D-Link®

DIR-300S

Wireless N150 Router

November 2017

Contents

CHAPTER 1.   INTRODUCTION

Contents and Audience

This manual describes the router DIR-300S and explains how to configure and operate it.

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

Conventions

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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the router DIR-300S and configure a PC in order to access its web-based interface.

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

Chapter 5 includes safety instructions and tips for networking.

Chapter 6 introduces abbreviations and acronyms used in this manual.

CHAPTER 2. OVERVIEW

General Information

The DIR-300S device is a wireless router with a built-in 4-port switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

You are able to connect the wireless router DIR-300S 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-300S device, you are able to quickly create a wireless network at home or in your office, which lets your relatives or employees connect to your wireless network virtually anywhere (within the operational range of your wireless network). The router can operate as a base station for connecting wireless devices of the standards 802.11b, 802.11g, and 802.11n (at the rate up to 150Mbps).

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

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

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

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

The wireless router DIR-300S 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.

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

You can configure the settings of the wireless router DIR-300S 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-300S 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-300S supports configuration and management via D-Link Click'n'Connect 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	· RTL8196E (400MHz)
RAM	· 32MB, SDRAM
Flash	· 4MB, SPI
Interfaces	· 10/100BASE-TX WAN port · 4 10/100BASE-TX LAN ports
LEDs	· POWER · WLAN · WPS · INTERNET · 4 LAN LEDs
Buttons	· ON/OFF button to power on/power off · RESET button to restore factory default settings · WPS button to set up wireless connection and enable/disable wireless network
Antenna	· External omnidirectional antenna (5dBi gain)
Power connector	· Power input connector (DC)

Software	
WAN connection types	· PPPoE · IPv6 PPPoE · PPPoE Dual Stack · Static IPv4 / Dynamic IPv4 · Static IPv6 / Dynamic IPv6 · PPPoE + Static IP (PPPoE Dual Access) · PPPoE + Dynamic IP (PPPoE Dual Access) · PPTP/L2TP · PPTP/L2TP + Static IP · PPTP/L2TP + Dynamic IP
Network functions	· DHCP server/relay · Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation · DNS relay · Dynamic DNS · Static IP routing · Static IPv6 routing · IGMP Proxy · RIP · Support of UPnP IGD · Support of VLAN · WAN ping respond · Support of SIP ALG · Support of RTSP · Autonegotiation of speed, duplex mode, and flow control/Manual speed and duplex mode setup for each Ethernet port · Setup of maximum TX rate for each port of the router · Built-in UDPXY application

---

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

Software	
Firewall functions	· Network Address Translation (NAT) · Stateful Packet Inspection (SPI) · IP filter · IPv6 filter · MAC filter · URL filter · DMZ · Prevention of ARP and DDoS attacks · Virtual servers · Built-in Yandex.DNS web content filtering service
VPN	· IPsec/PPTP/L2TP/PPPoE pass-through
Management	· Local and remote access to settings through TELNET/WEB (HTTP/HTTPS) · Multilingual web-based interface for configuration and management · Support of Click'n'Connect application for Android smartphones · Notification on connection problems and auto redirect to settings · Firmware update via web-based interface · Automatic notification on new firmware version · Saving/restoring configuration to/from file · Support of logging to remote host · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility · TR-069 client

Wireless Module Parameters	
Standards	· IEEE 802.11b/g/n
Frequency range	· 2400 ~ 2483.5MHz
Wireless connection security	· WEP · WPA/WPA2 (Personal/Enterprise) · MAC filter · WPS (PBC/PIN)
Advanced functions	· Support of client mode · WMM (Wi-Fi QoS) · Information on connected Wi-Fi clients · Advanced settings · Smart adjustment of Wi-Fi clients · Guest Wi-Fi / support of MBSSID · Limitation of wireless network rate · Periodic scan of channels, automatic switch to least loaded channel
Wireless connection rate	· IEEE 802.11b: 1, 2, 5.5, and 11Mbps · IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11n: from 6.5 to 150Mbps (from MCS0 to MCS7)

Transmitter output power
 	
The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country
	· 802.11b (typical at room temperature 25 °C)
	  15dBm (+/-1.5dB) at 1, 2, 5.5, 11Mbps
	
	· 802.11g (typical at room temperature 25 °C)
	  15dBm (+/-1.5dB) at 6, 9, 12, 18, 24, 36, 48, 54Mbps
	
	· 802.11n (typical at room temperature 25 °C)
	  HT20
	  15dBm (+/-1.5dB) at MCS0/1/2/3/4/5/6
	  14dBm (+/-1.5dB) at MCS7
	  HT40
	  15dBm (+/-1.5dB) at MCS0/1/2/3/4/5/6
	  14dBm (+/-1.5dB) at MCS7

Wireless Module Parameters	
Receiver sensitivity	· 802.11b (typical at PER = 8% at room temperature 25 °C) -82dBm at 1Mbps -80dBm at 2Mbps -78dBm at 5.5Mbps -76dBm at 11Mbps · 802.11g (typical at PER = 10% at room temperature 25 °C) -85dBm at 6Mbps -84dBm at 9Mbps -82dBm at 12Mbps -80dBm at 18Mbps -77dBm at 24Mbps -73dBm at 36Mbps -69dBm at 48Mbps -68dBm at 54Mbps · 802.11n (typical at PER = 10% at room temperature 25 °C) HT20 -82dBm at MCS0 -79dBm at MCS1 -77dBm at MCS2 -74dBm at MCS3 -70dBm at MCS4 -66dBm at MCS5 -65dBm at MCS6 -64dBm at MCS7 HT40 -79dBm at MCS0 -76dBm at MCS1 -74dBm at MCS2 -71dBm at MCS3 -67dBm at MCS4 -63dBm at MCS5 -62dBm at MCS6 -61dBm at MCS7
Modulation schemes	· 802.11b: DQPSK, DBPSK, DSSS, CCK · 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM · 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM

Physical Parameters	
Dimensions (L x W x H)	· 175 x 123 x 31 mm (7 x 5 x 1 in)
Weight	· 249 g (0.5 lb)

Operating Environment	
Power	· Output: 12V DC, 0.5A
Temperature	· Operating: from 0 to 40 °C · Storage: from -20 to 65 °C
Humidity	· Operating: from 10% to 90% (non-condensing) · Storage: from 5% to 95% (non-condensing)

Product Appearance

Top Panel

Figure 1. Top panel view.

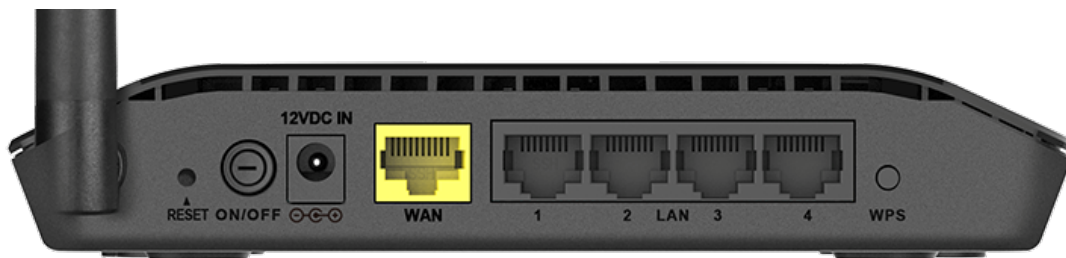| LED	Mode	Description
POWER	*Solid green*	The router is powered on.
	No light	The router is powered off.
WLAN	*Solid green*	The router's WLAN is on.
	Blinking green	The WLAN interface is active (upstream or downstream traffic).
	No light	The router's WLAN is off.
WPS	*Blinking green*	Attempting to add a wireless device via the WPS function.
	No light	The WPS function is not in use.
INTERNET	*Solid green*	The cable is connected.
	Blinking green	Attempting to establish WAN connection; after connection establishment – traffic transmission.
	No light	The cable is not connected.
LAN 1-4	*Solid green*	A device (computer) is connected to the relevant port, the connection is on.
	Blinking green	The LAN port is active (upstream or downstream traffic). When the router is being loaded, the LEDs are blinking one at a time. When the firmware is being upgraded, the LEDs are blinking two at a time.
	No light	The cable is not connected to the relevant port.

Back Panel

Figure 2. Back panel view.

Name	Description
RESET	A button to restore the factory default settings. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.
ON/OFF	A button to turn the router on/off.
12VDC IN	Power connector.
WAN	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).
LAN 1-4	4 Ethernet ports to connect computers or network devices.
WPS	A button to set up a wireless connection (the WPS function) and enable/disable the wireless network. To use the WPS function: with the device turned on, push the button, hold it for 2 seconds, and release. The **WPS** LED should start blinking. To disable the router's wireless network: with the device turned on, press the button, hold for 7 seconds, and release. The **WLAN** LED should turn off.

The device is also equipped with an external Wi-Fi antenna.

Delivery Package

The following should be included:

- Router DIR-300S

- Power adapter DC 12V/0.5A

- Ethernet cable (CAT 5)

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

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

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

CHAPTER 3. INSTALLATION AND CONNECTION

Before You Begin

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

Operating System

Configuration of the wireless router DIR-300S with a built-in 4-port switch (hereinafter referred to as "the router") is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

Web Browser

The following web browsers are recommended:

- Apple Safari 8 and later

- Google Chrome 48 and later

- Microsoft Internet Explorer 10 and later

- Microsoft Edge 20.10240 and later

- Mozilla Firefox 44 and later

- Opera 35 and later.

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

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

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

Wireless Connection

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

Connecting to PC

PC with Ethernet Adapter

1. Make sure that your PC is powered off.
2. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
3. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
4. Turn on the router by pressing the **ON/OFF** button on its back panel.
5. Turn on your PC and wait until your operating system is completely loaded.

Obtaining IP Address Automatically in OS Windows XP

1. Click the **Start** button and proceed to the **Control Panel > Network and Internet Connections > Network Connections** window.

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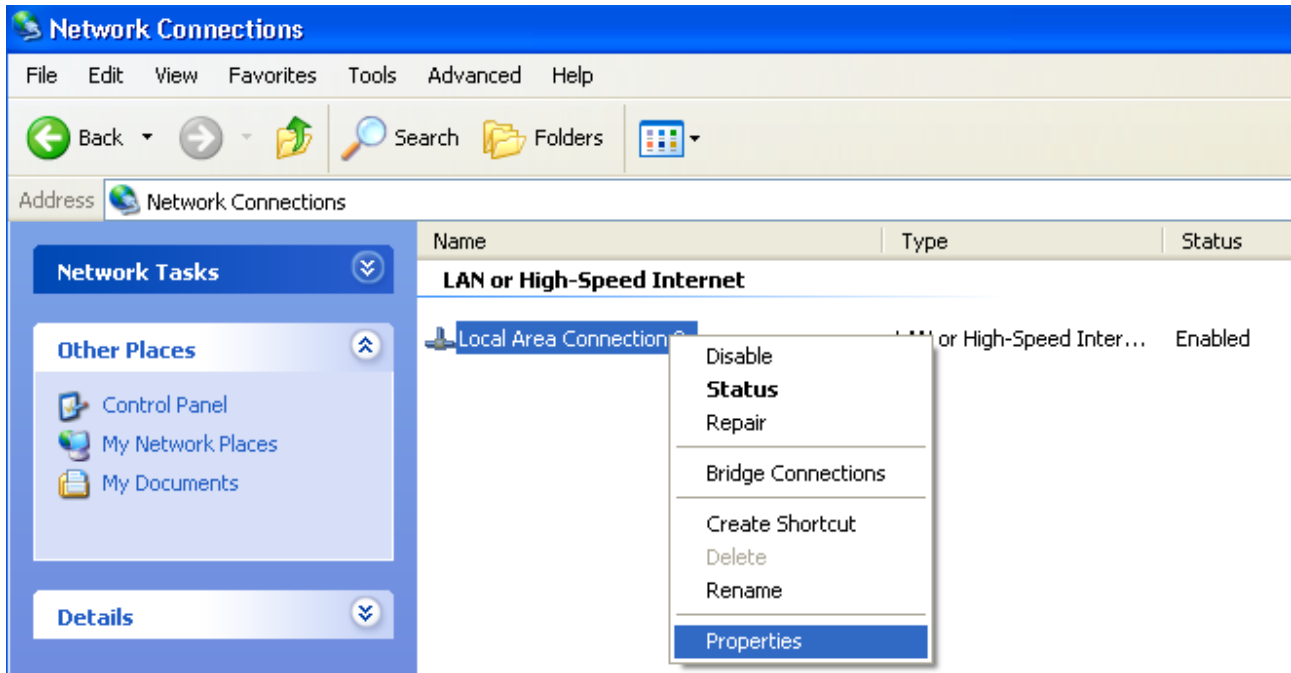

*Figure 3. The **Network Connections** window.*

3. In the **Local Area Connection Properties** window, on the **General** tab, select the **Internet Protocol (TCP/IP)** line. Click the **Properties** button.
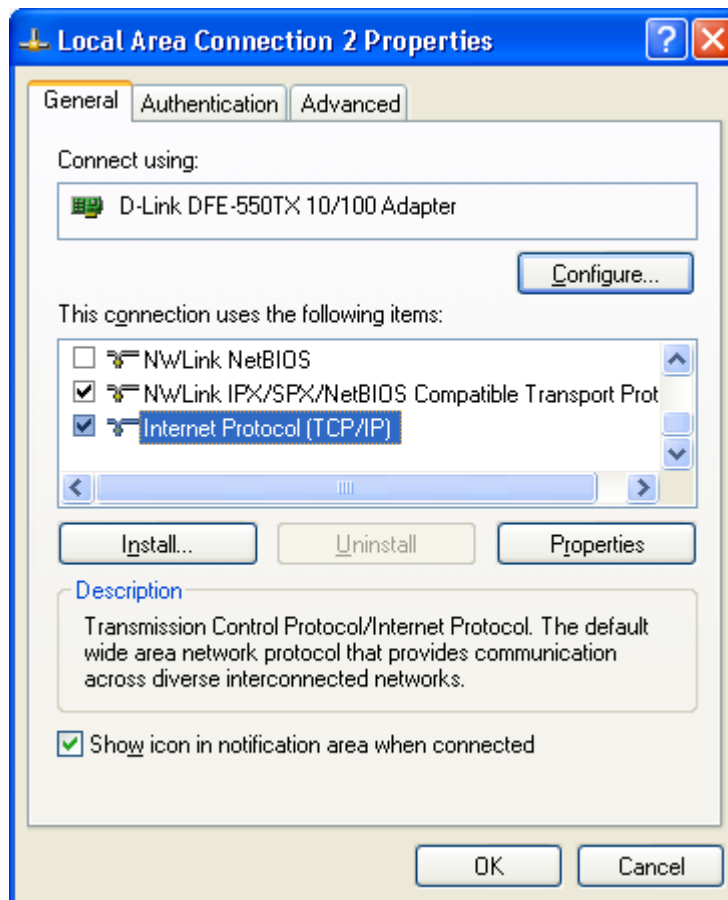

*Figure 4. The **Local Area Connection Properties** window.*

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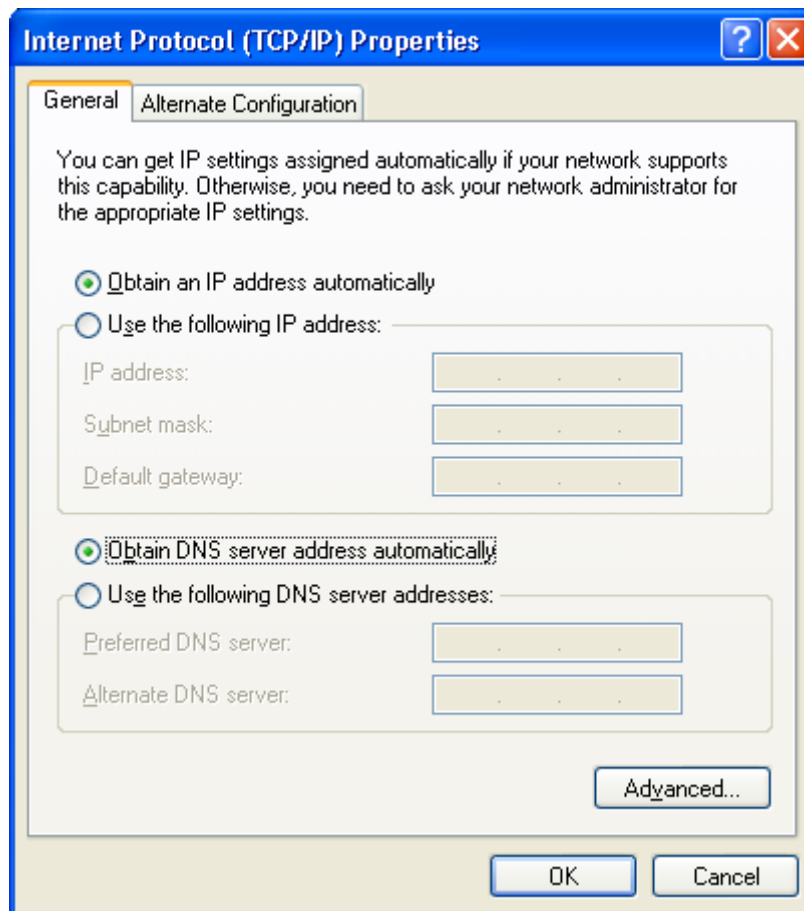

*Figure 5. The **Internet Protocol (TCP/IP) Properties** window.*

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

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

Obtaining IP Address Automatically in OS Windows 7

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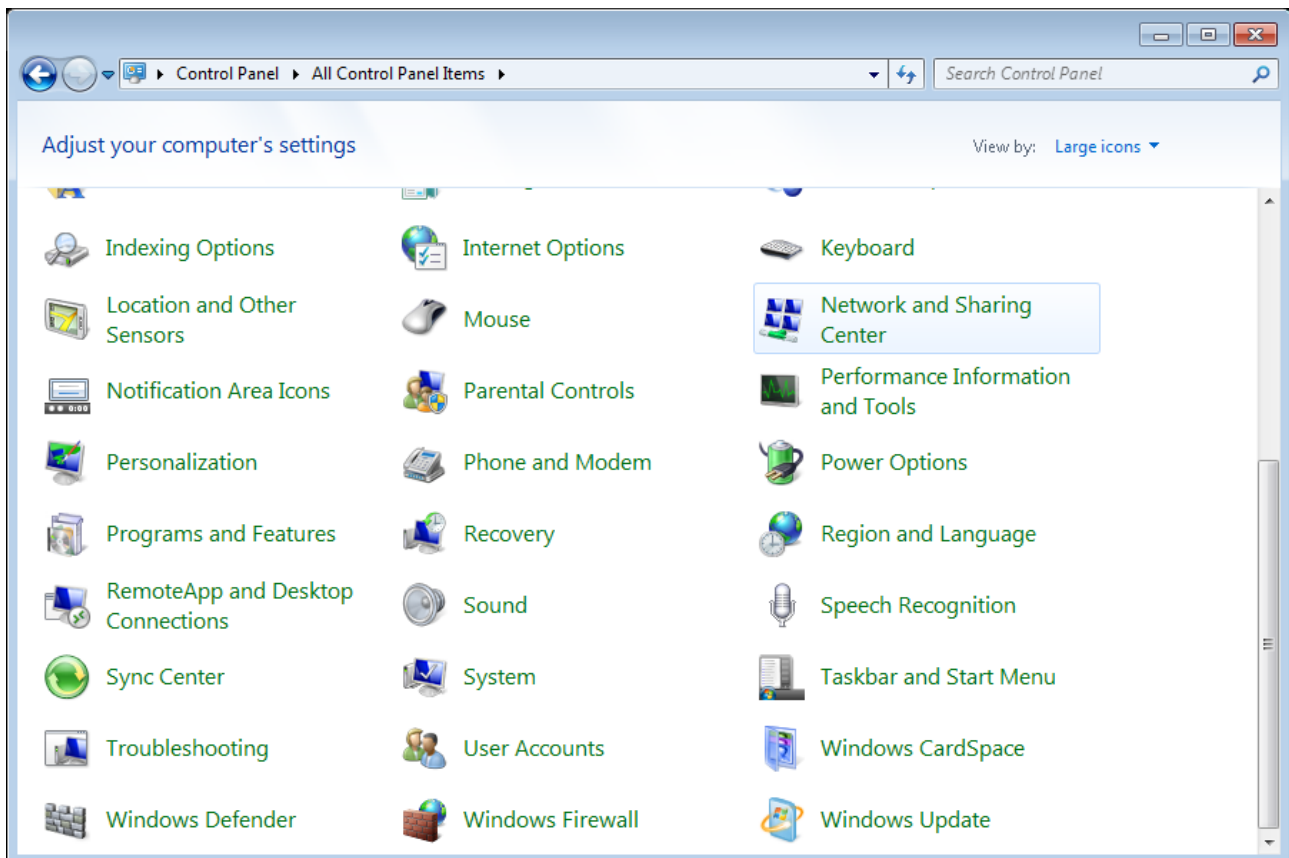

*Figure 6. The **Control Panel** window.*

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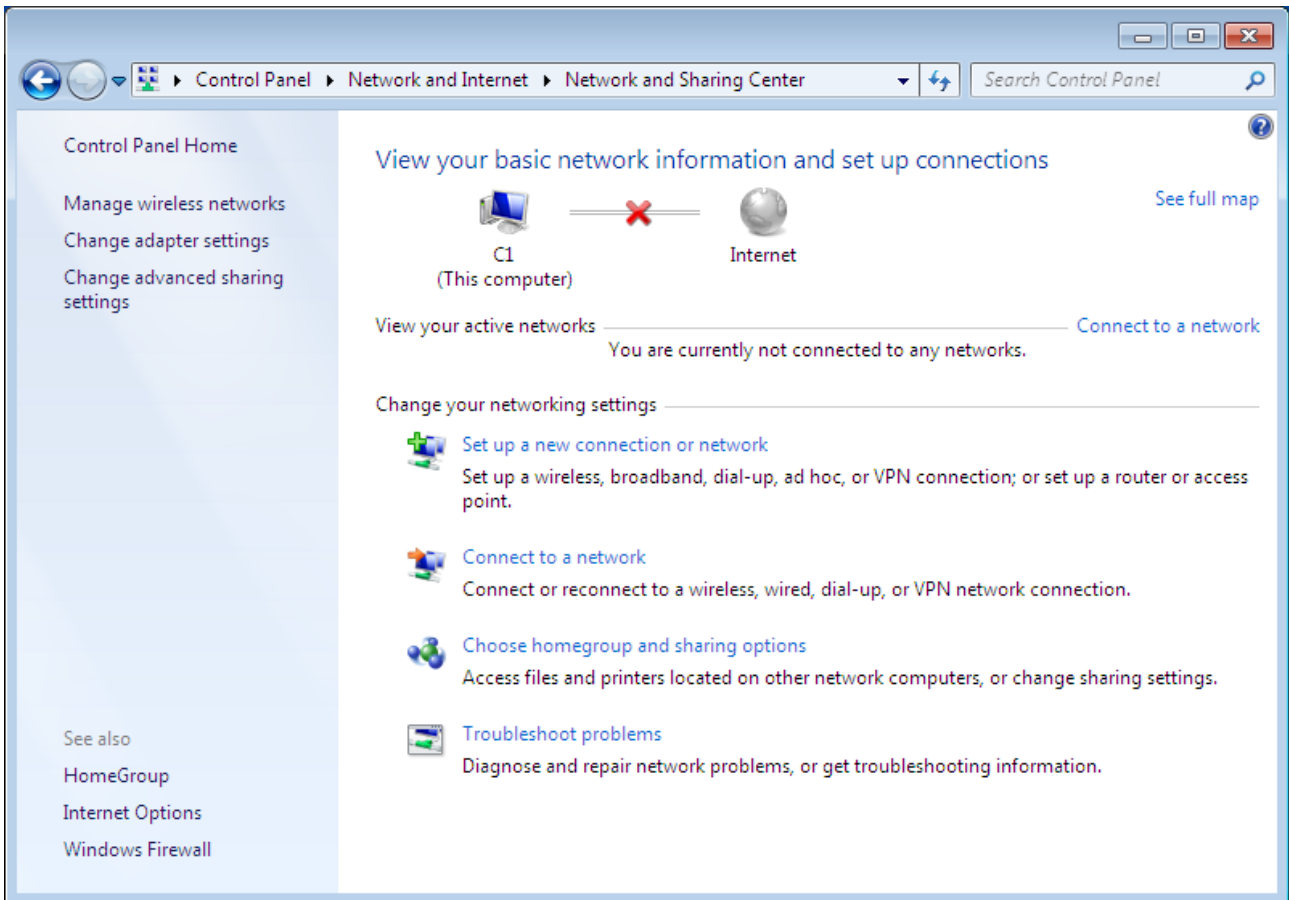

*Figure 7. The **Network and Sharing Center** window.*

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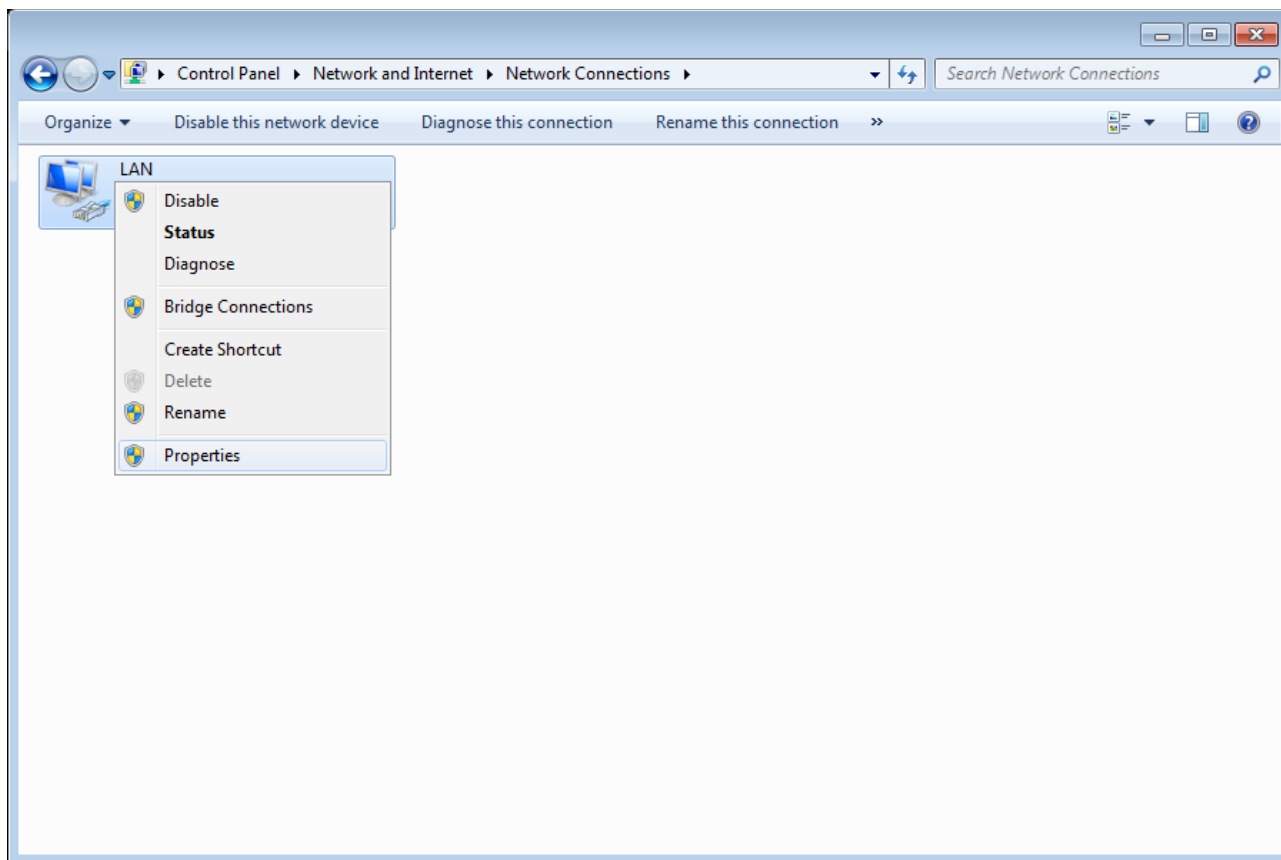

*Figure 8. The **Network Connections** window.*

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.

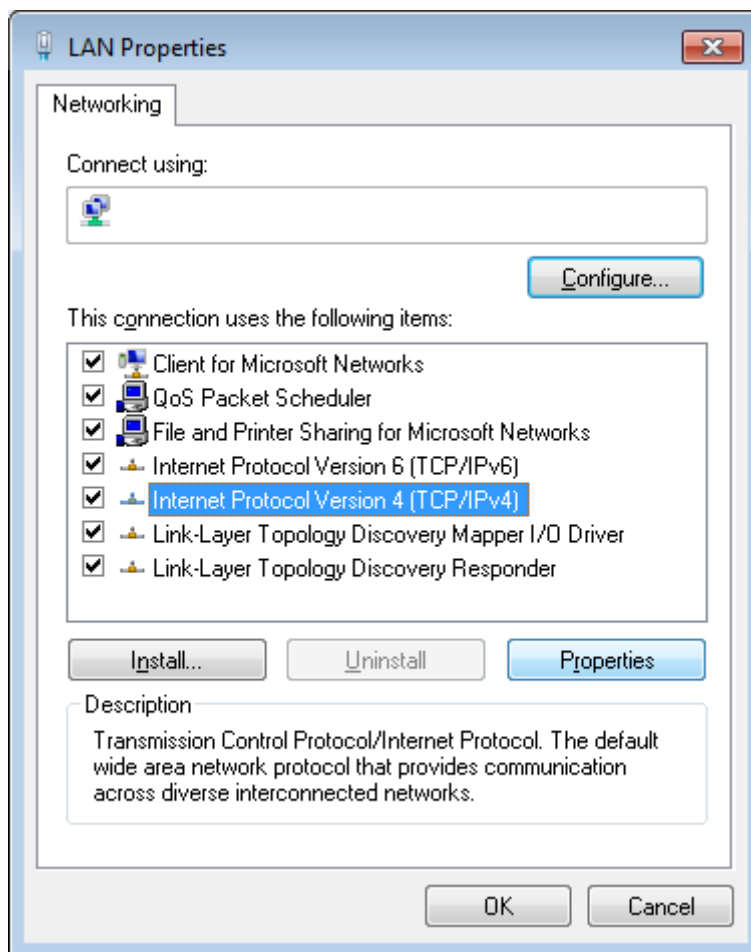*Figure 9. The **Local Area Connection Properties** window.*

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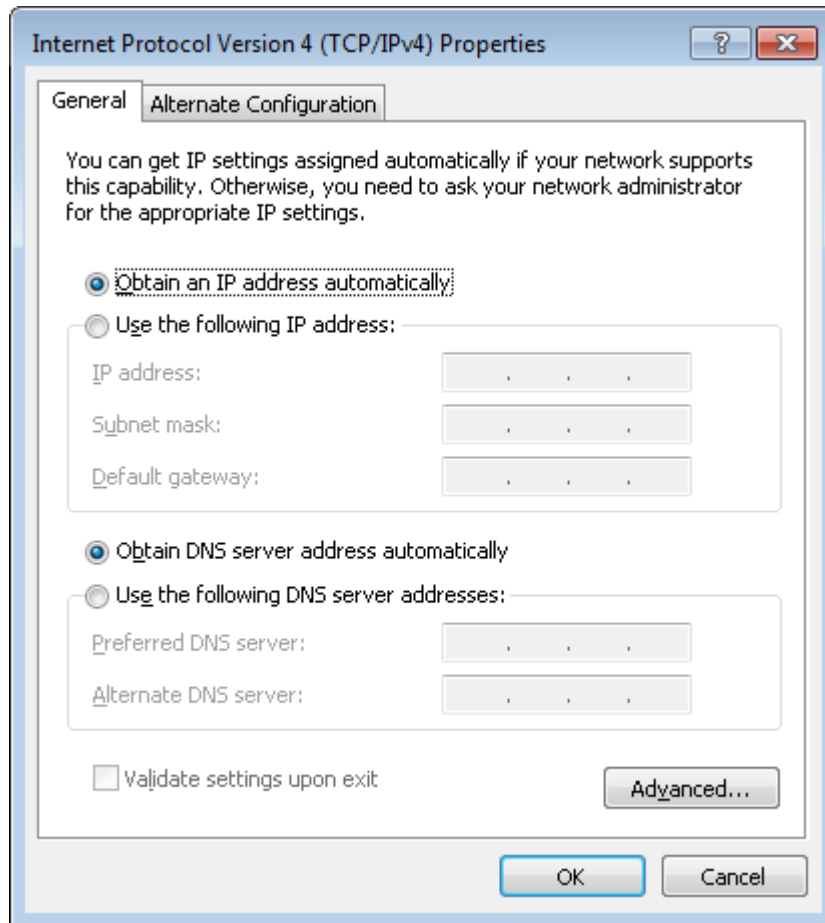

*Figure 10. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

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

PC with Wi-Fi Adapter

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

3. Turn on your PC and wait until your operating system is completely loaded.

4. Turn on your Wi-Fi adapter. 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.

Configuring Wi-Fi Adapter in OS Windows XP

1. Click the **Start** button and proceed to the **Control Panel > Network and Internet Connections > Network Connections** window.

2. Select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.
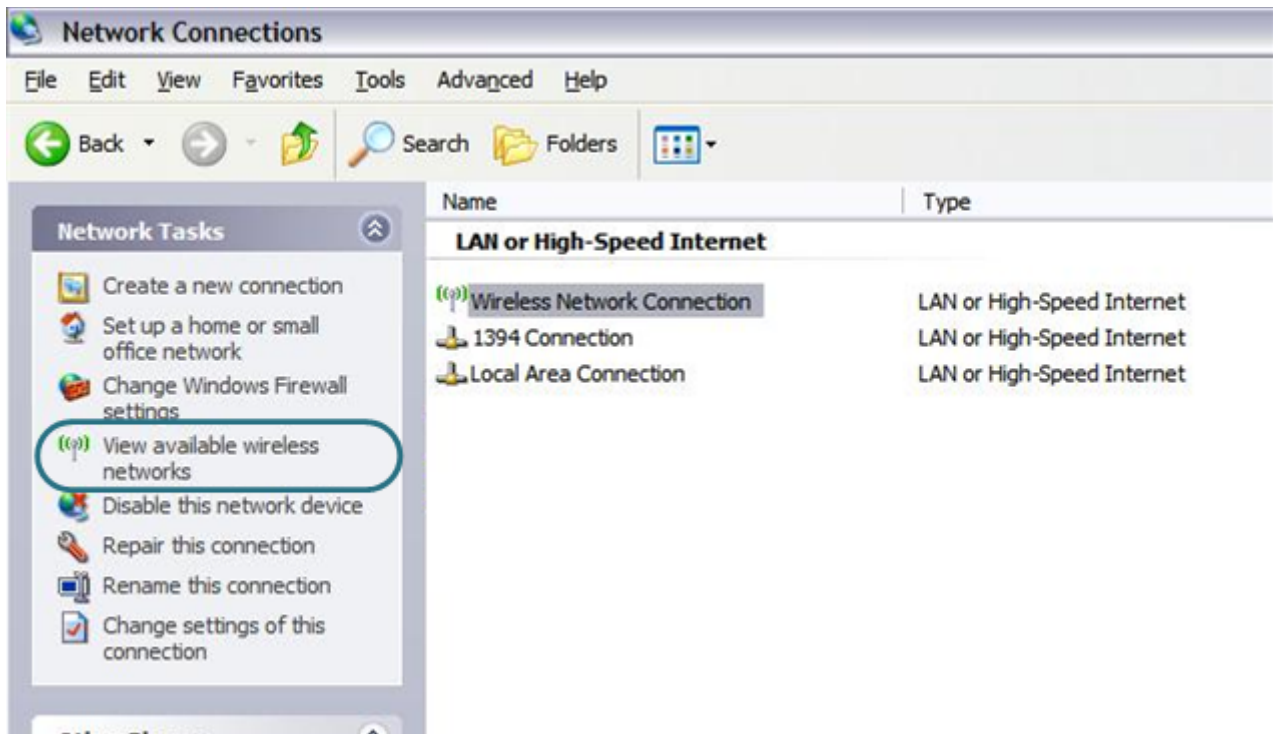
*Figure 11. The **Network Connections** window.*

3. Search for available wireless networks.

4. In the opened **Wireless Network Connection** window, select the wireless network `DIR-300` and click the **Connect** button.

5. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Network key** and **Confirm network key** fields and click the **Connect** button.

After that the **Wireless Network Connection Status** window appears.

> ! 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.

Configuring Wi-Fi Adapter in OS Windows 7

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

2. Select the **Network and Sharing Center** section. (If the Control Panel has the category view (the **Category** value is selected from the **View by** drop-down list in the top right corner of the window), choose the **View network status and tasks** line under the **Network and Internet** section.)
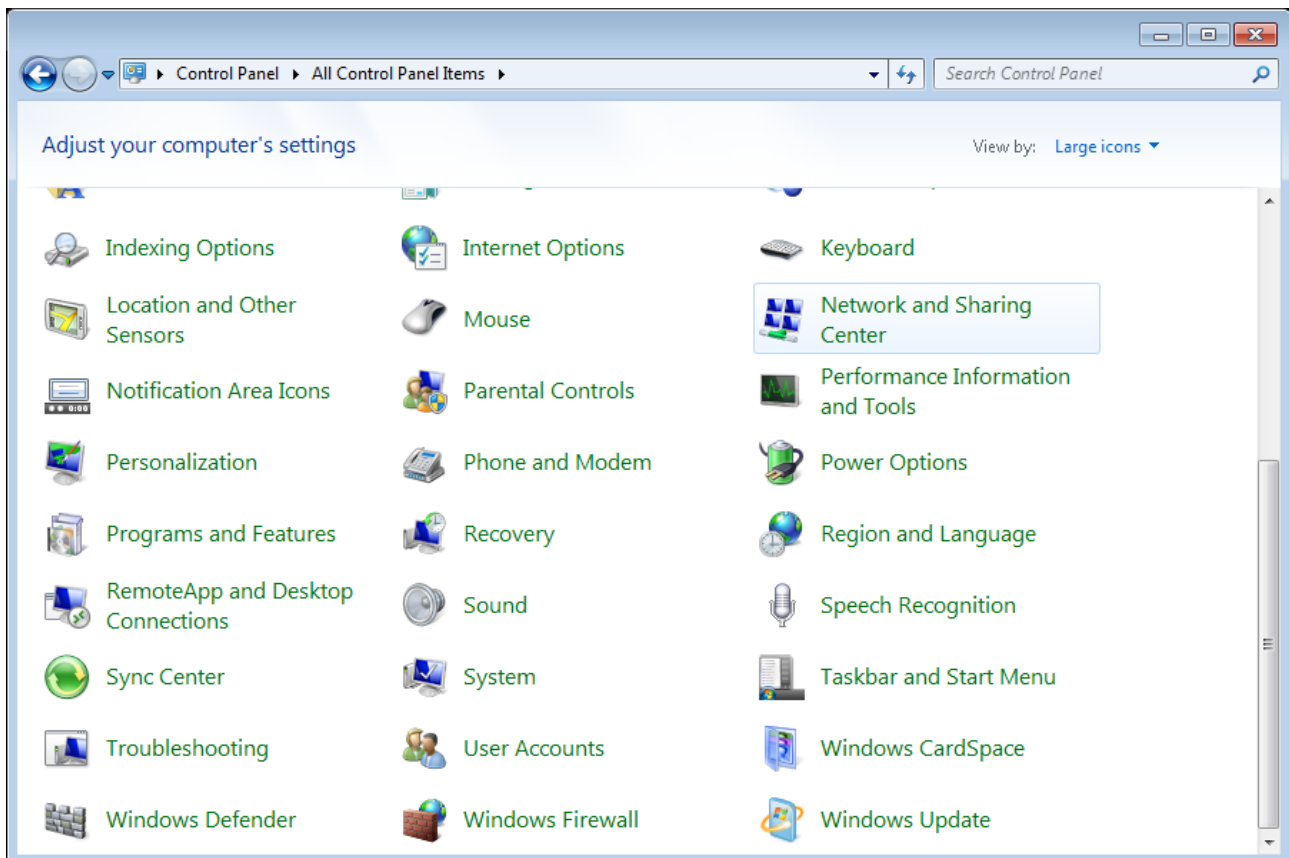
*Figure 12. The **Control Panel** window.*

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

4. In the opened window, select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.

5. 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.
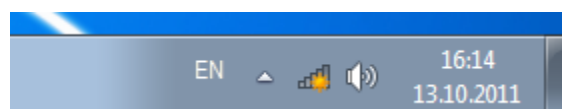
Figure 13. The notification area of the taskbar.

6. In the opened **Wireless Network Connection** window, select the wireless network `DIR-300` and click the **Connect** button.
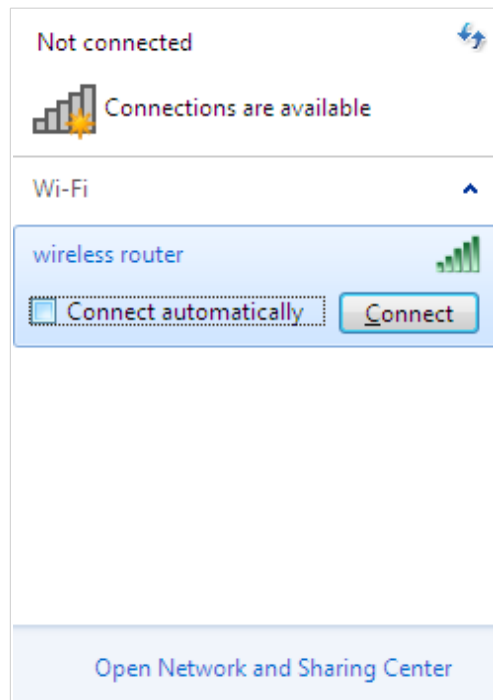
Figure 14. The list of available networks.

7. 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.

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

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

Connecting to Web-based Interface

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

> ❗ For security reasons, DIR-300S 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 13). In the address bar of the web browser, enter the IP address of the router (by default, the following IP address is specified: `192.168.0.1`). Press the **Enter** key.

Figure 15. Connecting to the web-based interface of the DIR-300S 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 34).
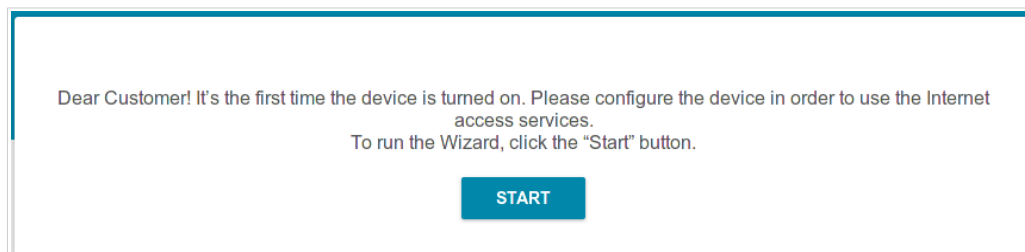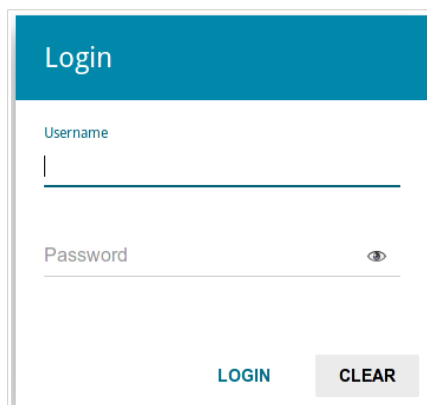
Figure 16. The page for running the Initial Configuration Wizard.

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

Figure 17. The login page.

Web-based Interface Structure

Summary Page

On the **Summary** page, detailed information on the device state is displayed.
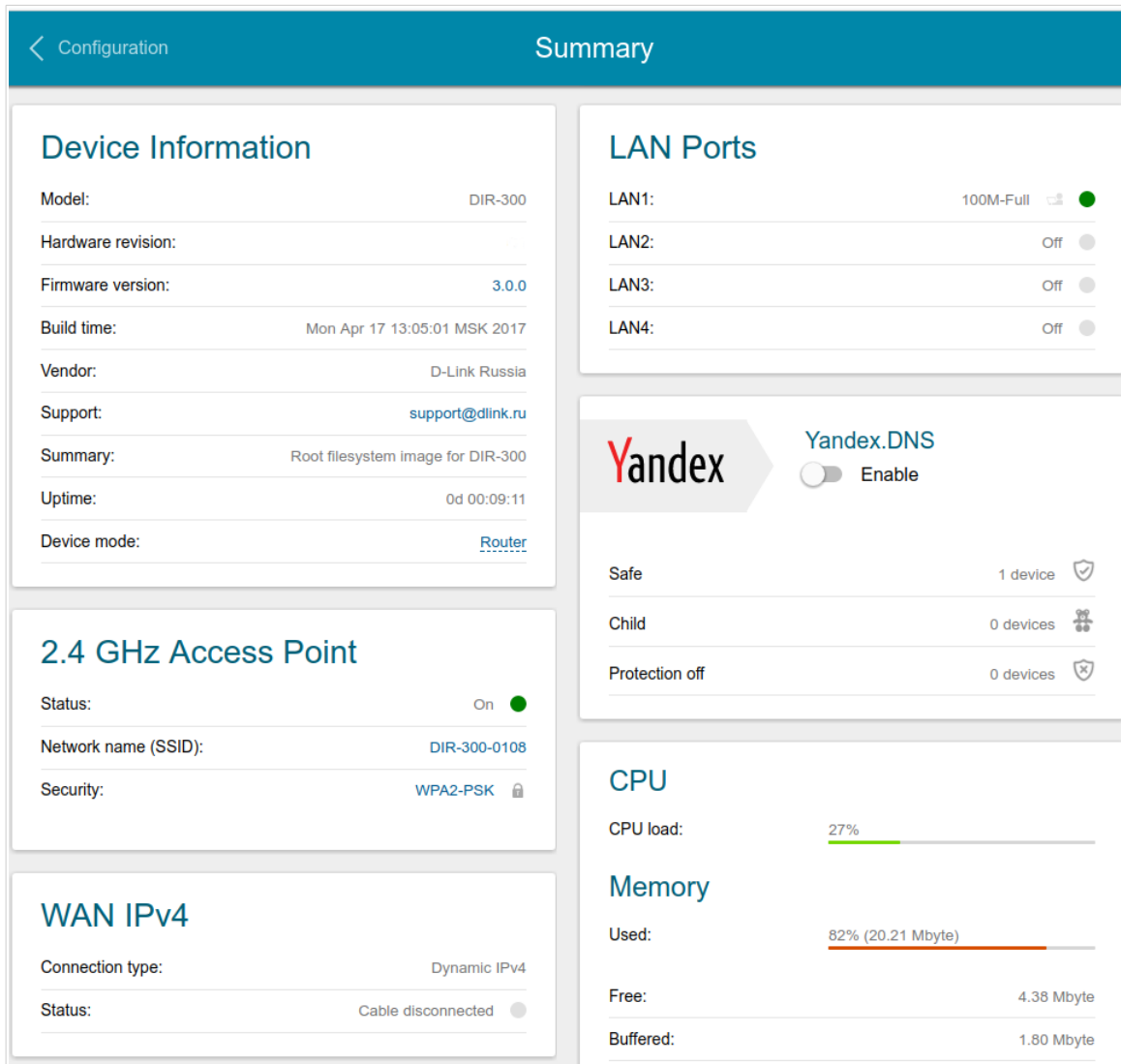
Figure 18. The summary page.

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

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

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **initial setup wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 34).

The **2.4 GHz Access Point** section displays data on the state of the device's wireless network, its name and the authentication type.

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

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

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

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

Home Page

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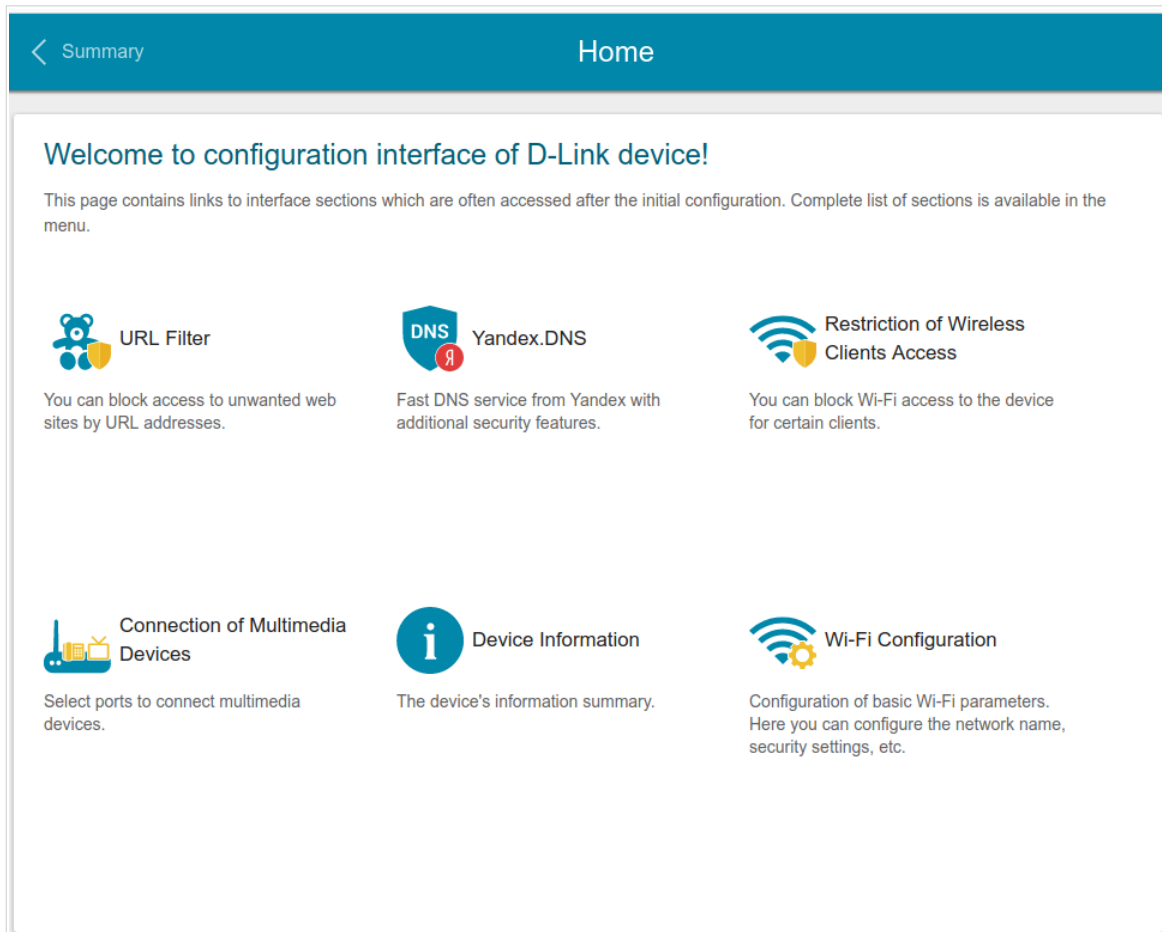

*Figure 19. The **Home** page.*

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 34).

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 58).

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 65).

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 94).

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 119).

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 142).

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 153).

The pages of the **Yandex.DNS** section are designed for configuring the Yandex.DNS web content filtering service (for the description of the pages, see the ***Yandex.DNS*** section, page 166).

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.
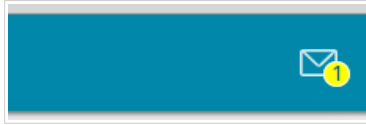
Figure 20. The web-based interface notifications.

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.

In order to run the initial setup wizard, the device should be reset to factory defaults.

CANCEL   OK
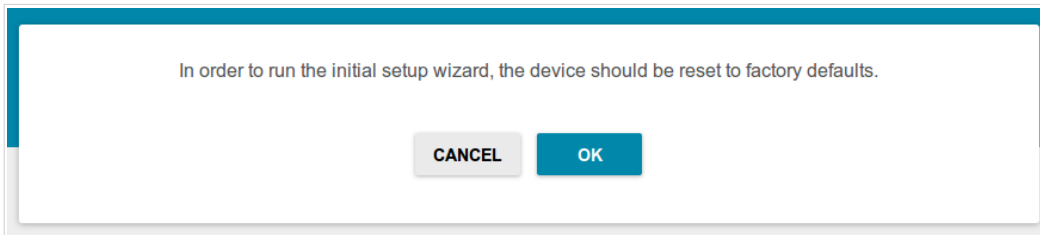
Figure 21. Restoring the default settings in the Wizard.

Click the **START** button.

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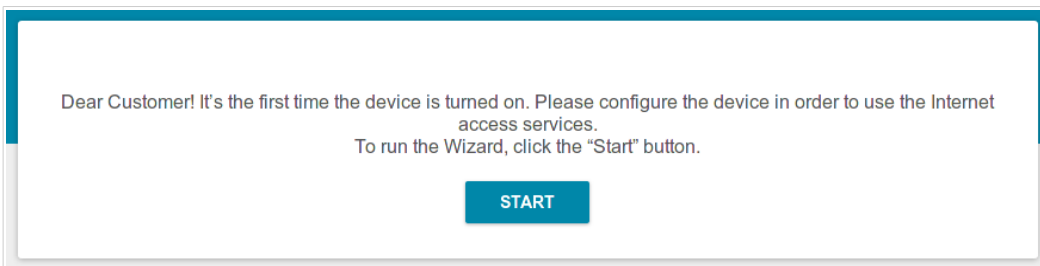
START

Figure 22. 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.

Maybe your language is English?

NO   YES
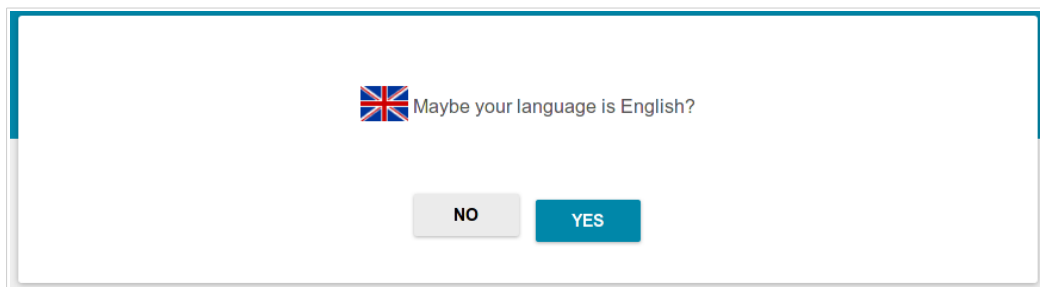
Figure 23. Selecting a language.

You can finish the wizard earlier and go to the menu of the web-based interface. To do this, click the **ADVANCED SETTINGS** button. On the opened page, change the default settings: specify the administrator password in the **Admin password** field and the name of the wireless network in the **Network name (SSID)** field. Then click the **APPLY** button.

Figure 24. Changing the default settings.

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

Selecting Operation Mode

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

*Figure 25. Selecting an operation mode. The **Router** mode.*

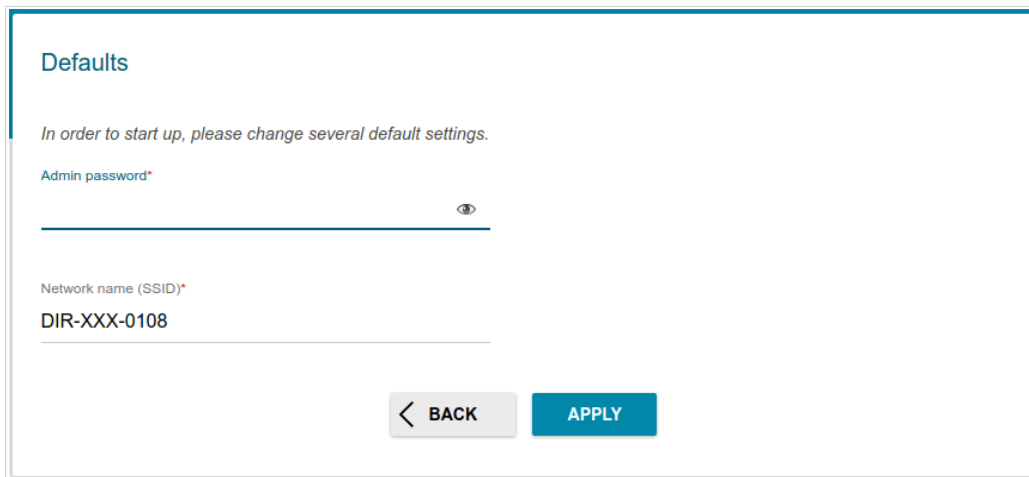In order to connect your device to a wireless ISP (WISP), on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **WISP Repeater** value. In this mode you can connect your device to another access point, configure a WAN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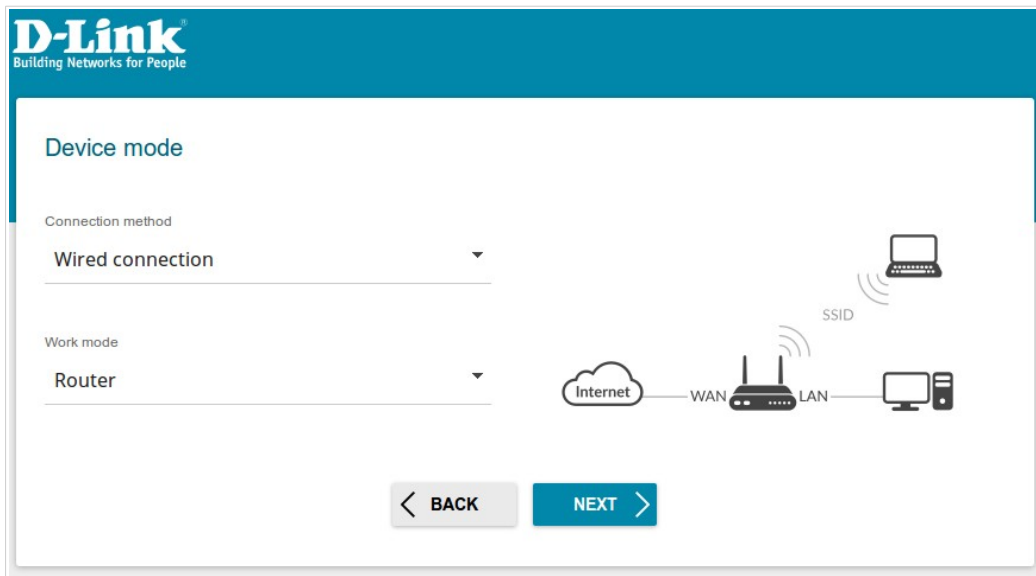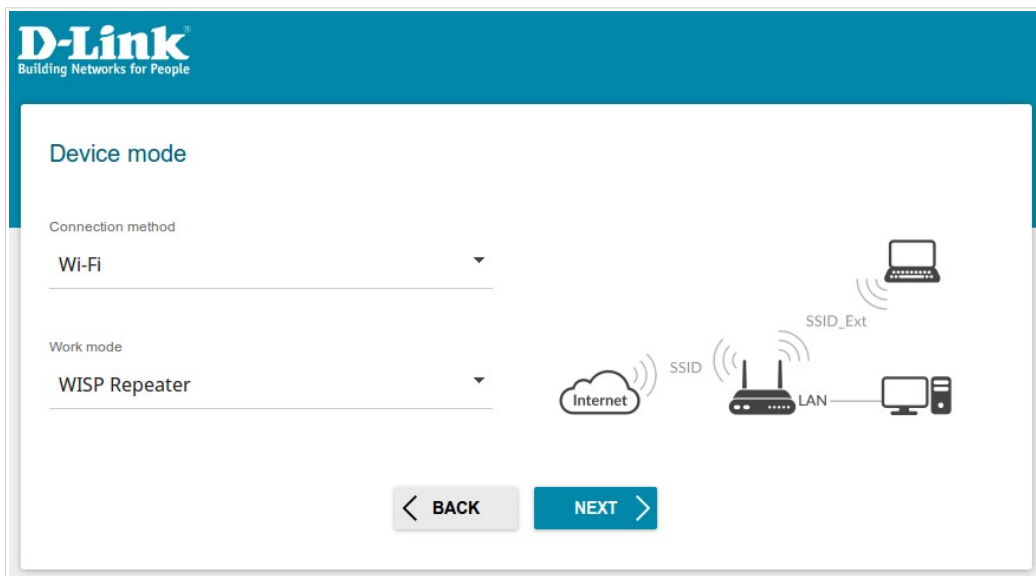

*Figure 26. Selecting an operation mode. The **WISP Repeater** mode.*

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

*Figure 27. Selecting an operation mode. The **Access point** mode.*

In order to connect your device to a wireless router for extending the range of the existing wireless network, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **Repeater** value. In this mode you can change the LAN IP address, connect your device to another access point, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.
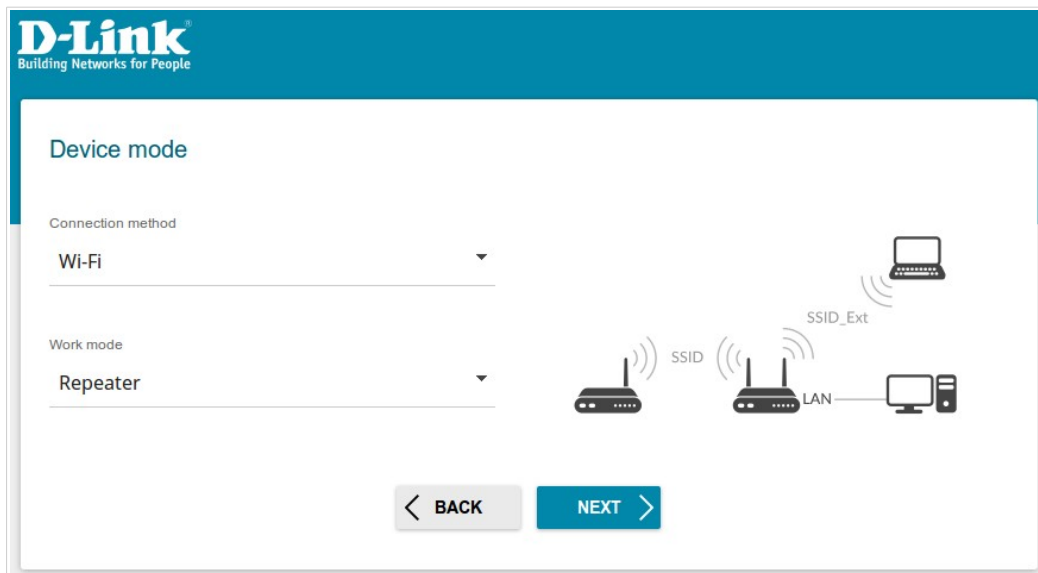
*Figure 28. Selecting an operation mode. The **Repeater** mode.*

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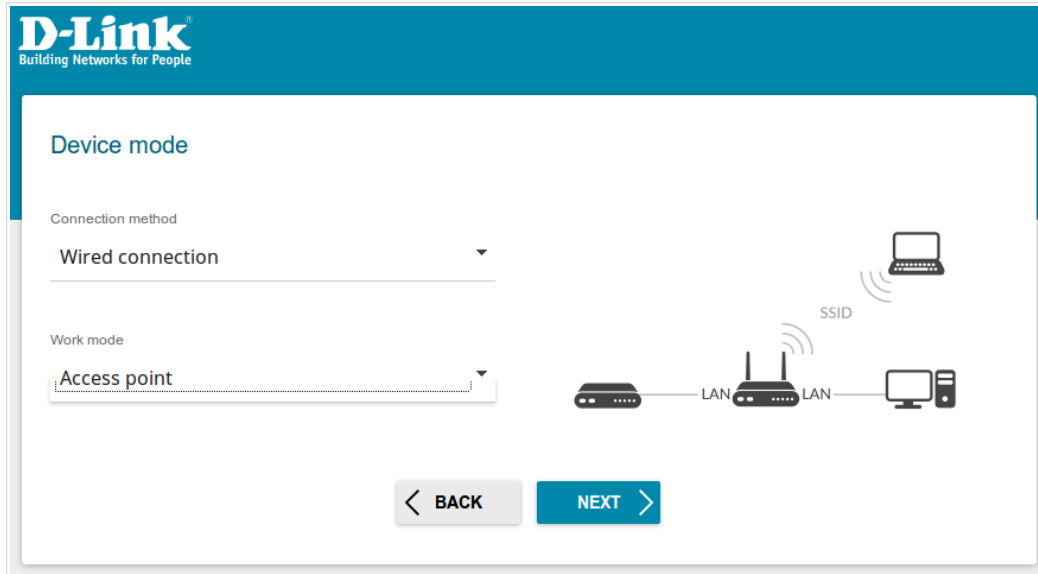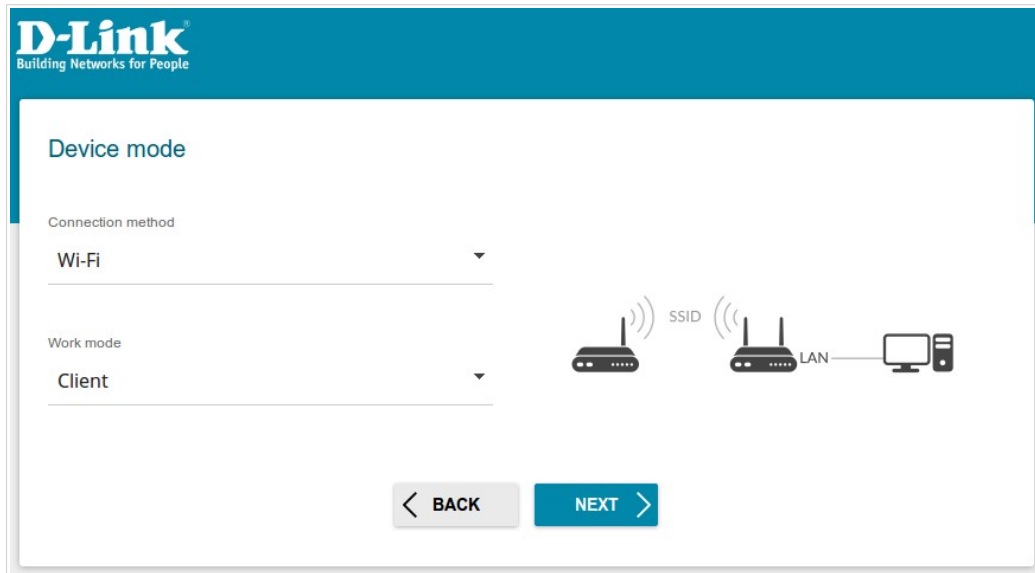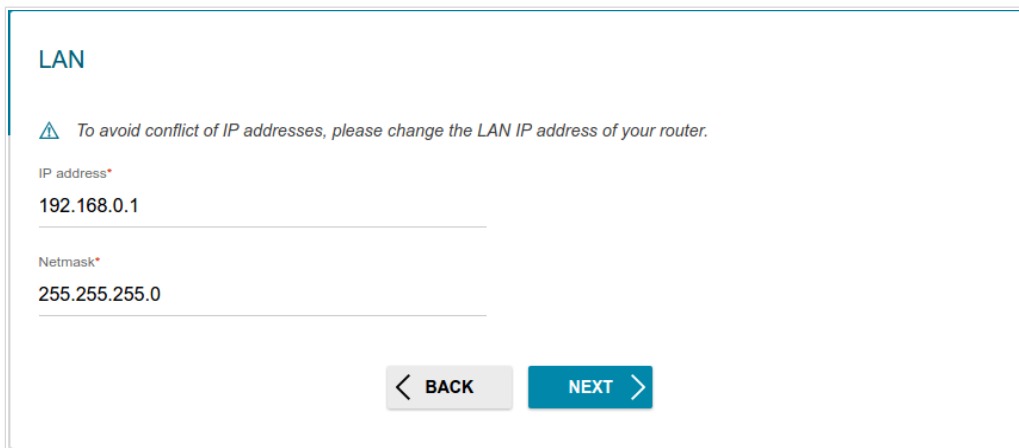

*Figure 29. Selecting an operation mode. The **Client** mode.*

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

Changing LAN IPv4 Address

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

1. If the LAN IPv4 address of DIR-300S coincides with the LAN IPv4 address of the router to which it connects, then set another LAN IPv4 address of DIR-300S in the **IP address** field.

LAN

⚠ To avoid conflict of IP addresses, please change the LAN IP address of your router.

IP address*

192.168.0.1

Netmask*

255.255.255.0

〈 BACK   NEXT 〉

Figure 30. The page for changing the LAN IPv4 address.

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

Wi-Fi Client

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

1. On the **Wi-Fi client** page, in the **Wireless Networks** section, select the network to which you want to connect. 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** button.

2. If a password is needed to connect to the selected network, fill in the relevant field.

Figure 31. The page for configuring the Wi-Fi client.

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

Figure 32. The page for configuring connection to a hidden network.

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

Creating WAN Connection

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

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

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

Static IPv4 Connection

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

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

Static IPv6 Connection

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

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

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

Figure 35. The page for configuring PPPoE WAN connection.

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

PPPoE + Static IP (PPPoE Dual Access) Connection

Figure 36. The page for configuring PPPoE + Static IP (PPPoE Dual Access) WAN connection.

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

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

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

Figure 37. The page for configuring PPTP + Dynamic IP WAN connection.

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

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

PPTP + Static IP or L2TP + Static IP Connection

Figure 38. The page for configuring PPTP + Static IP WAN connection.

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

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

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

Configuring Wireless Network

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

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

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

3. You can restore the parameters of the wireless network specified before resetting to factory defaults. To do this, click the **RESTORE** button.
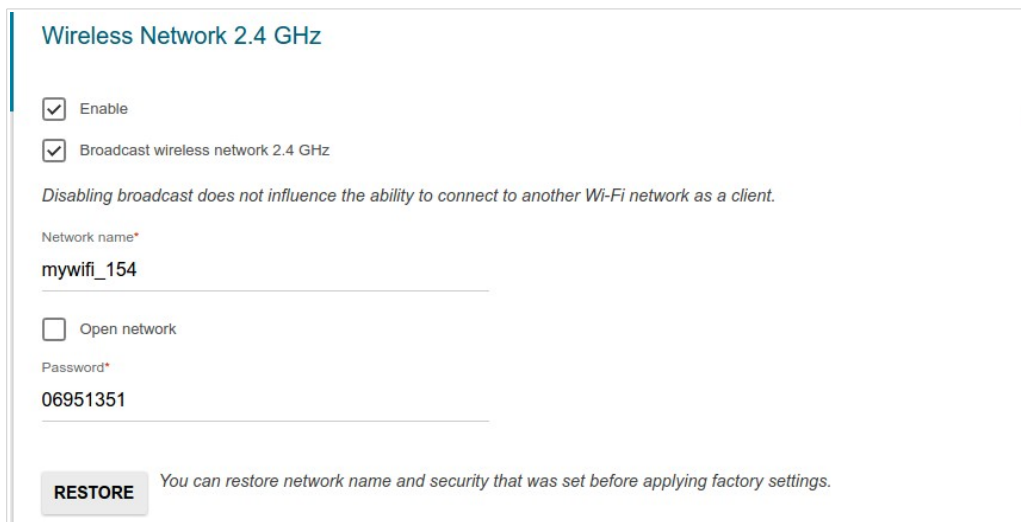
Figure 39. The page for configuring the wireless network.

4. If you want to create an additional wireless network isolated from your LAN, select the **Enable guest network** checkbox (available for the **Router** and **WISP Repeater** modes only).
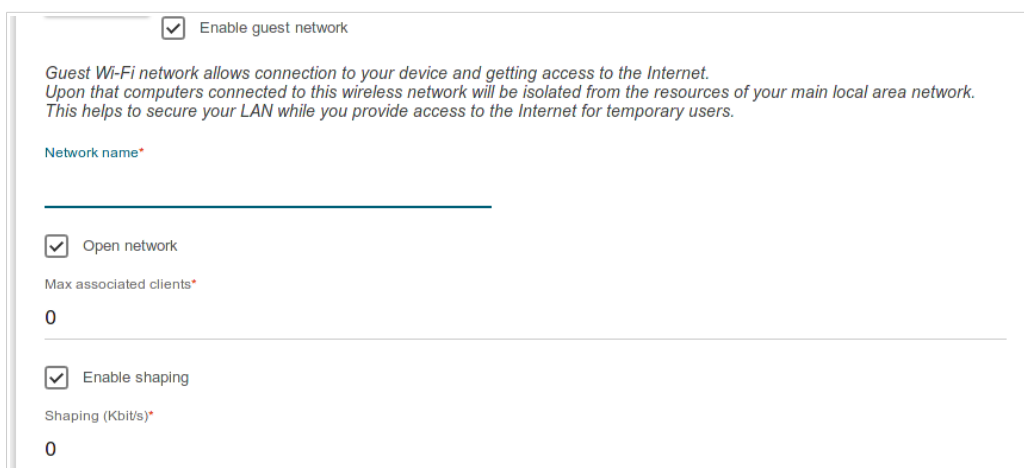
Figure 40. The page for configuring the wireless network.

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

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

7. If you want to limit the bandwidth of the guest wireless network, select the **Enable shaping** checkbox and fill in the **Shaping** field.

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

Configuring LAN Ports for IPTV/VoIP

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

1. On the **IPTV** page, select the **Is an STB connected to the device** checkbox.
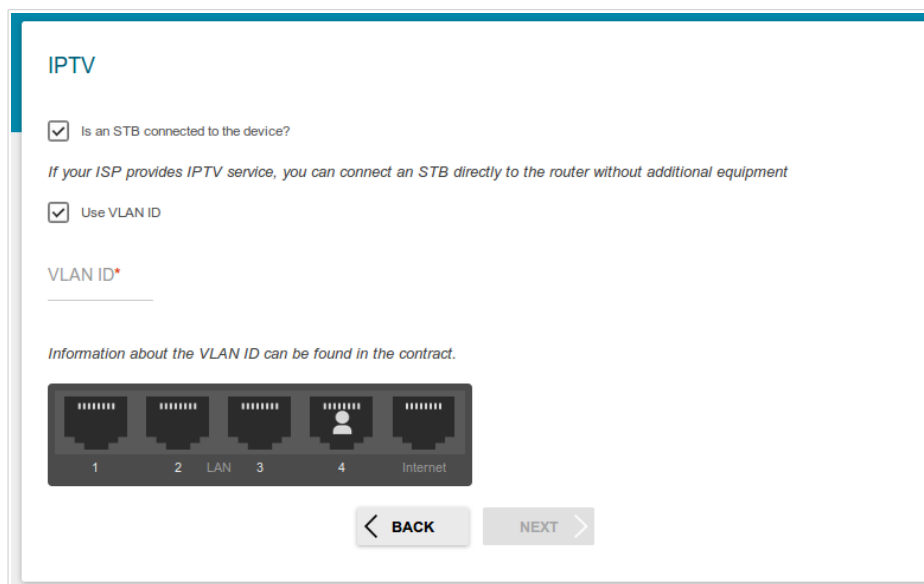
Figure 41. The page for selecting a LAN port to connect an IPTV set-top box.

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 **In an IP phone connected to the device** checkbox.
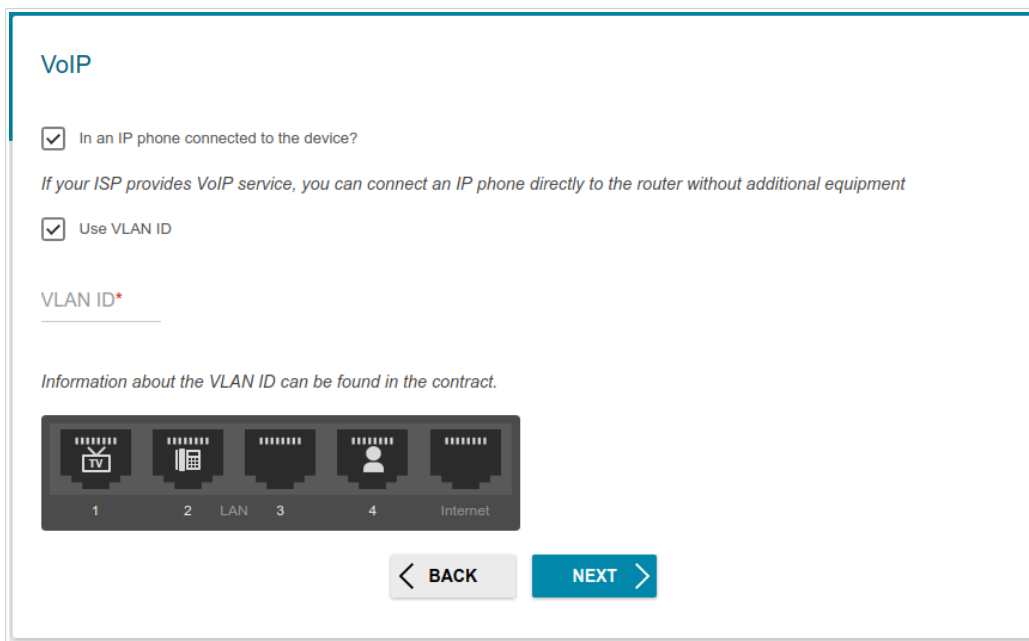
Figure 42. The page for selecting a LAN port to connect an VoIP phone.

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

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

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

Changing Web-based Interface Password

On this page, you should change the default administrator password. You may set any password except `admin`. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[1]
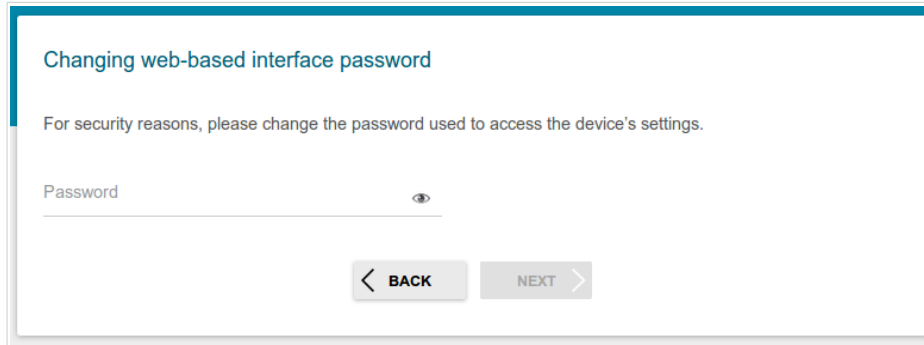
Figure 43. The page for changing the web-based interface password.

!

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.

---

1   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.

Connection to the Internet is configured and ready to use

Click "Finish" to get started on the Internet

ADVANCED SETTINGS   **FINISH**
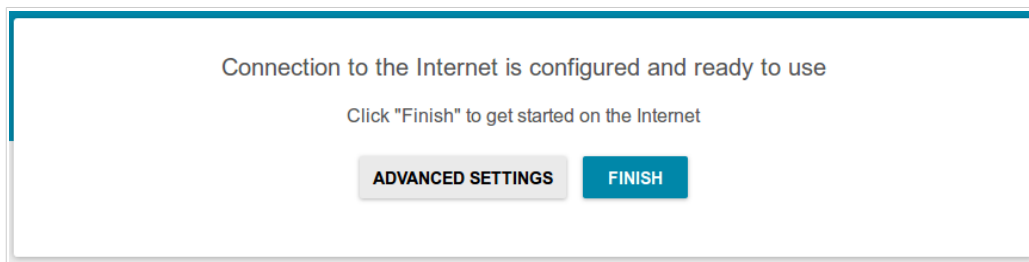
Figure 44. Checking the Internet availability.

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 **Summary** page opens (see the *Summary Page* section, page 29).

Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports or available wireless interfaces of the router for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DIR-300S 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.
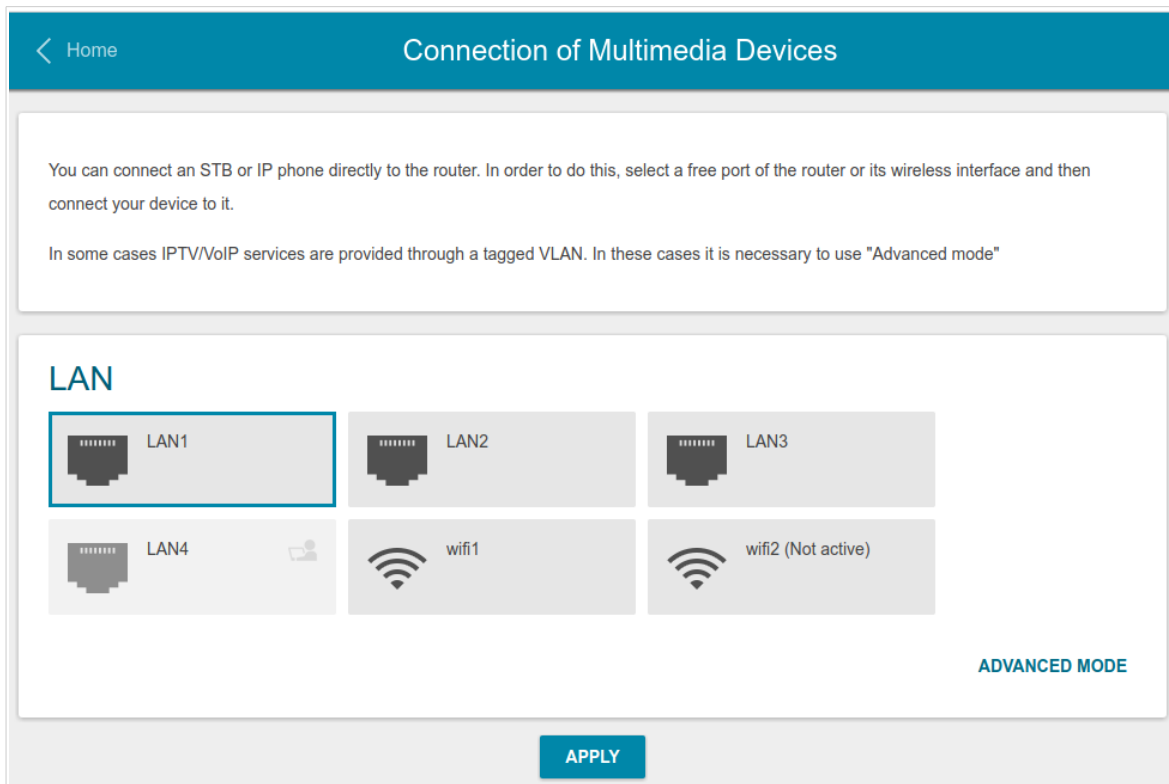
Figure 45. The Multimedia Devices Connection Wizard. The simple mode.

If you need to configure a connection via VLAN, click the **ADVANCED MODE** button.
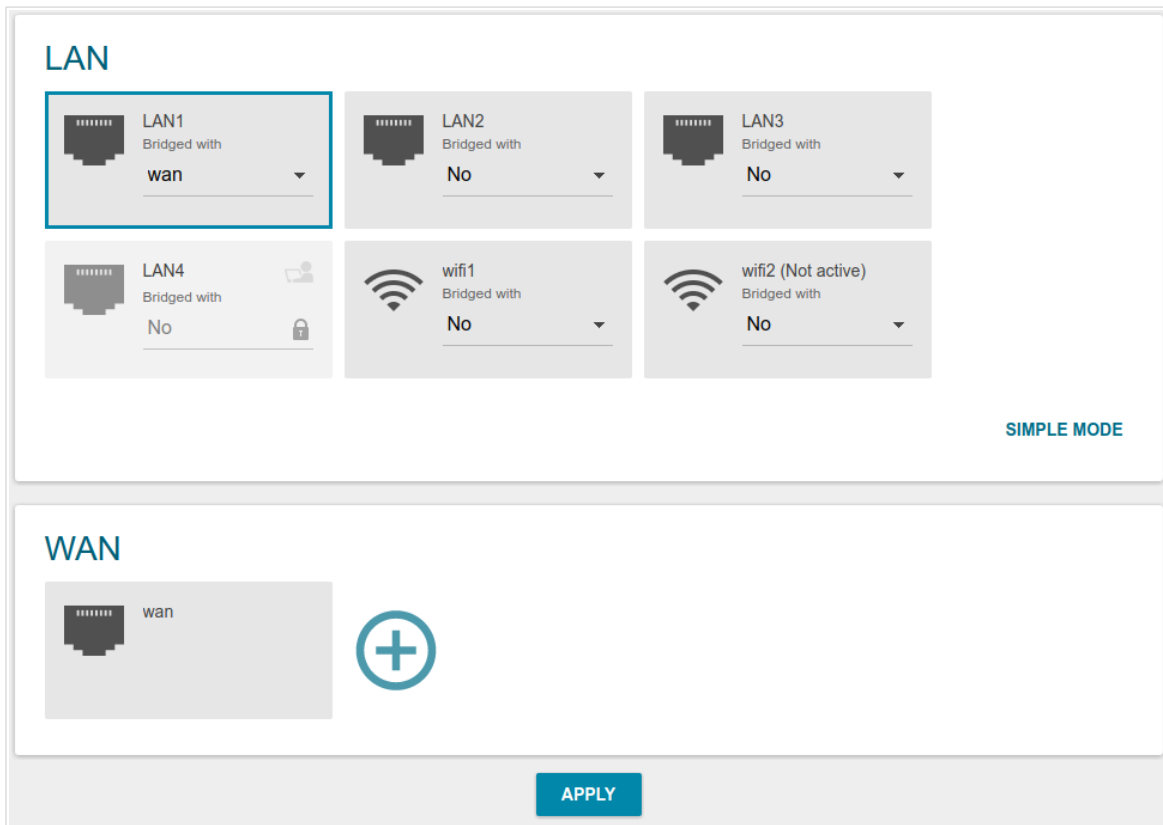
Figure 46. The Multimedia Devices Connection Wizard. The advanced mode.

In the **WAN** section, click the **Add** icon (⊕).
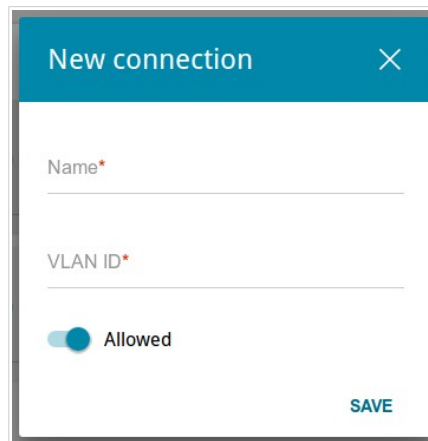
Figure 47. Adding a connection.

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

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

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

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

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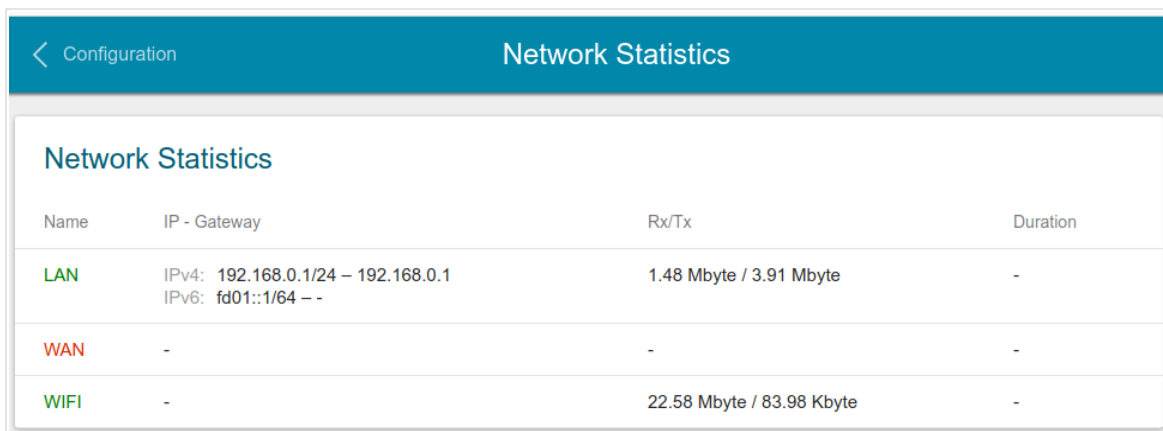
Statistics

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

- network statistics
- IP addresses leased by the DHCP server
- the routing table
- data on devices connected to the router's network and its web-based interface
- statistics for traffic passing through ports of the router
- addresses of active multicast groups
- active sessions.

Network Statistics

On the **Statistics / Network Statistics** page, you can view statistics for all connections existing in the system (WAN connections, LAN, WLAN). For each connection the following data are displayed: name and state (when the connection is on, its name is highlighted in green, when the connection is off, its name is highlighted in red), IP address and subnet mask, gateway (if the connection is established), MAC address, and volume of data received and transmitted (with increase of the volume the units of measurement are changed automatically: byte, Kbyte, Mbyte, Gbyte).
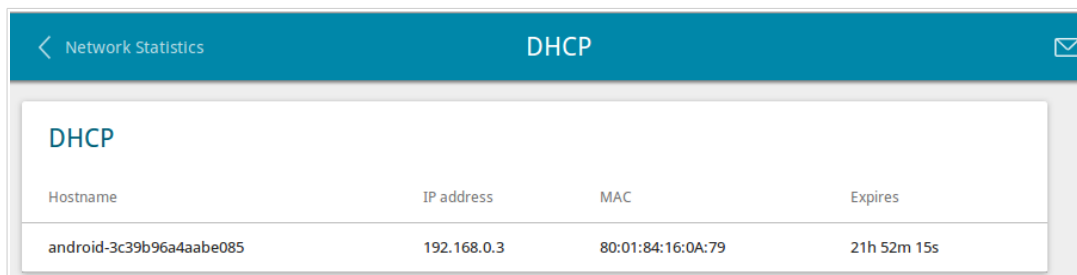
*Figure 48. The **Statistics / Network Statistics** page.*

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

DHCP

The **Statistics / DHCP** page displays the information on computers that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the device, as well as the IP address expiration periods (the lease time).
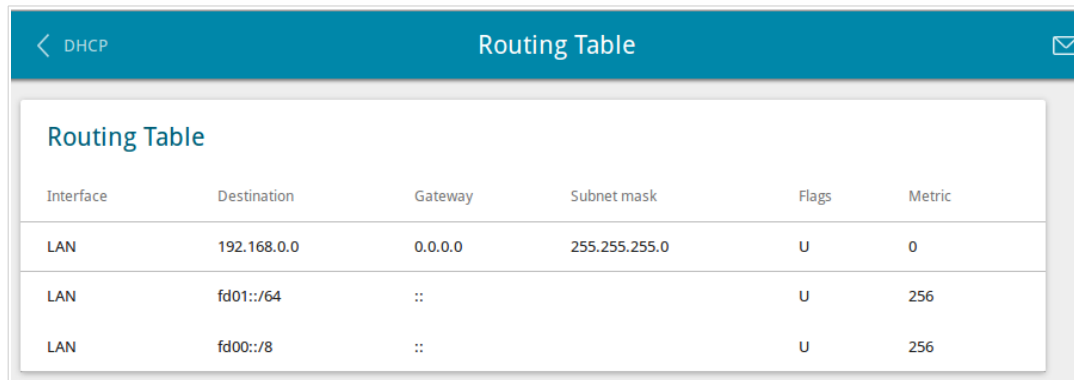
Hostname	IP address	MAC	Expires
android-3c39b96a4aabe085	192.168.0.3	80:01:84:16:0A:79	21h 52m 15s

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

Routing Table

The **Statistics / Routing Table** page displays the information on routes. The table contains destination IP addresses, gateways, subnet masks, and other data.
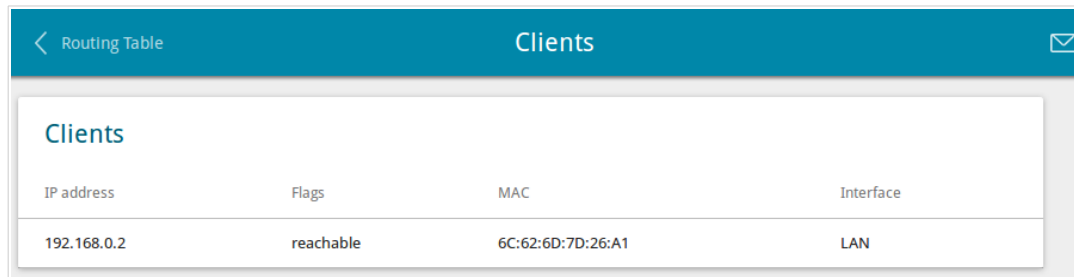
Interface	Destination	Gateway	Subnet mask	Flags	Metric
LAN	192.168.0.0	0.0.0.0	255.255.255.0	U	0
LAN	fd01::/64	::		U	256
LAN	fd00::/8	::		U	256

*Figure 50. The **Statistics / Routing Table** page.*

Clients

On the **Statistics / Clients** page, you can view the list of devices connected to the local network of the router.
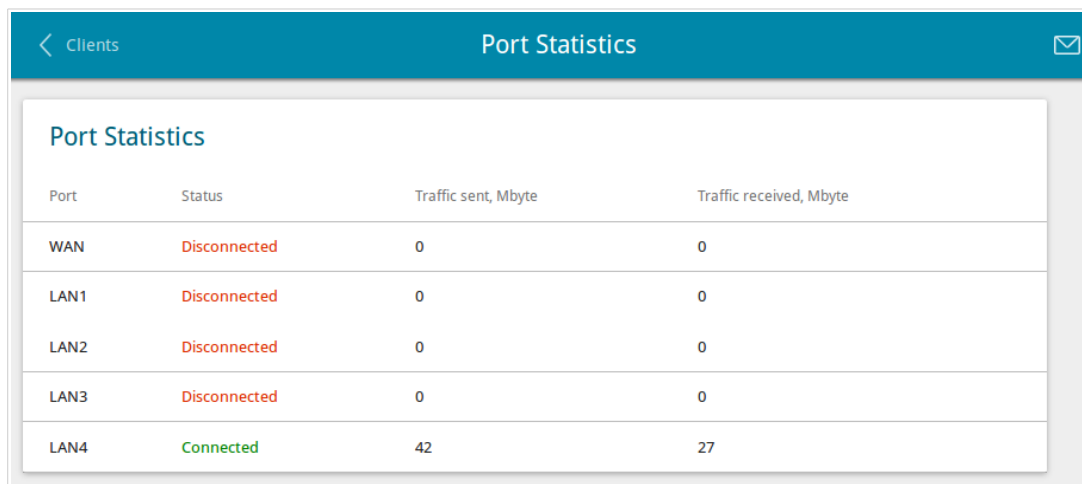
*Figure 51. The **Statistics / Clients** page.*

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

Port Statistics

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

*Figure 52. The **Statistics / Port Statistics** page.*

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

Multicast Groups

The **Statistics / Multicast Groups** page displays addresses of active multicast groups (including IPTV channels and groups for transferring service information) to which the device is subscribed, and the interface through which the device is subscribed.
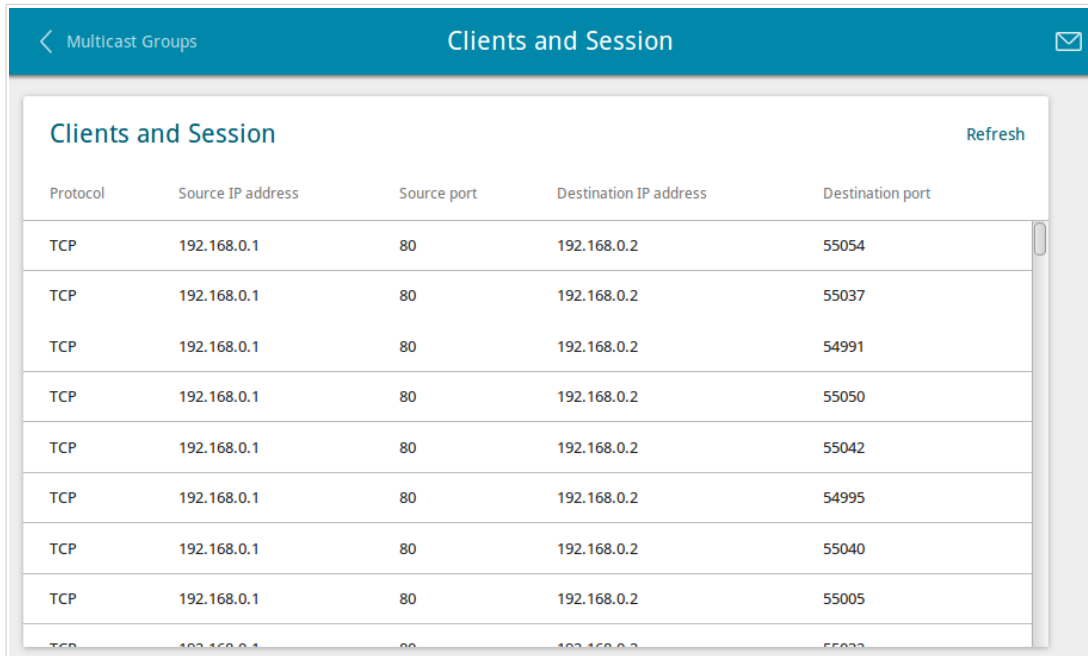
*Figure 53. The **Statistics / Multicast Groups** page.*

Clients and Session

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

*Figure 54. The **Statistics / Clients and Session** page.*

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

Connections Setup

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

WAN

On the **Connections Setup / WAN** page, you can create and edit connections used by the router.

By default, a **Dynamic IPv4** connection is configured in the system. It is assigned to the WAN port of the router. You can edit this connection or delete it.
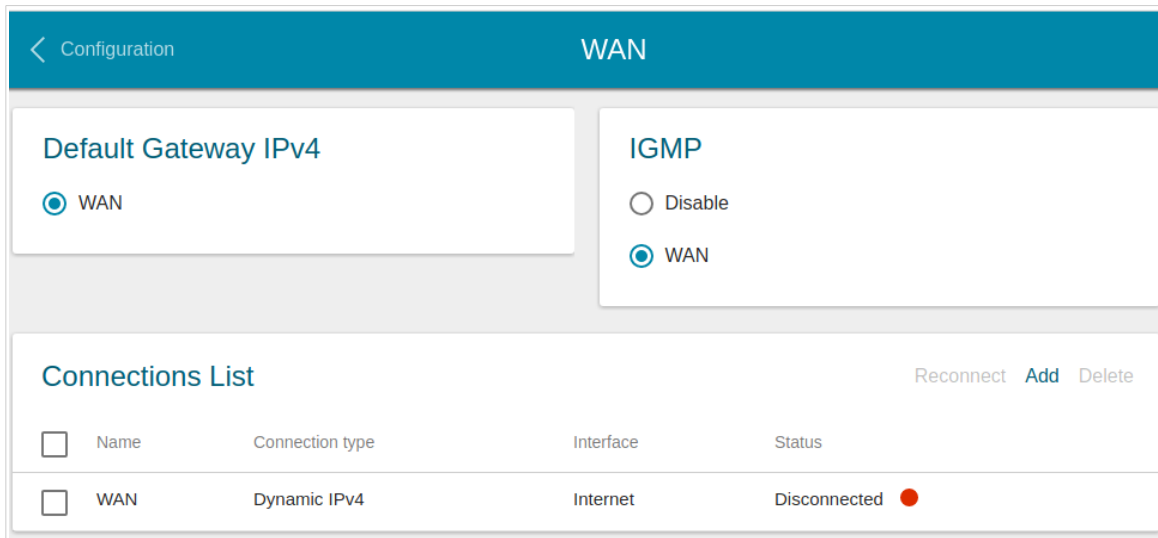
*Figure 55. The **Connections Setup / WAN** page.*

To create a new connection, click the **Add** button in the **Connections List** section. On the opened page, specify relevant parameters.

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

On the **Basic** tab, mandatory settings of a WAN connection are displayed. To view all available settings of the needed WAN connection, go to the **All Settings** tab.

To remove a connection, in the **Connections List** section, select the checkbox located to the left of the relevant line in the table and click the **Delete** button. Also you can remove a connection on the editing page.
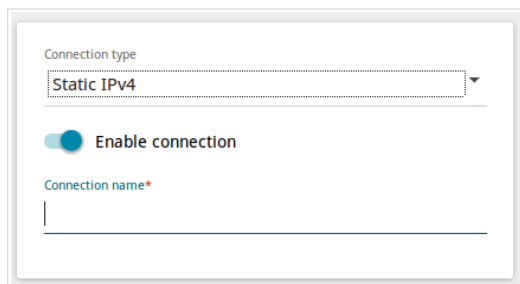
To allow multicast traffic (e.g. streaming video) for a connection, in the **IGMP** section, select the choice of the radio button which corresponds to this connection (only for connections of the Dynamic IPv4 or Static IPv4 type).

To forbid multicast traffic for all WAN connections, select the **Disable** choice of the radio button.

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.

Creating Dynamic IPv4 or Static IPv4 WAN Connection

To create a connection of the Dynamic IPv4 or Static IPv4 type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.

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

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

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

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

*Figure 58. The page for creating a new **Static IPv4** connection. The **IPv4** section.*

Parameter	Description
IPv4	
*For **Static IPv4** type*	
IP Address	Enter an IP address for this WAN connection.
Netmask	Enter a subnet mask for this WAN connection.
Gateway IP address	Enter an IP address of the gateway used by this WAN connection.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
*For **Dynamic IPv4** type*	
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the **Primary DNS server** and **Secondary DNS server** fields are not available for editing.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. *Optional*.
Host name	A name of the router specified by your ISP. *Optional*.
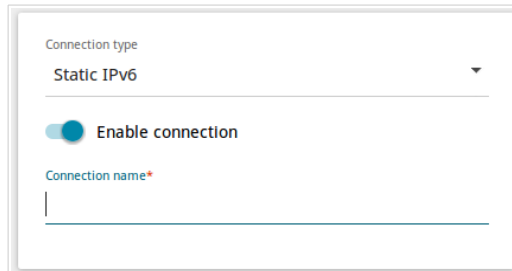
*Figure 59. The page for creating a new **Static IPv4** connection. The **Miscellaneous** section.*

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

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

Creating Dynamic IPv6 or Static IPv6 WAN Connection

To create a connection of the Dynamic IPv6 or Static IPv6 type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.

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

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.
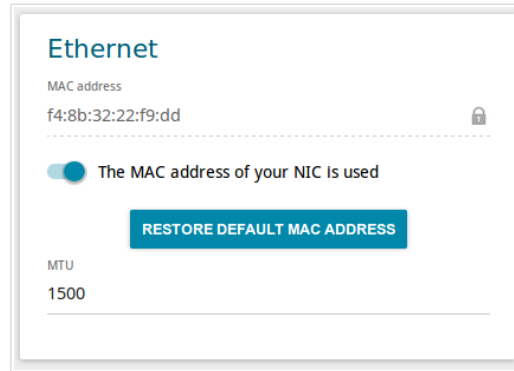
*Figure 61. The page for creating a new **Static IPv6** connection. The **Ethernet** section.*

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

*Figure 62. The page for creating a new **Static IPv6** connection. The **IPv6** section.*

Parameter	Description
IPv6	
*For **Static IPv6** type*	
IPv6 address	Enter an IPv6 address for this WAN connection.
Prefix	The length of the subnet prefix. The value 64 is used usually.
Gateway IPv6 address	Enter an IPv6 address of the gateway used by this WAN connection.
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
*For **Dynamic IPv6** type*	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (*Stateless Address Autoconfiguration*).
Gateway IPv6 address	The address of the IPv6 gateway. The field is available for editing, if the **Gateway by SLAAC** switch is moved to the left.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the **Primary IPv6 DNS server** and **Secondary IPv6 DNS server** fields are not available for editing.

Parameter	Description
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
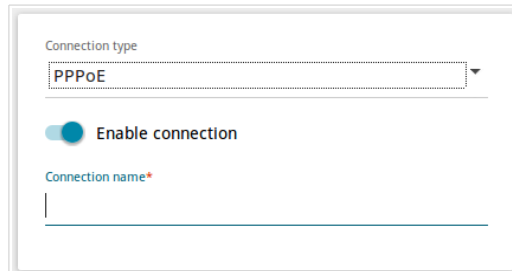
*Figure 63. The page for creating a new **Static IPv6** connection. The **Miscellaneous** section.*

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

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

Creating PPPoE WAN Connection

To create a connection of the PPPoE type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.

*Figure 64. The page for creating a new **PPPoE** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.
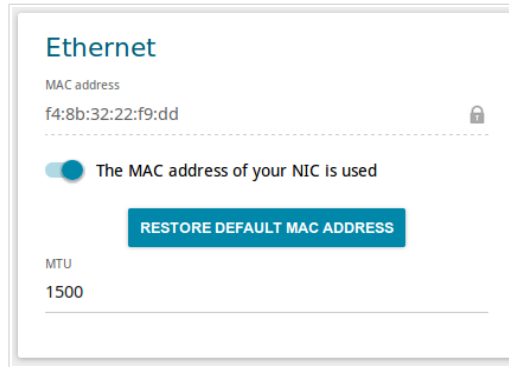
*Figure 65. The page for creating a new **PPPoE** connection. The **Ethernet** section.*

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

*Figure 66. The page for creating a new **PPPoE** connection. The **PPP** section.*

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

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

*Figure 67. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.*

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

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

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

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

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

Creating PPTP or L2TP WAN Connection

To create a connection of the PPTP or L2TP type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.

*Figure 68. The page for creating a new **PPTP** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

*Figure 69. The page for creating a new **PPTP** connection. The **PPP** section.*

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

Parameter	Description
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Encryption protocol	Select a method of MPPE encryption. • **No encryption**: MPPE encryption is not applied. • **MPPE 40/128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied. • **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied. • **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the **MS-CHAP, MS-CHAPV2**, or **AUTO** value is selected from the **Authentication protocol** drop-down list.
Keep Alive	Move the switch to the right if you want the router to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the **Maximum idle time** field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Extra options	Advanced options of the pppd daemon which need to be specified for this connection. *Optional*.
Static IP Address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

*Figure 70. The page for creating a new **PPTP** connection. The **Miscellaneous** section.*

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

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

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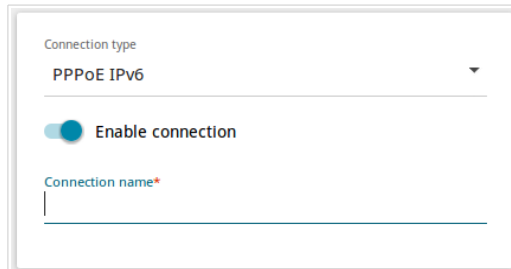
If you want to use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select the existing connection which will be used to access the PPTP/L2TP server or select the **create a new connection** choice of the radio button.

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

Click the **OK** button.

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

To create a connection of the PPPoE IPv6 or PPPoE Dual Stack type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.

*Figure 71. The page for creating a new **PPPoE IPv6** connection. Selecting a connection type.*

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

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

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

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

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

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

*Figure 74. The page for creating a new **PPPoE Pv6** connection. The **IP** section.*

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

*Figure 75. The page for creating a new **PPPoE IPv6** connection. The **Miscellaneous** section.*

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

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

LAN

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

IPv4

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

*Figure 76. Configuring the local interface. The I**Pv4** tab. The **IP** section.*
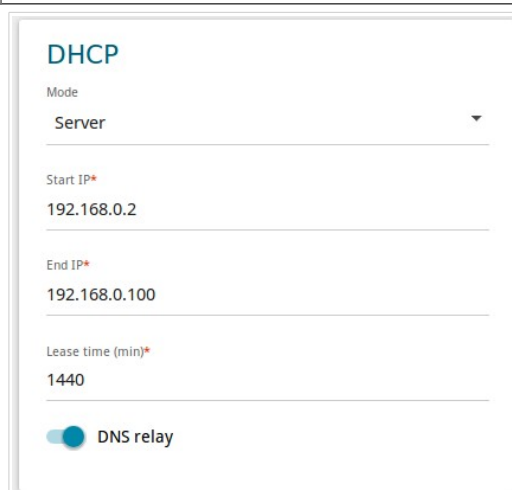
Parameter	Description
IP	
IP Address	The IP address of the router in the local subnet. By default, the following value is specified: `192.168.0.1`.
Netmask	The mask of the local subnet. By default, the following value is specified: `255.255.255.0`.
Device domain name	The name of the device attached to its IP address in the local subnet.

*Figure 77. Configuring the local interface. The I**Pv4** tab. The **DHCP** section.*

Parameter	Description
DHCP	
Mode	An operating mode of the router's DHCP server. **Server**: the router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the **Start IP**, **End IP**, **Lease time** fields and the **DNS Relay** switch are displayed on the tab. **Disable**: the router's DHCP server is disabled, clients' IP addresses are assigned manually. **Relay**: an external DHCP server is used to assign IP addresses to clients. When this value is selected, the **External DHCP server IP** field is displayed on the tab.
Start IP	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
DNS Relay	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the **Advanced / DNS** page as the DNS server address.
External DHCP server IP	The IP address of the external DHCP server which assigns IP addresses to the router's clients.

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

In the **Static DHCP** section, you can specify MAC address and IP address pairs (set a fixed IPv4 address in the local area network for a device with a certain MAC address). The router assigns IP addresses in accordance with the specified pairs only when the DHCP server is enabled (in the **DHCP** section, the **Server** value is selected from the **Mode** drop-down list).
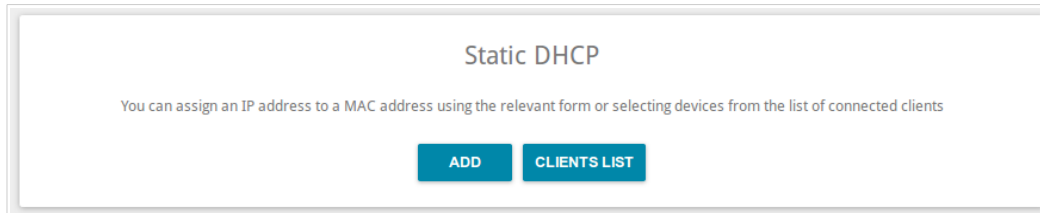
Figure 78. The section for creating MAC-IP pairs.

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

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

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

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

IPv6

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

Figure 79. Configuring the local interface. The IPv4 tab. The IP section.

Parameter	Description
IP	
Addressing Mode	Select the needed value from the drop-down list. **Static**: an IPv6 address and a prefix are specified manually. **Prefix delegation**: the router requests a prefix to configure an IPv6 address from a delegating router.
IP address	The IPv6 address of the router in the local subnet. By default, the following value is specified: `fd01::1`. The field is available for editing, if the **Static** value is selected from the **Addressing Mode** drop-down list.
Prefix	The length of the prefix subnet. By default, the value `64` is specified. The field is available for editing, if the **Static** value is selected from the **Addressing Mode** drop-down list.
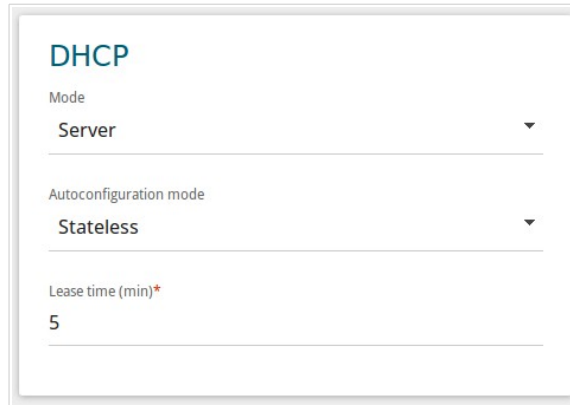
Figure 80. Configuring the local interface. The IPv6 tab. The DHCP section.

Parameter	Description
DHCP	
Mode	Select a mode of IPv6 address assignment from the drop-down list. **Server**: the router assigns IPv6 addresses to clients automatically in accordance with the specified parameters. When this value is selected, the **Autoconfiguration mode** drop-down list and the **Lease time** field are displayed on the tab. **Disable**: clients' IPv6 addresses are assigned manually.
Autoconfiguration mode	Select a mode from the drop-down list. **Stateless**: clients themselves configure IPv6 addresses using the prefix. **Stateful**: the built-in DHCPv6 server of the router allocates addresses from the range specified in the **Start IP** and **End IP** fields.
Start IP	The start IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
End IP	The end IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
Lease Time	The lifetime of IPv6 addresses provided to clients. The field is available for editing, if the **Static** value is selected from the **Addressing mode** list in the **IP** section.

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

Wi-Fi

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

Basic Settings

In the **Wi-Fi / Basic Settings** section, you can change basic parameters for the wireless interface of the router and configure the basic and additional wireless networks.
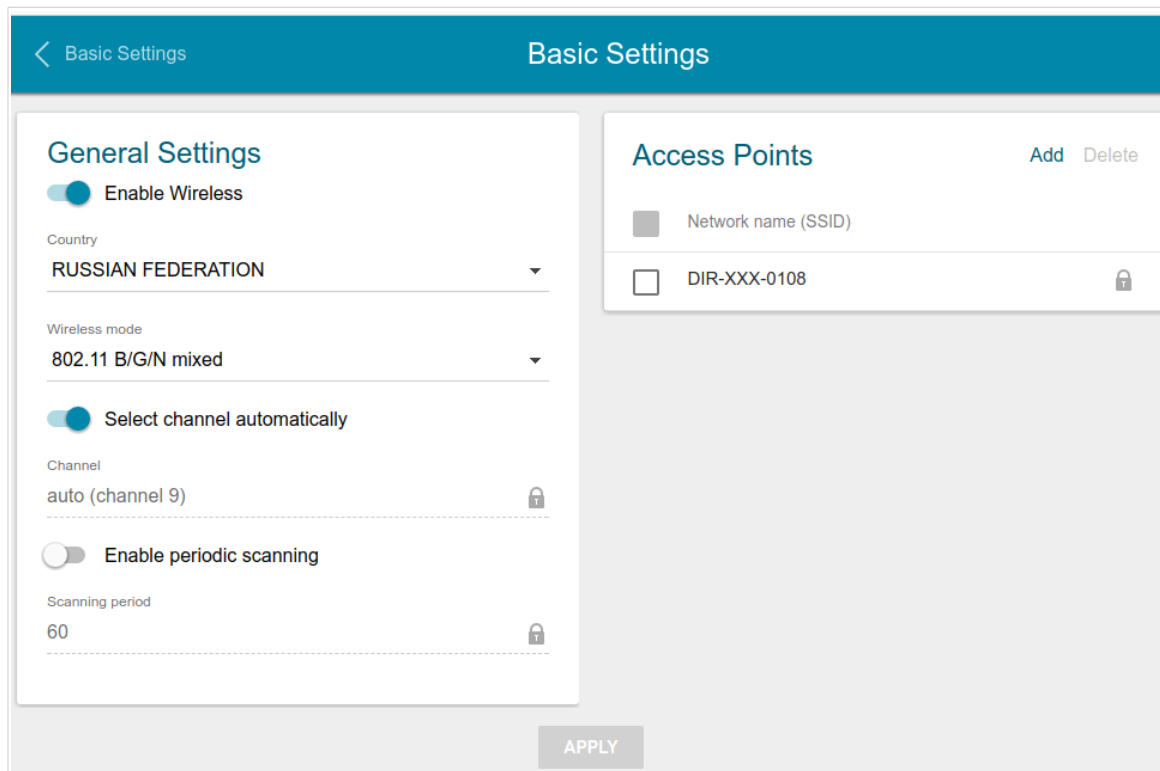
Figure 81. Basic settings of the wireless LAN.

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

Parameter	Description
Enable Wireless	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left.
Country	The country you are in. Select a value from the drop-down list.
Wireless mode	Operating mode of the wireless network of the router. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
Select channel automatically	Move the switch to the right to let the router itself choose the channel with the least interference.
Channel	The wireless channel number. Left-click to open the window for selecting a channel (the action is available, when the **Select channel automatically** switch is moved to the left).

Parameter	Description
Enable periodic scanning	Move the switch to the right to let the router search for a free channel in certain periods of time. When the switch is moved to the right, the **Scanning period** field is available for editing.
Scanning period	Specify a period of time (in seconds) after which the router rescans channels.

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

To edit the settings of the basic wireless network, in the **Access Points** section, left-click the needed network. On the opened page, change the needed parameters and click the **APPLY** button.

Also you can create an additional wireless network. To do this, click the **ADD** button in the **Access Points** section. On the opened page, specify the relevant parameters.

Figure 82. Creating a wireless network.

Parameter	Description
Wi-Fi Network	
Network name (SSID)	A name for the wireless network. The name can consist of digits and Latin characters.
Hide SSID	If the switch is moved to the right, other users cannot see your Wi-Fi network. It is recommended not to hide the network in order to simplify initial configuration of the wireless network.
BSSID	The unique identifier for this wireless network. You cannot change the value of this parameter, it is determined in the device's internal settings. The field is displayed in the settings of the existing wireless network.
Max associated clients	The maximum number of devices connected to the wireless network. When the value 0 is specified, the device does not limit the number of connected clients.
Enable shaping	Move the switch to the right to limit the maximum bandwidth of the wireless network. In the **Shaping** field displayed, specify the maximum value of speed (Kbit/s). Move the switch to the left not to limit the maximum bandwidth.
Broadcast wireless network	If the switch is moved to the left, devices cannot connect to the wireless network. Upon that the router can connect to another access point as a wireless client.
Clients isolation	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
Enable guest network	This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.

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

By default, the **WPA2-PSK** network authentication type of the wireless network is specified. WPS PIN from the barcode label is used as the network key.
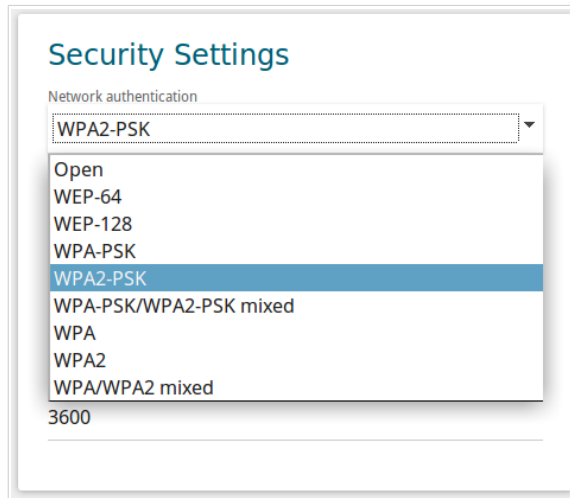
Figure 83. Network authentication types supported by the router.

The router supports the following authentication types:

Authentication type	Description
Open	Open authentication (with WEP encryption for wireless network modes not supporting 802.11n devices).
WEP-64	Authentication with a 64-bit shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n devices is selected from the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page.
WEP-128	Authentication with a 128-bit shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n devices is selected from the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page.
WPA	WPA-based authentication using a RADIUS server.
WPA-PSK	WPA-based authentication using a PSK.
WPA2	WPA2-based authentication using a RADIUS server.
WPA2-PSK	WPA2-based authentication using a PSK.
WPA/WPA2 mixed	A mixed type of authentication. When this value is selected, devices using the **WPA** authentication type and devices using the **WPA2** authentication type can connect to the wireless network.

Authentication type	Description
WPA-PSK/WPA2-PSK mixed	A mixed type of authentication. When this value is selected, devices using the **WPA-PSK** authentication type and devices using the **WPA2-PSK** authentication type can connect to the wireless network.

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

When the **Open**, **WEP-64**, or **WEP-128** value is selected, the following settings are displayed on the page (unavailable for the wireless network operating modes which support the standard 802.11n):
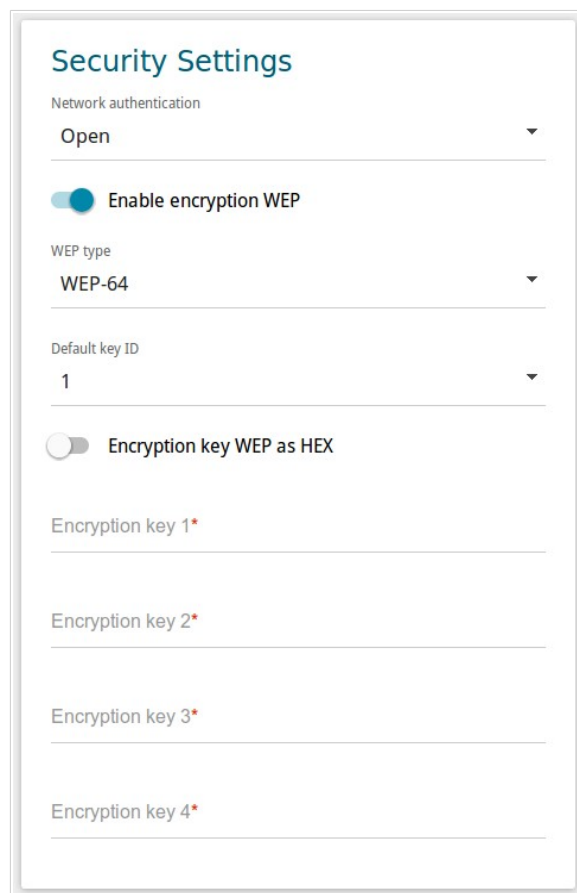
*Figure 84. The **Open** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
Enable encryption WEP	*For **Open** authentication type only.* To activate WEP encryption, move the switch to the right. Upon that the **WEP type** and **Default key ID** drop-down lists, the **Encryption key WEP as HEX** switch, and four **Encryption key** fields are displayed on the page.
WEP type	*For **Open** authentication type only.* WEP encryption type with a 64-bit or 128-bit key. Select the **WEP-64** value to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the **WEP-128** value to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the following fields are displayed on the page:
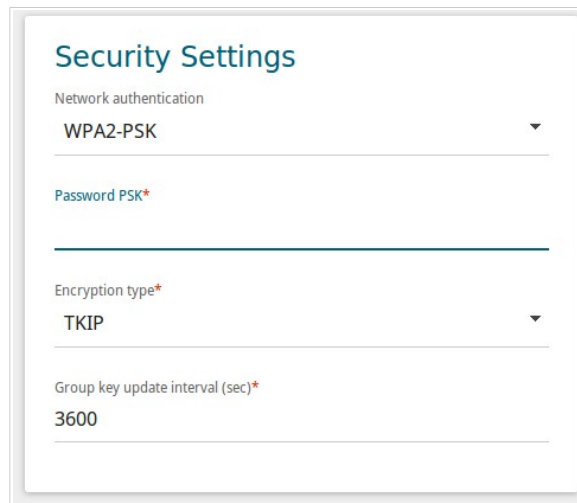
*Figure 85. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.*

Parameter	Description
Password PSK	A password for WPA encryption. The password can contain digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[2]
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed.

---

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

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

*Figure 86. The **WPA2** value is selected from the **Network authentication** drop-down list.*

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

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

Client Management

On the **Wi-Fi / Client Management** page, you can view the list of wireless clients connected to the router.
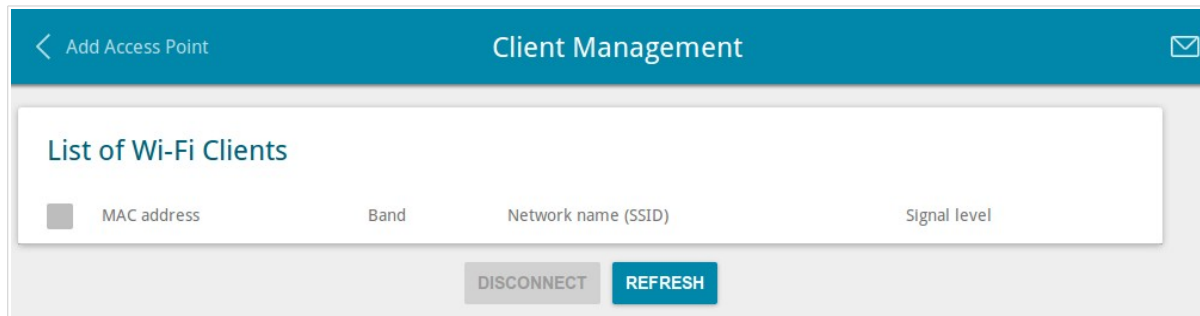
Figure 87. The page for managing the wireless clients.

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

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

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 are not available.
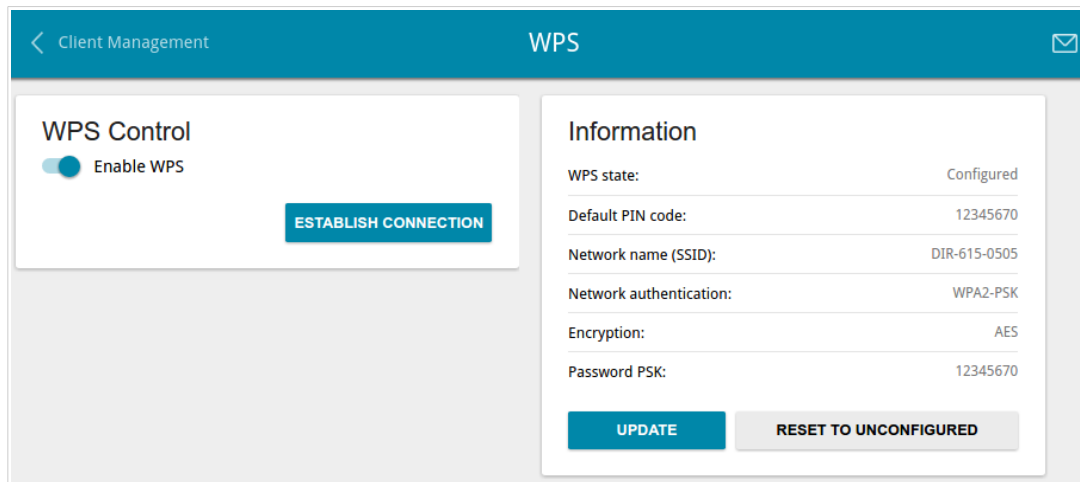
Figure 88. The page for configuring the WPS function.

To activate the WPS function, move the **Enable WPS** switch to the right.

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

Parameter	Description
WPS state	The state of the WPS function: • **Configured** (all needed settings are specified; these settings will be used upon establishing the wireless connection) • **Unconfigured** (after activating the WPS function, the SSID and the encryption key will be configured automatically, the network authentication type will be changed to WPA2-PSK).
Default PIN code	The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function.
Network name (SSID)	The name of the router's wireless network.
Network Authentication	The network authentication type specified for the wireless network.
Encryption	The encryption type specified for the wireless network.
Password PSK	The encryption password specified for the wireless network.
UPDATE	Click the button to update the data on the page.
RESET TO UNCONFIGURED	Click the button to reset the parameters of the WPS function.

Using WPS Function via Web-based Interface

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

1. Move the **Enable WPS** switch to the right.

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. Move the **Enable WPS** switch to the right.

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. Move the **WPS Enable** switch to the right.
3. Save the settings and close the web-based interface (click the **SAVE** button in the notification and then click the **Logout** line of the menu).

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

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

WMM

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

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

To enable the function, move the **Enable** switch to the right. Upon that the **Access Point** and **Station** sections are displayed on the page.
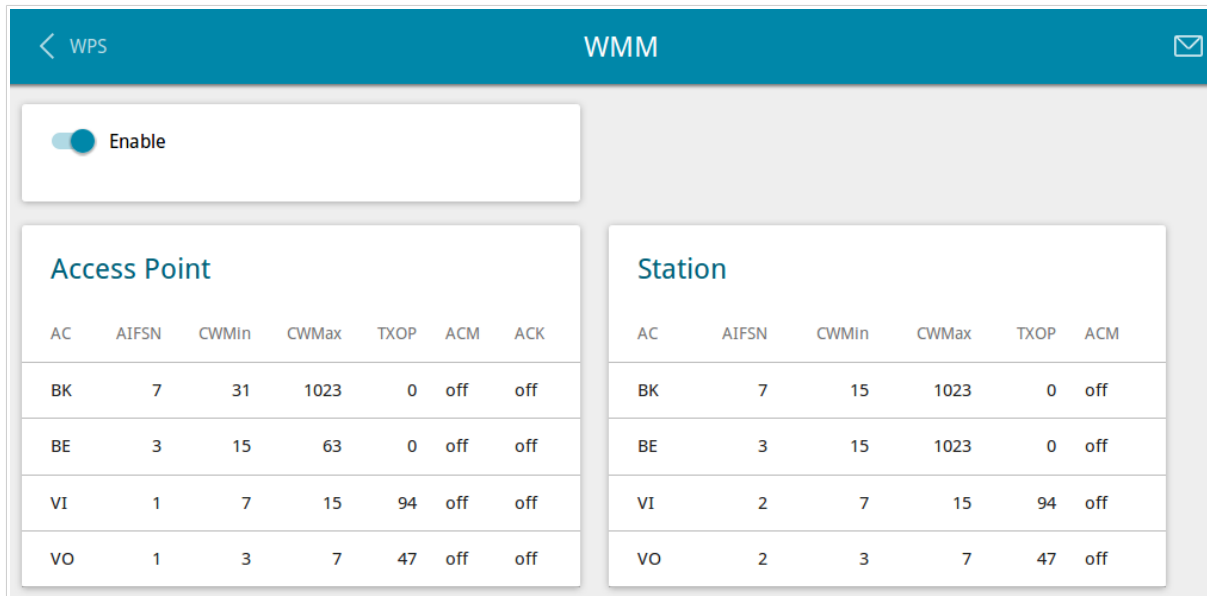
Figure 89. The page for configuring the WMM function.

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

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

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

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

To edit the parameters of an Access Category, left-click the relevant line. In the opened window, change the needed parameters.
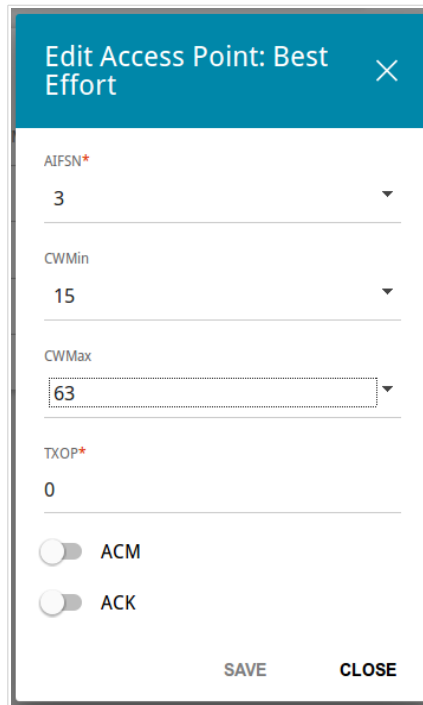
Figure 90. The window for changing parameters of the WMM function.

Parameter	Description
AIFSN	*Arbitrary Inter-Frame Space Number*. This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
CWMin/CWMax	*Contention Window Minimum/Contention Window Maximum*. Both fields influence time delays for the relevant Access Category. The **CWMax** field value should not be lower, than the **CWMin** field value. The lower the difference between the **CWMax** field value and the **CWMin** field value, the higher is the Access Category priority.
TXOP	*Transmission Opportunity*. The higher the value, the higher is the Access Category priority.
ACM	*Admission Control Mandatory*. If the switch is moved to the right, the device cannot use the relevant Access Category.
ACK	*Acknowledgment*. Answering response requests while transmitting. Displayed only in the **Access Point** section. If the switch is moved to the left, the router answers requests. If the switch is moved to the right, the router does not answer requests.

Click the **SAVE** button.

To disable the WMM function, move the **Enable** switch to the left.

Client

On the **Wi-Fi / Client** page, you can configure the router as a client to connect to a wireless access point or to a WISP.
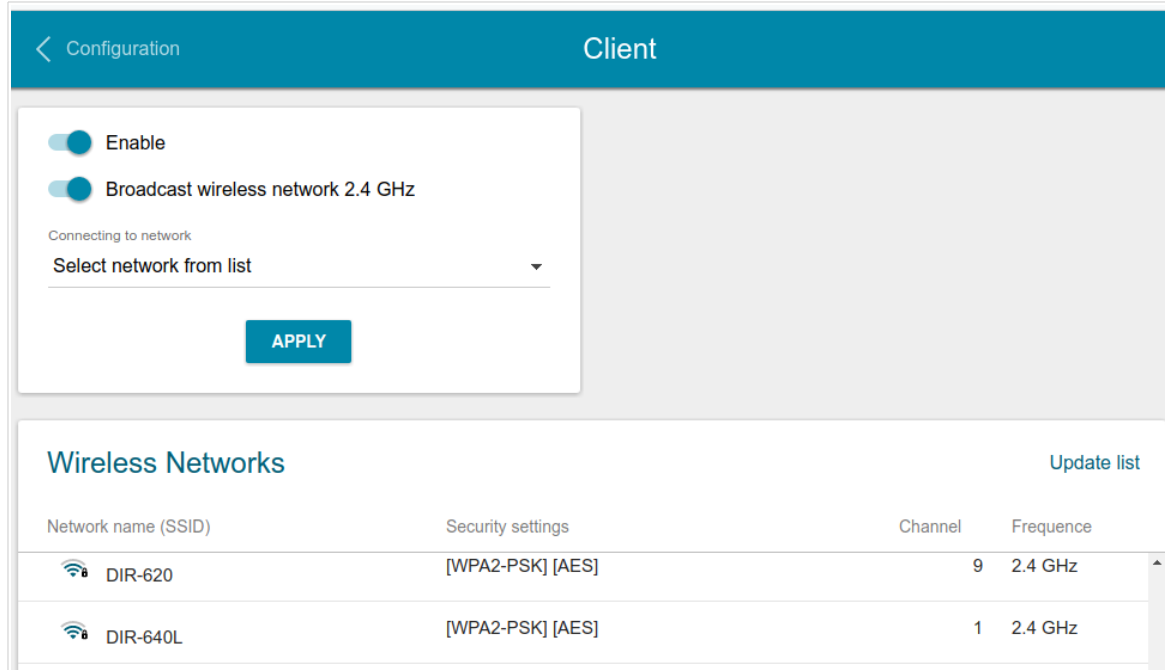
Figure 91. The page for configuring the client mode.

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

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

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

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

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

When the **Open**, **WEP-64**, or **WEP-128** authentication type is selected, the following settings are displayed on the page:

Parameter	Description
Enable encryption WEP	*For **Open** authentication type only.* To activate WEP encryption, move the switch to the right. Upon that the **WEP type** and **Default key ID** drop-down lists, the **Encryption key WEP as HEX** switch, and four **Encryption key** fields are displayed on the page.
WEP type	*For **Open** authentication type only.* WEP encryption type with a 64-bit or 128-bit key. Select the **WEP-64** value to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the **WEP-128** value to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default key ID** drop-down list. It is required to specify all the fields.

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

Parameter	Description
Password PSK	A password for WPA encryption.
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.

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

When connecting to a wireless access point, the wireless channel of DIR-300S will switch to the channel of the access point to which you have connected.

If the router has been successfully connected to the network, the line of the selected network will be highlighted in blue.

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

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

Additional

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

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

Figure 92. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	The channel bandwidth for 802.11n standard. **20MHz**: 802.11n clients operate at 20MHz channels. **40MHz**: 802.11n clients operate at 40MHz channels. **20/40MHz -**: 802.11n clients operate at 20MHz or 40MHz channels (the channel is combined with the previous adjacent channel). **20/40MHz +**: 802.11n clients operate at 20MHz or 40MHz channels (the channel is combined with the next adjacent channel).
TX power	The transmit power (in percentage terms) of the router.

Parameter	Description
BG protection	The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Select a value from the drop-down list. **Auto**: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices). **Always On**: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network). **Always Off**: The protection function is always disabled.
Short GI	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices. **Enable**: the router uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n standard (see the value of the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page). **Disable**: the router uses the 800 ns standard guard interval.
Drop multicast	Move the switch to the right to disable multicasting for the router's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected in the **IGMP** section on the **Connections Setup / WAN** page.
Adaptivity mode	Move the switch to the right to prevent your wireless network from interfering with radars and other mobile or stationary radio systems. Such a setting can slow down the router's WLAN.
Beacon period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS threshold	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
Frag threshold	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).
DTIM period	The time period (in seconds) between sending a DTIM (a message notifying on broadcast or multicast transmission) and data transmission.
Station Keep Alive	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value **0** is specified, the checking is disabled.

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

MAC Filter

On the **Wi-Fi / MAC Filter** page, you can define a set of MAC addresses of devices which will be allowed to access the WLAN, or define MAC addresses of devices which will not be allowed to access the WLAN.
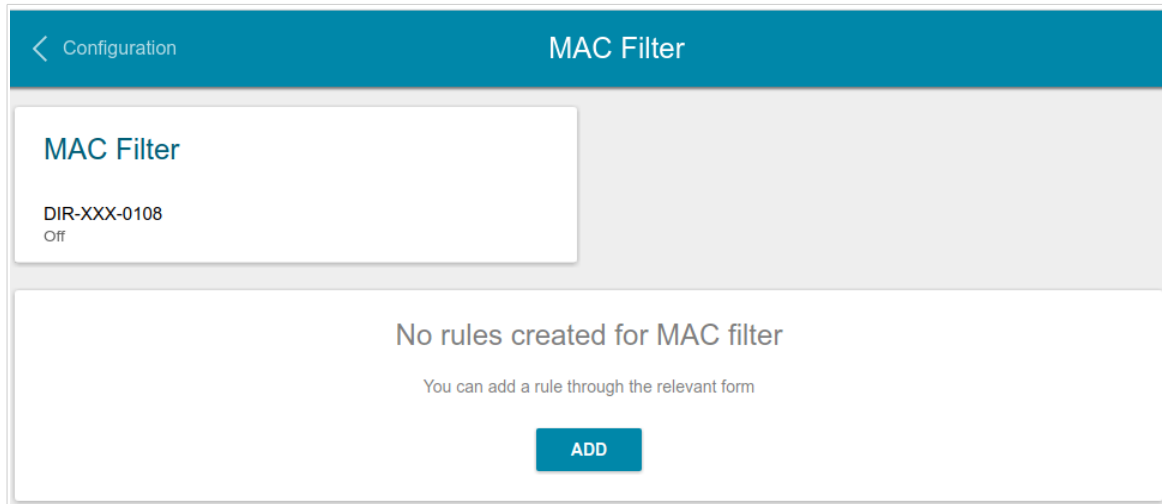
Figure 93. The page for configuring the MAC filter for the wireless network.

By default, MAC filtering is disabled.

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 **MAC Filter** section, 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.

Click the **ADD** button to add a rule for MAC filtering.
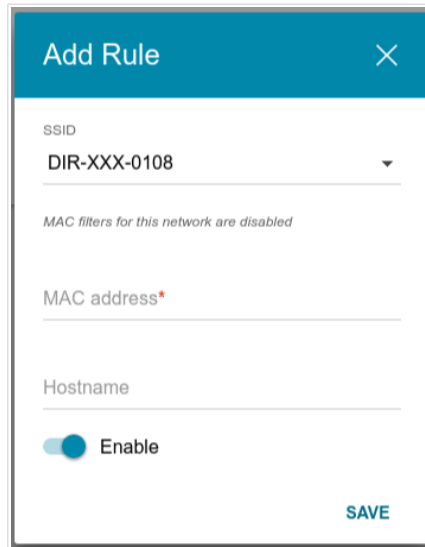
Figure 94. The window for adding a rule for the MAC filter.

You can specify the following parameters:

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

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

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

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

Roaming

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

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

*Figure 95. The **Wi-Fi / Roaming** page.*

To enable the function, move the **Enable** switch to the right. Upon that the following settings are available on the page.

Parameter	Description
Port number	The number of the port used for data exchange between access points (routers).
Use multicast for service data exchange	Move the switch to the right in order to use multicast traffic for service data exchange between access points (routers). This setting is needed if the devices which support the smart adjustment function are located in different subnets. If the switch is moved to the right, the **Multicast Settings** section is displayed on the page. If the switch is moved to the left, broadcast traffic is used for service data exchange.
Maximum time of storing data on adjacent clients	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.

Parameter	Description
Minimum level of connection quality	The threshold value of the signal strength upon which the access point (router) starts scanning other devices.
Dead zone	This parameter is used for calculation of the signal strength upon which the smart adjustment function goes off. If the signal strength provided by the device is less than the sum of the **Minimum level of connection quality** field value and the **Dead zone** field value, then the client disconnects from the access point (router) and connects to another device. You can specify the values from `−50%` to `+50%`.
Multicast Settings	
Multicast TTL	Specify the TTL (*Time to live*) parameter value. The recommended value is `4`.
Multicast group address	Specify the address of the multicast group (from the subnet 239.255.0.0/16).

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

To disable the function of smart adjustment of Wi-Fi clients, move the **Enable** switch to the left.

Advanced

In this menu you can configure advanced settings of the router:
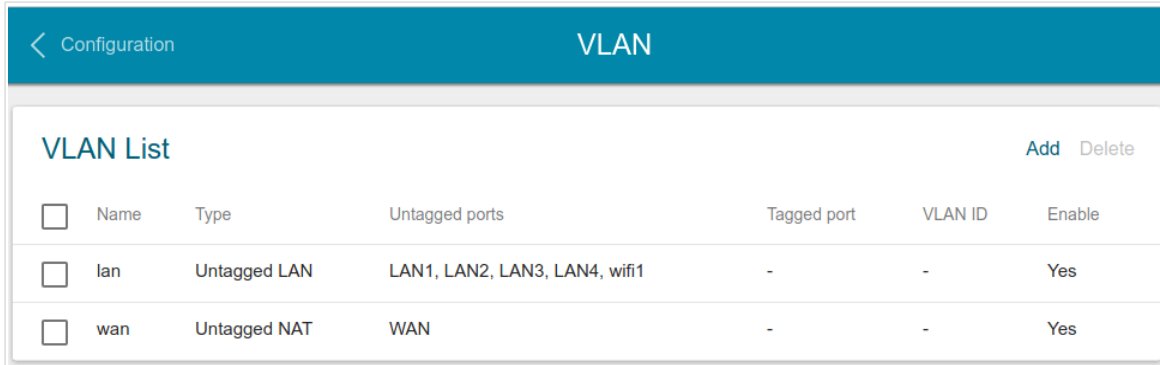
- create groups of ports for VLANs

- add name servers

- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the router

- setup the rate limit for traffic transmitted from every port of the router

- configure notifications on the reason of the Internet connection failure

- configure a DDNS service

- define static routes

- configure TR-069 client

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

- enable the UPnP IGD protocol

- enable the built-in UDPXY application for the router

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

VLAN

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

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

- **lan**: it includes ports 1-4. You cannot delete this group.
- **wan**: for the WAN interface; it includes the **WAN** port. You can edit or delete this group.
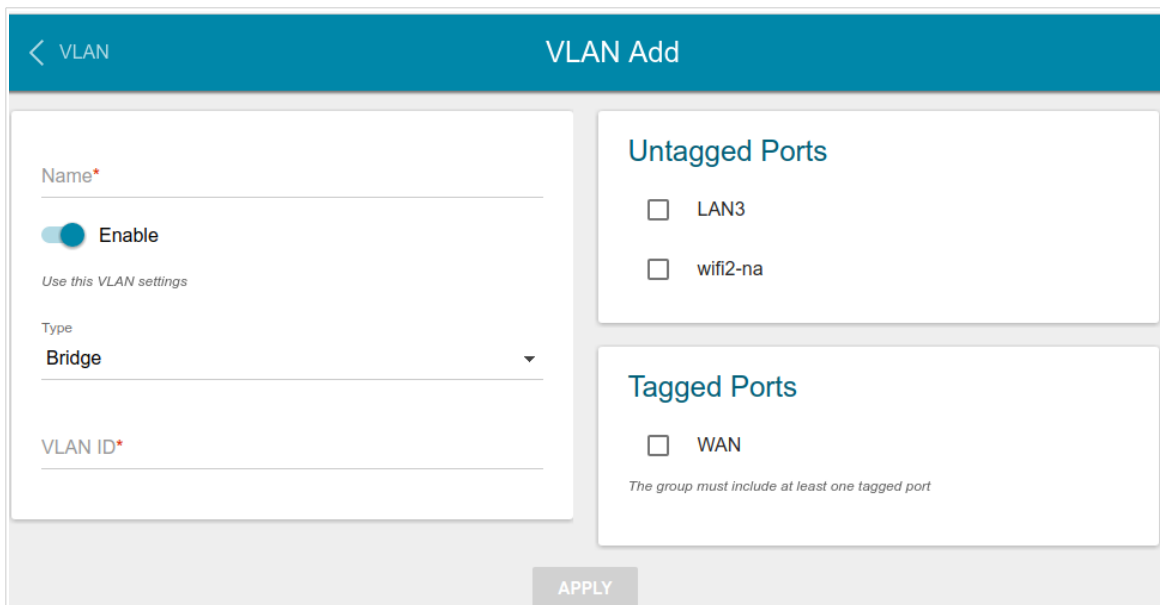
*Figure 96. The **Advanced / VLAN** page.*

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

To create a new group for VLAN, click the **Add** button.

Figure 97. The page for adding a group of ports for VLAN.

You can specify the following parameters:

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

Click the **APPLY** button.

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

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

DNS

On the **Advanced / DNS** page, you can add DNS servers to the system.
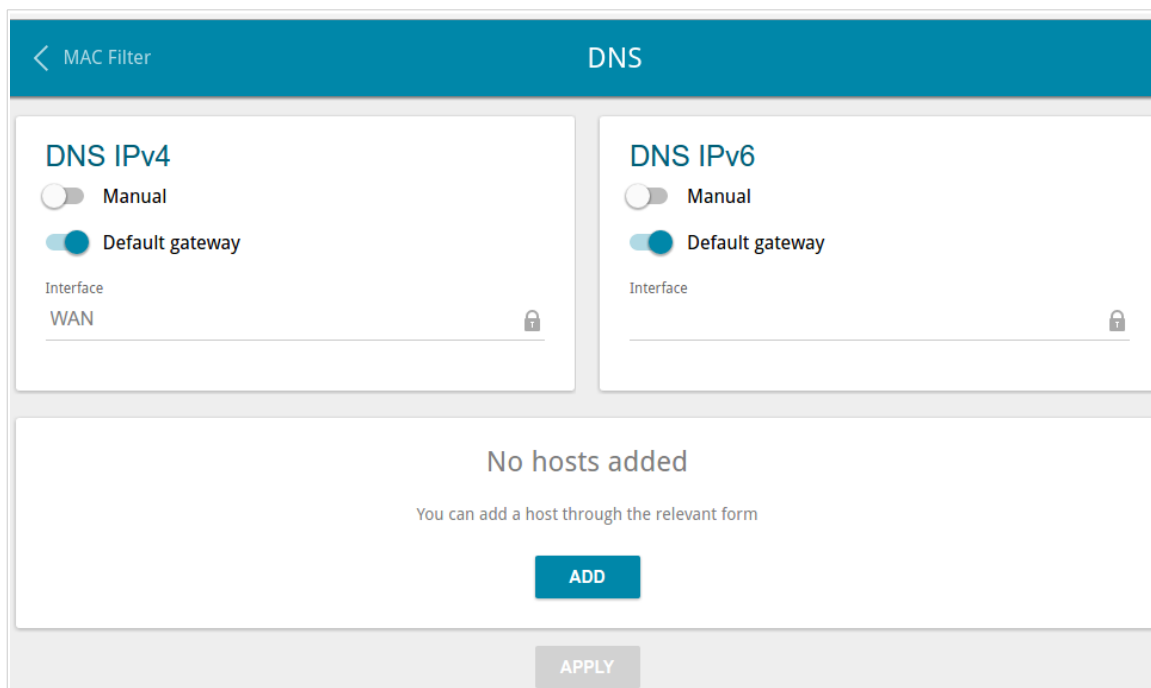
*Figure 98. The **Advanced / DNS** page.*

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

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

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

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

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

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

If needed, you can add your own address resource record. To do this, click the **ADD** button.
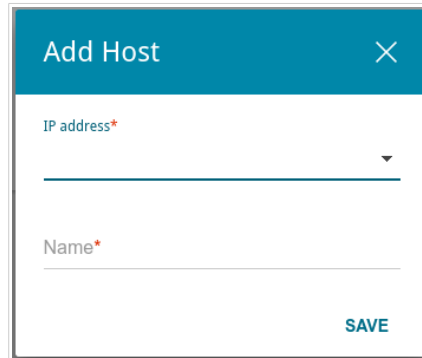
Figure 99. The window for adding a DNS record.

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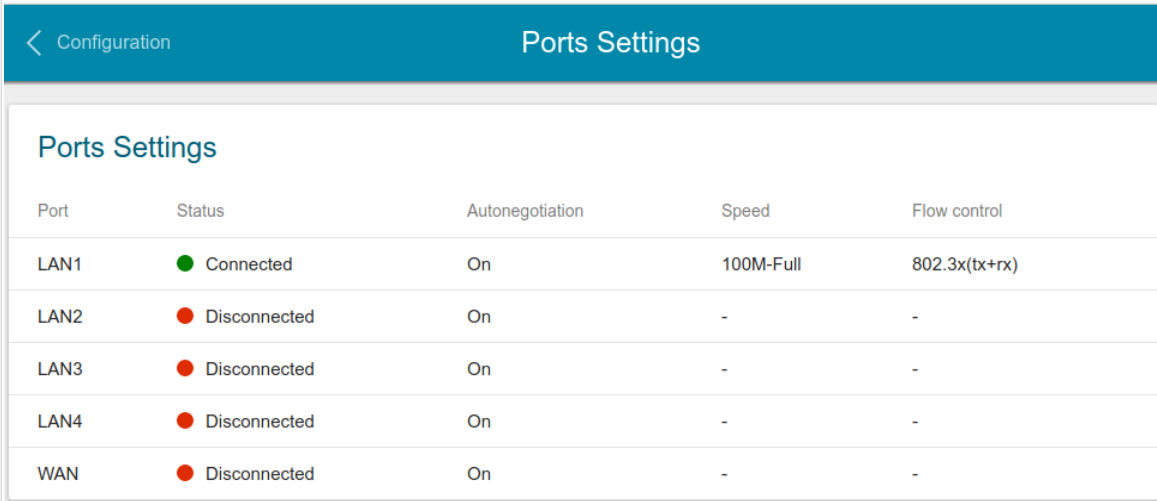
To edit an existing record, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a record, select the checkbox located to the left of the relevant line in the table and click the **Delete** button.

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

Port Settings

On the **Advanced / Port Settings** page, you can configure or disable autonegotiation of speed and duplex mode or manually configure speed and duplex mode for each Ethernet port of the router.

Also you can enable or disable data flow control in the autonegotiation mode. This function is used for equal load balancing in ISPs' networks. Contact your ISP to clarify if this function needs to be enabled.

*Figure 100. The **Advanced / Port Settings** page.*

By default, autonegotiation of speed, duplex mode, and data flow control is configured for each Ethernet port of the router. If you need to specify speed and duplex mode manually or change autonegotiation settings (speed, duplex mode, or enable/disable data flow control) for a port, select the relevant port 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.
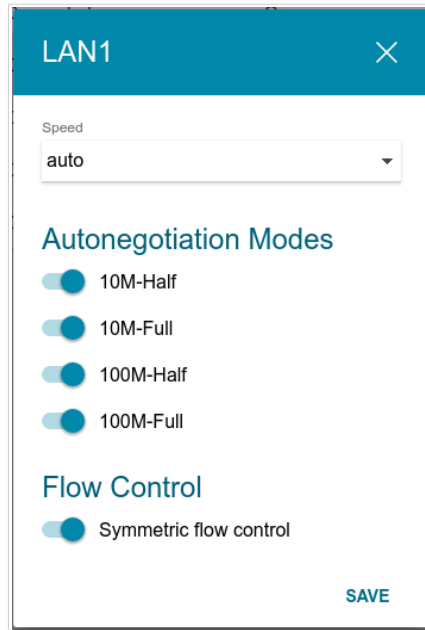
Figure 101. The window for changing the settings of the router's port.

In the opened window, specify the needed parameters:

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

To enable the needed data transfer modes, move relevant switches to the right.

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

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

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

Bandwidth Control

On the **Advanced / Bandwidth Control** page, you can setup the rate limit for traffic transmitted from every port of the router.
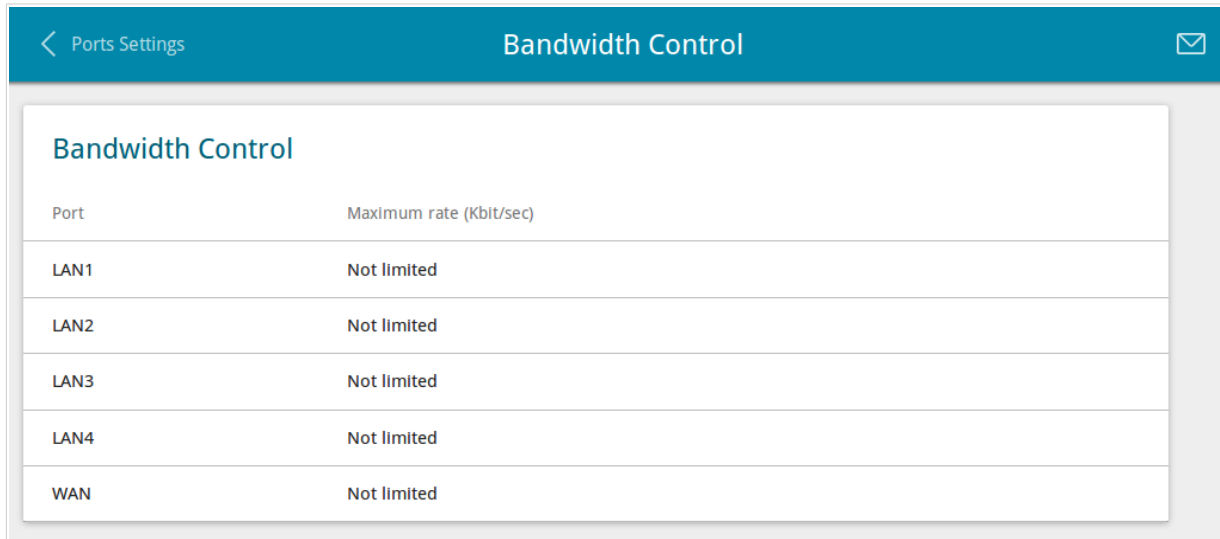
*Figure 102. The **Advanced / Bandwidth control** page.*

By default, the rate is not limited. If you want to limit the rate for traffic transmitted from a port, select the line corresponding to this port.
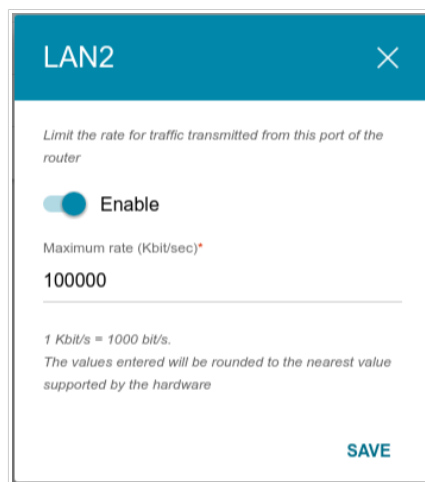
Figure 103. The window for setting up rate limit.

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

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

Redirect

On the **Advanced / Redirect** page, you can enable notifications on the reason of the Internet connection failure. Notifications will be displayed in the browser window when a user is attempting to open a web site on the Internet.
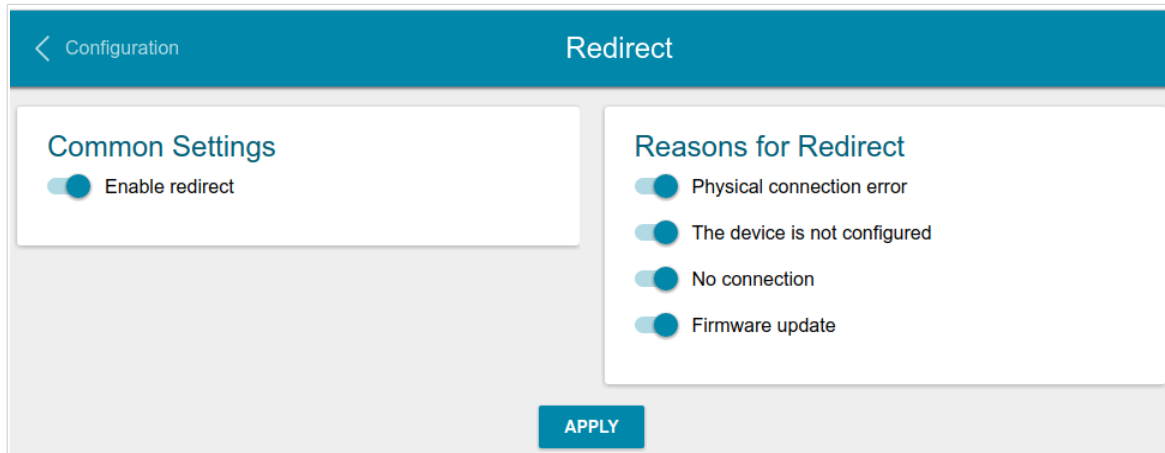
*Figure 104. The **Advanced / Redirect** page.*

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

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

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

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

DDNS

On the **Advanced / DDNS** page, you can define parameters of the DDNS service, which allows associating a domain name with dynamic IP addresses.
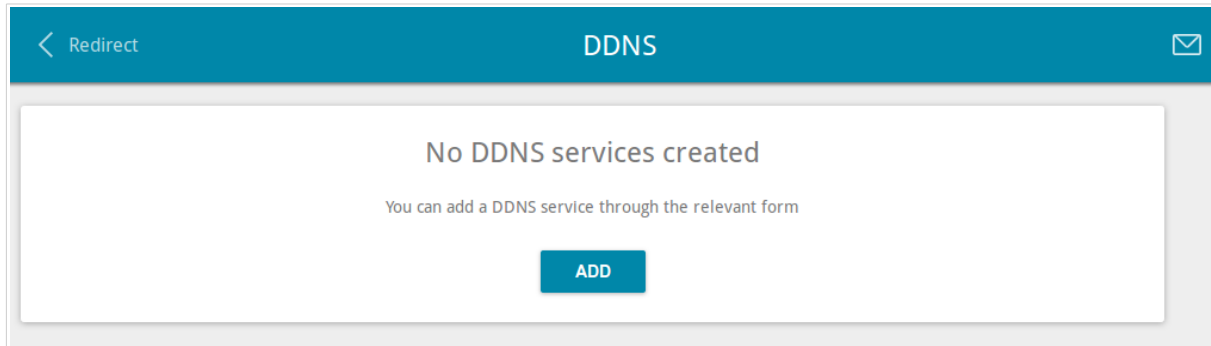
*Figure 105. The **Advanced / DDNS** page.*

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

Figure 106. The window for adding a DDNS service.

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

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

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

To edit parameters of the existing DDNS service, select the relevant line in the table. In the opened window, 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.

Routing

On the **Advanced / Routing** page, you can add static routes (routes for networks that are not connected directly to the device but are available through the interfaces of the device) into the system.
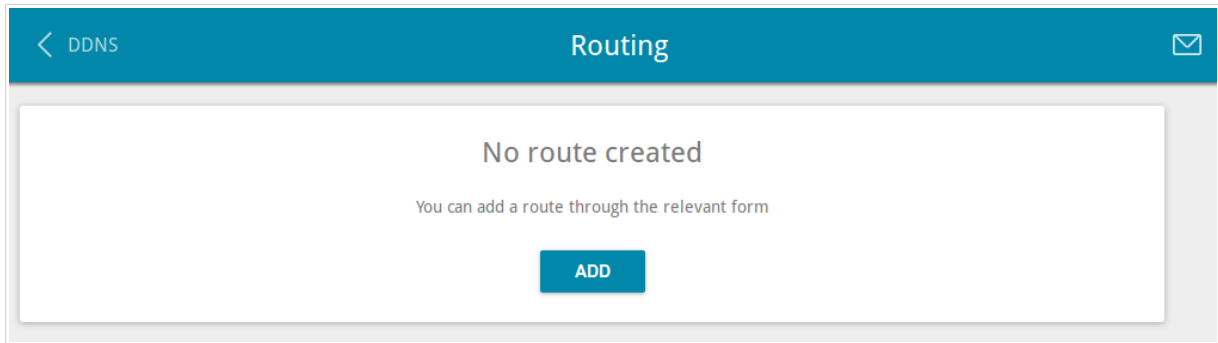
*Figure 107. The **Advanced / Routing** page.*

To create a new route, click the **ADD** button.
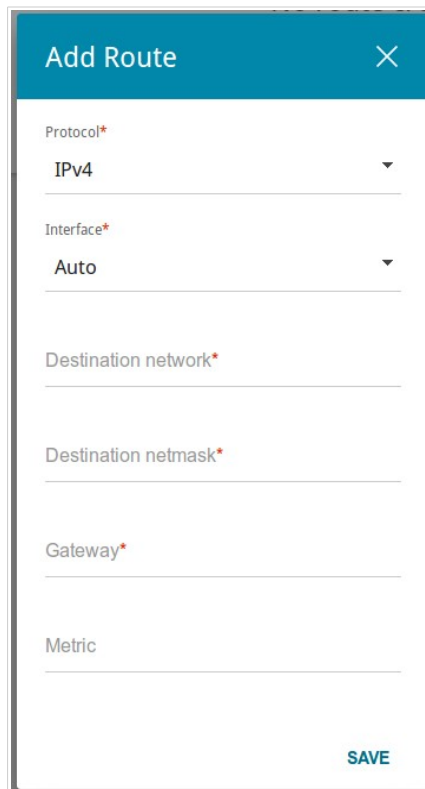
Figure 108. The window for adding a new route.

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

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

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

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

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

TR-069 Client

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

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

Figure 109. The page for configuring the TR-069 client.

You can specify the following parameters:

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

Parameter	Description
Inform settings	
Enable	Move the switch to the right so the router may send reports (data on the device and network statistics) to the ACS.
Interval	Specify the time period (in seconds) between sending reports.
Auto Configuration Server Settings	
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS.
Connection Request Settings	
Username	The username used by the ACS to transfer a connection request to the router.
Password	The password used by the ACS.
Request port	The port used by the ACS. By default, the port `8999` is specified.
Request path	The path used by the ACS.

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

Remote Access

On the **Advanced / Remote Access** page, you can configure access to the web-based interface of the router. By default, the access from external networks to the router is closed. If you need to allow access to the router from the external network, create relevant rules.
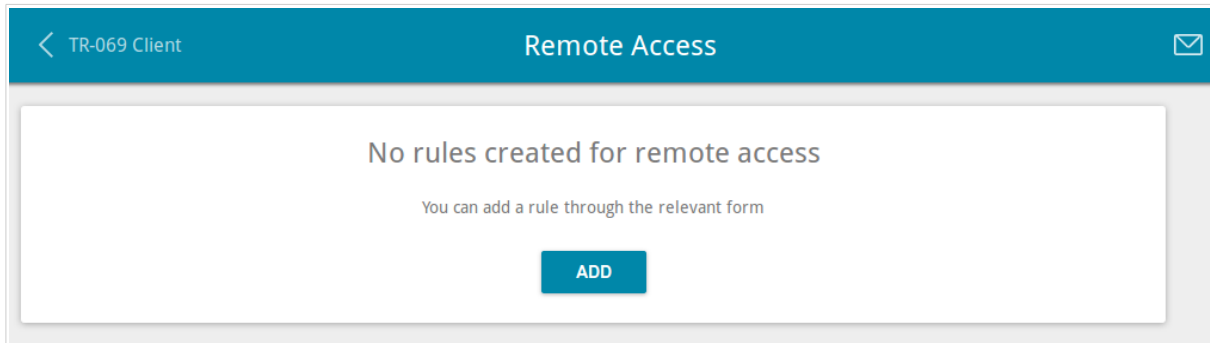
*Figure 110. The **Advanced / Remote Access** page.*

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

Figure 111. The window for adding a rule for remote management.

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

Parameter	Description
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Open access from any external host	Move the switch to the right to allow access to the router for any host. Upon that the **IP address** and **Mask** fields are not displayed.

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

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

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

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

UPnP IGD

On the **Advanced / UPnP IGD** page, you can enable the UPnP IGD protocol. The router uses the UPnP IGD protocol for automatic configuration of its parameters for network applications requiring an incoming connection to the router.
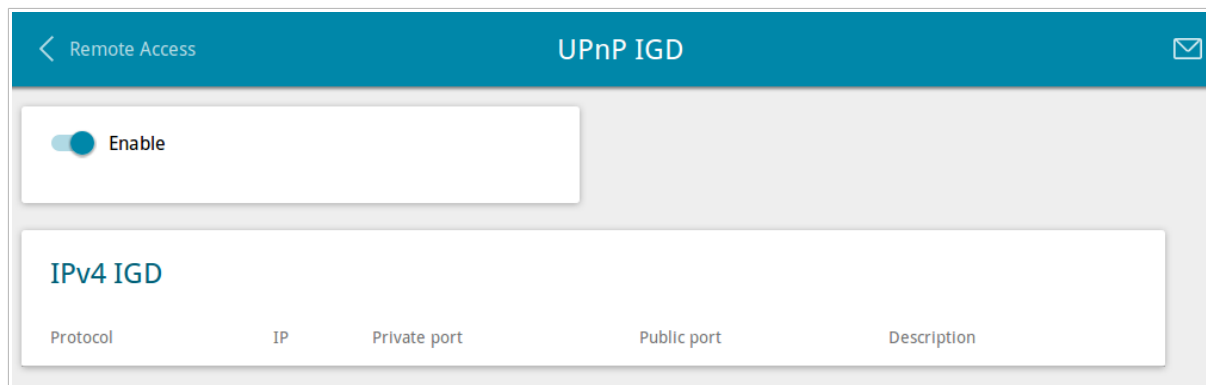
*Figure 112. The **Advanced / UPnP IGD** page.*

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

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

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

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

UDPXY

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

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

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

Upon that the following fields are displayed on the page:

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

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
2443	192.168.0.1:4022	202.254.1.2	0

Restart

Available HTTP requests:

Request template	Function
http://address:port/udp/mcast_addr:mport/	Relay multicast traffic from mcast_addr:mport
http://address:port/status/	Display udpxy status
http://address:port/restart/	Restart udpxy

udpxy v. 1.0 (Build 23) standard - [Thu Jan 1 00:31:30 1970]
udpxy and udpxrec are Copyright (C) 2008-2013 Pavel V. Cherenkov and licensed under GNU GPLv3

Figure 114. The UDPXY application status page.

IGMP/ALG/Passthrough

On the **Advanced / IGMP/ALG/Passthrough** page, you can allow the router to use IGMP and RTSP, enable the SIP ALG and PPPoE/PPTP/L2TP/IPsec pass through functions.

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

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 PPPoE 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.
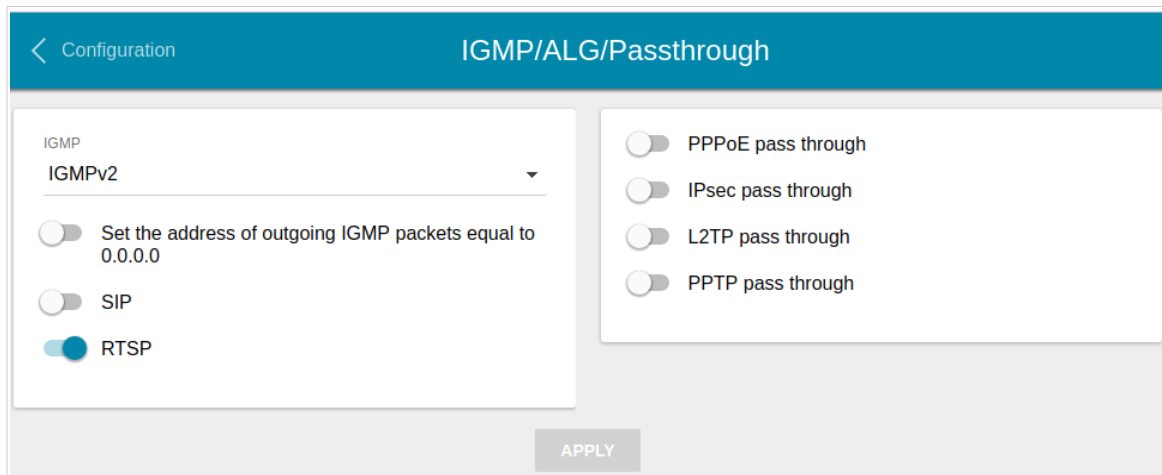
*Figure 115. The **Advanced / IGMP/ALG/Passthrough** page.*

The following elements are available on the page:

Parameter	Description
IGMP	Select a version of IGMP from the drop-down list. Such a setting allows to enable multicasting from the WAN connection selected in the **IGMP** section on the **Connections Setup / WAN** page.
Set the address of outgoing IGMP packets equal to 0.0.0.0	Move the switch to the right if you want all outgoing IGMP packets to have the IP address 0.0.0.0.
SIP	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled router.[3]
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.

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

---

3 On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / IGMP/ALG/Passthrough** page, connect the phone 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).

Firewall

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

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

IP Filter

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

*Figure 116. The **Firewall / IP Filter** page.*

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

Figure 117. The page for adding a rule for IP filtering.

You can specify the following parameters:

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

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

Click the **APPLY** button.

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

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

Virtual Servers

On the **Firewall / Virtual Servers** page, you can create virtual servers for redirecting incoming Internet traffic to a specified IP address in the local area network.
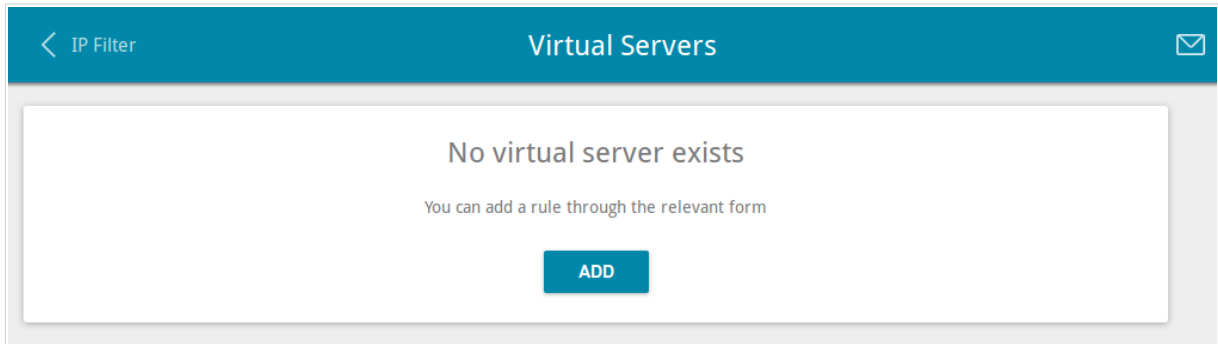
*Figure 118. The **Firewall / Virtual Servers** page.*

To create a new virtual server, click the **ADD** button.
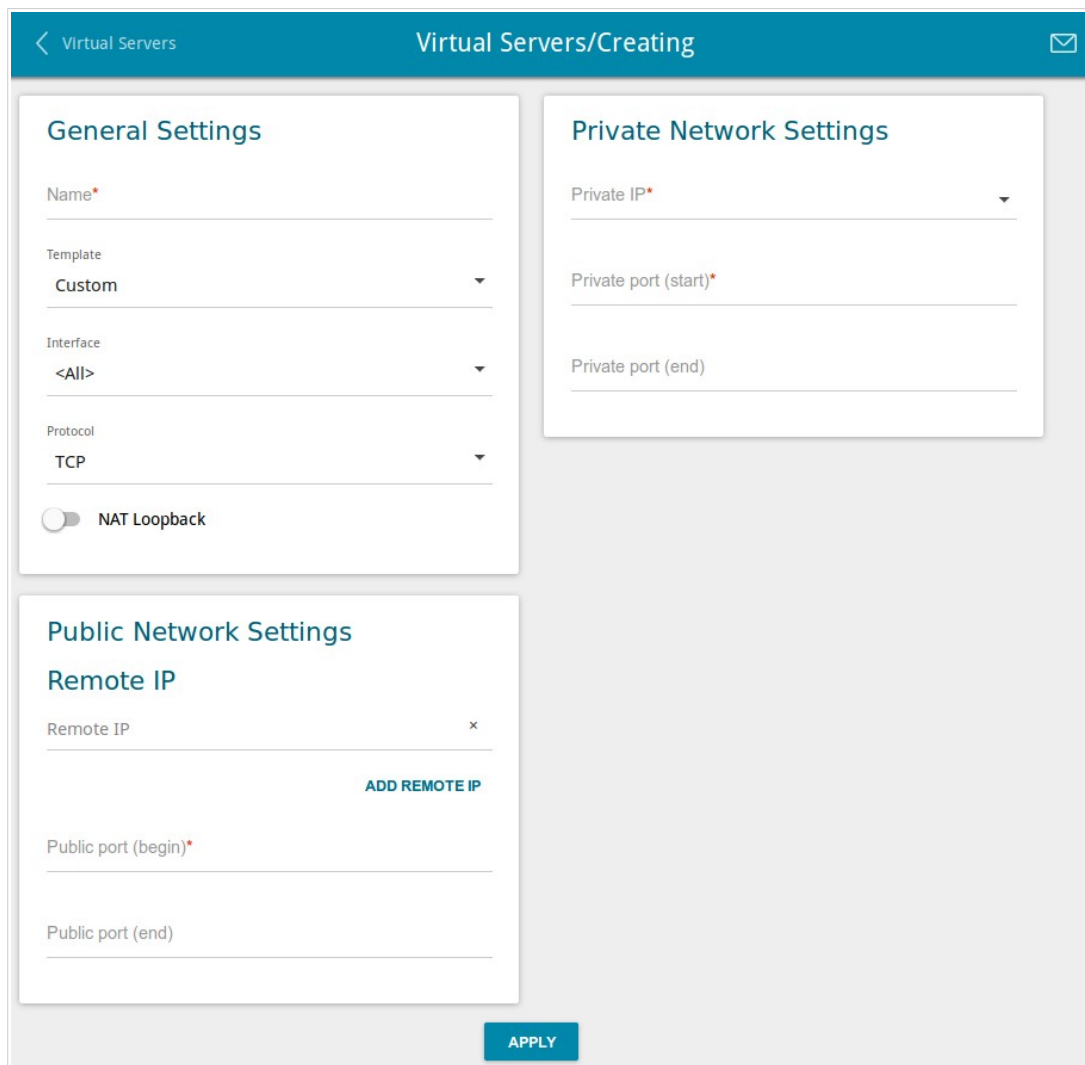
Figure 119. The page for adding a virtual server.

You can specify the following parameters:

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

Click the **APPLY** button.

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

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

DMZ

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

On the **Firewall / DMZ** page, you can specify the IP address of the DMZ host.
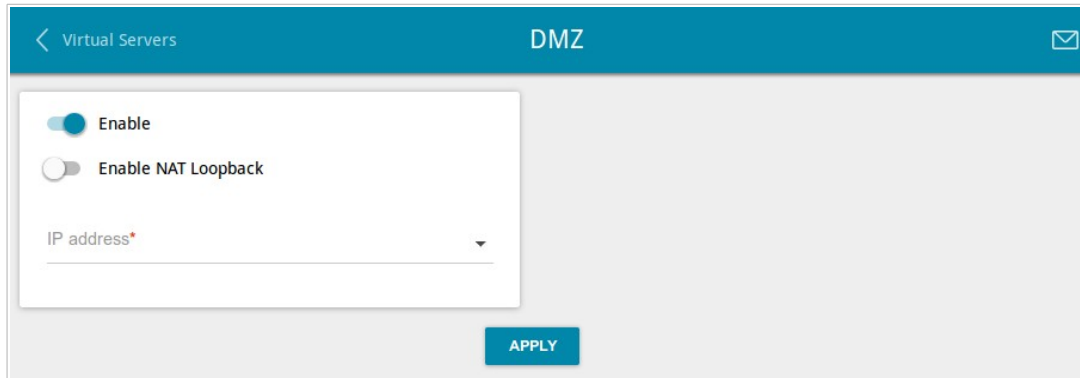
*Figure 120. The **Firewall / DMZ** page.*

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

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

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

Click the **APPLY** button.

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

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

MAC Filter

On the **Firewall / MAC Filter** page, you can configure MAC-address-based filtering for computers of the router's LAN.
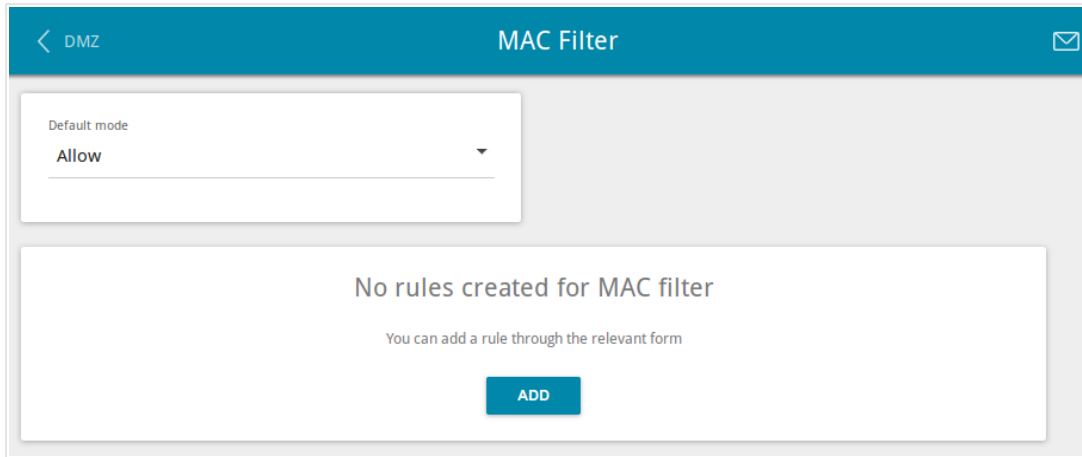
*Figure 121. The **Firewall / MAC Filter** page.*

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.

If you need to specify a filtering mode for each device separately, create a relevant rule. To do this, click the **ADD** button.
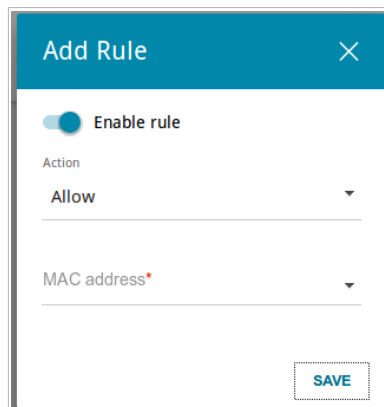
Figure 122. The window for adding a rule for the MAC filter.

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

Parameter	Description
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. **Deny**: Blocks access to the router's network for the device with the specified MAC address. **Allow**: Allows access to the router's network and to the Internet for the device with the specified MAC address when the rules on the **Firewall / IP Filter** page block access for this device.
MAC address	The MAC address of a device from the router's LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).

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

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

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

URL Filter

On the **Firewall / URL Filter** page, you can specify restrictions on access to certain web sites.
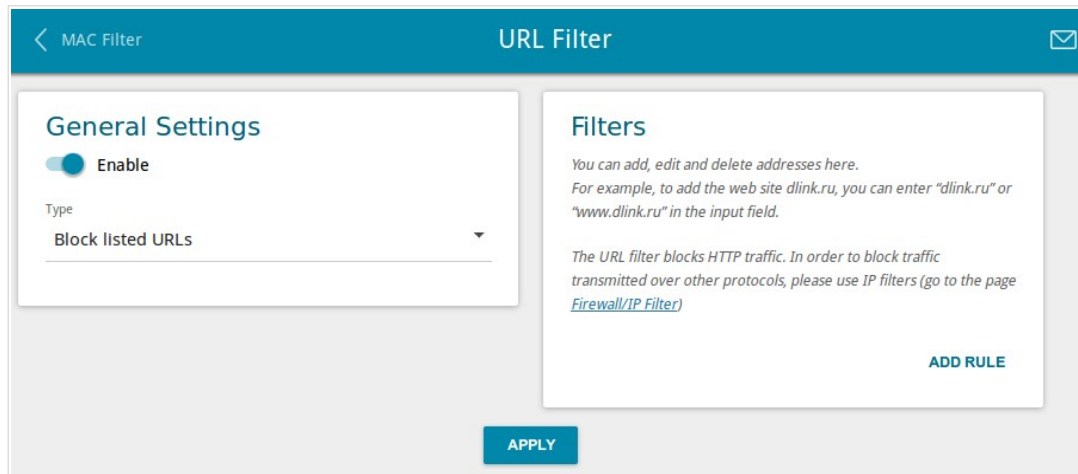
*Figure 123. The **Firewall / URL Filter** page.*

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

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

Click the **APPLY** button.

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

To remove an address from the list of URL addresses, click the **Delete** icon (✕) in the line of the relevant URL address. Then click the **APPLY** button.

System

In this menu you can do the following:

- change the password used to access the router's settings

- restore the factory default settings

- create a backup of the router's configuration

- restore the router's configuration from a previously saved file

- save the current settings to the non-volatile memory

- reboot the router

- change the web-based interface language

- update the firmware of the router

- configure automatic notification on new firmware version

- view the system log; configure sending the system log to a remote host

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

- trace the route to a host

- allow or forbid access to the router via TELNET

- configure automatic synchronization of the system time or manually configure the date and time for the router.

Configuration

On the **System / Configuration** page, you can change the password for the administrator account used to access the web-based interface of the router and to access the device settings via TELNET, restore the factory defaults, backup the current configuration, restore the router's configuration from a previously created file, save the changed settings to the non-volatile memory, reboot the device, or change the web-based interface language.
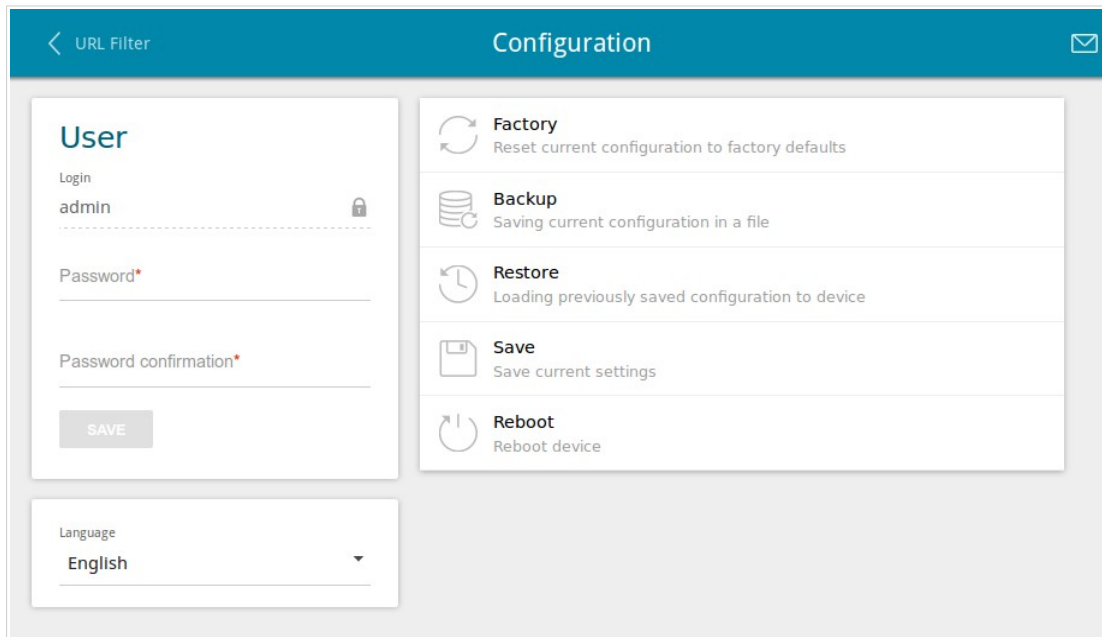
*Figure 124. The **System / Configuration** page.*

In order to change the password for the administrator account, in the **User** section, enter a new password in the **Password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[4] Then click the **SAVE** button.

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

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

---

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

The following buttons are also available on the page:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware **RESET** button (see the *Back Panel* section, page 11).
Backup	Click the button to save the configuration (all settings of the router) to your PC. The configuration backup will be stored in the download location of your web browser.
Restore	Click the button and follow the dialog box appeared to select a previously saved configuration file (all settings of the router) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. Please, save settings every time you change the router's parameters. Otherwise the changes will be lost upon hardware reboot of the router.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

Firmware Update

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

> **!** <u>Update the firmware only when the router is connected to your PC via a wired connection.</u>
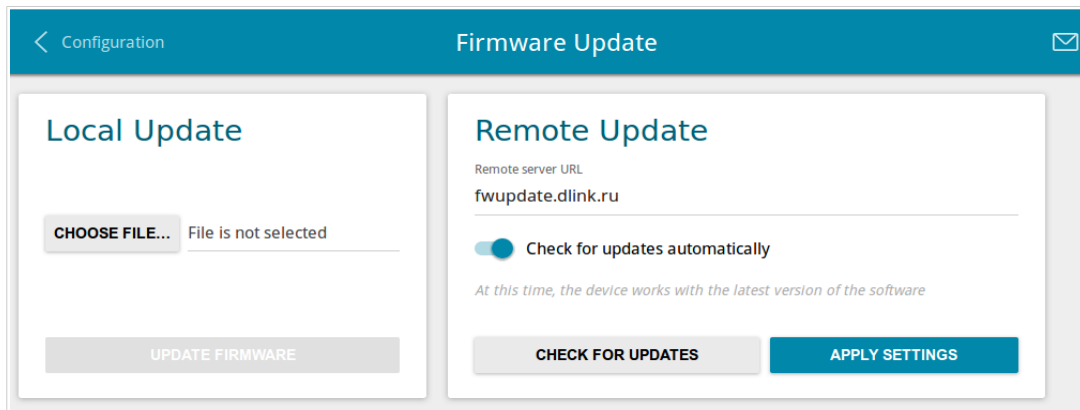
*Figure 125. The **System / Firmware Update** page.*

You can view the current version of the router's firmware on the **Summary** page.

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

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

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

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

Local Update

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

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

1. Download a new version of the firmware from www.dlink.ru.

2. Click the **CHOOSE FILE** button in the **Local Update** section on the **System / Firmware Update** page to locate the new firmware file.

3. Click the **UPDATE FIRMWARE** button.

4. Wait until the router is rebooted (about one and a half or two minutes).

5. Log into the web-based interface using the login (`admin`) and the current password.

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

Remote Update

> **!** <u>Attention! Do not turn off the router before the firmware update is completed. This may cause the device breakdown.</u>

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

1. On the **System / Firmware Update** page, in the **Remote Update** section, click the **CHECK FOR UPDATES** button to check if a newer firmware version exists.

2. Click the **UPDATE FIRMWARE** button (the button is displayed if a newer version of the firmware is available).

3. Wait until the router is rebooted (about one and a half or two minutes).

4. Log into the web-based interface using the login (`admin`) and the current password.

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

Log

On the **System / Log** page, you can set the system log options and configure sending the system log to a remote host.
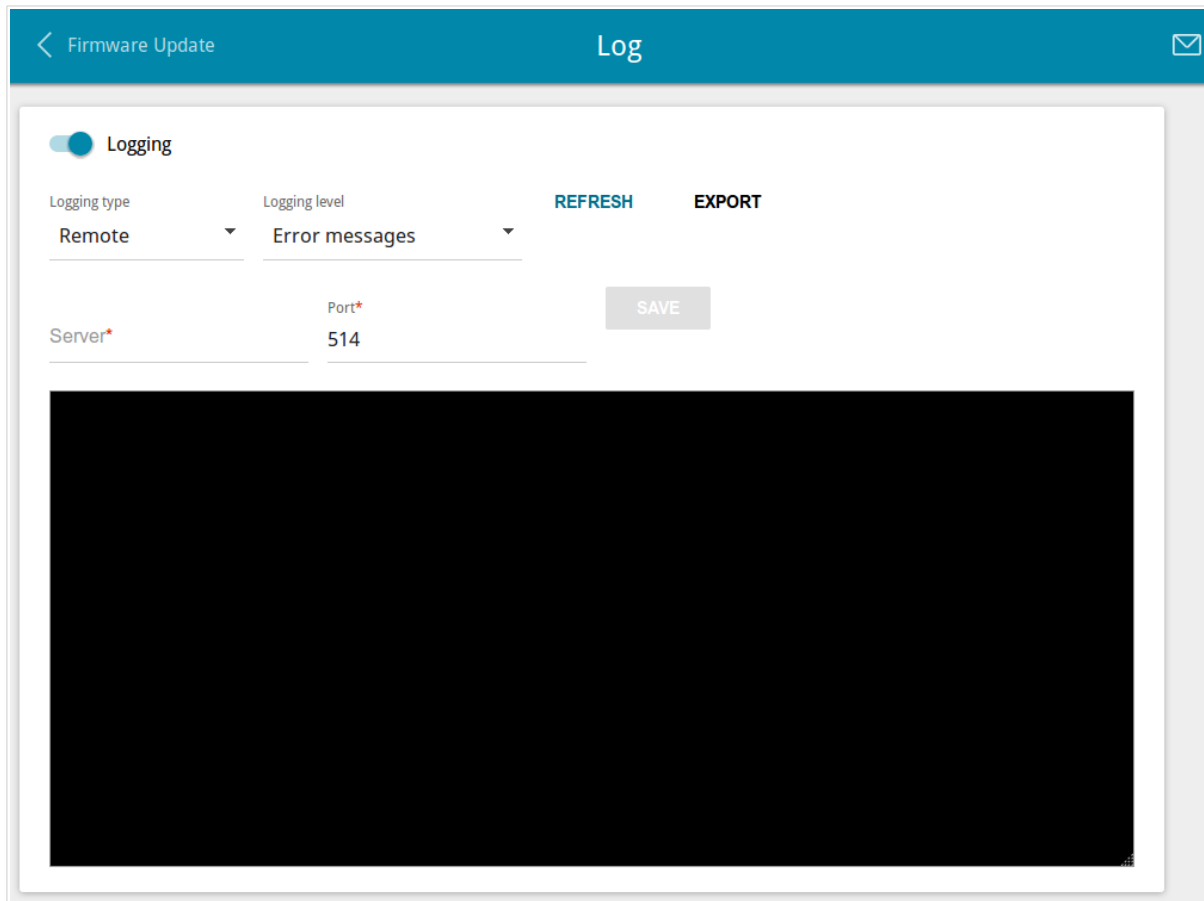
*Figure 126. The **System / Log** page.*

To enable logging of the system events, move the **Logging** switch to the right. Then specify the needed parameters.

Parameter	Description
Logging type	Select a type of logging from the drop-down list. • **Local**: the system log is stored in the router's memory. When this value is selected, the **Server** and **Port** fields are not displayed. • **Remote**: the system log is sent to the remote host specified in the **Server** field. • **Local and remote**: the system log is stored in the router's memory and sent to the remote host specified in the **Server** field.
Logging level	Select a type of messages and alerts/notifications to be logged.

Parameter	Description
Server	The IP or URL address of the host from the local or global network, to which the system log will be sent.
Port	A port of the host specified in the **Server** field. By default, the value `514` is specified.

After specifying the needed parameters in the **Server** and **Port** fields, click the **SAVE** button.

To disable logging of the system events, move the **Logging** switch to the left.

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

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

Ping

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

The Ping utility sends echo requests to a specified host and receives echo replies.
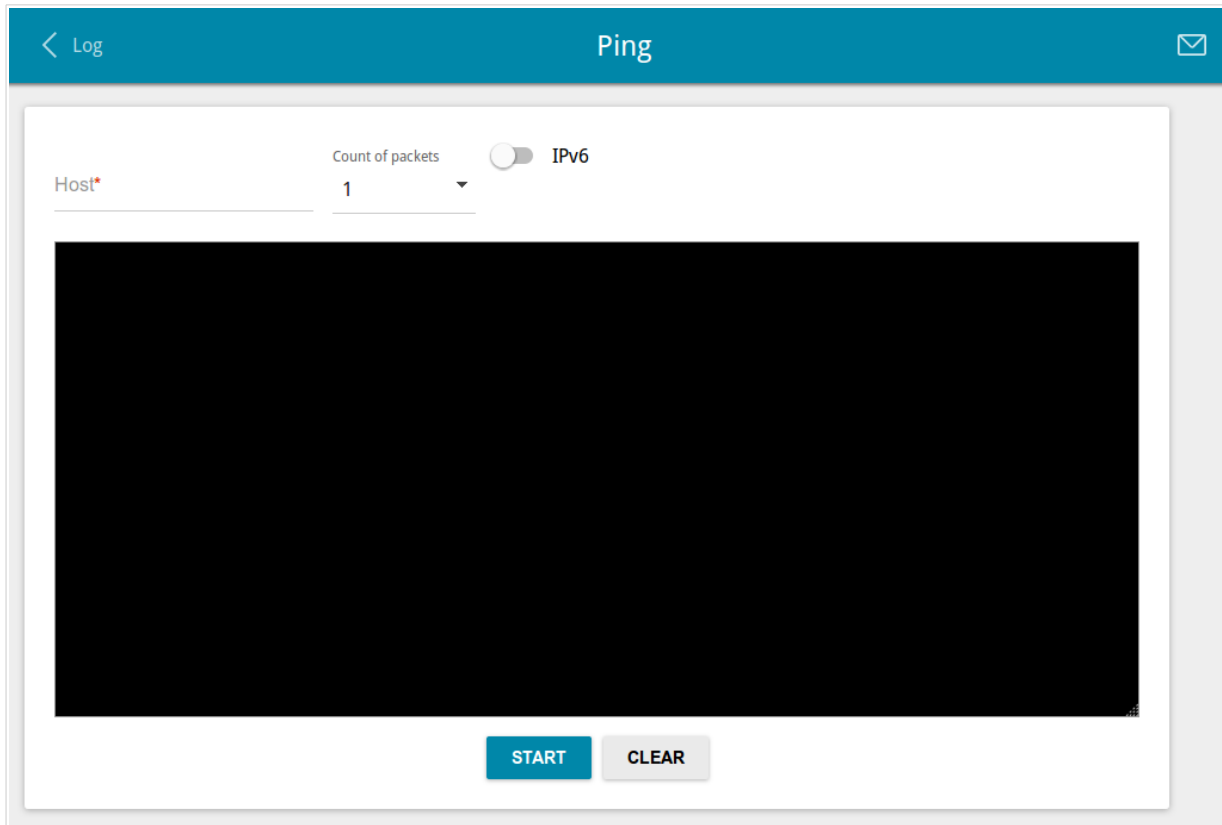
*Figure 127. The **System / Ping** page.*

To check availability of a host, enter the IP address or name of this host in the **Host** field and select a number of requests that will be sent in order to check its availability from the **Count of packets** drop-down list. If availability check should be performed with IPv6, move the **IPv6** switch to the right. Click the **START** button. After a while, the results will be displayed on the page.

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

Traceroute

On the **System / Traceroute** page, you can determine the route of data transfer to a host via the traceroute utility.
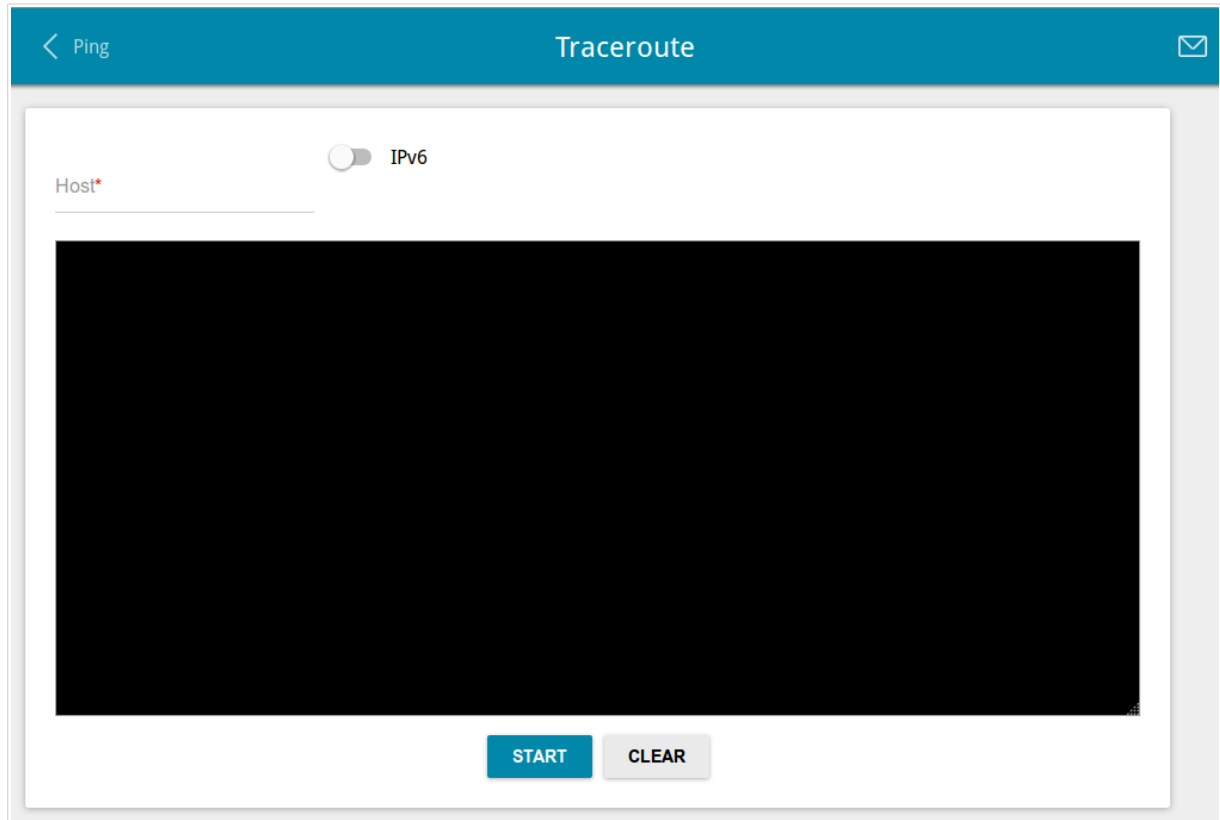
*Figure 128. The **System / Traceroute** page.*

To determine the route, enter the name or IP address of a host in the **Host** field. If the route should be determined using IPv6, move the **IPv6** switch to the right. Click the **START** button. After a while, the results will be displayed on the page.

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

Telnet

On the **System / Telnet** page, you can enable or disable access to the device settings via TELNET from your LAN. By default, access is enabled.
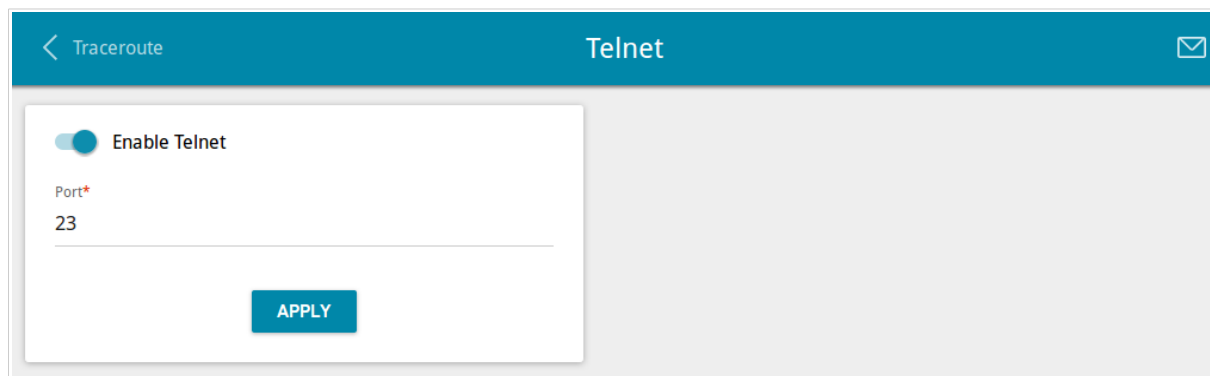
*Figure 129. The **System / Telnet** page.*

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

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

System Time

On the **System / System Time** page, you can manually set the time and date of the router or configure automatic synchronization of the system time with a time server on the Internet.
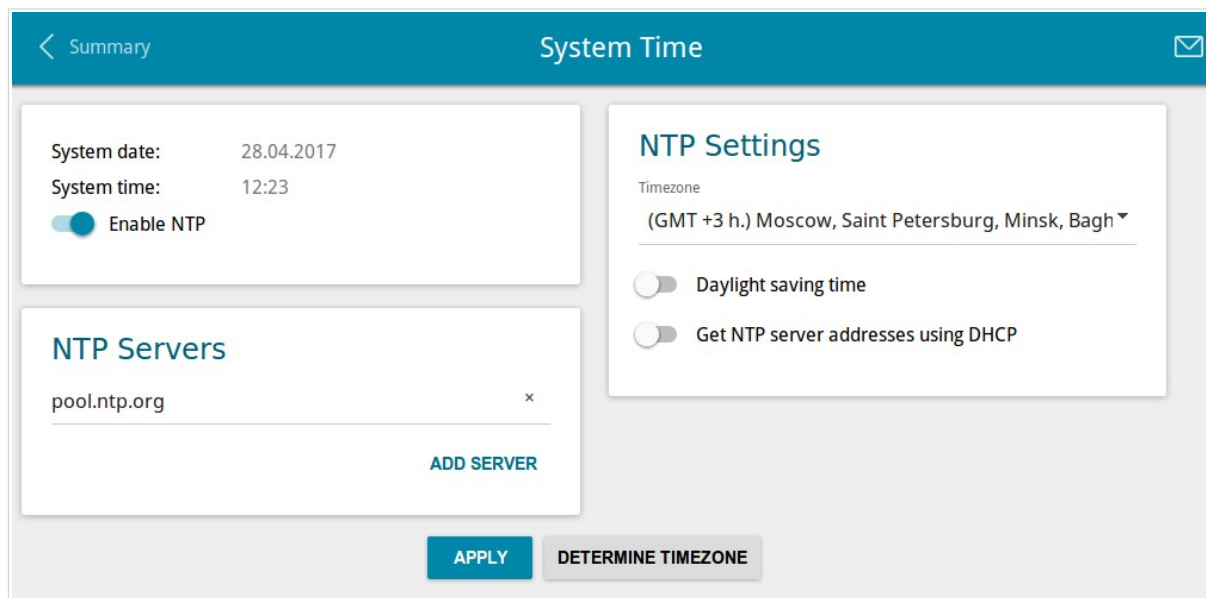
*Figure 130. The **System / System Time** page.*

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 **Timezone** drop-down list in the **NTP Settings** section. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.

4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

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

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

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

Yandex.DNS

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

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

Settings

On the **Yandex.DNS / Settings** page, you can enable the Yandex.DNS service and configure its operating mode.
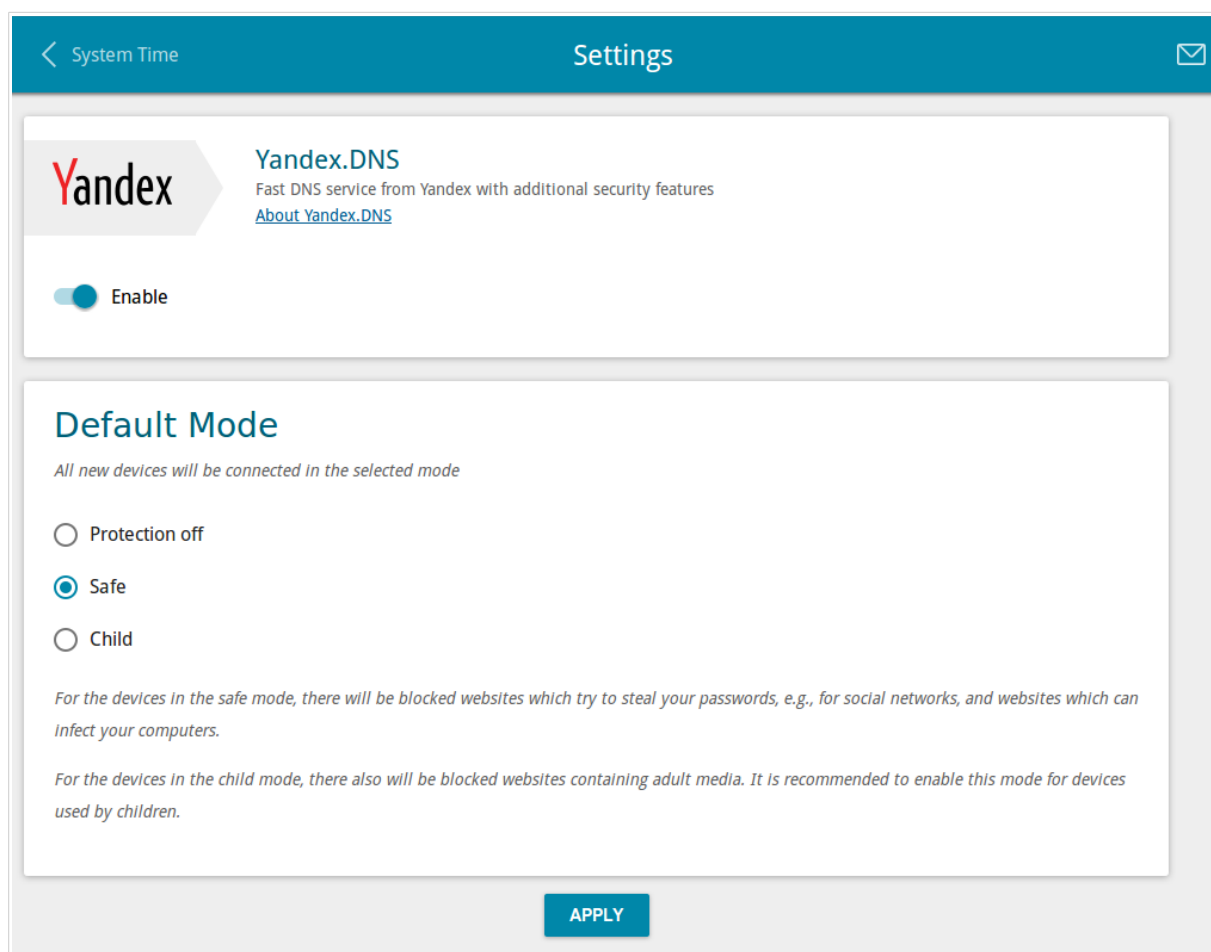
*Figure 131. The **Yandex.DNS / Settings** page.*

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

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

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

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

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

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

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

Devices and Rules

On the **Yandex.DNS / Devices and Rules** page, you can specify a filtering mode for each device separately.
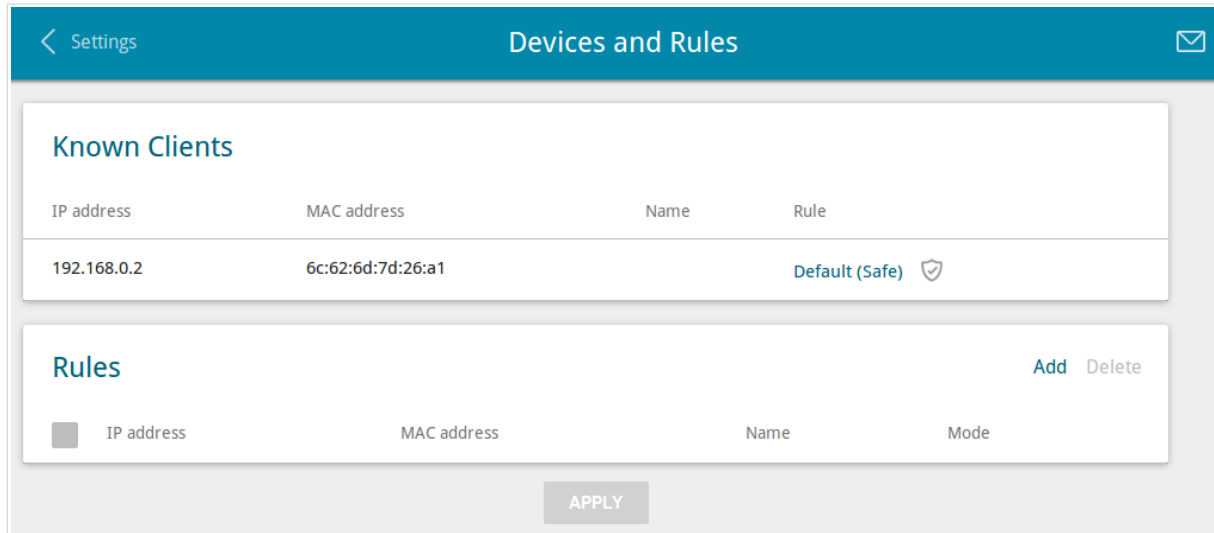
*Figure 132. The **Yandex.DNS / Devices and Rules** page.*

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

To create[5] a new filtering rule for a device, click the **Add** button in the **Rules** section, or left-click the name of the filtering mode in the line of the device for which a rule should be created in the **Known Clients** section.

Figure 133. Adding a new rule for the Yandex.DNS service.

---

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

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

Parameter	Description
MAC address	The MAC address of a device from the router's LAN.
IP address	The IP address of a device from the router's LAN.
Name	Enter a name for the rule for easier identification. *Optional*.
Mode	Select an operating mode of the Yandex.DNS service for this rule. **Protection off**: when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites. **Safe**: when this value is selected, the service blocks access to malicious and fraudulent web sites. **Child**: when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

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

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

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

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

CHAPTER 5.   OPERATION GUIDELINES

Safety Rules and Conditions

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

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

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

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

The service life of the device is 2 years.

Wireless Installation Considerations

The DIR-300S 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-300S device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).

2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone in not in use.

CHAPTER 6.   ABBREVIATIONS AND ACRONYMS

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

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