



DIR-841

AC1200 MU-MIMO Wi-Fi Gigabit Router with Fast Ethernet LAN Ports

Contents

Chapter 1. Introduction.....	5
Contents and Audience.....	5
Conventions.....	5
Document Structure.....	5
Chapter 2. Overview.....	6
General Information.....	6
Specifications*.....	8
Product Appearance.....	14
Upper Panel.....	14
Back and Bottom Panels.....	16
Delivery Package.....	18
Chapter 3. Installation and Connection.....	19
Before You Begin.....	19
Connecting to PC.....	20
PC with Ethernet Adapter.....	20
Obtaining IP Address Automatically (OS Windows 7).....	21
PC with Wi-Fi Adapter.....	26
Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 7).....	26
Connecting to Web-based Interface.....	29
Web-based Interface Structure.....	31
Summary Page.....	31
Home Page.....	33
Menu Sections.....	34
Notifications.....	35
Chapter 4. Configuring via Web-based Interface.....	36
Initial Configuration Wizard.....	36
Selecting Operation Mode.....	38
Changing LAN IPv4 Address.....	41
Wi-Fi Client.....	42
Configuring WAN Connection.....	44
Static IPv4 Connection.....	45
Static IPv6 Connection.....	46
PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections.....	47
PPPoE + Static IP (PPPoE Dual Access) Connection.....	48
PPTP + Dynamic IP or L2TP + Dynamic IP Connection.....	49
PPTP + Static IP or L2TP + Static IP Connection.....	50
Configuring Wireless Network.....	51
Configuring LAN Ports for IPTV/VoIP.....	53
Changing Web-based Interface Password.....	55
Connection of Multimedia Devices.....	57
Statistics.....	60
Network Statistics.....	60
DHCP.....	61
Routing Table.....	62
Clients and Session.....	63
Port Statistics.....	64
Multicast Groups.....	65

Connections Setup	66
WAN	66
<i>Creating Dynamic IPv4 or Static IPv4 WAN Connection</i>	68
<i>Creating Dynamic IPv6 or Static IPv6 WAN Connection</i>	73
<i>Creating PPPoE WAN Connection</i>	77
<i>Creating PPTP or L2TP WAN Connection</i>	82
<i>Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection</i>	86
LAN	92
IPv4	92
IPv6	95
WAN Reservation	98
Wi-Fi	100
Basic Settings	100
Client Management	108
WPS	109
<i>Using WPS Function via Web-based Interface</i>	111
<i>Using WPS Function without Web-based Interface</i>	112
WMM	113
Client	116
Client Shaping	119
Additional	121
MAC Filter	124
Roaming	127
Advanced	129
VLAN	130
DNS	132
DDNS	134
Ports Settings	136
Bandwidth Control	139
Redirect	140
Routing	141
TR-069 Client	143
Remote Access	145
UPnP IGD	147
UDPXY	148
IGMP/MLD	150
ALG/Passthrough	152
IPsec	154
Firewall	160
IP Filter	160
Virtual Servers	164
DMZ	167
MAC Filter	168
URL Filter	170
DoS Protection	172

System.....	175
Configuration.....	176
Firmware Update.....	178
<i>Local Update.....</i>	<i>179</i>
<i>Remote Update.....</i>	<i>180</i>
Log.....	181
Ping.....	183
Traceroute.....	185
Telnet.....	187
System Time.....	188
Yandex.DNS.....	190
Settings.....	190
Devices and Rules.....	192
Chapter 5. Operation Guidelines.....	194
Safety Rules and Conditions.....	194
Wireless Installation Considerations.....	195
Chapter 6. Abbreviations and Acronyms.....	196


CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DIR-841 and explains how to configure and operate it.

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

Conventions

Example	Description
text	The body text of the manual.
<i>Before You Begin</i>	A reference to a chapter or section of this manual.
<i>“Quick Installation Guide”</i>	A reference to a document.
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.
 <u>Information</u>	An important note.

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the router DIR-841 and configure a PC in order to access its web-based interface.

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

Chapter 5 includes safety instructions and tips for networking.

Chapter 6 introduces abbreviations and acronyms used in this manual.

CHAPTER 2. OVERVIEW

General Information

The DIR-841 device is a wireless dual band router with a built-in 4-port switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

You are able to connect the wireless router DIR-841 to a cable or DSL modem or to a private Ethernet line and use a high-speed Internet connection to successfully fulfill a wide range of professional tasks. The built-in 4-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network.

Using the DIR-841 device, you are able to quickly create a high-speed wireless network at home or in your office, which lets computers and mobile devices access the Internet virtually anywhere (within the operational range of your wireless network). Simultaneous activity of 2.4GHz band and 5GHz band allows performing a wide range of tasks. The router can operate as a base station for connecting wireless devices of the standards 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac (at the wireless connection rate up to 1167Mbps¹).

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

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

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

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

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

The wireless router DIR-841 includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

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

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

You can configure the settings of the wireless router DIR-841 via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

¹ Up to 300Mbps for 2.4GHz and up to 867Mbps for 5GHz.

The configuration wizard allows you to quickly switch DIR-841 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-841 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	<ul style="list-style-type: none">· RTL8197H (1GHz)
RAM	<ul style="list-style-type: none">· 64MB, DDR2, built in processor
Flash	<ul style="list-style-type: none">· 8MB, SPI
Interfaces	<ul style="list-style-type: none">· 10/100/1000BASE-T WAN port· 4 10/100BASE-TX LAN ports
LEDs	<ul style="list-style-type: none">· Power· Internet· 4 LAN LEDs· WLAN 2.4G· WLAN 5G· WPS
Buttons	<ul style="list-style-type: none">· POWER button to power on/power off· WIFI button to enable/disable wireless network· WPS button to set up wireless connection· RESET button to restore factory default settings
Antenna	<ul style="list-style-type: none">· Four external non-detachable antennas (5dBi gain)
MIMO	<ul style="list-style-type: none">· 2 x 2, MU-MIMO
Power connector	<ul style="list-style-type: none">· Power input connector (DC)

Software	
WAN connection types	<ul style="list-style-type: none">· 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

* 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	<ul style="list-style-type: none"> • Support of IEEE 802.1X for Internet connection • DHCP server/relay • Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation • Automatic obtainment of LAN IP address (for access point/repeater/client modes) • DNS relay • Dynamic DNS • Static IP routing • Static IPv6 routing • IGMP Proxy • MLD Proxy • RIP • Support of UPnP IGD • Support of VLAN • WAN ping respond • Support of SIP ALG • Support of RTSP • WAN reservation • Autonegotiation of speed, duplex mode, and flow control/Manual speed and duplex mode setup for each Ethernet port • Setup of maximum TX rate for each port of the router • Built-in UDPXY application
Firewall functions	<ul style="list-style-type: none"> • Network Address Translation (NAT) • Stateful Packet Inspection (SPI) • IP filter • IPv6 filter • MAC filter • URL filter • DMZ • Prevention of ARP and DDoS attacks • Virtual servers • Built-in Yandex.DNS web content filtering service
VPN	<ul style="list-style-type: none"> • IPsec/PPTP/L2TP/PPPoE pass-through • IPsec tunnels
Management	<ul style="list-style-type: none"> • Local and remote access to settings through TELNET/WEB (HTTP/HTTPS) • Bilingual web-based interface for configuration and management (Russian/English) • Support of 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

Wireless Module Parameters	
Standards	<ul style="list-style-type: none"> • IEEE 802.11a/n/ac • IEEE 802.11b/g/n
Frequency range	<ul style="list-style-type: none"> • 2400 ~ 2483.5MHz • 5150 ~ 5350MHz • 5650 ~ 5725MHz

Wireless Module Parameters	
Wireless connection security	<ul style="list-style-type: none">• WEP• WPA/WPA2 (Personal/Enterprise)• MAC filter• WPS (PBC/PIN)
Advanced functions	<ul style="list-style-type: none">• Support of client mode• WMM (Wi-Fi QoS)• Information on connected Wi-Fi clients• Advanced settings• Smart adjustment of Wi-Fi clients• Guest Wi-Fi / support of MBSSID• Rate limitation for wireless network/separate MAC addresses• Periodic scan of channels, automatic switch to least loaded channel• Support of 802.11ac (5GHz) and 802.11n (2.4GHz) TX Beamforming• Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence)
Wireless connection rate	<ul style="list-style-type: none">• 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): from 6.5 to 300Mbps (MCS0–MCS15)• IEEE 802.11n (5GHz): from 6.5 to 300Mbps (from MCS0 to MCS15)• IEEE 802.11ac (5GHz): from 6.5 to 867Mbps (from MCS0 to MCS9)

Wireless Module Parameters

Transmitter output power

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

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

Wireless Module Parameters

Receiver sensitivity

- 802.11a (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C)
-82dBm at 6Mbps
-81dBm at 9Mbps
-79dBm at 12Mbps
-77dBm at 18Mbps
-74dBm at 24Mbps
-70dBm at 36Mbps
-66dBm at 48Mbps
-65dBm at 54Mbps
- 802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C)
-80dBm at 1Mbps
-80dBm at 2Mbps
-76dBm at 5.5Mbps
-76dBm at 11Mbps
- 802.11g (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C)
-82dBm at 6Mbps
-81dBm at 9Mbps
-79dBm at 12Mbps
-77dBm at 18Mbps
-74dBm at 24Mbps
-70dBm at 36Mbps
-66dBm at 48Mbps
-65dBm at 54Mbps
- 802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C)
2.4GHz, HT20
-82dBm at MCS0
-79dBm at MCS1
-77dBm at MCS2
-74dBm at MCS3
-70dBm at MCS4
-66dBm at MCS5
-65dBm at MCS6
-64dBm at MCS7
2.4GHz, HT40
-79dBm at MCS0
-76dBm at MCS1
-74dBm at MCS2
-71dBm at MCS3
-67dBm at MCS4
-63dBm at MCS5
-62dBm at MCS6
-61dBm at MCS7
5GHz, HT20
-82dBm at MCS0
-79dBm at MCS1
-77dBm at MCS2
-74dBm at MCS3
-70dBm at MCS4
-66dBm at MCS5
-65dBm at MCS6
-64dBm at MCS7
5GHz, HT40
-79dBm at MCS0
-76dBm at MCS1
-74dBm at MCS2
-71dBm at MCS3
-67dBm at MCS4
-63dBm at MCS5
-62dBm at MCS6
-61dBm at MCS7

Wireless Module Parameters

	<ul style="list-style-type: none"> 802.11ac (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) HT20 -82dBm at MCS0 -79dBm at MCS1 -77dBm at MCS2 -74dBm at MCS3 -70dBm at MCS4 -66dBm at MCS5 -65dBm at MCS6 -64dBm at MCS7 -56dBm at MCS8 HT40 -79dBm at MCS0 -76dBm at MCS1 -74dBm at MCS2 -71dBm at MCS3 -67dBm at MCS4 -63dBm at MCS5 -62dBm at MCS6 -61dBm at MCS7 -56dBm at MCS8 -54dBm at MCS9 HT80 -76dBm at MCS0 -73dBm at MCS1 -71dBm at MCS2 -68dBm at MCS3 -64dBm at MCS4 -60dBm at MCS5 -59dBm at MCS6 -58dBm at MCS7 -53dBm at MCS8 -51dBm at MCS9
Modulation schemes	<ul style="list-style-type: none"> 802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM 802.11b: DQPSK, DBPSK, DSSS, CCK 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM 802.11ac: BPSK, QPSK, 16QAM, 64QAM, up to 256QAM with OFDM

Physical Parameters

Dimensions (L x W x H)	<ul style="list-style-type: none"> 205 x 136 x 33 mm (8.07 x 5.35 x 1.3 in)
-------------------------------	--

Operating Environment

Power	<ul style="list-style-type: none"> Output: 12V DC, 1A
Temperature	<ul style="list-style-type: none"> Operating: from 0 to 40 °C Storage: from -20 to 65 °C
Humidity	<ul style="list-style-type: none"> 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	<i>Solid green</i>	The router is powered on.
	<i>No light</i>	The router is powered off.
Internet	<i>Solid green</i>	The cable is connected to the port.
	<i>Blinking green</i>	Data transfer through the WAN port.
	<i>No light</i>	The cable is not connected.

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

Back and Bottom Panels



Figure 2. Back panel view.

Port	Description
WIFI	A button to enable/disable wireless network. To disable the router's wireless network: with the device turned on, press the button and release. The WLAN 2.4G and WLAN 5G LEDs should turn off.
WPS	A button to set up wireless connection (the WPS function). To use the WPS function: with the device turned on, push the button, hold it for 2 seconds, and release. The WPS LED should start blinking.
LAN 1-4	4 Ethernet ports to connect computers or network devices.
WAN	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).

Port	Description
POWER	A button to turn the router on/off.

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

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

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

Delivery Package

The following should be included:

- Router DIR-841
- 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.

Operating System

Configuration of the wireless dual band router with a built-in 4-port switch DIR-841 (hereinafter referred to as “the router”) is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

Web Browser

The following web browsers are recommended:

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

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

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

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

Wireless Connection

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

Connecting to PC

PC with Ethernet Adapter

1. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
2. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
3. Turn on the router by pressing the **POWER** button on its back panel.

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

Obtaining IP Address Automatically (OS Windows 7)

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

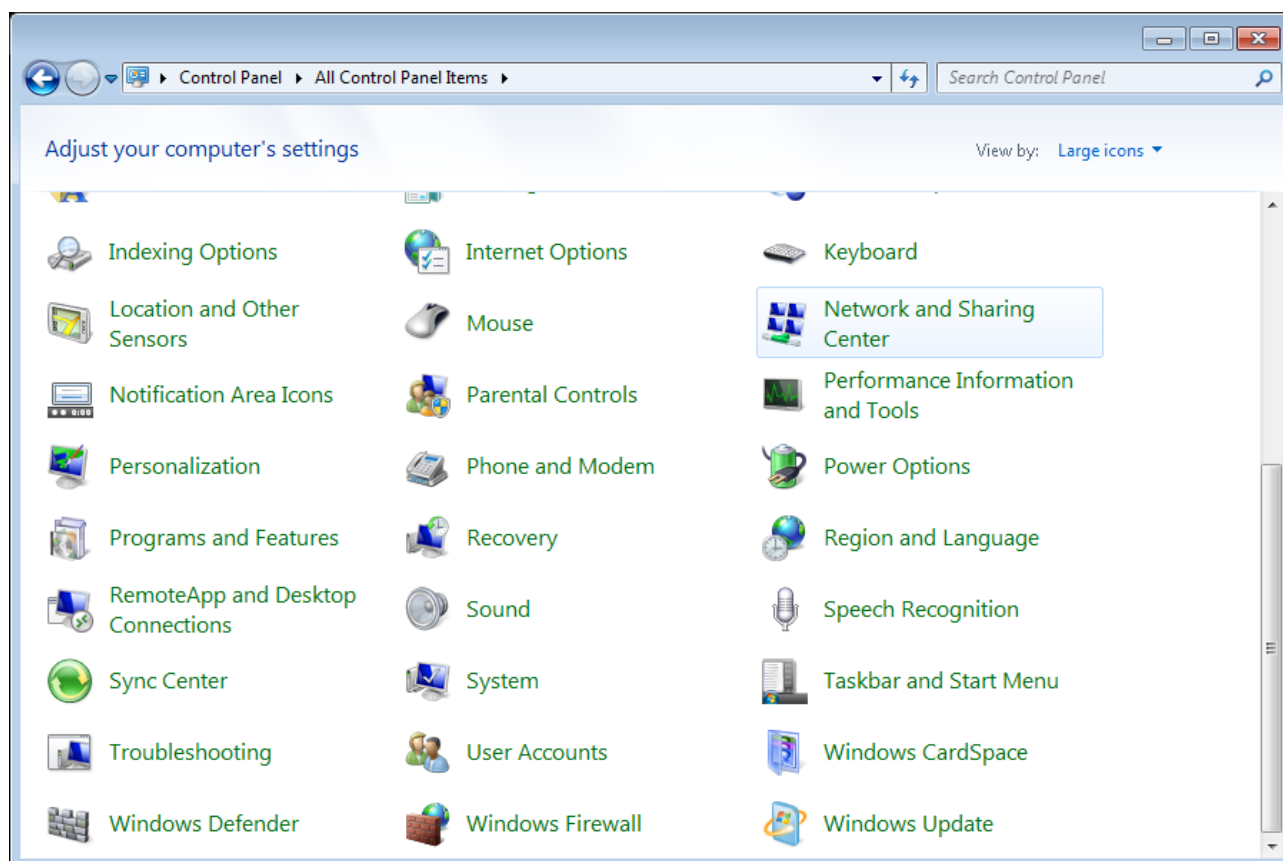


Figure 3. The **Control Panel** window.

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

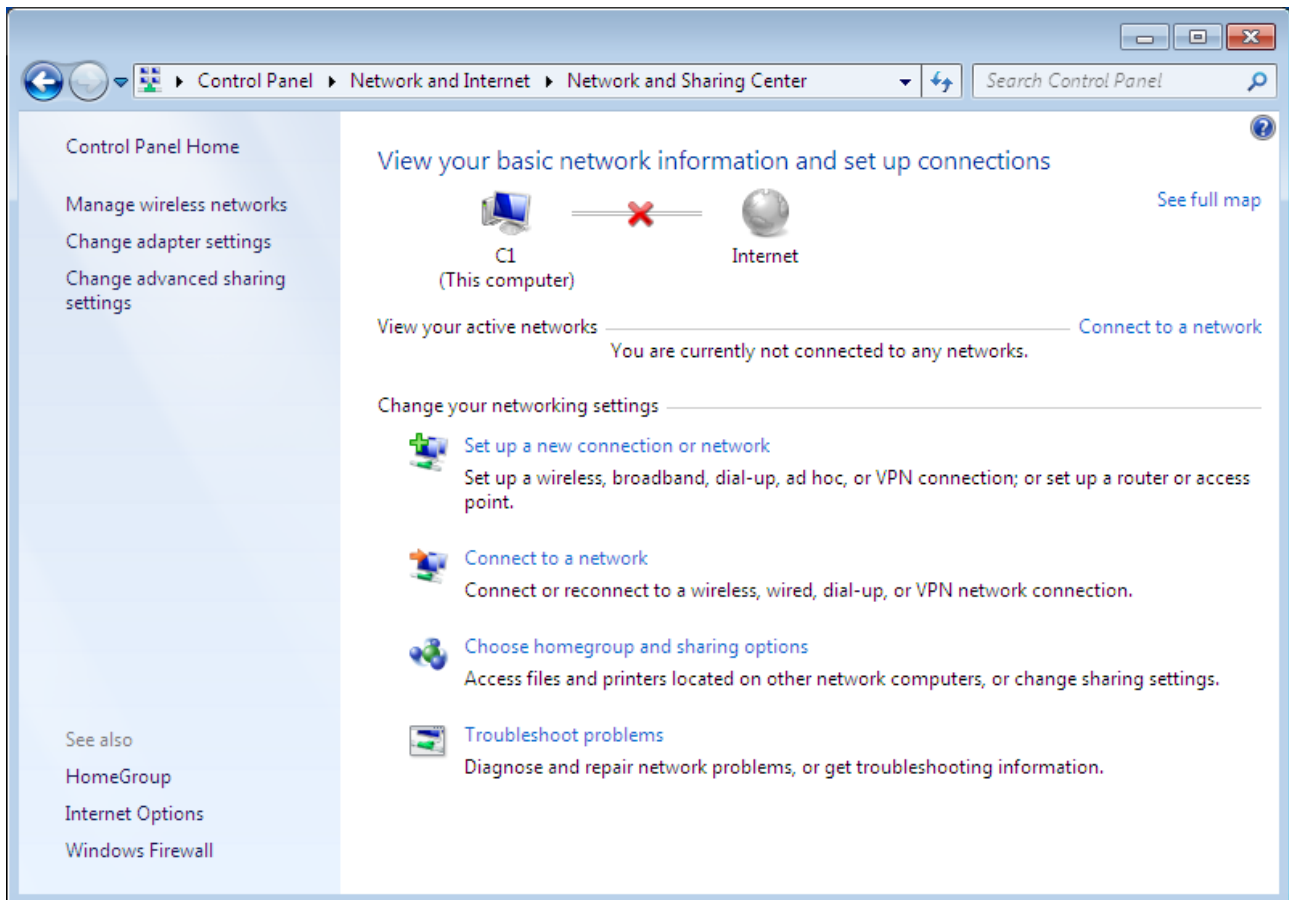


Figure 4. The **Network and Sharing Center** window.

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

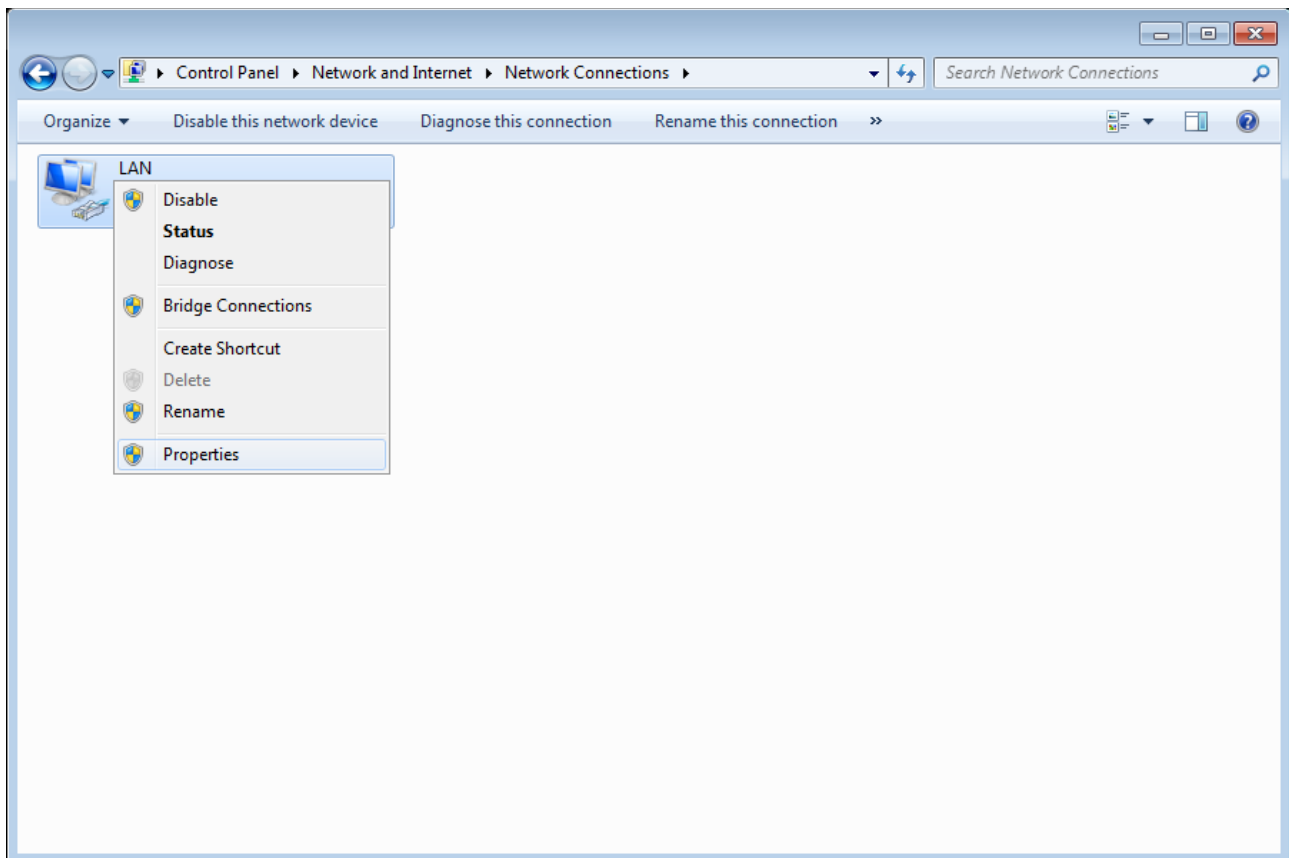


Figure 5. The **Network Connections** window.

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

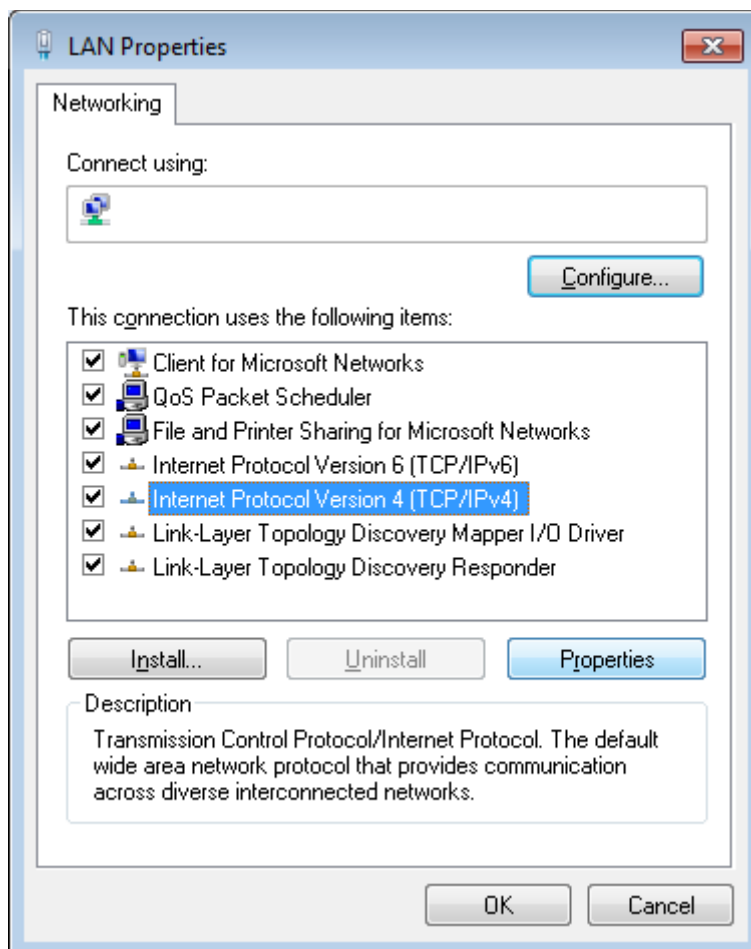


Figure 6. The **Local Area Connection Properties** window.

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

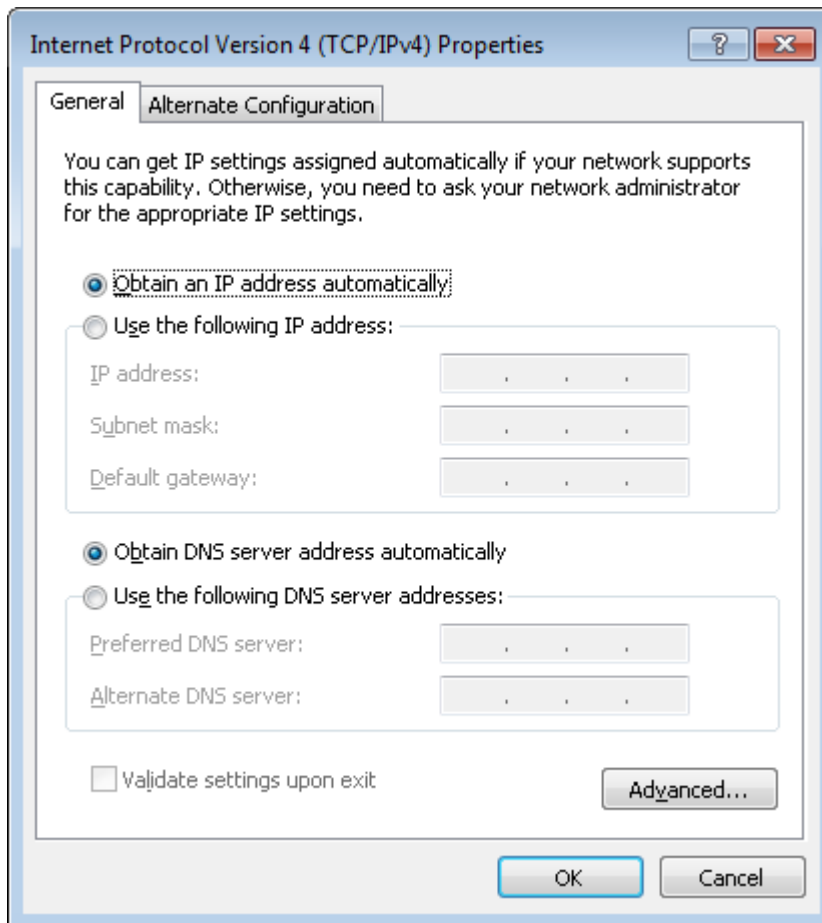


Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

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.)

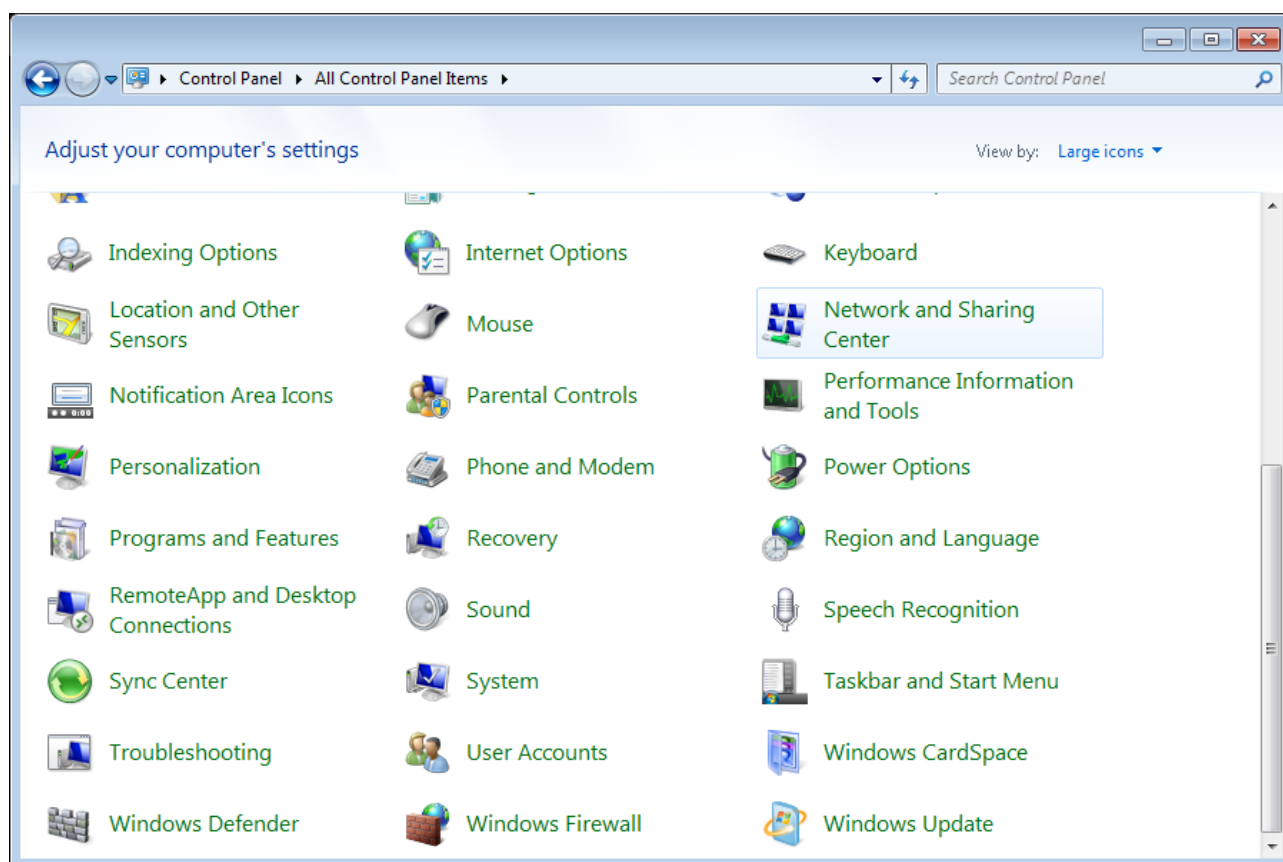


Figure 8. The **Control Panel** window.

3. In the menu located on the left part of the window, select the **Change adapter settings** line.
4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.
5. In the **Wireless Network Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.
6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.

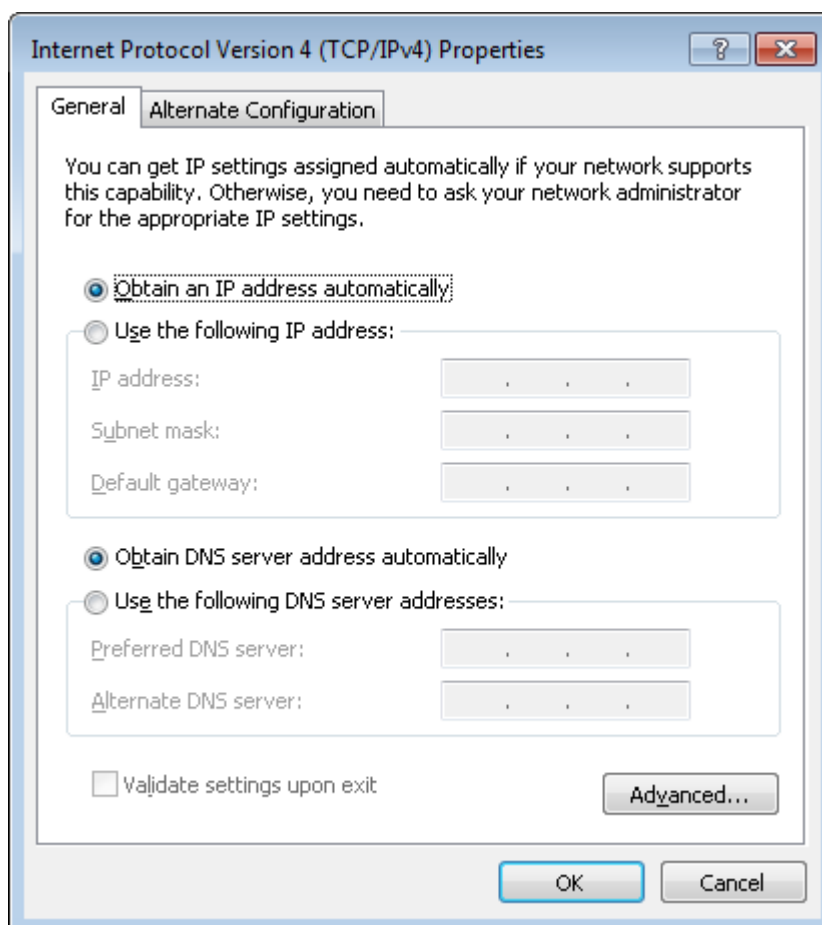


Figure 9. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

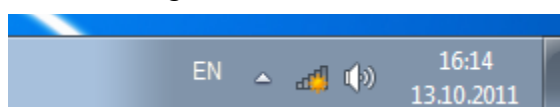


Figure 10. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network **DIR-841** (for operating in the 2.4GHz band) or **DIR-841-5G** (for operating in the 5GHz band) and click the **Connect** button.

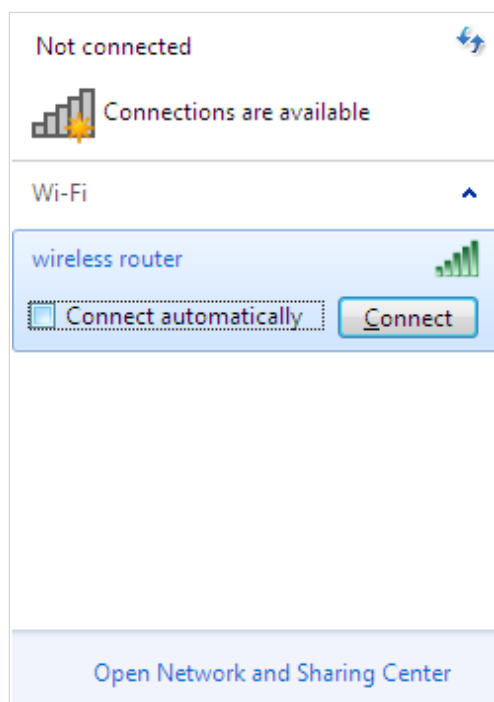


Figure 11. The list of available networks.

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.

Connecting to Web-based Interface

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

! For security reasons, DIR-841 with default settings cannot connect to the Internet. To get started, please set your own password used to access the web-based interface and, if needed, configure other settings recommended by your ISP.

Start a web browser (see the **Before You Begin** section, page 19). In the address bar of the web browser, enter the domain name of the router (by default, **dlinkrouter.local**) with a dot at the end and press the **Enter** key. Also you can enter the IP address of the device (by default, **192.168.0.1**).



Figure 12. Connecting to the web-based interface of the DIR-841 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 36).

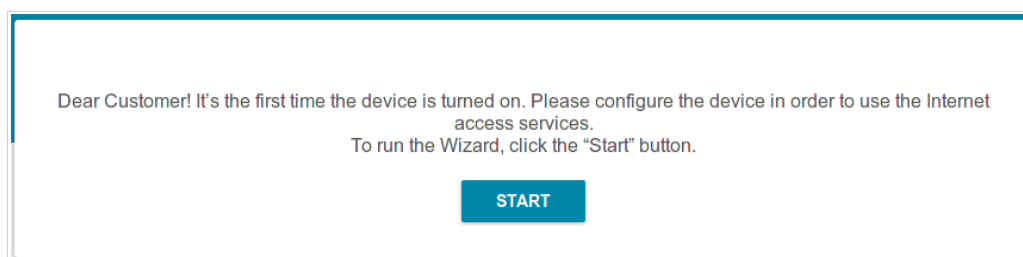


Figure 13. The page for running the Initial Configuration Wizard.

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

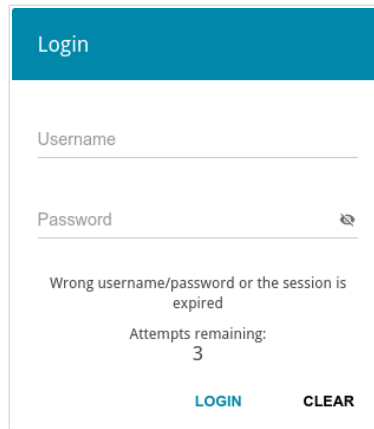


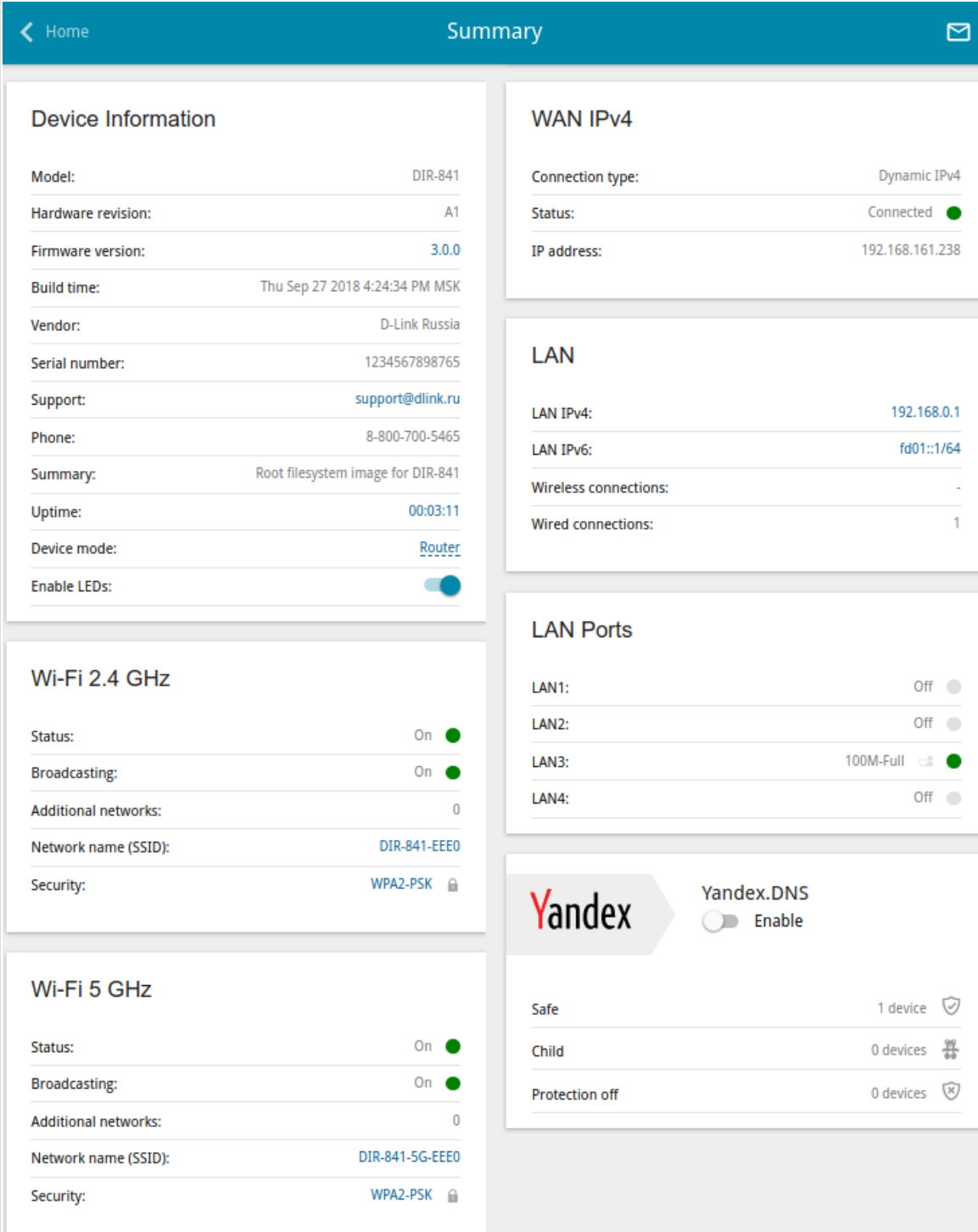
Figure 14. The login page.

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

Web-based Interface Structure

Summary Page

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



The screenshot displays the 'Summary' page of the DIR-841 web-based interface. The page is organized into several sections:

- Device Information:** Model: DIR-841, Hardware revision: A1, Firmware version: 3.0.0, Build time: Thu Sep 27 2018 4:24:34 PM MSK, Vendor: D-Link Russia, Serial number: 1234567898765, Support: support@dlink.ru, Phone: 8-800-700-5465, Summary: Root filesystem image for DIR-841, Uptime: 00:03:11, Device mode: Router, Enable LEDs: ☒.
- WAN IPv4:** Connection type: Dynamic IPv4, Status: Connected, IP address: 192.168.161.238.
- LAN:** LAN IPv4: 192.168.0.1, LAN IPv6: fd01::1/64, Wireless connections: 0, Wired connections: 1.
- LAN Ports:** LAN1: Off, LAN2: Off, LAN3: 100M-Full, LAN4: Off.
- Wi-Fi 2.4 GHz:** Status: On, Broadcasting: On, Additional networks: 0, Network name (SSID): DIR-841-EEEE, Security: WPA2-PSK.
- Wi-Fi 5 GHz:** Status: On, Broadcasting: On, Additional networks: 0, Network name (SSID): DIR-841-5G-EEEE, Security: WPA2-PSK.
- Yandex DNS:** Yandex logo, Yandex.DNS status: Off, Enable button, Safe: 1 device, Child: 0 devices, Protection off: 0 devices.

Figure 15. The summary page.

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

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

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **initial setup wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 36).

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

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

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

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

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

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

Home Page

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

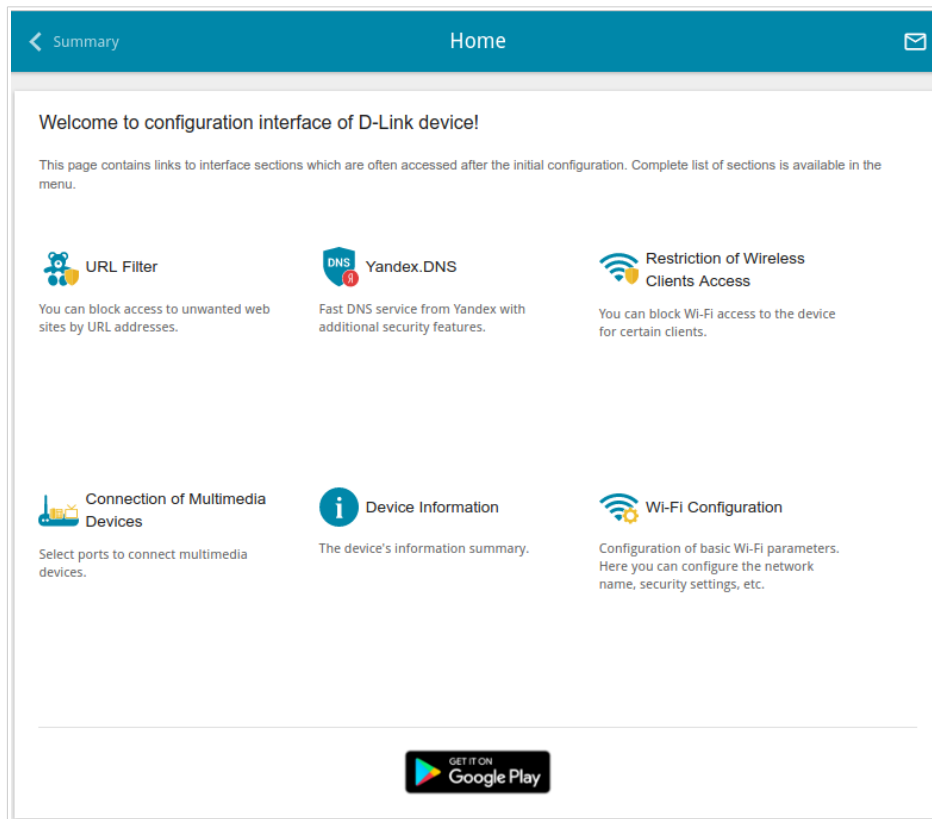


Figure 16. The **Home** page.

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

Menu Sections

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

In the **Initial Configuration** section you can run the Initial Configuration Wizard. The Wizard allows you to configure the router for operation in the needed mode and specify all parameters necessary for getting started (for the description of the Wizard, see the **Initial Configuration Wizard** section, page 36).

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 60).

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 66).

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 100).

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 129).

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 160).

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 175).

The pages of the **Yandex.DNS** section are designed for configuring the Yandex.DNS web content filtering service (for the description of the pages, see the **Yandex.DNS** section, page 190).

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

Notifications

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

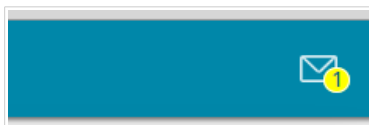


Figure 17. The web-based interface notifications.

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

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration Wizard

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

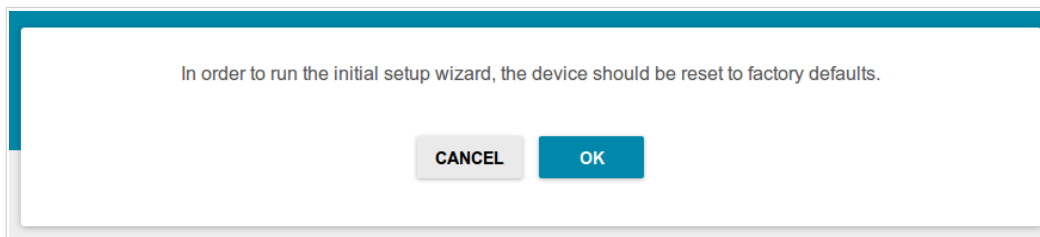


Figure 18. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network of DIR-841 (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

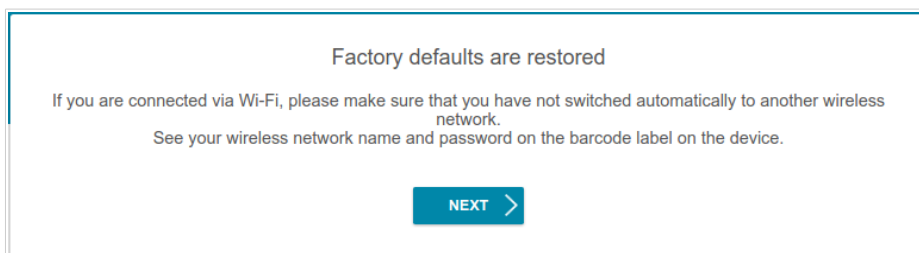


Figure 19. Checking connection to the wireless network.

Click the **START** button.

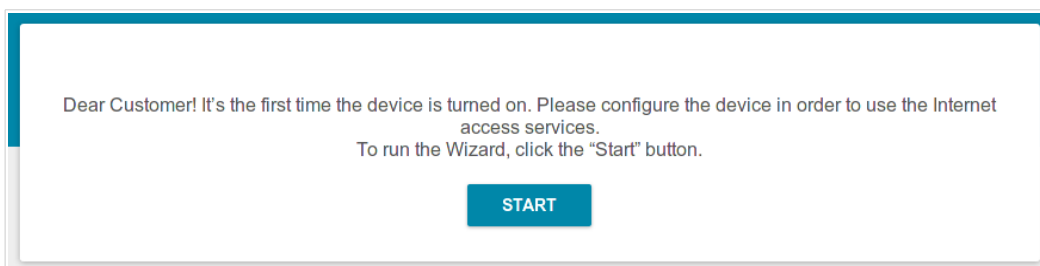


Figure 20. Starting the Wizard.

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

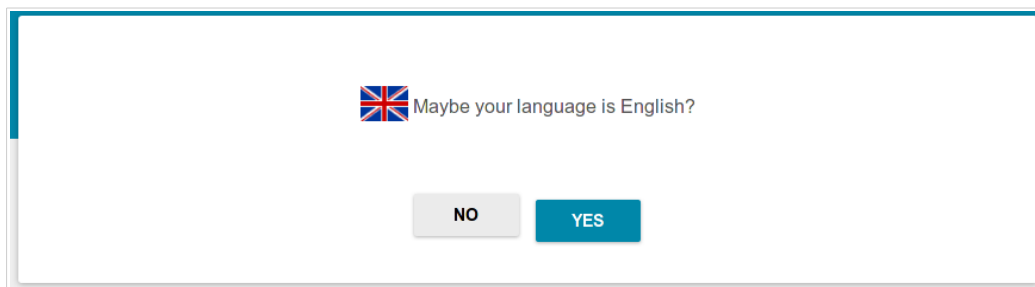


Figure 21. Selecting a language.

You can finish the wizard earlier and go to the menu of the web-based interface. To do this, click the **ADVANCED SETTINGS** button. On the opened page, change the default settings: specify the administrator password in the **Admin password** 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.

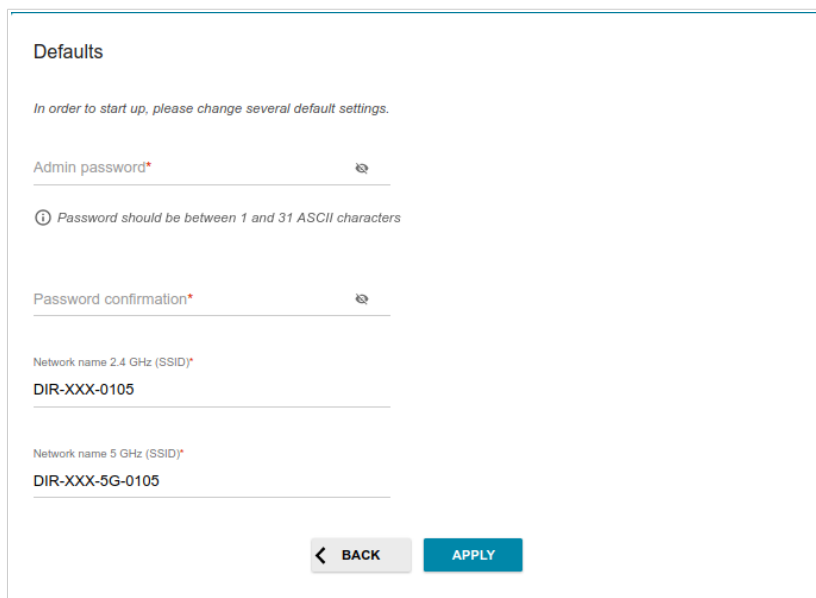
A screenshot of a web-based configuration page titled "Defaults". Below the title, there is a note: "In order to start up, please change several default settings." The page contains four input fields, each with a red asterisk indicating it is required. The first field is "Admin password*" with a password icon. Below it is a hint: "Password should be between 1 and 31 ASCII characters". The second field is "Password confirmation*" with a password icon. The third field is "Network name 2.4 GHz (SSID)*" with the value "DIR-XXX-0105". The fourth field is "Network name 5 GHz (SSID)*" with the value "DIR-XXX-5G-0105". At the bottom of the form, there are two buttons: a light gray button labeled "BACK" with a left arrow and a blue button labeled "APPLY".

Figure 22. Changing the default settings.

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

Selecting Operation Mode

In order to connect your device to a wired ISP, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Router** value. In this mode you can configure a WAN connection, set your own settings for the wireless network 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.

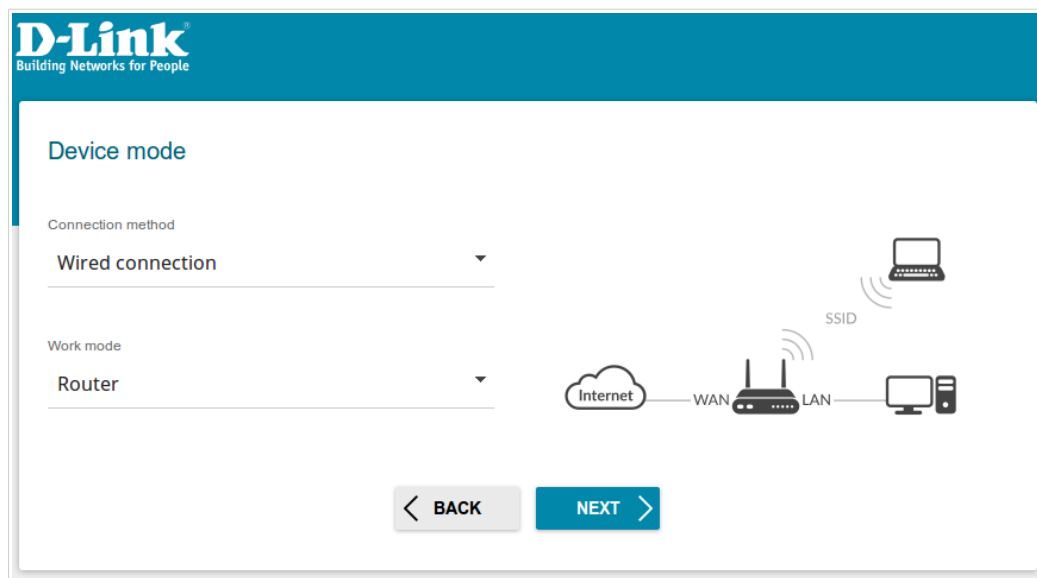


Figure 23. Selecting an operation mode. The **Router** mode.

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

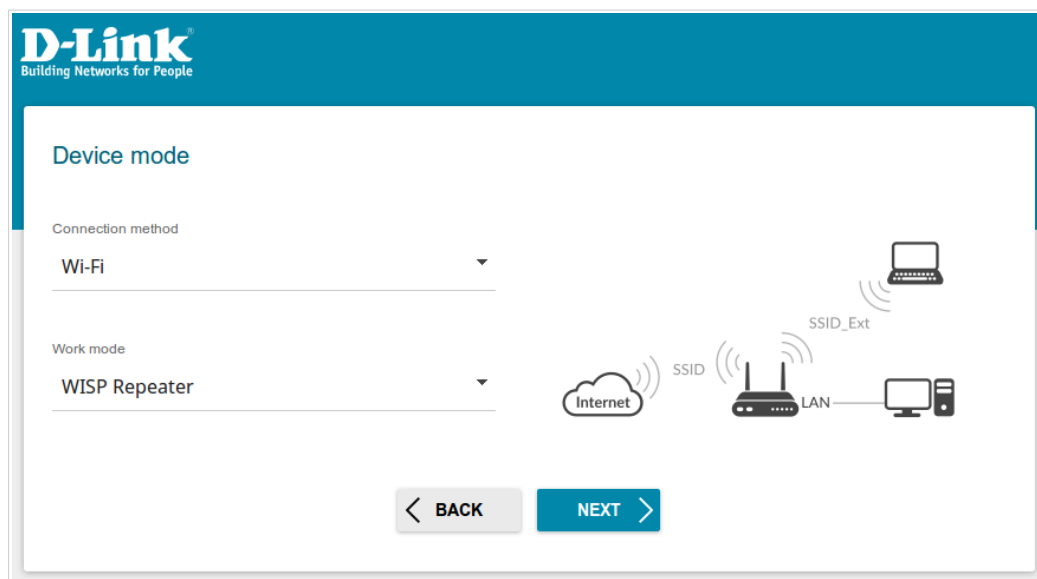


Figure 24. Selecting an operation mode. The **WISP Repeater** mode.

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

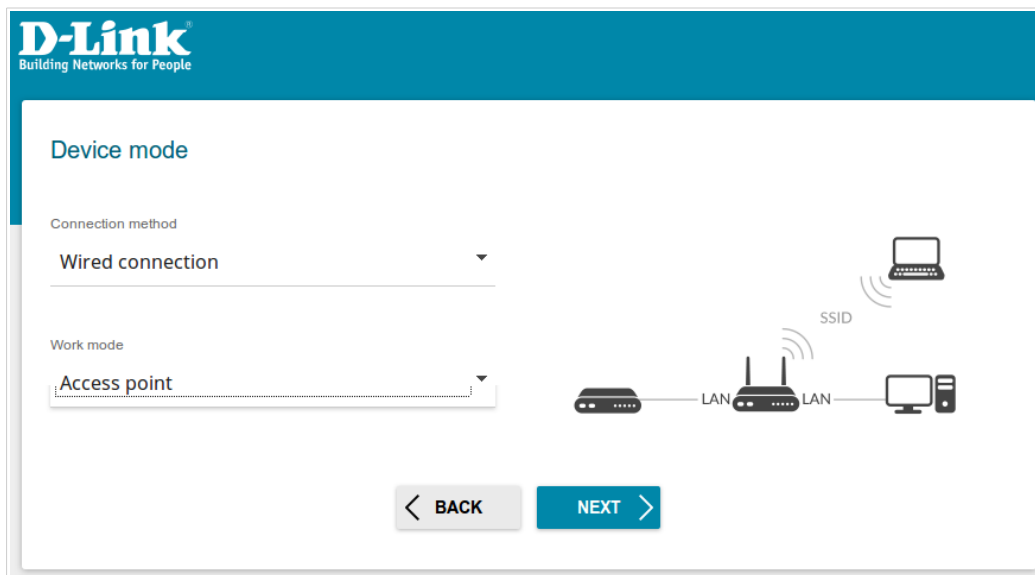


Figure 25. Selecting an operation mode. The **Access point** mode.

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

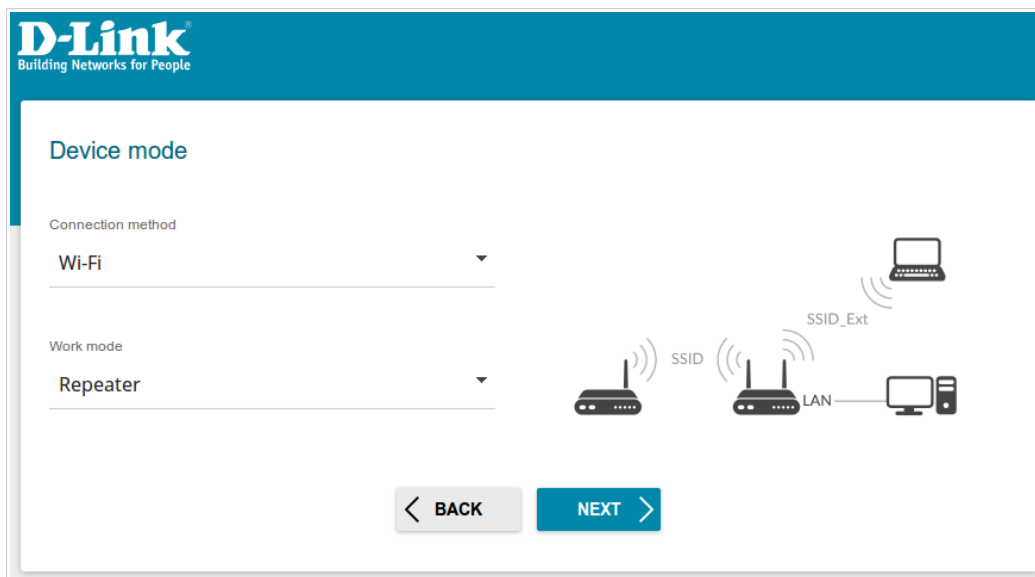


Figure 26. Selecting an operation mode. The **Repeater** mode.

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

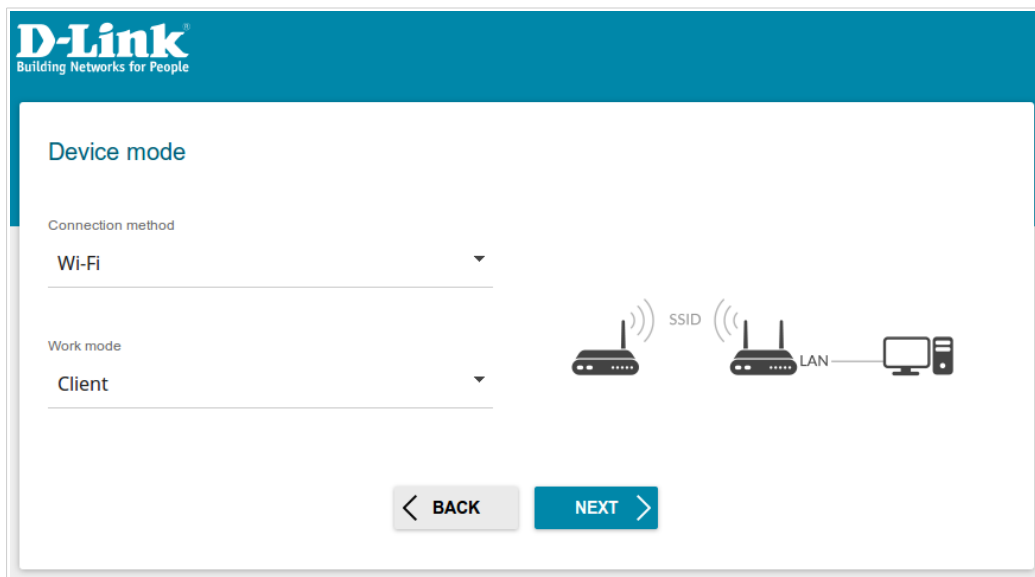


Figure 27. Selecting an operation mode. The **Client** mode.

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

Changing LAN IPv4 Address

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

1. Select the **Automatic obtainment of IPv4 address** to let DIR-841 automatically obtain the LAN IPv4 address.
2. In the **Device domain name** 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-841, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Netmask**, **Device domain name** fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.

LAN

☐ Automatic obtainment of IPv4 address

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

IP address*

192.168.0.1

Netmask*

255.255.255.0

Gateway IP address

Device domain name*

dlinkapEEEE.local

① Specify a domain name ending with .local. In order to access the web-based interface using the domain name, enter this name with a dot and slash at the end in the address bar of the web browser (for example, dlinkap12ab.local/)

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


Figure 28. The page for changing the LAN IPv4 address.


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

Wi-Fi Client

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

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

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

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

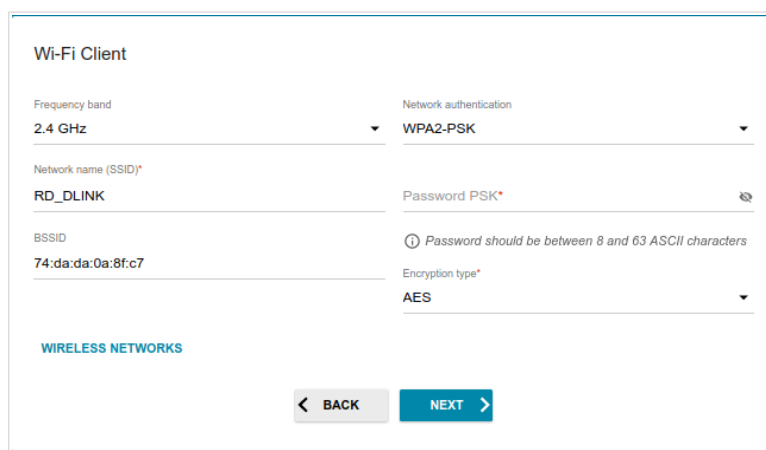



Figure 29. The page for configuring the Wi-Fi client.


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

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

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

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

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

Configuring WAN Connection

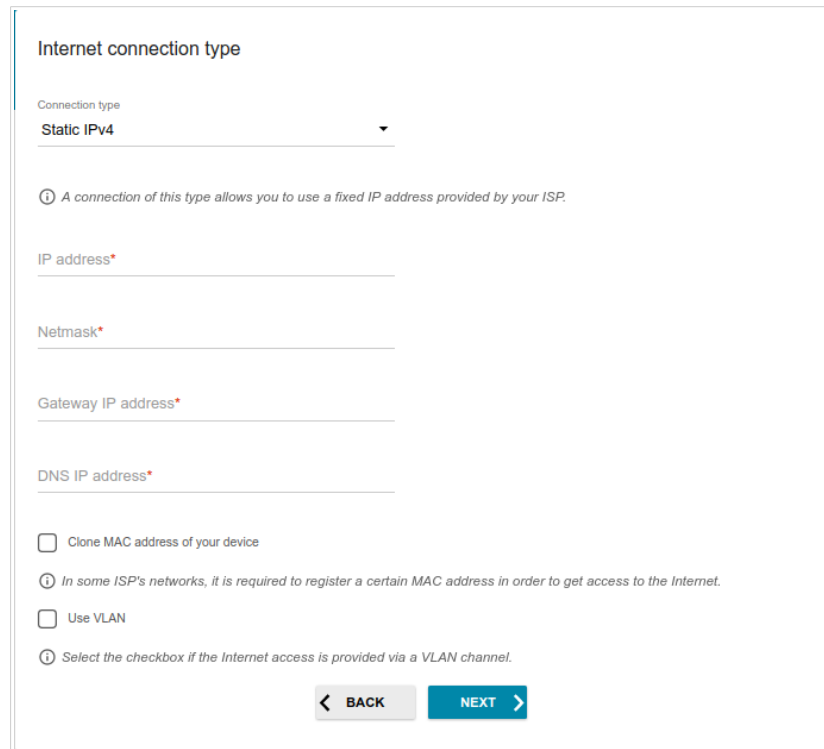
This configuration step is available for the **Router** and **WISP Repeater** modes.



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

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

Static IPv4 Connection

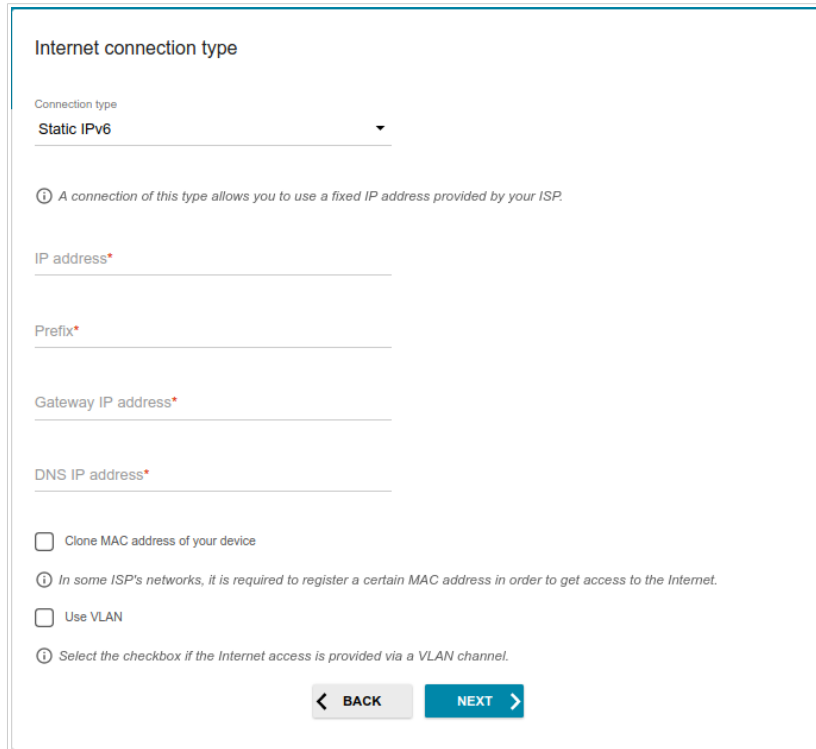


The screenshot shows the 'Internet connection type' configuration page. At the top, 'Connection type' is set to 'Static IPv4'. Below this, a note states: 'A connection of this type allows you to use a fixed IP address provided by your ISP.' There are four text input fields, each with a red asterisk indicating it is required: 'IP address*', 'Netmask*', 'Gateway IP address*', and 'DNS IP address*'. Below these fields are two checkboxes: 'Clone MAC address of your device' and 'Use VLAN'. A note below the checkboxes says: 'In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet.' and 'Select the checkbox if the Internet access is provided via a VLAN channel.' At the bottom right are 'BACK' and 'NEXT' buttons.

Figure 30. The page for configuring Static IPv4 WAN connection.

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

Static IPv6 Connection

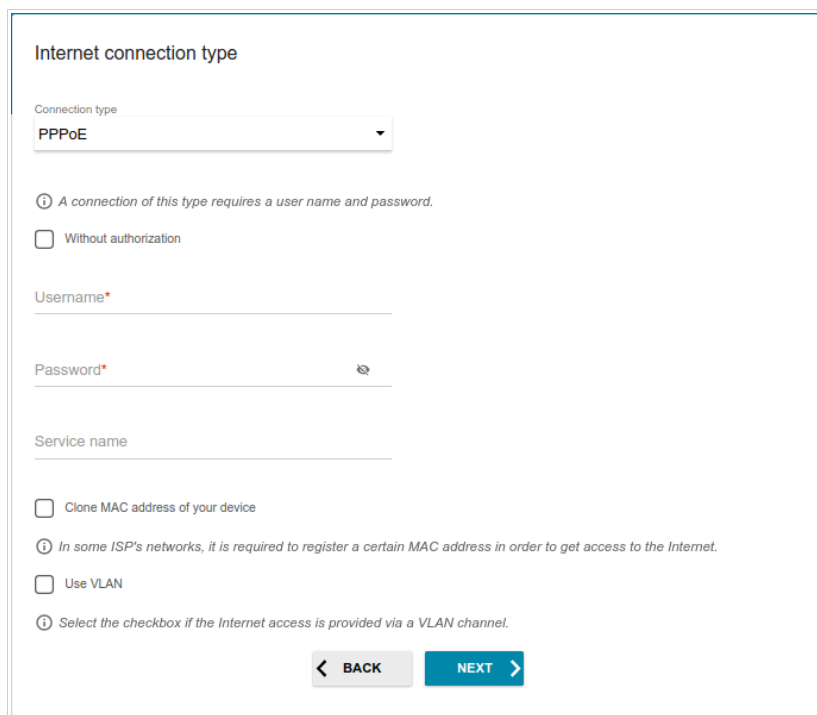


The screenshot shows a web-based configuration interface for a Static IPv6 connection. The title is "Internet connection type". Below it, a dropdown menu is set to "Static IPv6". A help icon and text state: "A connection of this type allows you to use a fixed IP address provided by your ISP." There are four text input fields, each with a red asterisk indicating it is required: "IP address*", "Prefix*", "Gateway IP address*", and "DNS IP address*". Below these fields are two checkboxes: "Clone MAC address of your device" and "Use VLAN". A second help icon and text state: "In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet." and "Select the checkbox if the Internet access is provided via a VLAN channel." At the bottom are two buttons: a grey "BACK" button with a left arrow and a blue "NEXT" button with a right arrow.

Figure 31. The page for configuring Static IPv6 WAN connection.

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

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

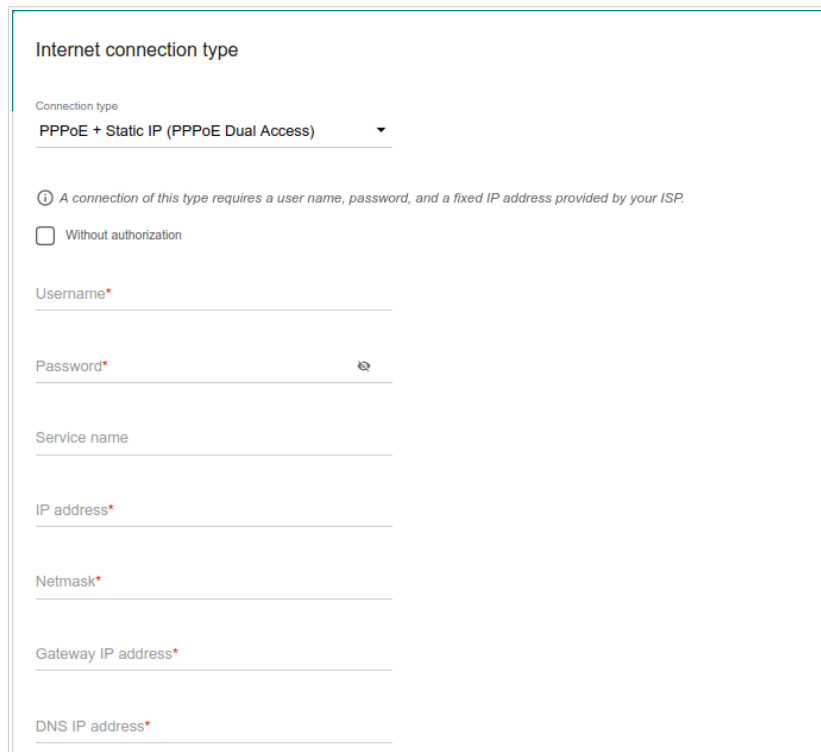


The screenshot shows a web-based configuration interface for setting up an Internet connection. The title is "Internet connection type". Below it, a dropdown menu labeled "Connection type" has "PPPoE" selected. A note indicates that a connection of this type requires a username and password. There are two checkboxes: "Without authorization" (unchecked) and "Clone MAC address of your device" (unchecked). Below these are input fields for "Username*", "Password*" (with a "Show" icon), and "Service name". A note explains that in some ISP networks, a specific MAC address is required for Internet access. Another checkbox "Use VLAN" is present, with a note to select it if Internet access is provided via a VLAN channel. At the bottom are "BACK" and "NEXT" buttons.

Figure 32. The page for configuring PPPoE WAN connection.

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

PPPoE + Static IP (PPPoE Dual Access) Connection



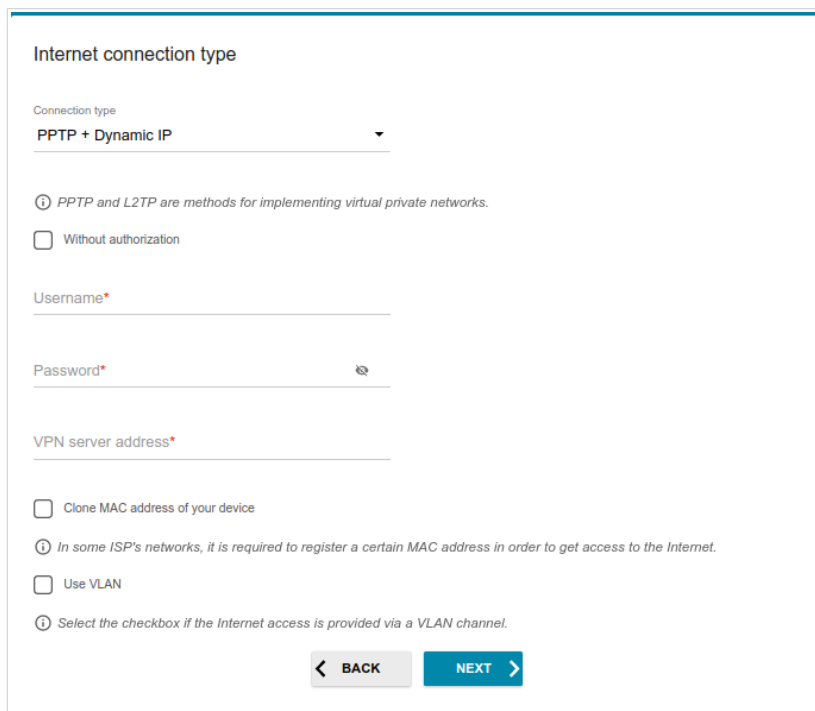
The screenshot shows a web-based configuration interface for a WAN connection. The title is "Internet connection type". Below it, a dropdown menu is set to "PPPoE + Static IP (PPPoE Dual Access)". A note states: "A connection of this type requires a user name, password, and a fixed IP address provided by your ISP." There is a checkbox labeled "Without authorization" which is currently unchecked. Below this are several text input fields, each with a red asterisk indicating it is required: "Username*", "Password*" (with a "Show" icon to its right), "Service name", "IP address*", "Netmask*", "Gateway IP address*", and "DNS IP address*".

Figure 33. 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**, **Netmask**, **Gateway IP address**, and **DNS IP address**.

PPTP + Dynamic IP or L2TP + Dynamic IP Connection



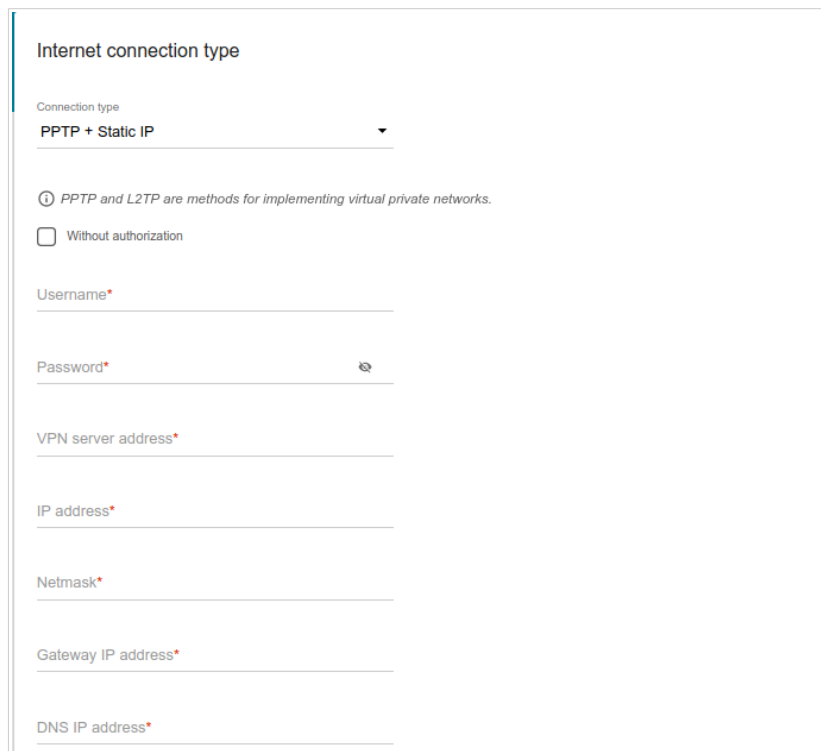
The screenshot shows a web-based configuration page titled "Internet connection type". The "Connection type" dropdown menu is set to "PPTP + Dynamic IP". Below this, there is an information icon and text stating "PPTP and L2TP are methods for implementing virtual private networks." A checkbox labeled "Without authorization" is present. The "Username*" field is empty. The "Password*" field has a "Show" icon (an eye with a slash) to its right. The "VPN server address*" field is empty. There are three checkboxes: "Clone MAC address of your device", "Use VLAN", and a checkbox with an information icon and text "In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet." and "Select the checkbox if the Internet access is provided via a VLAN channel." At the bottom, there are "BACK" and "NEXT" buttons.

Figure 34. The page for configuring PPTP + Dynamic IP WAN connection.

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

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

PPTP + Static IP or L2TP + Static IP Connection



The screenshot shows the 'Internet connection type' configuration page. At the top, 'Connection type' is set to 'PPTP + Static IP'. Below this, there is an information icon and a note: 'PPTP and L2TP are methods for implementing virtual private networks.' A checkbox labeled 'Without authorization' is present. The form includes several required fields, each marked with a red asterisk: 'Username', 'Password' (with a 'Show' icon), 'VPN server address', 'IP address', 'Netmask', 'Gateway IP address', and 'DNS IP address'.

Figure 35. The page for configuring PPTP + Static IP WAN connection.

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

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

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

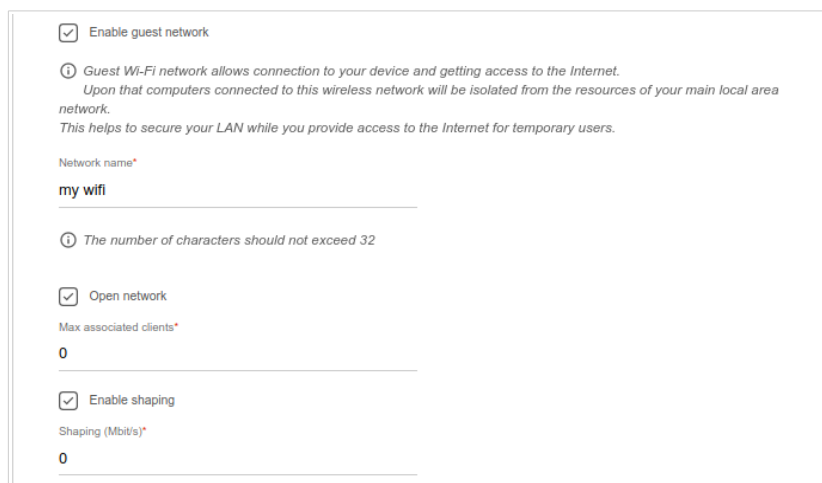
Configuring Wireless Network

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 **Repeater** mode 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 36. The page for configuring the wireless network.

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



☒ Enable guest network

① Guest Wi-Fi network allows connection to your device and getting access to the Internet.
Upon that computers connected to this wireless network will be isolated from the resources of your main local area network.
This helps to secure your LAN while you provide access to the Internet for temporary users.

Network name*

my wifi

① The number of characters should not exceed 32

☒ Open network

Max associated clients*

0

☒ Enable shaping

Shaping (Mbit/s)*

0

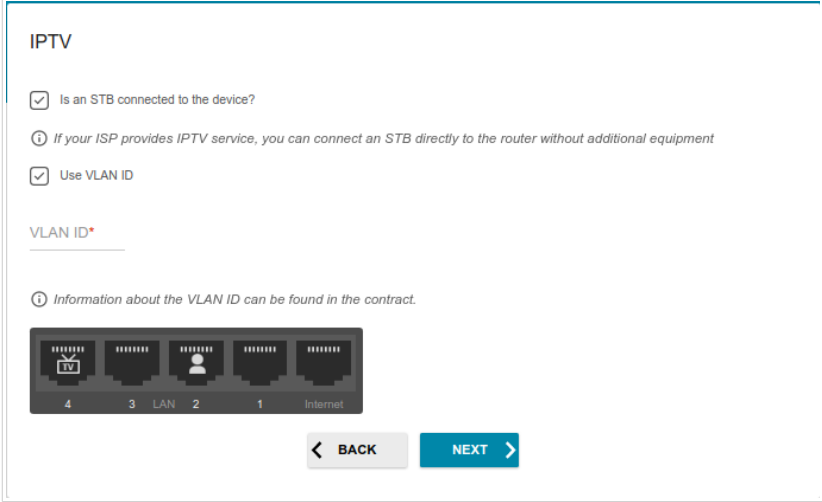
Figure 37. The page for configuring the wireless network.

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

Configuring LAN Ports for IPTV/VoIP

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

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

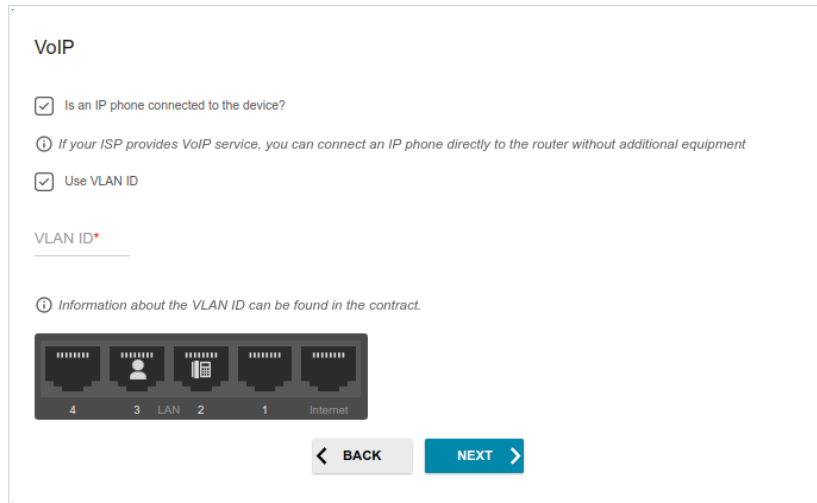


The screenshot shows the 'IPTV' configuration page. At the top, there is a title 'IPTV'. Below it, there are two checkboxes: 'Is an STB connected to the device?' which is checked, and 'Use VLAN ID' which is also checked. A help icon (i) is present next to the first checkbox with the text 'If your ISP provides IPTV service, you can connect an STB directly to the router without additional equipment'. Below the checkboxes, there is a 'VLAN ID*' field with a red asterisk. Another help icon (i) is present with the text 'Information about the VLAN ID can be found in the contract.' Below this, there is a diagram of the router's ports: four LAN ports (labeled 4, 3, 2, 1) and an Internet port. Port 4 is highlighted with a TV icon. At the bottom right, there are two buttons: 'BACK' and 'NEXT'.

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

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

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



The screenshot shows the 'VoIP' configuration page. At the top, there is a title 'VoIP'. Below it, there are two checkboxes: 'Is an IP phone connected to the device?' (checked) and 'Use VLAN ID' (checked). A note below the first checkbox states: 'If your ISP provides VoIP service, you can connect an IP phone directly to the router without additional equipment'. Below the 'Use VLAN ID' checkbox, there is a 'VLAN ID' field with a red asterisk indicating it is required. A note below the field states: 'Information about the VLAN ID can be found in the contract.' At the bottom of the page, there is a diagram of the router's ports: four LAN ports (labeled 4, 3, 2, 1 from left to right) and an Internet port. Port 3 is highlighted with a person icon, indicating it is selected for the IP phone connection. At the bottom right, there are two buttons: 'BACK' and 'NEXT'.

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

6. Select a free LAN port for connecting your IP phone.
7. If the VoIP service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.
8. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **Admin 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.²

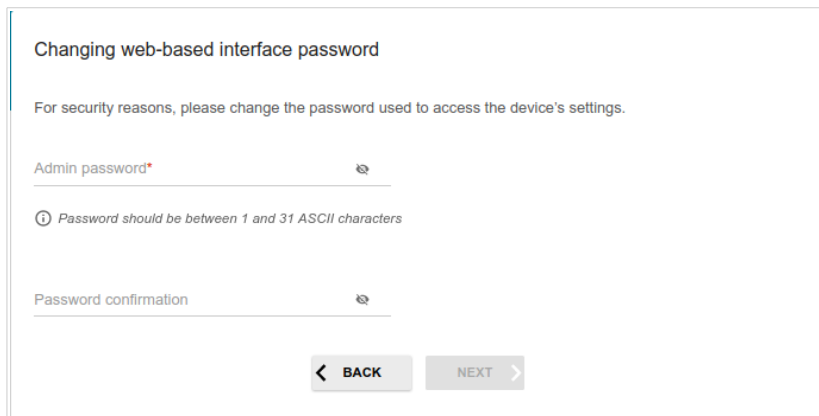


Figure 40. The page for changing the web-based interface password.



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

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

On the next page, check all specified settings.

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

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

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

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

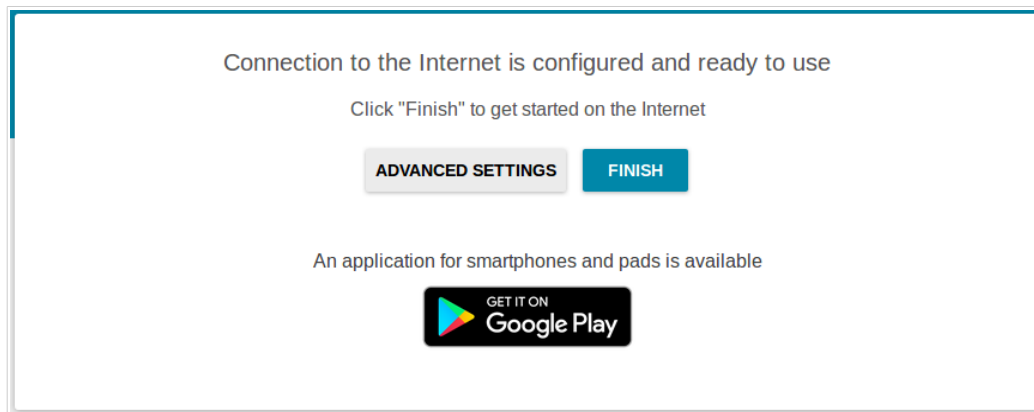


Figure 41. Checking the Internet availability.

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

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

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

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 33).

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-841 in order to use these devices.

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

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

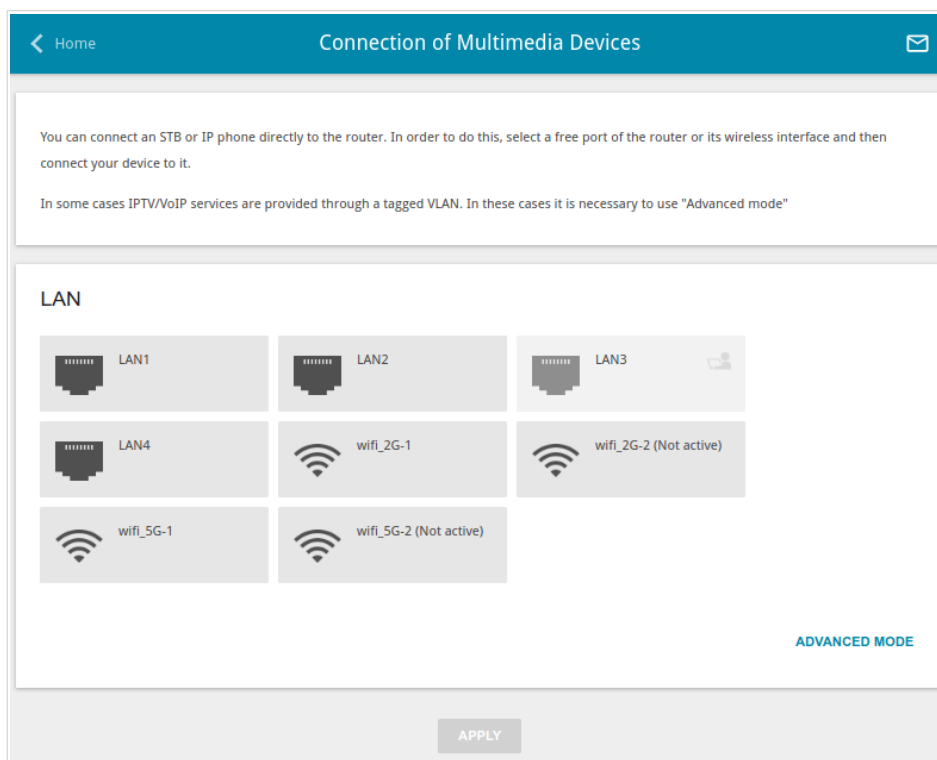


Figure 42. The Multimedia Devices Connection Wizard. The simple mode.

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

The screenshot shows the 'Multimedia Devices Connection Wizard' in 'ADVANCED MODE'. The 'LAN' section contains seven device cards. Each card displays a device icon, a name (LAN1, LAN2, LAN3, LAN4, wifi_2G-1, wifi_2G-2, wifi_5G-1, or wifi_5G-2 (Not active)), and a 'Bridged with' dropdown menu. All dropdown menus are currently set to 'No'. A 'SIMPLE MODE' link is visible in the bottom right of the LAN section. The 'WAN' section shows a 'wan' port icon and a large blue plus icon. An 'APPLY' button is located at the bottom center of the wizard.

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


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

The 'New Connection' dialog box is shown. It has a title bar with a close button. Inside, there are two text input fields: 'Name*' and 'VLAN ID*'. Below these fields is a toggle switch labeled 'Allowed', which is currently turned on. A 'SAVE' button is located in the bottom right corner of the dialog.

Figure 44. Adding a connection.

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

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

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

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

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

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).

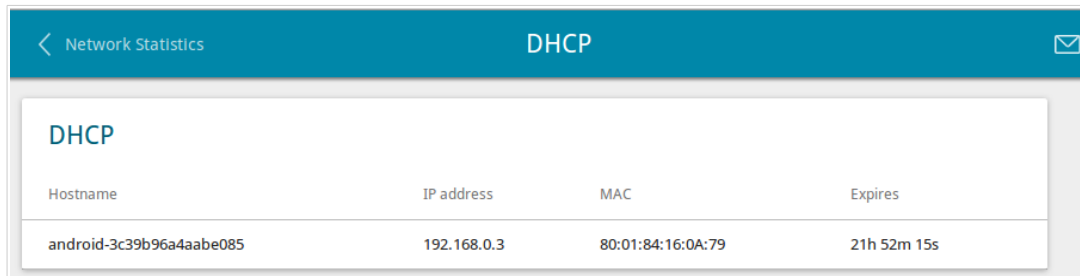
Network Statistics				
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 -- IPv6: fd01::1/64 --	180.50 Kbyte / 219.69 Kbyte	-	-
WAN	-	-	-	-
WIFI_2.4GHZ	-	- / -	-	-
WIFI_5GHZ	-	- / -	-	-

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

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

DHCP

The **Statistics / DHCP** page displays the information on computers that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the device, as well as the IP address expiration periods (the lease time).

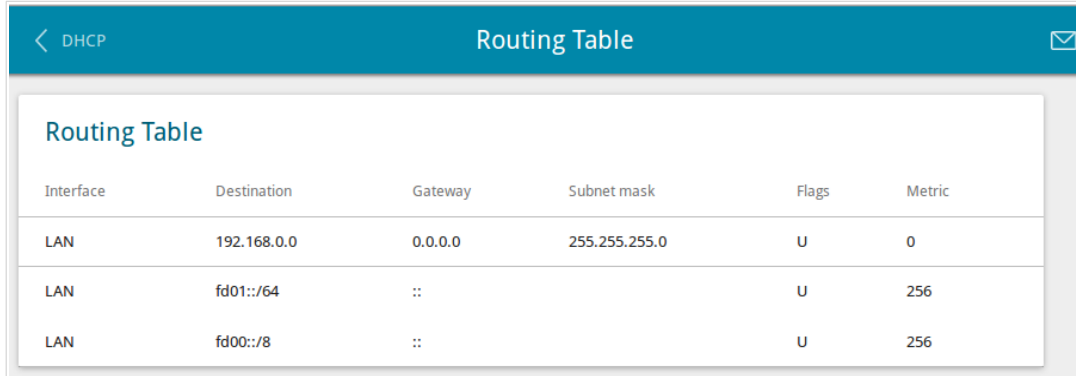


DHCP			
Hostname	IP address	MAC	Expires
android-3c39b96a4aabe085	192.168.0.3	80:01:84:16:0A:79	21h 52m 15s

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

Routing Table

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

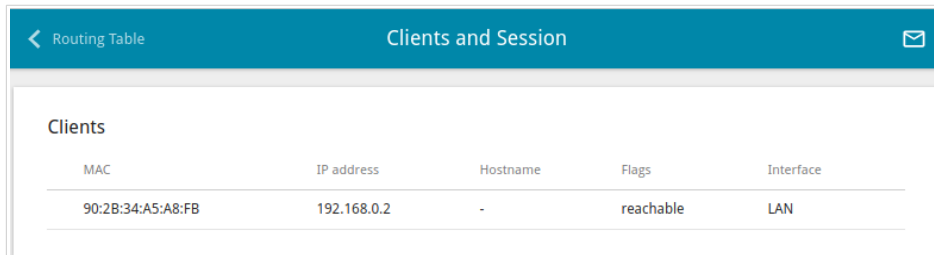


Interface	Destination	Gateway	Subnet mask	Flags	Metric
LAN	192.168.0.0	0.0.0.0	255.255.255.0	U	0
LAN	fd01::/64	::		U	256
LAN	fd00::/8	::		U	256

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

Clients and Session

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



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

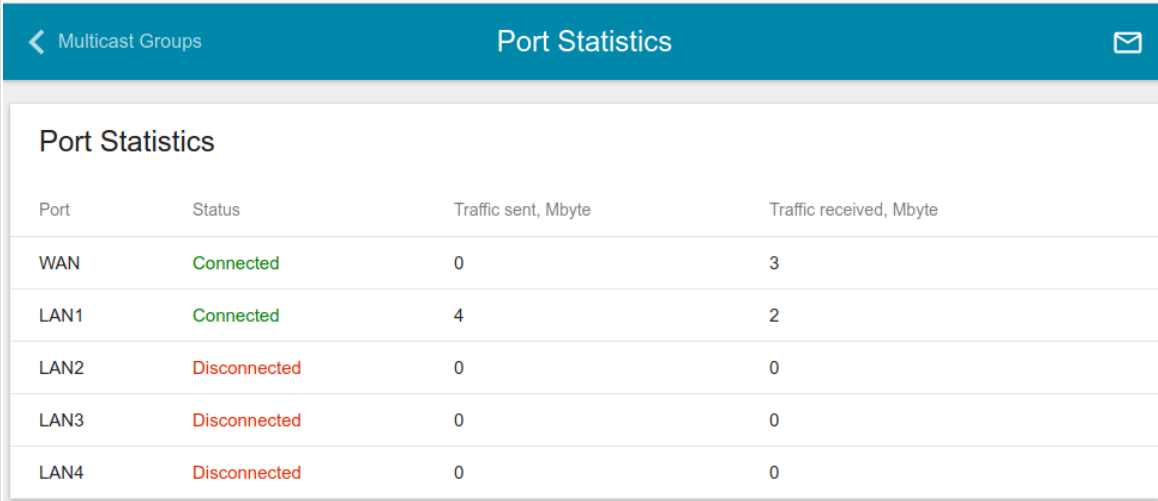
Figure 48. The **Statistics / Clients and Session** page.

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

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

Port Statistics

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



Port Statistics			
Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte
WAN	Connected	0	3
LAN1	Connected	4	2
LAN2	Disconnected	0	0
LAN3	Disconnected	0	0
LAN4	Disconnected	0	0

Figure 49. The **Statistics / Port Statistics** page.

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

Multicast Groups

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



IPv4	
IP address	Interface
239.255.255.250	LAN

IPv6	
IP address	Interface

Figure 50. The **Statistics / Multicast Groups** page.

Connections Setup

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

WAN

On the **Connections Setup / WAN** page, you can create and edit connections used by the router. By default, a **Dynamic IPv4** connection is configured in the system. It is assigned to the WAN port of the router.

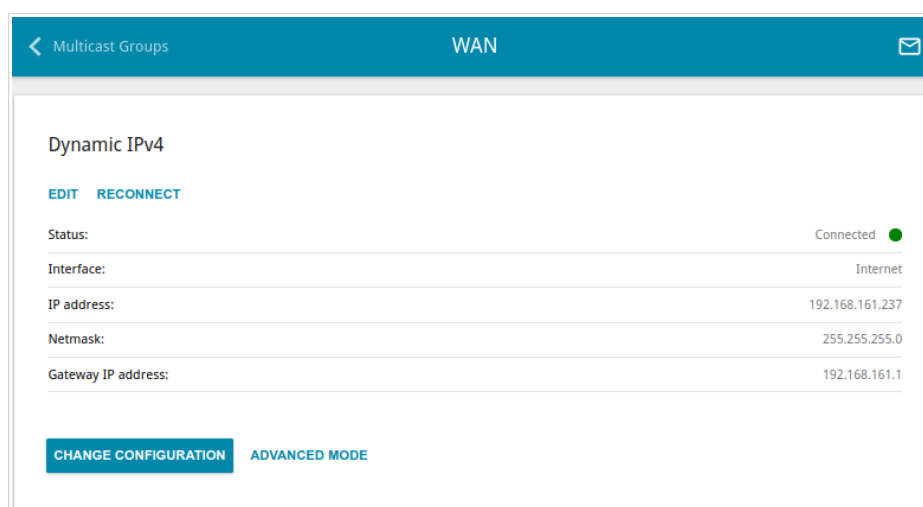


Figure 51. The **Connections Setup / WAN** page. The simplified mode.

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

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

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

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



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

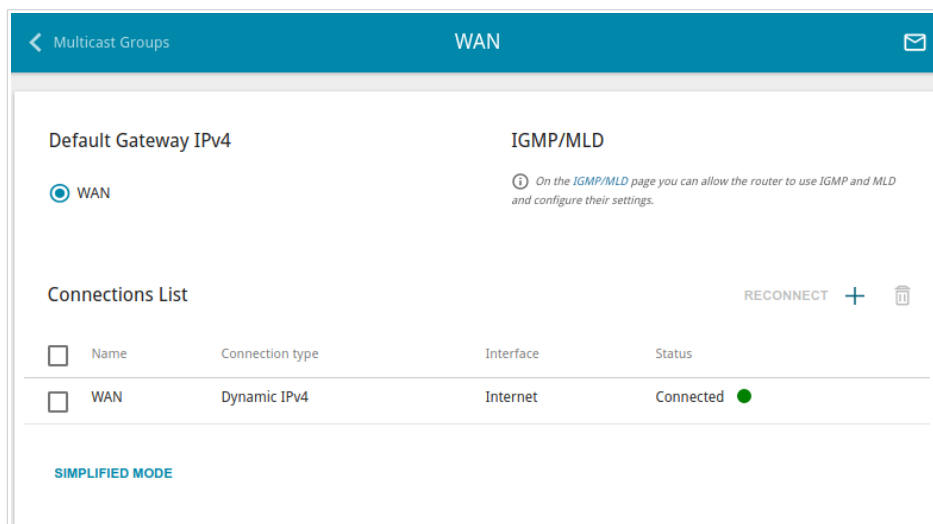




Figure 52. The **Connections Setup / WAN** page. The advanced mode.

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

To edit an existing connection, in the **Connections List** section, left-click the relevant line in the table. On the opened page, on the **Basic** tab, the mandatory settings of this WAN connection will be displayed. To view all available settings of the WAN connection, go to the **All Settings** tab. Change the needed parameters and click the **APPLY** button.

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

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

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP / MLD** link (for the description of the page, see the **IGMP/MLD** section, page 150).

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

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

Creating Dynamic IPv4 or Static IPv4 WAN Connection

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

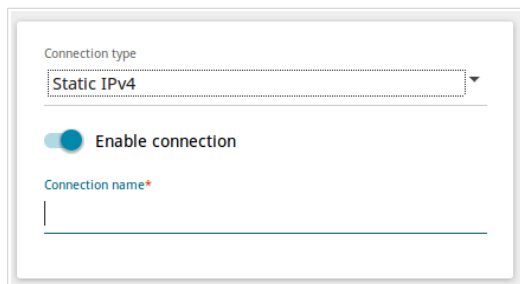
The screenshot shows a web interface for creating a connection. At the top, there is a label 'Connection type' above a dropdown menu that currently displays 'Static IPv4'. Below this, there is a toggle switch labeled 'Enable connection', which is currently turned on (blue). At the bottom, there is a text input field labeled 'Connection name' with a red asterisk indicating it is required.

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

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

Ethernet

MAC address*

9C:D6:43:3D:01:05

☐

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

RESTORE DEFAULT MAC ADDRESS

MTU*

1500

Figure 54. The page for creating a new **Static IPv4** connection. The **Ethernet** section.

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

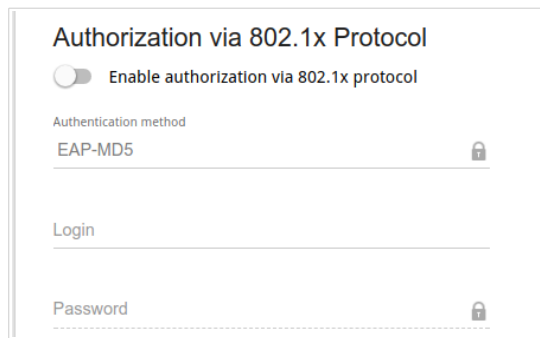


Figure 55. The page for creating a new **Static IPv4** connection. The **Authorization via 802.1x Protocol** section.

Parameter	Description
Authorization via 802.1x Protocol	
Enable authorization via 802.1x protocol	Move the switch to the right to allow authorization in the ISP's network via the 802.1x protocol.
Authentication method	Select a needed authentication method from the drop-down list.
Login	Enter the username provided by your ISP.
Password	Enter the password provided by your ISP.

IPv4

IP address*

Netmask*

Gateway IP address*

Primary DNS*

Secondary DNS

① If the connection is created for the IPTV service only and no data on IP addressing is given by your ISP, then you can set the following values: IP address = 1.0.0.1, Netmask = 255.255.255.252, Gateway IP address = 1.0.0.2, Primary DNS server = 1.0.0.2

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

Parameter	Description
IPv4	
<i>For Static IPv4 type</i>	
IP address	Enter an IP address for this WAN connection.
Netmask	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.
<i>For Dynamic IPv4 type</i>	
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. <i>Optional.</i>
Hostname	A name of the router specified by your ISP. <i>Optional.</i>

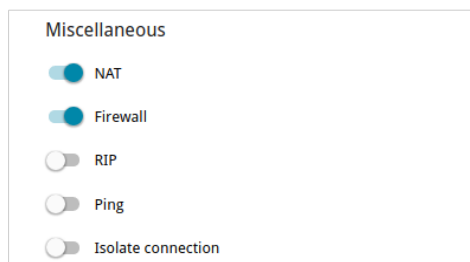


Figure 57. The page for creating a new **Static IPv4** connection. The **Miscellaneous** section.

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

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

Creating Dynamic IPv6 or Static IPv6 WAN Connection

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

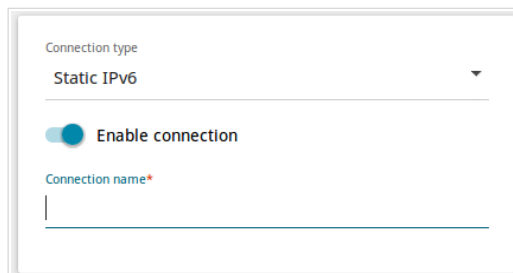


Figure 58. The page for creating a new **Static IPv6** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

Ethernet

MAC address*

9C:D6:43:3D:01:05

☐

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

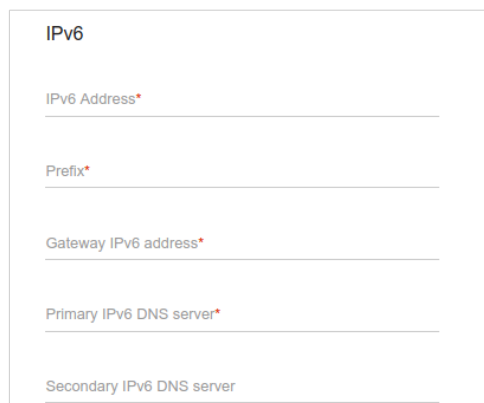
RESTORE DEFAULT MAC ADDRESS

MTU*

1500

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

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



IPv6

IPv6 Address*

Prefix*

Gateway IPv6 address*

Primary IPv6 DNS server*

Secondary IPv6 DNS server

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

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

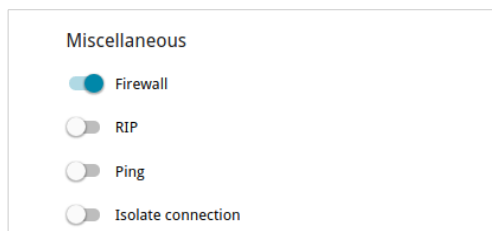


Figure 61. The page for creating a new **Static IPv6** connection. The **Miscellaneous** section.

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

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

Creating PPPoE WAN Connection

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

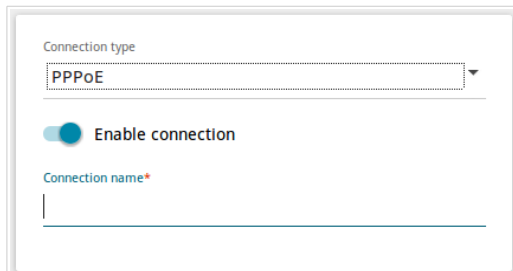


Figure 62. The page for creating a new **PPPoE** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

Ethernet

MAC address*

9C:D6:43:3D:01:05

☐

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

RESTORE DEFAULT MAC ADDRESS

MTU*

1500

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

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

PPP

☐ Without authorization

Username*

Password*

Service name

MTU*

1492

Authentication protocol

AUTO

☒ Keep Alive

LCP interval*

30

LCP fails*

3

☐ Dial on demand

Maximum idle time (in seconds)

0

Static IP address

☐ PPP IP extension

☐ PPP debug

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

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

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

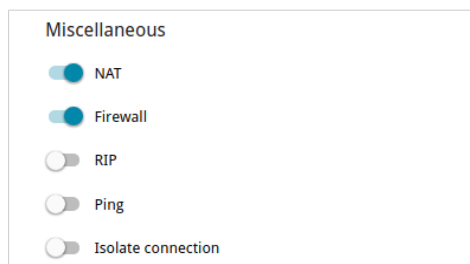


Figure 65. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.

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

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

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

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

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

Creating PPTP or L2TP WAN Connection

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

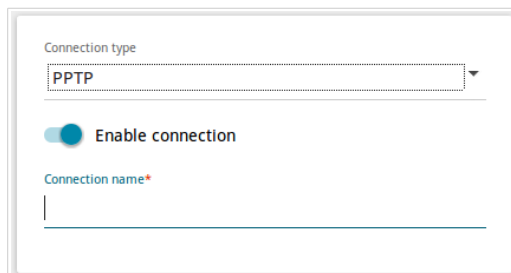
The screenshot shows a web interface for creating a connection. At the top, there is a label 'Connection type' above a dropdown menu that currently displays 'PPTP'. Below this, there is a toggle switch labeled 'Enable connection', which is currently turned on (indicated by a blue circle). At the bottom,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

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

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

PPP

☐ Without authorization

Username*

Password*

VPN server address*

MTU*

Authentication protocol

AUTO

Encryption protocol

No encryption

☒ Keep Alive

LCP interval*

LCP fails*

☐ Dial on demand

Maximum idle time (in seconds)

Extra options

Static IP address

☐ PPP debug

☒ Enable MPPE

Figure 67. The page for creating a new **PPTP** connection. The **PPP** section.

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the Show icon (🔍) to display the entered password.
VPN server address	The IP or URL address of the PPTP or L2TP authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the AUTO value.

Parameter	Description
Encryption protocol	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • 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. <p>MPPE encryption can be applied only if the MS-CHAP, MS-CHAPV2, or AUTO value is selected from the Authentication protocol drop-down list.</p>
Keep Alive	<p>Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the LCP interval and LCP fails fields are available. Specify the required values.</p>
Dial on demand	<p>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.</p>
Extra options	<p>Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional.</i></p>
Static IP address	<p>Fill in the field if you want to use a static IP address to access the Internet.</p>
PPP debug	<p>Move the switch to the right if you want to log all data on PPP connection debugging.</p>
Enable MPPC	<p><i>(Microsoft Point-to-Point Compression)</i> <i>For the PPTP type only.</i></p> <p>Move the switch to the right if it is necessary to use the data compression function in order to configure the connection.</p> <p>Move the switch to the left to disable the function.</p>

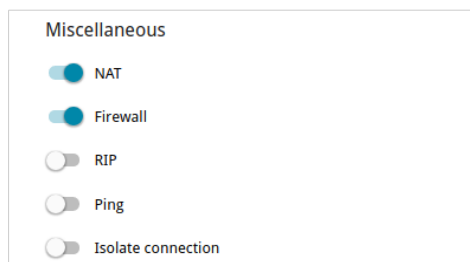


Figure 68. The page for creating a new **PPTP** connection. The **Miscellaneous** section.

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

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

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

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

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

Click the **OK** button.

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

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

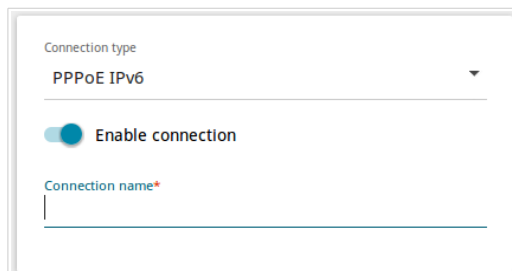


Figure 69. The page for creating a new **PPPoE IPv6** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	<i>Available for the advanced mode only.</i> A name for the connection for easier identification.

Ethernet

MAC address*

9C:D6:43:3D:01:05

☐

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

RESTORE DEFAULT MAC ADDRESS

MTU*

1500


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

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

PPP

☐ Without authorization

Username*

Password* 

Service name

MTU*
1492


Authentication protocol
AUTO ▼

☒ Keep Alive

LCP interval*
30

LCP fails*
3


☐ Dial on demand

Maximum idle time (in seconds)
0 

☐ PPP IP extension

☐ PPP debug

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

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the Show icon () to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the AUTO value.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the LCP interval and LCP fails fields are available. Specify the required values.

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

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

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

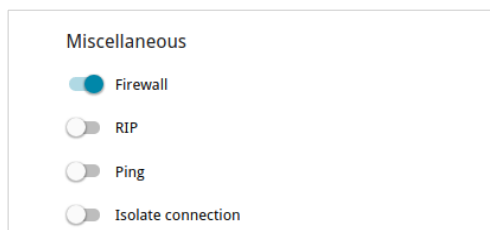


Figure 73. The page for creating a new **PPPoE IPv6** connection. The **Miscellaneous** section.

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

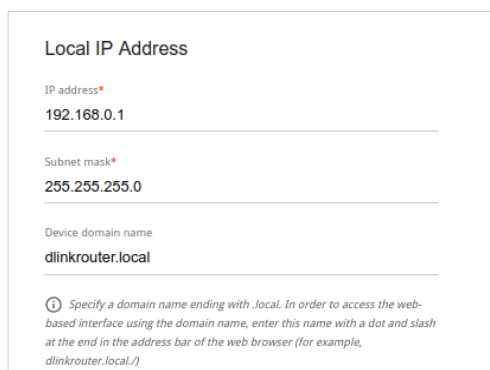
When all needed settings are configured, click the **APPLY** button.

LAN

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

IPv4

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



The screenshot shows the 'Local IP Address' configuration section. It includes three input fields: 'IP address*' with the value '192.168.0.1', 'Subnet mask*' with the value '255.255.255.0', and 'Device domain name' with the value 'dlinkrouter.local'. Below these fields is a note: '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 74. Configuring the local interface. The **IPv4** tab. The **Local IP Address** section.

Parameter	Description
Local IP Address	
Mode of local IP address assignment	<i>For the Access point, Repeater, and Client modes only.</i> Select the needed value from the drop-down list. Static : the IP address, subnet mask, and the gateway IP address are assigned manually. Dynamic : the router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.
IP address	The IP address of the router in the local subnet. By default, the following value is specified: 192.168.0.1 .
Subnet mask	The mask of the local subnet. By default, the following value is specified: 255.255.255.0 .
Gateway IP address	<i>For the Access point, Repeater, and Client modes only.</i> The gateway IP address which is used by the router to connect to the Internet (e.g., for synchronizing the system time with an NTP server). <i>Optional</i> .
Device domain name	The name of the device assigned to its IP address in the local subnet.

Figure 75. Configuring the local interface. The IPv4 tab. The **Dynamic IP Addresses** section.

Parameter	Description
Dynamic IP Addresses	
Mode of dynamic IP address assignment	<p>An operating mode of the router's DHCP server.</p> <p>Disable: the router's DHCP server is disabled, clients' IP addresses are assigned manually.</p> <p>DHCP server: the router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the Start IP, End IP, Lease time fields and the DNS relay switch are displayed on the tab.</p> <p>DHCP relay: an external DHCP server is used to assign IP addresses to clients. When this value is selected, the External DHCP server IP and Option 82 Remote ID fields are displayed on the tab.</p>
Start IP	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
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	<p>Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address.</p> <p>Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the Advanced / DNS page as the DNS server address.</p>

Parameter	Description
External DHCP server IP	<p>The IP address of the external DHCP server which assigns IP addresses to the router's clients.</p> <p>To specify several IP addresses, click the ADD button, and in the line displayed, enter an IP address.</p> <p>To remove the IP address, click the Delete icon (✕) in the line of the address.</p>
Option 82 Remote ID	<p>The value of the Remote ID field of DHCP option 82 in accordance with RFC3046.</p> <p>Do not fill in the field unless your ISP or the administrator of the external DHCP server provided this value.</p>

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

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

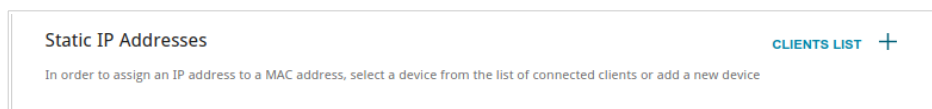


Figure 76. The section for creating MAC-IPv4 pairs.

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

In order to view MAC addresses of the devices connected to the router at the moment, click the **CLIENTS LIST** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

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

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

IPv6

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

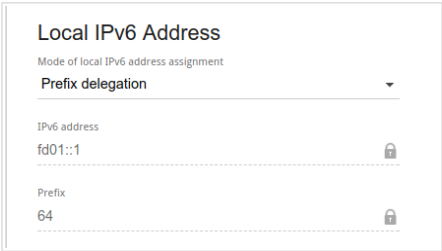


Figure 77. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.

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

Figure 78. Configuring the local interface. The IPv6 tab. The **Dynamic IPv6 Addresses** section.

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

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

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

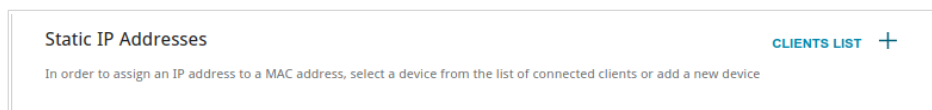




Figure 79. The section for creating MAC-IPv6 pairs.

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

In order to view MAC addresses of the devices connected to the router at the moment, click the **CLIENTS LIST** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

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

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

WAN Reservation

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

Figure 80. The **Connections Setup / WAN Reservation** page.

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

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

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

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

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.

The screenshot shows the 'Basic Settings' page for the 2.4 GHz Wi-Fi network. The page is divided into two main sections: General Settings and Security Settings.

General Settings:

- Enable Wireless:** ☒
- Country:** RUSSIAN FEDERATION
- Wireless mode:** 802.11 G
- Select channel automatically:** ☒
- Enable additional channels:** ☒
- Channel:** auto (channel 1)
- Enable periodic scanning:** ☐
- Scanning period (in seconds):** 60

Wi-Fi Network:

- Network name (SSID):** DIR-XXX-0105
- Hide SSID:** ☐
- Max associated clients:** 0
- Enable shaping:** ☐
- Broadcast wireless network:** ☒
- Clients isolation:** ☐

Security Settings:

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

Buttons at the bottom: APPLY, ADD WI-FI NETWORK

Figure 81. Basic settings of the wireless LAN in the 2.4GHz band.

In the **General 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.
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.
Channel	The wireless channel number. Left-click to open the window for selecting a channel (the action is available, when the Select channel automatically switch is moved to the left).
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.

The screenshot displays the 'Add Access Point' configuration page. The top navigation bar includes a back arrow, 'Basic Settings', the title 'Add Access Point', and a mail icon. The main content area is divided into two columns: 'Wi-Fi Network' and 'Security Settings'.

Wi-Fi Network Section:

- Network name (SSID)*:** A text field containing 'DIR-XXX-39a2.2'.
- Hide SSID:** A toggle switch that is currently turned off.
- Max associated clients*:** A text field containing '0'.
- Enable shaping:** A toggle switch that is currently turned off.
- Broadcast wireless network:** A toggle switch that is currently turned on.
- Clients isolation:** A toggle switch that is currently turned off.
- Enable guest network:** A toggle switch that is currently turned off.

Security Settings Section:

- Network authentication:** A dropdown menu set to 'WPA2-PSK'.
- Password PSK*:** A text field with masked characters (dots) and a show/hide icon.
- Encryption type*:** A dropdown menu set to 'AES'.
- Group key update interval (in seconds)*:** A text field containing '3600'.

At the bottom left of the form is a blue button labeled 'APPLY'.

Figure 82. Creating a wireless network.

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

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

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

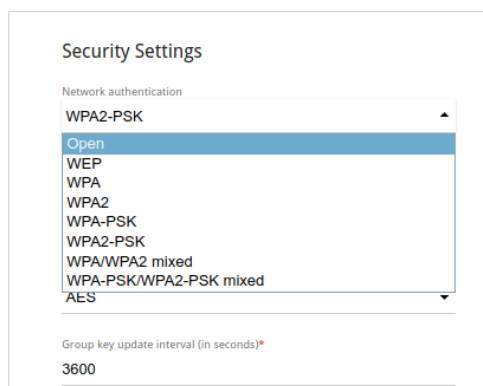


Figure 83. Network authentication types supported by the router.

The router supports the following authentication types:

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



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

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

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

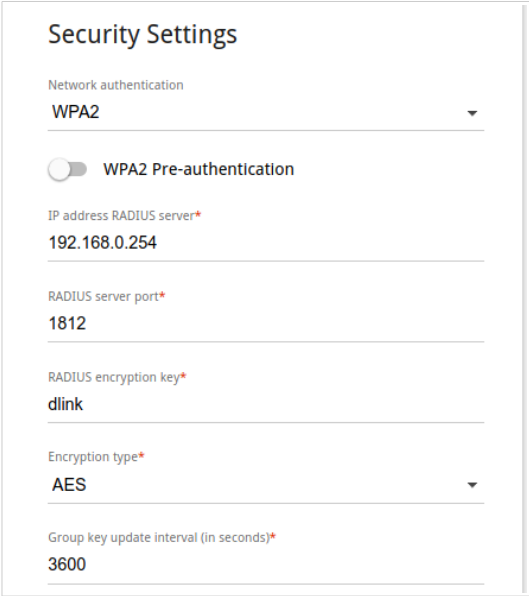
The screenshot shows the 'Security Settings' section of a web interface. Under 'Network authentication', 'WPA2-PSK' is selected from a dropdown menu. Below this is the 'Password PSK' field, which is masked with dots and has a 'Show' icon (an eye with a slash) to its right. A red asterisk is next to the label. A hint below the field states: 'Password should be between 8 and 63 ASCII characters'. Under 'Encryption type', 'TKIP' is selected from a dropdown menu, also marked with a red asterisk. At the bottom, the 'Group key update interval (in seconds)' is set to '3600'.

Figure 85. 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. ³ Click the Show icon (👁) to display the entered password.
Encryption type	An encryption method: TKIP , AES , or TKIP+AES .
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed.

³ 0-9, A-Z, a-z, space, !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~.

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




The screenshot shows the 'Security Settings' page. At the top, 'Network authentication' is set to 'WPA2'. Below this, 'WPA2 Pre-authentication' is a toggle switch that is currently turned off. The 'IP address RADIUS server*' is set to '192.168.0.254'. The 'RADIUS server port*' is set to '1812'. The 'RADIUS encryption key*' is set to 'dlink'. The 'Encryption type*' is set to 'AES'. The 'Group key update interval (in seconds)*' is set to '3600'.

Figure 86. 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.

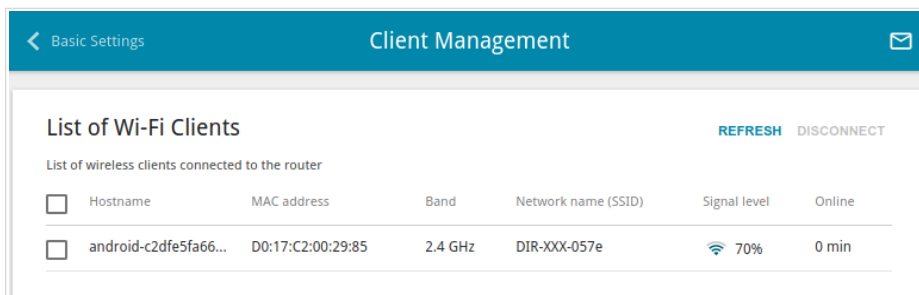


Figure 87. The page for managing the wireless clients.

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.

The screenshot shows the WPS configuration page. At the top, there's a header with 'Client Management' and 'WPS'. Below that, there are tabs for '2.4 GHz' and '5 GHz'. The main content area is titled 'WPS' and includes a description: '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.' Below this, there's a 'DISABLE WPS' link. The 'WPS Control' section features an 'ESTABLISH CONNECTION' button. The 'Information' section displays the following details:

WPS state:	Configured
Default PIN code:	12345670
Network name (SSID):	DIR-XXX-0105
Network authentication:	WPA2-PSK
Encryption:	AES
Password PSK:	12345670

At the bottom of the Information section, there are two buttons: 'UPDATE' and 'RESET TO UNCONFIGURED'.

Figure 88. The page for configuring the WPS function.

To activate the WPS function, on the tab of the relevant band, click the **ENABLE WPS** button.

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

Parameter	Description
WPS state	The state of the WPS function: <ul style="list-style-type: none">• Configured (all needed settings are specified; these settings will be used upon establishing the wireless connection)• Unconfigured (after activating the WPS function, the SSID and the encryption key will be configured automatically, the network authentication type will be changed to WPA2-PSK).
Default PIN code	The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function.
Network name (SSID)	The name of the router's wireless network.
Network authentication	The network authentication type specified for the wireless network.
Encryption	The encryption type specified for the wireless network.
Password PSK	The encryption password specified for the wireless network.
UPDATE	Click the button to update the data on the page.
RESET TO UNCONFIGURED	Click the button to reset the parameters of the WPS function.

Using WPS Function via Web-based Interface

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

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

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

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

Using WPS Function without Web-based Interface

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

1. Specify relevant security settings for the wireless network of the router.
2. Click the **ENABLE WPS** button.
3. Save the settings and close the web-based interface (click the **Logout** line of the menu).

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

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

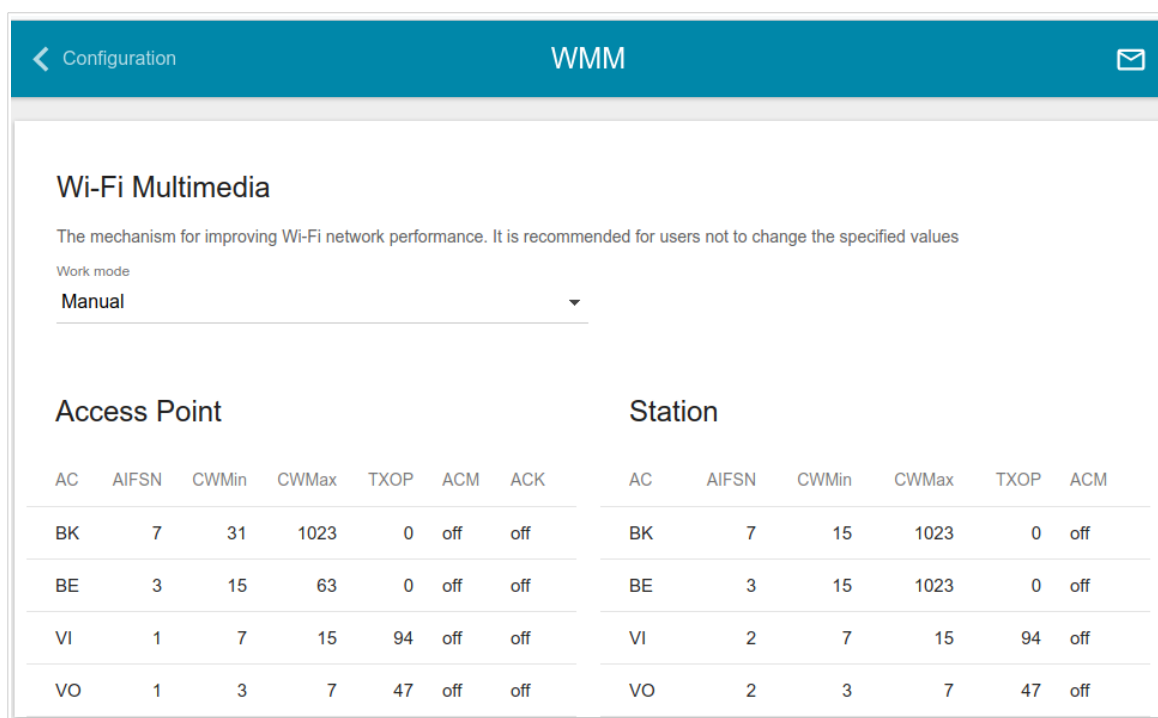
WMM

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

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

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.
- **Disabled**: the WMM function is disabled.



Wi-Fi Multimedia

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

Work mode
Manual

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

Figure 89. 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.

The screenshot shows a web-based configuration window titled "Edit Access Point: Best Effort". It contains the following fields and controls:

- AIFSN***: A dropdown menu with the value "3" selected.
- CWMin**: A dropdown menu with the value "15" selected.
- CWMax**: A dropdown menu with the value "63" selected.
- TXOP***: A text input field with the value "0".
- ACM**: A toggle switch that is currently turned off.
- ACK**: A toggle switch that is currently turned off.
- At the bottom right, there are two buttons: "SAVE" and "CLOSE".

Figure 90. The window for changing parameters of the WMM function.

Parameter	Description
AIFSN	<i>Arbitrary Inter-Frame Space Number.</i> This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
CWMin/CWMax	<i>Contention Window Minimum/Contention Window Maximum.</i> 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	<i>Transmission Opportunity.</i> The higher the value, the higher is the Access Category priority.

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

The screenshot shows the 'Client' configuration page. At the top, there is a blue header with a back arrow and 'WAN' on the left, and 'Client' in the center, with an envelope icon on the right. Below the header, there are three toggle switches, all of which are turned on (blue). The first is labeled 'Enable'. The second is labeled 'Broadcast wireless network 2.4 GHz'. The third is labeled 'Broadcast wireless network 5 GHz'. Below these is a section titled 'Connecting to network' with a dropdown menu labeled 'Select network from list'. There is a blue 'APPLY' button. At the bottom, there is a table titled 'Wireless Networks' with a blue 'UPDATE LIST' link on the right. The table has four columns: 'Network name (SSID)', 'Security settings', 'Channel', and 'Frequency'. There is one entry in the table: 'DIR-815-4411' with security settings '[WPA2-PSK] [AES]', channel '13', and frequency '2.4 GHz'.

Figure 91. 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. Select the band where the hidden network operates from the **Frequency band** list and enter the network name in the **Network name (SSID)** field. If needed, fill in the **BSSID** field. Then select the needed type of authentication from the **Network authentication** drop-down list.

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

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

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

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

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

When connecting to a wireless access point, the wireless channel of DIR-841 will switch to the channel of the access point to which you have connected.

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

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

Client Shaping

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

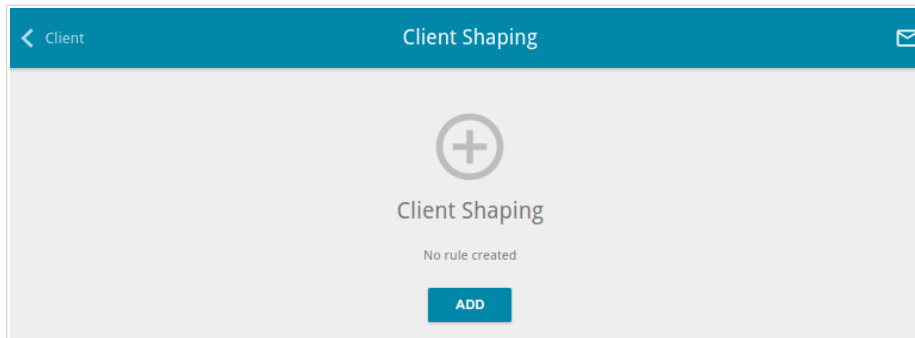



Figure 92. The **Wi-Fi / Client Shaping** page.

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

The screenshot shows the 'Add Rule' window. It has a blue header bar with the title 'Add Rule' and a close button. The window contains several settings: a toggle switch for 'Enabled' which is turned on; a text input field for 'MAC address*' with a dropdown arrow; a section for 'Upload' with a toggle switch for 'Not limited' which is turned off, and a text input field for 'Maximum rate (Mbit/s)*'; a section for 'Download' with a toggle switch for 'Not limited' which is turned off, and a text input field for 'Maximum rate (Mbit/s)*'. At the bottom right of the window, there is a blue button labeled 'SAVE'.


Figure 93. The window for setting up rate limit.

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

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

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

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

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

Additional

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



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

The screenshot shows the 'Additional' settings page for the 2.4 GHz WLAN band. The page is divided into two main sections: '2.4 GHz' (active) and '5 GHz'. The '2.4 GHz' section contains the following settings:

- Bandwidth:** 20/40 MHz (dropdown menu)
- Current bandwidth:** 40 MHz (info icon)
- Autonegotiation 20/40 (Coexistence):** Disabled (toggle switch)
- TX power (in percent):** 100 (dropdown menu)
- B/G protection:** Auto (dropdown menu)
- Short GI:** Enable (dropdown menu)
- Drop multicast:** Disabled (toggle switch)
- Enable TX Beamforming:** Enabled (toggle switch)
- Adaptivity mode:** Disabled (toggle switch)

The '5 GHz' section contains the following settings:

- Beacon period (in milliseconds)*:** 100
- RTS threshold (in bytes)*:** 2347
- Frag threshold (in bytes)*:** 2346
- DTIM period (in beacon frames)*:** 1
- Station Keep Alive (in seconds)*:** 0

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

Figure 94. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	<p>The channel bandwidth for 802.11n standard in the 2.4GHz band (the 2.4 GHz tab).</p> <p>20 MHz: 802.11n clients operate at 20MHz channels.</p> <p>20/40 MHz: 802.11n clients operate at 20MHz or 40MHz channels.</p> <p>The channel bandwidth for 802.11n and 802.11ac standards in 5GHz band (the 5 GHz tab).</p> <p>20 MHz: 802.11n and 802.11ac clients operate at 20MHz channels.</p> <p>20/40 MHz: 802.11n and 802.11ac clients operate at 20MHz or 40MHz channels.</p> <p>20/40/80 MHz: 802.11ac clients operate at 20MHz, 40MHz, or 80MHz channels.</p>
Autonegotiation 20/40 (Coexistence)	<p><i>Available on the 2.4 GHz tab.</i></p> <p>Move the switch to the right to let the router to automatically choose the most suitable channel bandwidth (20MHz or 40MHz) for the connected devices (this setting can substantially lower the data transfer rate of your wireless network).</p>
TX power	The transmit power (in percentage terms) of the router.
B/G protection	<p><i>Available on the 2.4 GHz tab.</i></p> <p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <p>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).</p> <p>Always On: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</p> <p>Always Off: The protection function is always disabled.</p>
Short GI	<p>Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices.</p> <p>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).</p> <p>Disable: the router uses the 800 ns standard guard interval.</p>

Parameter	Description
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.
Enable TX Beamforming	TX Beamforming is the signal processing/directing technique which helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation. Move the switch to the right to improve the signal quality.
Adaptivity mode	Move the switch to the right to prevent your wireless network from interfering with radars and other mobile or stationary radio systems. Such a setting can slow down the router's WLAN.
Beacon period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS threshold	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
Frag threshold	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).
DTIM period	The time period (in seconds) between sending a DTIM (a message notifying on broadcast or multicast transmission) and data 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-841.

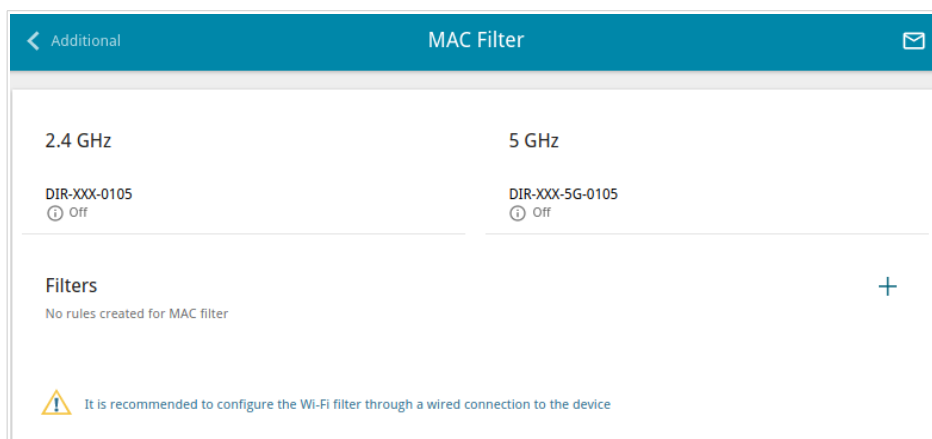


Figure 95. The page for configuring the MAC filter for the wireless network.

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 96. 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.
Hostname	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.

Roaming

On the **Wi-Fi / Roaming** page, you can enable the function of smart adjustment of Wi-Fi clients. This function is designed for wireless networks based on several access points or routers. If the function is enabled for all access points (routers) which establish a wireless network, then wireless clients will always connect to the device with the highest signal level.

Figure 97. 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	<p>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.</p> <p>If the switch is moved to the left, broadcast traffic is used for service data exchange.</p>

Parameter	Description
Multicast TTL	Specify the TTL (<i>Time to live</i>) parameter value. The recommended value is 4 .
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% .

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:

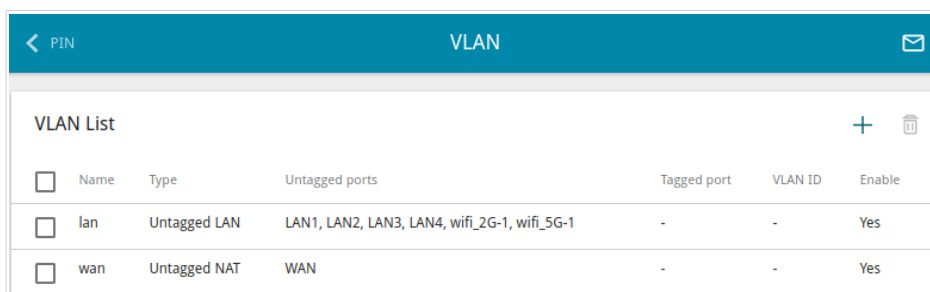
- create groups of ports for VLANs
- add name servers
- configure a DDNS service
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the router
- setup the rate limit for traffic transmitted from every port of the router
- configure notifications on the reason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

VLAN

On the **Advanced / VLAN** page, you can create and edit groups of ports for virtual networks (VLANs).

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

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

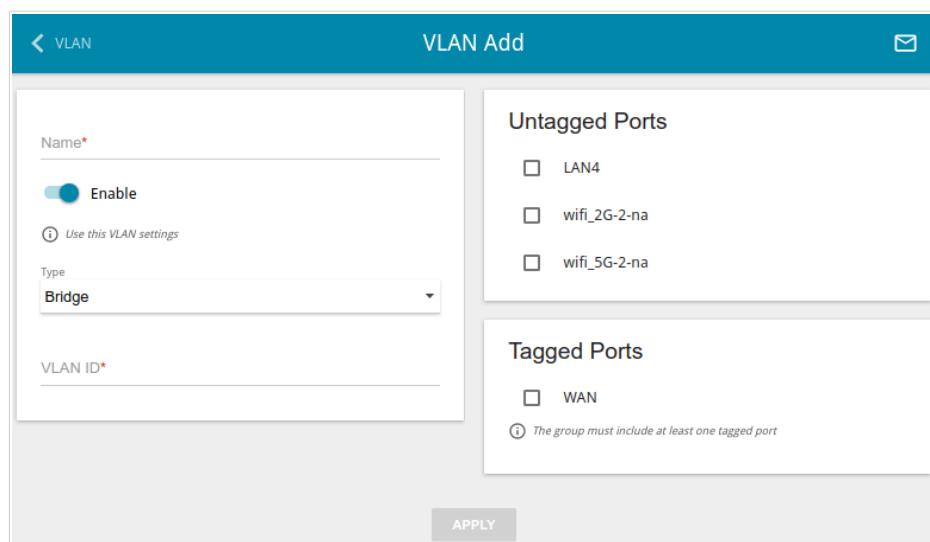


< PIN		VLAN					
VLAN List							
<input type="checkbox"/>	Name	Type	Untagged ports	Tagged port	VLAN ID	Enable	
<input type="checkbox"/>	lan	Untagged LAN	LAN1, LAN2, LAN3, LAN4, wifi_2G-1, wifi_5G-1	-	-	Yes	
<input type="checkbox"/>	wan	Untagged NAT	WAN	-	-	Yes	

Figure 98. The **Advanced / VLAN** page.

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

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



< VLAN

VLAN Add

Name*

Enable

Use this VLAN settings

Type

Bridge

VLAN ID*

Untagged Ports

☐ LAN4

☐ wifi_2G-2-na

☐ wifi_5G-2-na

Tagged Ports

☐ WAN

The group must include at least one tagged port

APPLY

Figure 99. The page for adding a group of ports for VLAN.


You can specify the following parameters:

Parameter	Description
Name	A name for the port for easier identification.
Enable	Move the switch to the right to allow using this group of ports.

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

Click the **APPLY** button.

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

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

DNS

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

The screenshot shows the 'Advanced / DNS' configuration page. The top navigation bar has a blue header with 'VLAN' and 'DNS' tabs. The main content area is titled 'DNS' and includes a descriptive paragraph: 'DNS servers are used to determine the IP address from the name of a server in Intranets or the Internet. 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.' Below this, there are two sections: 'DNS IPv4' and 'DNS IPv6'. Each section has a 'Manual' toggle switch (currently off) and a 'Default gateway' toggle switch (currently on). Under each section, there is an 'Interface' dropdown menu with 'WAN' selected. At the bottom, there is a 'Hosts' section with 'No hosts added' and a '+' icon. An 'APPLY' button is at the bottom left.

Figure 100. The **Advanced / DNS** page.

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

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




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

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

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

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

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

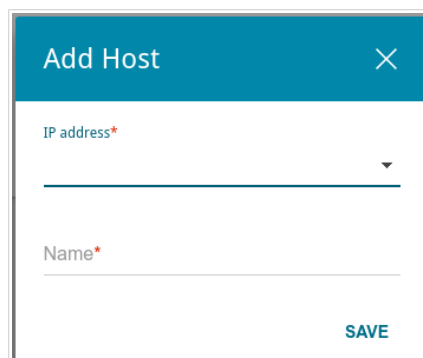



Figure 101. The window for adding a DNS record.

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

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

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

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

DDNS

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

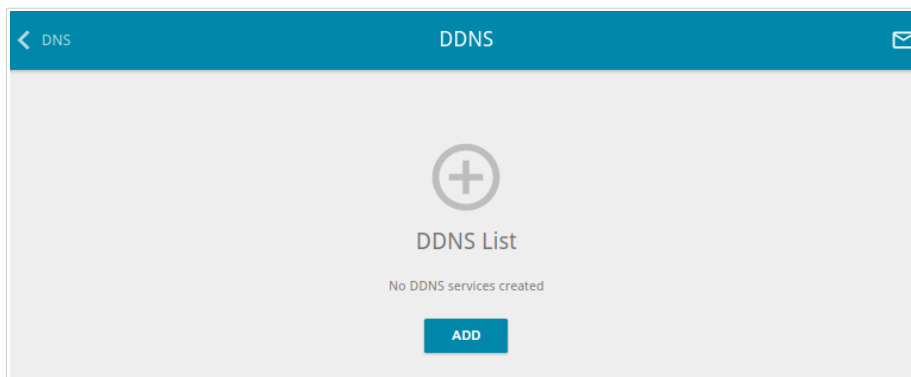


Figure 102. The **Advanced / DDNS** page.



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


Figure 103. The page for adding a DDNS service.

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

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

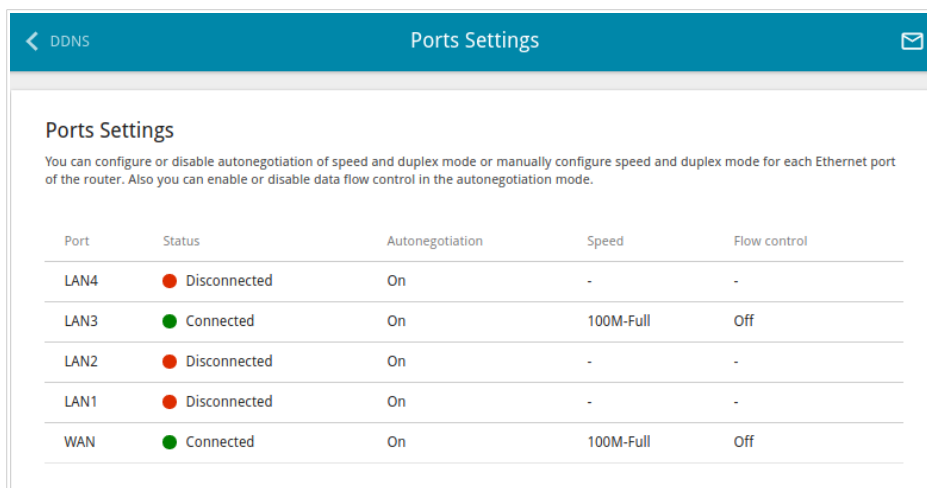
After specifying the needed parameters, click the **SAVE** button.

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

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

Ports Settings

On the **Advanced / Ports Settings** page, you can configure or disable autonegotiation of speed and duplex mode or manually configure speed and duplex mode for each Ethernet port of the router. Also you can enable or disable data flow control in the autonegotiation mode. This function is used for equal load balancing in ISPs' networks. Contact your ISP to clarify if this function needs to be enabled.



Port	Status	Autonegotiation	Speed	Flow control
LAN4	Disconnected	On	-	-
LAN3	Connected	On	100M-Full	Off
LAN2	Disconnected	On	-	-
LAN1	Disconnected	On	-	-
WAN	Connected	On	100M-Full	Off

Figure 104. 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.

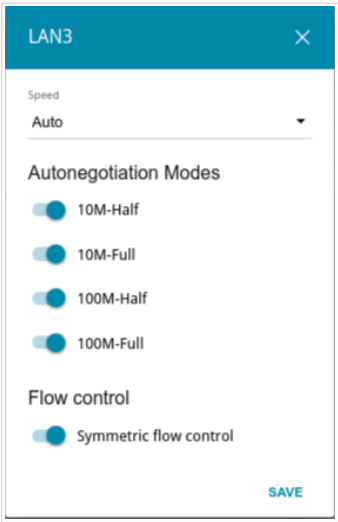


Figure 105. The window for changing the settings of the router's port.

In the opened window, specify the needed parameters:

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

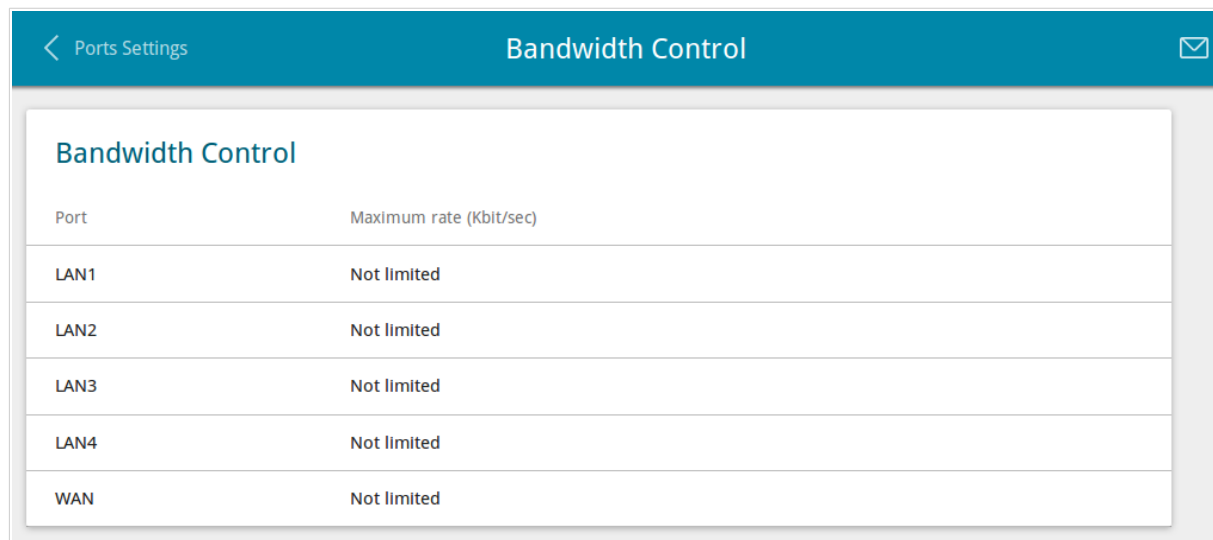
Parameter		Description
Flow control		
Symmetric flow control		Move the switch to the right to enable the flow control function for the port.
		Move the switch to the left to disable the flow control function for the port.

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.

Bandwidth Control

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



Port	Maximum rate (Kbit/sec)
LAN1	Not limited
LAN2	Not limited
LAN3	Not limited
LAN4	Not limited
WAN	Not limited

Figure 106. The **Advanced / Bandwidth Control** page.

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

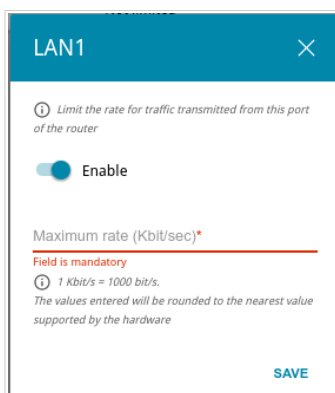


Figure 107. The window for setting up rate limit.

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

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

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.

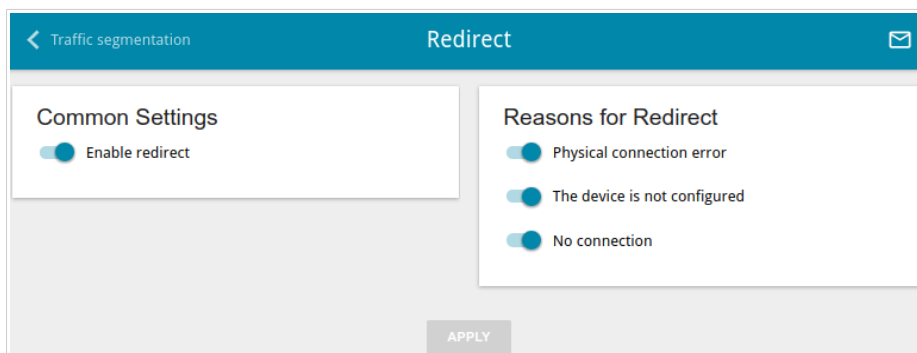


Figure 108. The **Advanced / Redirect** page.

To configure notifications, in the **Common Settings** section, move the **Enable redirect** switch to the right. Then, in the **Reasons for Redirect** section, move the needed switches to the right.

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

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

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

Routing

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

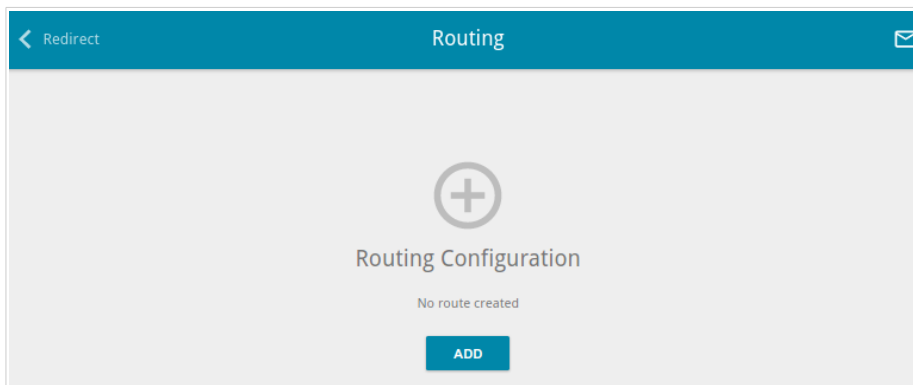


Figure 109. The **Advanced / Routing** page.

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

The screenshot shows a modal dialog box titled 'Add Route' with a close button (X) in the top right corner. The dialog has a white background and a blue header. It contains several input fields: 'Protocol*' with a dropdown menu showing 'IPv4'; 'Interface*' with a dropdown menu showing 'Auto'; 'Destination network*'; 'Destination netmask*'; 'Gateway*'; and 'Metric'. Each field has a red asterisk indicating it is required. At the bottom right of the dialog, there is a blue button labeled 'SAVE'.


Figure 110. The window for adding a new route.

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

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

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

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

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

TR-069 Client

On the **Advanced / TR-069 Client** page, you can configure the router for communication with a remote Auto Configuration Server (ACS).

The TR-069 client is used for remote monitoring and management of the device.

The screenshot shows the 'TR-069 Client' configuration page. The top navigation bar includes a back arrow, 'Routing', and 'TR-069 Client' tabs. The page is divided into four main sections. The first section, 'TR-069 Client', contains an 'Interface' dropdown menu currently set to 'Automatic' and a toggle switch labeled 'Enable TR-069 Client'. The second section, 'Inform Settings', features a toggle switch set to 'On' and an 'Interval (in seconds)' input field with the value '120'. The third section, 'Auto Configuration Server Settings', includes input fields for 'URL address', 'Username', and 'Password'. The fourth section, 'Connection Request Settings', includes input fields for 'Username', 'Password', 'Request port' (pre-filled with '8999'), and 'Request path'. An 'APPLY' button is located at the bottom right of the page.

Figure 111. The page for configuring the TR-069 client.

You can specify the following parameters:

Parameter	Description
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.
Enable TR-069 Client	Move the switch to the right to enable the TR-069 client.
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.

Parameter	Description
Auto Configuration Server Settings	
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS.
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.
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.

Remote Access

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

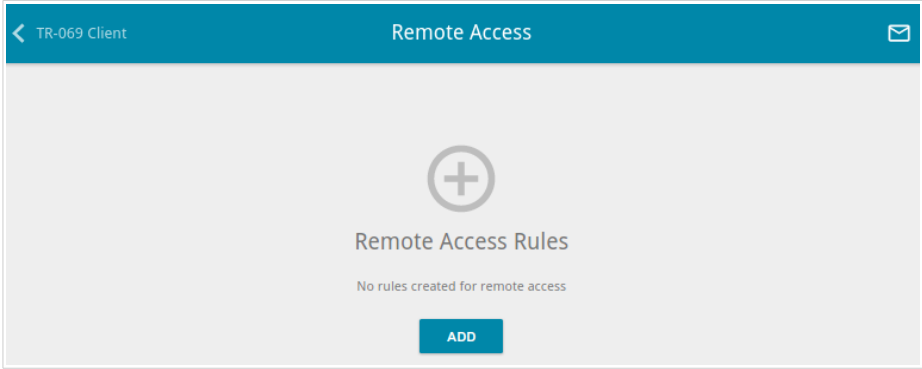


Figure 112. The **Advanced / Remote Access** page.

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

Figure 113. The window for adding a rule for remote management.


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

Parameter	Description
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.

Parameter	Description
IP address	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.
Mask	<i>For the IPv4-based network only.</i> The mask of the subnet.
Public port	<i>For the IPv4-based network only.</i> An external port of the router. You can specify only one port.
Protocol	The protocol available for remote management of the router.

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

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

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

UPnP IGD

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

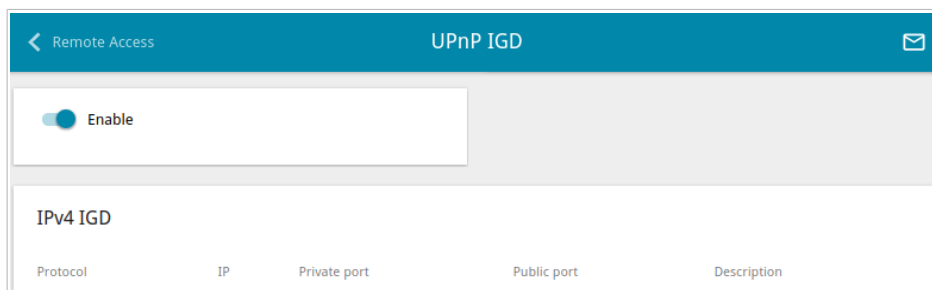


Figure 114. The **Advanced / UPnP IGD** page.

If you want to manually specify all parameters needed for network applications, move the **Enable** switch to the left. Then go to the **Firewall / Virtual Servers** page and specify needed settings.

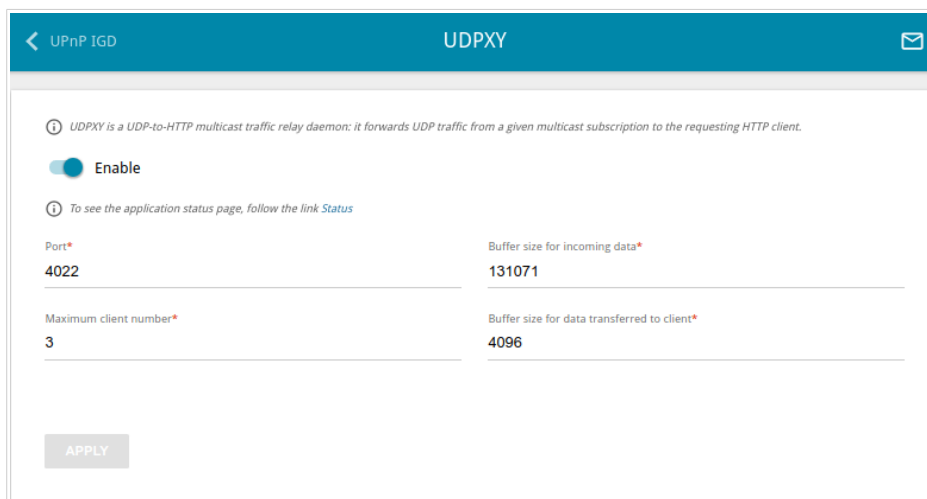
If you want to enable the UPnP IGD protocol in the router, move the **Enable** switch to the right.

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

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

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.



UDPXY is a UDP-to-HTTP multicast traffic relay daemon: it forwards UDP traffic from a given multicast subscription to the requesting HTTP client.

☒ Enable

To see the application status page, follow the link [Status](#)

Port*
4022

Buffer size for incoming data*
131071

Maximum client number*
3

Buffer size for data transferred to client*
4096

APPLY

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

To enable the application, move the **Enable** switch to the right. When the application is enabled, the IGMP Proxy function is automatically disabled.

Upon that the following fields are displayed on the page:

Parameter	Description
Port	The port of the router which the UDPXY application uses.
Maximum client number	Maximum number of devices from the router's LAN which will be served by the application.
Buffer size for incoming data	Size of intermediate buffer for received data. By default, the minimum acceptable value is specified.
Buffer size for data transferred to client	Size of intermediate buffer for transmitted data. By default, the minimum acceptable value is specified.

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

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

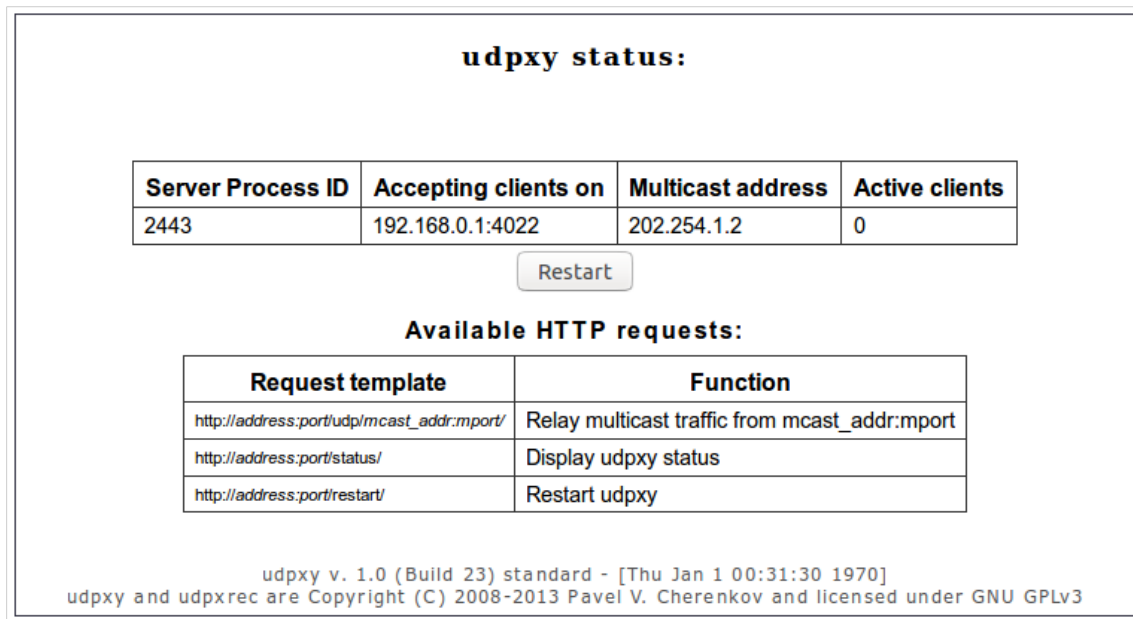


Figure 116. The UDPXY application status page.

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.

The screenshot shows the 'Advanced / IGMP/MLD' configuration page. The page has a teal header with a back arrow, 'Configuration', 'IGMP/MLD', and an envelope icon. The main content area is divided into two columns: IGMP and MLD. The IGMP column includes a description, an 'Enable' toggle (checked), a dropdown for 'IGMP version' (set to 'IGMPv2'), a dropdown for 'Interface' (set to 'Dynamic_IPv4'), and a toggle for 'Set the address of outgoing IGMP packets equal to 0.0.0.0' (unchecked). The MLD column includes a description, an 'Enable' toggle (checked), a dropdown for 'MLD version' (set to 'MLDv1/MLDv2'), and a dropdown for 'Interface' (set to 'Dynamic_IPv6'). An 'APPLY' button is at the bottom left.

Figure 117. 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).
Set the address of outgoing IGMP packets equal to 0.0.0.0		Move the switch to the right if you want all outgoing IGMP packets to have the IP address 0.0.0.0.

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 allow the router to use RTSP, enable the SIP ALG and PPPoE/PPTP/L2TP/IPsec pass through functions.

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

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

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

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

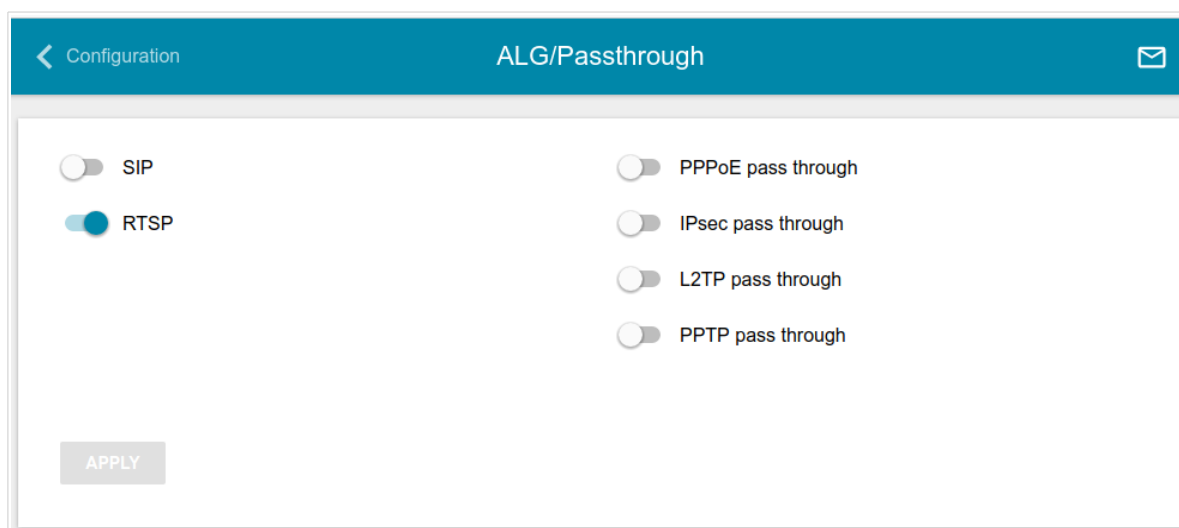


Figure 118. The **Advanced / ALG/Passthrough** page.

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. ⁴
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.

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

⁴ On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / ALG/Passthrough** page, connect an Ethernet cable between a LAN port of the router and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

IPsec

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

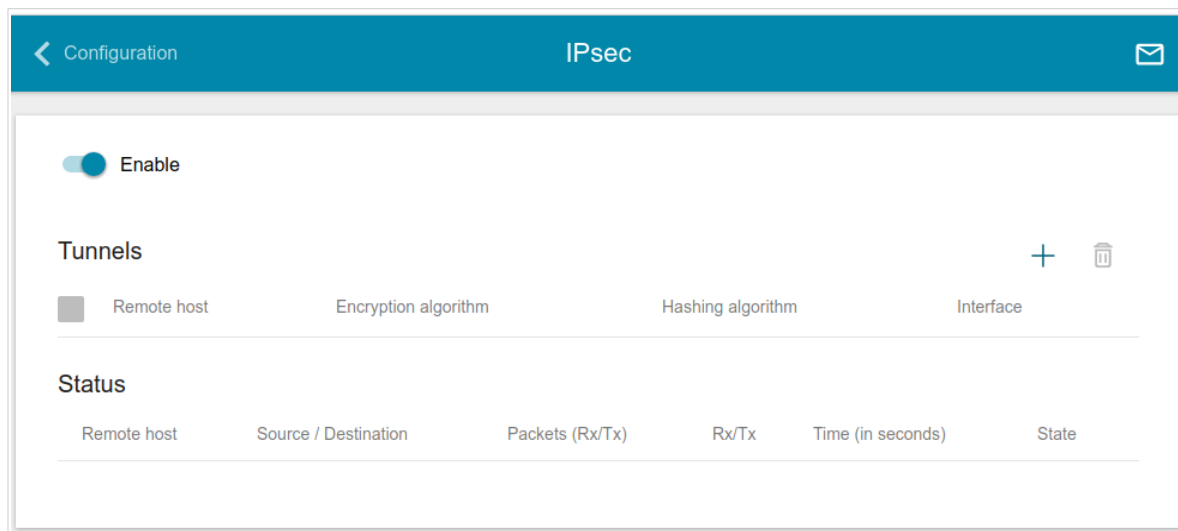


Figure 119. The **Advanced / IPsec** page.

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

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

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



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

Figure 120. The page for adding an IPsec tunnel. The **General Settings** section.

You can specify the following parameters:

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

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


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

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

Figure 121. The page for adding an IPsec tunnel. **The First Phase / The Second Phase** sections.

Parameter	Description
The First Phase	
First phase encryption algorithm	Select encryption algorithm from the drop-down list.
Hashing algorithm	Select hashing algorithm from the drop-down list.
First phase DHgroup type	A Diffie-Hellman key group for Phase 1. Select a value from the drop-down list.
IKE-SA lifetime	The lifetime of IKE-SA keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should exceed the value specified in the IPsec-SA lifetime field. Specify 0 if you don't want to limit the lifetime of the keys.
The Second Phase	
Second phase encryption algorithm	Select encryption algorithm from the drop-down list.
Authentication algorithm	Select authentication algorithm from the drop-down list.
Enable PFS	Move the switch to the right to enable the PFS option (<i>Perfect Forward Secrecy</i>). If the switch is moved to the right, a new encryption key exchange will be used for Phase 2. This option increases the security level of data transfer.
Second phase PFSgroup type	A Diffie-Hellman key group for Phase 2. Select a value from the drop-down list. The field is available, if the Enable PFS switch is moved to the right.

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

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

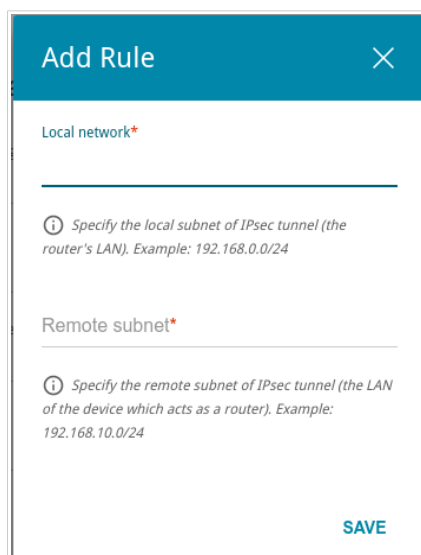



Figure 122. The page for adding an IPsec tunnel. The window for adding a tunneled network.

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


Parameter	Description
Local network	A local subnet IP address and mask.
Remote subnet	A remote subnet IP address and mask.

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

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

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

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

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

To disable VPN tunnels based on IPsec protocol, move the **Enable** switch to the left.

Firewall

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

- add rules for IP filtering
- create virtual servers
- define a DMZ
- configure the MAC filter
- specify restrictions on access to certain web sites
- configure protection against DoS attacks.

IP Filter

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

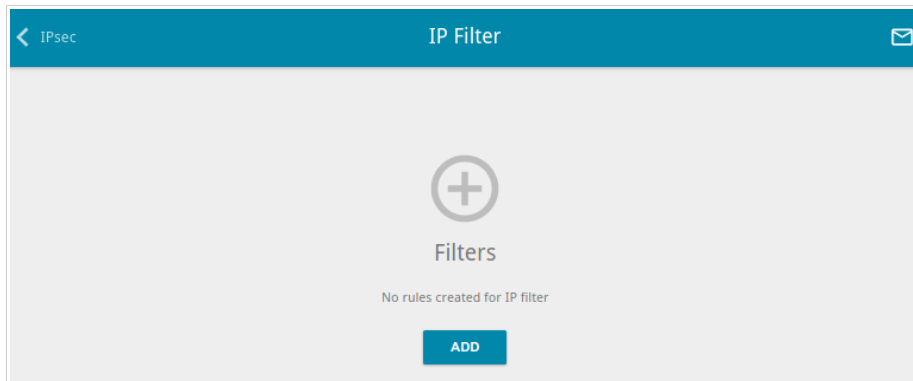


Figure 123. The **Firewall / IP Filter** page.

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

Figure 124. The page for adding a rule for IP filtering.

You can specify the following parameters:


Parameter	Description
General Settings	
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Name	A name for the rule for easier identification. You can specify any name.
Action	Select an action for the rule. Allow: Allows packet transmission in accordance with the criteria specified by the rule. Deny: Denies packet transmission in accordance with the criteria specified by the rule.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.

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

Parameter	Description
Source port	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

Click the **APPLY** button.

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

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

Virtual Servers

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

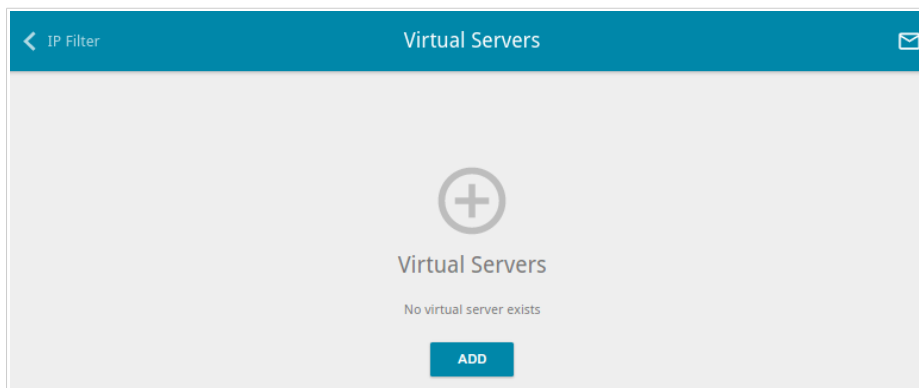


Figure 125. The **Firewall / Virtual Servers** page.


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

Figure 126. The page for adding a virtual server.


You can specify the following parameters:

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

Parameter	Description
Private port (start)/ Private port (end)	A port of the IP address specified in the Private IP field to which traffic is directed from the Public port . Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the Private port (start) field and leave the Private port (end) field blank.

Click the **APPLY** button.

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

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

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.

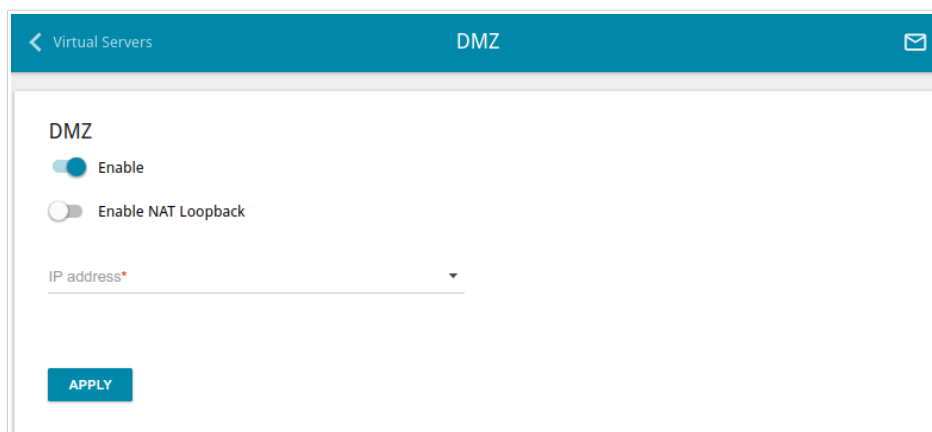


Figure 127. The **Firewall / DMZ** page.

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

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

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

Click the **APPLY** button.

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

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

MAC Filter

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

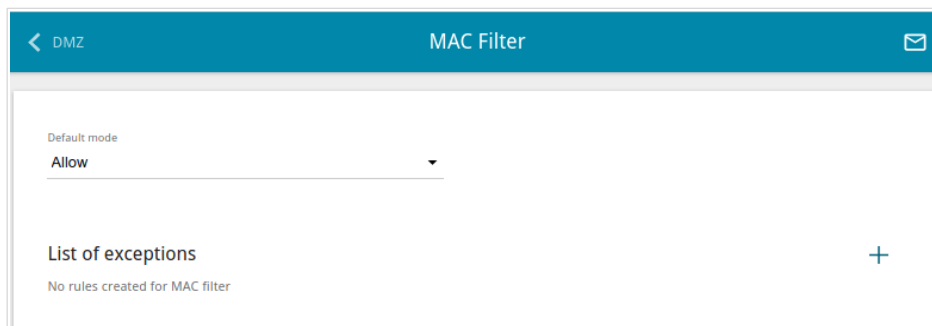


Figure 128. The **Firewall / MAC Filter** page.

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 (**+**).

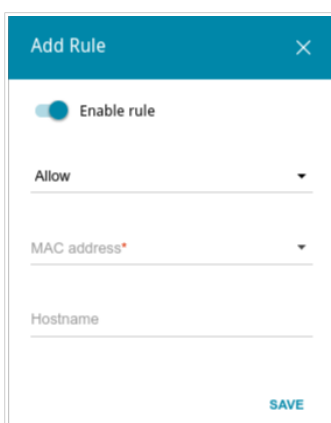



Figure 129. The window for adding a rule for the MAC filter.

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

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

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

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

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

URL Filter


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

The screenshot shows the 'URL Filter' configuration page. At the top, there is a blue header bar with a back arrow, 'MAC Filter', 'URL Filter', and an envelope icon. Below the header, the page title 'URL Filter' is followed by a descriptive text: 'You can specify restrictions on access to certain web sites. Rules can be applied to those devices that are added to the list or to all but devices from the list.' Below this text is an 'Enable' toggle switch, which is currently turned on. The page is divided into two main sections: 'Addresses' and 'Clients'. The 'Addresses' section has a dropdown menu for 'Address filtering' with 'Block listed URLs' selected. Below this is a table with two columns: 'URL address' and 'Match with template'. The 'Clients' section has a dropdown menu for 'Client filtering' with 'All but devices from list' selected. Below this is a table with two columns: 'Name' and 'MAC address'. Both tables have a '+' icon and a trash icon for adding and deleting entries. At the bottom left, there is a blue 'APPLY' button.


Figure 130. The **Firewall / URL Filter** page.

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

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


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


Parameter	Description
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.

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.

In the **Clients** section, you can 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). Then specify a name of the device for easier identification in the **Name** field and click the **SAVE** button.

To remove a client from the list, select the checkbox located to the left of the relevant rule 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.

DoS Protection

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

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

The screenshot shows the 'DoS Protection' configuration page. At the top, there is a blue header bar with a back arrow, 'System Time', 'DoS Protection', and an envelope icon. Below the header, the 'Enable' switch is turned on. A warning icon and text state: 'Enabling DOS filter may lead to a slight decrease in the overall performance of the device'. The page is divided into two main sections: 'Per-source IP Flood' and 'Other Settings'. The 'Per-source IP Flood' section contains four sub-sections, each with a toggle switch and a threshold value: 'TCP/SYN' (enabled, 200 pps), 'TCP/FIN' (enabled, 200 pps), 'UDP' (enabled, 200 pps), and 'ICMP' (enabled, 200 pps). The 'Other Settings' section contains seven toggle switches: 'TCP/UDP port scan' (disabled), 'IP Land' (disabled), 'IP Spoof' (disabled), 'IP TearDrop' (disabled), 'TCP scan' (disabled), 'TCP/SYN with data' (disabled), and 'UDP Bomb' (disabled). Below these is the 'Block source IP' toggle (enabled) and a 'Block time (sec)' field set to 120. An 'APPLY' button is at the bottom right.

Figure 131. The **Firewall / DoS Protection** page.

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

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

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

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

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

Parameter	Description
TCP/UDP port scan	<p>Blocks the source of TCP or UDP packets which check the ports state if the router receives more than 200 requests per second from one IP address. The source of packets will be blocked during the time period specified in the Block time field (the field is displayed if the Block source IP switch is moved to the right).</p> <p>If the switch is moved to the right, the High sensitivity switch is displayed on the page. Activate the setting to let the router block the source if it sends more than 10 requests per second.</p>
IP Land	Blocks TCP packets with the SYN flag in which the source IP address and port coincides with the destination IP address and port.
IP Spoof	Block packets in which the source IP address coincides with the router's LAN IP address.
IP TearDrop	Blocks fragmented IP packets if errors can occur upon assembling these packets.
TCP scan	Blocks TCP packets with invalid flags.
TCP/SYN with data	Blocks TCP packets with the SYN flag if they are fragmented or contain data.

Parameter	Description
UDP Bomb	Blocks UDP packets if they contain incorrect service data.
Block source IP	Move the switch to the right to block the sources of packets protection against which is activated in the Other Settings section for a certain time period. Then, in the Block time field displayed, specify the needed value (in seconds).

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

System

In this menu you can do the following:

- change the password used to access the router's settings
- restore the factory default settings
- create a backup of the router's configuration
- restore the router's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the router
- change the web-based interface language
- update the firmware of the router
- configure automatic notification on new firmware version
- view the system log; configure sending the system log to a remote host
- check availability of a host on the Internet through the web-based interface of the router
- trace the route to a host
- allow or forbid access to the router via TELNET
- configure automatic synchronization of the system time or manually configure the date and time for the router.

Configuration

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

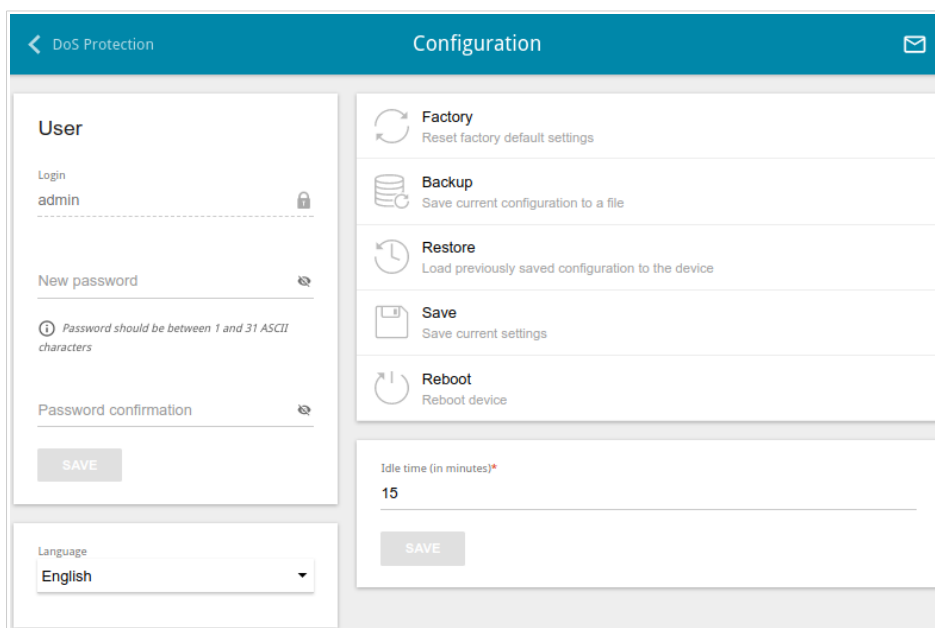


Figure 132. The **System / Configuration** page.

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.⁵ Click the **Show** icon (👁) to display the entered values. Then click the **SAVE** button.



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

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

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

The following buttons are also available on the page:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button (see the <i>Back and Bottom Panels</i> section, page 16).
Backup	Click the button to save the configuration (all settings of the router) to your PC. The configuration backup will be stored in the download location of your web browser.
Restore	Click the button and follow the dialog box appeared to select a previously saved configuration file (all settings of the router) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The router saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

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

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.

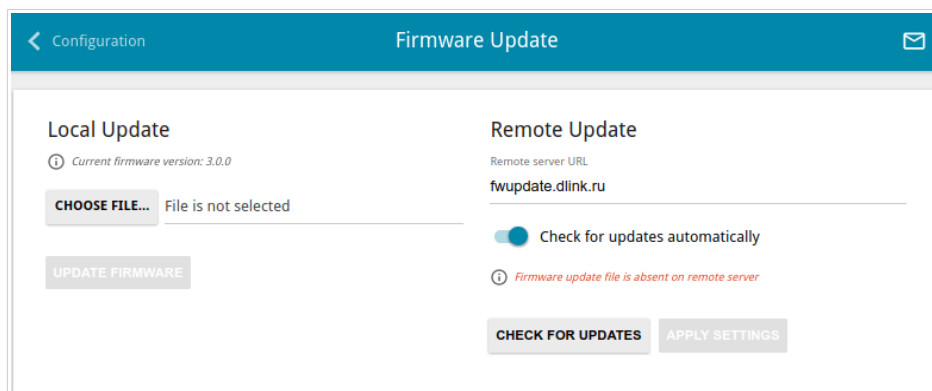


Figure 133. The **System / Firmware Update** page.

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

By default, the automatic check for the router's firmware updates is enabled. If a firmware update is available, a notification will be displayed in the top right corner of the page.

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

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

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

Local Update



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

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

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

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

Remote Update



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

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

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

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

Log

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

The screenshot shows the 'Log' page with the 'Settings' tab selected. Under the 'Logging' section, there is a message 'You can set the system log options'. An 'Enable' toggle switch is turned on. Below it, the 'Type' dropdown is set to 'Remote and local', and the 'Level' dropdown is set to 'Informational messages'. There is a 'Server*' text field and a 'Port*' dropdown set to '514'. An 'APPLY' button is at the bottom.

Figure 134. The **System / Log** page. The **Settings** tab.

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

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

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

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

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

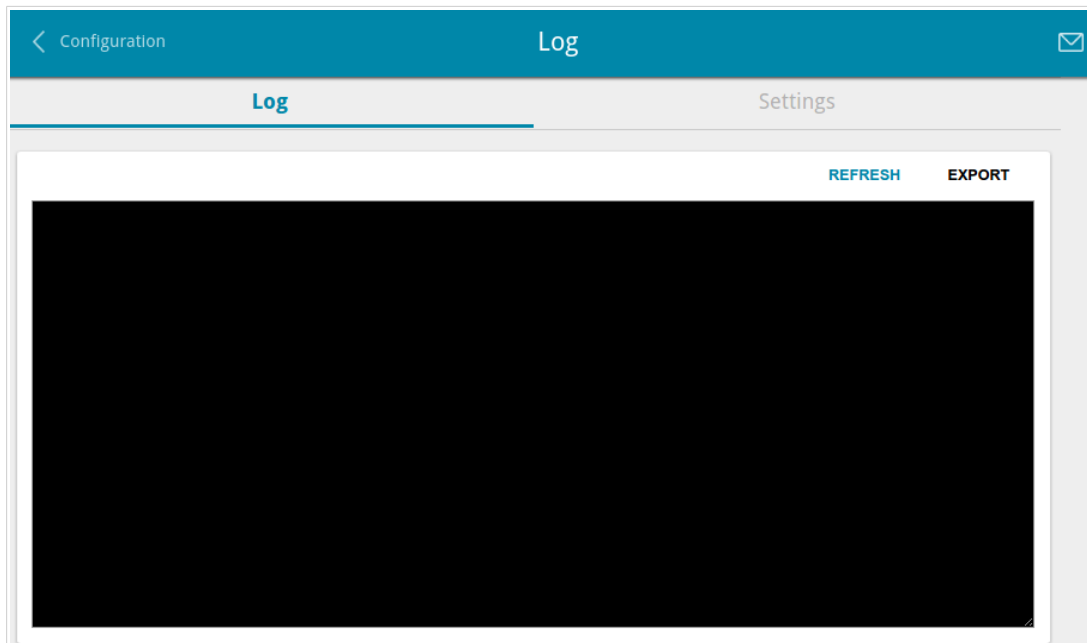


Figure 135. The **System / Log** page. The **Log** tab.

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

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

Ping

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

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

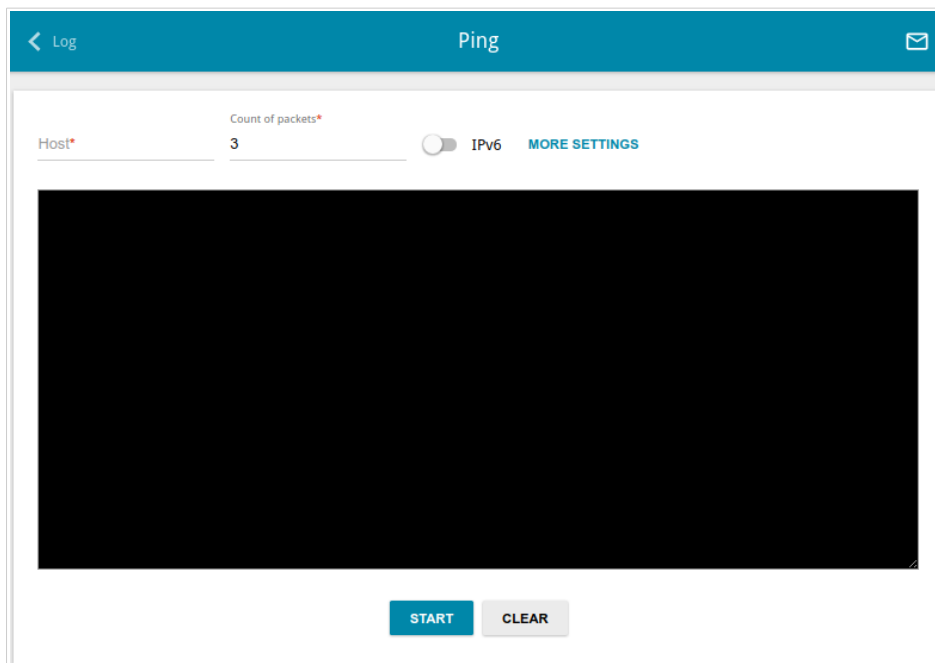
The screenshot shows the 'Ping' utility page. At the top, there's a blue header with a back arrow, 'Log', and 'Ping' text, and a mail icon. Below the header, there's a form with a 'Host*' field, a 'Count of packets*' field set to '3', an 'IPv6' toggle switch, and a 'MORE SETTINGS' link. A large black rectangular area occupies the center of the page. At the bottom, there are 'START' and 'CLEAR' buttons.

Figure 136. The **System / Ping** page.

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

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

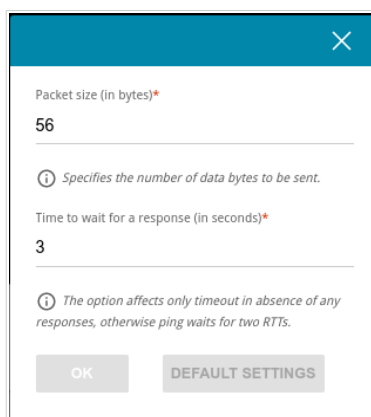
The screenshot shows a modal window titled 'Additional settings'. It has a close button (X) in the top right corner. Inside, there are two fields: 'Packet size (in bytes)*' with a value of '56' and a tooltip that says 'Specifies the number of data bytes to be sent.'; and 'Time to wait for a response (in seconds)*' with a value of '3' and a tooltip that says 'The option affects only timeout in absence of any responses, otherwise ping waits for two RTTs.' At the bottom, there are 'OK' and 'DEFAULT SETTINGS' buttons.

Figure 137. The **System / Ping** page. The additional settings window.

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

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

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

Traceroute

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

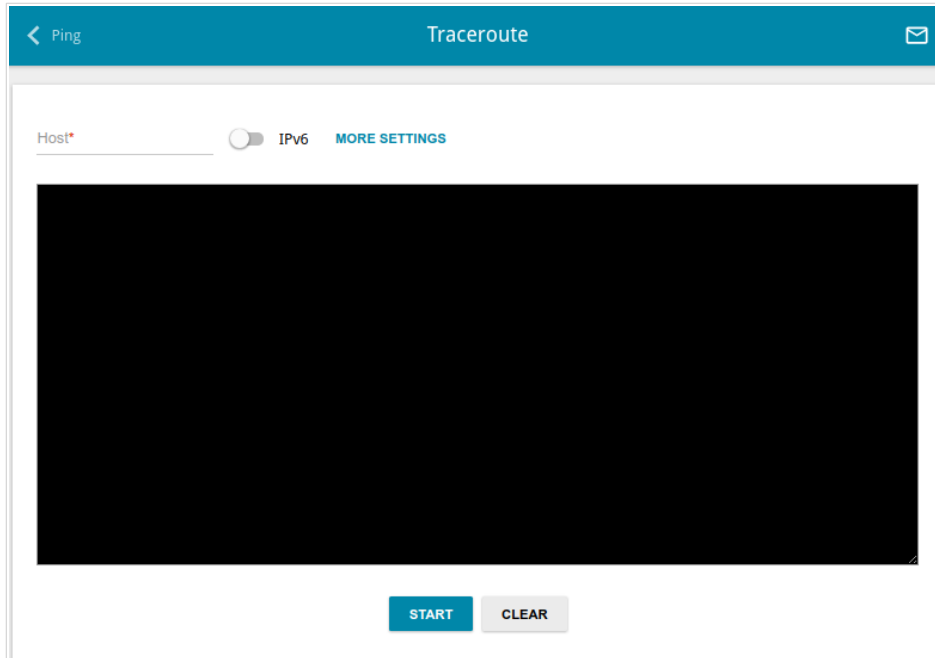
The screenshot shows the 'Traceroute' page in a web-based interface. At the top, there is a blue header bar with a back arrow and the text 'Ping' on the left, and 'Traceroute' in the center, with an envelope icon on the right. Below the header, there is a form area. On the left, there is a label 'Host*' followed by a text input field. To the right of the input field is a toggle switch labeled 'IPv6', which is currently turned off. Further right is a link labeled 'MORE SETTINGS'. Below these elements is a large black rectangular area, likely a placeholder for the traceroute results. At the bottom of the form, there are two buttons: a blue 'START' button and a grey 'CLEAR' button.

Figure 138. The **System / Traceroute** page.

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

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

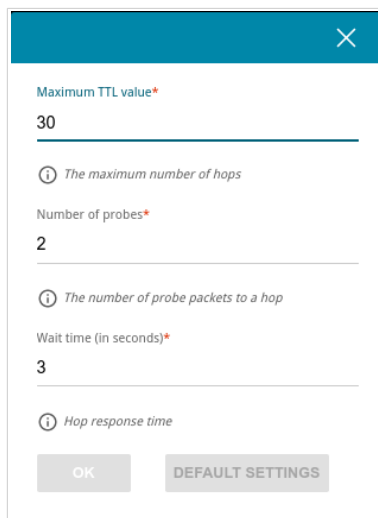


Figure 139. The **System** / **Traceroute** page. The additional settings window.

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

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

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

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

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

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

Telnet

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

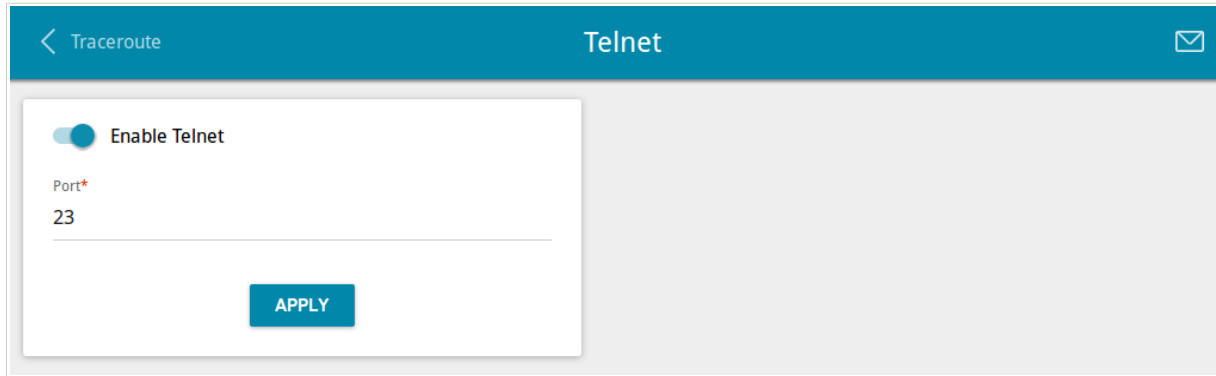


Figure 140. The **System / Telnet** page.

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

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

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.

The screenshot shows the 'System Time' configuration page. At the top, there's a blue header with a back arrow, 'Telnet', 'System Time', and an envelope icon. Below the header, the page is titled 'System time' with a subtitle: 'You can set up automatic synchronization the system time with a time server on the Internet.' The main content area is divided into several sections. On the left, there's a toggle switch for 'Enable NTP' which is currently turned on. Below this, there are input fields for 'System date:' (showing '25.10.2018') and 'System time:' (showing '14:23'). To the right of these fields is the 'NTP Settings' section, which includes three toggle switches: 'Daylight saving time' (off), 'Get NTP server addresses using DHCP' (off), and 'Run as a server for the local network' (off). Below the NTP Settings is the 'NTP Servers' section, which shows a list with 'pool.ntp.org' and an 'ADD SERVER' button. To the right of the NTP Servers is a 'Change time zone' dropdown menu, which is currently set to 'GMT+03:00'. Below the dropdown, a list of time zones is visible: Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Volgograd, Nairobi, Tehran, Bahrain, Turkey, Iraq, Iran, Qatar, Kuwait, Saudi Arabia. At the bottom of the page, there are two buttons: 'APPLY' and 'DETERMINE TIMEZONE'.

Figure 141. The **System / System Time** page.

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

1. Move the **Enable NTP** switch to the left.
2. In the **Time Settings** section, specify needed values. To specify the time set up your PC or portable device, click the **SET LOCAL TIME** button.
3. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

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

1. Move the **Enable NTP** switch to the right.
2. Specify the needed NTP server or leave the value specified by default in the **NTP Servers** section. If you need to specify several servers, click the **ADD SERVER** button.
3. Select your time zone from the **Change time zone** drop-down list in the **NTP Settings** section. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.
4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

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

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

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



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

Yandex.DNS

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

Yandex.DNS is a web content filtering service which provides the DNS server, protects a computer against malicious web sites, and blocks access to adult web sites.

Settings

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

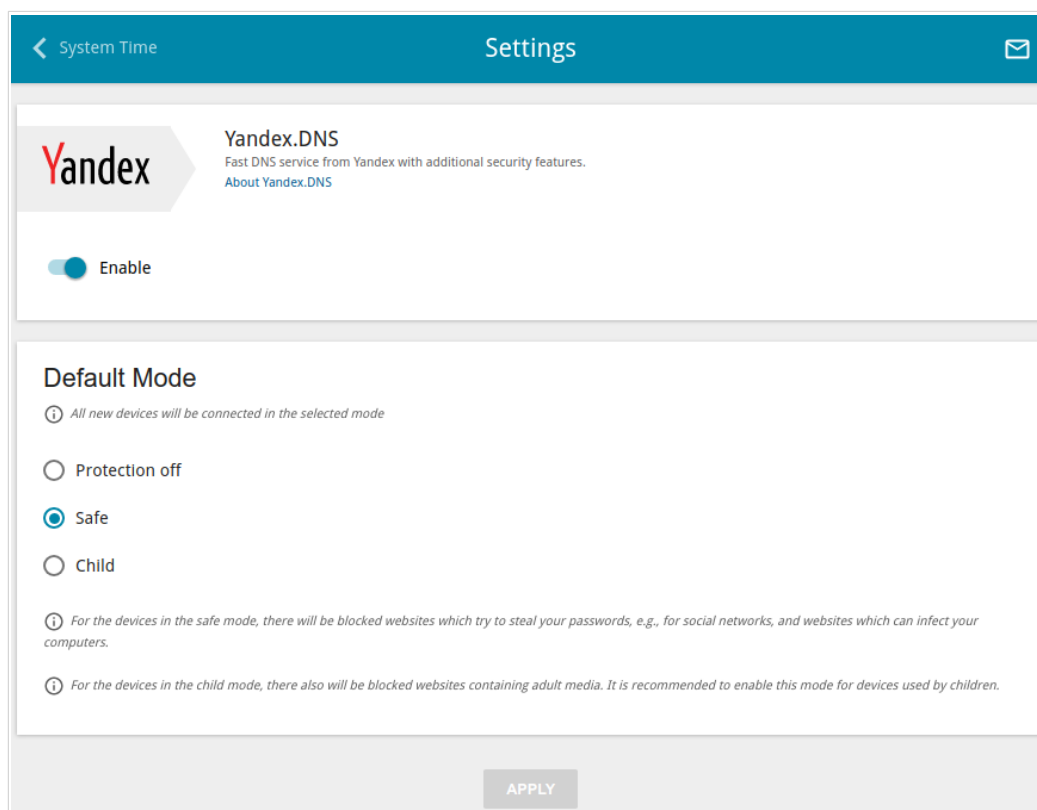


Figure 142. The **Yandex.DNS / Settings** page.

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

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

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

- **Protection off**: when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites;
- **Safe**: when this value is selected, the service blocks access to malicious and fraudulent web sites;
- **Child**: when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

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

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

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

Devices and Rules

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

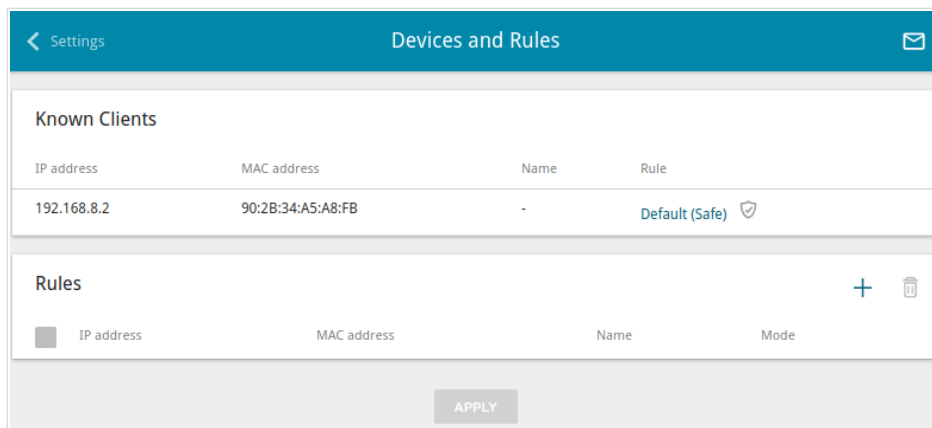



Figure 143. The **Yandex.DNS / Devices and Rules** page.

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

To create⁶ a new filtering rule for a device, click the **ADD** button () in the **Rules** section, or left-click the name of the filtering mode in the line of the device for which a rule should be created in the **Known Clients** section.

MAC address*

IP address

ADD

Name

☐ Protection off

☒ Safe

☐ Child

SAVE

Figure 144. Adding a new rule for the **Yandex.DNS** service.

⁶ When a new rule for filtering is created, a MAC address and IP address pair is displayed on the **Connections Setup / LAN** page. The created pair will be deleted with the relevant rule.

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

Parameter	Description
MAC address	The MAC address of a device from the router's LAN.
IP address	<p>The IP address of a device from the router's LAN.</p> <p>To assign several fixed IP addresses to a device with a certain MAC address, click the ADD button, and in the line displayed, enter an IP address. A device of your LAN can have one IPv4 address and several IPv6 addresses.</p> <p>To remove the IP address, click the Delete icon (✕) in the line of the address.</p>
Name	Enter a name for the rule for easier identification. <i>Optional.</i>
Mode	<p>Select an operating mode of the Yandex.DNS service for this rule.</p> <p>Protection off: when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites.</p> <p>Safe: when this value is selected, the service blocks access to malicious and fraudulent web sites.</p> <p>Child: when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.</p>

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

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

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

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

CHAPTER 5. OPERATION GUIDELINES

Safety Rules and Conditions

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

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

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

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

The service life of the device is 2 years.

Wireless Installation Considerations

The DIR-841 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-841 device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).
2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone is not in use.

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

AC	Access Category
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BSSID	Basic Service Set Identifier
CRC	Cyclic Redundancy Check
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTIM	Delivery Traffic Indication Message
GMT	Greenwich Mean Time
IGD	Internet Gateway Device
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PBC	Push Button Configuration
PIN	Personal Identification Number

PPPoE	Point-to-point protocol over Ethernet
PPTP	Point-to-point tunneling protocol
PSK	Pre-shared key
QoS	Quality of Service
RADIUS	Remote Authentication in Dial-In User Service
RIP	Routing Information Protocol
RTS	Request To Send
RTSP	Real Time Streaming Protocol
SIP	Session Initiation Protocol
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup