



DAP-600P

Wireless AC2600 Wave 2 MU-MIMO Dual Band PoE Access Point / Router

Contents

Chapter 1. Introduction.....	5
Contents and Audience.....	5
Conventions.....	5
Document Structure.....	5
Chapter 2. Overview.....	6
General Information.....	6
Specifications.....	8
Product Appearance.....	13
Upper Panel.....	13
Back Panel.....	14
Delivery Package.....	16
Chapter 3. Installation and Connection.....	17
Before You Begin.....	17
Connecting to Mobile Device with D-Link Assistant Application.....	18
Connecting to PC.....	22
PC with Ethernet Adapter.....	22
Configuring IP Address in OS Windows 7.....	23
Configuring IP Address in OS Windows 10.....	28
PC with Wi-Fi Adapter.....	33
Configuring Wi-Fi Adapter in OS Windows 7.....	34
Configuring Wi-Fi Adapter in OS Windows 10.....	37
Connecting to Web-based Interface.....	40
Web-based Interface Structure.....	42
Summary Page.....	42
Home Page.....	44
Menu Sections.....	45
Notifications.....	46
Chapter 4. Configuring via Web-based Interface.....	47
Initial Configuration Wizard.....	47
Selecting Operation Mode.....	49
Router.....	49
Access Point or Repeater.....	51
Mesh Network Main Device (Master).....	53
Mesh Network Subordinate Device (Slave).....	55
Changing LAN IPv4 Address.....	56
Wi-Fi Client.....	57
Configuring WAN Connection.....	59
Static IPv4 Connection.....	60
Static IPv6 Connection.....	61
PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections.....	62
PPPoE + Static IP (PPPoE Dual Access) Connection.....	63
PPTP + Dynamic IP or L2TP + Dynamic IP Connection.....	64
PPTP + Static IP or L2TP + Static IP Connection.....	65
Configuring Wireless Network.....	66
Changing Web-based Interface Password.....	68
Connection of Multimedia Devices.....	70

Statistics	73
Network Statistics.....	73
DHCP.....	74
Clients and Session.....	75
Port Statistics.....	76
Multicast Groups.....	77
Routing Table.....	78
Connections Setup	79
LAN.....	79
IPv4.....	79
IPv6.....	85
WAN.....	89
<i>Creating Dynamic IPv4 or Static IPv4 WAN Connection</i>	91
<i>Creating Dynamic IPv6 or Static IPv6 WAN Connection</i>	95
<i>Creating PPPoE WAN Connection</i>	99
<i>Creating PPTP, L2TP, or L2TP over IPsec WAN Connection</i>	104
<i>Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection</i>	109
WAN Reservation.....	115
Wi-Fi	117
Basic Settings.....	117
Client Management.....	127
WPS.....	128
<i>Using WPS Function via Web-based Interface</i>	130
WMM.....	131
Client.....	134
Additional.....	137
MAC Filter.....	141
Super Mesh.....	144
Roaming.....	149
Advanced	151
DNS.....	152
Ports Settings.....	154
MAC Filter.....	157
VLAN.....	159
SNMP.....	162
DDNS.....	166
Redirect.....	168
Routing.....	169
TR-069 Client.....	171
Remote Access.....	173
UPnP IGD.....	175
UDPXY.....	176
IGMP.....	178
ALG/Passthrough.....	179
IPsec.....	181
Firewall	189
IP Filter.....	189
Virtual Servers.....	194
DMZ.....	197
URL Filter.....	198

System	201
Configuration.....	202
Firmware Update.....	204
<i>Local Update</i>	205
<i>Remote Update</i>	206
Schedule.....	207
Log.....	211
Ping.....	213
Traceroute.....	215
Telnet/SSH.....	217
System Time.....	218
Auto Provision.....	220
Yandex.DNS	222
Settings.....	222
Devices and Rules.....	224
SkyDNS	226
Settings.....	227
Devices.....	228
Chapter 5. Operation Guidelines	230
Safety Rules and Conditions	230
Wireless Installation Considerations	231
Chapter 6. Abbreviations and Acronyms	232

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the access point DAP-600P and explains how to configure and operate it.

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

Conventions

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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the access point DAP-600P and configure a PC in order to access its web-based interface.

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

Chapter 5 includes safety instructions and tips for networking.

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

CHAPTER 2. OVERVIEW

General Information

The DAP-600P device is a wireless dual band access point supporting the router mode. It is an affordable solution for creating wireless networks at home or in an office.

Using the DAP-600P 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 it 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 access point can operate as a base station for connecting wireless devices of the standards 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac.

DAP-600P delivers reliable, high-speed wireless performance up to 1733Mbps for 5GHz using the enhanced 802.11ac Wave 2 standard and up to 800Mbps for 2.4GHz.

The device supports multiple functions for the wireless interface: several security standards (WEP, WPA/WPA2), MAC address filtering, different operation modes (access point, router, client), WPS, WMM.

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

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

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

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

Support of guest Wi-Fi network in the router mode 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 access point's LAN.

The access point is equipped with a WAN port with Power over Ethernet (PoE) support which allows to use one Ethernet cable for data and power transfer. In the access point mode, the port with PoE support is used as a LAN port.

In the access point mode, you are able to use DAP-600P to create a wireless network or to connect to a wired router. In the router mode, you are able to connect DAP-600P to a cable or DSL modem or to a private Ethernet line and use a high-speed Internet connection to successfully fulfill a wide range of professional tasks.

The “client” function is available in both modes and allows using DAP-600P as a wireless client and a wireless repeater in the access point mode and as a WISP repeater in the router mode.

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

Now the schedules are also implemented; they can be applied to the rules of various filters and used to reboot the access point at the specified time or every specified time period and to enable/disable the wireless network.

You can configure the settings of the DAP-600P device via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

The configuration wizard allows you to connect DAP-600P to a wired or wireless ISP (when switched to the router mode) in several simple steps or quickly set needed parameters for operation as an access point, repeater, or client (when switched to the access point mode).

You can simply update the firmware: when the Internet access is provided, the access point itself finds approved firmware on D-Link update server and notifies when ready to install it.

Specifications*

Hardware	
Processor	<ul style="list-style-type: none">· MT7621AT (880MHz, dual core)
RAM	<ul style="list-style-type: none">· 128MB, DDR3 SDRAM
Flash	<ul style="list-style-type: none">· 16MB, SPI
Interfaces	<ul style="list-style-type: none">· 10/100/1000BASE-T WAN port with PoE support· 10/100/1000BASE-T LAN port
LEDs	<ul style="list-style-type: none">· POWER / WLAN· INTERNET· LAN
Buttons	<ul style="list-style-type: none">· RESET button to restore factory default settings
Antenna	<ul style="list-style-type: none">· Four internal dual band antennas (3dBi gain)
MIMO	<ul style="list-style-type: none">· 4 x 4, MU-MIMO
Power connector	<ul style="list-style-type: none">· Power input connector (DC)

Software	
Operation Modes	<ul style="list-style-type: none">· Access point· Router
WAN connection types	<ul style="list-style-type: none">· PPPoE· IPv6 PPPoE· PPPoE Dual Stack· Static IPv4 / Dynamic IPv4· Static IPv6 / Dynamic IPv6· PPPoE + Static IP (PPPoE Dual Access)· PPPoE + Dynamic IP (PPPoE Dual Access)· PPTP/L2TP + Static IP· PPTP/L2TP + Dynamic IP

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

Software	
Network functions	<ul style="list-style-type: none"> · DHCP server/relay · Advanced configuration of built-in DHCP server · Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation · Automatic obtainment of LAN IP address (for access point/repeater/client modes) · DNS relay · Dynamic DNS · Static IPv4/IPv6 routing · IGMP Proxy · RIP · Support of UPnP IGD · Support of VLAN · WAN ping respond · Support of SIP ALG · Support of RTSP · WAN failover · Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port · Built-in UDPXY application
Firewall functions	<ul style="list-style-type: none"> · Network Address Translation (NAT) · Stateful Packet Inspection (SPI) · IPv4/IPv6 filter · MAC filter · URL filter · DMZ · Virtual servers · Built-in Yandex.DNS web content filtering service · Built-in SkyDNS web content filtering service
VPN	<ul style="list-style-type: none"> · IPsec/PPTP/L2TP/PPPoE pass-through · PPTP/L2TP tunnels · IPsec tunnels · Transport/Tunnel mode · IKEv1/IKEv2 support · DES encryption · NAT Traversal · Support of DPD (Keep-alive for VPN tunnels)
Management and monitoring	<ul style="list-style-type: none"> · Local and remote access to settings through SSH/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 logging to remote host · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility · TR-069 client · SNMP agent (SNMPv2/v3) · Schedules for filters rules, automatic reboot, and enabling/disabling wireless network · Automatic upload of configuration file from ISP's server (Auto Provision)

Wireless Module Parameters	
Standards	<ul style="list-style-type: none"> · IEEE 802.11a/n/ac · IEEE 802.11b/g/n
Frequency range <i>The frequency range depends upon the radio frequency regulations applied in your country</i>	<ul style="list-style-type: none"> · 2400 ~ 2483.5MHz · 5150 ~ 5350MHz · 5650 ~ 5850MHz
Wireless connection security	<ul style="list-style-type: none"> · WEP · WPA/WPA2 (Personal/Enterprise) · MAC filter · WPS (PBC/PIN)
Advanced functions	<ul style="list-style-type: none"> · Super Mesh function · "Client" function (access point mode) Wireless network client Wireless network repeater · "Client" function (router mode) WISP repeater · 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 · Support of 802.11ac (5GHz) and 802.11n (2.4GHz) TX Beamforming · Wider bandwidth (up to 160MHz) · Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence) · Support of STBC
Wireless connection rate¹	<ul style="list-style-type: none"> · IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11b: 1, 2, 5.5, and 11Mbps · IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11n (2.4GHz): 6.5–600Mbps (MCS0–MCS30) to 800Mbps (QAM256) · IEEE 802.11n (5GHz): from 6.5 to 600Mbps (from MCS0 to MCS30) · IEEE 802.11ac (5GHz): from 6.5 to 1733Mbps (from MCS0 to MSC9)

¹ Maximum wireless signal rate is derived from IEEE standard 802.11ac and 802.11n specifications. In order to get the rate of 800Mbps in the 2.4GHz band, a Wi-Fi client should support MIMO 4x4 and QAM256 modulation scheme. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Wireless Module Parameters	
<p>Transmitter output power</p> <p><i>The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country</i></p>	<ul style="list-style-type: none"> · 802.11a (typical at room temperature 25 °C) 17dBm at 6, 54Mbps · 802.11b (typical at room temperature 25 °C) 17dBm at 1, 11Mbps · 802.11g (typical at room temperature 25 °C) 17dBm at 6, 54Mbps · 802.11n (typical at room temperature 25 °C) 17dBm at MCS0~6 16dBm at MCS7 · 802.11ac (typical at room temperature 25 °C) 17dBm at MCS0~6 16dBm at MCS7 15dBm at MCS8~9
<p>Receiver sensitivity</p>	<ul style="list-style-type: none"> · 802.11a (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -82dBm at 6Mbps -81dBm at 9Mbps -79dBm at 12Mbps -77dBm at 18Mbps -74dBm at 24Mbps -70dBm at 36Mbps -66dBm at 48Mbps -65dBm at 54Mbps · 802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C) -90dBm at 1Mbps -90dBm at 2Mbps -88dBm at 5.5Mbps -86dBm at 11Mbps · 802.11g (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -82dBm at 6Mbps -81dBm at 9Mbps -79dBm at 12Mbps -77dBm at 18Mbps -74dBm at 24Mbps -70dBm at 36Mbps -66dBm at 48Mbps -65dBm at 54Mbps · 802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) HT20 -82dBm at MCS0 -79dBm at MCS1 -77dBm at MCS2 -74dBm at MCS3 -70dBm at MCS4 -66dBm at MCS5 -65dBm at MCS6 -64dBm at MCS7 HT40 -79dBm at MCS0 -76dBm at MCS1 -74dBm at MCS2 -71dBm at MCS3 -67dBm at MCS4 -63dBm at MCS5

Wireless Module Parameters

	<ul style="list-style-type: none">-62dBm at MCS6-61dBm at MCS7
Modulation schemes	<ul style="list-style-type: none">· 802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM· 802.11b: DQPSK, DBPSK, DSSS, CCK· 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM· 802.11n: BPSK, QPSK, 16QAM, 64QAM, 256QAM with OFDM· 802.11ac: BPSK, QPSK, 16QAM, 64QAM, up to 256QAM with OFDM

Physical Parameters

Dimensions	<ul style="list-style-type: none">· 213 x 213 x 38 mm (8 x 8 x 1.5 in)
-------------------	--

Operating Environment

Power	<ul style="list-style-type: none">· 48V, 0.5A or 802.3at PoE· External DC power adapter 12V/1.5A (not included in the delivery package)
Temperature	<ul style="list-style-type: none">· Operating: from 0 to 40 °C· Storage: from -20 to 65 °C
Humidity	<ul style="list-style-type: none">· Operating: from 10% to 90% (non-condensing)· Storage: from 5% to 95% (non-condensing)

Product Appearance

Upper Panel



Figure 1. Upper panel view.

LED	Mode	Description
POWER / WLAN	<i>Solid red</i>	The device is being loaded or the WLAN of both bands is off.
	<i>Slow blinking red</i>	The firmware is being updated.
	<i>Solid blue</i>	The device's WLAN of one or both bands is on.
	<i>Blinking blue</i>	Attempting to add a wireless device via the WPS function.
	<i>No light</i>	The device is powered off.

Back Panel

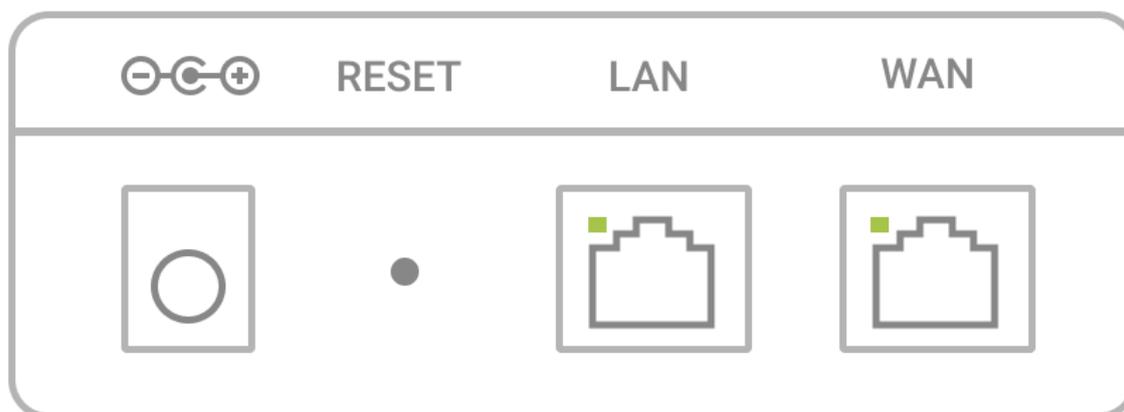


Figure 2. Back panel view.

Port	Description	
RESET	A button to restore the factory defaults. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.	
LAN	An Ethernet port to connect a computer or network device. A LAN LED corresponds to the port. The operating modes:	
	<i>Solid green</i>	A device (computer) is connected to the port, the connection is on.
	<i>Blinking green</i>	Data transfer through the LAN port.
WAN (PoE)	A port with PoE support to connect to a switch, a private Ethernet line, or a cable or DSL modem. In the access point mode, it is used as the LAN port. An INTERNET LED corresponds to the port. The operating modes:	
	<i>Solid green</i>	The cable is connected to the port.
	<i>Blinking green</i>	Data transfer through the WAN port.
	<i>No light</i>	The cable is not connected.

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

The device is equipped with four internal dual band Wi-Fi antennas.

Delivery Package

The following should be included:

- Access point DAP-600P
- Wall mounting bracket with mounting kit
- “***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 different parameters than those indicated on the device will cause damage and void the warranty for this product.

CHAPTER 3. INSTALLATION AND CONNECTION

Before You Begin

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

Computer or Mobile Device

Configuration of the access point DAP-600P supporting the router mode (hereinafter referred to as “the access point”) is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

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

PC Web Browser

The following PC 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 access point 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 access point.

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 access point for all these wireless workstations.

Connecting to Mobile Device with D-Link Assistant Application

1. Connect the power adapter (not included in the delivery package) to the power connector port on the back panel of the access point, then plug the power adapter into an electrical outlet or power strip.
2. Make sure that the Wi-Fi connection on your mobile device is on. To switch it on, go to the mobile device settings.
3. In the list of available wireless networks on your mobile device, select the wireless network **DAP-600P** (for operating in the 2.4GHz band) or **DAP-600P-5G** (for operating in the 5GHz band).
4. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) as the password and connect to the wireless network of DAP-600P.
5. In the settings of the wireless network **DAP-600P** (for operating in the 2.4GHz band) or **DAP-600P-5G** (for operating in the 5GHz band) on your mobile device, in the **IP Settings** field, select the **Static** value (for Android) or the **Manual** value (for iOS).²
6. Enter the value **192.168.0.51** in the **IP address** field. For iOS devices, also specify the subnet mask **255.255.255.0**. Confirm the changed settings.
7. Launch D-Link Assistant application on your mobile device. The application is available for Android and iPhone smartphones in AppStore and Google Play.



D-Link Assistant for Android



D-Link Assistant for iOS

² Field names may vary in different versions of operating systems on mobile devices.

8. In the application menu, in the **Connection method** section select the **Connection by IP address** value.

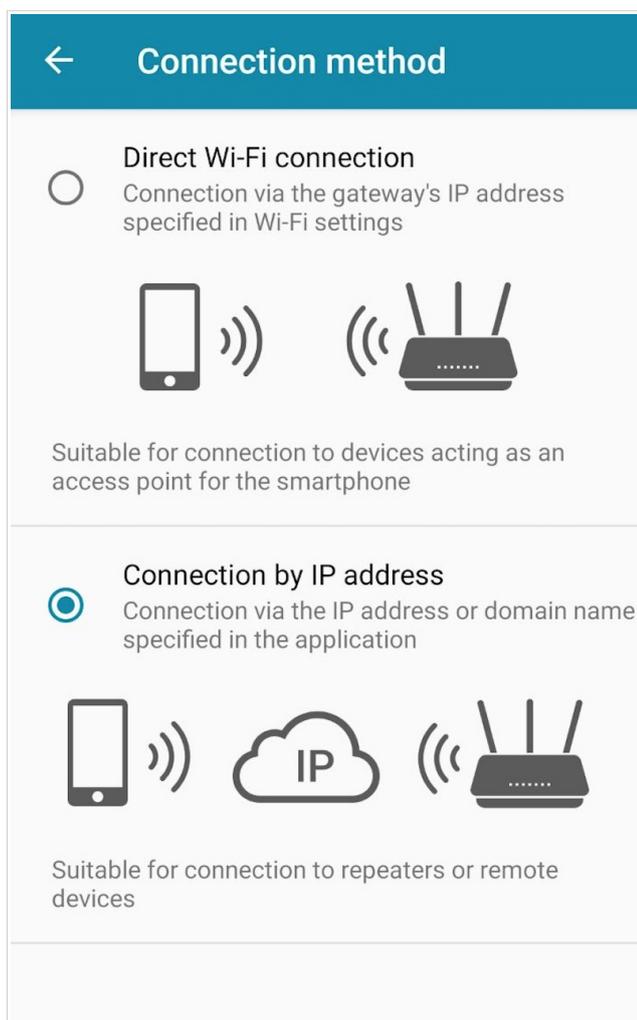


Figure 3. The **Connection method** section.

9. On the application main page click the **CHANGE ADDRESS** button.

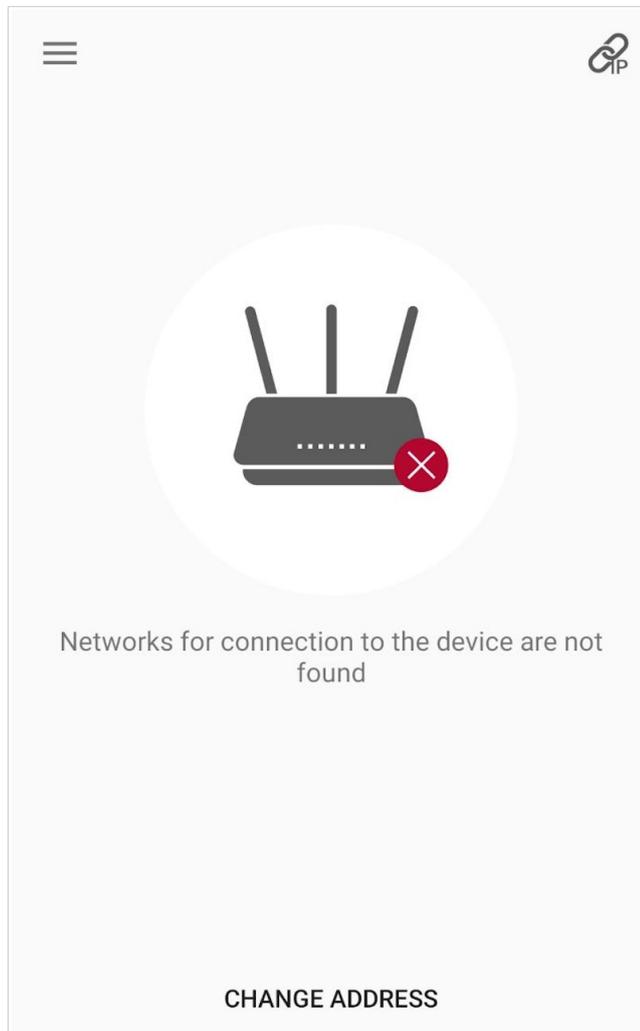


Figure 4. The application main page.

10. On the opened page, enter the IP address of the access point (by default, the following IP address is specified: **192.168.0.50**) in the device URL address field and click the button to confirm ().

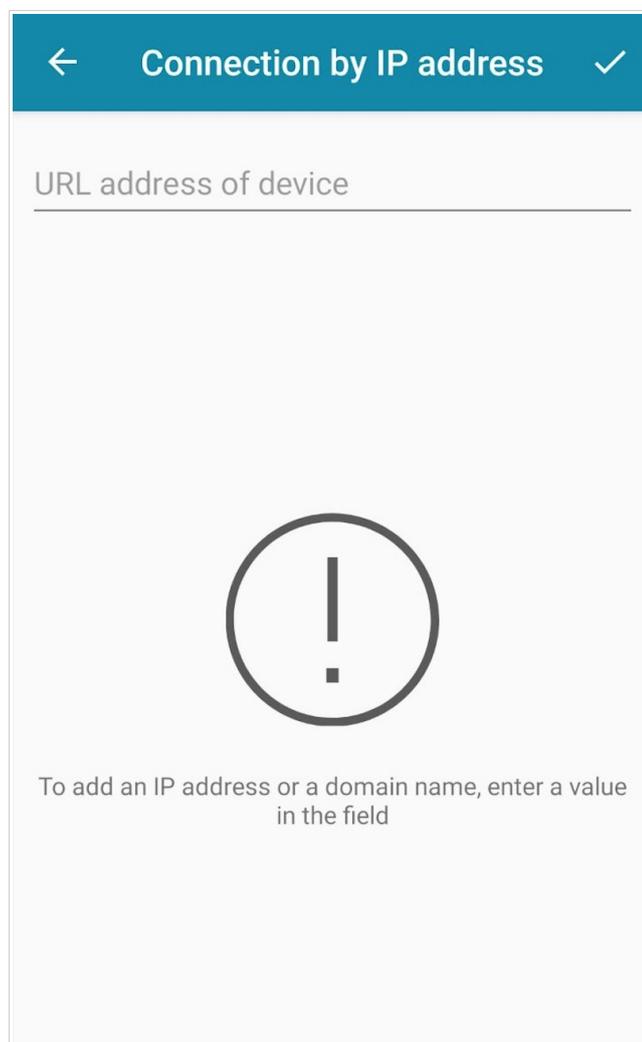


Figure 5. The device URL settings page.

11. Make sure that the application correctly identified the access point to which you connect, and click the **Open** button to configure all needed parameters of DAP-600P.

You can go through the Initial Configuration Wizard or finish the Wizard earlier and go the configuration menu (for the description of the configuration pages, see the relevant section of the *Configuring via Web-based Interface* chapter).

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

When DAP-600P is accessed with the application the next time and after, the authorization page opens. Enter the username (**admin**) and the password you specified.

Connecting to PC

PC with Ethernet Adapter

1. Connect an Ethernet cable between the LAN port of the access point and the Ethernet port of your PC.
2. ***For a switch supporting PoE:*** connect an Ethernet cable between the PoE-enabled switch and the WAN port of the access point.
3. ***For a switch not supporting PoE or router:*** connect an Ethernet cable between the switch or router and any Ethernet port of the access point.
4. Connect the power adapter (not included in the delivery package) to the power connector port on the back panel of the access point, then plug the power adapter into an electrical outlet or power strip.

Now you need to configure an IP address for the Ethernet adapter of your PC.

Configuring IP Address in OS Windows 7

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

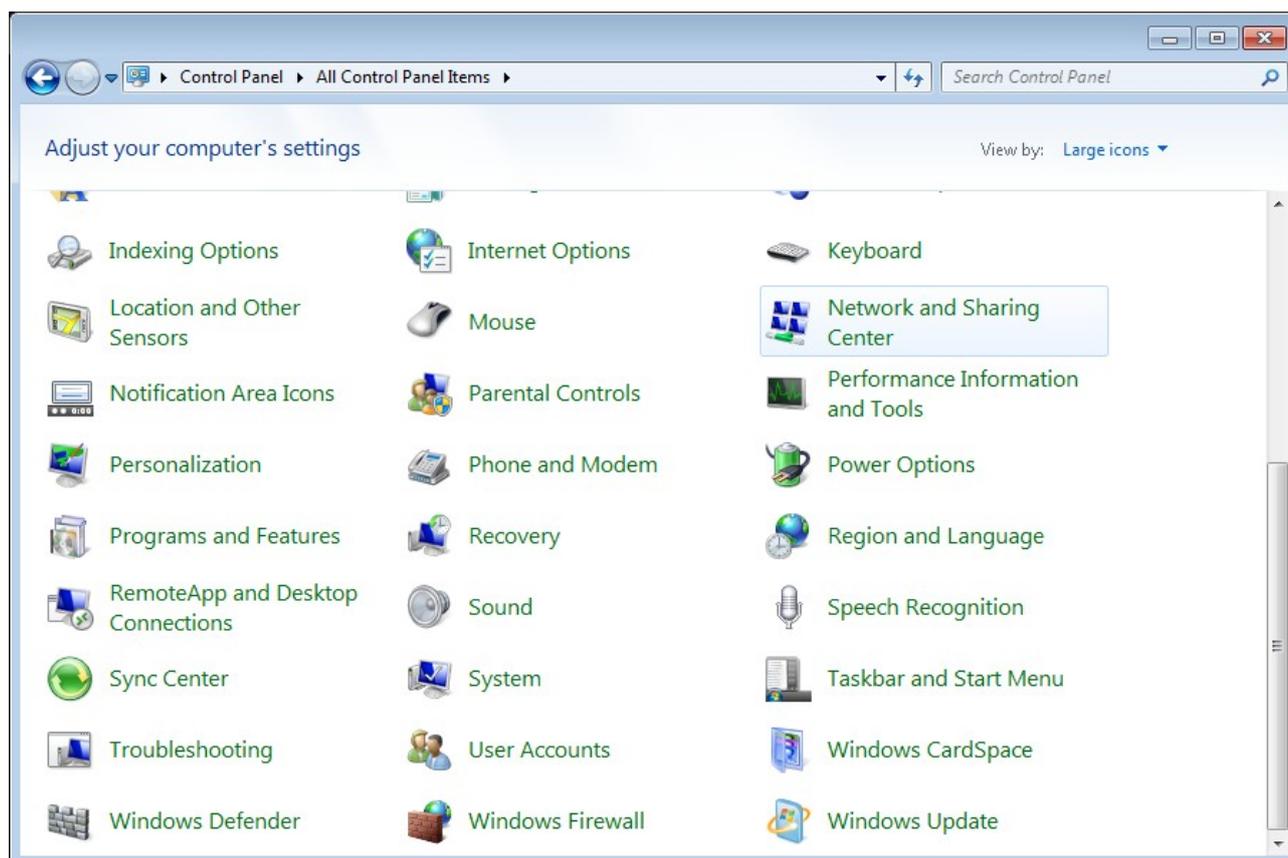


Figure 6. The **Control Panel** window.

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

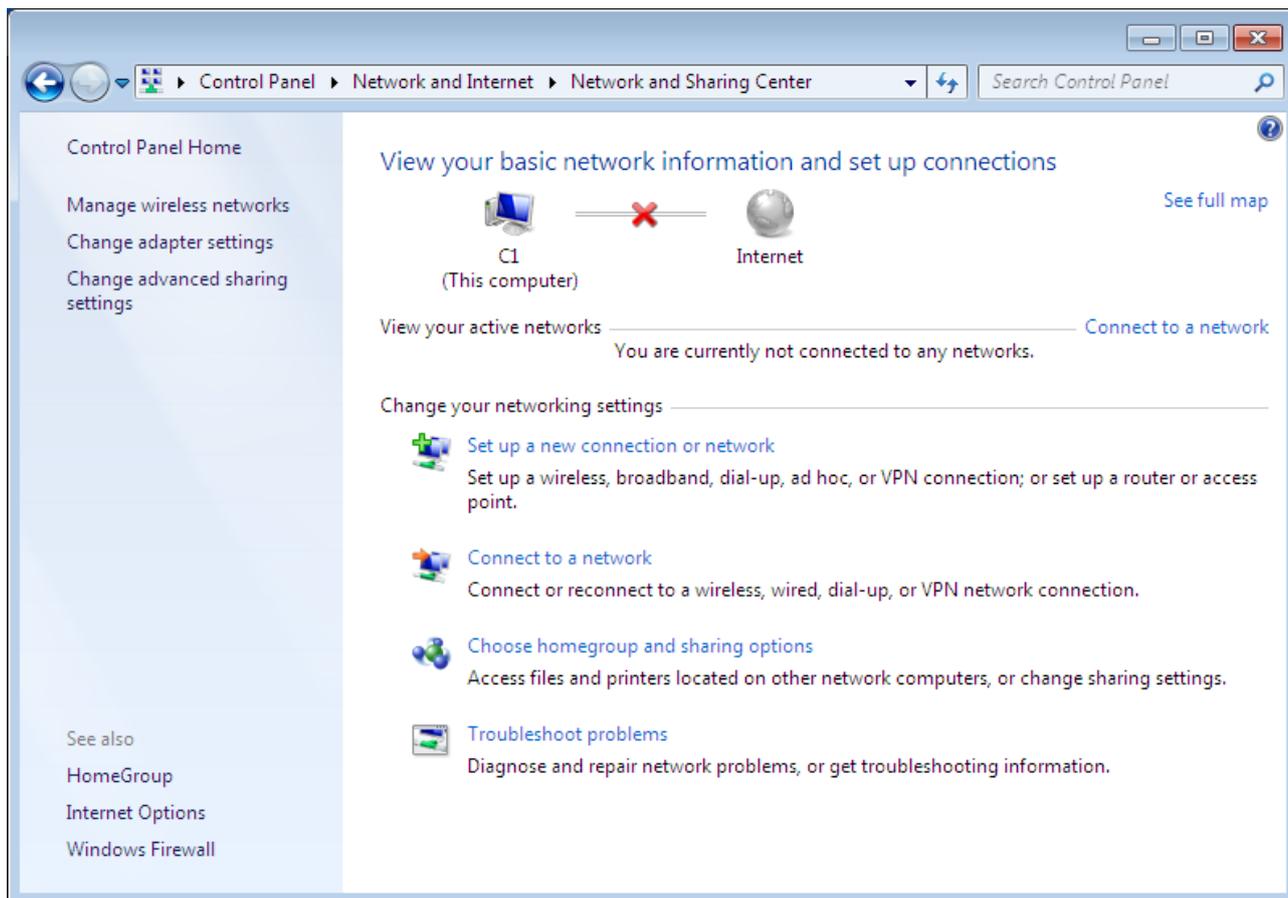


Figure 7. The **Network and Sharing Center** window.

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

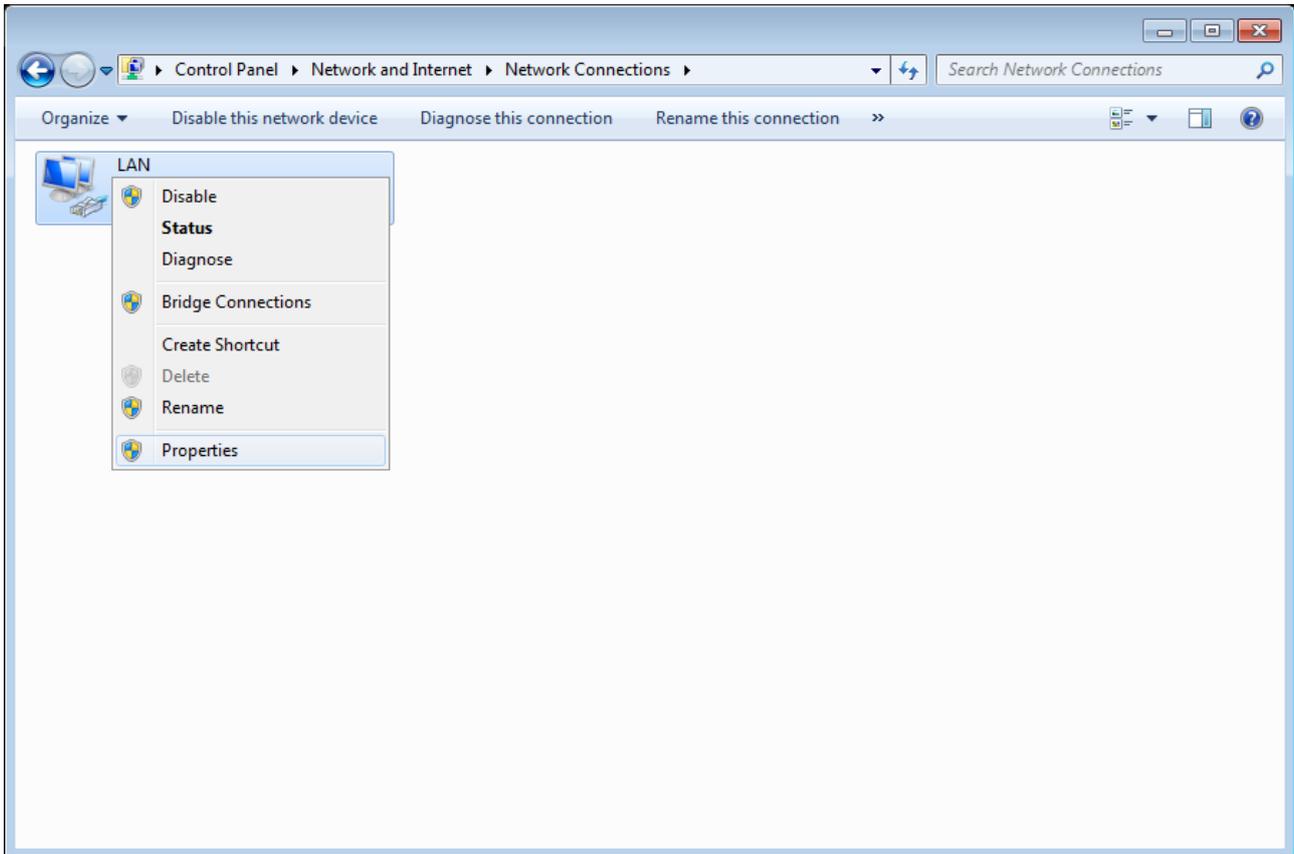


Figure 8. The **Network Connections** window.

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

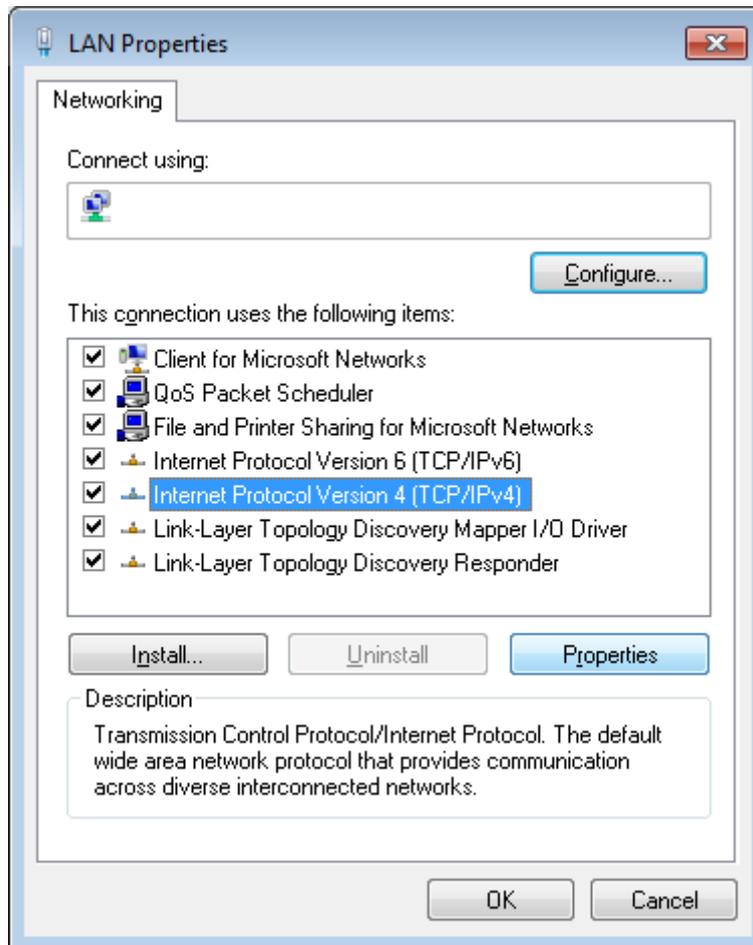


Figure 9. The **Local Area Connection Properties** window.

6. Select the **Use the following IP address** radio button and enter the value **192.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

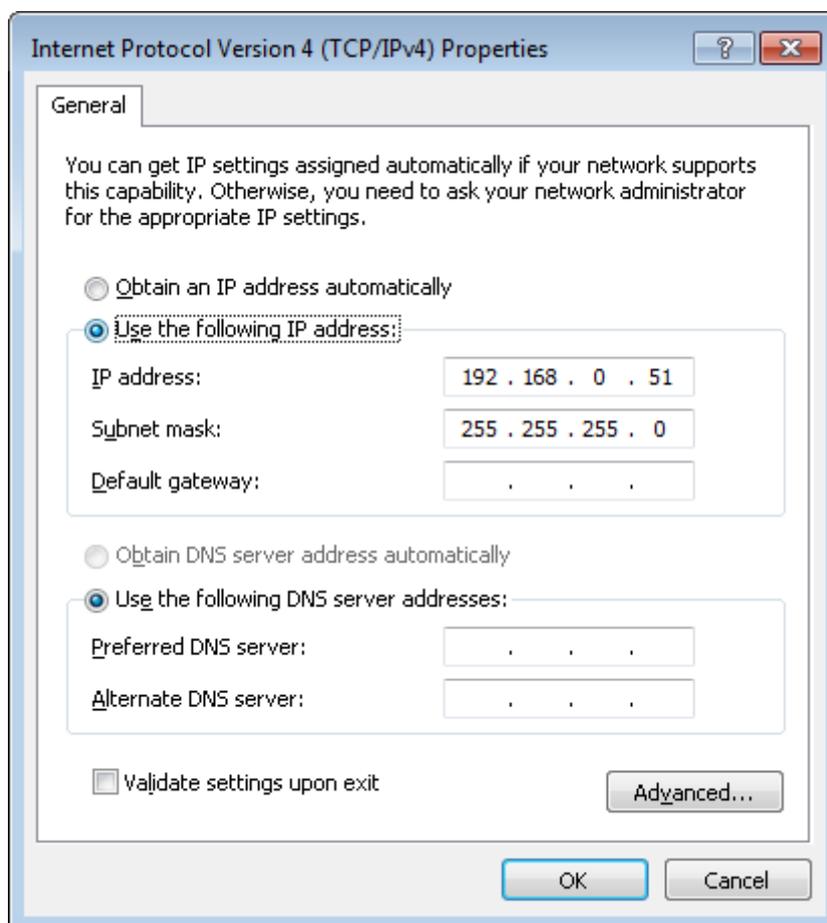


Figure 10. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now you can connect to the web-based interface of DAP-600P for configuring all needed parameters. To gain access to an external network (to the Internet), you also need to specify the default gateway and the addresses of DNS servers.

Configuring IP Address in OS Windows 10

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

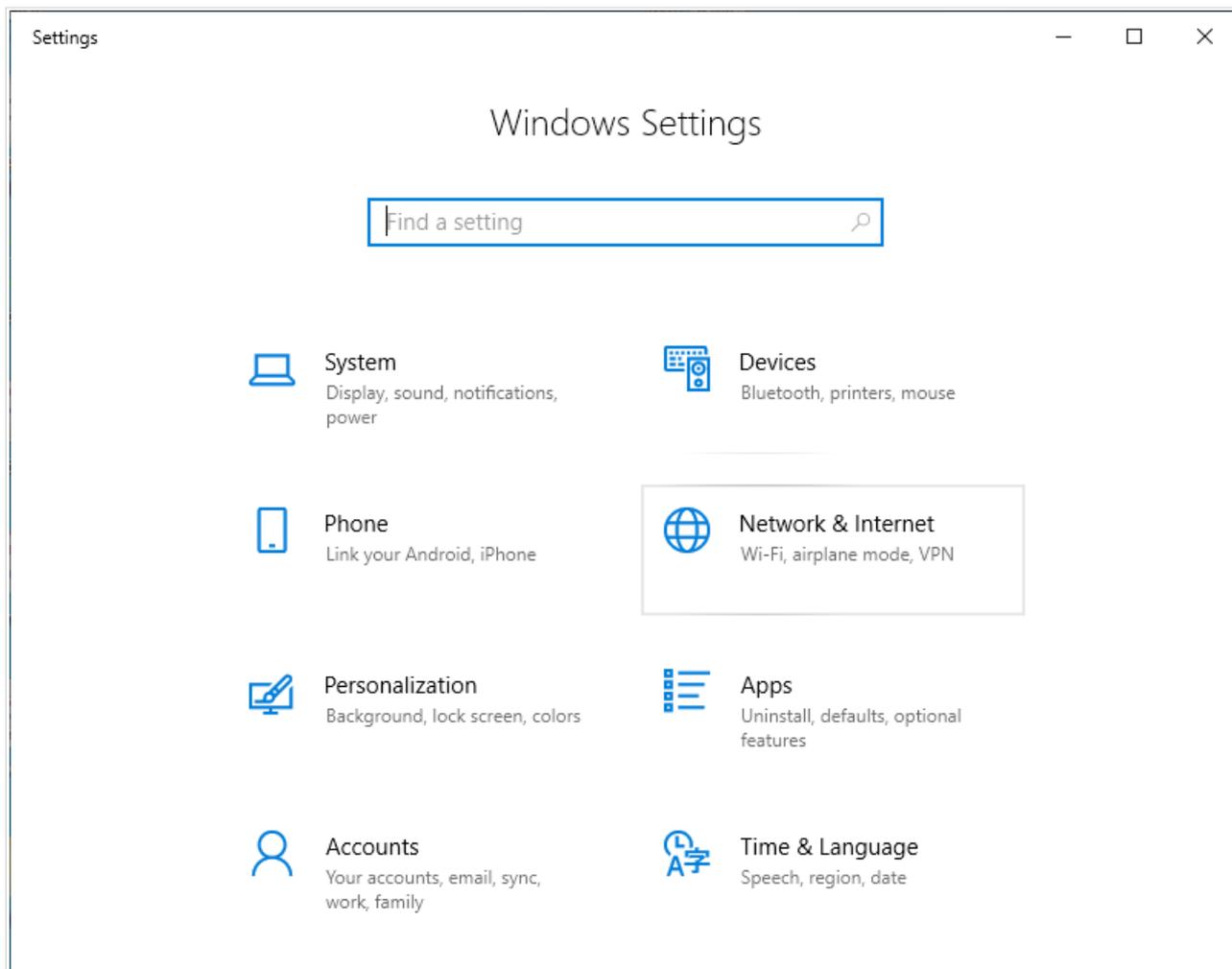


Figure 11. The Windows Settings window.

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

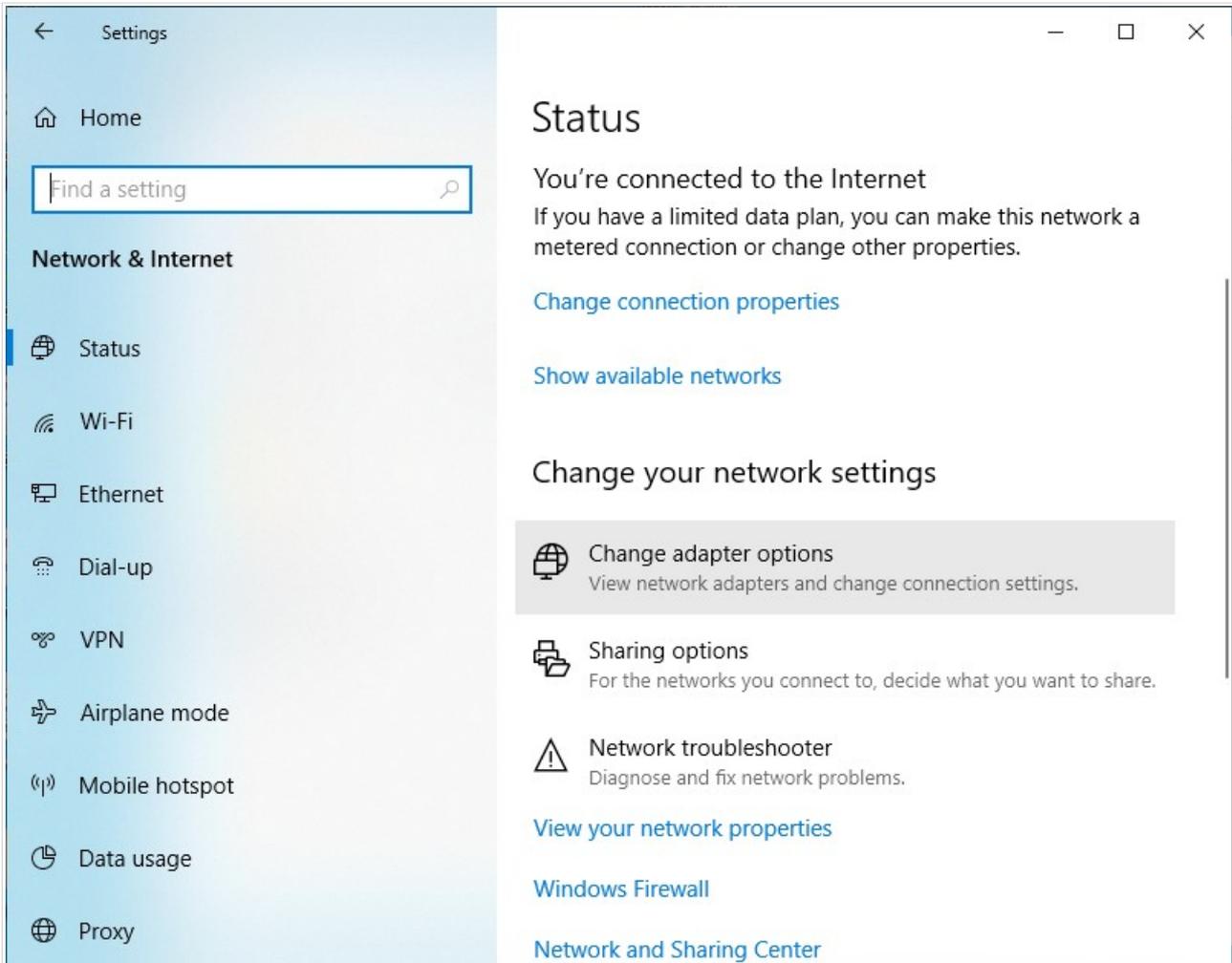


Figure 12. The **Network & Internet** window.

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

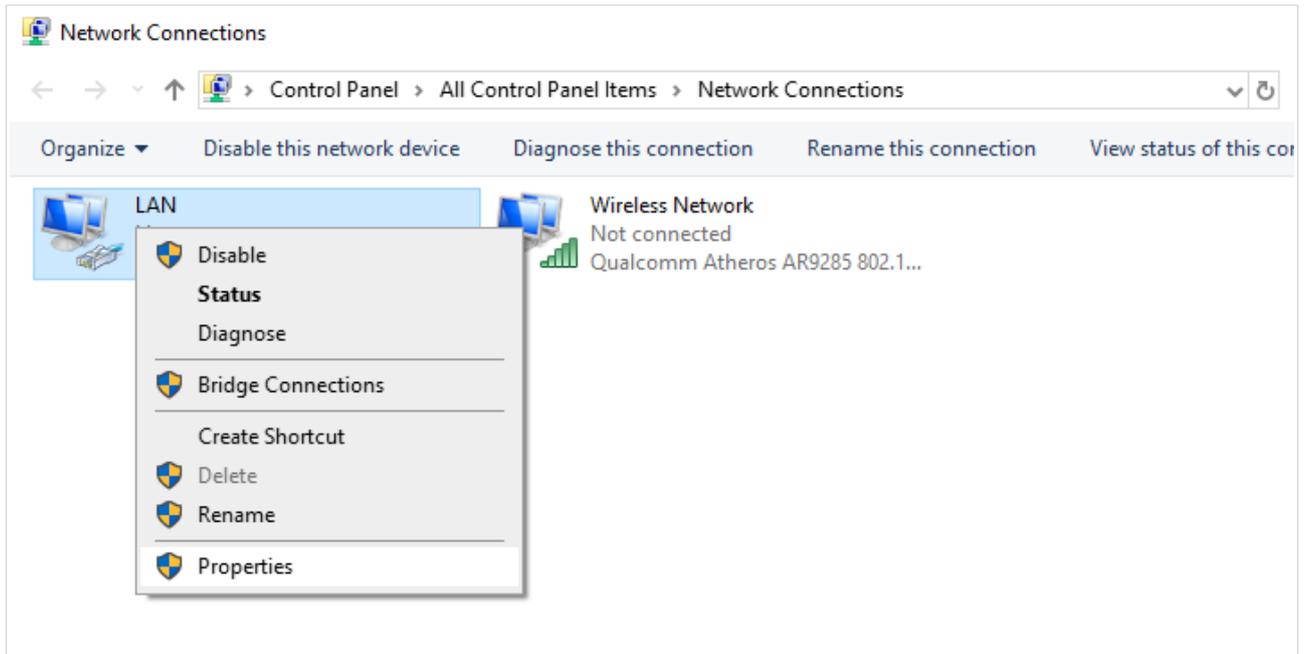


Figure 13. The **Network Connections** window.

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.

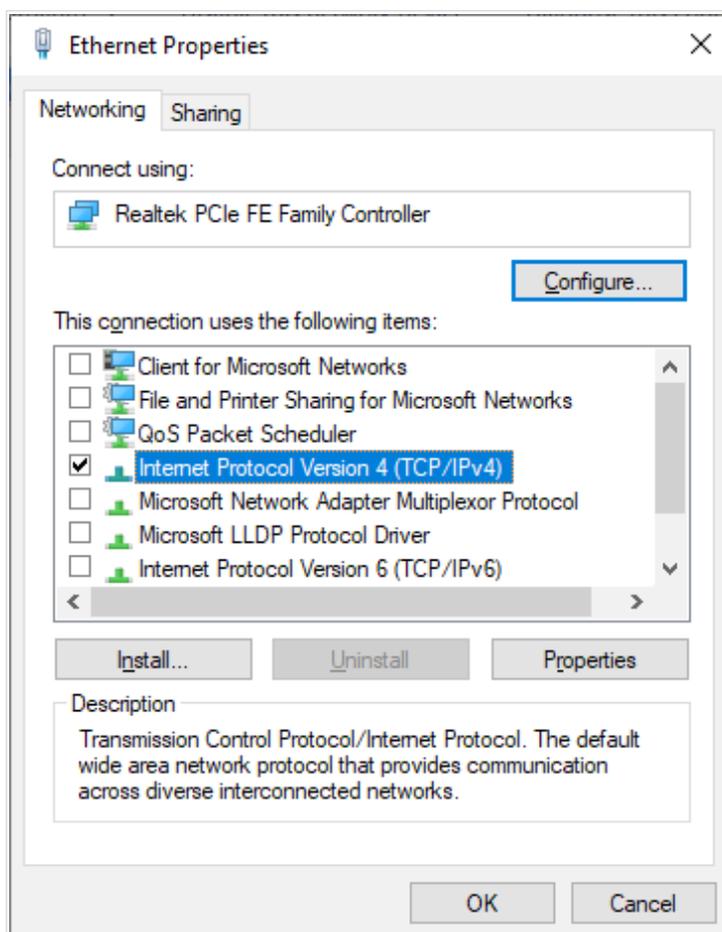


Figure 14. The local area connection properties window.

6. Select the **Use the following IP address** radio button and enter the value **192.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

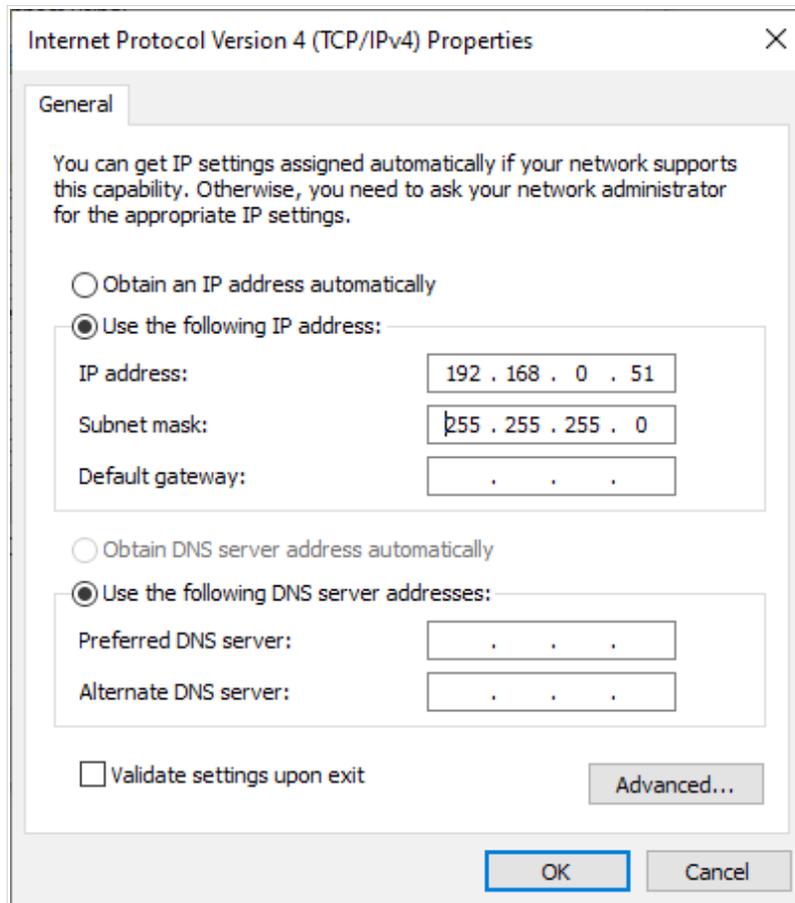


Figure 15. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now you can connect to the web-based interface of DAP-600P for configuring all needed parameters. To gain access to an external network (to the Internet), you also need to specify the default gateway and the addresses of DNS servers.

PC with Wi-Fi Adapter

1. ***For a switch supporting PoE:*** connect an Ethernet cable between the PoE-enabled switch and the WAN port of the access point.
2. ***For a switch not supporting PoE or router:*** connect an Ethernet cable between the switch or router and any Ethernet port of the access point.
3. Connect the power adapter (not included in the delivery package) to the power connector port on the back panel of the access point, then plug the power adapter into an electrical outlet or power strip.
4. Make sure that the Wi-Fi adapter of your PC 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.

Now you should configure your Wi-Fi adapter.

Configuring Wi-Fi Adapter in OS Windows 7

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

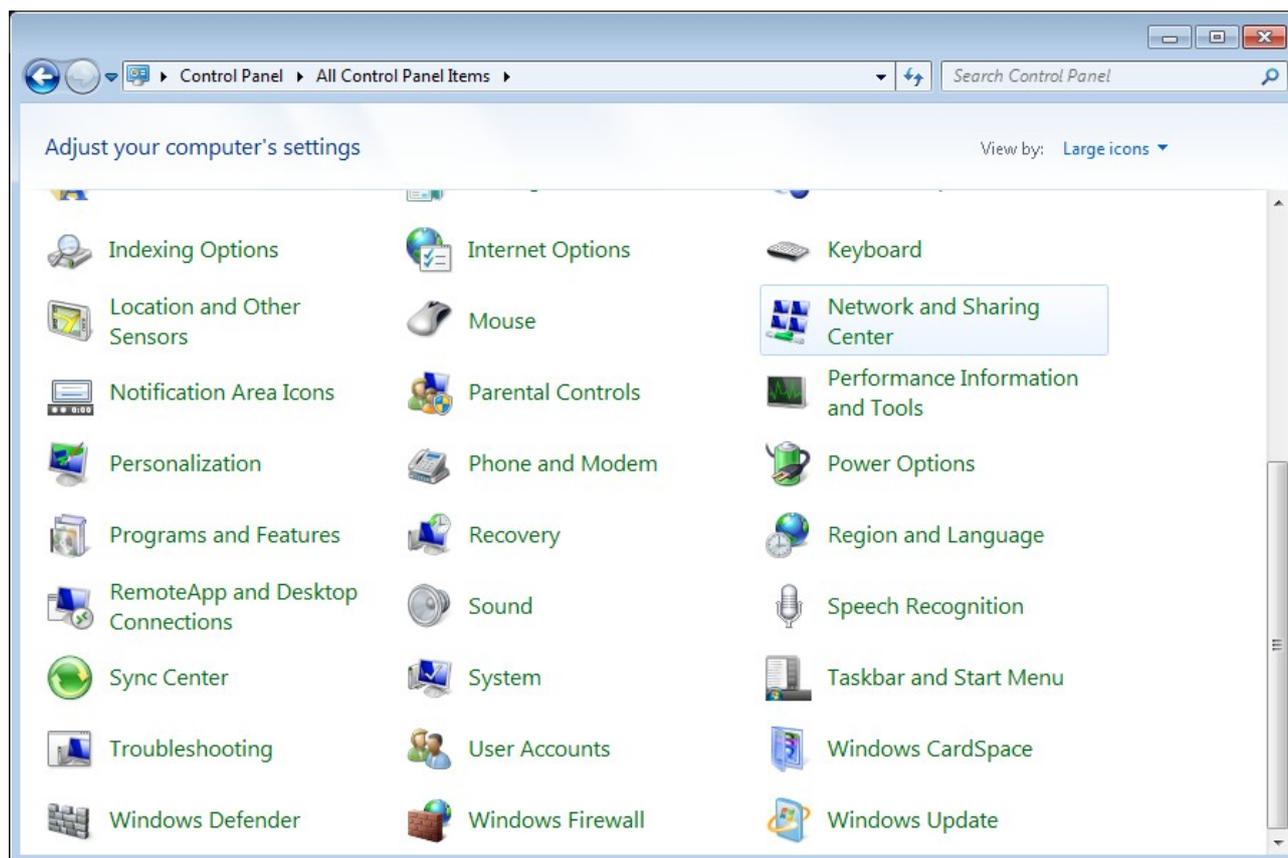


Figure 16. The **Control Panel** window.

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. Select the **Use the following IP address** radio button and enter the value **192.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

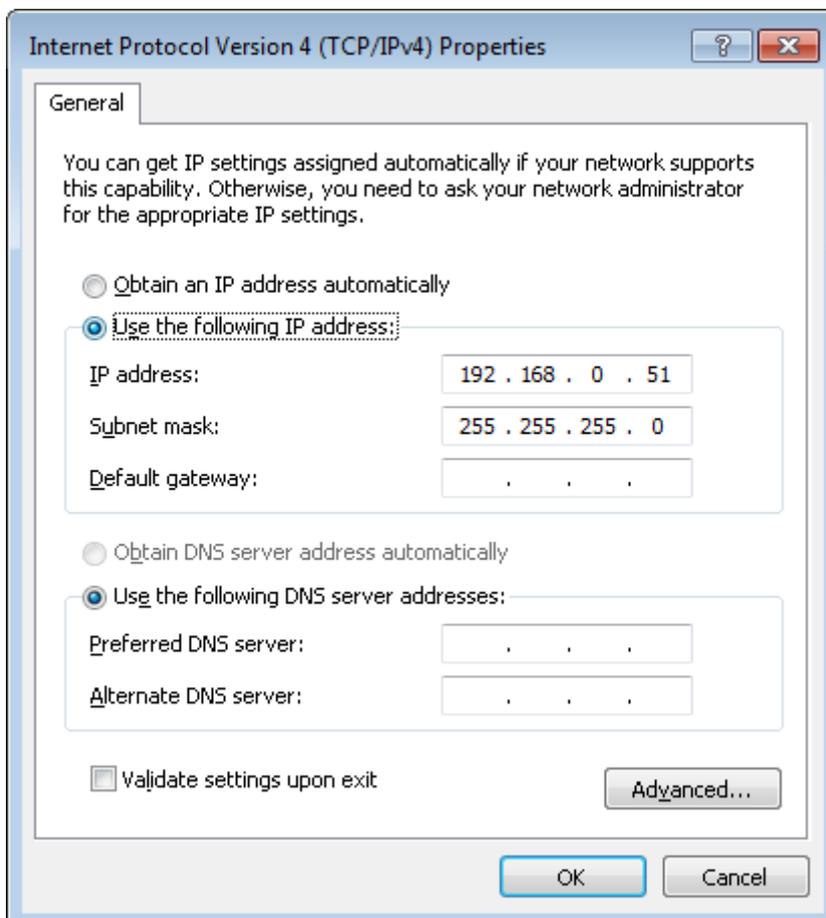


Figure 17. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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 18. The notification area of the taskbar.

- In the opened window, in the list of available wireless networks, select the wireless network **DAP-600P** (for operating in the 2.4GHz band) or **DAP-600P-5G** (for operating in the 5GHz band) and click the **Connect** button.

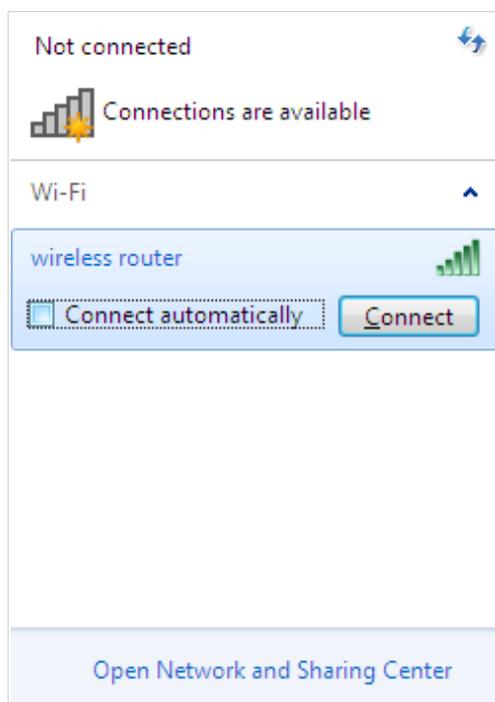


Figure 19. The list of available networks.

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

Now you can connect to the web-based interface of DAP-600P for configuring all needed parameters. To gain access to an external network (to the Internet), you also need to specify the default gateway and the addresses of DNS servers.

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

Configuring Wi-Fi Adapter in OS Windows 10

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

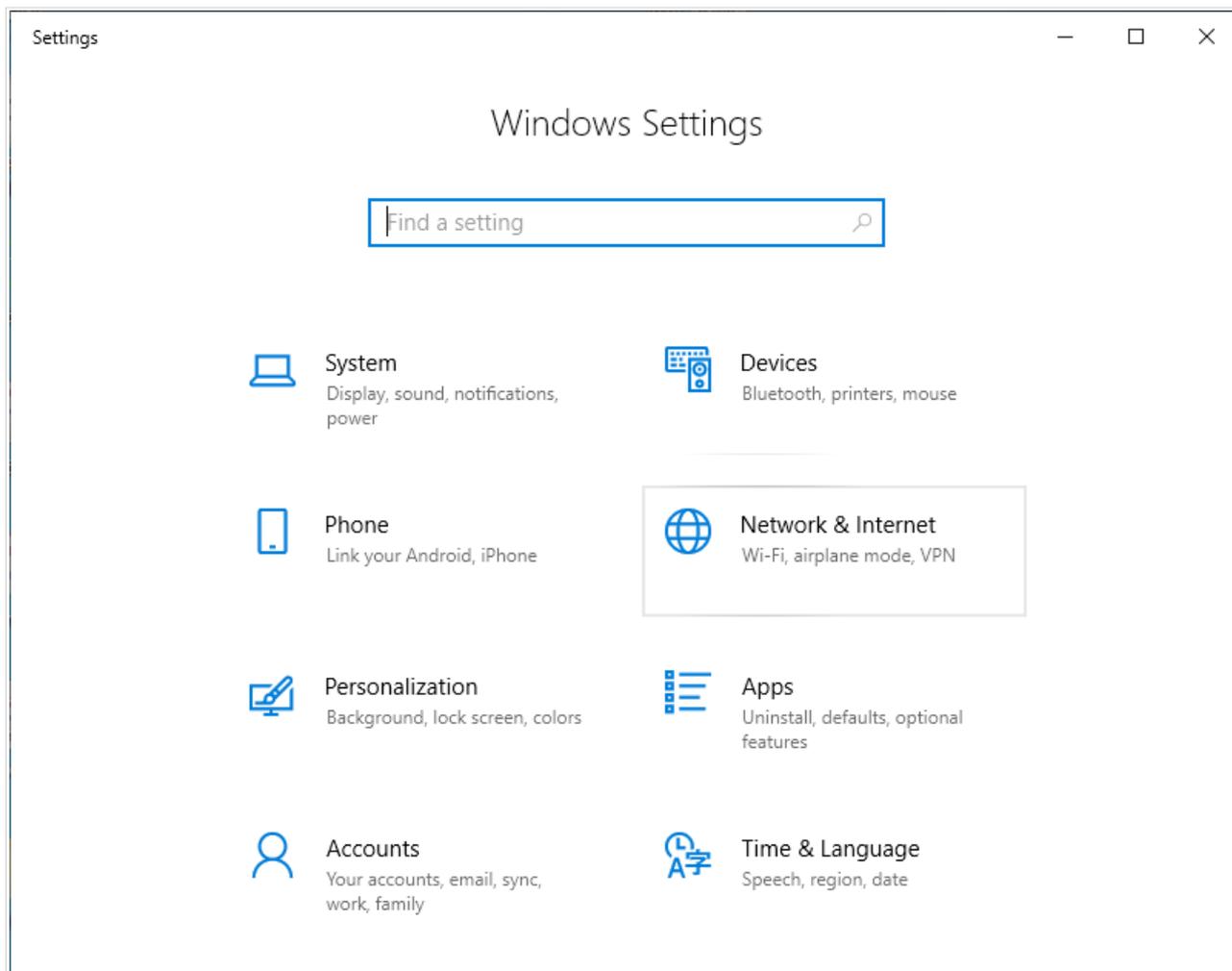


Figure 20. The **Windows Settings** window.

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

6. Select the **Use the following IP address** radio button and enter the value **192.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

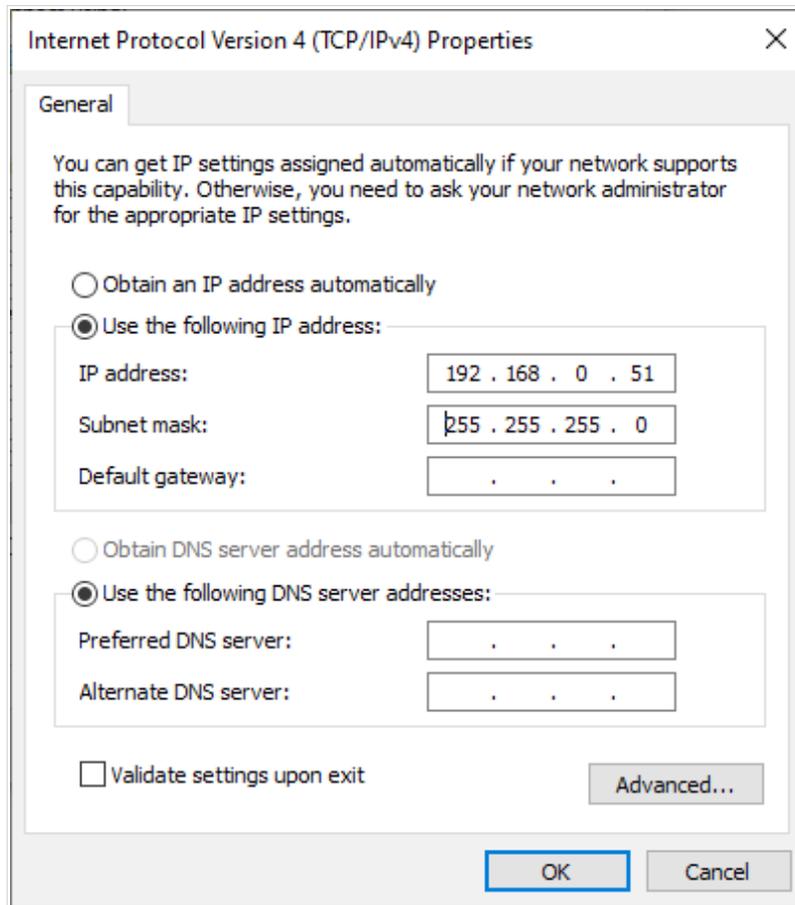


Figure 21. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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



Figure 22. The notification area of the taskbar.

- In the opened **Wireless Network Connection** window, select the wireless network **DAP-600P** (for operating in the 2.4GHz band) or **DAP-600P-5G** (for operating in the 5GHz band) and click the **Connect** button.

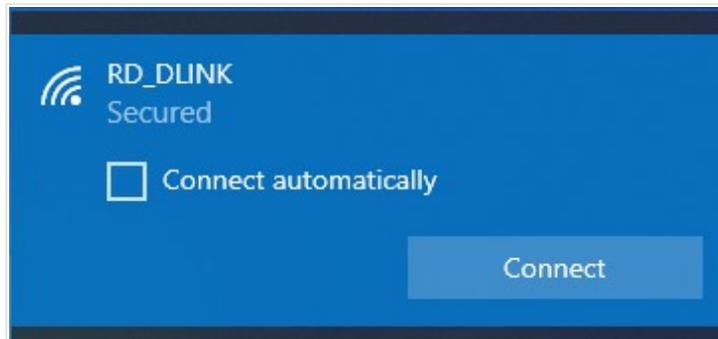


Figure 23. The list of available networks.

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

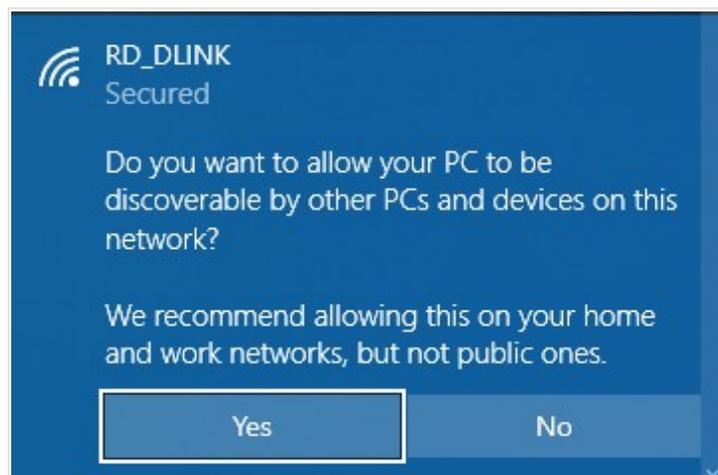


Figure 24. PC discovery settings.

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

Now you can connect to the web-based interface of DAP-600P for configuring all needed parameters. To gain access to an external network (to the Internet), you also need to specify the default gateway and the addresses of DNS servers.

! If you perform initial configuration of the access point via Wi-Fi connection, note that immediately after changing the wireless default settings of the access point 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 (configure the wireless network, change the operating mode of the device, specify the settings of the firewall, etc.).

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 access point (by default, the following IP address is specified: **192.168.0.50**). Press the **Enter** key.

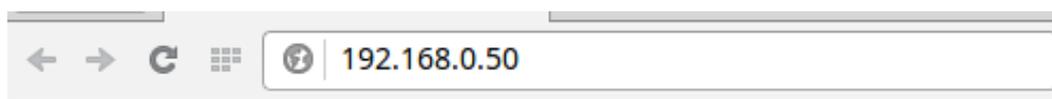


Figure 25. Connecting to the web-based interface of the DAP-600P device.

! 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 access point, make sure that you have properly connected the access point to your computer.

If the device has not been configured previously or the default settings have been restored, after access to the web-based interface the Initial Configuration Wizard opens (see the **Initial Configuration Wizard** section, page 47).

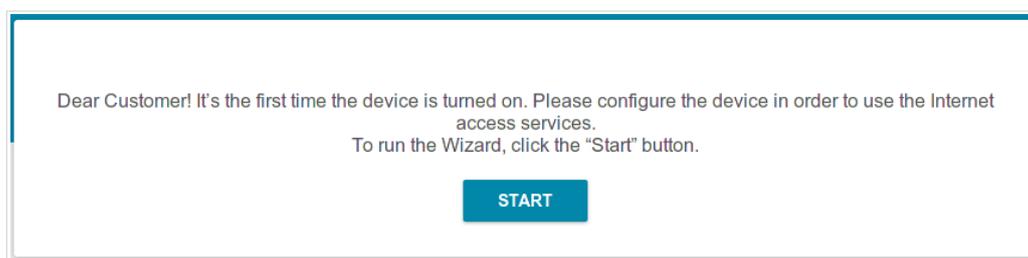
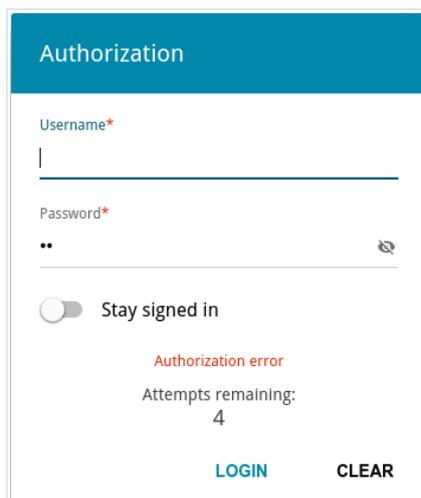


Figure 26. The page for running the Initial Configuration Wizard.

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



Authorization

Username*

admin

Password*

••

Stay signed in

Authorization error

Attempts remaining:
4

LOGIN CLEAR

Figure 27. The login page.

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

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

Web-based Interface Structure

The operating mode defines available sections and pages of the web-based interface.

Summary Page

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

The screenshot displays the 'Summary' page of a D-Link router. The page is organized into several panels:

- Device Information:** Model: DAP-600P; Hardware revision: A1; Firmware version: 4.0.1; Build time: Mon Sep 16 2019 4:43:49 PM MSK; UI version: 1.5.0.19f3001-embedded; Vendor: D-Link Russia; Serial number: 1234567890ABC; Support: support@dlink.ru; Summary: Root filesystem image for DAP_600P_MT7621AT; Uptime: 00:23:26; Device mode: Router.
- WAN IPv4:** Connection type: Dynamic IPv4; Status: Connected; IP address: 192.168.161.222.
- LAN:** LAN IPv4: 192.168.0.50; MAC address: e4:6f:13:ac:bd:27; Wireless connections: 0; Wired connections: 1.
- LAN Ports:** LAN1: 1000M-Full.
- Wi-Fi 2.4 GHz:** Status: On; Broadcasting: On; Additional networks: 0; Network name (SSID): DAP-600P-BD26; Security: WPA2-PSK.
- Wi-Fi 5 GHz:** Status: On; Broadcasting: On; Additional networks: 0; Network name (SSID): DAP-600P-5G-BD26; Security: WPA2-PSK.
- Yandex.DNS:** Enabled. Protection levels: Safe (1 device), Child (0 devices), Protection off (0 devices).

Figure 28. The summary page in the router mode.

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

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

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **initial setup wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 47).

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

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

In the **LAN** section, the IPv4 address of the access point, the LAN MAC address, 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 port and its data transfer mode.

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

Home Page

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

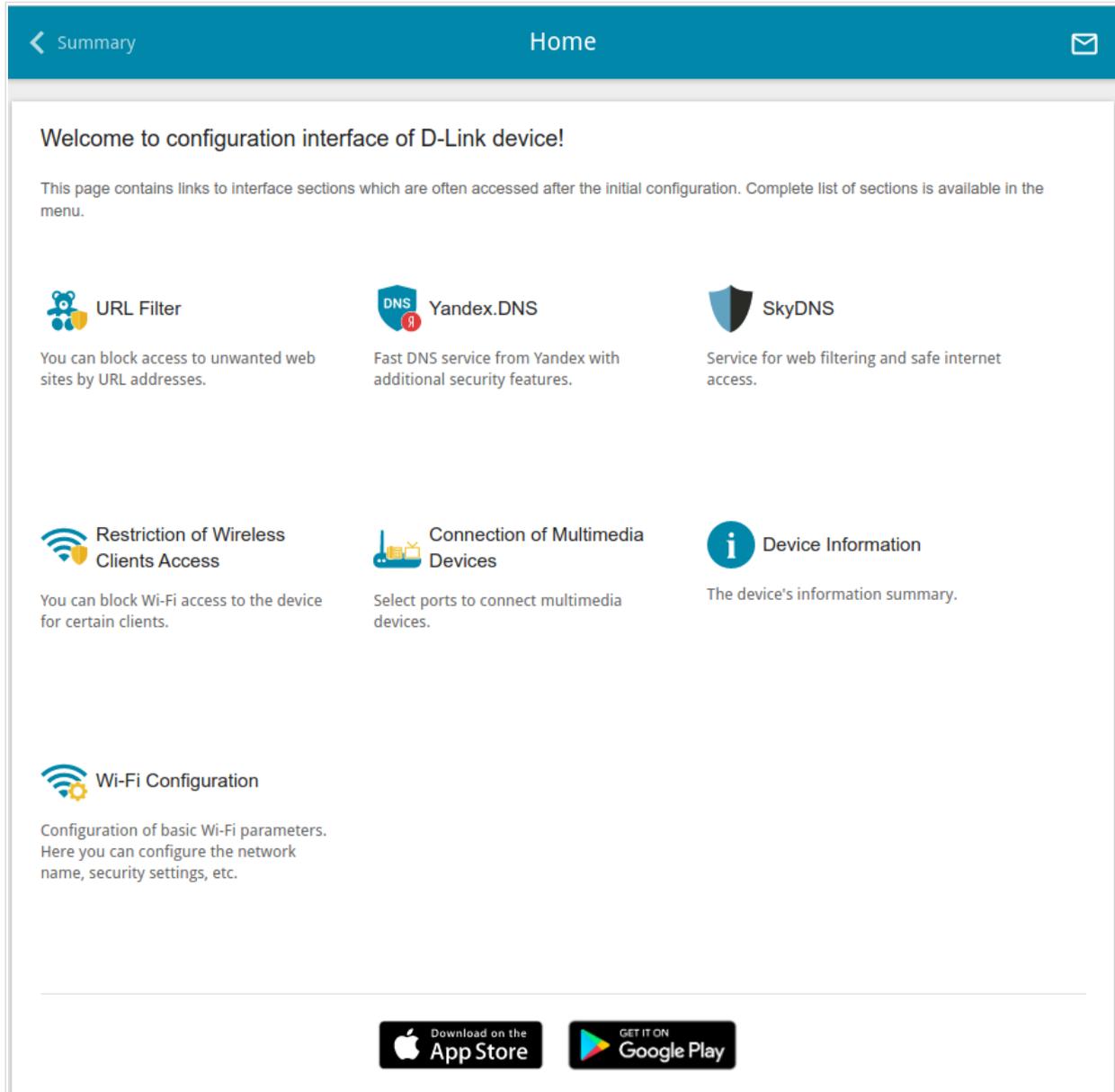


Figure 29. The **Home** page.

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

Menu Sections

To configure the access point use the menu in the left part of the page.

In the **Initial Configuration** section you can run the Initial Configuration Wizard. The Wizard allows you to configure the access point for operation in the needed mode and specify all parameters necessary for getting started (for the description of the Wizard, see the *Initial Configuration Wizard* section, page 47).

The pages of the **Statistics** section display data on the current state of the access point (for the description of the pages, see the *Statistics* section, page 73).

The pages of the **Connections Setup** section are designed for configuring basic parameters of the LAN interface of the access point and creating a connection to the Internet (for the description of the pages, see the *Connections Setup* section, page 79).

The pages of the **Wi-Fi** section are designed for specifying all needed settings of the access point's wireless network (for the description of the pages, see the *Wi-Fi* section, page 117).

The pages of the **Advanced** section are designed for configuring additional parameters of the access point (for the description of the pages, see the *Advanced* section, page 151).

The pages of the **Firewall** section are designed for configuring the firewall of the access point (for the description of the pages, see the *Firewall* section, page 189).

The pages of the **System** section provide functions for managing the internal system of the access point (for the description of the pages, see the *System* section, page 201).

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 222).

The pages of the **SkyDNS** section are designed for configuring the SkyDNS web content filtering service (for the description of the pages, see the *SkyDNS* section, page 226).

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

Notifications

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

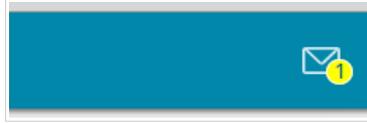


Figure 30. The web-based interface notifications.

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

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration Wizard

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

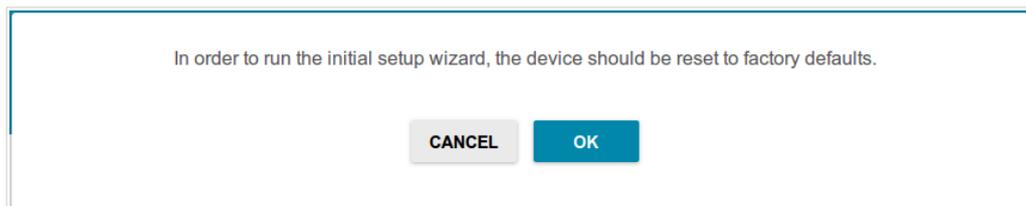


Figure 31. Restoring the default settings in the Wizard.

If you perform initial configuration of the access point via Wi-Fi connection, please make sure that you are connected to the wireless network of DAP-600P (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

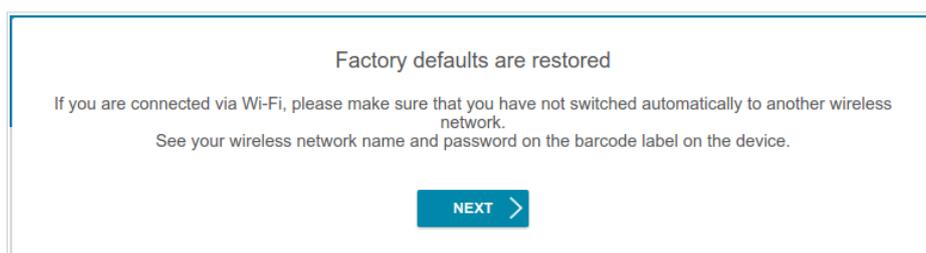


Figure 32. Checking connection to the wireless network.

Click the **START** button.

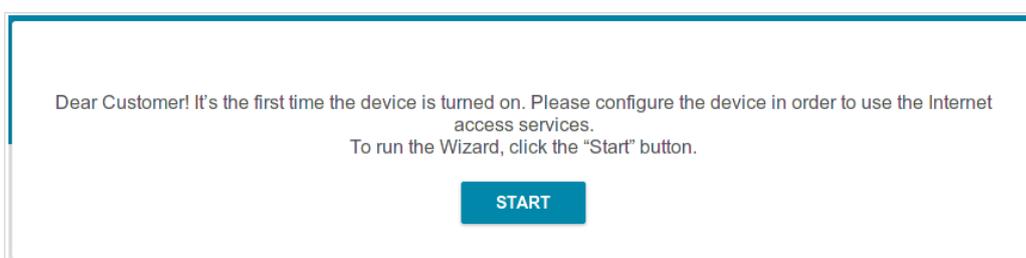


Figure 33. Starting the Wizard.

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

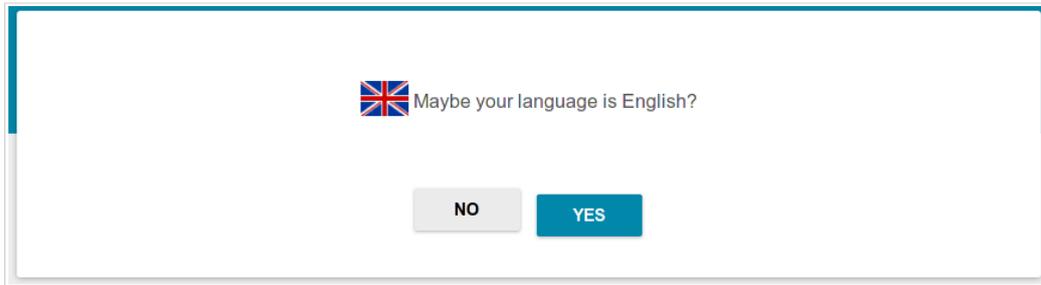


Figure 34. Selecting a language.

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

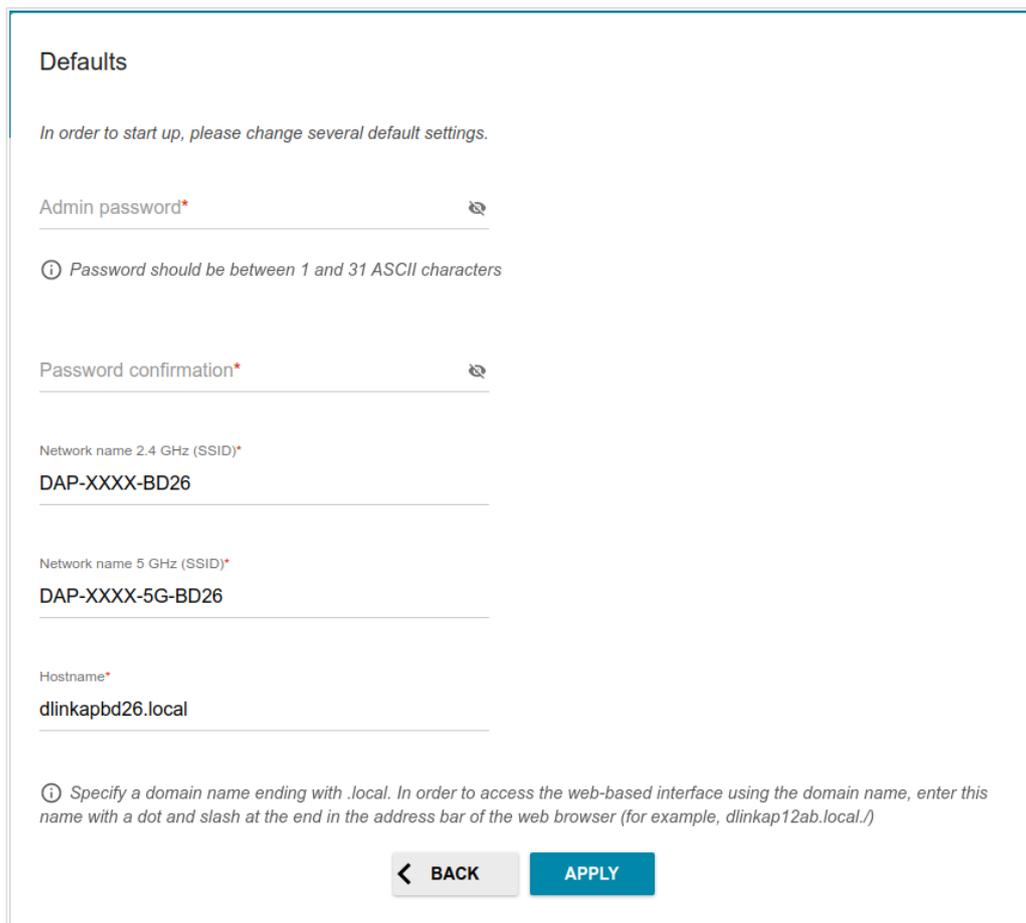


Figure 35. Changing the default settings.

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

Selecting Operation Mode

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

Router

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

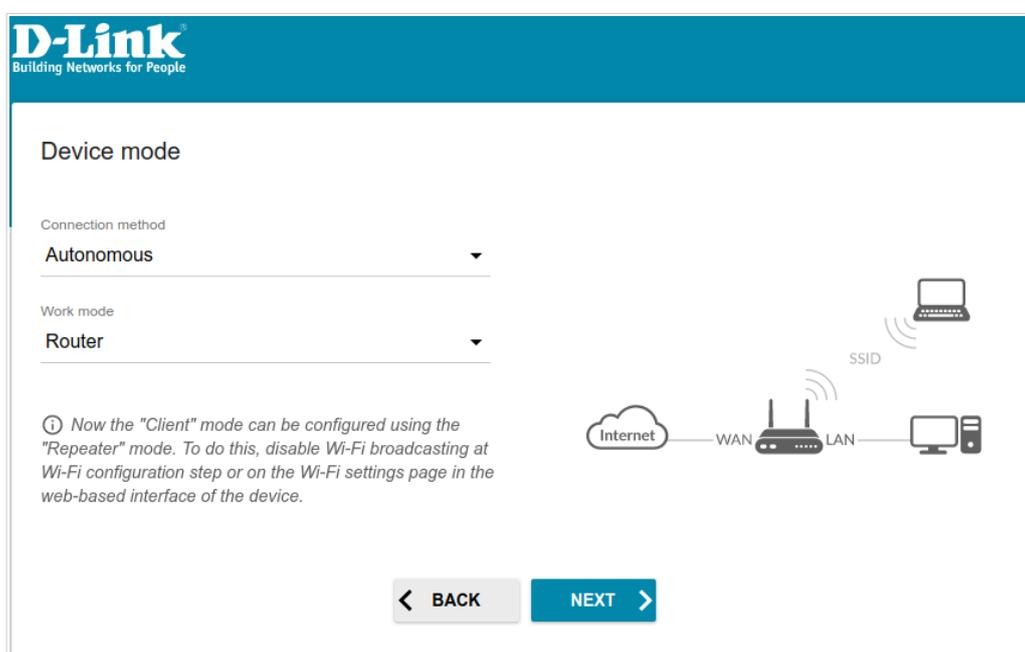


Figure 36. Selecting an operation mode. The **Router** mode.

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

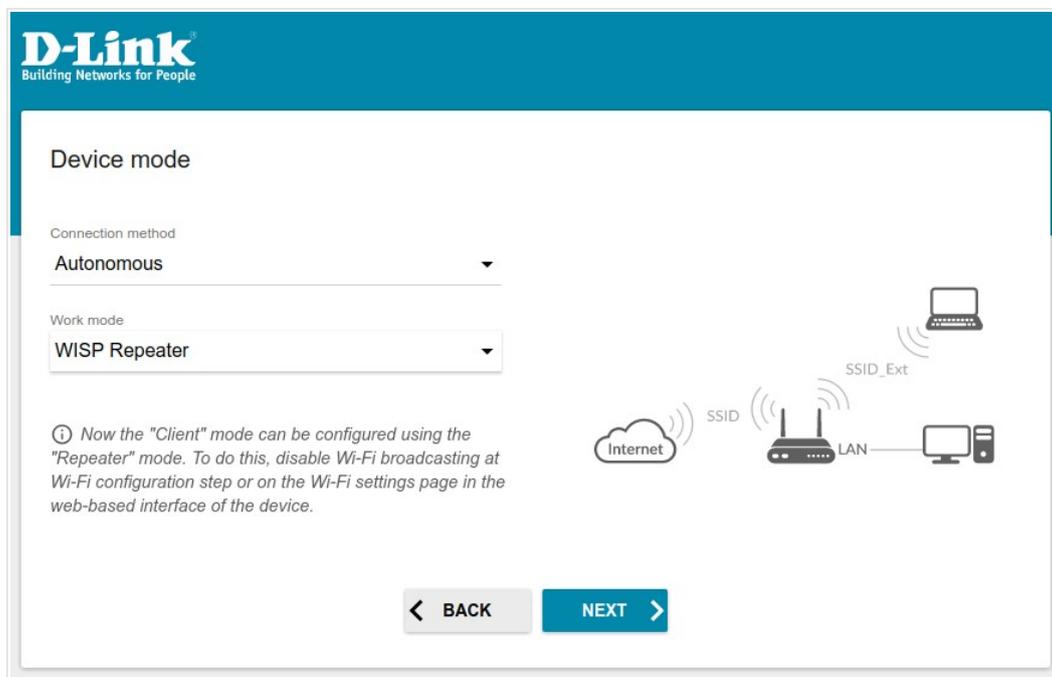


Figure 37. Selecting an operation mode. The **WISP Repeater** mode.

Access Point or Repeater

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

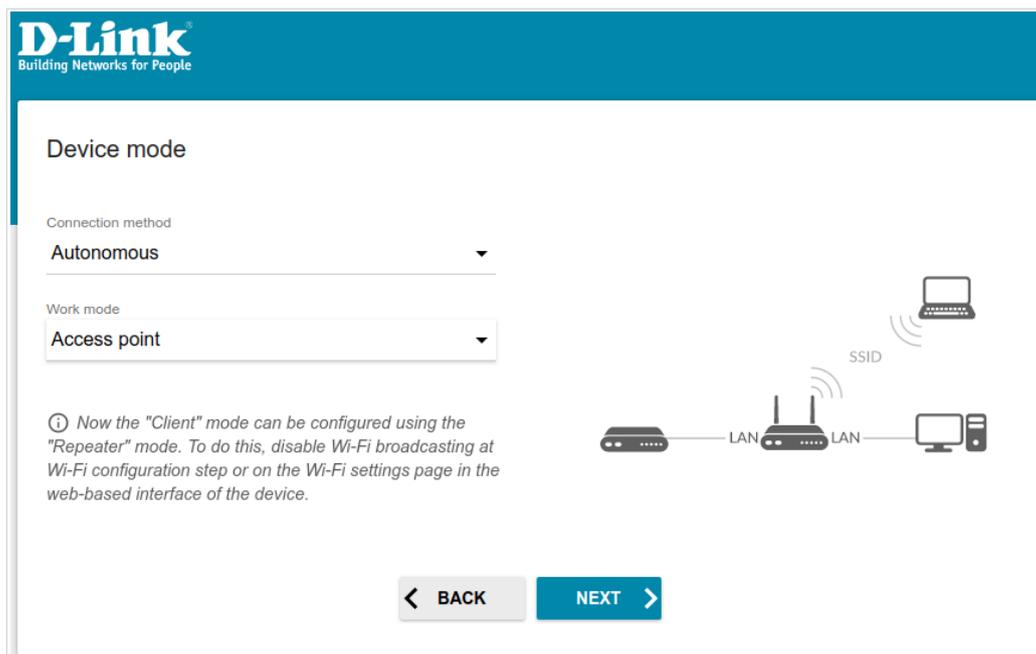


Figure 38. Selecting an operation mode. The **Access point** mode.

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

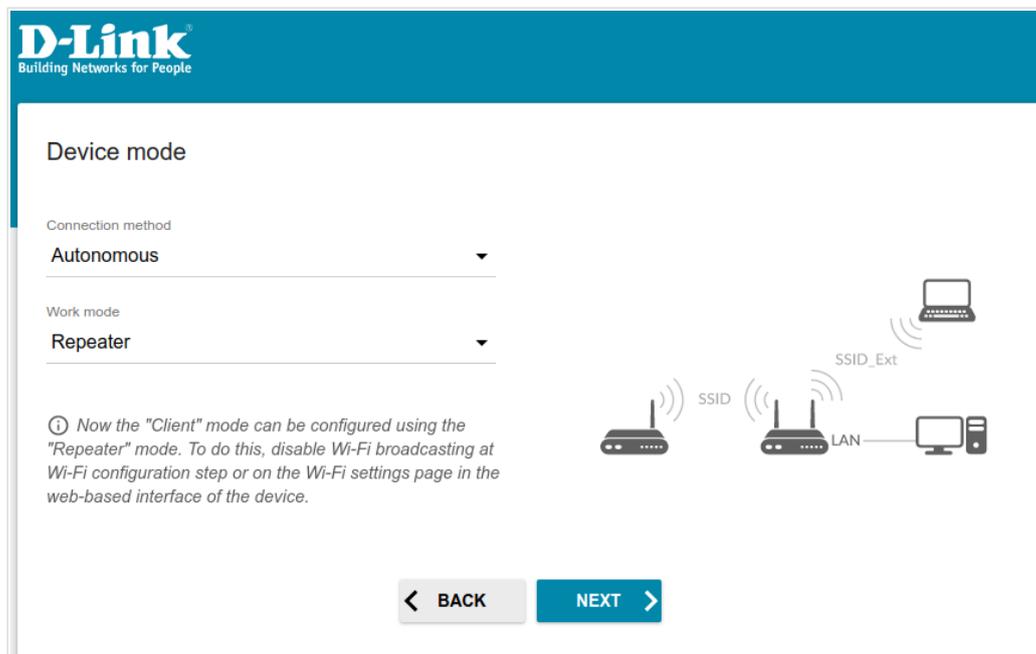


Figure 39. Selecting an operation mode. The **Repeater** mode.

Mesh Network Main Device (Master)

In order to configure DAP-600P as a main device of your Mesh network, from the **Connection method** list, select the **Super Mesh** value. Then from the **Device Role** list, select the **Master** value. From the **Frequency band** list, select the band where your Mesh network operates.

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

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

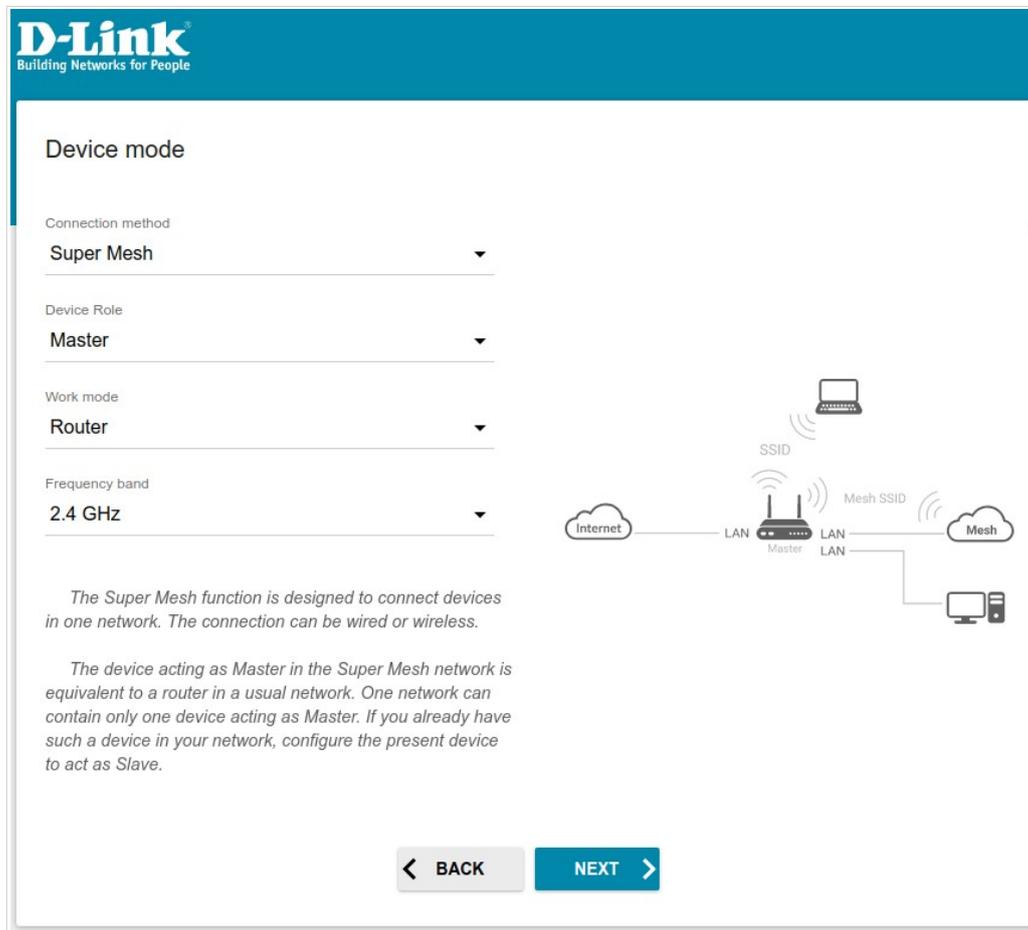


Figure 40. Configuring the Super Mesh function for a main device. The **Router** mode.

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

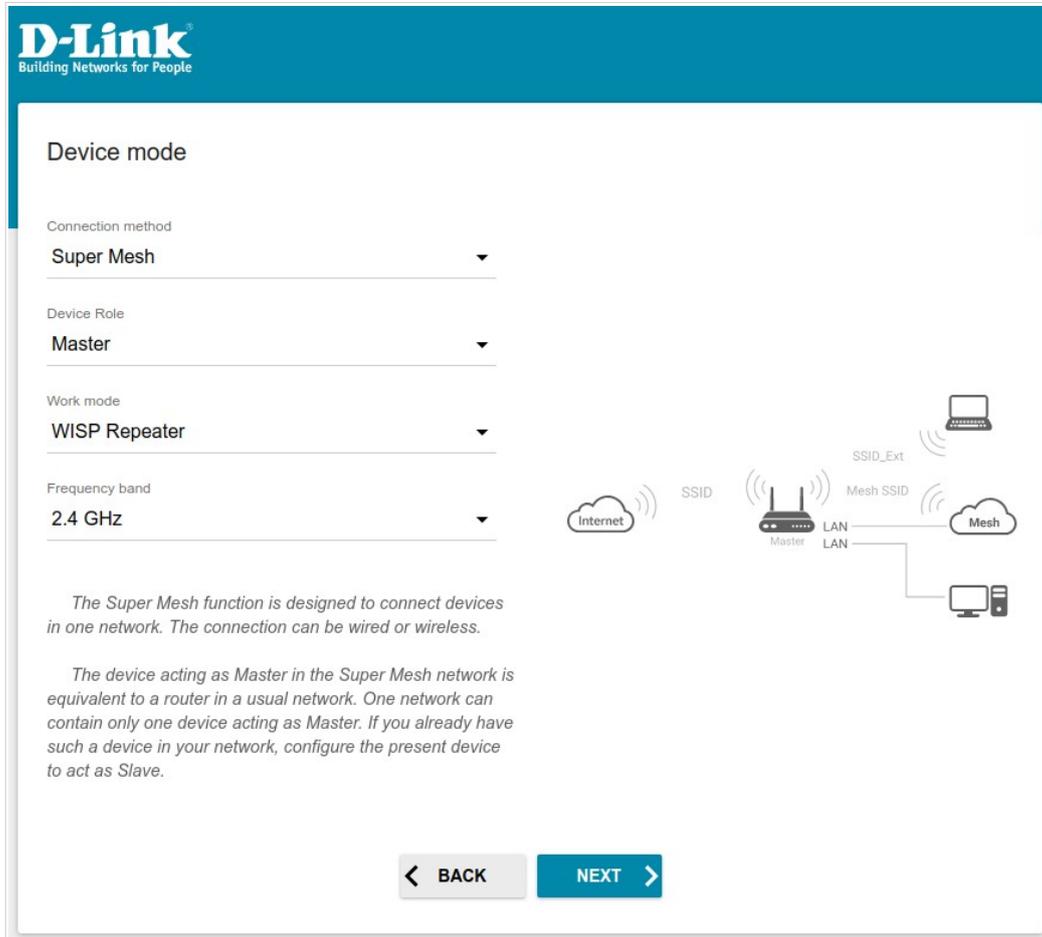


Figure 41. Configuring the Super Mesh function for a main device. The **WISP Repeater** mode.

Mesh Network Subordinate Device (Slave)

In order to configure DAP-600P as a subordinate device of your Mesh network, from the **Connection method** list, select the **Super Mesh** value. Then from the **Device Role** list, select the **Slave** value. From the **Frequency band** list, select the band where your main device (in the Master role) operates.

Then a device in the Slave role is configured in the access point mode. In this mode you can change the LAN IP address, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

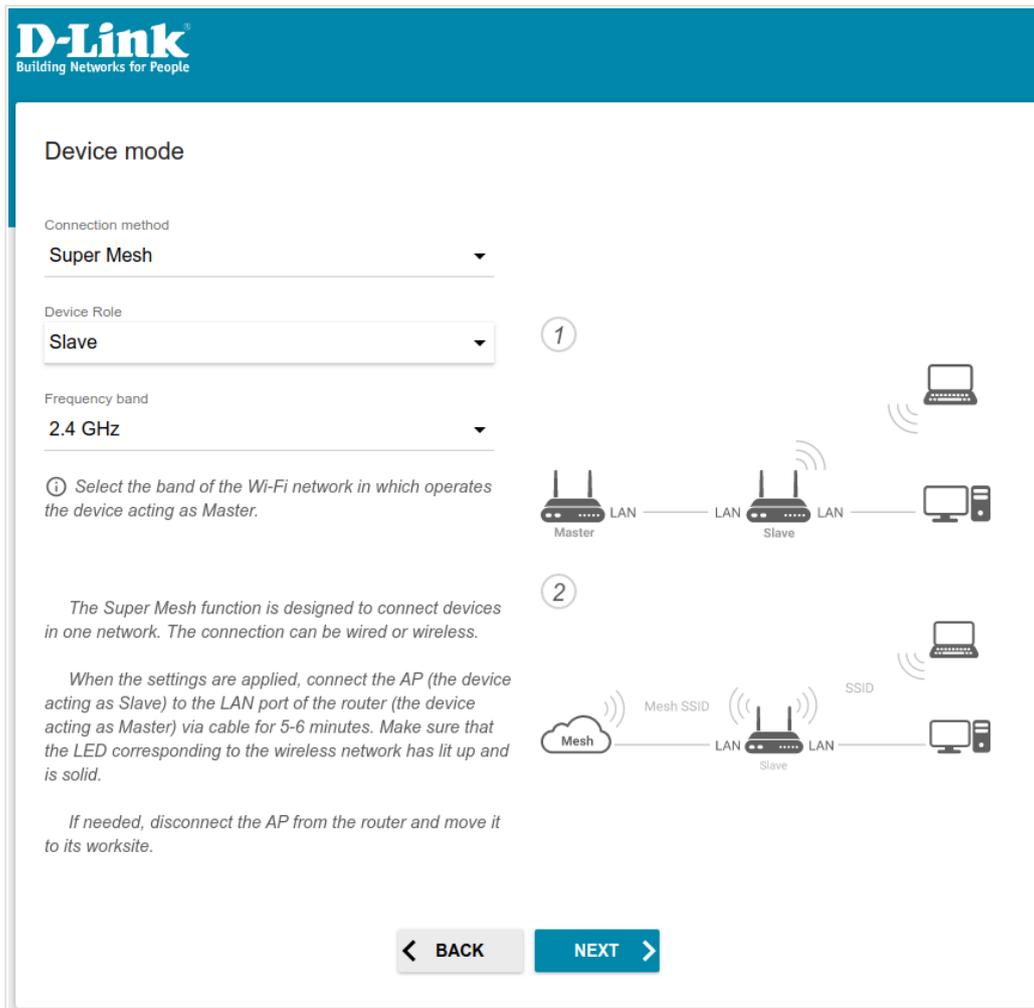


Figure 42. Configuring the Super Mesh function for a subordinate device.

Changing LAN IPv4 Address

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

1. Select the **Automatic obtainment of IPv4 address** to let DAP-600P automatically obtain the LAN IPv4 address.

If you want to manually assign the LAN IPv4 address for DAP-600P, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Subnet mask**, **DNS IP address**, **Hostname** fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.

- ! If the LAN IPv4 address of DAP-600P was changed, it may be necessary to change your PC's NIC settings.

LAN

Automatic obtainment of IPv4 address

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

IP address*
192.168.0.50

Subnet mask*
255.255.255.0

Gateway IP address

DNS IP address*
8.8.8.8

Hostname*
dlinkapa377.local

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

[← BACK](#) [NEXT →](#)

Figure 43. The page for changing the LAN IPv4 address.

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

Wi-Fi Client

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

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

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

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

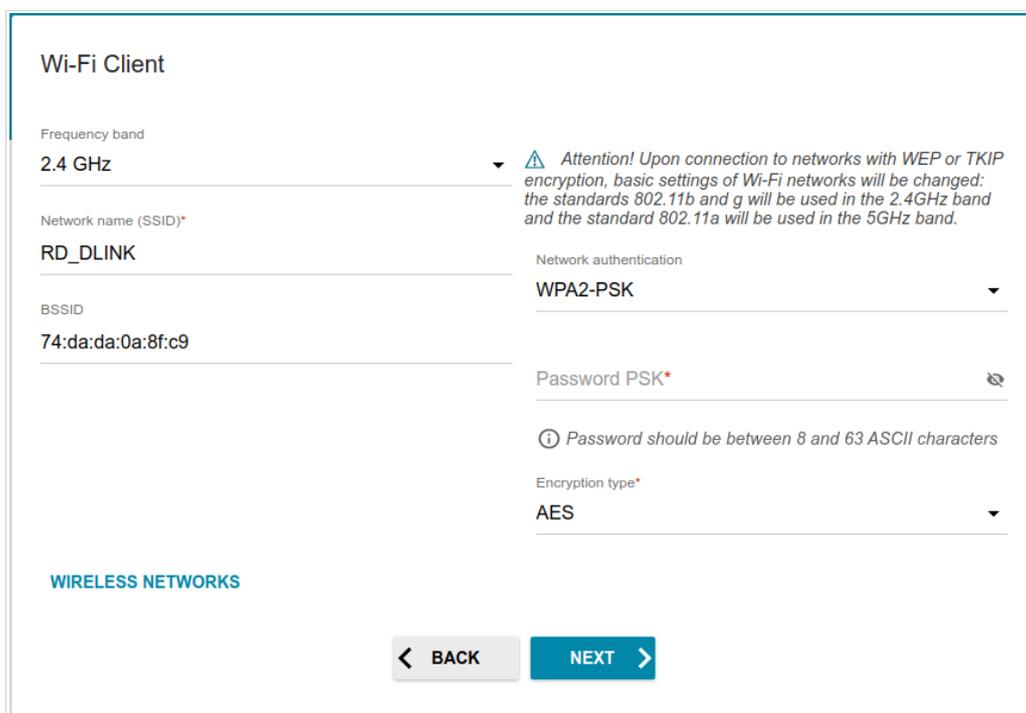


Figure 44. The page for configuring the Wi-Fi client.

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

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

Parameter	Description
Enable encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the Default key ID drop-down list, the Encryption key WEP as HEX checkbox, and four Encryption key fields are displayed on the page.

Parameter	Description
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The access point uses the key selected from the Default key ID drop-down list. It is required to specify all the fields. Click the Show icon (🔍) to display the entered key.

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

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

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

Configuring WAN Connection

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

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

1. On the **Internet connection type** page, click the **SCAN** button (available for the **Router** mode only) to automatically specify the connection type used by your ISP or manually select the needed value from the **Connection type** list.
2. Specify the settings necessary for the connection of the selected type.
3. If your ISP uses MAC address binding, select the **Clone MAC address of your device** checkbox.
4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field.
5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Static IPv4 Connection

Internet connection type

Connection type
Static IPv4

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

SCAN Network scan for connection type and parameters detection

IP address*

Subnet mask*

Gateway IP address*

DNS IP address*

Clone MAC address of your device

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

Use VLAN

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

Use IGMP

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

< BACK **NEXT >**

Figure 45. The page for configuring Static IPv4 WAN connection.

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

Static IPv6 Connection

Internet connection type

Connection type
Static IPv6

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

SCAN Network scan for connection type and parameters detection

IP address*

Prefix*

Gateway IP address*

DNS IP address*

Clone MAC address of your device

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

Use VLAN

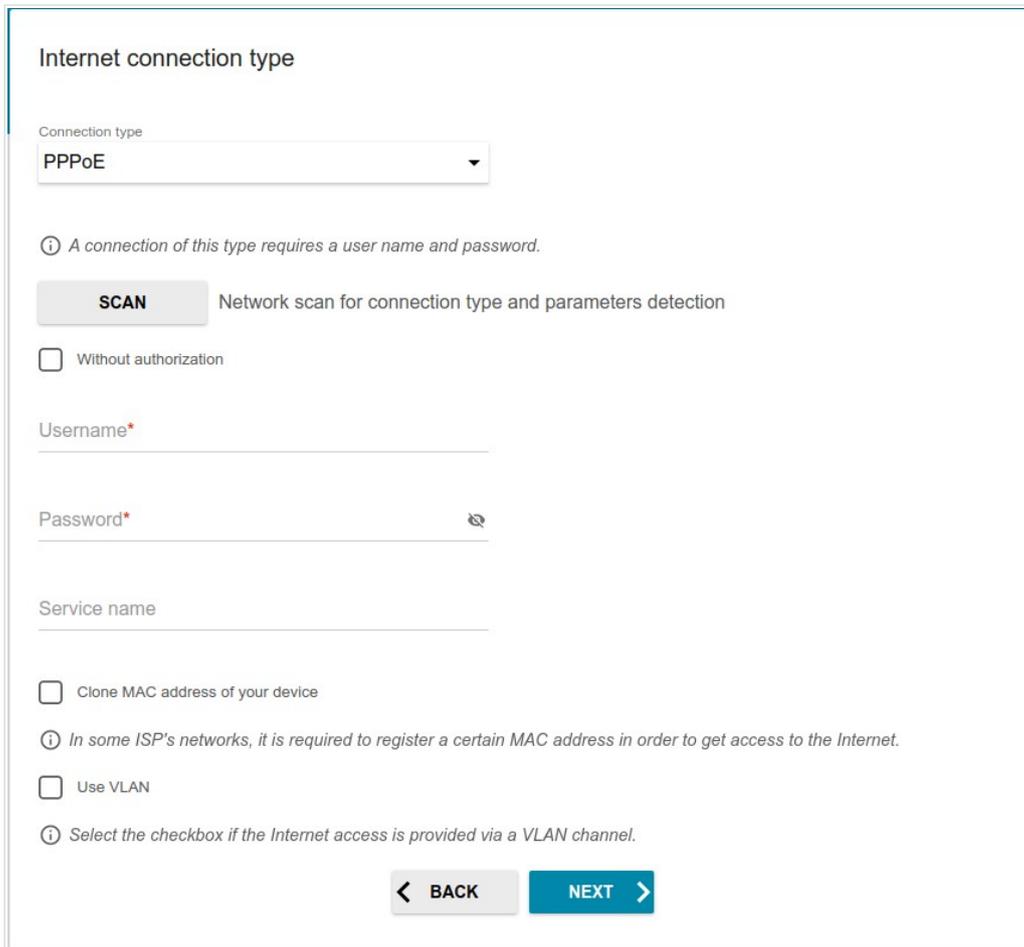
i Select the checkbox if the Internet access is provided via a VLAN channel.

< BACK **NEXT >**

Figure 46. The page for configuring Static IPv6 WAN connection.

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

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

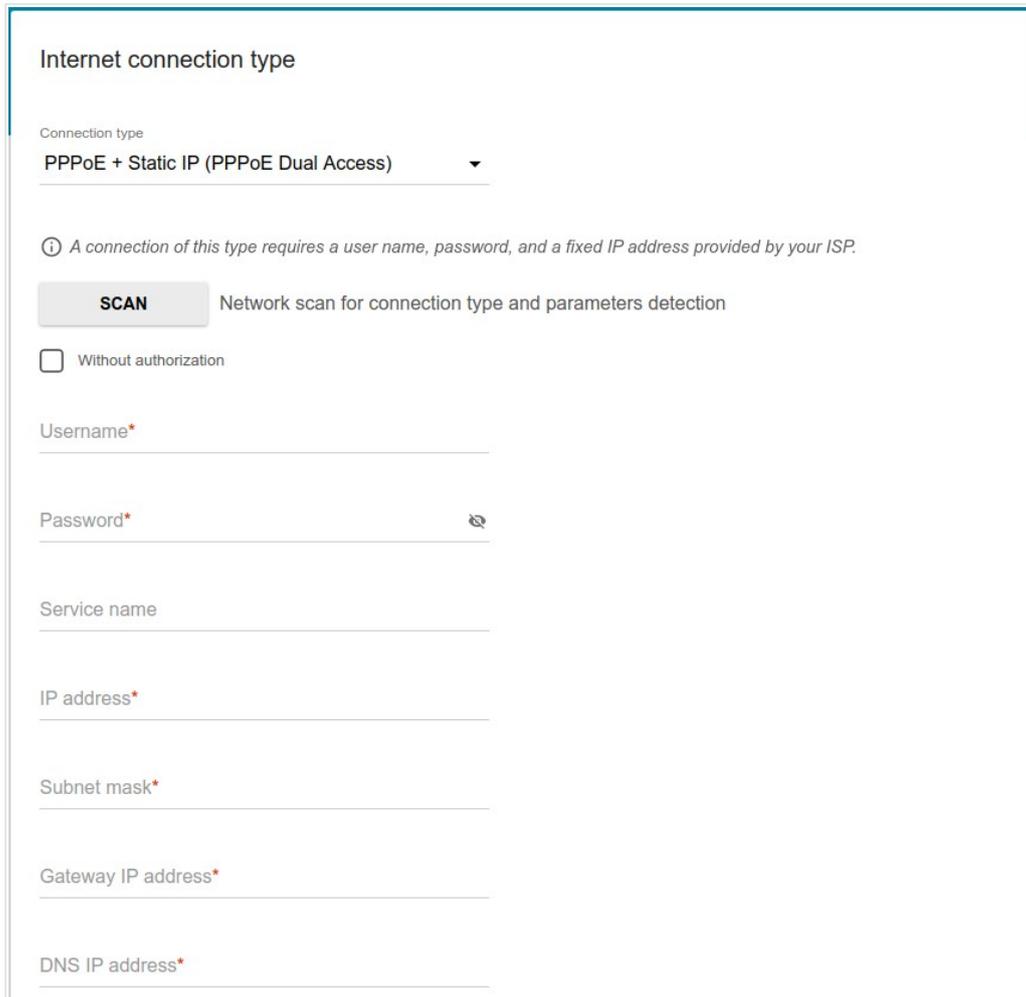


The screenshot shows a web-based configuration page titled "Internet connection type". At the top, there is a dropdown menu for "Connection type" with "PPPoE" selected. Below this, an information icon (i) is followed by the text: "A connection of this type requires a user name and password." There is a "SCAN" button with the text "Network scan for connection type and parameters detection" next to it. Below the scan button is a checkbox labeled "Without authorization". There are three input fields: "Username*" (with a red asterisk), "Password*" (with a red asterisk and a "Show" icon (eye with slash)), and "Service name". Below the input fields are two more checkboxes: "Clone MAC address of your device" and "Use VLAN". Below the "Use VLAN" checkbox is another information icon (i) with the text: "Select the checkbox if the Internet access is provided via a VLAN channel." At the bottom of the form, there are two buttons: "BACK" (with a left arrow) and "NEXT" (with a right arrow).

Figure 47. The page for configuring PPPoE WAN connection.

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

PPPoE + Static IP (PPPoE Dual Access) Connection



The screenshot shows a configuration page titled "Internet connection type". Under "Connection type", a dropdown menu is set to "PPPoE + Static IP (PPPoE Dual Access)". Below this is an information icon and a note: "A connection of this type requires a user name, password, and a fixed IP address provided by your ISP." There is a "SCAN" button with the text "Network scan for connection type and parameters detection" next to it. A checkbox labeled "Without authorization" is present and unchecked. Below are several input fields: "Username*", "Password*" (with a "Show" icon), "Service name", "IP address*", "Subnet mask*", "Gateway IP address*", and "DNS IP address*".

Figure 48. The page for configuring PPPoE + Static IP (PPPoE Dual Access) WAN connection.

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

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

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

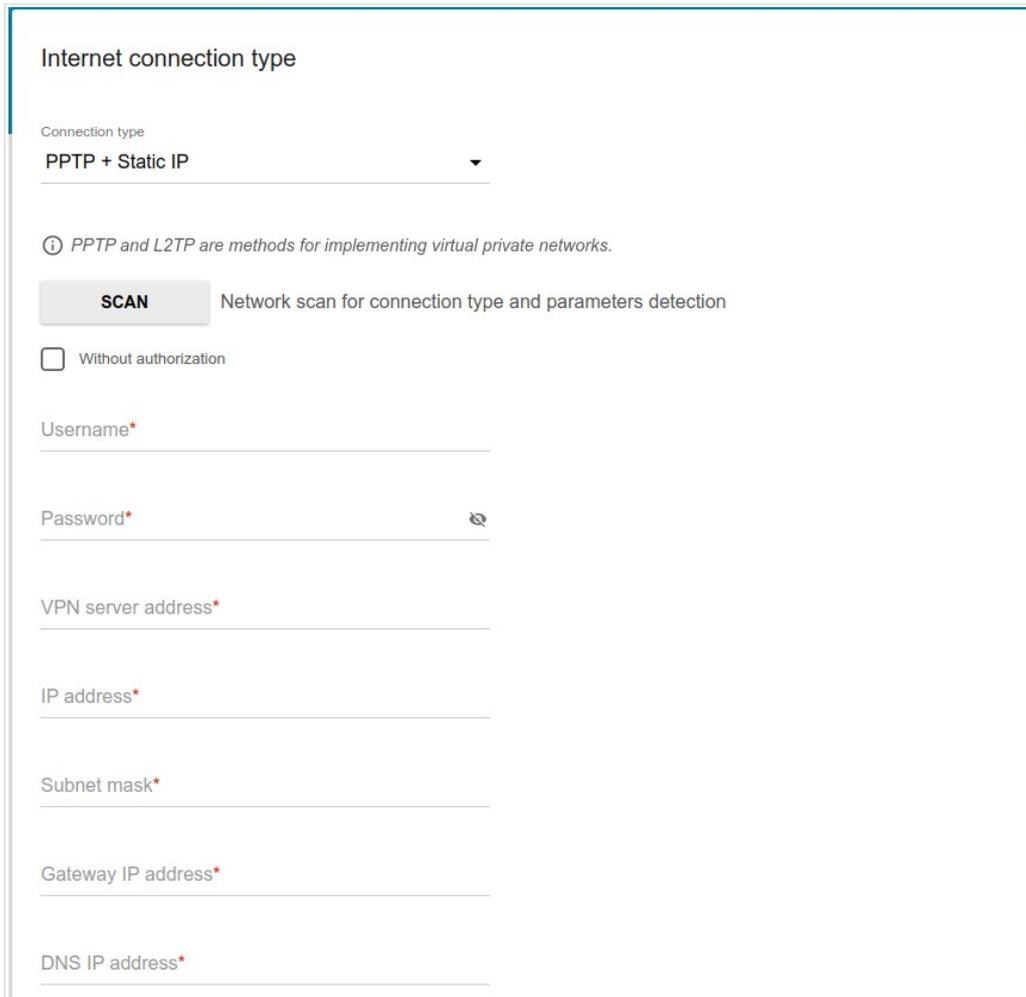
The screenshot shows a configuration page titled "Internet connection type". At the top, there is a dropdown menu labeled "Connection type" with "PPTP + Dynamic IP" selected. Below this is an information icon and the text "PPTP and L2TP are methods for implementing virtual private networks." A "SCAN" button is present with the text "Network scan for connection type and parameters detection". There is a checkbox labeled "Without authorization". Below that are three text input fields: "Username*", "Password*" (with a "Show" icon), and "VPN server address*". At the bottom, there are three checkboxes: "Clone MAC address of your device", "Use VLAN", and "Use IGMP" (which is checked). Each checkbox has an associated information icon and explanatory text. At the very bottom are "BACK" and "NEXT" buttons.

Figure 49. The page for configuring PPTP + Dynamic IP WAN connection.

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

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

PPTP + Static IP or L2TP + Static IP Connection



The screenshot shows a configuration page titled "Internet connection type". The "Connection type" dropdown menu is set to "PPTP + Static IP". Below this, there is an information icon and a note: "PPTP and L2TP are methods for implementing virtual private networks." A "SCAN" button is present with the text "Network scan for connection type and parameters detection". There is a checkbox labeled "Without authorization" which is currently unchecked. The form includes several input fields, each with an asterisk indicating it is required: "Username*", "Password*" (with a show/hide icon), "VPN server address*", "IP address*", "Subnet mask*", "Gateway IP address*", and "DNS IP address*".

Figure 50. The page for configuring PPTP + Static IP WAN connection.

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

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

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

Configuring Wireless Network

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

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

Wireless Network 2.4 GHz

Enable

Broadcast wireless network 2.4 GHz

Disabling broadcast does not influence the ability to connect to another Wi-Fi network as a client.

Network name*

my wi-fi

The number of characters should not exceed 32

Open network

Password*

.....

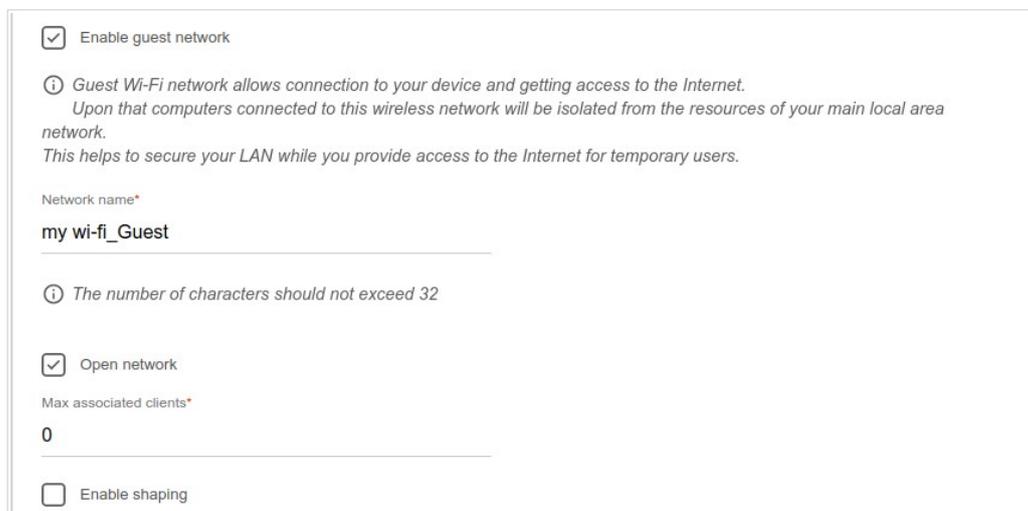
Password should be between 8 and 63 ASCII characters

USE *Use the same parameters as on the root access point.*

RESTORE *You can restore network name and security that was set before applying factory settings.*

Figure 51. The page for configuring the wireless network.

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



The screenshot shows a web-based configuration interface for a wireless network. At the top, there is a checked checkbox labeled 'Enable guest network'. Below this is a help icon (i) followed by the text: 'Guest Wi-Fi network allows connection to your device and getting access to the Internet. Upon that computers connected to this wireless network will be isolated from the resources of your main local area network. This helps to secure your LAN while you provide access to the Internet for temporary users.' Below the help text is a text input field for 'Network name*' with the value 'my wi-fi_Guest' entered. Underneath the input field is another help icon (i) with the text: 'The number of characters should not exceed 32'. Below this is another checked checkbox labeled 'Open network'. Underneath is a text input field for 'Max associated clients*' with the value '0' entered. At the bottom of the section is an unchecked checkbox labeled 'Enable shaping'.

Figure 52. The page for configuring the wireless network.

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

Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **Admin password** and **Password confirmation** fields. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.³

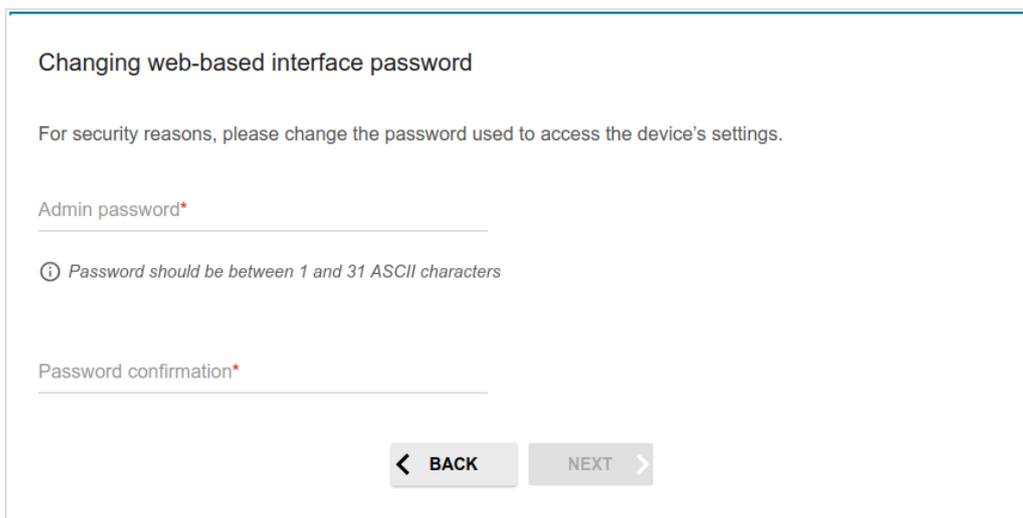


Figure 53. The page for changing the web-based interface password.

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

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

On the next page, check all specified settings.

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

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

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

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

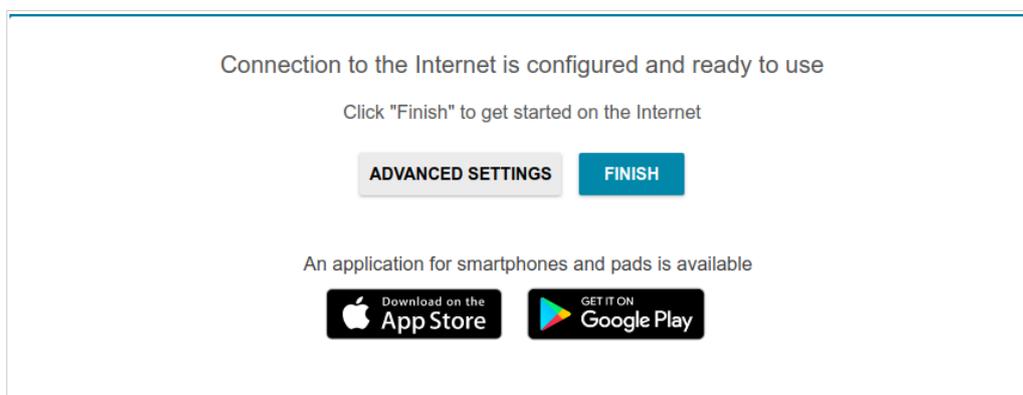


Figure 54. Checking the Internet availability.

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

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

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

To specify other settings, click the **ADVANCED SETTINGS** button. After clicking the **ADVANCED SETTINGS** button, the **Home** page opens (see the *Home Page* section, page 44).

Connection of Multimedia Devices

This section is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

The Multimedia Devices Connection Wizard helps to configure the LAN port of the access point for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DAP-600P in order to use these devices.

! Configuration of the LAN port is available only via Wi-Fi connection to DAP-600P.

To start the Wizard, on the **Home** page, select the **Connection of Multimedia Devices** section. If you need to select the port in order to use an additional device, left-click the **LAN1** port in the **LAN** section (the selected element will be marked with a frame). Then click the **APPLY** button.

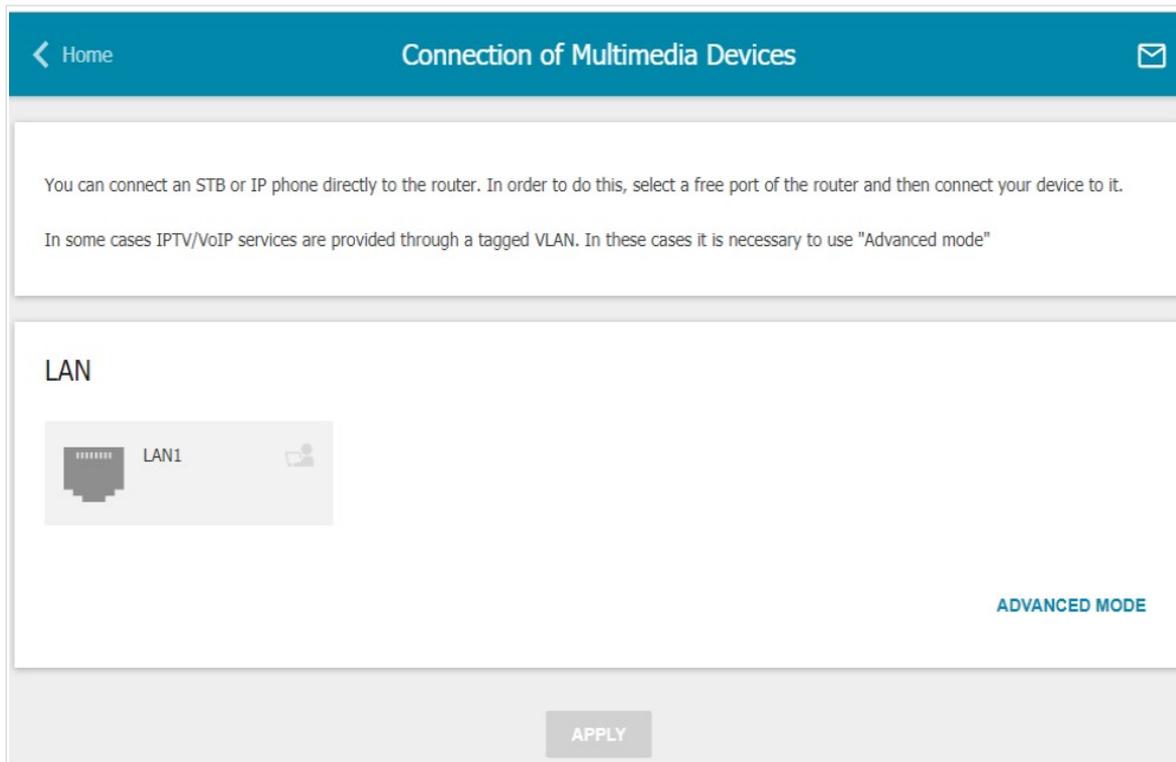


Figure 55. The Multimedia Devices Connection Wizard. The simplified mode.

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

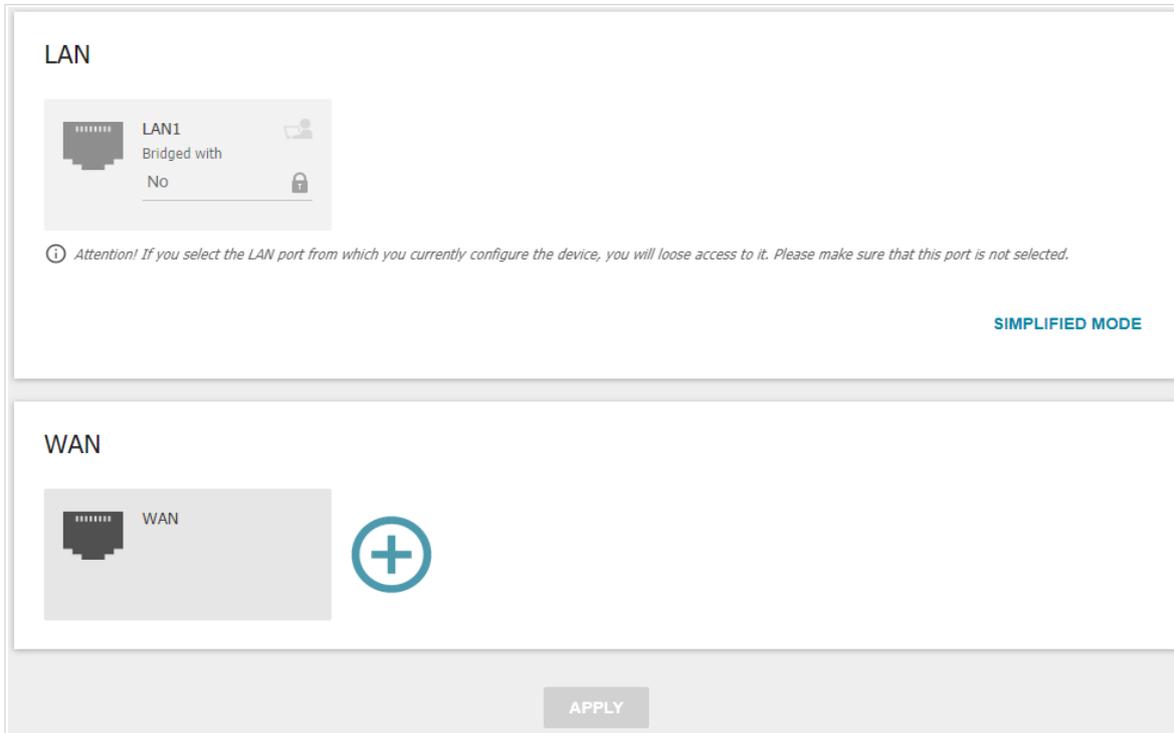


Figure 56. The Multimedia Devices Connection Wizard. The advanced mode.

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

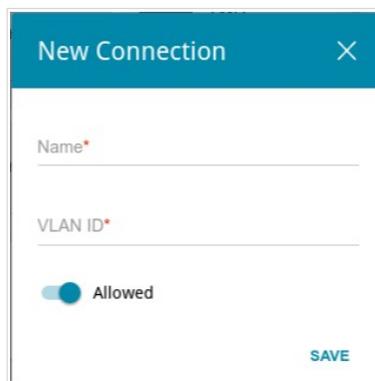


Figure 57. Adding a connection.

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 **LAN1** port, select the created connection. Click the **APPLY** button.

! The selected port cannot use the default connection to access the Internet.

To deselect the **LAN1** port in the simplified mode, left-click on it (the frame will disappear) and click the **APPLY** button.

To deselect the **LAN1** port in the advanced mode, select the **No** value from the **Bridged with** drop-down list. Then in the **WAN** section, select the connection via VLAN which will not be used any longer and click the **DELETE** button. Then click the **APPLY** button.

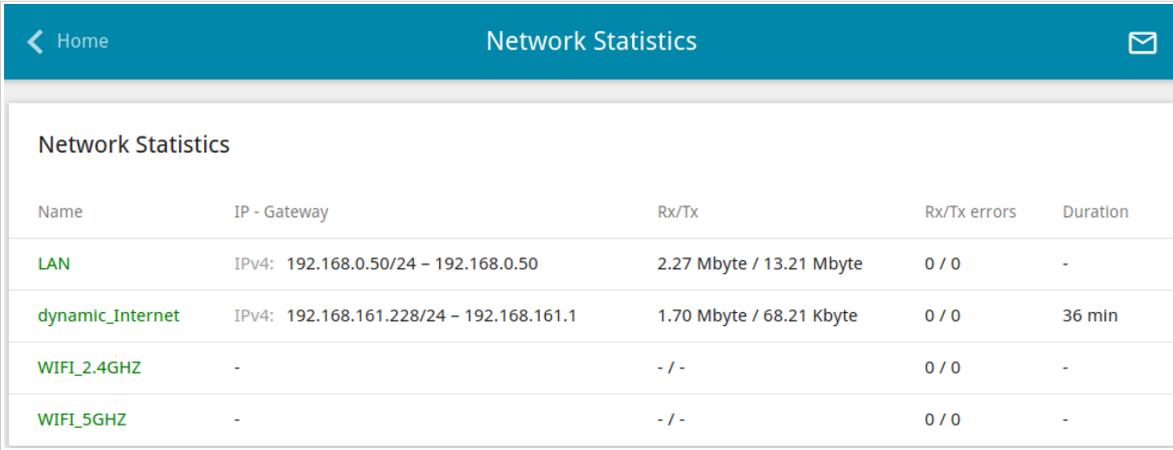
Statistics

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

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

Network Statistics

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



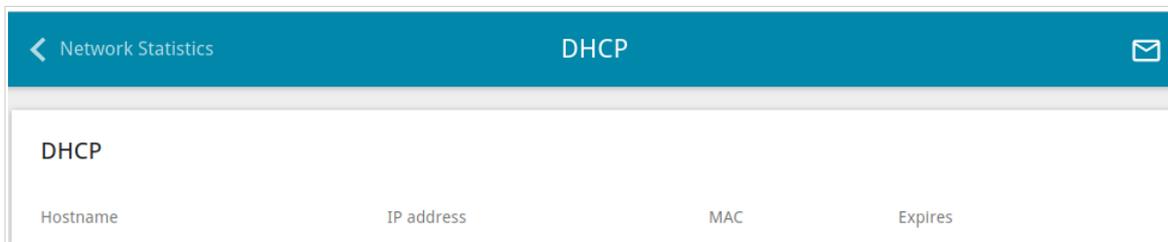
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.50/24 – 192.168.0.50	2.27 Mbyte / 13.21 Mbyte	0 / 0	-
dynamic_Internet	IPv4: 192.168.161.228/24 – 192.168.161.1	1.70 Mbyte / 68.21 Kbyte	0 / 0	36 min
WIFI_2.4GHZ	-	- / -	0 / 0	-
WIFI_5GHZ	-	- / -	0 / 0	-

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

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

DHCP

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

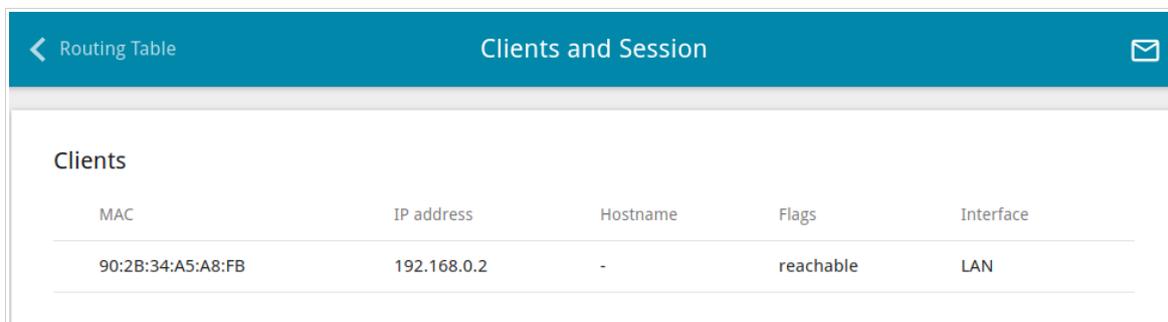


DHCP			
Hostname	IP address	MAC	Expires

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

Clients and Session

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



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

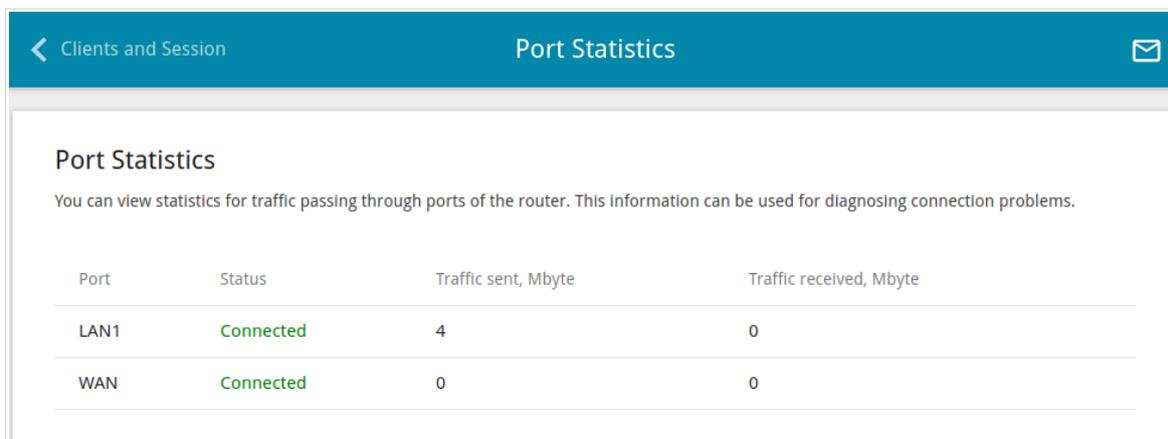
Figure 60. The **Statistics / Clients and Session** page.

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

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

Port Statistics

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



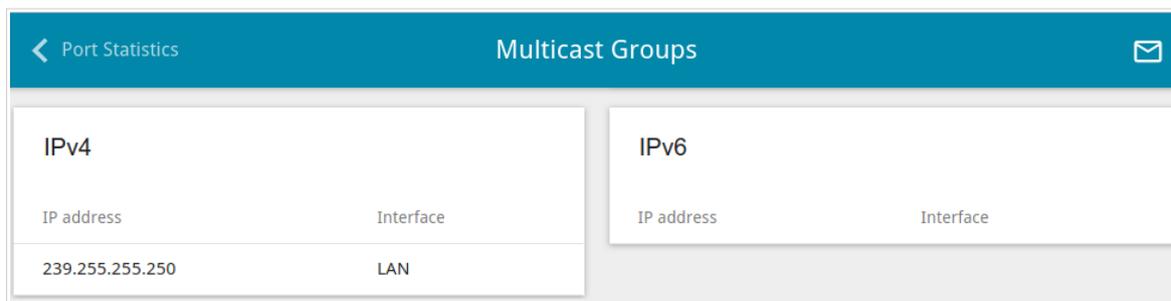
Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte
LAN1	Connected	4	0
WAN	Connected	0	0

Figure 61. The **Statistics / Port Statistics** page.

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

Multicast Groups

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



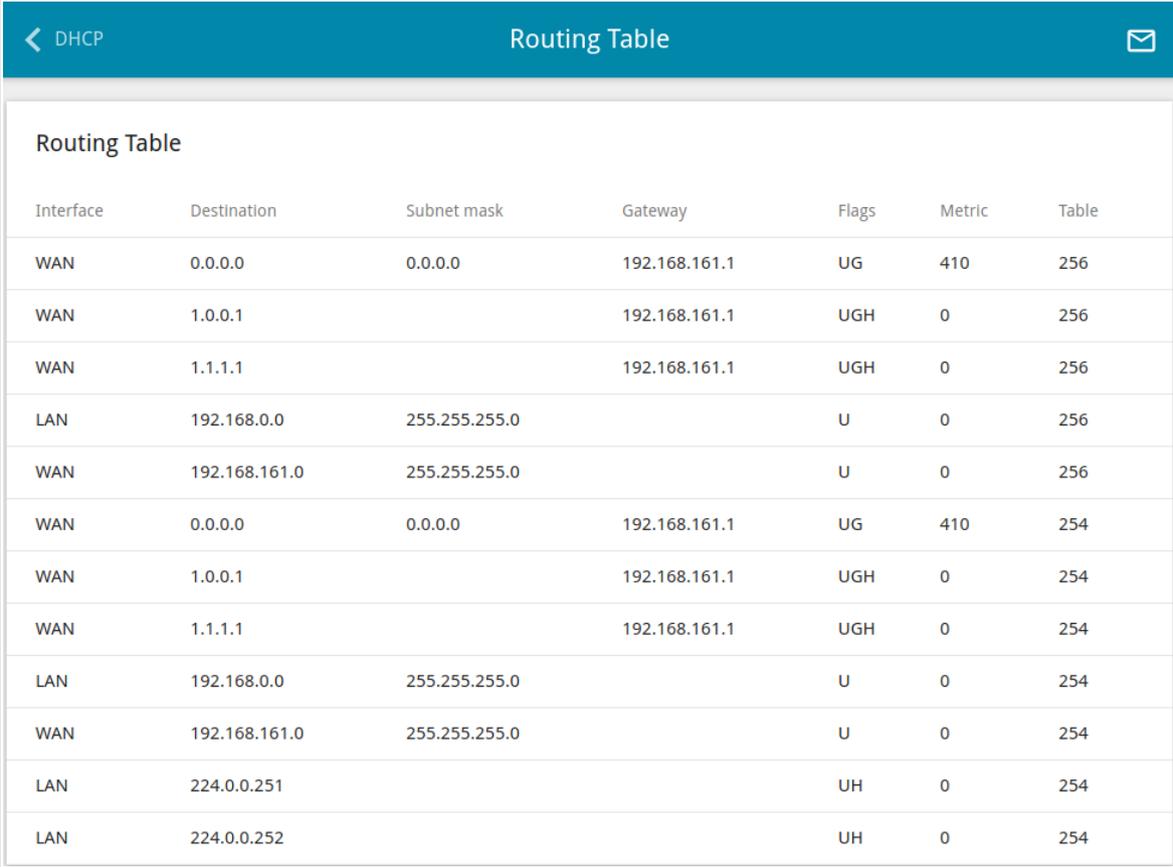
IPv4		IPv6	
IP address	Interface	IP address	Interface
239.255.255.250	LAN		

Figure 62. The **Statistics / Multicast Groups** page.

Routing Table

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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



Interface	Destination	Subnet mask	Gateway	Flags	Metric	Table
WAN	0.0.0.0	0.0.0.0	192.168.161.1	UG	410	256
WAN	1.0.0.1		192.168.161.1	UGH	0	256
WAN	1.1.1.1		192.168.161.1	UGH	0	256
LAN	192.168.0.0	255.255.255.0		U	0	256
WAN	192.168.161.0	255.255.255.0		U	0	256
WAN	0.0.0.0	0.0.0.0	192.168.161.1	UG	410	254
WAN	1.0.0.1		192.168.161.1	UGH	0	254
WAN	1.1.1.1		192.168.161.1	UGH	0	254
LAN	192.168.0.0	255.255.255.0		U	0	254
WAN	192.168.161.0	255.255.255.0		U	0	254
LAN	224.0.0.251			UH	0	254
LAN	224.0.0.252			UH	0	254

Figure 63. The **Statistics / Routing Table** page.

Connections Setup

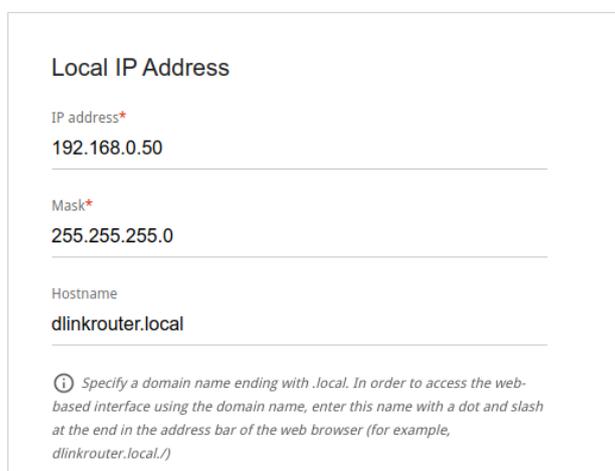
In this menu section you can configure basic parameters of the access point's local area network and connection to the Internet (create one or several WAN connections and define rules for their use).

LAN

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

IPv4

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



The screenshot shows a configuration form titled "Local IP Address". It contains three input fields: "IP address*" with the value "192.168.0.50", "Mask*" with the value "255.255.255.0", and "Hostname" with the value "dlinkrouter.local". Below the fields is a note: "Specify a domain name ending with .local. In order to access the web-based interface using the domain name, enter this name with a dot and slash at the end in the address bar of the web browser (for example, dlinkrouter.local/)." The form is enclosed in a light gray border.

Figure 64. Configuring the local interface. The **IPv4** tab. The **Local IP Address** section.

Parameter	Description
Local IP Address	
Mode of local IP address assignment	<p>Available if the Access point or Repeater mode was selected in the Initial Configuration Wizard.</p> <p>Select the needed value from the drop-down list.</p> <ul style="list-style-type: none"> • Static: The IPv4 address, subnet mask, and the gateway IP address are assigned manually. • Dynamic: The access point automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.
IP address	The IPv4 address of the access point in the local subnet. By default, the following value is specified: 192.168.0.50 .
Mask	The mask of the local subnet. By default, the following value is specified: 255.255.255.0 .
Gateway IP address	<p>Available if the Access point or Repeater mode was selected in the Initial Configuration Wizard.</p> <p>The gateway IPv4 address which is used by the access point to connect to the Internet (e.g., for synchronizing the system time with an NTP server). <i>Optional</i>.</p>
Hostname	The name of the device assigned to its IPv4 address in the local subnet.

Dynamic IP Addresses

Mode of dynamic IP address assignment
 Server ▼

Start IP*
 192.168.0.100

End IP*
 192.168.0.199

Lease time (in minutes)*
 1440

DNS relay

Figure 65. Configuring the local interface. The IPv4 tab. The Dynamic IP Addresses section.

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

Parameter	Description
Option 82 Circuit ID Option 82 Remote ID Option 82 Subscriber ID	<p>Available if the Router or WISP Repeater mode was selected in the Initial Configuration Wizard.</p> <p>The value of the relevant field of DHCP option 82. Do not fill in the fields unless your ISP or the administrator of the external DHCP server provided these values.</p>

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

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



Figure 66. Configuring the local interface. The **IPv4** tab. The section for configuring DHCP options.

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

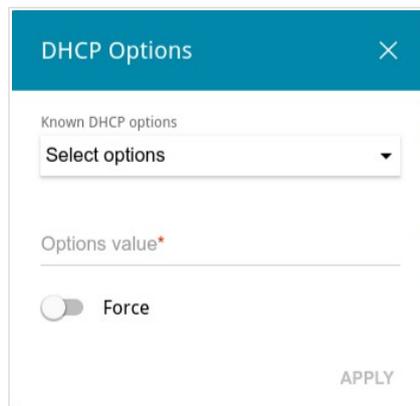


Figure 67. Configuring the local interface. The **IPv4** tab. The window for configuring a DHCP option.

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

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

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

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

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

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

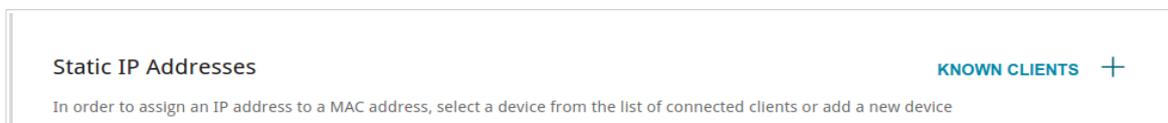


Figure 68. Configuring the local interface. The **IPv4** tab. The section for creating MAC-IPv4 pairs.

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

To create MAC-IPv4 pairs for the devices connected to the access point at the moment, click the **KNOWN CLIENTS** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

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

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

If needed, you can add your own address resource records. To do this, click the **ADD** button () in the **Hosts** section (available if the **Router** or **WISP Repeater** mode was selected in the *Initial Configuration Wizard*).

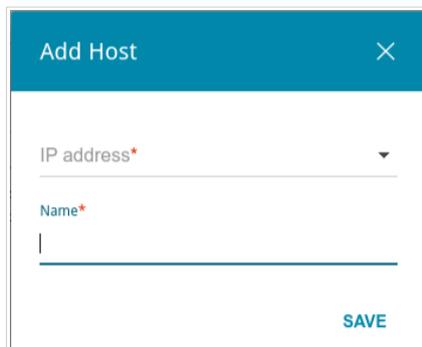


Figure 69. Configuring the local interface. The **IPv4** tab. The window for adding a DNS record.

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

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

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

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

IPv6

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

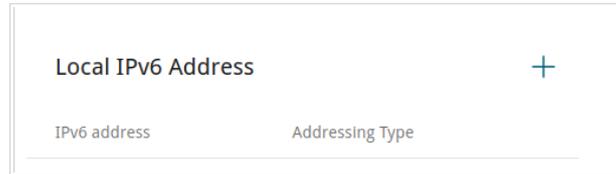


Figure 70. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.

To add an IPv6 address of the access point, click the **ADD** button (+). To change the IPv6 address of the access point, select it in the table.

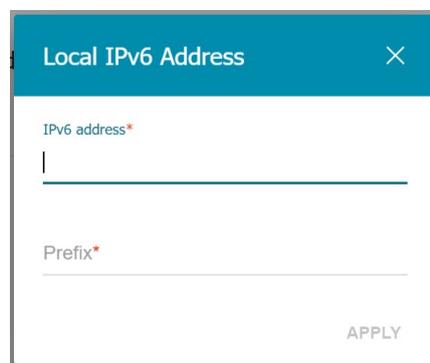


Figure 71. Configuring the local interface. The **IPv6** tab. The window for adding an IPv6 address.

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

Local IPv6 Address	
IPv6 address	The IPv6 address of the access point in the local subnet. By default, the following value is specified: fd00::1 .
Prefix	The length of the prefix subnet. By default, the value 64 is specified.
Gateway IPv6 address	<i>Available if the Access point or Repeater mode was selected in the Initial Configuration Wizard.</i> The gateway IPv6 address which is used by the access point to connect to the Internet (e.g., for synchronizing the system time with an NTP server). <i>Optional.</i>

Click the **APPLY** button.

To remove the IPv6 address, select it in the table and click the **DELETE** button in the opened window. Then click the **APPLY** button.

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

The screenshot shows the 'Dynamic IPv6 Addresses' configuration interface. At the top, the title 'Dynamic IPv6 Addresses' is displayed. Below it, there is a dropdown menu for 'Mode of dynamic IPv6 address assignment' which is currently set to 'Stateful'. Underneath, the 'Address range' is configured with two input fields: the first contains '2' and the second contains '64', separated by a hyphen. Above each of these fields is the text '(1-FFFF)*'. At the bottom, the 'Lease time (in minutes)*' is set to '5'.

Figure 72. Configuring the local interface. The IPv6 tab. The **Dynamic IPv6 Addresses** section.

Parameter	Description
Dynamic IPv6 Addresses	
Mode of dynamic IPv6 address assignment	Select the needed value from the drop-down list. <ul style="list-style-type: none"> • Disable: Clients' IPv6 addresses are assigned manually. • Stateful: The built-in DHCPv6 server of the access point allocates addresses from the range specified in the Address range fields. Also when this value is selected, the Static IP Addresses and Hosts sections are displayed on the tab. • Stateless: Clients themselves configure IPv6 addresses using the prefix.
Address range	The start and the end values for the latest hexet (16 bit) of the range of IPv6 addresses which the DHCPv6 server distributes to clients.
Lease time	The lifetime of IPv6 addresses provided to clients.

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

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

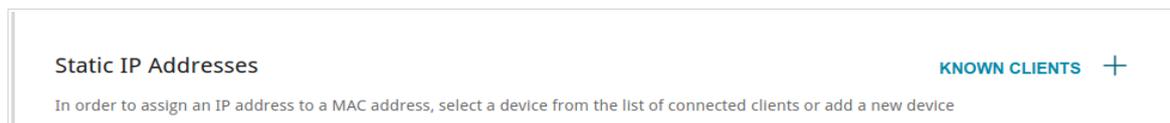


Figure 73. Configuring the local interface. The **IPv6** tab. The section for creating MAC-IPv6 pairs.

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

To create MAC-IPv6 pairs for the devices connected to the access point at the moment, click the **KNOWN CLIENTS** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

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

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

If needed, you can add your own address resource records. To do this, click the **ADD** button () in the **Hosts** section (available if the **Router** or **WISP Repeater** mode was selected in the *Initial Configuration Wizard*).

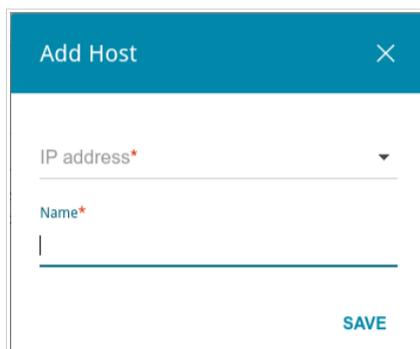


Figure 74. Configuring the local interface. The **IPv6** tab. The window for adding a DNS record.

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

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

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

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

WAN

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

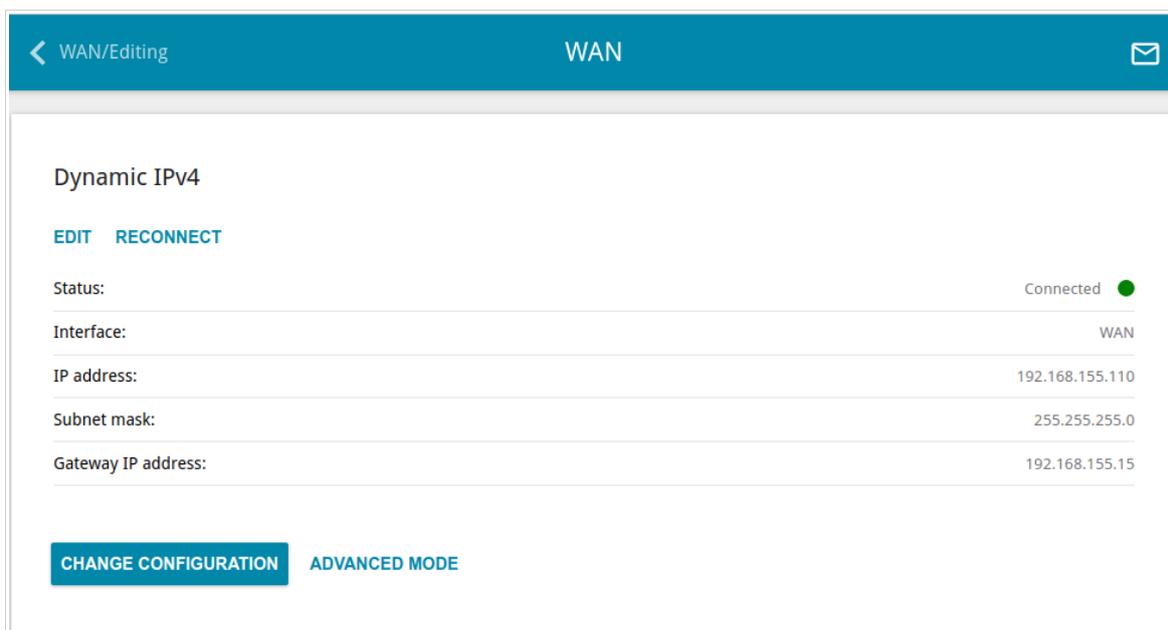


Figure 75. The **Connections Setup / WAN** page. The simplified mode.

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

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

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

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

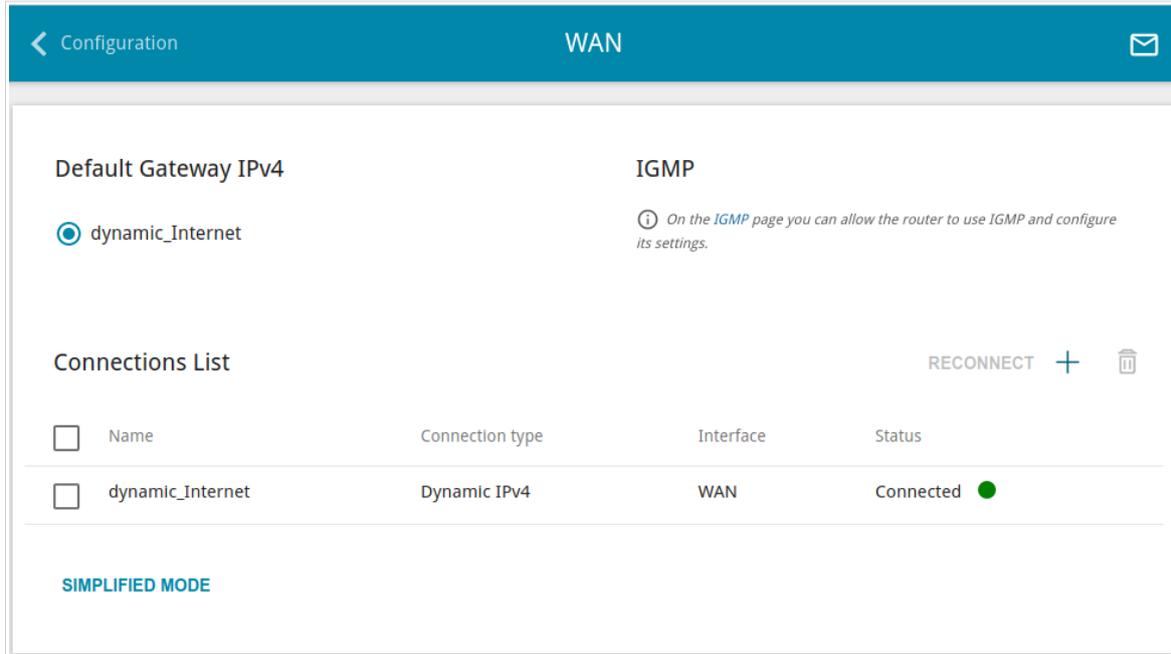


Figure 76. The **Connections Setup / WAN** page. The advanced mode.

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

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

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

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

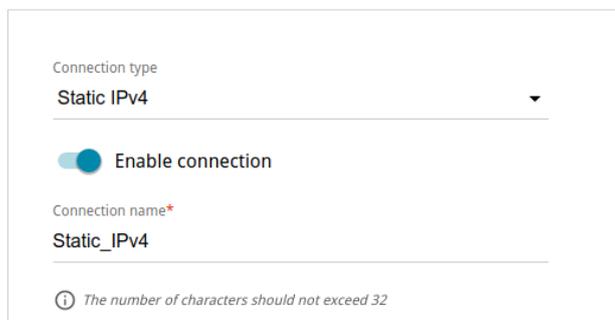
To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP** link (for the description of the page, see the **IGMP** section, page 178).

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

To return to the simplified mode, click the **SIMPLIFIED MODE** button.

Creating Dynamic IPv4 or Static IPv4 WAN Connection

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



The screenshot shows a web interface for creating a connection. It features a 'Connection type' dropdown menu with 'Static IPv4' selected. Below this is a toggle switch labeled 'Enable connection' which is turned on. Underneath is a text input field for 'Connection name*' containing 'Static_IPv4'. A small information icon and a note at the bottom state: 'The number of characters should not exceed 32'.

Figure 77. The page for creating a new **Static IPv4** connection. Selecting a connection type.

Parameter	Description
Interface	<p><i>The drop-down list is displayed if additional WAN interfaces are specified in the system (see the VLAN section, page 159).</i></p> <p>A physical or virtual WAN interface to which the new connection will be assigned.</p>
Enable connection	<p>Move the switch to the right to enable the connection.</p> <p>Move the switch to the left to disable the connection.</p>
Connection name	<p><i>Available for the advanced mode only.</i></p> <p>A name for the connection for easier identification.</p>

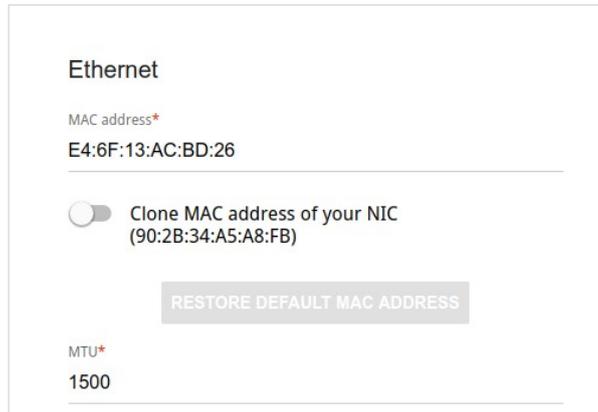


Figure 78. The page for creating a new **Static IPv4** connection. The **Ethernet** section.

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

IPv4

IP address*

Subnet mask*

Gateway IP address*

Primary DNS*

Secondary DNS

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

Figure 79. The page for creating a new **Static IPv4** connection. The **IPv4** section.

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



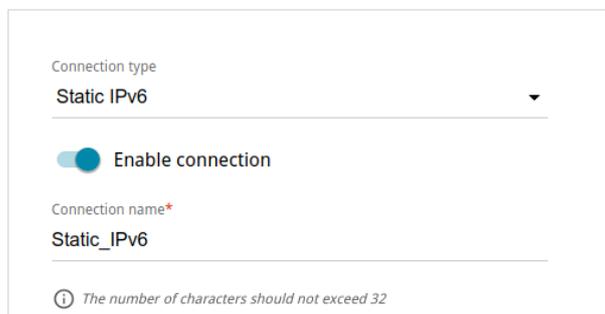
Figure 80. The page for creating a new **Static IPv4** connection. The **Miscellaneous** section.

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.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the access point responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

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

Creating Dynamic IPv6 or Static IPv6 WAN Connection

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



The screenshot shows a web form for creating a connection. It includes a dropdown menu for 'Connection type' with 'Static IPv6' selected. Below it is a toggle switch for 'Enable connection' which is turned on. There is a text input field for 'Connection name*' containing 'Static_IPv6'. A small information icon and note at the bottom state: 'The number of characters should not exceed 32'.

Figure 81. The page for creating a new **Static IPv6** connection. Selecting a connection type.

Parameter	Description
Interface	<p><i>The drop-down list is displayed if additional WAN interfaces are specified in the system (see the VLAN section, page 159).</i></p> <p>A physical or virtual WAN interface to which the new connection will be assigned.</p>
Enable connection	<p>Move the switch to the right to enable the connection.</p> <p>Move the switch to the left to disable the connection.</p>
Connection name	<p><i>Available for the advanced mode only.</i></p> <p>A name for the connection for easier identification.</p>



Figure 82. The page for creating a new **Static IPv6** connection. The **Ethernet** section.

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

IPv6

IPv6 address*

Prefix*

Gateway IPv6 address*

Primary IPv6 DNS server*

Secondary IPv6 DNS server

Figure 83. The page for creating a new **Static IPv6** connection. The **IPv6** section.

Parameter	Description
IPv6	
<i>For Static IPv6 type</i>	
IPv6 address	Enter an IPv6 address for this WAN connection.
Prefix	The length of the subnet prefix. The value 64 is used usually.
Gateway IPv6 address	Enter an IPv6 address of the gateway used by this WAN connection.
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
<i>For Dynamic IPv6 type</i>	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the Automatically value.
Enable prefix delegation	Move the switch to the right if it is necessary that the access point requests a prefix to configure IPv6 addresses for the local network from a delegating router.
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.
<div style="border: 1px solid #ccc; padding: 10px; width: fit-content; margin: 0 auto;"> <p>Miscellaneous</p> <p><input type="checkbox"/> RIPng</p> <p><input type="checkbox"/> Ping</p> </div>	

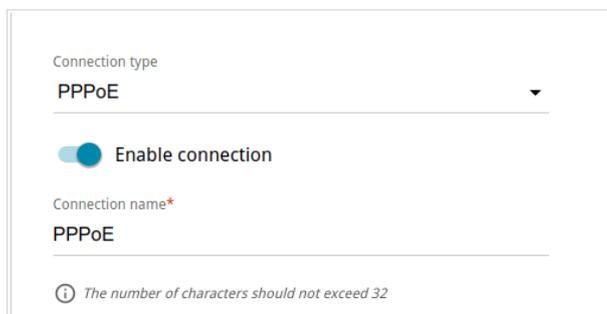
Figure 84. The page for creating a new **Static IPv6** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
RIPng	Move the switch to the right to allow using RIPng for this connection.
Ping	If the switch is moved to the right, the access point responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

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

Creating PPPoE WAN Connection

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



Connection type
PPPoE

Enable connection

Connection name*
PPPoE

The number of characters should not exceed 32

Figure 85. The page for creating a new **PPPoE** connection. Selecting a connection type.

Parameter	Description
Interface	<p><i>The drop-down list is displayed if additional WAN interfaces are specified in the system (see the VLAN section, page 159).</i></p> <p>A physical or virtual WAN interface to which the new connection will be assigned.</p>
Enable connection	<p>Move the switch to the right to enable the connection.</p> <p>Move the switch to the left to disable the connection.</p>
Connection name	<p><i>Available for the advanced mode only.</i></p> <p>A name for the connection for easier identification.</p>

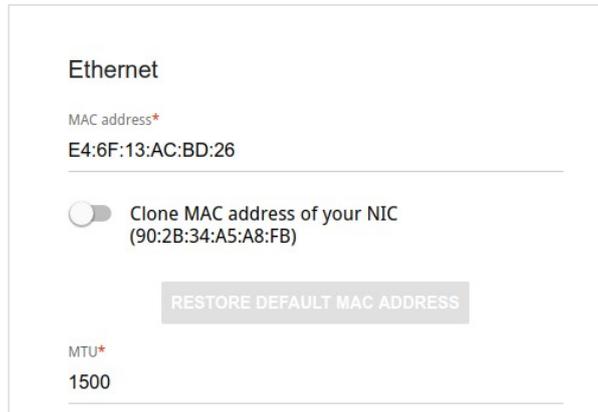


Figure 86. The page for creating a new PPPoE connection. The Ethernet section.

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

PPP

Without authorization

Username*

Password* 

Service name

MTU*
1492

Authentication protocol
AUTO ▼

Encryption protocol
No encryption ▼

Keep Alive

LCP interval*
30

LCP fails*
3

Dial on demand

Maximum idle time (in seconds)
0 

Extra options

Static IP address

PPP debug

Figure 87. 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.

Parameter	Description
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.
Encryption protocol	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encryption: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP or MS-CHAPV2 value is selected from the Authentication protocol drop-down list.</p>
Keep Alive	Move the switch to the right if you want the access point 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 access point 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. <i>Optional.</i>
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 88. 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.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the access point responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

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

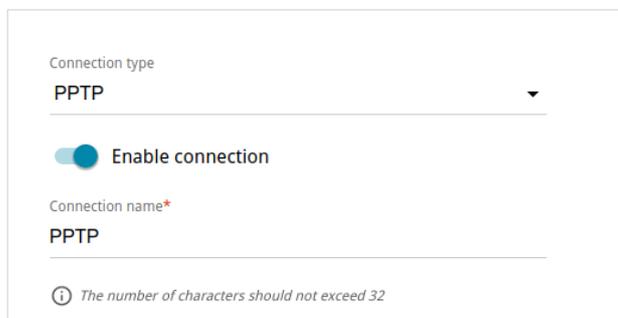
After clicking the button, the window for creating an additional connection opens.

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

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

Creating PPTP, L2TP, or L2TP over IPsec WAN Connection

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



The screenshot shows a web interface for creating a connection. It features a dropdown menu for 'Connection type' with 'PPTP' selected. Below this is a toggle switch for 'Enable connection' which is turned on. A text input field for 'Connection name*' contains 'PPTP'. A small information icon and text at the bottom indicate that the number of characters should not exceed 32.

Figure 89. The page for creating a new **PPTP** connection. Selecting a connection type.

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

PPP

Without authorization

Username*

Password* 

VPN server address*

MTU*
1456

Authentication protocol
AUTO ▼

Encryption protocol
No encryption ▼

Keep Alive

LCP interval*
30

LCP fails*
3

Dial on demand

Maximum idle time (in seconds)
0 

Extra options

Static IP address

PPP debug

Figure 90. 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.

Parameter	Description
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.
Encryption protocol	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encryption: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP or MS-CHAPV2 value is selected from the Authentication protocol drop-down list.</p>
Keep Alive	Move the switch to the right if you want the access point 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 access point 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. <i>Optional.</i>
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.

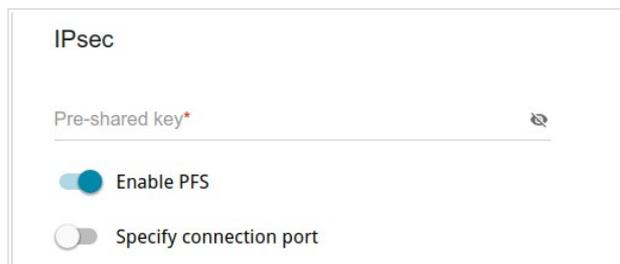


Figure 91. The page for creating a new **L2TP over IPsec** connection. The **IPsec** section.



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

Parameter	Description
IPsec (for the L2TP over IPsec type only)	
Pre-shared key	A key for mutual authentication of the parties. Click the Show icon (👁) to display the entered key.
Enable PFS	Move the switch to the right to enable the PFS option (<i>Perfect Forward Secrecy</i>). If the switch is moved to the right, a new encryption key exchange will be used upon establishing the IPsec tunnel. This option enhances the security level of data transfer, but increases the load on DAP-600P.
Specify connection port	Move the switch to the right to change the port used for data exchange with the other party enter the needed value in the Port field displayed. By default, the value 1701 is specified.



Figure 92. 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.
Ping	<i>For the PPTP and L2TP types only.</i> If the switch is moved to the right, the access point responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

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.

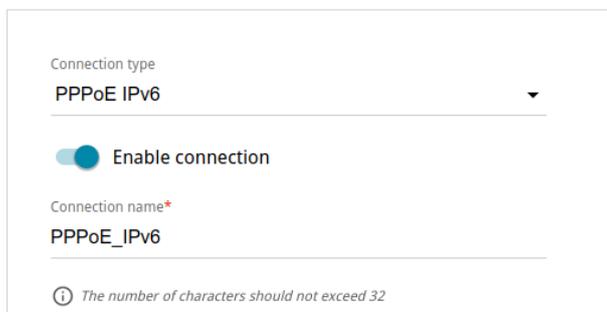
If you have already configured the connection to the Internet and you want to use this WAN connection only to connect to the virtual private network, select the **to the virtual private network** choice of the radio button.

Click the **OK** button.

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

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

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



Connection type
PPPoE IPv6

Enable connection

Connection name*
PPPoE_IPv6

The number of characters should not exceed 32

Figure 93. The page for creating a new **PPPoE IPv6** connection. Selecting a connection type.

Parameter	Description
Interface	<p>The drop-down list is displayed if additional WAN interfaces are specified in the system (see the VLAN section, page 159).</p> <p>A physical or virtual WAN interface to which the new connection will be assigned.</p>
Enable connection	<p>Move the switch to the right to enable the connection.</p> <p>Move the switch to the left to disable the connection.</p>
Connection name	<p>Available for the advanced mode only.</p> <p>A name for the connection for easier identification.</p>



Figure 94. The page for creating a new PPPoE IPv6 connection. The Ethernet section.

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

PPP

Without authorization

Username*

Password* 

Service name

MTU*
1492

Authentication protocol
AUTO ▼

Encryption protocol
No encryption ▼

Keep Alive

LCP interval*
30

LCP fails*
3

Dial on demand

Maximum idle time (in seconds)
0 

Extra options

Static IP address

PPP debug

Figure 95. 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.

Parameter	Description
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.
Encryption protocol	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encryption: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP or MS-CHAPV2 value is selected from the Authentication protocol drop-down list.</p>
Keep Alive	Move the switch to the right if you want the access point 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 access point 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. <i>Optional.</i>
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.

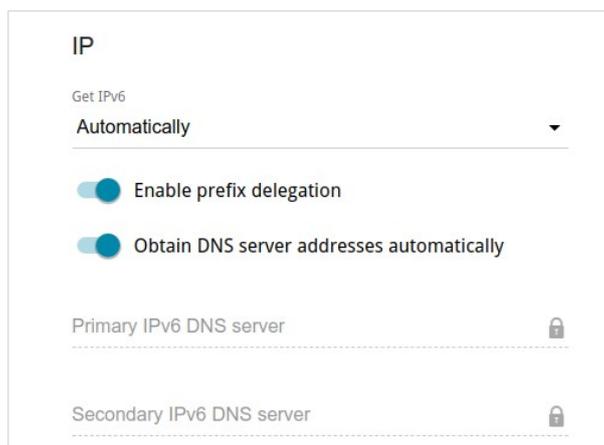


Figure 96. The page for creating a new PPPoE Pv6 connection. The IP section.

Parameter	Description
IP	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the Automatically value.
Enable prefix delegation	Move the switch to the right if it is necessary that the access point requests a prefix to configure IPv6 addresses for the local network from a delegating router.
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.

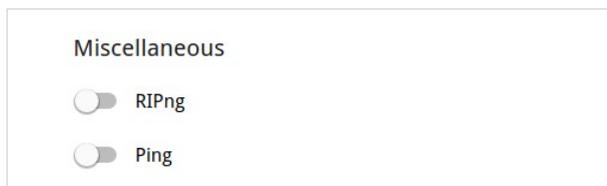


Figure 97. The page for creating a new **PPPoE IPv6** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
NAT	<p><i>For the PPPoE Dual Stack type only.</i></p> <p>If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.</p>
RIP	<p><i>For the PPPoE Dual Stack type only.</i></p> <p>Move the switch to the right to allow using RIP for this connection.</p>
RIPng	<p>Move the switch to the right to allow using RIPng for this connection.</p>
Ping	<p>If the switch is moved to the right, the access point responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.</p>

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

WAN Reservation

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

Figure 98. The **Connections Setup / WAN Reservation** page.

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

Parameter	Description
Basic connection	From the drop-down list, select a WAN connection which will be used as the main one.
Backup connections	Click the ADD CONNECTION button and, from the drop-down list displayed, select a WAN connection which will be used as the reserve one. You can add several WAN connections . To remove a reserve connection from the list, click the Delete icon (×) in the line of the connection.

Parameter	Description
Check interval	<p>A time period (in seconds) between regular checks of the main connection status. By default, the value 30 is specified. The value of this field should be higher than product of Timeout check and Number of checks fields values.</p> <p>Several attempts are sent to check the status. After a successful attempt the access point keeps using the main connection. After several failed attempts a reserve connection is enabled.</p>
Timeout check	<p>A time period (in milliseconds) for one attempt to check the status of the main connection. By default, the value 1000 is specified.</p>
Number of checks	<p>A number of failed attempts to check the status of the main connection after which a reserve connection is enabled.</p>
Test hosts	<p>An IP address that the access point will check for availability via ICMP ping mechanism.</p> <p>Click the ADD HOST button, and in the line displayed, enter an IP address or leave values suggested by the access point.</p> <p>To remove an IP address from the list, click the Delete icon (✕) in the line of the address.</p>

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 access point and configure the basic and additional wireless networks. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

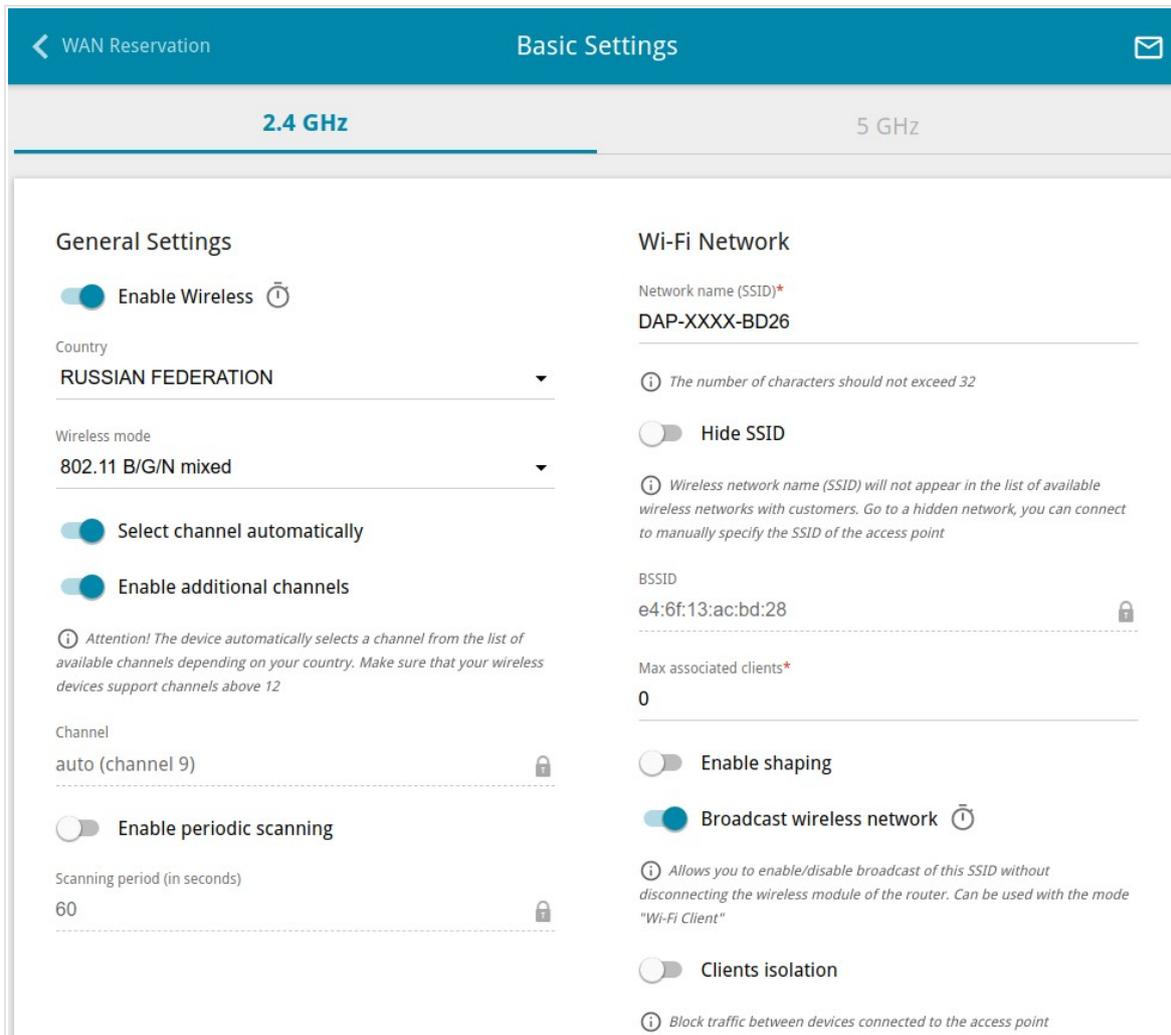


Figure 99. Basic settings of the wireless LAN in the 2.4GHz band.

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

Parameter	Description
<p>Enable Wireless</p>	<p>To enable Wi-Fi connection, move the switch to the right.</p> <p>To disable Wi-Fi connection, move the switch to the left.</p> <p>To enable/disable Wi-Fi connection on a schedule, click the Set schedule button (). In the opened window, you can create a new schedule (see the <i>Schedule</i> section, page 207) or use the existing one. Existing schedules are displayed in the Interval of execution drop-down list in the simplified mode.</p> <p>To enable Wi-Fi connection at the time specified in the schedule and disable it at the other time, select the Enable value from the Action for rule upon activation of schedule drop-down list and click the SAVE button.</p> <p>To disable Wi-Fi connection at the time specified in the schedule and enable it at the other time, select the Disable value from the Action for rule upon activation of schedule drop-down list and click the SAVE button.</p> <p>To change or delete the schedule, click the Set schedule button (). In the opened window, change the parameters and click the SAVE button or click the DELETE FROM SCHEDULE button.</p>
<p>Country</p>	<p>The country you are in. Select a value from the drop-down list.</p>
<p>Wireless mode</p>	<p>Operating mode of the wireless network of the access point. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.</p>
<p>Select channel automatically</p>	<p>Move the switch to the right to let the access point itself choose the channel with the least interference.</p>
<p>Enable additional channels</p>	<p>If the switch is moved to the left, the device automatically selects one of available standard channels. To use additional channels (the 12th and 13th – in the 2.4 GHz band, the 100th and higher – in the 5 GHz band), move the switch to the right.</p>
<p>Channel</p>	<p>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).</p>
<p>Enable periodic scanning</p>	<p>Move the switch to the right to let the access point 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.</p>

Parameter	Description
Scanning period	Specify a period of time (in seconds) after which the access point rescans channels.

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

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

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

The screenshot shows the 'Add Wi-Fi Network' configuration page. The page has a blue header with a back arrow, 'Basic Settings', 'Add Wi-Fi Network', and an envelope icon. The main content is split into two columns:

- Wi-Fi Network:**
 - Network name (SSID)*: DAP-XXXX-BD26.2
 - Hide SSID:
 - Max associated clients*: 0
 - Enable shaping:
 - Broadcast wireless network:
 - Clients isolation:
 - Enable guest network:
- Security Settings:**
 - Network authentication: WPA2-PSK
 - Password PSK*: [masked]
 - Encryption type*: AES
 - Group key update interval (in seconds)*: 3600

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

Figure 100. 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 (Mbit/s). Move the switch to the left not to limit the maximum bandwidth.

Parameter	Description
<p>Broadcast wireless network</p>	<p>If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DAP-600P can connect to another access point as a wireless client.</p> <p>To enable/disable broadcasting on a schedule, click the Set schedule button (). In the opened window, you can create a new schedule (see the <i>Schedule</i> section, page 207) or use the existing one. Existing schedules are displayed in the Interval of execution drop-down list in the simplified mode.</p> <p>To enable broadcasting at the time specified in the schedule and disable it at the other time, select the Enable value from the Action for rule upon activation of schedule drop-down list and click the SAVE button. When the wireless connection is disabled, the device will not be able to enable broadcasting of this wireless network on schedule.</p> <p>To disable broadcasting at the time specified in the schedule and enable it at the other time, select the Disable value from the Action for rule upon activation of schedule drop-down list and click the SAVE button.</p> <p>To change or delete the schedule, click the Set schedule button (). In the opened window, change the parameters and click the SAVE button or click the DELETE FROM SCHEDULE button.</p> <p>If you created an additional network, you can configure, change or delete a schedule for each network. To do this, click the button in the line of the network.</p>
<p>Clients isolation</p>	<p>Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.</p>
<p>Enable guest network</p>	<p>This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the access point's LAN.</p>

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

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

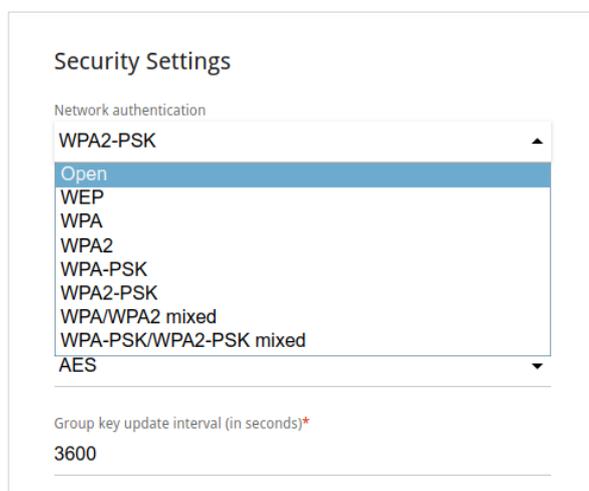


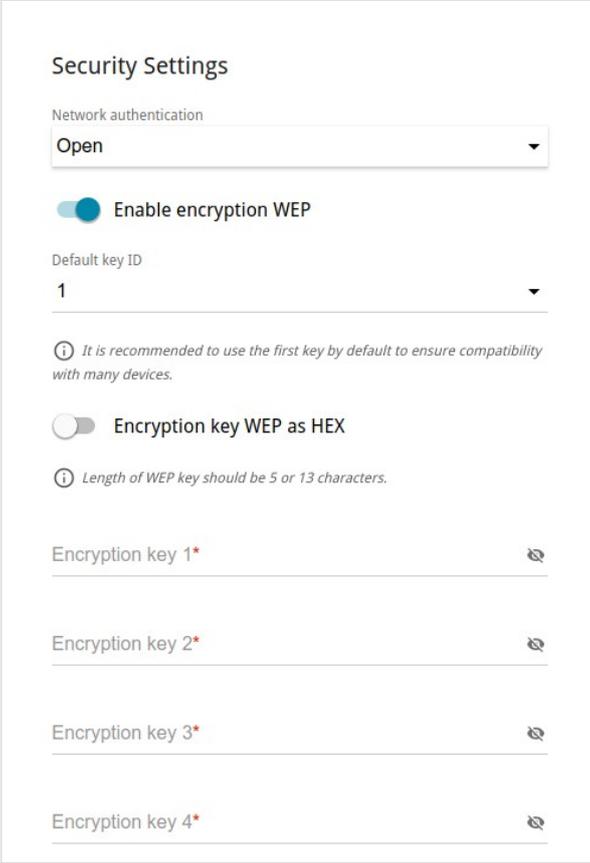
Figure 101. Network authentication types supported by the access point.

The access point supports the following authentication types:

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

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

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



The screenshot displays the 'Security Settings' section of a web interface. At the top, the title 'Security Settings' is centered. Below it, a 'Network authentication' dropdown menu is set to 'Open'. Underneath, there is a toggle switch for 'Enable encryption WEP', which is currently turned on. Below the toggle is a 'Default key ID' dropdown menu set to '1'. A small information icon (i) is followed by the text: 'It is recommended to use the first key by default to ensure compatibility with many devices.' Below this is another toggle switch for 'Encryption key WEP as HEX', which is currently turned off. Another information icon (i) is followed by the text: 'Length of WEP key should be 5 or 13 characters.' At the bottom, there are four input fields for 'Encryption key 1*', 'Encryption key 2*', 'Encryption key 3*', and 'Encryption key 4*', each with a small lock icon to its right.

Figure 102. The **Open** value is selected from the **Network authentication** drop-down list.

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

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

Figure 103. 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. ⁴ Click the Show icon (🔍) to display the entered password.
Encryption type	An encryption method: TKIP , AES , or TKIP+AES .
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed.

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

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

The screenshot shows the 'Security Settings' section of a web interface. It includes a 'Network authentication' dropdown menu with 'WPA2' selected. Below it is a 'WPA2 Pre-authentication' toggle switch that is currently turned off. Further down are input fields for 'IP address RADIUS server*' (192.168.0.254), 'RADIUS server port*' (1812), 'RADIUS encryption key*' (dlink), 'Encryption type*' (AES), and 'Group key update interval (in seconds)*' (3600).

Figure 104. 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 access point 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 access point.

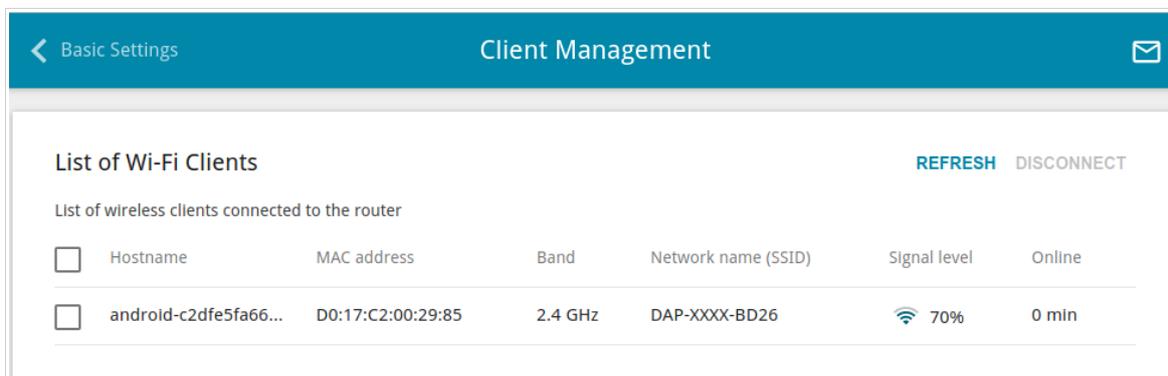


Figure 105. The page for managing the wireless clients.

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 access point.

! 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.

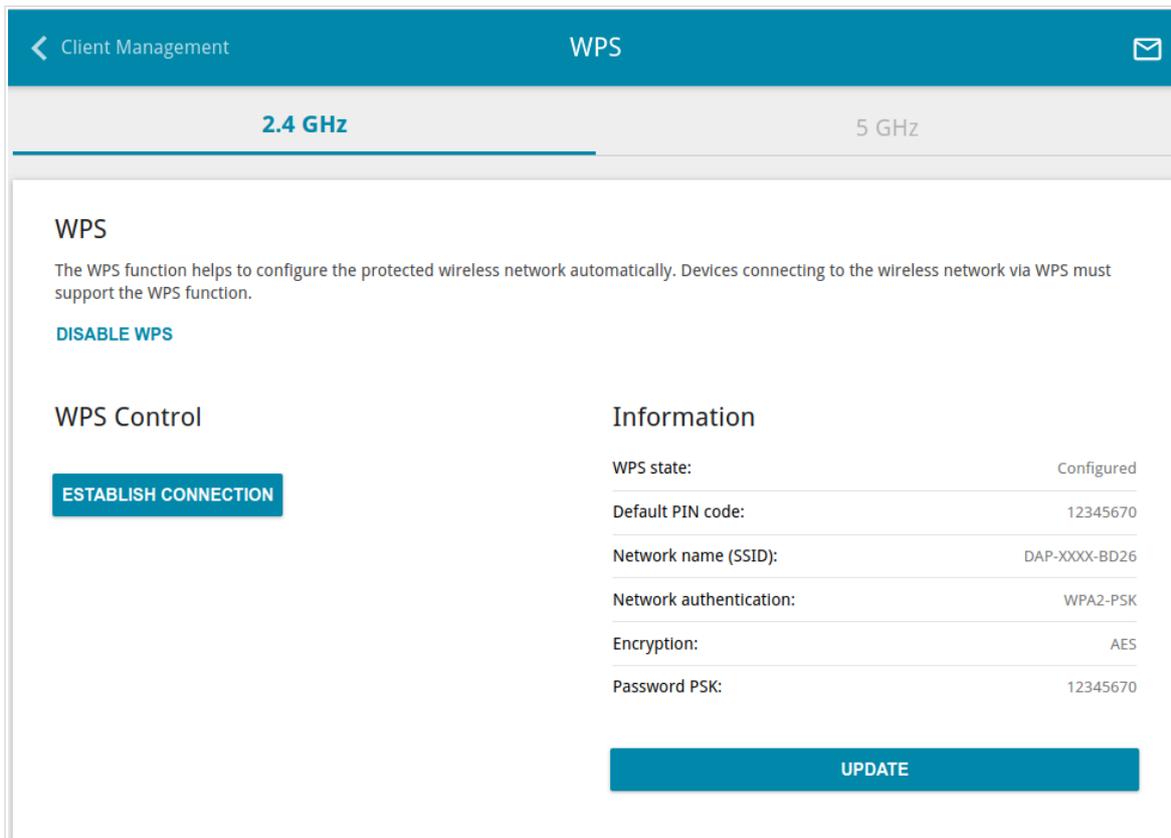


Figure 106. The page for configuring the WPS function.

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

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

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

Using WPS Function via Web-based Interface

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

1. Click the **ENABLE WPS** button.
2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.
3. In the opened window, select the **PIN** value from the **WPS method** drop-down list.
4. Select the PIN method in the software of the wireless device that you want to connect to the access point'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 access point.

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

1. Click the **ENABLE WPS** button.
2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.
3. In the opened window, select the **PBC** value from the **WPS method** drop-down list.
4. Select the PBC method in the software of the wireless device that you want to connect to the access point'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 access point.

WMM

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

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

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

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

The screenshot shows the WMM configuration page. At the top, there are tabs for '2.4 GHz' and '5 GHz'. The main content area is titled 'Wi-Fi Multimedia' and includes a description: 'The mechanism for Improving Wi-Fi network performance. It is recommended for users not to change the specified values'. Below this is a 'Work mode' dropdown menu set to 'Manual'. Underneath, there are two sections: 'Access Point' and 'Station', each containing a table of QoS parameters.

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

Figure 107. The page for configuring the WMM function.

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

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

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

Parameters of the Access Categories are defined for both the access point 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.

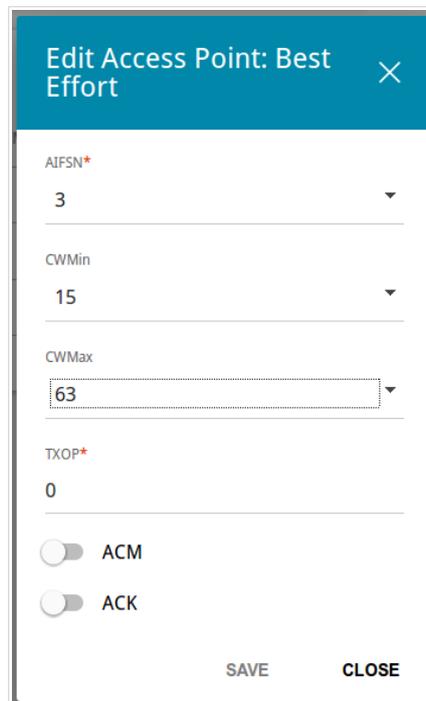


Figure 108. The window for changing parameters of the WMM function.

Parameter	Description
AIFSN	<i>Arbitrary Inter-Frame Space Number.</i> This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
CWMin/CWMax	<i>Contention Window Minimum/Contention Window Maximum.</i> Both fields influence time delays for the relevant Access Category. The CWMax field value should not be lower, than the CWMin field value. The lower the difference between the CWMax field value and the CWMin field value, the higher is the Access Category priority.

Parameter	Description
TXOP	<i>Transmission Opportunity.</i> The higher the value, the higher is the Access Category priority.
ACM	<i>Admission Control Mandatory.</i> If the switch is moved to the right, the device cannot use the relevant Access Category.
ACK	<i>Acknowledgment.</i> Answering response requests while transmitting. Displayed only in the Access Point section. If the switch is moved to the left, the access point answers requests. If the switch is moved to the right, the access point does not answer requests.

Click the **SAVE** button.

Client

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

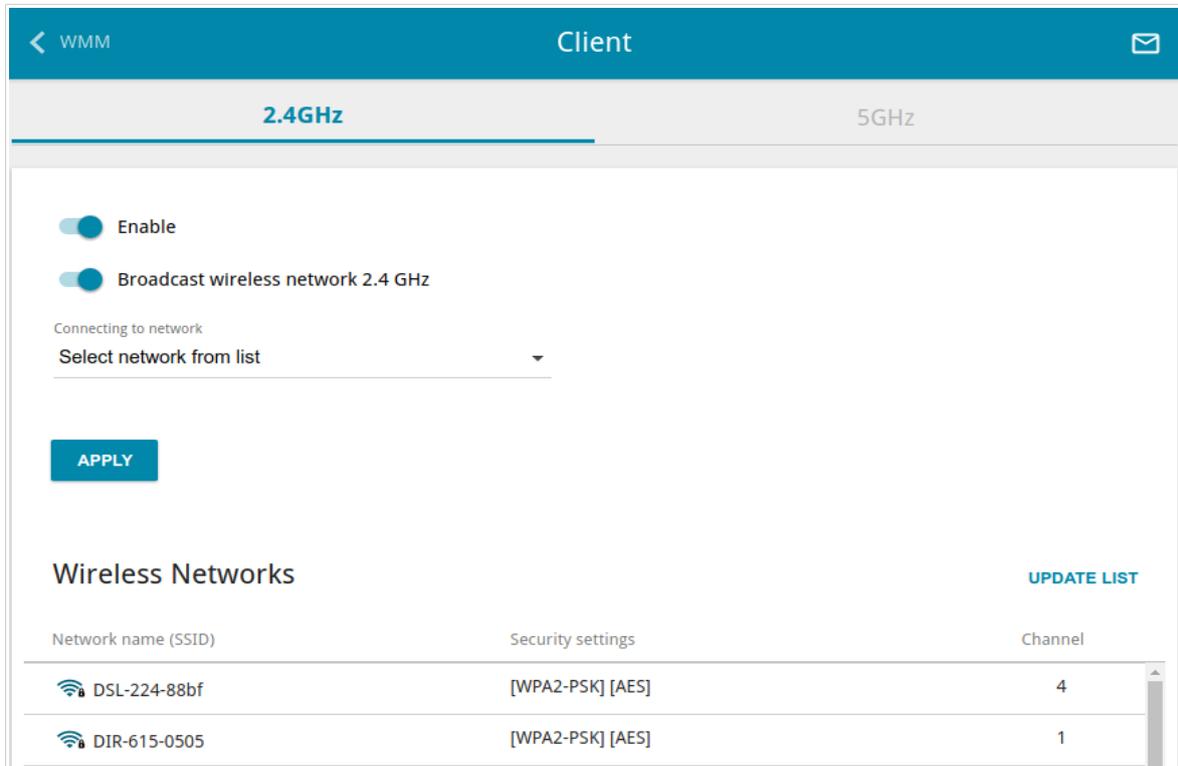


Figure 109. The page for configuring the client mode.

To configure the access point 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 access point's WLAN. Upon that the access point 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 access point connects. If a password is required, enter it in the relevant field. Click the **CONNECT** button.

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

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

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

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

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

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

When connecting to a wireless access point, the wireless channel of DAP-600P 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 **WiFi_Station** interface in the 2.4GHz band or for the **WiFi_Station-5G** interface in the 5GHz band.

Additional

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

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

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

Figure 110. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
<p>Bandwidth</p>	<p>The channel bandwidth for 802.11n standard in the 2.4GHz band (the 2.4 GHz tab).</p> <ul style="list-style-type: none"> • 20 MHz: 802.11n clients operate at 20MHz channels. • 20/40 MHz: 802.11n clients operate at 20MHz or 40MHz channels. • Auto: the access point automatically chooses the most suitable channel bandwidth for 802.11n clients. <p>The channel bandwidth for 802.11n and 802.11ac standards in 5GHz band (the 5 GHz tab).</p> <ul style="list-style-type: none"> • 20 MHz: 802.11n and 802.11ac clients operate at 20MHz channels. • 20/40 MHz: 802.11n and 802.11ac clients operate at 20MHz or 40MHz channels. • 20/40/80 MHz: 802.11ac clients operate at 20MHz, 40MHz, or 80MHz channels. • 20/40/80/160 MHz: 802.11ac clients operate at 20MHz, 40MHz, 80MHz, or 160MHz channels. • Auto: the access point automatically chooses the most suitable channel bandwidth for 802.11n and 802.11ac clients.
<p>Autonegotiation 20/40 (Coexistence)</p>	<p><i>Available on the 2.4 GHz tab.</i></p> <p>Move the switch to the right to let the access point automatically choose the channel bandwidth (20MHz or 40MHz) depending on availability of other APs within its operational range (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the 20/40 MHz value is selected from the Bandwidth drop-down list.</p>
<p>TX power</p>	<p>The transmit power (in percentage terms) of the access point.</p>
<p>Drop multicast</p>	<p>Move the switch to the right to disable multicasting for the access point's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected on the Advanced / IGMP page.</p>
<p>Enable TX Beamforming</p>	<p>TX Beamforming is the signal processing/directing technique which helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation.</p> <p>Move the switch to the right to improve the signal quality.</p>

Parameter	Description
STBC	<p>The STBC (<i>Space-time block coding</i>) technique allows increasing data transfer reliability even for portable devices equipped with poor antennas (smartphones, pads, etc.) due to using several data streams and processing several versions or received data.</p> <p>Move the switch to the right if you need to use the STBC technique.</p>
B/G protection	<p><i>Available on the 2.4 GHz tab.</i></p> <p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> • 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	<p>Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the access point is communicating to wireless devices.</p> <ul style="list-style-type: none"> • Enable: the access point 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 access point uses the 800 ns standard guard interval.
Beacon period	<p>The time interval (in milliseconds) between packets sent to synchronize the wireless network.</p>
RTS threshold	<p>The minimum size (in bytes) of a packet for which an RTS frame is transmitted.</p>
Frag threshold	<p>The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).</p>

Parameter	Description
DTIM period	The number of beacon frames between sending DTIM messages (messages notifying on broadcast or multicast transmission).
Station Keep Alive	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value 0 is specified, the checking is disabled.

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

MAC Filter

On the **Wi-Fi / MAC Filter** page, you can define a set of MAC addresses of devices which will be allowed to access the WLAN, or define MAC addresses of devices which will not be allowed to access the WLAN.

! It is recommended to configure the Wi-Fi MAC filter through a wired connection to DAP-600P.

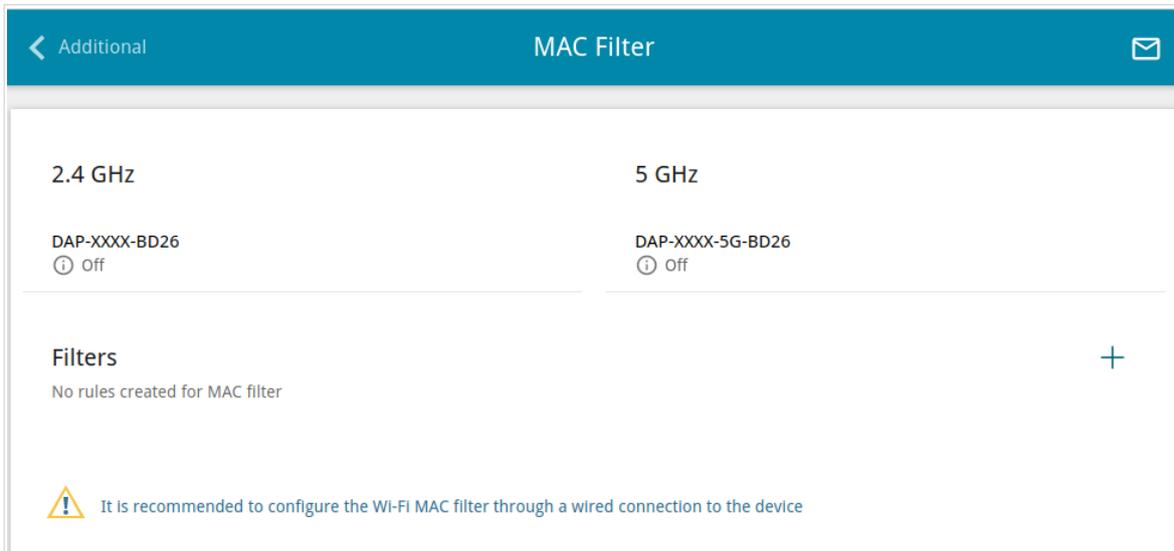


Figure 111. The page for configuring the MAC filter for the wireless network.

By default, the Wi-Fi MAC filter is disabled.

To configure the MAC filter, first you need to create rules (specify MAC addresses of devices for which the specified filtering modes will be applied). To do this, click the **ADD** button (**+**).

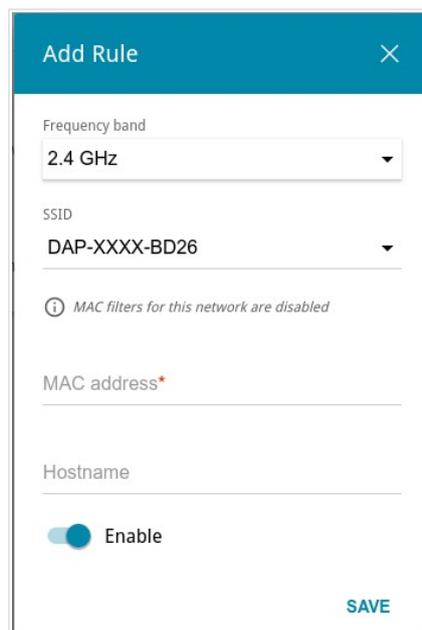


Figure 112. The window for adding a rule for the MAC filter.

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 (<i>optional</i>). You can specify any name.
Enable	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.

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

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

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

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

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

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

To set a schedule for the MAC filter rule, click the **Add Schedule** button () in the line corresponding to this rule. In the opened window, you can create a new schedule (see the *Schedule* section, page 207) or use the existing one. Existing schedules are displayed in the **Interval of execution** drop-down list in the simplified mode.

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

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

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

Super Mesh

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

A Mesh network consists of a main device (the Master role) and subordinate devices (the Slave role). Devices connect to each other via wireless or wired connection. Settings are transmitted from the main device to a subordinate one at the final step of configuring the Super Mesh function while the devices are connected via an Ethernet cable (you don't need to manually specify all the parameters on subordinate devices).

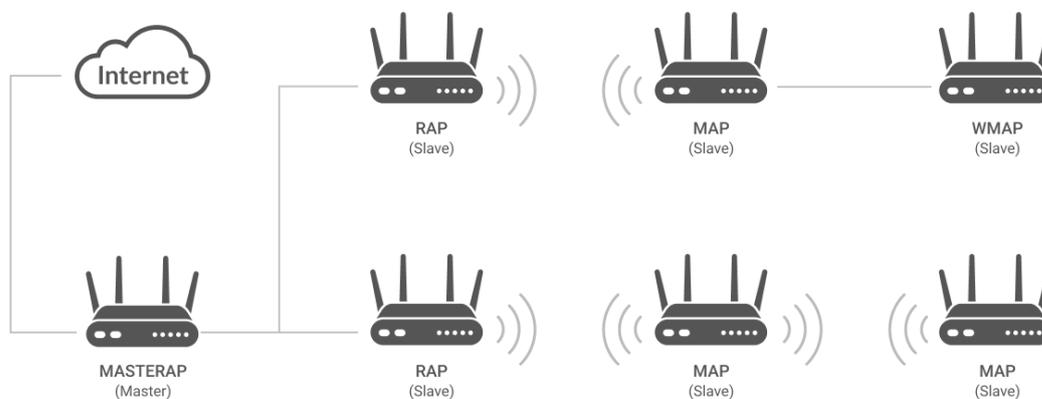


Figure 113. A Mesh network structure.

If the device is in the router mode (the **Router** value is displayed in the **Device mode** line on the **Summary** page), you can configure it as a main device (the Master role). If the device is in the access point mode (the **Access point** value is displayed in the **Device mode** line on the **Summary** page), you can configure it as a subordinate device (the Slave role).

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

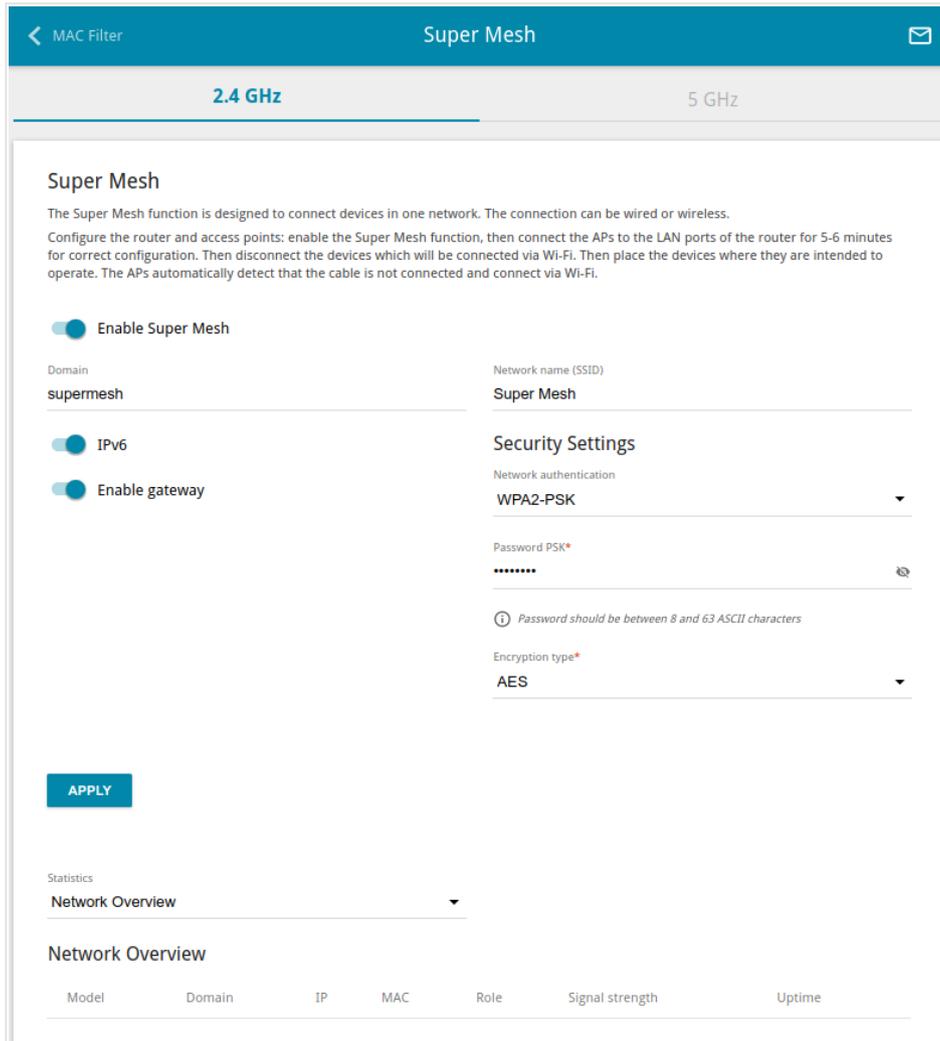


Figure 114. The **Wi-Fi / Super Mesh** page.

To activate the Super Mesh function, on the tab of the relevant band, move the **Enable Super Mesh** switch to the right. You can specify the following parameters:

Parameter	Description
Domain	An identifier which shows that the device belongs to a certain Mesh network. This value should be the same for all devices of your Mesh network.
IPv6	If you need to use IPv6 for configuring the Mesh network, move the IPv6 switch to the right.
Enable gateway	Move the switch to the right to allow devices of the Mesh network to use this device for connecting to the Internet. It is recommended to move the switch to the right when configuring the main device. It is recommended to move the switch to the left when configuring a subordinate device.

Parameter	Description
Network name (SSID)	<p>A name of the Mesh network. This value should be the same for all devices of your Mesh network.</p> <p>Clients connected to devices of a Mesh network cannot see the Mesh network and cannot connect to it.</p>

In the **Security Settings** section, specify security settings of your Mesh network.⁵ To do this, select the needed type of authentication⁶ from the **Network authentication** drop-down list.

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

Parameter	Description
Password PSK	A password for WPA encryption. Click the Show icon (🔍) to display the entered key. By default, WPS PIN from the barcode label is used as the network key.
Encryption type	An encryption method: AES .

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

To complete your Mesh network configuration, connect the subordinate device to a LAN port of the main device using an Ethernet cable. Wait for about 5-6 minutes. When all the settings are applied, the **POWER/WLAN LED** should be solid blue. Then, if needed, disconnect the Ethernet cable and move the subordinate device to its workplace.

To view data on the current state of your Mesh network, select the needed value from the **Statistics** drop-down list.

- **Network Overview:** When this value is selected, information on all devices of your Mesh network is displayed on the page. The value is unavailable if your device is configured as a subordinate one.
- **List of APs:** When this value is selected, information on all devices of your Mesh network is displayed on the page.
- **List of Clients:** When this value is selected, information on all clients connected to the devices of your Mesh network is displayed on the page.
- **Neighbours:** When this value is selected, a connection scheme of your Mesh network devices is displayed on the page.

Parameter	Description
Network Overview / List of APs	
Model	The model of a device.

⁵ Security settings should be the same for all devices of your Mesh network.

⁶ The full list will be available in the next firmware version.

Parameter	Description
Domain	The identifier which shows that a device belongs to the Mesh network.
IP	The IPv4 and/or IPv6 address of a device.
MAC	The MAC address of a device.
Role	<p>The short name for a Mesh network device.</p> <ul style="list-style-type: none"> • MASTERAP (Master Access Point): The main device which provides connection to the Internet. • RAP (Router Access Point): A subordinate device connected to the main device via a cable (directly to the main one or via some subordinate devices connected via a cable). • MAP (Mesh Access Point): A subordinate device with a wireless connection. • WMAP (Wired Mesh Access Point): A subordinate device connected via a cable to another subordinate device with a wireless connection.
Signal strength	<p><i>Available for the Network Overview section only.</i></p> <p>The strength of a device's wireless signal.</p>
Uptime	The operational time of a device.
List of Clients	
AP MAC	The MAC address of the Mesh network device to which a client is connected.
Client MAC Address	The MAC address of a client.
Bandwidth	The bandwidth at which a client operates.
Wireless mode	The operating mode of a client's wireless connection.
Status	Information on a client's current state.
Neighbours	
MAC	The MAC address of the device to which a Mesh network node is connected. The MAC address of this node is displayed in the Neighbour MAC Address field.
Neighbour MAC Address	The MAC address of the device connected to a Mesh network node. The MAC address of this node is displayed in the MAC field.

Parameter	Description
Role	<p>The short name for the Mesh network device which MAC address is displayed in the Neighbour MAC Address field.</p> <ul style="list-style-type: none"> • MASTERAP (Master Access Point): The main device which provides connection to the Internet. • RAP (Router Access Point): A subordinate device connected to the main device via a cable (directly to the main one or via some subordinate devices connected via a cable). • MAP (Mesh Access Point): A subordinate device with a wireless connection. • WMAP (Wired Mesh Access Point): A subordinate device connected via a cable to another subordinate device with a wireless connection.
Connection status	<p>The current connection state of the Mesh network node which MAC address is displayed in the Neighbour MAC Address field.</p>
Hops	<p>The number of intermediate Mesh network nodes from the device which MAC address is displayed in the Neighbour MAC Address field to the main device.</p> <p>If the MAC address of the main device is displayed in the Neighbour MAC Address field, the number of intermediate nodes is 0.</p>
Rate at path to upper-level host	<p>The maximum allowed value of connection speed from the device which MAC address is displayed in the Neighbour MAC Address field to the device which MAC address is displayed in the MAC field.</p>
Host capacity	<p>The capacity of the device which MAC address is displayed in the MAC field.</p>

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

Roaming

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

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

MAC Filter Roaming

Smart Adjustment of Wi-Fi Clients

Smart adjustment of Wi-Fi clients is designed for wireless networks based on several access points or routers. If the function is enabled for all access points (routers) which establish a wireless network, then wireless clients will always connect to the device with the highest signal level. For proper operation of the function, it is recommended to specify the same parameters of the WLAN (SSID, authentication type, and password) for all devices.

DISABLE

Port*
7890

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

2.4 GHz

Maximum time of storing data (in seconds)*
60
Maximum time of storing data on adjacent clients

Minimum level of connection quality (in percent)*
50

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

Threshold value of connection quality (in percent)*
40

5 GHz

Maximum time of storing data (in seconds)*
60
Maximum time of storing data on adjacent clients

Minimum level of connection quality (in percent)*
50

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

Threshold value of connection quality (in percent)*
40

APPLY

Figure 115. The **Wi-Fi / Roaming** page.

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

Parameter	Description
Port	The number of the port used for data exchange between access points (routers).

Parameter	Description
Use multicast for service data exchange	<p>Move the switch to the right in order to use multicast traffic for service data exchange between access points (routers). This setting is needed if the devices which support the smart adjustment function are located in different subnets. If the switch is moved to the right, the Multicast TTL and Multicast group address fields are displayed on the page.</p> <p>If the switch is moved to the left, broadcast traffic is used for service data exchange.</p>
Multicast TTL	Specify the TTL (<i>Time to live</i>) parameter value. The recommended value is 4 .
Multicast group address	Specify the address of the multicast group (from the subnet 239.255.0.0/16).
2.4 GHz / 5 GHz	
Maximum time of storing data	The maximum time period (in seconds) during which the access point (router) stores data on the signal strength of the client located on its coverage area.
Minimum level of connection quality	The signal strength upon which the access point (router) starts scanning other devices in order to find a device with a higher signal level.
Dead zone	This parameter is used for calculation of the signal strength upon which the smart adjustment function goes off. If the signal strength provided by another device is less than the sum of the Minimum level of connection quality field value and the Dead zone field value, then the client disconnects from the access point (router). You can specify the values from -50% to +50% .
Threshold value of connection quality	The signal strength upon which the access point (router) disconnects the client from its wireless network regardless of the signal levels of other devices. This value should not be greater than the value specified in the field Minimum level of connection quality .

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

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

Advanced

In this menu you can configure advanced settings of the access point:

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

DNS

On the **Advanced / DNS** page, you can add⁷ DNS servers to the system.

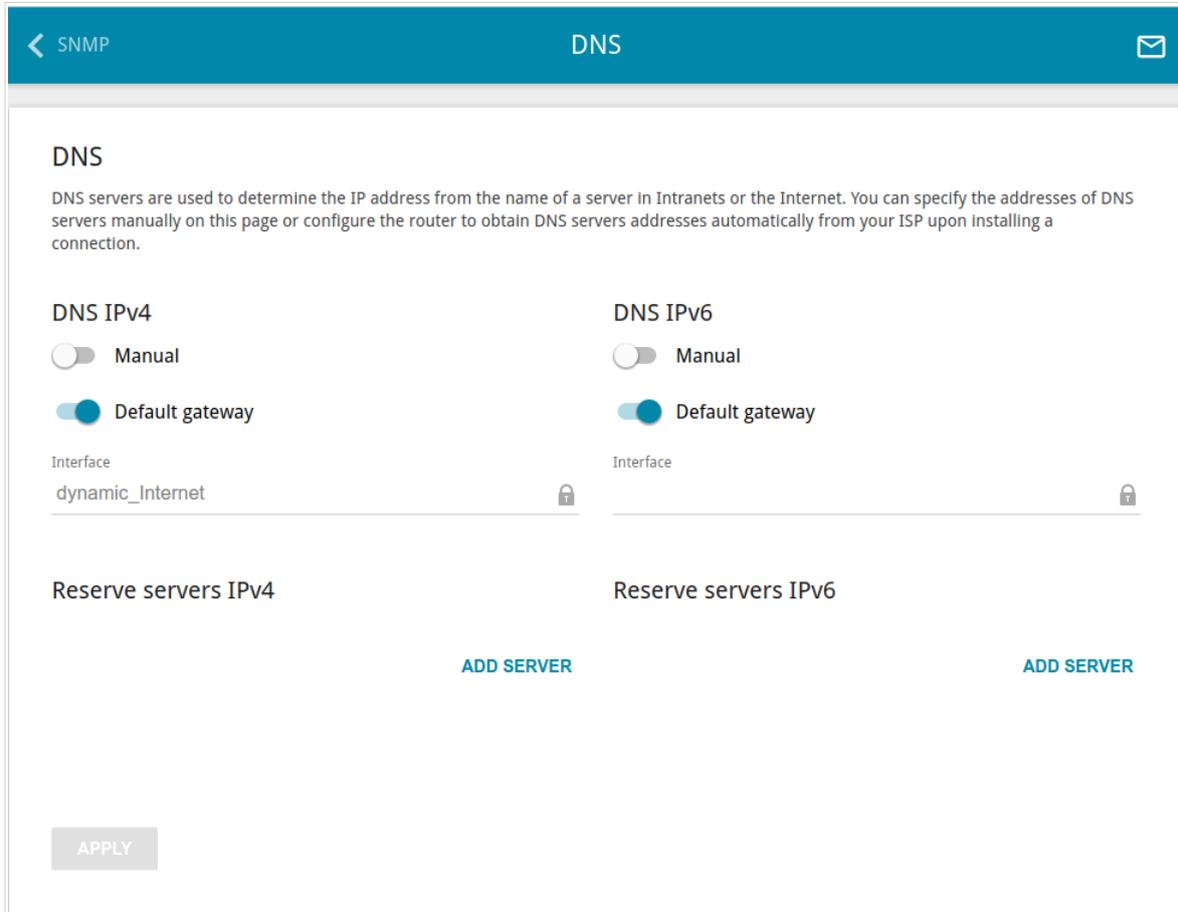


Figure 116. The **Advanced / DNS** page.

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 access point to obtain DNS servers addresses automatically from your ISP upon installing a connection. Also here you can specify addresses of reserve DNS servers which the access point can use if the addresses specified manually or obtained automatically are unavailable.



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

⁷ Correct operation of the page displayed if the **Access point** or **Repeater** mode was selected in the Initial Configuration Wizard will be implemented in the next firmware version.

Specify needed settings for IPv4 in the **DNS IPv4** section and for IPv6 in the **DNS IPv6** section.

If you want to configure automatic obtainment of DNS servers addresses, move the **Manual** switch to the left. Then move the **Default gateway** switch to the left and from the **Interface** drop-down list select a WAN connection which will be used to obtain addresses of DNS servers automatically. If you want the access point to use the default WAN connection to obtain addresses of DNS servers, move the **Default gateway** switch to the right.

To specify a DNS server manually, move the **Manual** switch to the right. In the **Name Servers** section of the relevant IP version, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server.

To specify a reserve DNS server, in the **Reserve servers** section of the relevant IP version, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server.

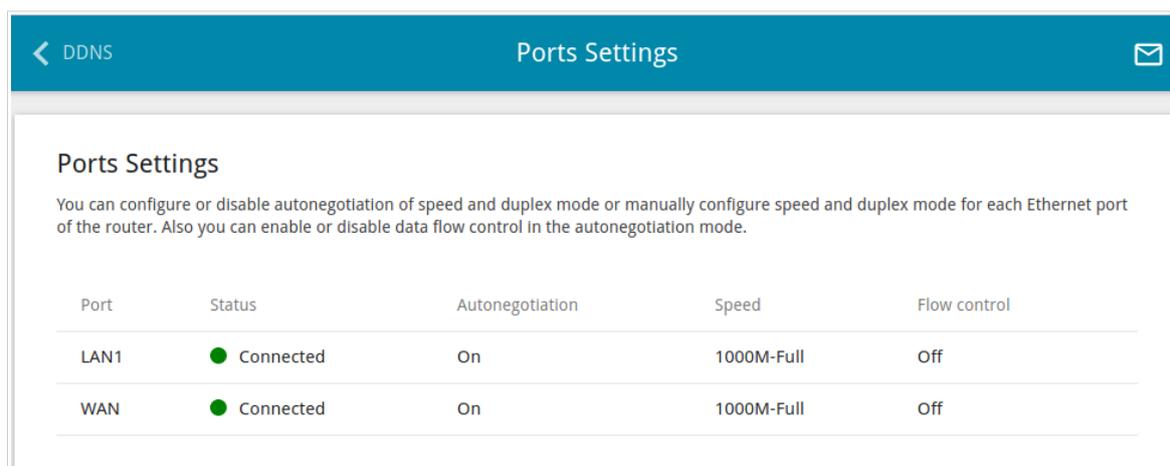
To remove a DNS server from the page, click the **Delete** icon (✕) in the line of the address.

When all needed settings are configured, 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 access point.

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



Port	Status	Autonegotiation	Speed	Flow control
LAN1	● Connected	On	1000M-Full	Off
WAN	● Connected	On	1000M-Full	Off

Figure 117. 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.

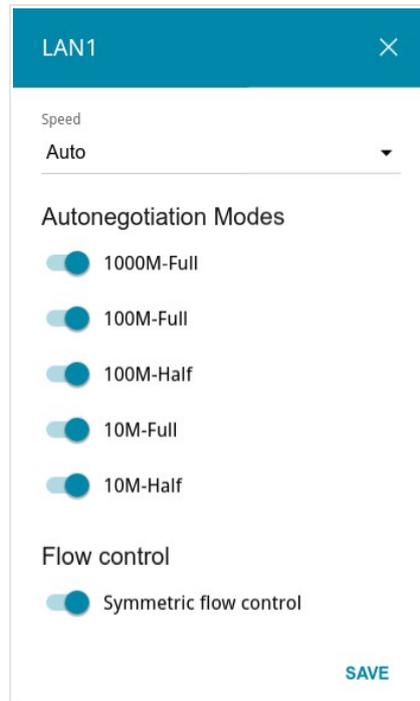


Figure 118. The window for changing the settings of the access point's port.

In the opened window, specify the needed parameters:

Parameter	Description
<p>Speed</p>	<p>Data transfer mode.</p> <p>Select the Auto value to enable autonegotiation. When this value is selected, the Autonegotiation Modes and Flow control sections are displayed.</p> <p>Select the 10M-Half, 10M-Full, 100M-Half, or 100M-Full value to manually configure speed and duplex mode for the selected port:</p> <ul style="list-style-type: none"> • 10M-Half: Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 10Mbps. • 10M-Full: Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 10Mbps. • 100M-Half: Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 100Mbps. • 100M-Full: Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 100Mbps.

Parameter	Description
Autonegotiation Modes	
To enable the needed data transfer modes, move relevant switches to the right.	
Flow control	
Symmetric flow control	Move the switch to the right to enable the flow control function for the port. Move the switch to the left to disable the flow control function for the port.

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

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

MAC Filter

On the **Advanced / MAC Filter** page, you can configure MAC-address-based filtering for computers of the access point's LAN. This page is also available in the **Firewall** section if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

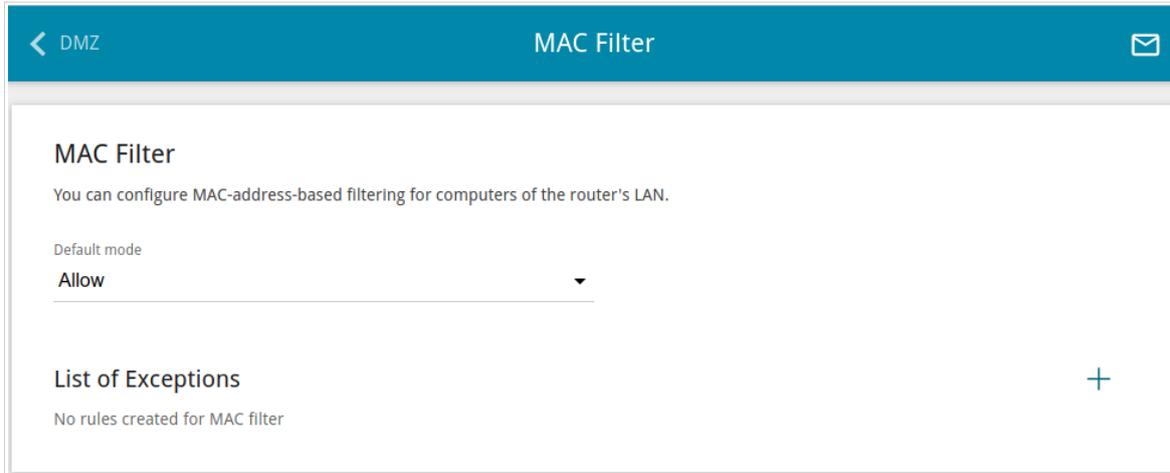


Figure 119. The **Advanced / MAC Filter** page.

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

- **Allow:** Allows access to the access point's network and to the Internet for devices (the value is specified by default);
- **Deny:** Blocks access to the access point'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 a special filtering mode will be applied), click the **ADD** button (+).

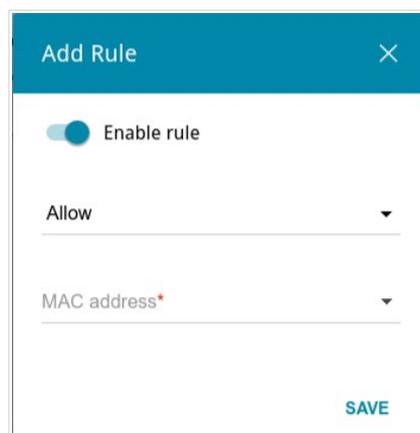


Figure 120. The window for adding a rule for the MAC filter.

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

Parameter	Description
Enable rule	<p>Move the switch to the right to enable the rule.</p> <p>Move the switch to the left to disable the rule.</p>
Action	<p>Select an action for the rule.</p> <ul style="list-style-type: none"> • 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 access point'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	<p>The MAC address of a device from the access point's LAN. You can enter the MAC address of a device connected to the access point's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).</p>

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.

To set a schedule⁸ for the MAC filter rule, click the **Add Schedule** button () in the line corresponding to this rule. In the opened window, you can create a new schedule (see the *Schedule* section, page 207) or use the existing one. Existing schedules are displayed in the **Interval of execution** drop-down list in the simplified mode.

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

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

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

⁸ Schedule settings are available on the **Firewall / MAC filter** page if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

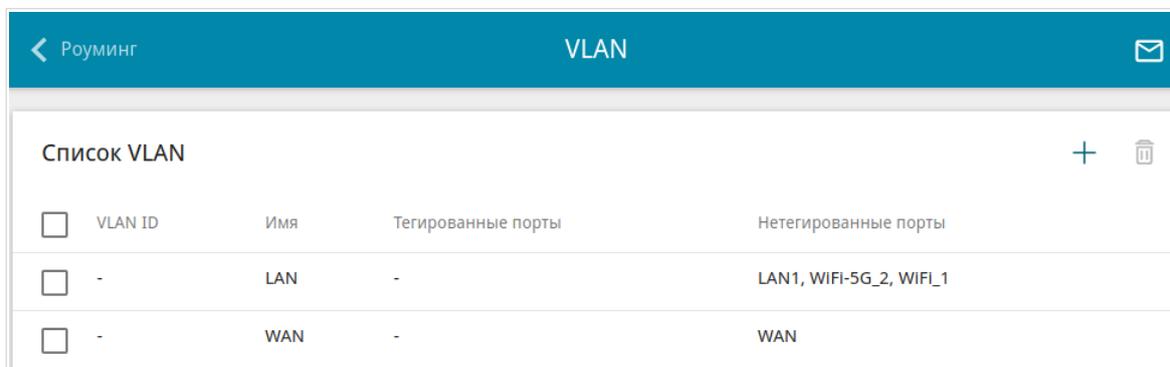
VLAN

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

By default, 2 VLANs are created in the access point's system:

- **LAN:** for the LAN interface, it includes the LAN port and Wi-Fi networks. You cannot delete this VLAN.
- **WAN:** for the WAN interface; it includes the **WAN (PoE)** port. You can edit or delete this VLAN.



<input type="checkbox"/>	VLAN ID	Имя	Тегированные порты	Нетегированные порты
<input type="checkbox"/>	-	LAN	-	LAN1, WIFI-5G_2, WIFI_1
<input type="checkbox"/>	-	WAN	-	WAN

Figure 121. The **Advanced / VLAN** page.

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

! Configuration of the LAN port is available only via Wi-Fi connection to DAP-600P.

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

Figure 122. The page for adding a VLAN.

You can specify the following parameters:

Parameter	Description
Name	A name for the VLAN for easier identification.
VLAN ID	An identifier of the VLAN.
QoS	A priority tag for the transmitted traffic.
Ports	<p>Select a type for each port included in the VLAN.</p> <ul style="list-style-type: none"> • Untagged. Untagged traffic will be transmitted through the specified port. • Tagged. Tagged traffic will be transmitted through the specified port. If at least one port of this type is included to the VLAN, it is required to fill in the VLAN ID and QoS fields. <p>Leave the Excluded value for the ports not included in the VLAN.</p>

Parameter	Description
Wireless interfaces	Select the Untagged value for each Wi-Fi interface included in the VLAN. Leave the Excluded value for the Wi-Fi interfaces not included in the VLAN.

Click the **APPLY** button.

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

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

SNMP

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

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

SNMP

You can enable and configure the SNMP agent of the router. The SNMP agent is a service which sends data on the state and settings of the device where is it enabled to the SNMP manager (the network management system of your ISP or system administrator).

Configuration

Enable SNMP

Remote subnet
0.0.0.0/0

Hostname
Router

The contact information for the administrator
Admin <root@localhost>

System location
Test room

Communities

ADD

Users

There are no users

+

APPLY

Figure 123. The **Advanced / SNMP** page.

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

Parameter	Description
Configuration	
Remote subnet	The IP address of the remote subnet where the SNMP manager is located.
Hostname	A name of the access point for identification in the SNMP manager.
The contact information for the administrator	Additional information used to contact the administrator of the access point.
System location	Additional information used to locate the access point.

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

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

If the SNMP manager operates over SNMPv2c, create a read-only community which will be used by the SNMP manager to get data on the device. To do this, in the **Communities** section, click the **ADD** button and specify the community name in the line displayed. Then click the **APPLY** button.

To remove a community, click the **Delete** icon (✕) in the relevant line. Then click the **APPLY** button.

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

Figure 124. The window for adding a user.

In the opened window, specify the needed parameters:

Parameter	Description
Name	Specify a username for access from the SNMP manager.
Authentication protocol	Select a required authentication method from the drop-down list or leave the None value if authentication is not required.
Authentication password	Specify a password for user authentication from the SNMP manager. The field is displayed if the MD5 or SHA value is selected from the Authentication protocol drop-down list.
Encryption protocol	Select a required encryption method from the drop-down list or leave the None value if encryption is not required. The list is displayed if the MD5 or SHA value is selected from the Authentication protocol drop-down list.
Encryption key	Specify an encryption key for data exchange between the SNMP agent and SNMP manager. The field is displayed if the DES or AES value is selected from the Encryption protocol drop-down list.
MIB subtree	Specify a MIB element which will be available to the SNMP manager.

Click the **SAVE** button.

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

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

DDNS

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

On the **Advanced / DDNS** page, you can configure the access point to use one or several DDNS services.

A DDNS service allows associating a domain name with dynamic IP addresses. In order to use a service, it is necessary to register a domain name on the web site of your DDNS provider.



Figure 125. The **Advanced / DDNS** page.

To configure needed settings for the access point, click the **ADD** button (**+**).

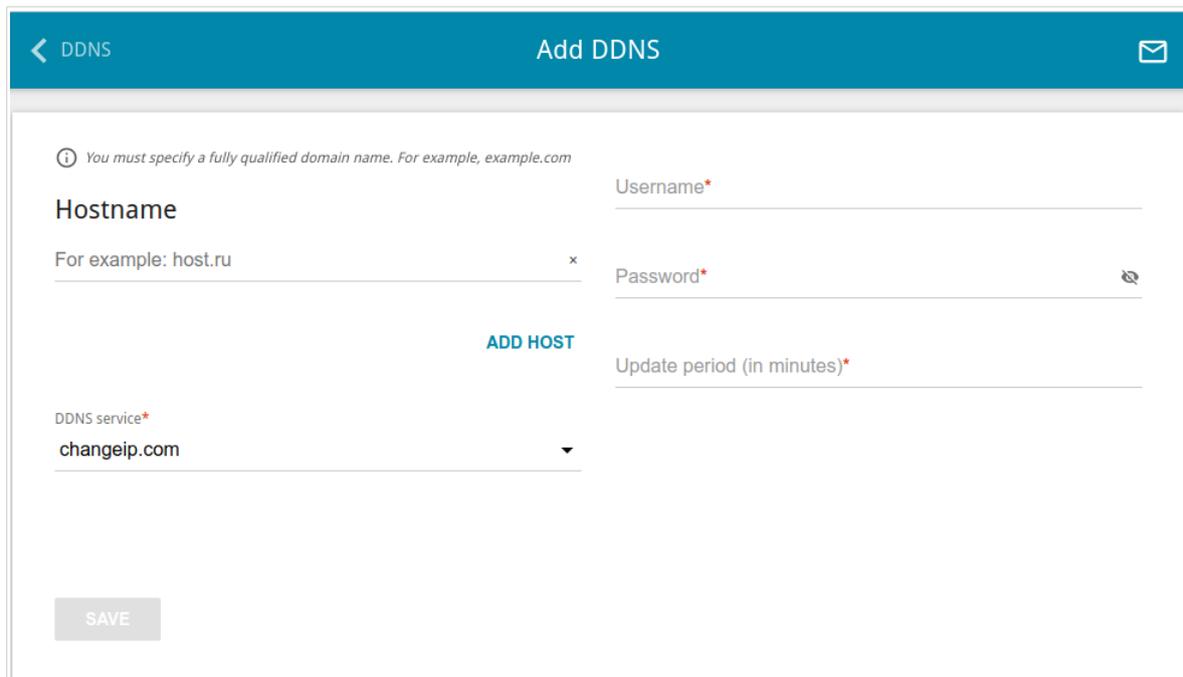
The screenshot shows the 'Add DDNS' configuration page. The header is teal with a back arrow, 'DDNS', and 'Add DDNS' in the center. Below the header is a white form area. At the top of the form, there is a note: 'You must specify a fully qualified domain name. For example, example.com'. The form contains several fields: 'Hostname' with the example 'For example: host.ru', 'Username*', 'Password*' with a toggle icon, 'Update period (in minutes)*', and 'DDNS service*' with a dropdown menu currently showing 'changeip.com'. At the bottom left of the form is a grey 'SAVE' button. In the center of the form, there is a blue 'ADD HOST' button.

Figure 126. The page for configuring the access point to use a DDNS service.

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

Parameter	Description
Hostname	Enter the full domain name registered at your DDNS provider. If you want to use another domain name of this DDNS provider, click the ADD HOST button, and in the line displayed, enter the needed value. To remove a domain name, click the Delete icon (✕) in the line of the name.
DDNS service	Select the DDNS provider from the drop-down list. If your provider is not in the list, select the Custom provider value and fill in the fields displayed on the page. Specify the DDNS provider name in the Name field, the domain name of the provider's server in the Server field, and the location of settings in the Path field.
Username	The username to authorize for your DDNS provider.
Password	The password to authorize for your DDNS provider. Click the Show icon (👁) to display the entered password.
Update period	An interval (in minutes) between sending data on the access point's external IP address to the relevant DDNS service.

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

To specify other parameters for a DDNS service, select the relevant line in the table. On the opened page, change the needed parameters and click the **SAVE** button.

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

Redirect

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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.

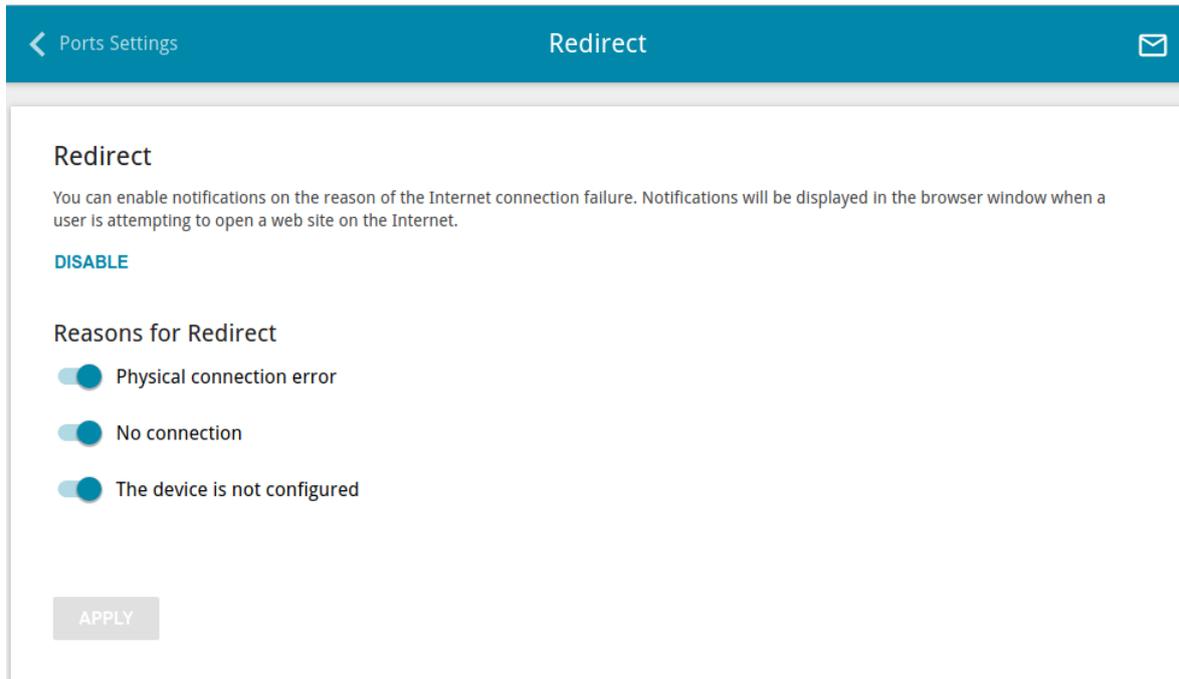


Figure 127. The **Advanced / Redirect** page.

To configure notifications, click the **ENABLE** button. Then, in the **Reasons for Redirect** section, move the needed switches to the right.

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

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

To disable notifications, click the **DISABLE** button.

Routing

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

On the **Advanced / Routing** page, you can specify static (fixed) routes.

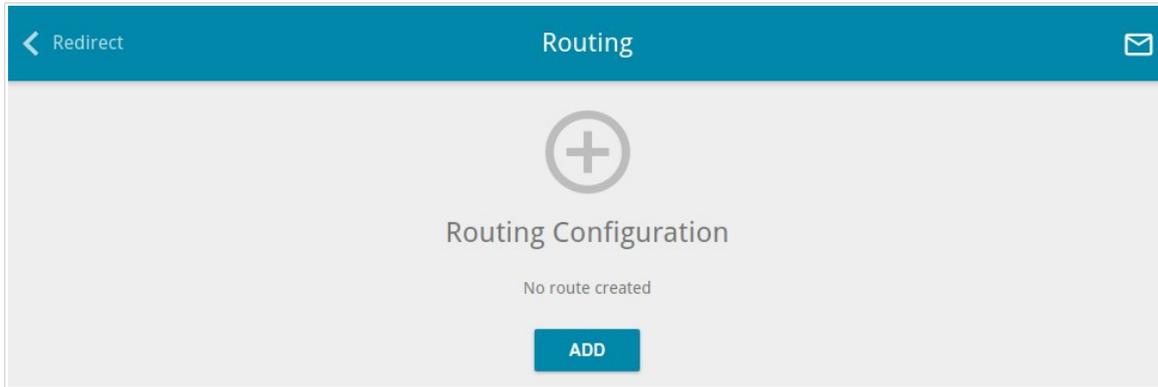


Figure 128. The **Advanced / Routing** page.

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

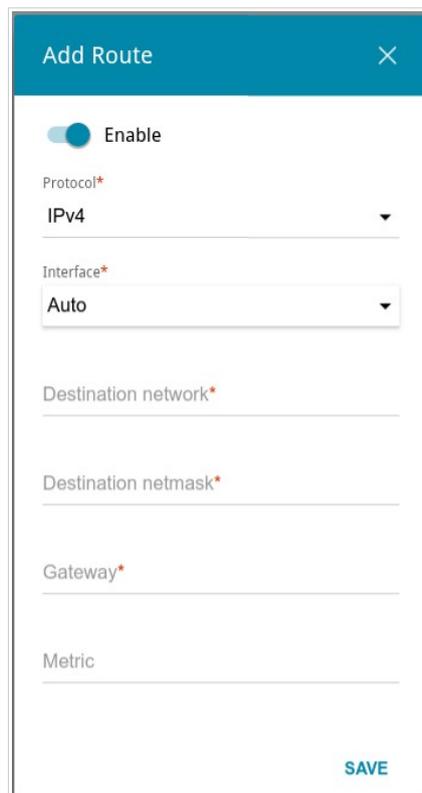
The screenshot shows a modal window titled 'Add Route' with a close button (X) in the top right corner. The window contains several configuration options: an 'Enable' toggle switch which is turned on; a 'Protocol*' dropdown menu set to 'IPv4'; an 'Interface*' dropdown menu set to 'Auto'; and four text input fields for 'Destination network*', 'Destination netmask*', 'Gateway*', and 'Metric'. A teal 'SAVE' button is located at the bottom right of the window.

Figure 129. The window for adding a new route.

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

Parameter	Description
Enable	Move the switch to the right to enable the route. Move the switch to the left to disable the route.
Protocol	An IP version.
Interface	From the drop-down list, select an interface (connection) through which the device will communicate with the remote network. If you have selected the Auto value, the access point itself sets the interface according to the data on the existing dynamic routes.
Destination network	A remote network which can be accessed with help of this route. You can specify an IPv4 or IPv6 address. The format of a host IPv6 address is 2001:db8:1234::1 , the format of a subnet IPv6 address is 2001:db8:1234::/64 .
Destination netmask	<i>For IPv4 protocol only.</i> The remote network mask.
Gateway	An IP address through which the destination network can be accessed.
Metric	A metric for the route. The lower the value, the higher is the route priority. <i>Optional.</i>

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

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

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

TR-069 Client

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

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

Figure 130. The page for configuring the TR-069 client.

You can specify the following parameters:

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

Parameter	Description
Inform Settings	
On	Move the switch to the right so the access point may send reports (data on the device and network statistics) to the ACS.
Interval	Specify the time period (in seconds) between sending reports.
Auto Configuration Server Settings	
Get URL address via DHCP	If the switch is moved to the right, the access point obtains the URL address of the ACS upon establishing the Dynamic IP type connection. If you need to specify the URL address manually, move the switch to the left and enter the needed value in the URL address field.
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS. Click the Show icon (👁) to display the entered password.
Connection Request Settings	
Username	The username used by the ACS to transfer a connection request to the access point.
Password	The password used by the ACS. Click the Show icon (👁) to display the entered password.
Request port	The port used by the ACS. By default, the port 8999 is specified.
Request path	The path used by the ACS.

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

Remote Access

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

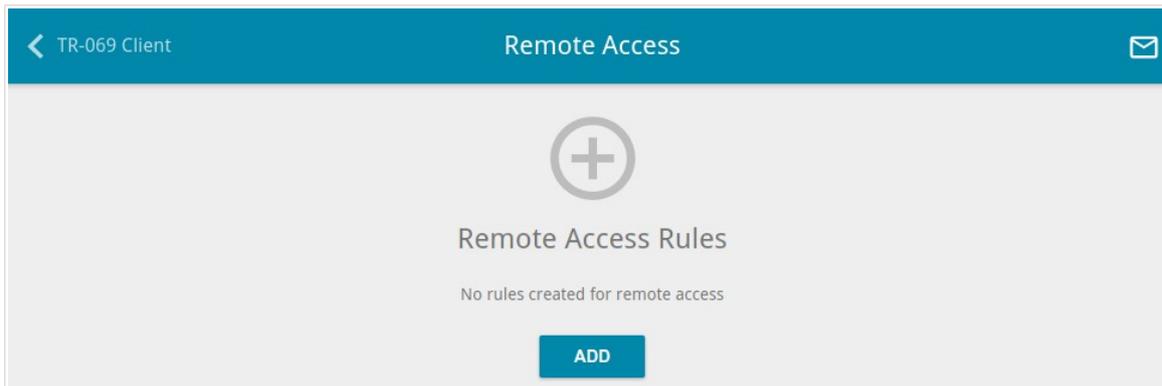


Figure 131. The **Advanced / Remote Access** page.

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

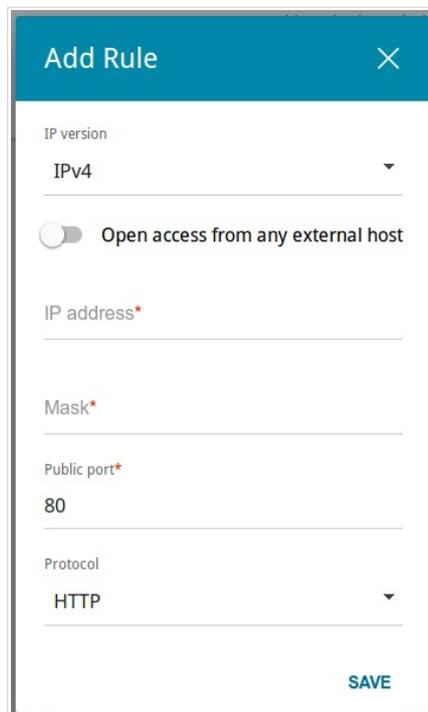
The image shows a modal dialog box titled 'Add Rule' with a close button (X) in the top right corner. The dialog contains several configuration options: 'IP version' is set to 'IPv4'; there is a toggle switch for 'Open access from any external host' which is currently turned off; 'IP address*' is an empty text input field; 'Mask*' is an empty text input field; 'Public port*' is set to '80'; and 'Protocol' is set to 'HTTP'. A blue 'SAVE' button is located at the bottom right of the dialog.

Figure 132. 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 access point for any host. Upon that the IP address and Mask fields are not displayed.
IP address	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.
Mask	<i>For the IPv4-based network only.</i> The mask of the subnet.
Public port	<i>For the IPv4-based network only.</i> An external port of the access point. You can specify only one port.
Protocol	The protocol available for remote management of the access point.

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

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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



Figure 133. 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 access point, move the **Enable** switch to the right.

When the protocol is enabled, the following parameters of the access point are displayed on the page:

Parameter	Description
Protocol	A protocol for network packet transmission.
IP address	The IP address of a client from the local area network.
Private port	A port of a client's IP address to which traffic is directed from a public port of the access point.
Public port	A public port of the access point from which traffic is directed to a client's IP address.
Description	Information transmitted by a client's network application.
Duration	The time period during which the UPnP IGD protocol has been used.

UDPXY

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

Figure 134. The **Advanced / UDPXY** page.

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

Upon that the following fields are displayed on the page:

Parameter	Description
Port	The port of the access point which the UDPXY application uses.
Maximum client number	Maximum number of devices from the access point's LAN which will be served by the application.
Buffer size for incoming data	Size of intermediate buffer for received data. By default, the minimum acceptable value is specified.
Buffer size for data transferred to client	Size of intermediate buffer for transmitted data. By default, the minimum acceptable value is specified.
WAN interface	From the drop-down list, select a WAN connection which will be used for operation with streaming video.

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

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

udpxy status:

Server Process ID	Accepting clients on	Multicast address	Active clients
13394	192.168.0.50:4022	192.168.161.244	0

Available HTTP requests:

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

udpxy v. 1.0 (Build 23) standard - [Wed Feb 12 15:27:35 2020]
udpxy and udxrec are Copyright (C) 2008-2013 Pavel V. Cherenkov and licensed under GNU GPLv3

Figure 135. The UDPXY application status page.

IGMP

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

On the **Advanced / IGMP** page, you can allow the access point to use IGMP.

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.

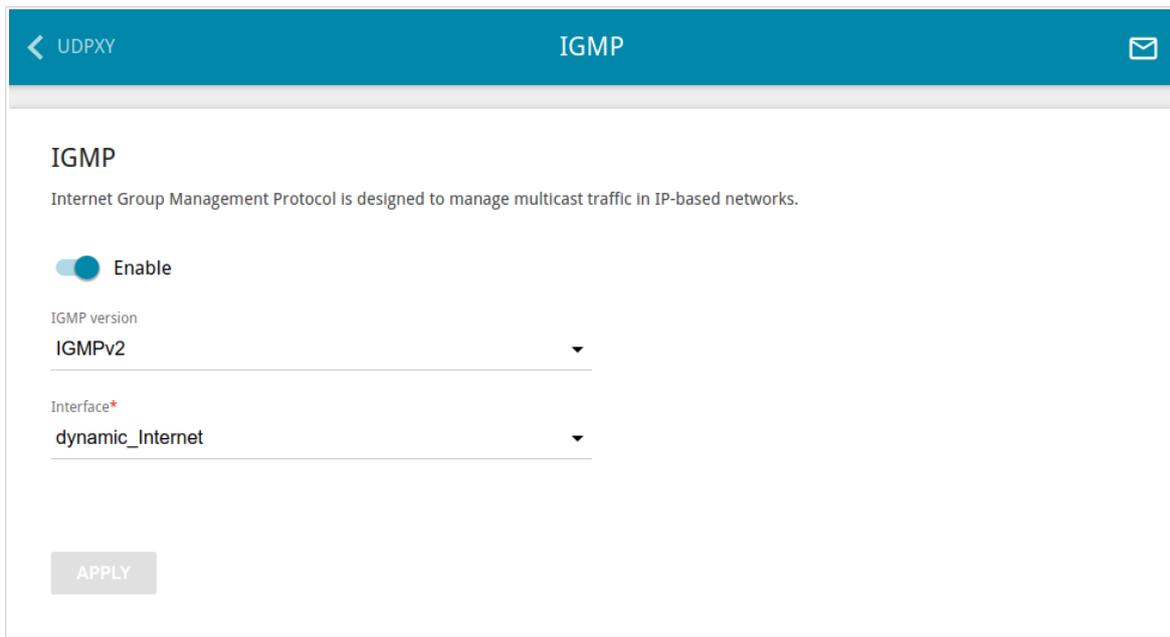


Figure 136. The **Advanced / IGMP** page.

The following elements are available on the page:

Parameter	Description
Enable	Move the switch to the right to enable IGMP.
IGMP version	Select a version of IGMP from the drop-down list.
Interface	From the drop-down list, select a connection of the Dynamic IPv4 or Static IPv4 type for which you need to allow multicast traffic (e.g. streaming video).

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

ALG/Passthrough

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

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

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

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

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

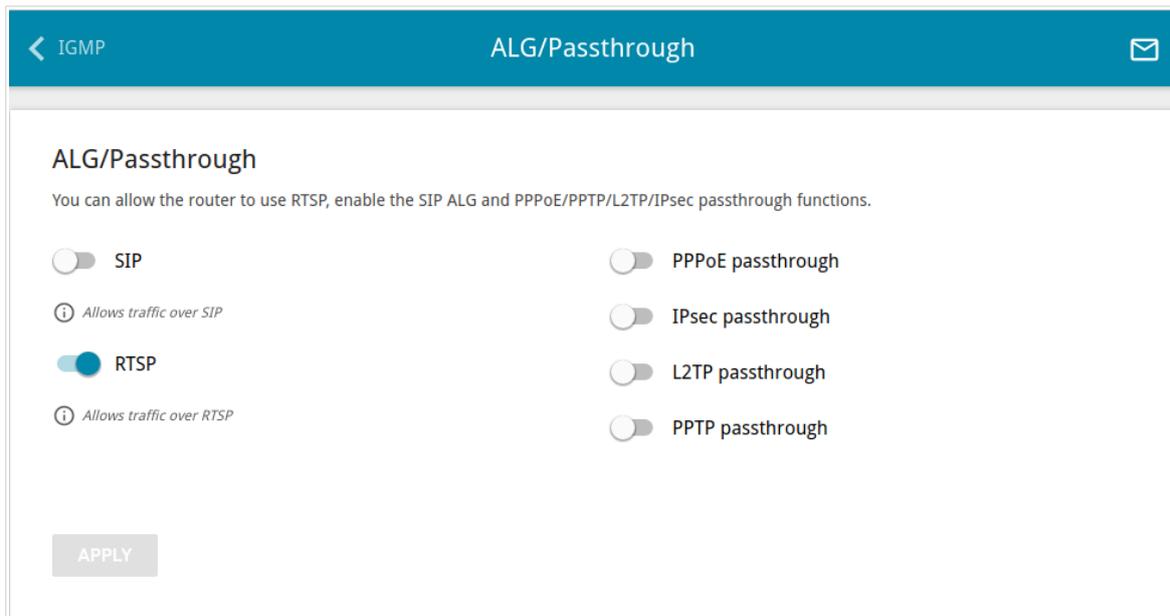


Figure 137. The **Advanced / ALG/Passthrough** page.

The following elements are available on the page:

Parameter	Description
SIP	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled access point. ⁹
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.

⁹ On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / ALG/Passthrough** page, connect an Ethernet cable between the LAN port of the access point and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

IPsec

This page is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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

IPsec is a protocol suite for securing IP communications.

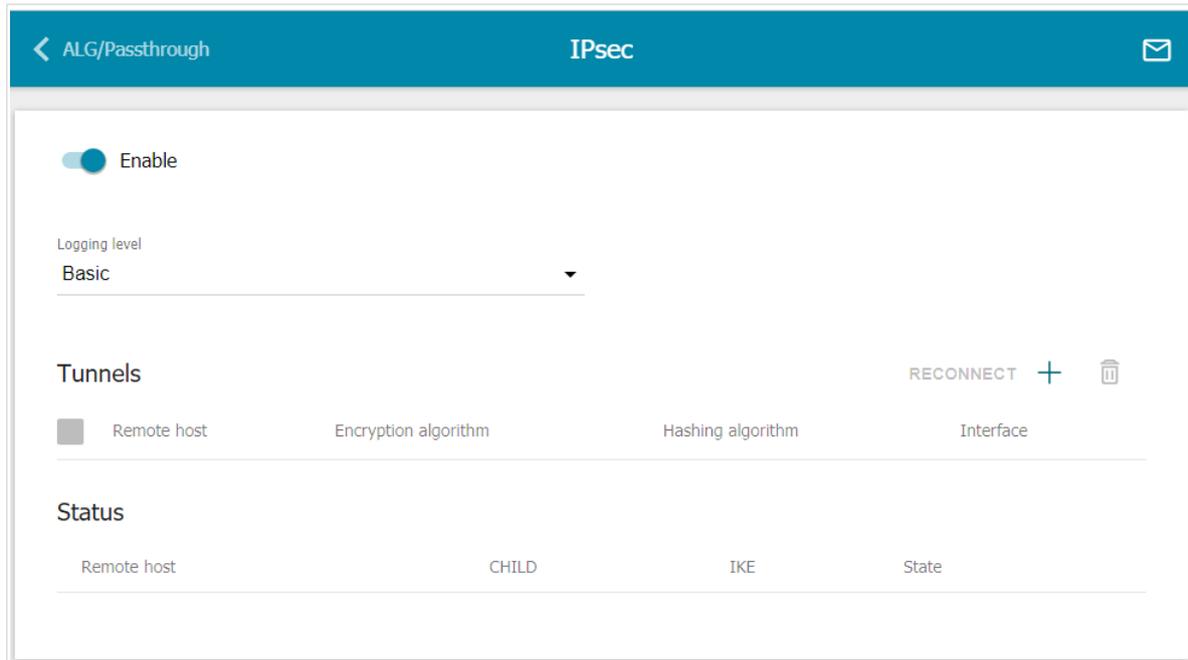


Figure 138. The **Advanced / IPsec** page.

To allow IPsec tunnels, move the **Enable** switch to the right. Upon that the **Tunnels** and **Status** sections and the **Logging level** drop-down list are displayed on the page.

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

From the **Logging level** drop-down list, select a detail level of messages recorded to the system log or leave the value specified by default. The **Basic** value is recommended to establish an IPsec tunnel faster. To view the log, go to the **System / Log** page (see the **Log** section, page 211).

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

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

The screenshot shows the 'IPsec/Adding' configuration page. At the top, there is a blue header with a back arrow, 'IPsec', 'IPsec/Adding', and a mail icon. Below the header, there is a toggle switch for 'Enable' which is turned on. Under the 'General Settings' section, there is a 'Dynamic IPsec' toggle switch which is turned off. To the right of this is a 'DPD - Dead Peer Detection' section with an 'Enable DPD' toggle switch turned on. Below this are input fields for 'DPD delay (in seconds)*' (value: 30) and 'DPD timeout, sec*' (value: 120). There is also a 'TCP MSS' dropdown menu set to 'Path MTU discovery'. On the left side, there are several dropdown menus: 'Type' (set to 'Address'), 'Remote host*', 'Identifier value*', 'Local WAN' (set to 'All interfaces'), 'NAT Traversal' (set to 'Enabled'), and another 'Type' dropdown (set to 'TUNNEL'). There is also a 'Pre-shared key*' field with a copy icon.

Figure 139. 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 access point via IPsec protocol. Such a setting can be specified for one IPsec tunnel only. Connection requests via this tunnel can be sent by a remote host only.

Parameter	Description
<p>Type</p>	<p>Select an identification method for the remote host (router) from the drop-down list:</p> <ul style="list-style-type: none"> • Address: The remote host is identified by its IP address. • FQDN: The remote host is identified by its domain name. <p>The drop-down list is displayed if the Dynamic IPsec switch is moved to the left.</p>
<p>Remote host</p>	<p>Enter the remote subnet VPN gateway IP address if the Address value is selected from the Type drop-down list.</p> <p>Enter the remote subnet VPN gateway domain name if the FQDN value is selected from the Type drop-down list.</p> <p>The field is available for editing if the Dynamic IPsec switch is moved to the left.</p>
<p>Identifier value</p>	<p>Specify a unique name of the tunnel.</p>
<p>Pre-shared key</p>	<p>A PSK key for mutual authentication of the parties. Click the Show icon (🔑) to display the entered key.</p>
<p>Local WAN</p>	<p>A WAN connection through which the tunnel will pass. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> • Interface: When this value is selected, the Interface drop-down list is displayed. Select an existing WAN connection from the list. • All interfaces: When this value is selected, the access point uses the default WAN connection.
<p>NAT Traversal</p>	<p>The NAT Traversal function allows VPN traffic to pass through the NAT-enabled device. DAP-600P allows to forcibly encapsulate VPN traffic in UDP packets for passing through a remote device regardless of whether it supports address translation.</p> <p>If you need to enable forced encapsulation of VPN traffic, select the Enabled value.</p> <p>If you need to disable forced encapsulation of VPN traffic, select the Disabled value.</p>

Parameter	Description
<p>Type</p>	<p>An operation mode of the IPsec tunnel. Select a value from the drop-down list.</p> <ul style="list-style-type: none"> • TUNNEL: As a rule, it is used to create a secure connection to remote networks. In this mode, the source IP packet is fully encrypted and added to a new IP packet and data transfer is based on the header of the new IP packet. • TRANSPORT: As a rule, it is used to encrypt data stream within one network. In this mode, only the content of the source IP packet is encrypted, its header remains unchanged and data transfer is based on the source header.
<p>Enable DPD</p>	<p>Move the switch to the right to enable using DPD protocol for this tunnel. Such a setting allows to check the status of the remote host: if encrypted packets exchange between the access point and the remote host breaks down, the access point starts sending DPD messages to the remote host. If the switch is moved to the left, the DPD delay and DPD timeout fields are not available for editing.</p>
<p>DPD delay</p>	<p>A time period (in seconds) between DPD messages. By default, the value 30 is specified.</p>
<p>DPD timeout</p>	<p>A waiting period for the response to a DPD message (in seconds). If the host does not answer in the specified time, the access point breaks down the tunnel connection, updates information on it, and tries to reestablish the connection. By default, the value 120 is specified.</p>
<p>TCP MSS</p>	<p><i>Maximum Segment Size of a TCP packet.</i> This parameter influences the size of a TCP packet which will be sent from the remote host to the access point.</p> <p>If the Manual value is selected, you can specify the value of this parameter for each subnet of the tunnel in the MTU field. The field is displayed in the window for adding a subnet in the Tunneled Networks section.</p> <p>If the Path MTU discovery value is selected, the parameter will be configured automatically for all created subnets.</p>

The First Phase	The Second Phase
Encryption mode CBC	Encryption mode CBC
Encryption key length 128	Encryption key length 128
First phase encryption algorithm DES	Second phase encryption algorithm DES
Hashing mode HMAC	Hashing mode HMAC
Size of hash 96	Size of hash 96
Hashing algorithm MD5	Hashing algorithm MD5
First phase DHgroup type MODP1024	<input checked="" type="checkbox"/> Enable PFS
IKE-SA lifetime* 10800	Second phase DHgroup type MODP1024
<input type="checkbox"/> Aggressive Mode	IPsec-SA lifetime* 3600
IKE version 1	

Figure 140. The page for adding an IPsec tunnel. **The First Phase / The Second Phase** sections.

Parameter	Description
The First Phase	
Encryption mode	Select an encryption mode from the drop-down list.
Encryption key length	The encryption key length in bits.
First phase encryption algorithm	Select an available encryption algorithm from the drop-down list.
Hashing mode	Select a hashing mode from the drop-down list.
Size of hash	The length of the hash in bits.
Hashing algorithm	Select a 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.

Parameter	Description
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 be greater than the value specified in the IPsec-SA lifetime field.
Aggressive Mode	The mode which provides faster operation as it skips several stages of negotiation of the authentication procedures. Move the switch to the right to enable the mode. Move the switch to the left to disable the mode. The switch is displayed on the page if 1 is selected from the IKE version drop-down list.
IKE version	IKE (<i>Internet Key Exchange</i>) is a protocol of keys exchange between two hosts of VPN connections. Select a version of the protocol from the drop-down list.
The Second Phase	
Encryption mode	Select an encryption mode from the drop-down list.
Encryption key length	The encryption key length in bits.
Second phase encryption algorithm	Select an available encryption algorithm from the drop-down list.
Hashing mode	Select a hashing mode from the drop-down list.
Size of hash	The length of the hash in bits.
Hashing algorithm	Select a hashing algorithm from the drop-down list.
Enable PFS	Move the switch to the right to enable the PFS option (<i>Perfect Forward Secrecy</i>). If the switch is moved to the right, a new encryption key exchange will be used for Phase 2. This option enhances the security level of data transfer, but increases the load on DAP-600P.
Second phase DHgroup type	A Diffie-Hellman key group for Phase 2. Select a value from the drop-down list. The drop-down list is available if the Enable PFS switch is moved to the right.

Parameter	Description
IPsec-SA lifetime	The lifetime of Phase 2 keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should be greater than zero.

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

If the IPsec tunnel operates over IKEv1 (**1** is selected from the **IKE version** list in the **The First Phase** section), you can create only one subnet.

If the IPsec tunnel operates over IKEv2 (**2** is selected from the **IKE version** list in the **The First Phase** section), you can create several subnets.

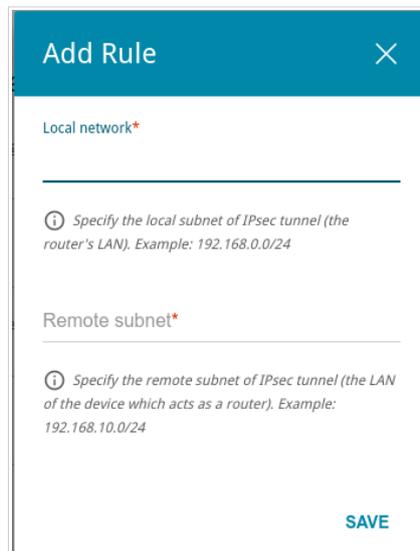


Figure 141. The page for adding an IPsec tunnel. The window for adding a tunneled network.

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.
MTU	The maximum size (in bytes) of a non-fragmented packet. The field is displayed when the Manual value is selected from the TCP MSS drop-down list in the General Settings section.

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

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

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

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

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

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

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

Firewall

This section is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

In this menu you can configure the firewall of the access point:

- add rules for IP filtering
- create virtual servers
- define a DMZ
- 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.

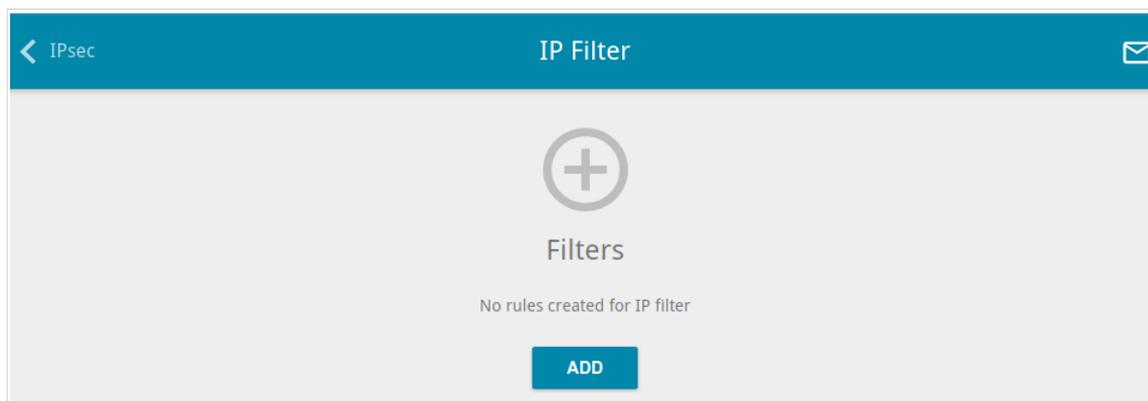


Figure 142. The **Firewall / IP Filter** page.

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

Figure 143. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
General Settings	
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Name	A name for the rule for easier identification. You can specify any name.

Parameter	Description
Action	<p>Select an action for the rule.</p> <ul style="list-style-type: none"> • Allow: Allows packet transmission in accordance with the criteria specified by the rule. • Deny: Denies packet transmission in accordance with the criteria specified by the rule.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Direction	<p>The direction of network packet transmission to which the rule will be applied. Select the relevant value from the drop-down list.</p> <ul style="list-style-type: none"> • LAN to WAN: The rule will be applied to the packets transmitted from the local network to the external network. • WAN to LAN: The rule will be applied to the packets transmitted from the external network to the local network. • LAN to Router: The rule will be applied to the packets transmitted from the local network to DAP-600P.
Source IP address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	<p>The source host start IPv4 or IPv6 address.</p> <p>If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank.</p> <p>You can choose a device connected to the access point's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).</p>
End IPv4 address / End IPv6 address	The source host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The source subnet IPv4 or IPv6 address. The field is displayed when the Subnet value is selected from the Set as drop-down list.
Destination IP address	
Set as	Select the needed value from the drop-down list.

Parameter	Description
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 access point's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The destination host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The destination subnet IPv4 or IPv6 address. The field is displayed when the Subnet value is selected from the Set as drop-down list.
Ports	
Destination port	A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.
Set source port manually	Move the switch to the right to specify a port of the source IP address manually. Upon that the Source port field is displayed.
Source port	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

Click the **APPLY** button.

To set a schedule for the IP filter rule, click the **Add Schedule** button (🕒) in the line corresponding to this rule. In the opened window, you can create a new schedule (see the *Schedule* section, page 207) or use the existing one. Existing schedules are displayed in the **Interval of execution** drop-down list in the simplified mode.

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

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

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

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

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

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 144. The **Firewall / Virtual Servers** page.

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

Figure 145. The page for adding a virtual server.

You can specify the following parameters:

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

Parameter	Description
NAT Loopback	Move the switch to the right in order to let the users of the access point's LAN access the local server using the external IP address of the access point or its DDNS name (if a DDNS service is configured). Users from the external network access the access point using the same address (or DDNS name).
Public Network Settings	
Remote IP	The IP address of the host/subnet of the client that will connect to the virtual server. To add one more IP address, click the ADD REMOTE IP button and enter the address in the displayed line. To remove the IP address, click the Delete icon (✕) in the line of the address.
Public port	A port of the access point from which traffic is directed to the IP address specified in the Private IP field in the Private Network Settings section. You can specify one port or several ports separated by a comma.
Private Network Settings	
Private IP	The IP address of the server from the local area network. To choose a device connected to the access point's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).
Private port	A port of the IP address specified in the Private IP field to which traffic is directed from the Public port . You can specify one port or several ports separated by a comma.

Click the **APPLY** button.

To 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 device, the DMZ implements the capability to transfer a request coming to a port of the access point 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.

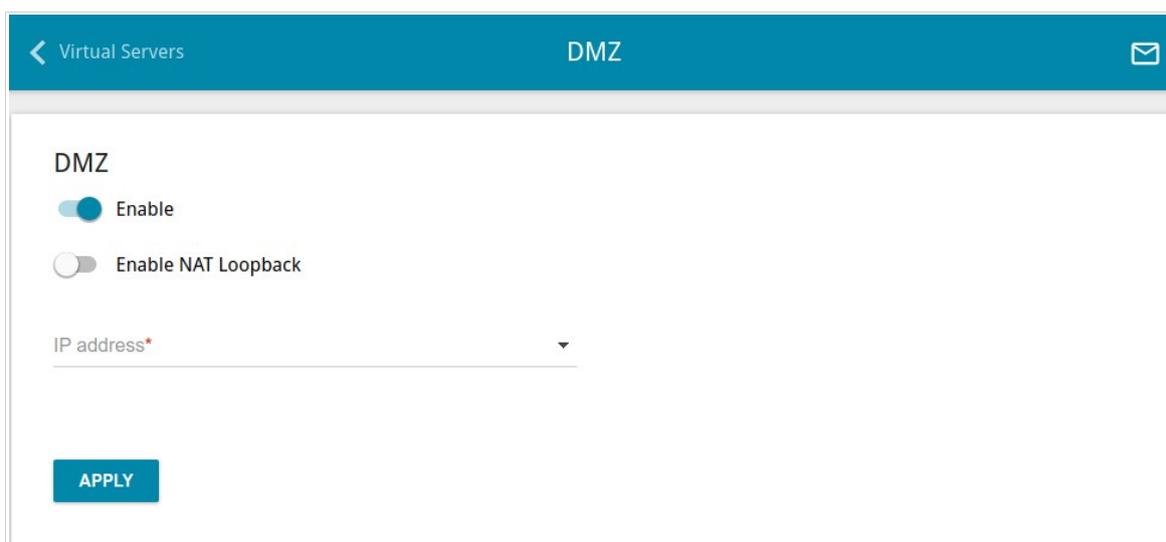


Figure 146. The **Firewall / DMZ** page.

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

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

Click the **APPLY** button.

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

URL Filter

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

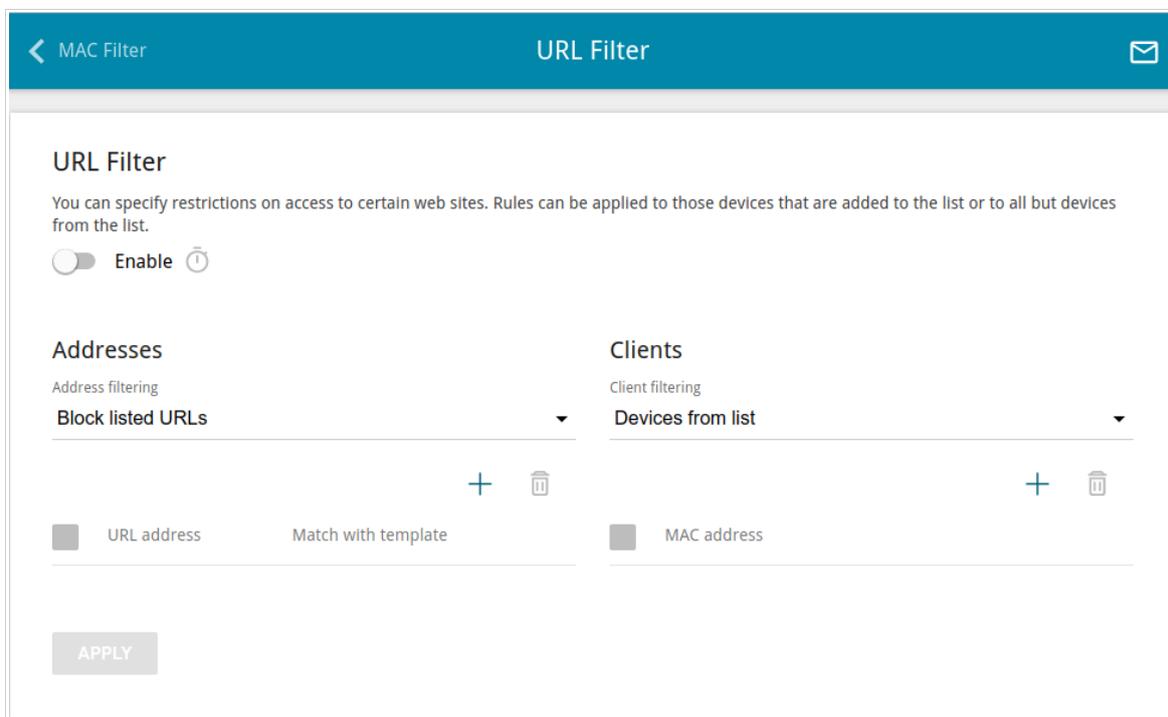


Figure 147. The **Firewall / URL Filter** page.

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

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

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

Parameter	Description
URL address	A URL address, a part of URL address, or a keyword.
Match with template	<p>Select a value from the drop-down list.</p> <ul style="list-style-type: none"> • Full: The request address should exactly match the value specified in the field above. • Begin: The request address should begin with the value specified in the field above. • End: The request address should end with the value specified in the field above. • Partly: The request address should contain the value specified in the field above in any part of it.

Click the **SAVE** button.

To remove a URL address from the list, select the checkbox located to the left of the relevant address in the table and click the **DELETE** button (). Also you can remove an address in the editing window.

In the **Clients** section, you can define devices to which the specified restrictions will be applied. Select a needed value from the **Client filtering** drop-down list:

- **Devices from list:** When this value is selected, the access point applies restrictions only to the devices specified in the **Clients** section;
- **All but devices from list:** When this value is selected, the access point does not apply restrictions to the devices specified in the **Clients** section, but applies restrictions to other devices.

To add a client to the list, in the **Clients** section, click the **ADD** button (). In the opened window, in the **MAC address** field, enter the MAC address of the device from the LAN. You can enter the MAC address of a device connected to the access point's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically) and click the **SAVE** button.

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

To set a schedule for the URL filter, click the **Set Schedule** button (). In the opened window, you can create a new schedule (see the *Schedule* section, page 207) or use the existing one. Existing schedules are displayed in the **Interval of execution** drop-down list in the simplified mode.

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

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

To change or delete the schedule for URL filter, click the **Set Schedule** button () in the **URL Filter** section. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

After completing configuration of the URL filter, click the **APPLY** button.

System

In this menu you can do the following:

- change the password used to access the access point's settings
- restore the factory default settings
- create a backup of the access point's configuration
- restore the access point's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the access point
- change the web-based interface language
- update the firmware of the access point
- configure automatic notification on new firmware version
- enable/disable Wi-Fi connection and configure automatic reboot of the device on a schedule, and set a schedule for different filter rules
- 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 access point
- trace the route to a host
- allow or forbid access to the access point via TELNET and SSH
- configure automatic synchronization of the system time or manually configure the date and time for the access point
- enable the Auto Provision function.

Configuration

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

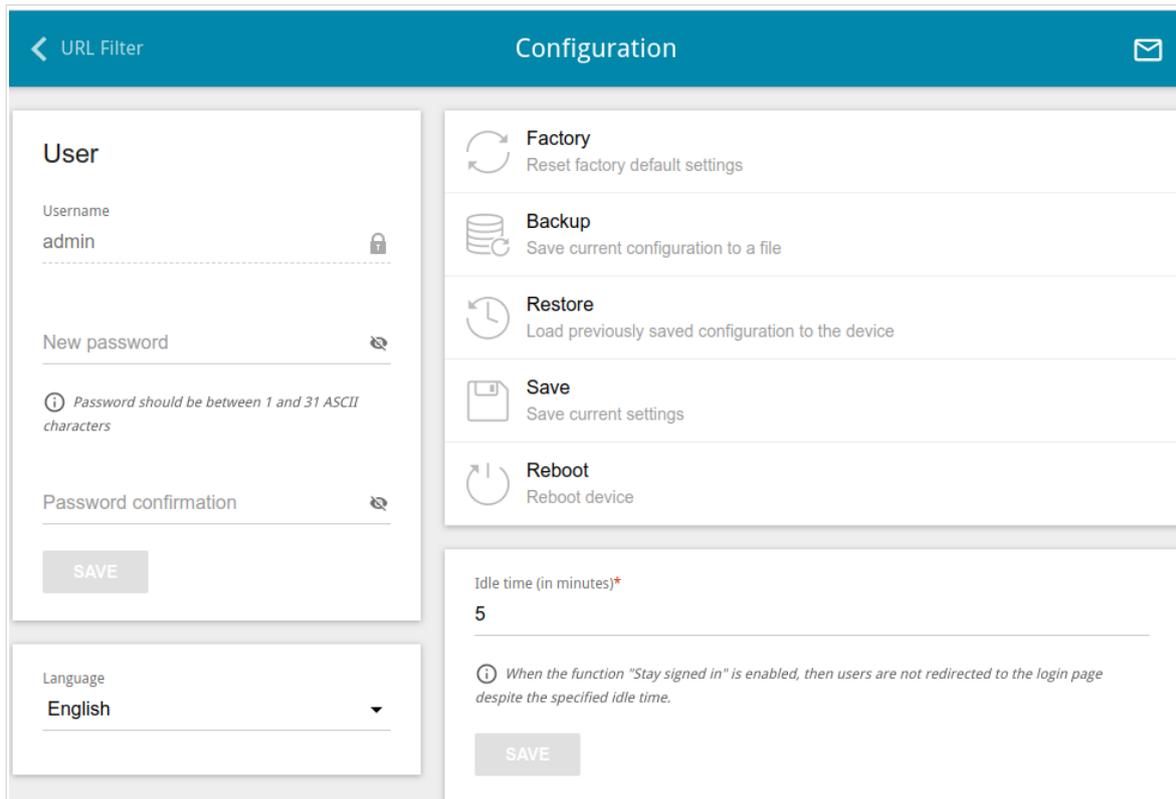


Figure 148. The **System / Configuration** page.

In order to change the password for the administrator account, in the **User** section, enter a new password in the **New password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.¹⁰ Click the **Show** icon (👁) to display the entered values. Then click the **SAVE** button.

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

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

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

The following buttons are also available on the page:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button (see the <i>Back Panel</i> section, page 14).
Backup	Click the button to save the configuration (all settings of the access point) 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 access point) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The access point saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

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

Firmware Update

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

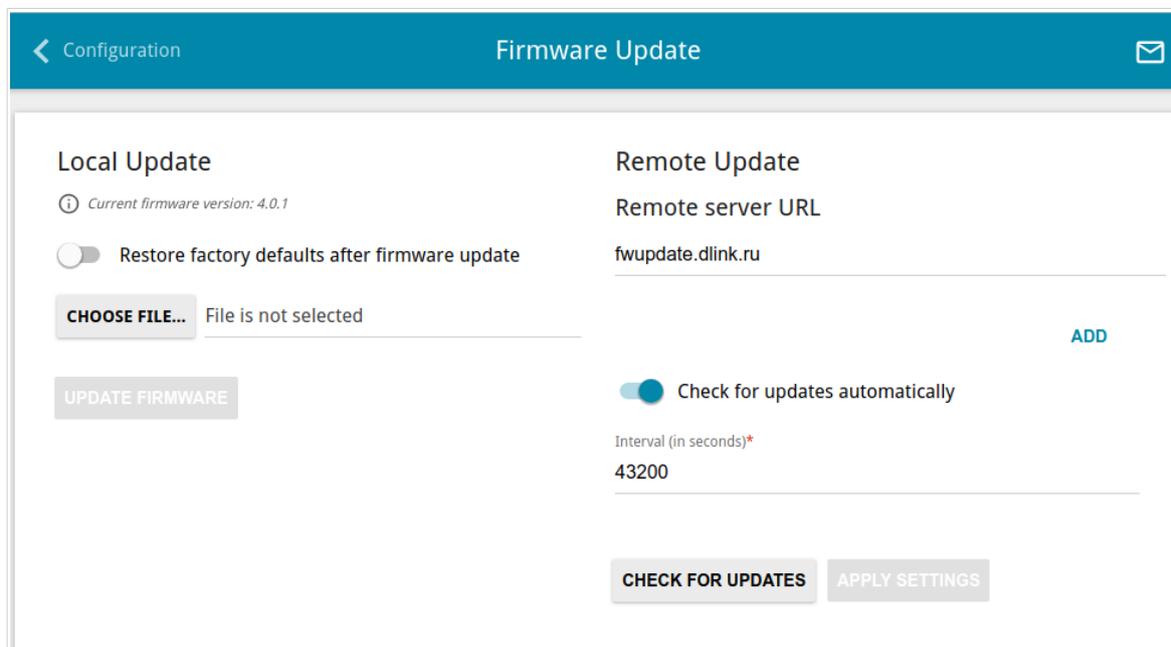


Figure 149. The **System / Firmware Update** page.

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

By default, the automatic check for the access point's firmware updates is enabled. If the **Access point** or **Repeater** mode was selected in the Initial Configuration Wizard and the **Static** value is selected from the **Mode of local IP address assignment** list on the **Connections Setup / LAN** page, the **Gateway IP address** field should also be filled in on order to realize automatic check.

If a firmware update is available, a notification will be displayed in the top right corner of the page.

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

To enable the automatic check for firmware updates, in the **Remote Update** section, move the **Check for updates automatically** switch to the right. In the **Interval** field, specify the time period (in seconds) between checks or leave the value specified by default (**43200**).

By default, in the **Remote server URL** field, the D-Link update server address (**fwupdate.dlink.ru**) is specified. To add one more address, click the **ADD** button and enter the address in the displayed line. To remove the address, click the **Delete** icon (**x**) in the line of the address.

Click the **APPLY SETTINGS** button.

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

Local Update



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

To update the firmware of the access point locally, follow the next steps:

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **CHOOSE FILE** button in the **Local Update** section on the **System / Firmware Update** page to locate the new firmware file.
3. If you want to restore the factory default settings immediately after updating the firmware, move the **Restore factory defaults after firmware update** switch to the right.
4. Click the **UPDATE FIRMWARE** button.
5. Wait until the access point is rebooted (about one and a half or two minutes).
6. Log into the web-based interface using the login (**admin**) and the current password.

If after updating the firmware the access point 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 access point is rebooted.

Remote Update

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

To update the firmware of the access point 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 access point 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 access point 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 access point is rebooted.

Schedule

On the **System / Schedule** page, you can enable/disable Wi-Fi connection and configure automatic reboot of the device on a schedule, and set a schedule for different filter rules.

! Before creating a schedule you need to configure automatic synchronization of the system time with a time server on the Internet (see the **System Time** section, page 218).

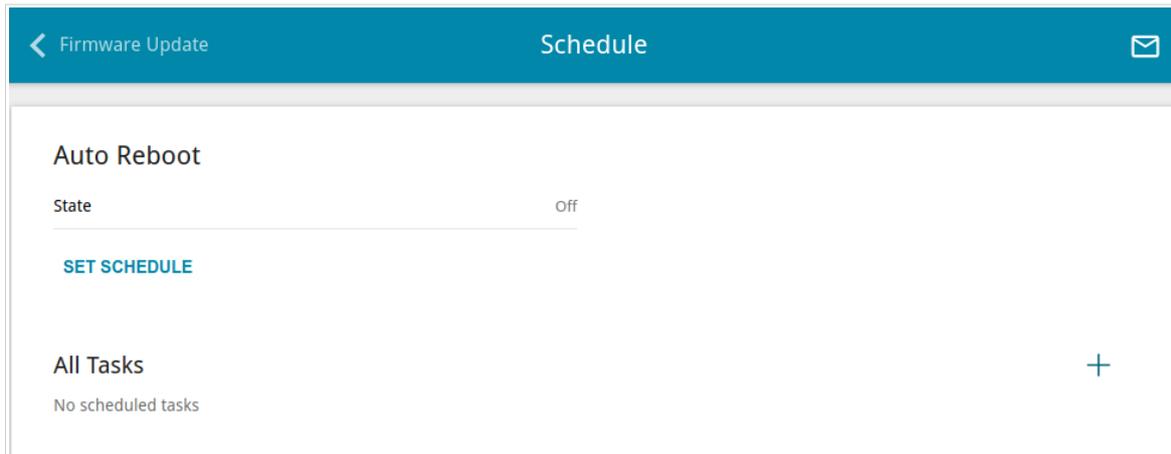


Figure 150. The **System / Schedule** page.

To configure automatic reboot of the device on a schedule, click the **SET SCHEDULE** button in the **Auto Reboot** section.¹¹

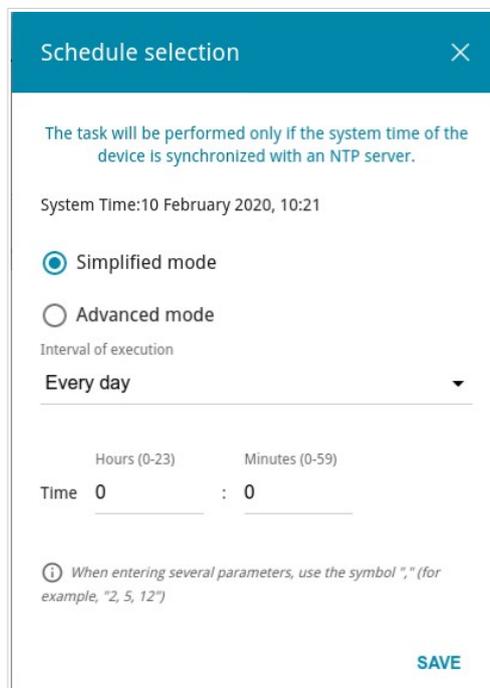


Figure 151. The window for configuring automatic reboot on a schedule.

¹¹ The function will be implemented in the next firmware version.

In the opened window, in the **System Time** field, the system time of the device is displayed. You can select the **Simplified mode** choice of the radio button and specify the following parameters:

Parameter	Description
Simplified mode	
Interval of execution	Specify the time period for the device's reboot. <ul style="list-style-type: none"> • Every day: When this value is selected, the Time field is displayed in the section. • Every week: When this value is selected, the names of days of the week and the Time field are displayed in the section. • Every month: When this value is selected, the Day of month and Time fields are displayed in the section.
Time	Specify the time for the device's reboot.
Days of week	Select a day or days of the week when the device will be automatically rebooted. To do this, select the checkbox located to the left of the relevant value.
Day of month	Specify a day of the month. You can specify one value or several values separated by a comma.

In the advanced mode, you can specify more parameters for the schedule using a cron expression. To do this, select the **Advanced mode** choice of the radio button and specify the needed values in the fields displayed. You can specify one value or several values separated by a comma. You can use the character * (asterisk) to specify the entire range of possible values. Upon that the **Schedule** field will be filled in automatically.

Click the **SAVE** button.

To edit the automatic reboot schedule, click the **EDIT** button in the **Auto Reboot** section. In the opened window, change the needed parameters and click the **SAVE** button.

To disable automatic reboot of the device on a schedule, click the **EDIT** button in the **Auto Reboot** section. In the opened window, click the **DISABLE** button.

To set a schedule for a task which will be applied to a filter rule or will enable/disable Wi-Fi connection, click the **ADD** button (**+**) in the **All Tasks** section.

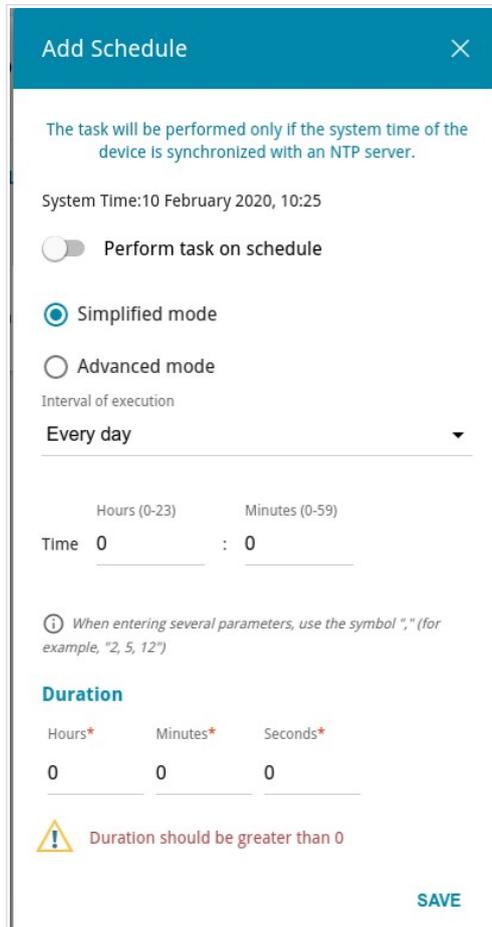


Figure 152. The window for adding a schedule for a task.

In the opened window, in the **System Time** field, the system time of the device is displayed. You can select the **Simplified mode** choice of the radio button and specify the following parameters:

Parameter	Description
Perform task on schedule	Move the switch to the right to enable the schedule. Move the switch to the left to disable the schedule.

Parameter	Description
Simplified mode	
Interval of execution	<p>Specify the time period for performing a task.</p> <ul style="list-style-type: none"> • Every minute. • Every hour: When this value is selected, the Time field is displayed in the section. • Every day: When this value is selected, the Time field is displayed in the section. • Every week: When this value is selected, the names of days of the week and the Time field are displayed in the section. • Every month: When this value is selected, the Day of month and Time fields are displayed in the section.
Duration	Specify the interval during which the task will be performing.
Time	Specify the time when the task should start running.
Days of week	Select a day or days of the week when the task will be performing. To do this, select the checkbox located to the left of the relevant value.
Day of month	Specify a day of the month. You can specify one value or several values separated by a comma.

In the advanced mode, you can specify more parameters for the schedule using a cron expression. To do this, select the **Advanced mode** choice of the radio button and specify the needed values in the fields displayed. You can specify one value or several values separated by a comma. You can use the character * (asterisk) to specify the entire range of possible values. Upon that the **Schedule** field will be filled in automatically.

Click the **SAVE** button.

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

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

To assign a created schedule to a task which will be applied to a filter rule or will enable/disable Wi-Fi connection, go to the relevant page of the web-based interface of the device.

Log

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

Figure 153. The **System / Log** page. The **Settings** tab.

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

Parameter	Description
Type	<p>Select a type of logging from the drop-down list.</p> <ul style="list-style-type: none"> • Local: The system log is stored in the access point'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 access point's memory and sent to the remote host specified in the Server field.
Level	Select a type of messages and alerts/notifications to be logged.

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

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

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

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

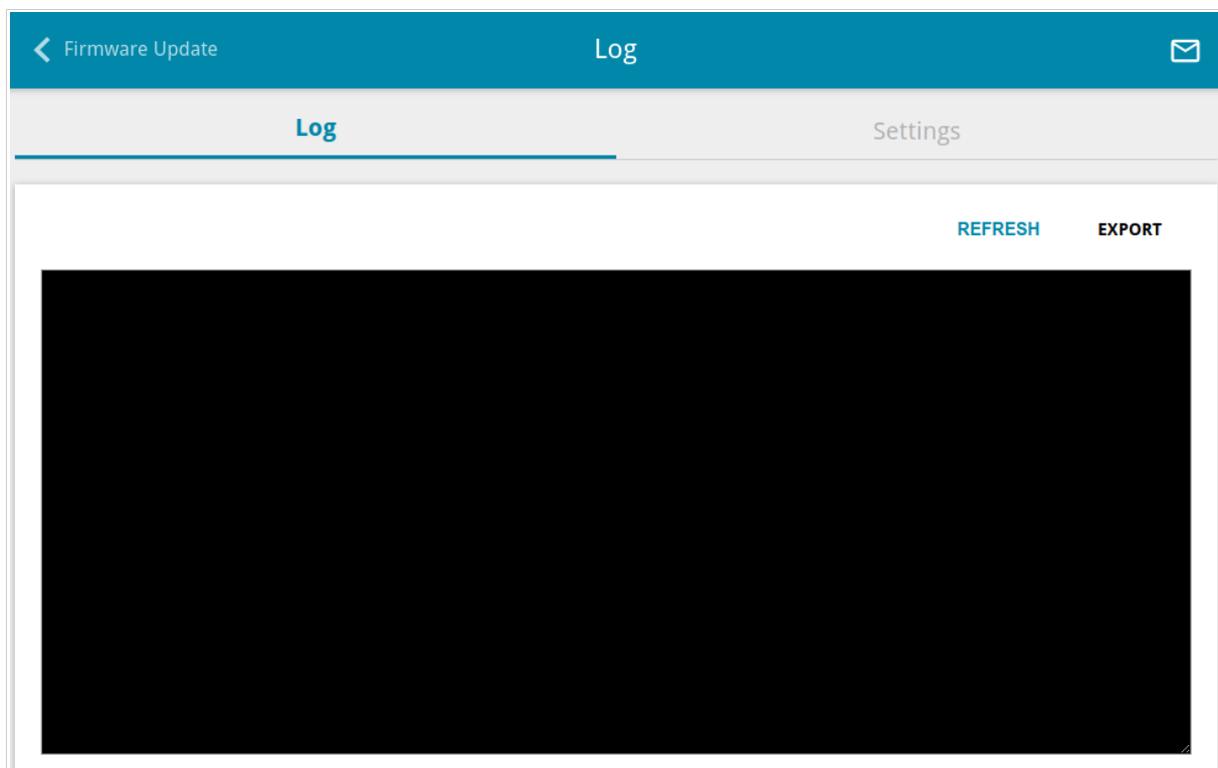


Figure 154. The System / Log page. The Log tab.

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

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

Ping

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

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

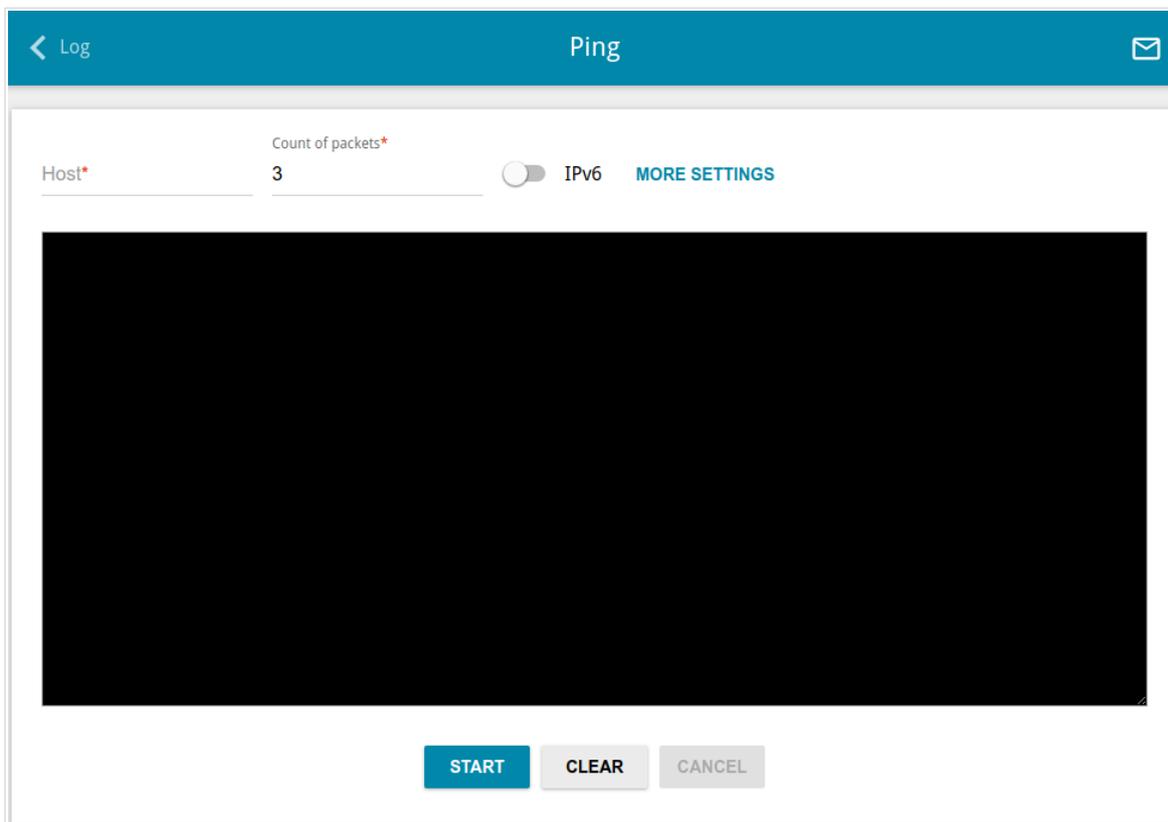
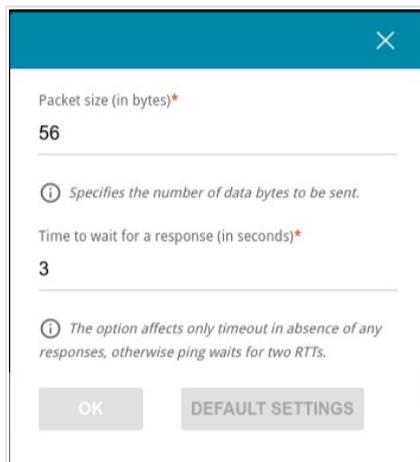


Figure 155. The **System / Ping** page.

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

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



Packet size (in bytes)*
56

Specifies the number of data bytes to be sent.

Time to wait for a response (in seconds)*
3

The option affects only timeout in absence of any responses, otherwise ping waits for two RTTs.

OK DEFAULT SETTINGS

Figure 156. The **System / Ping** page. The additional settings window.

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

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

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

If you need to interrupt the check, click the **CANCEL** button (the button is available from the moment the check starts).

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

Traceroute

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

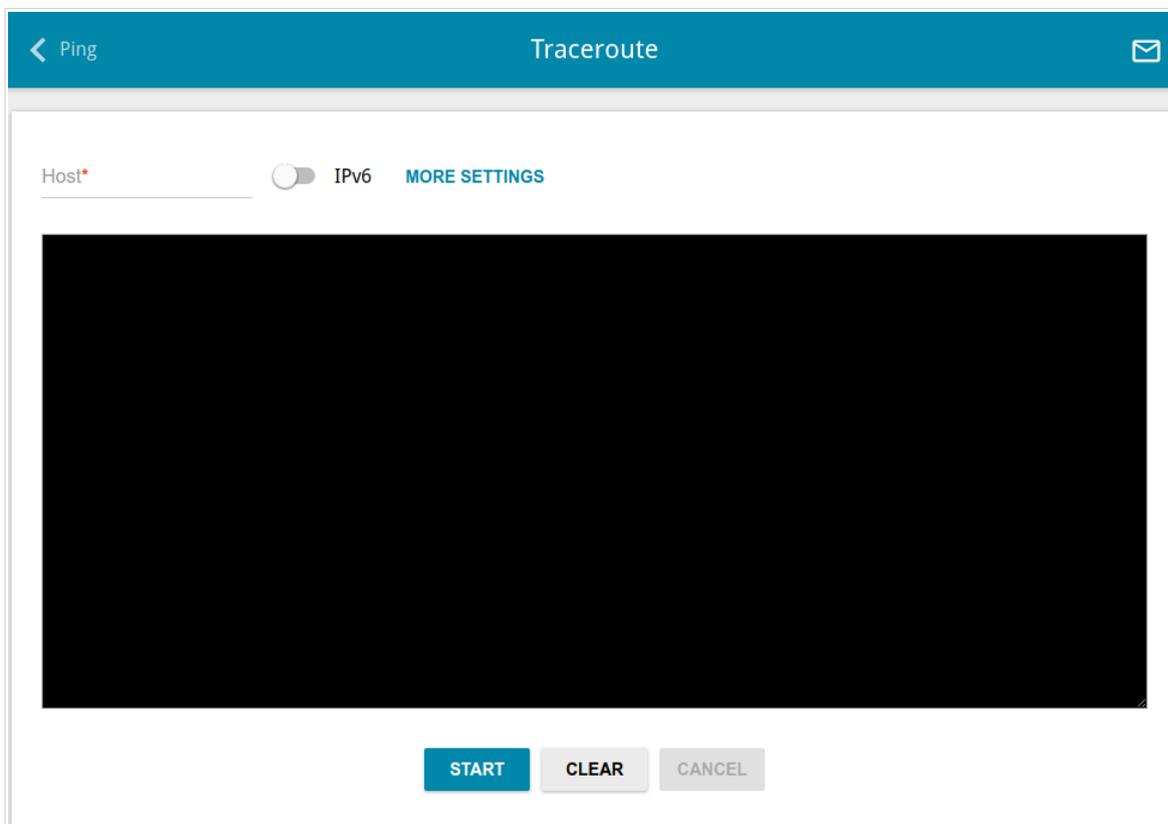


Figure 157. The **System / Traceroute** page.

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

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

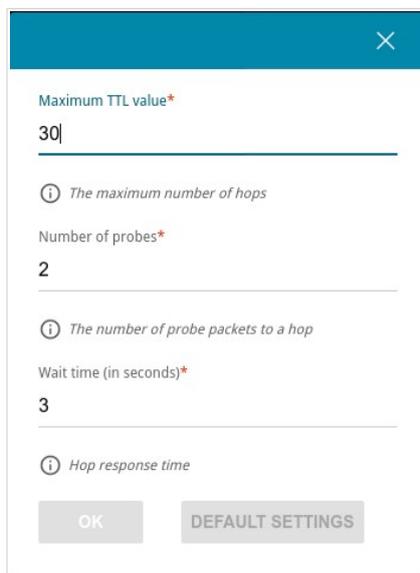


Figure 158. The **System / Traceroute** page. The additional settings window.

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

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

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

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

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

If you need to interrupt the check, click the **CANCEL** button (the button is available from the moment the check starts).

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

Telnet/SSH

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

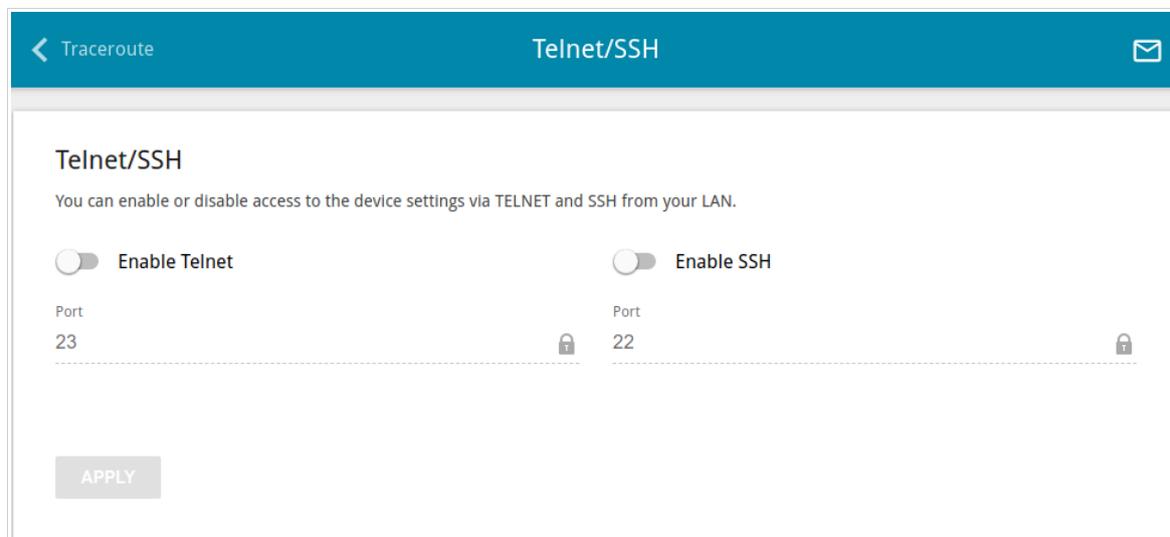


Figure 159. The **System / Telnet/SSH** page.

To enable access via TELNET and/or SSH, move the **Enable Telnet** switch and/or **Enable SSH** switch to the right. In the **Port** field, enter the number of the access point's port through which access will be allowed (by default, the port **23** is specified for Telnet and the port **22** is specified for SSH). Then click the **APPLY** button.

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

System Time

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

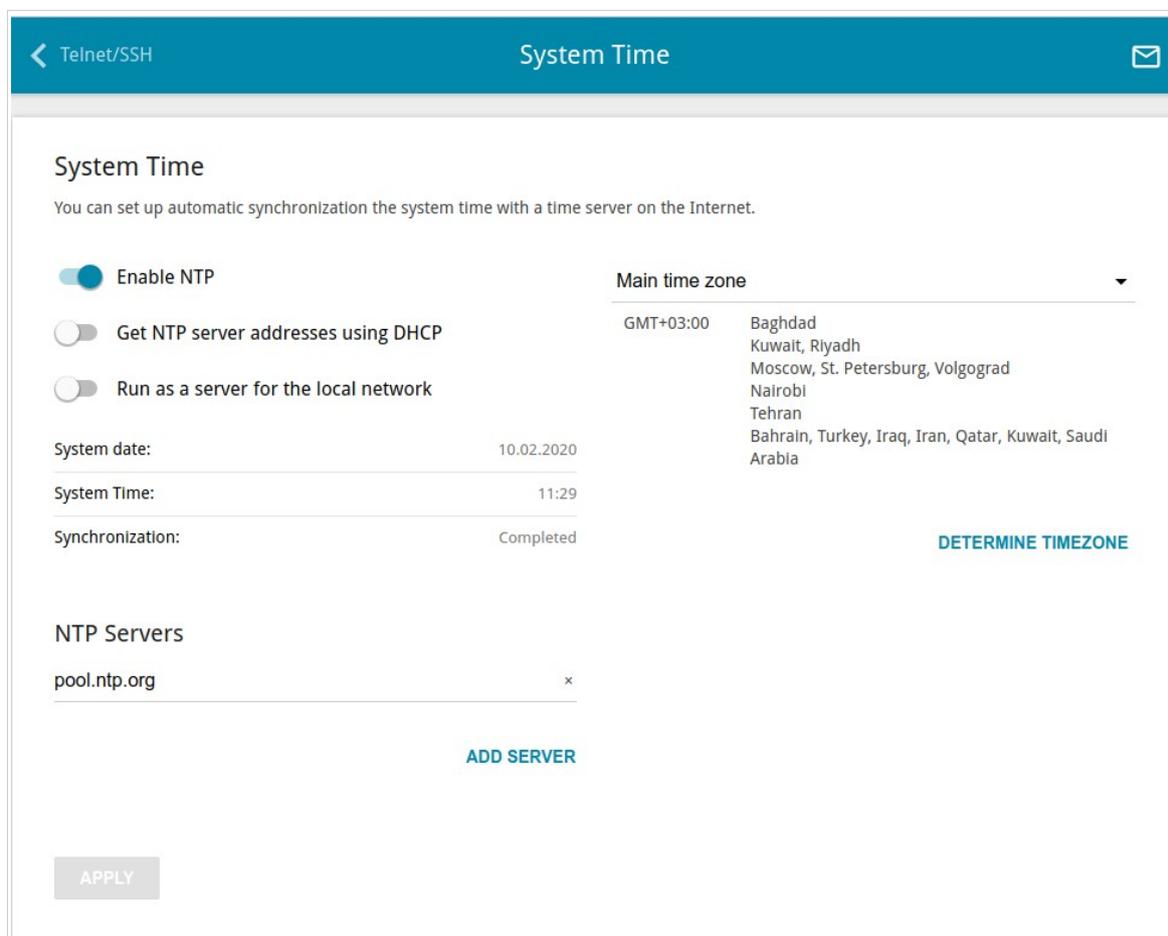


Figure 160. The **System / System Time** page.

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

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

In 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 to the right and click the **APPLY** button. Contact your ISP to clarify if this setting needs to be enabled. If the **Get NTP server addresses using DHCP** switch is moved to the right, the **NTP Servers** section is not displayed.

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



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

Auto Provision

On the **System / Auto Provision** page, you can enable the Auto Provision function.

The Auto Provision function allows your ISP to manage the device's settings remotely: DAP-600P connects to the ISP's server, compares the current configuration file with the configuration file stored on this server, and updates its settings if the files are different.

The screenshot shows the 'Auto Provision' configuration page. At the top, there is a blue header with a back arrow, 'System Time', 'Auto Provision', and an envelope icon. Below the header, the page title 'Auto Provision' is displayed. There are two toggle switches: 'Enable Auto Provision' (currently off) and 'Use BOOTP option' (currently off). To the right of these toggles, the 'Status' is shown as 'No check has been run yet'. A blue 'CHECK STATUS' button is located below the status. Below the toggles, there are four input fields: 'Autoconfiguration server address', 'File name', 'File check period (in seconds)' (set to 1800), and 'Protocol type' (set to TFTP). An 'APPLY' button is located at the bottom left of the form area.

Figure 161. The page for configuring the Auto Provision function.

You can specify the following parameters:

Parameter	Description
Enable Auto Provision	<p>Move the switch to the right to enable the Auto Provision function. If the Access point or Repeater mode was selected in the Initial Configuration Wizard and the Static value is selected from the Mode of local IP address assignment list on the Connections Setup / LAN page, the Gateway IP address field should also be filled in.</p> <p>Move the switch to the left to disable the Auto Provision function.</p>

Parameter	Description
Use BOOTP option	<p>If the switch is moved to the right, the parameters of your ISP's server (the address, the location of the configuration file, and the protocol) are automatically specified using DHCP options 66 and 67. If the Access point or Repeater mode was selected in the Initial Configuration Wizard, the Dynamic value should be selected from the Mode of local IP address assignment list on the Connections Setup / LAN page.</p> <p>If the switch is moved to the left, the parameters of your ISP's server should be specified manually.</p>
Autoconfiguration server address	The IP or URL address of your ISP's server where the configuration file is stored.
File name	The location of the configuration file on the ISP's server.
File check period	A time period (in seconds) between attempts to compare the current configuration file with the configuration file on the ISP's server.
Protocol type	A protocol for communication with the ISP's server where the configuration file is stored.

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

If you need to check manually if the current configuration file corresponds to the configuration file on the ISP's server, click the **CHECK STATUS** button. The check result will be displayed in the **Status** field. If the files are different, the device's settings will be updated.

Yandex.DNS

This section is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

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.

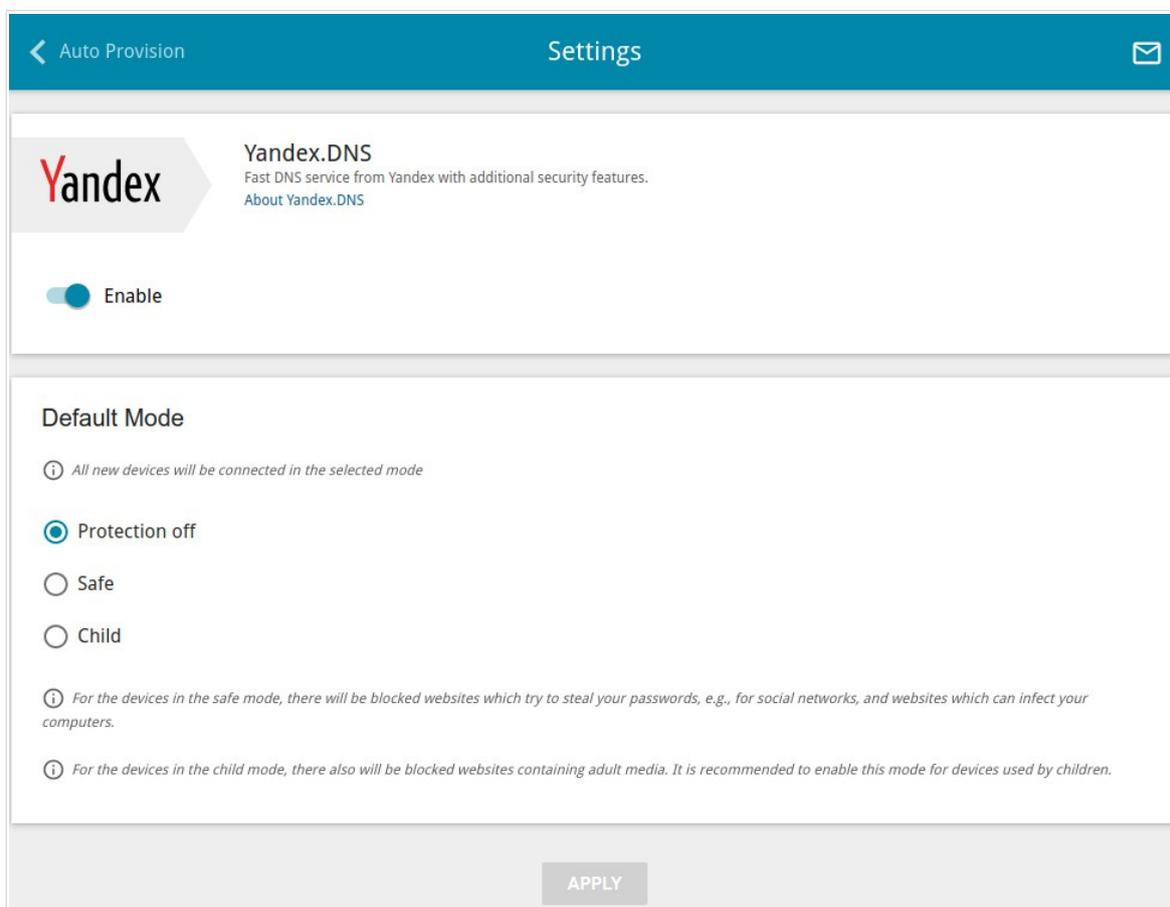


Figure 162. The **Yandex.DNS / Settings** page.

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 access point'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 access point'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.

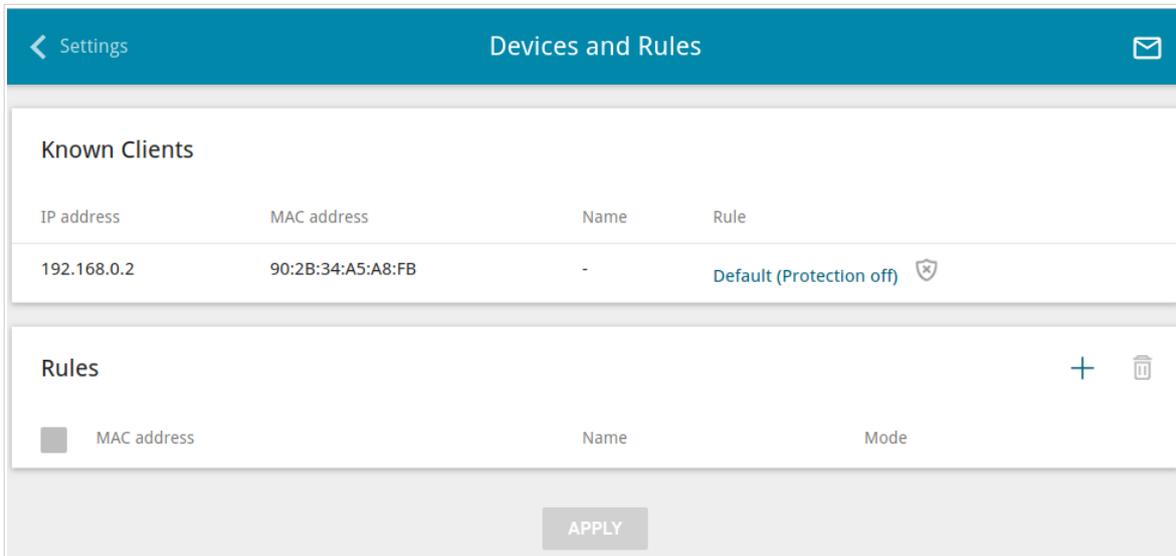


Figure 163. The **Yandex.DNS / Devices and Rules** page.

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

To create 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.

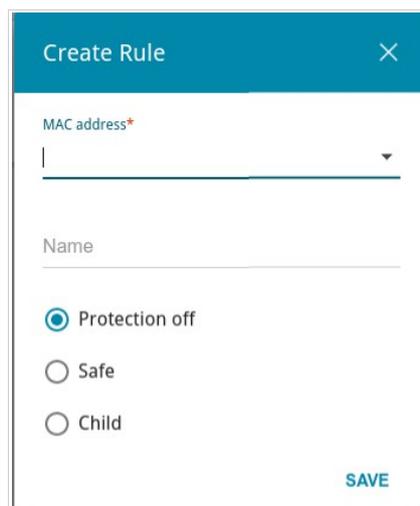


Figure 164. Adding a new rule for the Yandex.DNS service.

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

Parameter	Description
MAC address	The MAC address of a device from the access point's LAN. You can enter the MAC address of a device connected to the access point's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Name	Enter a name for the rule for easier identification. <i>Optional</i> .
Mode	Select an operating mode of the Yandex.DNS service for this rule. <ul style="list-style-type: none">• 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.

SkyDNS

This section is available if the **Router** or **WISP Repeater** mode was selected in the Initial Configuration Wizard.

This menu is designed to configure the SkyDNS service.

SkyDNS is a web content filtering service which provides protection against malicious web sites for devices connected to the access point's network, and also allows to configure filtering, block access to adult web sites, and use search engines safely. In order to use the service, first register an account on the SkyDNS service web site.

Settings

On the **SkyDNS / Settings** page, you can enable the SkyDNS service and specify settings for its operation.

! The SkyDNS service is unavailable when the Yandex.DNS service is enabled.

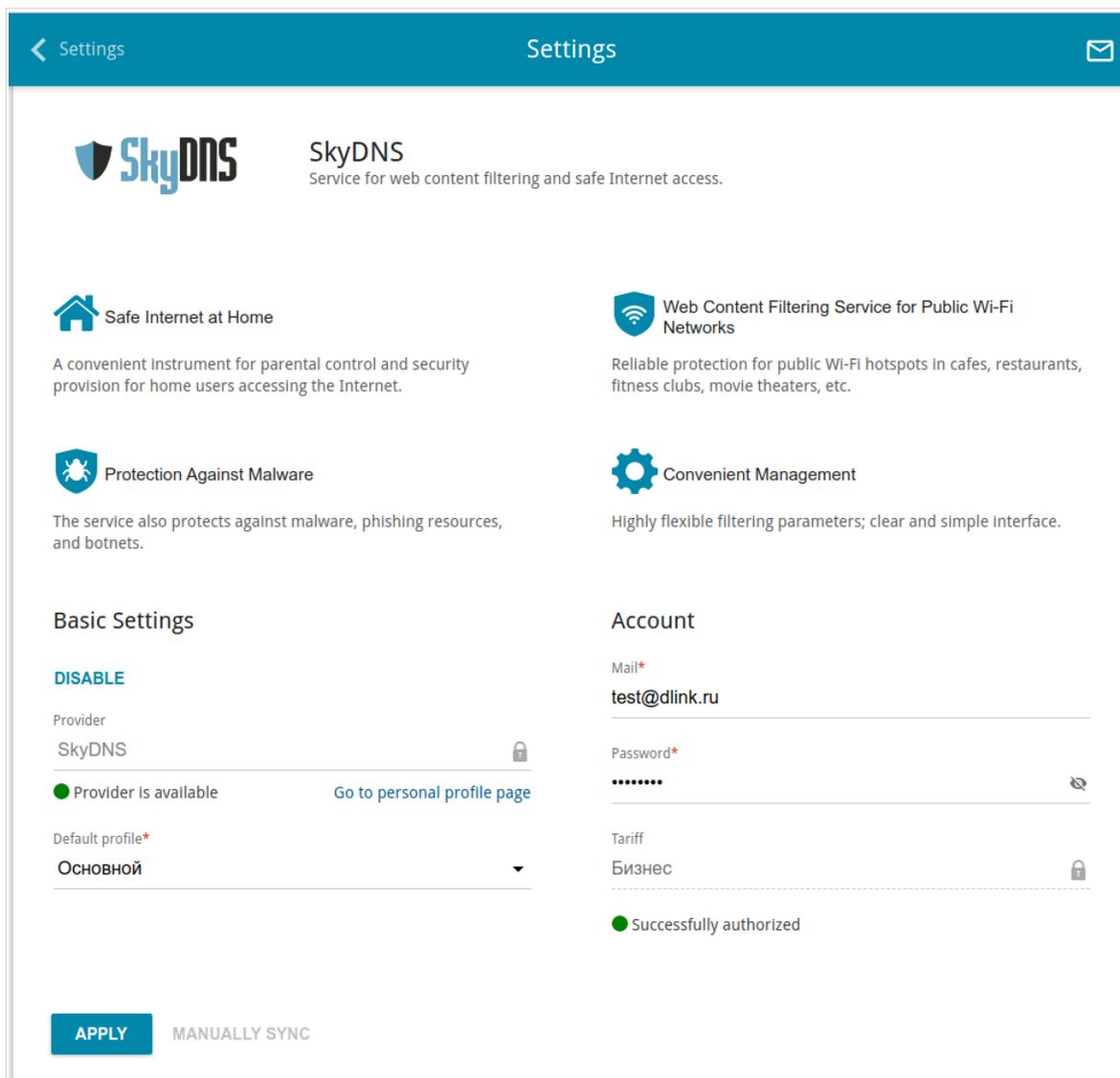


Figure 165. The **SkyDNS / Settings** page.

To enable the SkyDNS service, click the **ENABLE** button. Then in the **Mail** and **Password** fields, enter the account data (the e-mail address and the password correspondingly) specified upon registration on the SkyDNS service web site. Click the **APPLY** button. The account data (authorization status, the tariff used) and the **Default profile** drop-down list will be displayed on the page. If needed, from the **Default profile** list, select another filtering profile which will be used for all devices of your LAN and click the **APPLY** button again.

The default filtering profile will be applied to all devices newly connected to the access point's network.

To change the parameters of your account on the SkyDNS service web site, click the **Go to personal profile page** link.

By default, the account parameters are automatically synchronized with the SkyDNS service web site once an hour. To start synchronization manually, click the **MANUALLY SYNC** button.

To use another account, specify its data in the **Mail** and **Password** fields and click the **APPLY** button.

To disable the SkyDNS service, click the **DISABLE** button.

Devices

On the **SkyDNS / Devices** page, you can assign a specific filtering profile to a device connected to the access point's network.

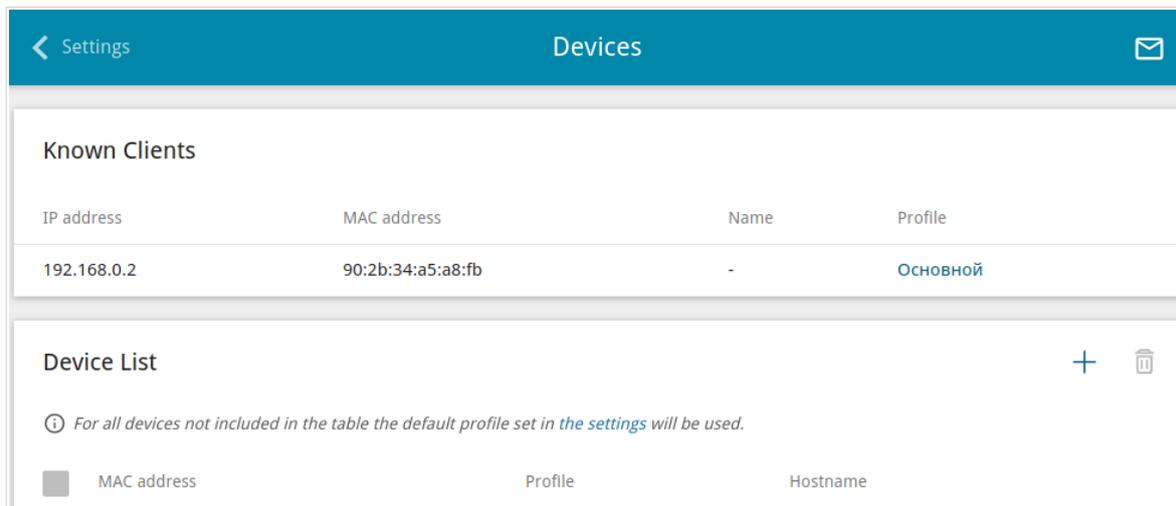


Figure 166. The **SkyDNS / Devices** page.

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

To assign a specific filtering profile for a device, click the **ADD** button () in the **Device List** section or left-click the name of the filtering profile in the line of the device for which a profile should be assigned in the **Known Clients** section.

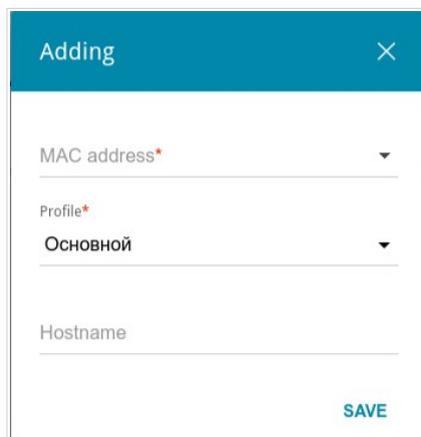


Figure 167. The **SkyDNS / Devices** page. The window for adding a rule.

In the opened window, specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the access point's LAN to which the specified filtering profile will be applied. You can enter the MAC address of a device connected to the access point's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Profile	Select the filtering profile which will be used for the device with the specified MAC address from the drop-down list.
Hostname	Enter a name for the rule for easier identification. <i>Optional.</i>

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

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

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

CHAPTER 5. OPERATION GUIDELINES

Safety Rules and Conditions

Please carefully read this section before installation and connection of the device. Make sure that the device is 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.

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.

The service life of the device is 2 years.

Wireless Installation Considerations

The DAP-600P 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 DAP-600P 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 access point and wireless network devices 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 access point away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone is not in use.

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

AC	Access Category
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BPSK	Binary Phase-shift Keying
BSSID	Basic Service Set Identifier
CCK	Complementary Code Keying
DBSK	Differential Binary Phase-shift Keying
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DPD	Dead Peer Detection
DQPSK	Differential Quadrature Phase-shift Keying
DSL	Digital Subscriber Line
DSSS	Direct-sequence Spread Spectrum
DTIM	Delivery Traffic Indication Message
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ID	Identifier
IGD	Internet Gateway Device

IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPTV	Internet Protocol Television
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light-emitting diode
MAC	Media Access Control
MBSSID	Multiple Basic Service Set Identifier
MIB	Management Information Base
MIMO	Multiple Input Multiple Output
MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Controller
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PBC	Push Button Configuration
PFS	Perfect Forward Secrecy
PIN	Personal Identification Number
PoE	Power over Ethernet
PPP	Point-to-Point Protocol

pppd	Point-to-Point Protocol Daemon
PPPoE	Point-to-point protocol over Ethernet
PPTP	Point-to-point tunneling protocol
PSK	Pre-shared key
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-shift Keying
RADIUS	Remote Authentication in Dial-In User Service
RIP	Routing Information Protocol
RIPng	Next Generation Routing Information Protocol
RTS	Request To Send
RTSP	Real Time Streaming Protocol
SA	Security Association
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
STBC	Space-time block coding
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup