



## **DIR-853**

### **AC1300 Wave 2 MU-MIMO Wi-Fi Gigabit Router with 3G/LTE Support and USB Port**

## Contents

<b>Chapter 1. Introduction.....</b>	<b>6</b>
Contents and Audience.....	6
Conventions.....	6
Document Structure.....	6
<b>Chapter 2. Overview.....</b>	<b>7</b>
General Information.....	7
Specifications.....	9
Product Appearance.....	17
Upper Panel.....	17
Back Panel.....	19
Delivery Package.....	21
<b>Chapter 3. Installation and Connection.....</b>	<b>22</b>
Before You Begin.....	22
Connecting to Mobile Device with D-Link Assistant Application.....	23
Connecting to PC.....	24
PC with Ethernet Adapter.....	24
Obtaining IP Address Automatically (OS Windows 7).....	25
Obtaining IP Address Automatically (OS Windows 10).....	30
PC with Wi-Fi Adapter.....	35
Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 7).....	36
Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 10).....	39
Connecting to Web-based Interface.....	42
Web-based Interface Structure.....	44
Summary Page.....	44
Home Page.....	46
Menu Sections.....	47
Notifications.....	48
<b>Chapter 4. Configuring via Web-based Interface.....</b>	<b>49</b>
Initial Configuration Wizard.....	49
Selecting Operation Mode.....	51
Router.....	51
Access Point or Repeater.....	53
Creating 3G/LTE WAN Connection.....	54
Changing LAN IPv4 Address.....	56
Wi-Fi Client.....	57
Configuring Wired WAN Connection.....	59
Static IPv4 Connection.....	60
Static IPv6 Connection.....	61
PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections.....	62
PPPoE + Static IP (PPPoE Dual Access) Connection.....	63
PPTP + Dynamic IP or L2TP + Dynamic IP Connection.....	64
PPTP + Static IP or L2TP + Static IP Connection.....	65
Configuring Wireless Network.....	66
Configuring LAN Ports for IPTV/VoIP.....	68
Changing Web-based Interface Password.....	70
Connection of Multimedia Devices.....	72

<b>Statistics</b>	<b>75</b>
Network Statistics	75
DHCP	76
Routing	77
Clients and Sessions	79
Port Statistics	80
Multicast Groups	81
IPsec Statistics	82
VPN Statistics	83
<b>Connections Setup</b>	<b>84</b>
WAN	84
Creating Dynamic IPv4 or Static IPv4 WAN Connection	86
Creating Dynamic IPv6 or Static IPv6 WAN Connection	89
Creating PPPoE WAN Connection	92
Creating PPTP, L2TP, L2TP Dual Stack, or L2TP over IPsec WAN Connection	97
Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection	104
Creating Mobile Internet WAN Connection	110
Creating IPIP6 WAN Connection	116
Creating 6in4 WAN Connection	119
Creating 6to4 WAN Connection	121
Creating 6rd WAN Connection	122
LAN	124
IPv4	124
IPv6	130
WAN Failover	135
Auto Configuration of 3G/LTE	138
Traffic Balancing	140
<b>VPN</b>	<b>142</b>
IPsec	142
GRE	151
IPIP	153
PPTP/L2TP Servers	155
VPN Users	161
EoGRE	162
EoIP	164
<b>Wi-Fi</b>	<b>167</b>
Basic Settings	167
Client Management	178
WPS	179
Using WPS Function via Web-based Interface	181
Using WPS Function without Web-based Interface	182
WMM	183
Client	186
Additional	189
MAC Filter	193
Roaming	196
<b>Print Server</b>	<b>198</b>

<b>USB Storage</b>	<b>199</b>
Information	199
USB Users	200
Samba	201
FTP	203
Filebrowser	205
DLNA	206
Torrent Client	208
XUPNPD	212
<b>USB Modem</b>	<b>214</b>
Basic Settings	215
SMS	218
USSD	220
<b>Advanced</b>	<b>221</b>
VLAN	222
WAN Assignment	225
<i>Using LAN Ports as WAN Ports</i>	225
<i>Using WAN Port as LAN Port</i>	226
SNMP	227
DNS	230
DDNS	232
Ports Settings	234
Redirect	237
Routing	238
TR-069 Client	240
Port Mirroring	242
UPnP	244
UDPHY	246
IGMP/MLD	248
ALG/Passthrough	250
CoovaChilli	252
VRRP	256
Wake-on-LAN	259
<b>Firewall</b>	<b>260</b>
IP Filter	260
Virtual Servers	266
DMZ	270
MAC Filter	272
URL Filter	274
AdBlock	277
Remote Access	278

<b>System</b>	<b>281</b>
Configuration	282
<i>Creating Configuration Backup</i>	285
Buttons Configuration	286
Firmware Update	288
<i>Local Update</i>	290
<i>Remote Update</i>	291
Schedule	292
Logging	297
<i>Local</i>	297
<i>Remote</i>	299
<i>Record to File</i>	301
Ping	303
Traceroute	305
Telnet/SSH	307
System Time	308
Auto Provision	311
<b>SkyDNS</b>	<b>313</b>
Settings	314
Devices and Rules	316
<b>Chapter 5. Operation Guidelines</b>	<b>318</b>
<b>Terms and Conditions for Installation, Safe Operation,</b>	
<b>Storage, Transportation, and Disposal</b>	<b>318</b>
<b>Wireless Installation Considerations</b>	<b>319</b>
<b>Chapter 6. Abbreviations and Acronyms</b>	<b>320</b>


## CHAPTER 1. INTRODUCTION

### Contents and Audience

This manual describes the router DIR-853 and explains how to configure and operate it.

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

### Conventions

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

### Document Structure

**Chapter 1** describes the purpose and structure of the document.

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

**Chapter 3** explains how to install the router DIR-853 and configure a PC in order to access its web-based interface.

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

**Chapter 5** includes safety instructions and tips for networking.

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

## CHAPTER 2. OVERVIEW

### General Information

The DIR-853 device is a wireless dual band gigabit router with 3G/LTE support. It provides a fast and simple way to create a wireless and wired network at home or in an office.

The router is equipped with a USB port for connecting a USB modem<sup>1</sup>, which can be used to establish connection to the Internet. In addition, to the USB port of the router you can connect a USB storage device, which will be used as a network drive, or a printer.

In order to use the multifunction USB port effectively, the router supports simultaneous operation of several USB devices. For example, you can access multimedia content of the connected HDD storage and at the same time share a USB printer.<sup>2</sup>

You can use any Ethernet port of the router as LAN or WAN port. The new-generation firmware supports assigning several WAN ports, for example, in order to configure the primary and backup WAN connection of different ISPs. In addition, you can configure the WAN failover using a 3G/4G modem.

Also you are able to connect the wireless router DIR-853 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-853 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 1300Mbps<sup>3</sup>).

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

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

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.

1 Not included in the delivery package. D-Link does not guarantee compatibility with all USB modems. For the list of supported USB modems, see the *Specifications* section, page 9.

2 When using a USB hub with external power supply.

3 Up to 400Mbps for 2.4GHz and up to 867Mbps for 5GHz.

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-853 includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

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

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

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

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

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

You can configure the settings of the wireless router DIR-853 via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

The configuration wizard allows you to quickly switch DIR-853 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-853 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"><li>MT7621DAT (880MHz, dual core)</li></ul>
RAM	<ul style="list-style-type: none"><li>128MB, DDR3</li></ul>
Flash	<ul style="list-style-type: none"><li>128MB, NAND</li></ul>
Interfaces	<ul style="list-style-type: none"><li>10/100/1000BASE-T WAN port</li><li>4 10/100/1000BASE-T LAN ports</li><li>USB 2.0 port</li></ul>
LEDs	<ul style="list-style-type: none"><li>Power</li><li>Internet</li><li>4 LAN LEDs</li><li>WLAN 2.4G</li><li>WLAN 5G</li><li>WPS</li><li>USB</li></ul>
Buttons	<ul style="list-style-type: none"><li>POWER button to power on/power off</li><li>WIFI button to enable/disable wireless network</li><li>WPS button to set up wireless connection</li><li>RESET button to restore factory default settings</li></ul>
Antenna	<ul style="list-style-type: none"><li>Four external non-detachable antennas (5dBi gain)</li></ul>
MIMO	<ul style="list-style-type: none"><li>2 x 2, MU-MIMO</li></ul>
Power connector	<ul style="list-style-type: none"><li>Power input connector (DC)</li></ul>
Mounting	<ul style="list-style-type: none"><li>Desktop</li><li>Wall</li></ul>

Software	
WAN connection types	<ul style="list-style-type: none"><li>Mobile Internet (via supported USB modem)</li><li>PPPoE</li><li>IPv6 PPPoE</li><li>PPPoE Dual Stack</li><li>Static IPv4 / Dynamic IPv4</li><li>Static IPv6 / Dynamic IPv6</li><li>PPPoE + Static IP (PPPoE Dual Access)</li><li>PPPoE + Dynamic IP (PPPoE Dual Access)</li><li>PPTP/L2TP + Static IP</li><li>PPTP/L2TP + Dynamic IP</li><li>L2TP Dual Stack</li><li>IPV6 in DSLite mode</li><li>6in4</li><li>6to4</li><li>6rd</li></ul>

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

Software	
<b>Network functions</b>	<ul style="list-style-type: none"> <li>• DHCP server/relay</li> <li>• Advanced configuration of built-in DHCP server</li> <li>• Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation</li> <li>• Automatic obtainment of LAN IP address (for access point/repeater/client modes)</li> <li>• DNS relay</li> <li>• Dynamic DNS</li> <li>• Static IPv4/IPv6 routing</li> <li>• IGMP/MLD Proxy</li> <li>• RIP</li> <li>• Support of UPnP</li> <li>• Support of VLAN</li> <li>• WAN ping respond</li> <li>• Support of SIP ALG</li> <li>• Support of RTSP</li> <li>• WAN failover</li> <li>• LAN/WAN conversion</li> <li>• Multi-WAN support</li> <li>• Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port</li> <li>• Built-in UDPXY application</li> <li>• XUPNPD plug-in</li> <li>• Equal load distribution while using several WAN connections (traffic balancing)</li> <li>• Support of VRRP</li> <li>• Port mirroring</li> <li>• Wake-on-LAN support</li> </ul>
<b>Firewall functions</b>	<ul style="list-style-type: none"> <li>• Network Address Translation (NAT)</li> <li>• Stateful Packet Inspection (SPI)</li> <li>• IPv4/IPv6 filter</li> <li>• MAC filter</li> <li>• URL filter</li> <li>• Ad blocking function</li> <li>• DMZ</li> <li>• Virtual servers</li> <li>• Built-in SkyDNS web content filtering service</li> </ul>
<b>VPN</b>	<ul style="list-style-type: none"> <li>• IPsec/PPTP/L2TP/PPPoE pass-through</li> <li>• PPTP/L2TP servers</li> <li>• PPTP/L2TP tunnels</li> <li>• L2TP over IPsec client</li> <li>• GRE/EoGRE/EoIP/IPIP tunnels</li> <li>• IPsec tunnels</li> <li>• Transport/Tunnel mode</li> <li>• IKEv1/IKEv2 support</li> <li>• DES encryption</li> <li>• NAT Traversal</li> <li>• Support of DPD (Keep-alive for VPN tunnels)</li> </ul>
<b>USB interface functions</b>	<ul style="list-style-type: none"> <li>• USB modem <ul style="list-style-type: none"> <li>Auto connection to available type of supported network (4G/3G/2G)</li> <li>Auto configuration of connection upon plugging in USB modem</li> <li>Enabling/disabling PIN code check, changing PIN code<sup>4</sup></li> <li>Sending/receiving/reading/removing SMS messages<sup>4</sup></li> <li>Support of USSD requests<sup>4</sup></li> </ul> </li> <li>• USB storage <ul style="list-style-type: none"> <li>File browser</li> <li>Print server</li> <li>Access to storage via accounts</li> <li>Built-in Samba server</li> <li>Built-in FTP server supporting TLS</li> <li>Built-in DLNA server</li> <li>Built-in Transmission torrent client; uploading/downloading files from/to USB storage</li> </ul> </li> </ul>

<sup>4</sup> For some models of USB modems.

Software	
<b>Management and monitoring</b>	<ul style="list-style-type: none"> <li>Local and remote access to settings through SSH/TELNET/WEB (HTTP/HTTPS)</li> <li>Bilingual web-based interface for configuration and management (Russian/English)</li> <li>Support of D-Link Assistant application for Android smartphones</li> <li>Notification on connection problems and auto redirect to settings</li> <li>Firmware update via web-based interface</li> <li>Automatic notification on new firmware version</li> <li>Saving/restoring configuration to/from file</li> <li>Support of logging to remote host/connected USB storage</li> <li>Automatic synchronization of system time with NTP server and manual time/date setup</li> <li>Ping utility</li> <li>Traceroute utility</li> <li>TR-069 client</li> <li>SNMP agent</li> <li>Schedules for rules and settings of firewall, automatic reboot and saving a configuration backup to a connected USB storage, and enabling/disabling wireless network and Wi-Fi filter</li> <li>Automatic upload of configuration file from ISP's server (Auto Provision)</li> <li>Configuration of action for hardware buttons</li> </ul>

Wireless Module Parameters	
<b>Standards</b>	<ul style="list-style-type: none"> <li>IEEE 802.11ac Wave 2</li> <li>IEEE 802.11a/b/g/n</li> <li>IEEE 802.11k/v</li> </ul>
<b>Frequency range</b>  <i>The frequency range depends upon the radio frequency regulations applied in your country</i>	<ul style="list-style-type: none"> <li>2400 ~ 2483.5MHz</li> <li>5150 ~ 5350MHz</li> <li>5650 ~ 5850MHz</li> </ul>
<b>Wireless connection security</b>	<ul style="list-style-type: none"> <li>WEP</li> <li>WPA/WPA2 (Personal/Enterprise)</li> <li>WPA3 (Personal)</li> <li>MAC filter</li> <li>WPS (PBC/PIN)</li> </ul>
<b>Advanced functions</b>	<ul style="list-style-type: none"> <li>Support of client mode</li> <li>WMM (Wi-Fi QoS)</li> <li>Information on connected Wi-Fi clients</li> <li>Advanced settings</li> <li>Smart adjustment of Wi-Fi clients</li> <li>Guest Wi-Fi / support of MBSSID</li> <li>Limitation of wireless network rate</li> <li>Periodic scan of channels, automatic switch to least loaded channel</li> <li>Support of 2.4GHz/5GHz TX Beamforming</li> <li>Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence)</li> <li>Support of STBC</li> <li>CoovaChilli authentication portal</li> </ul>

Wireless Module Parameters	
<b>Wireless connection rate<sup>5</sup></b>	<ul style="list-style-type: none"> <li>IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54Mbps</li> <li>IEEE 802.11b: 1, 2, 5.5, and 11Mbps</li> <li>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps</li> <li>IEEE 802.11n (2.4GHz): 6.5–300Mbps (MCS0–MCS15) to 400Mbps (QAM256)</li> <li>IEEE 802.11n (5GHz): from 6.5 to 300Mbps (from MCS0 to MCS15)</li> <li>IEEE 802.11ac (5GHz): from 6.5 to 867Mbps (from MCS0 to MCS9)</li> </ul>
<b>Transmitter output power</b>  <i>The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country</i>	<ul style="list-style-type: none"> <li>2.4GHz Less than 20dBm (100mW)</li> <li>5GHz Less than 19dBm (79.4mW)</li> </ul>
<b>Receiver sensitivity</b>	<ul style="list-style-type: none"> <li>802.11a (typical at PER &lt; 10% (1000-byte PDUs) at room temperature 25 °C) <ul style="list-style-type: none"> <li>-82dBm at 6Mbps</li> <li>-81dBm at 9Mbps</li> <li>-79dBm at 12Mbps</li> <li>-77dBm at 18Mbps</li> <li>-74dBm at 24Mbps</li> <li>-70dBm at 36Mbps</li> <li>-66dBm at 48Mbps</li> <li>-65dBm at 54Mbps</li> </ul> </li> <li>802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C) <ul style="list-style-type: none"> <li>-80dBm at 1Mbps</li> <li>-80dBm at 2Mbps</li> <li>-76dBm at 5.5Mbps</li> <li>-76dBm at 11Mbps</li> </ul> </li> <li>802.11g (typical at PER &lt; 10% (1000-byte PDUs) at room temperature 25 °C) <ul style="list-style-type: none"> <li>-82dBm at 6Mbps</li> <li>-81dBm at 9Mbps</li> <li>-79dBm at 12Mbps</li> <li>-77dBm at 18Mbps</li> <li>-74dBm at 24Mbps</li> <li>-70dBm at 36Mbps</li> <li>-66dBm at 48Mbps</li> <li>-65dBm at 54Mbps</li> </ul> </li> </ul>

<sup>5</sup> Maximum wireless signal rate is derived from IEEE standard 802.11ac and 802.11n specifications. In order to get the rate of 400Mbps in the 2.4GHz band, a Wi-Fi client should support MIMO 2x2 and QAM256 modulation scheme. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

## Wireless Module Parameters

	<ul style="list-style-type: none"> <li>802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) 2.4GHz, HT20 -82dBm at MCS0/8 -79dBm at MCS1/9 -77dBm at MCS2/10 -74dBm at MCS3/11 -70dBm at MCS4/12 -66dBm at MCS5/13 -65dBm at MCS6/14 -64dBm at MCS7/15 2.4GHz, HT40 -79dBm at MCS0/8 -76dBm at MCS1/9 -74dBm at MCS2/10 -71dBm at MCS3/11 -67dBm at MCS4/12 -63dBm at MCS5/13 -62dBm at MCS6/14 -61dBm at MCS7/15 5GHz, HT20 -82dBm at MCS0/8 -79dBm at MCS1/9 -77dBm at MCS2/10 -74dBm at MCS3/11 -70dBm at MCS4/12 -66dBm at MCS5/13 -65dBm at MCS6/14 -64dBm at MCS7/15 5GHz, HT40 -79dBm at MCS0/8 -76dBm at MCS1/9 -74dBm at MCS2/10 -71dBm at MCS3/11 -67dBm at MCS4/12 -63dBm at MCS5/13 -62dBm at MCS6/14 -61dBm at MCS7/15</li> <li>802.11ac (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) VHT20 -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 VHT40 -79dBm at MCS0 -76dBm at MCS1 -74dBm at MCS2 -71dBm at MCS3 -67dBm at MCS4 -63dBm at MCS5 -62dBm at MCS6 -61dBm at MCS7 -56dBm at MCS8 -54dBm at MCS9</li> </ul>
--	--

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

Physical Parameters	
Dimensions (L x W x H)	<ul style="list-style-type: none"> <li>205 x 136 x 44 mm (8.07 x 5.35 x 1.73 in)</li> </ul>

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

## Supported USB modems<sup>6</sup>

### GSM

- Alcatel X500
- D-Link DWM-152C1
- D-Link DWM-156A6
- D-Link DWM-156A7
- D-Link DWM 156A8
- D-Link DWM-156C1
- D-Link DWM-157B1
- D-Link DWM-157B1 (Velcom)
- D-Link DWM-158D1
- D-Link DWR-710
- Huawei E150
- Huawei E1550
- Huawei E156G
- Huawei E160G
- Huawei E169G
- Huawei E171
- Huawei E173 (Megafon)
- Huawei E220
- Huawei E3131 (MTS 420S)
- Huawei E352 (Megafon)
- Huawei E3531
- Prolink PHS600
- Prolink PHS901
- ZTE MF112
- ZTE MF192
- ZTE MF626
- ZTE MF627
- ZTE MF652
- ZTE MF667
- ZTE MF668
- ZTE MF752

<sup>6</sup> The manufacturer does not guarantee proper operation of the router with every modification of the firmware of USB modems.

Supported USB modems	
LTE	<ul style="list-style-type: none"><li>· Alcatel IK40V</li><li>· Brovi E3372-325</li><li>· D-Link DWM-222</li><li>· D-Link DWR-910 (revision D1)</li><li>· Huawei E3131</li><li>· Huawei E3272</li><li>· Huawei E3351</li><li>· Huawei E3372s</li><li>· Huawei E3372h-153</li><li>· Huawei E3372h-320</li><li>· Huawei E367</li><li>· Huawei E392</li><li>· Megafon M100-1</li><li>· Megafon M100-2</li><li>· Megafon M100-3</li><li>· Megafon M100-4</li><li>· Megafon M150-1</li><li>· Megafon M150-2</li><li>· Megafon M150-3</li><li>· Megafon M150-4</li><li>· Quanta 1K6E (Beeline 1K6E)</li><li>· MTS 824F</li><li>· MTS 827F</li><li>· Yota LU-150</li><li>· Yota WLTUBA-107</li><li>· ZTE MF823</li><li>· ZTE MF823D</li><li>· ZTE MF827</li><li>· ZTE MF833T</li><li>· ZTE MF833V</li></ul>
Smartphones in USB tethering mode	<ul style="list-style-type: none"><li>· Some models of Android smartphones</li></ul>



## Product Appearance

### Upper Panel



Figure 1. Upper panel view.

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

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

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

## Back Panel



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 <b>WLAN 2.4G</b> and <b>WLAN 5G</b> 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, press the button, hold it for 2 seconds, and release. The <b>WPS</b> LED should start blinking.
USB	A port for connecting a USB device (modem, storage, printer).
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
<b>POWER</b>	A button to turn the router on/off.

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

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

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

## ***Delivery Package***

The following should be included:

- Router DIR-853
- Power adapter DC 12V/1A
- Ethernet cable
- “***Quick Installation Guide***” (brochure).

The “***User Manual***” and “***Quick Installation Guide***” documents are available on D-Link website (see [www.dlink.ru](http://www.dlink.ru)).



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

## CHAPTER 3. INSTALLATION AND CONNECTION

### *Before You Begin*

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

#### **Computer or Mobile Device**

Configuration of the wireless dual band gigabit router with 3G/LTE support DIR-853 (hereinafter referred to as “the router”) is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

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

#### **PC Web Browser**

The following web browsers are recommended:

- Apple Safari 14 and later for macOS
- Microsoft Edge 40 and later for Windows OS
- Mozilla Firefox 55 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.

#### **USB Modem**

To connect to an LTE or 3G network, you should use a USB modem. Connect it to the USB port of the router, then access the web-based interface of the router, and you will be able to configure a connection to the Internet<sup>7</sup>.

Your USB modem should be equipped with an active SIM card of your operator.

Some operators require subscribers to activate their USB modems prior to using them.



Please, refer to connection guidelines provided by your operator when concluding the agreement or placed on its website.

For some models of USB modems, it is required to disable the PIN code check on the SIM card prior to connecting the USB modem to the router.

---

<sup>7</sup> Contact your operator to get information on the service coverage and fees.

## Connecting to Mobile Device with D-Link Assistant Application

1. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
2. Turn on the router by pressing the **POWER** button on its back panel.
3. Make sure that the Wi-Fi connection on your mobile device is on. To switch it on, go to the mobile device settings.
4. In the list of available wireless networks on your mobile device, select the wireless network **DIR-853** (for operating in the 2.4GHz band) or **DIR-853-5G** (for operating in the 5GHz band).
5. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) as the password and connect to the wireless network of DIR-853.
6. Launch D-Link Assistant application on your mobile device. The application is available for Android smartphones in Google Play.



*D-Link Assistant for Android*

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

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

If you changed the administrator password via the web-based interface, when DIR-853 is accessed with the application the next time, click the **ENTER LOGIN/PASSWORD** button. Enter the username (**admin**) and the password you specified.

## Connecting to PC

### PC with Ethernet Adapter

1. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
2. **To connect via USB modem:** connect your USB modem to the USB port<sup>8</sup> located on the back panel of the router.



In some cases you will need to reboot the router after connection of the USB modem.

3. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
4. Turn on the router by pressing the **POWER** button on its back panel.

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

---

<sup>8</sup> It is recommended to use a USB extension cable to connect a USB modem to the router.



## Obtaining IP Address Automatically (OS Windows 7)

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

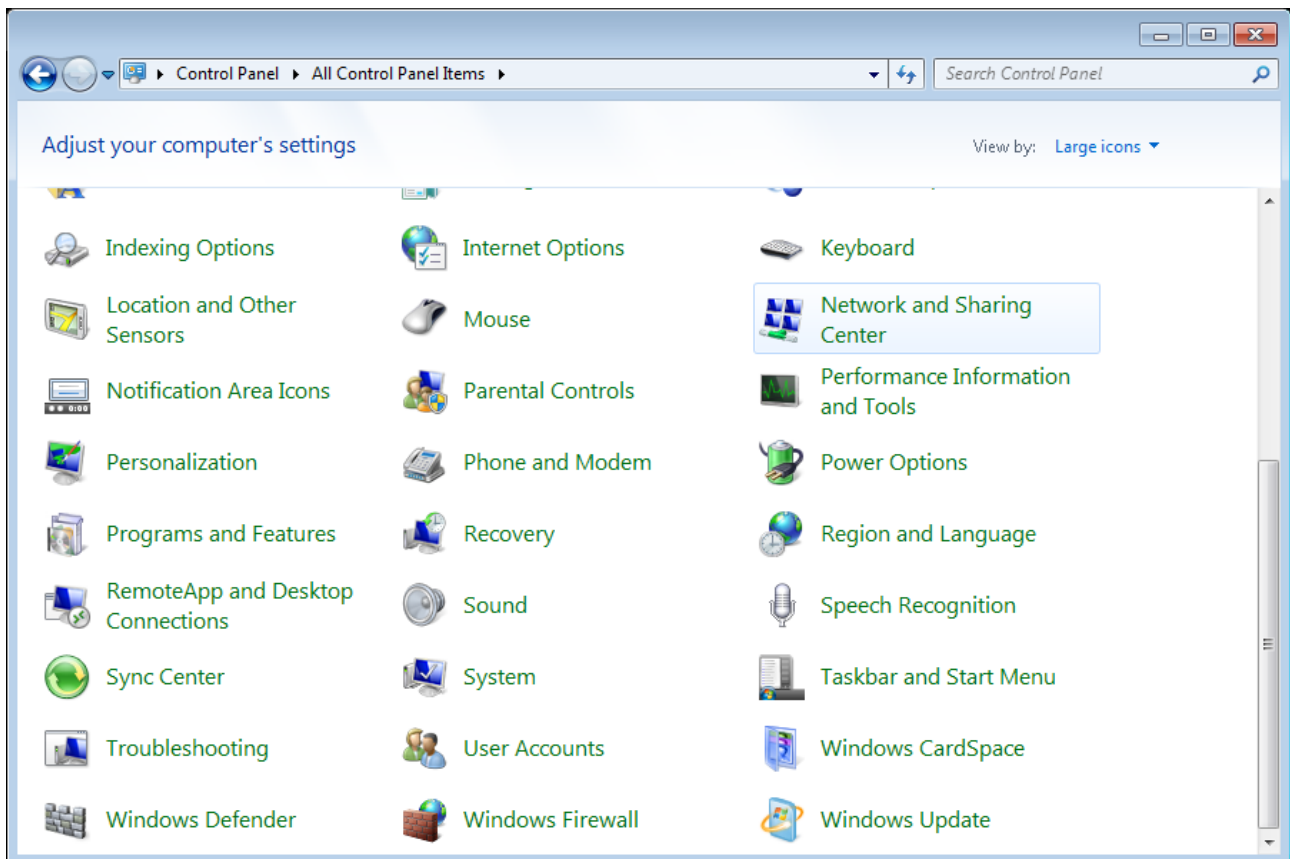


Figure 3. The **Control Panel** window.

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

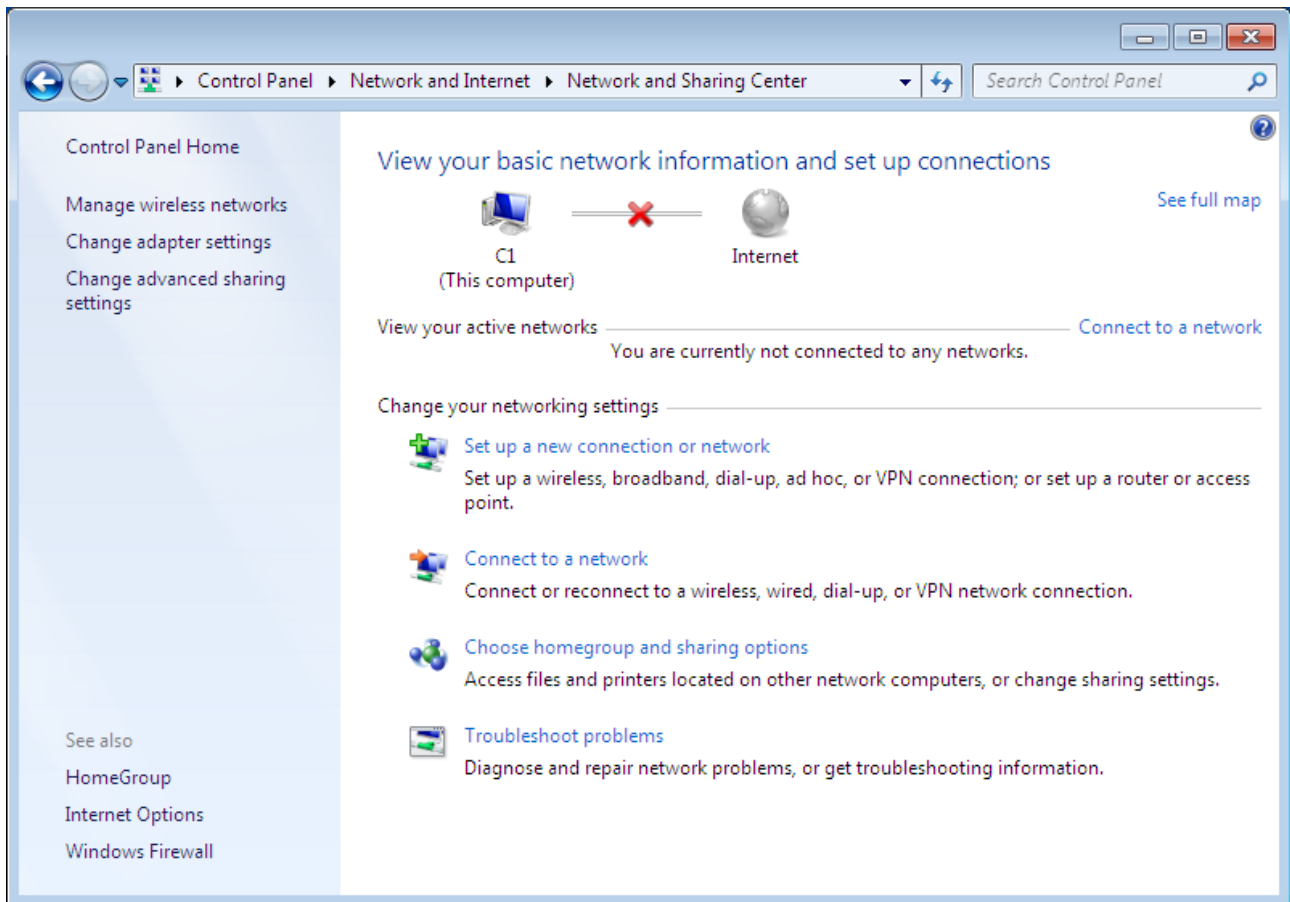


Figure 4. The **Network and Sharing Center** window.

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

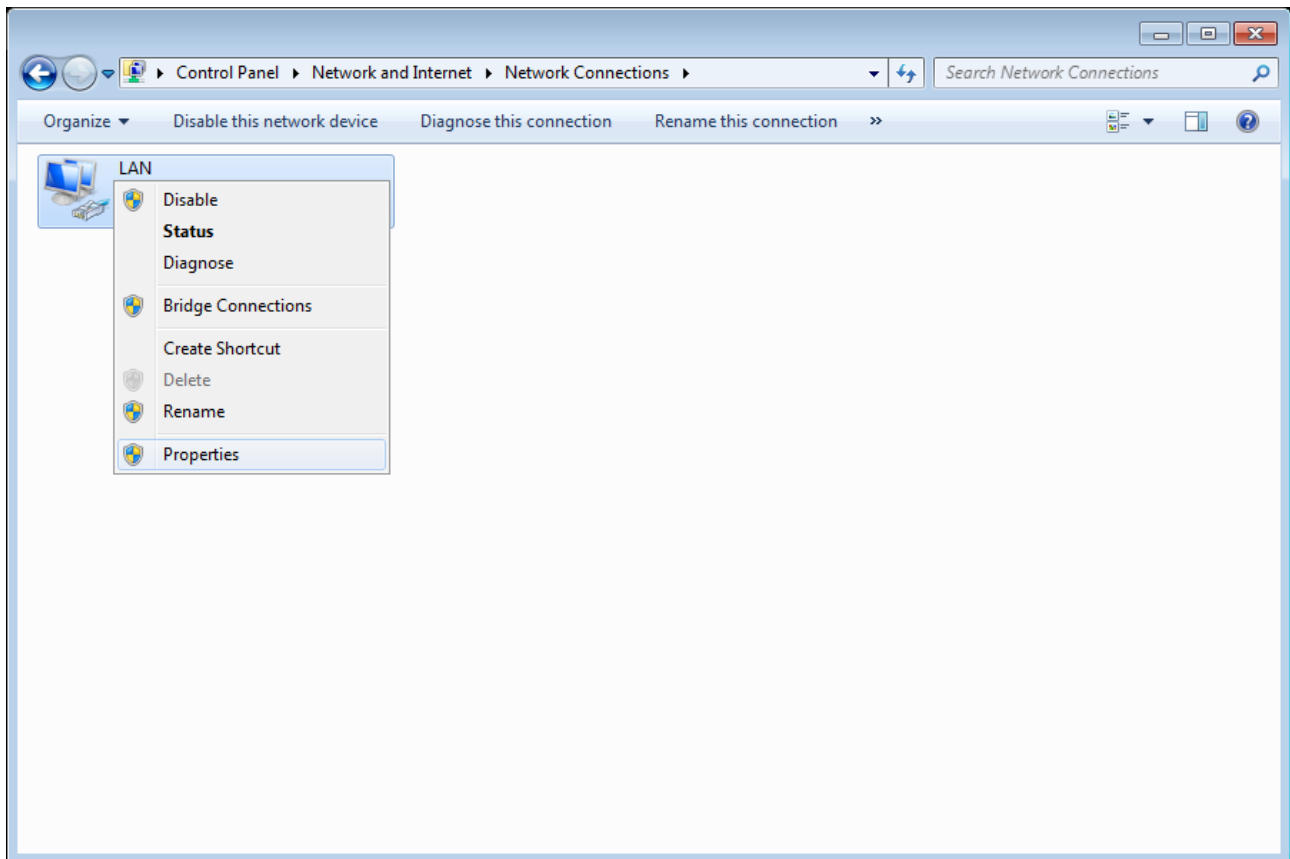


Figure 5. The **Network Connections** window.

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

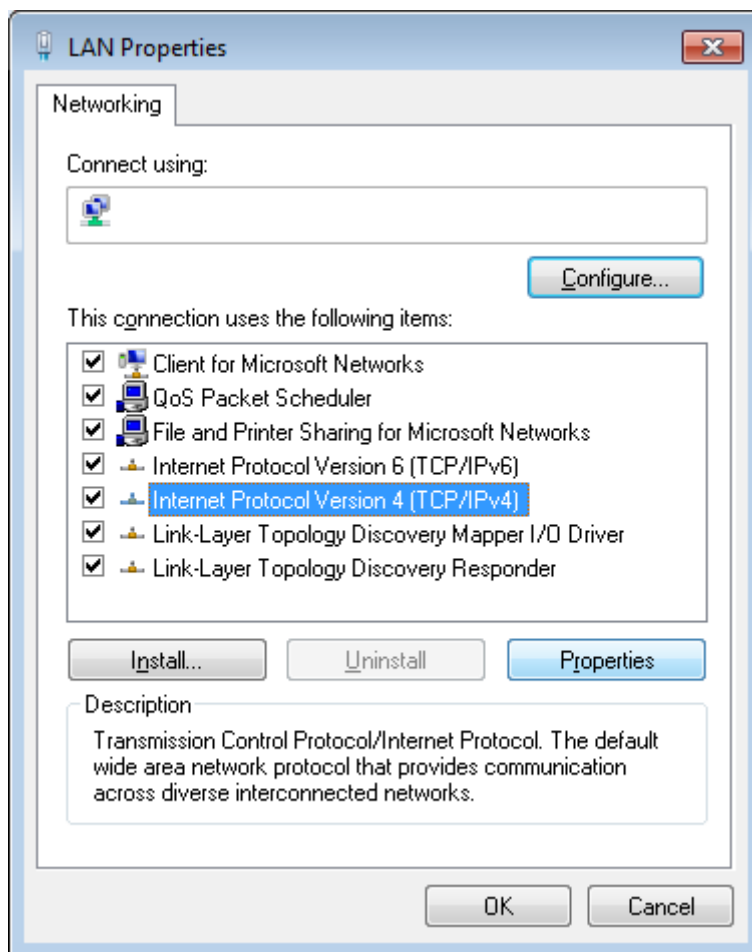


Figure 6. The **Local Area Connection Properties** window.

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

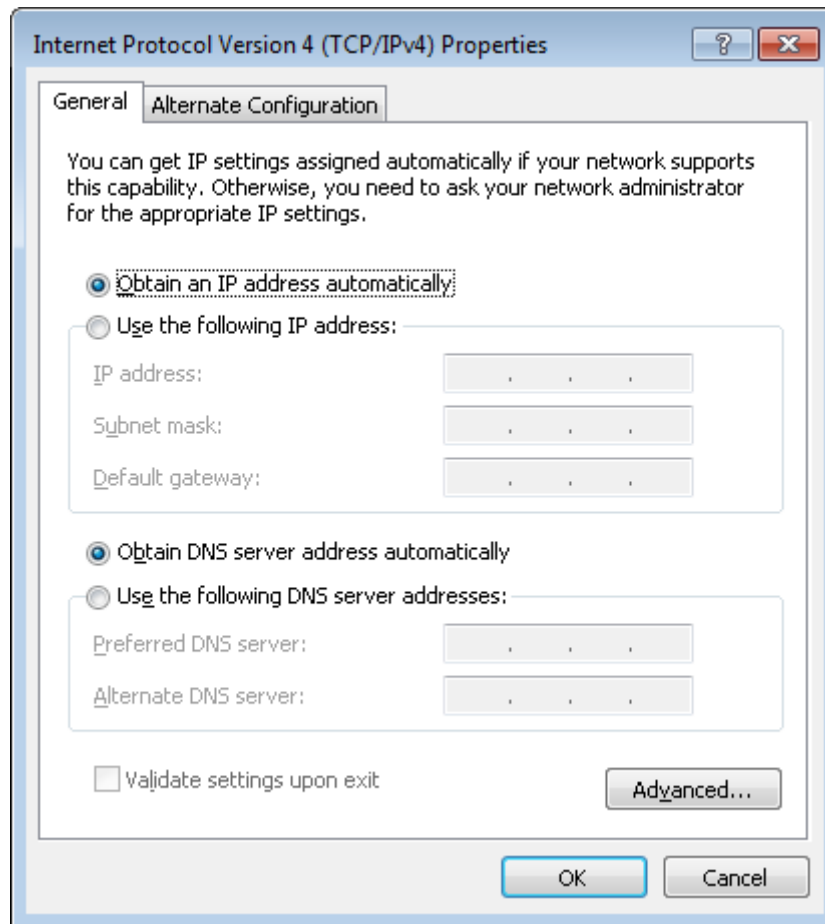


Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

## Obtaining IP Address Automatically (OS Windows 10)

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

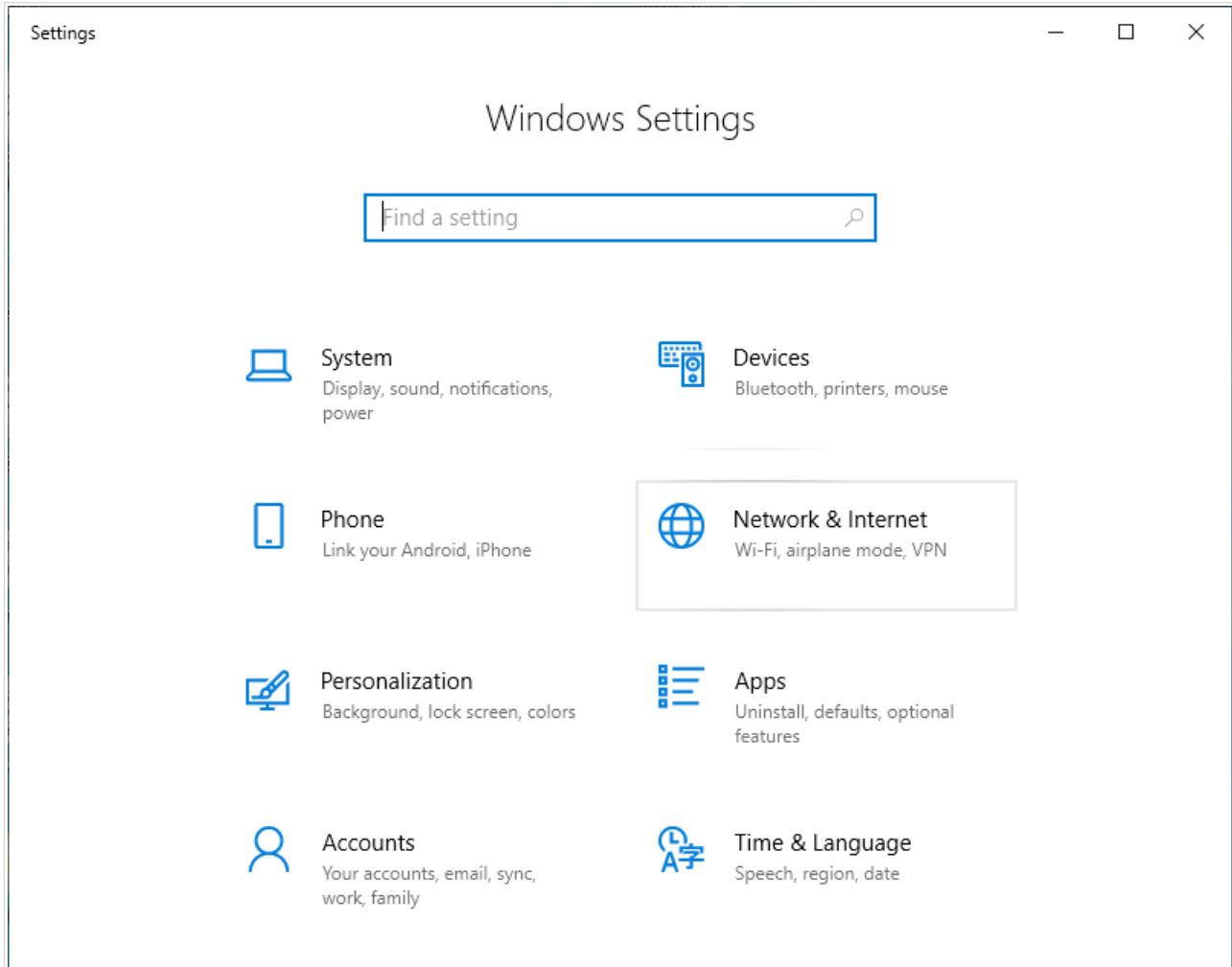


Figure 8. The **Windows Settings** window.

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

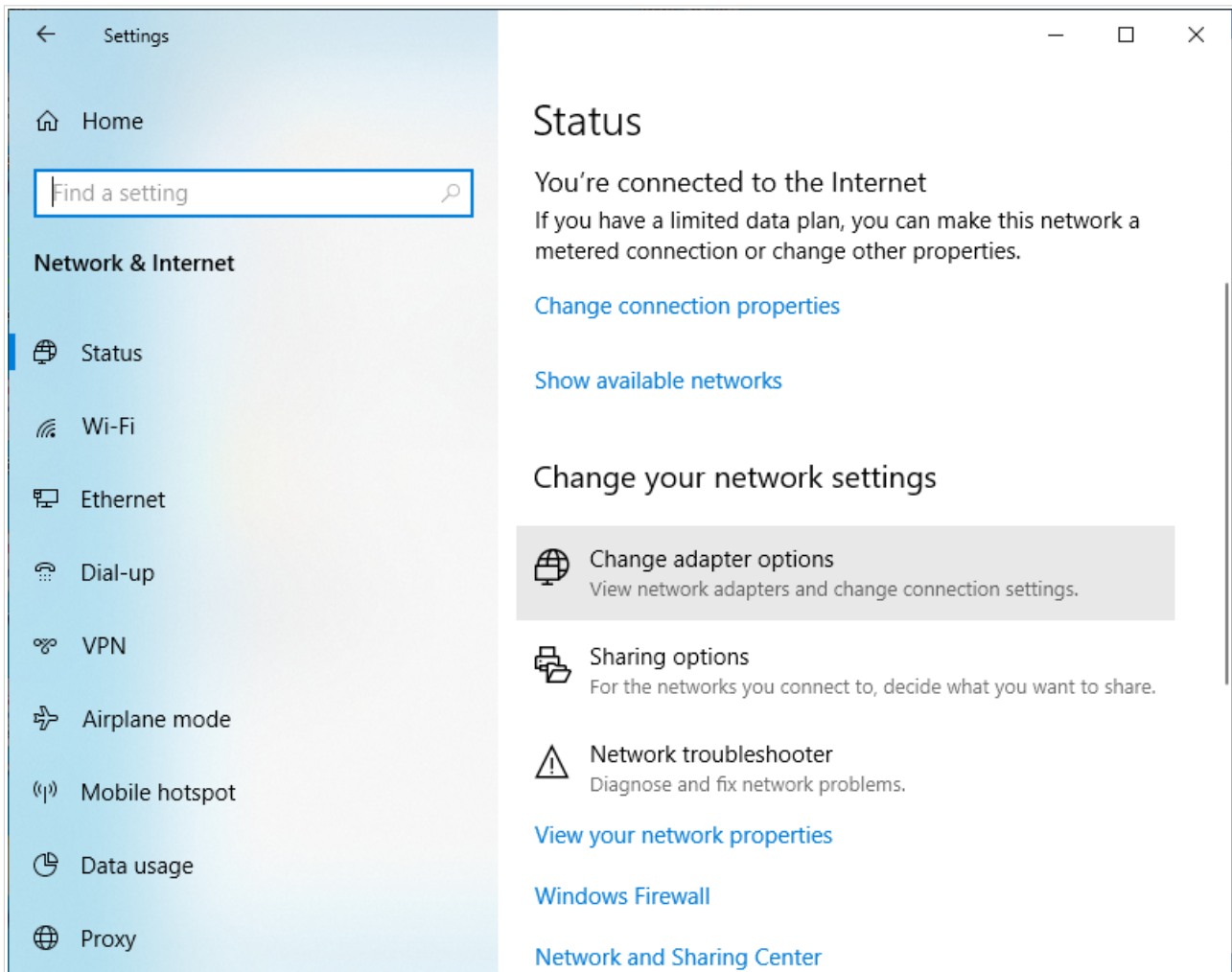


Figure 9. The **Network & Internet** window.

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

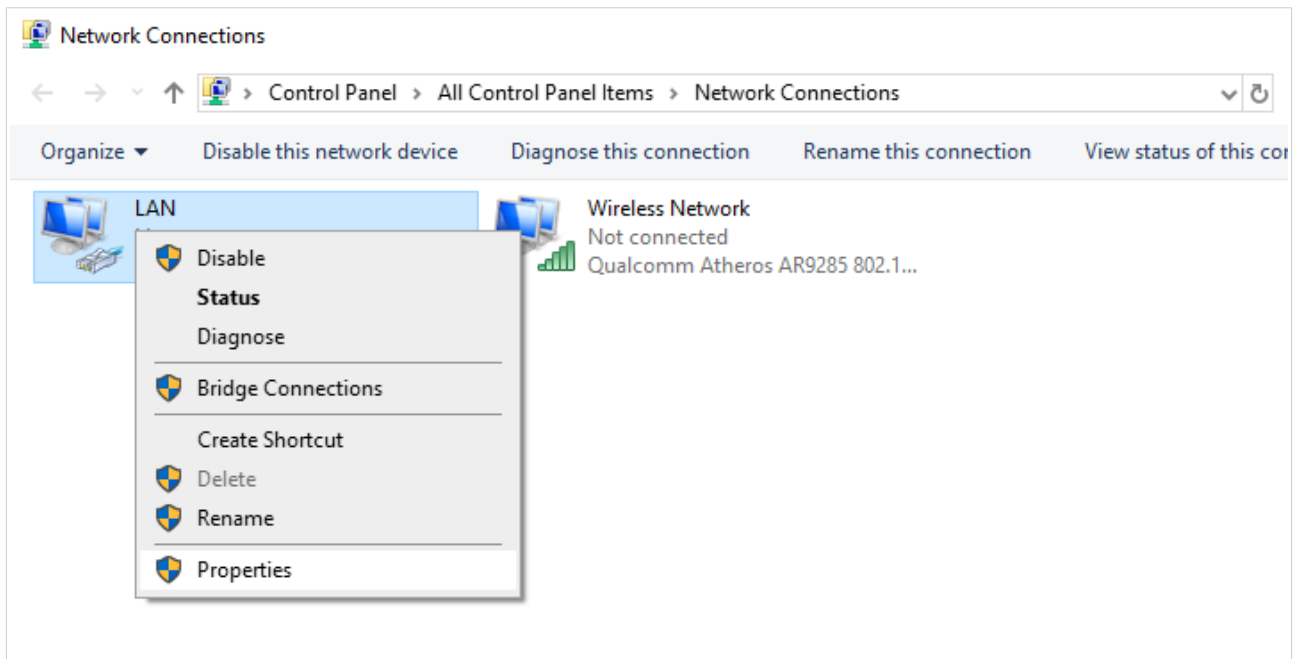


Figure 10. The **Network Connections** window.



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

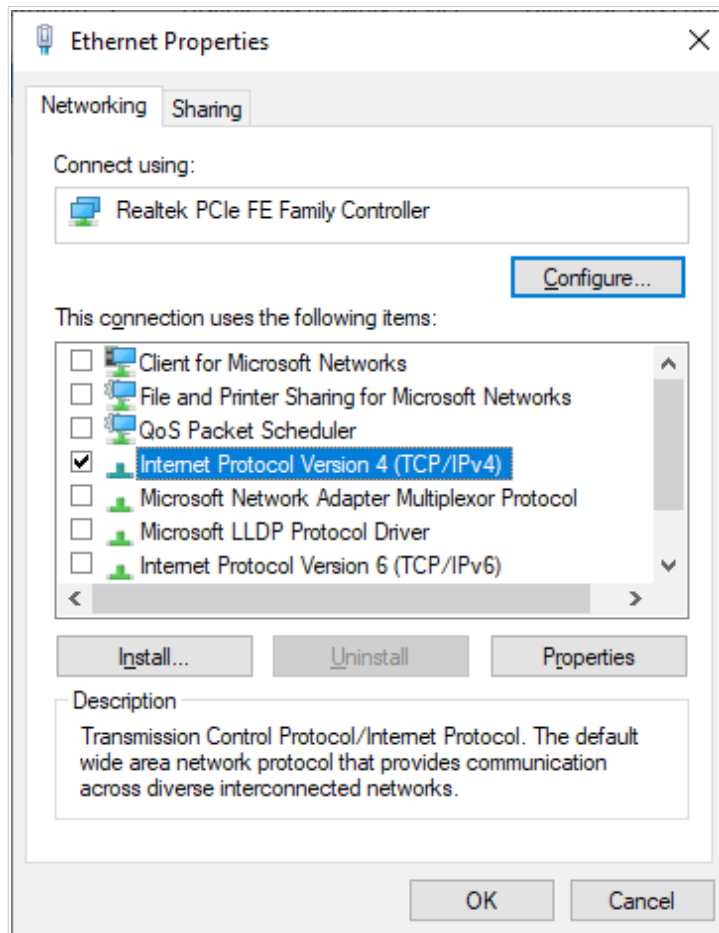


Figure 11. The local area connection properties window.

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

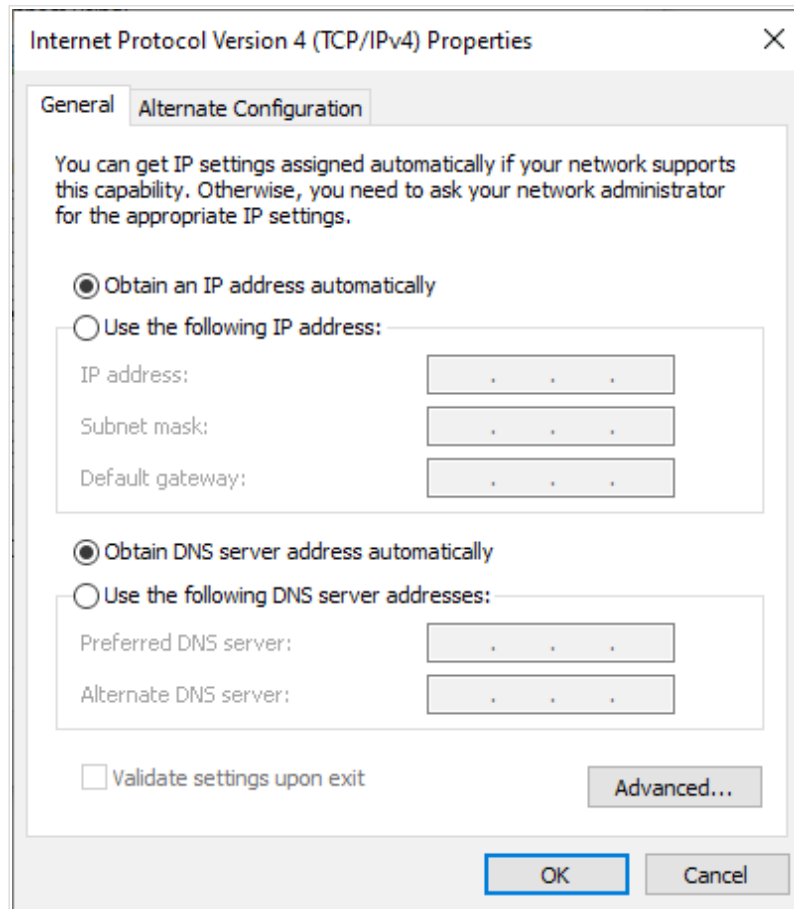


Figure 12. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

## PC with Wi-Fi Adapter

1. **To connect via USB modem:** connect your USB modem to the USB port<sup>9</sup> located on the back panel of the router.



In some cases you will need to reboot the router after connection of the USB modem.

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

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

---

<sup>9</sup> It is recommended to use a USB extension cable to connect a USB modem to the router.

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

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

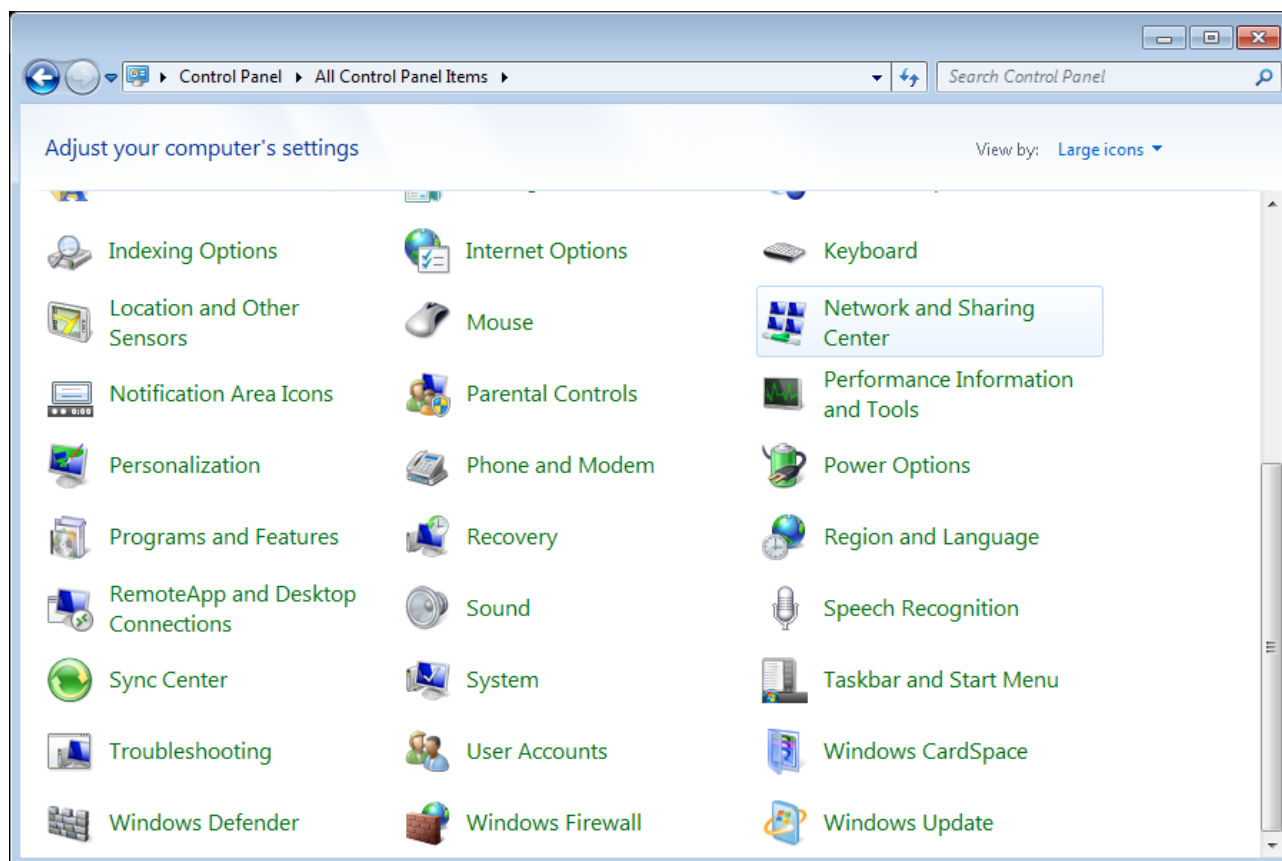


Figure 13. The **Control Panel** window.

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

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

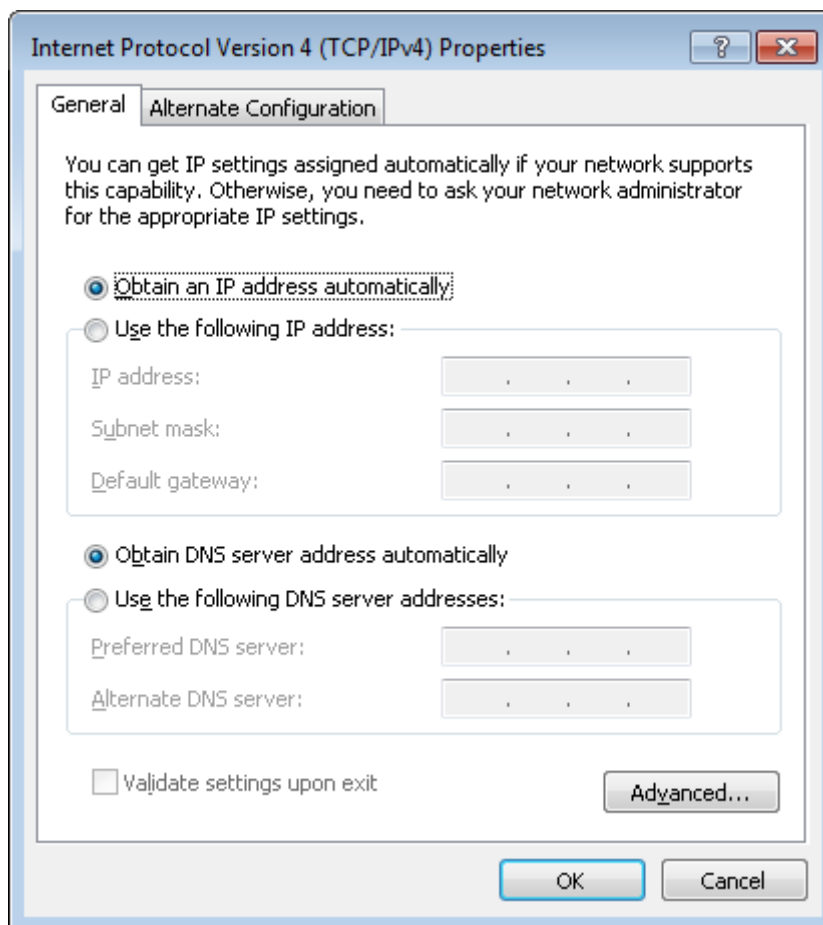


Figure 14. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

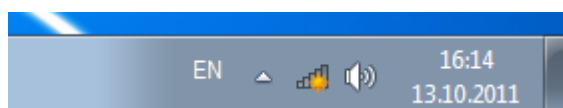


Figure 15. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network **DIR-853** (for operating in the 2.4GHz band) or **DIR-853-5G** (for operating in the 5GHz band) and click the **Connect** button.

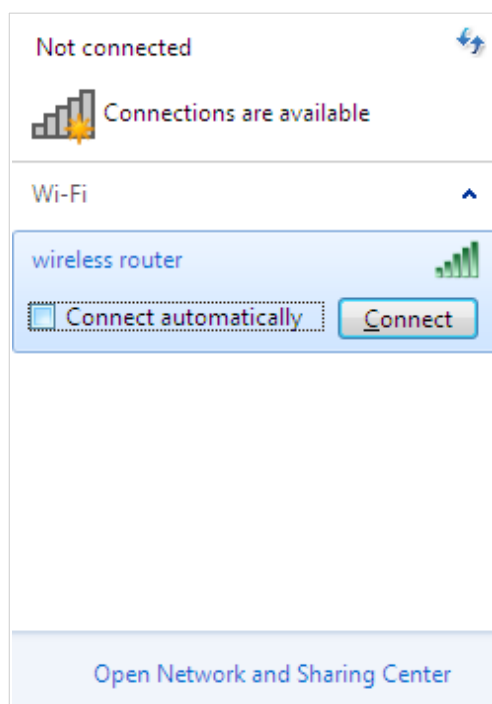


Figure 16. The list of available networks.

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

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

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

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

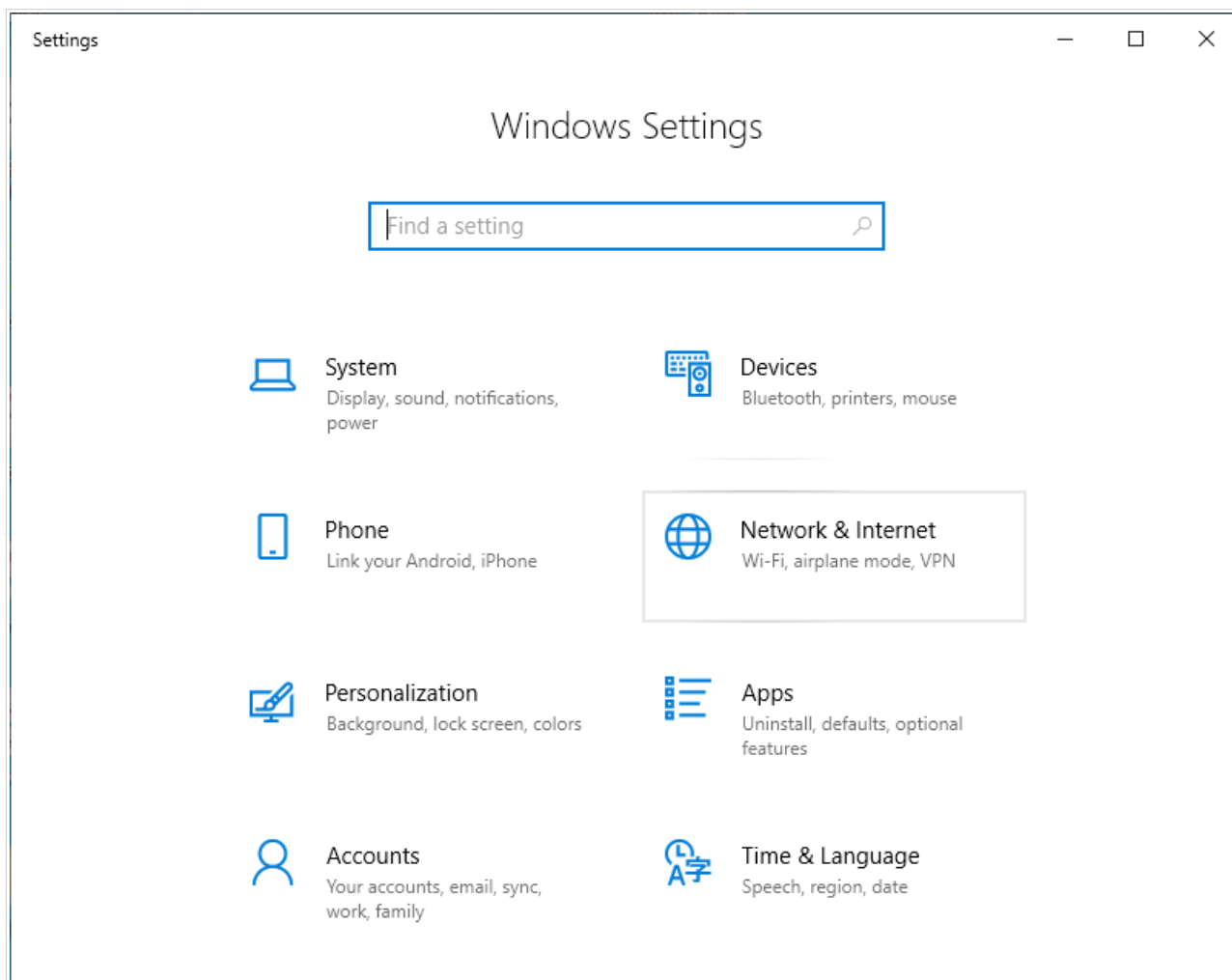


Figure 17. The **Windows Settings** window.

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

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

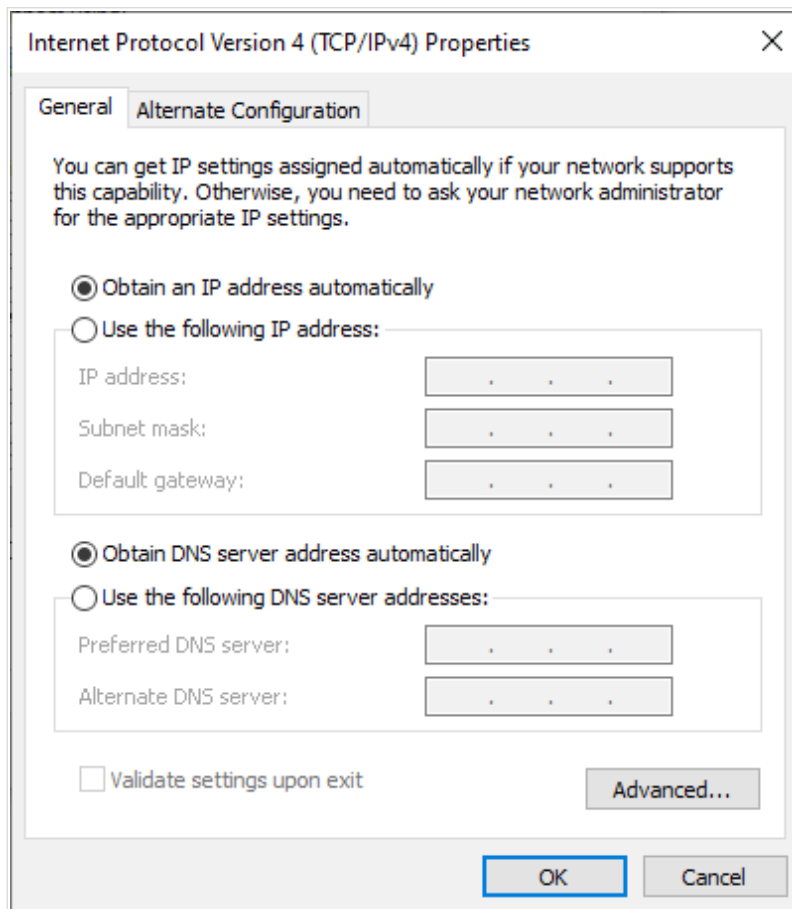


Figure 18. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

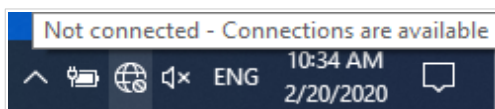


Figure 19. The notification area of the taskbar.



9. In the opened **Wireless Network Connection** window, select the wireless network **DIR-853** (for operating in the 2.4GHz band) or **DIR-853-5G** (for operating in the 5GHz band) and click the **Connect** button.

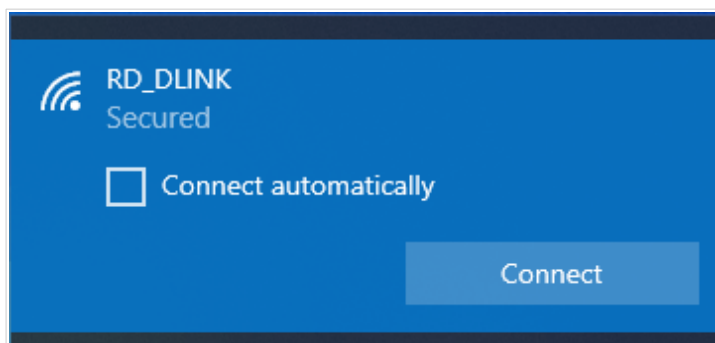


Figure 20. The list of available networks.

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

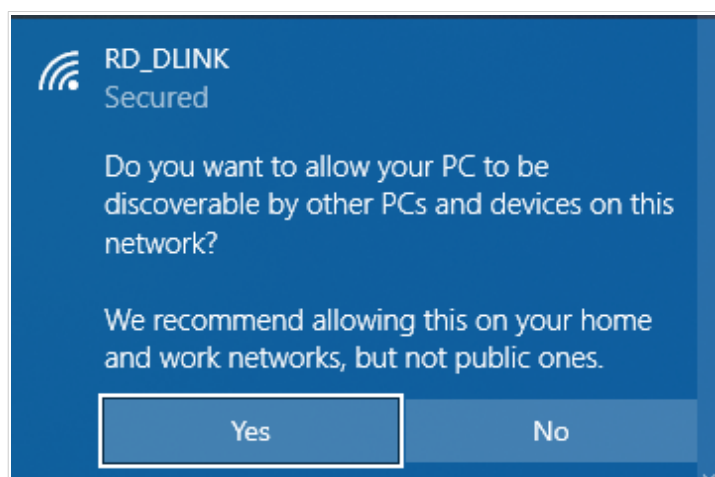


Figure 21. PC discovery settings.

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

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

## Connecting to Web-based Interface

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

**!** For security reasons, DIR-853 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 22). In the address bar of the web browser, enter the domain name of the router (by default, **dlinkrouter.local**) with a dot at the end and press the **Enter** key. Also you can enter the IP address of the device (by default, **192.168.0.1**).



Figure 22. Connecting to the web-based interface of the DIR-853 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 49).

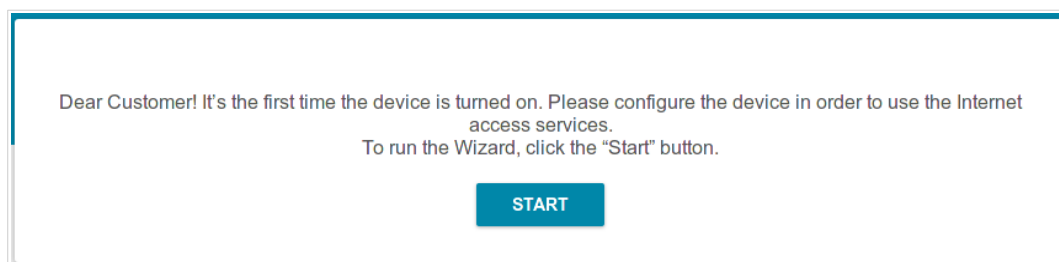
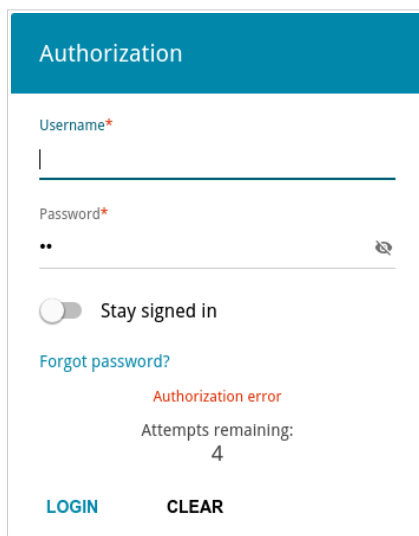


Figure 23. The page for running the Initial Configuration Wizard.

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



The screenshot shows a web-based login interface titled "Authorization". It features two input fields: "Username\*" and "Password\*", both with red asterisks indicating required fields. The "Username" field contains the text "admin". Below the password field is a toggle switch labeled "Stay signed in" which is currently turned off. A link "Forgot password?" is visible. A red error message "Authorization error" is displayed, followed by "Attempts remaining: 4". At the bottom are two buttons: "LOGIN" and "CLEAR".

Figure 24. The login page.

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

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

## Web-based Interface Structure

### Summary Page

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

The screenshot displays the 'Summary' page of the DIR-853 web-based interface. The page is organized into several sections:

- Device Information:** Model: DIR-853, Hardware version: R3, Firmware version: 4.0.1, Build time: Mon Mar 17 2025 12:28:12 PM MSK, UI version: 1.54.1.4e88076-embedded, Vendor: D-Link Russia, Serial number: DIR853RUR3001, Support: support@dlink.ru, Summary: Root filesystem image for DIR\_853R3\_MT7621, Uptime: 45 min., Device mode: Router, Enable LEDs: (toggle switch).
- WAN IPv4:** Connection type: Dynamic IPv4, Status: Connected, MAC address: A8:CB:DD:00:A2:FE, IP address: 192.168.161.225.
- LAN:** LAN IPv4: 192.168.0.1, Wireless connections: -, Wired connections: 1.
- LAN Ports:** LAN4: (status), LAN3: 1000M-Full (status), LAN2: (status), LAN1: (status).
- Wi-Fi 2.4 GHz:** Status: On, Broadcasting: On, Additional networks: 0, Network name (SSID): DIR-853-A2FE, Security: WPA2-PSK.
- Wi-Fi 5 GHz:** Status: On, Broadcasting: On, Additional networks: 0, Network name (SSID): DIR-853-5G-A2FE, Security: WPA2-PSK.
- USB Devices:** No connected devices.

Figure 25. The summary page.

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

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

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **Initial Configuration Wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 49).

If needed, you can disable the LEDs of the device (except the **Power**, **Internet**, and **LAN 1-4** 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 **USB Devices** section displays the device connected to the USB port of the router.

## Home Page

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

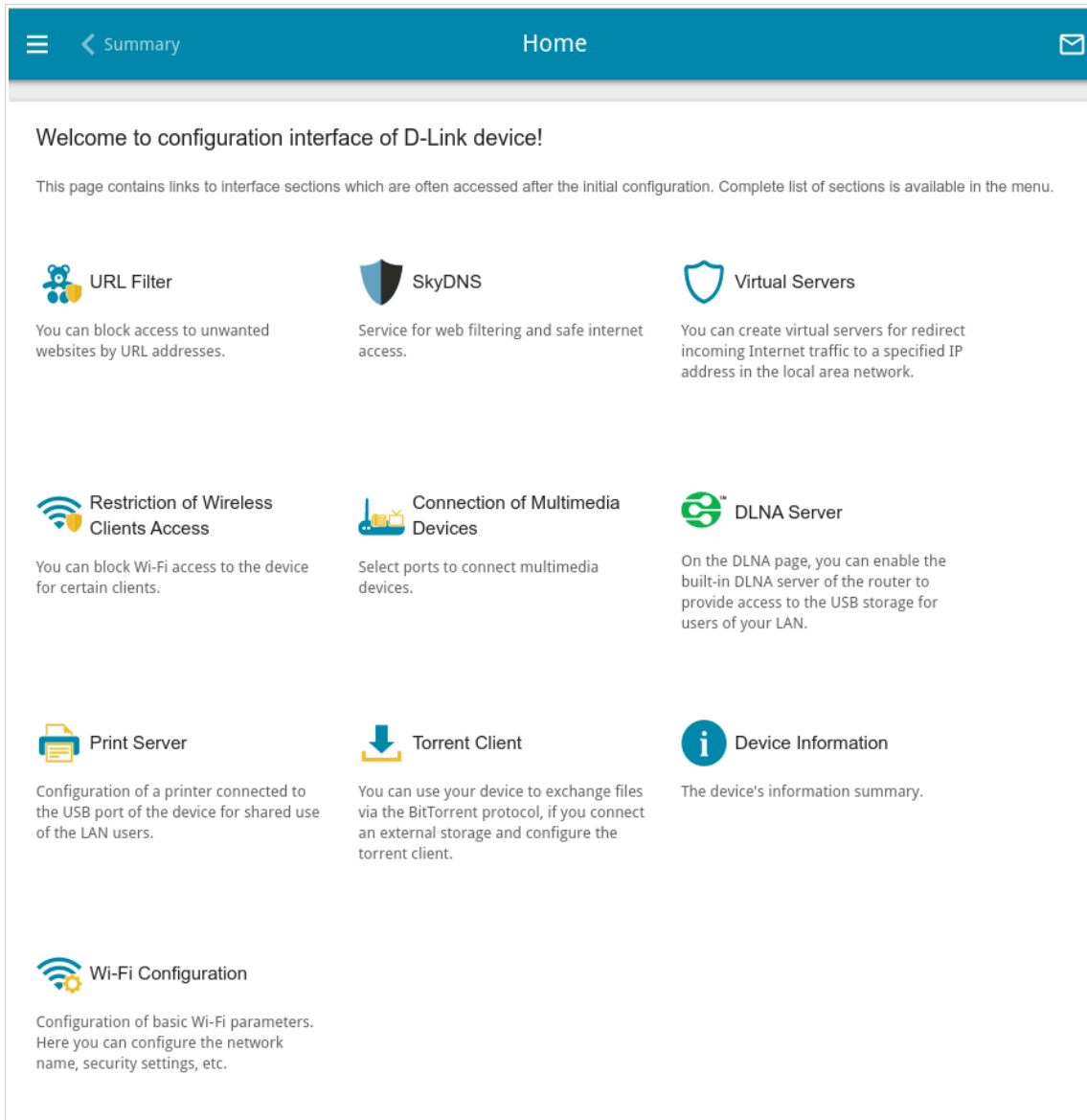


Figure 26. The **Home** page.

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

## Menu Sections

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

In the **Initial Configuration** section you can run the Initial Configuration Wizard. The Wizard allows you to configure the router for operation in the needed mode and specify all parameters necessary for getting started (for the description of the Wizard, see the **Initial Configuration Wizard** section, page 49).

The pages of the **Statistics** section display data on the current state of the router (for the description of the pages, see the **Statistics** section, page 75).

The pages of the **Connections Setup** section are designed for configuring basic parameters of the LAN interface of the router and creating a connection to the Internet (for the description of the pages, see the **Connections Setup** section, page 84).

The pages of the **VPN** section are designed for configuring VPN connections based on IPsec/GRE/EoGRE/EoIP/IPIP protocols and creating a PPTP or L2TP server and accounts for access to it (for the description of the pages, see the **VPN** section, page 142).

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 167).

The **Print Server** section is designed for configuring the router as a print server (see the **Print Server** section, page 198).

The pages of the **USB Storage** section are designed for operating the connected USB storage (for the description of the pages, see the **USB Storage** section, page 199).

The pages of the **USB Modem** section are designed for operating the connected 3G or LTE USB modem (for the description of the pages, see the **USB Modem** section, page 214).

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 221).

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 260).

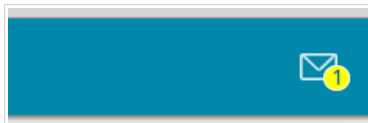
The pages of the **System** section provide functions for managing the internal system of the router (for the description of the pages, see the **System** section, page 281).

The pages of the **SkyDNS** section are designed for configuring the SkyDNS web content filtering service (for the description of the pages, see the **SkyDNS** section, page 313).

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

## Notifications

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



*Figure 27. The web-based interface notifications.*

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



## CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

### Initial Configuration Wizard

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

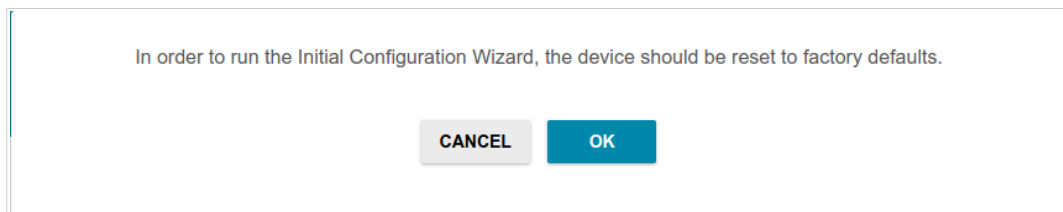


Figure 28. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network **DIR-853** (for operating in the 2.4GHz band) or **DIR-853-5G** (for operating in the 5GHz band) and click the **NEXT** button.

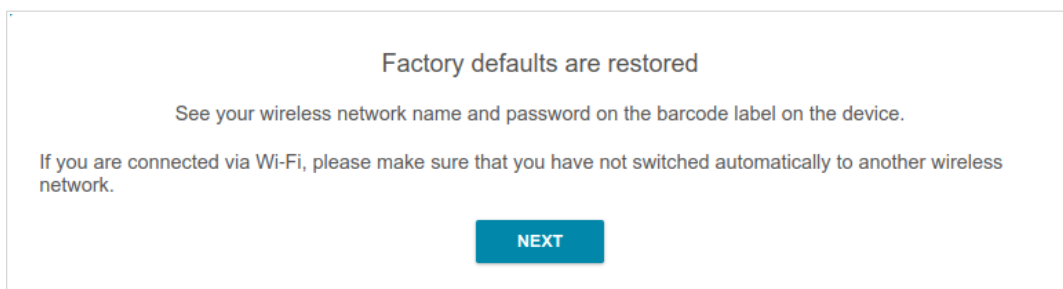


Figure 29. Checking connection to the wireless network.

Click the **START** button.

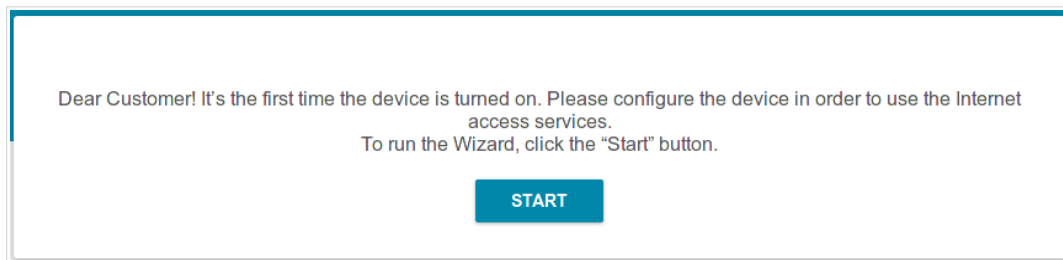


Figure 30. Starting the Wizard.

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

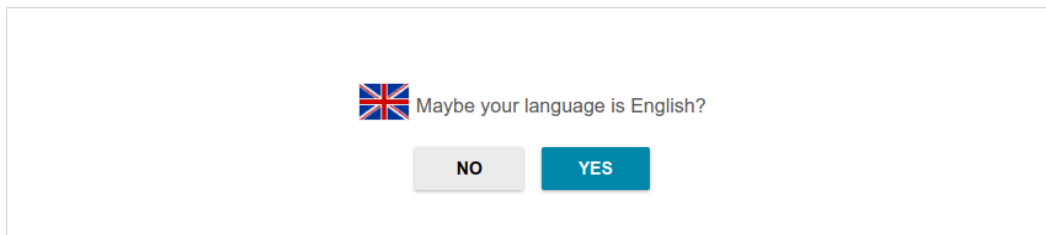


Figure 31. Selecting a language.

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

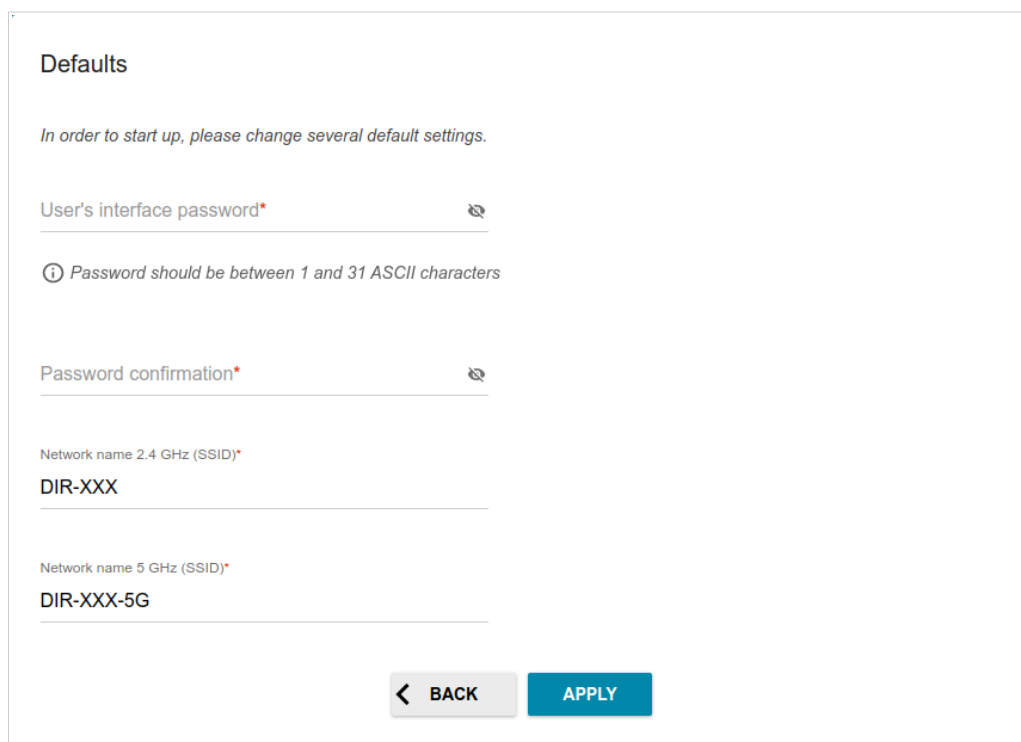
A screenshot of a web-based configuration page titled "Defaults". Below the title, there is a message: "In order to start up, please change several default settings." The page contains four input fields, each with a red asterisk indicating it is required. The first field is "User's interface password"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

Figure 32. Changing the default settings.

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

## Selecting Operation Mode

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

### Router

In order to connect your device to a wired ISP, on the **Device mode** page, from the **Connection method** list, select the **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.

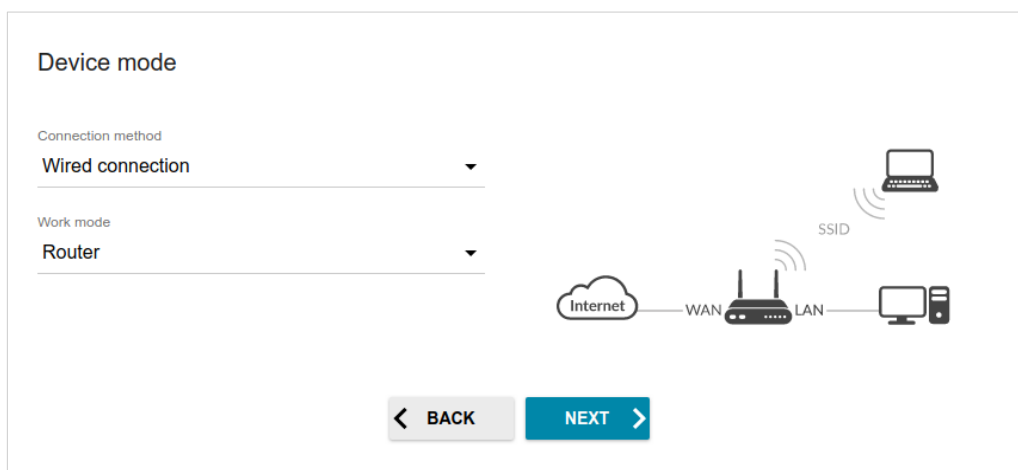


Figure 33. Selecting an operation mode. The **Router** mode.

In order to connect your device to the network of a 3G or LTE operator, on the **Device mode** page, from the **Connection method** list, select the **Mobile Internet** value. In this mode you can configure a 3G/LTE WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

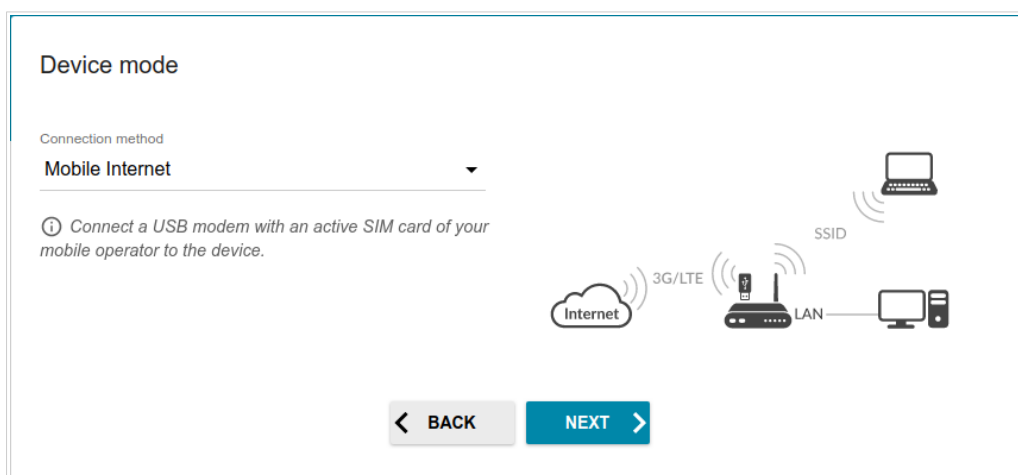


Figure 34. Selecting an operation mode. The **Mobile Internet** mode.

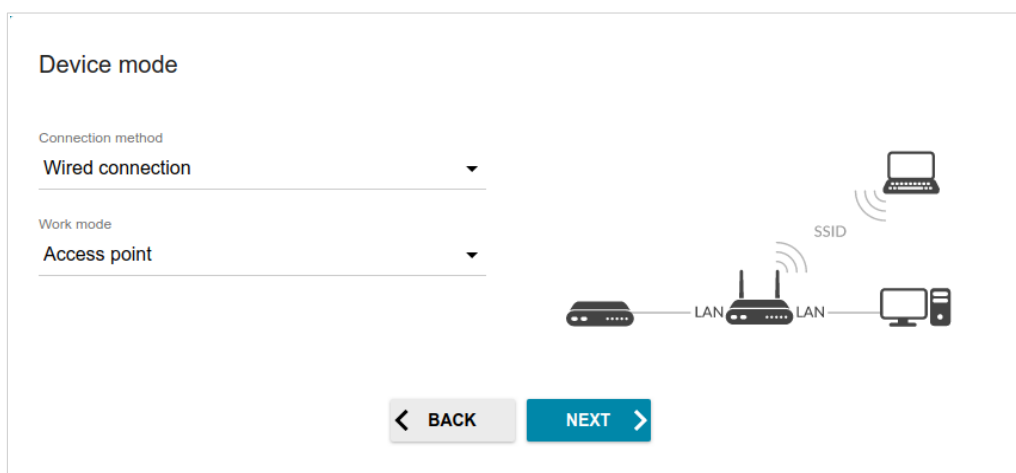
In order to connect your device to a wireless ISP (WISP), on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **WISP Repeater** value. In this mode you can connect your device to another access point, configure a WAN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

The screenshot shows the 'Device mode' configuration page. It has two dropdown menus: 'Connection method' with 'Wi-Fi' selected, and 'Work mode' with 'WISP Repeater' selected. To the right of these menus is a diagram illustrating the WISP Repeater setup. The diagram shows a cloud labeled 'Internet' connected to a router via 'SSID'. This router is then connected to another router via 'SSID\_Ext'. The second router is connected to a computer via 'LAN'. At the bottom of the page are two buttons: 'BACK' and 'NEXT'.

Figure 35. Selecting an operation mode. The **WISP Repeater** mode.

## Access Point or Repeater

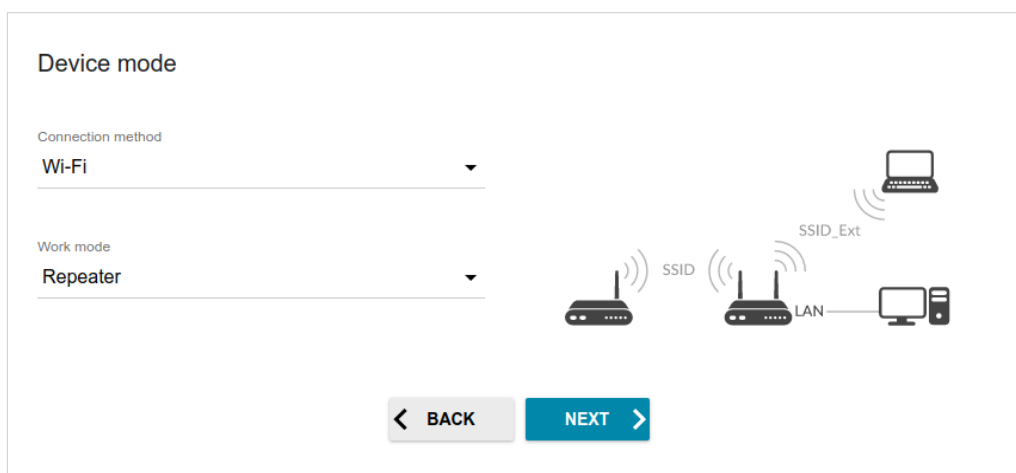
In order to connect your device to a wired router for adding a wireless network to the existing local network, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Access point** value. In this mode you 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.



The screenshot shows the 'Device mode' configuration page. Under 'Connection method', 'Wired connection' is selected. Under 'Work mode', 'Access point' is selected. To the right, a diagram illustrates a router connected via LAN to another router, which is then connected via LAN to a computer. A laptop is shown connected wirelessly to the second router, labeled 'SSID'. At the bottom are 'BACK' and 'NEXT' buttons.

Figure 36. 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.



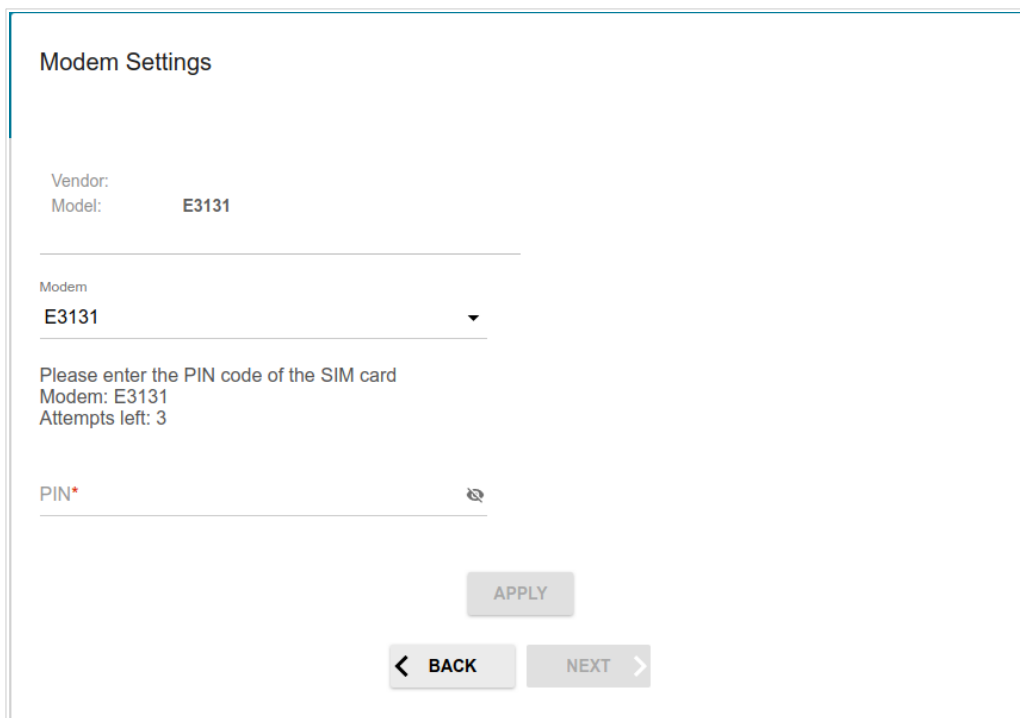
The screenshot shows the 'Device mode' configuration page. Under 'Connection method', 'Wi-Fi' is selected. Under 'Work mode', 'Repeater' is selected. To the right, a diagram illustrates a router connected wirelessly to another router, labeled 'SSID'. The second router is connected via LAN to a computer. A laptop is shown connected wirelessly to the second router, labeled 'SSID\_Ext'. At the bottom are 'BACK' and 'NEXT' buttons.

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

## Creating 3G/LTE WAN Connection

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

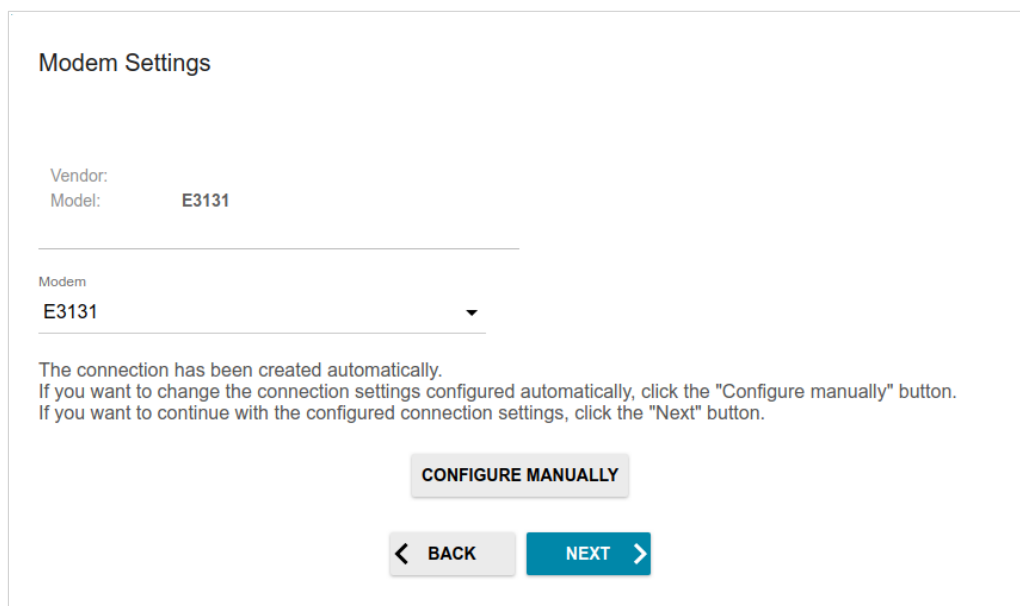
1. If the PIN code check is enabled for the SIM card inserted into your USB modem, enter the PIN code in the **PIN** field and click the **APPLY** button.



The screenshot shows the 'Modem Settings' page. At the top, it displays 'Vendor:' and 'Model: E3131'. Below this is a 'Modem' dropdown menu currently set to 'E3131'. A message states: 'Please enter the PIN code of the SIM card', 'Modem: E3131', and 'Attempts left: 3'. There is a text input field labeled 'PIN\*' with a small eye icon to its right. At the bottom, there are three buttons: 'APPLY', '< BACK', and 'NEXT >'.

Figure 38. The page for entering the PIN code.

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



The screenshot shows the 'Modem Settings' page after the connection has been created. It displays 'Vendor:' and 'Model: E3131'. Below this is a 'Modem' dropdown menu currently set to 'E3131'. A message states: 'The connection has been created automatically. If you want to change the connection settings configured automatically, click the "Configure manually" button. If you want to continue with the configured connection settings, click the "Next" button.' At the bottom, there are three buttons: 'CONFIGURE MANUALLY', '< BACK', and 'NEXT >'.

Figure 39. The page for creating 3G/LTE connection.

3. Click the **NEXT** button.

If the router failed to create a WAN connection automatically or you want to change the WAN connection settings configured automatically, click the **CONFIGURE MANUALLY** button. On the **Modem Settings** page, configure all needed settings and click the **NEXT** button.

## Changing LAN IPv4 Address

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

1. Select the **Automatic obtainment of IPv4 address** to let DIR-853 automatically obtain the LAN IPv4 address.
2. In the **Hostname** field, you should specify a domain name of the router using which you can access the web-based interface after finishing the Wizard. Enter a new domain name of the router ending with **.local** or leave the value suggested by the router.

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

If you want to manually assign the LAN IPv4 address for DIR-853, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Subnet mask**, **DNS IP address**, **Hostname** fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.

LAN

☐ Automatic obtainment of IPv4 address

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

IP address\*

192.168.0.1

Subnet mask\*

255.255.255.0

Gateway IP address

DNS IP address\*

8.8.8.8

Hostname\*

dlinkapa34e.local

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

< BACK    NEXT >

Figure 40. The page for changing the LAN IPv4 address.


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




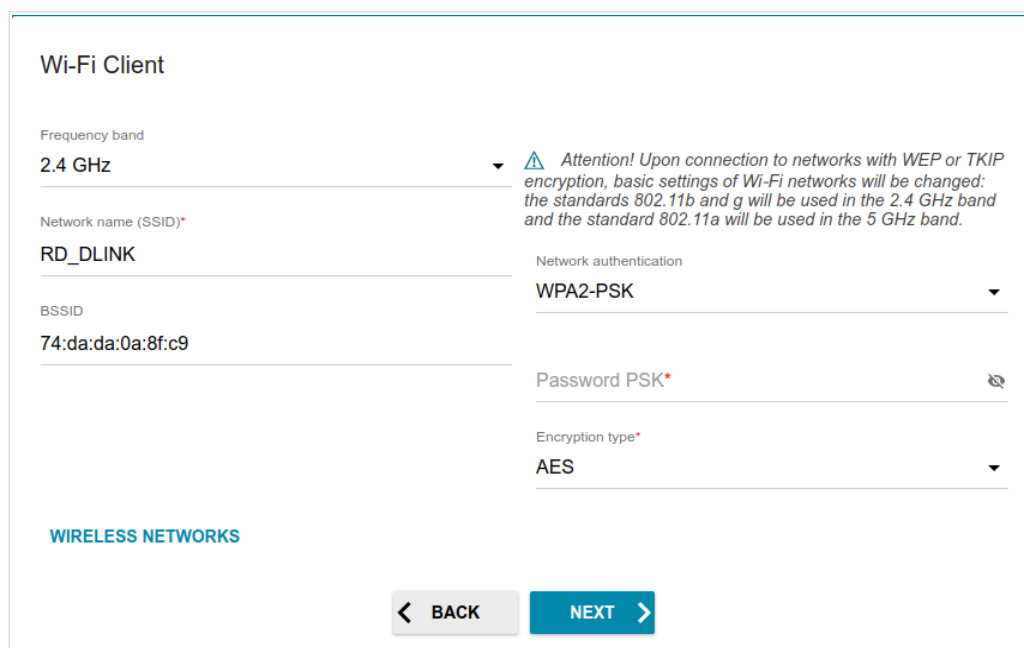
## Wi-Fi Client

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

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

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

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



Wi-Fi Client

Frequency band  
2.4 GHz

Network name (SSID)\*  
RD\_DLINK

BSSID  
74:da:da:0a:8f:c9

WIRELESS NETWORKS

Network authentication  
WPA2-PSK

Password PSK\*

Encryption type\*  
AES

BACK NEXT

⚠ Attention! Upon connection to networks with WEP or TKIP encryption, basic settings of Wi-Fi networks will be changed: the standards 802.11b and g will be used in the 2.4 GHz band and the standard 802.11a will be used in the 5 GHz band.

Figure 41. The page for configuring the Wi-Fi client.

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

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

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

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

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

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

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

## Configuring Wired WAN Connection

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



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

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

## Static IPv4 Connection

### Internet connection type

Connection type

Static IPv4

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

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

IP address\*

Subnet mask\*

Gateway IP address\*

DNS IP address\*

MAC address assignment method

Default MAC address

MAC address

C0:43:34:19:12:22

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

☐ Use VLAN

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

☒ Use IGMP

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

☐ Ping

☒ Enable automatic creation of Mobile Internet connection

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

Figure 42. The page for configuring Static IPv4 WAN connection.

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

## Static IPv6 Connection

### Internet connection type

Connection type  
Static IPv6

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

SCAN

Network scan for connection type and parameters detection

IP address\*

Prefix\*

Gateway IP address\*

DNS IP address\*

MAC address assignment method  
Default MAC address

MAC address  
74:DA:DA:00:54:10

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

☐ Use VLAN

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

☐ Ping

☒ Enable automatic creation of Mobile Internet connection

< BACK

NEXT >

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

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

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

### Internet connection type


Connection type  
PPPoE

*A connection of this type requires a user name and password.*

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


☐ Without authorization

Username\*

Password\* 

Service name

MAC address assignment method  
Default MAC address

MAC address  
74:DA:DA:00:54:10 

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

☐ Use VLAN


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

☐ Ping

☒ Enable automatic creation of Mobile Internet connection

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

Figure 44. The page for configuring PPPoE WAN connection.

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

## PPPoE + Static IP (PPPoE Dual Access) Connection

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 is set to "PPPoE + Static IP (PPPoE Dual Access)". A note with an information icon states: "A connection of this type requires a user name, password, and a fixed IP address provided by your ISP." There is a "SCAN" button and a text label "Network scan for connection type and parameters detection". A checkbox labeled "Without authorization" is present. Below these are several input fields, each with an asterisk indicating it is required: "Username\*", "Password\*" (with a "Show" icon), "Service name", "IP address\*", "Subnet mask\*", "Gateway IP address\*", and "DNS IP address\*".

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

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

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

## PPTP + Dynamic IP or L2TP + Dynamic IP Connection

### Internet connection type


Connection type  
PPTP + Dynamic IP

*PPTP and L2TP are methods for implementing virtual private networks.*

SCAN Network scan for connection type and parameters detection


☐ Without authorization

Username\*

Password\* 

VPN server address\*

MAC address assignment method  
Default MAC address

MAC address  
74:DA:DA:00:54:10 

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

☐ Use VLAN

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

☒ Use IGMP

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


☐ Ping

☒ Enable automatic creation of Mobile Internet connection

BACK

NEXT

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

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

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



## PPTP + Static IP or L2TP + Static IP Connection

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

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

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

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

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

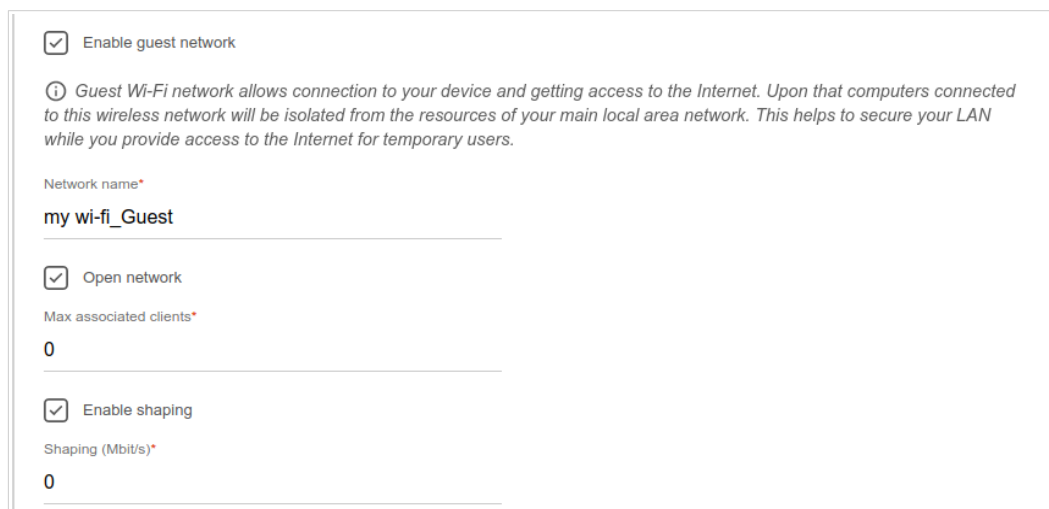
## Configuring Wireless Network

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

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

Figure 48. The page for configuring the wireless network.

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



The screenshot shows a web-based configuration interface for a wireless network. It contains the following elements:

- A checked checkbox labeled "Enable guest network".
- A paragraph of explanatory text: "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."
- A text input field labeled "Network name\*" with the value "my wi-fi\_Guest".
- A checked checkbox labeled "Open network".
- A text input field labeled "Max associated clients\*" with the value "0".
- A checked checkbox labeled "Enable shaping".
- A text input field labeled "Shaping (Mbit/s)\*" with the value "0".

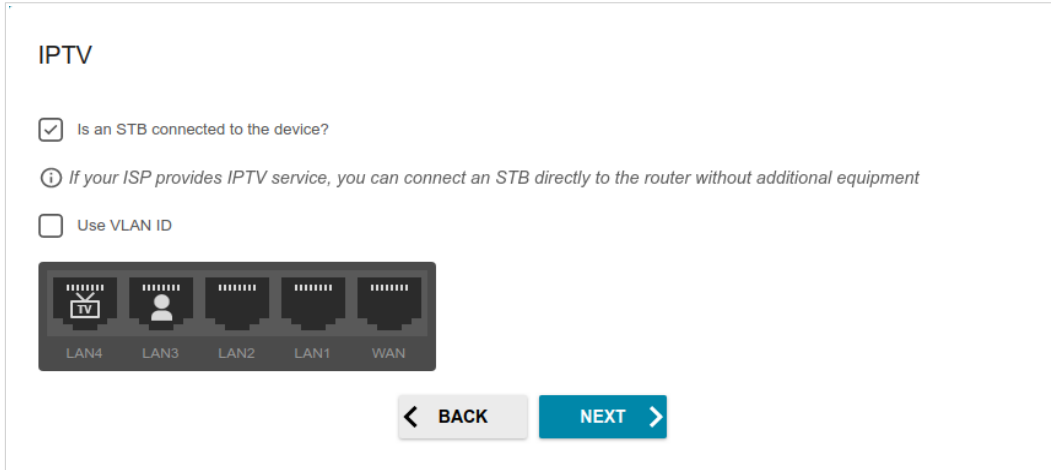
Figure 49. The page for configuring the wireless network.

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

## Configuring LAN Ports for IPTV/VoIP

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

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



**IPTV**

☒ Is an STB connected to the device?

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

☐ Use VLAN ID

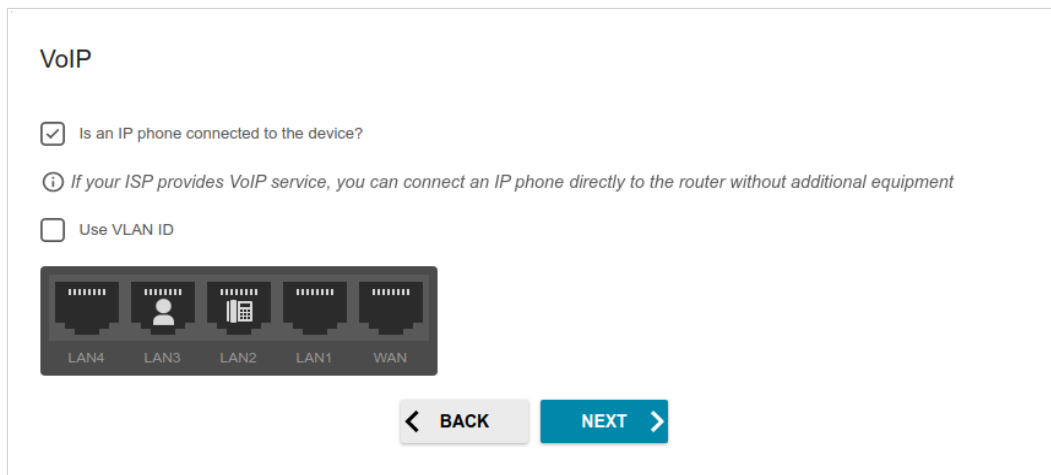
Diagram showing LAN ports: LAN4 (selected with TV icon), LAN3, LAN2, LAN1, and WAN.

**BACK** **NEXT**

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

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

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



The screenshot shows the 'VoIP' configuration page. At the top, the title 'VoIP' is displayed. Below it, there is a checked checkbox labeled 'Is an IP phone connected to the device?'. Underneath this checkbox is an information icon followed by the text: 'If your ISP provides VoIP service, you can connect an IP phone directly to the router without additional equipment'. Below this is an unchecked checkbox labeled 'Use VLAN ID'. At the bottom of the form is a diagram of the router's ports: LAN4, LAN3, LAN2, LAN1, and WAN. LAN3 is highlighted with a person icon, indicating it is selected for the IP phone connection. At the bottom right of the form are two buttons: a grey 'BACK' button with a left arrow and a blue 'NEXT' button with a right arrow.

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

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

## Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **User's interface password** and **Password confirmation** fields. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.<sup>10</sup>

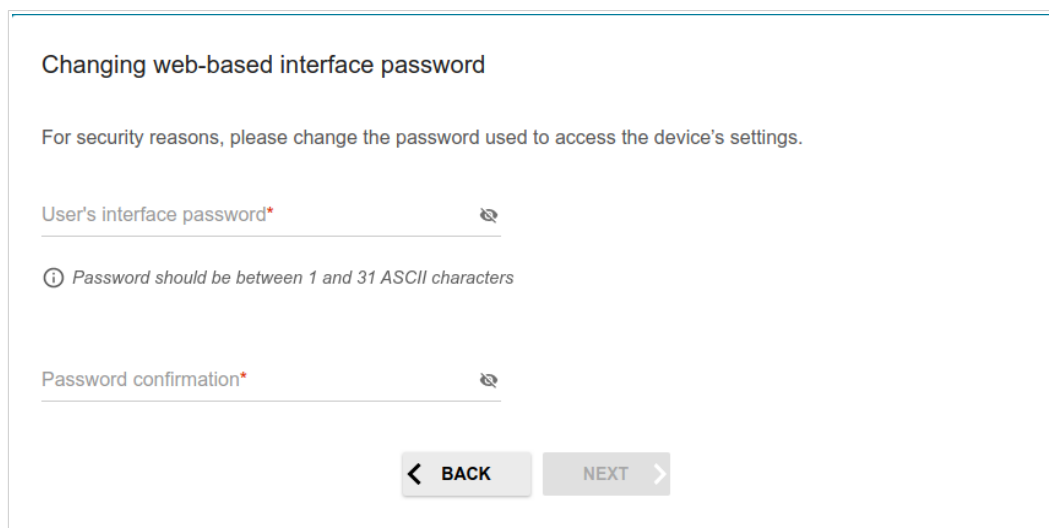


Figure 52. The page for changing the web-based interface password.



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

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

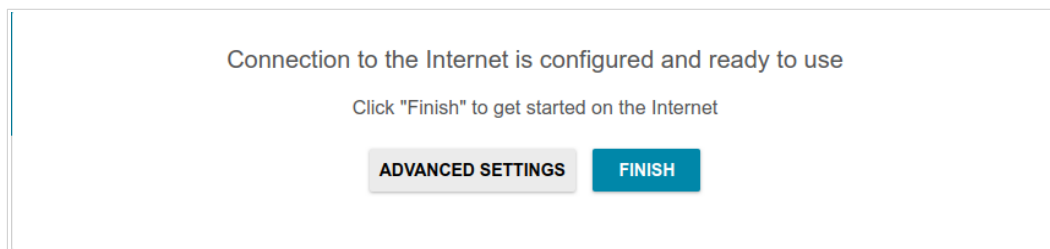
On the next page, check all specified settings.

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

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

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

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



*Figure 53. Checking the Internet availability.*

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

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

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

To specify other settings, click the **ADVANCED SETTINGS** button. After clicking the **ADVANCED SETTINGS** button, the **Home** page opens (see the *Home Page* section, page 46).

## 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-853 in order to use these devices.

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

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

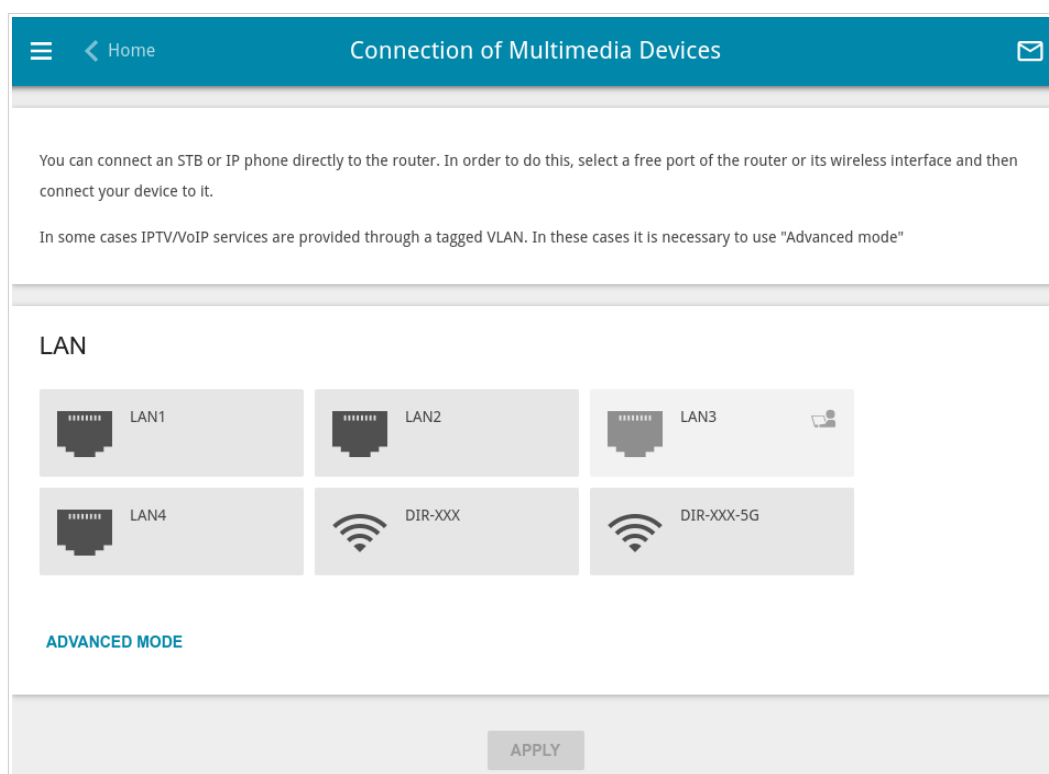


Figure 54. The Multimedia Devices Connection Wizard. The simplified mode.



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

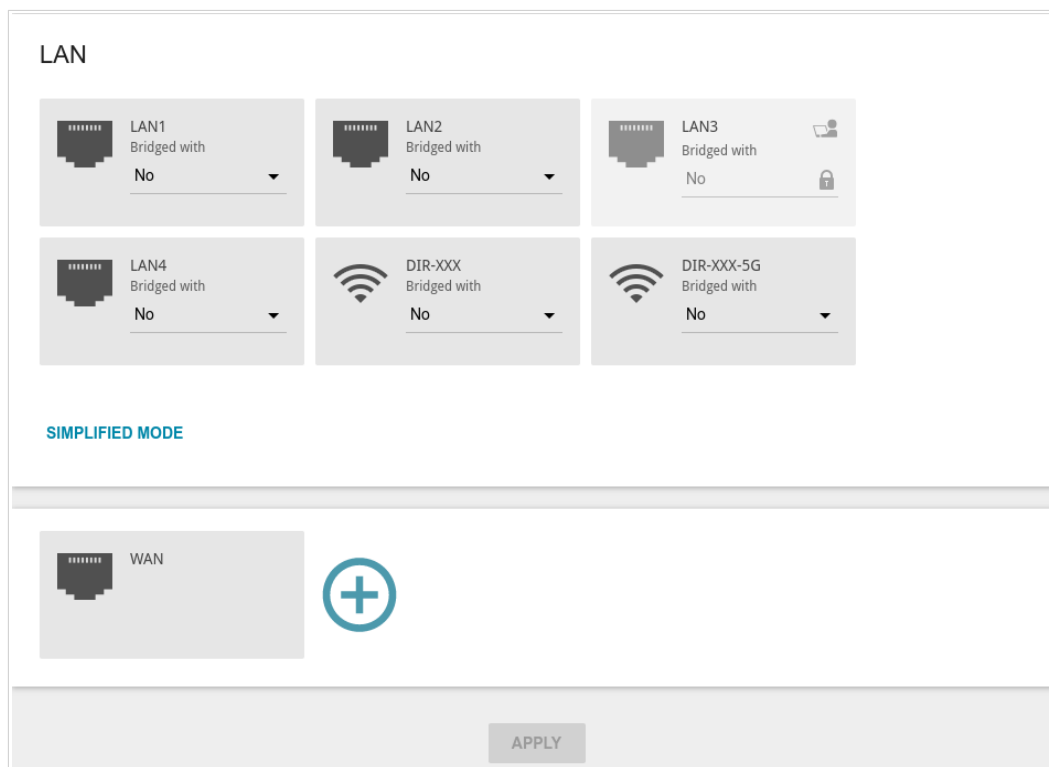


Figure 55. The Multimedia Devices Connection Wizard. The advanced mode.

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

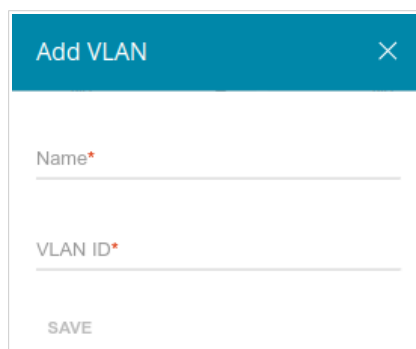



Figure 56. Adding a connection.

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

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

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

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

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

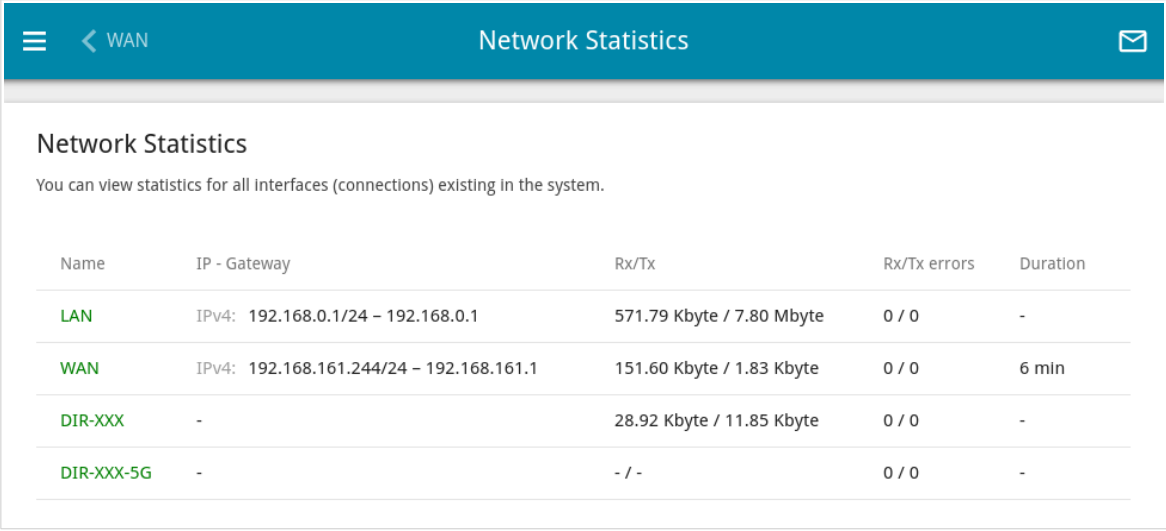
## Statistics

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

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

## Network Statistics

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



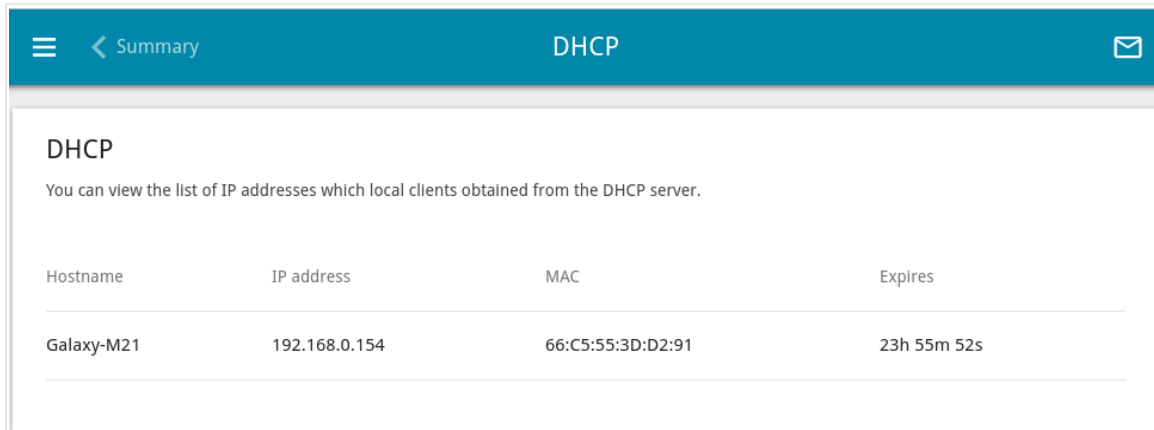
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 – 192.168.0.1	571.79 Kbyte / 7.80 Mbyte	0 / 0	-
WAN	IPv4: 192.168.161.244/24 – 192.168.161.1	151.60 Kbyte / 1.83 Kbyte	0 / 0	6 min
DIR-XXX	-	28.92 Kbyte / 11.85 Kbyte	0 / 0	-
DIR-XXX-5G	-	- / -	0 / 0	-

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

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

## DHCP

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

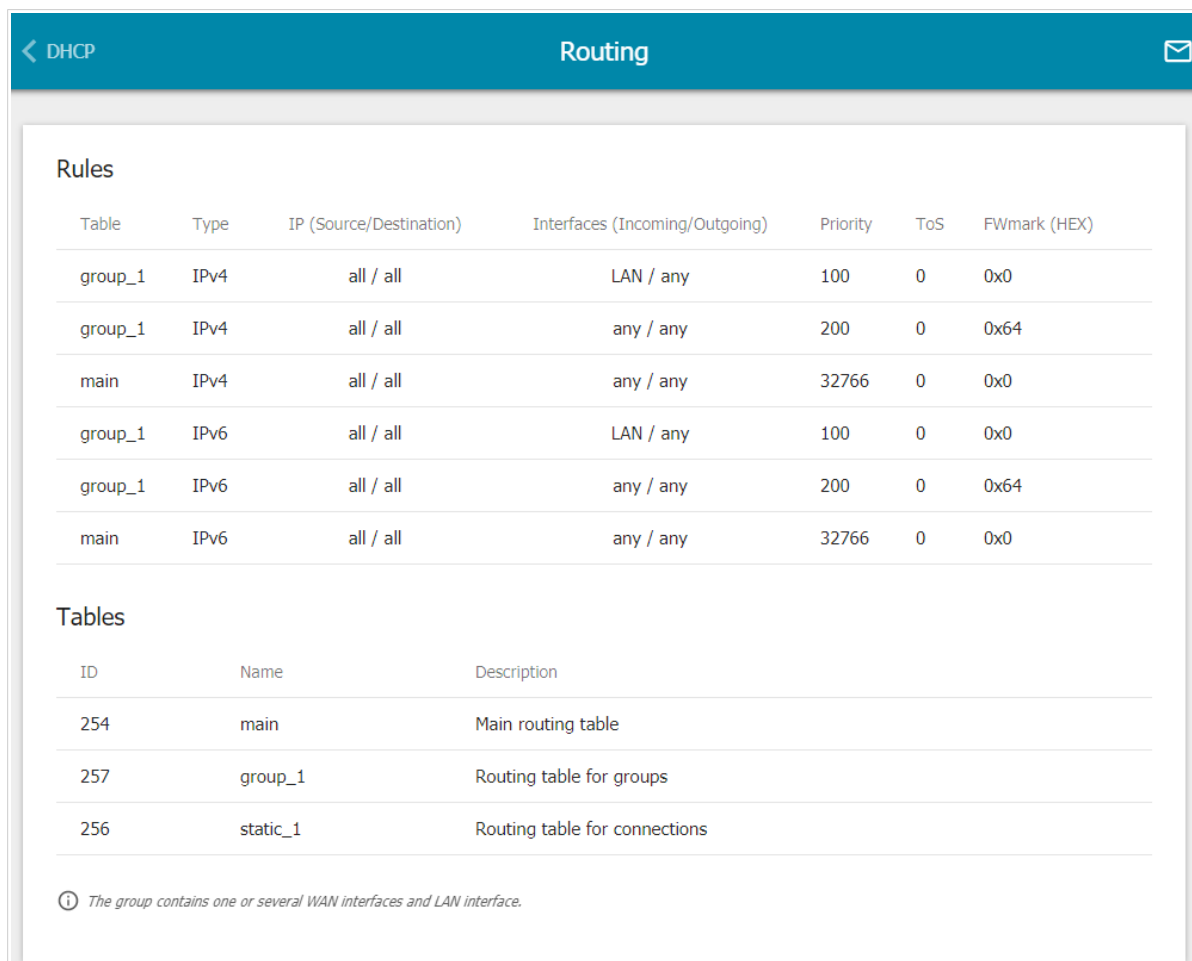


DHCP			
You can view the list of IP addresses which local clients obtained from the DHCP server.			
Hostname	IP address	MAC	Expires
Galaxy-M21	192.168.0.154	66:C5:55:3D:D2:91	23h 55m 52s

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

## Routing

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



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

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

① The group contains one or several WAN interfaces and LAN interface.

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

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

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

Routing Table main

You can view the information on routes.

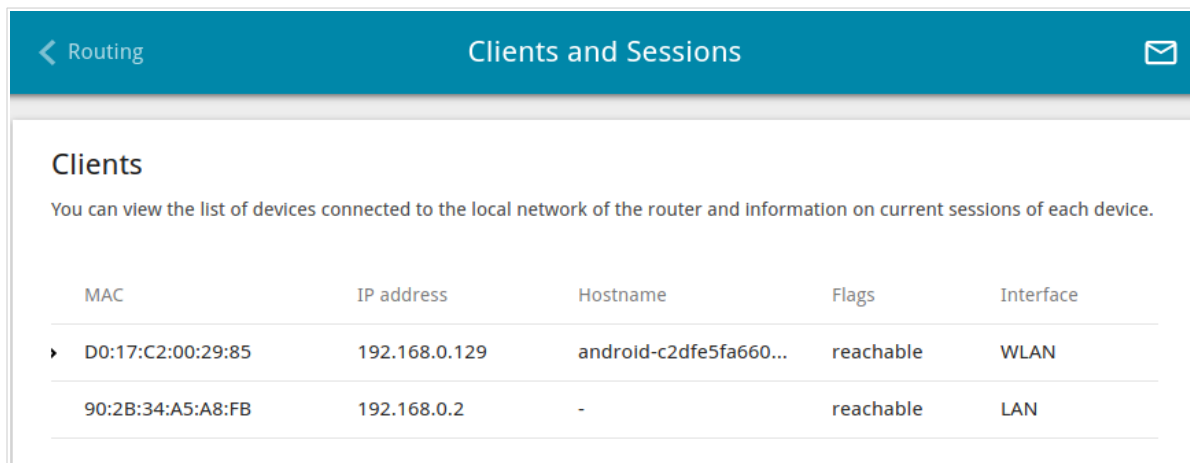
Interface	Destination	Subnet mask	Gateway	Flags	Metric	Table
WAN	0.0.0.0	0.0.0.0	192.168.161.1	UG	410	254
WAN	1.1.1.1		192.168.161.1	UGH	0	254
LAN	192.168.0.0	255.255.255.0		U	0	254
WAN	192.168.161.0	255.255.255.0		U	0	254

Figure 60. The routing table page.

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

## Clients and Sessions

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



Clients				
You can view the list of devices connected to the local network of the router and information on current sessions of each device.				
MAC	IP address	Hostname	Flags	Interface
▶ D0:17:C2:00:29:85	192.168.0.129	android-c2dfe5fa660...	reachable	WLAN
90:2B:34:A5:A8:FB	192.168.0.2	-	reachable	LAN

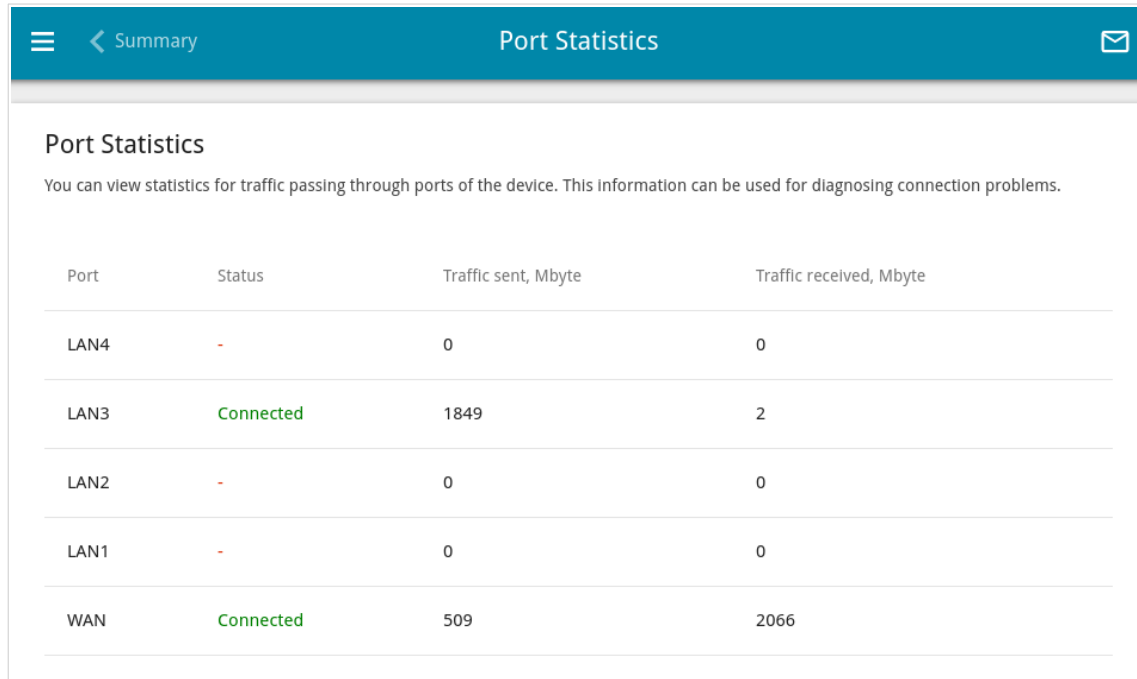
Figure 61. The **Statistics / Clients and Sessions** page.

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

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

## Port Statistics

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



Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte
LAN4	-	0	0
LAN3	Connected	1849	2
LAN2	-	0	0
LAN1	-	0	0
WAN	Connected	509	2066

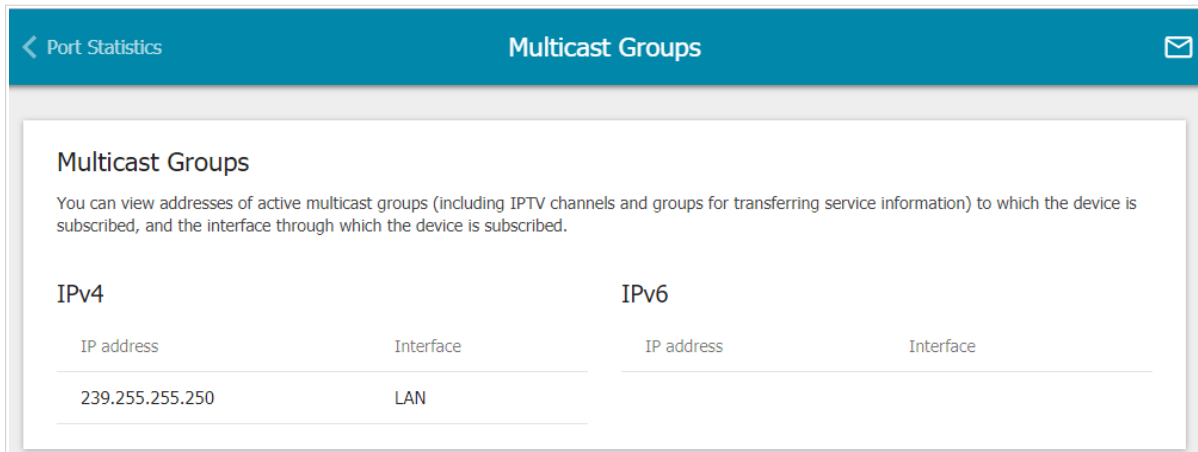
Figure 62. The **Statistics / Port Statistics** page.

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



## Multicast Groups

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

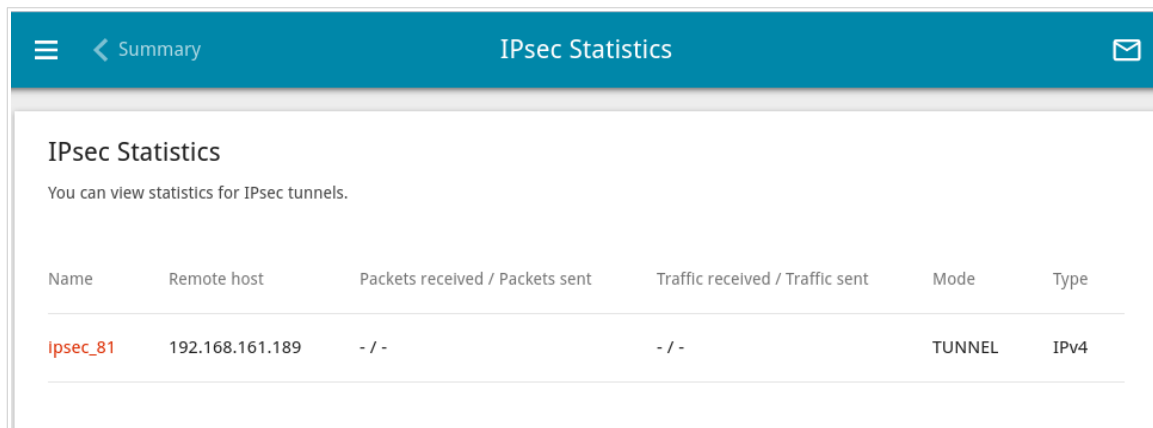


IPv4		IPv6	
IP address	Interface	IP address	Interface
239.255.255.250	LAN		

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

## IPsec Statistics

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



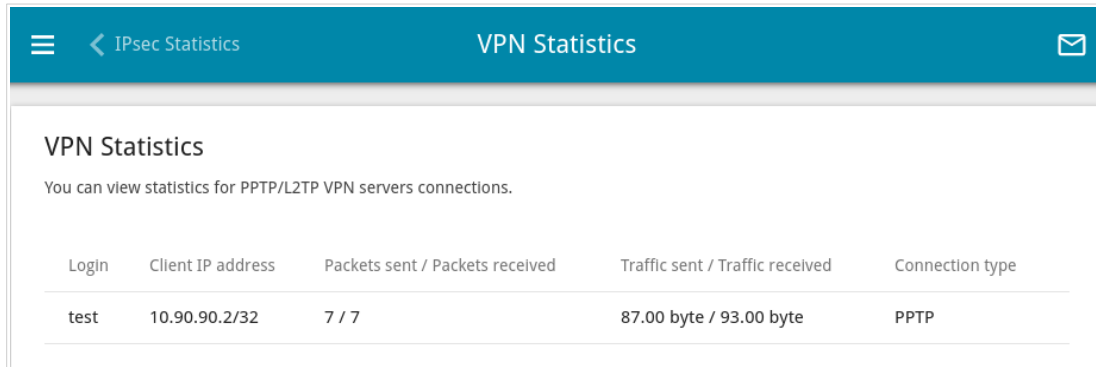
Name	Remote host	Packets received / Packets sent	Traffic received / Traffic sent	Mode	Type
ipsec_81	192.168.161.189	- / -	- / -	TUNNEL	IPv4

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

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

## VPN Statistics

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



Login	Client IP address	Packets sent / Packets received	Traffic sent / Traffic received	Connection type
test	10.90.90.2/32	7 / 7	87.00 byte / 93.00 byte	PPTP

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

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

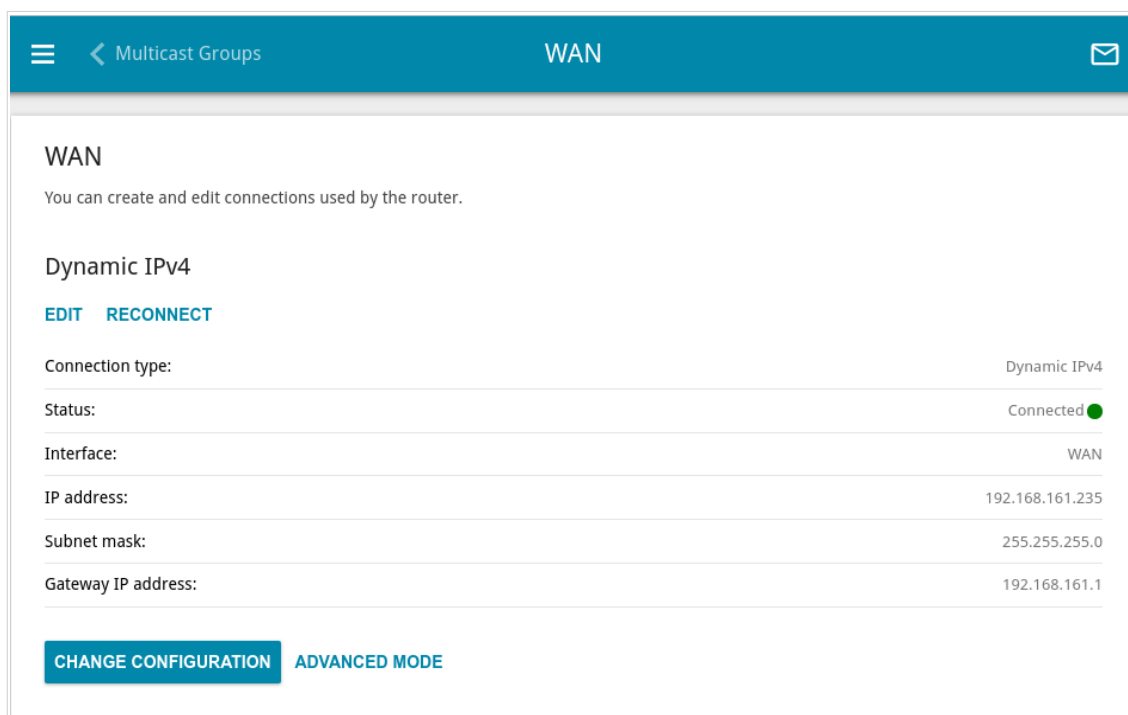
To view detailed data on a connected VPN client, click the line corresponding to this client.

## Connections Setup

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

### WAN

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



The screenshot shows the WAN configuration page in simplified mode. The page has a blue header with a menu icon, a back arrow labeled 'Multicast Groups', the title 'WAN', and an envelope icon. Below the header, the page is titled 'WAN' with a subtitle 'You can create and edit connections used by the router.' A 'Dynamic IPv4' connection is listed with 'EDIT' and 'RECONNECT' buttons. Below this, a table displays connection details: Connection type (Dynamic IPv4), Status (Connected with a green dot), Interface (WAN), IP address (192.168.161.235), Subnet mask (255.255.255.0), and Gateway IP address (192.168.161.1). At the bottom, there are two buttons: 'CHANGE CONFIGURATION' and 'ADVANCED MODE'.

Connection type:	Dynamic IPv4
Status:	Connected <span style="color: green;">●</span>
Interface:	WAN
IP address:	192.168.161.235
Subnet mask:	255.255.255.0
Gateway IP address:	192.168.161.1

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

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

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

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

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



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

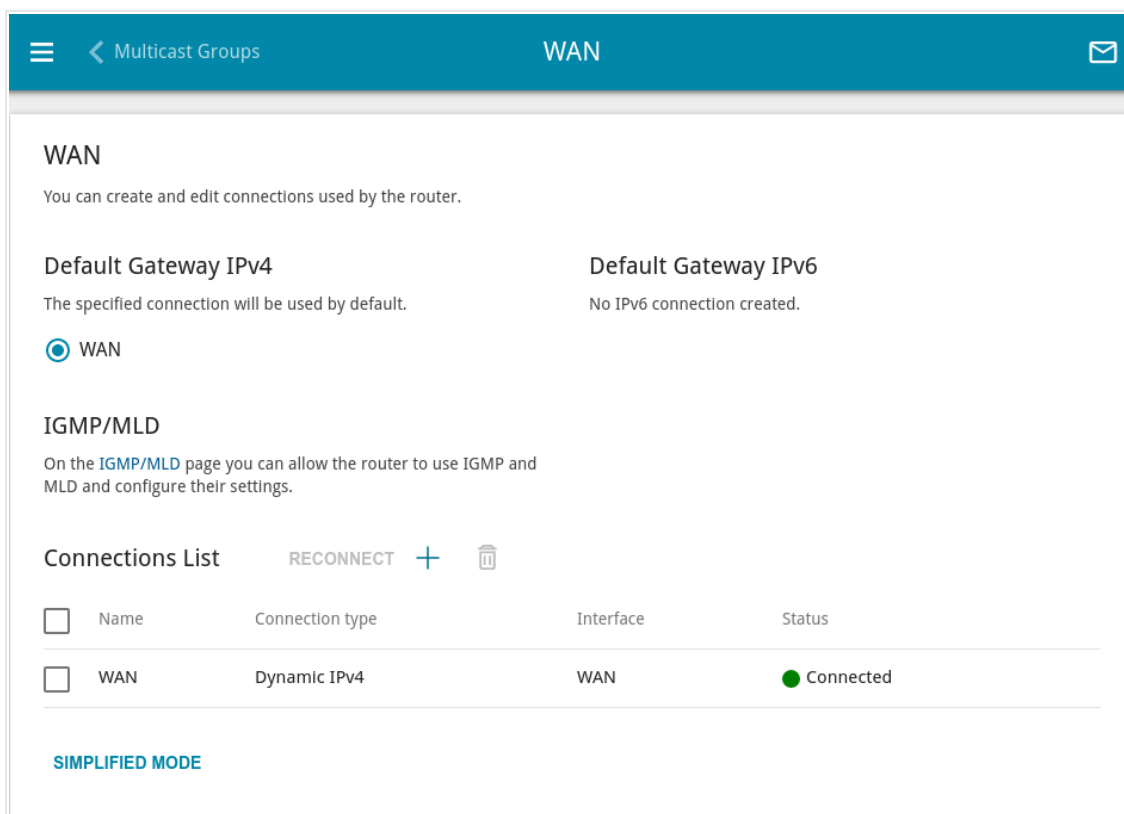




Figure 67. The **Connections Setup / WAN** page. The advanced mode.

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

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

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

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

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP/MLD** link (for the description of the page, see the **IGMP/MLD** section, page 248).

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

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

## Creating Dynamic IPv4 or Static IPv4 WAN Connection

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

**General Settings**

Connection type  
Static IPv4

Interface  
WAN

Connection name\*  
statip

☒ Enable connection

☒ NAT

*The network address translation function. It is recommended not to disable unless your ISP requires it.*

☐ Ping

*WAN Ping Respond allows the device to respond to ping requests from the external network.*

☐ RIP

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

Parameter	Description
<b>General Settings</b>	
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
<b>Ping</b>	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

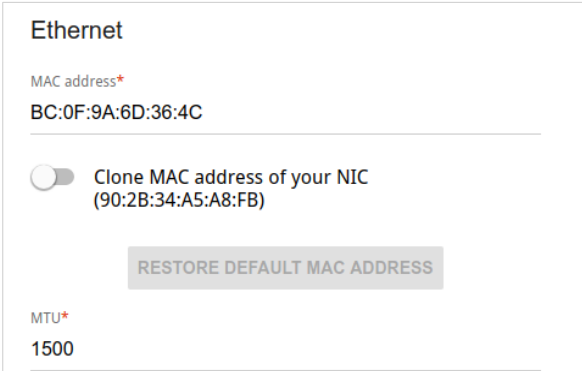
Parameter	Description
<b>RIP</b>	Move the switch to the right to allow using RIP for this connection.
	

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

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

### IPv4

IP address\*

192.168.161.224

---

Subnet mask\*

255.255.255.0

---

Gateway IP address\*

192.168.161.1

---

Primary DNS\*

1.1.1.1

---

Secondary DNS

1.0.0.1

---

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

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

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

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



## Creating Dynamic IPv6 or Static IPv6 WAN Connection

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

**General Settings**

Connection type  
Static IPv6

Interface  
WAN

Connection name\*  
statipv6\_43

☒ Enable connection

☐ NATv6  
① The network address translation function. It is recommended not to disable unless your ISP requires it.

☐ Ping  
① WAN Ping Respond allows the device to respond to ping requests from the external network.

☐ RIPng

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

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

Ethernet

MAC address\*

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

☐

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

RESTORE DEFAULT MAC ADDRESS

MTU\*

1500

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

Parameter	Description
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 <b>Clone MAC address of your NIC</b> switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the router's MAC address, click the <b>RESTORE DEFAULT MAC ADDRESS</b> button (the button is available when the switch is moved to the right).</p>
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 73. The page for creating a new **Static IPv6** connection. The **IPv6** section.

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

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

## Creating PPPoE WAN Connection

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

**General Settings**

Connection type  
PPPoE

Interface  
WAN

Connection name\*  
pppoe

☒ Enable connection

☒ NAT

The network address translation function. It is recommended not to disable unless your ISP requires it.

☐ Ping

WAN Ping Respond allows the device to respond to ping requests from the external network.

☐ RIP

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

Parameter	Description
<b>General Settings</b>	
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
<b>Ping</b>	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
<b>RIP</b>	Move the switch to the right to allow using RIP for this connection.

Ethernet

MAC address\*

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

☐

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

RESTORE DEFAULT MAC ADDRESS

MTU\*

1500

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

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

### PPP

☐ Without authorization

Username\*

Password\*

Service name

MTU\*

Encryption protocol
 

No encryption

Authentication protocol
 

AUTO

☒ Keep Alive

LCP interval (in seconds)\*

LCP failures\*


☐ Dial on demand

Maximum idle time (in seconds)

Static IP address

☐ PPP debug

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

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

Parameter	Description
<b>Encryption protocol</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encryption</b>: MPPE encryption is not applied.</li> <li>• <b>MPPE 40 128 bit</b>: MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit</b>: MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit</b>: MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MS-CHAP</b>, <b>MS-CHAPv2</b>, or <b>AUTO</b> value is selected from the <b>Authentication protocol</b> drop-down list.</p>
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.
<b>Keep Alive</b>	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the <b>LCP interval</b> and <b>LCP failures</b> fields correspondingly or leave the default values.
<b>Dial on demand</b>	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.
<b>Static IP address</b>	Fill in the field if you want to use a static IP address to access the Internet.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list in the settings of the corresponding event log in the <b>Logging</b> section (see the <b>Logging</b> section, page 297).

IPv4

Obtain DNS server addresses automatically

Primary DNS

Secondary DNS

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

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

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

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

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



## Creating PPTP, L2TP, L2TP Dual Stack, or L2TP over IPsec WAN Connection

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

**General Settings**

Connection type  
PPTP

Connection name\*  
pptp\_11

☒ Enable connection

☒ NAT

i The network address translation function. It is recommended not to disable unless your ISP requires it.

☐ Ping

i WAN Ping Respond allows the device to respond to ping requests from the external network.

☐ RIP

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


Parameter	Description
<b>General Settings</b>	
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
<b>NATv6</b>	<i>For the <b>L2TP Dual Stack</b> type only.</i> If the switch is moved to the right, the network address translation function for IPv6 is enabled. Do not disable the function unless your ISP requires this.
<b>Ping</b>	<i>For the <b>PPTP</b>, <b>L2TP</b>, and <b>L2TP Dual Stack</b> types only.</i> If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

Parameter	Description
<b>RIP</b>	<p>For the <b>PPTP</b> and <b>L2TP</b> types only.</p> <p>Move the switch to the right to allow using RIP for this connection.</p>

**PPP**

☐ Without authorization

Username\*

Password\* 

VPN server address\*

MTU\*  
1456

Encryption protocol  
No encryption ▼


Authentication protocol  
AUTO ▼

☒ Keep Alive

LCP interval (in seconds)\*  
30

LCP failures\*  
3


☐ Dial on demand

Maximum idle time (in seconds)  
30 

Static IP address

☐ PPP debug


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

Parameter	Description
<b>PPP</b>	
<b>Without authorization</b>	Move the switch to the right if you don't need to enter a username and password to access the Internet.
<b>Username</b>	A username (login) to access the Internet.
<b>Password</b>	A password to access the Internet. Click the <b>Show</b> icon (  ) to display the entered password.

Parameter	Description
<b>VPN server address</b>	The IP address or full domain name of the PPTP or L2TP authentication server.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>Encryption protocol</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encryption</b>: MPPE encryption is not applied.</li> <li>• <b>MPPE 40 128 bit</b>: MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit</b>: MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit</b>: MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MS-CHAP</b>, <b>MS-CHAPv2</b>, or <b>AUTO</b> value is selected from the <b>Authentication protocol</b> drop-down list.</p>
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.
<b>Keep Alive</b>	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the <b>LCP interval</b> and <b>LCP failures</b> fields correspondingly or leave the default values.
<b>Dial on demand</b>	<p><i>For the <b>PPTP</b>, <b>L2TP</b>, and <b>L2TP over IPsec</b> types only.</i></p> <p>Move the switch to the right if you want the router to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.</p>
<b>Static IP address</b>	Fill in the field if you want to use a static IP address to access the Internet.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list in the settings of the corresponding event log in the <b>Logging</b> section (see the <b>Logging</b> section, page 297).

IPv4

☒ Obtain DNS server addresses automatically

Primary DNS 




Secondary DNS 

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


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

IPv6

Get IPv6  
Automatically 

Enable prefix delegation  
Auto 

☒ Obtain DNS server addresses automatically

Primary IPv6 DNS server 


Secondary IPv6 DNS server 

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

Parameter	Description
<b>IPv6 (for the L2TP Dual Stack type)</b>	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the <b>Automatically</b> value.

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

IPsec

Pre-shared key\*

☒ Enable PFS

DPD action  
Restart

DPD - Dead Peer Detection

DPD delay (in seconds)\*  
30

DPD timeout (in seconds)\*  
120

☐ Specify connection port

IKE version  
1

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



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

Parameter	Description
<b>IPsec (for the L2TP over IPsec type)</b>	
<b>Pre-shared key</b>	A key for mutual authentication of the parties. Click the <b>Show</b> icon (🔍) to display the entered key.
<b>Enable PFS</b>	Move the switch to the right to enable the PFS option ( <i>Perfect Forward Secrecy</i> ). If the switch is moved to the right, a new encryption key exchange will be used upon establishing the IPsec tunnel. This option enhances the security level of data transfer, but increases the load on DIR-853.
<b>DPD action</b>	<p>Using DPD protocol (<i>Dead Peer Detection</i>) allows to check the status of the remote host in the tunnel: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD requests to the remote host. Select the needed action from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Restart</b>: Restart the tunnel connection immediately.</li> <li>• <b>Hold</b>: Reestablish the connection upon request when the traffic matching the tunnel appears.</li> <li>• <b>Clear</b>: Close the tunnel connection with no further action.</li> <li>• <b>Off</b>: Disable DPD. When this value is selected, the <b>DPD delay</b> and <b>DPD timeout</b> fields are not available for editing.</li> </ul>
<b>DPD delay</b>	A time period (in seconds) between DPD messages. By default, the value <b>30</b> is specified.
<b>DPD timeout</b>	A waiting period for the response to a DPD message (in seconds). If the host does not answer in the specified time, the router breaks down the tunnel connection, updates information on it, and tries to reestablish the connection. By default, the value <b>120</b> is specified.
<b>Specify connection port</b>	Move the switch to the right to change the port used for data exchange with the other party enter the needed value in the <b>Port</b> field displayed. By default, the value <b>1701</b> is specified.
<b>IKE version</b>	IKE ( <i>Internet Key Exchange</i> ) is a protocol of keys exchange between two hosts of VPN connections. Select a version of the protocol from the drop-down list.

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

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

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

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

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

## Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

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

**General Settings**

Connection type  
PPPoE IPv6

Interface  
WAN

Connection name\*  
pppoev6\_19

☒ Enable connection

☐ NATv6

You can't use prefix delegation and NATv6 simultaneously

The network address translation function. It is recommended not to disable unless your ISP requires it.

☐ Ping

WAN Ping Respond allows the device to respond to ping requests from the external network.

☐ RIPng

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

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



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

Ethernet

MAC address\*

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

---

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

RESTORE DEFAULT MAC ADDRESS

MTU\*

1500

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

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

PPP

Without authorization

Username\*

Password\*

Service name

MTU\*

1492

Encryption protocol

No encryption

Authentication protocol

AUTO

Keep Alive

LCP interval (in seconds)\*

30


LCP failures\*

3

Static IP address

PPP debug

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

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

Parameter	Description
<b>Encryption protocol</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encryption</b>: MPPE encryption is not applied.</li> <li>• <b>MPPE 40 128 bit</b>: MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit</b>: MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit</b>: MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MS-CHAP</b>, <b>MS-CHAPv2</b>, or <b>AUTO</b> value is selected from the <b>Authentication protocol</b> drop-down list.</p>
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.
<b>Keep Alive</b>	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the <b>LCP interval</b> and <b>LCP failures</b> fields correspondingly or leave the default values.
<b>Static IP address</b>	Fill in the field if you want to use a static IP address to access the Internet.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list in the settings of the corresponding event log in the <b>Logging</b> section (see the <b>Logging</b> section, page 297).

IPv4

Obtain DNS server addresses automatically

Primary DNS

Secondary DNS

Figure 86. The page for creating a new **PPPoE Dual Stack** connection. The **IPv4** section.

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

IPv6

Get IPv6

Automatically

Enable prefix delegation

Auto

Obtain DNS server addresses automatically

Primary IPv6 DNS server

Secondary IPv6 DNS server

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

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

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

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

## Creating Mobile Internet WAN Connection

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

**General Settings**

Connection type  
**Mobile Internet**

Connection name\*  
**mobileinet\_78**

☒ Enable connection

☐ Use as interface

① This option allows creating a network interface to connect clients to the modem through a transparent bridge. Attention! Only clients connected to the interfaces which are included into this transparent bridge will have access to the Internet. For further configuration, please go to the VLAN page

☒ NAT

① The network address translation function. It is recommended not to disable unless your ISP requires it.

☐ Ping

① WAN Ping Respond allows the device to respond to ping requests from the external network.

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

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

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

Modem Settings

**MODEM/SIM CARD SELECTION**

Mode  
Auto

APN

Dial number  
\*99#

☒ Without authorization

Authentication protocol  
PAP

Username

Password

Type  
IPv4

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

Parameter	Description
<b>Modem Settings</b>	
<b>MODEM/SIM CARD SELECTION</b>	Click the button in order to assign the connection to one of connected USB modems. <sup>11</sup>

<sup>11</sup> When several devices are connected to one USB port of the router, it is recommended to use a self-powered USB hub.

Parameter	Description
<b>Mode</b>	The value of the field specifies the type of the network to which the router connects. Leave the <b>Auto</b> value to let the router connect automatically to an available type of network, or select a needed value from the drop-down list.
<b>APN</b>	An access point name.
<b>Dial number</b>	A number dialed to connect to the authorization server of the operator.
<b>Without authorization</b>	Move the switch to the right if your operator does not require authorization.
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list.
<b>Username</b>	A username (login) to connect to the network of the operator.
<b>Password</b>	A password to connect to the network of the operator. Click the <b>Show</b> icon (🔍) to display the entered password.
<b>Type</b>	An IP version which will be used by this connection. Select the <b>IPv4</b> , <b>IPv6</b> , or <b>Dual</b> value from the drop-down list.

PPP

MTU\*  
1370

☒ Keep Alive

LCP interval (in seconds)\*  
30

LCP failures\*  
3

☐ Dial on demand

Maximum idle time (in seconds)  
30

☐ PPP debug

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

Parameter	Description
<b>PPP</b>	
<b>MTU</b>	The maximum size of units transmitted by the interface.



Parameter	Description
<b>Keep Alive</b>	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the <b>LCP interval</b> and <b>LCP failures</b> fields correspondingly or leave the default values.
<b>Dial on demand</b>	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list in the settings of the corresponding event log in the <b>Logging</b> section (see the <b>Logging</b> section, page 297).

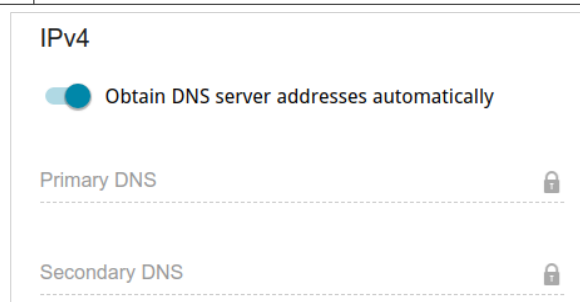



Figure 91. The page for creating a new **Mobile Internet** connection. The **IPv4** section.

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

IPv6

☒ Obtain DNS server addresses automatically

Primary IPv6 DNS server 



Secondary IPv6 DNS server 

Figure 92. The page for creating a new **Mobile Internet** connection. The **IPv6** section.


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

Health Check


☐ Enable

 Checking connection status using the ping command


The maximum number of attempts

10 

☐ Connection restart

 The connection will be restarted after the number of attempts to check the destination host availability reaches the maximum value

Addresses

 List is empty (Default 2001:4860:4860::8888)

ADD

☒ Modem IP address verification



 When the IP address of the modem is changed, the request to update the IP address is sent to all actual connections

Figure 93. The page for creating a new **Mobile Internet** connection. The **Health Check** section.

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

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

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

## Creating IPIP6 WAN Connection

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

**General Settings**

Connection type  
IPIP6

Connection name\*  
ipip6\_33

☒ Enable connection

☐ NAT  
The network address translation function. It is recommended not to disable unless your ISP requires it.

☐ Ping  
WAN Ping Respond allows the device to respond to ping requests from the external network.

Figure 94. The page for creating a new **IPIP6** connection. The **General Settings** section.

Parameter	Description
General Settings	
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
<b>Ping</b>	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

Figure 95. The page for creating a new **IPIP6** connection. The **IP** section.

Parameter	Description
<b>IP</b>	
<b>Obtain remote host address automatically</b>	Move the switch to the right to configure automatic assignment of a remote host IPv6 address.
<b>Type</b>	<p>Select an identification method for the remote host from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Address</b>: The remote host is identified by its IPv6 address.</li> <li>• <b>FQDN</b>: The remote host is identified by its domain name.</li> </ul> <p>The drop-down list is displayed if the <b>Obtain remote host address automatically</b> switch is moved to the left.</p>
<b>Remote host</b>	<p>Enter the remote host IPv6 address if the <b>Address</b> value is selected from the <b>Type</b> drop-down list.</p> <p>Enter the remote host domain name if the <b>FQDN</b> value is selected from the <b>Type</b> drop-down list.</p> <p>The field is available for editing, if the <b>Obtain remote host address automatically</b> switch is moved to the left.</p>
<b>Mode</b>	<p>An operation mode of the connection.</p> <p>From the drop-down list, select the <b>DSLite</b> value.</p>
<b>Set MTU automatically</b>	<p>Move the switch to the right to set the maximum size of units transmitted by the interface automatically.</p> <p>Move the switch to the left to specify this parameter manually. Upon that the <b>MTU</b> field is displayed.</p>
<b>MTU</b>	The maximum size of units transmitted by the interface.

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

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

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

## Creating 6in4 WAN Connection



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

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

**General Settings**

Connection type  
6in4

Connection name\*  
6in4\_59

☒ Enable connection

☐ Ping

WAN Ping Respond allows the device to respond to ping requests from the external network.

☐ RIPng

Remote host\*

Client IPv6 address\*

Server IPv6 address\*

Enter the server and client IPv6 addresses received from the tunnel broker without specifying the prefix length (for example, 2001:0DB8::1)

Routed IPv6 network\*

Enter the IPv6 subnet which will be routed through the connection of 6in4 type without specifying the prefix length (for example, 2001:0DB8::)

☒ Set MTU automatically

Figure 96. The page for creating a new **6in4** connection.

Parameter	Description
General Settings	
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>Ping</b>	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
<b>RIPng</b>	Move the switch to the right to allow using RIPng for this connection.
<b>Remote host</b>	Enter the IPv4 address of the server provided by the tunnel broker.
<b>Client IPv6 address</b>	Enter the IPv6 address of the router provided by the tunnel broker (without specifying the prefix length).
<b>Server IPv6 address</b>	Enter the IPv6 address of the server provided by the tunnel broker (without specifying the prefix length).

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

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

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

To use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select an existing connection which will be used to access the server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.



## Creating 6to4 WAN Connection

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

The screenshot shows the 'General Settings' configuration page for a '6to4 Relay Router' with IP address '192.88.99.1'. The 'Connection type' is set to '6to4'. The 'Connection name' is '6to4\_74'. There are two toggle switches: 'Enable connection' is turned on, and 'Ping' is turned off. A note at the bottom indicates that 'WAN Ping Respond' allows the device to respond to ping requests from the external network.

Figure 97. The page for creating a new **6to4** connection.

Parameter	Description
<b>General Settings</b>	
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>Ping</b>	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
<b>6to4 Relay Router</b>	The IPv4 address of the gateway which is used to transfer IPv6 packets.
<b>Set MTU automatically</b>	Move the switch to the right to set the maximum size of units transmitted by the interface automatically. Move the switch to the left to specify this parameter manually. Upon that the <b>MTU</b> field is displayed.
<b>MTU</b>	The maximum size of units transmitted by the interface.

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

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

To use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select an existing connection which will be used to access the server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

## Creating 6rd WAN Connection

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

The screenshot shows the 'General Settings' section for creating a new 6rd connection. It includes a toggle for 'Obtain 6rd settings automatically' (checked), a 'Connection type' dropdown set to '6rd', and a 'Connection name' field with '6rd\_18'. There are also toggles for 'Enable connection' (checked), 'Ping' (unchecked), and 'Hub and spoke' (unchecked). A note states: 'WAN Ping Respond allows the device to respond to ping requests from the external network.' On the right, there are fields for '6rd Border Relay', '6rd IPv6 prefix', '6rd IPv6 prefix length' (set to 32), and 'IPv4 mask length' (set to 0), all of which are locked. At the bottom, there is a 'Set MTU automatically' toggle (checked).

Figure 98. The page for creating a new **6rd** connection.

Parameter	Description
<b>General Settings</b>	
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>Ping</b>	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
<b>Obtain 6rd settings automatically</b>	Move the switch to the right to let the router obtain 6rd domain settings automatically from the LAN DHCP server or from a delegating router. Upon that the <b>6rd Border Relay</b> , <b>6rd IPv6 prefix</b> , <b>6rd IPv6 prefix length</b> , and <b>IPv4 mask length</b> fields are not available for editing.
<b>6rd Border Relay</b>	Enter the IPv4 address of the router provided by your ISP for the 6rd domain.
<b>6rd IPv6 prefix</b>	The IPv6 prefix for the 6rd domain provided by your ISP.
<b>6rd IPv6 prefix length</b>	The IPv6 prefix length for the 6rd domain (in bits) allocated by your ISP. By default, the value <b>32</b> is specified.

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

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

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

To use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select an existing connection which will be used to access the server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

## LAN

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

### IPv4

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

Local IP Address

IP address\*

192.168.0.1

Mask\*

255.255.255.0


Hostname

dlinkrouter.local

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

Parameter	Description
<b>Local IP Address</b>	
<b>Mode of local IP address assignment</b>	<p>Available if the <b>Access point</b> or <b>Repeater</b> mode was selected in the Initial Configuration Wizard.</p> <p>Select the needed value from the drop-down list.</p> <ul style="list-style-type: none"> <li><b>Static:</b> The IPv4 address, subnet mask, and the gateway IP address are assigned manually.</li> <li><b>Dynamic:</b> The router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects. When this value is selected, the controls of the <b>Dynamic IP Addresses</b> section are not available. Also when this value is selected, the <b>Obtain DNS server addresses automatically</b> switch is displayed on the tab.</li> </ul>
<b>IP address</b>	The IPv4 address of the router in the local subnet. By default, the following value is specified: <b>192.168.0.1</b> .
<b>Mask</b>	The mask of the local subnet. By default, the following value is specified: <b>255.255.255.0</b> .

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

### Dynamic IP Addresses

Mode of IPv4 address assignment

DHCP

Start IP\*

192.168.0.100

End IP\*

192.168.0.199

[SELECT ADDRESS RANGE](#)

Lease time (in minutes)\*


1440

☒ DNS relay

(i) Assigns the LAN IP address of the device as the DNS server for connected clients.

Figure 100. Configuring the local interface. The **IPv4** tab. The **Dynamic IP Addresses** section.

Parameter	Description
<b>Dynamic IP Addresses</b>	
<b>Mode of IPv4 address assignment</b>	<p>An operating mode of the router's DHCP server.</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>: The router's DHCP server is disabled, clients' IP addresses are assigned manually.</li> <li>• <b>DHCP</b>: The router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the <b>Start IP</b>, <b>End IP</b>, <b>Lease time</b> fields, the <b>SELECT ADDRESS RANGE</b> button, and the <b>DNS relay</b> switch are displayed on the tab. Also when this value is selected, the <b>DHCP Options</b>, <b>Static IP Addresses</b>, and <b>Hosts</b> sections are displayed on the tab.</li> <li>• <b>Relay</b>: An external DHCP server is used to assign IP addresses to clients. When this value is selected, the <b>External DHCP server IP</b>, <b>Option 82 Circuit ID</b>, <b>Option 82 Remote ID</b>, and <b>Option 82 Subscriber ID</b> fields are displayed on the tab. <i>Available if the <b>Router</b>, <b>WISP Repeater</b>, or <b>Mobile Internet</b> mode was selected in the Initial Configuration Wizard.</i></li> </ul>
<b>Start IP</b>	The start IP address of the address range used by the DHCP server to distribute IP addresses to clients.
<b>End IP</b>	The end IP address of the address range used by the DHCP server to distribute IP addresses to clients.
<b>SELECT ADDRESS RANGE</b>	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the <b>SAVE</b> button to automatically fill in the <b>Start IP</b> and <b>End IP</b> fields.
<b>Lease time</b>	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
<b>DNS relay</b>	<p>Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address.</p> <p>Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the <b>Advanced / DNS</b> page as the DNS server address.</p>

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

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

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



Figure 101. Configuring the local interface. The **IPv4** tab. The section for configuring DHCP options.

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

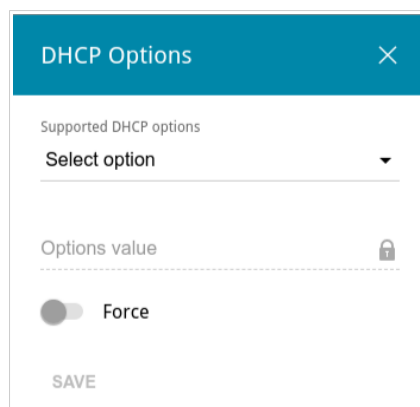



Figure 102. Configuring the local interface. The **IPv4** tab. The window for configuring a DHCP option.

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

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

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

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

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

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

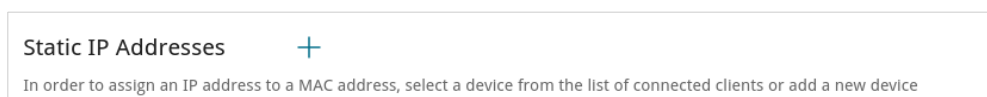





Figure 103. Configuring the local interface. The **IPv4** tab. The section for creating MAC-IPv4 pairs.

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

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

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



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

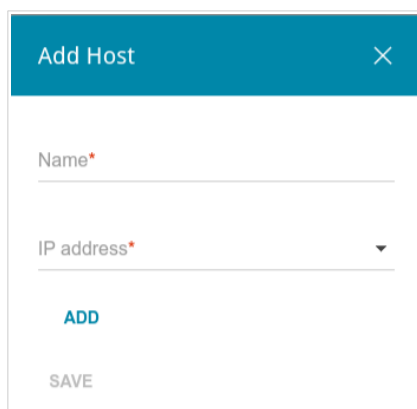



Figure 104. Configuring the local interface. The **IPv4** tab. The window for adding a DNS record.

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

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

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

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

## IPv6

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


Figure 105. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.

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

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

Also you can specify the following parameters:

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

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

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

### Dynamic IP Addresses

Mode of IPv6 address assignment

Stateful

Start IP\*

::2


End IP\*

::64

SELECT ADDRESS RANGE

Lease time (in minutes)\*

1440

 Lease time will be chosen by ISP based on the delegated prefix life time.

☐ The default route for LAN clients

☒ DNS relay



 Assigns the LAN IP address of the device as the DNS server for connected clients.

Figure 106. Configuring the local interface. The **IPv6** tab. The **Dynamic IP Addresses** section.

Parameter	Description
<b>Dynamic IP Addresses</b>	
<b>Mode of IPv6 address assignment</b>	<p>Select the needed value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Disable:</b> Clients' IPv6 addresses are assigned manually.</li> <li>• <b>Stateless:</b> Clients themselves configure IPv6 addresses using the prefix.</li> <li>• <b>Stateful:</b> The built-in DHCPv6 server of the router allocates addresses from the range specified in the <b>Start IP</b> and <b>End IP</b> fields. Also when this value is selected, the <b>Static IP Addresses</b> and <b>Hosts</b> sections are displayed on the tab.</li> <li>• <b>Relay:</b> An external DHCP server is used to assign IPv6 addresses to clients. When this value is selected, the <b>External DHCP server IP</b> field is displayed on the tab. <i>Available if the <b>Router</b>, <b>WISP Repeater</b>, or <b>Mobile Internet</b> mode was selected in the Initial Configuration Wizard.</i></li> </ul>
<b>Start IP / End IP</b>	The start and the end values for the latest hexet (16 bit) of the range of IPv6 addresses which the DHCPv6 server distributes to clients.
<b>SELECT ADDRESS RANGE</b>	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the <b>SAVE</b> button to automatically fill in the <b>Start IP</b> and <b>End IP</b> fields.
<b>Lease time</b>	The lifetime of IPv6 addresses provided to clients.
<b>The default route for LAN clients</b>	Move the switch to the right to let the clients, that received IPv6 addresses or configured them using the prefix, use the router as the default IPv6 route.
<b>DNS relay</b>	<p>Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address.</p> <p>Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the <b>Advanced / DNS</b> page as the DNS server address.</p>
<b>External DHCP server IP</b>	<p>The IPv6 address of the external DHCP server which assigns IPv6 addresses to the router's clients.</p> <p>To specify several IPv6 addresses, click the <b>ADD</b> button, and in the line displayed, enter an IPv6 address.</p> <p>To remove the IPv6 address, click the <b>DELETE</b> button (  ) in the line of the address.</p>

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

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

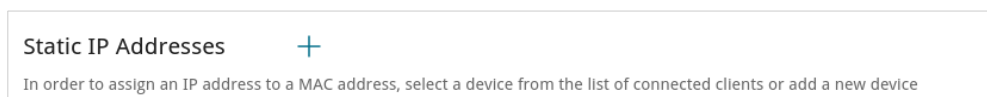





Figure 107. Configuring the local interface. The **IPv6** tab. The section for creating MAC-IPv6 pairs.

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

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

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

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

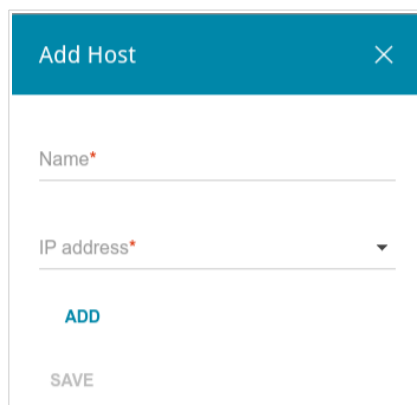



Figure 108. Configuring the local interface. The **IPv6** tab. The window for adding a DNS record.

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

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

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

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

## WAN Failover

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

The screenshot shows the 'WAN Failover' configuration page. At the top, there's a blue header with a menu icon, a 'Home' link, the title 'WAN Failover', and an email icon. Below the header, the page title 'WAN Failover' is followed by a descriptive paragraph. A toggle switch labeled 'Enable' is currently turned on. The page is divided into two main sections: 'Connections IPv4' and 'Check with ping'. The 'Connections IPv4' section includes a table of available connections. The 'Check with ping' section contains input fields for 'Interval between checks (in seconds)\*' (set to 30), 'Waiting for response (in seconds)\*' (set to 1), and 'Number of ping requests\*' (set to 3). Below these are 'Hosts' listed as 8.8.8.8, 77.88.55.55, and 94.100.180.200, each with a delete icon. An 'ADD HOST' link is at the bottom of the hosts list. An 'APPLY' button is located at the bottom left of the page.

Connection	Check with ping
pppoe_95	On
WAN	On

Interval between checks (in seconds)\*  
30

Waiting for response (in seconds)\*  
1

Number of ping requests\*  
3

Hosts

- 8.8.8.8 x
- 77.88.55.55 x
- 94.100.180.200 x

[ADD HOST](#)

**APPLY**

Figure 109. The **Connections Setup / WAN Failover** page.

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

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

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

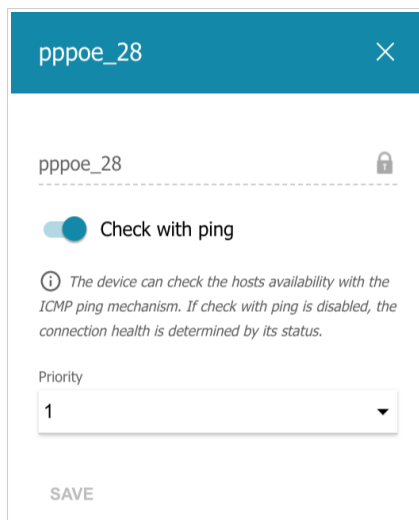


Figure 110. The window for changing the priority of a connection.

In the opened window, specify the needed parameters.

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

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



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

Parameter	Description
<b>Check with ping</b>	
<b>Interval between checks</b>	<p>A time period (in seconds) between regular checks of the hosts' availability. By default, the value <b>30</b> is specified. The value of this field should be higher than product of <b>Waiting for response</b> and <b>Number of ping requests</b> fields values.</p> <p>After a successful check the router keeps using the main connection. If the check fails, the router repeats it. After two failed checks the next operational connection from the list will be used as the default connection.</p>
<b>Waiting for response</b>	<p>A time period (in seconds) allocated for a response to one ping request.</p>
<b>Number of ping requests</b>	<p>The number of ping requests sent for each check.</p> <p>A check is considered failed in case none of the sent ping requests receive a response.</p>
<b>Hosts</b>	<p>External IP addresses that the router will check for availability via ICMP ping mechanism.</p> <p>Click the <b>ADD HOST</b> button, and in the line displayed, enter an IP address or leave values suggested by the router.</p> <p>To remove an IP address from the list, click the <b>Delete</b> icon (✕) in the line of the address.</p>

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

## Auto Configuration of 3G/LTE

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

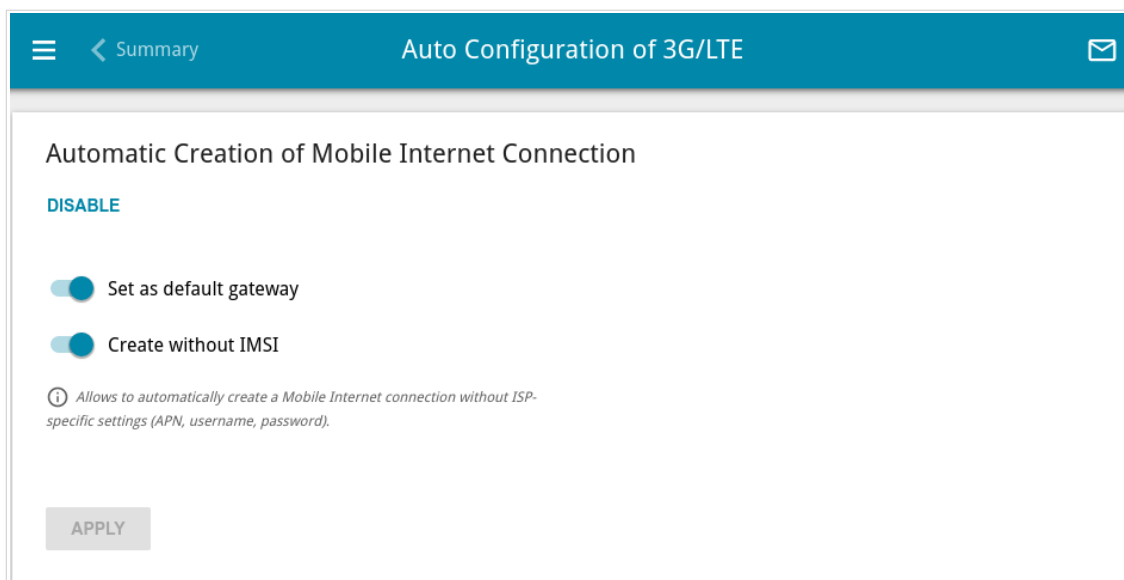


Figure 111. The **Connections Setup / Auto Configuration of 3G/LTE** page.

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

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

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

If the PIN code check for the SIM card inserted into your USB modem is disabled, then an active WAN connection with the operator's settings will be automatically created when plugging the USB modem into the router. The connection will be displayed on the **Connections Setup / WAN** page.

If you want to disable the function for automatic creation of a mobile WAN connection, click the **DISABLE** button.

## Traffic Balancing

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

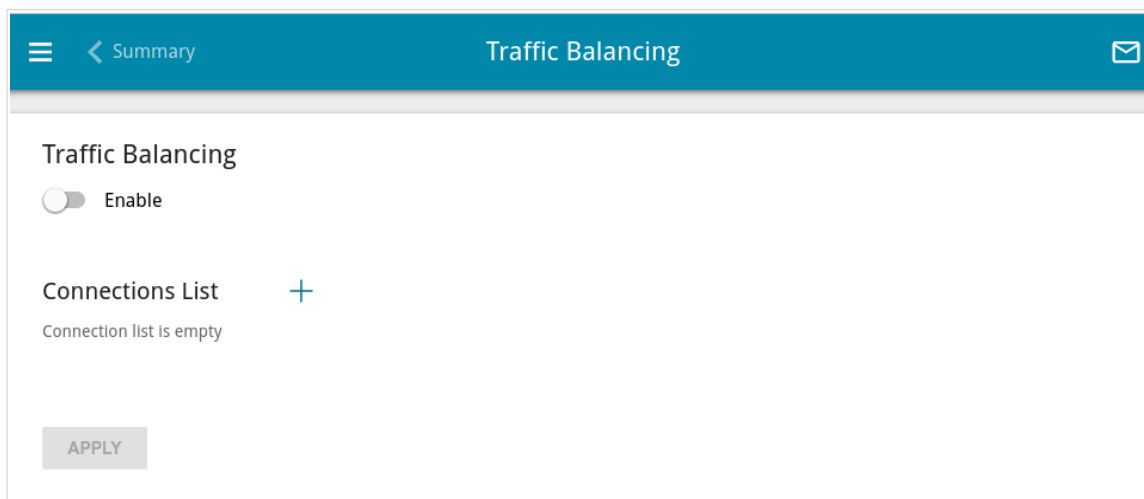


Figure 112. The **Connections Setup / Traffic Balancing** page.

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

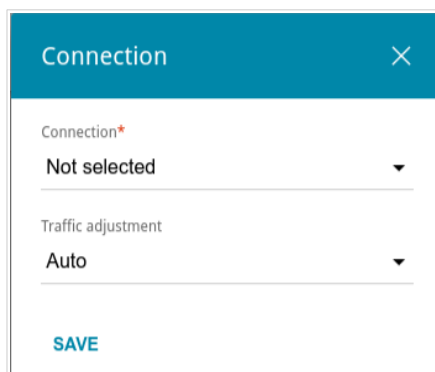



Figure 113. The window for adding a new connection to the page.

In the opened window, specify the needed parameters.

Parameter	Description
<b>Connection</b>	From the drop-down list, select a WAN connection to which traffic balancing will be applied.
<b>Traffic adjustment</b>	Select a value from the drop-down list. <ul style="list-style-type: none"><li>• <b>Auto</b>: Traffic is equally divided among connections with the same setting.</li><li>• <b>Manual</b>: Traffic is equally divided among connections in accordance with the value specified in the <b>Weight</b> field.</li></ul>
<b>Weight</b>	Specify the percentage of traffic which will pass through the connection.

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

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

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

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

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

## VPN

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

### IPsec

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

IPsec is a protocol suite for securing IP communications.

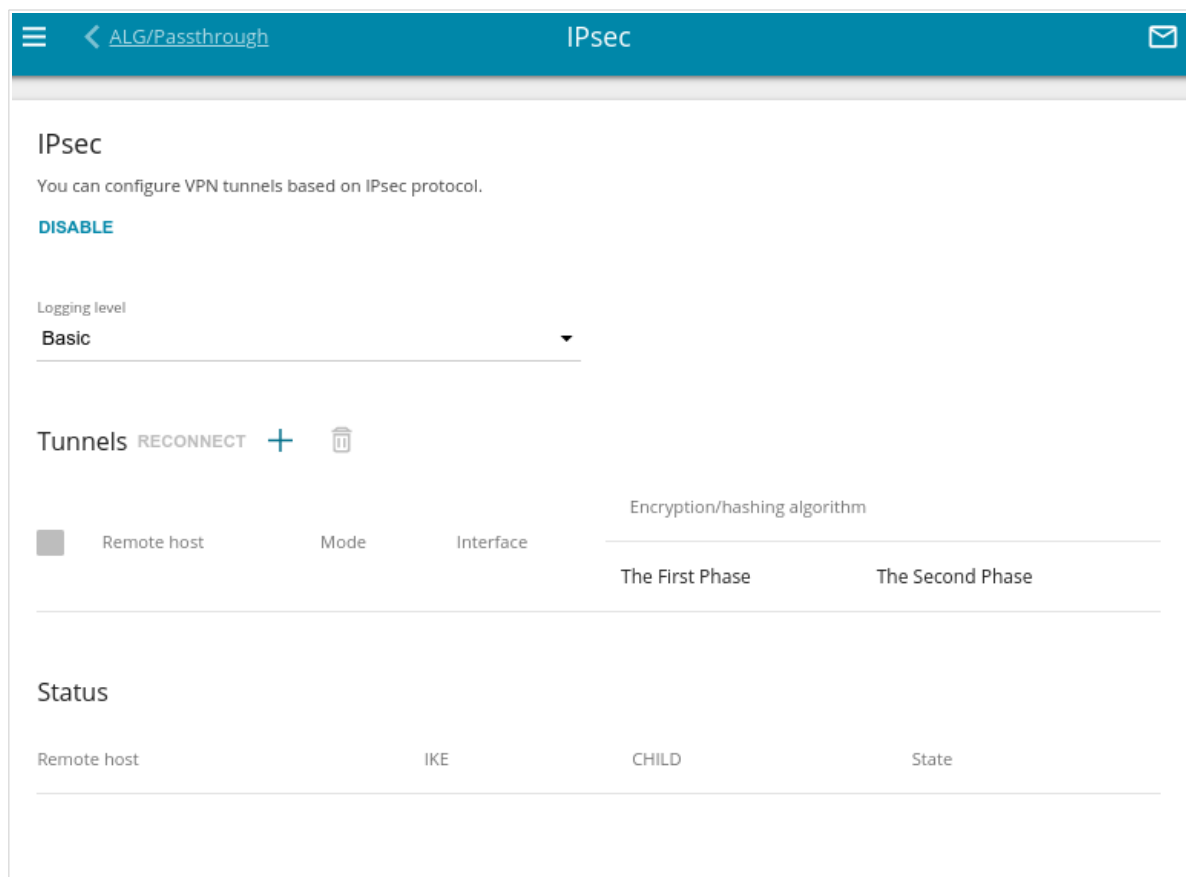



Figure 114. The **VPN / IPsec** page.

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

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

From the **Logging level** drop-down list, select a detail level of messages recorded to the system log or leave the value specified by default. The **Basic** value is recommended to establish an IPsec tunnel faster. To view the log, go to the **System / Logging / Local** page (see the *Local* section, page 297).

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



The values selected from the **IP version**, **Mode**, **IKE version** lists and the values of the **Pre-shared key** field and elements in the **The First Phase** and **The Second Phase** sections should be the same for both parties of the tunnel.

The values of the remote settings for one party of the tunnel should be the same as the values of the local settings for the other party of the tunnel.

< IPsec

IPsec/Adding

General Settings

Enable

Name\*

IPsec\_72

IP version

IPv4

Dynamic IPsec

Type

Address

Remote host\*

Remote identifier

Remote port

Pre-shared key\*

Local WAN

Default gateway

Local identifier

Local port

NAT Traversal

Enabled

Mode

TUNNEL

Allow traffic from IPsec to router

DPD action

Restart

i

DPD - Dead Peer Detection

DPD delay (in seconds)\*

30

DPD timeout (in seconds)\*

120

TCP MSS

Path MTU discovery

Aggressive Mode

IKE version

1

i

When the IKE version is changed, the first and second phase parameters can be changed.

Figure 115. The page for adding an IPsec tunnel. The **General Settings** section.

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

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


Page 143 of 323

Parameter	Description
<b>Name</b>	A name for the tunnel for easier identification.
<b>IP version</b>	An IP version.
<b>Dynamic IPsec</b>	Move the switch to the right to allow a remote host with any public IP address to connect to the router via IPsec protocol. Such a setting can be specified for one IPsec tunnel only. Connection requests via this tunnel can be sent by a remote host only.
<b>Type</b>	<p>Select an identification method for the remote host (router) from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Address</b>: The remote host is identified by its IP address.</li> <li>• <b>FQDN</b>: The remote host is identified by its domain name.</li> </ul> <p>The drop-down list is displayed if the <b>Dynamic IPsec</b> switch is moved to the left.</p>
<b>Remote host</b>	<p>Enter the remote subnet VPN gateway IP address if the <b>Address</b> value is selected from the <b>Type</b> drop-down list.</p> <p>Enter the remote subnet VPN gateway domain name if the <b>FQDN</b> value is selected from the <b>Type</b> drop-down list.</p> <p>The field is available for editing if the <b>Dynamic IPsec</b> switch is moved to the left.</p>
<b>Remote identifier</b>	A remote host identifier to establish connection over IPsec with particular hosts only. Use an IP address of a host or subnet, the value <b>%any</b> (all IP addresses), a domain name, or certificate CN. By default, the value specified in the <b>Remote host</b> field is used.
<b>Remote port</b>	A port of the remote host, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If at the same time the network address translation (NAT) function is used for the connection, port 4500 is used.
<b>Pre-shared key</b>	A PSK key for mutual authentication of the parties. Click the <b>Show</b> icon (🔍) to display the entered key.
<b>Local WAN</b>	<p>A WAN connection through which the tunnel will pass. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Interface</b>: When this value is selected, the <b>Interface</b> drop-down list is displayed. Select an existing WAN connection from the list.</li> <li>• <b>Default gateway</b>: When this value is selected, the router uses the default WAN connection.</li> </ul>



Parameter	Description
<b>Local identifier</b>	A local identifier of the router to establish connection over IPsec with particular hosts only. Use an IP address, domain name, or certificate CN. <i>Optional</i> .
<b>Local port</b>	A port of the router, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If at the same time the network address translation (NAT) function is used for the connection, port 4500 is used.
<b>NAT Traversal</b>	<p>The NAT Traversal function allows VPN traffic to pass through the NAT-enabled device. DIR-853 allows to forcibly encapsulate VPN traffic in UDP packets for passing through a remote device regardless of whether it supports address translation.</p> <p>If you need to enable forced encapsulation of VPN traffic, select the <b>Enabled</b> value.</p> <p>If you need to disable forced encapsulation of VPN traffic, select the <b>Disabled</b> value.</p>
<b>Mode</b>	<p>An operation mode of the IPsec tunnel. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>TUNNEL</b>: As a rule, it is used to create a secure connection to remote networks. In this mode, the source IP packet is fully encrypted and added to a new IP packet and data transfer is based on the header of the new IP packet.</li> <li>• <b>TRANSPORT</b>: As a rule, it is used to encrypt data stream within one network. In this mode, only the content of the source IP packet is encrypted, its header remains unchanged and data transfer is based on the source header.</li> </ul>
<b>Allow traffic from IPsec to router</b>	Move the switch to the left to deny access to your router from the remote subnet via IPsec. The switch is displayed when the <b>TUNNEL</b> value is selected from the <b>Mode</b> drop-down list.

Parameter	Description
<b>DPD action</b>	<p>Using DPD protocol (<i>Dead Peer Detection</i>) allows to check the status of the remote host in the tunnel: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD requests to the remote host. Select the needed action from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Restart:</b> Restart the tunnel connection immediately.</li> <li>• <b>Hold:</b> Reestablish the connection upon request when the traffic matching the tunnel appears.</li> <li>• <b>Clear:</b> Close the tunnel connection with no further action.</li> <li>• <b>Off:</b> Disable DPD. When this value is selected, the <b>DPD delay</b> and <b>DPD timeout</b> fields are not available for editing.</li> </ul>
<b>DPD delay</b>	A time period (in seconds) between DPD messages. By default, the value <b>30</b> is specified.
<b>DPD timeout</b>	A waiting period for the response to a DPD message (in seconds). If the host does not answer in the specified time, the router breaks down the tunnel connection, updates information on it, and tries to reestablish the connection. By default, the value <b>120</b> is specified.
<b>TCP MSS</b>	<p><i>Maximum Segment Size of a TCP packet.</i> This parameter influences the size of a TCP packet which will be sent from the remote host to the router.</p> <p>If the <b>Manual</b> value is selected, you can specify the value of this parameter for each subnet of the tunnel in the <b>MTU</b> field. The field is displayed in the window for adding a subnet in the <b>Tunneled Networks</b> section.</p> <p>If the <b>Path MTU discovery</b> value is selected, the parameter will be configured automatically for all created subnets.</p>
<b>Aggressive Mode</b>	<p>Move the switch to the right to enable the aggressive mode for mutual authentication of the parties. Such a setting accelerates the connection establishment, but reduces its security.</p> <p>The switch is displayed when the <b>1</b> value is selected from the <b>IKE version</b> drop-down list.</p>
<b>IKE version</b>	IKE ( <i>Internet Key Exchange</i> ) is a protocol of keys exchange between two hosts of VPN connections. Select a version of the protocol from the drop-down list.

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

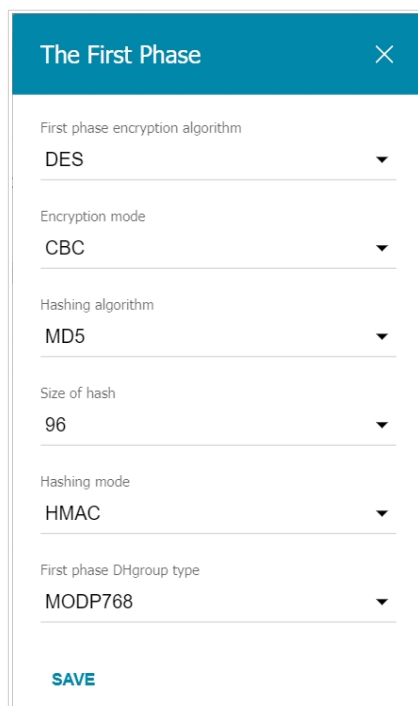



Figure 116. The window for configuring the first phase of the IPsec tunnel. **The First Phase** section.


Parameter	Description
<b>The First Phase</b>	
<b>First phase encryption algorithm</b>	Select an available encryption algorithm from the drop-down list.
<b>Encryption mode</b>	Select an encryption mode from the drop-down list.
<b>Hashing algorithm</b>	Select a hashing algorithm from the drop-down list.
<b>Size of hash</b>	The length of the hash in bits.
<b>Hashing mode</b>	Select a hashing mode from the drop-down list.
<b>First phase DHgroup type</b>	A Diffie-Hellman key group for the First Phase. Select a value from the drop-down list.
<b>The Second Phase</b>	
<b>Second phase encryption algorithm</b>	Select an available encryption algorithm from the drop-down list.
<b>Encryption mode</b>	Select an encryption mode from the drop-down list.

Parameter	Description
<b>Hashing algorithm</b>	Select a hashing algorithm from the drop-down list.
<b>Size of hash</b>	The length of the hash in bits.
<b>Hashing mode</b>	Select a hashing mode from the drop-down list.
<b>Second phase DHgroup type</b>	A Diffie-Hellman key group for the Second Phase. Select a value from the drop-down list. The drop-down list is available if the <b>Enable PFS</b> switch is moved to the right.
<b>Enable PFS</b>	Move the switch to the right to enable the PFS option ( <i>Perfect Forward Secrecy</i> ). If the switch is moved to the right, a new encryption key exchange will be used for the Second Phase. This option enhances the security level of data transfer, but increases the load on DIR-853.

Click the **SAVE** button.

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

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

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

**Add Rule** [X]

Local network

\_\_\_\_\_

**ADD SUBNET**

*Specify the local subnet of IPsec tunnel (the router's LAN). Example: 192.168.0.0/24*

Remote subnet

\_\_\_\_\_

**ADD SUBNET**

*Specify the remote subnet of IPsec tunnel (the LAN of the device which acts as a router). Example: 192.168.10.0/24*

MTU\*  
1300

**SAVE**


Figure 117. The window for adding a tunneled network.

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

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

Click the **SAVE** button.


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

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

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

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

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

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

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

## GRE

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

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

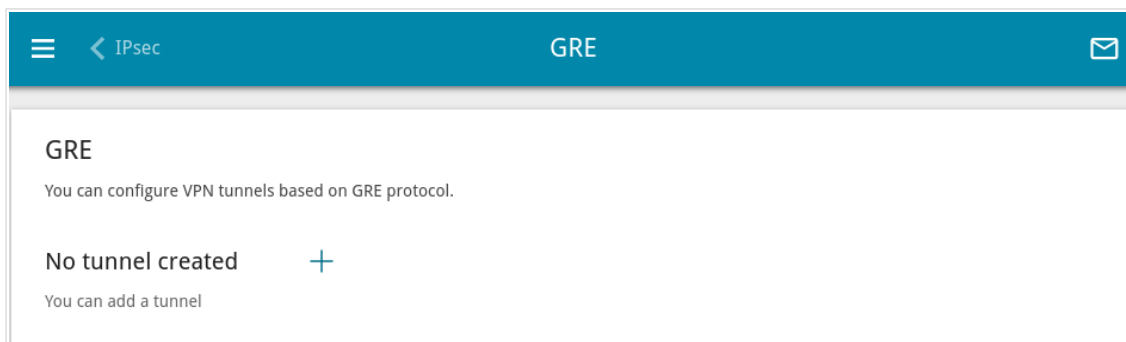


Figure 118. The **VPN / GRE** page.

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

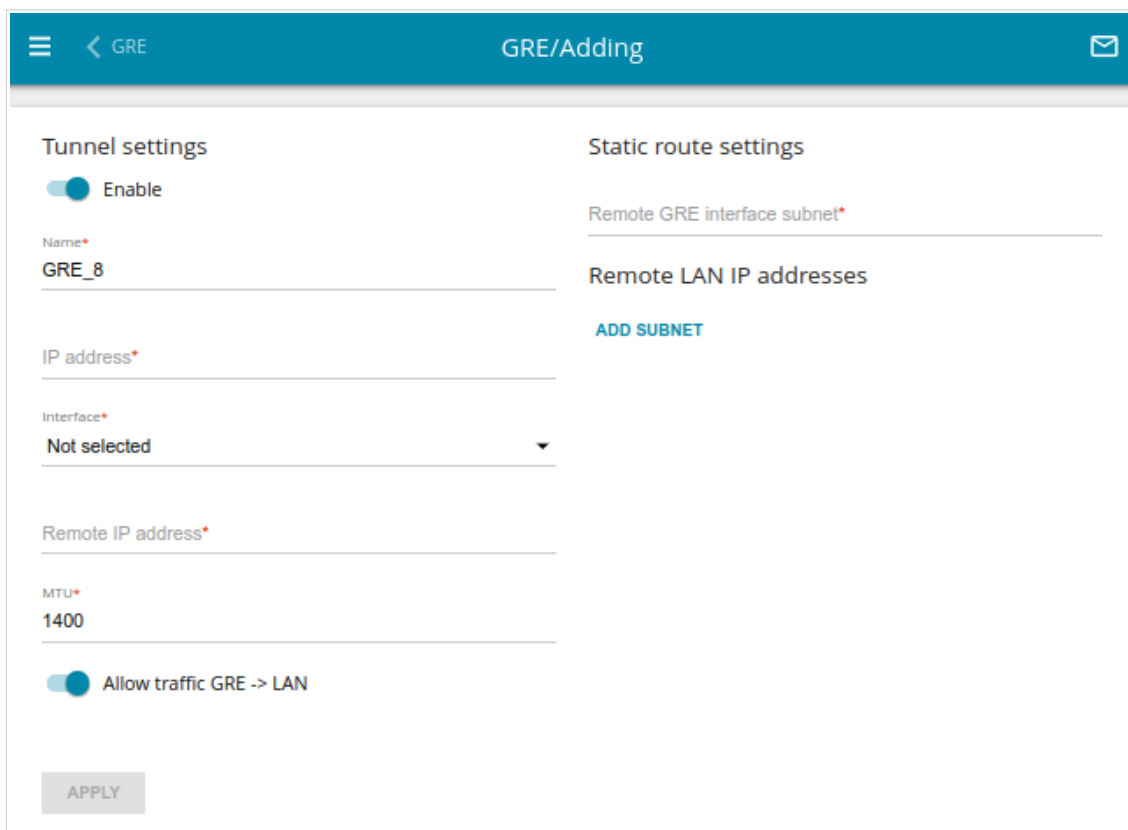


Figure 119. The page for adding a GRE tunnel.

You can specify the following parameters:

Parameter	Description
<b>Tunnel settings</b>	
<b>Enable</b>	Move the switch to the right to enable the GRE tunnel. Move the switch to the left to disable the GRE tunnel.
<b>Name</b>	A name of the tunnel for easier identification. You can specify any name.
<b>IP address</b>	The IP address of the GRE tunnel interface with the mask of the subnet.
<b>Interface</b>	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the <b>Default gateway</b> value to use the default WAN connection.
<b>Remote IP address</b>	Enter the IP address of the remote subnet VPN gateway.
<b>MTU</b>	The maximum size of units transmitted from the remote host to the router.
<b>Allow traffic GRE → LAN</b>	Move the switch to the right to allow GRE tunnel users access devices in the remote local subnet.
<b>Static route settings</b>	
<b>Remote GRE interface subnet</b>	The subnet and mask of the remote GRE interface.
<b>Remote LAN IP addresses</b>	
<b>Remote subnet</b>	To specify the IP address and mask of the remote local subnet, click the <b>ADD SUBNET</b> button, and in the line displayed, enter the needed value.  To remove a subnet, click the <b>Delete</b> icon (✕) in the corresponding line.

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

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

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



## IPIP

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

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

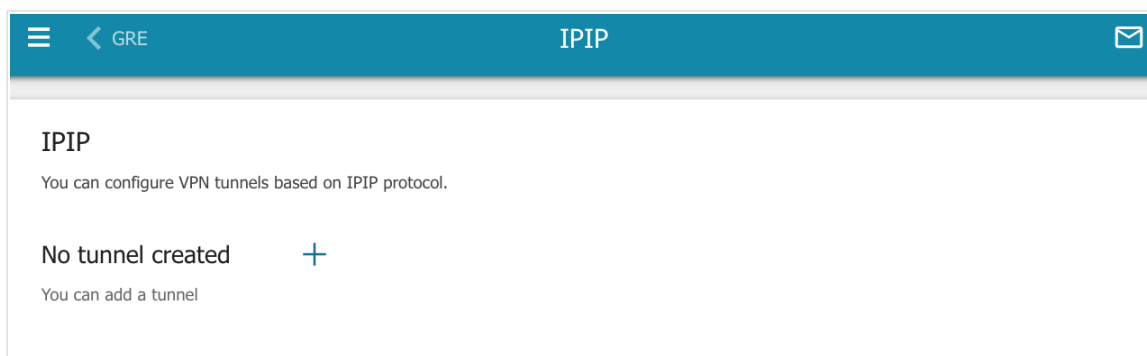


Figure 120. The **VPN / IPIP** page.

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

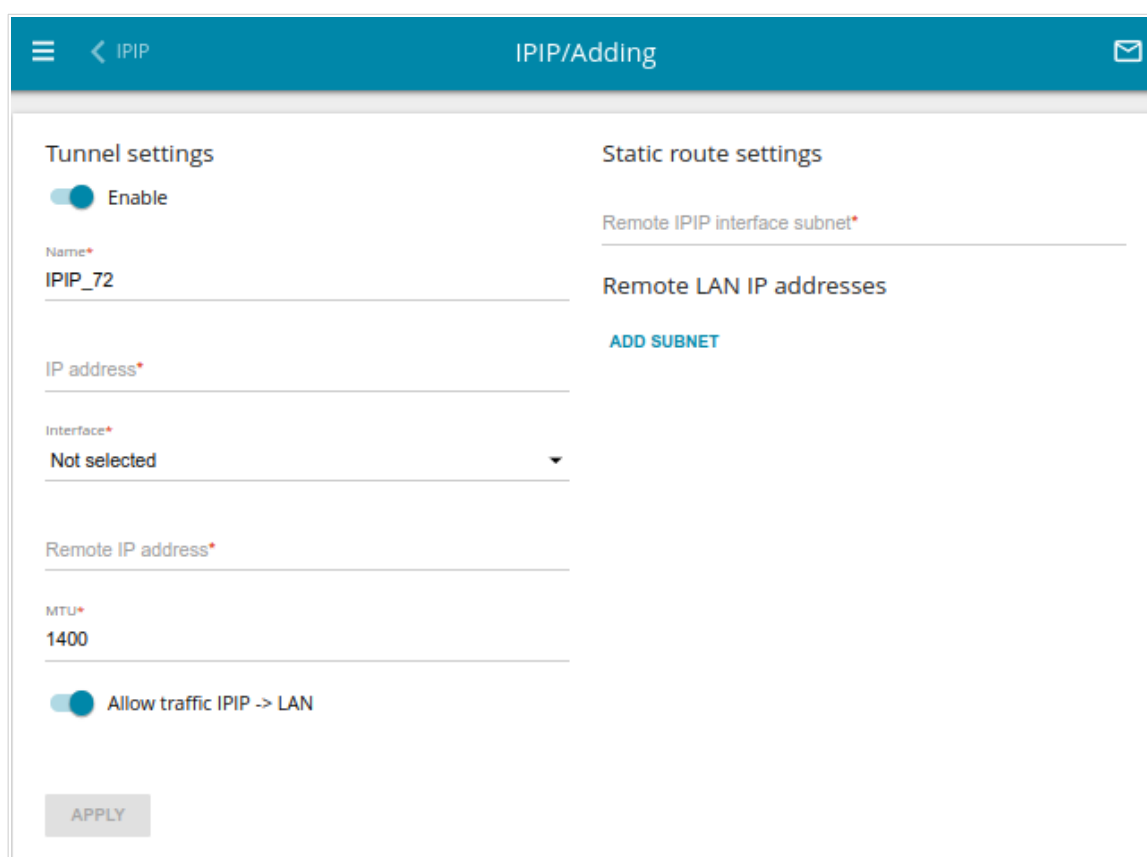


Figure 121. The page for adding an IPIP tunnel.

You can specify the following parameters:

Parameter	Description
<b>Tunnel settings</b>	
<b>Enable</b>	Move the switch to the right to enable the IPIP tunnel. Move the switch to the left to disable the IPIP tunnel.
<b>Name</b>	A name of the tunnel for easier identification. You can specify any name.
<b>IP address</b>	The IP address of the IPIP tunnel interface with the mask of the subnet.
<b>Interface</b>	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the <b>Default gateway</b> value to use the default WAN connection.
<b>Remote IP address</b>	Enter the IP address of the remote subnet VPN gateway.
<b>MTU</b>	The maximum size of units transmitted from the remote host to the router.
<b>Allow traffic IPIP → LAN</b>	Move the switch to the right to allow IPIP tunnel users access devices in the remote local subnet.
<b>Static route settings</b>	
<b>Remote IPIP interface subnet</b>	The subnet and mask of the remote IPIP interface.
<b>Remote LAN IP addresses</b>	
<b>Remote subnet</b>	To specify the IP address and mask of the remote local subnet, click the <b>ADD SUBNET</b> button, and in the line displayed, enter the needed value.  To remove a subnet, click the <b>Delete</b> icon (✕) in the corresponding line.

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

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

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

## PPTP/L2TP Servers

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

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

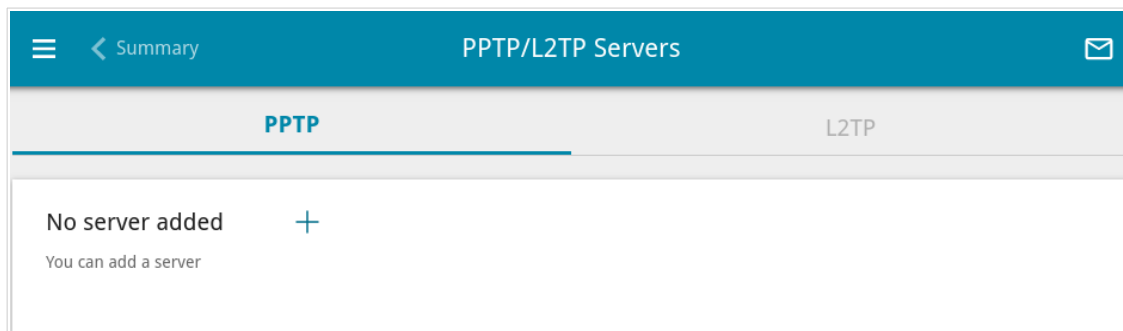


Figure 122. The **VPN / PPTP/L2TP Servers** page.

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



Before creating a PPTP or L2TP server with authentication enabled, it is required to create user accounts (see the *VPN Users* section, page 161).

Figure 123. The page for adding a PPTP server.

You can specify the following parameters:

Parameter	Description
<b>PPTP Server / L2TP Server</b>	
<b>Enable</b>	Move the switch to the right to enable the server. Move the switch to the left to disable the server.
<b>Name</b>	A name of the server for easier identification. You can specify any name.

Parameter	Description
<b>VPN network</b>	
<b>Server local IP address</b>	The IP address of the VPN server.
<b>Start client IP</b>	The start IP address of the address range for VPN server's clients.
<b>End client IP</b>	The end IP address of the address range for VPN server's clients.
<b>Interface</b>	Select a WAN connection through which this VPN server will be available. If the <b>Default gateway</b> value is selected, the router uses the default WAN connection.
<b>Access policies and NAT</b>	
<b>VPN ↔ LAN</b>	<p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>: VPN server's clients can access the router's local network; clients from the router's local network can access the VPN server's network.</li> <li>• <b>Deny</b>: VPN server's clients cannot access the router's local network; clients from the router's local network cannot access the VPN server's network.</li> </ul>
<b>VPN ↔ WAN</b>	<p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>: VPN server's clients can access the external network; clients from the external network can access the VPN server's network.</li> <li>• <b>Deny</b>: VPN server's clients cannot access the external network; clients from the external network cannot access the VPN server's network.</li> </ul>
<b>VPN → Router</b>	<p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>: VPN server's clients can access the router.</li> <li>• <b>Deny</b>: VPN server's clients cannot access the router.</li> </ul>
<b>NAT VPN → WAN</b>	If the switch is moved to the right, the network address translation function between the VPN server's interface and the external network interface is enabled.
<b>NAT VPN → LAN</b>	If the switch is moved to the right, the network address translation function between the VPN server's interface and the local network interface is enabled.

Parameter	Description
<b>Authentication</b>	
<b>Enable authentication</b>	Move the switch to the right to enable authentication. Upon that the <b>Multiple sessions</b> , <b>CHAP</b> , <b>MSCHAP</b> , <b>MSCHAPv2</b> , and <b>PAP</b> lists are displayed on the page.
<b>Multiple sessions</b>	<p>The mode of connection for the users listed in the <b>Users List</b> section. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>: Several users with the same user account are allowed to connect.</li> <li>• <b>Only new connections</b>: If there are several users with the same user account, only new users are allowed to connect.</li> <li>• <b>Only old connections</b>: If there are several users with the same user account, new users are not allowed to connect.</li> </ul>
<b>CHAP</b> <b>MSCHAP</b> <b>MSCHAPv2</b> <b>PAP</b>	<p><i>Challenge Handshake Authentication Protocol.</i> <i>Microsoft Challenge Handshake Authentication Protocol.</i> <i>Password Authentication Protocol.</i></p> <p>Select the needed action from the drop-down list for the relevant protocol.</p> <ul style="list-style-type: none"> <li>• <b>Auto</b>: Enable automatic client authentication over this protocol.</li> <li>• <b>Refuse</b>: Disable client authentication over this protocol.</li> <li>• <b>Require</b>: Require client authentication over this protocol.</li> </ul>
<b>MPPE</b>	
<b>Enable MPPE</b>	<p>Move the switch to the right to enable MPPE encryption.</p> <p>MPPE encryption can be applied only if the <b>Require</b> value is selected from the <b>MSCHAP</b> or <b>MSCHAPv2</b> drop-down list.</p>
<b>MPPE40</b> <b>MPPE128</b>	<p>MPPE encryption with a 40-bit or 128-bit key is applied. Select the needed action from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Auto</b>: Allow clients to connect to the VPN server automatically with MPPE encryption.</li> <li>• <b>Refuse</b>: Restrict clients from connecting to the VPN server with MPPE encryption.</li> <li>• <b>Require</b>: Allow clients to connect to the VPN server only with MPPE encryption.</li> </ul>

Parameter	Description
<b>Advanced Settings</b>	
<b>Maximum number of connections</b>	Available for a PPTP server. The maximum number of devices allowed to connect to the PPTP server.
<b>Port</b>	Available for an L2TP server. The port of L2TP server. By default, the value <b>1701</b> is specified.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on this VPN server debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list in the settings of the corresponding event log in the <b>Logging</b> section (see the <b>Logging</b> section, page 297).
<b>DNS</b>	
<b>Obtain DNS server addresses automatically</b>	Move the switch to the right to let VPN server's clients obtain DNS server addresses of the WAN connection which is selected from the <b>Interface</b> list. Upon that the <b>Primary DNS</b> and <b>Secondary DNS</b> fields are not available for editing.
<b>Primary DNS / Secondary DNS</b>	Enter addresses of the primary and secondary DNS servers in the relevant fields.

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

Figure 124. A window for adding a user.


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

Parameter	Description
<b>User</b>	Select a user account to allow access.

Parameter	Description
<b>Set IP address</b>	<p>The mode of IP address assignment. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Auto</b>: The IP address is assigned to the user automatically.</li> <li>• <b>Single IP</b>: The IP address is assigned to the user manually. When this value is selected, the <b>IP address</b> field is displayed.</li> </ul>
<b>IP address</b>	Specify an IP address from the range specified in the <b>Start client IP</b> and <b>End client IP</b> fields.


Click the **SAVE** button.

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

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

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

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

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



# VPN Users

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

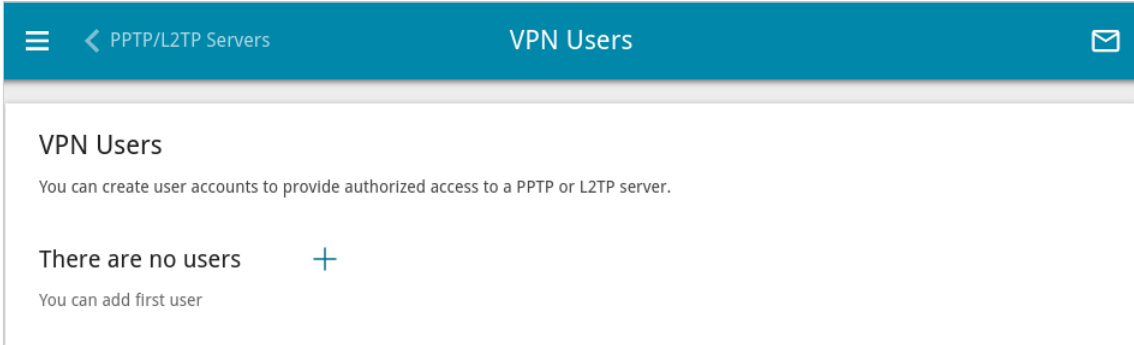




Figure 125. The **VPN / VPN Users** page.

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

The modal window is titled 'User' with a close button (X) in the top right corner. It contains two input fields: 'Username\*' and 'Password\*'. The 'Password\*' field has a 'Show' icon (an eye) to its right. At the bottom of the modal is a 'SAVE' button.


Figure 126. The window for adding a user.

In the opened window, in the **Username** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.<sup>12</sup> Click the **Show** icon (  ) to display the entered key.

Click the **SAVE** button.

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

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

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

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

# EoGRE

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

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

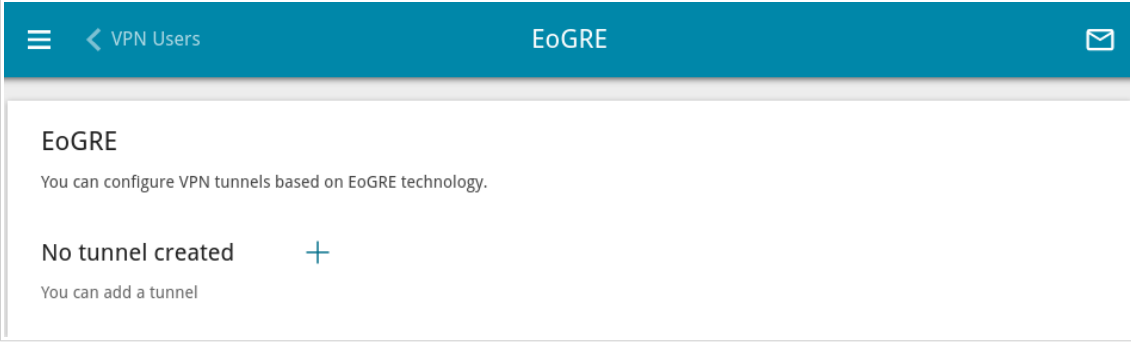


Figure 127. The **VPN / EoGRE** page.

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

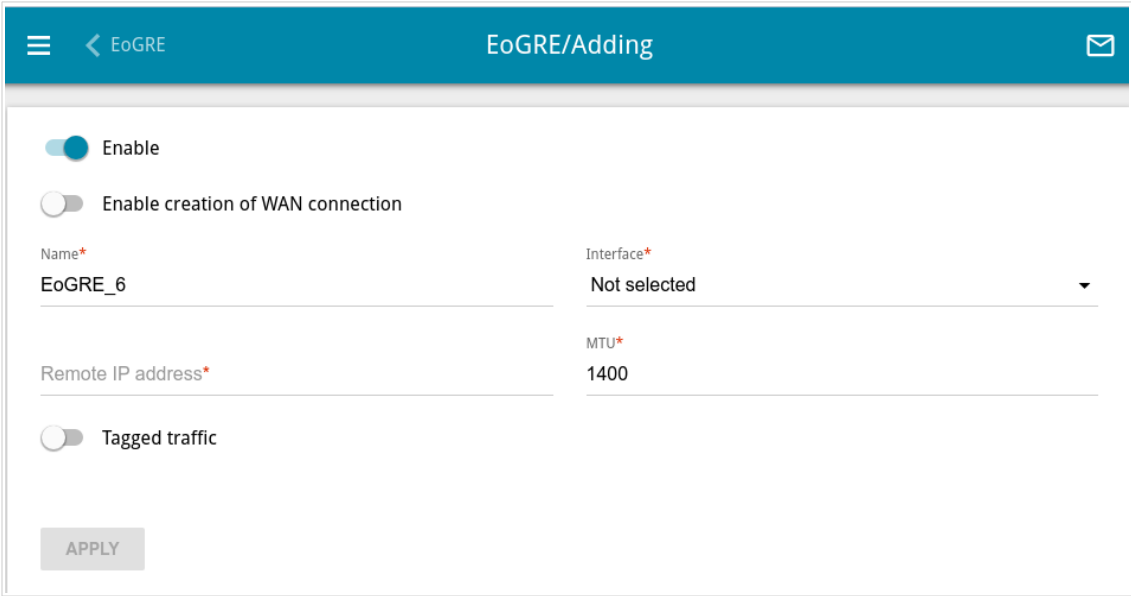


Figure 128. The page for adding an EoGRE tunnel.


You can specify the following parameters:

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

Parameter	Description
<b>Enable creation of WAN connection</b>	Move the switch to the right to use the EoGRE tunnel as an interface for creating a WAN connection. For further configuration, you need to create a VLAN which will include the EoGRE interface (see the <i>VLAN</i> section, page 222), and then create a WAN connection which will be assigned to the interface of this VLAN (see the <i>WAN</i> section, page 84). Move the switch to the left if creating a WAN connection is not required.
<b>Name</b>	A name of the tunnel for easier identification. You can specify any name.
<b>Remote IP address</b>	The IP address of the remote local subnet.
<b>Tagged traffic</b>	Move the switch to the right to assign a tag (VLAN ID) to EoGRE traffic and specify the needed value in the <b>VLAN ID</b> field displayed.
<b>Interface</b>	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the <b>Default gateway</b> value to use the default WAN connection.
<b>MTU</b>	The maximum size of units transmitted by the interface.

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

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

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

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

## EoIP

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

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

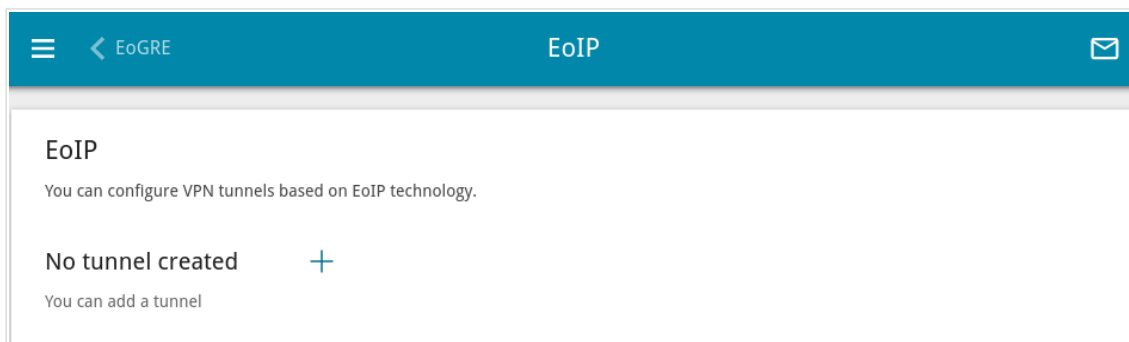


Figure 129. The **VPN / EoIP** page.

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

The screenshot shows the 'EoIP/Adding' configuration page. The header bar is blue with a menu icon, a back arrow labeled 'EoIP', the title 'EoIP/Adding', and an envelope icon. The main content area has a white background. It starts with two toggle switches: 'Enable' (turned on) and 'Enable creation of WAN connection' (turned off). Below these are two columns of fields. The left column has 'Name\*' with the value 'EoIP\_39', 'Remote IP address\*', 'Tunnel ID\*', and 'MAC address'. The right column has 'Interface\*' with a dropdown menu showing 'Not selected', 'MTU\*' with the value '1400', and a 'Keep Alive' toggle switch (turned off). At the bottom left, there is an 'APPLY' button.

Figure 130. The page for adding an EoIP tunnel.


You can specify the following parameters:

Parameter	Description
<b>Enable</b>	Move the switch to the right to enable the EoIP tunnel. Move the switch to the left to disable the EoIP tunnel.
<b>Enable creation of WAN connection</b>	Move the switch to the right to use the EoIP tunnel as an interface for creating a WAN connection. For further configuration, you need to create a VLAN which will include the EoIP interface (see the <i>VLAN</i> section, page 222), and then create a WAN connection which will be assigned to the interface of this VLAN (see the <i>WAN</i> section, page 84). Move the switch to the left if creating a WAN connection is not required.
<b>Name</b>	A name of the tunnel for easier identification. You can specify any name.
<b>Remote IP address</b>	Enter the IP address of the remote local subnet.
<b>Tunnel ID</b>	Specify a unique identifier of the tunnel. The value for both parties which establish the tunnel should be the same.
<b>MAC address</b>	A MAC address assigned to the EoIP tunnel interface. <i>Optional</i> . If the field is blank, the MAC address is assigned automatically.
<b>Tagged traffic</b>	Move the switch to the right to assign a tag (VLAN ID) to EoIP traffic and specify the needed value in the <b>Tag ID</b> field displayed.
<b>Interface</b>	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the <b>Default gateway</b> value to use the default WAN connection.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>Keep Alive</b>	Move the switch to the right to let the router detect the state of the tunnel on the other end. In the <b>Interval</b> and <b>Attempts</b> fields displayed, specify the required values. The router sends several check requests. If after several failed attempts the connection on the other end of the tunnel is inactive, the tunnel will be disabled. Upon that it will be enabled automatically when the other end tries to establish the connection.
<b>Interval</b>	A time period (in seconds) allocated for one request to check the state of the tunnel on the other end. By default, the value <b>5</b> is specified.

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

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

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

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

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

# Wi-Fi

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

## Basic Settings

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

Summary

Basic Settings

2.4 GHz

5 GHz

Basic Settings

You can change basic parameters for the wireless interface of the device.

Enable Wireless

Country

RUSSIAN FEDERATION

Wireless mode

802.11 B/G/N mixed

Select channel automatically

The least loaded data transfer channel will be used

Enable additional channels

Attention! The device automatically selects a channel from the list of available channels depending on your country. Make sure that your wireless devices support channels above 12

Channel

auto (channel 13)

Enable periodic scanning

The device will periodically check the channels load and switch to the least loaded one

Scanning period (in seconds)

0

Wi-Fi Network

Network name (SSID)\*

DIR-XXX

Hide SSID

Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point

BSSID

aa:cb:dd:20:a3:00

Max associated clients\*

0

Enable shaping

Shaping (Mbit/s)

0

Broadcast wireless network

Allows you to enable/disable broadcast of this SSID without disconnecting the wireless module of the router. Can be used with the mode "Wi-Fi Client"

Clients isolation


Figure 131. Basic settings of the wireless LAN in the 2.4GHz band.

Page 167 of 323

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

Parameter	Description
<b>Enable Wireless</b>	<p>To enable Wi-Fi connection, move the switch to the right.</p> <p>To disable Wi-Fi connection, move the switch to the left.</p> <p>To enable/disable Wi-Fi connection on a schedule, click the <b>Set schedule</b> icon (🕒). In the opened window, from the <b>Rule</b> drop-down list, select the <b>Create rule</b> value to create a new schedule (see the <i>Schedule</i> section, page 292) or select the <b>Select an existing one</b> value to use the existing one. Existing schedules are displayed in the <b>Rule name</b> drop-down list.</p> <p>To enable Wi-Fi connection at the time specified in the schedule and disable it at the other time, select the <b>Enable wireless connection</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button.</p> <p>To disable Wi-Fi connection at the time specified in the schedule and enable it at the other time, select the <b>Disable wireless connection</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button.</p> <p>To change or delete the schedule, click the <b>Edit schedule</b> icon (🕒). In the opened window, change the parameters and click the <b>SAVE</b> button or click the <b>DELETE FROM SCHEDULE</b> button.</p>
<b>Country</b>	The country you are in. Select a value from the drop-down list.
<b>Wireless mode</b>	Operating mode of the wireless network of the router. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
<b>Select channel automatically</b>	Move the switch to the right to let the router itself choose the channel with the least interference.
<b>Enable additional channels</b>	If the switch is moved to the left, the device automatically selects one of available standard channels. To use additional channels (the 12th and 13th – in the 2.4 GHz band, the 100th and higher – in the 5 GHz band), move the switch to the right.



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

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

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

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

Basic Settings

Add Wi-Fi Network

Wi-Fi Network

Network name (SSID)\*  
DIR-XXX.2

Hide SSID

Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point

Max associated clients\*  
0

Enable shaping

Shaping (Mbit/s)  
0

Broadcast wireless network

Allows you to enable/disable broadcast of this SSID without disconnecting the wireless module of the router. Can be used with the mode "Wi-Fi Client"

Clients isolation

Block traffic between devices connected to the access point

Enable guest network

Enable the guest network in order to isolate Wi-Fi clients from the LAN network

APPLY

Security Settings

Network authentication  
WPA2-PSK

Password PSK\*  
.....

Password should be between 8 and 63 ASCII characters

Encryption type\*  
AES

Group key update interval (in seconds)\*  
3600

Figure 132. Creating a wireless network.

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

Parameter	Description
<b>Broadcast wireless network</b>	<p>If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DIR-853 can connect to another access point as a wireless client.</p> <p>To enable/disable broadcasting on a schedule, click the <b>Set schedule</b> icon (🕒). In the opened window, from the <b>Rule</b> drop-down list, select the <b>Create rule</b> value to create a new schedule (see the <i>Schedule</i> section, page 292) or select the <b>Select an existing one</b> value to use the existing one. Existing schedules are displayed in the <b>Rule name</b> drop-down list.</p> <p>To enable broadcasting at the time specified in the schedule and disable it at the other time, select the <b>Enable wireless network broadcasting</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button. When the wireless connection is disabled, the device will not be able to enable broadcasting of this wireless network on schedule.</p> <p>To disable broadcasting at the time specified in the schedule and enable it at the other time, select the <b>Disable wireless network broadcasting</b> value from the <b>Action</b> drop-down list and click the <b>SAVE</b> button.</p> <p>To change or delete the schedule, click the <b>Edit schedule</b> icon (🕒). In the opened window, change the parameters and click the <b>SAVE</b> button or click the <b>DELETE FROM SCHEDULE</b> button.</p> <p>If you created an additional network, you can configure, change or delete a schedule for each network. To do this, click the icon in the line of the network.</p>
<b>Clients isolation</b>	<p>Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.</p>
<b>Enable guest network</b>	<p>This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.</p>

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

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

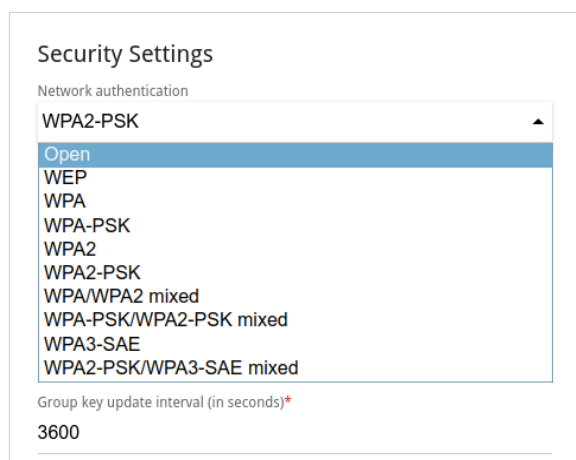


Figure 133. Network authentication types supported by the router.

The router supports the following authentication types:

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

Authentication type	Description
<b>WPA2-PSK/WPA3-SAE mixed</b>	A mixed type of authentication. When this value is selected, devices using the <b>WPA2-PSK</b> authentication type and devices using the <b>WPA3-SAE</b> authentication type can connect to the wireless network.



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

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

Figure 134. The **Open** value is selected from the **Network authentication** drop-down list.

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

When the **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK mixed**, **WPA3-SAE**, or **WPA2-PSK/WPA3-SAE 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 a 'Password PSK\*' field with a masked password '.....' and a 'Show' icon (🔍). A note indicates 'Password should be between 8 and 63 ASCII characters'. Under 'Encryption type\*', 'AES' is selected from a dropdown menu. At the bottom, 'Group key update interval (in seconds)\*' is set to '3600'.

Figure 135. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.

Parameter	Description
<b>Password PSK</b>	A password for WPA encryption. The password can contain digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout. <sup>13</sup> Click the <b>Show</b> icon (🔍) to display the entered password.
<b>Encryption type</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> . <i><b>TKIP</b> and <b>TKIP+AES</b> encryption types are not available for <b>WPA3-SAE</b> and <b>WPA2-PSK/WPA3-SAE mixed</b> authentication types.</i>

<sup>13</sup> 0-9, A-Z, a-z, space, !"#%&'()\*+,-./:;<=>?@[^\_`{|}~.

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

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

Security Settings

Network authentication  
WPA2

☐ WPA2 Pre-authentication

IP address RADIUS server\*

RADIUS server port\*  
1812

RADIUS encryption key\*

Encryption type\*  
AES

Group key update interval (in seconds)\*  
3600


Figure 136. The **WPA2** value is selected from the **Network authentication** drop-down list.

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

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



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

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

## Client Management

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

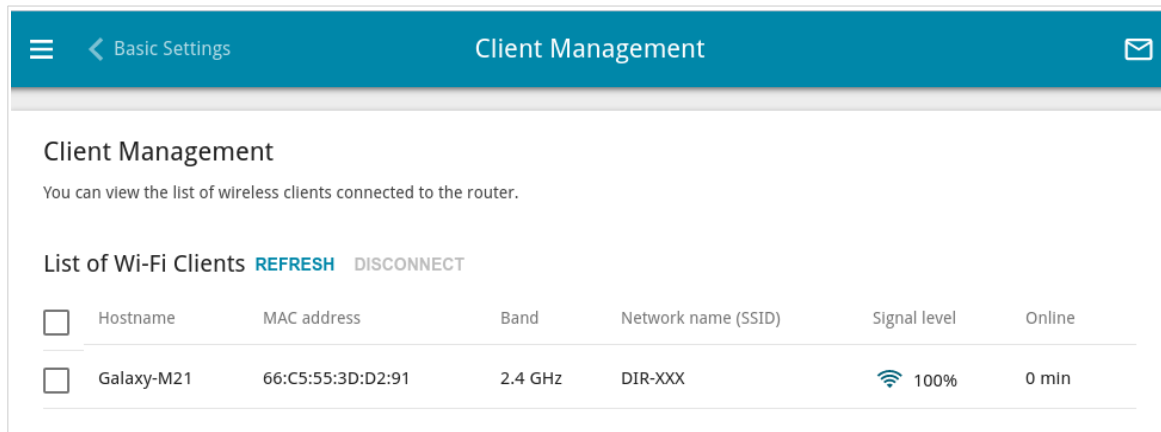


Figure 137. The page for managing the wireless clients.

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.

WPS	
The WPS function helps to automatically connect to the wireless network of the router. The connecting devices must support this function.	
<a href="#">DISABLE WPS</a>	
<b>WPS Control</b>	<b>Information</b>
<b>ESTABLISH CONNECTION</b>	Default PIN code: 12345670
<input checked="" type="checkbox"/> Enable WPS function with hardware button	Network name (SSID): DIR-XXX
<small>Move the switch to the left in order to forbid enabling the WPS function with the relevant hardware button</small>	Network authentication: WPA2-PSK
	Encryption: AES
	Password PSK: 12345670
<b>UPDATE</b>	

Figure 138. The page for configuring the WPS function.

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

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

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

To activate the WPS function via the web-based interface, on the tab of the relevant band, click the **ENABLE WPS** button.

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

Parameter	Description
<b>Default PIN code</b>	The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function.
<b>Network name (SSID)</b>	The name of the router's wireless network.
<b>Network authentication</b>	The network authentication type specified for the wireless network.
<b>Encryption</b>	The encryption type specified for the wireless network.
<b>Password PSK</b>	The encryption password specified for the wireless network.
<b>UPDATE</b>	Click the button to update the data on the page.

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

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

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

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

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

## ***Using WPS Function without Web-based Interface***

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

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

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

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

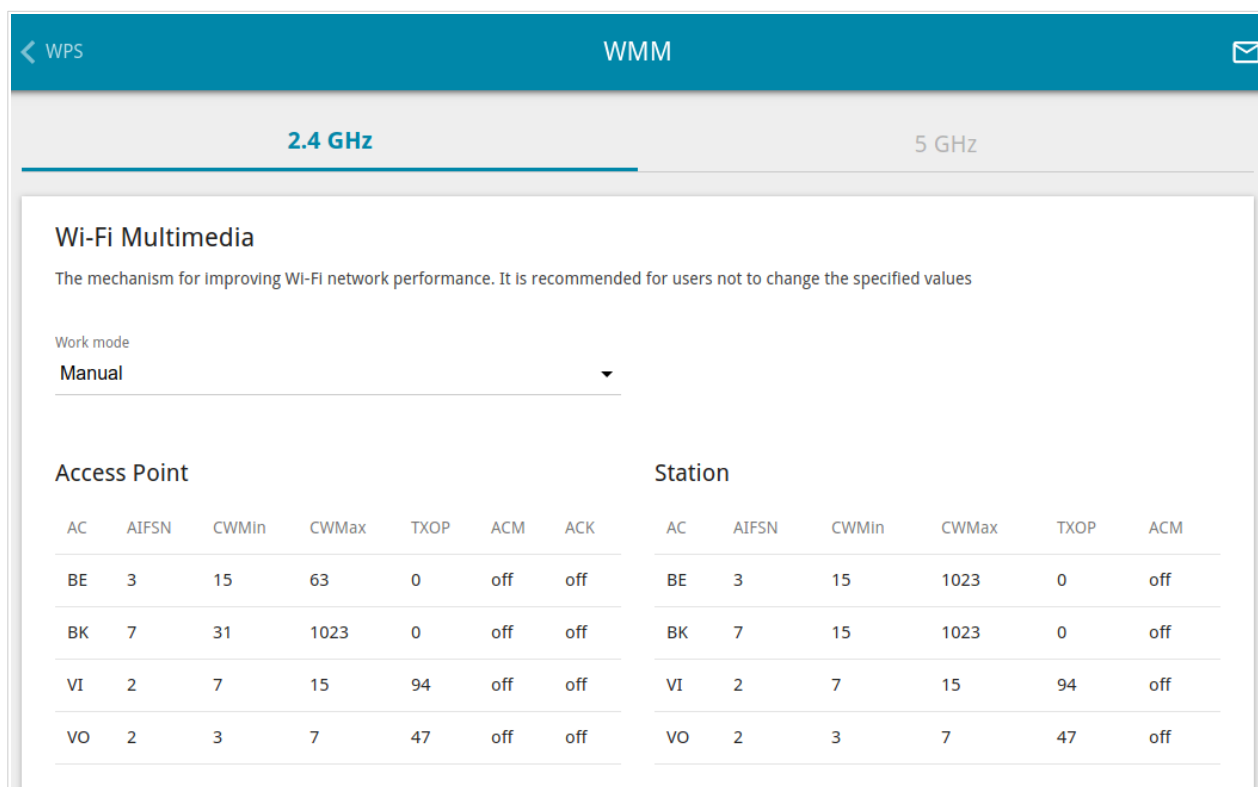
## WMM

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

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

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

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



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

Figure 139. The page for configuring the WMM function.

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

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

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

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

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

Figure 140. The window for changing parameters of the WMM function.

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



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

Click the **SAVE** button.

## Client

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

**Client**

**2.4GHz** 5GHz

**Wi-Fi Client**

You can configure the router as a client to connect to a wireless access point or to a WISP.

☒ Enable

☒ Broadcast wireless network 2.4 GHz

ⓘ If the broadcast 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

Select network from list

**APPLY**

**Wireless Networks** [UPDATE LIST](#)

Network name (SSID)	Security Settings	RSSI	Channel
[SDK2] DIR-825-799C-799B	[WPA2-PSK] [AES]	-79dBm	13
[SDK2] DWR-956-0002-0001	[WPA2-PSK] [AES]	-79dBm	6

Figure 141. The page for configuring the client mode.

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

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

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

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

To connect to a hidden network, select the **Connect to hidden network** value from the **Connecting to network** drop-down list. Enter the name of the network in the **Network name (SSID)** field. If needed, fill in the **BSSID** field. Then select the needed type of authentication from the **Network authentication** drop-down list.

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

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

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

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

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

When connecting to a wireless access point, the wireless channel of DIR-853 will switch to the channel of the access point to which you have connected.

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

If you want to connect to the WISP network, after configuring the device as a client, you need to create a WAN connection with relevant parameters for the **WiFiClient\_2GHz** interface in the 2.4GHz band or for the **WiFiClient\_5GHz** interface in the 5GHz band.

## Additional

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



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

The screenshot shows the 'Additional' settings page for the 2.4 GHz band. The page is titled 'Wi-Fi Additional Settings' and includes a description: 'You can define additional parameters for the WLAN of the router.' The settings are organized into two columns. The left column includes 'Bandwidth' (set to 'Auto'), 'TX power (in percent)' (set to '100'), 'Preamble\*' (set to 'Auto'), 'Drop multicast' (disabled), 'Enable TX Beamforming' (enabled), 'STBC' (enabled), and 'Enable 802.11k' (disabled). The right column includes 'B/G protection' (set to 'Auto'), 'Short GI' (set to 'Enable'), 'Beacon period (in milliseconds)\*' (set to '100'), 'RTS threshold (in bytes)\*' (set to '2347'), 'Frag threshold (in bytes)\*' (set to '2346'), 'DTIM period (in beacon frames)\*' (set to '1'), and 'Station Keep Alive (in seconds)\*' (set to '0'). An 'APPLY' button is located at the bottom left of the settings area.

Figure 142. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
<b>Bandwidth</b>	The channel bandwidth for devices operating on modern standards. When the <b>Auto</b> value is selected, router automatically chooses the most suitable channel bandwidth for these clients.
<b>Autonegotiation 20/40 (Coexistence)</b>	<i>Available on the <b>2.4 GHz</b> tab.</i> Move the switch to the right to let the router to automatically choose the most suitable channel bandwidth (20MHz or 40MHz) for the connected devices (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the <b>20/40 MHz</b> or <b>Auto</b> value is selected from the <b>Bandwidth</b> drop-down list.
<b>TX power</b>	The transmit power (in percentage terms) of the router.
<b>Preamble</b>	This parameter defines the length of the CRC block sent by the router when communicating to wireless devices. Select the needed value from the drop-down list. <ul style="list-style-type: none"> <li>• <b>Auto</b>: The length of the block is defined automatically.</li> <li>• <b>Long</b>: The long block.</li> <li>• <b>Short</b>: The short block (this value is recommended for networks with high-volume traffic).</li> </ul>
<b>Enable DFS</b>	<i>Available on the <b>5 GHz</b> tab.</i> Move the switch to the right to enable the DFS ( <i>Dynamic Frequency Selection</i> ) mechanism. Upon that the router uses the channels at which radars and other mobile or stationary radio systems can operate, but switches to other channels if these devices require this. In order to use the DFS mechanism, the automatic channel selection should be enabled (on the <b>Wi-Fi / Basic Settings</b> page). Move the switch to the left not to let the router use the channels at which radars and other mobile or stationary radio systems can operate.
<b>Drop multicast</b>	Move the switch to the right to disable multicasting for the router's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected on the <b>Advanced / IGMP/MLD</b> page. If the switch is moved to the right, the device will not be available by the domain name for Wi-Fi clients.

Parameter	Description
<b>Enable TX Beamforming</b>	<p>TX Beamforming is the signal processing/directing technique which helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation.</p> <p>Move the switch to the right to improve the signal quality.</p>
<b>STBC</b>	<p>The STBC (<i>Space-time block coding</i>) technique allows increasing data transfer reliability even for portable devices equipped with poor antennas (smartphones, pads, etc.) due to using several data streams and processing several versions or received data.</p> <p>Move the switch to the right if you need to use the STBC technique.</p>
<b>Enable 802.11k</b>	<p>802.11k standard allows faster roaming of clients between access points within the same network. Clients supporting 802.11k standard can request a list of neighbor access points with their signal levels and Wi-Fi channel numbers. The device does not need to probe all of the available channels, but selects an access point to roam to from the list.</p> <p>Move the switch to the right if you need to use 802.11k standard.</p>
<b>Enable 802.11v</b>	<p>802.11v roaming allows improving the wireless client load balancing.</p> <p>If the wireless access point supports 802.11v standard, then with a large number of devices connected to this point, a request may be sent to some clients to switch to a less loaded point with the same network parameters or to transfer from a loaded band to a freer band (in case the SSID and security settings are the same in both frequency bands) to improve operation of each client. The request is advisory, upon that the device does not forcibly disconnect clients.</p> <p>Move the switch to the right if you need to use 802.11v standard.</p> <p>The switch is displayed if the <b>Enable 802.11k</b> switch is moved to the right.</p>

Parameter	Description
<b>B/G protection</b>	<p>Available on the <b>2.4 GHz</b> tab.</p> <p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Auto:</b> The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices).</li> <li>• <b>Always On:</b> The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</li> <li>• <b>Always Off:</b> The protection function is always disabled.</li> </ul>
<b>Short GI</b>	<p>Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices.</p> <ul style="list-style-type: none"> <li>• <b>Enable:</b> The router uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n and 802.11ac standards (see the value of the <b>Wireless mode</b> drop-down list on the <b>Wi-Fi / Basic Settings</b> page).</li> <li>• <b>Disable:</b> The router uses the 800 ns standard guard interval.</li> </ul>
<b>Beacon period</b>	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
<b>RTS threshold</b>	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
<b>Frag threshold</b>	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).
<b>DTIM period</b>	The number of beacon frames between sending DTIM messages (messages notifying on broadcast or multicast transmission).
<b>Station Keep Alive</b>	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value <b>0</b> is specified, the checking is disabled.

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-853.

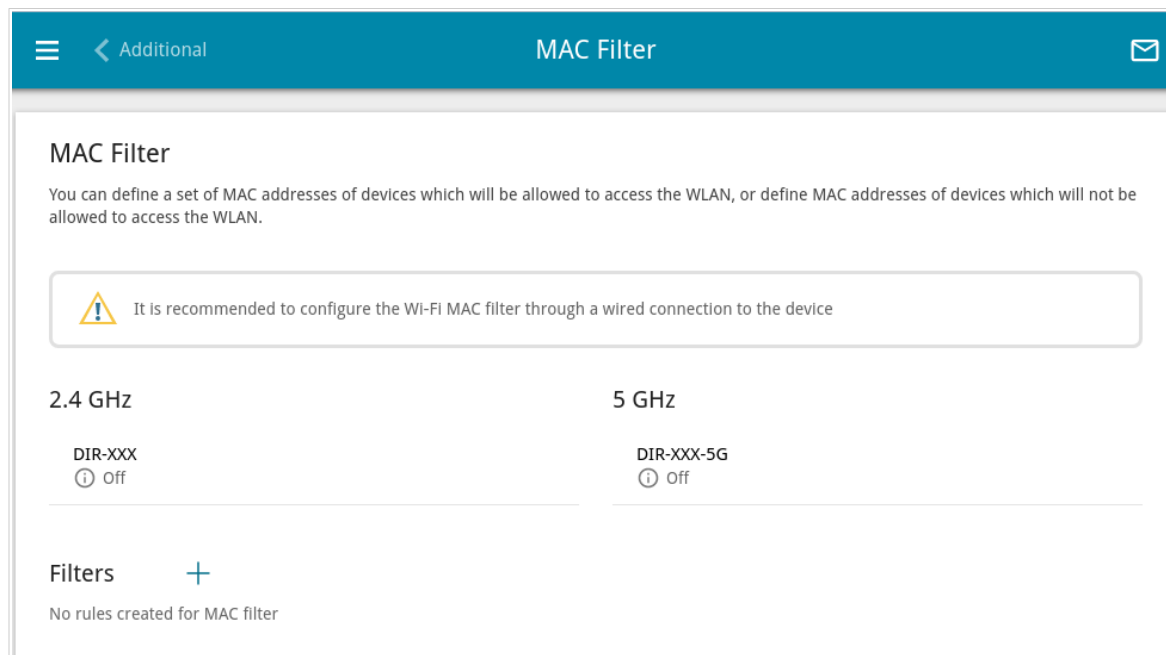


Figure 143. The page for configuring the MAC filter for the wireless network.

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 144. The window for adding a rule for the MAC filter.

You can specify the following parameters:

Parameter	Description
<b>Frequency band</b>	From the drop-down list, select a band of the wireless network.
<b>SSID</b>	A wireless network to which the rule will be applied. Select the needed value from the drop-down list.
<b>MAC address</b>	In the field, enter the MAC address to which the selected filtering mode will be applied.
<b>Name</b>	The name of the device for easier identification. You can specify any name.
<b>Enable</b>	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.

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

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

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

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

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

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

To set a schedule for the MAC filter rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 292) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

## Roaming

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

MAC FilterSmart Adjustment

### Smart Adjustment of Wi-Fi Clients

Smart adjustment of Wi-Fi clients 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.  
For proper operation of the function, it is recommended to specify the same parameters of the WLAN (SSID, authentication type, and password) for all devices.

**DISABLE**

Port\*  
7890

☐ Use multicast for service data exchange  
Select the checkbox if APs are located in different subnets

#### 2.4 GHz

Maximum time of storing data (in seconds)\*  
60

Maximum time of storing data on adjacent clients

Minimum level of connection quality (in percent)\*  
60

Dead zone (from -50% to 50%)\*  
15

Threshold value of connection quality (in percent)\*  
40

#### 5 GHz

Maximum time of storing data (in seconds)\*  
60

Maximum time of storing data on adjacent clients

Minimum level of connection quality (in percent)\*  
60

Dead zone (from -50% to 50%)\*  
15

Threshold value of connection quality (in percent)\*  
40

APPLY

Figure 145. 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
<b>Port</b>	The number of the port used for data exchange between access points (routers).
<b>Use multicast for service data exchange</b>	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 <b>Multicast TTL</b> and <b>Multicast group address</b> fields are displayed on the page.  If the switch is moved to the left, broadcast traffic is used for service data exchange.
<b>Multicast TTL</b>	Specify the TTL ( <i>Time to live</i> ) parameter value.
<b>Multicast group address</b>	Specify the address of the multicast group (from the subnet 239.255.0.0/16).
<b>2.4 GHz / 5 GHz</b>	
<b>Maximum time of storing data</b>	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.
<b>Minimum level of connection quality</b>	The signal strength upon which the access point (router) starts scanning other devices in order to find a device with a higher signal level.
<b>Dead zone</b>	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 <b>Minimum level of connection quality</b> field value and the <b>Dead zone</b> field value, then the client disconnects from the access point (router). You can specify the values from <b>-50%</b> to <b>+50%</b> .
<b>Threshold value of connection quality</b>	The signal strength upon which the access point (router) disconnects the client from its wireless network regardless of the signal levels of other devices. This value should not be greater than the value specified in the field <b>Minimum level of connection quality</b> .

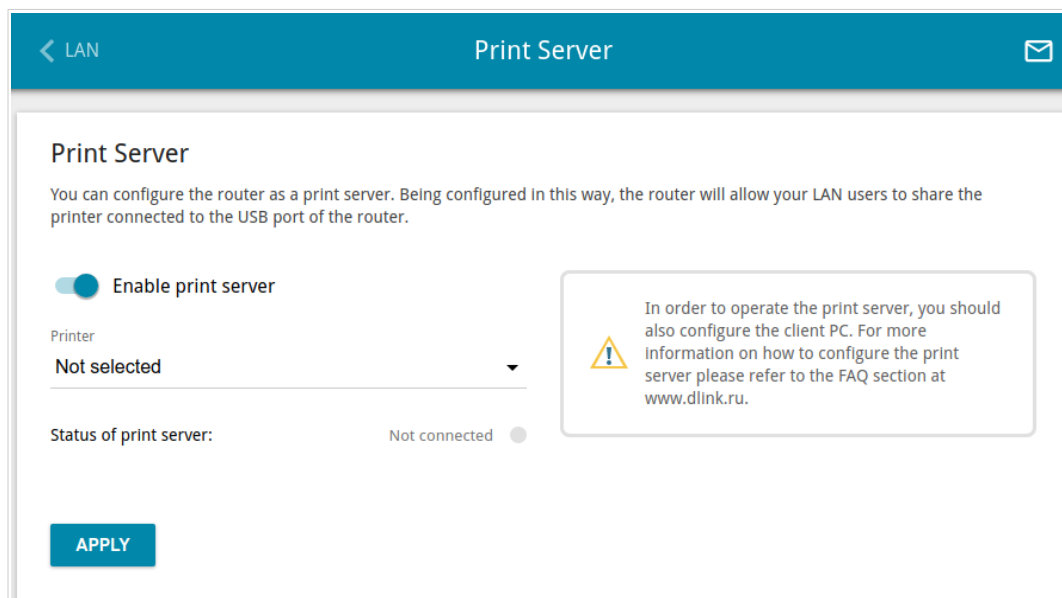
After specifying the needed parameters, click the **APPLY** button.

To disable the function of smart adjustment of Wi-Fi clients, click the **DISABLE** button.

## Print Server

On the **Print Server** page, you can configure the router as a print server. Being configured in this way, the router will allow your LAN users to share the printer connected to the USB port of the router.

To connect a printer to the router, power off both devices. Connect the printer to the USB port of the router, power on the printer, then power on the router.



The screenshot shows the 'Print Server' configuration page. At the top, there is a blue header bar with a back arrow and 'LAN' on the left, 'Print Server' in the center, and an envelope icon on the right. Below the header, the page title 'Print Server' is followed by a descriptive paragraph: 'You can configure the router as a print server. Being configured in this way, the router will allow your LAN users to share the printer connected to the USB port of the router.' There is a toggle switch for 'Enable print server' which is currently turned on. Below this is a 'Printer' dropdown menu showing 'Not selected'. To the right of these controls is a yellow warning box with an exclamation mark icon and text: 'In order to operate the print server, you should also configure the client PC. For more information on how to configure the print server please refer to the FAQ section at [www.dlink.ru](http://www.dlink.ru).' Below the printer selection, the 'Status of print server:' is shown as 'Not connected' with a grey circle indicator. At the bottom left is a blue 'APPLY' button.

Figure 146. The **Print Server** page.

To configure the router as a print server, move the **Enable print server** switch to the right. Make sure that the printer connected to the router is selected from the **Printer** drop-down list. Click the **APPLY** button. The status of the connected device will be displayed in the **Status of print server** field.

If you don't want to use the router as a print server, move the **Enable print server** switch to the left and click the **APPLY** button.

## USB Storage

This menu is designed to operate USB storages. Here you can do the following:

- view data on the connected USB storage
- create accounts for users to allow access to the content of the USB storage
- enable the built-in Samba server of the router
- enable the built-in FTP server of the router
- view content of the connected USB storage
- enable the built-in DLNA server of the router
- configure the built-in Transmission torrent client and manage distributing and downloading processes
- enable the XUPNPD plug-in.

## Information

On the **USB Storage / Information** page, you can view data on the USB storage connected to the router.

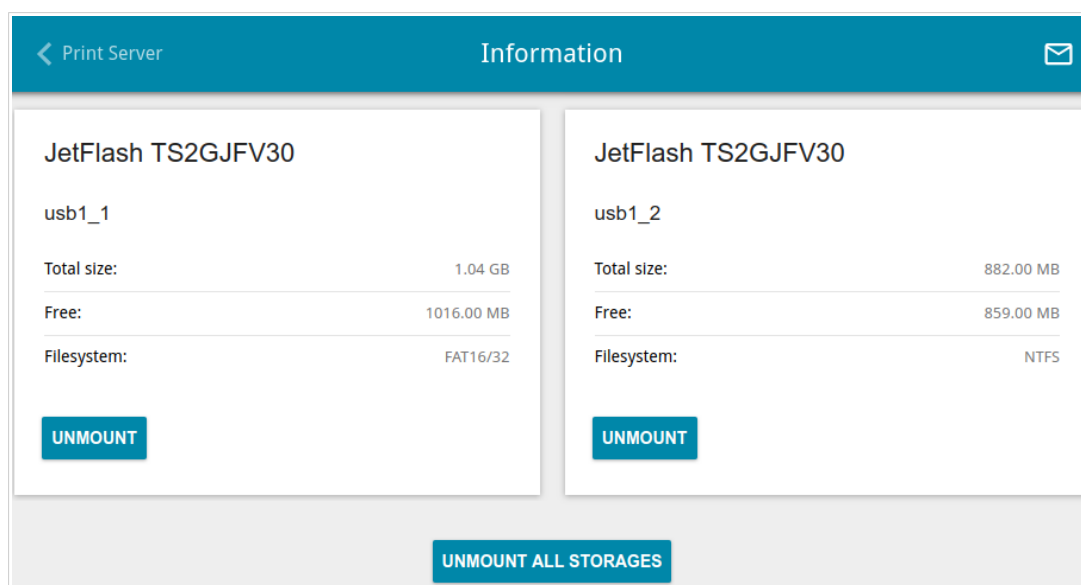


Figure 147. The **USB Storage / Information** page.

The following data are presented on the page: the name, total and free space of the storage, and the type of its file system (supported file systems: FAT16/32, exFAT, NTFS, ext2/3/4).

If the USB storage is divided into volumes, a section for every volume (partition) of the USB storage is displayed on the page.

To safely disconnect the USB storage or a volume of the USB storage, click the **UNMOUNT** button in the relevant section and wait for several seconds.

To disconnect all volumes of the USB storage, click the **UNMOUNT ALL STORAGES** button.

## USB Users

On the **USB Storage / USB Users** page, you can create user accounts to provide access to data on the USB storage connected to the router.

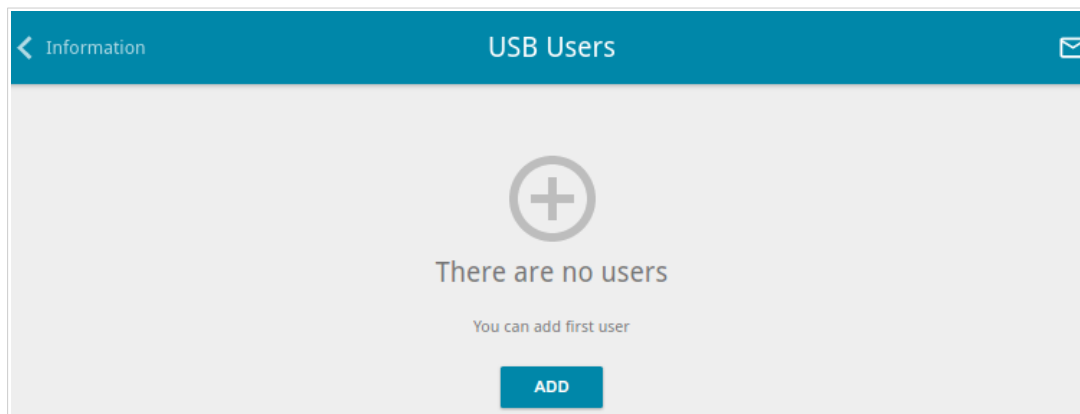



Figure 148. The **USB Storage / USB Users** page.

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

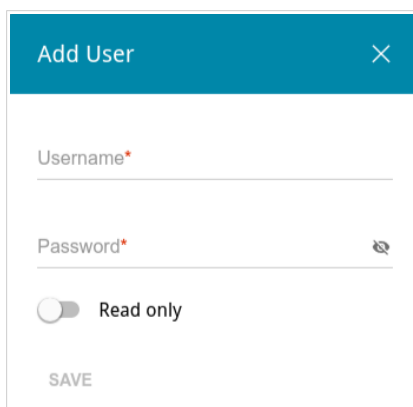


Figure 149. The window for adding a user.

In the opened window, in the **Username** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.<sup>14</sup>




Some reserved words (e.g., **root**, **admin**, **nobody**, etc.) cannot be usernames.

Move the **Read only** switch to the right not to let the user create, change, or delete files.

Click the **SAVE** button.

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

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

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

<sup>14</sup> 0-9, A-Z, a-z, space, !"#%&'()\*+,-./:;<=>?@[\\]^\_`{|}~.



## Samba

On the **USB Storage / Samba** page, you can enable the built-in Samba server of the router to provide access to the USB storage for users of your LAN.

The screenshot shows the 'Samba' configuration page. At the top, there is a blue header bar with a menu icon, a back arrow labeled 'USB Users', the title 'Samba', and an envelope icon. Below the header, the page content is as follows:

- Samba**  
On this page you can enable the built-in Samba server of the router to provide access to the USB storage for users of your LAN.
- Enable Samba server**: A toggle switch that is currently turned on (blue).
- Configuring a Samba Server**
  - Anonymous login**: A toggle switch that is currently turned on (blue).
  - i** If anonymous login is disabled, to access the USB storage content it will be needed to create users
  - Work group**: A text field containing 'WORKGROUP'.
  - Short description**: A text field containing 'D-LINK SERVER'.
  - NetBIOS**: A text field containing 'D-LINK'.
- Directories**: A section with a '+' icon and a trash icon. It contains a table with two columns: 'Name' and 'Path'.
- APPLY**: A blue button at the bottom left.

Figure 150. The **USB Storage / Samba** page.

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

The **Anonymous login** switch (by default, the switch is moved to the right) allows anonymous access to the content of the USB storage for users of your LAN.

If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

In the **Work group** field, leave the value specified by default (**WORKGROUP**) or specify a new name of a workgroup which participants will have access to the content of the USB storage.

In the **Short description** field, you can specify an additional description for the USB storage. This value will be displayed in some operating systems. Use digits and/or Latin characters.

In the **NetBIOS** field, specify a name of the USB storage which will be displayed for users of your LAN. Use digits and/or Latin characters.

To allow access only to a certain folder of the USB storage, click the **ADD** (+) button in the **Directories** section.

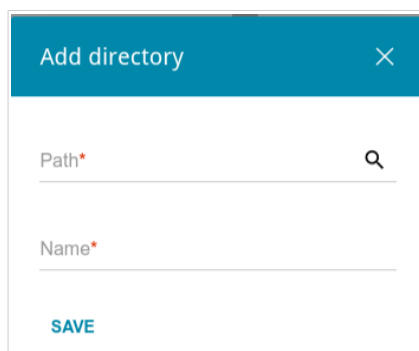


Figure 151. Specifying a folder.

In the opened window, locate a folder containing files. To do this, click the **Search** icon (🔍) in the **Path** field. Then go to the needed folder and click the **SELECT** button.

In the **Name** field, specify a name of the selected folder which will be displayed for users of your LAN. Use digits and/or Latin characters.

Click the **SAVE** button.

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

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

To disable the built-in Samba server of the router, move the **Enable Samba server** switch to the left and click the **APPLY** button.

## FTP

On the **USB Storage / FTP** page, you can enable the built-in FTP server of the router to provide access to the USB storage for users of your LAN.

FTP

You can enable the built-in FTP server of the router to provide access to the USB storage for users of your LAN.

☒ Enable FTP server

(i) For correct display of containing Cyrillic letters file names, please use UTF-8 encoding on the FTP client

Configuring FTP Server

☐ Anonymous login

(i) If anonymous login is disabled, to access the USB storage content it will be needed to create users

(i) When anonymous access is used, all users connected via the FTP server have read-only access rights

Port  
21

Directory

TLS  
Enabled

The use of TLS may reduce the data transfer rate.

APPLY

Figure 152. The **USB Storage / FTP** page.

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

Move the **Anonymous login** switch to the right to allow anonymous access to the content of the USB storage for users of your LAN. If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

If needed, change the router's port used by the FTP server in the **Port** field (by default, the standard port **21** is specified).

To allow access only to a certain folder of the USB storage for users of your LAN, locate a folder containing files. To do this, click the **Search** icon ( ) in the **Directory** field. Then go to the needed folder and click the **SELECT** button.

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

To allow access to all the content of the USB storage for users of your LAN again, remove the value specified in the **Directory** field and click the **APPLY** button.

By default, the TLS (*Transport Layer Security*) encryption protocol is enabled for the FTP server of the router. To change TLS usage parameters, select the required value from the **TLS** drop-down list:

- **Enabled**: When this value is selected, any type of connection to the server is allowed.
- **Disabled**: When this value is selected, attempts to connect via TLS will be rejected.
- **For control connection**: When this value is selected, TLS is required for the control connection, while data can be transferred without encryption.
- **For control connection and data**: When this value is selected, TLS is required both for the control connection and for data transfer.

To disable the built-in FTP server of the router, move the **Enable FTP server** switch to the left and click the **APPLY** button.

## Filebrowser

On the **USB Storage / Filebrowser** page, you can view the content of your USB storage connected to the router and remove separate folders and files from the USB storage.

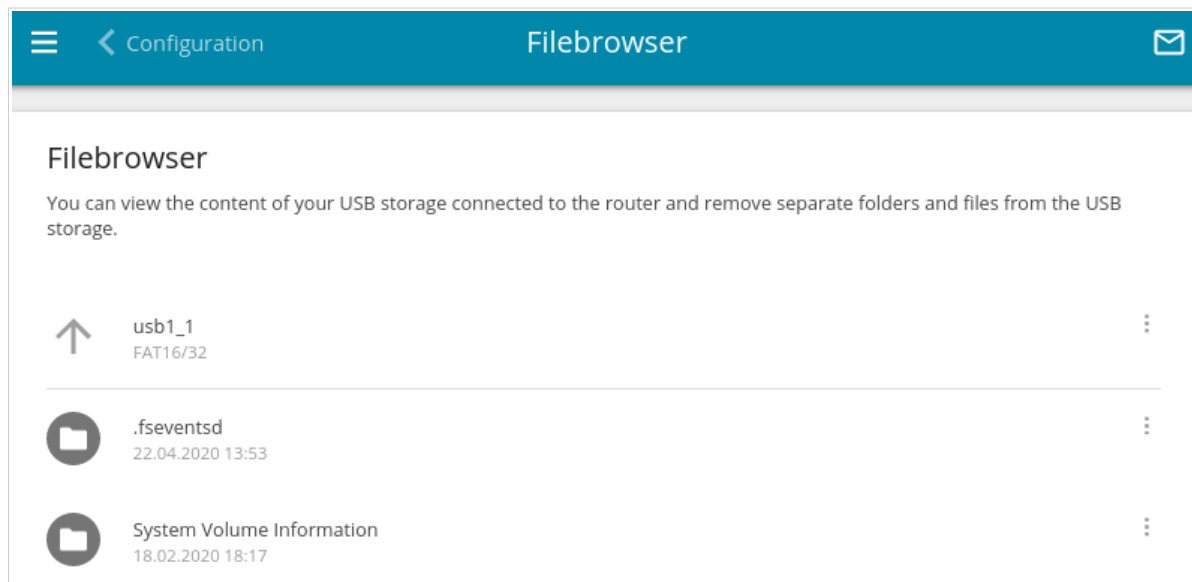




Figure 153. The **USB Storage / Filebrowser** page.

To view the content of the USB storage, click the icon of the storage or storage partition. The list of folders and files will be displayed on the page.

To go to a folder, click the line corresponding to this folder.

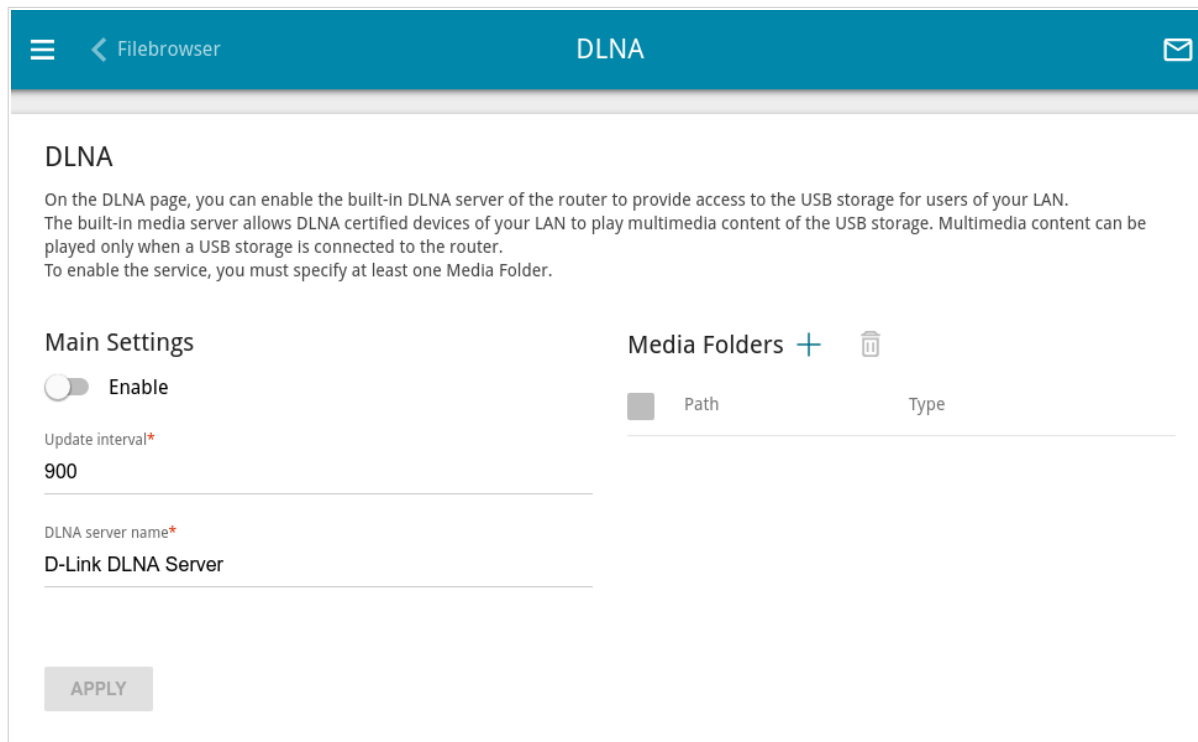
To refresh the folder contents, click the **Actions** icon (  ) in the line corresponding to this folder and select the **Refresh** value.

To remove a folder or file, click the **Actions** icon (  ) in the line corresponding to this folder or file and select the **Delete** value.

## DLNA

On the **USB Storage / DLNA** page, you can enable the built-in DLNA server of the router to provide access to the USB storage for users of your LAN.

The built-in media server allows DLNA certified devices of your LAN to play multimedia content of the USB storage. Multimedia content can be played only when a USB storage is connected to the router.



The screenshot shows the 'DLNA' configuration page. At the top, there is a blue header bar with a menu icon, a back arrow labeled 'Filebrowser', the title 'DLNA', and an envelope icon. Below the header, the page has a light gray background. The main content area is titled 'DLNA' and contains a descriptive paragraph: 'On the DLNA page, you can enable the built-in DLNA server of the router to provide access to the USB storage for users of your LAN. The built-in media server allows DLNA certified devices of your LAN to play multimedia content of the USB storage. Multimedia content can be played only when a USB storage is connected to the router. To enable the service, you must specify at least one Media Folder.' Below this, there are two sections. The 'Main Settings' section on the left includes an 'Enable' toggle switch (currently off), an 'Update interval\*' field with the value '900', and a 'DLNA server name\*' field with the value 'D-Link DLNA Server'. An 'APPLY' button is at the bottom left. The 'Media Folders' section on the right has a '+ ' icon and a trash icon. It contains a table with two columns: 'Path' and 'Type'. The table is currently empty.

Figure 154. The **USB Storage / DLNA** page.

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

In the **Update interval** field, specify the time period (in seconds), at the end of which the media server updates the file list of the USB storage, or leave the value specified by default (**900**).

In the **DLNA server name** field, specify a name of the DLNA server which will be displayed for users of your LAN or leave the value specified by default (**D-Link DLNA Server**). Use digits and/or Latin characters.

To allow access to the content of the USB storage for users of your LAN, click the **ADD (+)** button in the **Media Folders** section.

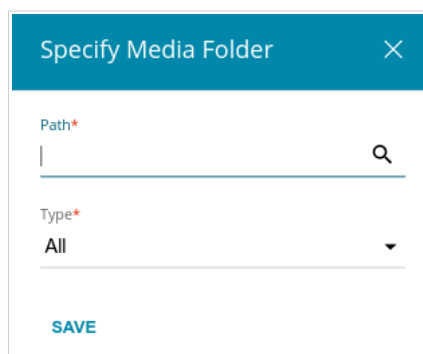

A dialog box titled "Specify Media Folder" with a close button (X) in the top right corner. It contains two fields: "Path\*" with a search icon (magnifying glass) on the right, and "Type\*" with a dropdown menu currently showing "All". At the bottom is a blue "SAVE" button.

Figure 155. Specifying a media folder.

In the opened window, locate a folder containing files. To do this, click the **Search** icon (  ) in the **Path** field. Then go to the needed folder and click the **SELECT** button.

For each folder you can define the type of files which will be available for users of your LAN. To do this, select the needed type of files from the **Type** drop-down list. To share all files of a folder, select the **All** value from the **Type** drop-down list.

Click the **SAVE** button.

To remove a folder from the list in the **Media Folders** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** (  ) button.

After specifying all needed settings on the **USB Storage / DLNA** page, click the **APPLY** button.

To disable the built-in DLNA server of the router, move the **Enable** switch to the left and click the **APPLY** button.

## Torrent Client


On the **USB Storage / Torrent Client** page, you can configure all needed settings for the built-in Transmission client.

Figure 156. The **USB Storage / Torrent Client** page.

You can specify the following parameters:

Parameter	Description
<b>Transmission</b>	
<b>Enable</b>	Move the switch to the right to activate the Transmission client.
<b>Main Settings</b>	
<b>Port</b>	The router's port which will be used by the Transmission client.



Parameter	Description
<b>Path</b>	Locate data of the Transmission client. To do this, click the <b>Search</b> icon (  ), select the needed value, and click the <b>SELECT</b> button.
<b>Directory</b>	The folder on the USB storage where data of the Transmission client will be stored.
<b>Enable download queue</b>	<p>Move the switch to the right if you want to limit the number of simultaneous downloads. Upon that the <b>Download queue size</b> field will be displayed.</p> <p>Move the switch to the left not to limit the number of simultaneous downloads.</p>
<b>Download queue size</b>	The maximum number of simultaneous downloads. By default, the value <b>1</b> is specified.
<b>Peer limit</b>	The maximum number of the service users from which you can download files.
<b>Enable download speed limit</b>	<p>Move the switch to the right to limit the maximum file download speed. In the <b>Download speed limit</b> field displayed, specify the maximum value of speed (KBps).</p> <p>Move the switch to the left not to limit the maximum download speed.</p>
<b>Use uTP</b>	<p>Move the switch to the right to enable <math>\mu</math>TP (<i>Micro Transport Protocol, a transport protocol for file sharing</i>). Such a setting can increase the load on the router.</p> <p>Move the switch to the left to disable <math>\mu</math>TP.</p>
<b>Web-based interface port</b>	The port on which the web-based interface of the Transmission client is available.
<b>Authorization</b>	
<b>Enable</b>	Move the switch to the right if you want the Transmission client to request for username and password when accessing its web-based interface. Then fill in the <b>Username</b> and <b>Password</b> fields.
<b>Username</b>	The username to access the web-based interface of the Transmission client.
<b>Password</b>	The password to access the web-based interface of the Transmission client.

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

In the **Web-based interface page** field, the address of the web-based interface of the Transmission client is displayed. To access the web-based interface of the Transmission client, click the link.

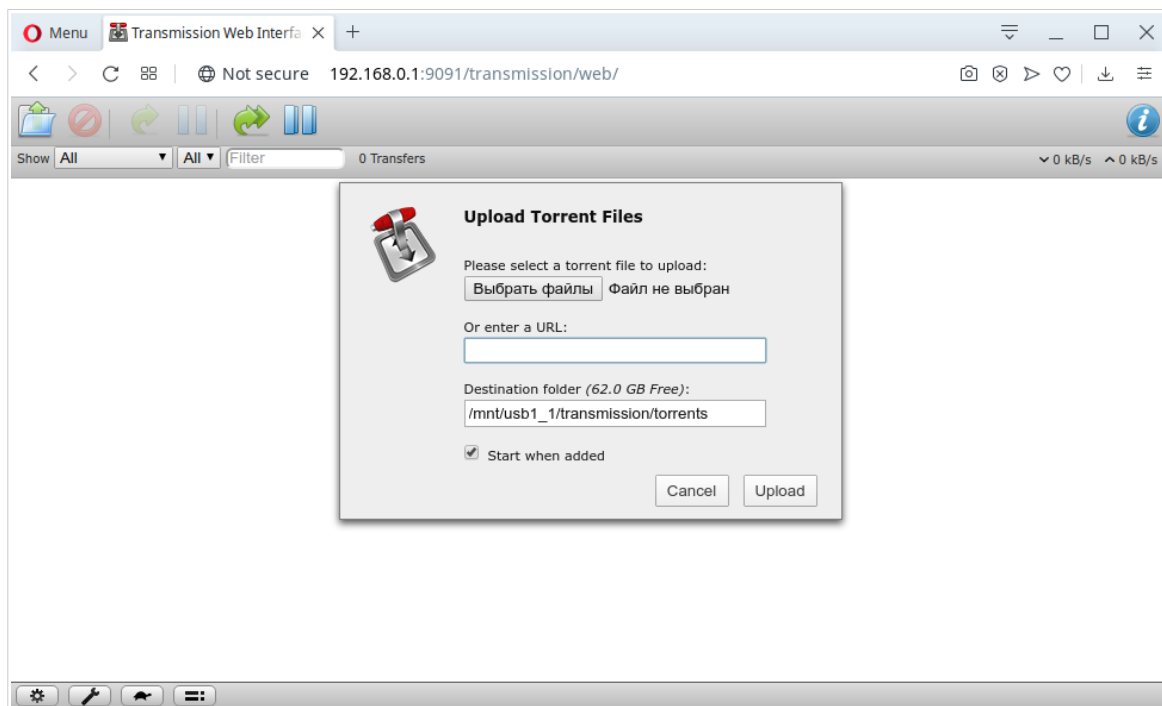









Figure 157. The web-based interface of the Transmission torrent client.

Using the web-based interface of the built-in Transmission torrent client you can manage the process of downloading files to the USB storage connected to the router.

The following buttons are available on the page:

Parameter	Description
 <b>Open Torrent</b>	Click the button to add a new torrent file (a metadata file according to which the Transmission client downloads files) to the download queue. In the dialog box appeared, select a file stored on your PC and click the <b>Upload</b> button.
 <b>Remove Selected Torrents</b>	Select the torrent file which you want to remove from the download queue and click the button.
 <b>Start Selected Torrents</b>	Select the torrent file corresponding to the download which should be restarted and click the button.
 <b>Start All Torrents</b>	Click the button to restart all downloads. If you limited the maximum number of simultaneous downloads, the Transmission client starts processing of the specified number of torrent files; after completing download of the first one, the client proceeds to the next file in the queue.

Parameter	Description
 <b>Pause Selected Torrents</b>	Select the torrent file corresponding to the download which should be stopped and click the button.
 <b>Pause All Torrents</b>	Click the button to stop all downloads.
 <b>Toggle Inspector</b>	Select a torrent file and click the button to view its data.

## XUPNPD

On the **USB Storage / XUPNPD** page, you can enable the XUPNPD plug-in. It allows to broadcast media content received from the Internet sources or IPTV service to DLNA-certified devices of your LAN.

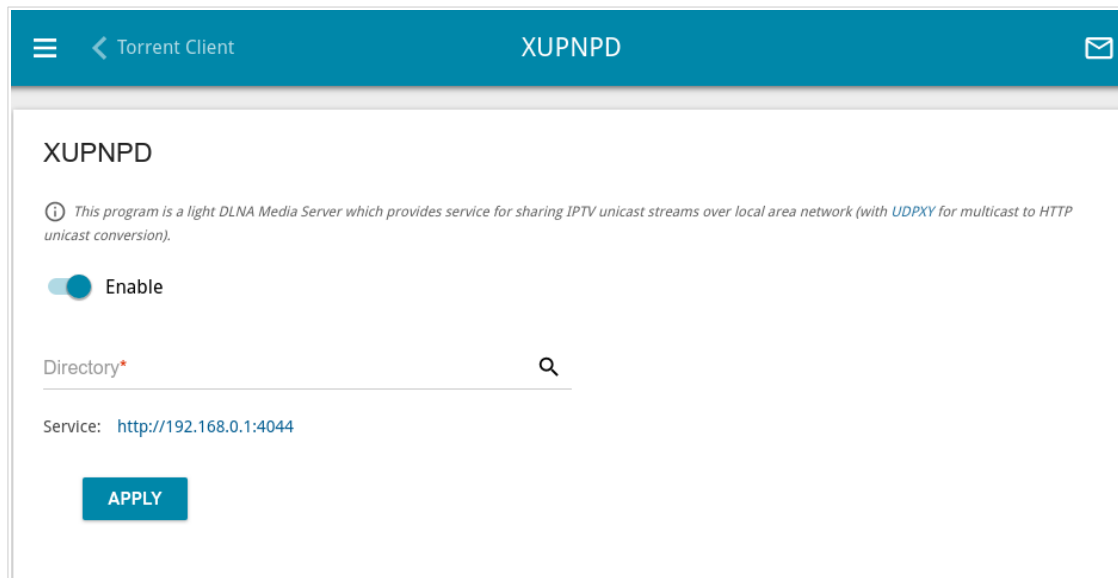



Figure 158. The **USB Storage / XUPNPD** page.

To use the XUPNPD plug-in, connect a USB storage to the router and move the **Enable** switch to the right.



To let IPTV services operate using the XUPNPD plug-in, enable the UDPXY application.

In the **Directory** field, locate a folder to which playlists added on the page of the XUPNPD plug-in will be saved. To do this, click the **Search** icon (  ), then go to the needed folder and click the **SELECT** button.

Click the **APPLY** button.

In the **Service** field, the address of the web-based interface of the XUPNPD plug-in is displayed. To access the page of the XUPNPD plug-in and configure all needed settings, click the link.

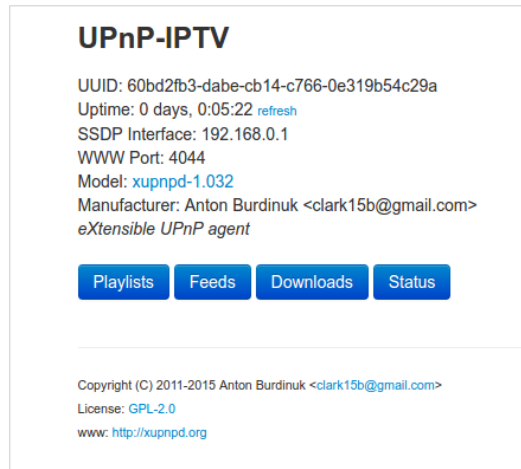


Figure 159. The XUPNPD plug-in page.

## USB Modem

This menu is designed to operate USB modems.



Some models of USB modems do not allow performing operations available in this menu section through the web-based interface of the router.

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

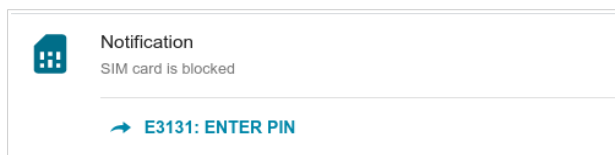


Figure 160. The notification on the PIN code check.

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

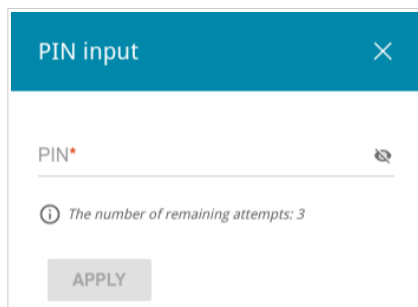


Figure 161. The window for entering the PIN code.

Some USB modems in the router mode and Android smartphones in the modem mode have an IP address from the subnet which coincides with the router's local subnet. In this case, the router's web-based interface can be unavailable. For correct operation, disconnect the device from the USB port and reboot the router. Then access the web-based interface, go to the **Connections Setup / LAN** page, and change the value of the **IP address** field on the **IPv4** tab (for example, specify the value **192.168.2.1**). Wait until the router is rebooted.

## Basic Settings

On the **USB Modem / Modem name / Basic Settings** page, you can view data on the USB modem connected to the router, change the PIN code of the SIM card inserted into your USB modem, disable or enable the check of the PIN code.

Information		Network information	
Model	E3131	Mode	3G
Vendor		RSSI	-67 dBm
IMEI	862733019089559	Signal level	74%
Interface		Operator name	"MTS RUS"
Revision	21.158.13.03.143	Roaming	Disable
Serial number	-	IMSI	250015602723576
		PIN status	Device is unlocked
		SMS	5
		<a href="#">DISABLE PIN CODE REQUEST</a> <a href="#">CHANGING PIN CODE</a> <a href="#">USSD</a>	

Figure 162. The **USB Modem / Modem name / Basic Settings** page.

If the PIN code check for the SIM card inserted into your USB modem is disabled, then an active WAN connection with default settings (for LTE modems) or the operator's settings (for GSM modems) will be automatically created when plugging the USB modem into the router. The connection will be displayed on the **Connections Setup / WAN** page.

When a USB modem is connected to the router, the following data are displayed on the page:

Parameter	Description
<b>Information</b>	
<b>Model</b>	The alphanumeric code of the model of your USB modem.
<b>Vendor</b>	The manufacturer of your USB modem.
<b>IMEI</b>	The code stored in the memory of the USB modem.
<b>Interface</b>	The network interface name.
<b>Revision</b>	The revision of the firmware of your USB modem.
<b>Serial number</b>	The unique identifier assigned to the device by its manufacturer.

Parameter	Description
<b>Network information</b>	
<b>Mode</b>	A type of the network to which the USB modem is connected.
<b>RSSI</b>	The strength of the signal received by the USB modem.
<b>Signal level</b>	The signal level at the input of the modem's receiver. The zero signal level shows that you are out of the coverage area of the selected operator's network.
<b>Operator name</b>	The name of the mobile operator proving the service.
<b>Roaming</b>	Roaming mode status of the SIM card inserted into the USB modem.
<b>IMSI</b>	The code stored in the SIM card inserted into your USB modem.
<b>PIN status</b>	PIN code request status of the SIM card inserted into the USB modem.
<b>SMS</b>	The number of text messages stored in the memory of the SIM card inserted into the USB modem. Click the number of text messages in the line to go to <b>USB Modem / Modem name / SMS</b> page.

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

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

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

To change the PIN code, click the **CHANGING PIN CODE** button (the button is displayed if the PIN code check is enabled). In the opened window, enter the current code in the **PIN code** field, then enter a new code in the **New PIN code** and **New PIN code confirmation** fields and click the **SAVE** button.



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

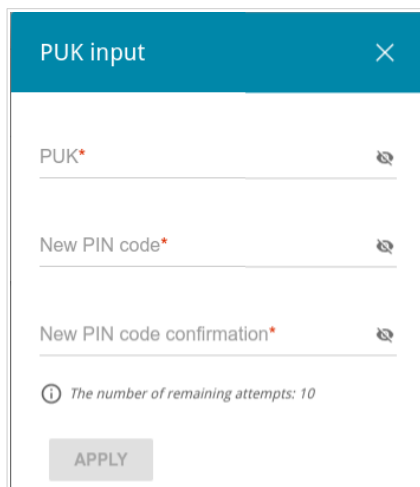
The image shows a web-based interface window titled "PUK input" with a close button (X) in the top right corner. The window contains three input fields: "PUK\*", "New PIN code\*", and "New PIN code confirmation\*", each with a "Show" icon (an eye with a slash) to its right. Below these fields is a message: "The number of remaining attempts: 10" preceded by an information icon (i). At the bottom of the window is an "APPLY" button.

Figure 163. The **USB Modem / Modem name / Basic Settings** page. The window for PUK code input.

For further use of the card, click the **PUK INPUT** button, enter the PUK code in the relevant field, and then specify a new PIN code for your SIM card in the **New PIN code** and **New PIN code confirmation** fields. Click the **Show** icon (👁) to display the entered values. Click the **APPLY** button.

Click the **USSD** button to go to the **USB Modem / Modem name / USSD** page.

## SMS

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

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

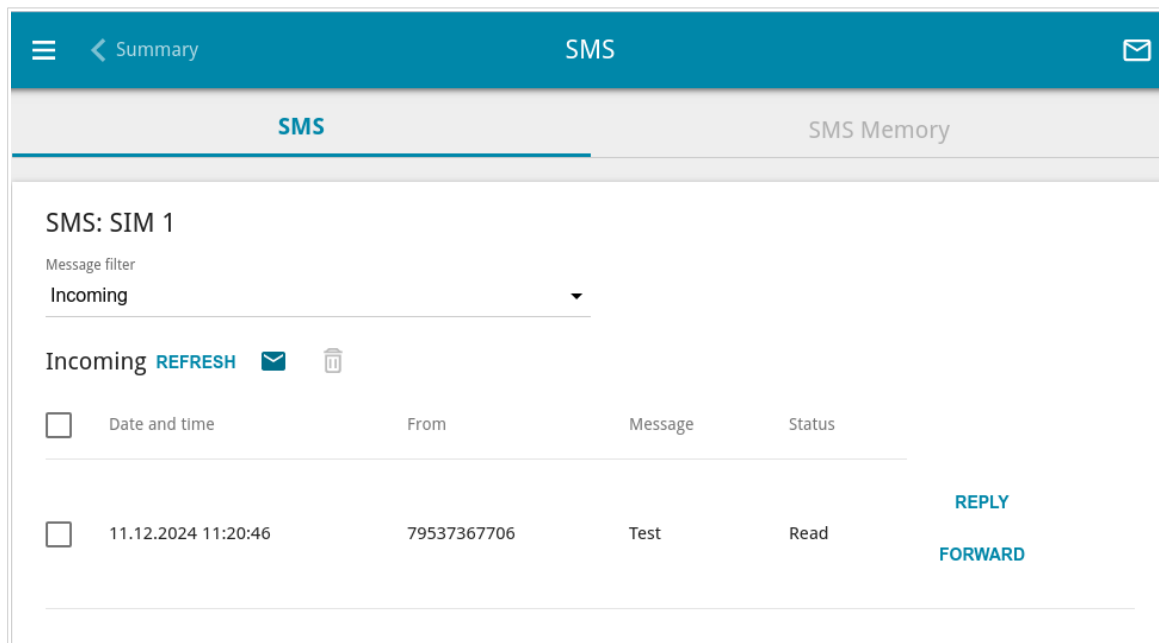



Figure 164. The **USB Modem / Modem name / SMS** page. The **SMS** tab.

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

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

To create and send a text message, click the **New message** button (.

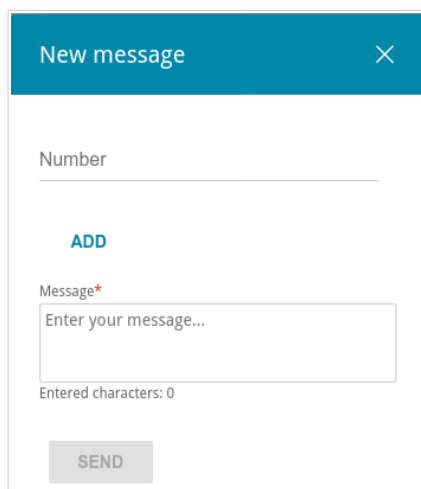

A screenshot of a 'New message' dialog box. It has a blue header bar with the text 'New message' and a close button (X). Below the header, there is a text input field labeled 'Number'. Underneath this field is a blue 'ADD' button. Below the 'ADD' button is a text input field labeled 'Message\*' with a red asterisk. Inside this field is a placeholder text 'Enter your message...'. Below the message field, it says 'Entered characters: 0'. At the bottom of the dialog is a grey 'SEND' button.

Figure 165. The window for creating a new text message.

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

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

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

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

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

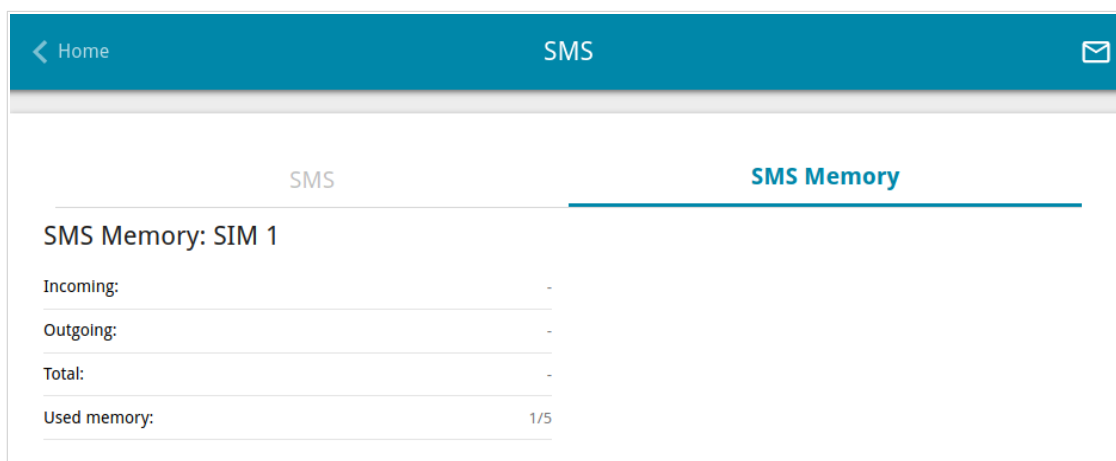
A screenshot of the 'SMS' page in a web interface. The top bar is blue with a back arrow and 'Home' on the left, 'SMS' in the center, and an envelope icon on the right. Below the bar, there are two tabs: 'SMS' and 'SMS Memory'. The 'SMS Memory' tab is selected and highlighted with a blue underline. Under the 'SMS Memory' tab, it says 'SMS Memory: SIM 1'. Below this, there is a table with four rows: 'Incoming:', 'Outgoing:', 'Total:', and 'Used memory:'. The 'Incoming:', 'Outgoing:', and 'Total:' rows have a dash '-' in the right column. The 'Used memory:' row has '1/5' in the right column.

Figure 166. The **USB Modem / Modem name / SMS** page. The **SMS Memory** tab.

## USSD

On the **USB Modem / Modem name / USSD** page, you can send a USSD command.<sup>15</sup>

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

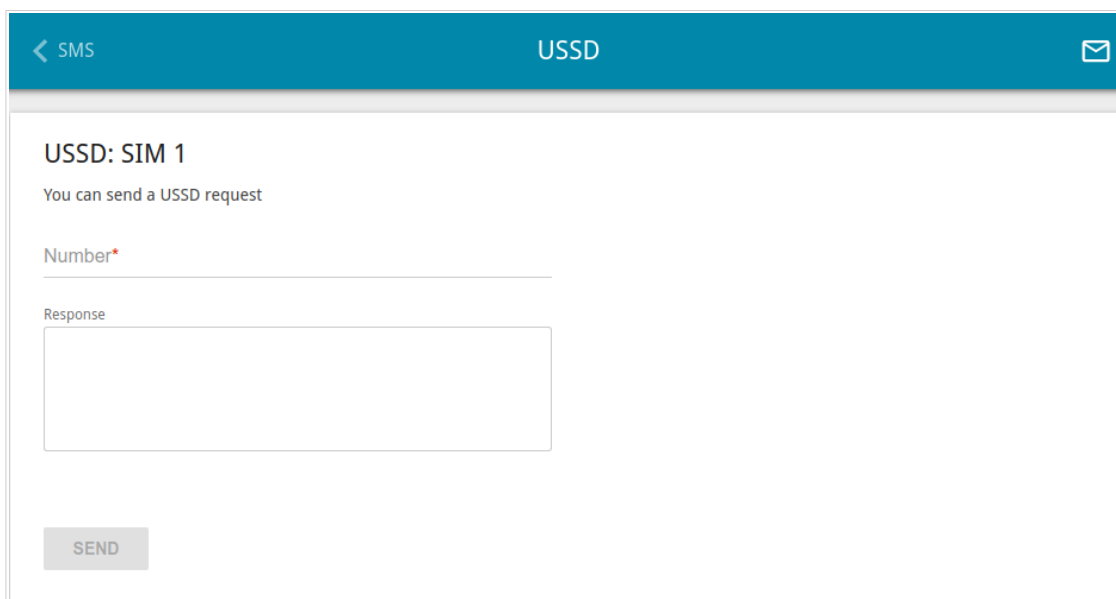
The screenshot shows a web interface for sending USSD commands. At the top, there is a blue header bar with a back arrow and 'SMS' on the left, 'USSD' in the center, and an envelope icon on the right. Below the header, the page title 'USSD: SIM 1' is displayed. Underneath, a message says 'You can send a USSD request'. There are two input fields: 'Number\*' with a red asterisk and 'Response'. A 'SEND' button is located at the bottom left of the form area.

Figure 167. The **USB Modem / Modem name / USSD** page.

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

---

<sup>15</sup> Contact your operator to get information on USSD commands and their functions.

## Advanced

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

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

## VLAN

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

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

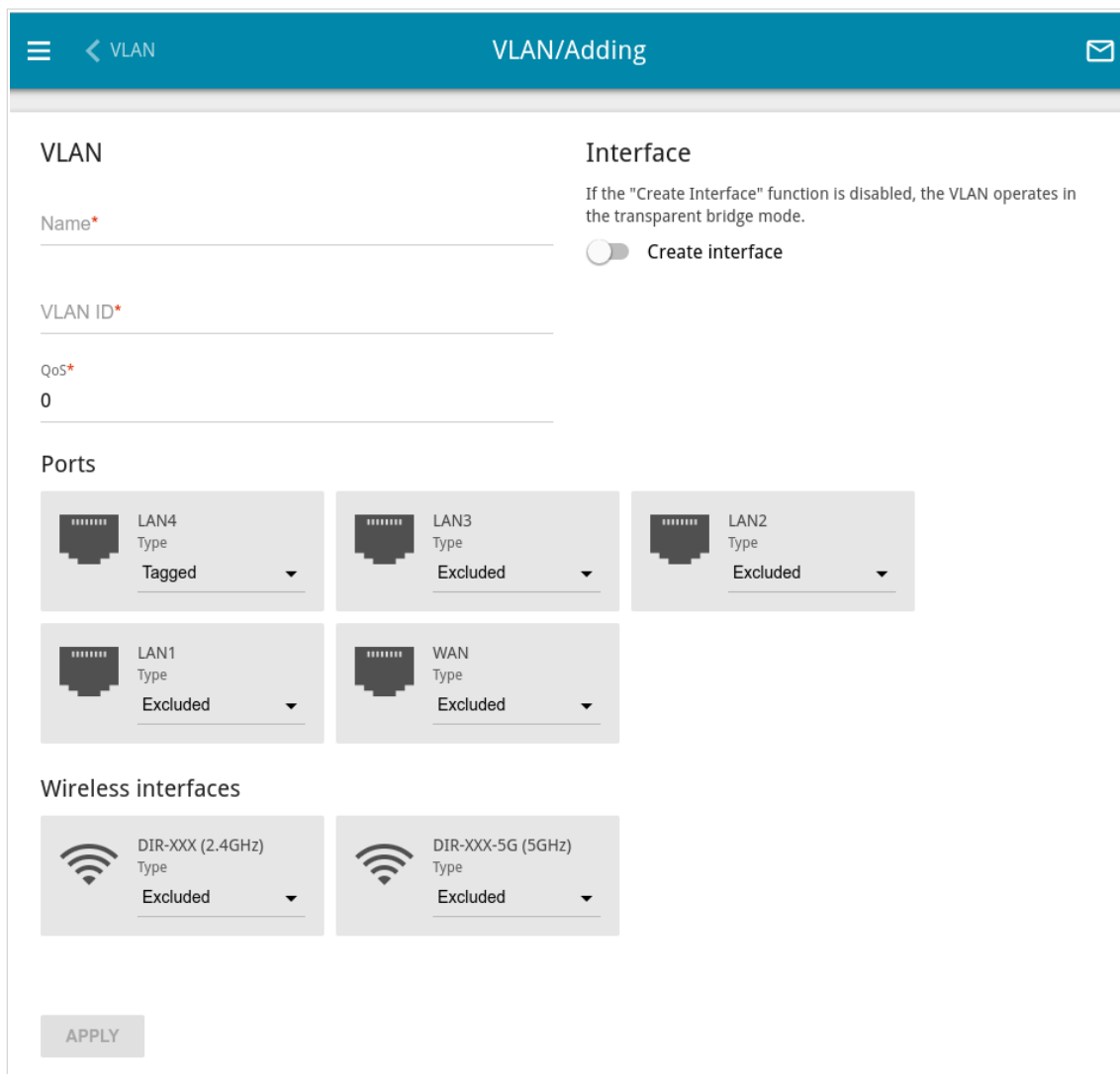
- **LAN:** For the LAN interface, it includes LAN ports and Wi-Fi networks. You cannot delete this VLAN.
- **WAN:** For the WAN interface; it includes the **WAN** port. You can edit or delete this VLAN.

VLAN ID	Name	Tagged Ports	Untagged ports
-	LAN	-	DIR-XXX (2.4GHz), DIR-XXX-5G (5GHz), LAN1, LAN2, LAN3, LAN4
-	WAN	-	WAN

Figure 168. The **Advanced / VLAN** page.

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

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



**VLAN**

Name\*

VLAN ID\*

QoS\*

0

**Interface**

If the "Create Interface" function is disabled, the VLAN operates in the transparent bridge mode.

☐ Create interface

**Ports**

LAN4  
Type  
Tagged

LAN3  
Type  
Excluded

LAN2  
Type  
Excluded

LAN1  
Type  
Excluded

WAN  
Type  
Excluded

**Wireless interfaces**

DIR-XXX (2.4GHz)  
Type  
Excluded

DIR-XXX-5G (5GHz)  
Type  
Excluded

APPLY

Figure 169. The page for adding a VLAN.


You can specify the following parameters:

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

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

Click the **APPLY** button.

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

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



## WAN Assignment

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

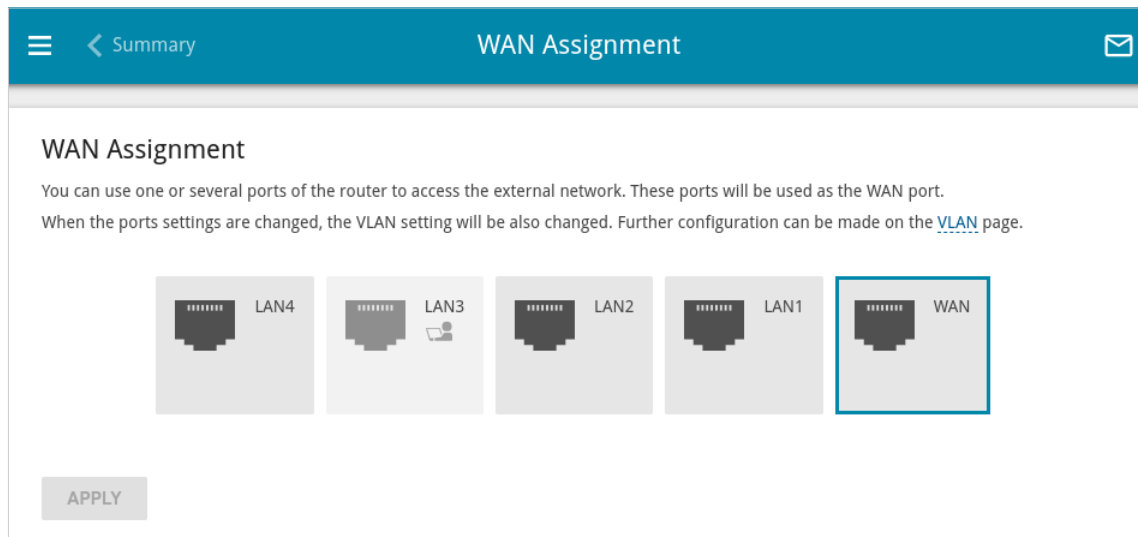


Figure 170. The **Advanced / WAN Assignment** page.

### Using LAN Ports as WAN Ports

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

1. On the **Advanced / WAN Assignment** page, select a LAN port and click the **APPLY** button.
2. In the window displayed, click the **APPLY** button to create a VLAN which will include the selected LAN port. Upon that the selected port is removed from all VLANs to which it was previously added. You can change the settings of the VLAN on the **Advanced / VLAN** page (see the *VLAN* section, page 222).
3. Go to the **Connections Setup / WAN** page and create a WAN connection which will be assigned to the network interface of the corresponding VLAN (see the *WAN* section, page 84).

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

1. Disconnect the ISP's cable from this LAN port.
2. On the **Connections Setup / WAN** page, remove the WAN connection assigned to the network interface of the VLAN which includes the corresponding LAN port (see the *WAN* section, page 84).
3. Go to the **Advanced / WAN Assignment** page, select the relevant LAN port, and click the **APPLY** button. In the window displayed, click the **APPLY** button to exclude the port from the VLAN. If the excluded port is the only one in the VLAN, the VLAN is completely removed.
4. Go to the **Advanced / VLAN** page and select the **LAN** line. On the opened page, in the **Ports** section, from the **Type** drop-down list, select the type of the element corresponding to this LAN port and click the **APPLY** button.

## Using WAN Port as LAN Port

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

1. Disconnect the ISP's cable from the WAN port.
2. On the **Connections Setup / WAN** page, remove the WAN connection assigned to the network interface of the VLAN which includes the WAN port (see the *WAN* section, page 84).
3. On the **Advanced / WAN Assignment** page, select the WAN port and click the **APPLY** button. In the window displayed, click the **APPLY** button to exclude the port from the VLAN. If the excluded port is the only one in the VLAN, the VLAN is completely removed.
4. Go to the **Advanced / VLAN** page and select the **LAN** line. On the opened page, in the **Ports** section, from the **Type** drop-down list, select the type of the element corresponding to the WAN port and click the **APPLY** button.

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

1. On the **Advanced / WAN Assignment** page, select the WAN port and click the **APPLY** button.
2. In the window displayed, click the **APPLY** button to create a VLAN which will include the WAN port. Upon that the selected port is removed from all VLANs to which it was previously added. You can change the settings of the VLAN on the **Advanced / VLAN** page (see the *VLAN* section, page 222).
3. Go to the **Connections Setup / WAN** page and create a WAN connection which will be assigned to the network interface of the VLAN (see the *WAN* section, page 84).

## SNMP

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

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

**SNMP**

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

**Configuration**

☐ Enable SNMP

Hostname  
Router

The contact information for the administrator  
Admin <root@localhost>

System location  
Test room

**Remote subnets**  
ADD

**Users** +  
There are no users

**Communities** +  
There are no communities

APPLY

Figure 171. The **Advanced / SNMP** page.

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

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

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

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

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

Figure 172. The window for adding a user.


In the opened window, specify the needed parameters:


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


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

Click the **SAVE** button.

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

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

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

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

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

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

## DNS

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

The screenshot shows the 'DNS' configuration page in a web interface. At the top, there is a blue header bar with a menu icon, a back arrow labeled 'VLAN', the title 'DNS', and an envelope icon. Below the header, the page is titled 'DNS' and contains 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 or configure the router to obtain DNS servers addresses automatically from your ISP upon installing a connection.'

The configuration is divided into two main sections: IPv4 and IPv6. Each section has a 'Manual' toggle (currently off) and a 'Default gateway' toggle (currently on). Below these, there is an 'Interface' field with the value 'statip\_81' and a lock icon.

Under the IPv4 section, there is a 'Name Servers' section with the text 'Designed to be used by the local network clients.' Below this, there are two input fields for IPv4 addresses: '1.1.1.1' and '1.0.0.1', each with a lock icon. An 'ADD SERVER' button is located below these fields.

Below the 'Name Servers' section is a 'Reserve Servers' section with the text 'Designed to be used by the router when the addresses specified manually or obtained automatically are unavailable.' This section also has input fields for IPv4 and IPv6 addresses, each with an 'ADD SERVER' button.

At the bottom of the page, there is an 'APPLY' button.

Figure 173. The **Advanced / DNS** page.

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

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



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

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

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

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

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

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

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

## DDNS

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

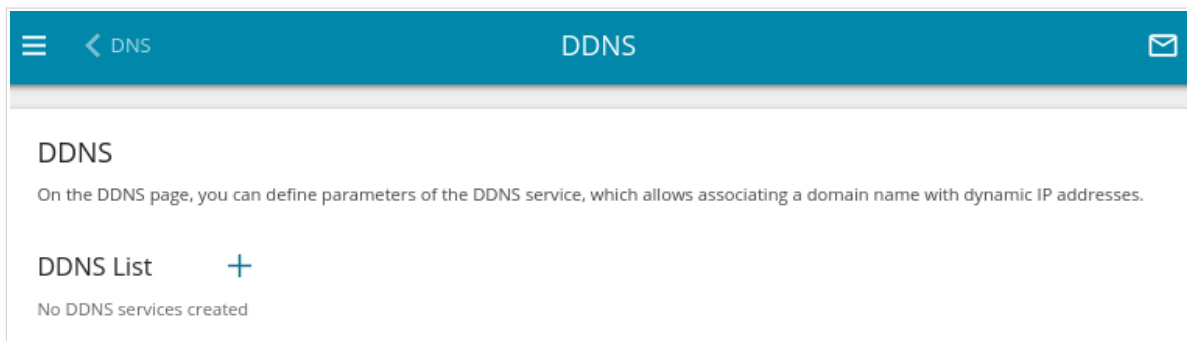



Figure 174. The **Advanced / DDNS** page.

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

The screenshot shows the 'DDNS/Adding' page in a web interface. At the top, there is a blue header bar with a menu icon, a back arrow labeled 'DDNS', the title 'DDNS/Adding', and an envelope icon. Below the header, the page contains several configuration fields. On the left, there is a toggle switch labeled 'Enable' which is currently turned on. Below it is a 'Hostname' field with the example 'For example: host.ru'. Under the hostname field is a blue 'ADD HOST' button. At the bottom left is a 'DDNS service\*' dropdown menu with 'changeip.com' selected. A 'SAVE' button is located at the bottom left. On the right side, there are four fields: 'Username\*', 'Password\*' (with an eye icon), 'Interface\*' (with a dropdown menu showing 'Default gateway'), and 'Update period (in minutes)\*'.

Figure 175. The page for adding a DDNS service.



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

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

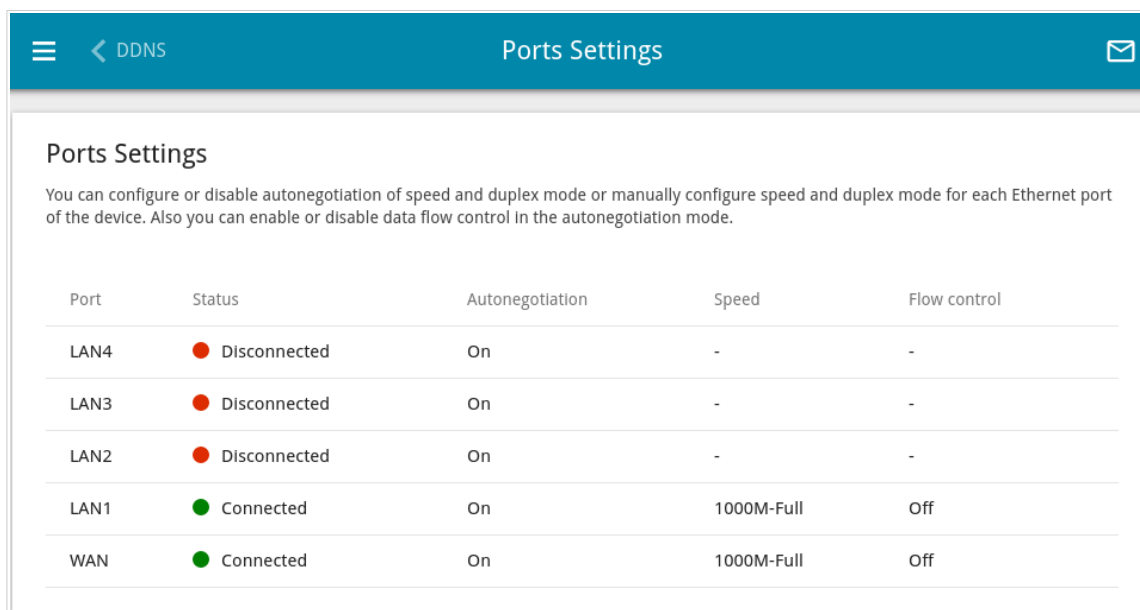
After specifying the needed parameters, click the **SAVE** button.

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

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

## Ports Settings

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



Port	Status	Autonegotiation	Speed	Flow control
LAN4	Disconnected	On	-	-
LAN3	Disconnected	On	-	-
LAN2	Disconnected	On	-	-
LAN1	Connected	On	1000M-Full	Off
WAN	Connected	On	1000M-Full	Off

Figure 176. 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.

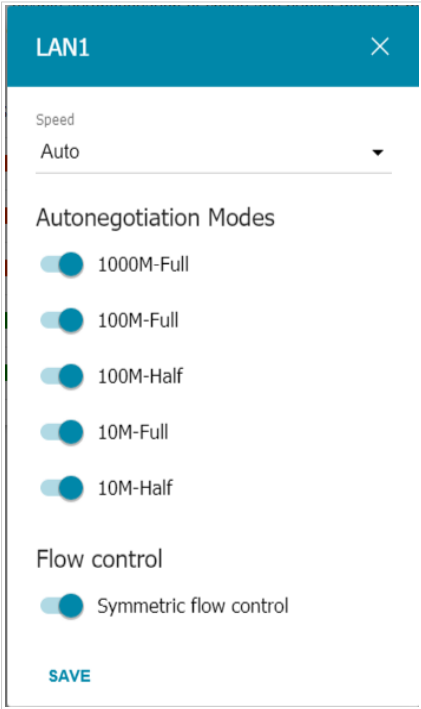


Figure 177. The window for changing the settings of the router's port.

In the opened window, specify the needed parameters:

Parameter	Description
Speed	<p>Select the <b>Auto</b> value to enable autonegotiation. When this value is selected, the <b>Autonegotiation Modes</b> and <b>Flow control</b> sections are displayed.</p> <p>Select the <b>10M-Half</b>, <b>10M-Full</b>, <b>100M-Half</b>, or <b>100M-Full</b> value to manually configure speed and duplex mode for the selected port.</p> <ul style="list-style-type: none"><li>• <b>10M-Half</b>: Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 10Mbps.</li><li>• <b>10M-Full</b>: Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 10Mbps.</li><li>• <b>100M-Half</b>: Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 100Mbps.</li><li>• <b>100M-Full</b>: Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 100Mbps.</li></ul>

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

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

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

## Redirect

On the **Advanced / Redirect** page, you can enable notifications on the reason of the Internet connection failure. Notifications will be displayed in the browser window when a user is attempting to open a web site on the Internet.

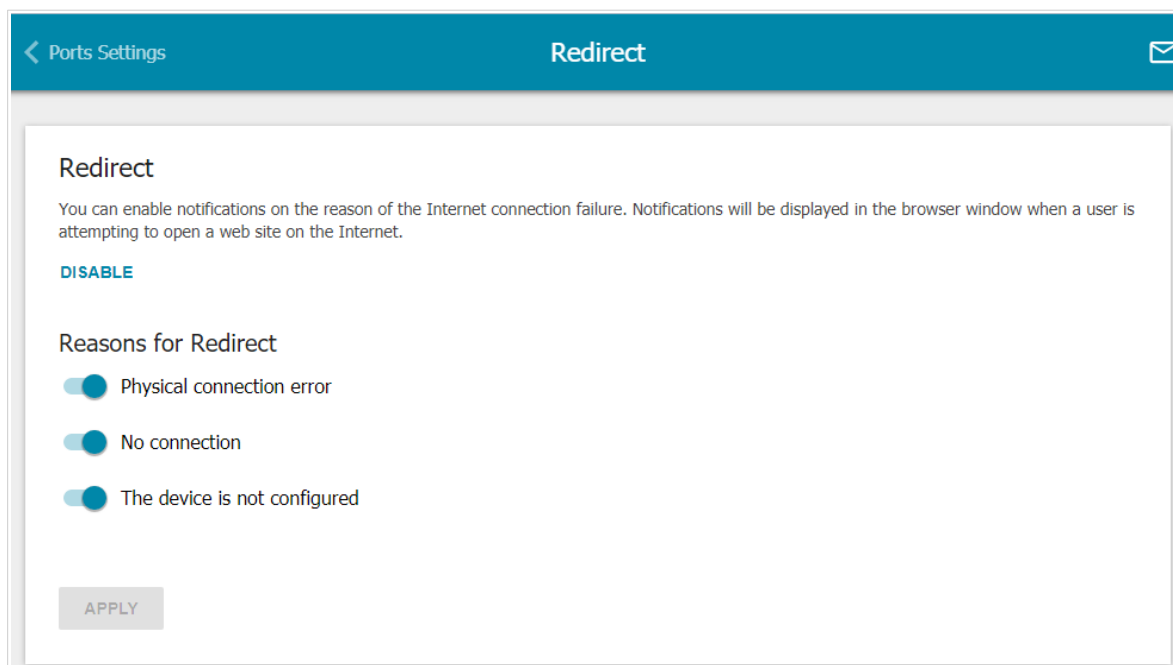


Figure 178. The **Advanced / Redirect** page.

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

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

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

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

## Routing

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

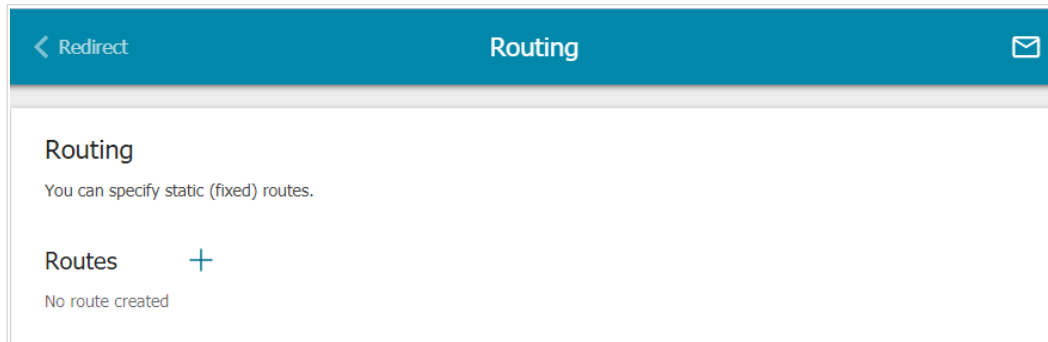


Figure 179. The **Advanced / Routing** page.

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

The screenshot shows the 'Add Route' window, which is a modal dialog box with a blue header bar containing the title 'Add Route' and a close button (X). The form inside the window has the following fields: a toggle switch labeled 'Enable' which is turned on; a 'Name\*' field with the value 'Route\_3'; a 'Protocol' dropdown menu set to 'IPv4'; an 'Interface' dropdown menu set to 'Auto'; a 'Destination network\*' field; a 'Destination netmask\*' field; a 'Gateway\*' field; a 'Metric' field; and a 'Table' dropdown menu set to 'group\_1'. At the bottom of the form is a 'SAVE' button.


Figure 180. The window for adding a new route.

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

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

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

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

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

# TR-069 Client

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

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

Routing

TR-069 Client

TR-069 Client

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.

Enable TR-069 client

Interface\*

Automatic

Auto Configuration Server Settings

Get URL address via DHCP

URL address

Username

Password

Inform Settings

On

Interval (in seconds)

120

Connection Request Settings

Username

Password

Request port

8999

Request path

APPLY

Figure 181. The page for configuring the TR-069 client.

You can specify the following parameters:

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

Page 240 of 323



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

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

## Port Mirroring

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

Figure 182. The **Advanced / Port Mirroring** page.

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

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

Parameter	Description
Source port	<p>Select the mode for each port traffic from which should be copied to the destination port:</p> <ul style="list-style-type: none"><li>• <b>Both</b>: Copy incoming and outgoing traffic from the source port to the destination port.</li><li>• <b>TX</b>: Copy outgoing traffic from the source port to the destination port.</li><li>• <b>RX</b>: Copy incoming traffic from the source port to the destination port.</li></ul> <p>Leave the <b>None</b> value for ports from which it is not required to copy traffic.</p>

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

To disable the function of port mirroring, click the **DISABLE** button.

## UPnP

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

Figure 183. The **Advanced / UPnP** page.

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

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

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

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

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

Parameter	Description
<b>IPv4 / IPv6</b>	
<b>Protocol</b>	A protocol for network packet transmission.
<b>IP address</b>	The IP address of a client from the local area network.
<b>Private port</b>	A port of a client's IP address to which traffic is directed from a public port of the router.
<b>Public port</b>	A public port of the router from which traffic is directed to a client's IP address.
<b>Description</b>	<i>For <b>IPv4</b> only.</i> Information transmitted by a client's network application.
<b>Pinhole ID</b>	<i>For <b>IPv6</b> only.</i> An identifier of the rule created by the client for an incoming connection to the router.

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

## UDPHY

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

Figure 184. The **Advanced / UDPXY** page.

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

Upon that the following fields are displayed on the page:

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

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

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

**udpxy status:**

Server Process ID	Accepting clients on	Multicast address	Active clients
1447	192.168.0.1:4022	192.168.161.235	0

[Restart](#)

**Available HTTP requests:**

Request template	Function
<a href="http://address:port/udp/mcast_addr:mport/">http://address:port/udp/mcast_addr:mport/</a>	Relay multicast traffic from mcast_addr:mport
<a href="http://address:port/status/">http://address:port/status/</a>	Display udpdy status
<a href="http://address:port/restart/">http://address:port/restart/</a>	Restart udpdy

udpxy v. 1.0 (Build 23) standard - [Mon Dec 16 12:08:29 2019]  
udpxy and udpdyrec are Copyright (C) 2008-2013 Pavel V. Cherenkov and licensed under GNU GPLv3

Figure 185. 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 'IGMP/MLD' configuration page. The header is blue with a menu icon, a 'Home' link, the title 'IGMP/MLD', and an email icon. The main content area is white with a light blue border. It is divided into two columns: 'IGMP' and 'MLD'. Each column has a description, an 'Enable' toggle switch, a version dropdown menu, and an interface dropdown menu. The IGMP version is set to 'IGMPv2' and the interface is 'WAN'. The MLD version is set to 'MLDv1v2' and the interface is 'Not selected'. An 'APPLY' button is at the bottom left.

Figure 186. The **Advanced / IGMP/MLD** page.

The following elements are available on the page:

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



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

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

## ALG/Passthrough

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

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

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

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

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

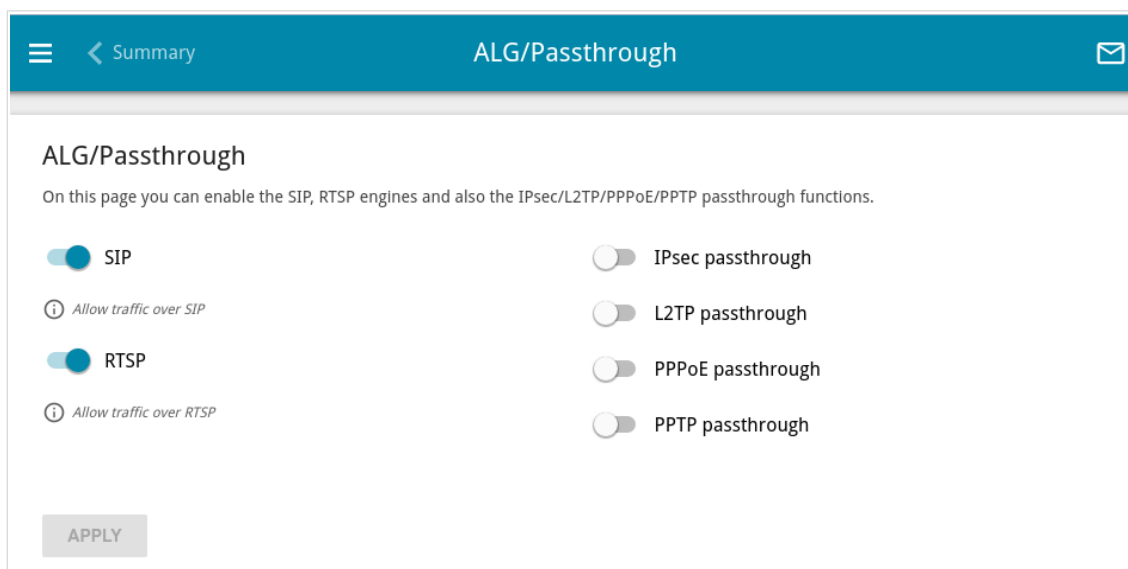


Figure 187. The **Advanced / ALG/Passthrough** page.

The following elements are available on the page:

Parameter	Description
<b>SIP</b>	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled router. <sup>16</sup>
<b>RTSP</b>	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
<b>IPsec pass through</b>	Move the switch to the right to enable the IPsec pass through function.
<b>L2TP pass through</b>	Move the switch to the right to enable the L2TP pass through function.
<b>PPPoE pass through</b>	Move the switch to the right to enable the PPPoE pass through function.
<b>PPTP pass through</b>	Move the switch to the right to enable the PPTP pass through function.

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

---

<sup>16</sup> On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / ALG/Passthrough** page, connect an Ethernet cable between a LAN port of the router and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

## CoovaChilli

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

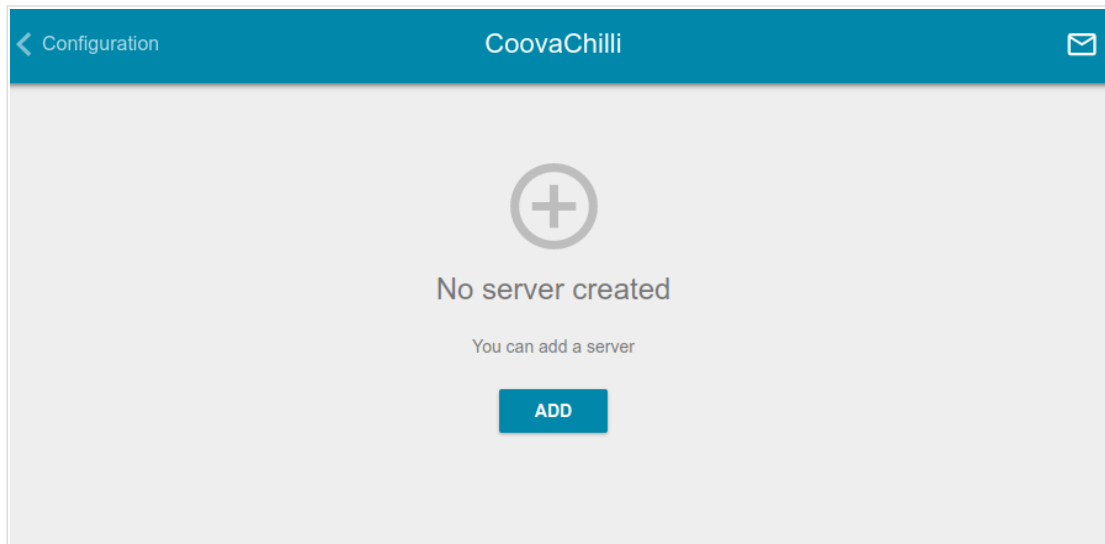



Figure 188. The **Advanced / CoovaChilli** page.

To add an authorization server, click the **ADD** button (+). On the opened page, move the **Enable** switch to the right to enable the CoovaChilli service.

### Main Settings

 There are no interfaces available for CoovaChilli

ⓘ If you want to use a separate LAN port or a Wi-Fi network as the interface, it is necessary to create another VLAN group for this port or network.

Lease time (in seconds)  
**86400**

Logging level  
**Error messages**

IP address\*

Mask\*

☐ Ping

Figure 189. The page for adding an authorization server. The **Main Settings** section.

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

Parameter	Description
<b>Interface</b>	From the drop-down list, select an interface to be used for the authorization server. A VLAN which includes a separate LAN port or a Wi-Fi network (see the <i>VLAN</i> section, page 222) is used as an interface for the server.
<b>Lease time</b>	The interval (in seconds) between sending authorization requests to clients.
<b>Logging level</b>	Select a type of messages and alerts/notifications to be logged.
<b>IP address</b>	Specify an IP address of the router to be used for authorized client access.
<b>Mask</b>	Specify a subnet mask.
<b>Ping</b>	If the switch is moved to the right, the router responds to ping requests by the IP address specified on this page. For security reasons, it is recommended to disable this function.

Figure 190. The page for adding an authorization server. The **RADIUS server** section.

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

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

Parameter	Description
<b>RADIUS encryption key</b>	The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings). Click the <b>Show</b> icon (🔍) to display the entered password.
<b>RADIUS server port</b>	A port of the RADIUS server.
<b>Authentication port</b>	The number of a router port which will be used to connect to the RADIUS server. By default, the value <b>1812</b> is specified.
<b>NASID</b>	A network access server ID (the value of this parameter is specified in the RADIUS server settings).

MAC authentication

☒ Enable

Password 🔍

Suffix

Figure 191. The page for adding an authorization server. The **MAC authentication** section.

In the **MAC authentication**<sup>17</sup> section, you can specify the following parameters:

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

<sup>17</sup> Will be available in future software versions.

Figure 192. The page for adding an authorization server. The **UAM** section.

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

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

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

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

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

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

## VRRP

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

The screenshot shows the VRRP configuration page. At the top, there is a blue header bar with a menu icon, a back arrow labeled 'Summary', the title 'VRRP', and an envelope icon. Below the header, the page title 'VRRP' is followed by a descriptive sentence: 'Virtual Router Redundancy Protocol is a network protocol designed to improve availability of the routers which act as default gateways.' The main configuration area includes a toggle switch for 'Enable VRRP' which is turned on. Below this, there are fields for 'Mode' (set to 'Backup'), 'Priority' (set to '100'), and 'Status' (set to 'Disable' with a red dot). A warning box with a yellow triangle icon states: 'For correct operation of the VRRP, it is necessary to disable Redirect'. Further down, there is a dropdown menu for 'Interface\*' set to 'LAN', a field for 'VRID\*' set to '1', and a field for 'Priority\*' set to '100'. To the right of these fields are two toggle switches: 'Assign virtual MAC address' (turned off) and 'Preempt mode' (turned on). Below these is a dropdown menu for 'Authorization' set to 'Without authorization', and another toggle switch 'Enable Object Tracking' (turned off). At the bottom left, there are fields for 'IP address\*', 'Mask\*', and 'Delay (in seconds)\*' set to '1'. An 'APPLY' button is located at the bottom left of the form.

Figure 193. The **Advanced / VRRP** page.



For correct operation of the router while using VRRP, it is required to disable notifications on the reason of the Internet connection failure on the **Advanced / Redirect** page (see the **Redirect** section, page 237).



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

Parameter	Description
<b>Mode</b>	<p>The operation mode of the router.</p> <ul style="list-style-type: none"> <li>• <b>Master</b>: The router ensuring data transfer at present. A device with a higher priority switches to the <b>Master</b> mode.</li> <li>• <b>Backup</b>: A reserve router, which switches to the <b>Master</b> mode upon the main router failure in accordance with its priority level.</li> </ul>
<b>Priority</b>	<p>The current priority level of the device. It can differ from the priority specified by the user if the <b>Enable Object Tracking</b> switch is moved to the right.</p>
<b>Status</b>	<p>The status of the service working over VRRP.</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>: The service is not active.</li> <li>• <b>Enabled</b>: The service is active.</li> </ul>
<b>Interface</b>	<p>A network interface used by VRRP.</p>
<b>VRID</b>	<p>Specify a unique ID of the virtual router. By default, the value <b>1</b> is specified.</p>
<b>Priority</b>	<p>The priority of the router over other devices, which is used to switch it to the <b>Master</b> mode. Specify a value from the range <b>1~255</b>. By default, the value <b>100</b> is specified. If several devices have the same priority level, the router with the highest IP address will switch to the <b>Master</b> mode.</p>
<b>IP address</b>	<p>The IP address used by LAN devices to access the router.</p>
<b>Mask</b>	<p>The subnet mask of the virtual router.</p>
<b>Delay</b>	<p>An interval (in seconds) between sending service advertisements, containing information on the priority level and connection status of the device working in the <b>Master</b> mode. By default, the value <b>1</b> is specified.</p>
<b>Assign virtual MAC address</b>	<p>Move the switch to the right to enable access to the virtual router by a virtual MAC address. A virtual MAC address is generated automatically.</p>

Parameter	Description
<b>Preempt mode</b>	<p>The preempt mode enables a backup router to switch to the <b>Master</b> mode if its priority level is higher than the priority of the current <b>Master</b>.</p> <p>Move the switch to the left to disable the preempt mode. If a device is the owner of the IP address specified on this page, it uses the preempt mode regardless of the position of this switch.</p>
<b>Authorization</b>	<p>Select the authorization method for devices working over VRRP.</p> <ul style="list-style-type: none"> <li>• <b>Without authorization:</b> Authorization is not required.</li> <li>• <b>PW:</b> Authorization by password (a HEX key). The maximum key length is 8 symbols. The key should begin with the <b>0x</b> prefix.</li> </ul>
<b>Enable Object Tracking</b>	<p>Move the switch to the right to track the status of the router connection. When the connection breaks down, the priority of the router is lowered. Select the relevant connection from the <b>Connection for Object Tracking</b> drop-down list displayed.</p> <p>Move the switch to the left to disable connection status tracking.</p>

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

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

## Wake-on-LAN

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



Make sure that the NIC of your device supports the Wake-on-LAN function.

Wake-on-LAN

Wake-on-LAN is a feature that allows you to remotely turn on or wake up a PC connected to the device's LAN.

☐ Enable

Interface  
<All>

Public port\*  
9

APPLY

Figure 194. The **Advanced / Wake-on-LAN** page.

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

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

## Firewall

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

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

## IP Filter

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

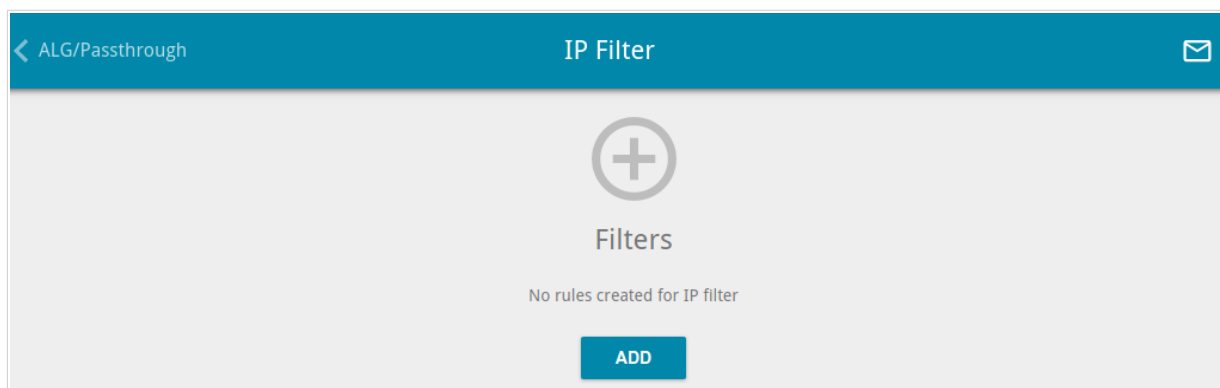


Figure 195. The **Firewall / IP Filter** page.

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

Figure 196. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
<b>General Settings</b>	
<b>Enable rule</b>	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
<b>Name</b>	A name for the rule for easier identification. You can specify any name.

Parameter	Description
<b>Priority</b>	The priority level of the rule. In the field, enter the needed value. The lower the value, the higher is the priority of the rule. You can specify a value from <b>0</b> to <b>5000</b> .
<b>Action</b>	Select an action for the rule. <ul style="list-style-type: none"> <li>• <b>Allow</b>: Allows packet transmission in accordance with the criteria specified by the rule.</li> <li>• <b>Deny</b>: Denies packet transmission in accordance with the criteria specified by the rule.</li> </ul>
<b>Protocol</b>	A protocol for network packet transmission. Select a value from the drop-down list.
<b>IP version</b>	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
<b>Direction</b>	The direction of network packet transmission to which the rule will be applied. Select the source of the packet direction from the <b>Source</b> drop-down list. <ul style="list-style-type: none"> <li>• <b>WAN</b>: The rule will be applied to the packets transmitted from the external network.</li> <li>• <b>LAN</b>: The rule will be applied to the packets transmitted from the local network.</li> <li>• <b>GRE</b>: The rule will be applied to the packets transmitted from the GRE tunnel (<i>available if a GRE tunnel has been created on the device</i>).</li> <li>• <b>IPIP</b>: The rule will be applied to the packets transmitted from the IPIP tunnel (<i>available if an IPIP tunnel has been created on the device</i>).</li> <li>• <b>IPsec</b>: The rule will be applied to the packets transmitted from the IPsec tunnel (<i>available if an IPsec tunnel has been created on the device</i>).</li> <li>• <b>PPTP Server</b>: The rule will be applied to the packets transmitted from the PPTP server (<i>available if a PPTP server has been created on the device</i>).</li> <li>• <b>L2TP Server</b>: The rule will be applied to the packets transmitted from the L2TP server (<i>available if an L2TP server has been created on the device</i>).</li> </ul>

Parameter	Description
	<p>Select the destination of the packet direction from the <b>Destination</b> drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Router</b>: The rule will be applied to the packets transmitted to DIR-853.</li> <li>• <b>WAN</b>: The rule will be applied to the packets transmitted to the external network.</li> <li>• <b>LAN</b>: The rule will be applied to the packets transmitted to the local network.</li> <li>• <b>GRE</b>: The rule will be applied to the packets transmitted to the GRE tunnel (<i>available if a GRE tunnel has been created on the device</i>).</li> <li>• <b>IPIP</b>: The rule will be applied to the packets transmitted to the IPIP tunnel (<i>available if an IPIP tunnel has been created on the device</i>).</li> <li>• <b>IPsec</b>: The rule will be applied to the packets transmitted to the IPsec tunnel (<i>available if an IPsec tunnel has been created on the device</i>).</li> <li>• <b>PPTP Server</b>: The rule will be applied to the packets transmitted to the PPTP server (<i>available if a PPTP server has been created on the device</i>).</li> <li>• <b>L2TP Server</b>: The rule will be applied to the packets transmitted to the L2TP server (<i>available if an L2TP server has been created on the device</i>).</li> </ul> <p>From the <b>Source interface</b> and <b>Destination interface</b> drop-down lists, select source and destination interfaces for which the rule will be applied. Leave the <b>Auto</b> values to apply the rule to all created WAN interfaces.</p>
<b>Source IP address</b>	
<b>Set as</b>	Select the needed value from the drop-down list.
<b>Start IPv4 address / Start IPv6 address</b>	<p>The source host start IPv4 or IPv6 address.</p> <p>If it is necessary to specify a single address, leave the <b>End IPv4 address / End IPv6 address</b> field blank.</p> <p>You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).</p>
<b>End IPv4 address / End IPv6 address</b>	The source host end IPv4 or IPv6 address.

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

Click the **APPLY** button.


To set a schedule for the IP filter rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 292) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.


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


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



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

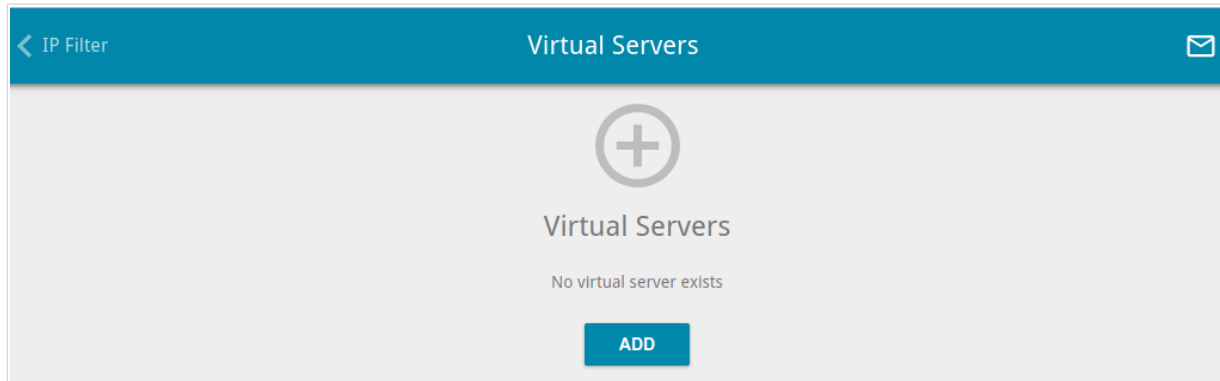
To create a copy of an IP filter rule, select the checkbox located to the left of the relevant line in the table and click the **Clone** (  ) icon. On the opened page, change the needed parameters and click the **APPLY** button.

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

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

## Virtual Servers

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



*Figure 197. The **Firewall / Virtual Servers** page.*


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

Figure 198. The page for adding a virtual server.

You can specify the following parameters:

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

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


Click the **APPLY** button.


To set a schedule for a virtual server, click the **Set schedule** icon (🕒) in the line corresponding to this server. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 292) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.


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

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

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

To create a copy of a virtual server, select the checkbox located to the left of the relevant line in the table and click the **Clone** (  ) icon. On the opened page, change the needed parameters and click the **APPLY** button.

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

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

## 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.

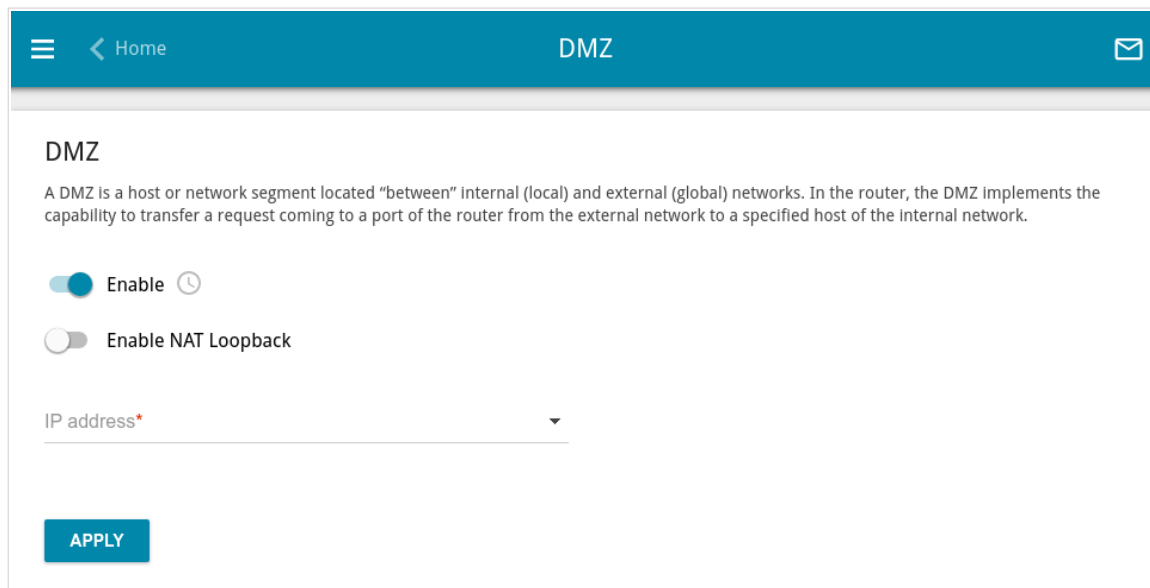


Figure 199. The **Firewall / DMZ** page.


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

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

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


Click the **APPLY** button.

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

To set a schedule for the DMZ, click the **Set schedule** icon (  ). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 292) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

## MAC Filter

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

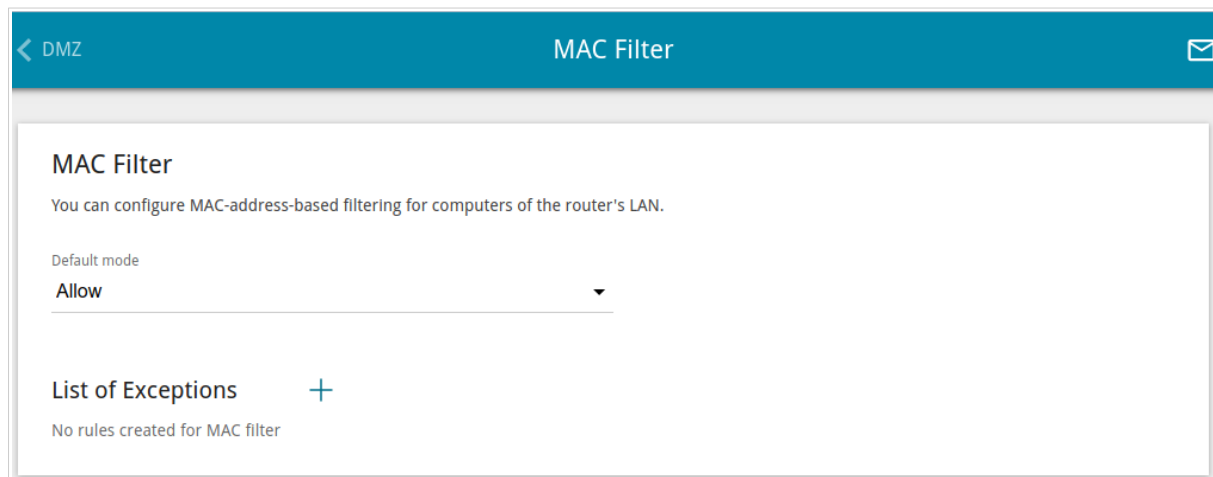


Figure 200. The **Firewall / MAC Filter** page.

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 ( **+** ).

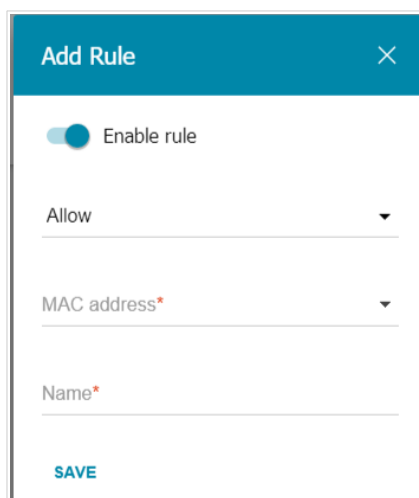


Figure 201. The window for adding a rule for the MAC filter.



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

Parameter	Description
<b>Enable rule</b>	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
<b>Action</b>	Select an action for the rule. <ul style="list-style-type: none"> <li><b>Deny:</b> Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices.</li> <li><b>Allow:</b> Allows access to the router's network and to the Internet for the device with the specified MAC address even if the default mode denies access for all devices.</li> </ul>
<b>MAC address</b>	The MAC address of a device from the router's LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
<b>Name</b>	The name of the device for easier identification. You can specify any name.

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

To set a schedule for the MAC filter rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 292) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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

## URL Filter

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

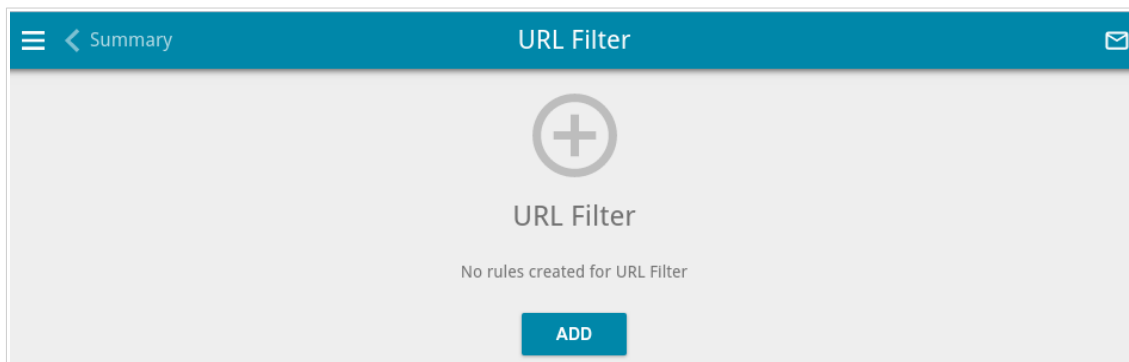


Figure 202. The **Firewall / URL Filter** page.

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

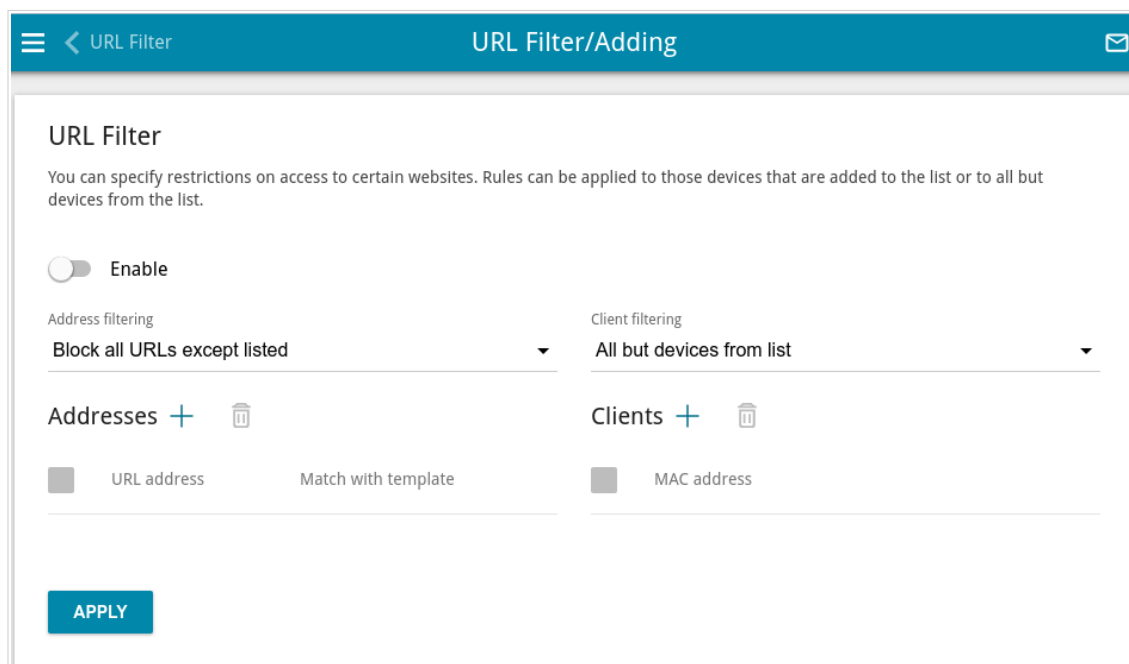



Figure 203. The page for adding a rule for URL filter.


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

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

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


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


Click the **SAVE** button.

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

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

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

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

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

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

To set a schedule for the URL filter rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 292) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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

## AdBlock

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

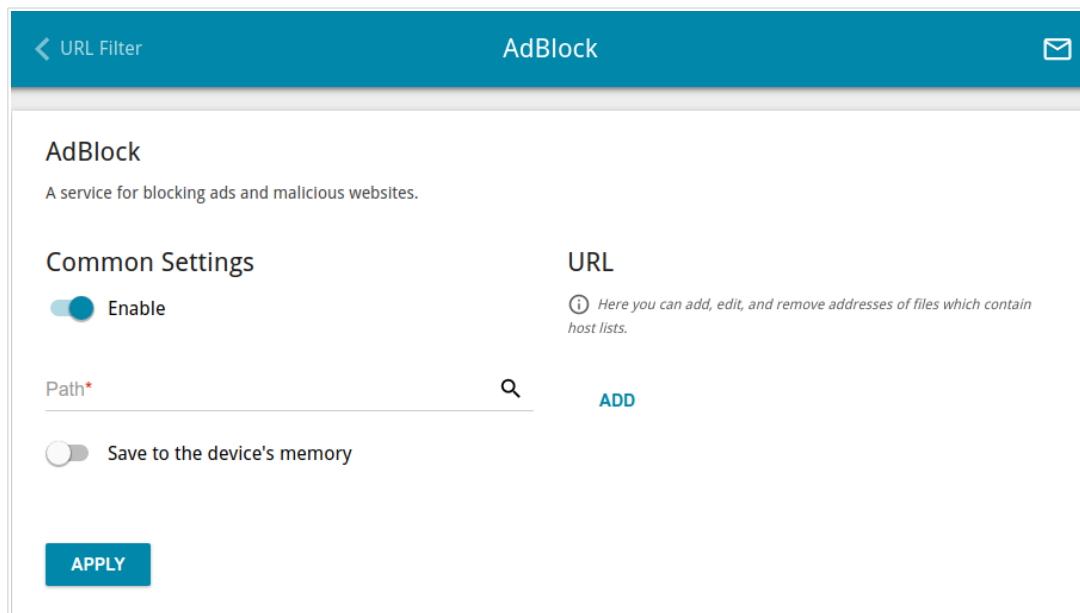


Figure 204. The **Firewall / AdBlock** page.

To enable the advertisements blocking function, in the **Common Settings** section, move the **Enable** switch to the right.

In the **Path** field, locate a folder to which a file for blocking advertisements will be saved. To do this, click the **Search** icon ( 🔍 ), go to the needed folder, and click the **SELECT** button.

Then in the **URL** section, click the **ADD** button and in the line displayed, enter a URL address of a file containing the list of advertising web sites which should be blocked.

Click the **APPLY** button and wait while the file is being loaded to the memory of the USB storage. Also you can save the file with the list of advertising web sites to the device's memory. To do this, move the **Save to the device's memory** switch to the right, and then click the **APPLY** button.



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

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

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

## Remote Access

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

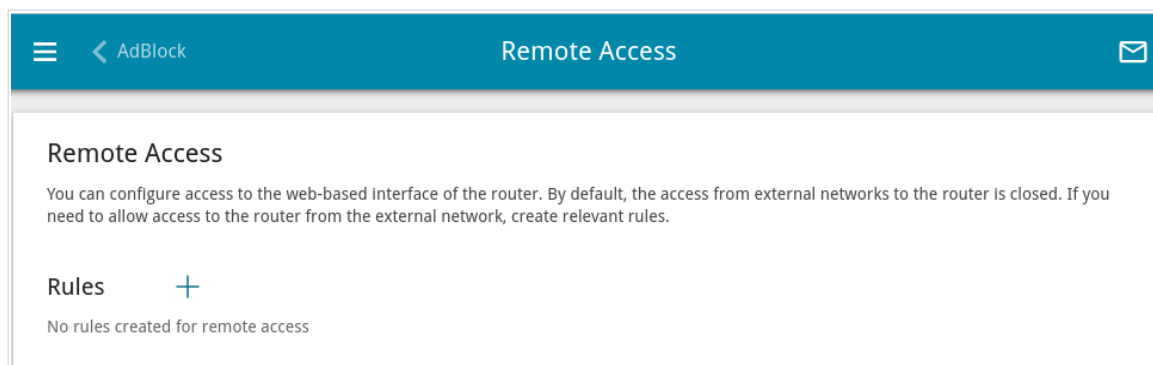


Figure 205. The **Firewall / Remote Access** page.

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

Figure 206. The window for adding a rule for remote management.

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

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


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


To set a schedule for the remote access rule, click the **Set schedule** icon (🕒) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 292) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

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

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



## System


In this menu you can do the following:

- change the password used to access the router's settings
- restore the factory default settings
- create a backup of the router's configuration
- restore the router's configuration from a previously saved file
- disable automatic save of the settings or save the changed settings manually to the non-volatile memory
- reboot the router
- change the web-based interface language
- edit or add commands for the hardware buttons
- update the firmware of the router
- configure automatic notification on new firmware version
- configure rules to enable/disable Wi-Fi connection and the Wi-Fi filter, automatic reboot of the device and saving a configuration backup to the connected USB storage on a schedule, and set a schedule for different rules and settings of the firewall
- enable event logging and set its basic options
- create rules for sending the event log to a remote server
- create rules for recording the event log to a USB storage connected to the router
- check availability of a host on the Internet through the web-based interface of the router
- trace the route to a host
- enable or disable access to the device settings via TELNET and/or SSH
- configure automatic synchronization of the system time or manually configure the date and time for the router
- enable the Auto Provision function.


## Configuration

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

Figure 207. The **System / Configuration** page.

In order to change the password for the administrator account, in the **User** section, enter a new password in the **New password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.<sup>18</sup> Click the **Show** icon (  ) to display the entered values. Then click the **SAVE** button.

<sup>18</sup> 0-9, A-Z, a-z, space, !"#%&'()\*+,-./:;<=>?@[\\]^\_`{|}~.


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

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

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

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

The following buttons are available in the **Action** section:

Control	Description
<b>Factory</b>	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware <b>RESET</b> button (see the <i>Back Panel</i> section, page 19).
<b>Backup</b>	Click the button to save the configuration (all settings of the router) to your PC or a USB storage connected to the router. See the <i>Creating Configuration Backup</i> section, page 285 for details on backup creation.
<b>Restore</b>	<p>Click the button to select and upload a previously saved configuration file (all settings of the router) located on your PC or a USB storage connected to the router.</p> <p>To upload a configuration file from your PC, select the <b>Local storage</b> value from the <b>File location</b> drop-down list. Click the <b>CHOOSE FILE</b> button and follow the dialog box appeared.</p> <p>To upload a configuration file from a USB storage connected to the router, select the <b>USB Storage</b> value from the <b>File location</b> drop-down list. Then locate the needed configuration file. To do this, click the <b>Search</b> icon (  ) in the <b>Path</b> field. Then choose the needed file and click the <b>SELECT</b> button.</p> <p>To upload the configuration file, click the <b>APPLY</b> button.</p>

Control	Description
<b>Save</b>	Click the button to save settings to the non-volatile memory. If the automatic save of the router's settings is disabled, save settings manually after you change the router's parameters. Otherwise the changes will be lost upon reboot of the router.
<b>Reboot</b>	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

## Creating Configuration Backup

To create a configuration backup, click the **Backup** button in the **Action** section.

Backup

File location  
USB Storage

☐ Backup manually  
☒ Schedule backup

Path to save on schedule\*  
Path is not selected

File name\*  
.tar.gz


ⓘ Attention! Unmount storage in 'USB storage/Information' menu before removing USB storage

SET SCHEDULE

Figure 208. The window for creating a configuration backup.

To save the configuration backup to your PC, select the **Local storage** value from the **File location** drop-down list and click the **SAVE** button. The configuration backup will be stored in the download location of your web browser.


To save the configuration backup to a USB storage connected to the router, select the **USB Storage** value from the **File location** drop-down list. Then select the **Backup manually** choice of the radio button and click the **SAVE** button. In the opened window, in the **File name** field, specify a name for the configuration file. Then go to the needed folder and click the **SELECT** button to save the file.

To configure automatic creation of a configuration backup on a schedule, select the **Schedule backup** choice of the radio button and locate a folder to save the files (available if the **USB Storage** value was selected in the **File location** drop-down list). To do this, click the **Search** icon (  ) in the **Path to save on schedule** field. Then go to the needed folder and click the **SELECT** button.

In the **File name** field, specify a name for the configuration file. Then click the **SET SCHEDULE** button.

In the opened window, specify a schedule name and the interval and time for its execution (see the **Schedule** section, page 292 for detailed description of the fields).

Click the **SAVE** button.

To change or delete the schedule, click the **Edit schedule** icon (  ). In the opened window, click the **CHANGE SCHEDULE** button, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button<sup>19</sup>.

<sup>19</sup> Correct operation of the button will be implemented in the next firmware version.

# Buttons Configuration

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

Summary

Buttons Configuration

Buttons Configuration

On this page you can configure actions of the device hardware buttons.

Reset

+

☐

Command

Action

Button press duration

☐

Reset config and reboot

Long press

7 - 60

Wi-Fi

+

☐

Command

Action

Button press duration

☐

Enable/Disable Wi-Fi

Long press

0 - 7

WPS

+

☐

Command

Action

Button press duration

☐

Enable WPS

Long press

0 - 7

APPLY

Figure 209. The **System / Buttons Configuration** page.

The page displays commands assigned to the buttons by default (for the description of the buttons actions with the commands assigned by default, see the **Product Appearance** section, page 17). You can edit or delete them.

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

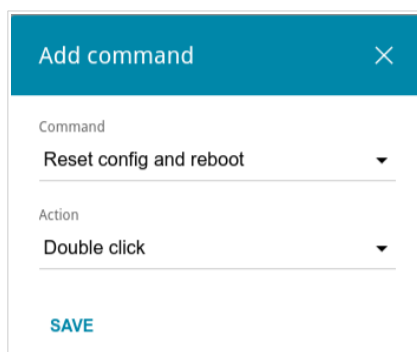



Figure 210. The window for adding a command.

In the opened window, specify the following parameters:

Control	Description
<b>Reset / Wi-Fi / WPS</b>	
<b>Command</b>	From the drop-down list, select a command.
<b>Action</b>	<p>From the drop-down list, select an action for the command.</p> <ul style="list-style-type: none"> <li>• <b>Single click:</b> One short press of the button lasting less than one second. The action is not available if the <b>Long press</b> action with the duration from 0 seconds has already been specified for the hardware button.</li> <li>• <b>Double click:</b> Two short presses of the button.</li> <li>• <b>Long press:</b> A prolonged press of the button. When this value is selected, the <b>Button press duration</b> section is displayed.</li> </ul>
<b>Button press duration</b>	Specify a period of time (in seconds) within which you should hold the button. You can specify values from <b>0</b> to <b>60</b> .

Click the **SAVE** button.

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

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

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

## Firmware Update

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

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

The screenshot shows the 'Firmware Update' page with a teal header bar containing a menu icon, a back arrow labeled 'Summary', the title 'Firmware Update', and an envelope icon. The page is divided into two main sections: 'Local Update' and 'Remote Update'. The 'Local Update' section on the left shows 'Current firmware version: 4.0.1', a toggle for 'Restore factory defaults after firmware update' (currently off), a 'CHOOSE FILE...' button with the text 'File is not selected', and an 'UPDATE FIRMWARE' button. The 'Remote Update' section on the right shows the 'Remote server URL' as 'fwupdate.dlink.ru' with a trash icon, an 'ADD' button, a toggle for 'Check for updates automatically' (currently on), and an 'Interval (in seconds)\*' field set to '43200'. A red error message at the bottom of the remote update section states 'Firmware update file is absent on remote server'. At the bottom of the page are 'CHECK FOR UPDATES' and 'APPLY SETTINGS' buttons.

Figure 211. The **System / Firmware Update** page.

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


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

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

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

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



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

Click the **APPLY SETTINGS** button.

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

## Local Update



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

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

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

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

## Remote Update



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

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

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

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

## Schedule

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



Before creating a schedule you need to configure automatic synchronization of the system time with a time server on the Internet(see the **System Time** section, page 308).

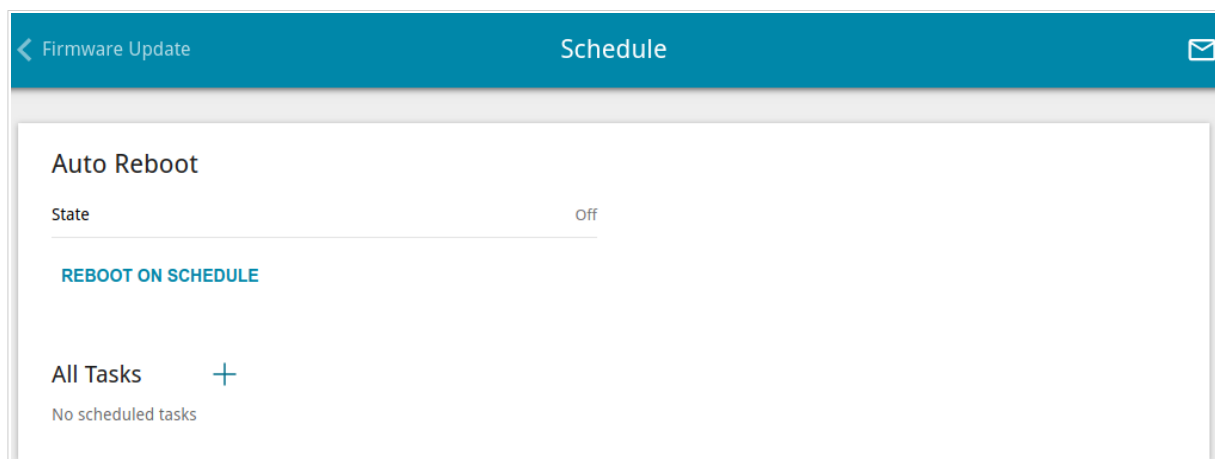


Figure 212. The **System / Schedule** page.

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

Figure 213. The window for configuring automatic reboot on a schedule.

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


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

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

Click the **SAVE** button.

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

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

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

Schedule

The task will be performed only if the system time of the device is synchronized with an NTP server.

System Time: 19 March 2024, 13:33

☐

Perform task on schedule

Mode  
Simplified mode

Schedule name\*

Interval of execution  
Every day

Hours (0-23)

Minutes (0-59)

Time 0 : 0

ⓘ

When entering several parameters, use the symbol "," or "-"  
(for example, "2, 5, 12" or "2-12")

Duration  

Hours\*

Minutes\*

Seconds\*

0030

SAVE

Figure 214. The window for adding a schedule for a task.

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

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


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

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

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

Click the **SAVE** button.

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

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

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



## Logging

In this menu you can enable event logging and create rules for sending the log to a remote server and/or a USB storage connected to the router.

### Local

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

The screenshot shows the 'Local' configuration page for logging. At the top, there is a blue header bar with a menu icon, a back arrow labeled 'Summary', the title 'Local', and an envelope icon. Below the header, the page is divided into two main sections. The first section, 'Logging to buffer', contains a toggle switch labeled 'Enable' which is currently turned on (blue). Below the toggle, there are two settings: 'Level' set to 'Informational messages' with a dropdown arrow, and 'Buffer size, Kbyte' set to '2048' with a lock icon. The second section, 'Log', features three buttons: 'REFRESH' (blue), 'CLEAR' (blue), and 'EXPORT' (black). Below these buttons is a large black rectangular area representing the log output. At the bottom left of the page, there is a grey 'APPLY' button.

Figure 215. The **System / Logging / Local** page.

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

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

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

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

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

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

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

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

## Remote

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

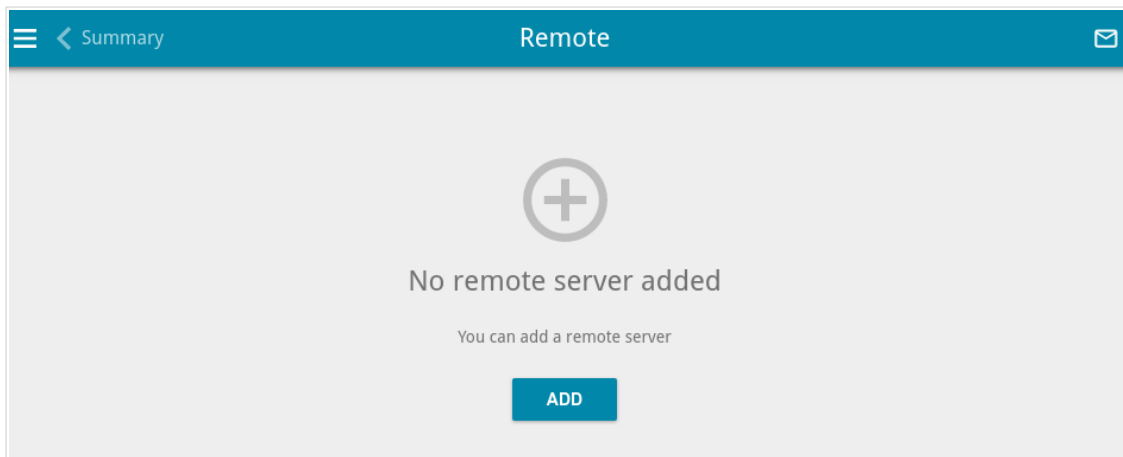


Figure 216. The **System / Logging / Remote** page.

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

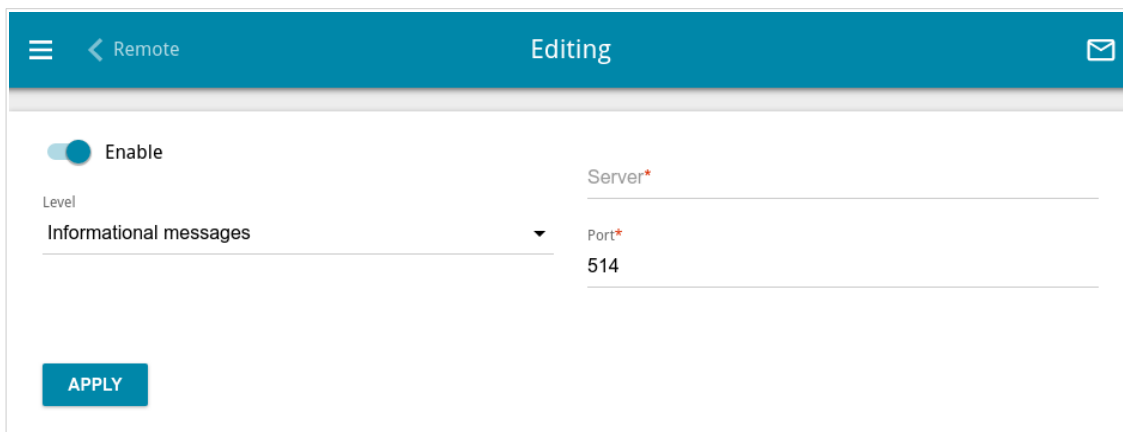


Figure 217. The page for adding a rule.


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

Parameter	Description
<b>Enable</b>	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
<b>Level</b>	From the drop-down list, select the severity level of messages which will be logged in the event log. Upon that messages which severity level is equal to the selected level or higher than the selected one will be logged.
<b>Server</b>	The IP address or full domain name of the host from the local or global network, to which the event log will be sent.

Parameter	Description
Port	A port of the host specified in the <b>Server</b> field. By default, the value <b>514</b> is specified.

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

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

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

### Record to File

On the **System / Logging / Record to file** page, you can create rules for recording the event log to a USB storage connected to the router.

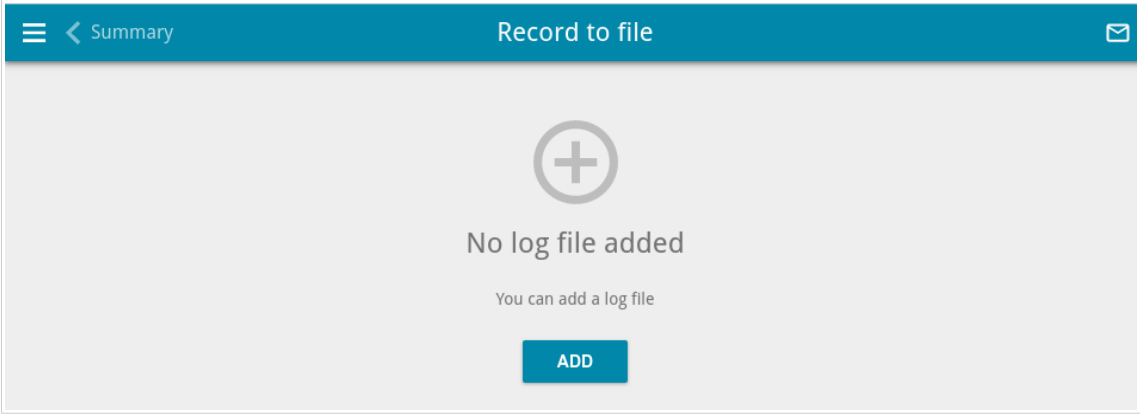


Figure 218. The **System / Logging / Record to file** page.

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

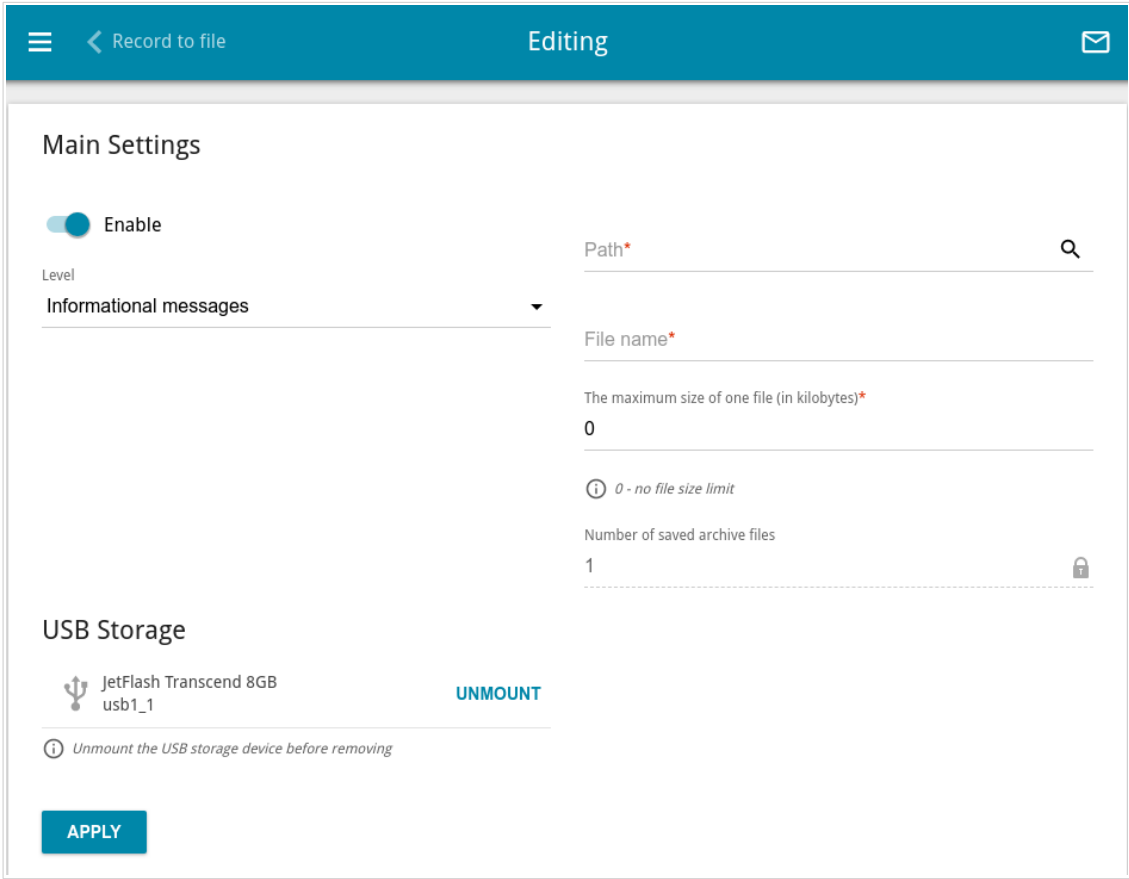



Figure 219. The page for adding a rule.


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

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

Parameter	Description
<b>Level</b>	From the drop-down list, select the severity level of messages which will be logged in the event log. Upon that messages which severity level is equal to the selected level or higher than the selected one will be logged.
<b>USB Storage</b>	If a USB storage is connected to the router, its name is displayed in the field. To safely disconnect the USB storage, click the <b>UNMOUNT</b> button.
<b>Path</b>	Click the <b>Search</b> icon (  ) located to the right of the field in order to locate the folder where system log files will be stored.
<b>File name</b>	A name for system log files.
<b>The maximum size of one file</b>	The maximum size (in kilobytes) of one system log file. When the value <b>0</b> is specified, the file size of the event log is not limited.
<b>Number of saved archive files</b>	The maximum number of archive files allowed to be recorded on the USB storage. When this number is exceeded, the archive file containing the oldest data will be deleted. The field is available for editing if the value specified in the <b>The maximum size of one file</b> field is greater than zero.

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

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

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

## Ping

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

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

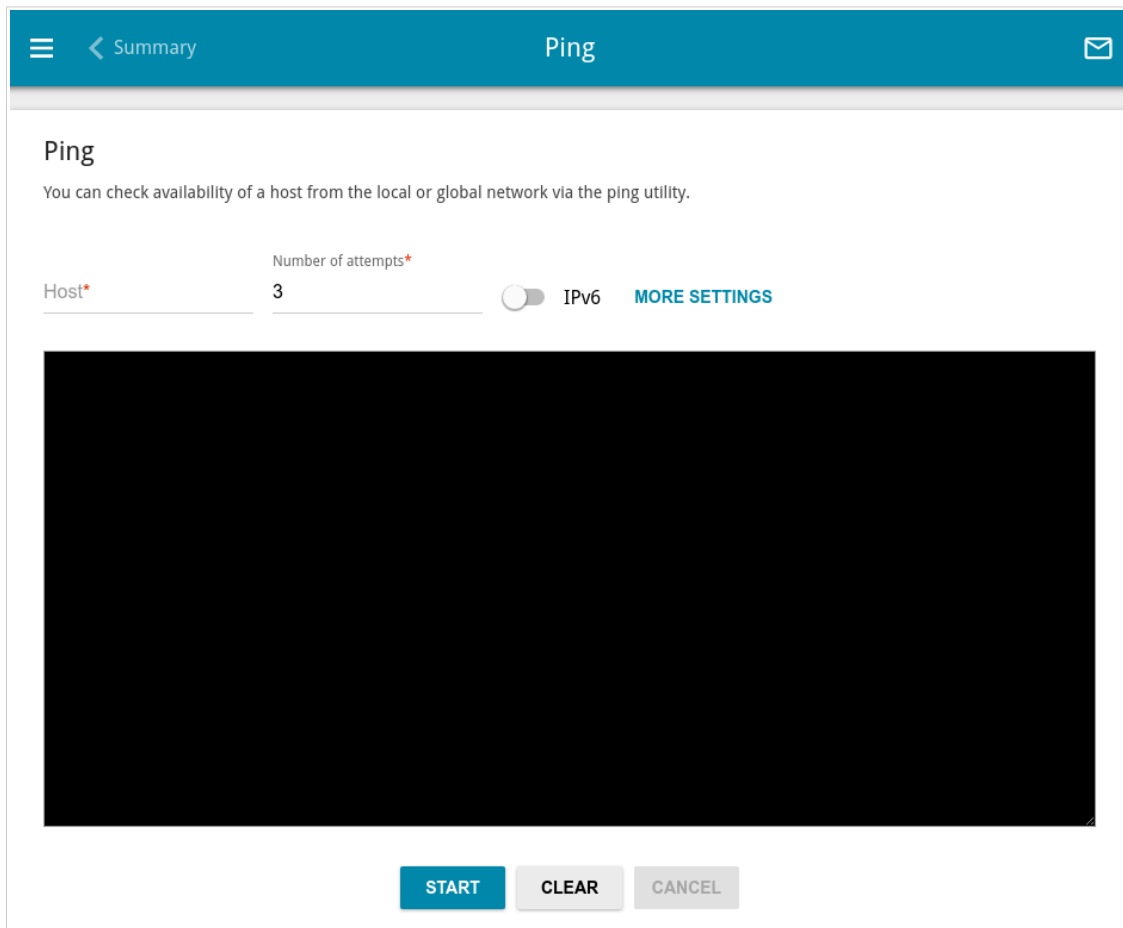
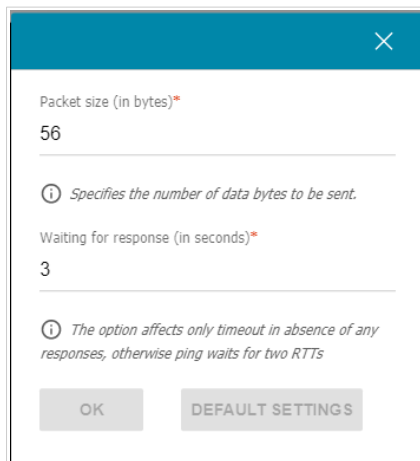
The screenshot shows the 'Ping' configuration page within a web interface. At the top, there is a blue header bar with a menu icon, a back arrow labeled 'Summary', the title 'Ping', and an envelope icon. Below the header, the page has a title 'Ping' and a descriptive text: 'You can check availability of a host from the local or global network via the ping utility.' The configuration area includes a 'Host\*' field, a 'Number of attempts\*' field set to '3', an 'IPv6' toggle switch (currently off), and a 'MORE SETTINGS' link. A large black rectangular area occupies the center of the page, likely representing a terminal or log output. At the bottom, there are three buttons: 'START' (blue), 'CLEAR' (grey), and 'CANCEL' (grey).

Figure 220. The **System / Ping** page.

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

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



The screenshot shows a modal window titled 'System / Ping' with a close button (X) in the top right corner. It contains two input fields: 'Packet size (in bytes)\*' with the value '56' and 'Waiting for response (in seconds)\*' with the value '3'. Below each field is an information icon (i) and a descriptive note. At the bottom, there are two buttons: 'OK' and 'DEFAULT SETTINGS'.

Packet size (in bytes)\*  
56

i Specifies the number of data bytes to be sent.

Waiting for response (in seconds)\*  
3

i The option affects only timeout in absence of any responses, otherwise ping waits for two RTTs

OK DEFAULT SETTINGS

Figure 221. The **System / Ping** page. The additional settings window.

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

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

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

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

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



## Traceroute

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

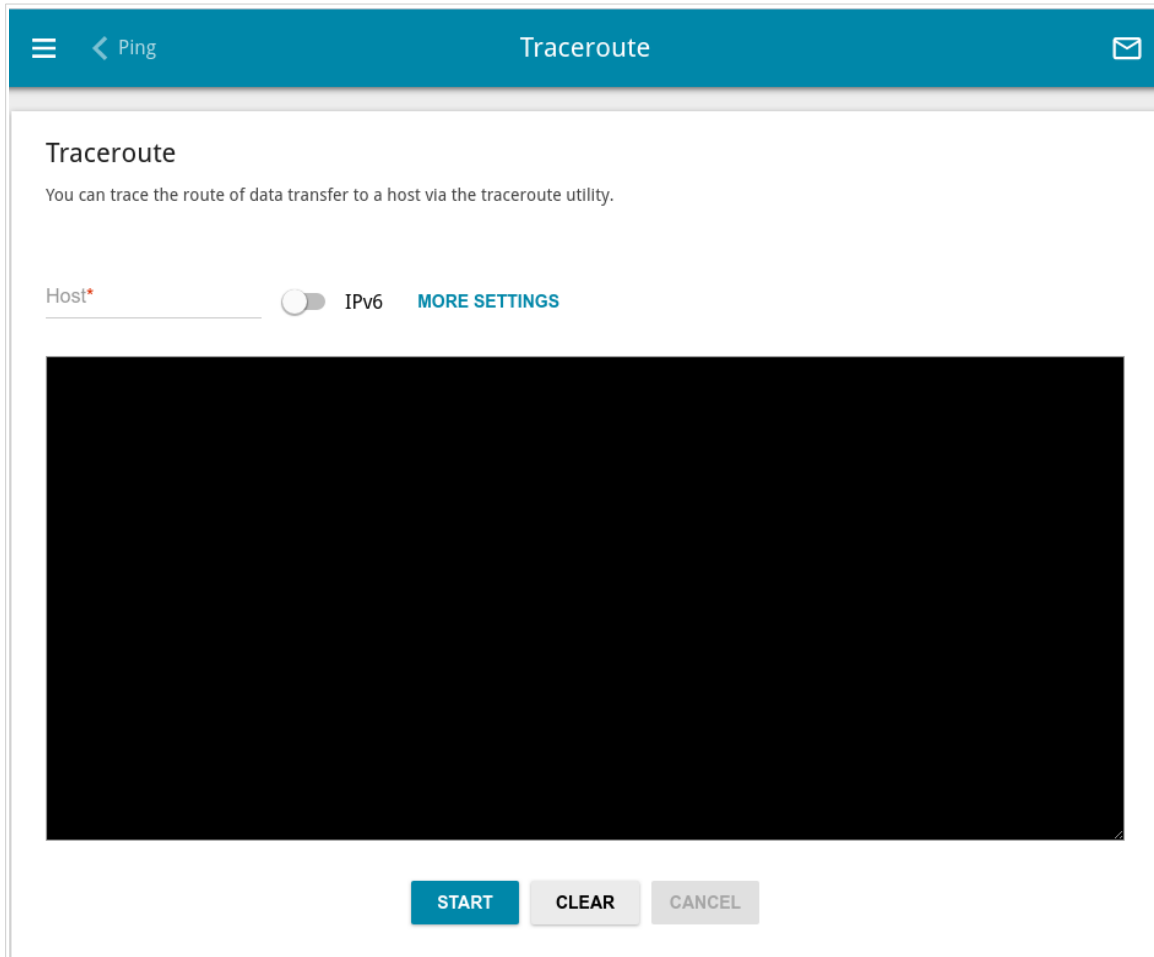


Figure 222. The **System / Traceroute** page.

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

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

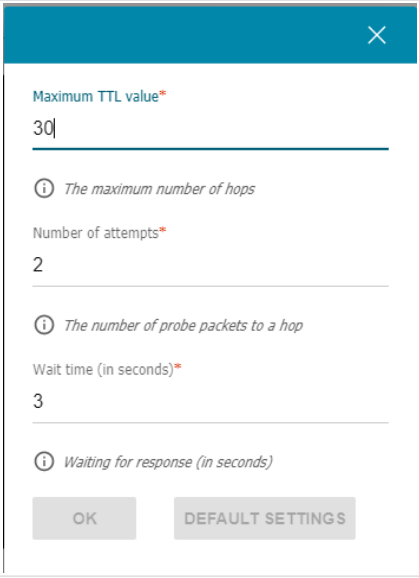


Figure 223. The **System / Traceroute** page. The additional settings window.

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

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

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

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

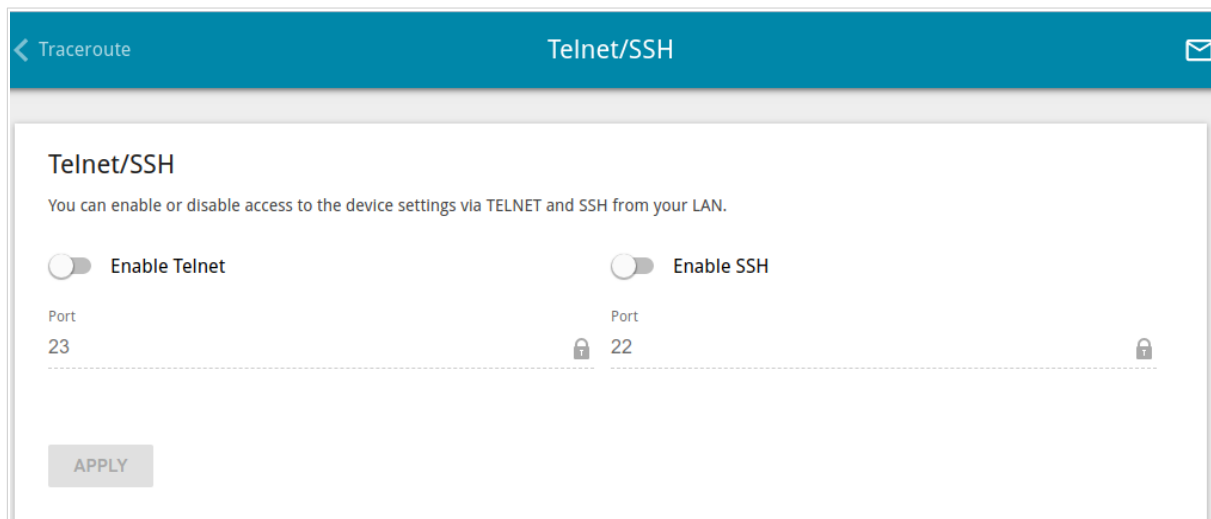
To run the check, click the **START** button. After a while, the results will be displayed on the page.

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

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

## Telnet/SSH

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



The screenshot shows the 'Telnet/SSH' configuration page. At the top, there is a blue header bar with a back arrow, the text 'Traceroute', the title 'Telnet/SSH', and an envelope icon. Below the header, the page title 'Telnet/SSH' is displayed. A descriptive text states: 'You can enable or disable access to the device settings via TELNET and SSH from your LAN.' There are two toggle switches: 'Enable Telnet' and 'Enable SSH', both currently turned off. Below each toggle is a 'Port' field. The 'Enable Telnet' port field contains the number '23'. The 'Enable SSH' port field contains the number '22'. Both port fields have a lock icon to their right, indicating they are locked. At the bottom left of the configuration area is a grey 'APPLY' button.

Figure 224. The **System / Telnet/SSH** page.

To enable access via TELNET and/or SSH, move the **Enable Telnet** switch and/or **Enable SSH** switch to the right. In the **Port** field, enter the number of the router's port through which access will be allowed (by default, the port **23** is specified for Telnet and the port **22** is specified for SSH). Then click the **APPLY** button.

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

## System Time

On the **System / System Time** page, you can manually set the time and date of the router or configure automatic synchronization of the system time with a time server on the Internet.

The screenshot shows the 'System Time' configuration page. At the top, there is a blue header bar with a menu icon, a back arrow, the text 'Summary', the title 'System Time', and an envelope icon. Below the header, the page is titled 'System time' with a subtitle: 'You can set up automatic synchronization of the system time with a time server on the Internet.' The main content area is divided into two columns. The left column contains five toggle switches: 'Enable NTP' (checked), 'UTC offset settings' (unchecked), 'Configure daylight saving time manually' (unchecked), 'Get NTP server addresses using DHCP' (unchecked), and 'Run as a server for the local network' (unchecked). Below these are three fields: 'System date:' with the value '17.02.2023', 'System time:' with the value '12:30', and 'Synchronization:' with the value 'Completed'. The right column contains two sections. The first is 'Time interval between NTP requests' with a subtitle 'After synchronization with NTP server (in seconds)' and a dropdown menu set to 'Auto'. Below this is another dropdown menu with the subtitle 'For unsynchronized NTP client (in seconds)' also set to 'Auto'. The second section is 'Time zone' with a subtitle 'Time zone\*' and a dropdown menu set to 'Europe/Moscow'. Below these sections is a blue button labeled 'DETERMINE TIMEZONE'. At the bottom left, there is a section titled 'NTP Servers' with a text input field containing 'pool.ntp.org' and a small 'x' icon to its right. Below this is a blue button labeled 'ADD SERVER'. At the very bottom left, there is a grey button labeled 'APPLY'.

Figure 225. The **System / System Time** page.

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

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

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

1. Move the **Enable NTP** switch to the right.
2. Specify the needed NTP server or leave the value specified by default in the **NTP Servers** section. If you need to specify several servers, click the **ADD SERVER** button.
3. Select your time zone from the **Time zone** drop-down list. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.

4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically. In case of successful synchronization with the NTP server, the **Completed** value will be displayed in the **Synchronization** field.

If the router failed to get data from the server, the **Failed** value will be displayed in the **Synchronization** field. Upon that the creation date and time of the router's current firmware version is specified.

Additional settings are also available on the page:

Parameter	Description
<b>UTC offset settings</b>	Move the switch to the right to set the UTC ( <i>Coordinated Universal Time</i> ) offset for the router clock manually. In the <b>UTC offset</b> field displayed, specify the required offset time (in minutes).
<b>Configure daylight saving time manually</b>	Move the switch to the right to configure settings for daylight saving time for the router clock manually. In the <b>Daylight Saving Time</b> section displayed, specify the required offset time for daylight saving time (in minutes), and specify the needed values in the <b>Beginning of daylight saving time</b> and <b>End of daylight saving time</b> sections.
<b>Get NTP server addresses using DHCP</b>	Move the switch to the right if NTP servers addresses are provided by your ISP. Obtained addresses will be displayed in the <b>NTP Servers</b> section. Contact your ISP to clarify if this setting needs to be enabled.  If the switch is moved to the right, settings of the <b>NTP Servers</b> section are unavailable.
<b>Run as a server for the local network</b>	Move the switch to the right to allow connected devices to use the IP address of the router in the local subnet as a time server.
<b>Time interval between NTP requests</b>	
<b>After synchronization with NTP server</b>	From the drop-down list, select a time period (in seconds) after which a request to update the system time will be sent to the NTP server or leave the <b>Auto</b> value.
<b>For unsynchronized NTP client</b>	A time period (in seconds) after which a request to synchronize the system time will be sent to the NTP server. Select the needed value from the drop-down list. <ul style="list-style-type: none"> <li>• <b>Auto</b>: The time period is defined automatically.</li> <li>• <b>Manual</b>: The time period is defined in accordance with the value specified in the <b>Interval value</b> field.</li> </ul>
<b>Interval value</b>	Specify the time period (in seconds). The minimum acceptable value is 3.

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



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

## Auto Provision

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

The Auto Provision function allows your ISP to manage the device's settings remotely: DIR-853 connects to the ISP's server, compares the current configuration file with the configuration file stored on this server, and updates its settings if the files are different.

The screenshot shows the 'Auto Provision' configuration page. At the top, there is a blue header bar with a back arrow and 'System Time' on the left, 'Auto Provision' in the center, and an envelope icon on the right. Below the header, the page title 'Auto Provision' is displayed. There are two toggle switches: 'Enable Auto Provision' (currently off) and 'Use BOOTP option' (currently off). To the right of these toggles, the 'Status' is shown as 'No check has been run yet'. Below the toggles is a blue 'CHECK STATUS' button. Further down, there are three input fields: 'Autoconfiguration server address', 'File name', and 'File check period (in seconds)' (set to 1800). Below these is a 'Protocol type' dropdown menu set to 'TFTP'. At the bottom left is a grey 'APPLY' button.

Figure 226. The page for configuring the Auto Provision function.

You can specify the following parameters:

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

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

After specifying the needed parameters, click the **APPLY** button.

If you need to check manually if the current configuration file corresponds to the configuration file on the ISP's server, click the **CHECK STATUS** button. The check result will be displayed in the **Status** field. If the files are different, the device's settings will be updated.



## ***SkyDNS***

This menu is designed to configure the SkyDNS service.

SkyDNS is a web content filtering service which provides protection against malicious web sites for devices connected to the router's network, and also allows to configure filtering, block access to adult web sites, and use search engines safely. In order to use the service, first register an account on the SkyDNS service web site.

## Settings

On the **SkyDNS / Settings** page, you can enable the SkyDNS service and specify settings for its operation.

The screenshot displays the SkyDNS Settings page. The header includes a navigation menu, a link to 'Auto Provision', the 'Settings' title, and an email icon. The main content area features the SkyDNS logo and tagline 'Service for web content filtering and safe Internet access.' Below this are four feature cards: 'Safe Internet at Home' (parental control), 'Web Content Filtering Service for Public Wi-Fi Networks' (public Wi-Fi protection), 'Protection Against Malware' (malware/phishing protection), and 'Convenient Management' (flexible filtering parameters). The 'Basic Settings' section shows the service is 'DISABLED' and includes fields for 'Provider' (SkyDNS), 'Default profile\*' (Основной), and 'Sync period (in seconds)\*' (3600). The 'Account' section shows 'Mail\*' (test@dlink.ru), 'Password\*' (masked), 'Tariff' (Домашний), and a 'Successfully authorized' status. At the bottom are 'APPLY' and 'MANUALLY SYNC' buttons.

Figure 227. The **SkyDNS / Settings** page.

To enable the SkyDNS service, click the **ENABLE** button. Then in the **Mail** and **Password** fields, enter the account data (the e-mail address and the password correspondingly) specified upon registration on the SkyDNS service web site. Click the **APPLY** button. The account data (authorization status, the tariff used), the **Default profile** drop-down list, and the **Sync period** field will be displayed on the page. If needed, from the **Default profile** list, select another filtering profile which will be used for all devices of your LAN and click the **APPLY** button again.

The default filtering profile will be applied to all devices newly connected to the router's network.

To change the parameters of your account on the SkyDNS service web site, click the **GO TO PERSONAL PROFILE PAGE** button.

By default, the account parameters are automatically synchronized with the SkyDNS service web site once an hour (3600 seconds). To change the automatic synchronization period, specify another value in the **Sync period** field and click the **APPLY** button. To start synchronization manually, click the **MANUALLY SYNC** button.

To use another account, specify its data in the **Mail** and **Password** fields and click the **APPLY** button.

To disable the SkyDNS service, click the **DISABLE** button.

# Devices and Rules

On the **SkyDNS / Devices and Rules** page, you can assign a specific filtering profile to a device connected to the router's network.

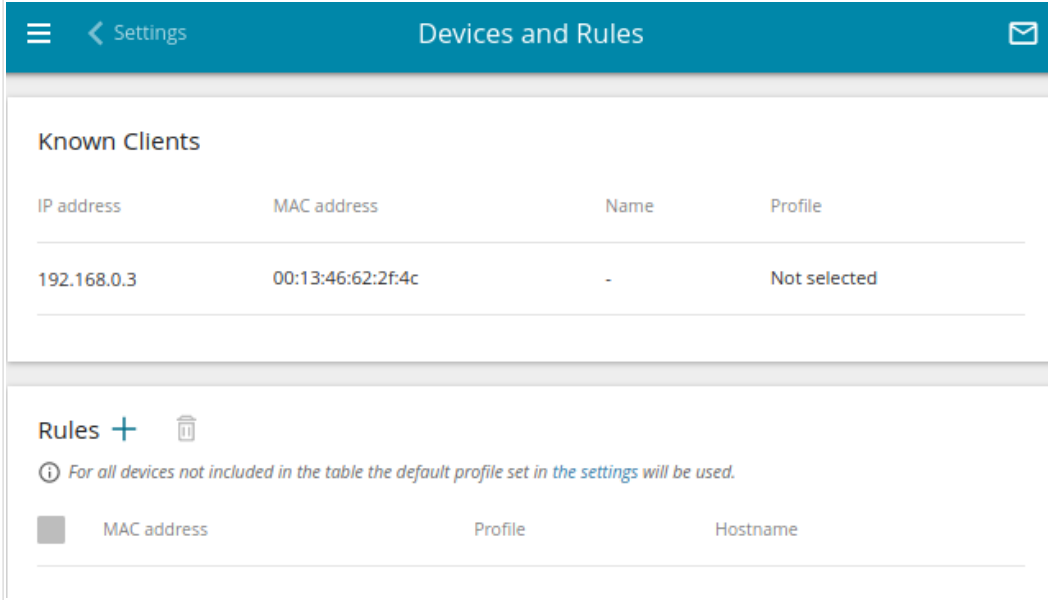


Figure 228. The **SkyDNS / Devices and Rules** page.

In the **Known Clients** section, the devices connected to the local network of the router at the moment and their relevant filtering profile are displayed.

To assign a specific filtering profile for a device, click the **ADD** button ( **+** ) in the **Rules** section or left-click the name of the filtering profile in the line of the device for which a profile should be assigned in the **Known Clients** section.


Figure 229. The **SkyDNS / Devices and Rules** page. The window for adding a rule.

In the opened window, specify the following parameters:

Parameter	Description
<b>MAC address</b>	The MAC address of a device from the router's LAN to which the specified filtering profile will be applied. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
<b>Profile</b>	Select the filtering profile which will be used for the device with the specified MAC address from the drop-down list.
<b>Hostname</b>	Enter a name for the rule for easier identification. <i>Optional</i> .

After specifying the needed parameters, click the **SAVE** button.

To edit a rule, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **DELETE** button (  ).

## CHAPTER 5. OPERATION GUIDELINES

### ***Terms and Conditions for Installation, Safe Operation, Storage, Transportation, and Disposal***

Please carefully read this section before installation and connection of the device. Make sure that the device, power adapter, and cables are not damaged. The device should be used only as intended (reception/transmission of data in computer networks); installation should be performed in accordance with the documents available on the official website.

The device is intended for use in dry, clean, dust-free, and well ventilated areas with normal humidity away from strong heat sources. Do not use the device outdoors or in the areas with high humidity. Do not place foreign objects on the device. Do not obstruct the ventilation openings of the device. The environmental temperature near the device and the temperature inside the device's cover should be within the range from 0 °C to +40 °C.

Only use the power adapter supplied with the device. Do not plug in the adapter, if its case or cable are damaged. Plug the adapter only into working electrical outlets with parameters indicated on the adapter. The electrical outlet must be installed near the equipment and must be easily accessible.

Do not open the cover of the device! Unplug the device before dusting and cleaning. Use a damp cloth to clean the device. Do not use liquid/aerosol cleaners or magnetic/static cleaning devices. Prevent moisture getting into the device or the power adapter.

The device may be stored and transported only in the original packaging at the temperature and humidity indicated in the specifications. No restrictions apply to sales. Please contact an authorized distributor to dispose of the equipment upon the end of its operation.

The service life of the device is 2 years.

The warranty period starts on the date of purchase from an authorized distributor within Russia or the CIS countries and extends for one year.

Irrespective of the date of purchase, the warranty period cannot exceed 2 years from the date of manufacture, which is determined by 6<sup>th</sup> (year) and 7<sup>th</sup> (month) digit in the serial number printed on the device label.

*Year: G – 2016, H – 2017, I – 2018, J – 2019, 0 – 2020, 1 – 2021, 2 – 2022, 3 – 2023, 4 – 2024, 5 – 2025.*

*Month: 1 – January, 2 – February, ..., 9 – September, A – October, B – November, C – December.*

If a fault is detected, please contact D-Link service center or technical support group.

## ***Wireless Installation Considerations***

The DIR-853 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-853 device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).
2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone is not in use.

## CHAPTER 6. ABBREVIATIONS AND ACRONYMS

<b>3G</b>	Third Generation
<b>AC</b>	Access Category
<b>AES</b>	Advanced Encryption Standard
<b>AP</b>	Access Point
<b>ARP</b>	Address Resolution Protocol
<b>BPSK</b>	Binary Phase-shift Keying
<b>BSSID</b>	Basic Service Set Identifier
<b>CCK</b>	Complementary Code Keying
<b>CHAP</b>	Challenge Handshake Authentication Protocol
<b>CoS</b>	Class of Service
<b>DBSK</b>	Differential Binary Phase-shift Keying
<b>DDNS</b>	Dynamic Domain Name System
<b>DDoS</b>	Distributed Denial of Service
<b>DES</b>	Data Encryption Standard
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DMZ</b>	DeMilitarized Zone
<b>DNS</b>	Domain Name System
<b>DPD</b>	Dead Peer Detection
<b>DQPSK</b>	Differential Quadrature Phase-shift Keying
<b>DSL</b>	Digital Subscriber Line
<b>DSSS</b>	Direct-sequence Spread Spectrum
<b>DTIM</b>	Delivery Traffic Indication Message
<b>EoGRE</b>	Ethernet over Generic Routing Encapsulation
<b>GMT</b>	Greenwich Mean Time
<b>GRE</b>	Generic Routing Encapsulation
<b>GSM</b>	Global System for Mobile Communications



<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>ICMP</b>	Internet Control Message Protocol
<b>ID</b>	Identifier
<b>IGD</b>	Internet Gateway Device
<b>IGMP</b>	Internet Group Management Protocol
<b>IKE</b>	Internet Key Exchange
<b>IMEI</b>	International Mobile Equipment Identity
<b>IMSI</b>	International Mobile Subscriber Identity
<b>IP</b>	Internet Protocol
<b>IPTV</b>	Internet Protocol Television
<b>IPsec</b>	Internet Protocol Security
<b>ISP</b>	Internet Service Provider
<b>L2TP</b>	Layer 2 Tunneling Protocol
<b>LAN</b>	Local Area Network
<b>LCP</b>	Link Control Protocol
<b>LED</b>	Light-emitting diode
<b>LTE</b>	Long Term Evolution
<b>MAC</b>	Media Access Control
<b>MBSSID</b>	Multiple Basic Service Set Identifier
<b>MIB</b>	Management Information Base
<b>MIMO</b>	Multiple Input Multiple Output
<b>MPPE</b>	Microsoft Point-to-Point Encryption
<b>MPU</b>	Maximum Packet Unit
<b>MS-CHAP</b>	Microsoft Challenge Handshake Authentication Protocol
<b>MTU</b>	Maximum Transmission Unit
<b>NAT</b>	Network Address Translation
<b>NIC</b>	Network Interface Controller

<b>NTP</b>	Network Time Protocol
<b>OFDM</b>	Orthogonal Frequency Division Multiplexing
<b>PAP</b>	Password Authentication Protocol
<b>PBC</b>	Push Button Configuration
<b>PCP</b>	Port Control Protocol
<b>PFS</b>	Perfect Forward Secrecy
<b>PIN</b>	Personal Identification Number
<b>PMP</b>	Port Mapping Protocol
<b>PoE</b>	Power over Ethernet
<b>PPP</b>	Point-to-Point Protocol
<b>pppd</b>	Point-to-Point Protocol Daemon
<b>PPPoE</b>	Point-to-point protocol over Ethernet
<b>PPTP</b>	Point-to-point tunneling protocol
<b>PSK</b>	Pre-shared key
<b>PUK</b>	PIN Unlock Key
<b>QAM</b>	Quadrature Amplitude Modulation
<b>QoS</b>	Quality of Service
<b>QPSK</b>	Quadrature Phase-shift Keying
<b>RADIUS</b>	Remote Authentication in Dial-In User Service
<b>RIP</b>	Routing Information Protocol
<b>RIPng</b>	Next Generation Routing Information Protocol
<b>RTS</b>	Request To Send
<b>RTSP</b>	Real Time Streaming Protocol
<b>SA</b>	Security Association
<b>SAE</b>	Simultaneous Authentication of Equals
<b>SIM</b>	Subscriber Identification Module
<b>SIP</b>	Session Initiation Protocol
<b>SMB</b>	Server Message Block

<b>SNMP</b>	Simple Network Management Protocol
<b>SSH</b>	Secure Shell
<b>SSID</b>	Service Set Identifier
<b>STBC</b>	Space-time block coding
<b>TCP</b>	Transmission Control Protocol
<b>TKIP</b>	Temporal Key Integrity Protocol
<b>TLS</b>	Transport Layer Security
<b>ToS</b>	Type of Service
<b>UAM</b>	Universal Access Method
<b>UDP</b>	User Datagram Protocol
<b>UPnP</b>	Universal Plug and Play
<b>URL</b>	Uniform Resource Locator
<b>USB</b>	Universal Serial Bus
<b>VLAN</b>	Virtual Local Area Network
<b>VPN</b>	Virtual Private Network
<b>VRID</b>	Virtual Router Identifier
<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>WAN</b>	Wide Area Network
<b>WEP</b>	Wired Equivalent Privacy
<b>Wi-Fi</b>	Wireless Fidelity
<b>WISP</b>	Wireless Internet Service Provider
<b>WLAN</b>	Wireless Local Area Network
<b>WMM</b>	Wi-Fi Multimedia
<b>WPA</b>	Wi-Fi Protected Access
<b>WPS</b>	Wi-Fi Protected Setup