User Manual

DPN-144DG

GPON ONT Dual Band Wireless AC1200 VoIP Gateway with 1 GPON Port, 4 10/100/1000Base-T Ports, 2 FXS Ports, and 1 USB Port

August 2018

Contents

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the GPON ONT dual band wireless VoIP gateway DPN-144DG 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 gateway's hardware and software features, describes its appearance and the package contents.

Chapter 3 explains how to install the gateway DPN-144DG 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 DPN-144DG device is a GPON ONT dual band wireless VoIP gateway with one GPON port, 3G/LTE support, four 10/100/1000Base-T ports, two FXS ports, and one USB port.

The DPN-144DG is equipped with a USB port for connecting a USB modem[1], which can be used to establish connection to the Internet. In addition, to the USB port of the gateway you can connect a USB storage device, which will be used as a network drive, or a printer.

The gateway DPN-144DG provides an optical line connection to a GPON OLT device. The key advantage of GPON technology is extraordinary bandwidth of the channel. This helps to deliver the next generation of high-speed Internet services to home and office users. DPN-144DG helps to provide a reliable, long-reaching last-mile connection by extending the high-bandwidth public network to people living and working in remote multi-unit buildings.

High-speed broadband access with the rate up to 2.4Gbps allows to provide customers with all high-demand services (such as HD IPTV, VoIP, Internet connection) simultaneously.

Also the device is equipped with two FXS ports which allow connection of analog phones for calls via Internet.

Any Ethernet port of the device can be configured to connect to a private Ethernet line.

Using the DPN-144DG device, you are able to quickly create a high-speed wireless network at home or in your office, which lets computers and mobile devices access the Internet virtually anywhere (within the operational range of your wireless network). Simultaneous activity of 2.4GHz band and 5GHz band allows performing a wide range of tasks. The gateway can operate as a base station for connecting wireless devices of the standards 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac (at the wireless connection rate up to 1167Mbps[2]).

The gateway 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 gateway's WLAN by pressing the button, and devices connected to the LAN ports of the gateway 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, gateway) 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 gateway's LAN.

1 Not included in the delivery package. D-Link does not guarantee compatibility with all USB modems. For the list of supported USB modems, see the ***Specifications**** section, page 8.

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

The VoIP gateway DPN-144DG includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

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

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

You can configure the settings of the gateway DPN-144DG via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

DPN-144DG itself checks the D-Link update server. If a new approved firmware is available, a notification will appear in the web-based interface of the device.

The built-in TR-069 client allows to perform remote configuration and diagnostics of the device independently from the customer.

*Specifications**

Hardware	
Processor	· RTL9607
RAM	· 128MB, DDR3
Flash	· 128MB, NAND
Interfaces	· GPON port (SC/APC connector) · 4 10/100/1000BASE-T LAN ports · 2 RJ-11 FXS ports · USB 2.0 port
LEDs	· Power · PON · LOS · 4 LAN LEDs · 2 Phone LEDs · WIFI 2.4GHz · WIFI 5GHz · WPS · USB · Internet
Buttons	· POWER 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	· Two internal antennas (3.5dBi gain for 2.4GHz and 5GHz)

PON	
GPON features	· Class B+ GPON optical transceiver · Upstream (transmitter): 1310nm ± 50nm, 1.244Gbps upstream burst data rate · Downstream (digital receiver): 1490nm ± 10nm, 2.488Gbit/s downstream continuous data rate · Single mode fiber cable · AES encryption · Support of IGMP v1/v2 Snooping, 16 entries, enable/disable, Fast leaving · MAC learning · UNI port configuration (rate, duplex mode, flow control, disable/enable, auto mode) · Maximum frame length to 1522 bytes · Compliance to ONT dying gasp · ONT authentication

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

Phone	
General SIP features	· Individual account per port · Invite with Challenge · Register by IP address or domain name of SIP server · Backup proxy support · Support of DHCP option 120 · RFC3986 SIP URI format support · Outbound proxy support · STUN client · NAT keep-alive · Call types: voice/modem/fax · User programmable Dial Plan · Manual peer table (P2P) · E.164 Numbering, ENUM support
Call features	· Direct IP-to-IP call without SIP proxy · Call hold/retrieve · Call awaiting · Forwarding (unconditional, busy, no answer) · Do Not Disturb · Blocking hidden number calls · Speed dialing · Phone book · Hotline · Vertical service codes · Filtering by IP address (white/black list) · Alarm clock
Voice features	· Codecs: G.711 a/μ-law, G.729A, G.726, G.722, G.723.1 · DTMF detection and generation · In-band DTMF, out-of-band DTMF (RFC2833, SIP-INFO) · Comfort Noise Generation (CNG) · Voice Activity Detection (VAD) · Dynamic Jitter Buffer · Call progress tone generation (FXS) · DTMF/PULSE dial support · Caller ID detection and generation · T.30 FAX bypass to G.711, T.38 Real Time FAX Relay · Adjustable Flash Time · Volume control (speaker/microphone)

Software	
WAN connection types	· Static IPv4 / Dynamic IPv4 · Static IPv6 / Dynamic IPv6 · PPPoE · PPPoE IPv6 · PPPoE Dual Stack · PPTP/L2TP · 3G/LTE[3]

3 In the next firmware versions.

Software	
Network functions	· Support of IEEE 802.1X for Internet connection · 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 · Support of MVR · 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
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 · IPsec tunnels
USB interface functions	· USB modem[4] Auto connection to available type of supported network (4G/3G/2G) Auto configuration of connection upon plugging in USB modem Enabling/disabling PIN code check, changing PIN code[5] · USB storage File browser Print server Access to storage via accounts Built-in Samba server Built-in FTP server Built-in DLNA server Built-in Transmission torrent client; uploading/downloading files from/to USB storage
Management	· Local and remote access to settings through TELNET/WEB (HTTP/HTTPS) · Bilingual web-based interface for configuration and management (Russian/English) · 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 remote logging · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility · TR-069 client

4 In the next firmware versions.

5 For GSM USB modems and some models of LTE USB modems.

Wireless Module Parameters	
Standards	· IEEE 802.11a/n/ac · IEEE 802.11b/g/n
Frequency range	· 2400 ~ 2483.5MHz · 5150 ~ 5350MHz · 5650 ~ 5725MHz
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 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11b: 1, 2, 5.5, and 11Mbps · IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11n (2.4GHz/5GHz): from 6.5 to 300Mbps (from MCS0 to MCS15) · IEEE 802.11ac (5GHz): from 6.5 to 867Mbps (from MCS0 to MSC9)

Physical Parameters	
Dimensions (L x W x H)	· 228 x 160 x 41 mm (9 x 6.3 x 1.6 in)

Operating Environment	
Power	· Output: 12V DC, 2.5A
Temperature	· Operating: from 0 to 40 °C · Storage: from -40 to 70 °C
Humidity	· Operating: from 10% to 90% (non-condensing) · Storage: from 5% to 95% (non-condensing)

Supported USB modems[6]	
GSM	· Alcatel X500 · D-Link DWM-152C1 · D-Link DWM-156A6 · D-Link DWM-156A7 · D-Link DWM-156C1 · D-Link DWM-157B1 · D-Link DWM-157B1 (Velcom) · D-Link DWM-158D1 · D-Link DWR-710 · Huawei E150 · Huawei E1550 · Huawei E156G · Huawei E160G · Huawei E169G · Huawei E171 · Huawei E173 (Megafon) · Huawei E220 · Huawei E3131 (MTS 420S) · Huawei E352 (Megafon) · Prolink PHS600 · Prolink PHS901 · ZTE MF112 · ZTE MF192 · ZTE MF626 · ZTE MF627 · ZTE MF652 · ZTE MF667 · ZTE MF668 · ZTE MF752
LTE	· Huawei E3131 · Huawei E3272 · Huawei E3351 · Huawei E3372 · Huawei E367 · Huawei E392 · Megafon M100-1 · Megafon M100-2 · Megafon M100-3 · Megafon M100-4 · Megafon M150-1 · Megafon M150-2 · Quanta 1K6E (Beeline 1K6E) · MTS 824F · MTS 827F · Yota LU-150 · Yota WLTUBA-107 · ZTE MF823 · ZTE MF827
Smartphones in USB tethering mode	· Some models of Android smartphones

6 The manufacturer does not guarantee proper operation of the gateway with every modification of the firmware of USB modems.

Product Appearance

Front and Right Side Panels

Figure 1. Front panel view.

LED	Mode	Description
Power	*Solid green*	The gateway is powered on.
	No light	The gateway is powered off.
PON	*Solid green*	The gateway is synchronized with the OLT device.
	Blinking green	Synchronization with the OLT device is in progress.
	No light	The fiber optic cable is not connected.
LOS	*Blinking red*	The fiber optic cable is not connected.
	No light	• The gateway is synchronized with the OLT device, or • synchronization with the OLT device is in progress.
LAN 1-4	*Solid green*	A device (computer) is connected to the port, the connection is on.
	Blinking green	Data transfer through the relevant LAN port.
	No light	The cable is not connected to the port.
Phone 1-2	*Solid green*	The phone is registered on the SIP server.
	Blinking green	Dialing a number, making or accepting a call.
	No light	The phone is not registered on the SIP server.

LED	Mode	Description
WIFI 2.4GHz **WIFI 5GHz**	*Solid green*	The gateway's WLAN of the relevant band is on.
	Blinking green	Data transfer through the Wi-Fi network of the relevant band.
	No light	The gateway's WLAN of the relevant band is off.
WPS	*Blinking green*	Attempting to add a wireless device via the WPS function.
	No light	The WPS function is not in use.
USB	*Solid green*	A USB device is connected to the gateway's USB port.
	No light	No USB device.
Internet	*Solid green*	The connection is on.
	No light	The connection is off.

On the right side panel of the gateway there is a **WPS** button designed 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 enable/disable the gateway's wireless network: with the device turned on, press the button, hold for 10 seconds, and then release it. The **WIFI 2.4GHz** and **WIFI 5GHz** LEDs should turn off.

Back Panel

Figure 2. Back panel view.

Name	Description
USB	A port for connecting a USB device (modem, storage, printer).
LAN 1-4	4 Ethernet ports to connect computers or network devices. One port can be used to connect to a private Ethernet line.
PHONE1 **PHONE2**	Ports to connect analog phones.
PON	An optical port to connect to a fiber optic line.
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.
12V-2.5A	Power connector.
POWER ON/OFF	A button to turn the gateway on/off.

The device is also equipped with two built-in Wi-Fi antennas.

Delivery Package

The following should be included:

- GPON ONT VoIP gateway DPN-144DG
- Power adapter DC 12V/2.5A
- "***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 GPON ONT dual band wireless VoIP gateway with fiber GPON port DPN-144DG (hereinafter referred to as "the gateway") 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 gateway 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 gateway.

Wireless Connection

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

VoIP

In order to use VoIP over SIP, you need to connect an analog phone to the FXS port of the gateway. Then access the web-based interface of the gateway, and you will be able to configure all needed settings.

USB Modem

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

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

Some operators require subscribers to activate their USB modems prior to using them. Please, refer to connection guidelines provided by your operator when concluding the agreement or placed on its website.

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

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

Connecting to PC

! Invisible laser radiation may be emitted from the end of the fiber and/or from DPN-144DG. Take all necessary precautions to avoid unnecessary exposure to this radiation.

PC with Ethernet Adapter

1. Connect an Ethernet cable between any of LAN ports located on the back panel of the gateway and the Ethernet port of your PC.
2. ***To connect via USB modem***: connect your USB modem to the USB port[8] located on the back panel of the gateway.

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

3. ***To connect the device to a fiber optic line***: connect the fiber optic cable to the PON port on the back panel of the gateway. Make sure that center conductor of the cable is inserted directly into the center of the PON connector. Secure the cable by carefully pushing the fiber connector onto the PON connector until tight. Be careful not to over-tighten the connector or you may damage either the cable or the device.
4. ***To connect the device to an Ethernet line***: in the web-based interface of the gateway, select the gateway's LAN port that will be used as the WAN port and create an Ethernet WAN connection. Then connect an Ethernet cable between an available Ethernet port of the gateway and the Ethernet line.

! Please connect the gateway to the ISP's Ethernet line only after setting the WAN port and creating the Internet connection.

5. Connect a phone cable between an FXS port of the gateway and the phone.
6. Connect the power cord to the power connector port on the back panel of the gateway, then plug the power adapter into an electrical outlet or power strip.
7. Turn on the gateway by pressing the **POWER ON/OFF** button on its back panel.
8. Wait for several minutes. When the device receives all needed settings, the **PON** LED will stop blinking and will light solid green. When the Internet connection is established, the **Internet** LED will light solid green.

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

8 It is recommended to use a USB extension cable to connect a USB modem to the gateway.

Obtaining IP Address Automatically (OS Windows 7)

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

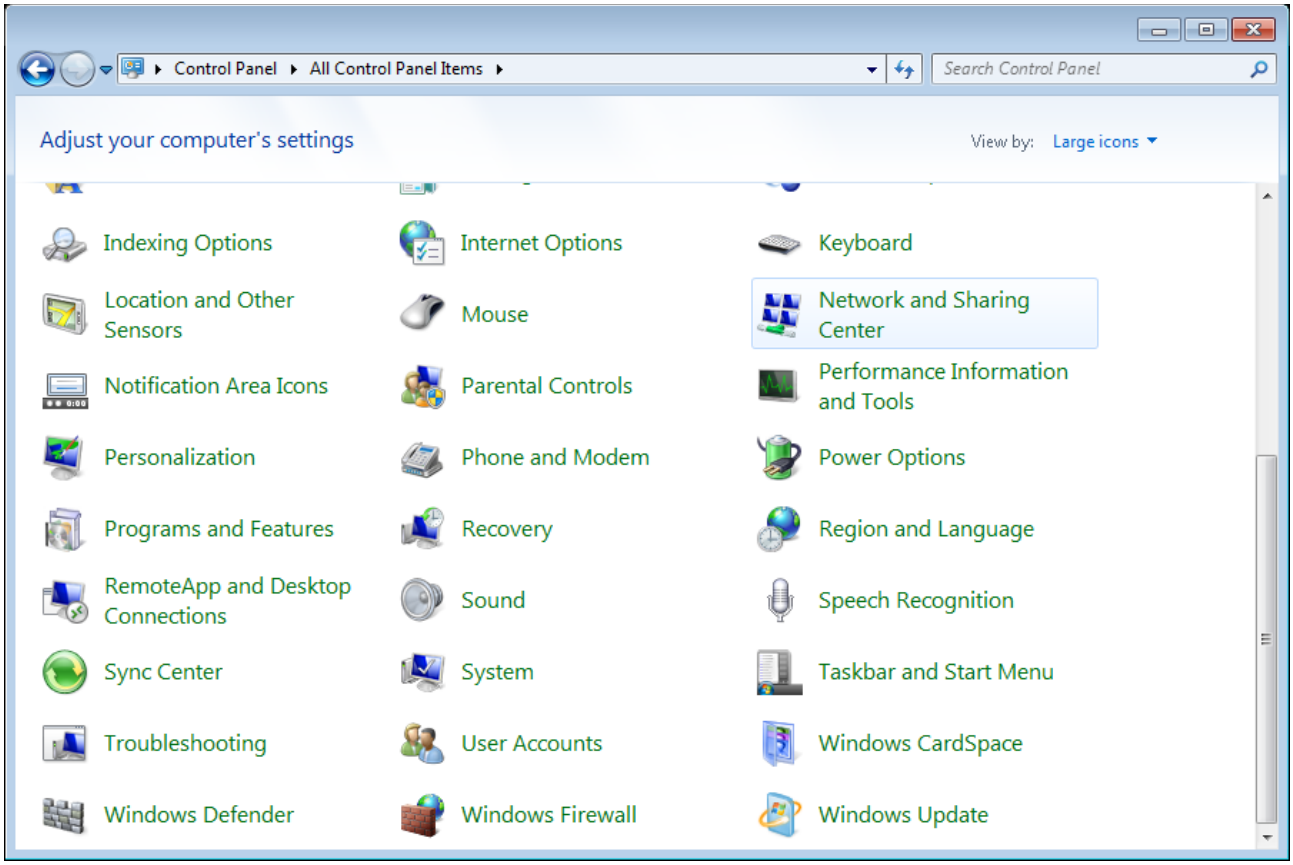

*Figure 3. The **Control Panel** window.*

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

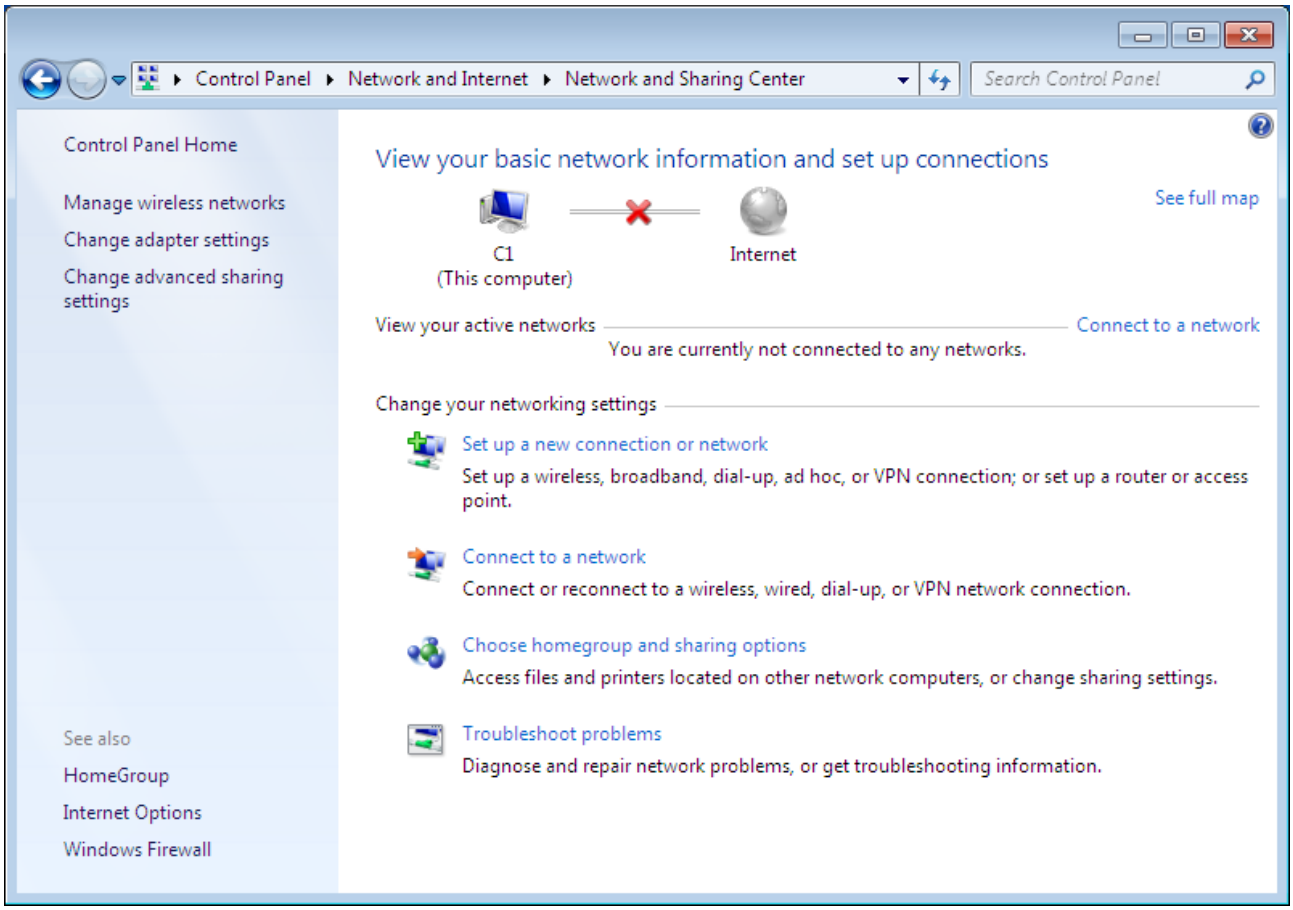

*Figure 4. The **Network and Sharing Center** window.*

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

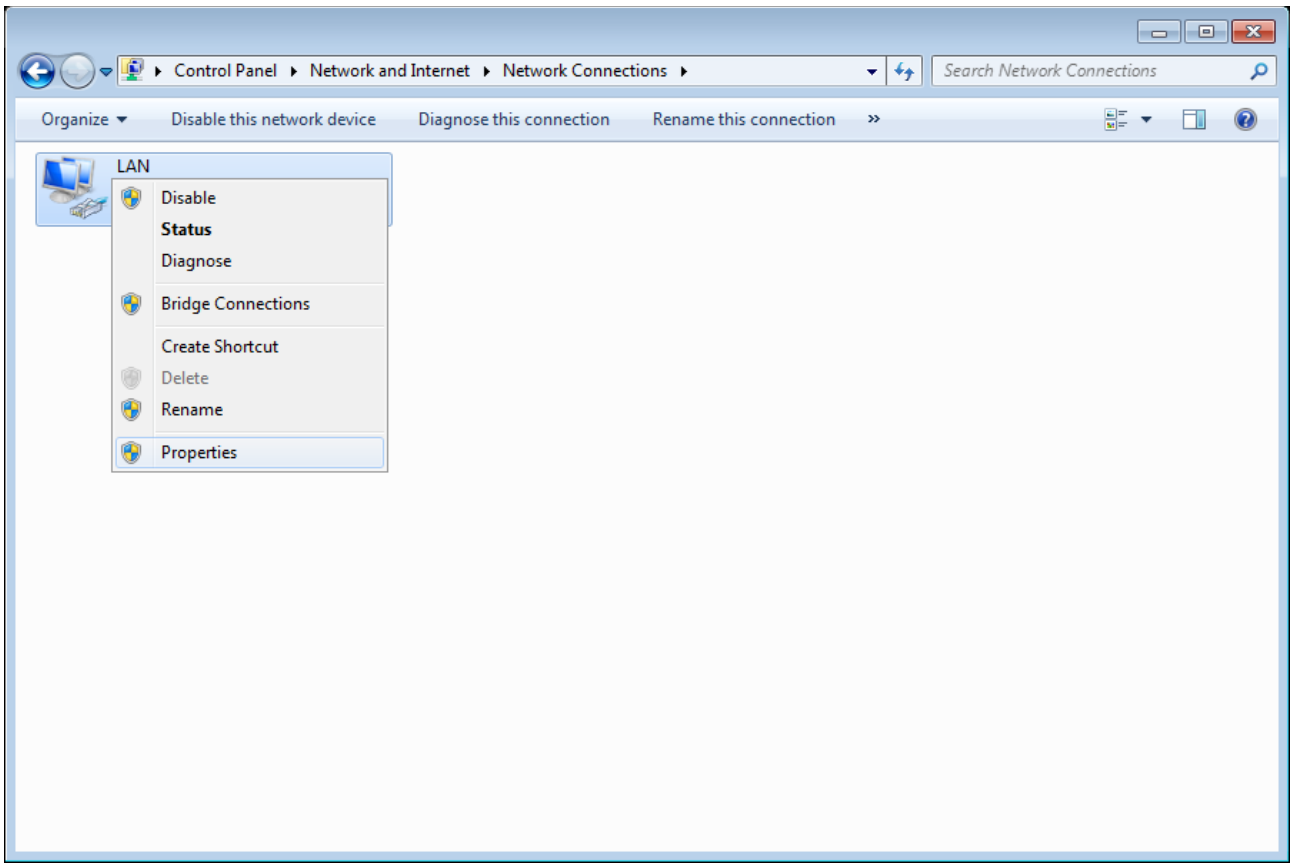

*Figure 5. The **Network Connections** window.*

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

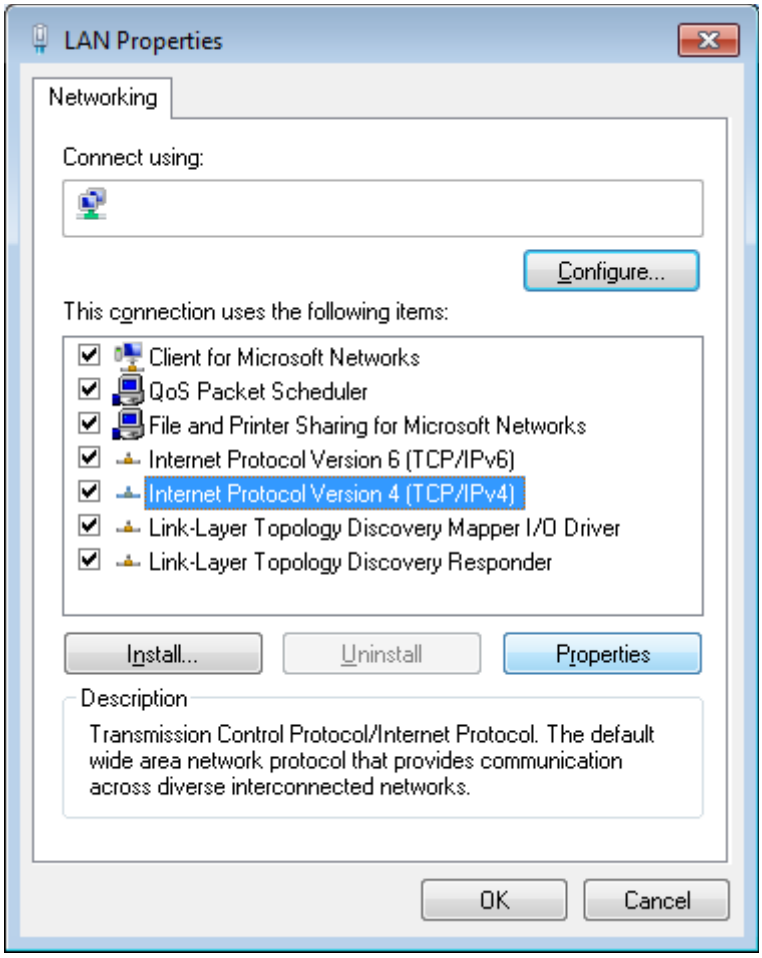

*Figure 6. The **Local Area Connection Properties** window.*

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

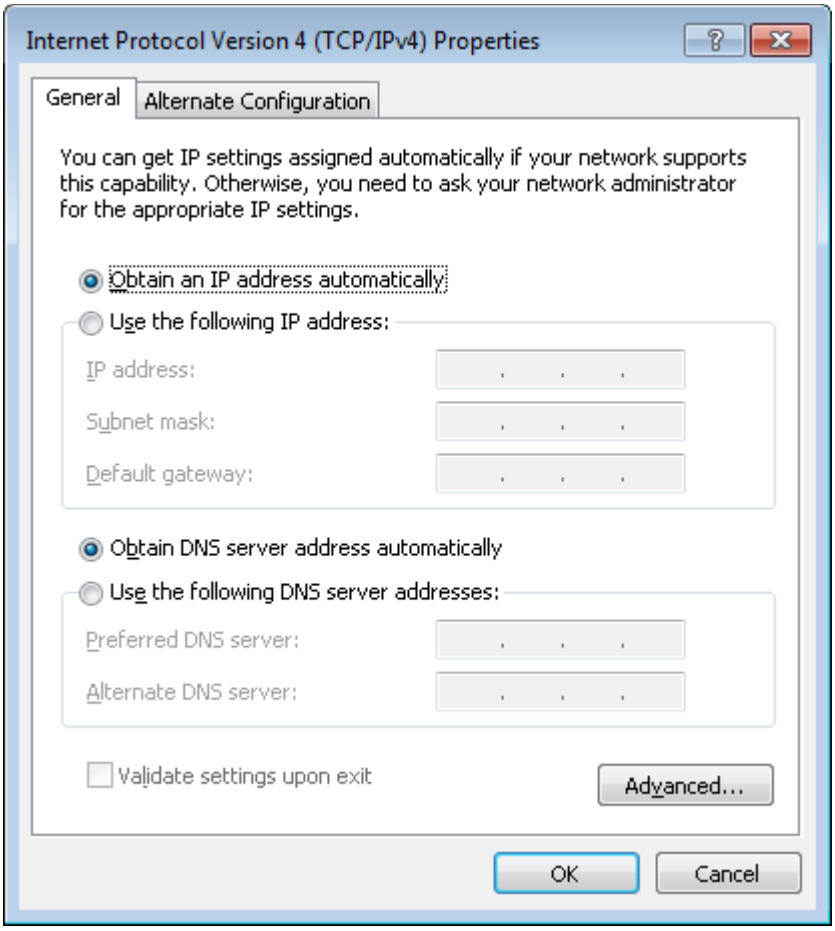

*Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

PC with Wi-Fi Adapter

1. ***To connect via USB modem***: connect your USB modem to the USB port[9] located on the back panel of the gateway.

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

2. ***To connect the device to a fiber optic line***: connect the fiber optic cable to the PON port on the back panel of the gateway. Make sure that center conductor of the cable is inserted directly into the center of the PON connector. Secure the cable by carefully pushing the fiber connector onto the PON connector until tight. Be careful not to over-tighten the connector or you may damage either the cable or the device.
3. ***To connect the device to an Ethernet line***: in the web-based interface of the gateway, select the gateway's LAN port that will be used as the WAN port and create an Ethernet WAN connection. Then connect an Ethernet cable between an available Ethernet port of the gateway and the Ethernet line.

! Please connect the gateway to the ISP's Ethernet line only after setting the WAN port and creating the Internet connection.

4. Connect the power cord to the power connector port on the back panel of the gateway, then plug the power adapter into an electrical outlet or power strip.
5. Turn on the gateway by pressing the **POWER ON/OFF** button on its back panel.
6. Make sure that your Wi-Fi adapter is on. As a rule, modern notebooks with built-in wireless NICs are equipped with a button or switch that turns on/off the wireless adapter (refer to your PC documents). If your PC is equipped with a pluggable wireless NIC, install the software provided with your Wi-Fi adapter.

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

9 It is recommended to use a USB extension cable to connect a USB modem to the gateway.

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

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

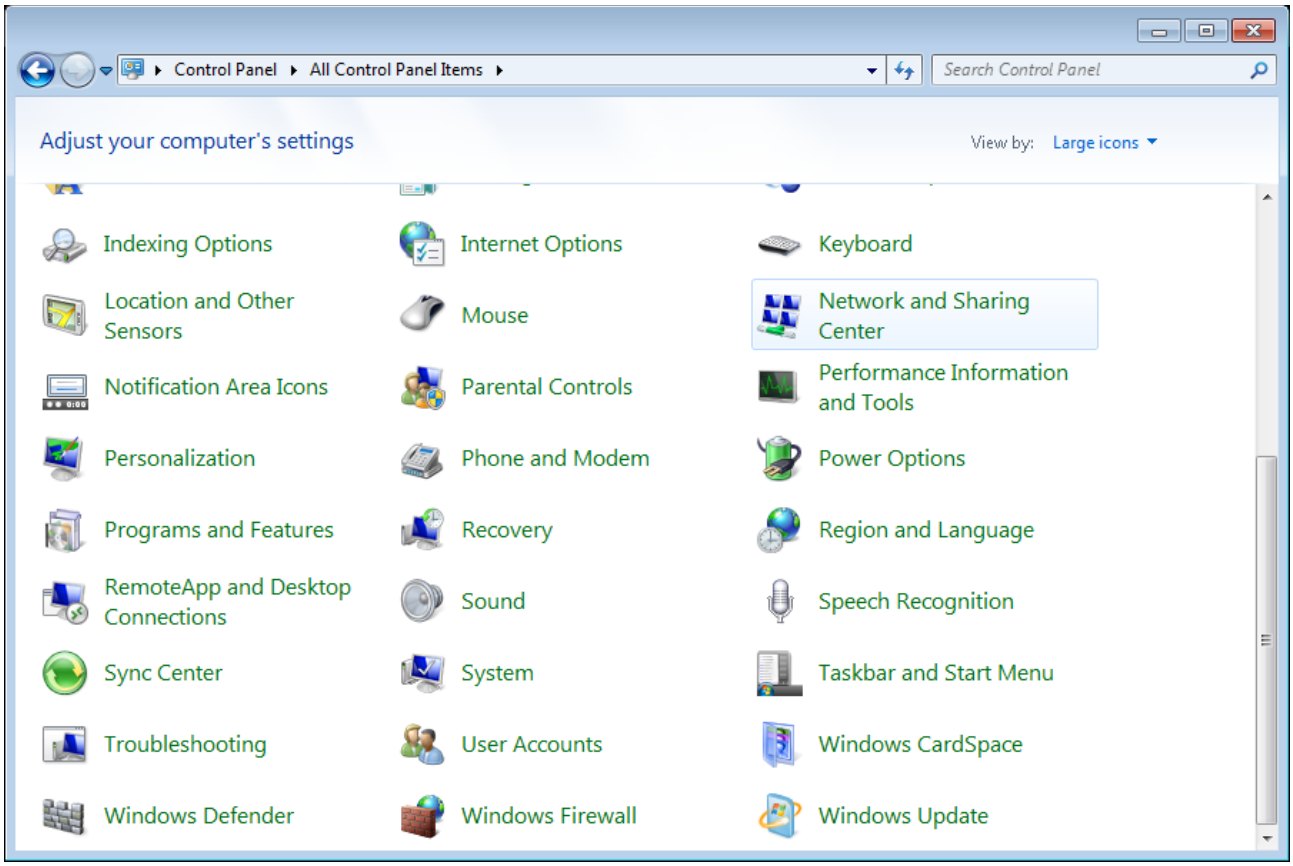

*Figure 8. The **Control Panel** window.*

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

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

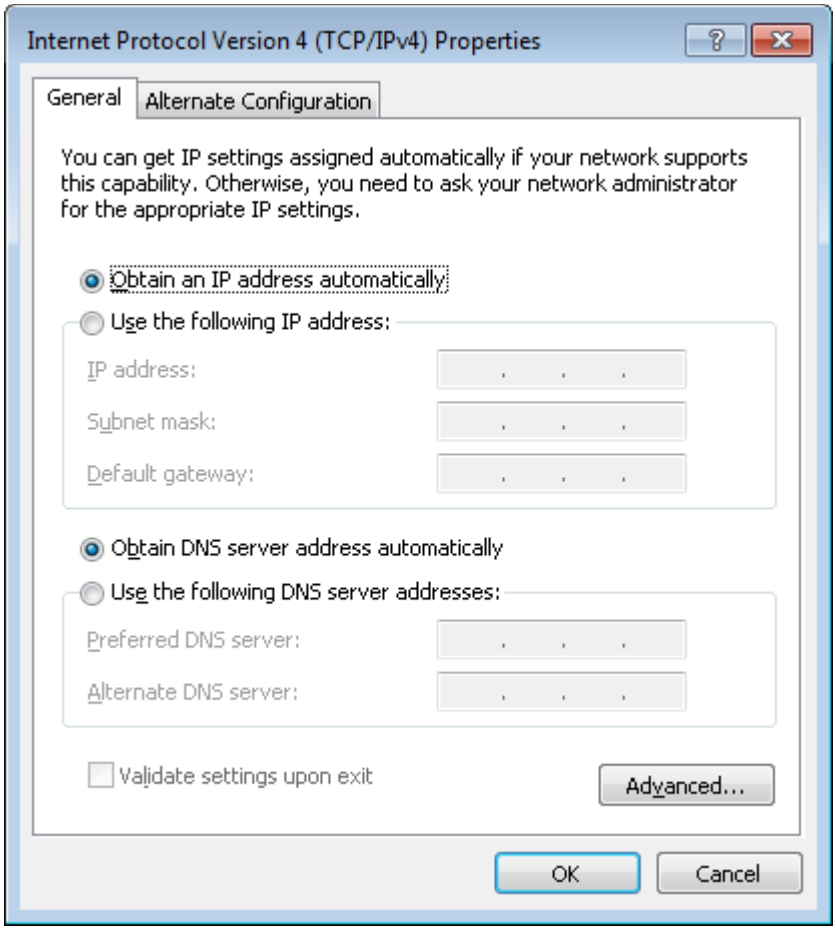

*Figure 9. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.*

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

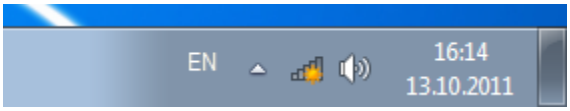

Figure 10. The notification area of the taskbar.

9. In the opened **Wireless Network Connection** window, select the wireless network **DPN-144DG** (for operating in the 2.4GHz band) or **DPN-144DG-5G** (for operating in the 5GHz band) and click the **Connect** button.

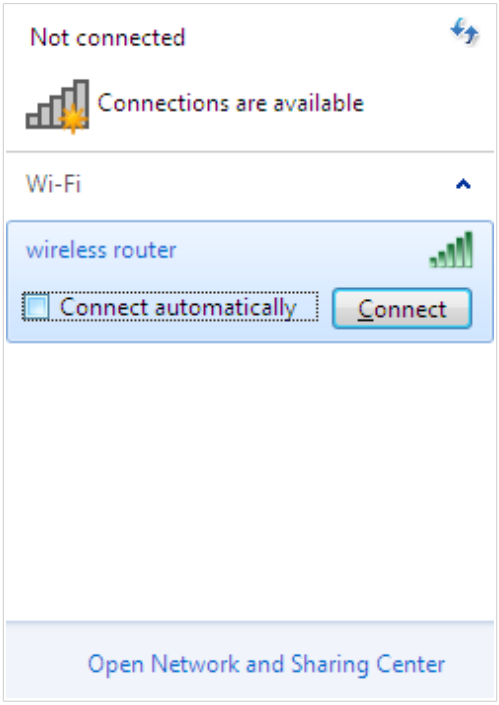

Figure 11. The list of available networks.

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

If you perform initial configuration of the gateway via Wi-Fi connection, note that immediately after changing the wireless default settings of the gateway 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, configure VoIP, specify the settings of the firewall, etc.).

For security reasons, DPN-144DG 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 17). In the address bar of the web browser, enter the IP address of the gateway (by default, `192.168.0.1`). Press the **Enter** key.

Figure 12. Connecting to the web-based interface of the DPN-144DG 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 gateway, make sure that you have properly connected the gateway 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 page opens (see the ***Initial Configuration*** section, page 36).

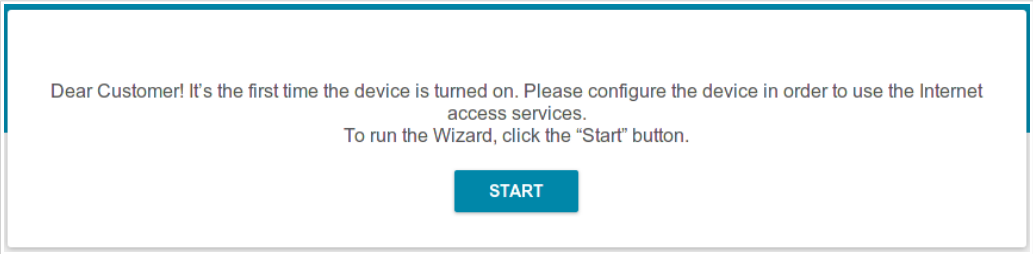

Figure 13. The Initial Configuration page.

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

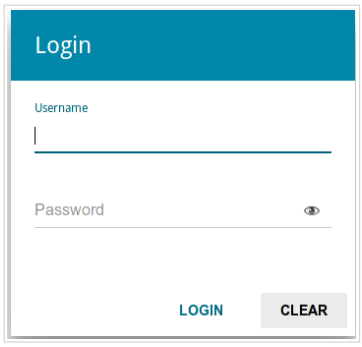

Figure 14. The login page.

Web-based Interface Structure

Summary Page

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

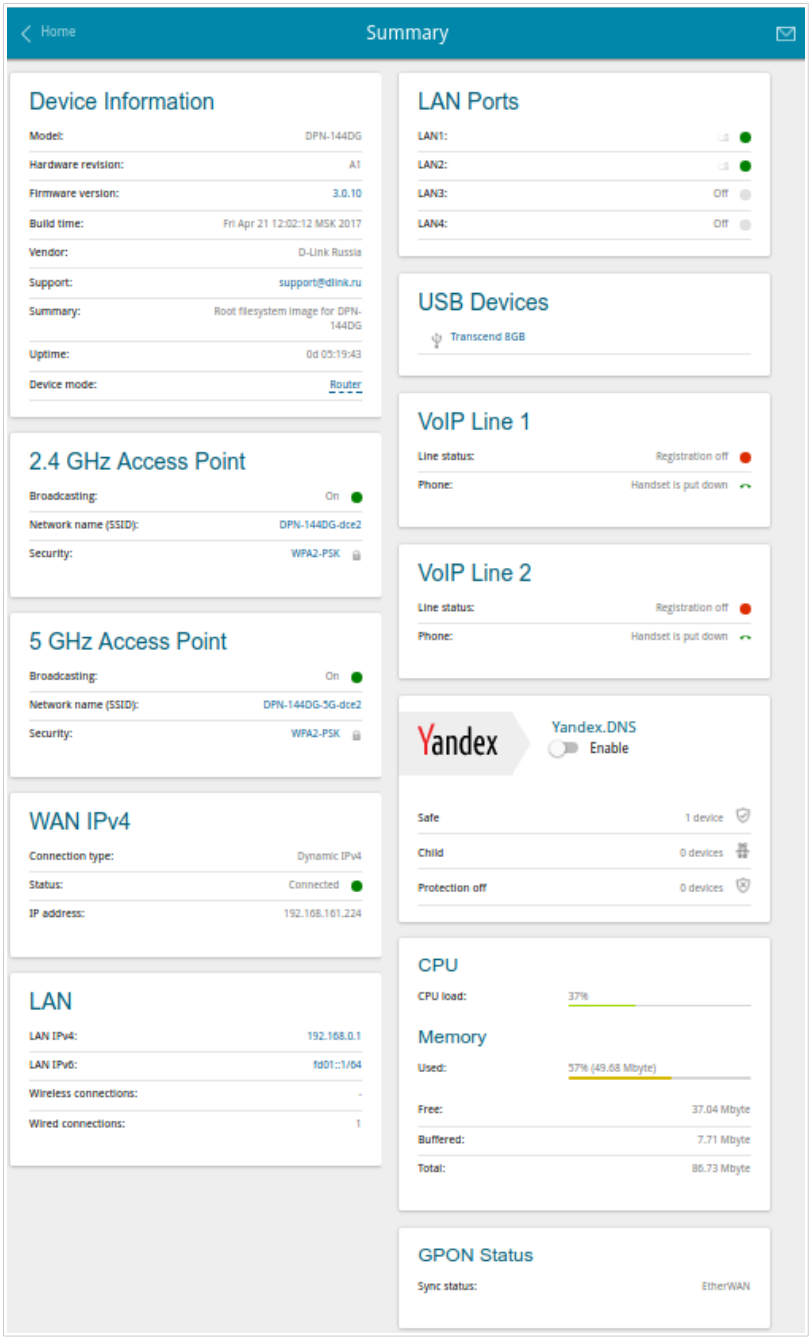

Figure 15. The summary page.

The **Device Information** section displays the model and hardware version of the gateway, 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.

The **2.4 GHz Access Point** and **5 GHz Access Point** sections display data on the state of the device's wireless network, its name and the authentication type in the relevant band.

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

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

The **USB Devices** section displays the device connected to the USB port of the gateway.

In the **VoIP Line 1** and **VoIP Line 2** sections, data on the status of registration on the SIP proxy server and the phone status are displayed.

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.

The **GPON Status** section displays the state of synchronization with the OLT.

Home Page

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

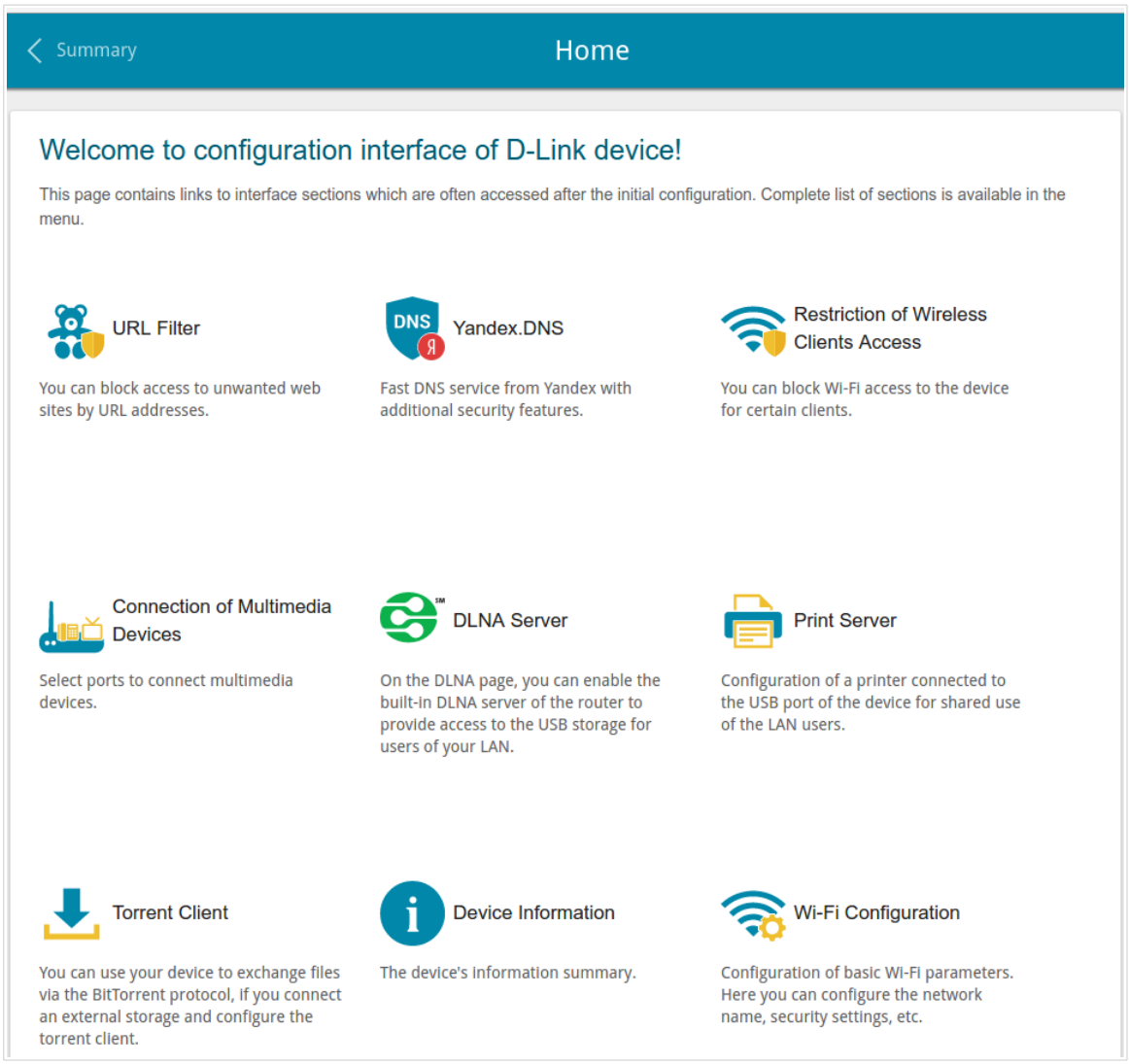

*Figure 16. The **Home** page.*

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

Menu Sections

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

In the **Initial Configuration** section, you can specify parameters necessary for getting started (for the description of the Initial Configuration, see the ***Initial Configuration*** section, page 36).

The pages of the **Statistics** section display data on the current state of the gateway (for the description of the pages, see the ***Statistics*** section, page 41).

The pages of the **Connections Setup** section are designed for configuring basic parameters of the LAN interface of the gateway and creating a connection to the Internet (for the description of the pages, see the ***Connections Setup*** section, page 48).

The pages of the **Wi-Fi** section are designed for specifying all needed settings of the gateway's wireless network (for the description of the pages, see the ***Wi-Fi*** section, page 87).

The **Print Server** section is designed for configuring the gateway as a print server (see the ***Print Server*** section, page 114).

The pages of the **USB Storage** section are designed for operating the connected USB storage (for the description of the pages, see the ***USB Storage*** section, page 115).

The pages of the **USB Modem** section are designed for operating the connected 3G or LTE USB modem (for the description of the pages, see the ***USB Modem*** section, page 126).

The pages of the **Advanced** section are designed for configuring additional parameters of the gateway (for the description of the pages, see the ***Advanced*** section, page 130).

The pages of the **VoIP** section are designed for specifying all settings needed for VoIP (for the description of the pages, see the ***VoIP*** section, page 161).

The pages of the **Firewall** section are designed for configuring the firewall of the gateway (for the description of the pages, see the ***Firewall*** section, page 185).

The pages of the **System** section provide functions for managing the internal system of the gateway (for the description of the pages, see the ***System*** section, page 196).

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 209).

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

Notifications

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

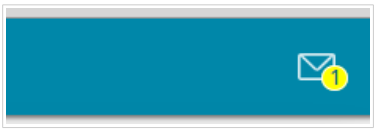

Figure 17. The web-based interface notifications.

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

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration

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

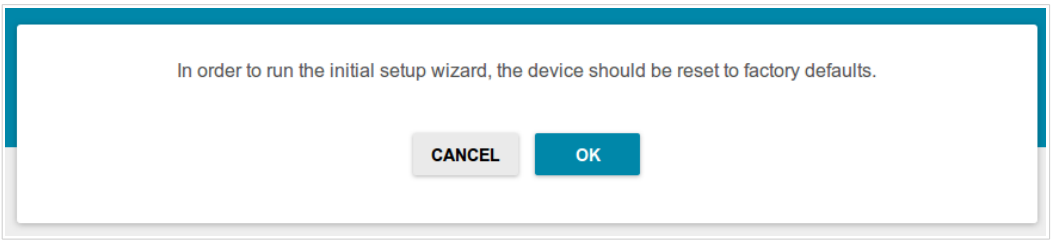

Figure 18. Restoring the default settings.

If you perform initial configuration of the gateway via Wi-Fi connection, please make sure that you are connected to the wireless network of DPN-144DG (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

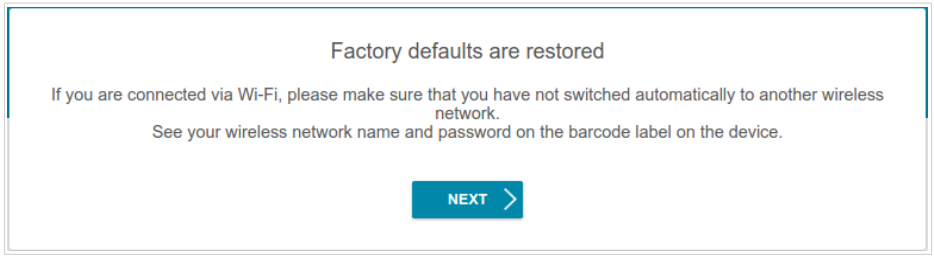

Figure 19. Checking connection to the wireless network.

Click the **START** button.

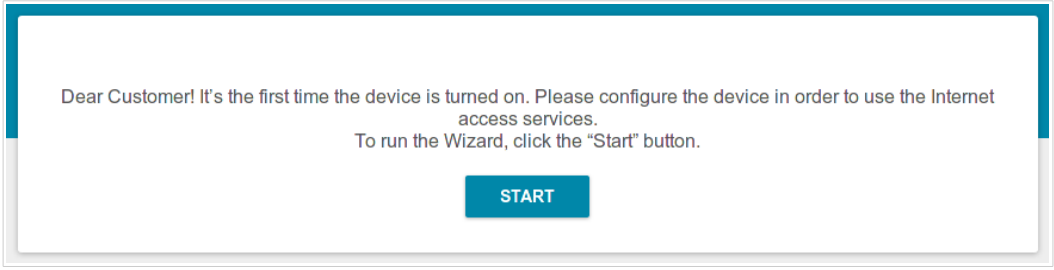

Figure 20. The initial configuration page.

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

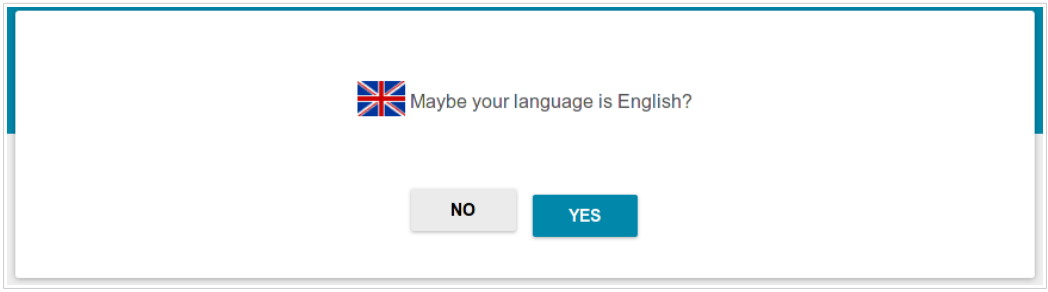

Figure 21. Selecting a language.

On the next page, change the default settings: specify the administrator password in the **Admin password** field and the name of the wireless network in the 2.4GHz and 5GHz bands in the **Network name 2.4GHz (SSID)** and **Network name 5GHz (SSID)** fields correspondingly. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[10]

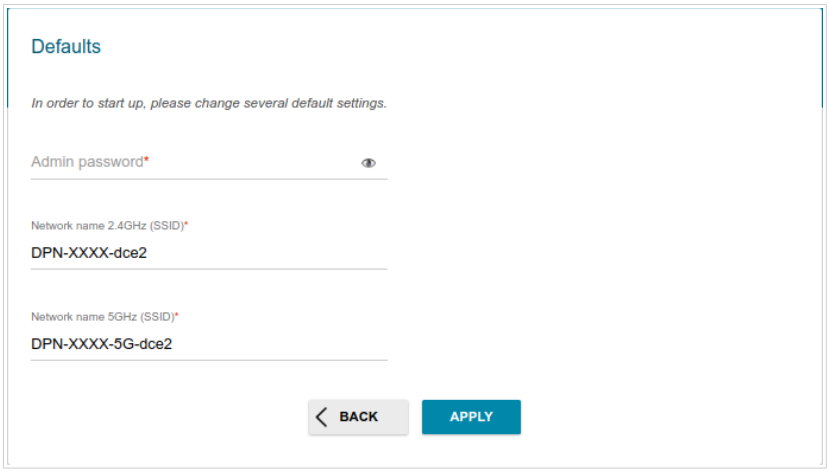

Figure 22. Changing the default settings

! 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 gateway only after restoring the factory default settings via the hardware **RESET** button. This procedure wipes out all settings that you have configured for your gateway.

Click the **APPLY** button to continue or click the **BACK** button to return to the previous page. After clicking the **APPLY** button, the **Home** page opens (see the ***Home Page*** section, page 33).

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

Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports or available wireless interfaces of the gateway for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DPN-144DG 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.

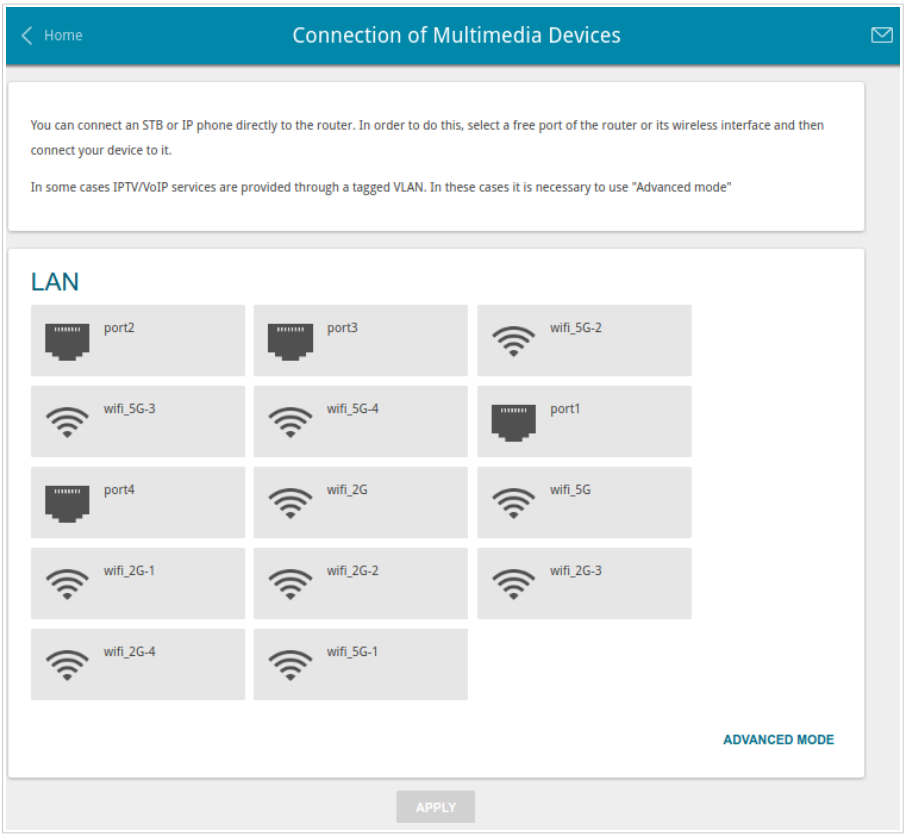

Figure 23. The Multimedia Devices Connection Wizard. The simple mode.

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

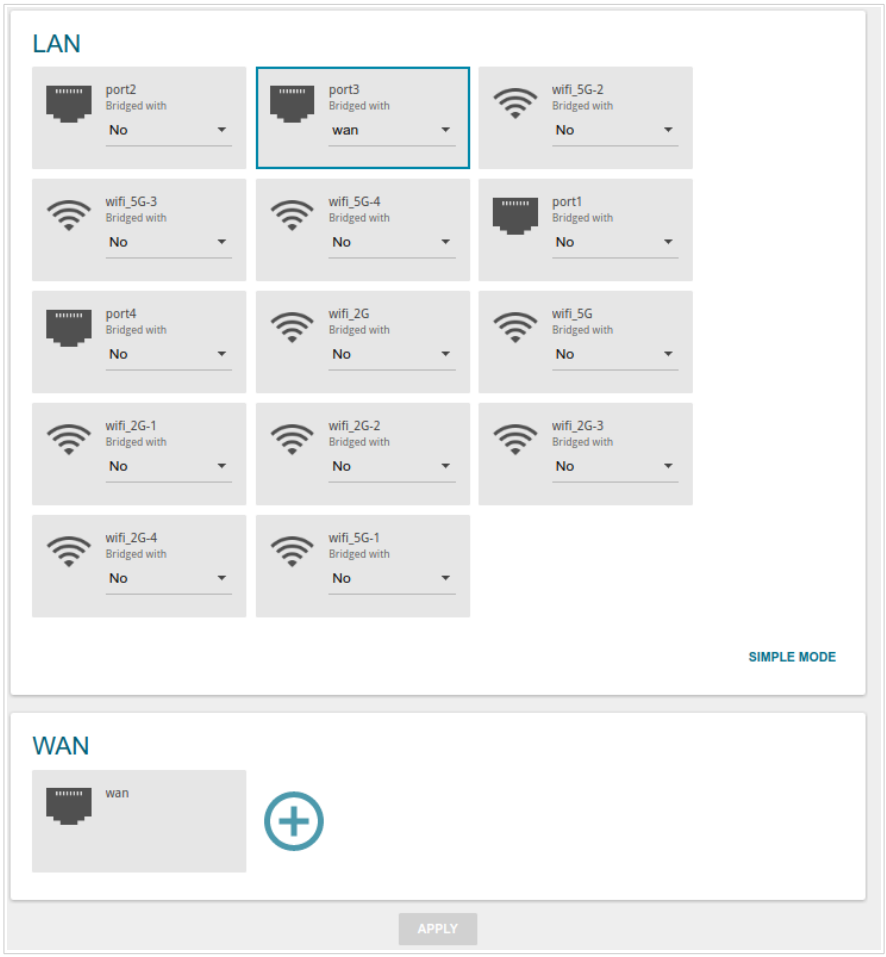

Figure 24. The Multimedia Devices Connection Wizard. The advanced mode.

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

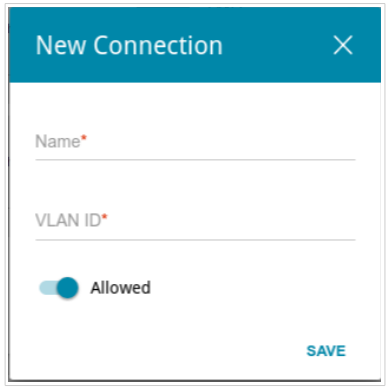

Figure 25. Adding a connection.

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 gateway:

- network statistics
- statistics for the PON interface
- IP addresses leased by the DHCP server
- the routing table
- data on devices connected to the gateway's network and its web-based interface
- 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). 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).

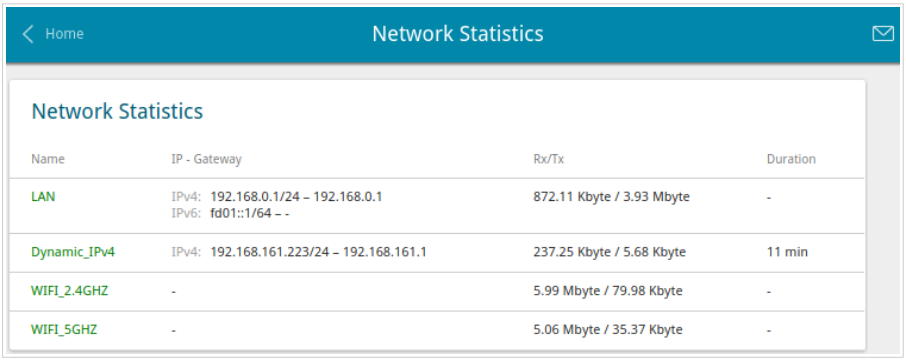

*Figure 26. The **Statistics / Network Statistics** page.*

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

PON Statistics

On the **Statistics / PON Statistics** page, you can view statistics for the PON interface (volume of data transmitted/received, number of packets of different types, and number of errors).

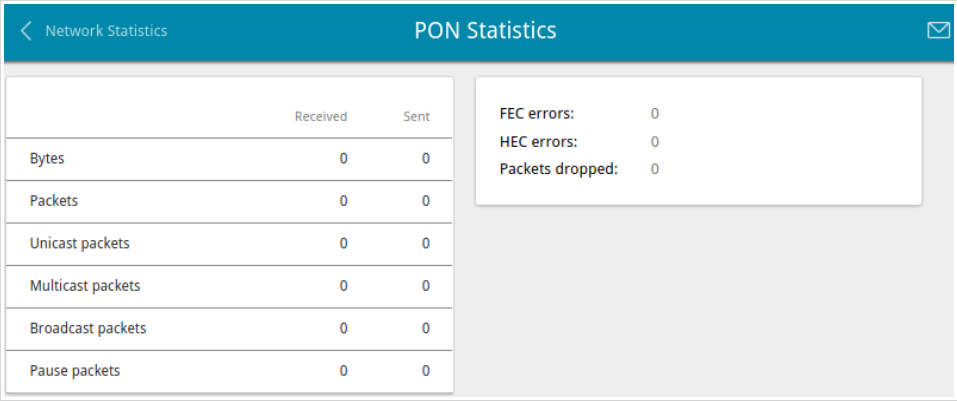

*Figure 27. The **Statistics / PON Statistics** page.*

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).

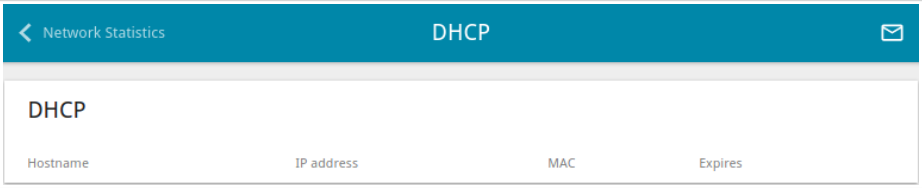

*Figure 28. The **Statistics / DHCP** page.*

Routing Table

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

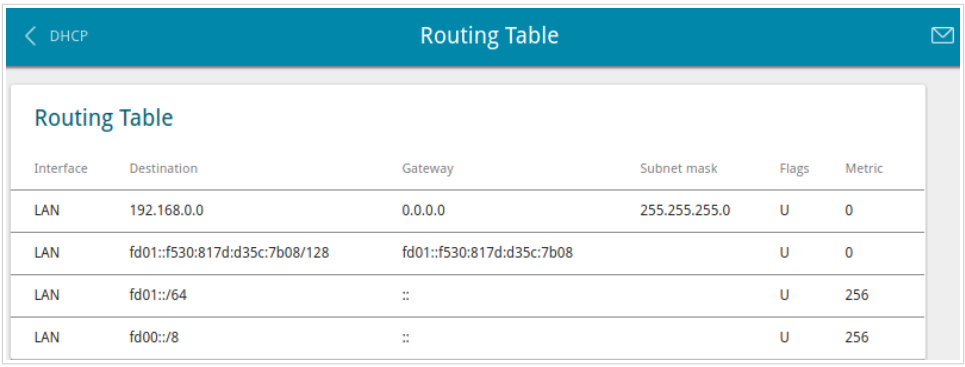

*Figure 29. The **Statistics / Routing Table** page.*

Clients

On the **Statistics / Clients** page, you can view the list of devices connected to the local network of the gateway.

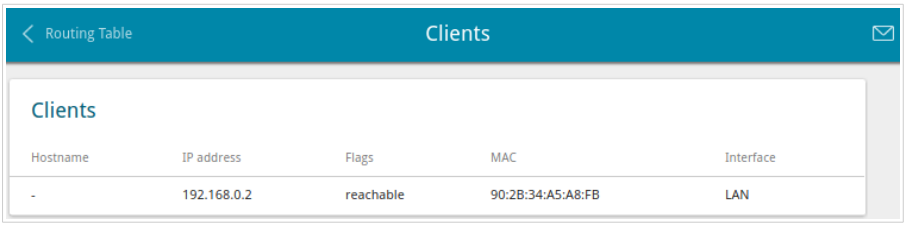

*Figure 30. The **Statistics / Clients** page.*

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

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 31. The **Statistics / Multicast Groups** page.*

Clients and Session

On the **Statistics / Clients and Session** page, you can view information on current sessions in the gateway'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 32. The **Statistics / Clients and Session** page.*

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

Connections Setup

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

WAN

When the gateway connects to a fiber optic line, a WAN connection is created and configured automatically.

! When the gateway connects to an Ethernet line or a mobile network, you should configure your Ethernet 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.

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

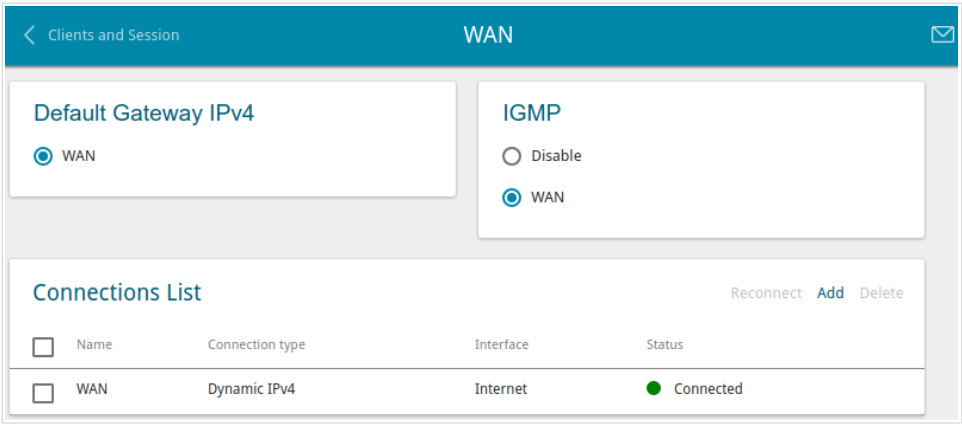

*Figure 33. The **Connections Setup / WAN** page.*

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.

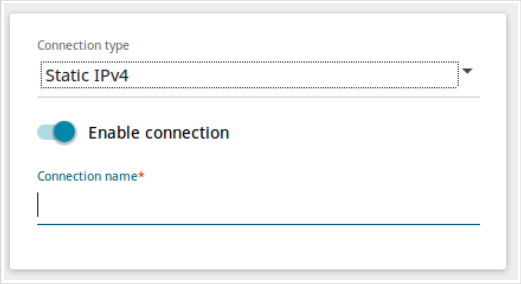

*Figure 34. The page for creating a new **Static IPv4** connection. Selecting a connection type.*

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.

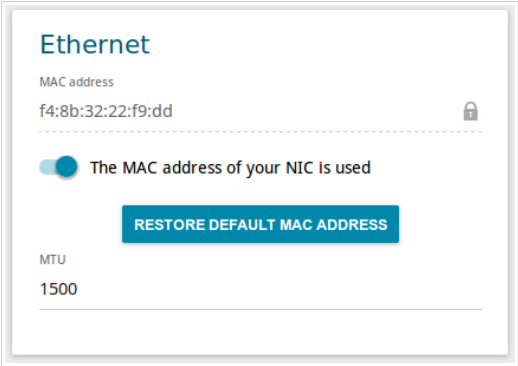

*Figure 35. The page for creating a new **Static IPv4** connection. The **Ethernet** section.*

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 gateway 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 gateway'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.

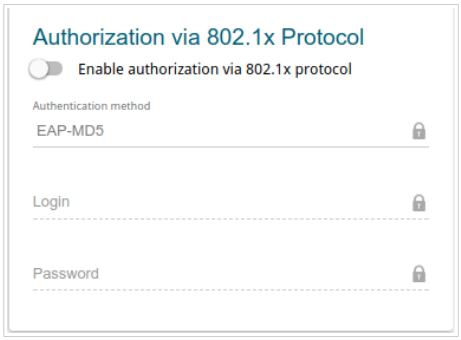

*Figure 36. The page for creating a new **Static IPv4** connection. The **Authorization via 802.1x Protocol** section.*

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

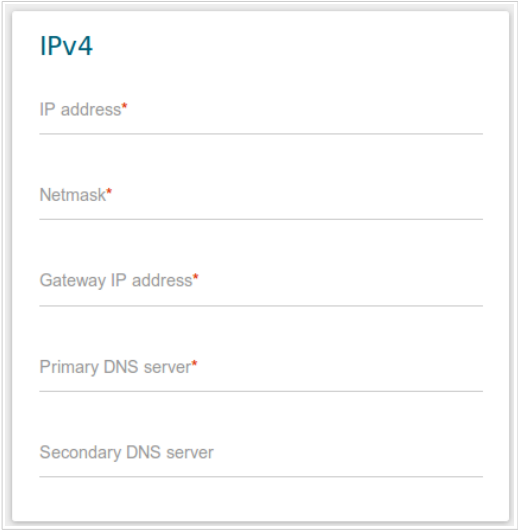

*Figure 37. The page for creating a new **Static IPv4** connection. The **IPv4** section.*

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 gateway specified by your ISP. *Optional*.

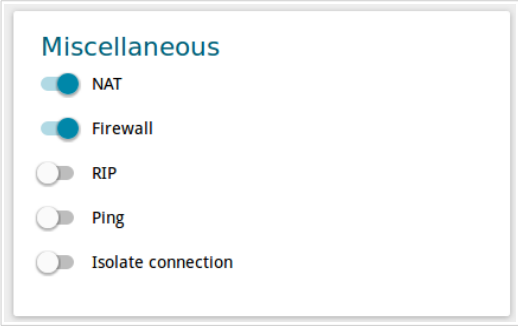

*Figure 38. The page for creating a new **Static IPv4** connection. The **Miscellaneous** section.*

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 gateway 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 gateway 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.

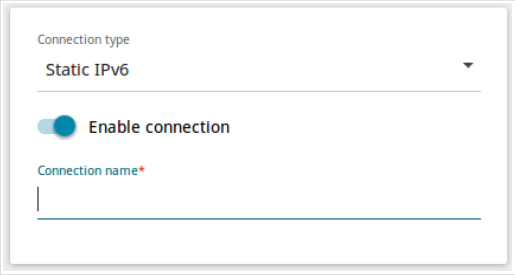

*Figure 39. The page for creating a new **Static IPv6** connection. Selecting a connection type.*

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.

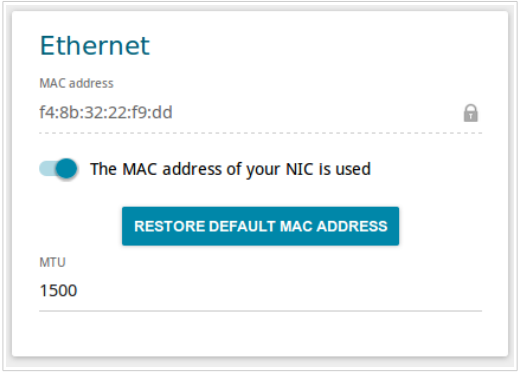

*Figure 40. The page for creating a new **Static IPv6** connection. The **Ethernet** section.*

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 gateway 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 gateway'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 41. 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 42. 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 gateway 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 gateway 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.

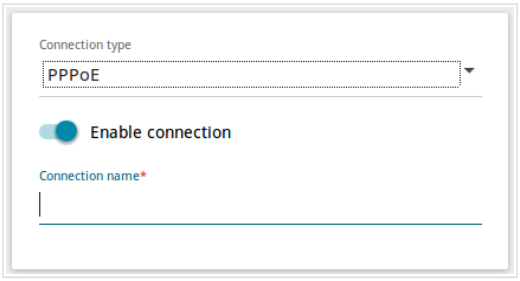

*Figure 43. The page for creating a new **PPPoE** connection. Selecting a connection type.*

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.

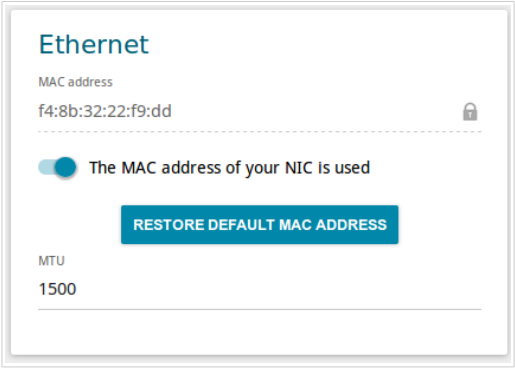

*Figure 44. The page for creating a new **PPPoE** connection. The **Ethernet** section.*

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 gateway 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 gateway'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.

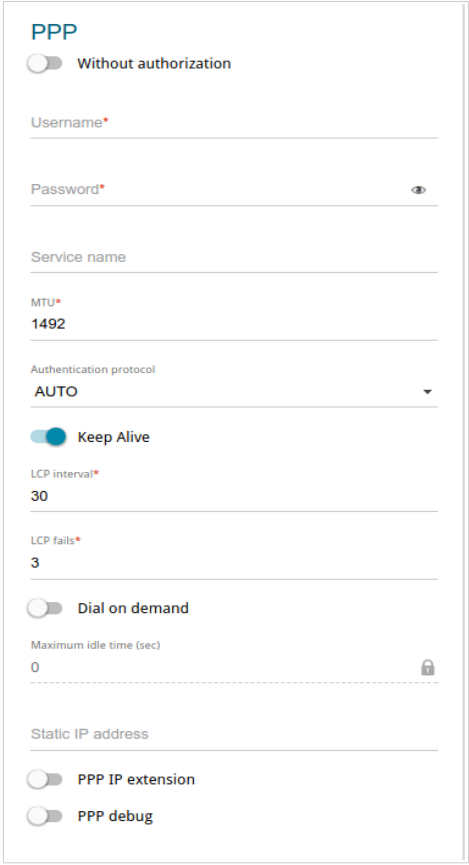

*Figure 45. The page for creating a new **PPPoE** connection. The **PPP** section.*

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.
Keep Alive	Move the switch to the right if you want the gateway to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the **LCP interval** and **LCP fails** fields are available. Specify the required values.

Parameter	Description
Dial on demand	Move the switch to the right if you want the gateway 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.

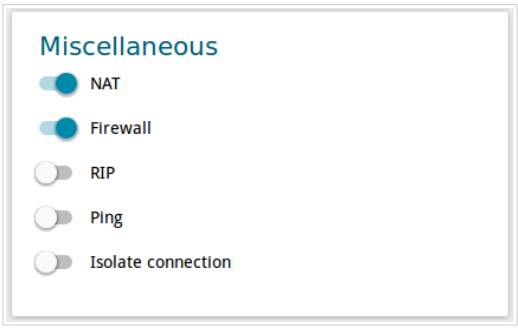

*Figure 46. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.*

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 gateway 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 gateway 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.

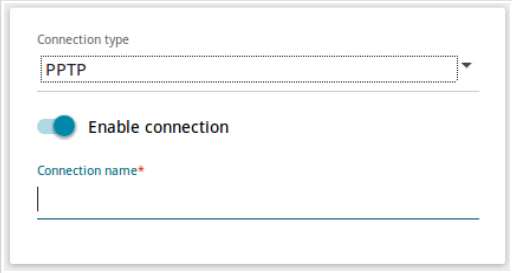

*Figure 47. The page for creating a new **PPTP** connection. Selecting a connection type.*

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.

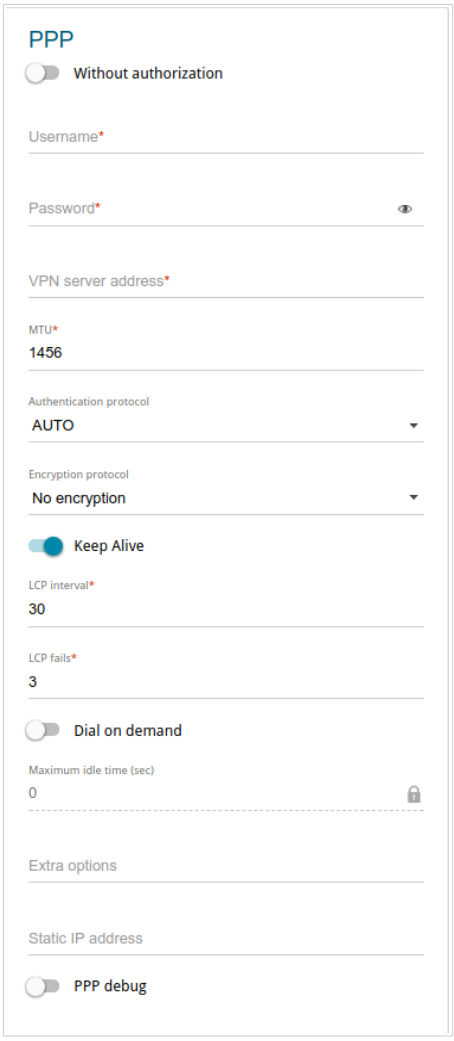

*Figure 48. The page for creating a new **PPTP** connection. The **PPP** section.*

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

Parameter	Description
Encryption protocol	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 gateway 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 gateway 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.

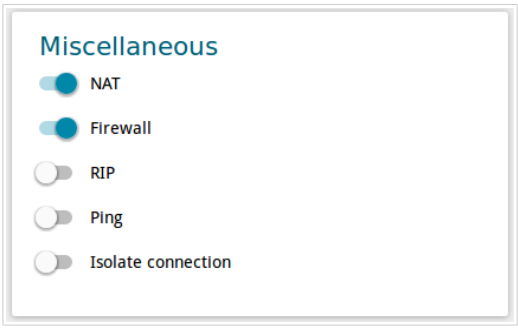

*Figure 49. The page for creating a new **PPTP** connection. The **Miscellaneous** section.*

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 gateway 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 gateway 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 50. 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.

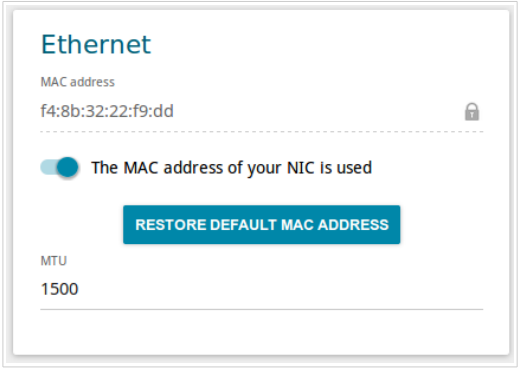

*Figure 51. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.*

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 gateway 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 gateway'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.

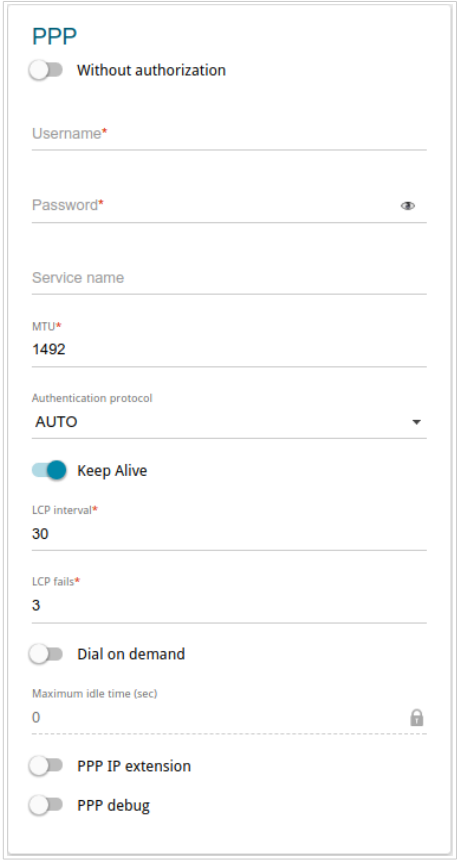

*Figure 52. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.*

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

Parameter	Description
Dial on demand	Move the switch to the right if you want the gateway 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 53. The page for creating a new **PPPoE IPv6** connection. The **IP** section.*

Parameter	Description
IP	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the **Automatically** value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (*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 54. 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 gateway 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 gateway 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 3G WAN Connection**

If the PIN code check is enabled for the SIM card inserted into your USB modem, then prior to creating a 3G WAN connection, go to the **USB Modem / PIN** page and enter the PIN code (see the ***USB Modem*** section, page 126). Then go to the **Connections Setup / WAN** page and click the **Add** button 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.

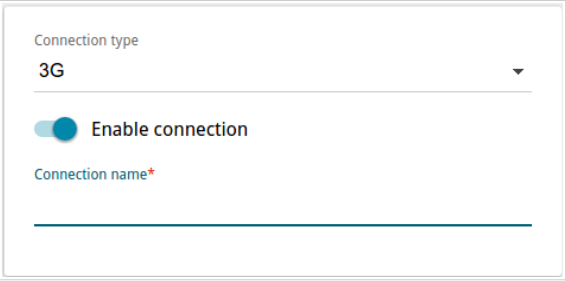

*Figure 55. The page for creating a new **3G** connection. Selecting a connection type.*

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.

* For correct operation of USB modems you may need to update the gateway's firmware.

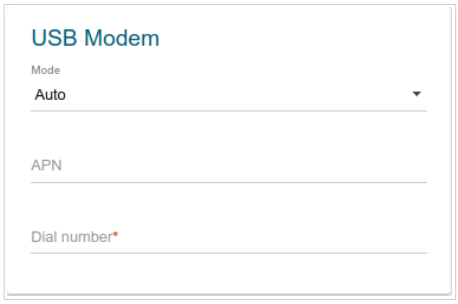

*Figure 56. The page for creating a new **3G** connection. The **USB Modem** section.*

Parameter	Description
USB Modem	
Mode	The value of the field specifies the type of the network to which the gateway connects. Leave the **Auto** value to let the gateway connect automatically to an available type of network, or select a needed value from the drop-down list.
APN	An access point name.
Dial number	A number dialed to connect to the authorization server of the operator.

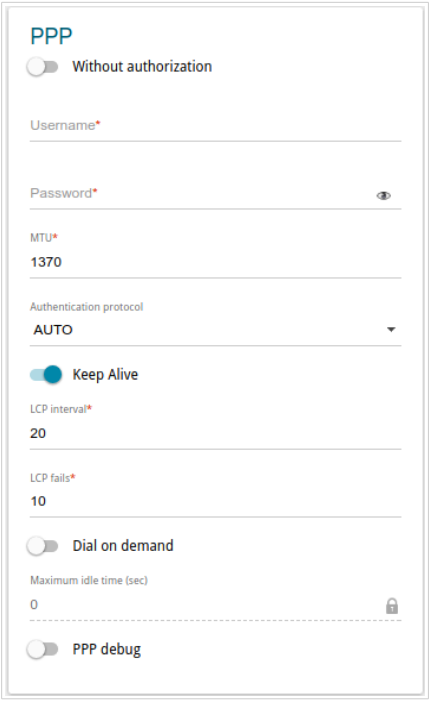

*Figure 57. The page for creating a new **3G** connection. The **PPP** section.*

Parameter	Description
PPP	
Without authorization	Move the switch to the right if your operator does not require authorization.
Username	A username (login) to connect to the network of the operator.
Password	A password to connect to the network of the operator. Click the **Show** icon ( ) to display the entered password.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the **AUTO** value.
Keep Alive	Move the switch to the right if you want the gateway to keep you connected to the network of your operator even when the connection has been inactive for a specified period of time. When the checkbox is selected, 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 gateway 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.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

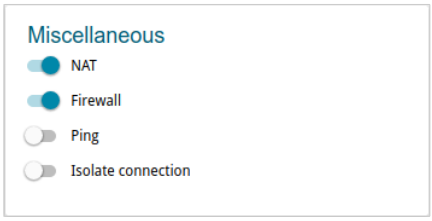

*Figure 58. The page for creating a new **3G** connection. The **Miscellaneous** section.*

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.
Ping	If the switch is moved to the right, the gateway 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 gateway 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 LTE WAN Connection**

! For the USB modem Megafon M100-1, please reboot the gateway after creating the WAN connection.

If the PIN code check is enabled for the SIM card inserted into your USB modem, then prior to creating an LTE WAN connection, go to the **USB Modem / PIN** page and enter the PIN code[11] on the page displayed (see the ***USB Modem*** section, page 126). Then on the connection creation page, go to the **All Settings** tab, select the relevant value from the **Connection type** drop-down list, and specify the needed values.

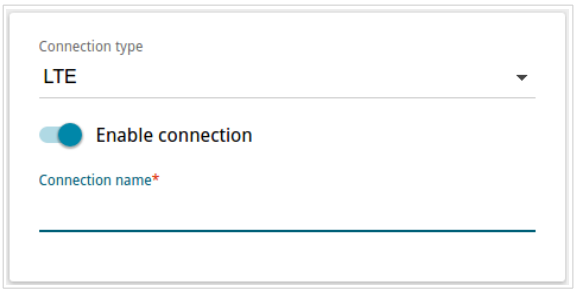

*Figure 59. The page for creating a new **LTE** connection. Selecting a connection type.*

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.

* For correct operation of USB modems you may need to update the gateway's firmware.

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

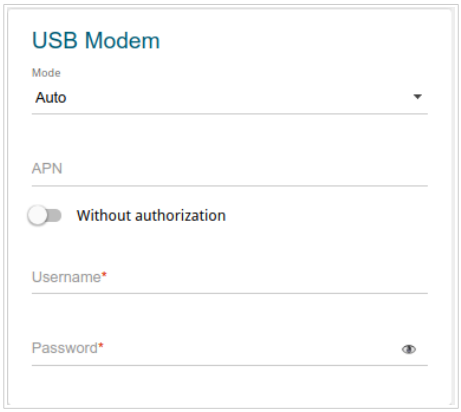

*Figure 60. The page for creating a new **LTE** connection. The **USB Modem** section.*

Parameter	Description
USB Modem	
Mode	The value of the field specifies the type of the network to which the gateway connects. Leave the **Auto** value to let the gateway connect automatically to an available type of network, or select a needed value from the drop-down list.[12]
APN	An access point name.
Without authorization	Move the switch to the right if your operator does not require authorization.
Username	A username (login) to connect to the network of the operator.
Password	A password to connect to the network of the operator. Click the **Show** icon ( ) to display the entered password.

12 Some LTE USB modems do not support network type selection and work in the **Auto** mode regardless of the value selected from the drop-down list.

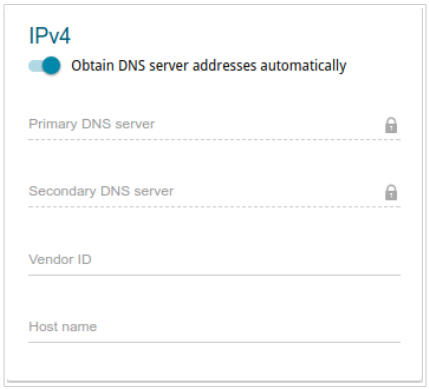

*Figure 61. The page for creating a new **LTE** connection. The **IPv4** section.*

Parameter	Description
IPv4	
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 gateway specified by your ISP. *Optional*.

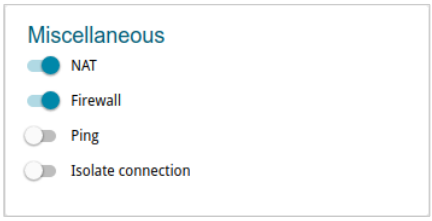

*Figure 62. The page for creating a new **LTE** connection. The **Miscellaneous** section.*

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.
Ping	If the switch is moved to the right, the gateway 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 gateway 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 gateway'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.

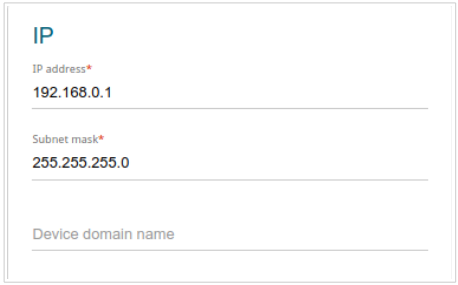

*Figure 63. Configuring the local interface. The **IPv4** tab. The **IP** section.*

Parameter	Description
IP	
IP address	The IP address of the gateway in the local subnet. By default, the following value is specified: `192.168.0.1`.
Subnet mask	The mask of the local subnet. By default, the following value is specified: `255.255.255.0`.
Device domain name	The name of the device assigned to its IP address in the local subnet.

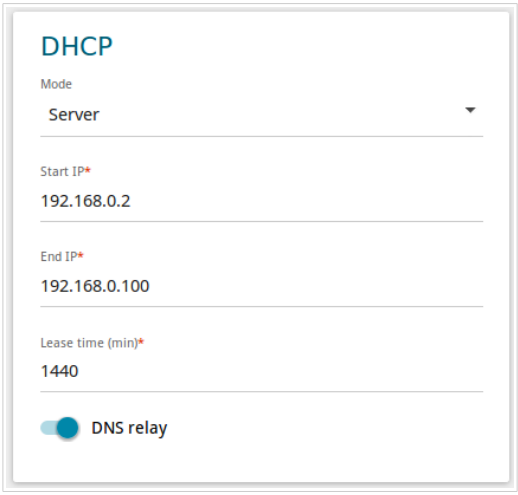

*Figure 64. Configuring the local interface. The **IPv4** tab. The **DHCP** section.*

Parameter	Description
DHCP	
Mode	An operating mode of the gateway's DHCP server. **Server**: the gateway 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 gateway'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 gateway obtain the address of the gateway as the DNS server address. Move the switch to the left so that the devices connected to the gateway 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 gateway'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 gateway 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).

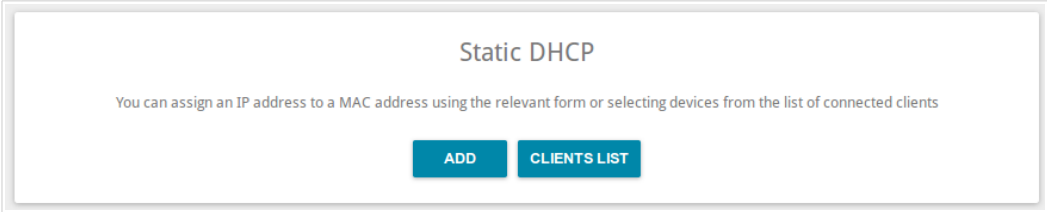

Figure 65. The section for creating MAC-IP pairs.

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 gateway'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 gateway and configure IPv6 addresses assignment settings.

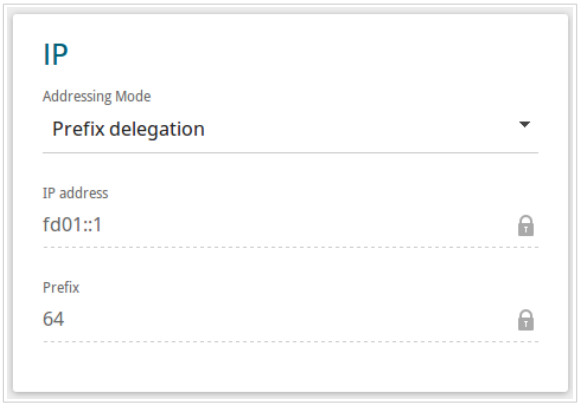

*Figure 66. Configuring the local interface. The **IPv6** tab. The **IP** section.*

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 gateway requests a prefix to configure an IPv6 address from a delegating router.
IP address	The IPv6 address of the gateway 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.

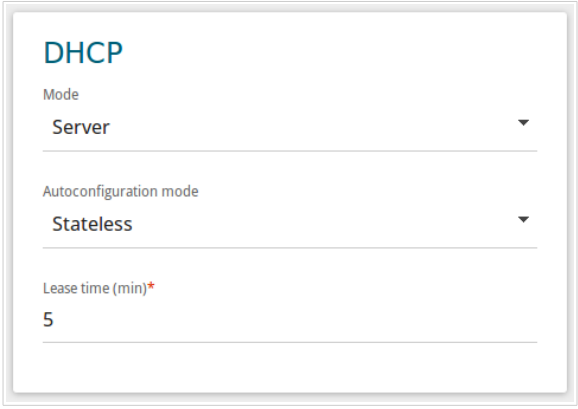

*Figure 67. Configuring the local interface. The **IPv6** tab. The **DHCP** section.*

Parameter	Description
DHCP	
Mode	Select a mode of IPv6 address assignment from the drop-down list. **Server**: the gateway 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 gateway 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 gateway and configure the basic and additional wireless networks. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

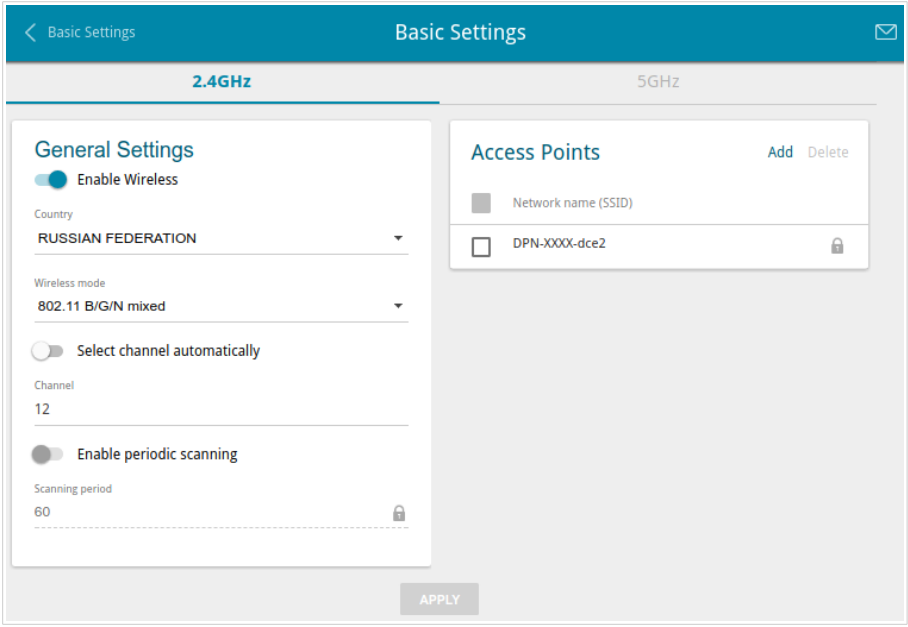

Figure 68. Basic settings of the wireless LAN in the 2.4GHz band.

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

Parameter	Description
Enable Wireless	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left.
Country	The country you are in. Select a value from the drop-down list.
Wireless mode	Operating mode of the wireless network of the gateway. 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 gateway 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).
Enable periodic scanning	Move the switch to the right to let the gateway 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 gateway 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.

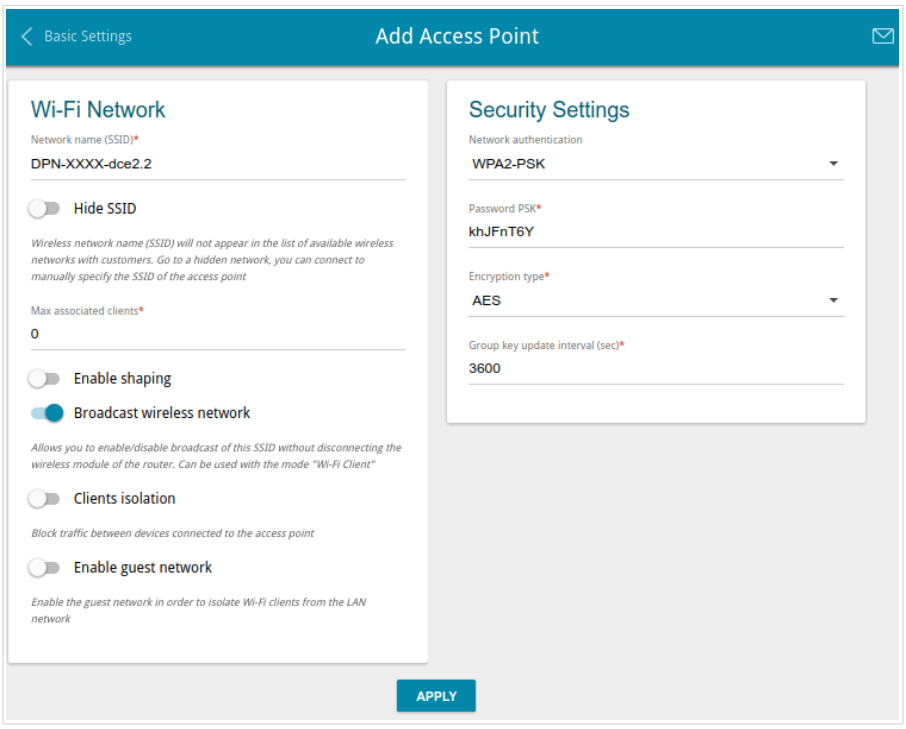

Figure 69. Creating a wireless network.

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 gateway 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 gateway's LAN.

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

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

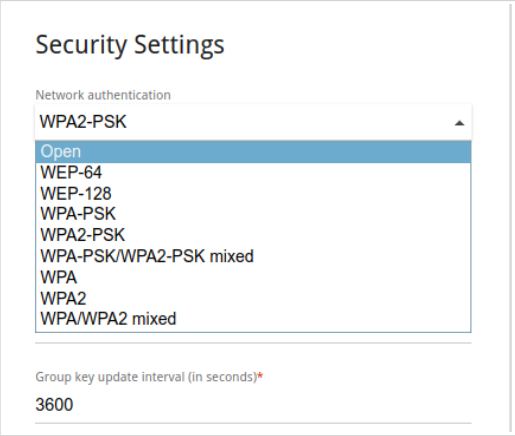

Figure 70. Network authentication types supported by the gateway.

The gateway supports the following authentication types:

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

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

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 or 802.11ac):

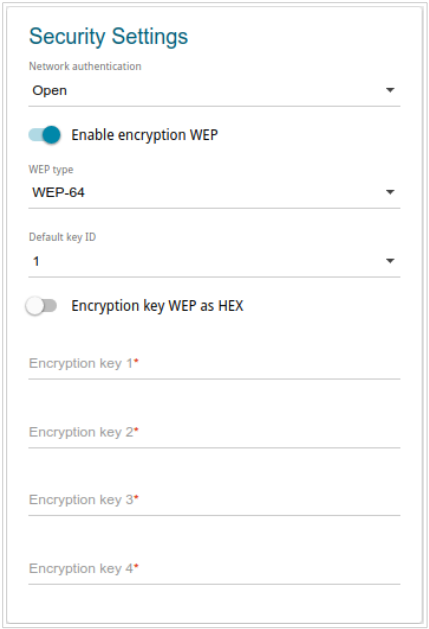

*Figure 71. The **Open** value is selected from the **Network authentication** drop-down list.*

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 gateway 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:

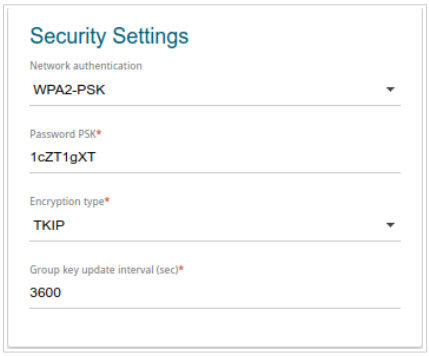

*Figure 72. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.*

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.[13]
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.

13 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:

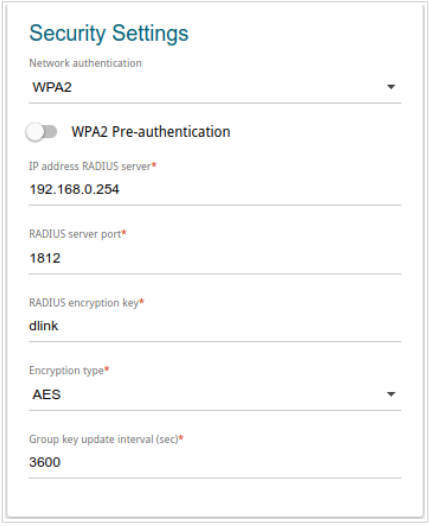

*Figure 73. The **WPA2** value is selected from the **Network authentication** drop-down list.*

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 gateway uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings).
Encryption type	An encryption method: **TKIP**, **AES**, or **TKIP+AES**.
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed.

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

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

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

Client Management

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

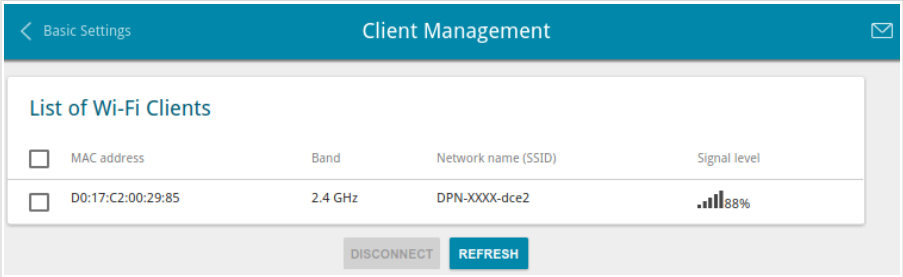

Figure 74. The page for managing the wireless clients.

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

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

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

WPS

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

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

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

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

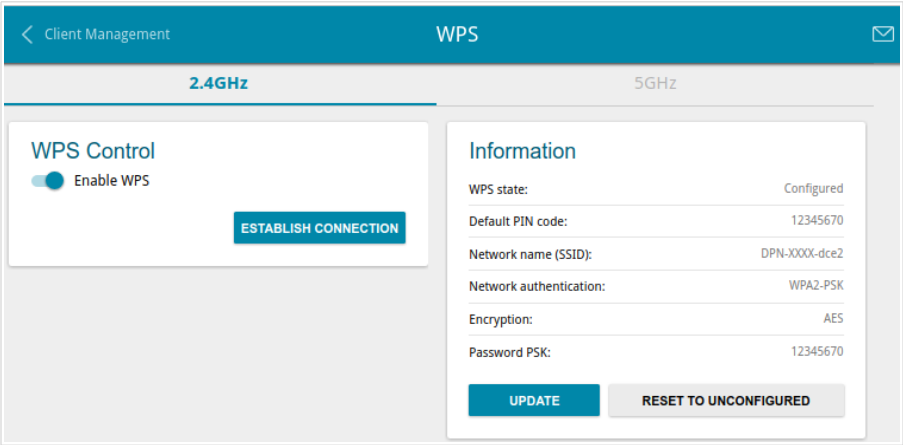

Figure 75. The page for configuring the WPS function.

To activate the WPS function, on the tab of the relevant band, 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 gateway. This parameter is used when connecting the gateway to a registrar to set the parameters of the WPS function.
Network name (SSID)	The name of the gateway'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 gateway'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 gateway.

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 gateway'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 gateway.

Using WPS Function without Web-based Interface

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

1. Specify relevant security settings for the wireless network of the gateway.
2. Move the **Enable WPS** switch to the right.
3. Save the settings and close the web-based interface (click the **Logout** line of the menu).

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

1. Select the PBC method in the software of the wireless device that you want to connect to the gateway'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 gateway and release. The **WPS** LED will start blinking green.

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.

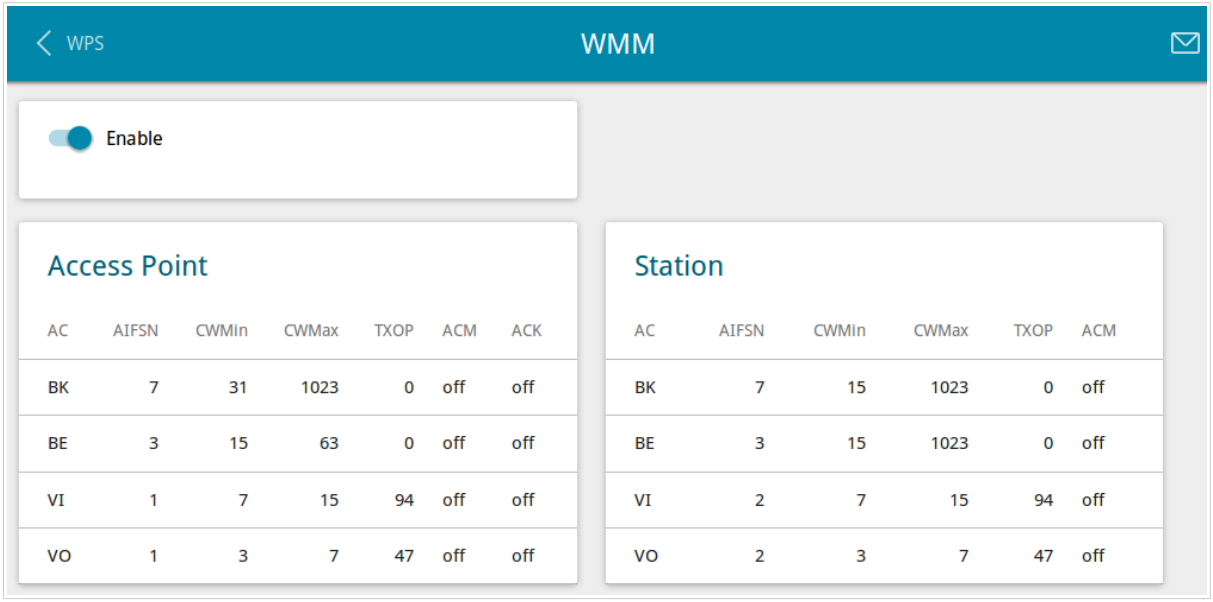

Figure 76. The page for configuring the WMM function.

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 gateway 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.

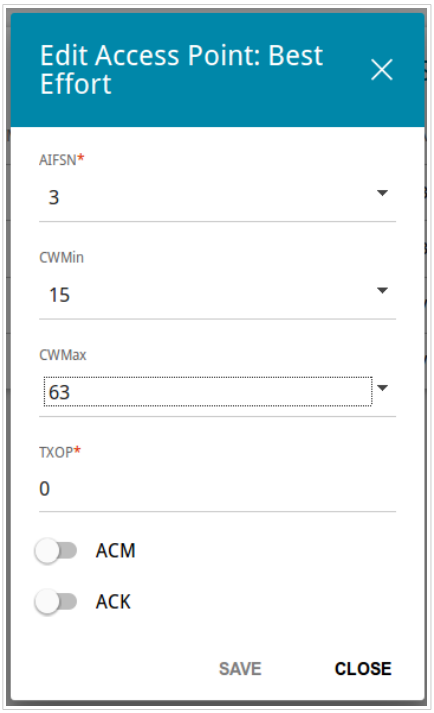

Figure 77. The window for changing parameters of the WMM function.

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

Parameter	Description
ACK	*Acknowledgment*. Answering response requests while transmitting. Displayed only in the **Access Point** section. If the switch is moved to the left, the gateway answers requests. If the switch is moved to the right, the gateway 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 gateway as a client to connect to a wireless access point or to a WISP.

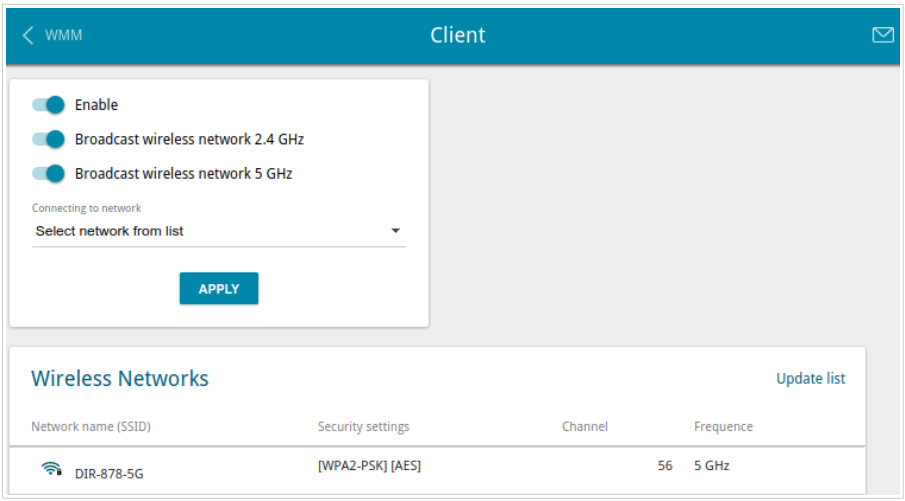

Figure 78. The page for configuring the client mode.

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

Parameter	Description
Broadcast wireless network 2.4 GHz / Broadcast wireless network 5 GHz	If the switch is moved to the left, devices cannot connect to the gateway's WLAN. Upon that the gateway 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 gateway 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 gateway 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 DPN-144DG will switch to the channel of the access point to which you have connected.

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

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

Additional

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

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

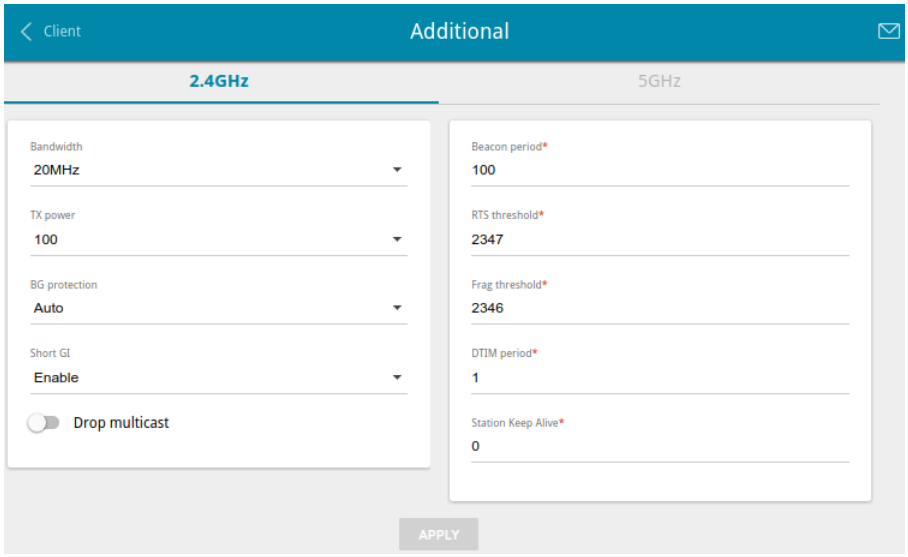

Figure 79. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	The channel bandwidth for 802.11n standard in the 2.4GHz band (the **2.4GHz** tab). **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). The channel bandwidth for 802.11n and 802.11ac standards in 5GHz band (the **5GHz** tab). **20MHz**: 802.11n and 802.11ac clients operate at 20MHz channels. **40MHz**: 802.11n and 802.11ac clients operate at 40MHz channels. **20/40MHz -**: 802.11n and 802.11ac clients operate at 20MHz or 40MHz channels (the channel is combined with the previous adjacent channel). **20/40MHz +**: 802.11n and 802.11ac clients operate at 20MHz or 40MHz channels (the channel is combined with the next adjacent channel). **80MHz**: 802.11ac clients operate at 80MHz channels. **20/40/80MHz -**: 802.11ac clients operate at 20MHz, 40MHz, or 80MHz channels (the channel is combined with the previous adjacent channels). **20/40/80MHz +**: 802.11ac clients operate at 20MHz, 40MHz, or 80MHz channels (the channel is combined with the next adjacent channels).
TX power	The transmit power (in percentage terms) of the gateway.

Parameter	Description
BG protection	*Available on the **2.4GHz** tab.* The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Select a value from the drop-down list. **Auto**: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices). **Always On**: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network). **Always Off**: The protection function is always disabled.
Short GI	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the gateway is communicating to wireless devices. **Enable**: the gateway uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n and 802.11ac standards (see the value of the **Wireless mode** drop-down list on the **Wi-Fi / Basic Settings** page). **Disable**: the gateway uses the 800 ns standard guard interval.
Drop multicast	Move the switch to the right to disable multicasting for the gateway'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.
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.

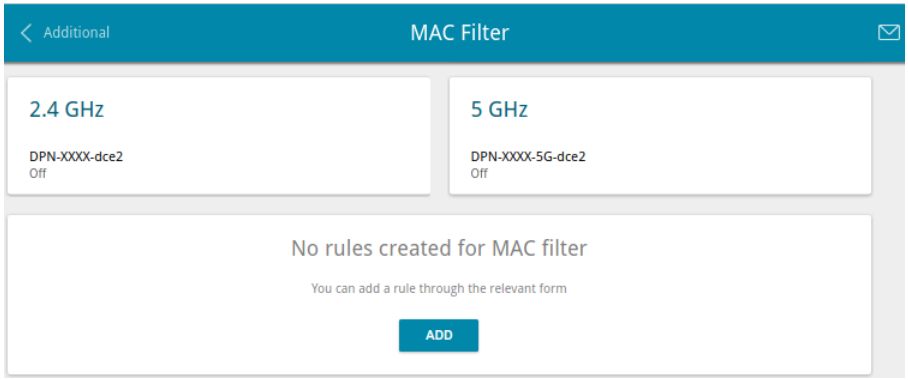

Figure 80. The page for configuring the MAC filter for the wireless network.

By default, MAC filtering is disabled.

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

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

Click the **ADD** button to add a rule for MAC filtering.

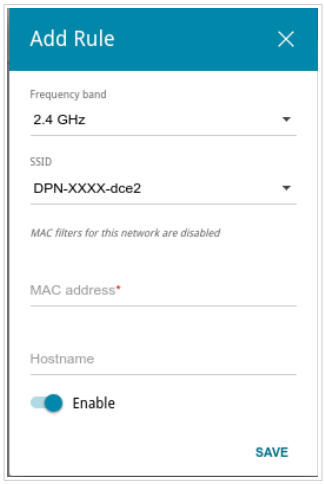

Figure 81. The window for adding a rule for the MAC filter.

You can specify the following parameters:

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

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

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

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

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

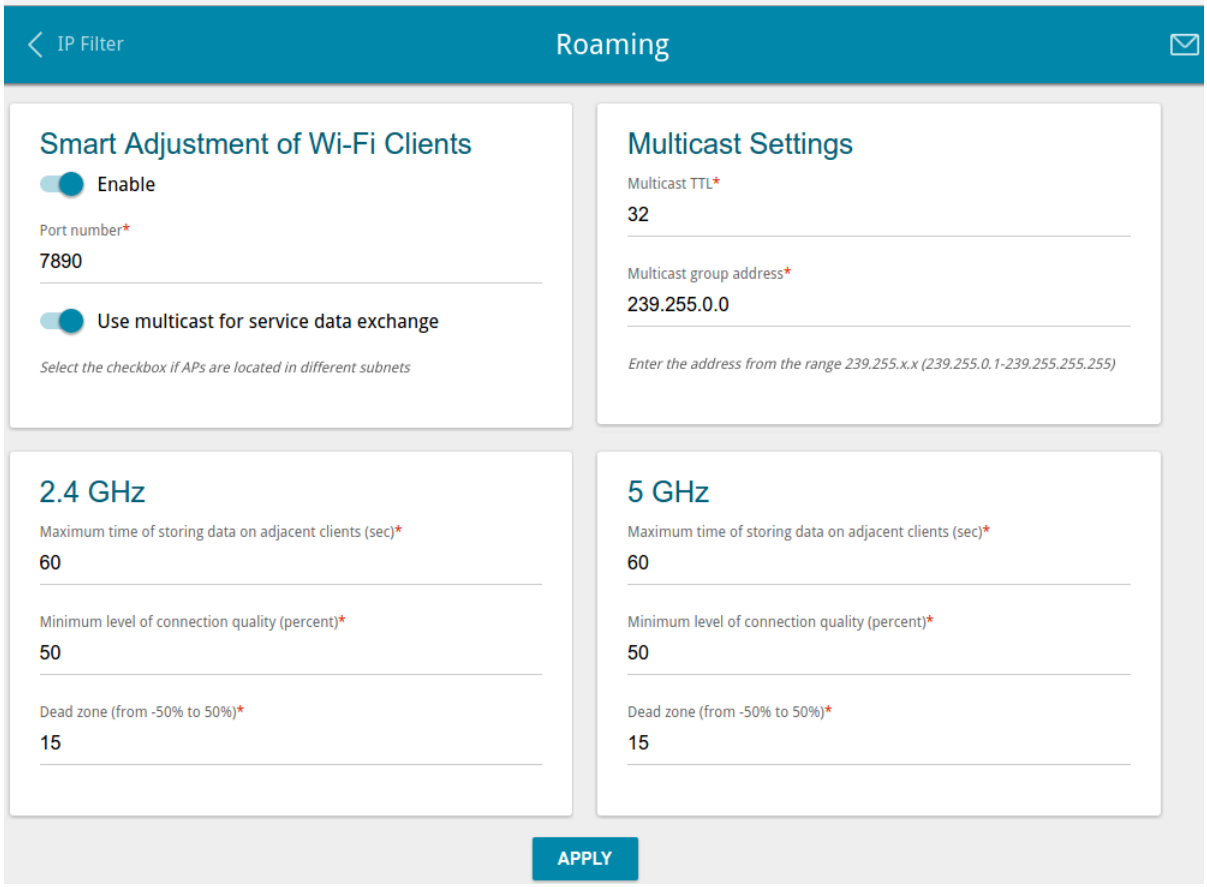

*Figure 82. The **Wi-Fi / Roaming** page.*

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, gateways).

Parameter	Description
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, gateways). 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.
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).
2.4 GHz / 5 GHz	
Maximum time of storing data on adjacent clients	The maximum time period (in seconds) during which the access point (router, gateway) stores data on the signal strength of the client located on its coverage area.
Minimum level of connection quality	The threshold value of the signal strength upon which the access point (router, gateway) 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, gateway) and connects to another device. You can specify the values from `-50%` to `+50%`.

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

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

Print Server

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

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

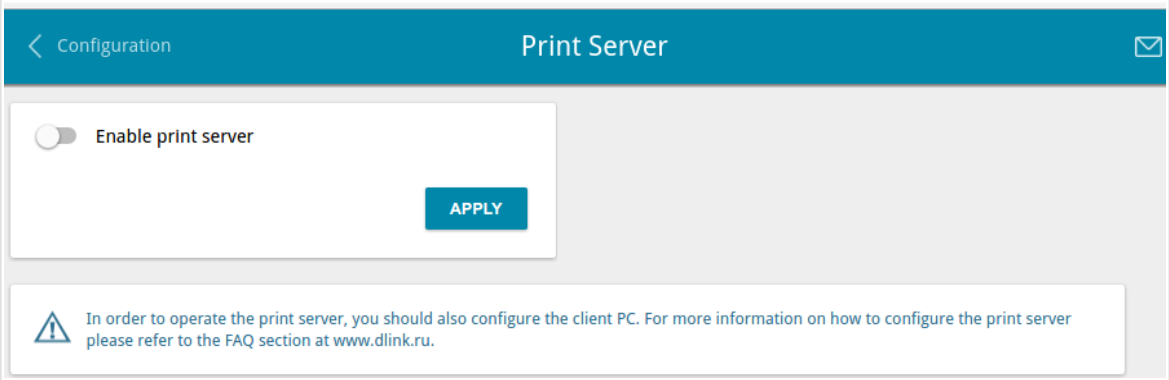

*Figure 83. The **Print Server** page.*

To configure the gateway as a print server, move the **Enable print server** switch to the right and click the **APPLY** button. Upon that the **Status of printer** field is displayed on the page.

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

USB Storage

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

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

Information

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

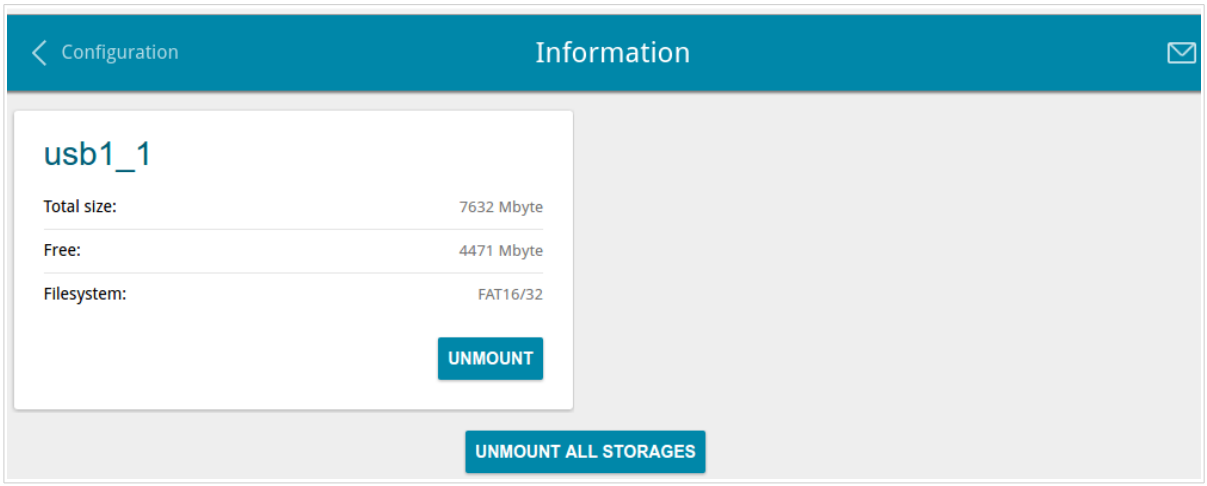

*Figure 84. The **USB Storage / Information** page.*

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

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

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

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

USB Users

On the **USB Storage / USB Users** page, you can create user accounts to provide access to data on the USB storage connected to the gateway.

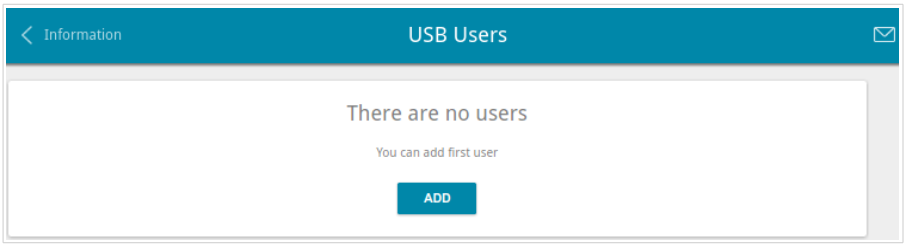

*Figure 85. The **USB Storage / USB users** page.*

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

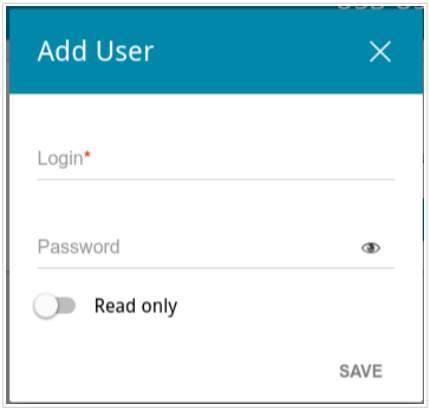

Figure 86. The window for adding a user.

In the opened window, in the **Login** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.[14]

! You cannot create accounts with the following usernames: **admin**, **support**, **user**, **nobody**.

For ext2, ext3, or FAT storages or storage partitions, it is possible to create users with limited rights. Move the **Read only** switch to the right not to let the user create, change, or delete files.

Click the **SAVE** button.

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

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

14 0-9, A-Z, a-z, space, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

Samba

On the **USB Storage / Samba** page, you can enable the built-in Samba server of the gateway to provide access to the USB storage for users of your LAN.

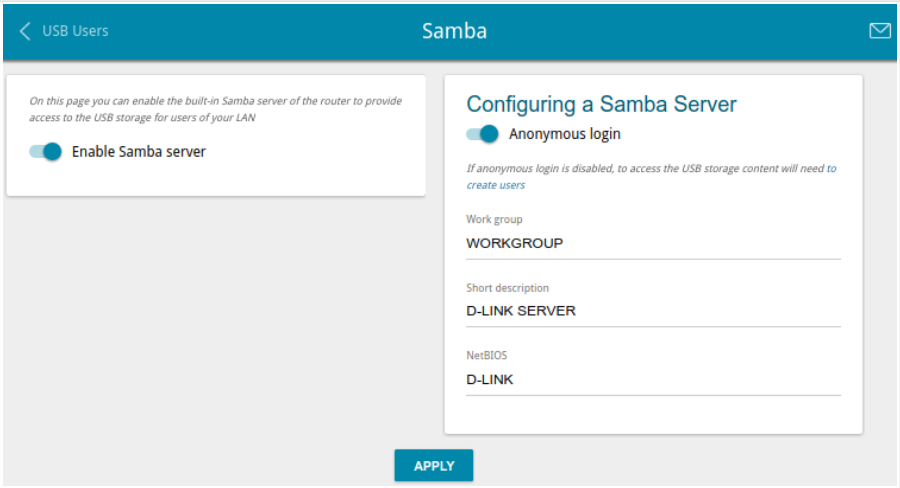

*Figure 87. The **USB Storage / Samba** page.*

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

The **Anonymous login** switch (by default, the switch is moved to the right) allows anonymous access to the content of the USB storage for users of your LAN.

If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

In the **Work group** field, leave the value specified by default (**WORKGROUP**) or specify a new name of a workgroup which participants will have access to the content of the USB storage.

In the **Short description** field, you can specify an additional description for the USB storage. This value will be displayed in some operating systems. Use digits and/or Latin characters.

In the **NetBIOS** field, specify a new name of the USB storage for identification in your LAN. Use digits and/or Latin characters.

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

To disable the built-in Samba server of the gateway, move the **Enable Samba server** switch to the left and click the **APPLY** button.

FTP

On the **USB Storage / FTP** page, you can enable the built-in FTP server of the gateway to provide access to the USB storage for users of your LAN.

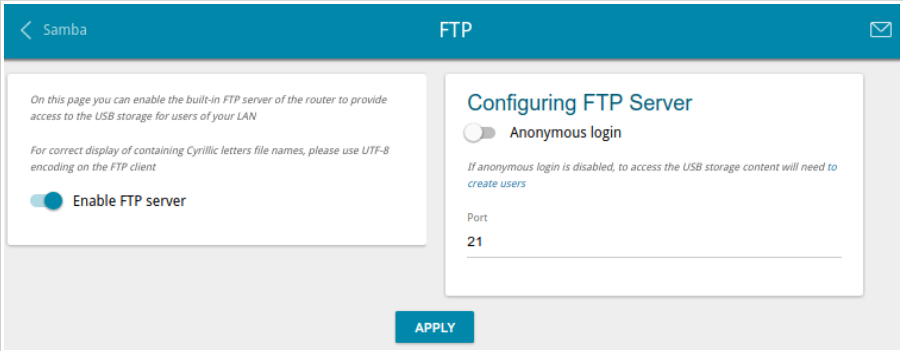

*Figure 88. The **USB Storage / FTP** page.*

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

Move the **Anonymous login** switch to the right to allow anonymous access to the content of the USB storage for users of your LAN. If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

If needed, change the gateway's port used by the FTP server in the **Port** field (by default, the standard port `21` is specified).

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

To disable the built-in FTP server of the gateway, move the **Enable FTP server** switch to the left and click the **APPLY** button.

Filebrowser

On the **USB Storage / Filebrowser** page, you can view the content of your USB storage connected to the gateway and remove separate folders and files from the USB storage.

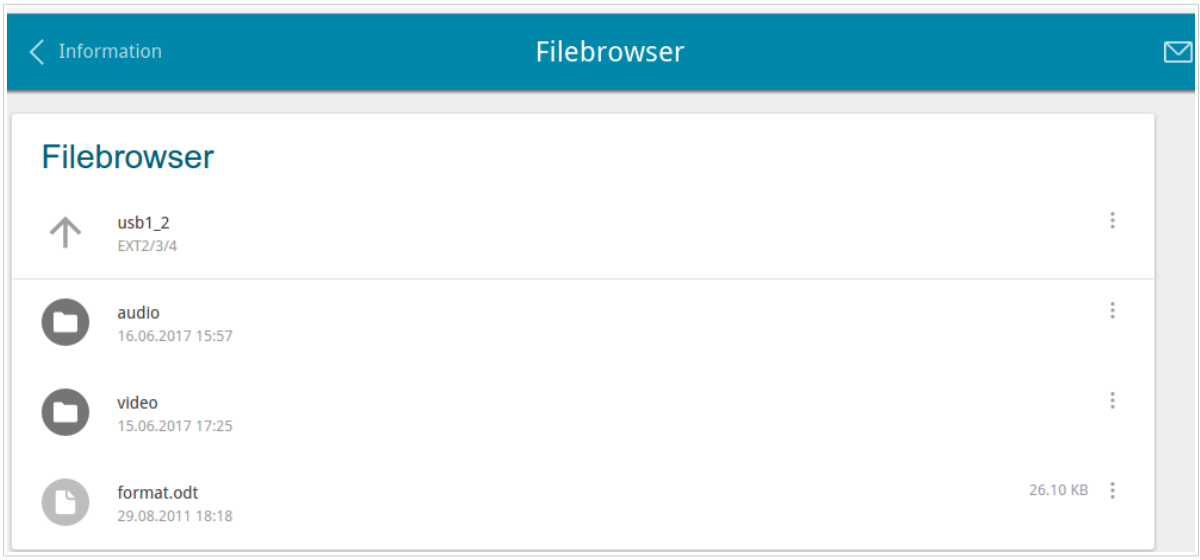

*Figure 89. The **USB Storage / Filebrowser** page.*

To view the content of the USB storage, click the icon of the storage or storage partition. The list of folders and files will be displayed on the page.

To go to a folder, click the line corresponding to this folder.

To refresh the folder contents, click the **Actions** icon (⋮) in the line corresponding to this folder and select the **Refresh** value.

To remove a folder or file, click the **Actions** icon (⋮) in the line corresponding to this folder or file and select the **Remove** value.

DLNA

On the **USB Storage / DLNA** page, you can enable the built-in DLNA server of the gateway to provide access to the USB storage for users of your LAN.

The built-in media server allows DLNA certified devices of your LAN to play multimedia content of the USB storage. Multimedia content can be played only when a USB storage is connected to the gateway.

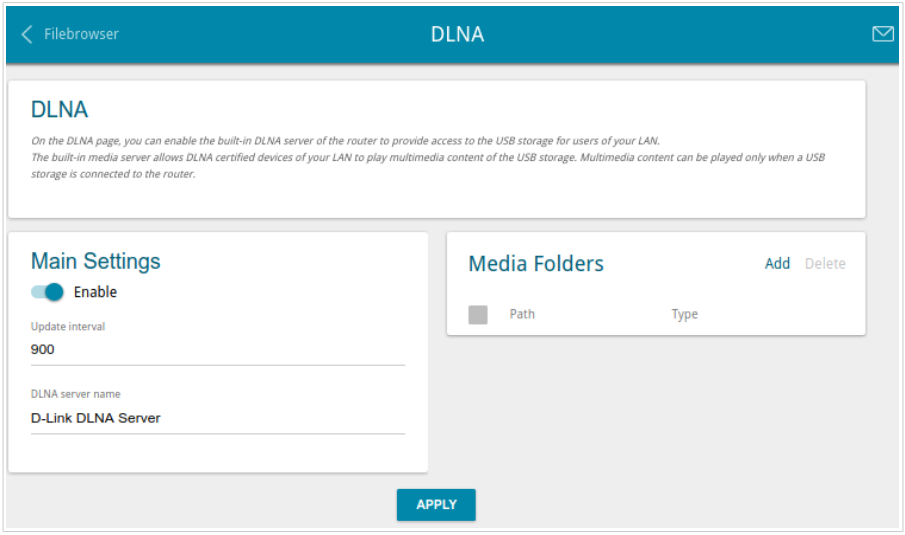

*Figure 90. The **USB Storage / DLNA** page.*

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

In the **Update interval** field, specify the time period (in seconds), at the end of which the media server updates the file list of the USB storage, or leave the value specified by default (**900**).

In the **DLNA server name** field, specify a new name of the DLNA server for easier identification in your LAN or leave the value specified by default (**D-Link DLNA Server**). Use digits and/or Latin characters.

To allow access to the content of the USB storage for users of your LAN, click the **Add** button in the **Media Folders** section.

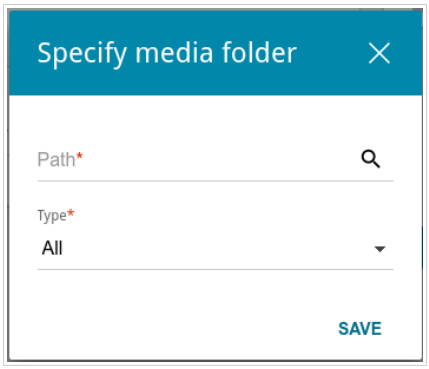

Figure 91. Specifying a media folder.

In the opened window, locate a folder containing files. To do this, click the **Search** icon ( ) in the **Path** field. Then go to the needed folder and click the **SELECT** button.

For each folder you can define the type of files which will be available for users of your LAN. To do this, select the needed type of files from the **Type** drop-down list. To share all files of a folder, select the **All** value from the **Type** drop-down list.

Click the **SAVE** button.

To remove a folder from the list in the **Media Folders** section, select the checkbox located to the left of the relevant line in the table and click the **Delete** button.

After specifying all needed settings on the **USB Storage / DLNA** page, click the **APPLY** button.

To disable the built-in DLNA server of the gateway, move the **Enable** switch to the left and click the **APPLY** button.

Torrent Client

On the **USB Storage / Torrent Client** page, you can configure all needed settings for the built-in Transmission client.

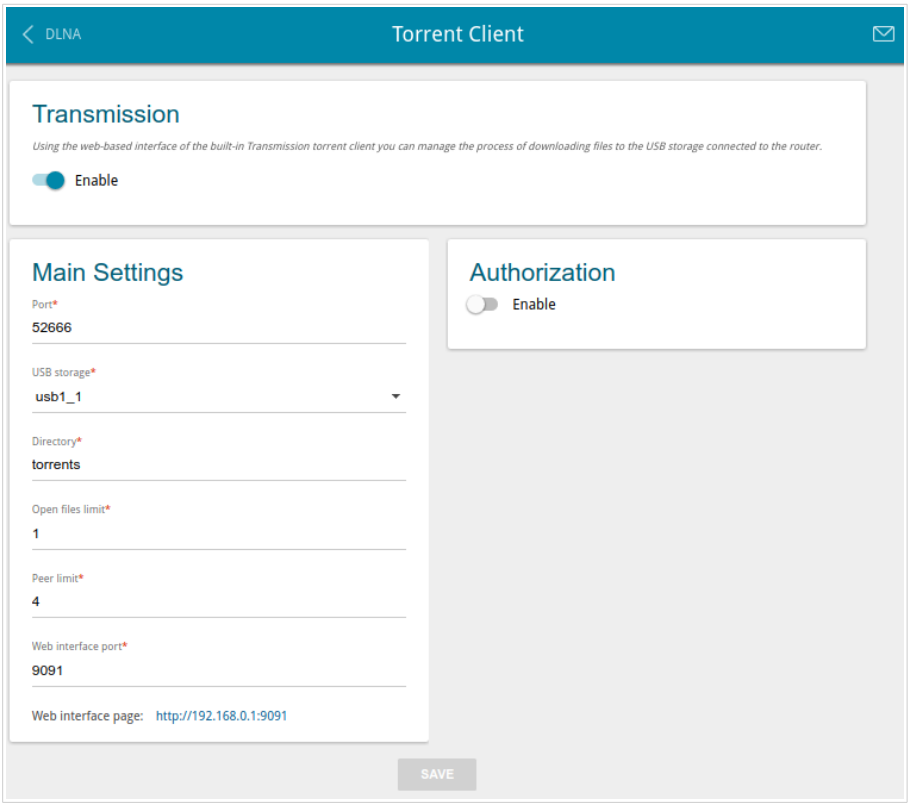

*Figure 92. The **USB Storage / Torrent Client** page.*

You can specify the following parameters:

Parameter	Description
Transmission	
Enable	Move the switch to the right to activate the Transmission client.
Main Settings	
Port	The gateway's port which will be used by the Transmission client.
USB storage	From the drop-down list, select a USB storage or a volume.
Directory	The folder on the USB storage where data of the Transmission client will be stored.
Open files limit	The maximum number of files which clients can download simultaneously.
Peer limit	The maximum number of the service users from which you can download files.

Parameter	Description
Web interface port	The port on which the web-based interface of the Transmission client is available.
Authorization	
Enable	Move the switch to the right if you want the Transmission client to request for username and password when accessing its web-based interface. Then fill in the **Username** and **Password** fields.
Username	The username to access the web-based interface of the Transmission client.
Password	The password to access the web-based interface of the Transmission client.

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

In the **Web-interface page** field, the address of the web-based interface of the Transmission client is displayed. To access the web-based interface of the Transmission client, click the link.

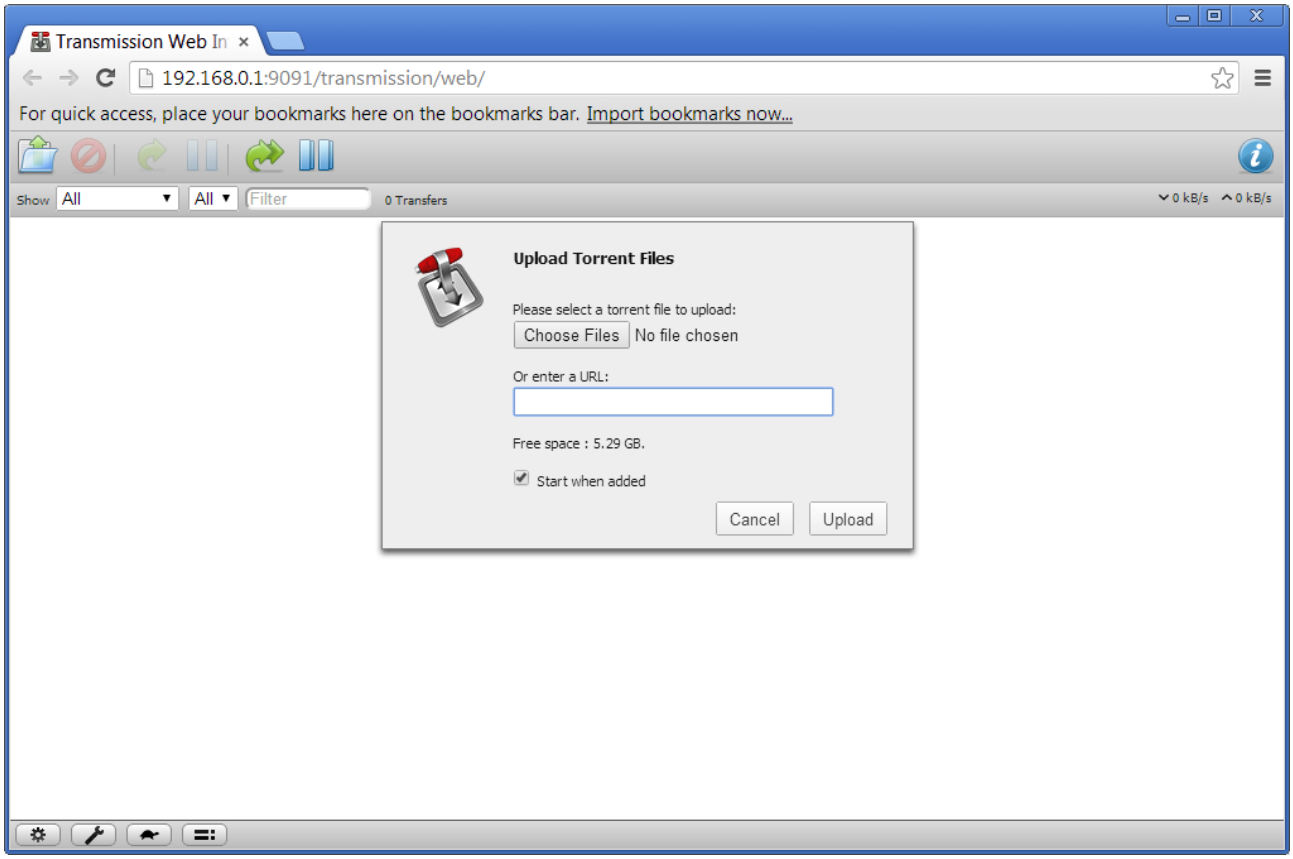

Figure 93. The web-based interface of the Transmission torrent client.

Using the web-based interface of the built-in Transmission torrent client you can manage the process of downloading files to the USB storage connected to the gateway.

The following buttons are available on the page:

Parameter	Description
 **Open Torrent**	Click the button to add a new torrent file (a metadata file according to which the Transmission client downloads files) to the download queue. In the dialog box appeared, select a file stored on your PC and click the **Upload** button.
 **Remove Selected Torrents**	Select the torrent file which you want to remove from the download queue and click the button.
 **Start Selected Torrents**	Select the torrent file corresponding to the download which should be restarted and click the button.

Parameter	Description
 **Start All Torrents**	Click the button to restart all downloads. If you limited the maximum number of simultaneous downloads, the Transmission client starts processing of the specified number of torrent files; after completing download of the first one, the client proceeds to the next file in the queue.
 **Pause Selected Torrents**	Select the torrent file corresponding to the download which should be stopped and click the button.
 **Pause All Torrents**	Click the button to stop all downloads.
 **Toggle Inspector**	Select a torrent file and click the button to view its data.

USB Modem

This menu is designed to operate USB modems.*

If the PIN code check for the SIM card inserted into your USB modem is not disabled, the relevant notification will be displayed in the top right corner of the page.

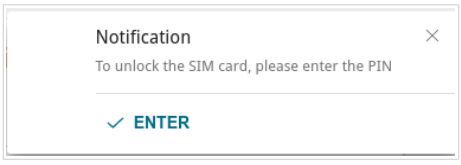

Figure 94. The notification on the PIN code check.

Click the **ENTER** button. When the **USB Modem / PIN** page opens, enter the PIN code in the **Authorization** section[15]. Click the **Show** icon ( ) to display the entered code. Then click the **APPLY** button.

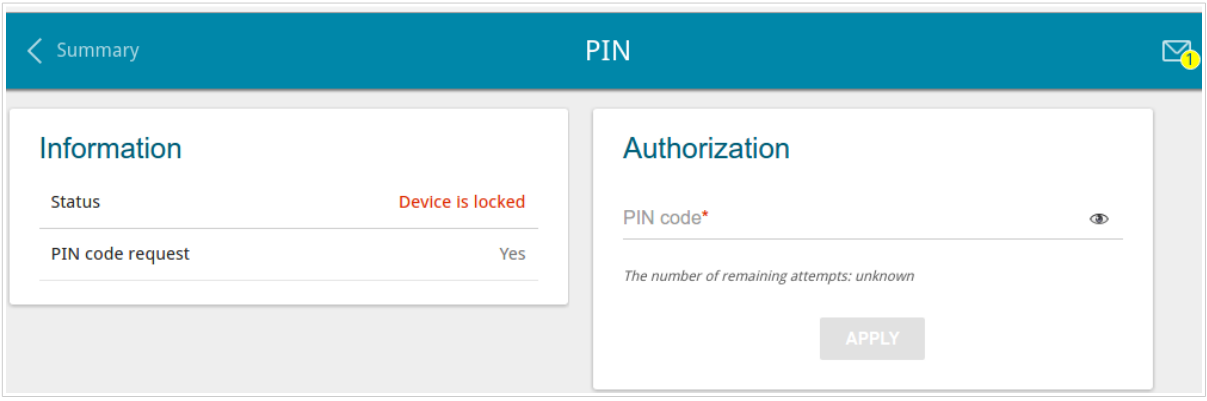

Figure 95. Entering the PIN code.

Some USB modems in the router mode and Android smartphones in the modem mode have an IP address from the subnet which coincides with the gateway's local subnet. In this case, the gateway's web-based interface can be unavailable. For correct operation, disconnect the device from the USB port and reboot the gateway. Then access the web-based interface, go to the **Connections Setup / LAN** page, and change the value of the **IP address** field on the **IPv4** tab (for example, specify the value `192.168.2.1`). Wait until the gateway is rebooted.

* For correct operation of USB modems you may need to update the gateway's firmware.

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

Basic Settings

On the **USB modem / Basic Settings** page, you can view data on the USB modem connected to the gateway and enable/disable the function for automatic creation of 3G/LTE WAN connection upon plugging a USB modem into the gateway.

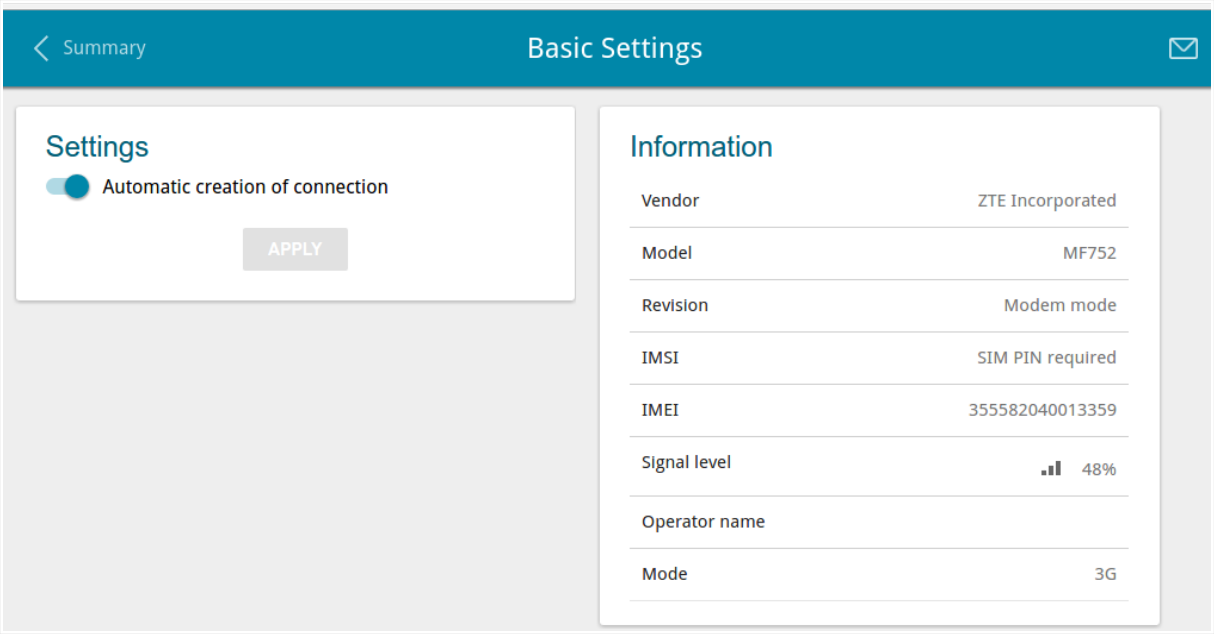

*Figure 96. The **USB modem / Basic Settings** page.*

If the **Automatic creation of connection** switch is moved to the right and the PIN code check for the SIM card inserted into your USB modem is disabled, then an active WAN connection with default settings (for LTE modems) or the operator's settings (for GSM modems) will be automatically created when plugging the USB modem into the gateway. The connection will be displayed on the **Connections Setup / WAN** page.

If you don't want to use this function, move the **Automatic creation of connection** switch to the left and click the **APPLY** button.

When a USB modem is connected to the gateway, the following data are displayed in the **Information** section:

Parameter	Description
Vendor	The manufacturer of your USB modem.
Model	The alphanumeric code of the model of your USB modem.
Revision	The revision of the firmware of your USB modem.
IMSI	The code stored in the SIM card inserted to your USB modem.
IMEI	The code stored in the memory of the USB modem.

Parameter	Description
Signal level	The signal level at the input of the modem's receiver. The zero signal level shows that you are out of the coverage area of the selected operator's network.
Operator name	When the needed network is available, the name of the operator is displayed in this field.
Mode	A type of the network to which the USB modem is connected.

PIN

On the **USB Modem / PIN** page, you can change the PIN code of the SIM card inserted into your USB modem, disable or enable the check of the PIN code.

! The operations presented on this page are unavailable for some models of LTE USB modems.

The current state of the SIM card inserted into your USB modem is displayed in the **Status** field. If the PIN code is entered incorrectly or the PIN code is not entered when the PIN code check is enabled, the **Device is locked** value is displayed in the **Status** field. If the PIN code is entered correctly or the PIN check is disabled, the **Device is unlocked** value is displayed in the **Status** field.

If the PIN code check for the SIM card inserted into your USB modem is not disabled, the **Yes** value is displayed in the **PIN code request** field. If the PIN check is disabled, the **No** value is displayed in the **PIN code request** field.

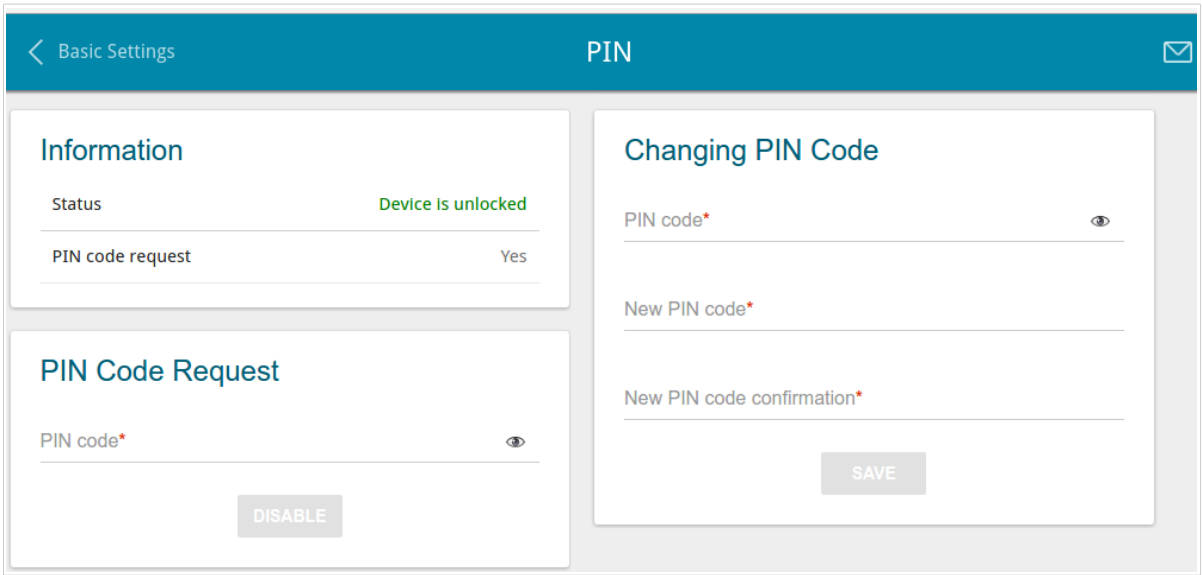

*Figure 97. The **USB Modem / PIN** page.*

To disable the PIN code check, in the **PIN Code Request** section, enter the current PIN code in the **PIN code** field and click the **DISABLE** button (the button is displayed if the PIN code check is enabled).

To enable the PIN code check, in the **PIN Code Request** section, enter the PIN code used before disabling the check in the **PIN code** field and click the **ENABLE** button (the button is displayed if the PIN code check is disabled).

To change the PIN code, in the **Changing PIN Code** section, enter the current code in the **PIN code** field, then enter a new code in the **New PIN code** and **New PIN code confirmation** fields and click the **SAVE** button.

If upon one of the operations described above you have entered an incorrect value in the **PIN code** field three times (the number of remaining attempts is displayed on the page), the SIM card inserted into your USB modem is blocked.

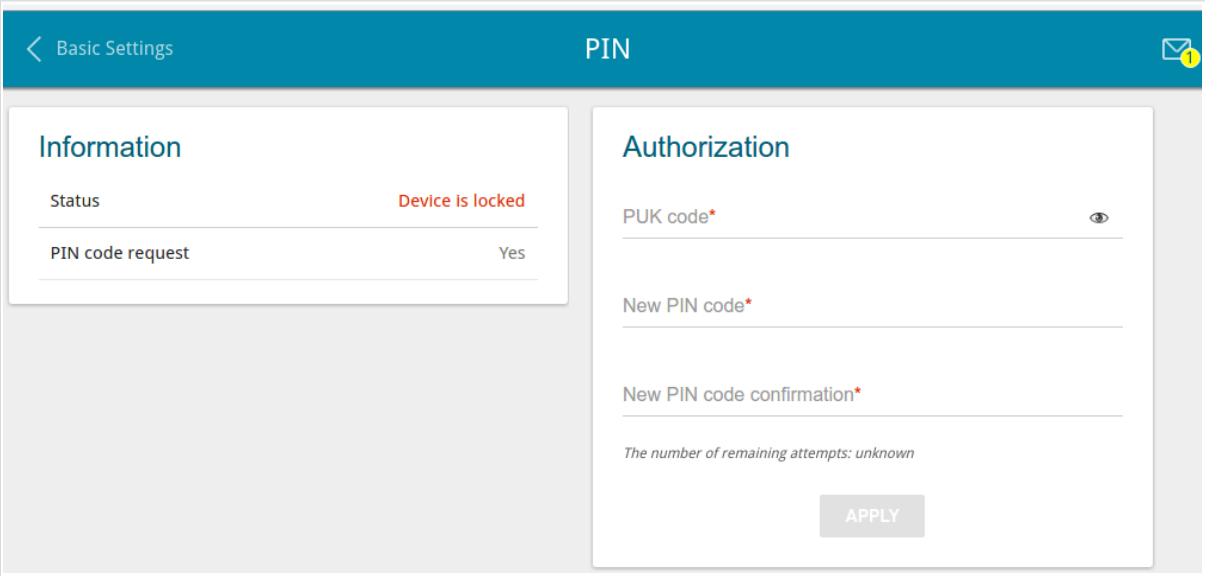

*Figure 98. The **USB Modem / PIN** page. The PUK code request.*

For further use of the card, in the **Authorization** section, enter the PUK code in the relevant field, and then specify a new PIN code for your SIM card in the **New PIN code** and **New PIN code confirmation** field. Click the **APPLY** button.

Advanced

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

- create groups of ports for VLANs
- allow using MVR technology
- view physical parameters of the gateway transmitter and the status of synchronization with the OLT device and specify data for authorization
- allow the gateway to connect to a private Ethernet line
- add name servers
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the gateway
- 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
- allow the gateway to use IGMP, RTSP, enable the SIP ALG, and the PPPoE/PPTP/L2TP/IPsec pass through functions
- configure VPN tunnels based on IPsec protocol.

VLAN

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

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

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

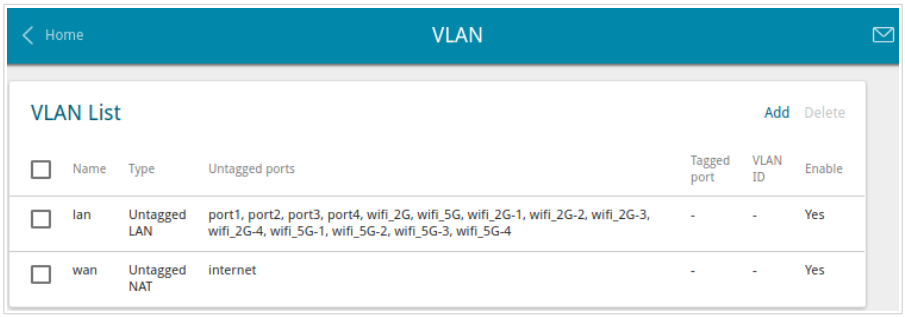

*Figure 99. The **Advanced / VLAN** page.*

If you want to create a group including LAN ports of the gateway, 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.

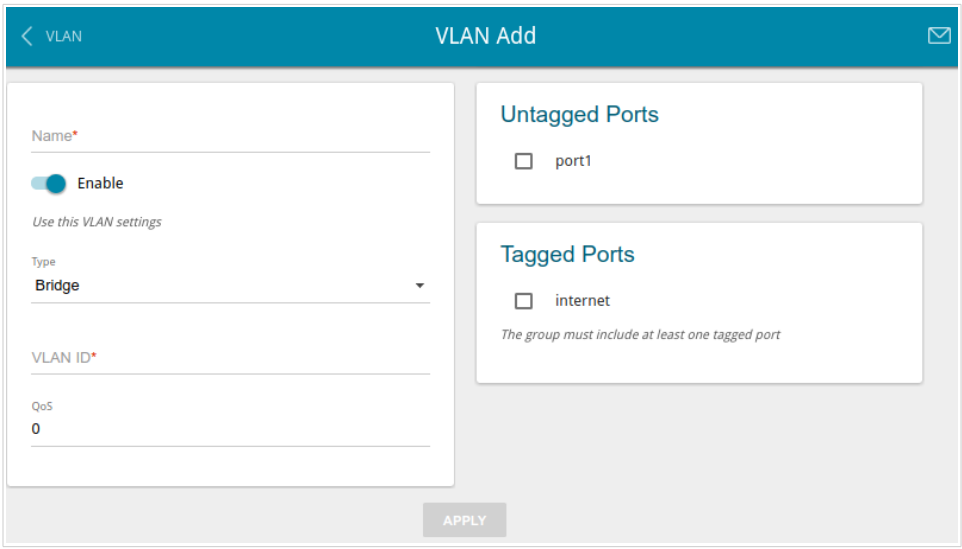

Figure 100. The page for adding a group of ports for VLAN.

You can specify the following parameters:

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

Parameter	Description
Type	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** and **QoS** fields 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. **Untagged LAN**. The group of untagged LAN ports is an internal connection with address translation without a VLAN tag for outgoing traffic. It is mostly used to connect to end devices (computers, servers). When this value is selected, the **VLAN ID** and **QoS** fields and the **Tagged Ports** section are not displayed. **Tagged LAN**. The group of tagged LAN ports is an internal connection with address translation with a VLAN tag for outgoing traffic. It is mostly used to connect to devices which recognize VLAN tags (switches, routers, gateways). When this value is selected, the **Untagged Ports** section is not displayed.
VLAN ID	An identifier of the VLAN to which this group of ports will be assigned.
QoS	A priority tag for the transmitted traffic.
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.

MVR

On the **Advanced / MVR** page, you can allow using MVR technology.

MVR technology (*Multicast VLAN Registration*) allows a server located in one VLAN to transmit multicast stream to clients located in other VLANs.

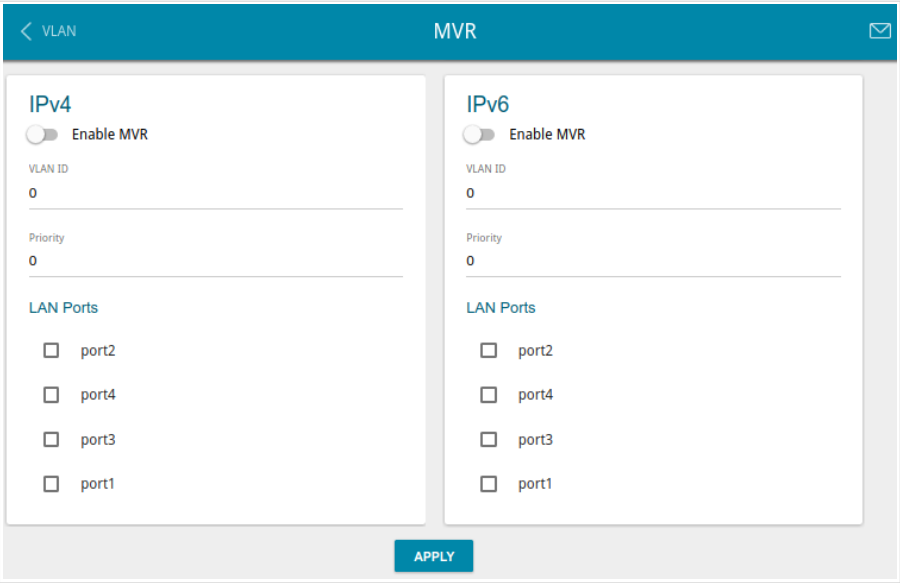

*Figure 101. The **Advanced / MVR** page.*

You can specify the following parameters:

Parameter	Description
IPv4/IPv6	
Enable MVR	Move the switch to the right to allow using MVR technology for the relevant protocol.
VLAN ID	An identifier of the VLAN which transmits multicast traffic.
Priority	A priority tag for multicast traffic.
LAN Ports	Select the checkboxes corresponding to the ports to which multicast traffic will be transmitted.

Click the **APPLY** button.

PON

On the **Advanced / PON** page, physical parameters of the gateway transmitter and the status of synchronization with the OLT device are displayed. In addition, you can specify data for authorization on this page.

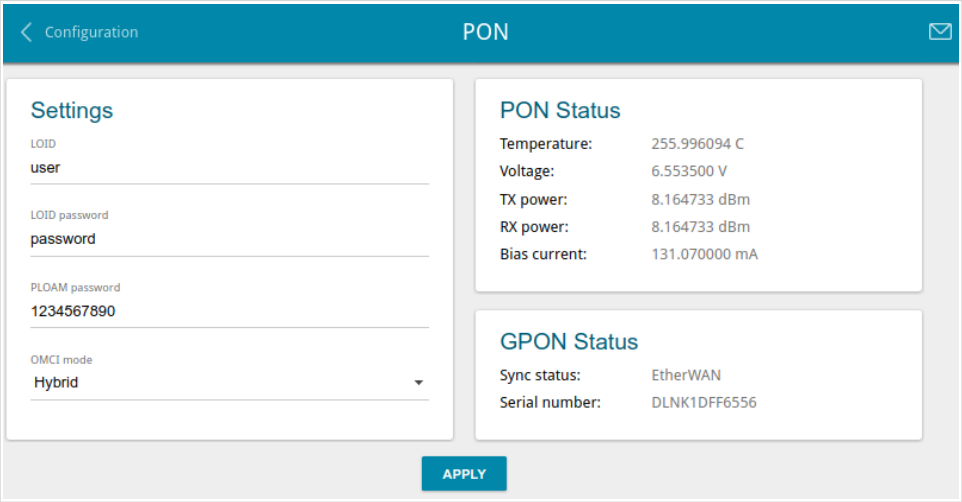

*Figure 102. The **Advanced / PON** page.*

If authorization is needed for synchronization with the OLT, enter the authorization data provided by your ISP in the fields of the **Settings** section and select the needed value from the **OMCI mode** drop-down list (*ONT Management and Control Interface*). Then click the **APPLY** button.

In the **PON Status** section, the current state of the transmitter is displayed.

In the **GPON Status** section, the state of synchronization with the OLT and the serial number of the gateway used for identification by the OLT are displayed.

EtherWAN

On the **Advanced / EtherWAN** page, you can configure the gateway to connect to a private Ethernet line.

! The Ethernet WAN function allows using any LAN port of the gateway to access the Internet via Ethernet technology. When the function is enabled, the optical port of the gateway is inactive.

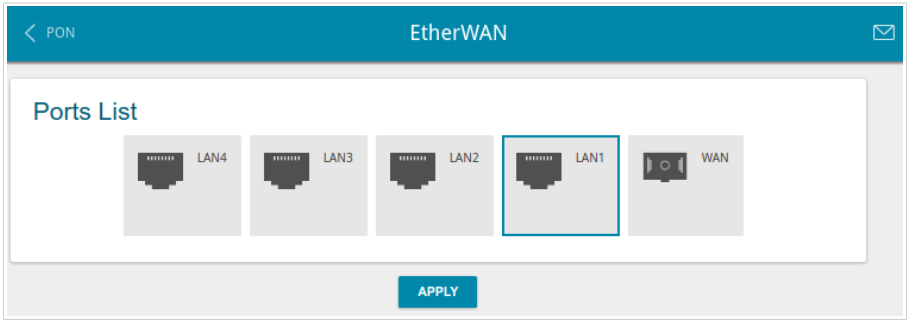

*Figure 103. The **Advanced / EtherWAN** page.*

To use one of the gateway's LAN port as the WAN port, click the icon corresponding to this port and click the **APPLY** button. Port configured as the WAN port is highlighted in blue.

If in the future you need to connect the gateway to a fiber optic line, click the **WAN** icon and then click the **APPLY** button.

DNS

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

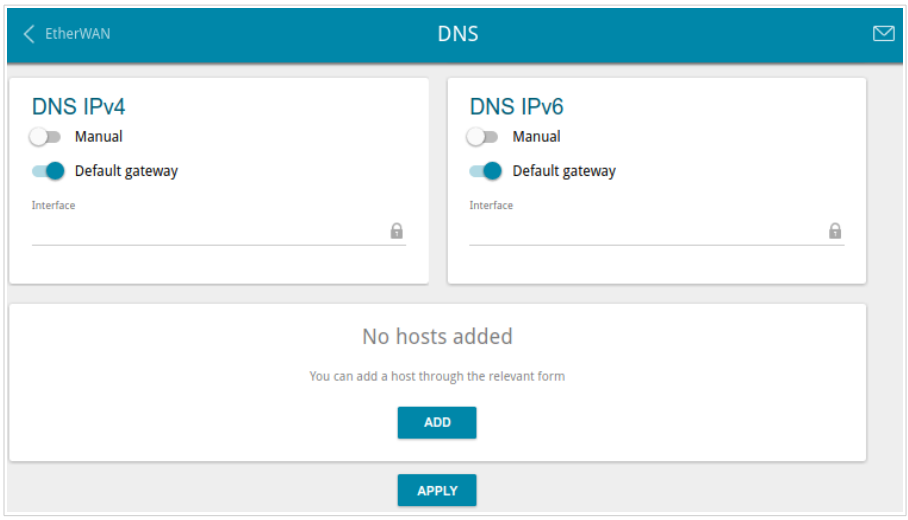

*Figure 104. The **Advanced / DNS** page.*

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 gateway 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 gateway 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.

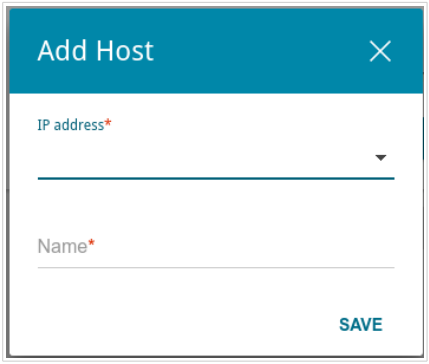

Figure 105. The window for adding a DNS record.

In the **IP address** field, specify a host from the internal or external network. You can choose a device connected to the gateway'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.

Ports Settings

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

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.

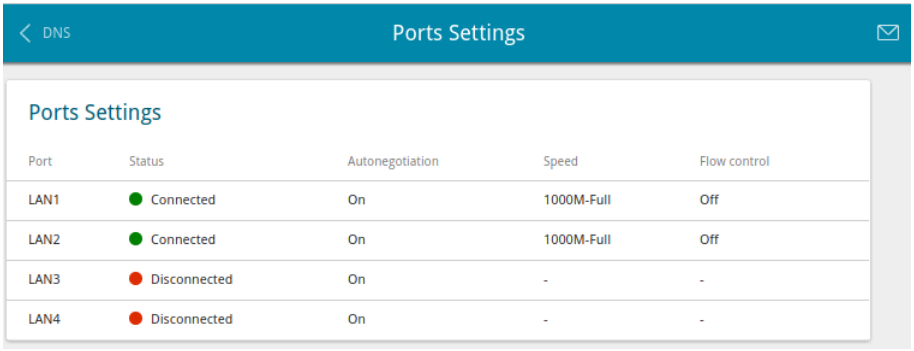

*Figure 106. The **Advanced / Ports Settings** page.*

In order to configure autonegotiation or configure speed and duplex mode manually for an Ethernet port, select it in the table.

! Autonegotiation should be enabled for both devices connected to each other.

! When autonegotiation is disabled, speed and duplex mode settings for both devices connected to each other should be the same.

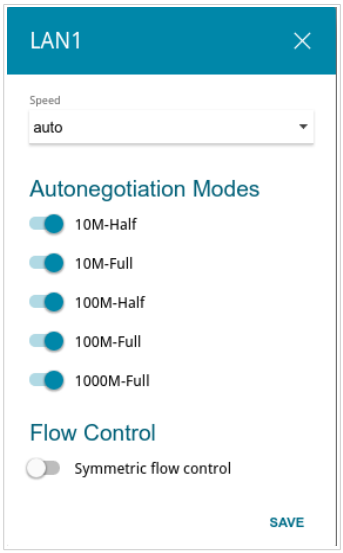

Figure 107. The window for changing the settings of the gateway's port.

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 gateway's port, select the port in the table. In the opened window, change the needed parameters and click the **SAVE** button.

Redirect

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

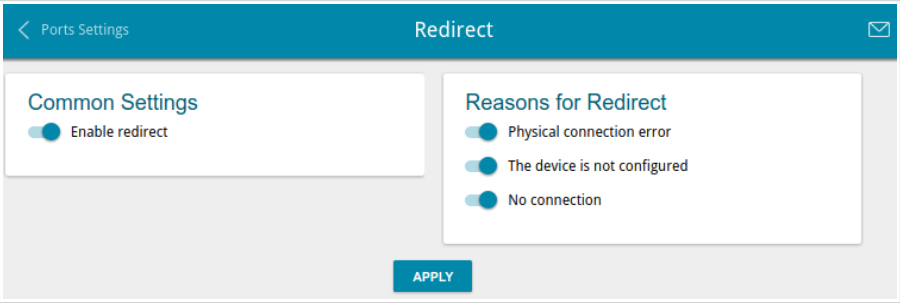

*Figure 108. The **Advanced / Redirect** page.*

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

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

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

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

DDNS

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

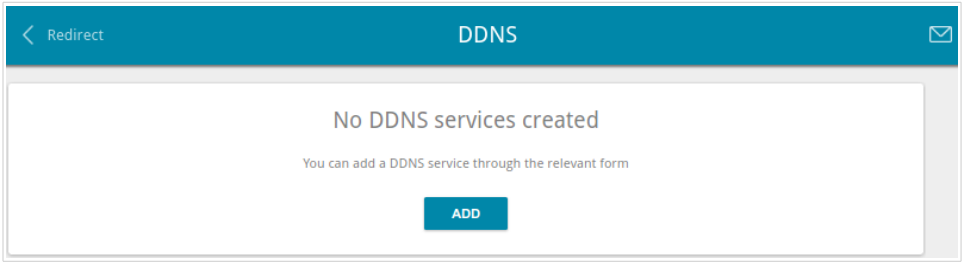

*Figure 109. The **Advanced / DDNS** page.*

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

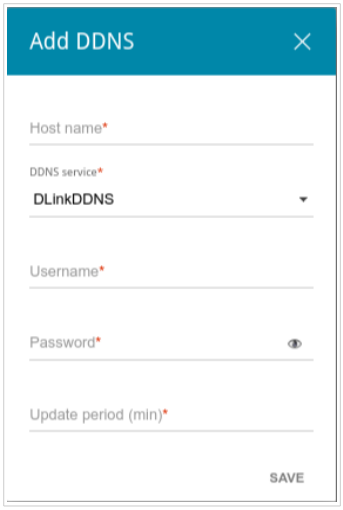

Figure 110. The window for adding a DDNS service.

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 gateway'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.

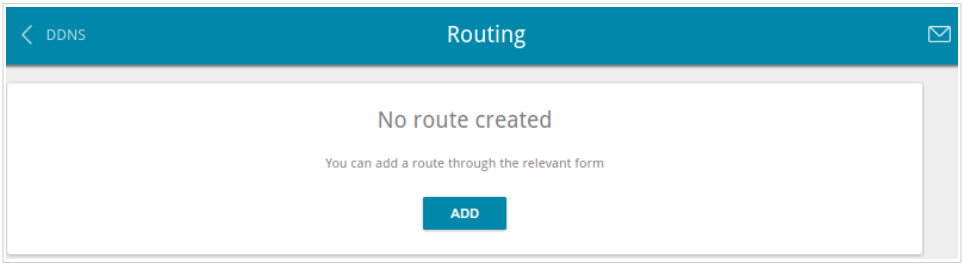

*Figure 111. The **Advanced / Routing** page.*

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

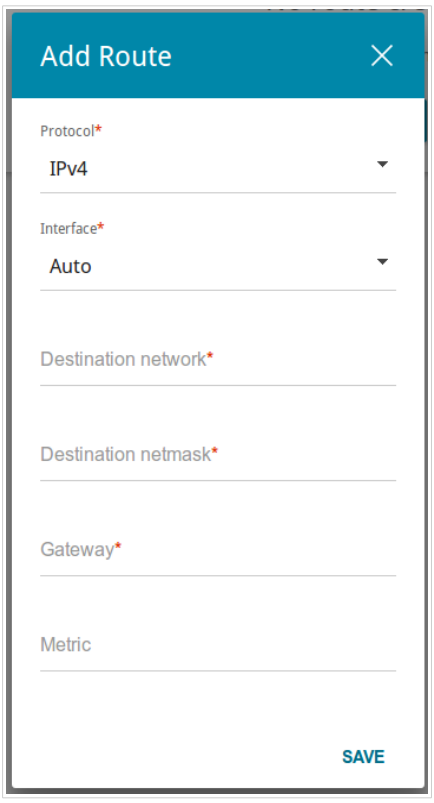

Figure 112. The window for adding a new route.

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 gateway 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. In the opened window, change the needed parameters and click the **SAVE** button.

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

TR-069 Client

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

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

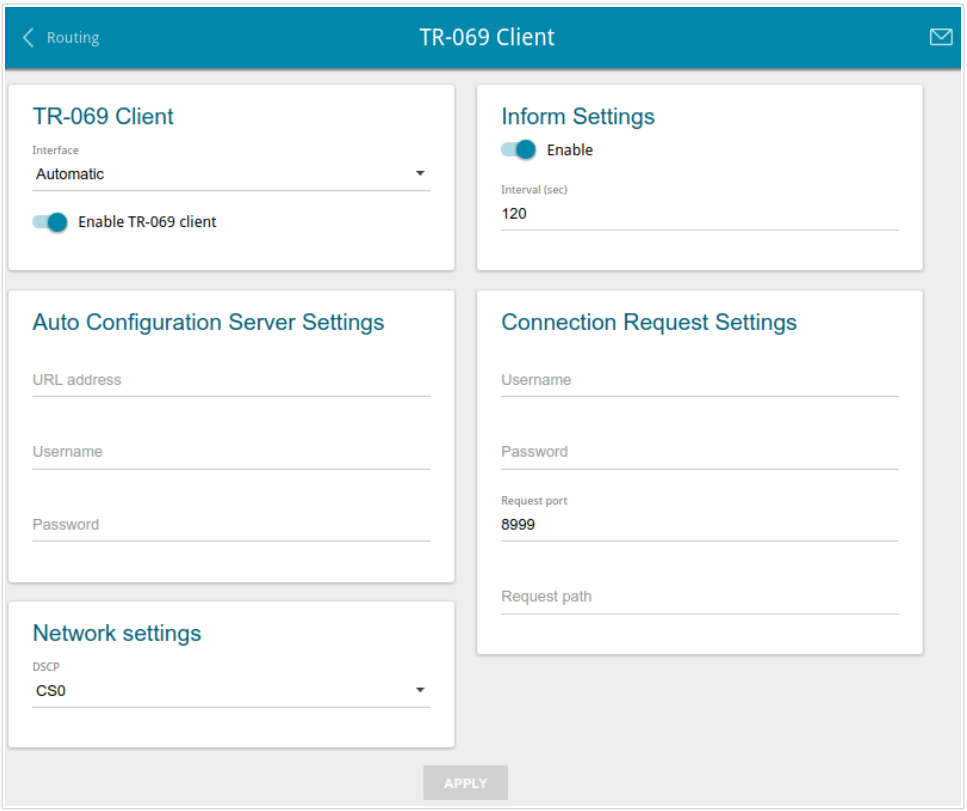

Figure 113. The page for configuring the TR-069 client.

You can specify the following parameters:

Parameter	Description
TR-069 Client	
Interface	The interface which the gateway uses for communication with the ACS. Leave the **Automatic** value to let the device select the interface basing on the routing table or select another value if required by your ISP.
Enable TR-069 client	Move the switch to the right to enable the TR-069 client.
Inform Settings	
Enable	Move the switch to the right so the gateway may send reports (data on the device and network statistics) to the ACS.
Interval	Specify the time period (in seconds) between sending reports.

Parameter	Description
Auto Configuration Server Settings	
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS.
Connection Request Settings	
Username	The username used by the ACS to transfer a connection request to the gateway.
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.
Network settings	
DSCP	*Differentiated Services Codepoint.* From the drop-down list, select a priority tag for the transmitted traffic.

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 gateway. By default, the access from external networks to the gateway is closed. If you need to allow access to the gateway from the external network, create relevant rules.

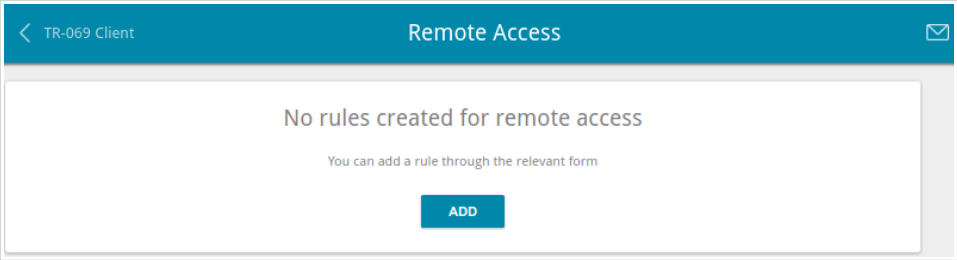

*Figure 114. The **Advanced / Remote Access** page.*

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

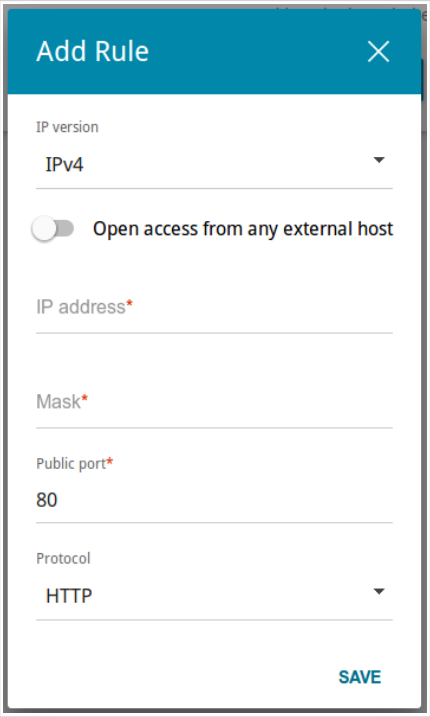

Figure 115. The window for adding a rule for remote management.

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 gateway for any host. Upon that the **IP address** and **Mask** fields are not displayed.
IP address	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.

Parameter	Description
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 gateway. You can specify only one port.
Protocol	The protocol available for remote management of the gateway.

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 gateway uses the UPnP IGD protocol for automatic configuration of its parameters for network applications requiring an incoming connection to the gateway.

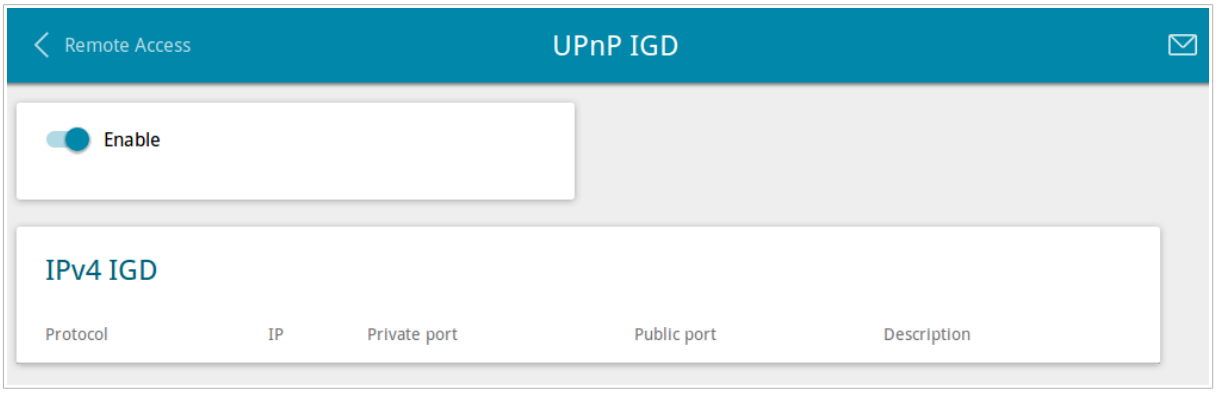

*Figure 116. The **Advanced / UPnP IGD** page.*

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 gateway, move the **Enable** switch to the right.

When the protocol is enabled, the gateway'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 gateway.
Public port	A public port of the gateway from which traffic is directed to a client's IP address.
Description	Information transmitted by a client's network application.

IGMP/ALG/Passthrough

On the **Advanced / IGMP/ALG/Passthrough** page, you can allow the gateway 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 connections of the gateway.

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

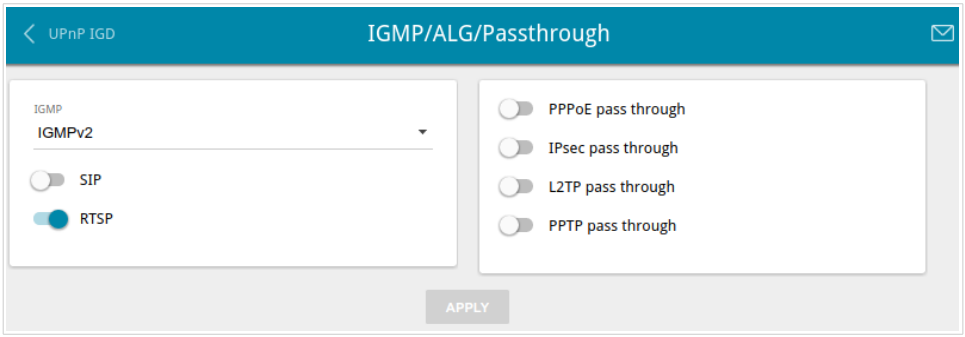

*Figure 117. The **Advanced / IGMP/ALG/Passthrough** page.*

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.
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 gateway.[16]
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.

16 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 an Ethernet cable between a LAN port of the gateway and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

IPsec

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

IPsec is a protocol suite for securing IP communications.

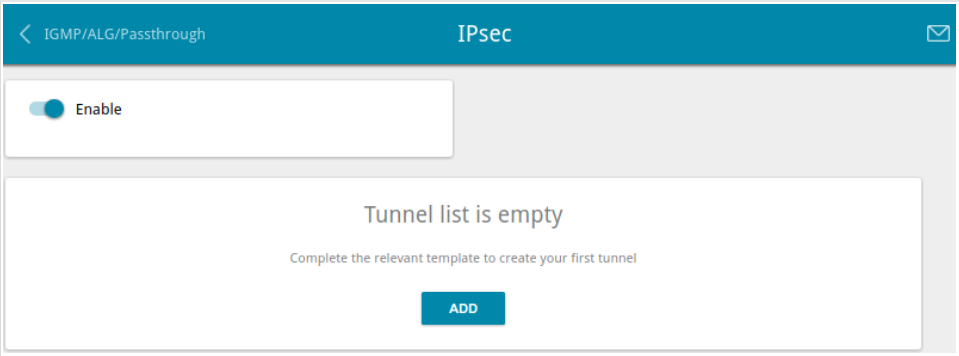

*Figure 118. The **Advanced / IPsec** page.*

To allow IPsec tunnels, move the **Enable** switch to the right. Then click the **ADD** button to create a new tunnel.

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

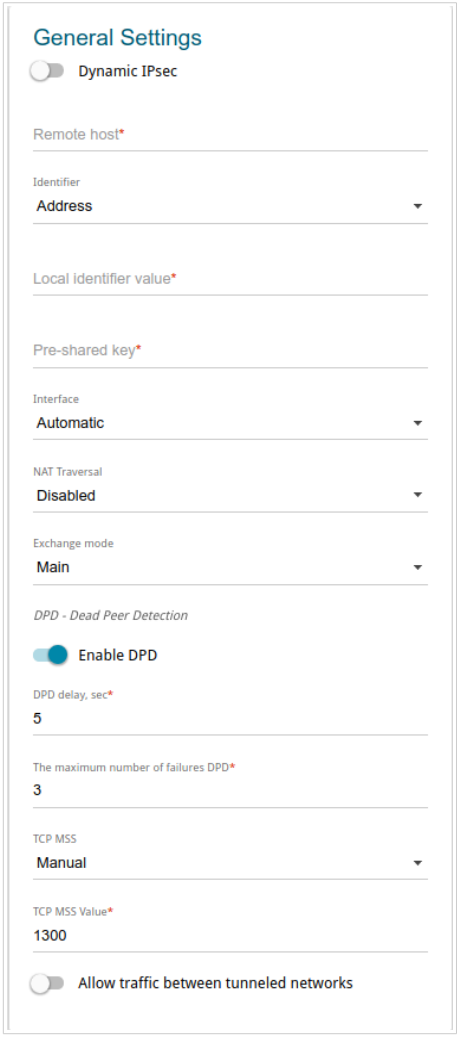

*Figure 119. The page for adding an IPsec tunnel. The **General Settings** section.*

You can specify the following parameters:

Parameter	Description
General Settings	
Dynamic IPsec	Move the switch to the right to allow a remote host with any public IP address to connect to the gateway via IPsec protocol. Such a setting can be specified for one tunnel only. Connection requests via this tunnel can be sent by a remote host only.
Remote host	A remote subnet VPN gateway IP address. The field is available if the **Dynamic IPsec** switch is moved to the left.

Parameter	Description
Identifier	Select an identification method for the local host (gateway) from the drop-down list: **Address:** The local host is identified by its IP address. **FQDN:** The local host is identified by its domain name. The value is unavailable if the **Main** value is selected from the **Exchange mode** list.
Local identifier value	Specify the local host identifier.
Pre-shared key	A key for mutual authentication of the parties.
Interface	Select a WAN connection through which the tunnel will pass. When the **Automatic** value is selected, the gateway uses the default WAN connection.
NAT Traversal	The NAT Traversal function allows VPN traffic to pass through the NAT-enabled gateway. Select the **Disabled** value to disable the function. Select the **Enabled** value to enable the function if it is supported by a remote host. Select the **Force** value to make the function be always on, even if it is not supported by a remote host.
Exchange mode	Select the mode of negotiation from the drop-down list: **Main:** The mode provides the most secure communication between the parties in the course of negotiation of the authentication procedures. **Base:** The draft negotiation mode with preliminary authentication of a host. **Aggressive:** The mode provides faster operation as it skips several stages of negotiation of the authentication procedures.
Enable DPD	Move the switch to the right to enable using DPD protocol for this tunnel. Such a setting allows to check the status of a remote host: if encrypted packets exchange between the gateway and the remote host breaks down, the gateway starts sending DPD messages to the remote host. If the switch is moved to the left, the **DPD delay** and **The maximum number of failures DPD** fields are not available for editing.
DPD delay	A time period (in seconds) between attempts to check the status of a remote host. By default, the value **5** is specified.

Parameter	Description
The maximum number of failures DPD	A number of DPD messages that were sent to check the status of a remote host and left unanswered. By default, the value **3** is specified. If a remote host does not answer the specified number of messages, the gateway breaks down the tunnel connection, removes the encryption keys, and tries to activate the connection.
TCP MSS	*Maximum Segment Size of a TCP packet.* This parameter influences the size of a TCP packet which will be sent from a remote host to the gateway. If the **Manual** value is selected, you can specify the parameter in the **TCP MSS Value** field. If the **Path MTU discovery** value is selected, the parameter will be configured automatically.
TCP MSS Value	The maximum size (in bytes) of a non-fragmented packet. The field is available for editing when the **Manual** value is selected from the **TCP MSS** drop-down list.
Allow traffic between tunneled networks	Move the switch to the right to allow data exchange between subnets with which IPsec tunnels have been created.

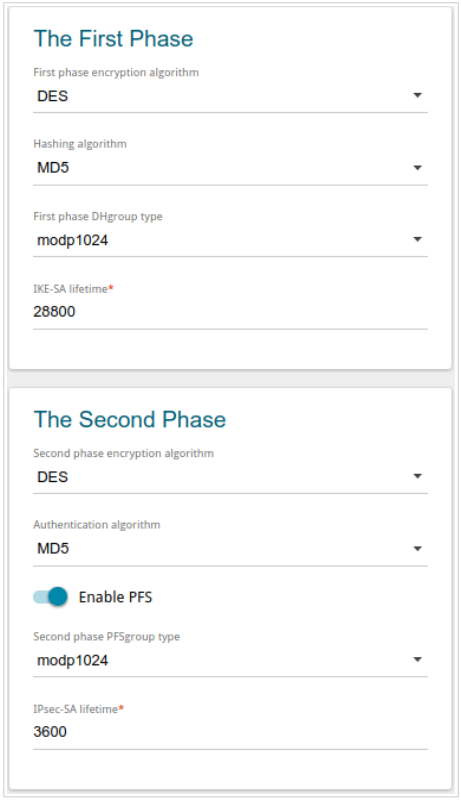

*Figure 120. The page for adding an IPsec tunnel. **The First Phase** / **The Second Phase** sections.*

Parameter	Description
The First Phase	
First phase encryption algorithm	Select encryption algorithm from the drop-down list.
Hashing algorithm	Select hashing algorithm from the drop-down list.
First phase DHgroup type	A Diffie-Hellman key group for Phase 1. Select a value from the drop-down list.
IKE-SA lifetime	The lifetime of IKE-SA keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should exceed the value specified in the **IPsec-SA lifetime** field. Specify `0` if you don't want to limit the lifetime of the keys.
The Second Phase	
Second phase encryption algorithm	Select encryption algorithm from the drop-down list.
Authentication algorithm	Select authentication algorithm from the drop-down list.

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

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

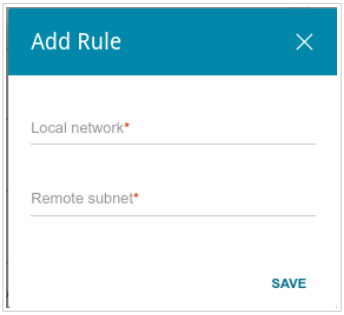

Figure 121. The page for adding an IPsec tunnel. The window for adding a tunneled network.

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

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

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

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

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

After clicking the **APPLY** button, the page with the **Tunnels** and **Status** sections opens. In the **Status** section, the current state of an existing tunnel is displayed.

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

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

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

VoIP

In this menu you can configure all parameters essential for VoIP via SIP and specify all needed settings for the phone connected to the gateway.

Basic Settings

On the **VoIP / Basic Settings** page, you can configure all needed settings for VoIP via SIP.

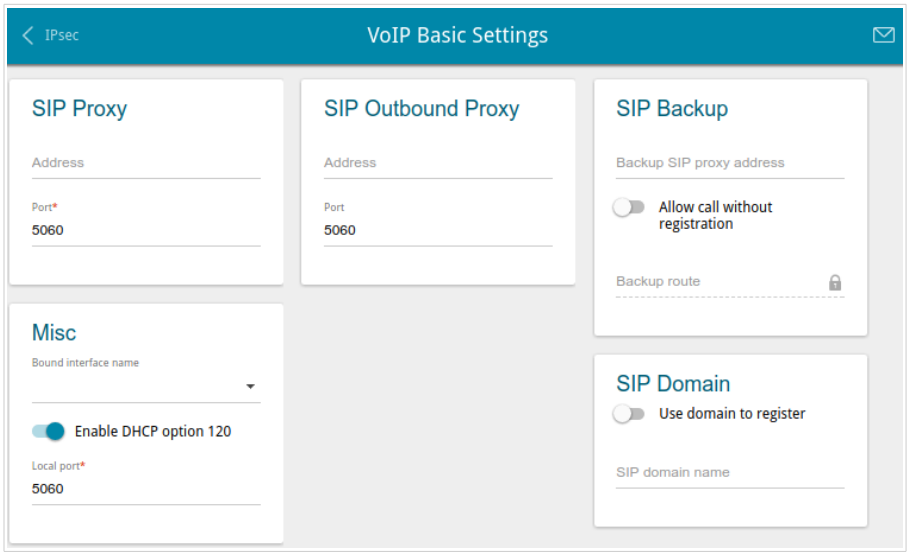

*Figure 122. The **VoIP / Basic Settings** page.*

Parameter	Description
SIP Proxy	
Address	An IP or URL address of the SIP proxy server.
Port	A port of the SIP proxy server. Unless another setting is given by your ISP, it is recommended to leave the default value (`5060`).
SIP Outbound Proxy	
Address	An IP or URL address of the SIP outbound proxy server.
Port	A port of the SIP outbound proxy server. Unless another setting is given by your ISP, it is recommended to leave the default value (`5060`).
SIP Backup	
Backup SIP proxy address	An IP address of the backup SIP proxy server. The gateway uses the backup SIP proxy server in case of no response from the main SIP proxy server.

Parameter	Description
Allow call without registration	Move the switch to the right to allow calls without registration on the main SIP proxy server.
Backup route	An IP address to which calls will be forwarded if the main or backup SIP proxy servers are unavailable.
Misc	
Bound interface name	From the drop-down list, select an interface (the local interface or an IPv4 WAN connection) which will be used for VoIP.
Enable DHCP option 120	Move the switch to the right to allow using DHCP option 120. When the option is enabled, the **Address** field in the **SIP Proxy** section and the **Backup SIP proxy address** field in the **SIP Backup** section are filled in automatically.
Local port	The gateway's port used for exchanging data with the SIP server. Unless another setting is given by your ISP, it is recommended to leave the default value (`5060`).
SIP Domain	
Use domain to register	Move the switch to the right if your ISP requires to specify a domain name upon registration on the SIP proxy server. Then fill in the **SIP domain name** field.
SIP domain name	When this field is filled in, the gateway registers on the SIP proxy server using the specified domain name. When the field is blank, the gateway uses the IP address assigned to it.

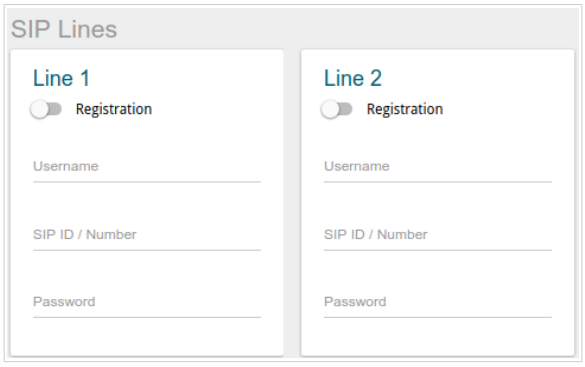

*Figure 123. The **VoIP / Basic Settings** page. The **SIP Lines** section.*

Parameter	Description
SIP Lines	
Line 1, Line 2	
Registration	Move the switch to the right to register the line on the SIP proxy server.
Username	A username for this line. For most SIP proxy servers the username coincides with the phone number.
SIP ID / Number	A number for this line. The called party sees the specified value as the caller number.
Password	A user password for this line.

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

Advanced

On the **VoIP / Advanced settings** page, you can specify additional settings for VoIP via SIP.

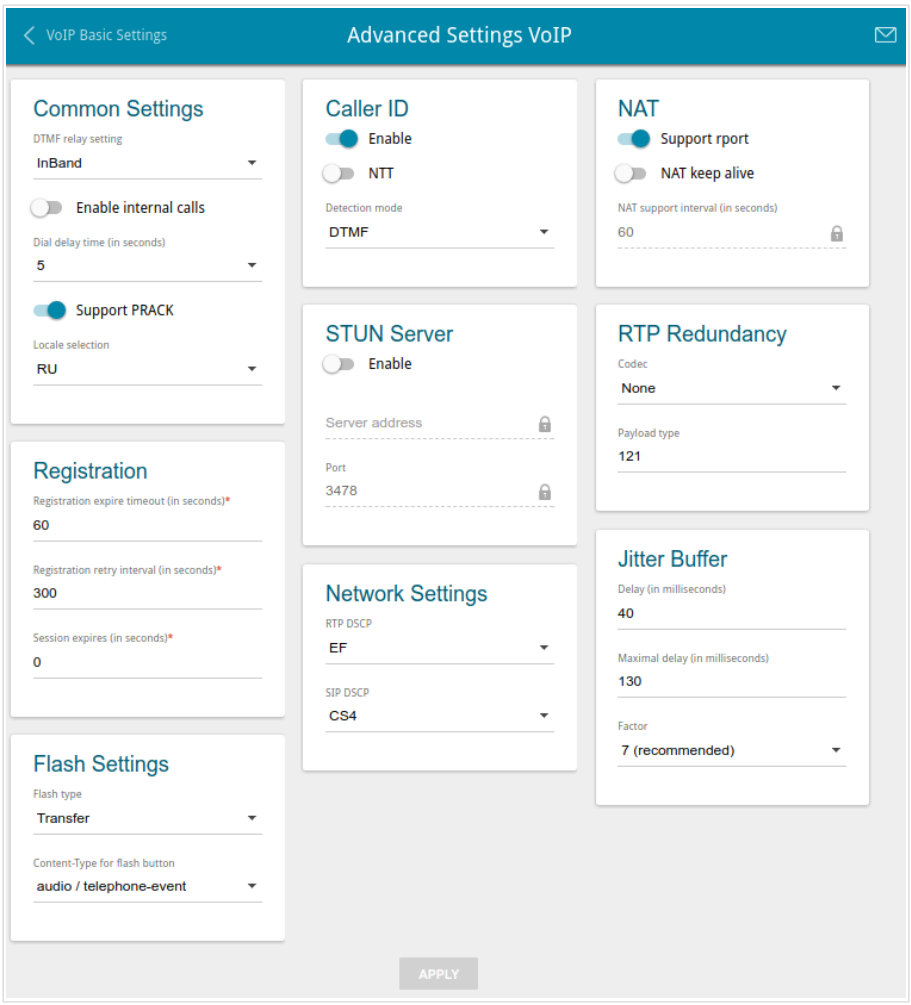

*Figure 124. The **VoIP / Advanced** page.*

Parameter	Description
Common Settings	
DTMF relay setting	From the drop-down list, select a mode for DTMF signal transmission. • **InBand**: transmission with voice data. • **RFC2833**: transmission in accordance with RFC2833. • **SIPInfo**: transmission in the relevant SIP messages.
Payload type	Select a data type from the drop-down list. The list is displayed if the **RFC2833** value is selected from the **DTMF relay setting** drop-down list.

Parameter	Description
Enable internal calls	Move the switch to the right to allow calls from the phones connected the FXS ports pass through the gateway without the SIP server.
Dial delay time	The delay time before the next digit is dialed (from 3 to 9 seconds). When this time expires, the gateway regards that the dialing is completed and sends the request to the server. Select a needed value from the drop-down list.
Support PRACK	Move the switch to the right to enable the PRACK method (*Provisional Response ACKnowledgement*). The PRACK method provides reliable transmission of packets with provisional responses to an initiating request upon setting a session in accordance with RFC3262.
Locale selection	Select your country from the drop-down list. By default, the value **RU** (Russia) is specified. This setting defines the parameters of the phone signals traditional for the specific country.
Caller ID	
Enable	Move the switch to the right to activate the automatic caller identification function for the phones connected to the FXS ports of the gateway.
NTT	Move the switch to the right to enable support of the NTT standard.
Detection mode	Select the Caller ID mode for the phones connected to the FXS ports of the gateway.
NAT	
Support rport	Move the switch to the right to enable the Symmetric Response Routing function in accordance with RFC3581. This function allows sending responses to a request to the port and IP address from which the request was received via the NAT-enabled gateway. The SIP proxy server must support the function.
NAT keep alive	Move the switch to the right to allow the gateway to support the state of automatically forwarded ports by periodic exchange of service messages. If the switch is moved to the right, the **NAT support interval** field is available for editing.
NAT support interval	The time interval between service messages. Specify a needed value.

Parameter	Description
Registration	
Registration expire timeout	A time period (in seconds) after which the gateway changes the registration status in case of no response from the SIP proxy server.
Registration retry interval	A time period (in seconds) after which the registration will be repeated.
Session expires	A time period (in seconds) between attempts to check the status of the voice session.
STUN Server	
Enable	Move the switch to the right to enable the STUN client (*Session Traversal Utilities for NAT*). The STUN client sends requests to a STUN server. On the basis of the received replies, the client allows VoIP traffic to pass through the NAT-enabled gateway. If the switch is moved to the right, the **Server address** and **Port** fields are available for editing.
Server address	An IP or URL address of a STUN server to which a connection is established.
Port	A port of a STUN server to which a connection is established. By default, the port `3478` is specified.
RTP Redundancy	
Codec	The RTP Redundancy function allows restoring a part of lost RTP packets while transmitting audio data. From the drop-down list, select a codec to which the function should be applied. To disable the function, select the **None** value from the drop-down list.
Payload type	Payload data type.
Flash Settings	
Flash type	The **FLASH** action type. • **Transfer**: switching between calls. • **SIPInfo**: sending a service message to the SIP server. The value is available if the **SIPInfo** value is selected from the **DTMF relay setting** drop-down list.

Parameter	Description
Content-Type for flash button	If the **SIPInfo** value is selected from the **Flash type** drop-down list, you can select the type of data transferred in SIP INFO messages upon pressing the **FLASH** key.
Network Settings	
RTP DSCP / SIP DSCP	*Differentiated Services Codepoint.* From the relevant drop-down list, select tags for voice and signaling traffic.
Jitter Buffer	
Delay / Maximal delay	The Jitter Buffer parameter improves the quality of voice transmission: received voice packets are specially delayed, which allows their reproducing in the order they were sent from the transmitting side. Specify the minimal and maximal packets waiting period (in milliseconds) in the relevant fields.
Factor	This parameter enhances efficiency of jitter buffer operation. When the minimal value is selected, the delay value will tend to be lower. Select the relevant value from the drop-down list.

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

SIP Lines

On the **VoIP / SIP Lines** page, you can specify incoming/outgoing call settings for the SIP line.

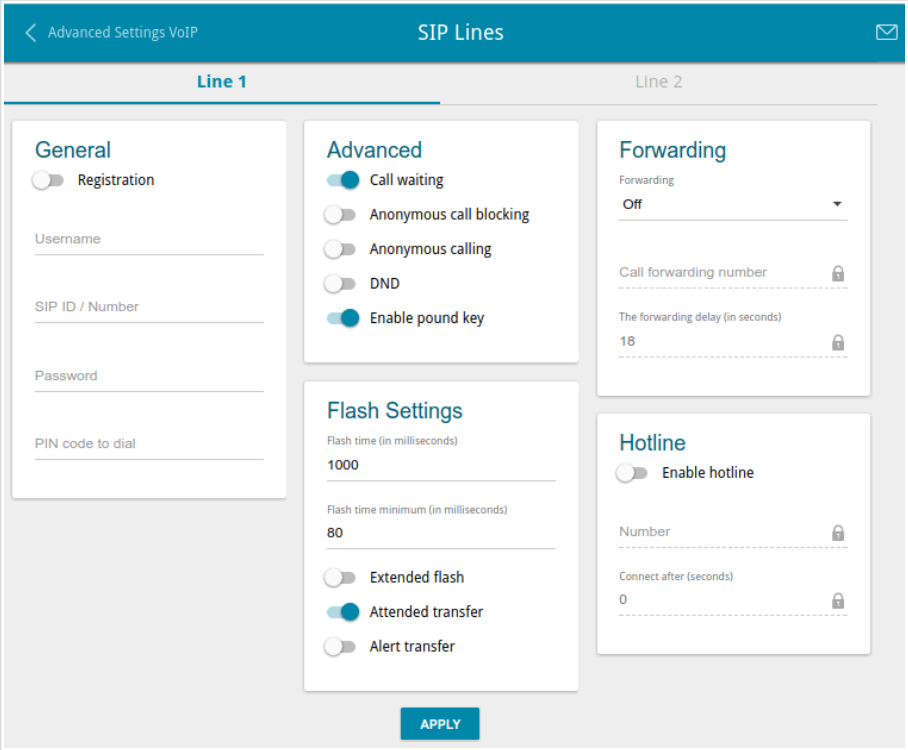

*Figure 125. The **VoIP / SIP Lines** page. The **Line 1** tab.*

On the relevant tab (**Line 1** or **Line 2**), you can specify the following parameters:

Parameter	Description
General	
Registration	Move the switch to the right to register the line on the SIP proxy server.
Username	A username for this line. For most SIP proxy servers the username coincides with the phone number.
SIP ID / Number	A number for this line. The called party sees the specified value as the caller number.
Password	A user password for this line.
PIN code to dial	Fill in the field to allow the user of the phone to make calls only after dialing the PIN code.

Parameter	Description
Advanced	
Call waiting	Move the switch to the right to accept incoming calls when the line is busy. To switch between calls, press the **FLASH** key on the phone.
Anonymous call blocking	Move the switch to the right to reject calls when the calling party conceals its number.
Anonymous calling	Move the switch to the right to conceal your number from the called party.
DND	*Do Not Disturb*. Move the switch to the right to reject all incoming calls (the busy tone will be heard).
Enable pound key	Move the switch to the right to speed up dialing with pressing # (the pound key) immediately after dialing numbers.
Forwarding	
Forwarding	From the drop-down list, select a forwarding mode for the current line. Leave the **Off** value if forwarding is not needed.
Call forwarding number	A number to which the gateway redirects calls in accordance with the mode selected from the **Forwarding** list.
The forwarding delay	A time period (in seconds) after which the gateway redirects calls to the number specified in the **Call forwarding number** field. The field is available for editing if the **If no answer** value is selected from the **Forwarding** list.
Flash Settings	
Flash time / Flash time minimum	The maximum and minimum value for flash time (the user hangs up the receiver and lifts it again) which the gateway will regard as pressing the **FLASH** key.

Parameter	Description
Extended flash	Move the switch to the right to use combination of the **FLASH** key and number keys of the phone in order to organize three-party calls or transfer calls . Use of **FLASH** key • The function is enabled. The phone connected to this line has an incoming call in the standby mode and an outgoing call in the talk mode. It's needed to press the **FLASH** key, hear the dial tone, and then press: ◦ the number key **0** in order to end the first call and continue the second call, ◦ the number key **1** in order to end the second call and continue the first call, ◦ the number key **2** in order to put the second call on hold and continue the first call, ◦ the number key **3** to have a three-party call with the first and second speakers. • The function is not enabled. The phone connected to this line has an incoming call in the standby mode and an outgoing call in the talk mode. It's needed: ◦ to press the **FLASH** key in order to put the second call on hold and continue the first call, ◦ to hang up the receiver in order to end both calls and connect the first and second speakers to each other.
Attended transfer	Move the switch to the right if you want to transfer calls when a called party's receiver is lifted.
Alert transfer	Move the switch to the right if you want to transfer calls when a dial tone is heard.
Hotline	
Enable hotline	Move the switch to the right to make the phone connected to this line dial the number specified in the **Number** field after the receiver is lifted.
Number	A number dialed by the phone connected to this line after the receiver is lifted. Also you can specify a number in the format `phone_number@IP_address` for direct IP calls bypassing the SIP proxy server. The field is available for editing if the **Enable hotline** switch is moved to the right.

Parameter	Description
Connect after	A time period (in seconds) between lifting up the receiver and dialing the hotline number. The field is available for editing if the **Enable hotline** switch is moved to the right.

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

Fax Settings

On the **VoIP / Fax Settings** page, you can specify settings of data receipt/transfer for the fax machines connected to the FXS ports of the gateway.

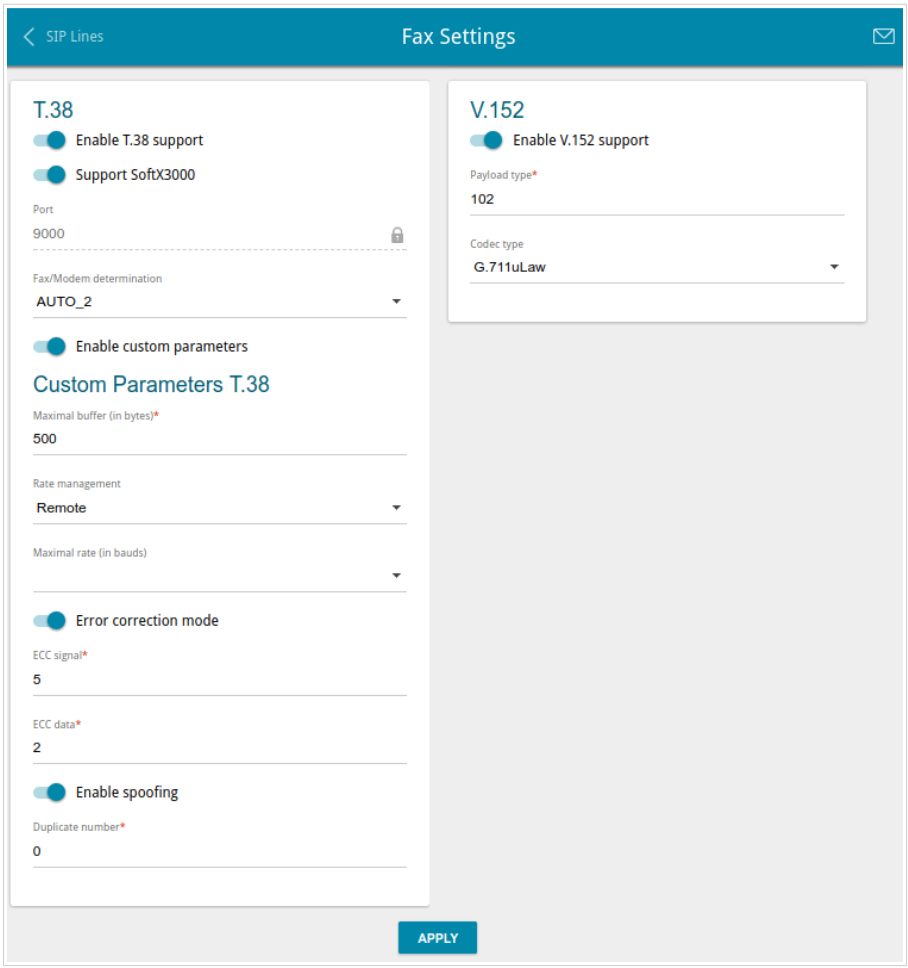

*Figure 126. The **VoIP / Fax Settings** page.*

Parameter	Description
T.38	
Enable T.38 support	Move the switch to the right to allow support of the T.38 protocol. If the switch is moved to the right, the **Support SoftX3000** switch, the **Port** field, the **Fax/Modem determination** drop-down list, and the **Enable custom parameters** switch are displayed on the page.
Support SoftX3000	Move the switch to the right to let the gateway support operation with SoftX3000. If the switch is moved to the right, the **Port** field is unavailable for editing.
Port	The gateway's port for data transfer via T.38.

Parameter	Description
Fax/Modem determination	From the drop-down list, select a mode of fax/modem signal detection.
Enable custom parameters	Move the switch to the right to specify additional parameters for T.38. Upon that the **Custom parameters T.38** section is displayed on the page.
Custom parameters T.38	
Maximal buffer	The maximum buffer size for data received by the gateway.
Rate management	From the drop-down list, select a method for facsimile data transfer rate management: **Local** or **Remote**.
Maximal rate	From the drop-down list, select the maximum rate for facsimile data receipt/transfer.
Error correction mode	Move the switch to the right to enable the error correction mode. When the switch is moved to the right, the **ECC signal** and **ECC data** fields are available for editing.
Enable spoofing	Move the switch to the right to let the gateway simulate facsimile data receipt/transfer in case of delays.
Duplicate number	Specify number of packet duplications.
V.152	
Enable V.152 support	Move the switch to the right to allow support of the V.152 recommendation. Upon that the **Payload type** field and the **Codec type** drop-down list are displayed on the page.
Payload type	Payload data type in accordance with RFC2833.
Codec type	From the drop-down list, select a codec for data transfer in accordance with V.152.

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

Audio Settings

On the **VoIP / Audio Settings** page, you can configure audio parameters, volume and voice codecs.

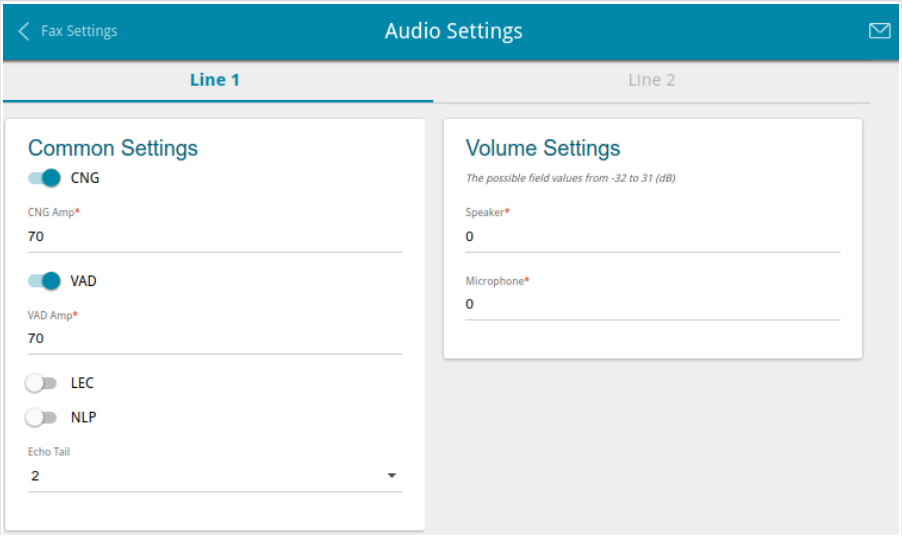

*Figure 127. The **VoIP / Audio Settings** page. The **Common settings** and **Volume Settings** sections. The **Line 1** tab.*

On the relevant tab (the **Line 1** or **Line 2**), you can specify the following parameters:

Parameter	Description
Common Settings	
CNG	*Comfort Noise Generation.* Move the switch to the right to enable the function.
CNG Amp	Signal amplitude threshold to start comfort noise generation. Specify a value from `0` to `200`. If `0` is specified, the threshold is not set.
VAD	*Voice Activity Detection.* Move the switch to the right to enable the function.
VAD Amp	Signal amplitude threshold to start silence compression. Specify a value from `0` to `200`.
LEC	*Line Echo Cancellation.* Move the switch to the right to enable the function.
NLP	*Nonlinear Processing.* Move the switch to the right to enable the function.
Echo Tail	Maximum echo tail length (in milliseconds). Select the needed value from the drop-down list.

Parameter	Description
Volume Settings	
Speaker	Specify the earphone volume for the phone connected to the FXS port of the gateway.
Microphone	Specify the microphone sensitivity for the phone connected to the FXS port of the gateway.

In the **Codecs Settings** section, you can configure work of voice codecs in use.

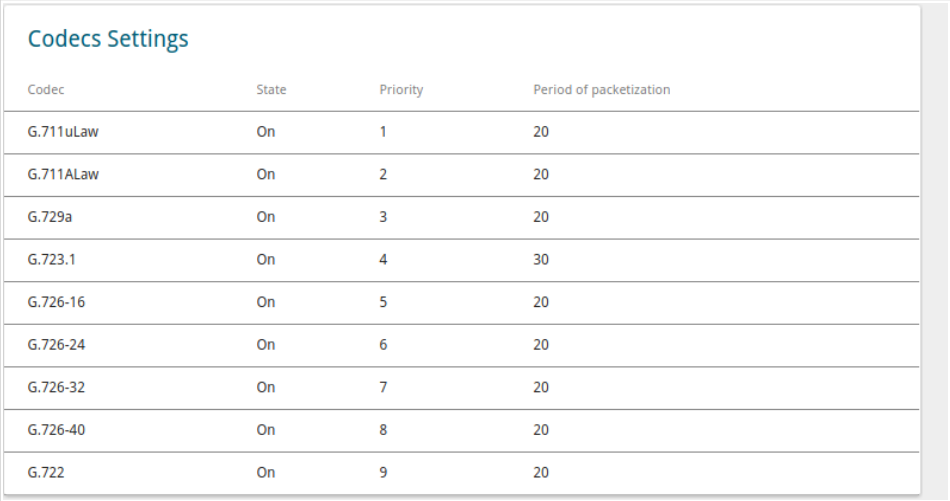

*Figure 128. The **VoIP / Audio Settings** page. The **Codecs Settings** section.*

To change parameters of a codec, left-click the relevant line in the table.

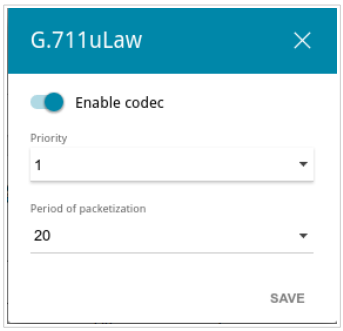

Figure 129. The window for changing the codec parameters.

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

Parameter	Description
Enable codec	To enable the codec, move the switch to the right. To disable the codec, move the switch to the left.
Priority	Priority of the codec upon setting a voice session. Select the needed value from the drop-down list.
Period of packetization	Quantity of milliseconds transmitted in one packet. Select the needed value from the drop-down list.

Click the **SAVE** button.

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

Routing call

On the **VoIP / Routing Call** page, you can fill in the phone book for devices connected to the FXS ports of the gateway. To do this, go to the relevant tab (the **Line 1** or **Line 2**).

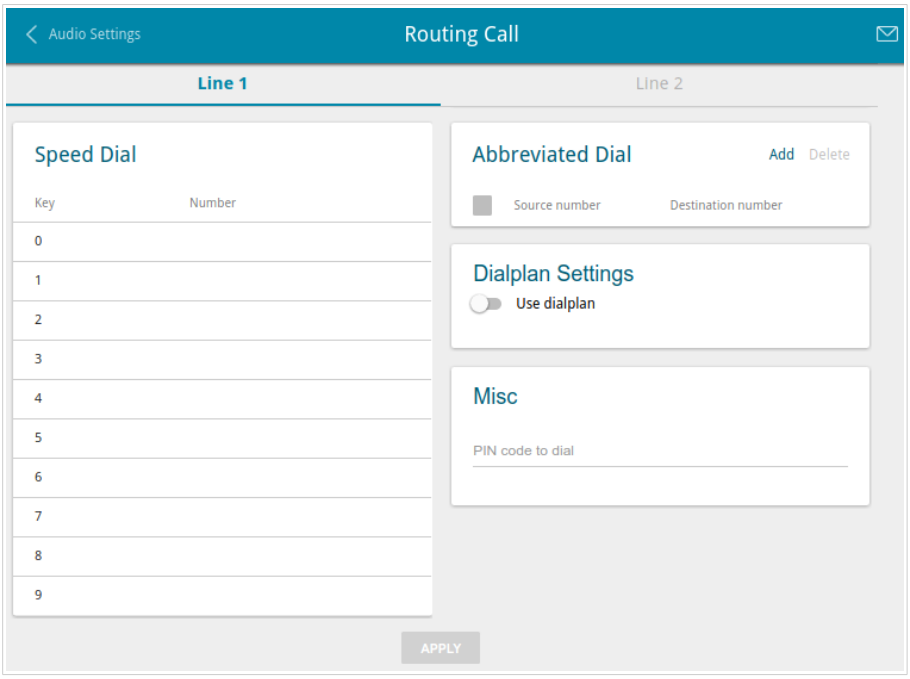

*Figure 130. The **VoIP / Routing call** page. The **Line 1** tab.*

In the **Speed Dial** section, you can assign phone numbers to the digital keys of the phone set connected to this line. To do this, left-click the line corresponding to the key of the phone set. In the opened window, enter the needed number in the **Number** field and click the **SAVE** button. Also you can specify a number in the format **`phone_number@IP_address`** for direct IP calls bypassing the SIP proxy server.

To change or delete the number assigned to the digital key, left-click the line corresponding to the key of the phone set, in the opened window, edit or remove the value of the **Number** field and click the **SAVE** button.

To use a number specified in the **Speed Dial** section, press # (the pound key) on the phone set, then press the relevant digital key.

In the **Abbreviated Dial** section, you can assign short numbers (as a rule, such numbers consist of two or three digits) to frequently used phone numbers. To do this, click the **Add** button. In the opened window, enter a short number in the **Source number** field, then enter the actual phone number in the **Destination number** field. Click the **SAVE** button. Also in the **Destination number** field you can specify a number in the format **`phone_number@IP_address`** for direct IP calls bypassing the SIP proxy server.

To change a short or actual phone number, select of the relevant line in the table. In the opened window, change needed parameters and click the **SAVE** button.

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

To use a number specified in the **Abbreviated Dial** section, dial the needed short number on the phone set.

In the **Dialplan Settings** section, you can configure the dial plan for VoIP. To do this, move the **Use dialplan** switch to the right and in the **Dialplan** field displayed, specify the needed rule. You can specify several rules separated by the character | (vertical bar). You can use digits (0-9), the characters * (asterisk) and # (pound), and the following characters:

Parameter	Description
[]	Digits and/or the characters * and # within square brackets specify a range of values for a certain position in the number.
X	Any digit, the character * or #.
.	Any number of repetitions (including none) of the previous digit or character.
<>	Angle brackets containing digits separated by : (colon) allow to substitute the digit after the colon for the digit before the colon.

In the **Misc** section, fill in the **PIN code to dial** field to allow the user of the phone to make calls only after dialing the PIN code.

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

Call Feature Codes

On the **VoIP / Call Feature Codes** page, you can allow changing some parameters of the gateway directly from the phone sets connected to the FXS ports of the gateway.

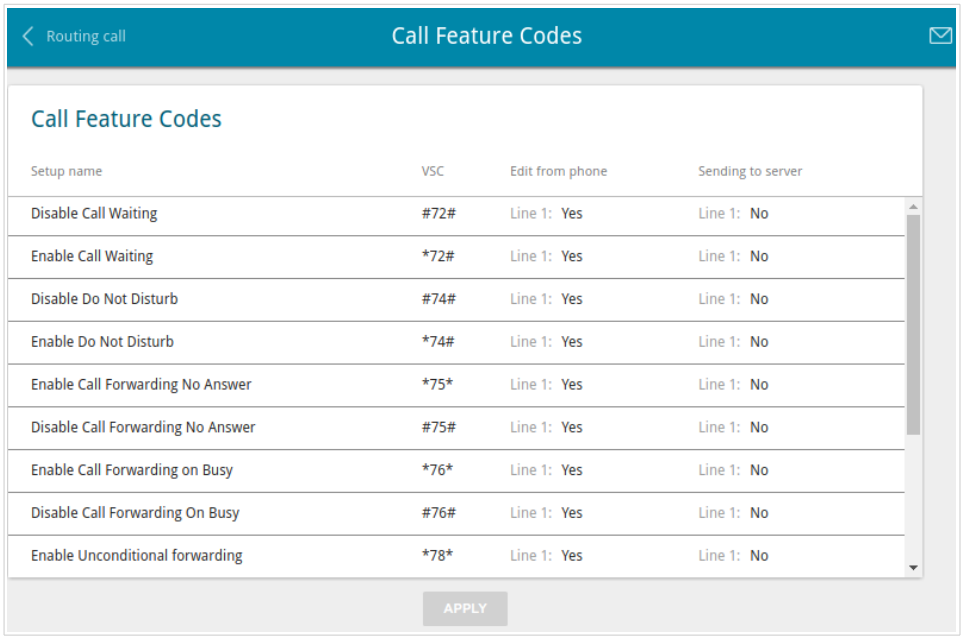

*Figure 131. The **VoIP / Call Feature Codes** page.*

The following call feature codes are available:

Parameter	Description
Disable Call Waiting	Disables the call waiting function.
Enable Call Waiting	Enables the call waiting function.
Disable Do Not Disturb	Disables rejection of incoming calls.
Enable Do Not Disturb	Enables rejection of all incoming calls (the busy tone will be heard).
Enable Call Forwarding No Answer	Enables call forwarding when this line gives no reply.
Disable Call Forwarding No Answer	Disables call forwarding when this line gives no reply.
Enable Call Forwarding On Busy	Enables call forwarding when this line is busy.
Disable Call Forwarding On Busy	Disables call forwarding when this line is busy.
Enable Unconditional forwarding	Enables forwarding for all calls.
Disable Unconditional forwarding	Disables forwarding for all calls.

Parameter	Description
Disable Hot Line	Disables the hotline.
Enable Hot Line	Enables the hotline.
Enable alarm clock	Enables the alarm clock for the time specified for this line.
Disable alarm clock	Disables the alarm clock.

To change parameters of a code, select the relevant line in the table.

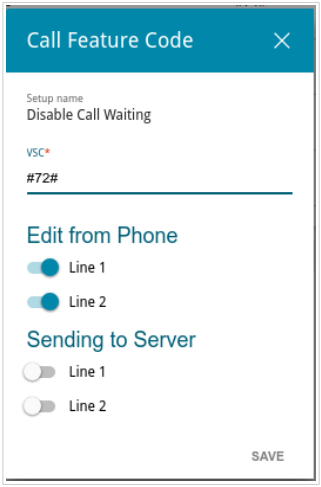

*Figure 132. The **VoIP / Call Feature Codes** page. The window for editing the code parameters.*

In the opened window, specify the needed parameters:

Parameter	Description
VSC	The value of the code. If the code ends with * (the asterisk key), further you can enter a value for the function in use (a number for call forwarding or time for the alarm clock). For example, the code for enabling the alarm clock: ***55*HHMM#**, where **HHMM** is time in 24-hour format.
Edit from Phone	
Line 1 / Line 2	Move the switch of the relevant line to the right to enable the code for the phone connected to the FXS port of the gateway. Move the switch of the relevant line to the left to disable the code for this phone.

Parameter	Description
Sending to server	
Line 1 / Line 2	Move the switch of the relevant line to the right to inform the SIP server when a user dials the code on the phone. Move the switch of the relevant line to the left if the server should not be informed.

Click the **SAVE** button.

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

Call Logging

On the **VoIP / Call Logging** page, you can configure the call log parameters, sending the log and conversation records to a USB storage connected to the gateway and view information on all calls.

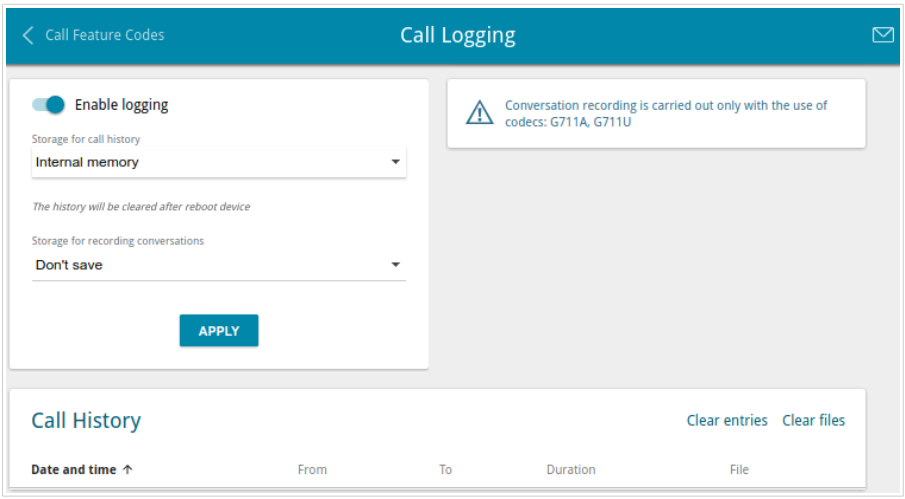

*Figure 133. The **VoIP / Call Logging** page.*

To enable logging of calls, move the **Enable logging** switch to the right. Then specify the needed parameters.

Parameter	Description
Storage for call history	Select a location for the call log from the drop-down list. • **USB storage**: the call log is stored in the memory of the USB storage connected to the gateway. • **Internal memory**: the call log is stored in the gateway's RAM.
Storage for recording conversations	Select the **USB storage** value to store conversation records in the memory of the USB storage connected to the gateway or leave the **Don't save** value if conversation records needn't be stored.

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

In the **Call History** section, the detailed information on all calls are displayed: date and time, call duration, and a caller or called party number.

To sort the log records, in the **Call History** section, left-click the name of a column and click the **Sort** icon (↑ (ascending), ↓ (descending)) displayed.

To remove the call log, click the **Clear entries** button. The call log is also removed when the device is rebooted or powered off.

To remove conversation records saved on the USB storage, click the **Clear files** button.

Security

On the **VoIP / Security** page, you can configure filtering rules for incoming calls of the phones connected to the FXS ports of the gateway.

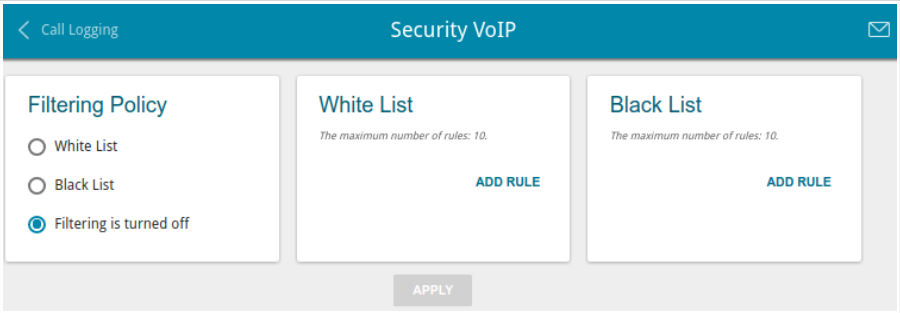

*Figure 134. The **VoIP / Security** page.*

In the **Filtering Policy** section, select the needed choice of the radio button.

- **White List**: the gateway accepts incoming calls (INVITE packets) only from IP addresses or domains specified in the **White List** section;
- **Black List**: the gateway accepts incoming calls (INVITE packets) from any IP addresses or domains except for those specified in the **Black List** section;
- **Filtering is turned off**: filtering by IP addresses or domain names is not performed.

To add an IP address or domain name, click the **ADD RULE** button in the **White List** or **Black List** section correspondingly. In the line displayed, specify the needed value.

To remove an IP address or domain name from the white or black list, click the **Delete** icon (×) in the relevant line.

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

Alarm Clock

On the **VoIP / Alarm Clock** page, you can configure the phones connected to the FXS ports of the gateway as alarm clocks.

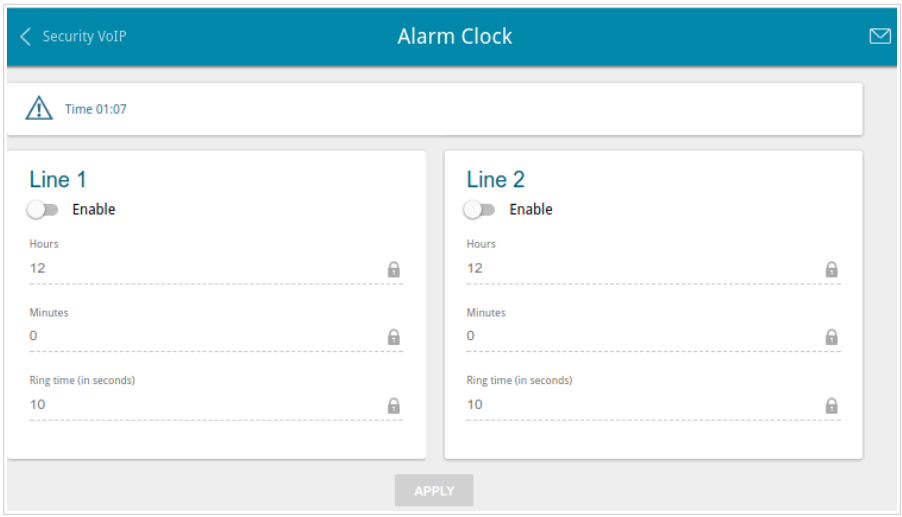

*Figure 135. The **VoIP / Alarm Clock** page.*

In the **Line 1** and/or **Line 2** section, move the **Enable** switch to the right. Then specify the time at which the phone should ring in the **Hours** and **Minutes** fields. In the **Ring time** field, specify the signal duration. Then click the **APPLY** button.

! When the gateway 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.

Firewall

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

- 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 136. The **Firewall / IP Filter** page.*

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

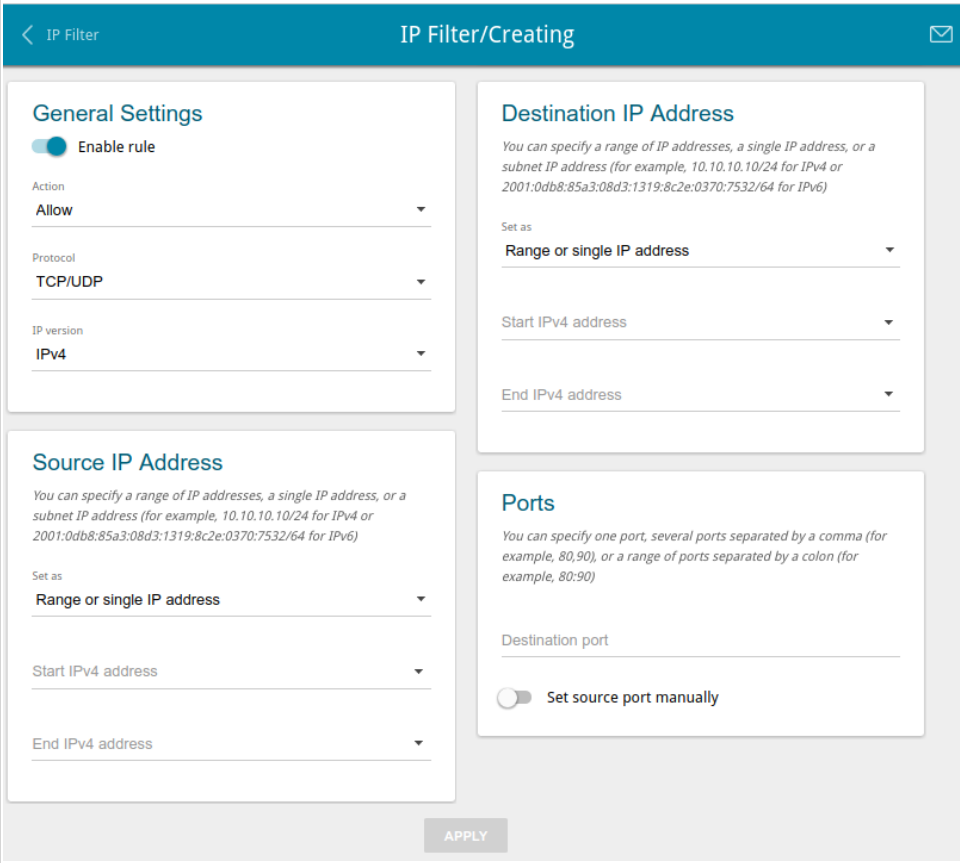

Figure 137. The page for adding a rule for IP filtering.

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.
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.

Parameter	Description
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 gateway'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 gateway'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.

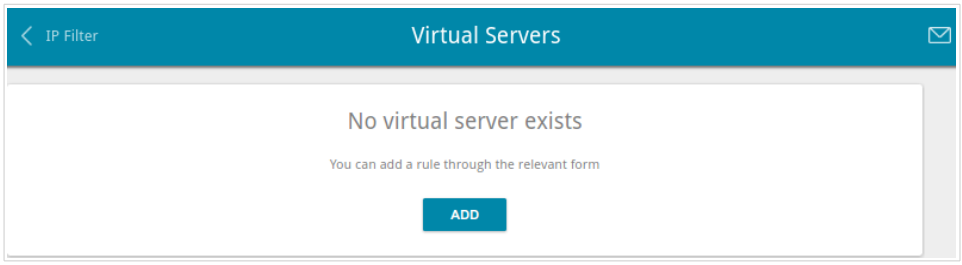

*Figure 138. The **Firewall / Virtual Servers** page.*

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

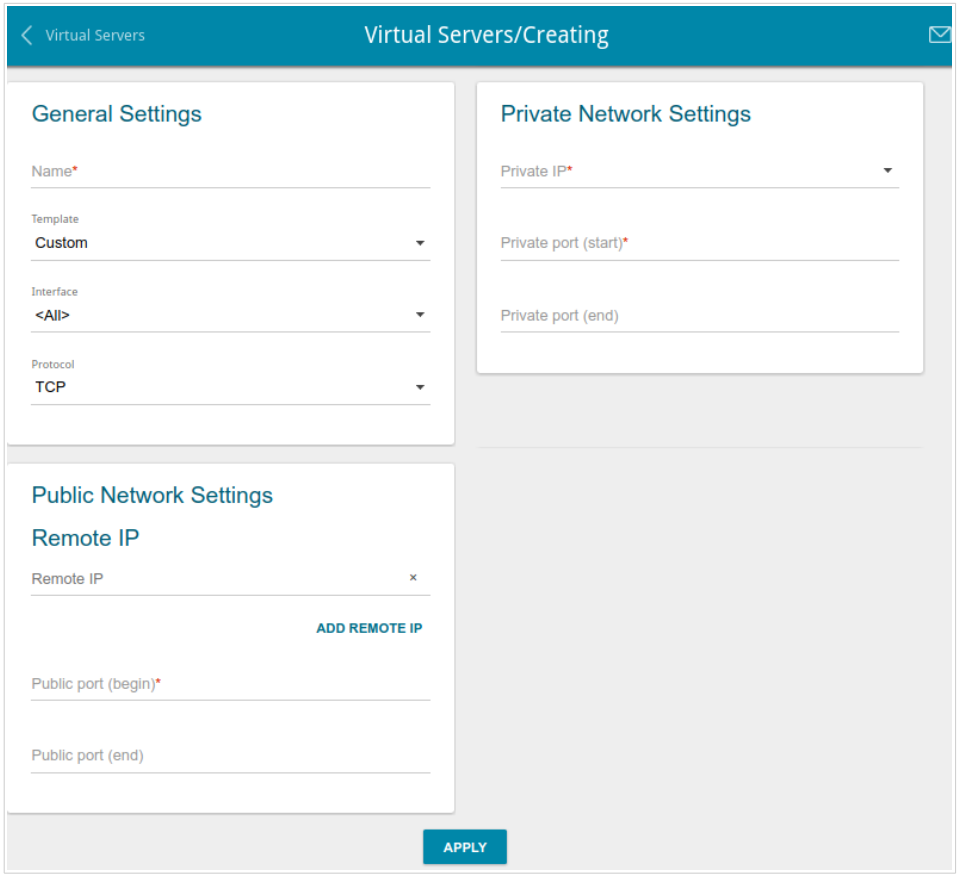

Figure 139. The page for adding a virtual server.

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.
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 gateway 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 gateway'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 gateway, the DMZ implements the capability to transfer a request coming to a port of the gateway 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.

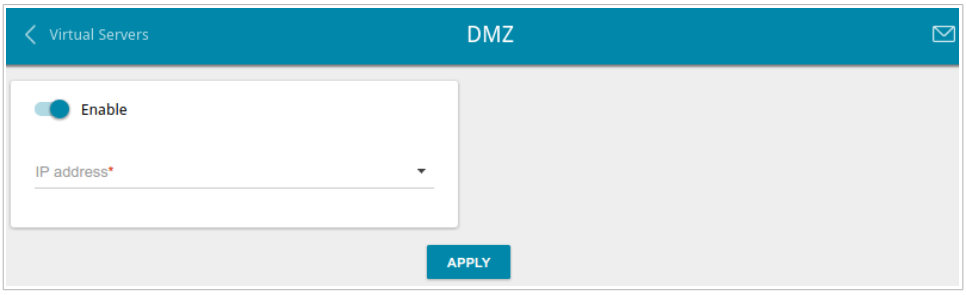

*Figure 140. The **Firewall / DMZ** page.*

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 gateway's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).

Click the **APPLY** button.

Note that when the DMZ is enabled, all traffic coming to a port of the WAN interface of the gateway 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 gateway's local network, then entering `http://gateway_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 gateway's LAN.*

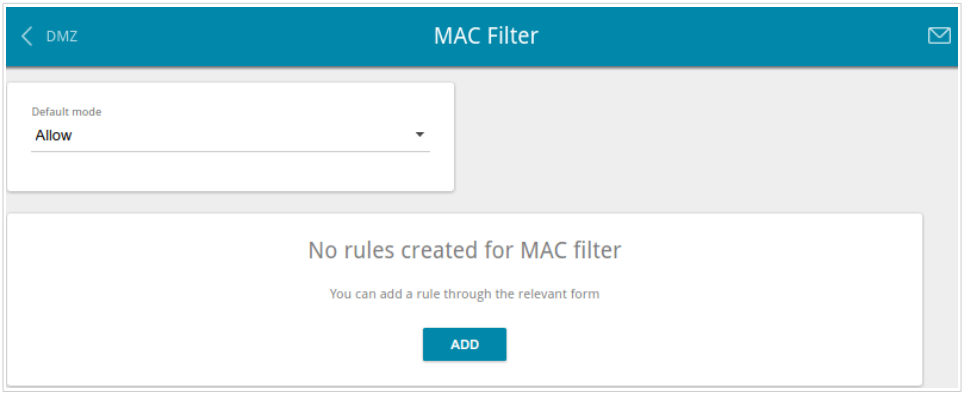

*Figure 141. The **Firewall / MAC Filter** page.*

Select the needed action from the drop-down list in the **Default mode** section to configure filtering for all devices of the gateway's network:

- **Allow**: Allows access to the gateway's network and to the Internet for devices (the value is specified by default);
- **Deny**: Blocks access to the gateway's network for devices.

! You can use the **Deny** mode only if an active rule which allows access to the device's network is created on the page.

To create a rule (specify a MAC address of a device for which the specified filtering mode will be applied), click the **ADD** button.

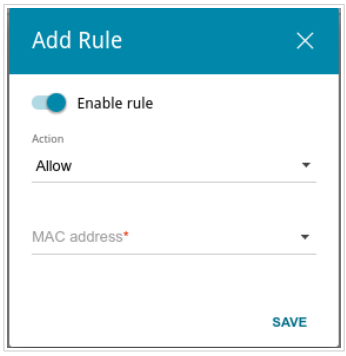

Figure 142. The window for adding a rule for the MAC filter.

* For correct operation of MAC filter you may need to update the gateway's firmware.

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

Parameter	Description
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. **Deny**: Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices. **Allow**: Allows access to the gateway's network and to the Internet for the device with the specified MAC address even if the default mode denies access for all devices.
MAC address	The MAC address of a device from the gateway's LAN. You can enter the MAC address of a device connected to the gateway'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.

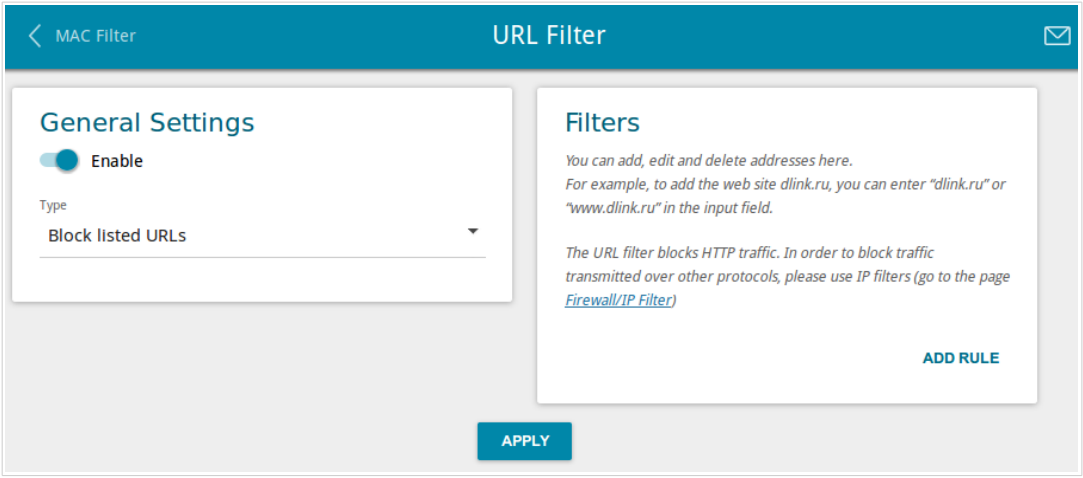

*Figure 143. The **Firewall / URL Filter** page.*

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 gateway blocks access to all addresses specified in the **Filters** section;
- **Block all URLs except listed**: when this value is selected, the gateway 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 gateway's settings
- restore the factory default settings
- create a backup of the gateway's configuration
- restore the gateway's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the gateway
- change the web-based interface language
- update the firmware of the gateway
- 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 gateway
- trace the route to a host
- allow or forbid access to the gateway via TELNET
- configure automatic synchronization of the system time or manually configure the date and time for the gateway.

Configuration

On the **System / Configuration** page, you can change the password for the administrator account used to access the web-based interface of the gateway and to access the device settings via TELNET, restore the factory defaults, backup the current configuration, restore the gateway'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.

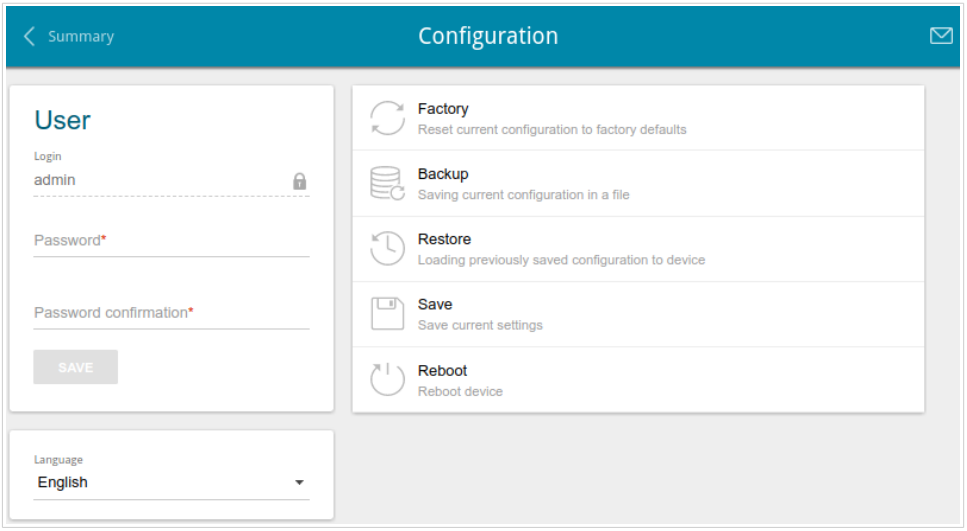

*Figure 144. The **System / Configuration** page.*

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.[17] 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 gateway only after restoring the factory default settings via the hardware **RESET** button. This procedure wipes out all settings that you have configured for your gateway.

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

17 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 15).
Backup	Click the button to save the configuration (all settings of the gateway) 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 gateway) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The gateway saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

Firmware Update

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

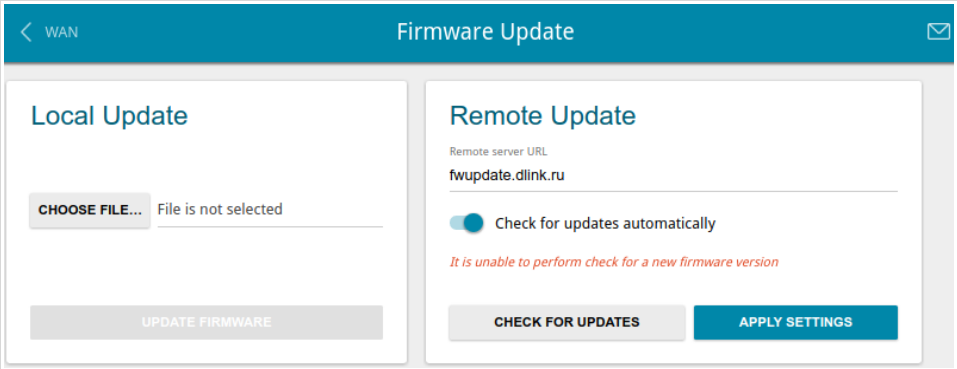

*Figure 145. The **System / Firmware Update** page.*

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

By default, the automatic check for the gateway'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 gateway locally (from the hard drive of your PC) or remotely (from the update server).

Local Update

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

To update the firmware of the gateway 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 gateway 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 gateway 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 gateway is rebooted.

Remote Update

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

To update the firmware of the gateway 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 gateway 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 gateway 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 gateway 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.

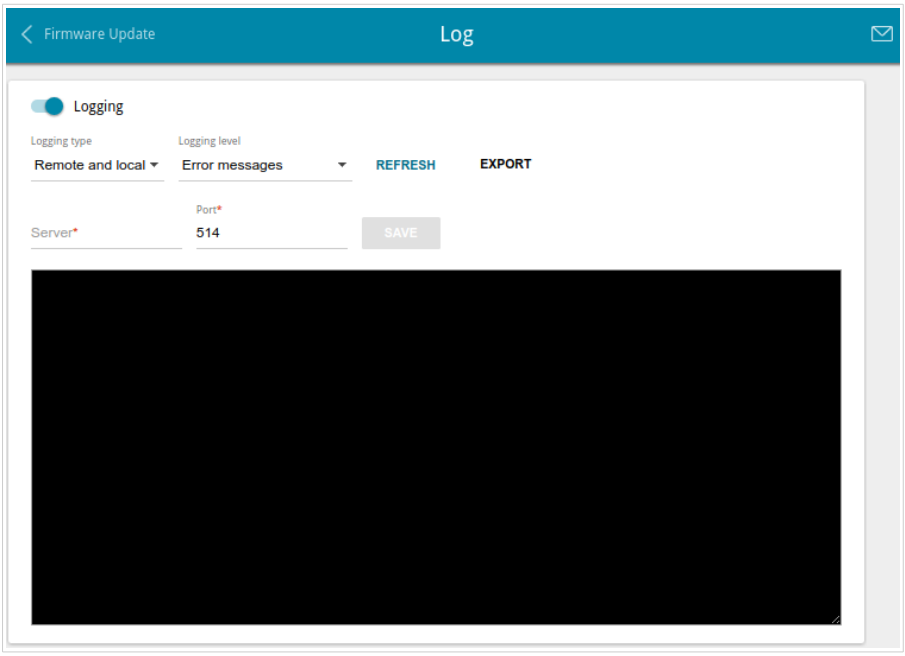

*Figure 146. The **System / Log** page.*

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 gateway's memory. When this value is selected, the **Server** and **Port** fields are not displayed. • **Remote**: the system log is sent to the remote host specified in the **Server** field. • **Remote and local**: the system log is stored in the gateway'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.
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.

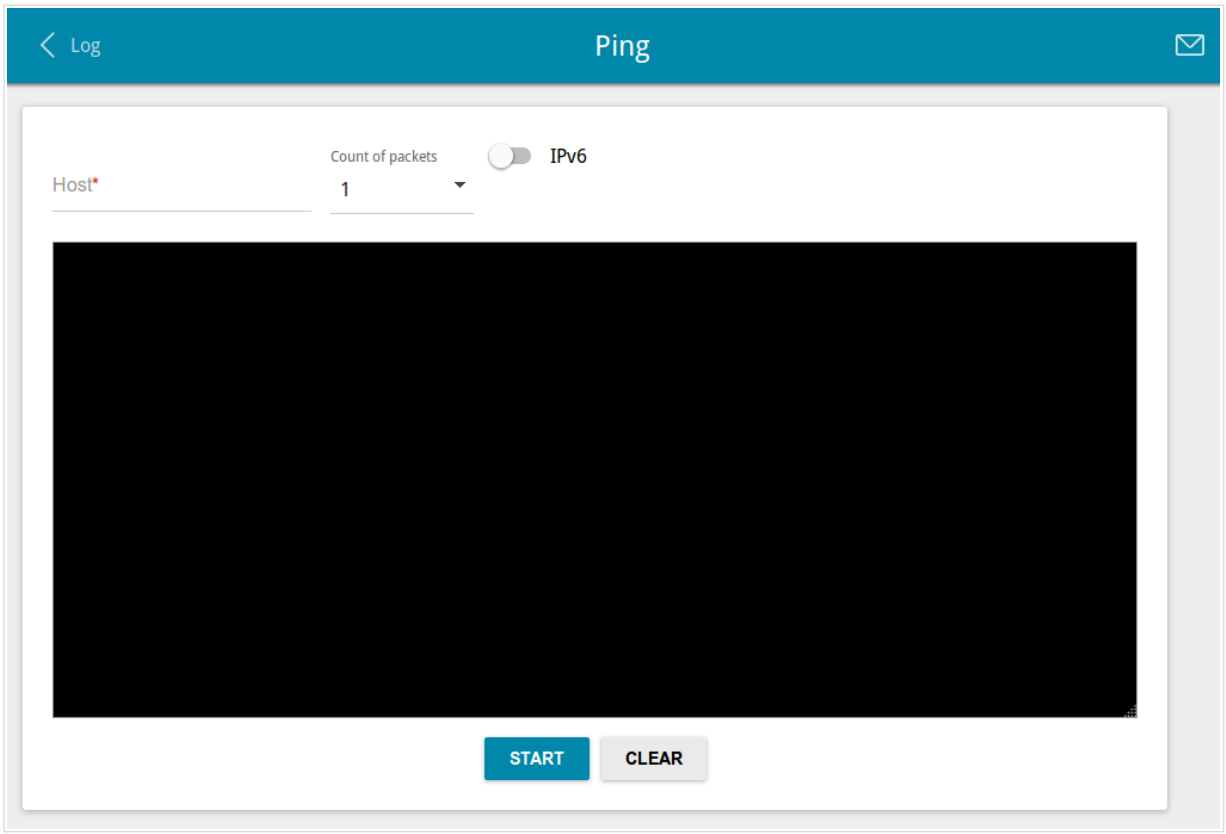

*Figure 147. The **System / Ping** page.*

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.

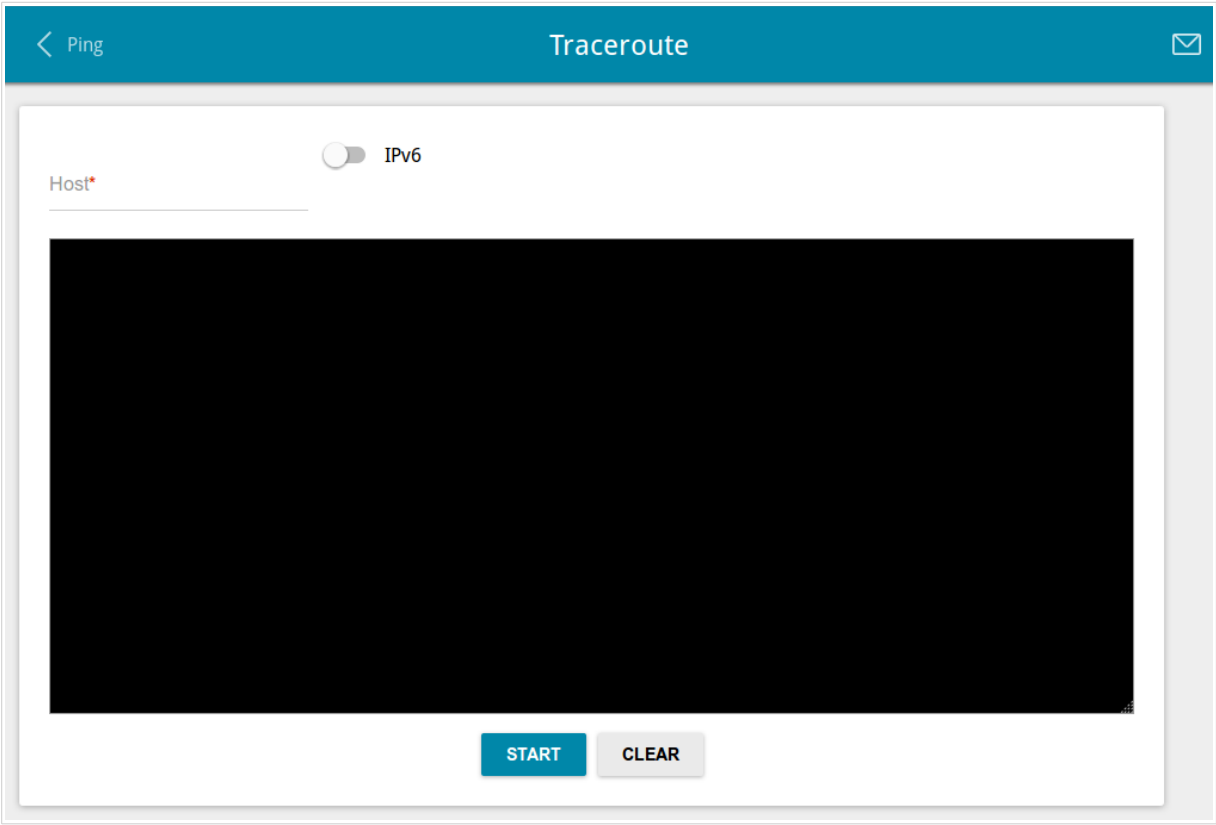

*Figure 148. The **System / Traceroute** page.*

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.

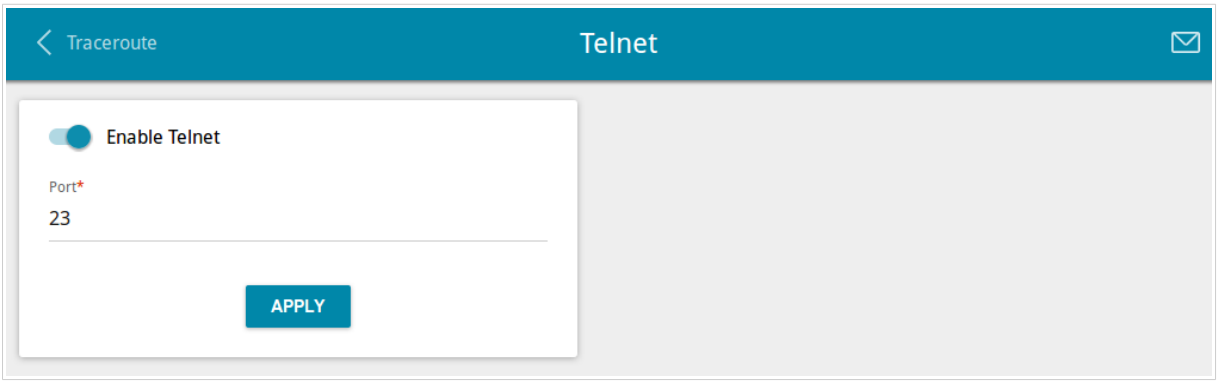

*Figure 149. The **System / Telnet** page.*

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 gateway'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 gateway or configure automatic synchronization of the system time with a time server on the Internet.

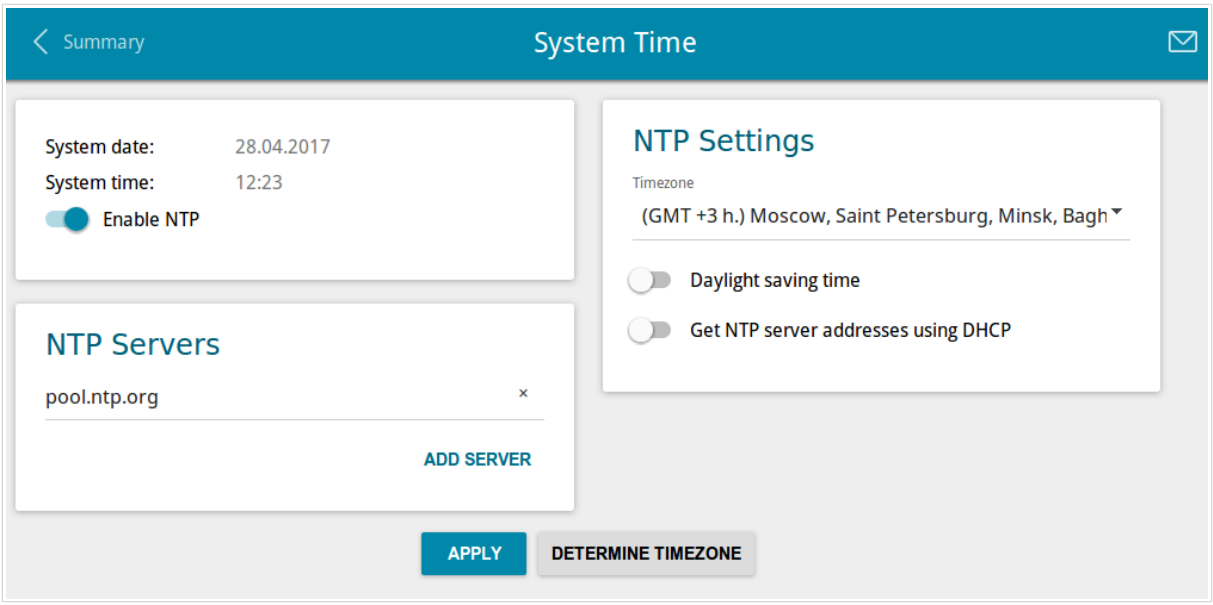

*Figure 150. The **System / System Time** page.*

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 gateway, move the **Daylight saving time** switch to the right in the **NTP Settings** section and click the **APPLY** button.

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

When the gateway 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.

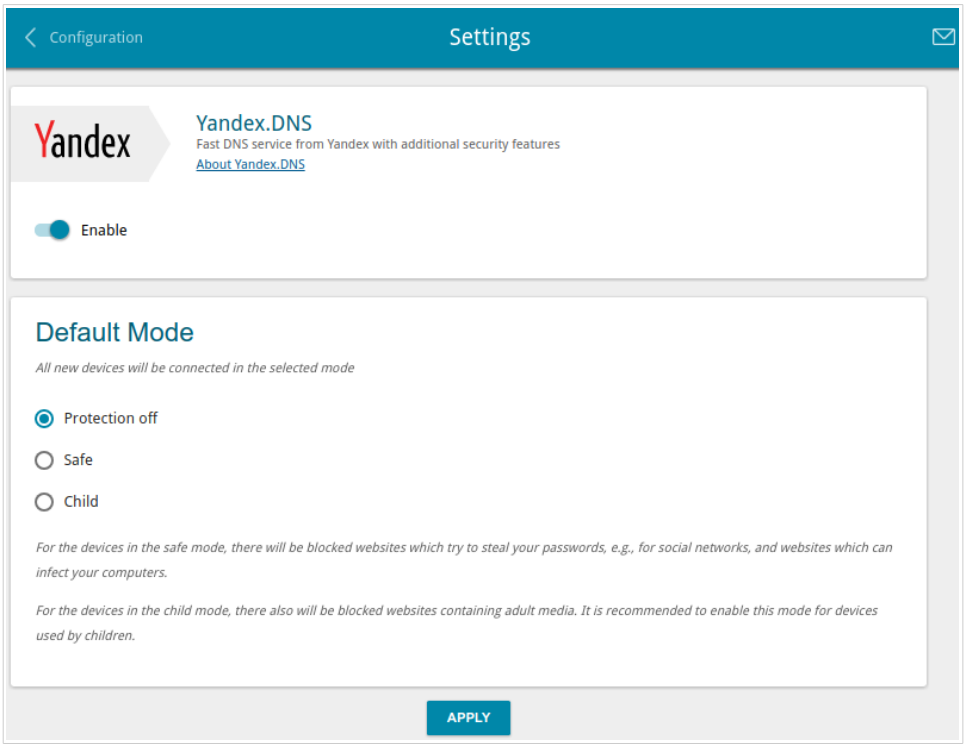

*Figure 151. The **Yandex.DNS / Settings** page.*

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 gateway'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 gateway'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.

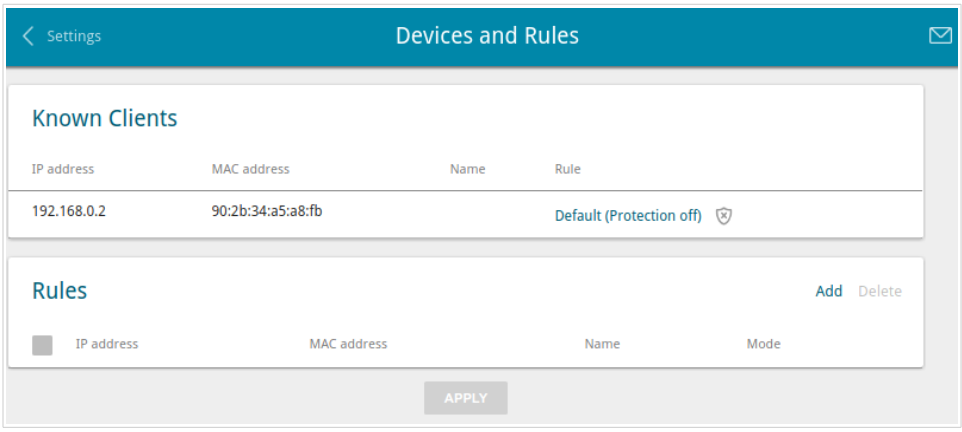

*Figure 152. The **Yandex.DNS / Devices and Rules** page.*

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

To create[18] 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.

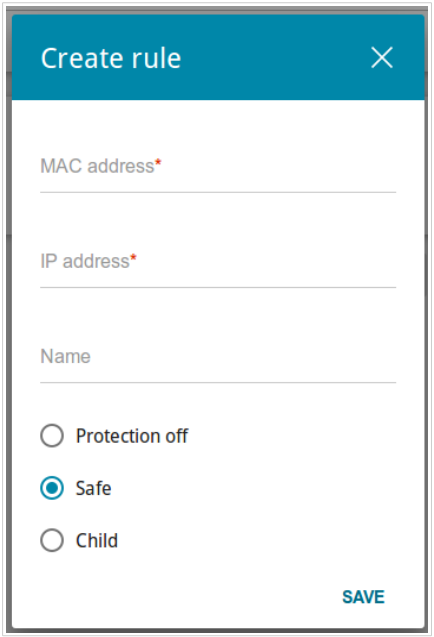

Figure 153. Adding a new rule for the Yandex.DNS service.

18 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 gateway's LAN.
IP address	The IP address of a device from the gateway'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 DPN-144DG 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 DPN-144DG 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 gateway, 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 gateway away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone in not in use.

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

3G	Third Generation
AC	Access Category
AES	Advanced Encryption Standard
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
GSM	Global System for Mobile Communications
IGD	Internet Gateway Device
IGMP	Internet Group Management Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LTE	Long Term Evolution
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
PUK	PIN Unlock 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
SIM	Subscriber Identification Module
SIP	Session Initiation Protocol
SMB	Server Message Block
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
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