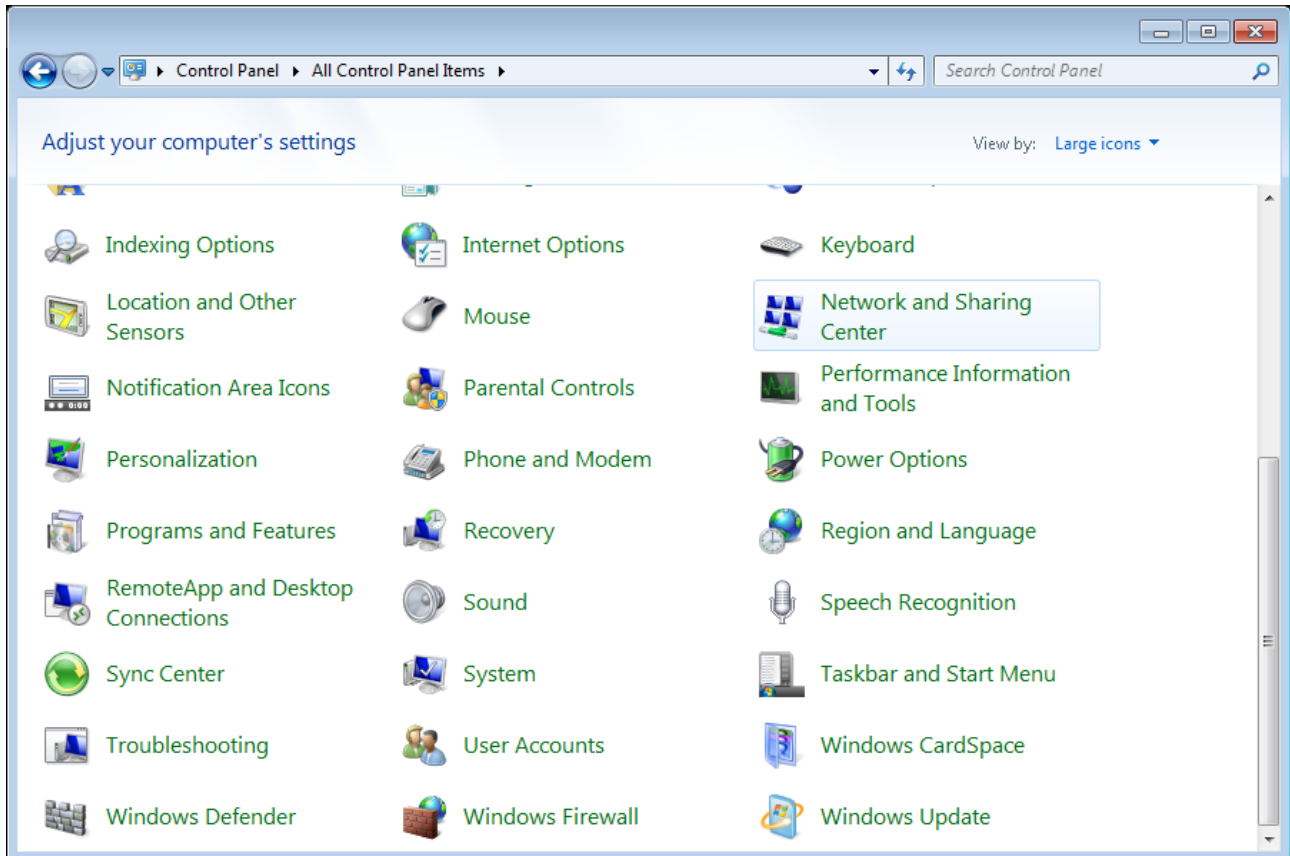

*Figure 13. The **Control Panel** window.*

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

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

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

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

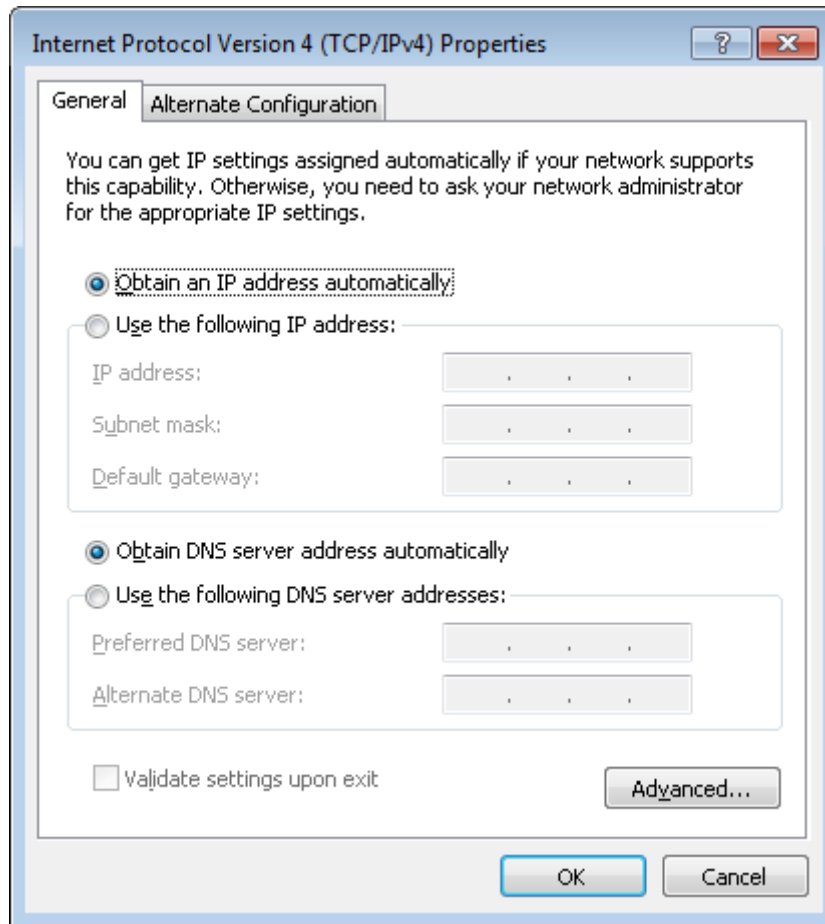*Figure 14. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

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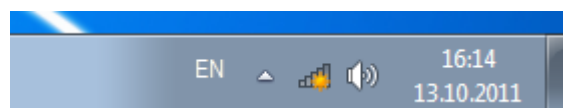

Figure 15. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network `DIR-X1860` (for operating in the 2.4GHz band) or `DIR-X1860-5G` (for operating in the 5GHz band) and click the **Connect** button.
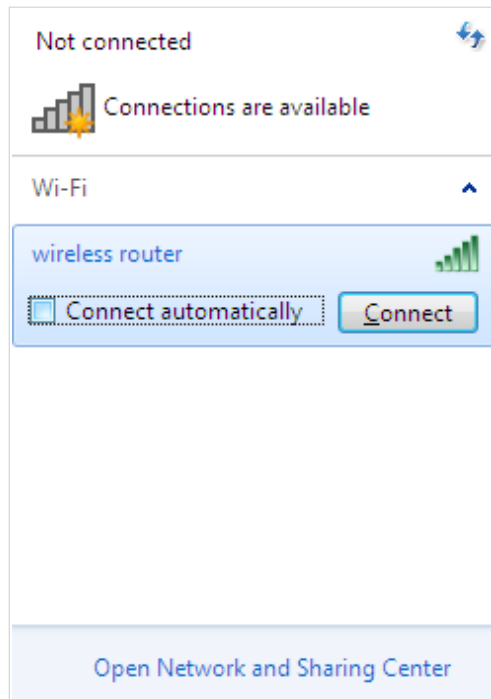
Figure 16. The list of available networks.

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

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

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

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

1. Click the **Start** button and proceed to the **Settings** window.

2. Select the **Network & Internet** section.
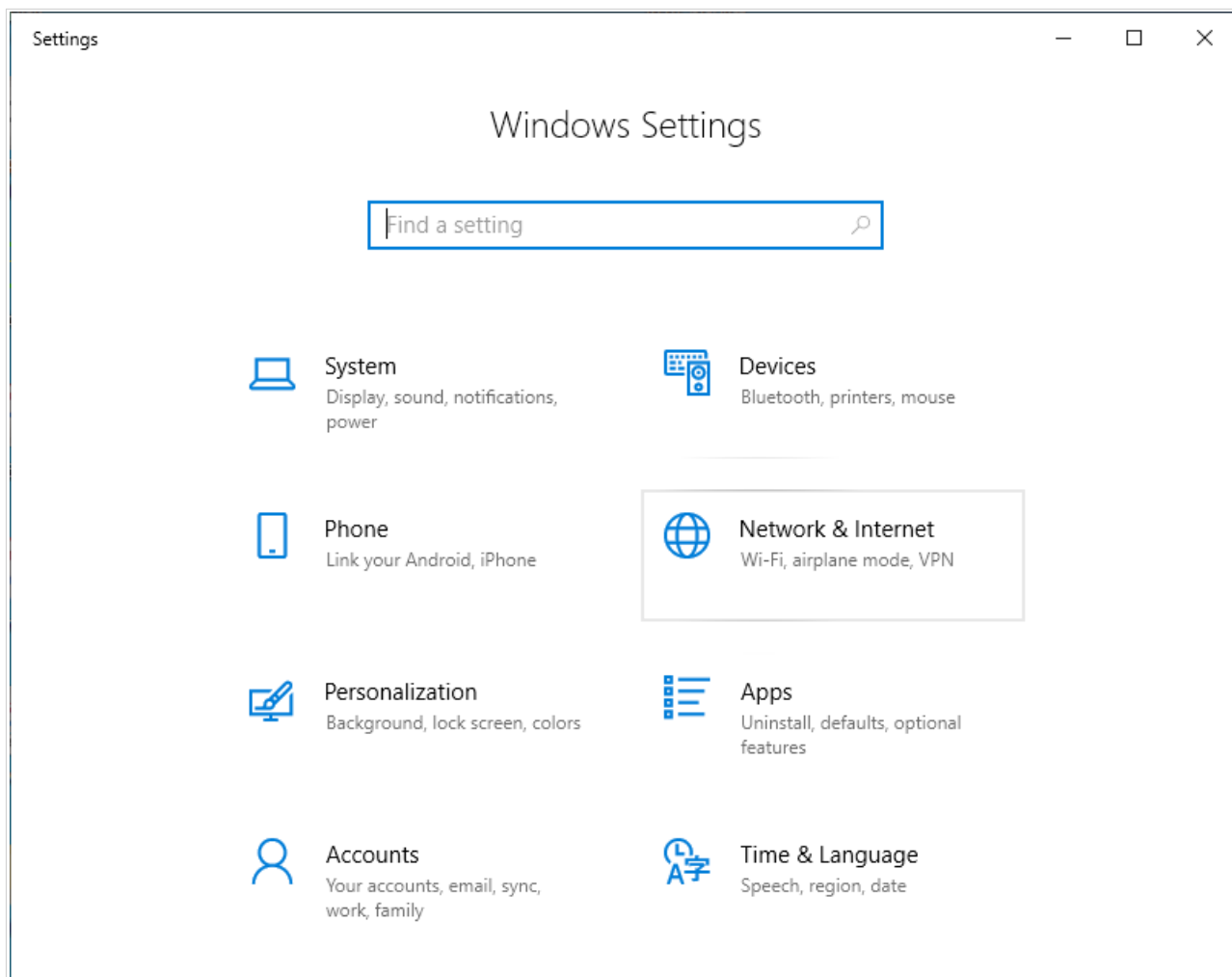
*Figure 17. The **Windows Settings** window.*

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

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

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

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.
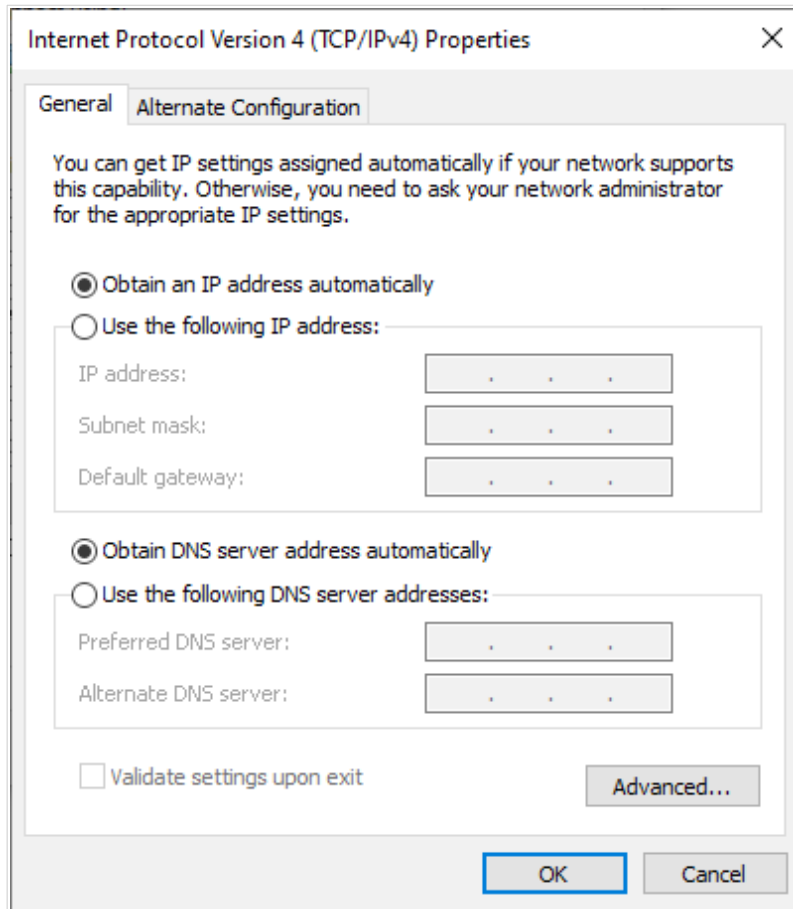
Figure 18. The Internet Protocol Version 4 (TCP/IPv4) Properties window.

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

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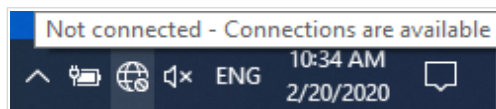

Figure 19. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network **DIR-X1860** (for operating in the 2.4GHz band) or **DIR-X1860-5G** (for operating in the 5GHz band) and click the **Connect** button.
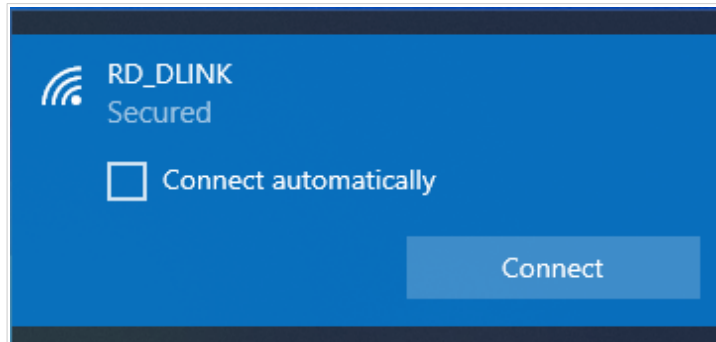
Figure 20. The list of available networks.

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

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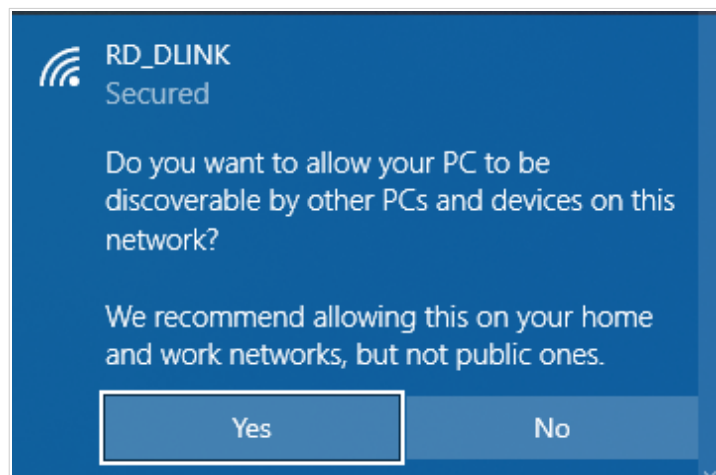
Figure 21. PC discovery settings.

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

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

Connecting to Web-based Interface

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

> **!** Clients connected to the router with default settings do not have access to the Internet. To get started, please set your own password used to access the web-based interface and, if needed, configure other settings recommended by your ISP.

Start a web browser (see the **Before You Begin** section, page 20). In the address bar of the web browser, enter the domain name of the router (by default, `dlinkrouter.local`) with a dot at the end and press the **Enter** key. Also you can enter the IP address of the device (by default, `192.168.0.1`).

Figure 22. Connecting to the web-based interface of the DIR-X1860 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 46).

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

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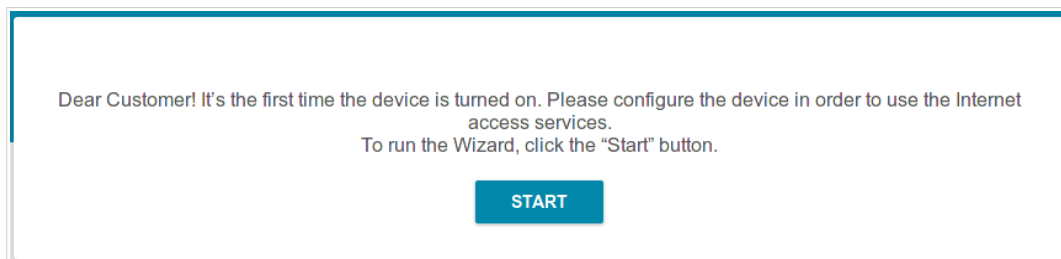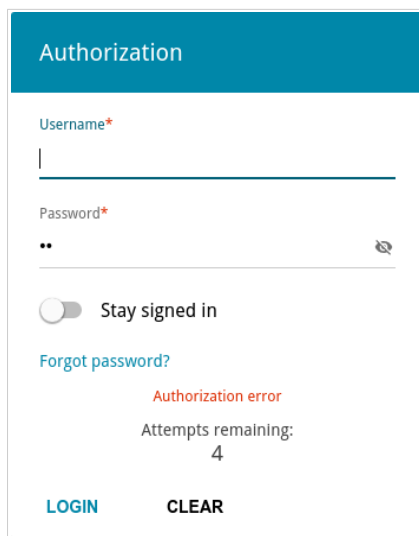
Figure 23. The page for running the Initial Configuration Wizard.

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

Figure 24. The login page.

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

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

Web-based Interface Structure

Summary Page

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

Figure 25. The summary page.

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

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

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **Initial Configuration Wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 46).

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.

Home Page

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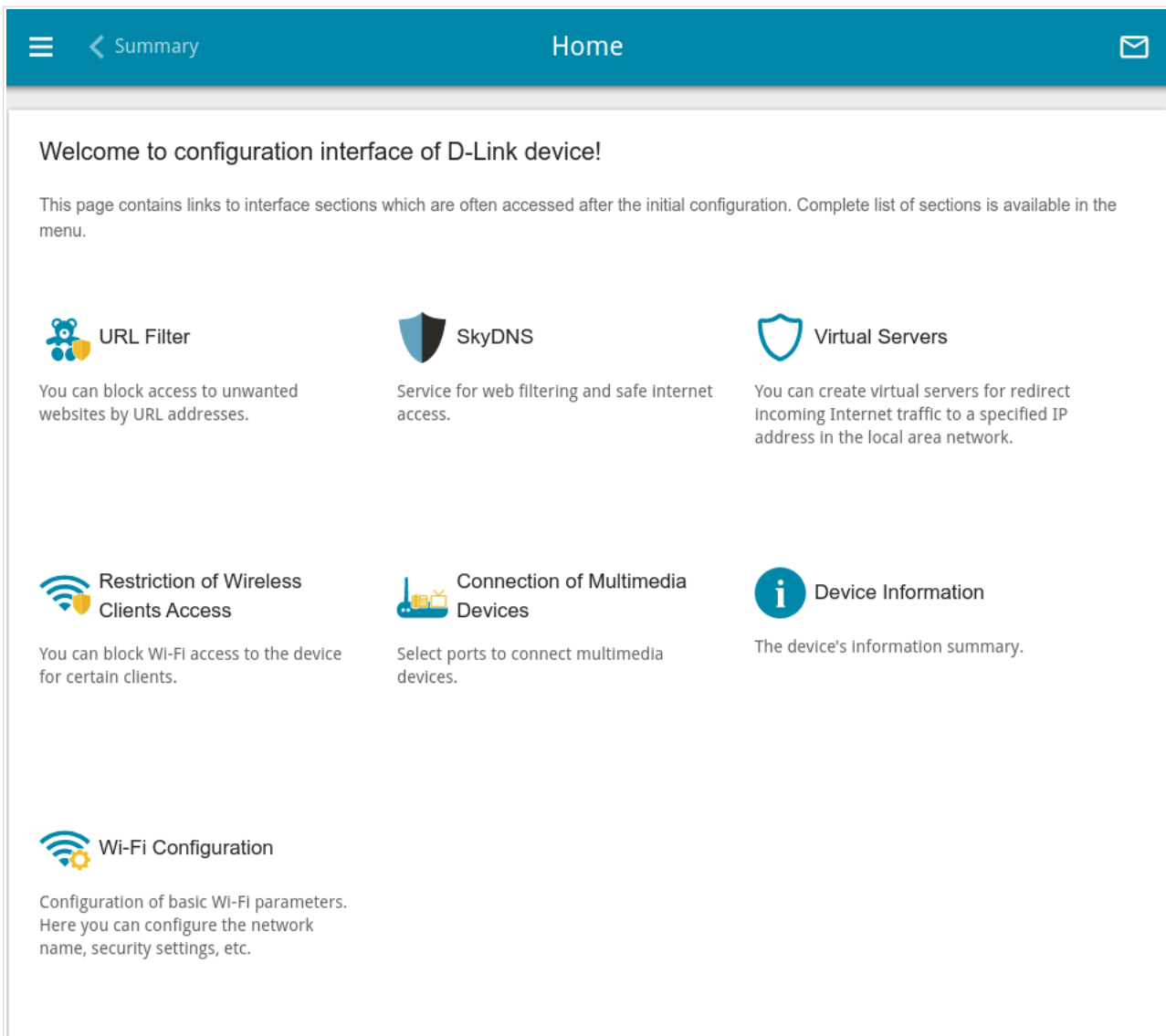

*Figure 26. The **Home** page.*

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

Menu Sections

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

In the **Initial Configuration** section you can run the Initial Configuration Wizard. The Wizard allows you to configure the router for operation in the needed mode and specify all parameters necessary for getting started (for the description of the Wizard, see the ***Initial Configuration Wizard*** section, page 46).

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 75).

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 84).

The pages of the **VPN** section are designed for configuring VPN connections based on IPsec/GRE/EoGRE/IPIP/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 131).

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 156).

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 191).

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 231).

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 252).

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 279).

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

Notifications

The router's web-based interface displays notifications in the top right part of the page.
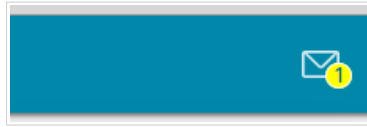
Figure 27. The web-based interface notifications.

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

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration Wizard

To start the Initial Configuration Wizard, go to the **Initial Configuration** section. On the opened page, click the **OK** button and wait until the factory default settings are restored.
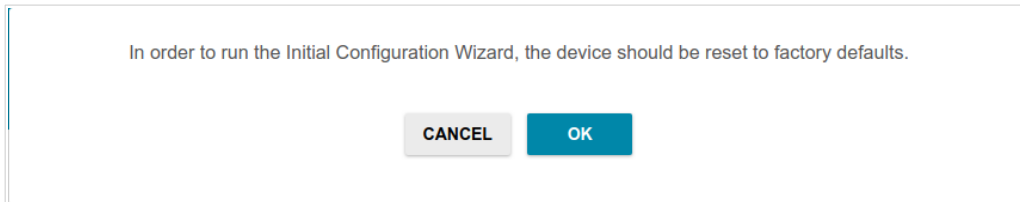
Figure 28. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network `DIR-X1860` (for operating in the 2.4GHz band) or `DIR-X1860-5G` (for operating in the 5GHz band) and click the **NEXT** button.
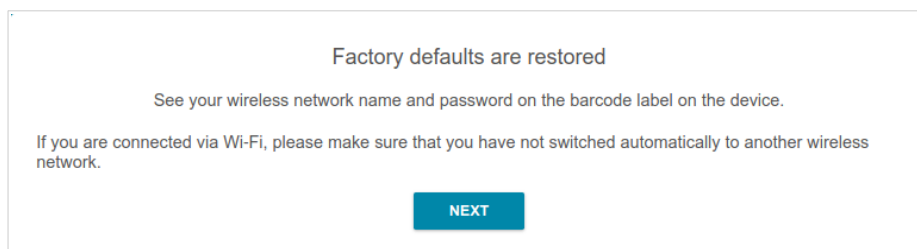
Figure 29. Checking connection to the wireless network.

Click the **START** button.
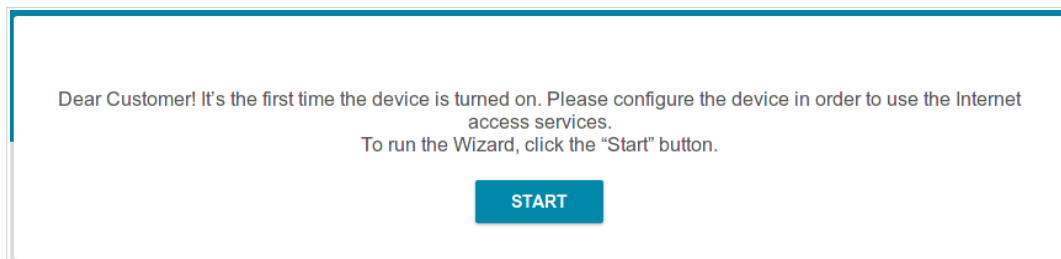
Figure 30. Starting the Wizard.

On the opened page, click **YES** in order to leave the current language of the web-based interface or click **NO** to select the other language.
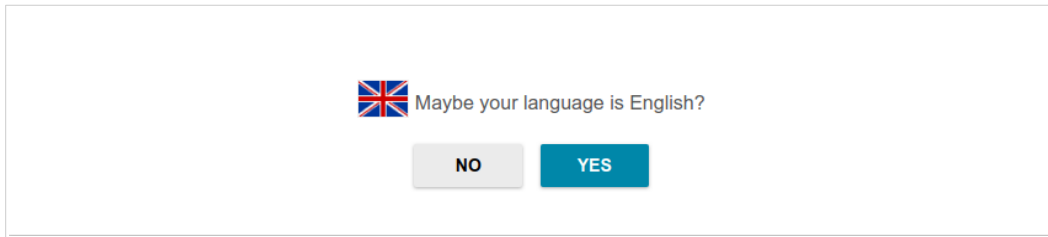
Figure 31. Selecting a language.

You can finish the wizard earlier and go to the menu of the web-based interface. To do this, click the **ADVANCED SETTINGS** button. On the opened page, change the default settings: specify the administrator password in the **User's interface password** and **Password confirmation** and the name of the wireless network in the 2.4GHz and 5GHz bands in the **Network name 2.4 GHz (SSID)** and **Network name 5 GHz (SSID)** fields correspondingly. Then click the **APPLY** button.
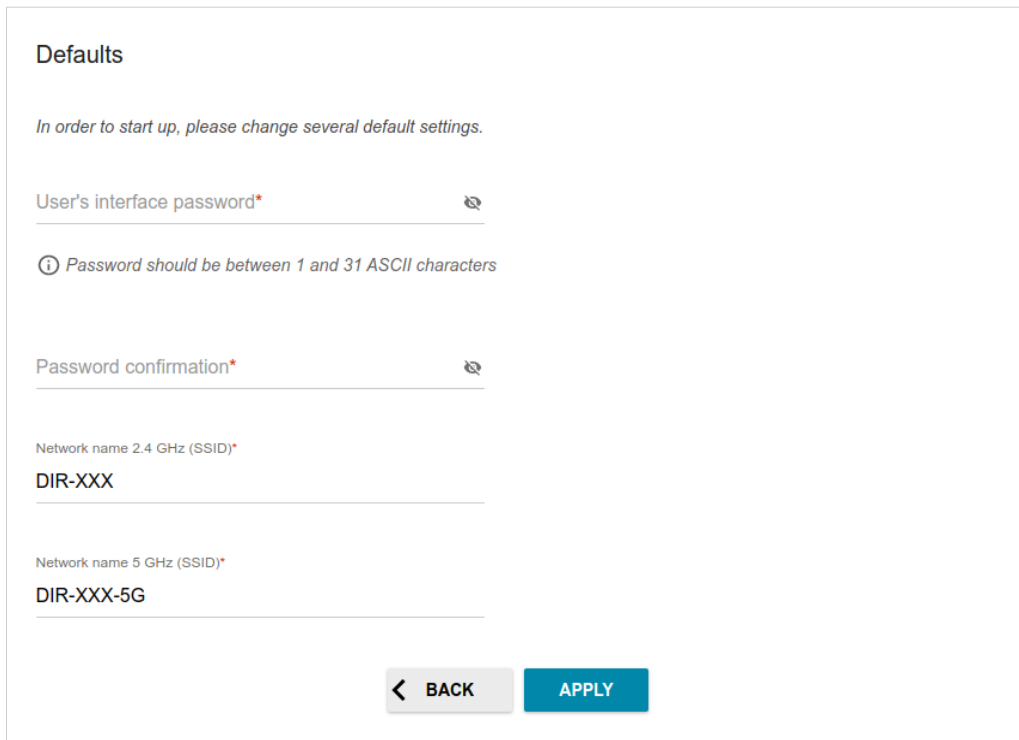
Figure 32. Changing the default settings.

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

Selecting Operation Mode

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

Router

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

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

In order to connect your device to a wireless ISP (WISP), on the **Device mode** page, from the **Connection method** list, select the **Autonomous** value. Then from the **Work mode** list select the **WISP Repeater** value. In this mode you can connect your device to another access point, configure a WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.
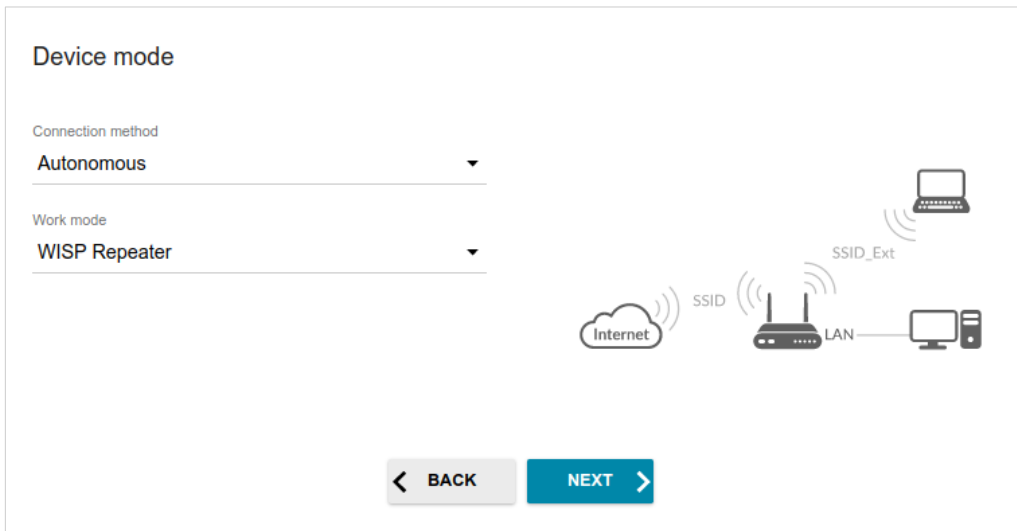
*Figure 34. Selecting an operation mode. The **WISP Repeater** mode.*

Access Point or Repeater

In order to connect your device to a wired router for adding a wireless network to the existing local network, on the **Device mode** page, from the **Connection method** list, select the **Autonomous** value. Then from the **Work mode** list select the **Access point** value. In this mode you can change the LAN IP address, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.
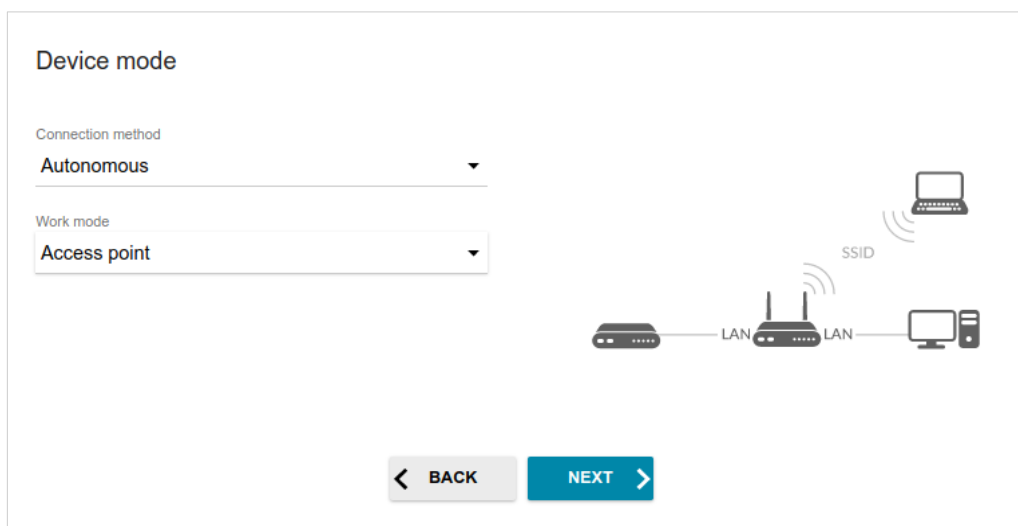
*Figure 35. Selecting an operation mode. The **Access point** mode.*

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

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

Mesh Network Main Device (Controller)

In order to configure DIR-X1860 as a main device of your mesh network, from the **Connection method** list, select the **EasyMesh** value. Then from the **Device role** list, select the **Controller** value. From the **Backhaul** list, select the band where your mesh network operates. Also you can connect devices into the mesh network using an Ethernet cable by connecting it to LAN ports of the main and subordinate device or two subordinate devices.

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

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

In order to connect your main device to a wired ISP, from the **Work mode** list, select the **Router** value. In this mode you can configure a WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, configure LAN ports to connect an STB or VoIP phone, and set your own password for access to the web-based interface of the device.

*Figure 37. Configuring the EasyMesh function for the main device. The **Router** mode.*

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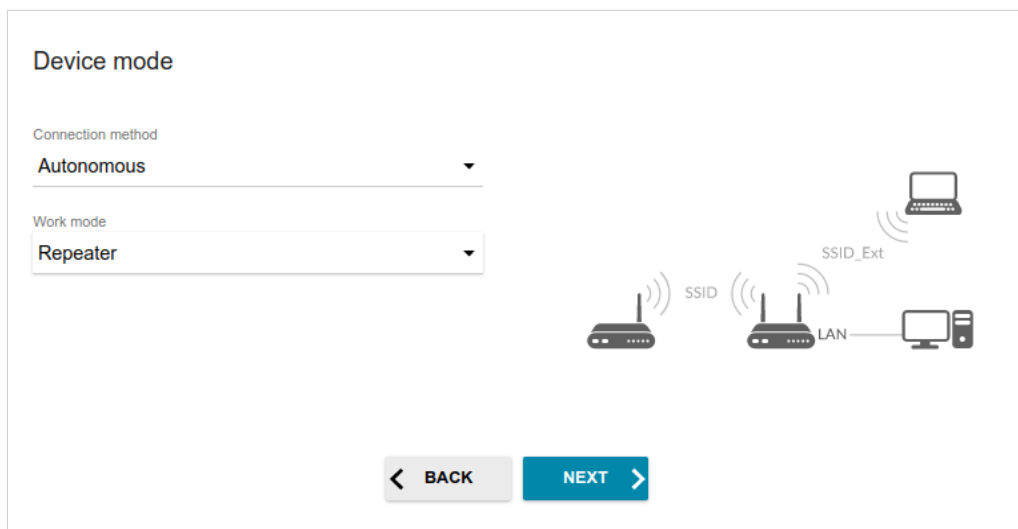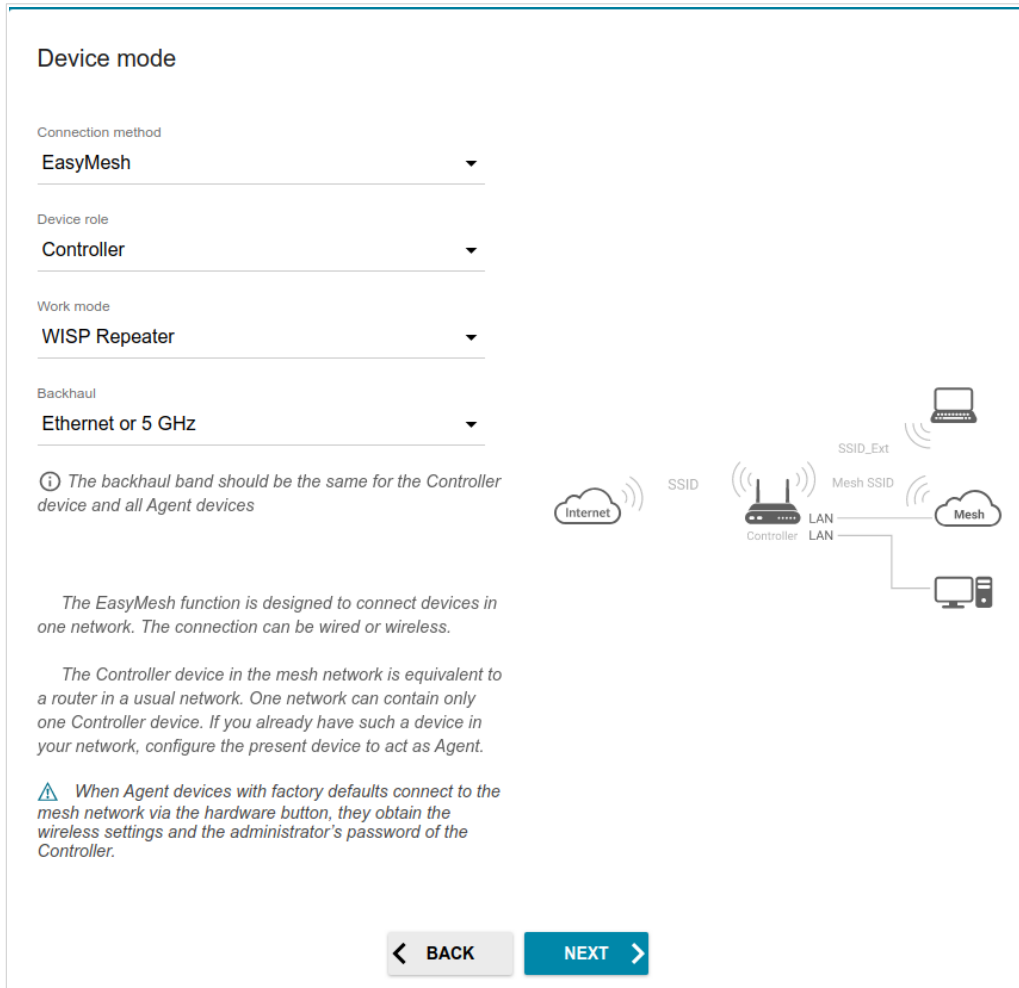

*Figure 38. Configuring the EasyMesh function for a main device. The **WISP Repeater** mode.*

Mesh Network Subordinate Device (Agent)

In order to configure DIR-X1860 as a subordinate device of your mesh network, from the **Connection method** list, select the **EasyMesh** value. Then from the **Device role** list, select the **Agent** value. From the **Backhaul** list, select the band where your main device (in the Controller role) operates. Also you can connect devices into the mesh network using an Ethernet cable by connecting it to LAN ports of the main and subordinate device or two subordinate devices.

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

Figure 39. Configuring the EasyMesh function for a subordinate device.

Changing LAN IPv4 Address

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

1. Select the **Automatic obtainment of IPv4 address** to let DIR-X1860 automatically obtain the LAN IPv4 address.

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

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

If you want to manually assign the LAN IPv4 address for DIR-X1860, 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 40. The page for changing the LAN IPv4 address.

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

Wi-Fi Client

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

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

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

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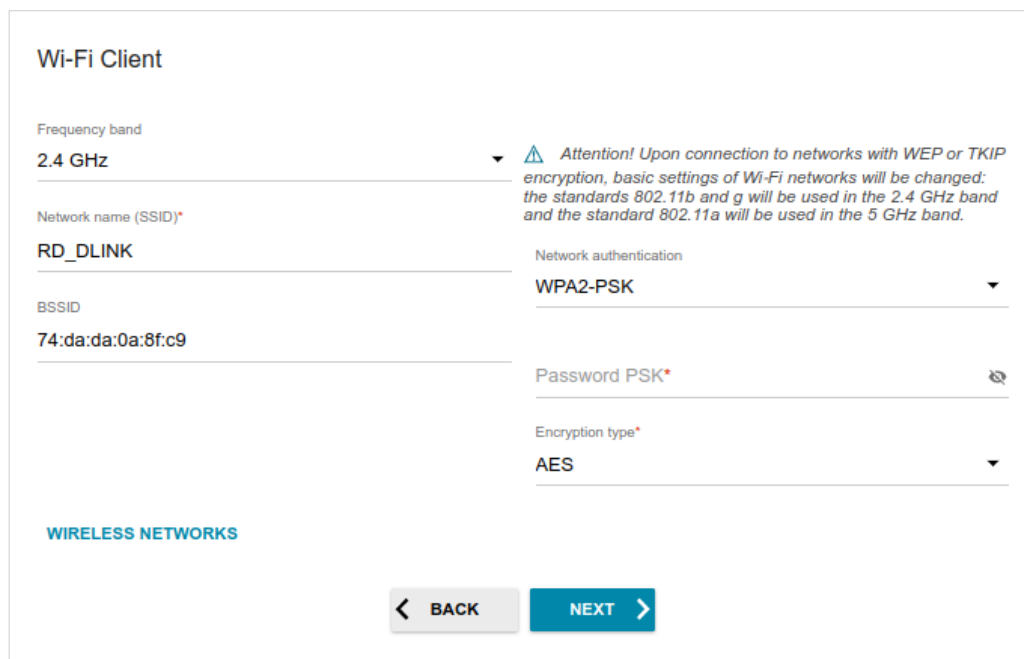
Figure 41. The page for configuring the Wi-Fi client.

If you connect to a hidden network, 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 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 42. The page for configuring Static IPv4 WAN connection.

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

Static IPv6 Connection

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

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

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

Figure 44. The page for configuring PPPoE WAN connection.

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

PPPoE + Static IP (PPPoE Dual Access) Connection

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

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

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

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

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

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

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

PPTP + Static IP or L2TP + Static IP Connection

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

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

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

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

Configuring Wireless Network

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

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

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

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

4. You can restore the parameters of the wireless network specified before resetting to factory defaults. To do this, click the **RESTORE** button.
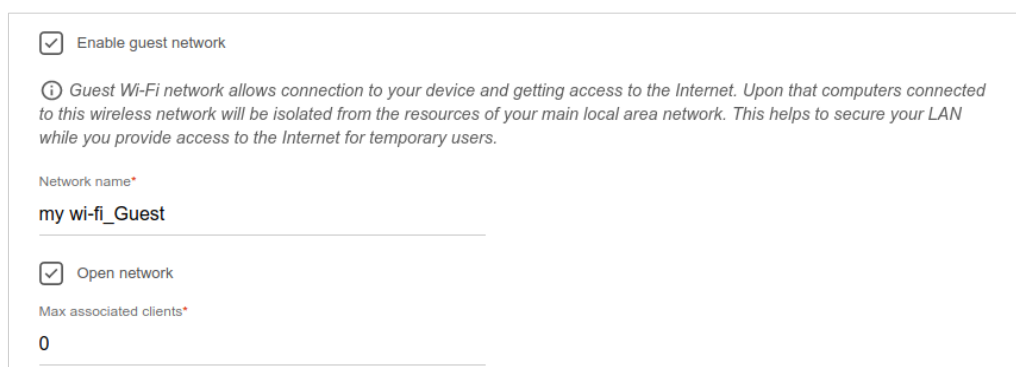
Figure 48. The page for configuring the wireless network.

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

Figure 49. The page for configuring the wireless network.

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

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

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

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

Configuring LAN Ports for IPTV/VoIP

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

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

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

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

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

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

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

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

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

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

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

Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **User's interface password** and **Password confirmation** fields. You may set any password except `admin`. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[4]
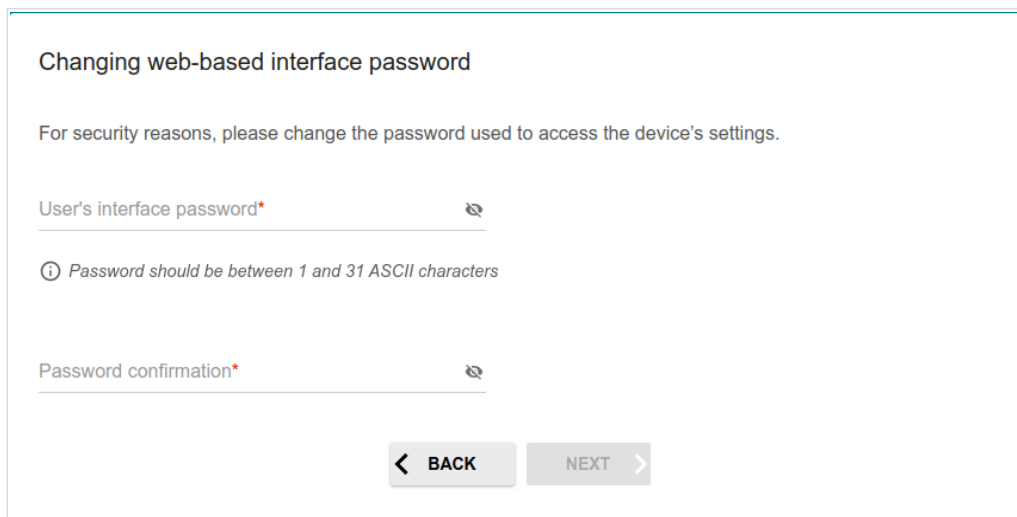
Figure 52. The page for changing the web-based interface password.

> **!** Remember or write down the new password for the administrator account. In case of losing the new password, you can access the settings of the router only after restoring the factory default settings via the hardware **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.

---

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

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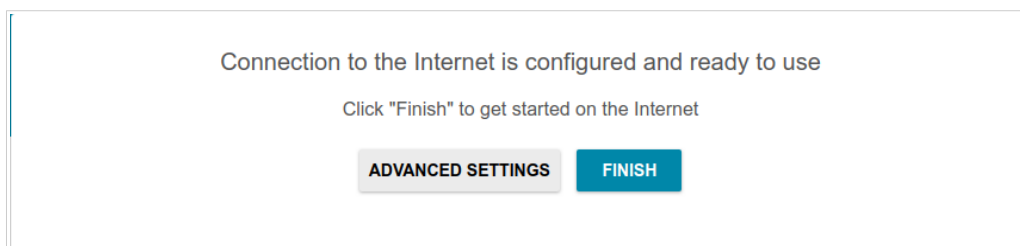
Figure 53. Checking the Internet availability.

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

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

If problems of connection have not been solved, contact the technical support of your ISP (as a rule, the technical support phone is provided with the agreement) or the D-Link technical support (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 43).

Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports or available wireless interfaces of the router for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DIR-X1860 in order to use these devices.

To start the Wizard, on the **Home** page, select the **Connection of Multimedia Devices** section.

If you need to select a port or wireless interface in order to use an additional device, left-click the relevant element in the **LAN** section (the selected element will be marked with a frame). Then click the **APPLY** button.
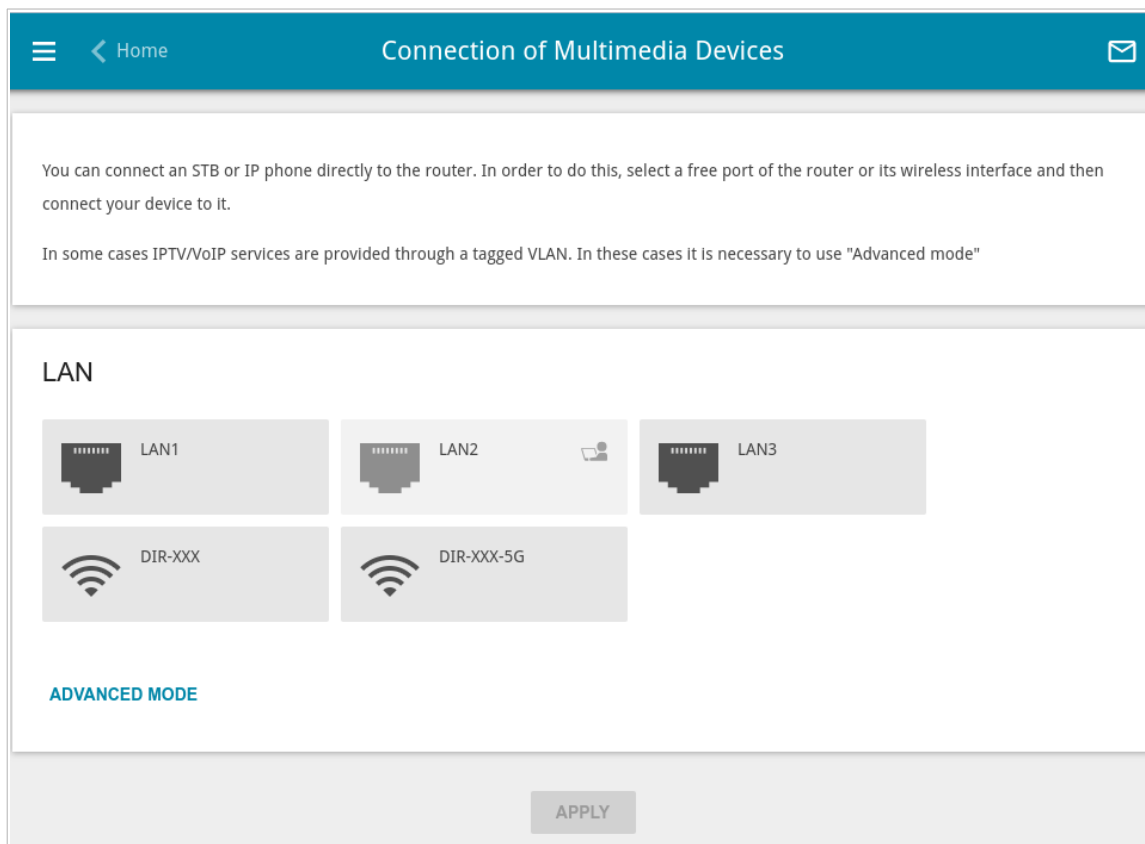
Figure 54. The Multimedia Devices Connection Wizard. The simplified mode.

If you need to configure a connection via VLAN, click the **ADVANCED MODE** button.
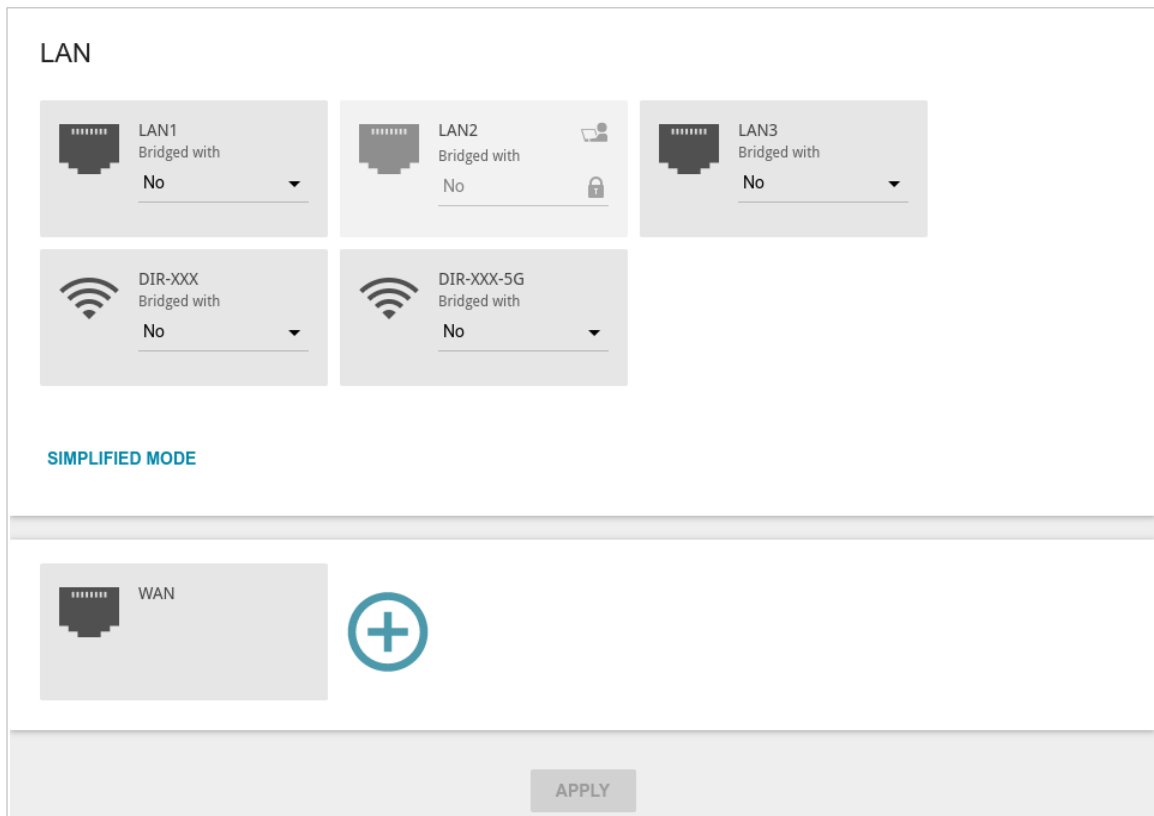
Figure 55. The Multimedia Devices Connection Wizard. The advanced mode.

In the **WAN** section, click the **Add** icon (⊕).
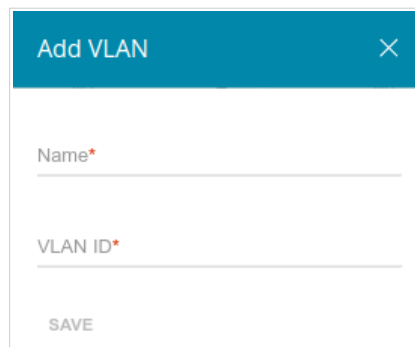
Figure 56. Adding a connection.

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

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

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

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

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

Statistics

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

- network statistics

- IP addresses leased by the DHCP server

- the routing rules and routing tables

- data on devices connected to the router's network and its web-based interface, and information on current sessions of these devices

- statistics for traffic passing through ports of the router

- addresses of active multicast groups

- statistics for IPsec 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).
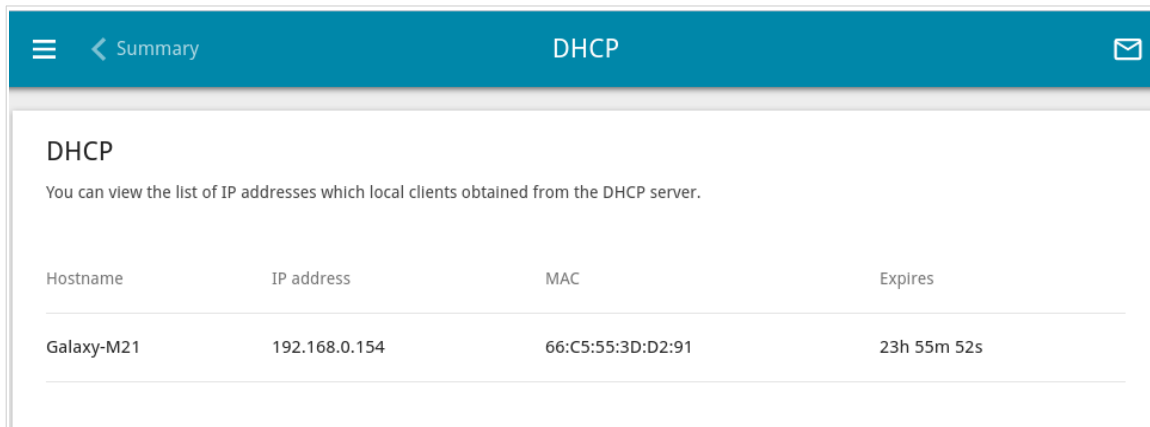
*Figure 57. The **Statistics / Network Statistics** page.*

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

DHCP

The **Statistics / DHCP** page displays the information on devices that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the router.
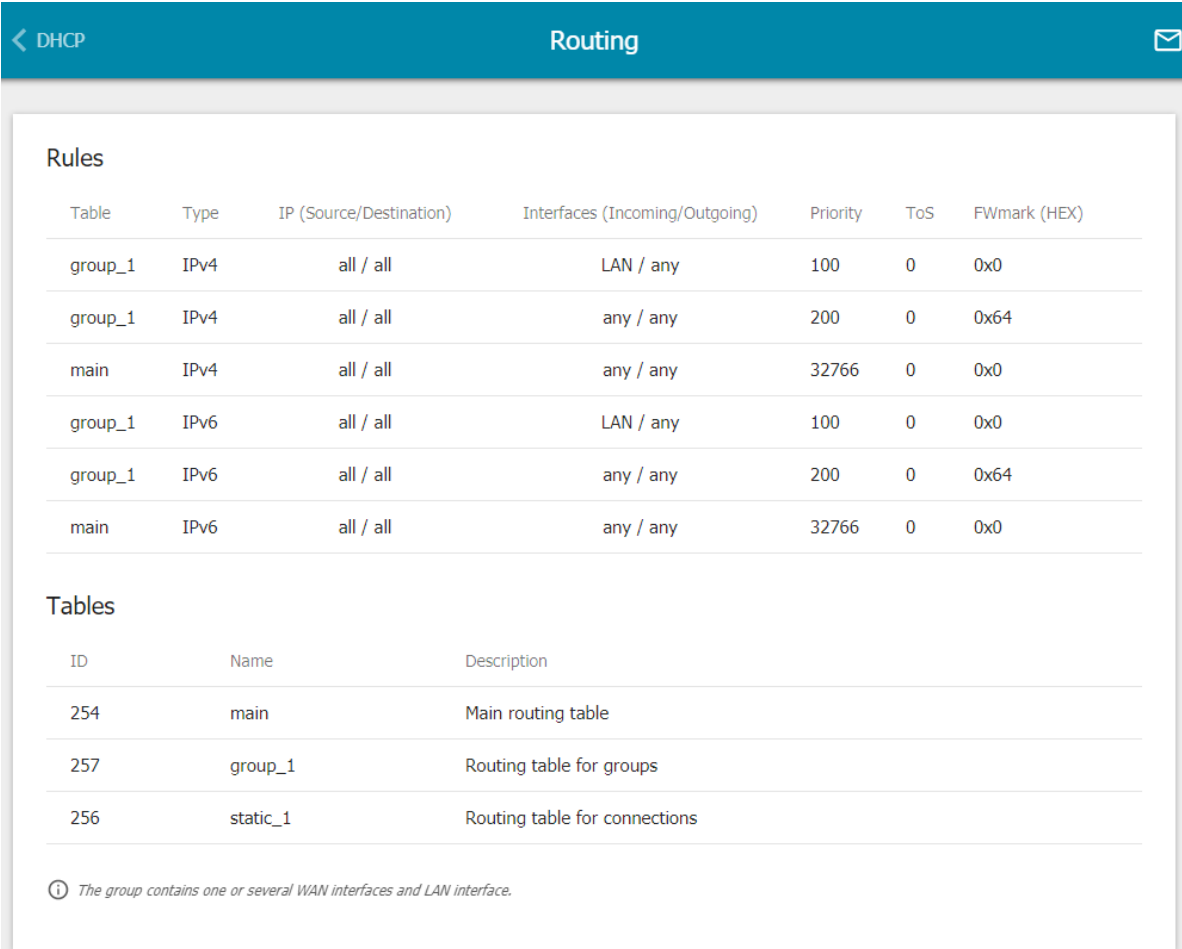
*Figure 58. The **Statistics / DHCP** page.*

Routing

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

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

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

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

Routing Table main

You can view the information on routes.
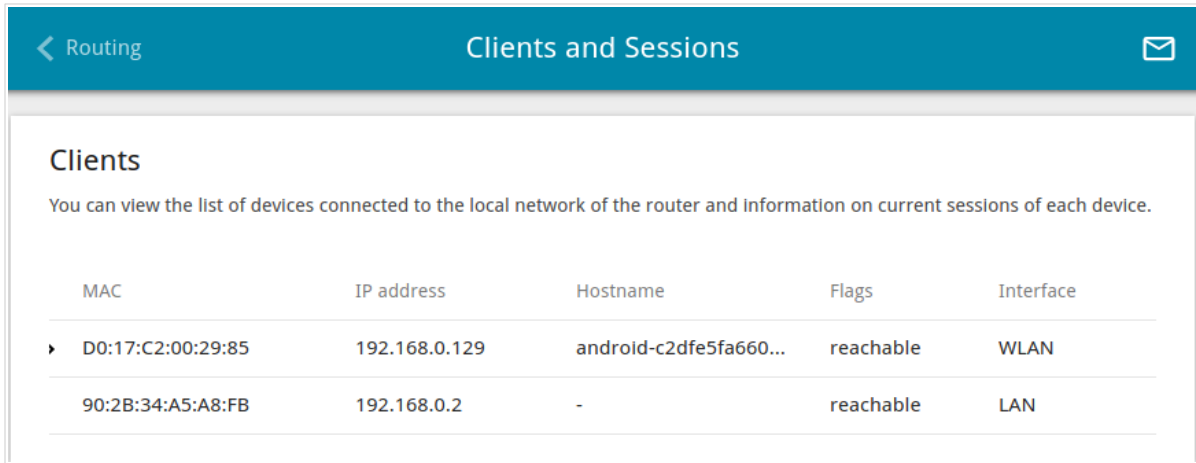
Interface	Destination	Subnet mask	Gateway	Flags	Metric	Table
WAN	0.0.0.0	0.0.0.0	192.168.161.1	UG	410	254
WAN	1.1.1.1		192.168.161.1	UGH	0	254
LAN	192.168.0.0	255.255.255.0		U	0	254
WAN	192.168.161.0	255.255.255.0		U	0	254

Figure 60. 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.
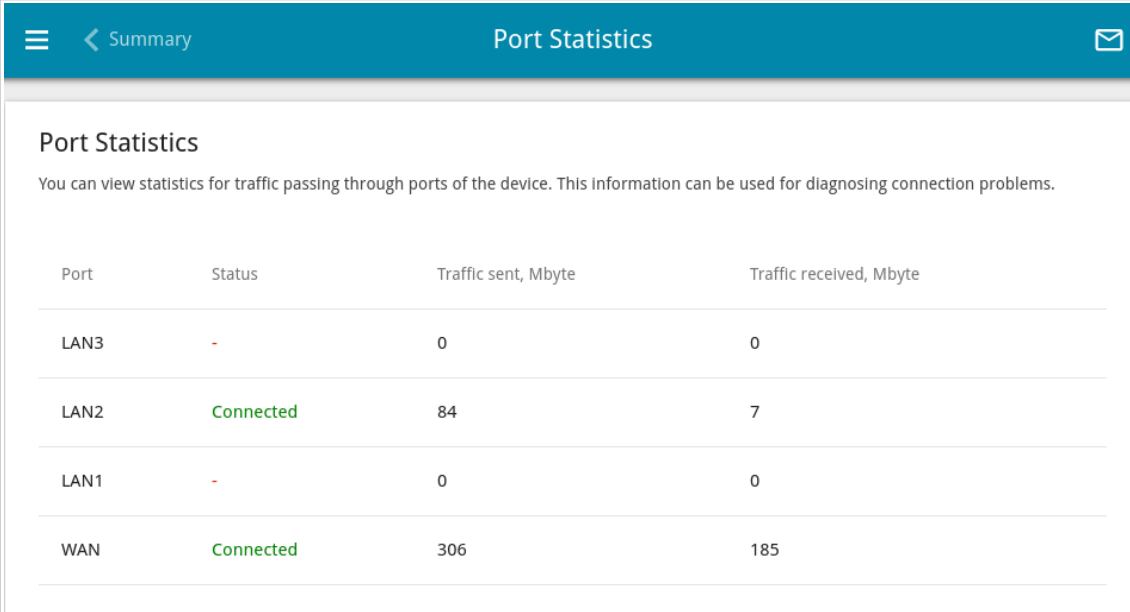
*Figure 61. The **Statistics / Clients and Sessions** page.*

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.
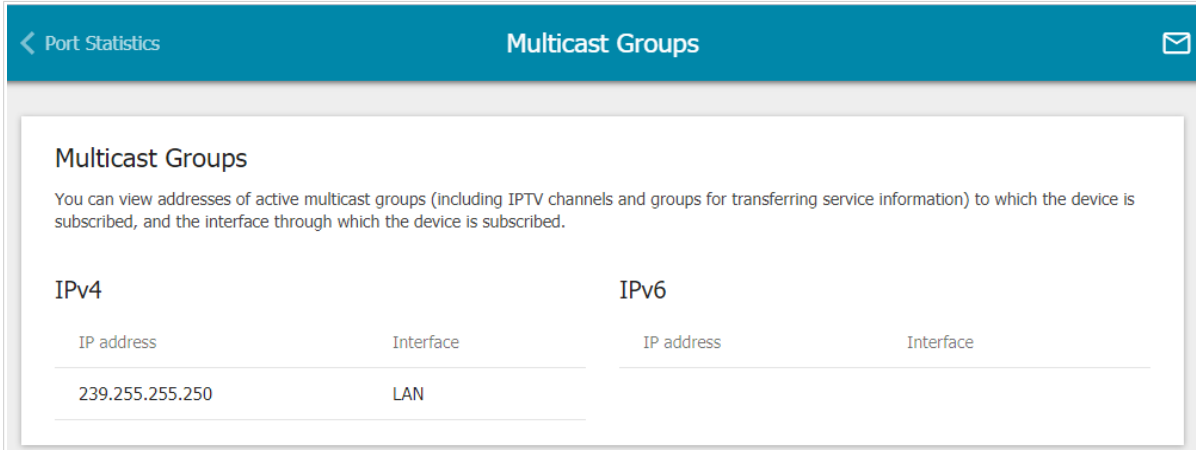
*Figure 62. The **Statistics / Port Statistics** page.*

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.
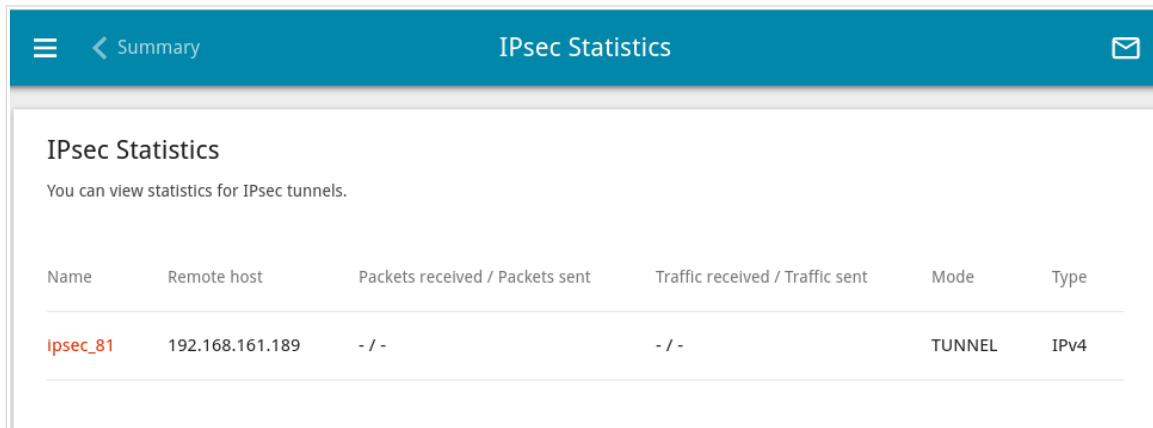
*Figure 63. The **Statistics / Multicast Groups** page.*

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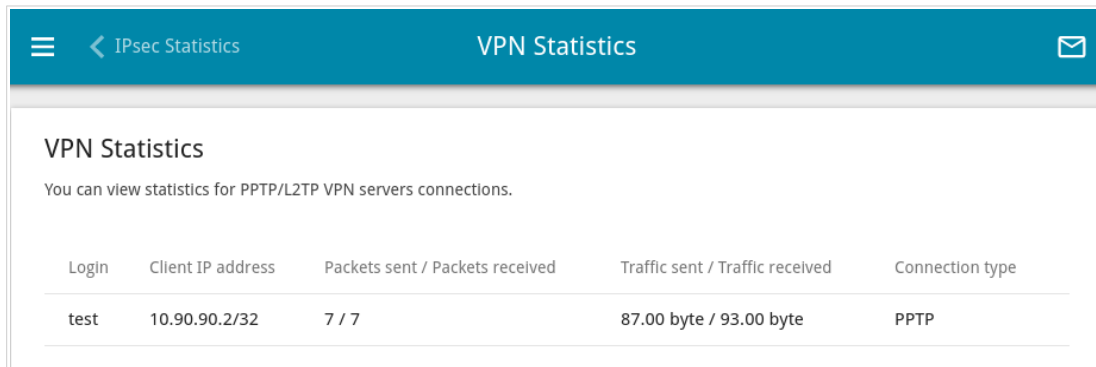
*Figure 64. The **Statistics / IPsec Statistics** page.*

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 65. 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 **INTERNET** port of the router.
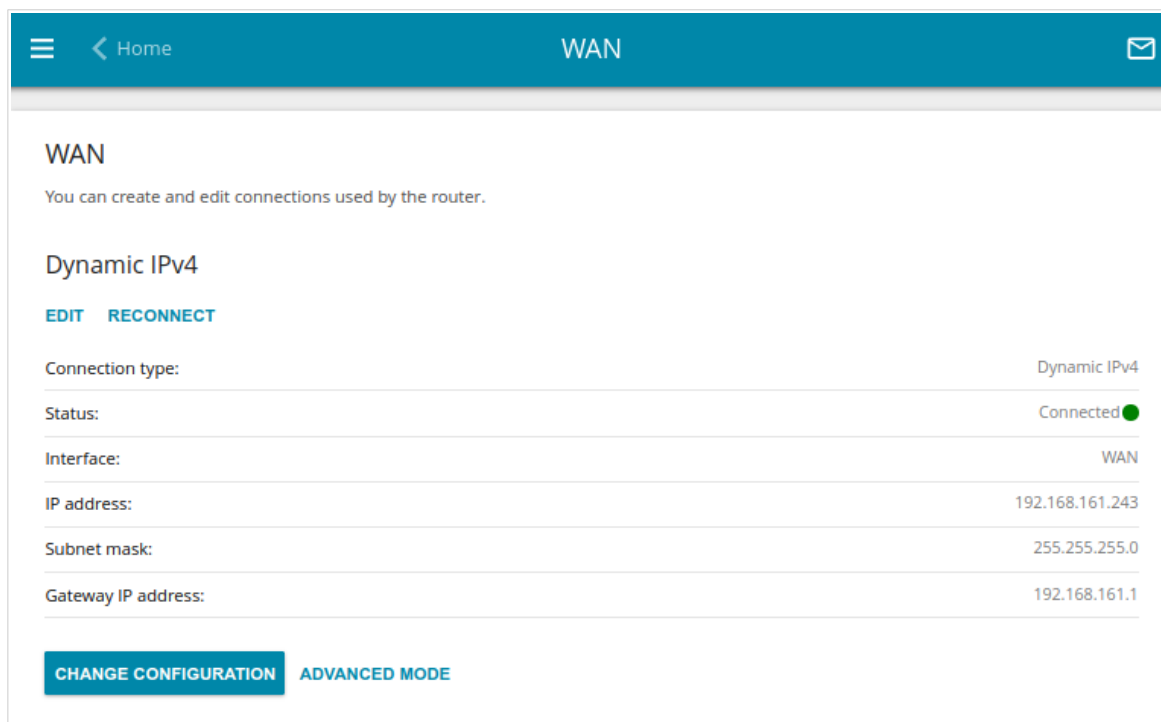
*Figure 66. The **Connections Setup / WAN** page. The simplified mode.*

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

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

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

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

> When connections of some types are created, the **Connections Setup / WAN** page is automatically displayed in the advanced mode.
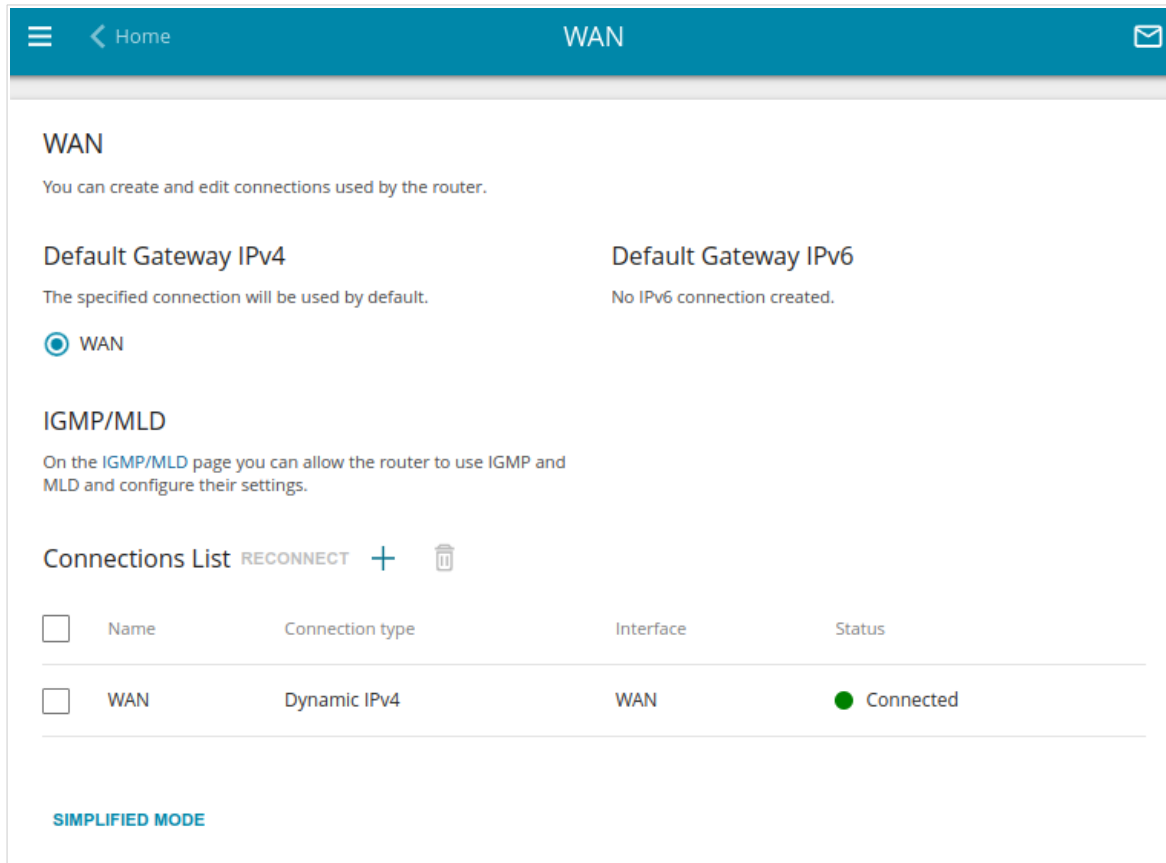
*Figure 67. The **Connections Setup / WAN** page. The advanced mode.*

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

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

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

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

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP/MLD** link (for the description of the page, see the *IGMP/MLD* section, page 218).

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 68. 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 for IPv4 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 69. 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 70. 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 71. 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.
RIPng	Move the switch to the right to allow using RIPng for this connection.

*Figure 72. 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 73. 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 74. 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 for IPv4 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 75. 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 76. 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	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the **LCP interval** and **LCP failures** fields correspondingly or leave the default 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 this PPP connection debugging. Upon that the **Debugging messages** value should be selected from the **Level** drop-down list in the settings of the corresponding event log in the **Logging** section (see the *Logging* section, page 265).

*Figure 77. 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, L2TP Dual Stack, 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 78. 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 for IPv4 is enabled. Do not disable the function unless your ISP requires this.
NATv6	*For the **L2TP Dual Stack** type only.* 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	*For the **PPTP**, **L2TP**, and **L2TP Dual Stack** 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.

Parameter	Description
RIP	*For the **PPTP** and **L2TP** types only.* Move the switch to the right to allow using RIP for this connection.

*Figure 79. 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 address or full domain name of the PPTP or L2TP authentication server.

Parameter	Description
MTU	The maximum size of units transmitted by the interface.
Encryption protocol	Select a method of MPPE encryption. • **No encryption**: MPPE encryption is not applied. • **MPPE 40 128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied. • **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied. • **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the **MS-CHAP**, **MS-CHAPv2**, or **AUTO** value is selected from the **Authentication protocol** drop-down list.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the **LCP interval** and **LCP failures** fields correspondingly or leave the default values.
Dial on demand	*For the **PPTP**, **L2TP**, and **L2TP over IPsec** types only.* 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 this PPP connection debugging. Upon that the **Debugging messages** value should be selected from the **Level** drop-down list in the settings of the corresponding event log in the **Logging** section (see the *Logging* section, page 265).

*Figure 80. 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 81. The page for creating a new **L2TP Dual Stack** connection. The **IPv6** section.*

Parameter	Description
IPv6 *(for the **L2TP Dual Stack** type)*	
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.

*Figure 82. The page for creating a new **L2TP over IPsec** connection. The **IPsec** section.*

! The value of the **Pre-shared key** field and the value selected from the **IKE version** list should be the same for both parties of the tunnel.

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 DIR-X1860.
DPD action	Using DPD protocol (*Dead Peer Detection*) allows to check the status of the remote host in the tunnel: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD requests to the remote host. Select the needed action from the drop-down list. • **Restart**: Restart the tunnel connection immediately. • **Hold**: Reestablish the connection upon request when the traffic matching the tunnel appears. • **Clear**: Close the tunnel connection with no further action. • **Off**: Disable DPD. When this value is selected, 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.
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.

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, and on the **IPsec Statistics** page 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 83. 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.
RIPng	Move the switch to the right to allow using RIPng for this connection.

Figure 84. 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 85. 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	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the **LCP interval** and **LCP failures** fields correspondingly or leave the default 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 this PPP connection debugging. Upon that the **Debugging messages** value should be selected from the **Level** drop-down list in the settings of the corresponding event log in the **Logging** section (see the *Logging* section, page 265).

*Figure 86. 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.
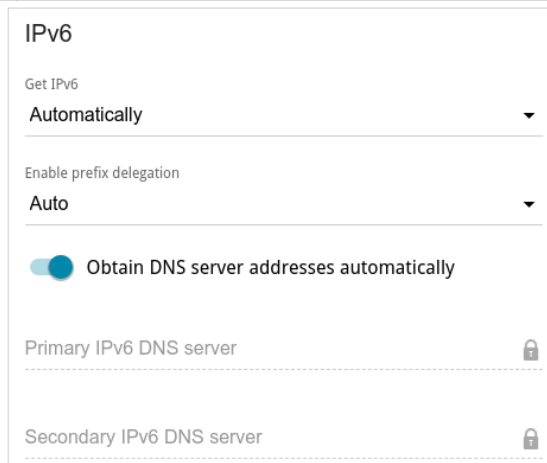
*Figure 87. The page for creating a new **PPPoE IPv6** connection. The **IPv6** section.*

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 6in4 WAN Connection

> **!** Before configuring the connection, please first register on a tunnel broker's web site.

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 88. The page for creating a new **6in4** connection.*

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.
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.
RIPng	Move the switch to the right to allow using RIPng for this connection.
Remote host	Enter the IPv4 address of the server provided by the tunnel broker.
Client IPv6 address	Enter the IPv6 address of the router provided by the tunnel broker (without specifying the prefix length).
Server IPv6 address	Enter the IPv6 address of the server provided by the tunnel broker (without specifying the prefix length).

Parameter	Description
Routed IPv6 network	Enter the address of the routed IPv6 subnet (without specifying the prefix length) provided by the tunnel broker.
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically. Move the switch to the left to specify this parameter manually. Upon that the **MTU** field is displayed.
MTU	The maximum size of units transmitted by the interface.

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

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

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 server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

Creating 6to4 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 89. The page for creating a new **6to4** connection.*

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.
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.
6to4 Relay Router	The IPv4 address of the gateway which is used to transfer IPv6 packets.
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically. Move the switch to the left to specify this parameter manually. Upon that the **MTU** field is displayed.
MTU	The maximum size of units transmitted by the interface.

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

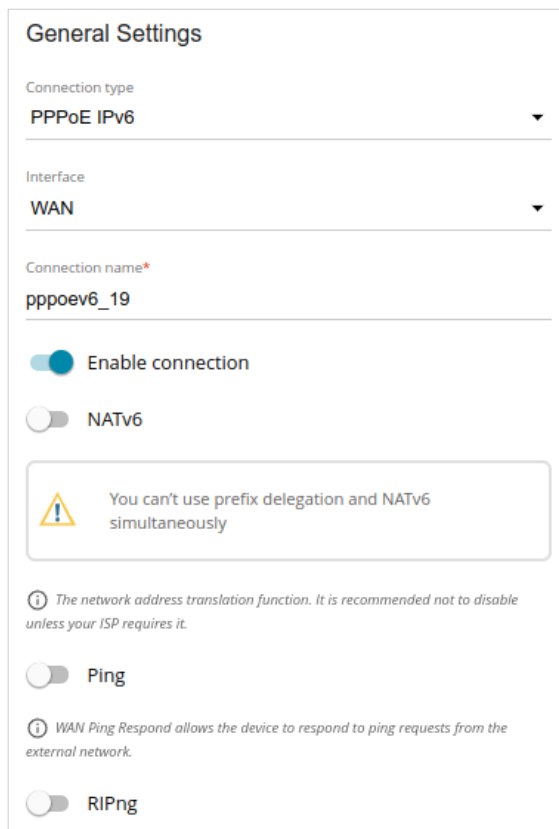After clicking the button, the window for additional configuration of the connection opens.

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 server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

Creating 6rd 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 90. The page for creating a new **6rd** connection.*

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.
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.
Obtain 6rd settings automatically	Move the switch to the right to let the router obtain 6rd domain settings automatically from the LAN DHCP server or from a delegating router. Upon that the **6rd Border Relay**, **6rd IPv6 prefix**, **6rd IPv6 prefix length**, and **IPv4 mask length** fields are not available for editing.
6rd Border Relay	Enter the IPv4 address of the router provided by your ISP for the 6rd domain.
6rd IPv6 prefix	The IPv6 prefix for the 6rd domain provided by your ISP.
6rd IPv6 prefix length	The IPv6 prefix length for the 6rd domain (in bits) allocated by your ISP. By default, the value **32** is specified.

Parameter	Description
IPv4 mask length	The number of bits in the IPv4 address of the router in the 6rd domain.
Hub and spoke	Move the switch to the right to exchange traffic between clients through the main host of the network in the 6rd domain.
	Move the switch to the left to exchange traffic between clients without the main host of the network.
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically.
	Move the switch to the left to specify this parameter manually. Upon that the **MTU** field is displayed.
MTU	The maximum size of units transmitted by the interface.

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

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

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 server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

LAN

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

IPv4

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

```
Local IP Address

IP address*
192.168.0.1

Mask*
255.255.255.0

Hostname
dlinkrouter.local

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

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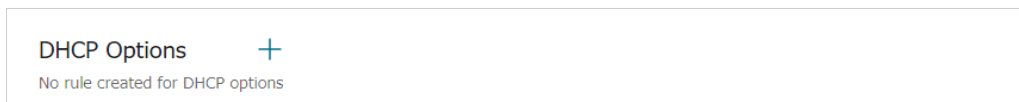
*Figure 93. Configuring the local interface. The **IPv4** tab. The section for configuring DHCP options.*

To do this, click the **ADD** button (＋).
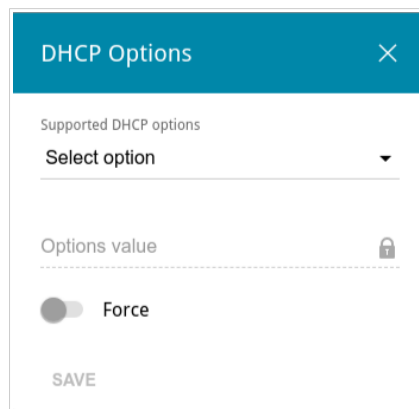
*Figure 94. Configuring the local interface. The **IPv4** tab. The window for configuring a DHCP option.*

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

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

After specifying the needed parameters, click the **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).
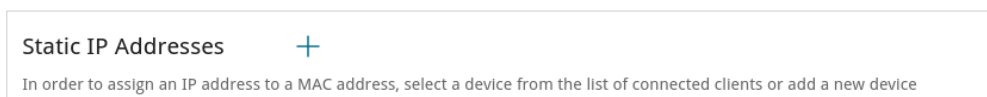
*Figure 95. Configuring the local interface. The **IPv4** tab. The section for creating MAC-IPv4 pairs.*

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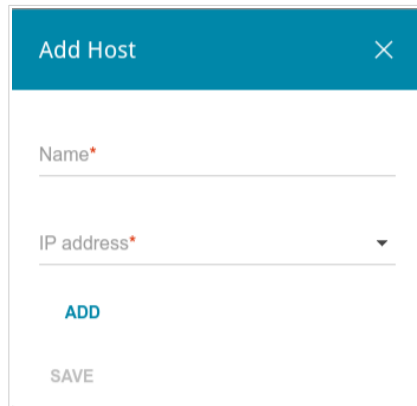
*Figure 96. Configuring the local interface. The **IPv4** tab. The window for adding a DNS record.*

In the **Name** field, specify the hostname or full 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** *or* **Repeater** *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** *or* **Repeater** *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** or **WISP Repeater** 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.
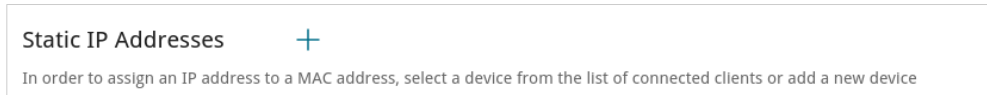
Figure 99. Configuring the local interface. The IPv6 tab. The section for creating MAC-IPv6 pairs.

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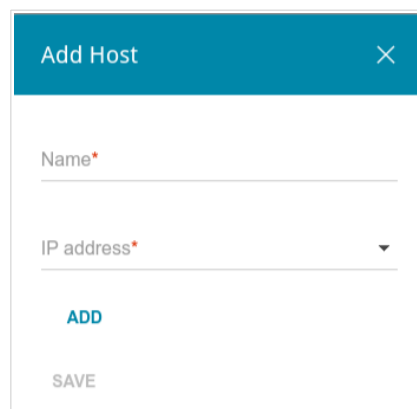
Figure 100. Configuring the local interface. The IPv6 tab. The window for adding a DNS record.

In the **Name** field, specify the hostname or full 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.
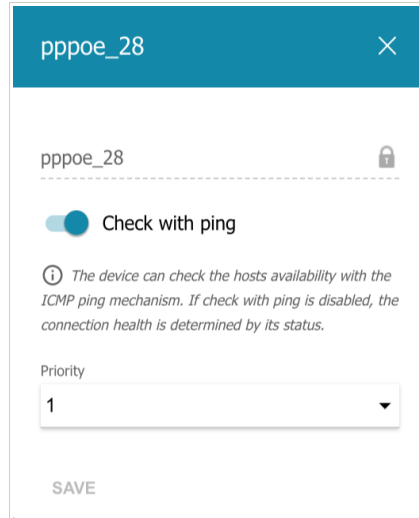
Figure 102. The window for changing the priority of a connection.

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 ping requests** fields values. After a successful check the router keeps using the main connection. If the check fails, the router repeats it. After two failed checks the next operational connection from the list will be used as the default connection.
Waiting for response	A time period (in seconds) allocated for a response to one ping request.
Number of ping requests	The number of ping requests sent for each check. A check is considered failed in case none of the sent ping requests receive a response.
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.

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).
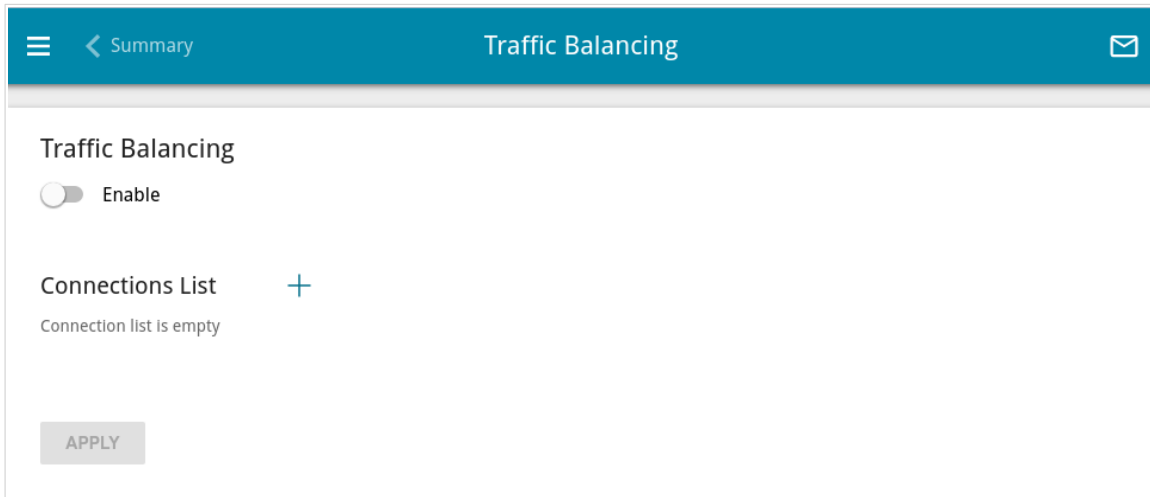
*Figure 103. The **Connections Setup / Traffic Balancing** page.*

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.
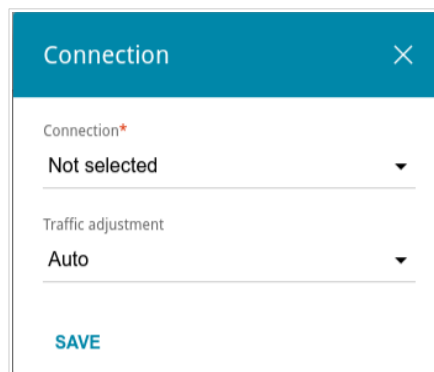
Figure 104. The window for adding a new connection to the page.

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/IPIP/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.
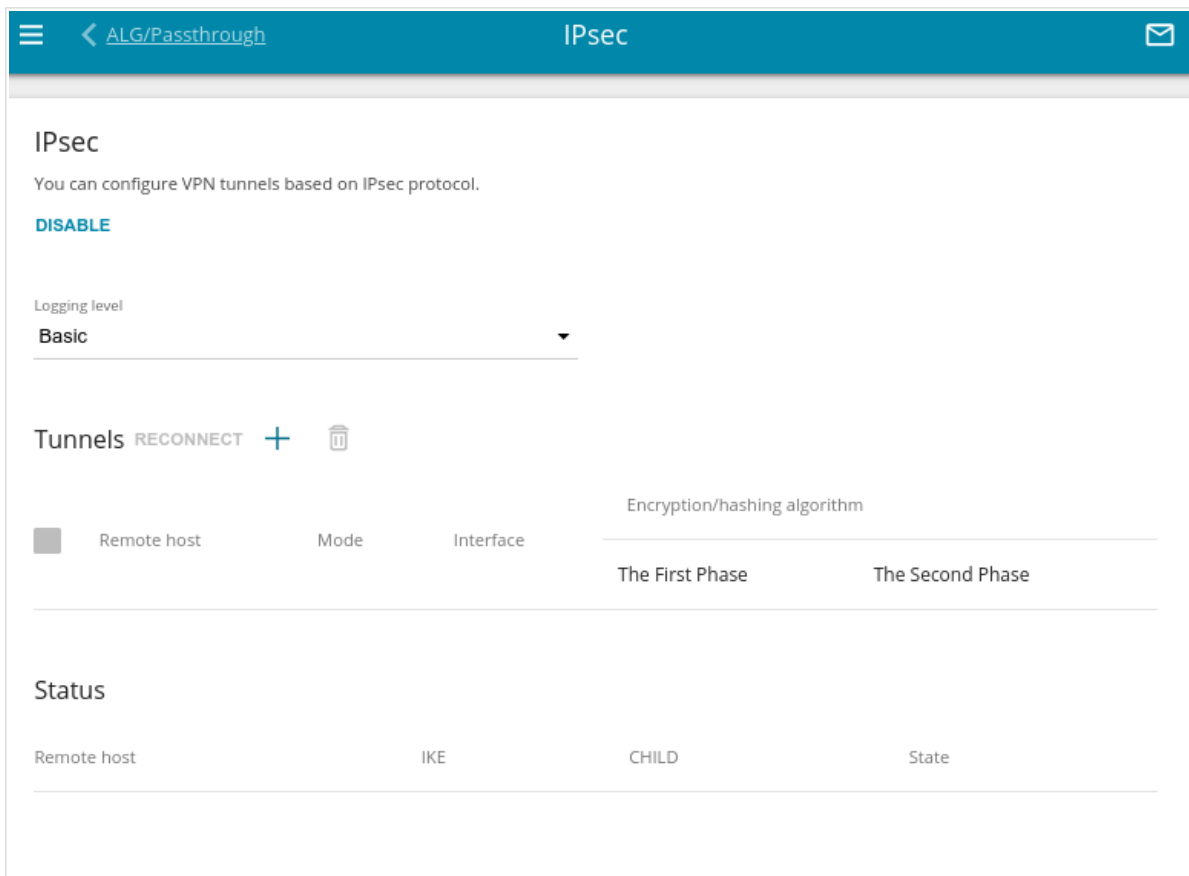
*Figure 105. The **VPN / IPsec** page.*

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 / Logging / Local** page (see the *Local* section, page 265).

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

> ! The values selected from the **IP version**, **Mode**, **IKE version** lists and the values of the **Pre-shared key** field and elements in the **The First Phase** and **The Second Phase** sections should be the same for both parties of the tunnel.
>
> The values of the remote settings for one party of the tunnel should be the same as the values of the local settings for the other party of the tunnel.
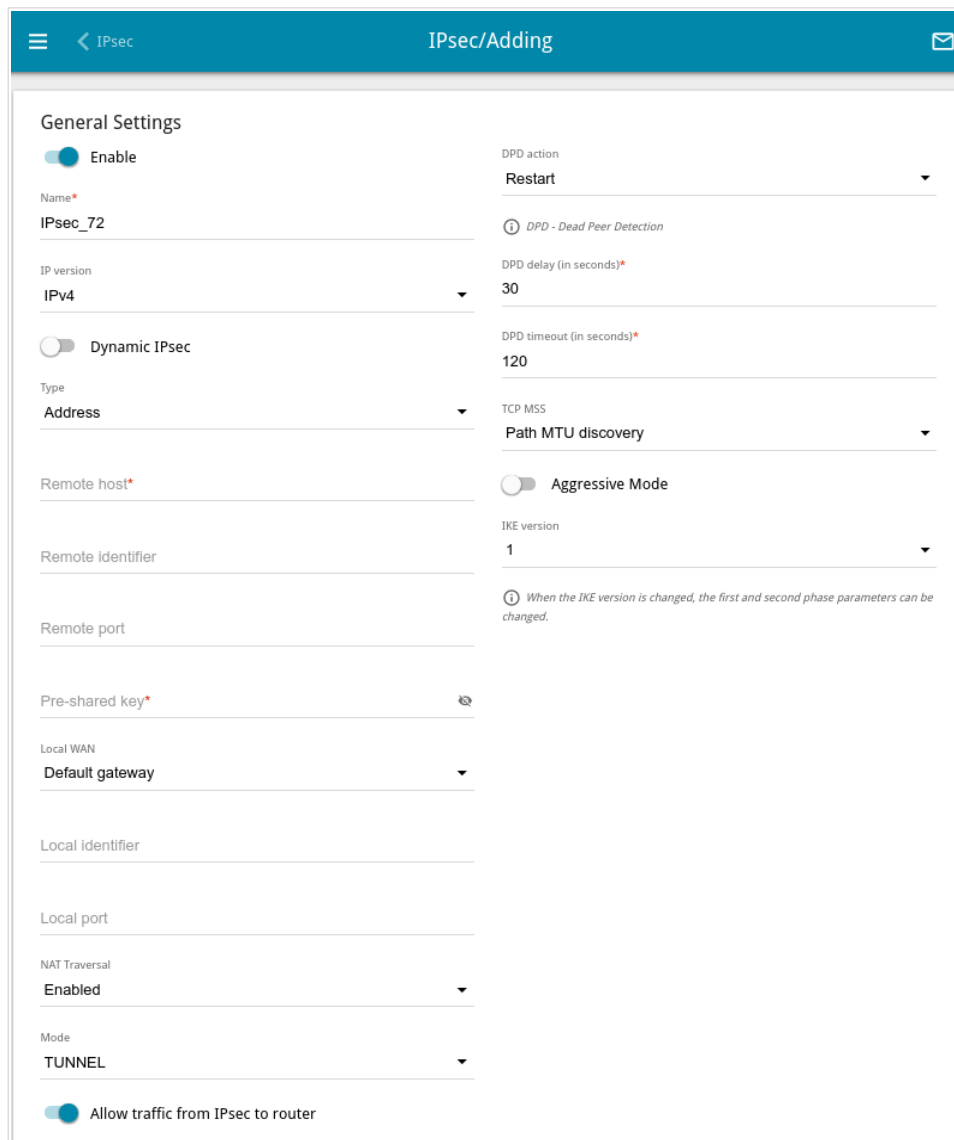
*Figure 106. The page for adding an IPsec tunnel. The **General Settings** section.*

In 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.
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. 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 at the same time 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.
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.

Parameter	Description
Local identifier	A local identifier of the router to establish connection over IPsec with particular hosts only. 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 at the same time 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. DIR-X1860 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
DPD action	Using DPD protocol (*Dead Peer Detection*) allows to check the status of the remote host in the tunnel: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD requests to the remote host. Select the needed action from the drop-down list. • **Restart**: Restart the tunnel connection immediately. • **Hold**: Reestablish the connection upon request when the traffic matching the tunnel appears. • **Clear**: Close the tunnel connection with no further action. • **Off**: Disable DPD. When this value is selected, 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.
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. The switch is displayed when the **1** value is selected from the **IKE version** drop-down list.
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.

To specify encryption algorithms for the first and second phases of the IPsec tunnel, click the **ADD** button (+) in the **The First Phase** and **The Second Phase** sections correspondingly. You can specify several combinations of encryption algorithms for each phase of the IPsec tunnel. In the opened window, you can specify the following parameters:
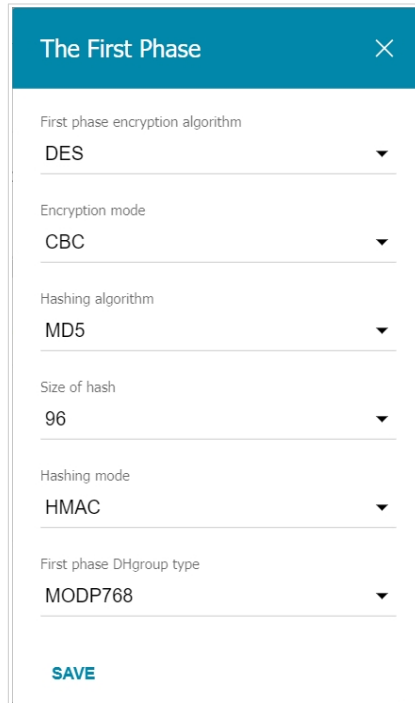
Figure 107. The window for configuring the first phase of the IPsec tunnel. ***The First Phase*** *section.*

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.
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.

Parameter	Description
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.
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.
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 DIR-X1860.

Click the **SAVE** button.

To edit the parameters for each phase of the IPsec tunnel, in the relevant section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

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

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

Figure 108. 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 **General Settings** 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 **General Settings** 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.
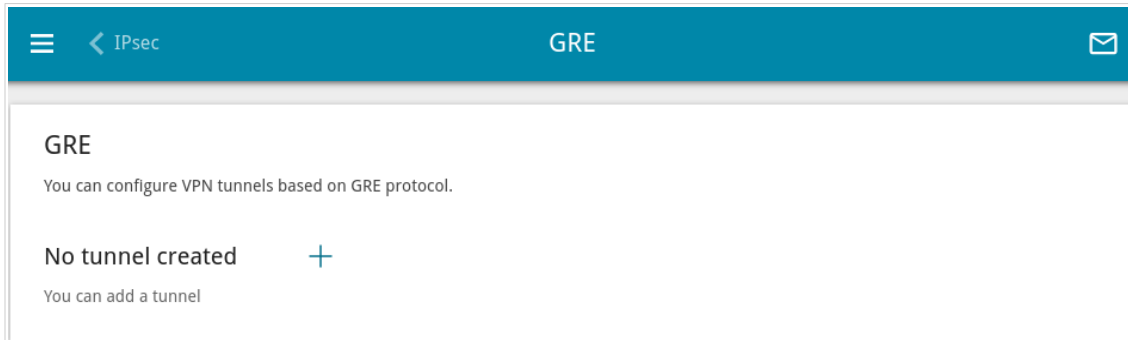
*Figure 109. The **VPN / GRE** page.*

To create a new tunnel, click the **ADD** button (+).
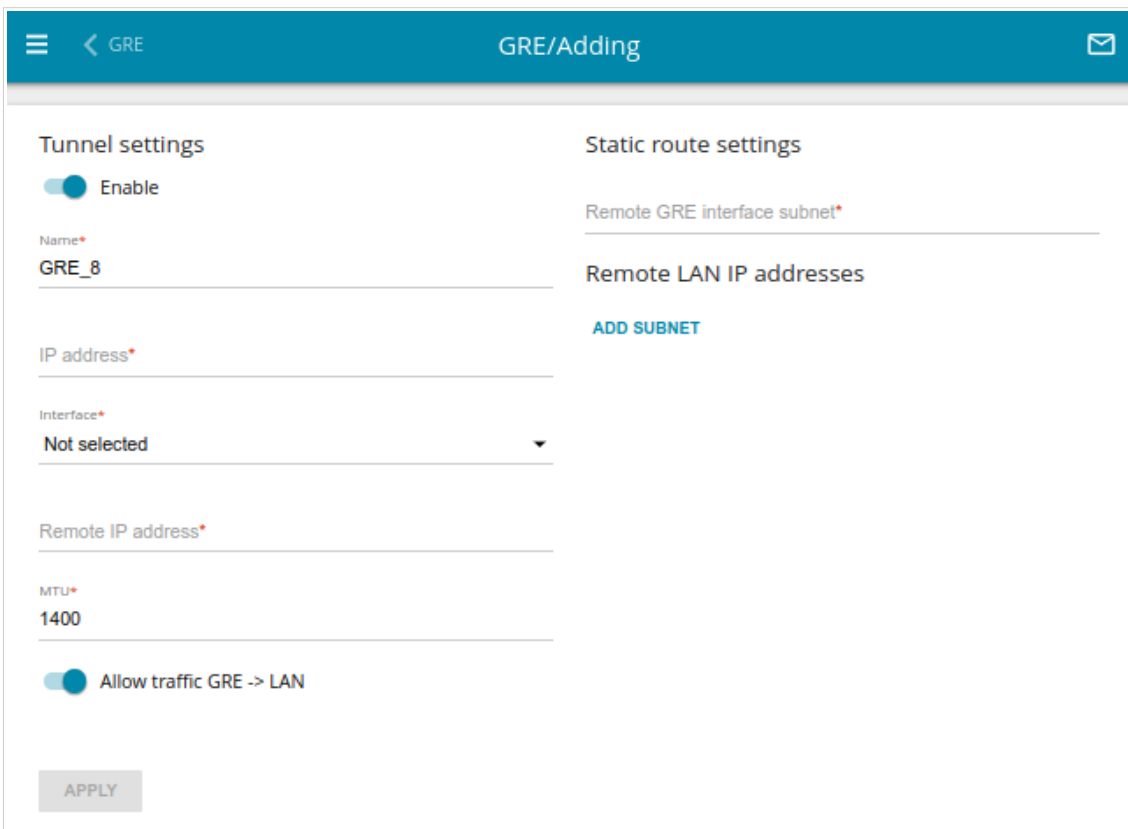
Figure 110. The page for adding a GRE tunnel.

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 with 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 address	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 GRE interface subnet	The subnet and mask of the remote GRE interface.
Remote LAN IP addresses	
Remote subnet	To specify the IP address and mask of the remote local subnet, click the **ADD SUBNET** button, and in the line displayed, enter the needed value. To remove a subnet, click the **Delete** icon (×) in the corresponding line.

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 (🗑).

IPIP

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

IPIP (*IP Encapsulation within IP*) is a protocol for IP-tunneling network packets, which enables you to create unprotected VPN tunnels, encapsulating IP packets within other IP packets.
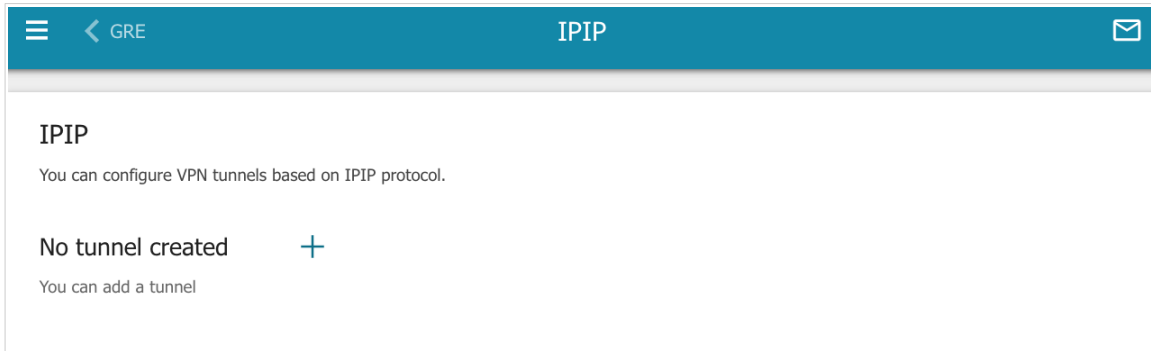
*Figure 111. The **VPN / IPIP** page.*

To create a new tunnel, click the **ADD** button ( ).
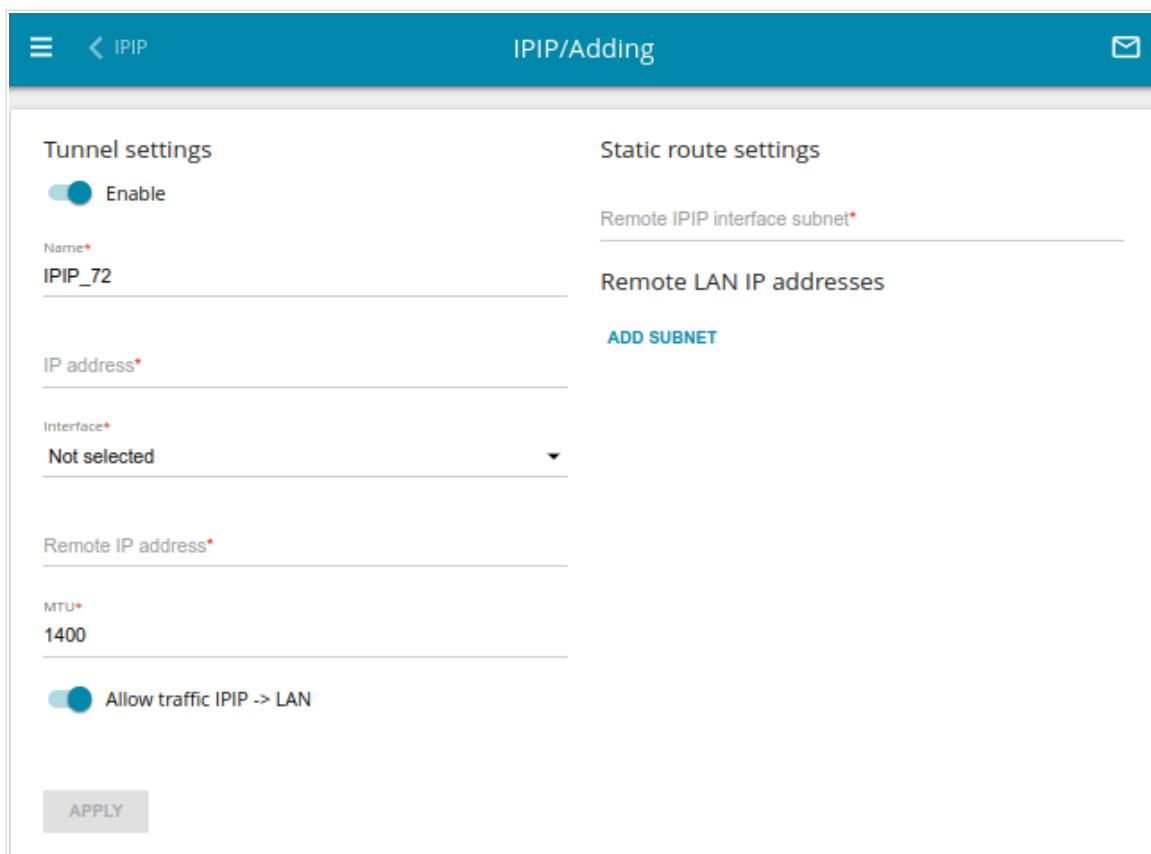
Figure 112. The page for adding an IPIP tunnel.

You can specify the following parameters:

Parameter	Description
Tunnel settings	
Enable	Move the switch to the right to enable the IPIP tunnel. Move the switch to the left to disable the IPIP tunnel.
Name	A name of the tunnel for easier identification. You can specify any name.
IP address	The IP address of the IPIP tunnel interface with 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 address	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 IPIP → LAN	Move the switch to the right to allow IPIP tunnel users access devices in the remote local subnet.
Static route settings	
Remote IPIP interface subnet	The subnet and mask of the remote IPIP interface.
Remote LAN IP addresses	
Remote subnet	To specify the IP address and mask of the remote local subnet, click the **ADD SUBNET** button, and in the line displayed, enter the needed value. To remove a subnet, click the **Delete** icon (✕) in the corresponding line.

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 create PPTP or L2TP VPN servers. To configure a 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.
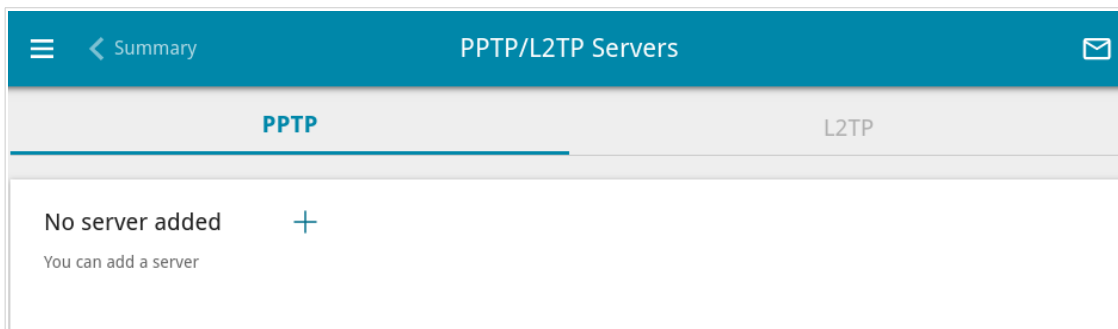
*Figure 113. The **VPN / PPTP/L2TP Servers** page.*

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

> ❗ Before creating a PPTP or L2TP server with authentication enabled, it is required to create user accounts (see the *VPN Users* section, page 150).
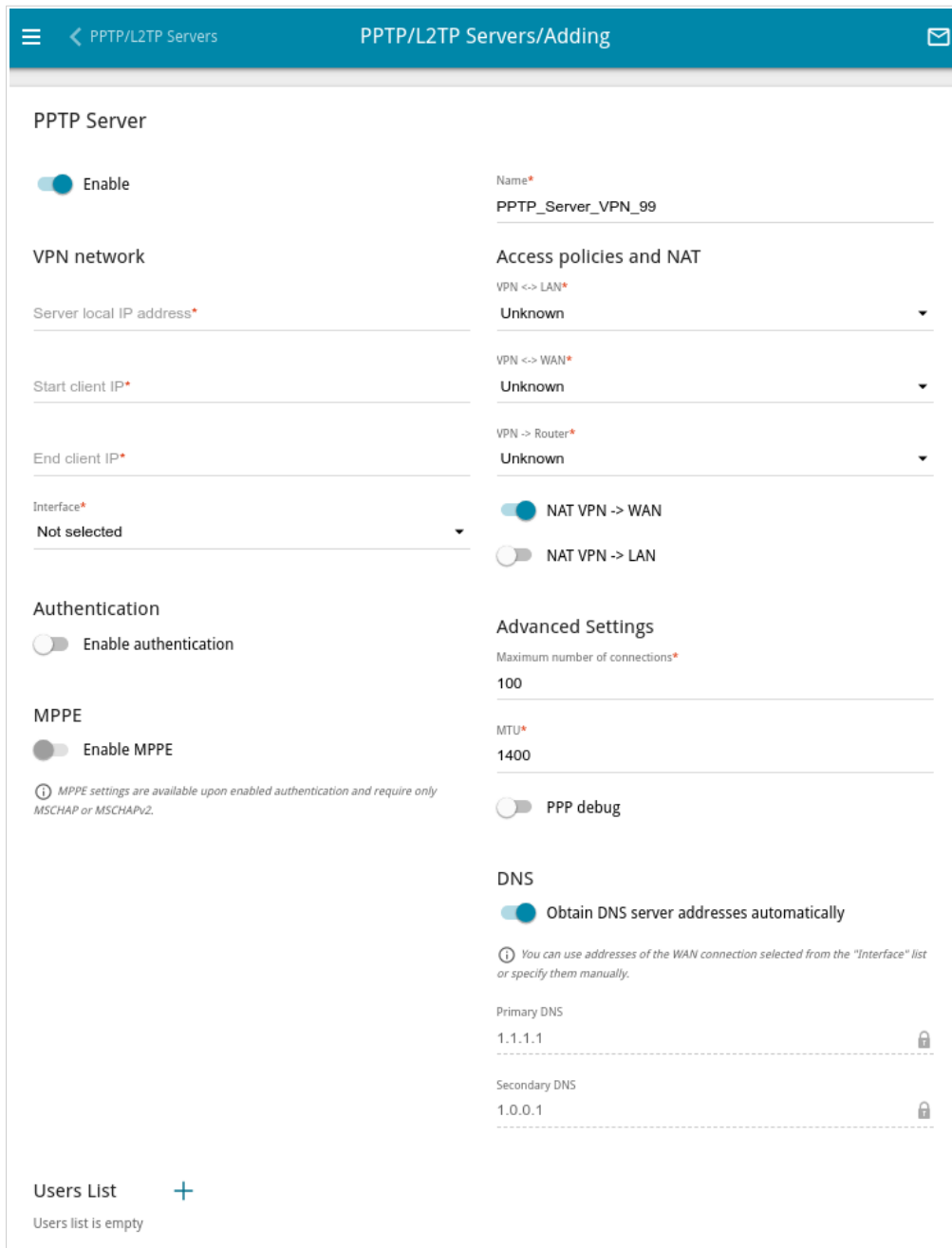
Figure 114. The page for adding a PPTP server.

You can specify the following parameters:

Parameter	Description
PPTP Server / L2TP Server	
Enable	Move the switch to the right to enable the server. Move the switch to the left to disable the server.
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 for a PPTP server.* The maximum number of devices allowed to connect to the PPTP server.
Port	*Available for an L2TP server.* The port of L2TP server. By default, the value `1701` is specified.
MTU	The maximum size of units transmitted by the interface.
PPP debug	Move the switch to the right if you want to log all data on this VPN server debugging. Upon that the **Debugging messages** value should be selected from the **Level** drop-down list in the settings of the corresponding event log in the **Logging** section (see the *Logging* section, page 265).
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.
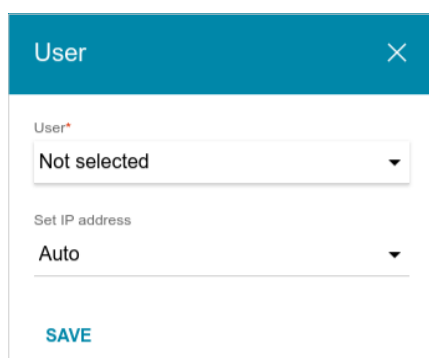
Figure 115. A window for adding a user.

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

Parameter	Description
User	Select a user account to allow access.

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

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

VPN Users

On the **VPN / VPN Users** page, you can create user accounts to provide authorized access to a PPTP or L2TP server.
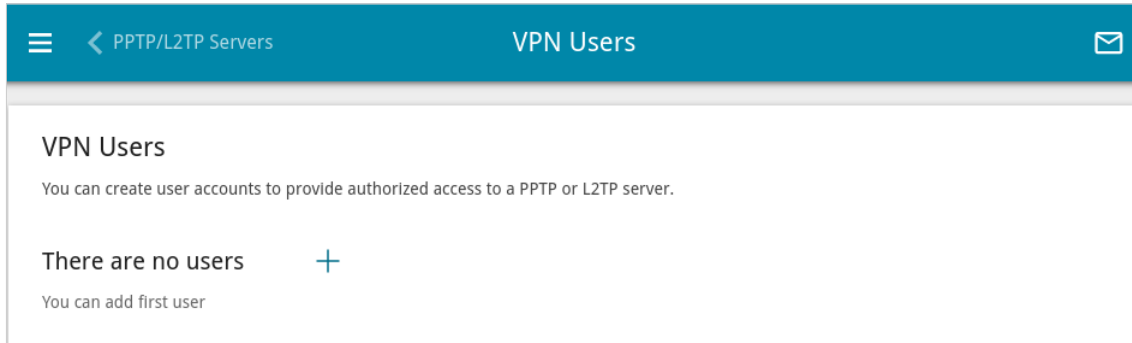
*Figure 116. The **VPN / VPN Users** page.*

To create a new user account, click the **ADD** button (+).
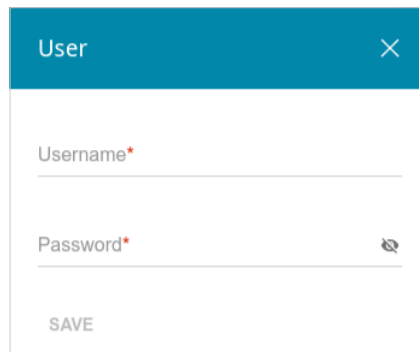
Figure 117. The window for adding a user.

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.[5] 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 ( ).

---

5   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 frames with the help of GRE protocol and transferring them over a network which uses a network protocol of another level.
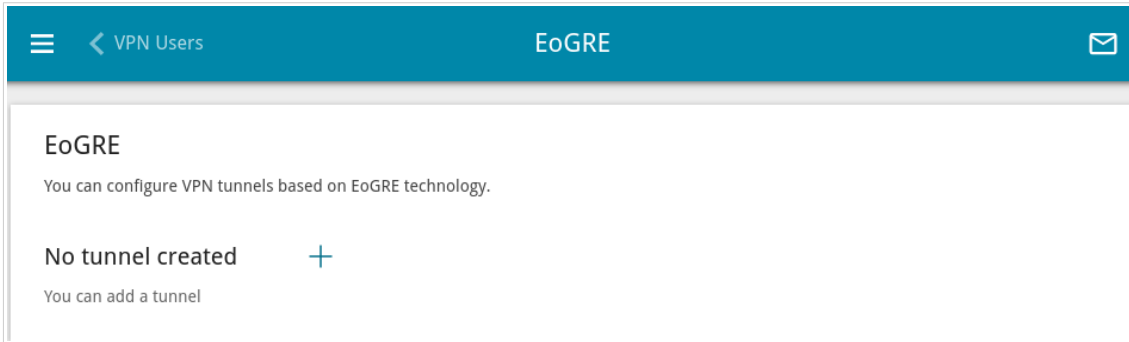
*Figure 118. The **VPN / EoGRE** page.*

To create a new tunnel, click the **ADD** button (+).
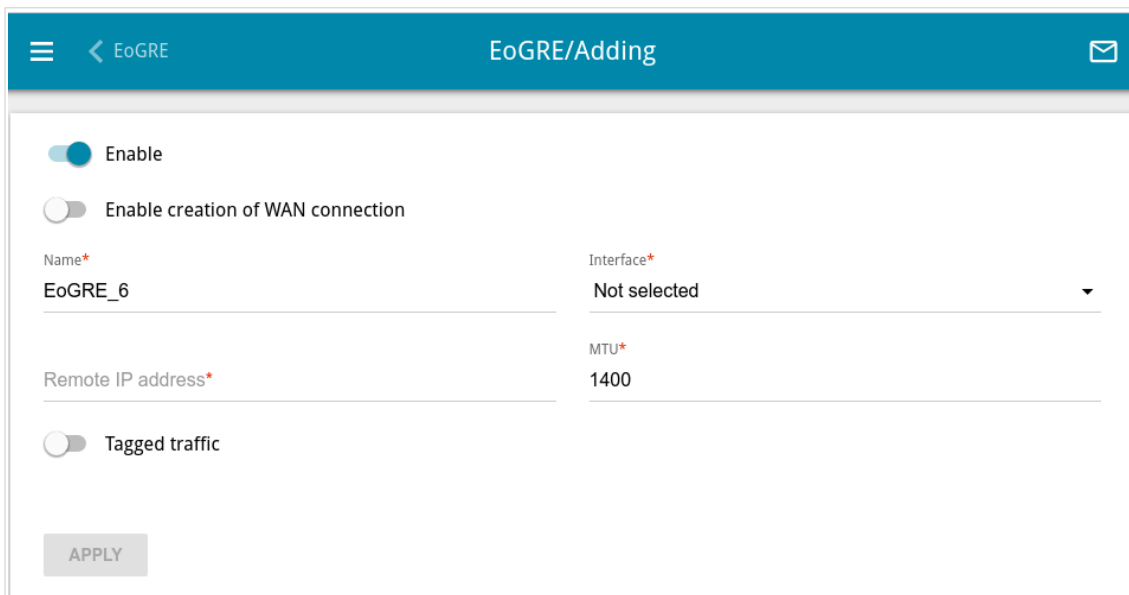
Figure 119. The page for adding an EoGRE tunnel.

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 192), and then create a WAN connection which will be assigned to the interface of this VLAN (see the *WAN* section, page 84). 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	The IP address of the remote local subnet.
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).
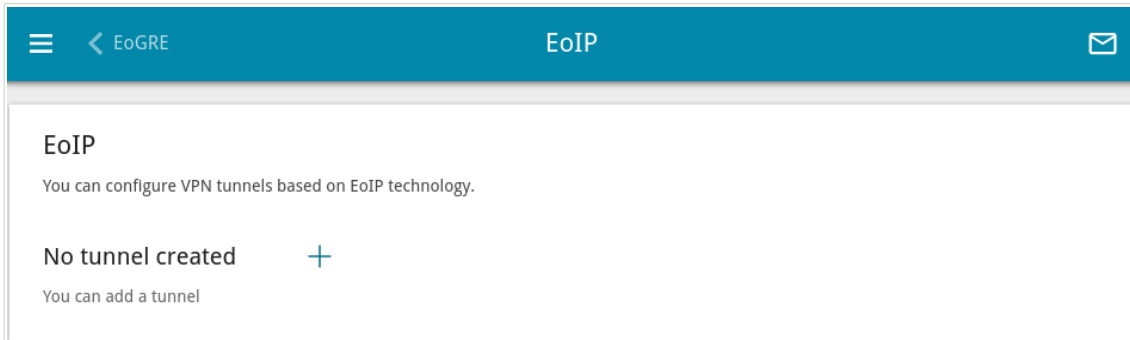
*Figure 120. The **VPN / EoIP** page.*

To create a new tunnel, click the **ADD** button (+).
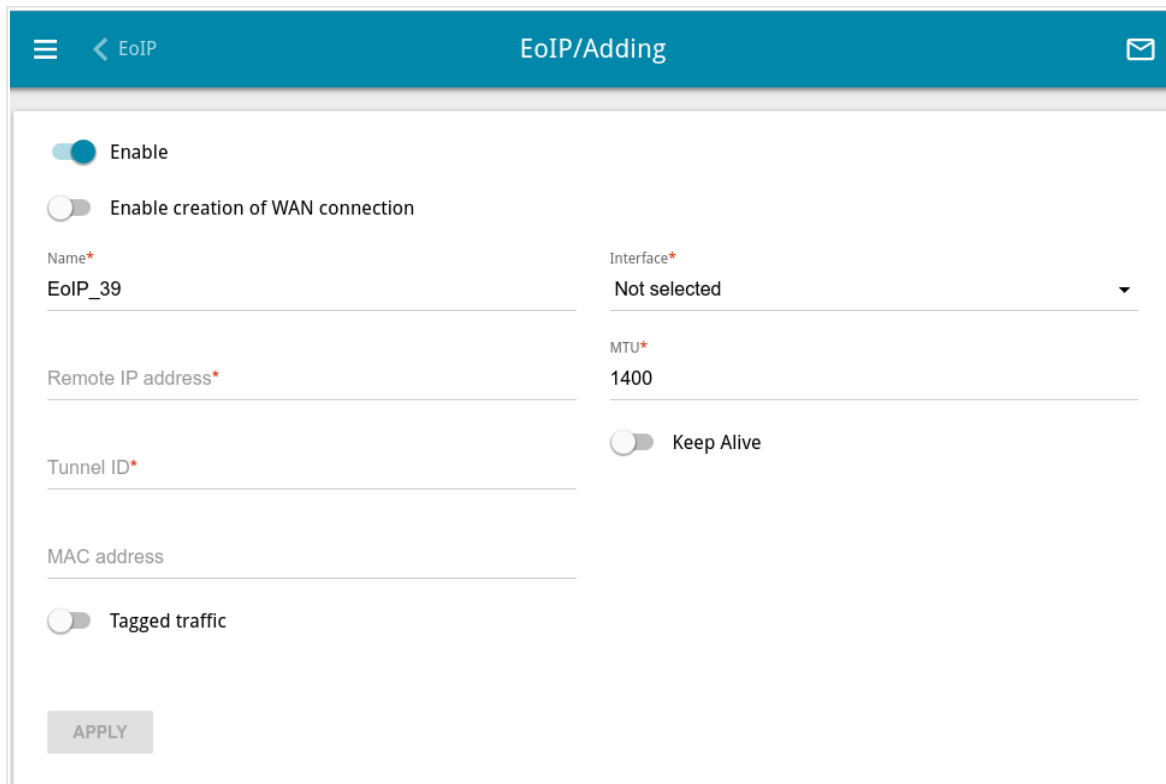
Figure 121. The page for adding an EoIP tunnel.

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 192), and then create a WAN connection which will be assigned to the interface of this VLAN (see the *WAN* section, page 84). 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 local subnet.
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. To configure the wireless network in which the wireless client automatically chooses the preferred band when it is connecting or when the network conditions change, use the Band Steering technology.
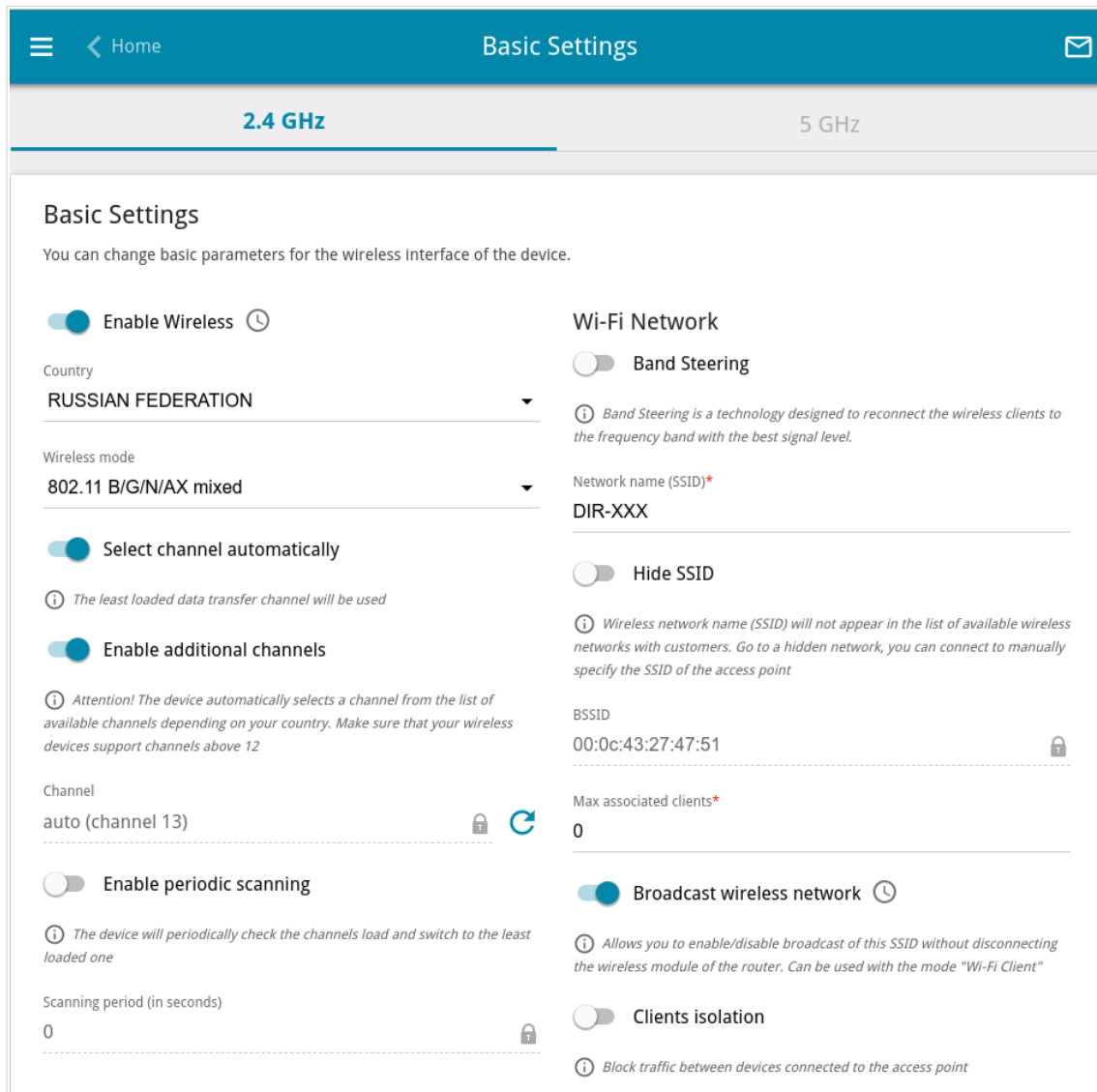
Figure 122. Basic settings of the wireless LAN in the 2.4GHz band.

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 261) 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.
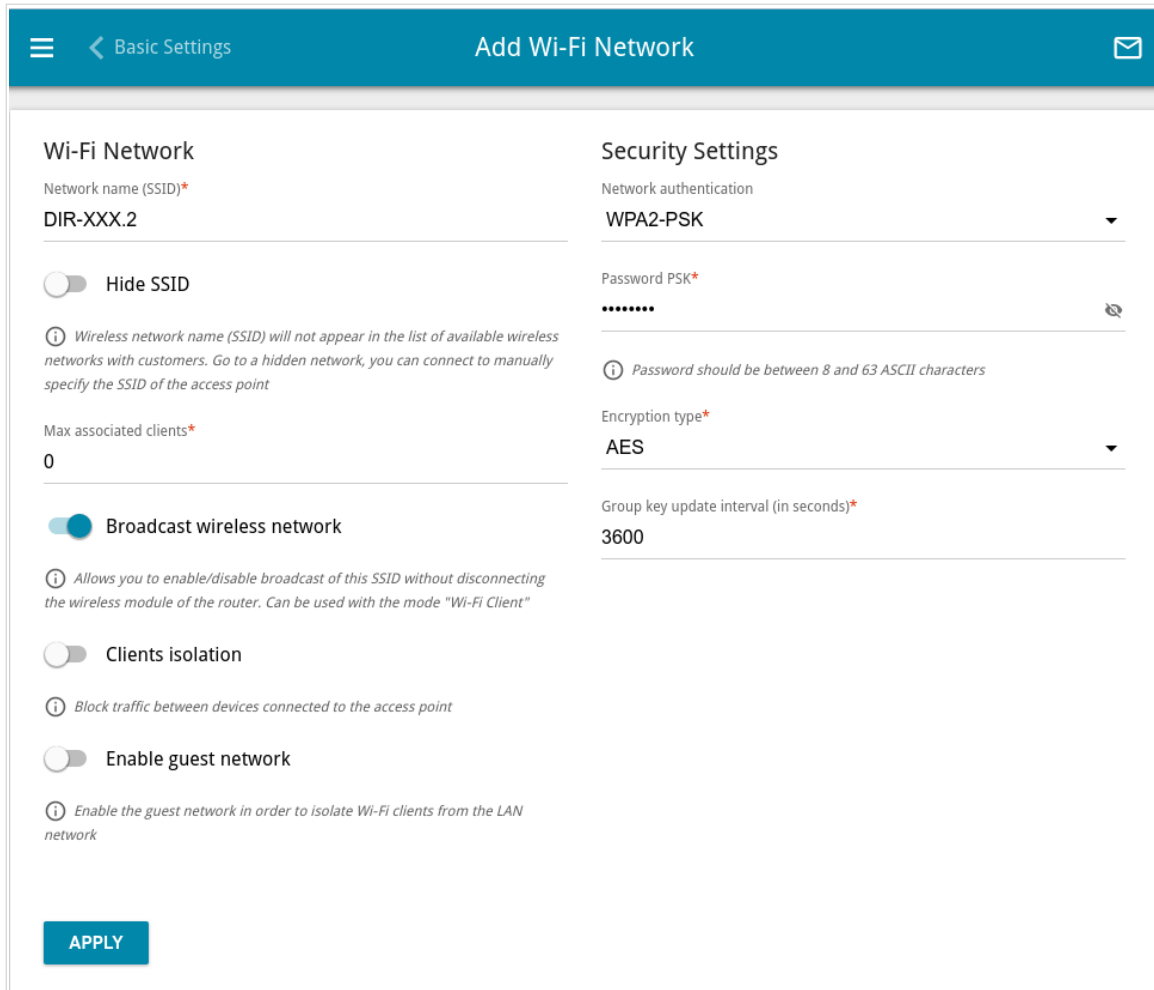
Figure 123. Creating a wireless network.

Parameter	Description
Wi-Fi Network	
Band Steering	The Band Steering technology allows wireless clients to choose the frequency band with the best signal strength. Move the switch to the right and specify the band for connecting and reconnecting wireless clients from the **Preferred band** drop-down list: **2.4 GHz**: A client chooses the 2.4 GHz band at good signal strength; **5 GHz**: A client chooses the 5 GHz band at good signal strength and remains in it longer when the signal degrades. When using the Band Steering technology in one of the bands, the same settings will be configured for the wireless network in the other band. *Available only for the basic wireless network.*

Parameter	Description
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.
Broadcast wireless network	If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DIR-X1860 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 261) 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 icon in the line of the network.

Parameter	Description
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.
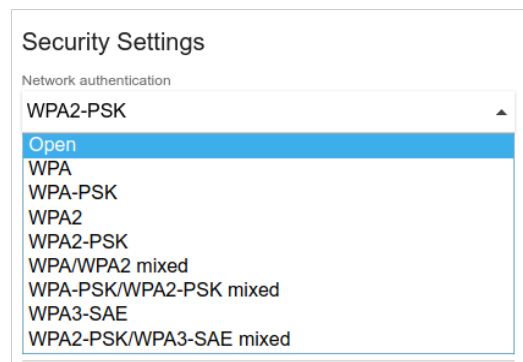
Figure 124. Network authentication types supported by the router.

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.

Authentication type	Description
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):
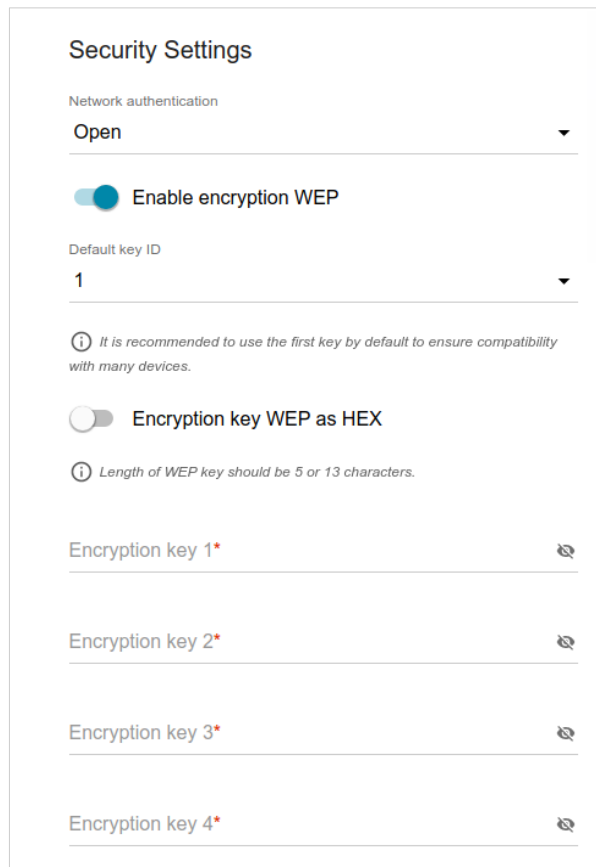
*Figure 125. The **Open** value is selected from the **Network authentication** drop-down list.*

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:

Security Settings

Network authentication
WPA2-PSK

Password PSK*
••••••••

ⓘ *Password should be between 8 and 63 ASCII characters*

Encryption type*
AES

Group key update interval (in seconds)*
3600
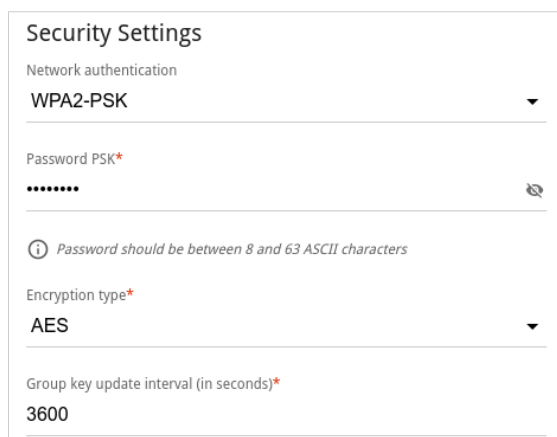
*Figure 126. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.*

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.[6] 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.*

---

6   0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

Parameter	Description
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed.

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

*Figure 127. The **WPA2** value is selected from the **Network authentication** drop-down list.*

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

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

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

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

Client Management

On the **Wi-Fi / Client Management** page, you can view the list of wireless clients connected to the router.
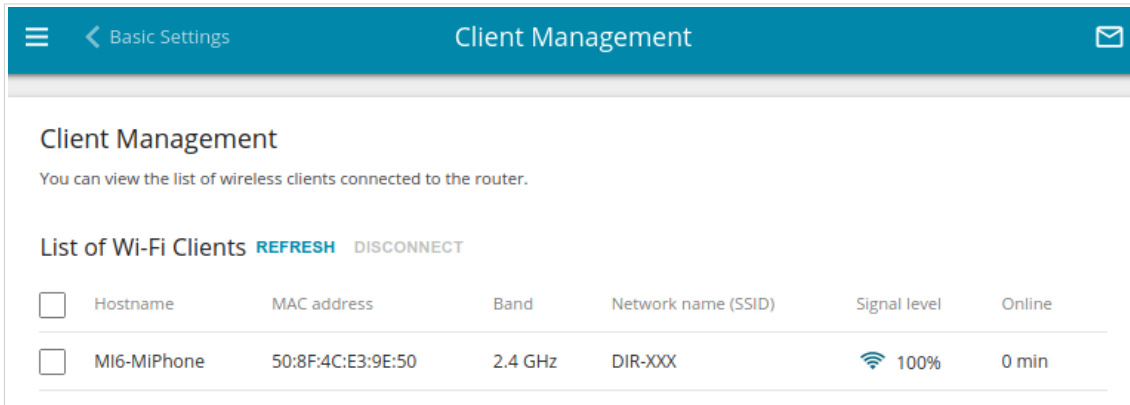
Figure 128. The page for managing the wireless clients.

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.
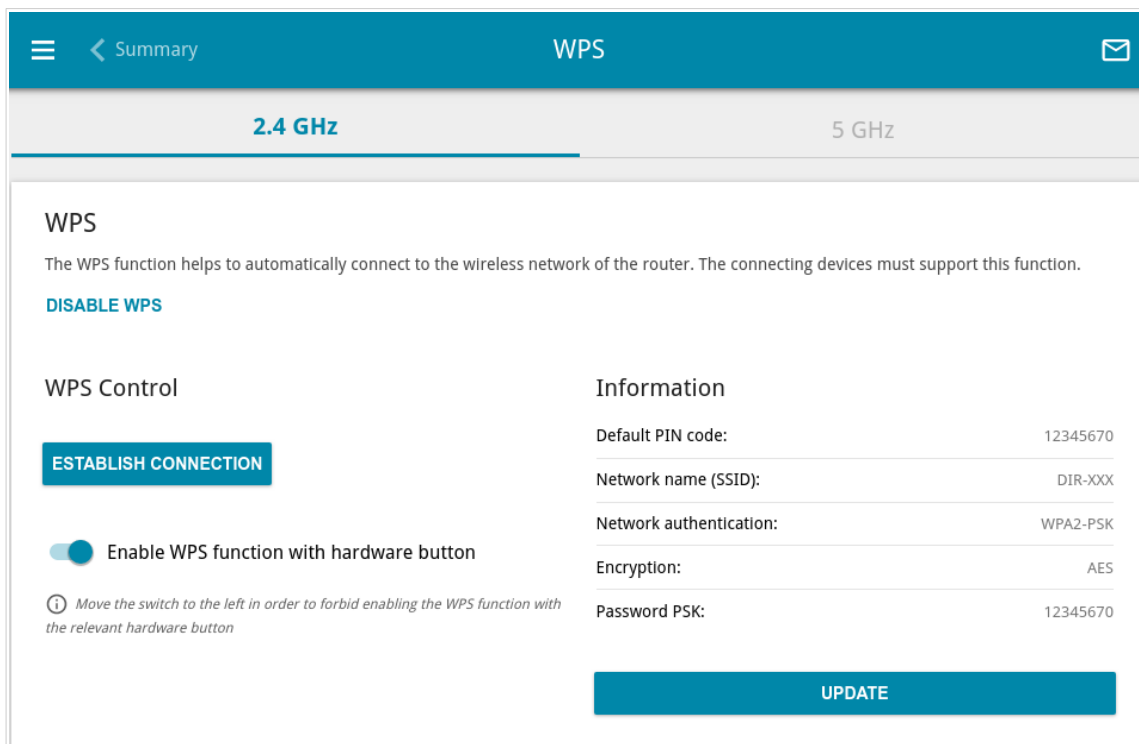
Figure 129. The page for configuring the WPS function.

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, hold it for 2 seconds, and release. The **WLAN 2.4G** and **WLAN 5G** 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
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** the button, hold it for 2 seconds, and release. The **WLAN 2.4G** and **WLAN 5G** 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 130. 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.
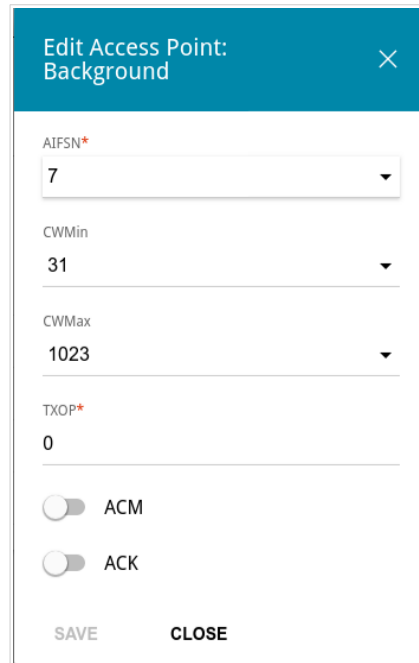
Figure 131. The window for changing parameters of the WMM function.

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.
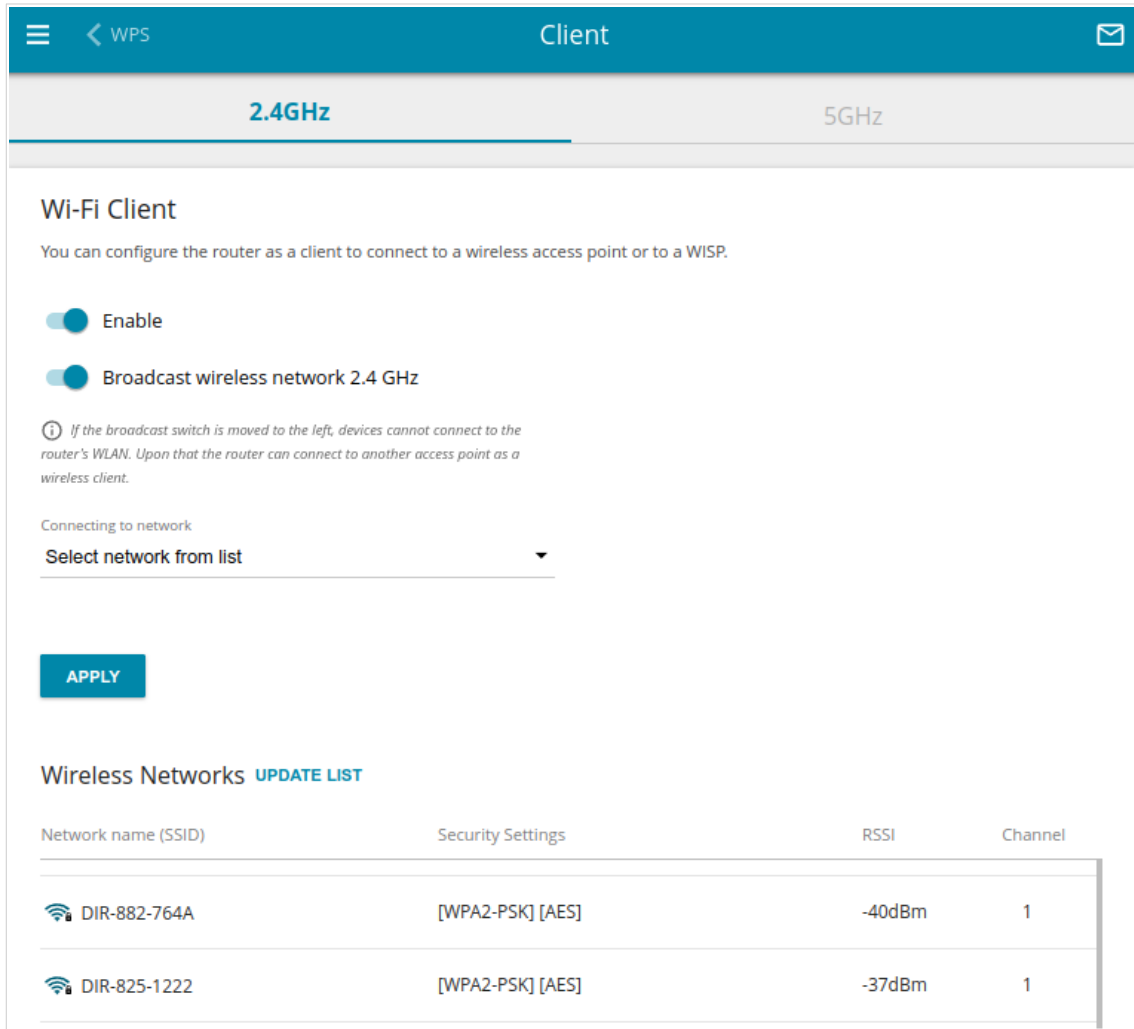
Figure 132. The page for configuring the client mode.

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**, and **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 DIR-X1860 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.

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!
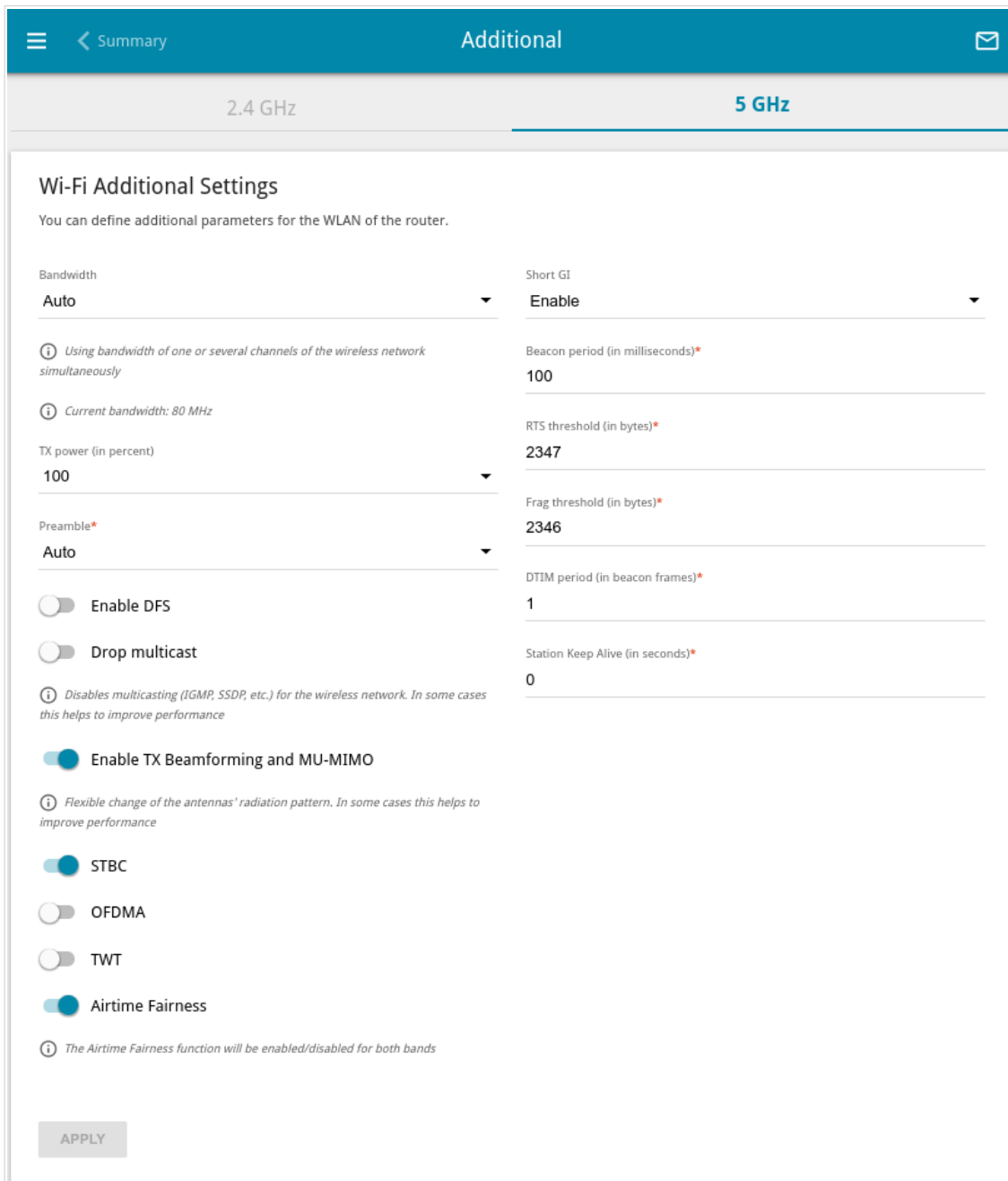
Figure 133. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	The channel bandwidth for devices operating on modern standards. When the **Auto** value is selected, router automatically chooses the most suitable channel bandwidth for these 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).
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/MLD** page. If the switch is moved to the right, the device will not be available by the domain name for Wi-Fi clients.

Parameter	Description
Enable TX Beamforming	*Available on the **2.4 GHz** tab.* TX Beamforming is the signal processing/directing technology 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.
Enable TX Beamforming and MU-MIMO	*Available on the **5 GHz** tab.* TX Beamforming is the signal processing/directing technology which helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation. MU-MIMO (*Multi-user Multiple Input Multiple Output)* is a technology that enables simultaneous data transmission to several devices, optimizing the use of the router's resources and the overall throughput of the Wi-Fi network. Move the switch to the right to enable TX Beamforming and MU-MIMO.
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.
OFDMA	OFDMA *(Orthogonal frequency-division multiple access)* is a Wi-Fi 6 standard technology, that improves performance of wireless networks with a large number of clients by establishing subcarriers with independent modulations. Move the switch to the right to improve the network performance.
TWT	TWT *(Target Wake Time)* is a Wi-Fi 6 standard technology, that allows to negotiate wireless devices' wake-up time for data exchange with the router and to conserve their battery life. Move the switch to the right to save the battery power for the connected wireless devices.

Parameter	Description
Airtime Fairness	Airtime Fairness is a technology which helps to equally distribute data transmission time between all wireless network clients operating on different standards. Upon that clients operating on modern standards transmit more data during the same period of time. Move the switch to the right to equally distribute data transmission time between network clients (this setting can substantially lower the data transfer rate for clients operating on legacy standards). If clients operating only on 802.11n, 802.11ac, and 802.11ax standards are connected to the wireless network, the use of this technology is not required.
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.
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).

Parameter	Description
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 DIR-X1860.
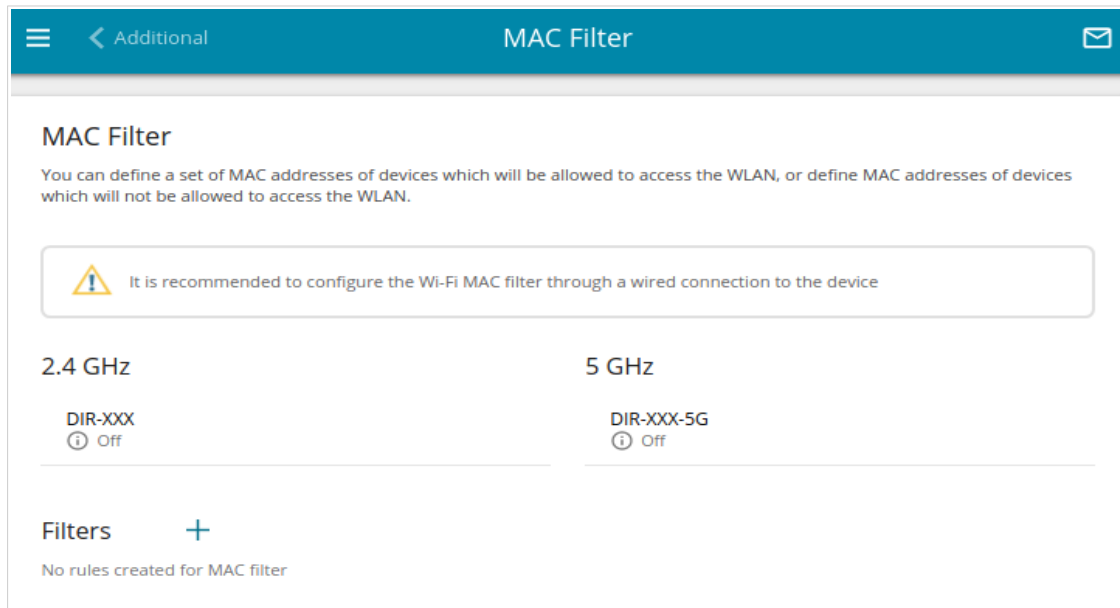
Figure 134. The page for configuring the MAC filter for the wireless network.

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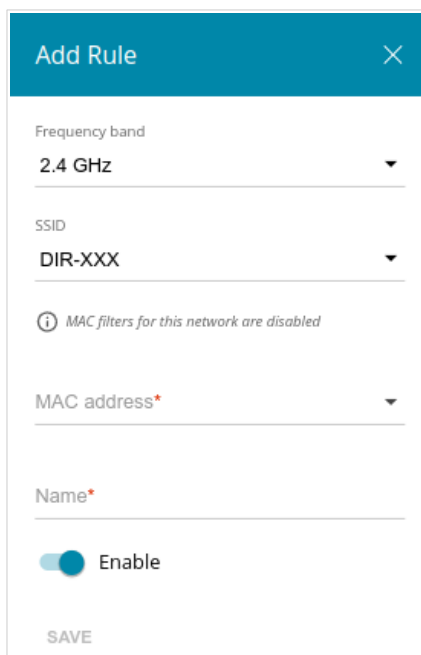
Figure 135. The window for adding a rule for the MAC filter.

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.
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 261) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

EasyMesh

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

A mesh network consists of a main device (the Controller role) and subordinate devices (the Agent role).[7] Devices connect to each other via wireless or wired connection. The Controller device enables connection and configuration of other devices of the mesh network, controls the data flow and the roaming of clients between devices in this network. Agents execute commands from the Controller device and serve as Wi-Fi access points for subordinate devices.

> **!** The EasyMesh function is unavailable when the function of smart adjustment of Wi-Fi clients (roaming) is enabled.
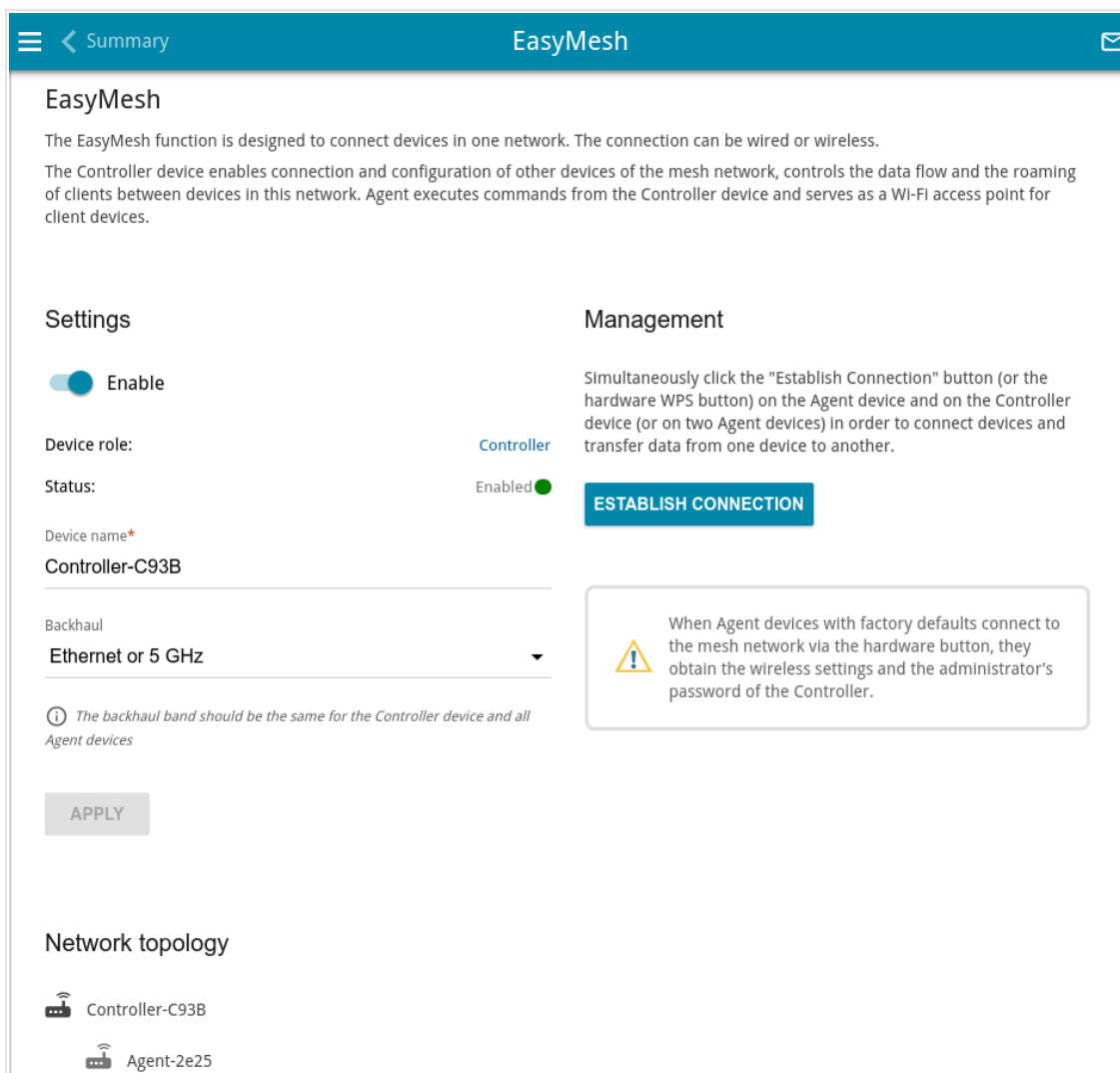
*Figure 136. The **Wi-Fi / EasyMesh** page.*

To activate the EasyMesh function, in the **Settings** section, move the **Enable** switch to the right.

---

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

The following fields are available on the page:

Parameter	Description
Device role	The current role of the device in the mesh network.
Status	The current status of the mesh network. • **Enabled**: The mesh network is enabled and configured. • **Waiting**: Establishing connection and exchanging parameters between the main and subordinate devices. • **Disabled**: The mesh network is disabled.
Device name	The name of the device for easier identification. You can specify any name.
Backhaul	The band in which the mesh network operates. Select one of the bands (2.4GHz or 5GHz) for all devices of the configured network.

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

To configure DIR-X1860 as the main or subordinate device of the mesh network, go to the **Initial Configuration** section (see the *Initial Configuration Wizard* section, page 46), from the **Connection method** list, select the **EasyMesh** value. Then from the **Device role** list, select the required value.

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

Connecting Subordinate Devices with Ethernet Cable

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

1. Connect an Ethernet cable between any of the LAN ports of the main and subordinate device.

2. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.

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

Connecting Subordinate Devices with Hardware Button

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

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

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

2. The **WLAN** LED of the band selected from the **Backhaul** drop-down list should start blinking white slowly. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.

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

Connecting Subordinate Devices via Web-based Interface

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

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

! <u>Do not press the button on more than two devices simultaneously.</u>

2. The **WLAN** LED of the band selected from the **Backhaul** drop-down list should start blinking white slowly. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.

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

To view detailed data on a mesh network device, click the line corresponding to this device in the **Network topology** section.
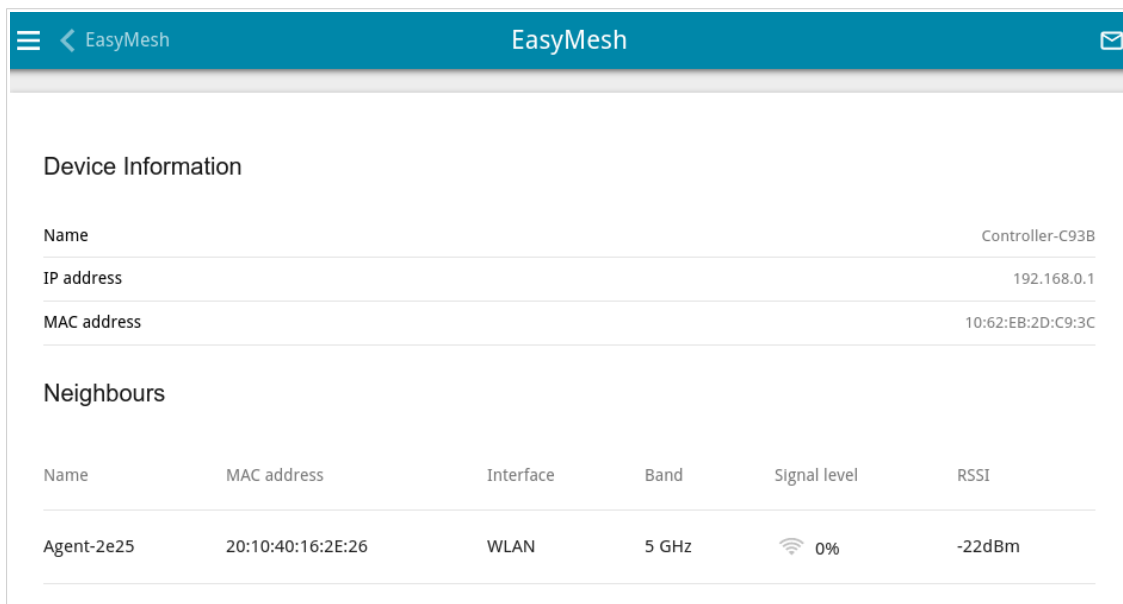
Figure 137. The device information page.

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.

! The function of smart adjustment of Wi-Fi clients (roaming) is unavailable when the EasyMesh function is enabled.

*Figure 138. 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.

Advanced

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

- create or edit VLANs
- use LAN ports of the router as additional WAN ports and also use the WAN port as a LAN port
- enable and configure the SNMP agent of the router
- add name servers
- configure a DDNS service
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the router
- configure notifications on the reason of the Internet connection failure
- define static routes
- configure TR-069 client
- enable the function of mirroring the router's ports
- enable the UPnP function
- enable the built-in UDPXY application for the router
- allow the router to use IGMP and MLD
- enable the RTSP, SIP ALG mechanisms, and PPPoE/PPTP/L2TP/IPsec pass through functions
- configure the CoovaChilli service
- enable VRRP
- enable the Wake-on-LAN function.

VLAN

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

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

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

- **WAN**: For the WAN interface; it includes the **INTERNET** port. You can edit or delete this VLAN.
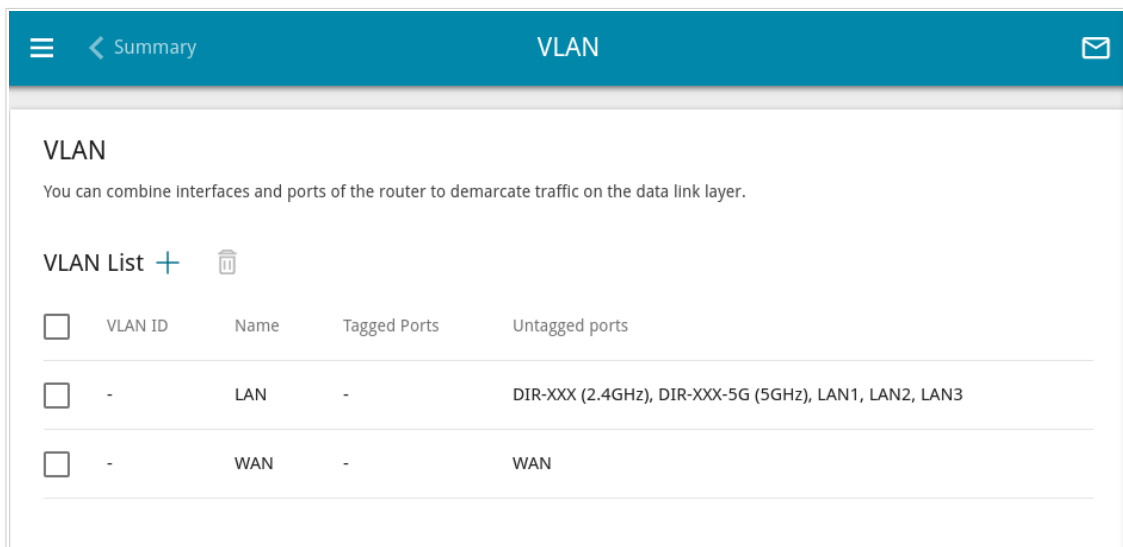
*Figure 139. The **Advanced / VLAN** page.*

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

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

Figure 140. 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 Assignment

On the **Advanced / WAN Assignment** page, you can use LAN ports of the router as additional WAN ports and also use the WAN port as a LAN port.
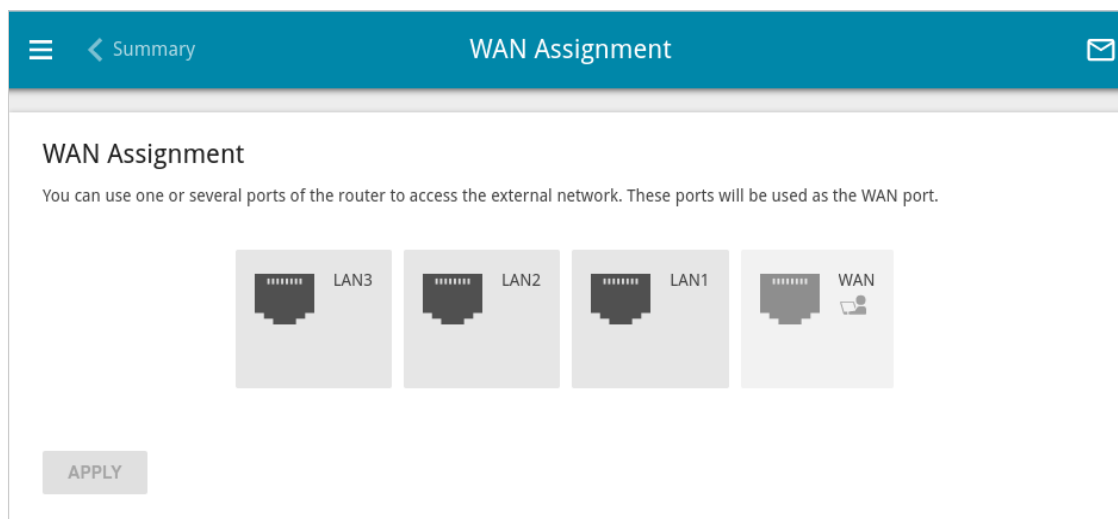
*Figure 141. The **Advanced / WAN Assignment** page.*

Using LAN Ports as WAN Ports

To configure a LAN port of the router to be used as a WAN port, follow the next steps:

1. On the **Advanced / WAN Assignment** page, select a LAN port.

2. In the window displayed, from the **VLAN List** drop-down list, select a VLAN which will include the selected LAN port and click the **APPLY** button; or select the **new_vlan** value to create a new VLAN. In the **Name** field displayed, specify a name of the VLAN for easier identification and click the **APPLY** button. You can change the settings of the VLAN on the **Advanced / VLAN** page (see the *VLAN* section, page 192).

3. Go to the **Connections Setup / WAN** page and create a WAN connection which will be assigned to the network interface of the corresponding VLAN (see the *WAN* section, page 84).

If you don't want to use a LAN port as a WAN port any longer, follow the next steps:

1. On the **Connections Setup / WAN** page, remove the WAN connection assigned to the network interface of the VLAN which includes the corresponding LAN port (see the *WAN* section, page 84).

2. Go to the **Advanced / WAN Assignment** page, select the corresponding LAN port, and in the window displayed, from the **VLAN List** list, select the **LAN** value. Then click the **APPLY** button.

Using WAN Port as LAN Port

To configure the WAN port of the router to be used as a LAN port, follow the next steps:

1. On the **Connections Setup / WAN** page, remove the WAN connection assigned to the network interface of the VLAN which includes the WAN port (see the *WAN* section, page 84).

2. On the **Advanced / WAN Assignment** page, select the WAN port, and in the window displayed, from the **VLAN List** list, select the **LAN** value. Then click the **APPLY** button.

If you don't want to use the WAN port as a LAN port any longer, follow the next steps:

1. On the **Advanced / WAN Assignment** page, select the WAN port.

2. In the window displayed, from the **VLAN List** list, select an existing VLAN which will include the WAN port and click the **APPLY** button; or select the **new_vlan** value to create a new VLAN. In the **Name** field displayed, specify a name of the VLAN for easier identification and click the **APPLY** button. You can change the settings of the VLAN on the **Advanced / VLAN** page (see the *VLAN* section, page 192).

3. Go to the **Connections Setup / WAN** page and create a WAN connection which will be assigned to the network interface of the VLAN (see the *WAN* section, page 84).

SNMP

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

The SNMP agent is a service which sends data on the state and settings of the device where is it enabled to the SNMP manager (the network management system of your ISP or system administrator).
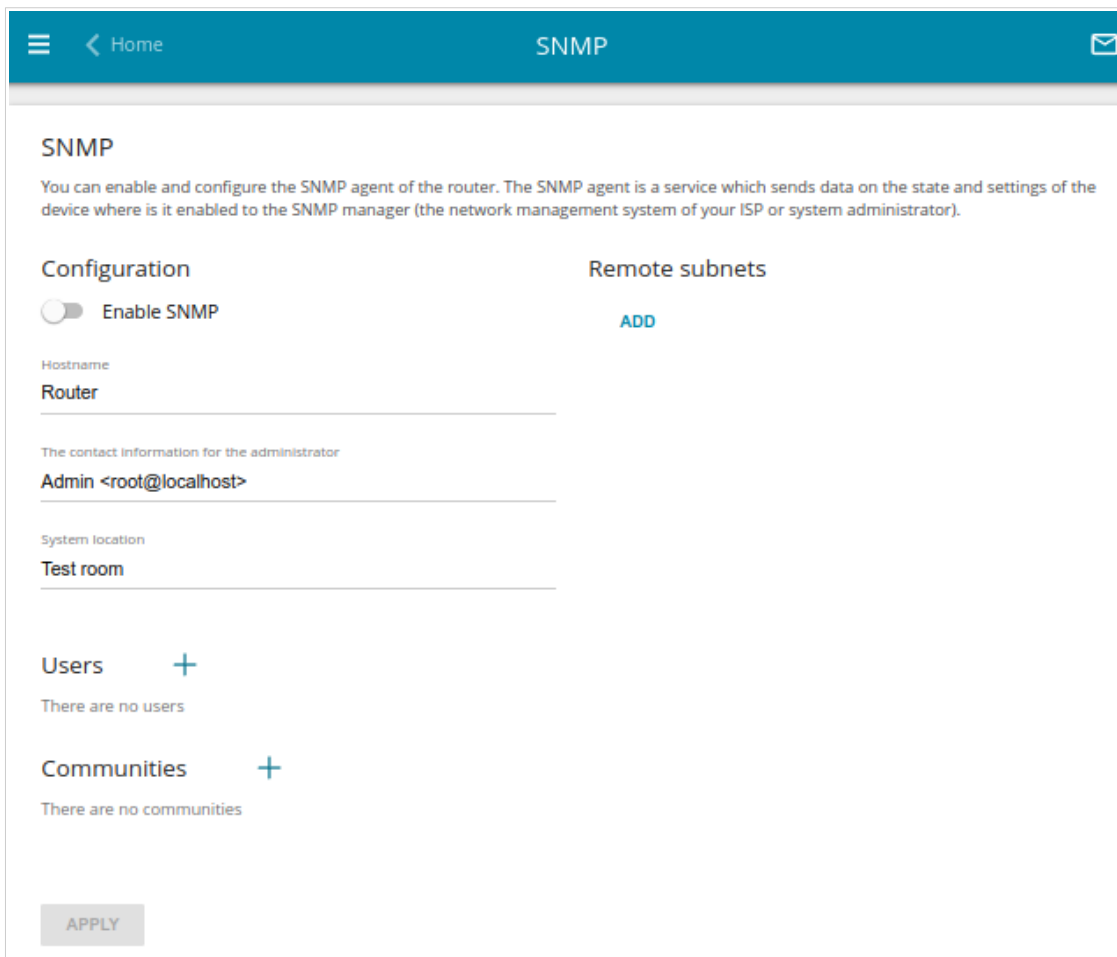
*Figure 142. The **Advanced / SNMP** page.*

In order to enable the SNMP agent, in the **Configuration** section, move the **Enable SNMP** switch to the right. Then specify the needed parameters.

Parameter	Description
Configuration	
Hostname	A name of the router for identification in the SNMP manager.
The contact information for the administrator	Additional information used to contact the administrator of the router.
System location	Additional information used to locate the router.

If needed, specify an IP address of the remote subnet for which access to the SNMP agent of the router will be allowed. To do this, in the **Remote subnets** section, click the **ADD** button and enter the address of the subnet in the line displayed.

To remove an IP address of the subnet, click the **Delete** icon (×) in the relevant line.

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

Figure 143. The window for adding a user.

In the opened window, specify the needed parameters:

Parameter	Description
Name	Specify a username for access from the SNMP manager.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **None** value if authentication is not required.
Authentication password	Specify a password for user authentication from the SNMP manager. The field is displayed if the **MD5** or **SHA** value is selected from the **Authentication protocol** drop-down list.
Encryption protocol	Select a required encryption method from the drop-down list or leave the **None** value if encryption is not required. The list is displayed if the **MD5** or **SHA** value is selected from the **Authentication protocol** drop-down list.

Parameter	Description
Encryption key	Specify an encryption key for data exchange between the SNMP agent and SNMP manager. The field is displayed if the **DES** or **AES** value is selected from the **Encryption protocol** drop-down list.
MIB subtree	Specify a MIB element which will be available to the SNMP manager.

Click the **SAVE** button.

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

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

If the SNMP manager operates over SNMPv2c, create a read-only community which will be used by the SNMP manager to get data on the device. To do this, in the **Communities** section, click the **ADD** button ( ) and specify the community name in the **Name** field in the opened window. Click the **SAVE** button.

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

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

In order to disable the SNMP agent, in the **Configuration** section, move the **Enable SNMP** switch to the left and click the **APPLY** button.

DNS

On the **Advanced / DNS** page, you can add DNS servers to the system.
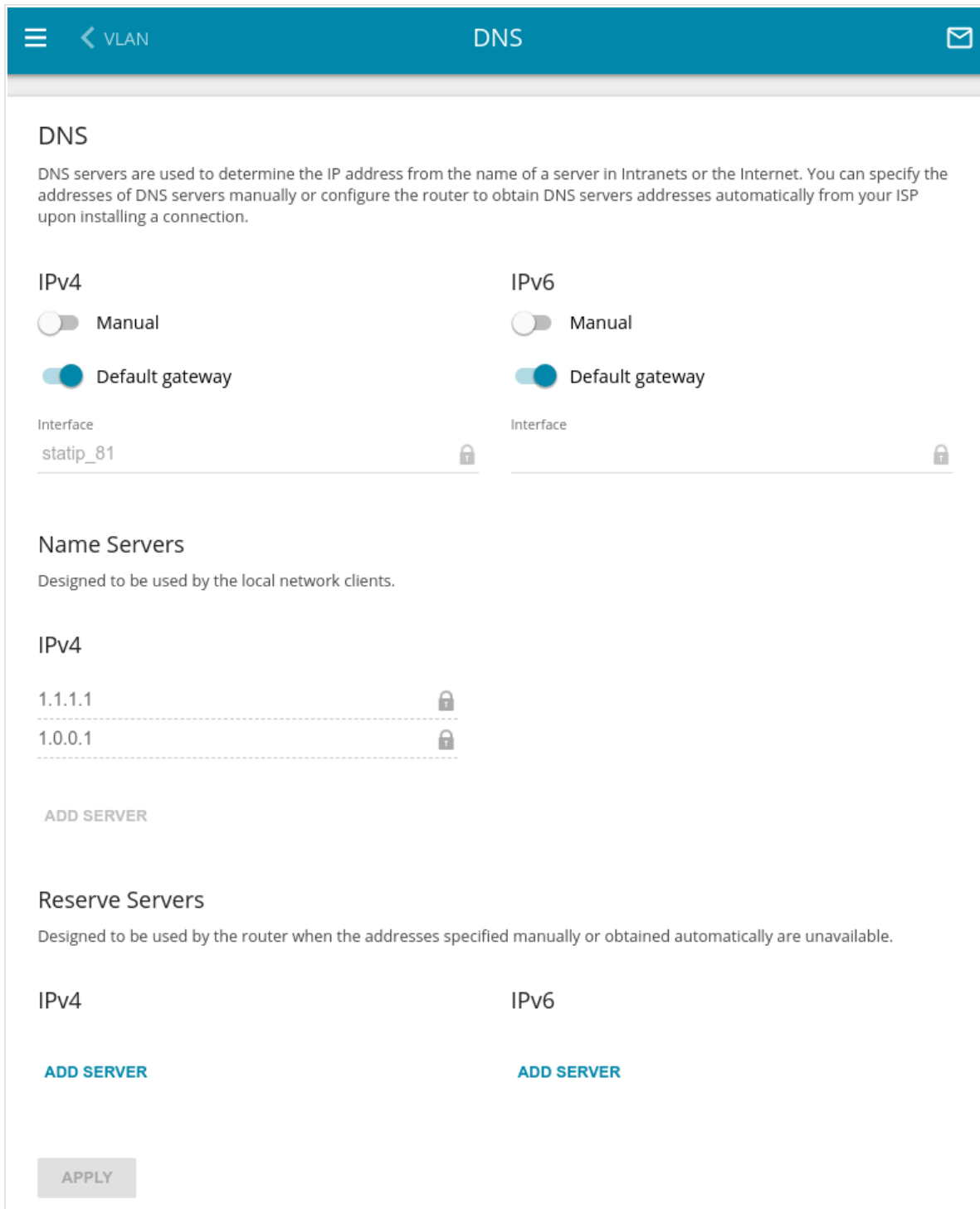
*Figure 144. The **Advanced / DNS** page.*

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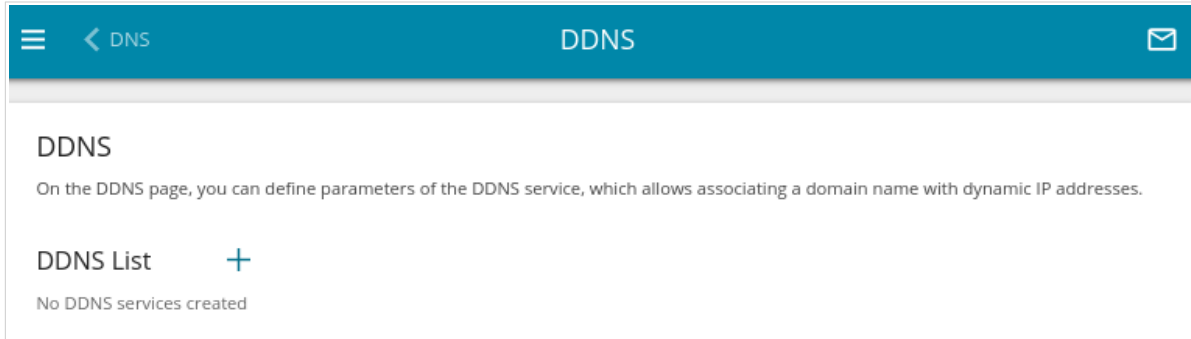
*Figure 145. The **Advanced / DDNS** page.*

To add a new DDNS service, click the **ADD** button (╋).
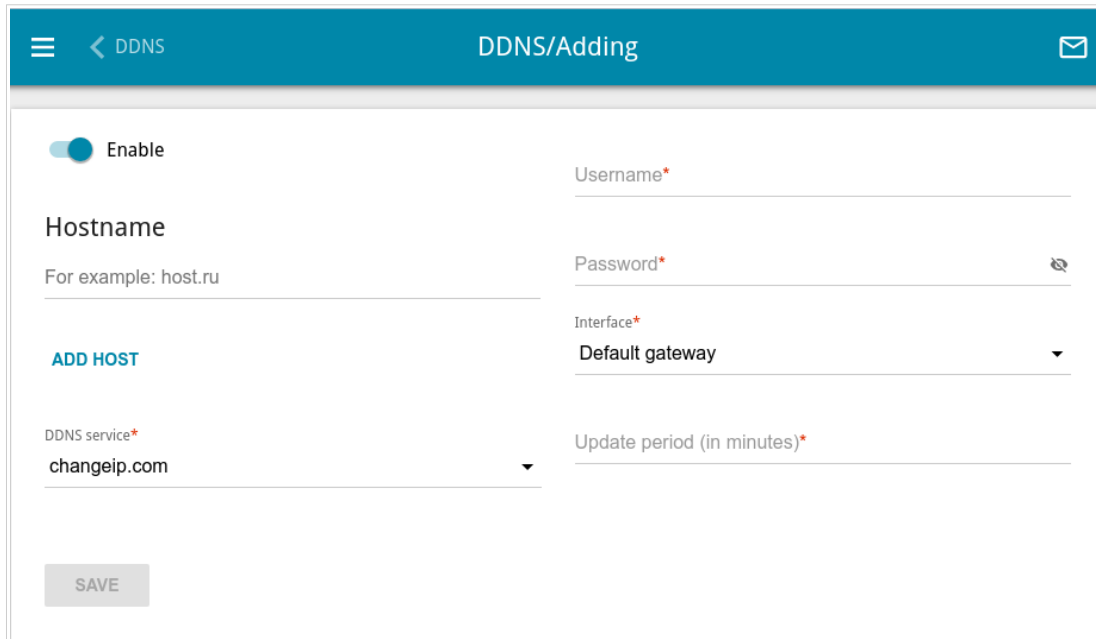
Figure 146. The page for adding a DDNS service.

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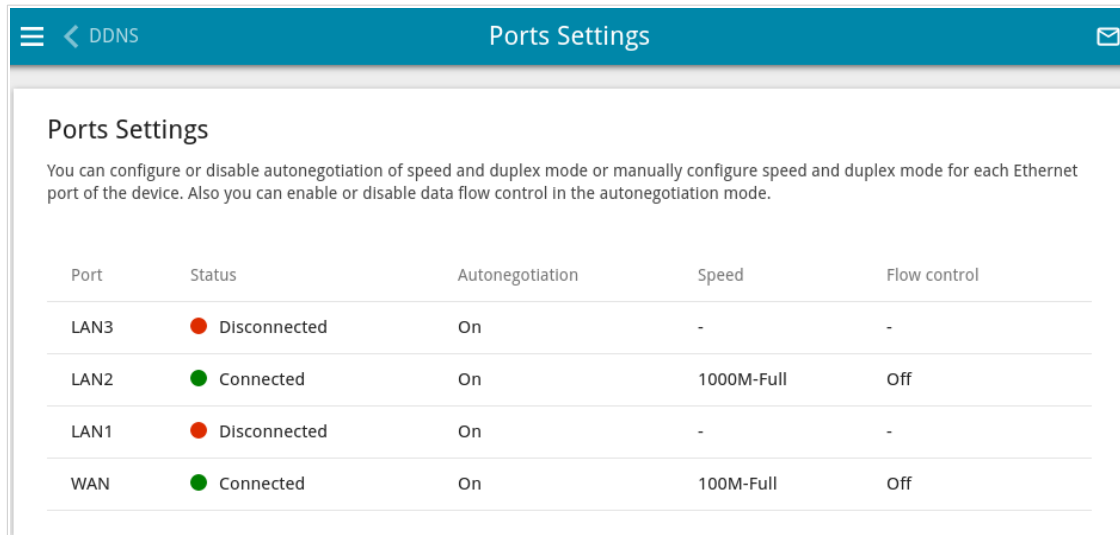
To edit parameters of the existing DDNS service, select the relevant line in the table. On the opened page, change the needed parameters and click the **SAVE** button.

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 147. 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.
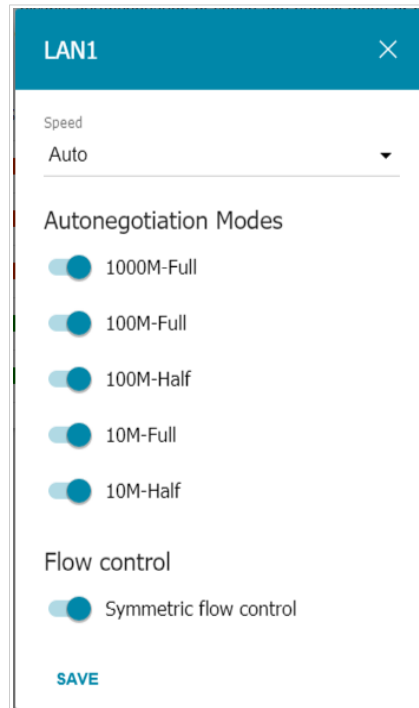
Figure 148. The window for changing the settings of the router's port.

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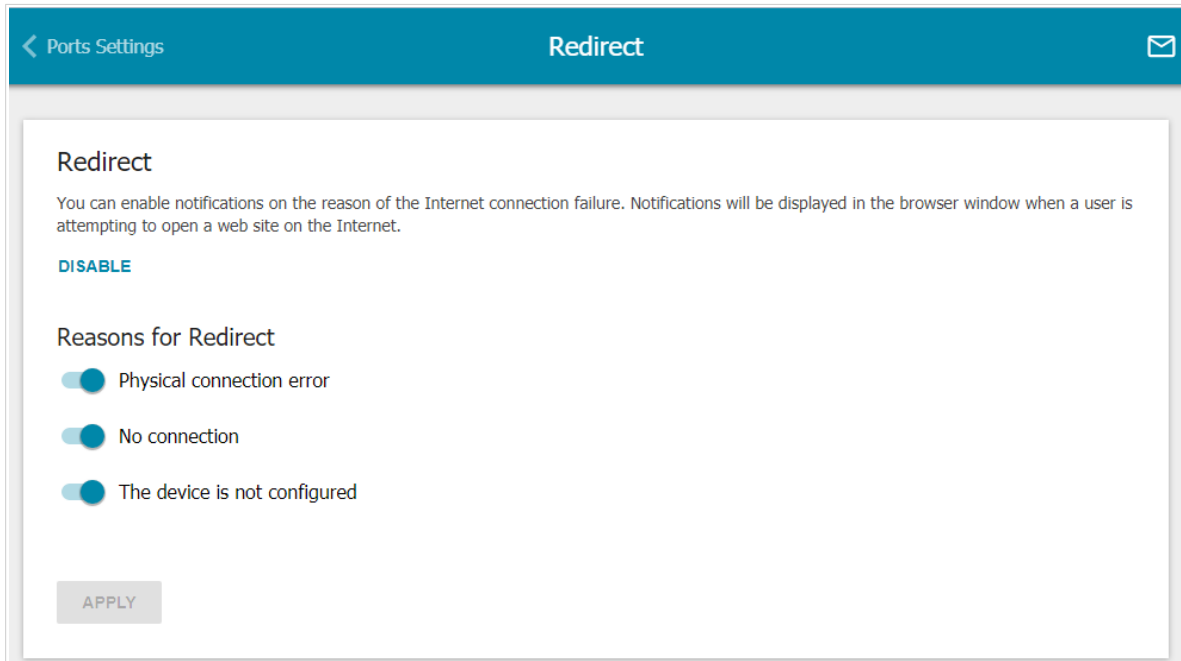
*Figure 149. The **Advanced / Redirect** page.*

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 ISP'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.
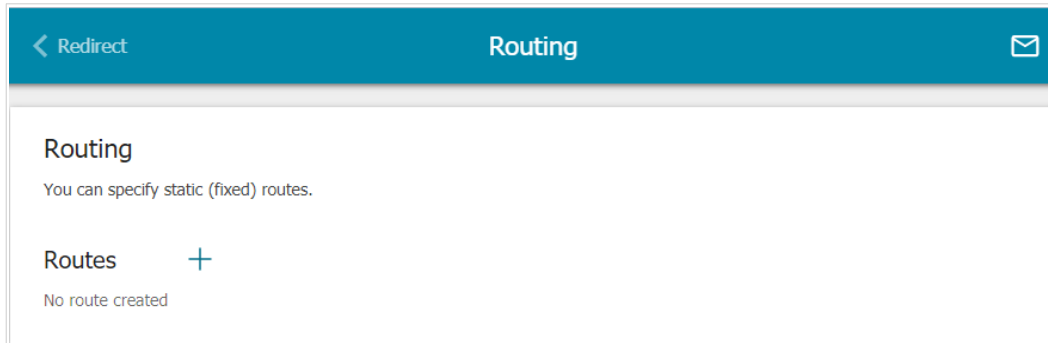
*Figure 150. The **Advanced / Routing** page.*

To specify a new route, click the **ADD** button ( ).
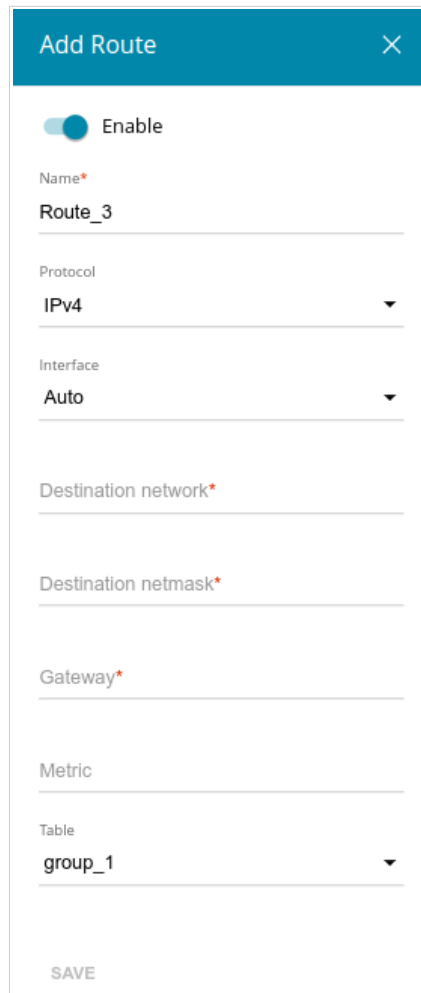
Figure 151. The window for adding a new route.

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.
Name	A name for the route for easier identification.
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 152. 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.

Port Mirroring

On the **Advanced / Port Mirroring** page, you can enable the function of mirroring the router's ports. This function allows to copy traffic from one or several ports to the destination port to monitor network issues with the help of traffic analysis software.
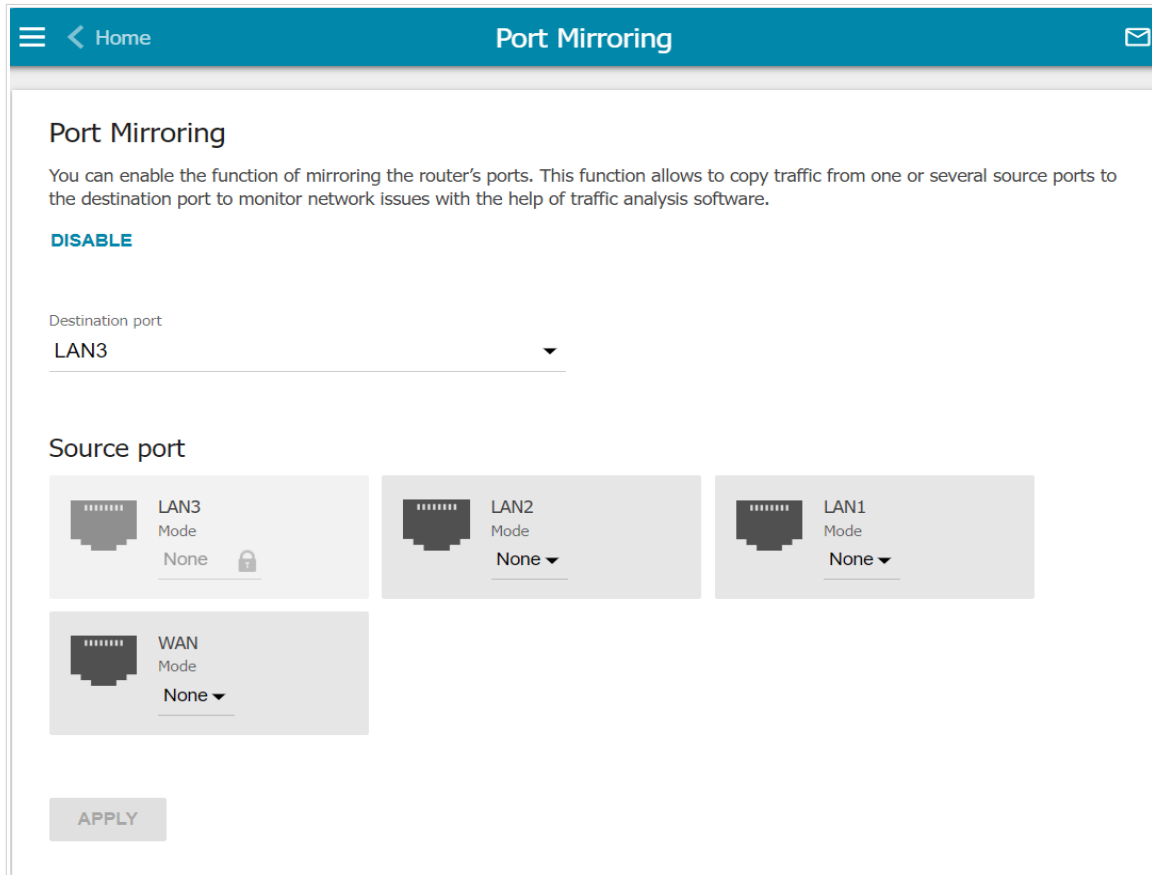
*Figure 153. The **Advanced / Port Mirroring** page.*

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

Parameter	Description
Destination port	The port of the router to which a copy of traffic from one or several ports will be sent. Select the relevant value from the drop-down list.

Parameter	Description
Source port	Select the mode for each port traffic from which should be copied to the destination port: • **Both**: Copy incoming and outgoing traffic from the source port to the destination port. • **TX**: Copy outgoing traffic from the source port to the destination port. • **RX**: Copy incoming traffic from the source port to the destination port. Leave the **None** value for ports from which it is not required to copy traffic.

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

To disable the function of port mirroring, click the **DISABLE** 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.
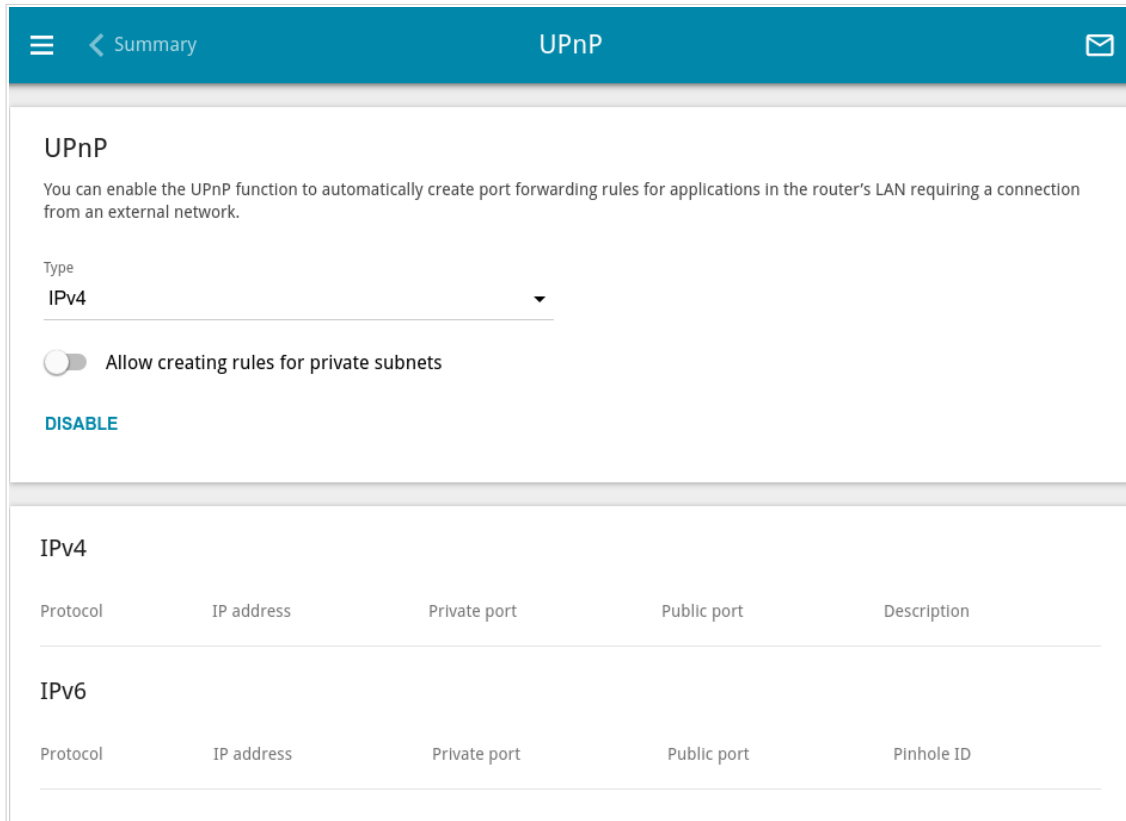
*Figure 154. The **Advanced / UPnP** page.*

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.

Move the **Allow creating rules for private subnets** switch to the right if it is necessary that the port forwarding function operates with the WAN interfaces which IPv4 addresses belong to the range for private networks.

> 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.
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 by the client 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 155. 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 recommended value is specified.
Buffer size for data transferred to client	Size of intermediate buffer for transmitted data. By default, the recommended 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 156. The UDPXY application status page.

IGMP/MLD

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

IGMP and MLD are used for managing multicast traffic (transferring data to a group of destinations) in IPv4 and IPv6 networks correspondingly. These protocols allow using network resources for some applications, e.g., for streaming video, more efficiently.
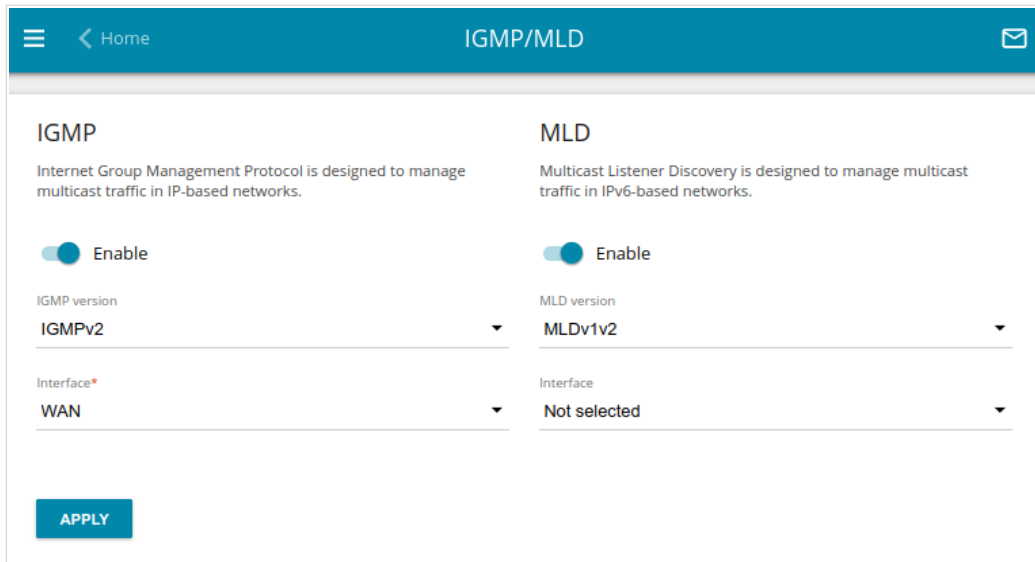
*Figure 157. The **Advanced / IGMP/MLD** page.*

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).

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

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

ALG/Passthrough

On the **Advanced / ALG/Passthrough** page, you can enable the RTSP, SIP ALG mechanisms, 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.
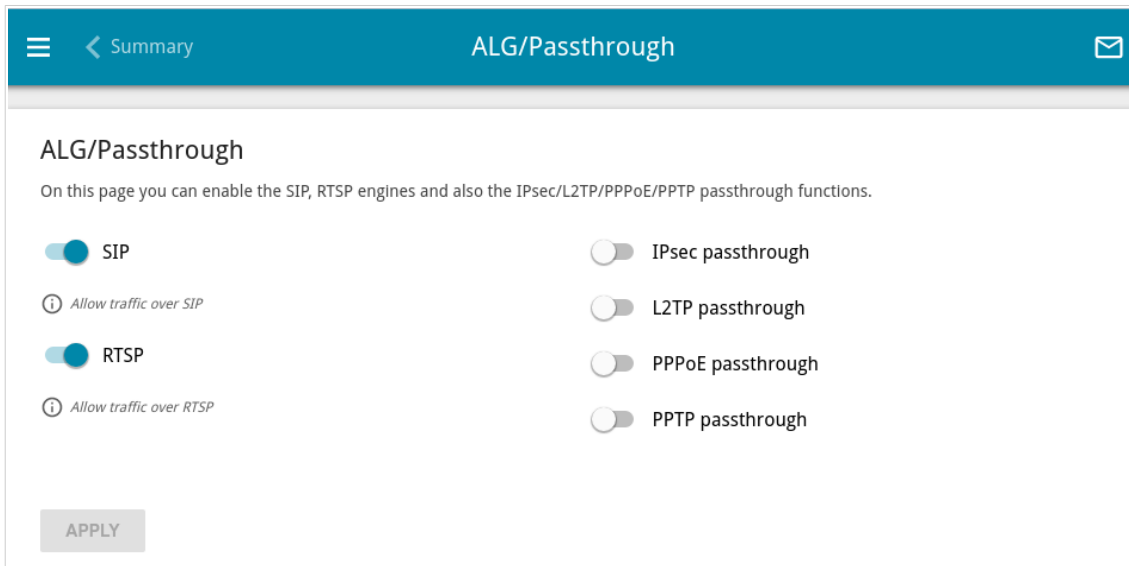
*Figure 158. The **Advanced / ALG/Passthrough** page.*

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.[8]
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.
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.
PPPoE pass through	Move the switch to the right to enable the PPPoE 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.

---

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

CoovaChilli

The CoovaChilli service provides authorized Internet access for clients in your corporate or public network. On the **Advanced / CoovaChilli** page, you can add an authorization server.
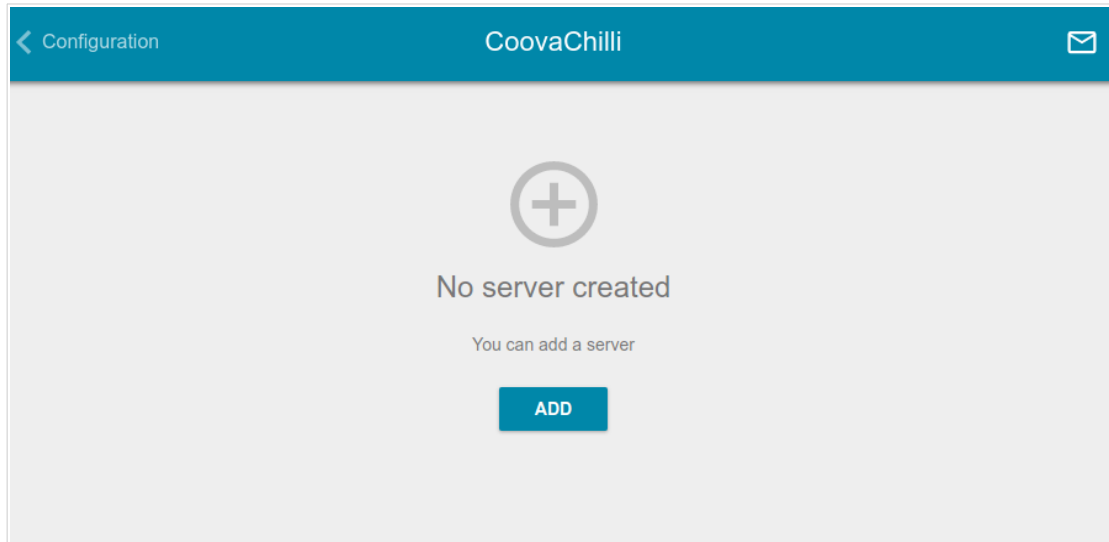
*Figure 159. The **Advanced / CoovaChilli** page.*

To add an authorization server, click the **ADD** button (+). On the opened page, move the **Enable** switch to the right to enable the CoovaChilli service.
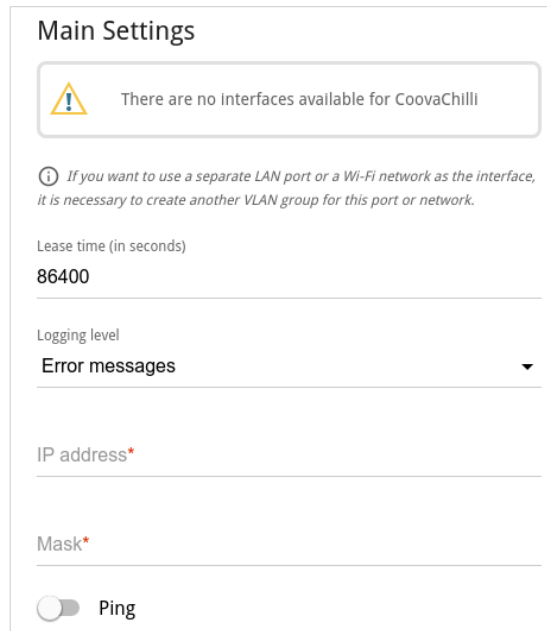
*Figure 160. The page for adding an authorization server. The **Main Settings** section.*

In the **Main Settings** section, you can specify the following parameters:

Parameter	Description
Interface	From the drop-down list, select an interface to be used for the authorization server. A VLAN which includes a separate LAN port or a Wi-Fi network (see the *VLAN* section, page 192) is used as an interface for the server.
Lease time	The interval (in seconds) between sending authorization requests to clients.
Logging level	Select a type of messages and alerts/notifications to be logged.
IP address	Specify an IP address of the router to be used for authorized client access.
Mask	Specify a subnet mask.
Ping	If the switch is moved to the right, the router responds to ping requests by the IP address specified on this page. For security reasons, it is recommended to disable this function.

RADIUS server

Primary RADIUS server address*

Secondary RADIUS server address

RADIUS encryption key*

RADIUS server port
1813

Authentication port
1812

NASID

*Figure 161. The page for adding an authorization server. The **RADIUS server** section.*

In the **RADIUS server** section, you can specify the following parameters:

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

Parameter	Description
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). Click the **Show** icon (👁) to display the entered password.
RADIUS server port	A port of the RADIUS server.
Authentication port	The number of a router port which will be used to connect to the RADIUS server. By default, the value `1812` is specified.
NASID	A network access server ID (the value of this parameter is specified in the RADIUS server settings).
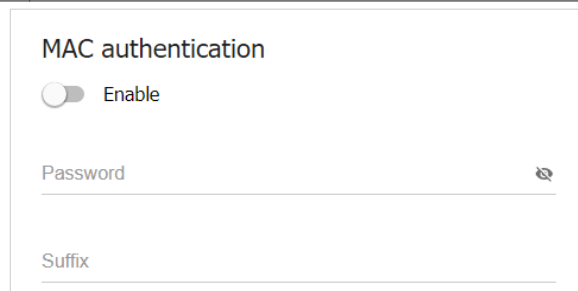
*Figure 162. The page for adding an authorization server. The **MAC authentication** section.*

In the **MAC authentication**[9] section, you can specify the following parameters:

Parameter	Description
Enable	MAC authentication allows the RADIUS server to authorize clients by their MAC addresses. Move the switch to the right to enable MAC authentication. Move the switch to the left to disable MAC authentication.
Password	If required, specify the password to authenticate clients by their MAC addresses. Click the **Show** icon (👁) to display the entered password.
Suffix	Specify a suffix for anonymous MAC authentication.

---

9 Will be available in future software versions.

*Figure 163. The page for adding an authorization server. The **UAM** section.*

In the **UAM** section, you can specify the following parameters:

Parameter	Description
Enable CHAP authentication	Move the switch to the right to enable CHAP authentication. Move the switch to the left to enable PAP authentication (the value of this parameter is specified in the RADIUS server settings).
Authorization port	The number of a router port which will be used for UAM server authorization. By default, the value `3990` is specified.
UAM encryption key	Specify the UAM authentication encryption key. Click the **Show** icon (👁) to display the entered key.
UAM server	Specify the URL of the UAM server which ensures client authorization. The address of the UAM server should start with a protocol. Example: `http://dlink.ru`
Access for unauthorized users	Specify the list of resources (separated by a comma) which unauthorized users are allowed to access. Please specify a site address and a port. Example: `dlink.ru:80`

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

After adding an authorization server, on the **Advanced / CoovaChilli** page, in the **Status** section, the current state of the server connection is displayed.

To edit the parameters of a server, left-click the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

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

VRRP

On the **Advanced / VRRP** page, you can enable VRRP (*Virtual Router Redundancy Protocol*), which is designed to improve availability of routers acting as default gateways. The protocol enables you to configure several devices as the default virtual router with a common IP address, which is used as the default gateway by LAN clients.

*Figure 164. The **Advanced / VRRP** page.*

> ❗ For correct operation of the router while using VRRP, it is required to disable notifications on the reason of the Internet connection failure on the **Advanced / Redirect** page (see the *Redirect* section, page 207).

If you want to enable VRRP, move the **Enable VRRP** switch to the right. When the protocol is enabled, the following elements are displayed on the page:

Parameter	Description
Mode	The operation mode of the router. • **Master**: The router ensuring data transfer at present. A device with a higher priority switches to the **Master** mode. • **Backup**: A reserve router, which switches to the **Master** mode upon the main router failure in accordance with its priority level.
Priority	The current priority level of the device. It can differ from the priority specified by the user if the **Enable Object Tracking** switch is moved to the right.
Status	The status of the service working over VRRP. • **Disable**: The service is not active. • **Enabled**: The service is active.
Interface	A network interface used by VRRP.
VRID	Specify a unique ID of the virtual router. By default, the value `1` is specified.
Priority	The priority of the router over other devices, which is used to switch it to the **Master** mode. Specify a value from the range `1~255`. By default, the value `100` is specified. If several devices have the same priority level, the router with the highest IP address will switch to the **Master** mode.
IP address	The IP address used by LAN devices to access the router.
Mask	The subnet mask of the virtual router.
Delay	An interval (in seconds) between sending service advertisements, containing information on the priority level and connection status of the device working in the **Master** mode. By default, the value `1` is specified.
Assign virtual MAC address	Move the switch to the right to enable access to the virtual router by a virtual MAC address. A virtual MAC address is generated automatically.

Parameter	Description
Preempt mode	The preempt mode enables a backup router to switch to the **Master** mode if its priority level is higher than the priority of the current **Master**. Move the switch to the left to disable the preempt mode. If a device is the owner of the IP address specified on this page, it uses the preempt mode regardless of the position of this switch.
Authorization	Select the authorization method for devices working over VRRP. • **Without authorization**: Authorization is not required. • **PW**: Authorization by password (a HEX key). The maximum key length is 8 symbols. The key should begin with the `0x` prefix.
Enable Object Tracking	Move the switch to the right to track the status of the router connection. When the connection breaks down, the priority of the router is lowered. Select the relevant connection from the **Connection for Object Tracking** drop-down list displayed. Move the switch to the left to disable connection status tracking.

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

If you want to disable VRRP, move the **Enable VRRP** switch to the left and click the **APPLY** button.

Wake-on-LAN

On the **Advanced / Wake-on-LAN** page, you can enable the Wake-on-LAN function. This function allows you to remotely power on or wake up devices connected to the router's LAN via a specific packet.

> ❗ Make sure that the NIC of your device supports the Wake-on-LAN function.
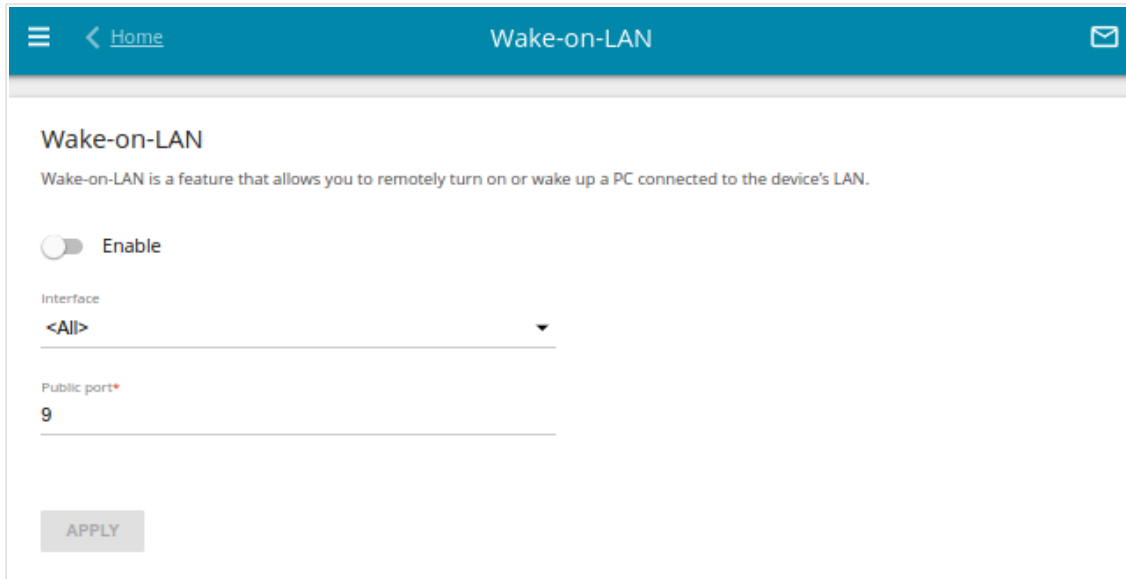
*Figure 165. The **Advanced / Wake-on-LAN** page.*

To enable the function, move the **Enable** switch to the right. Then from the **Interface** drop-down list, select an interface (WAN connection) through which the router will receive the packet to wake up the device or leave the **All** value to receive the packet through all existing WAN connections. If needed, change the port used by the router to receive the packet to wake up the device in the **Public port** field (by default, the standard port **9** is specified). Click the **APPLY** button.

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

Firewall

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

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

IP Filter

On the **Firewall / IP Filter** page, you can create new rules for filtering IP packets and edit or remove existing rules.
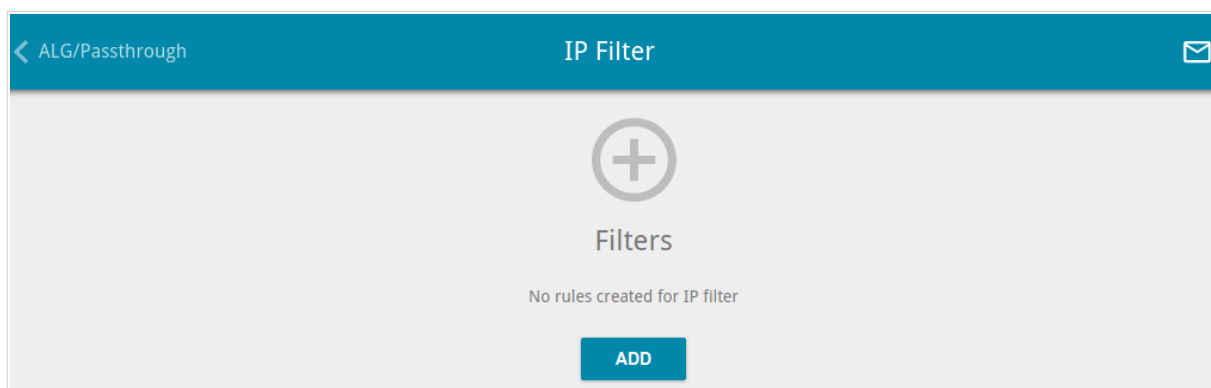
*Figure 166. The **Firewall / IP Filter** page.*

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

Figure 167. 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.

Parameter	Description
Priority	The priority level of the rule. In the field, enter the needed value. The lower the value, the higher is the priority of the rule. You can specify a value from 0 to 5000.
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*). • **IPIP**: The rule will be applied to the packets transmitted from the IPIP tunnel (*available if an IPIP 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 DIR-X1860. **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*). **IPIP**: The rule will be applied to the packets transmitted to the IPIP tunnel (*available if an IPIP 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).

Parameter	Description
End IPv4 address / End IPv6 address	The source host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The source subnet IPv4 or IPv6 address. The field is displayed when the **Subnet** value is selected from the **Set as** drop-down list.
Destination IP address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the **End IPv4 address / End IPv6 address** field blank. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
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 261) 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 create a copy of an IP filter rule, select the checkbox located to the left of the relevant line in the table and click the **Clone** (⬚) icon. 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 (🗑).

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.
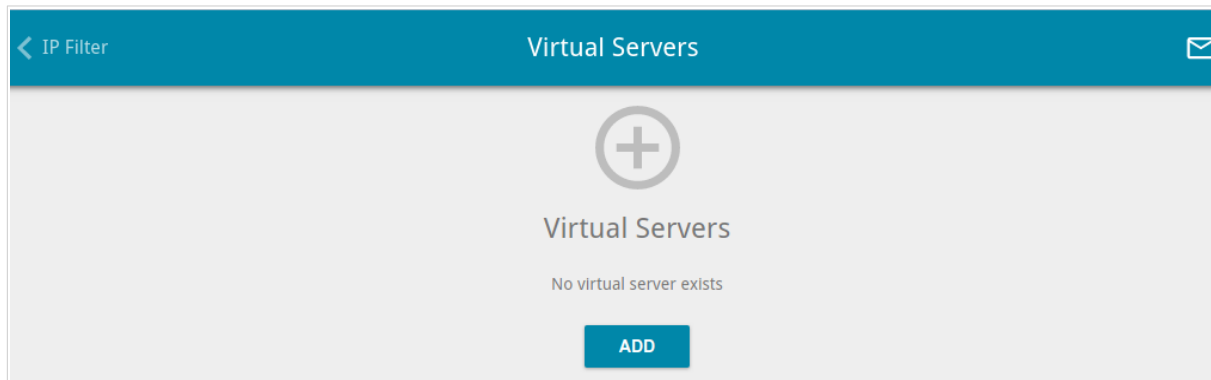
*Figure 168. The **Firewall / Virtual Servers** page.*

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

Figure 169. 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.
Template	Select a virtual server template from the drop-down list, or select **Custom** to specify all parameters of the new virtual server manually.

Parameter	Description
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 address	The IP address of the host/subnet of the client that will connect to the virtual server. 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 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 261) 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 create a copy of a virtual server, select the checkbox located to the left of the relevant line in the table and click the **Clone** ( ) icon. 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 rule. 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 ( ).

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.
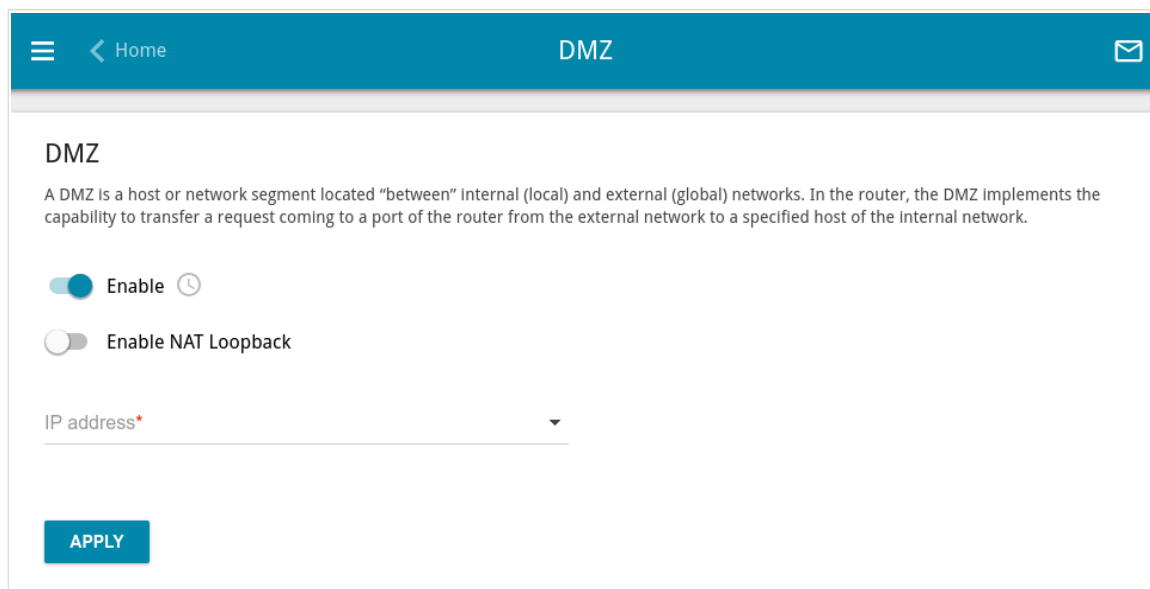
*Figure 170. The **Firewall / DMZ** page.*

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 261) 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.
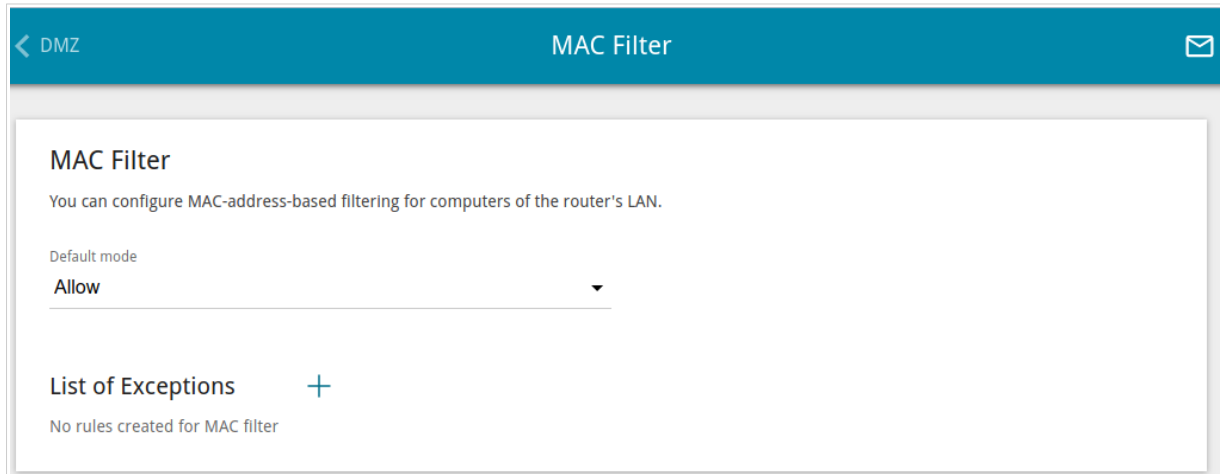
*Figure 171. The **Firewall / MAC Filter** page.*

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 (+).
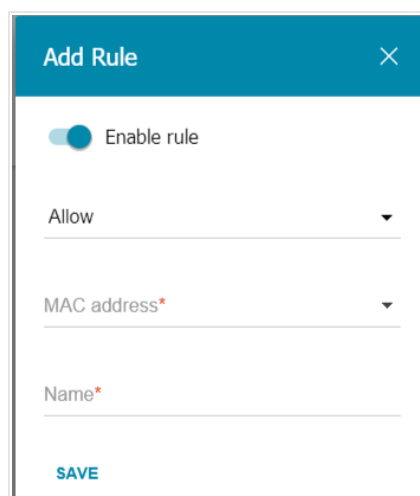
Figure 172. The window for adding a rule for the MAC filter.

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 261) 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.
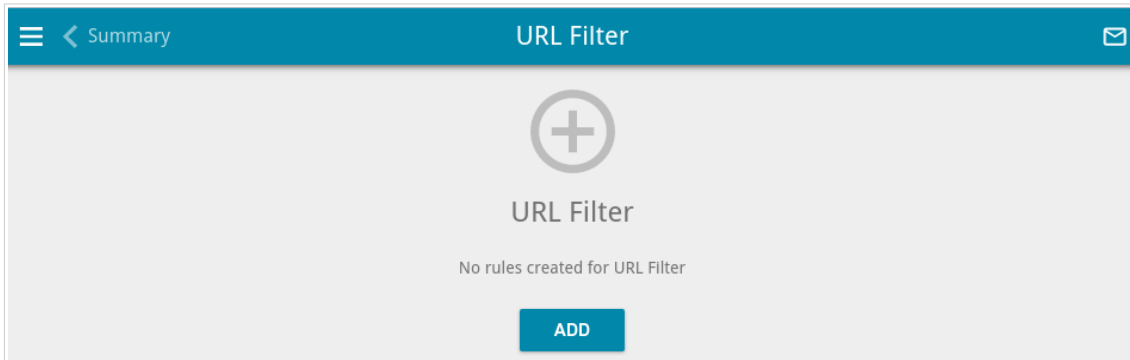
*Figure 173. The **Firewall / URL Filter** page.*

To create a new rule, click the **ADD** button (✛).
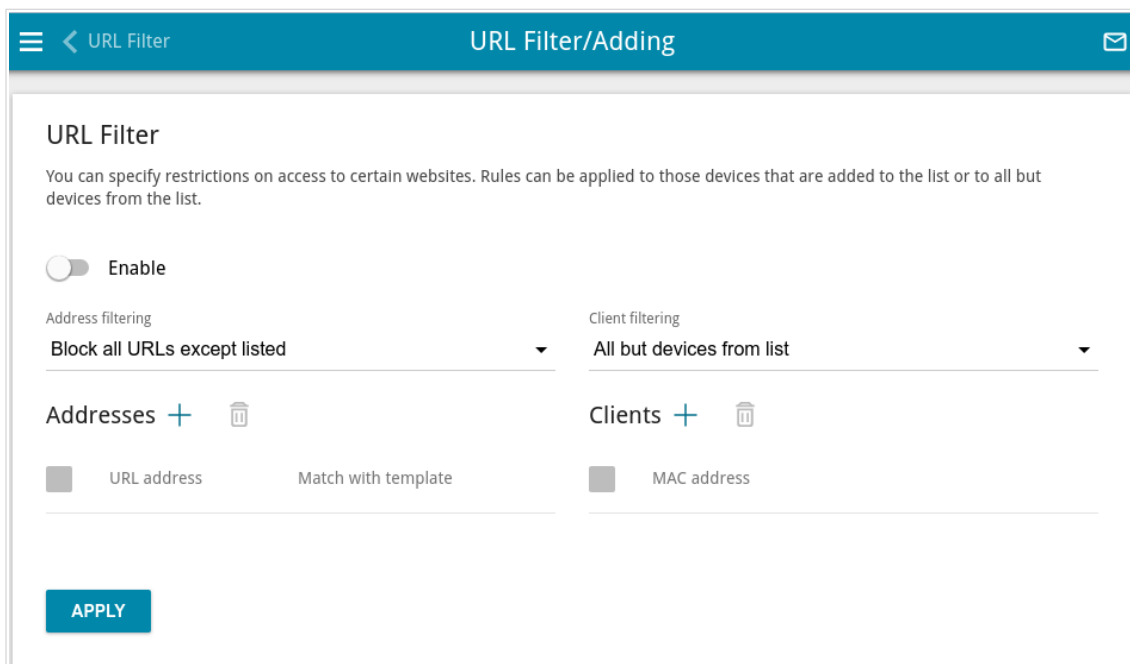
Figure 174. The page for adding a rule for URL filter.

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 261) 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 (🗑).

AdBlock

On the **Firewall / AdBlock** page, you can enable the function of blocking advertisements which appear during web surfing.
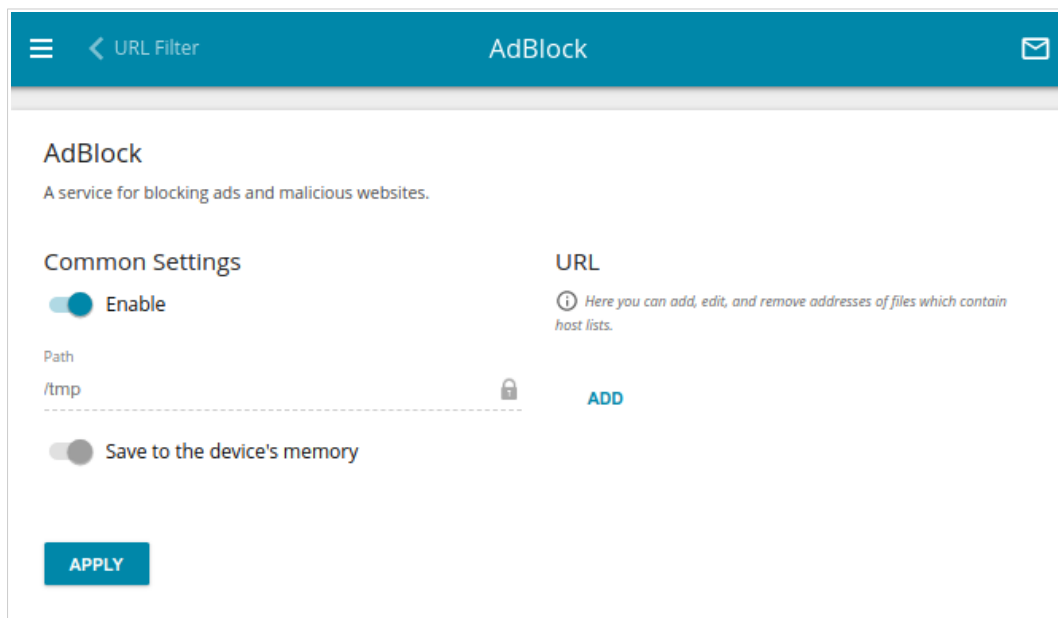
*Figure 175. The **Firewall / AdBlock** page.*

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

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

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

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

Remote Access

On the **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.
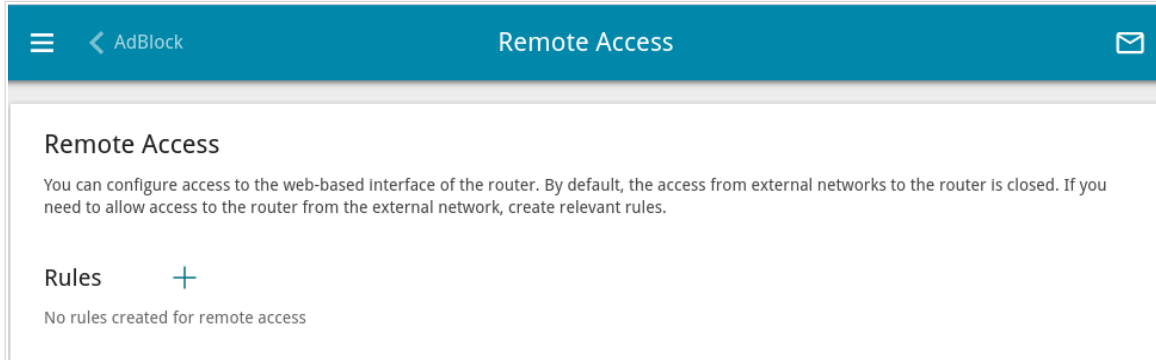
*Figure 176. The **Firewall / Remote Access** page.*

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

Figure 177. 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 261) 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

- disable automatic save of the settings or save the changed settings manually to the non-volatile memory

- reboot the router

- change the web-based interface language

- edit or add commands for the hardware buttons

- update the firmware of the router

- configure automatic notification on new firmware version

- enable/disable Wi-Fi connection and the Wi-Fi filter, configure automatic reboot of the device on a schedule, and set a schedule for different rules and settings of the firewall

- enable event logging and set its basic options

- create rules for sending the event log to a remote server

- check availability of a host on the Internet through the web-based interface of the router

- trace the route to a host

- enable or disable access to the device settings via TELNET and/or 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, disable automatic save of the settings or save the changed settings manually to the non-volatile memory, reboot the device, or change the web-based interface language.
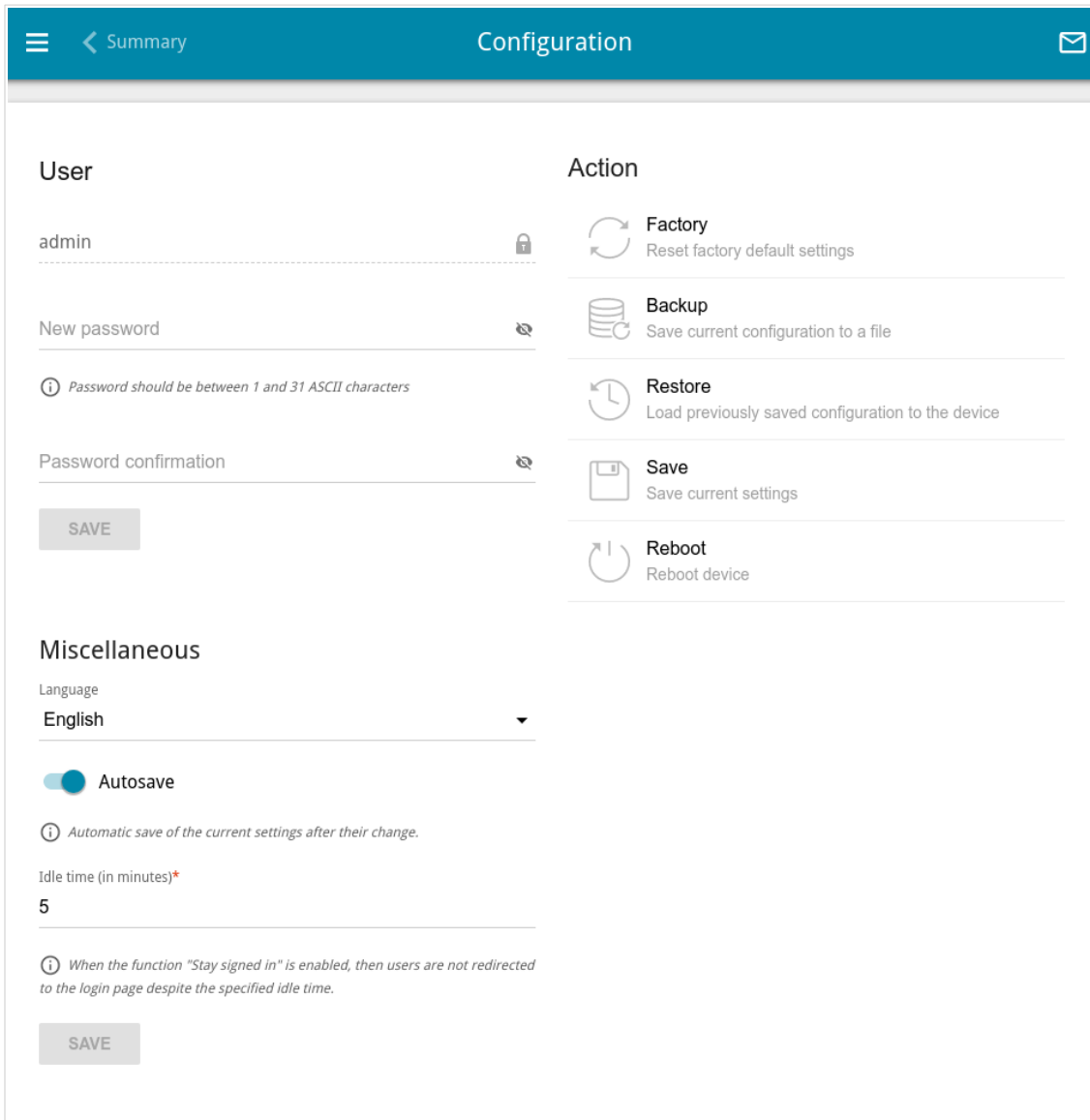
*Figure 178. The **System / Configuration** page.*

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.[10] Click the **Show** icon ( ) to display the entered values. Then click the **SAVE** button.

---

10 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

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

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

By default the router saves changed settings automatically (the **Autosave** switch in the **Miscellaneous** section is moved to the right). Move the **Autosave** switch to the left if you don't want the changed settings to be saved automatically. In this case, a notification will be displayed in the top right part of the page when the settings are changed.

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 ***Back Panel*** section, page 17).
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. If the automatic save of the router's settings is disabled, save settings manually after you change the router's parameters. Otherwise the changes will be lost upon reboot of the router.
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** and **WPS** hardware buttons.
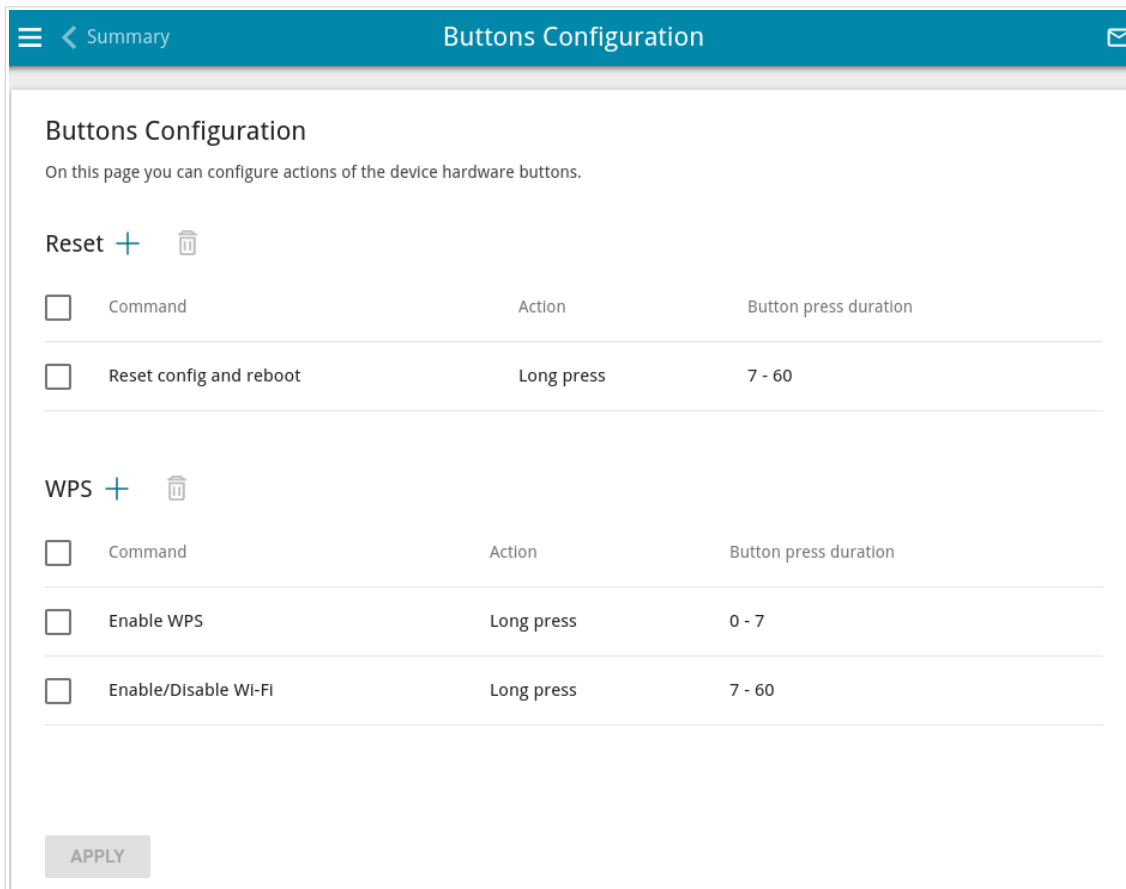
*Figure 179. The **System / Buttons Configuration** page.*

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 15). You can edit or delete them.

To add a command for a button, click the **ADD** button (+) in the relevant section.
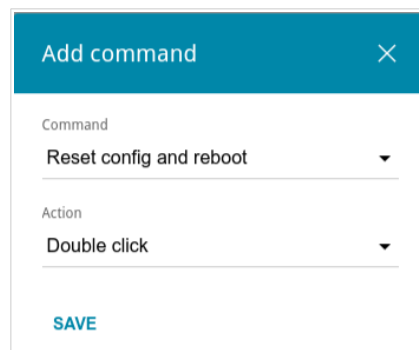
Figure 180. The window for adding a command.

In the opened window, specify the following parameters:

Control	Description
Reset / 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. The action is not available if the **Long press** action with the duration from 0 seconds has already been specified for the hardware button. • **Double click**: Two short presses of the button. • **Long press**: A prolonged press of the button. 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. You can specify values from 0 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.
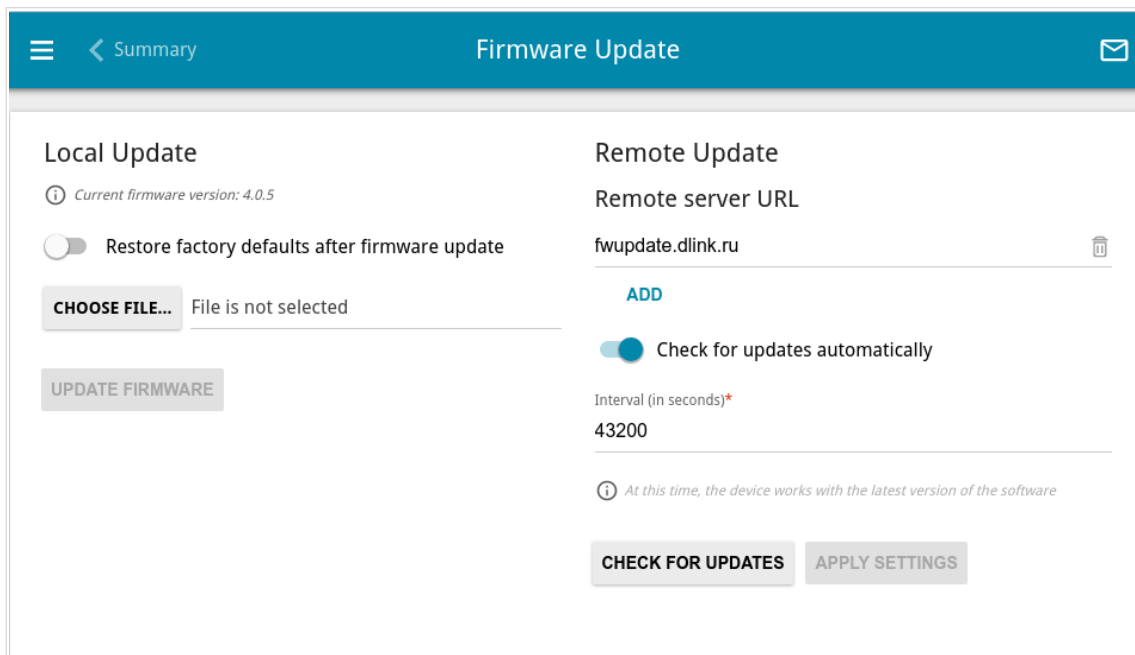
*Figure 181. The **System / Firmware Update** page.*

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** or **Repeater** 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, 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 274).
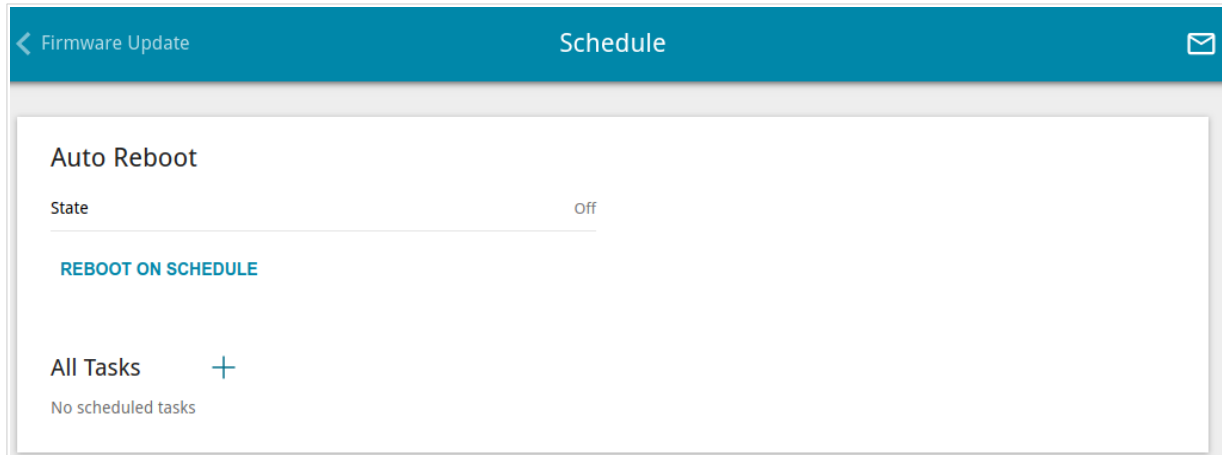
*Figure 182. The **System / Schedule** page.*

To configure automatic reboot of the device on a schedule, click the **REBOOT ON SCHEDULE** button in the **Auto Reboot** section.
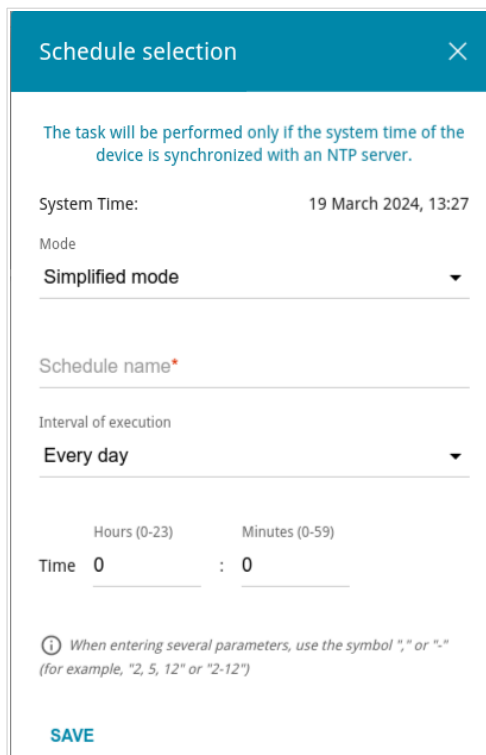
Figure 183. The window for configuring automatic reboot on a schedule.

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 or will enable/disable Wi-Fi connection or Wi-Fi filter, click the **ADD** button (+) in the **All Tasks** section.

Figure 184. 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 task. Move the switch to the left to disable the task.
Simplified mode	
Schedule name	Specify a schedule name for easier identification. You can specify any name.

Parameter	Description
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 or will enable/disable Wi-Fi connection or Wi-Fi filter, go to the relevant page of the web-based interface of the device.

Logging

In this menu you can enable event logging and create rules for sending the log to a remote server.

Local

On the **System / Logging / Local** page, you can enable event logging and set its basic options.
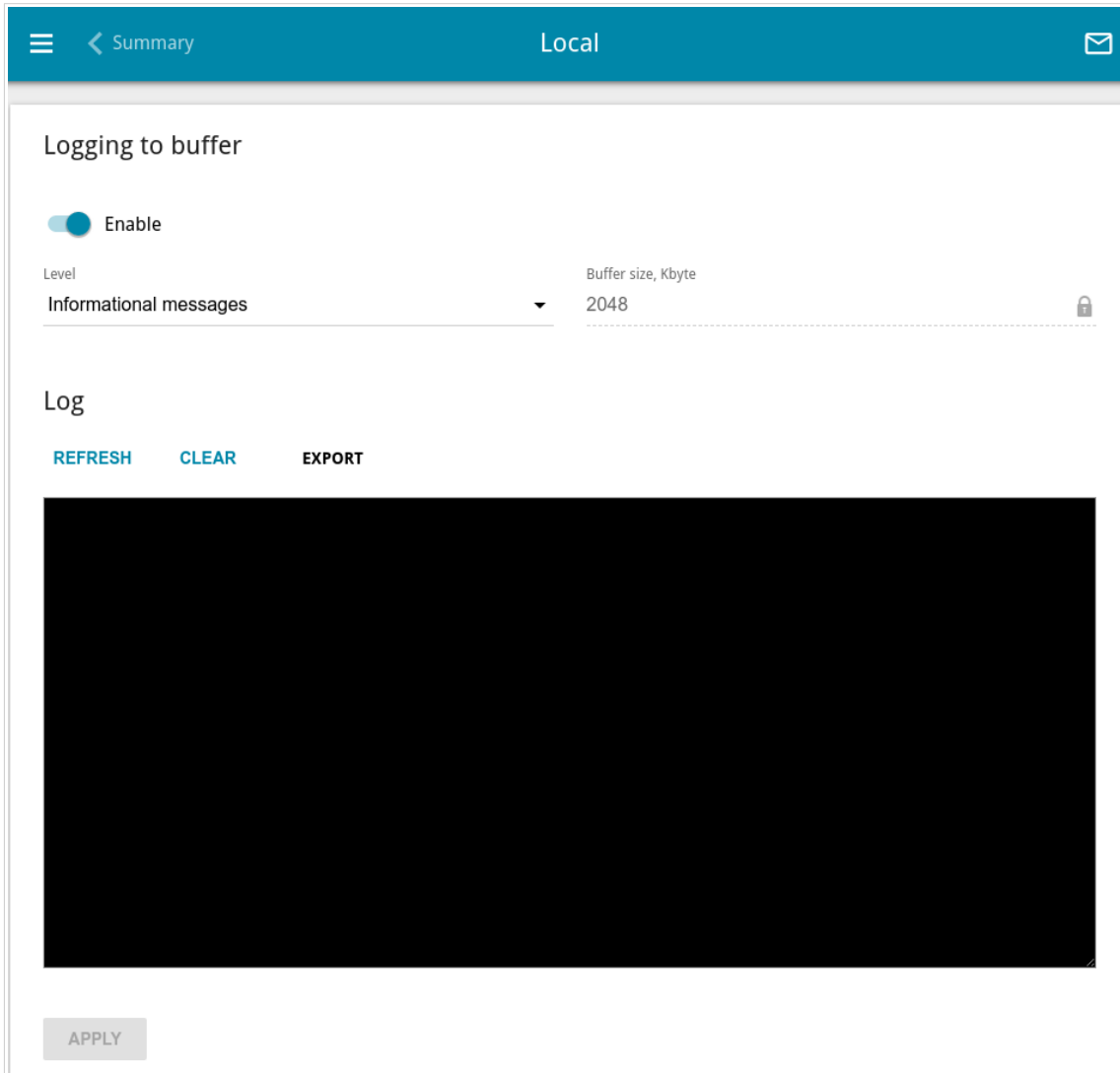
*Figure 185. The **System / Logging / Local** page.*

To enable logging of events to the router's RAM, in the **Logging to buffer** section, move the **Enable** switch to the right. Then specify the needed parameters.

Parameter	Description
Logging to buffer	
Level	From the drop-down list, select the severity level of messages which will be logged. Upon that messages which severity level is equal to the selected level or higher than the selected one will be logged.
Buffer size	The amount of RAM (in kilobytes) allocated for the system event log. You cannot change this value.

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

To disable logging of events to the router's RAM, move the **Enable** switch to the left and click the **APPLY** button.

You can view the event log in the **Log** section.

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

To remove all log entries from the router's RAM, click the **CLEAR** button.

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

Remote

On the **System / Logging / Remote** page, you can create rules for sending the event log to a remote server.
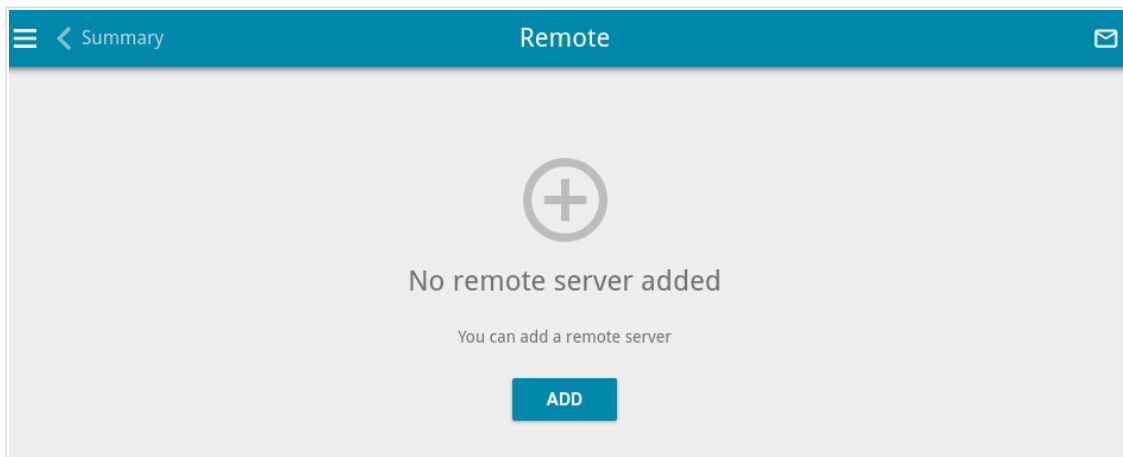
*Figure 186. The **System / Logging / Remote** page.*

To create a new rule, click the **ADD** button (+).
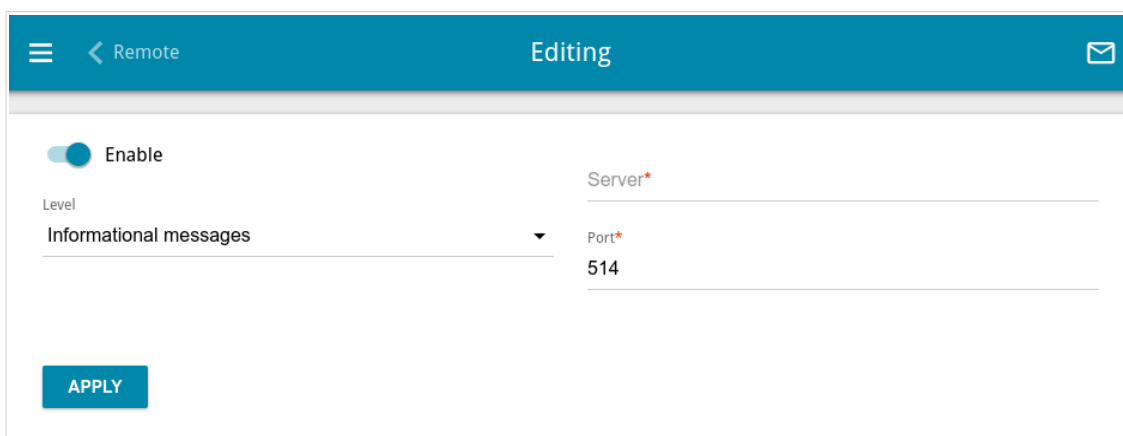
Figure 187. The page for adding a rule.

On the opened page, 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.
Level	From the drop-down list, select the severity level of messages which will be logged in the event log. Upon that messages which severity level is equal to the selected level or higher than the selected one will be logged.
Server	The IP address or full domain name of the host from the local or global network, to which the event log will be sent.

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

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

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.
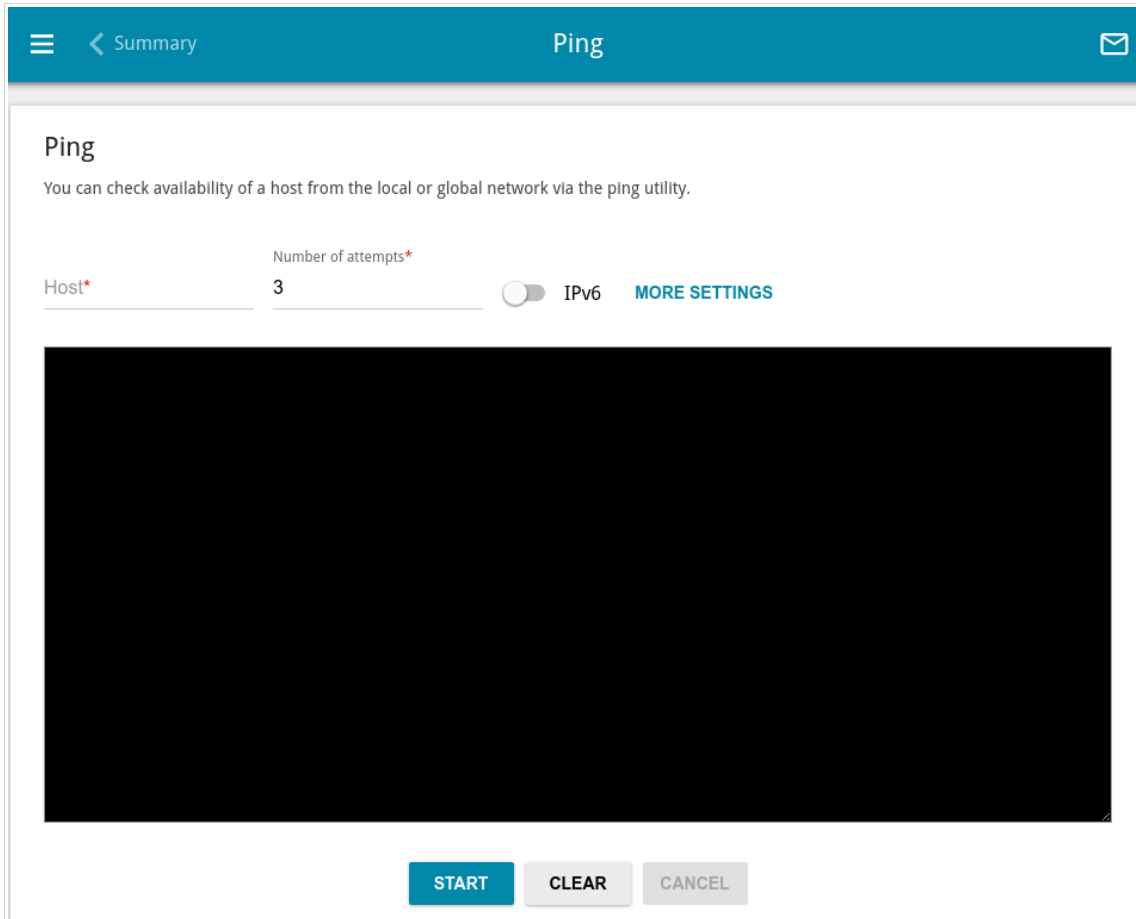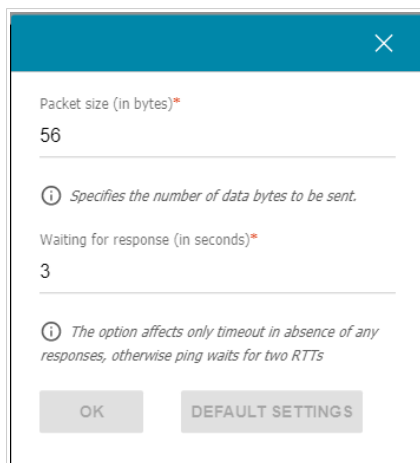
*Figure 188. The **System / Ping** page.*

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 189. 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 trace the route of data transfer to a host via the traceroute utility.
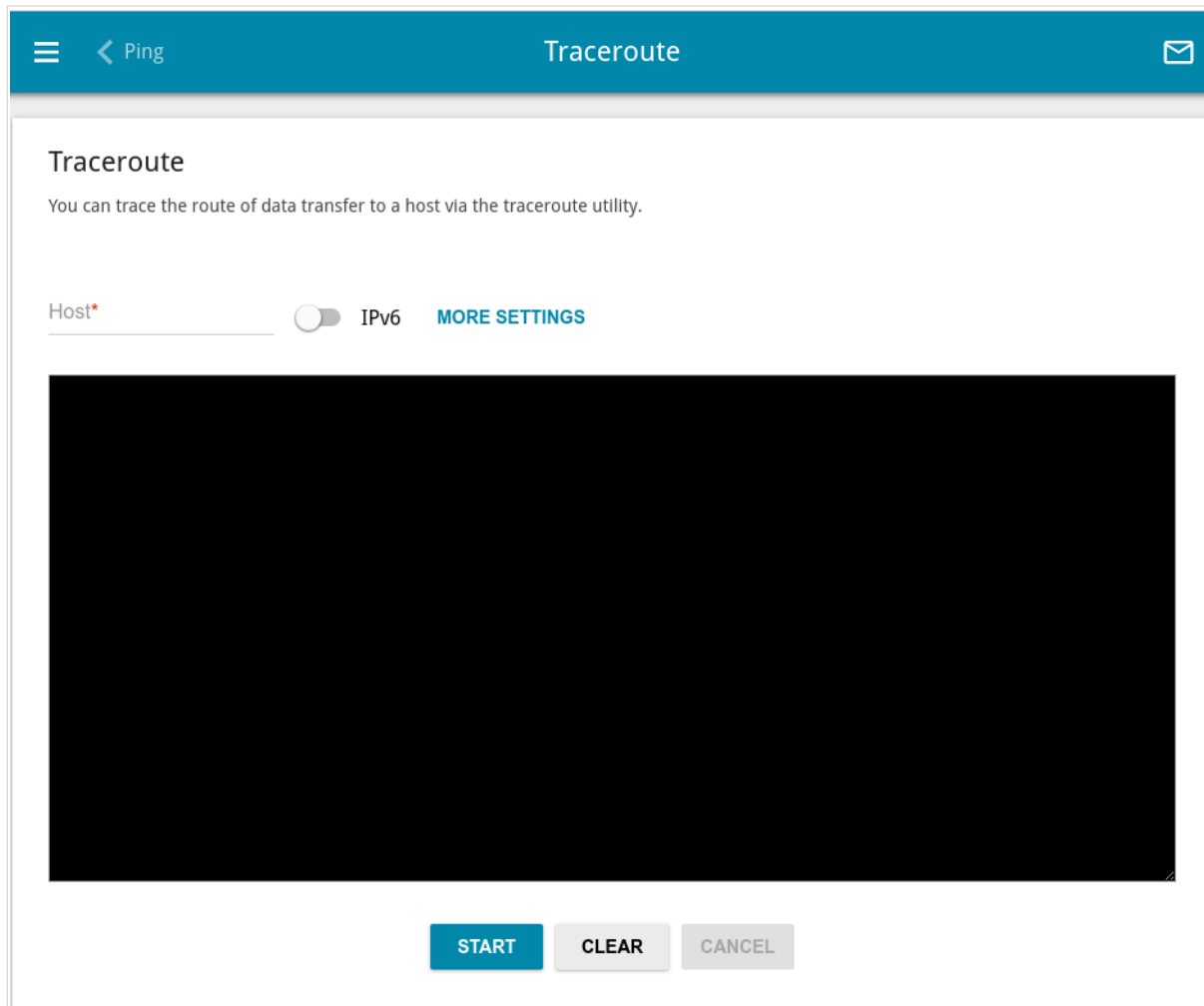
*Figure 190. The **System / Traceroute** page.*

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

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

*Figure 191. 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.
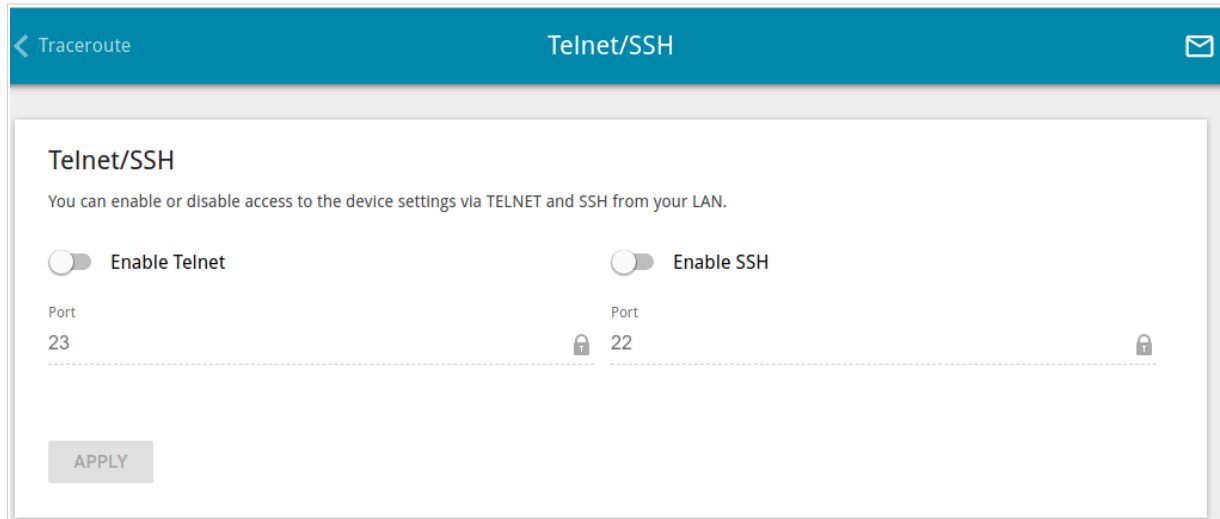
*Figure 192. The **System / Telnet/SSH** page.*

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.
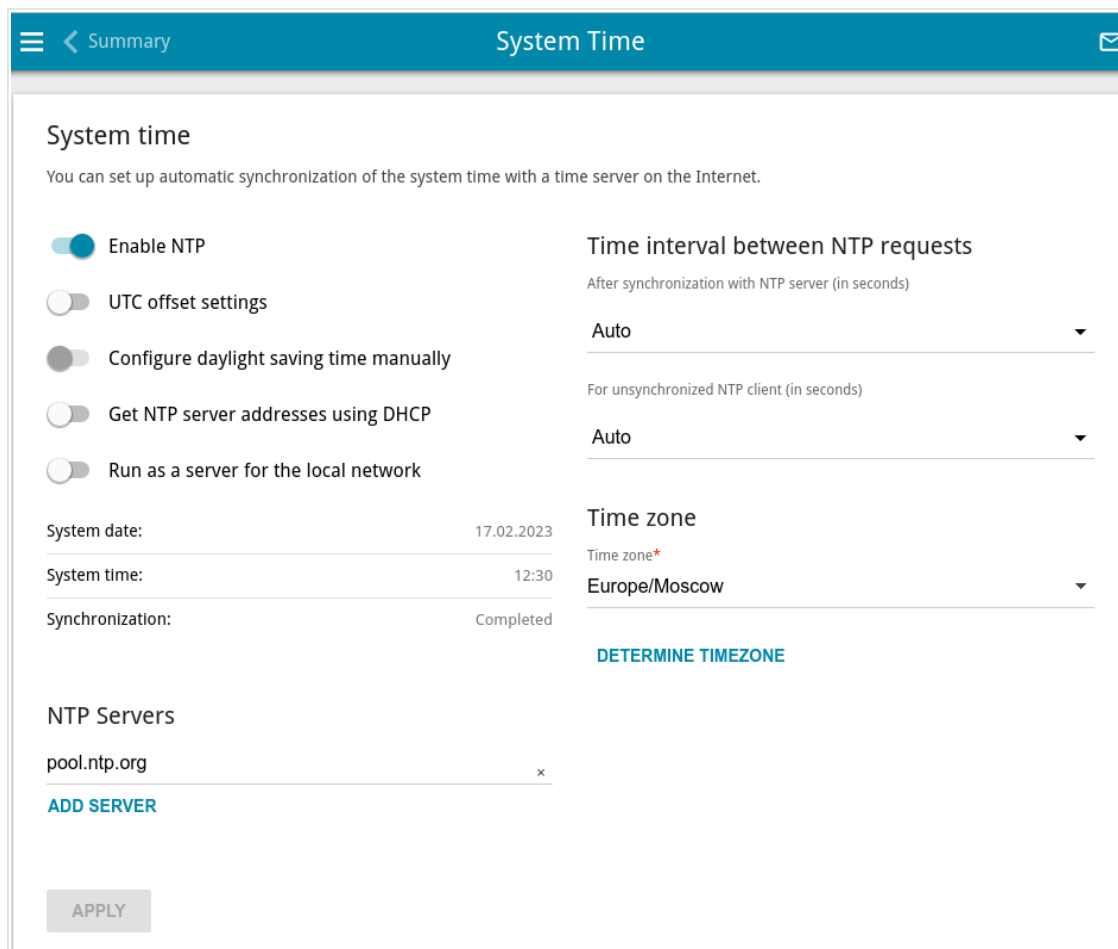
*Figure 193. The **System / System Time** page.*

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. Obtained addresses will be displayed in the **NTP Servers** section. Contact your ISP to clarify if this setting needs to be enabled. If the switch is moved to the right, settings of the **NTP Servers** section are unavailable.
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.
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: DIR-X1860 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 194. 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 address or full domain name 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.
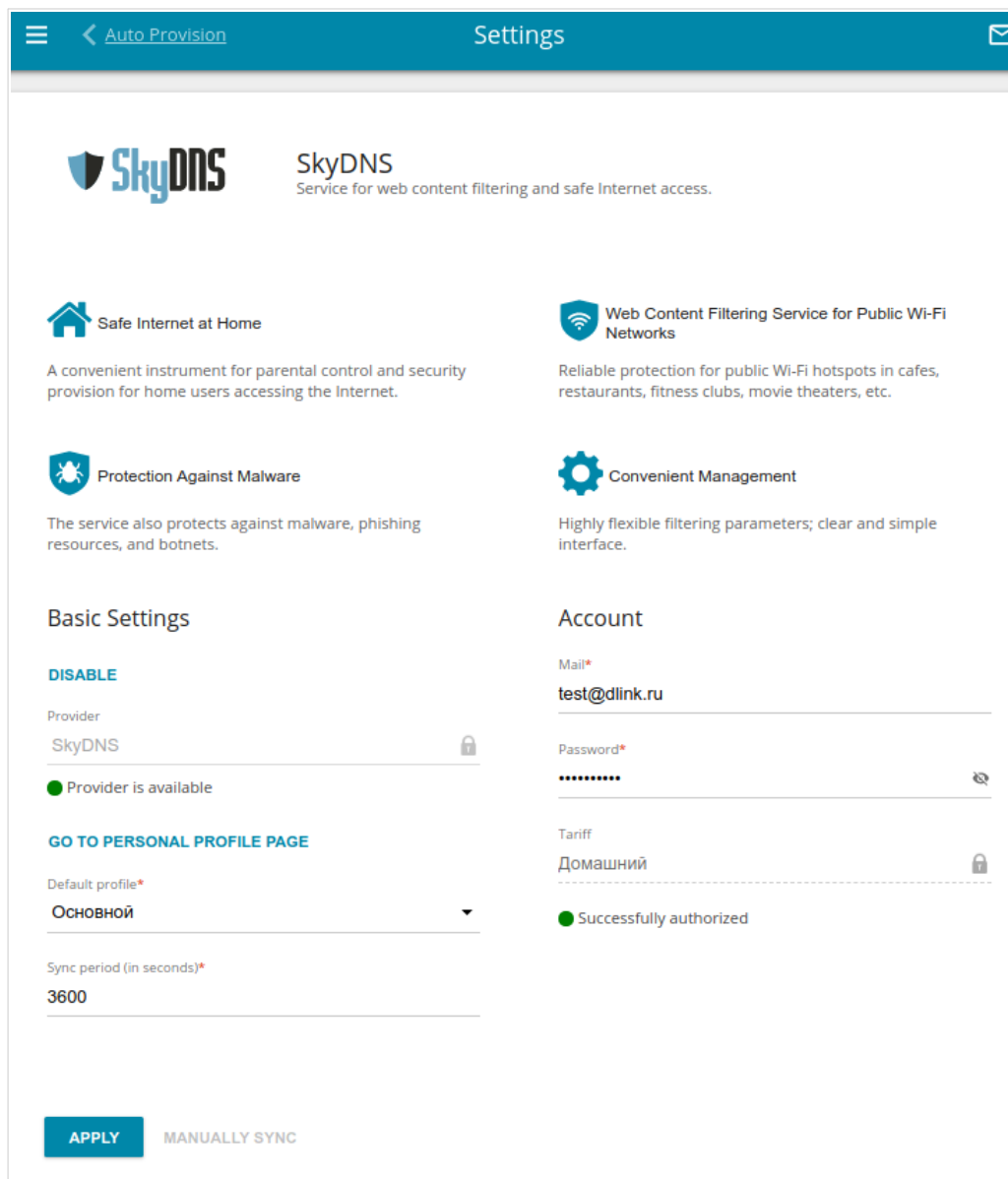
*Figure 195. The **SkyDNS / Settings** page.*

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.
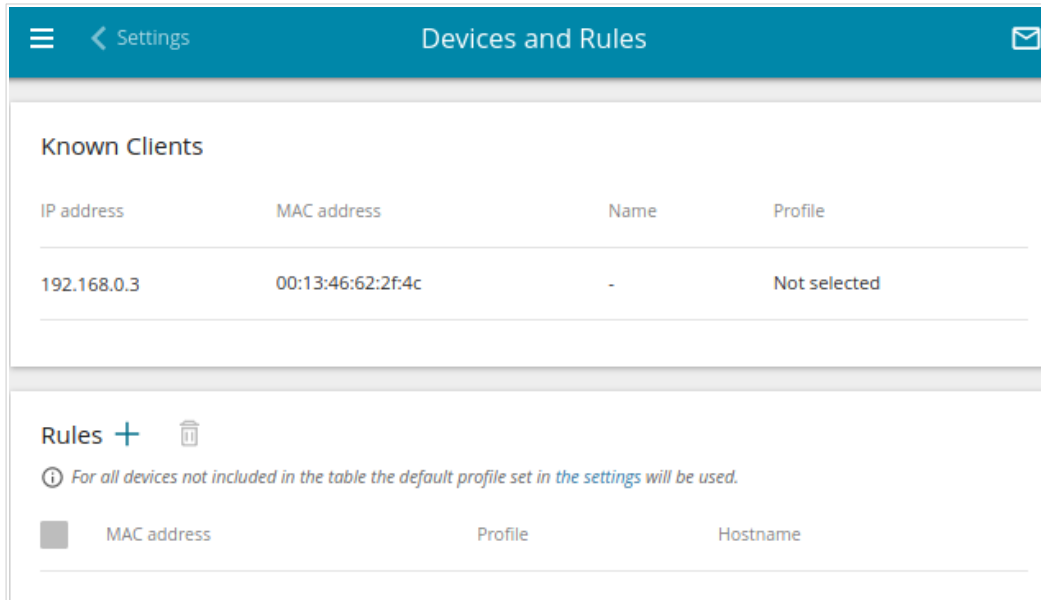
*Figure 196. The **SkyDNS / Devices and Rules** page.*

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.
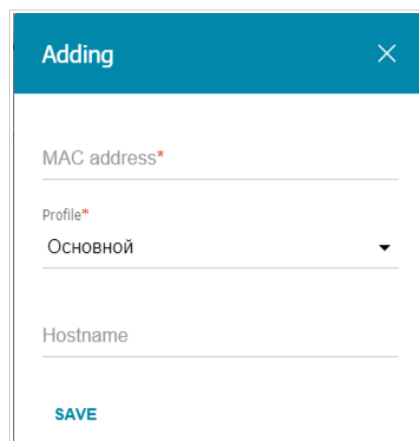
*Figure 197. The **SkyDNS / Devices and Rules** page. The window for adding a rule.*

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

Terms and Conditions for Installation, Safe Operation, Storage, Transportation, and Disposal

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 (reception/transmission of data in computer networks); installation should be performed in accordance with the documents available on the official website.

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. The electrical outlet must be installed near the equipment and must be easily accessible.

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 device may be stored and transported only in the original packaging at the temperature and humidity indicated in the specifications. No restrictions apply to sales. Please contact an authorized distributor to dispose of the equipment upon the end of its operation.

The service life of the device is 2 years.

The warranty period starts on the date of purchase from an authorized distributor within Russia or the CIS countries and extends for one year.

Irrespective of the date of purchase, the warranty period cannot exceed 2 years from the date of manufacture, which is determined by 6th (year) and 7th (month) digit in the serial number printed on the device label.

Year: G – 2016, H – 2017, I – 2018, J – 2019, 0 – 2020, 1 – 2021, 2 – 2022, 3 – 2023, 4 – 2024, 5 – 2025.

Month: 1 – January, 2 – February, ..., 9 – September, A – October, B – November, C – December.

If a fault is detected, please contact D-Link service center or technical support group.

Wireless Installation Considerations

The DIR-X1860 device lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF noise in your home or office. To maximize your wireless range, follow the guidelines below.

1. Keep the number of walls and ceilings between the DIR-X1860 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
CoS	Class of Service
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
MPU	Maximum Packet Unit
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
PCP	Port Control Protocol
PFS	Perfect Forward Secrecy
PIN	Personal Identification Number
PMP	Port Mapping Protocol
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
TLS	Transport Layer Security
ToS	Type of Service
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