



## **DAP-300P**

### **Wireless N300 PoE Access Point / Router**

## Contents

<b>Chapter 1. Introduction</b> .....	<b>5</b>
<b>Contents and Audience</b> .....	<b>5</b>
<b>Conventions</b> .....	<b>5</b>
<b>Document Structure</b> .....	<b>5</b>
<b>Chapter 2. Overview</b> .....	<b>6</b>
<b>General Information</b> .....	<b>6</b>
<b>Specifications</b> .....	<b>7</b>
<b>Product Appearance</b> .....	<b>10</b>
Upper Panel.....	10
Back Panel.....	11
<b>Delivery Package</b> .....	<b>12</b>
<b>Chapter 3. Installation and Connection</b> .....	<b>13</b>
<b>Before You Begin</b> .....	<b>13</b>
<b>Connecting to Mobile Device with D-Link Assistant Application</b> .....	<b>14</b>
<b>Connecting to PC</b> .....	<b>18</b>
PC with Ethernet Adapter.....	18
Configuring IP Address in OS Windows 7.....	19
Configuring IP Address in OS Windows 10.....	24
PC with Wi-Fi Adapter.....	28
Configuring Wi-Fi Adapter in OS Windows 7.....	29
Configuring Wi-Fi Adapter in OS Windows 10.....	32
<b>Connecting to Web-based Interface</b> .....	<b>35</b>
<b>Web-based Interface Structure</b> .....	<b>37</b>
Summary Page.....	37
Home Page.....	39
Menu Sections.....	40
Notifications.....	41
<b>Chapter 4. Configuring via Web-based Interface</b> .....	<b>42</b>
<b>Initial Configuration Wizard</b> .....	<b>42</b>
Selecting Operation Mode.....	44
Router.....	44
Access Point or Repeater.....	46
Changing LAN IPv4 Address.....	48
Wi-Fi Client.....	49
Configuring WAN Connection.....	51
Static IPv4 Connection.....	52
Static IPv6 Connection.....	53
PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections.....	54
PPPoE + Static IP (PPPoE Dual Access) Connection.....	55
PPTP + Dynamic IP or L2TP + Dynamic IP Connection.....	56
PPTP + Static IP or L2TP + Static IP Connection.....	57
Configuring Wireless Network.....	58
Configuring LAN Port for IPTV/VoIP.....	60
Changing Web-based Interface Password.....	62
<b>Connection of Multimedia Devices</b> .....	<b>64</b>

<b>Statistics</b> .....	<b>67</b>
Network Statistics.....	67
DHCP.....	68
Clients and Sessions.....	69
Routing Table.....	70
Multicast Groups.....	71
<b>Connections Setup</b> .....	<b>72</b>
LAN.....	72
IPv4.....	72
IPv6.....	77
WAN.....	80
<i>Creating Dynamic IPv4 or Static IPv4 WAN Connection</i> .....	81
<i>Creating Dynamic IPv6 or Static IPv6 WAN Connection</i> .....	85
<i>Creating PPPoE WAN Connection</i> .....	89
<i>Creating PPTP or L2TP WAN Connection</i> .....	93
<i>Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection</i> .....	97
WAN Failover.....	102
<b>Wi-Fi</b> .....	<b>104</b>
Basic Settings.....	104
Client Management.....	111
WPS.....	112
<i>Using WPS Function via Web-based Interface</i> .....	114
WMM.....	115
Client.....	118
Additional.....	120
MAC Filter.....	123
<b>Advanced</b> .....	<b>125</b>
DNS.....	126
Ports Settings.....	128
MAC Filter.....	131
VLAN.....	133
DDNS.....	136
Redirect.....	138
Routing.....	139
TR-069 Client.....	141
UPnP IGD.....	143
UDPHY.....	144
IGMP.....	146
ALG/Passthrough.....	147
<b>Firewall</b> .....	<b>149</b>
IP Filter.....	149
Virtual Servers.....	153
DMZ.....	156
URL Filter.....	157
Remote Access.....	158

<b>System</b> .....	<b>160</b>
Configuration.....	161
Firmware Update.....	163
<i>Local Update</i> .....	164
<i>Remote Update</i> .....	165
Log.....	166
Ping.....	169
Traceroute.....	171
Telnet.....	173
System Time.....	174
<b>Chapter 5. Operation Guidelines</b> .....	<b>176</b>
<b>Terms and Conditions for Installation, Safe Operation,</b>	
<b>Storage, Transportation, and Disposal</b> .....	<b>176</b>
<b>Wireless Installation Considerations</b> .....	<b>177</b>
<b>Chapter 6. Abbreviations and Acronyms</b> .....	<b>178</b>


# CHAPTER 1. INTRODUCTION

## Contents and Audience

This manual describes the access point DAP-300P and explains how to configure and operate it.

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

## Conventions

Example	Description
text	The body text of the manual.
<i>Before You Begin</i>	A reference to a chapter or section of this manual.
<i>“Quick Installation Guide”</i>	A reference to a document.
<b>Change</b>	A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.).
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-300P 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-300P device is a wireless access point supporting the router mode. It is an affordable solution for creating wireless networks at home or in an office.

Using the DAP-300P device, you are able to quickly create a 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). The access point can operate as a base station for connecting wireless devices of the standards 802.11b, 802.11g, and 802.11n (at the rate up to 300Mbps).

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.

Support of guest Wi-Fi network in the router mode allows you to create a separate wireless network with individual security settings. 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-300P to create a wireless network or to connect to a wired router. In the router mode, you are able to connect DAP-300P 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-300P as a wireless client and a wireless repeater in the access point mode and as a WISP repeater in the router mode.

You can configure the settings of the DAP-300P device via the user-friendly web-based interface (the interface is available in several languages).

The configuration wizard allows you to connect DAP-300P 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	
<b>Processor</b>	<ul style="list-style-type: none"> <li>MT7628DAN (580MHz)</li> </ul>
<b>RAM</b>	<ul style="list-style-type: none"> <li>64MB, built in processor</li> </ul>
<b>Flash</b>	<ul style="list-style-type: none"> <li>8MB, SPI</li> </ul>
<b>Interfaces</b>	<ul style="list-style-type: none"> <li>10/100BASE-TX WAN port with PoE support</li> <li>10/100BASE-TX LAN port</li> </ul>
<b>LEDs</b>	<ul style="list-style-type: none"> <li>POWER / WLAN</li> <li>INTERNET</li> <li>LAN</li> </ul>
<b>Buttons</b>	<ul style="list-style-type: none"> <li>RESET button to restore factory default settings</li> </ul>
<b>Antenna</b>	<ul style="list-style-type: none"> <li>Two internal antennas (3dBi gain)</li> </ul>
<b>MIMO</b>	<ul style="list-style-type: none"> <li>2 x 2</li> </ul>
<b>Power connector</b>	<ul style="list-style-type: none"> <li>Power input connector (12V DC, 0.5A)</li> </ul>

Software	
<b>Operation Modes</b>	<ul style="list-style-type: none"> <li>Access point</li> <li>Router</li> </ul>
<b>WAN connection types</b>	<ul style="list-style-type: none"> <li>PPPoE</li> <li>IPv6 PPPoE</li> <li>PPPoE Dual Stack</li> <li>Static IPv4 / Dynamic IPv4</li> <li>Static IPv6 / Dynamic IPv6</li> <li>PPPoE + Static IP (PPPoE Dual Access)</li> <li>PPPoE + Dynamic IP (PPPoE Dual Access)</li> <li>PPTP/L2TP + Static IP</li> <li>PPTP/L2TP + Dynamic IP</li> </ul>
<b>Network functions</b>	<ul style="list-style-type: none"> <li>Support of IEEE 802.1X for Internet connection</li> <li>DHCP server/relay</li> <li>Advanced configuration of built-in DHCP server</li> <li>Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation</li> <li>Automatic obtainment of LAN IP address (for access point/repeater/client modes)</li> <li>DNS relay</li> <li>Dynamic DNS</li> <li>Static IPv4/IPv6 routing</li> <li>IGMP Proxy</li> <li>RIP</li> <li>Support of UPnP IGD</li> <li>Support of VLAN</li> <li>WAN ping respond</li> <li>Support of SIP ALG</li> <li>Support of RTSP</li> <li>WAN failover</li> <li>Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port</li> <li>Built-in UDPXY application</li> </ul>

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

Software	
<b>Firewall functions</b>	<ul style="list-style-type: none"> <li>· Network Address Translation (NAT)</li> <li>· Stateful Packet Inspection (SPI)</li> <li>· IPv4/IPv6 filter</li> <li>· MAC filter</li> <li>· URL filter</li> <li>· DMZ</li> <li>· Virtual servers</li> </ul>
<b>VPN</b>	<ul style="list-style-type: none"> <li>· IPsec/PPTP/L2TP/PPPoE pass-through</li> <li>· PPTP/L2TP tunnels</li> </ul>
<b>Management and monitoring</b>	<ul style="list-style-type: none"> <li>· Local and remote access to settings through TELNET/WEB (HTTP/HTTPS)</li> <li>· Multilingual web-based interface for configuration and management</li> <li>· Notification on connection problems and auto redirect to settings</li> <li>· Firmware update via web-based interface</li> <li>· Automatic notification on new firmware version</li> <li>· Saving/restoring configuration to/from file</li> <li>· Support of logging to remote host</li> <li>· Automatic synchronization of system time with NTP server and manual time/date setup</li> <li>· Ping utility</li> <li>· Traceroute utility</li> <li>· TR-069 client</li> <li>· Automatic reboot on schedule</li> </ul>

Wireless Module Parameters	
<b>Standards</b>	<ul style="list-style-type: none"> <li>· IEEE 802.11b/g/n</li> </ul>
<b>Frequency range</b>  <i>The frequency range depends upon the radio frequency regulations applied in your country</i>	<ul style="list-style-type: none"> <li>· 2400 ~ 2483.5MHz</li> </ul>
<b>Wireless connection security</b>	<ul style="list-style-type: none"> <li>· WEP</li> <li>· WPA/WPA2 (Personal/Enterprise)</li> <li>· MAC filter</li> <li>· WPS (PBC/PIN)</li> </ul>
<b>Advanced functions</b>	<ul style="list-style-type: none"> <li>· "Client" function (access point mode) Wireless network client Wireless network repeater</li> <li>· "Client" function (router mode) WISP repeater</li> <li>· WMM (Wi-Fi QoS)</li> <li>· Information on connected Wi-Fi clients</li> <li>· Advanced settings</li> <li>· Guest Wi-Fi / support of MBSSID</li> <li>· Periodic scan of channels, automatic switch to least loaded channel</li> <li>· Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence)</li> <li>· Support of STBC</li> </ul>
<b>Wireless connection rate</b>	<ul style="list-style-type: none"> <li>· IEEE 802.11b: 1, 2, 5.5, and 11Mbps</li> <li>· IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps</li> <li>· IEEE 802.11n: from 6.5 to 300Mbps (from MCS0 to MCS15)</li> </ul>
<b>Transmitter output power</b>  <i>The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country</i>	<ul style="list-style-type: none"> <li>· 802.11b (typical at room temperature 25 °C) 17dBm at 1, 11Mbps</li> <li>· 802.11g (typical at room temperature 25 °C) 17dBm at 6, 54Mbps</li> <li>· 802.11n (typical at room temperature 25 °C) 17dBm at MCS0~6/8~14 16dBm at MCS7/15</li> </ul>



Wireless Module Parameters	
<b>Receiver sensitivity</b>	<ul style="list-style-type: none"> <li>· 802.11b (typical at PER = 8% (1000-byte PDUs))                             <ul style="list-style-type: none"> <li>-90dBm at 1Mbps</li> <li>-90dBm at 2Mbps</li> <li>-88dBm at 5.5Mbps</li> <li>-86dBm at 11Mbps</li> </ul> </li> <li>· 802.11g (typical at PER &lt; 10% (1000-byte PDUs))                             <ul style="list-style-type: none"> <li>-82dBm at 6Mbps</li> <li>-81dBm at 9Mbps</li> <li>-79dBm at 12Mbps</li> <li>-77dBm at 18Mbps</li> <li>-74dBm at 24Mbps</li> <li>-70dBm at 36Mbps</li> <li>-66dBm at 48Mbps</li> <li>-65dBm at 54Mbps</li> </ul> </li> <li>· 802.11n (typical at PER = 10% (1000-byte PDUs))                             <ul style="list-style-type: none"> <li>HT20                                     <ul style="list-style-type: none"> <li>-82dBm at MCS0/8</li> <li>-79dBm at MCS1/9</li> <li>-77dBm at MCS2/10</li> <li>-74dBm at MCS3/11</li> <li>-70dBm at MCS4/12</li> <li>-66dBm at MCS5/13</li> <li>-65dBm at MCS6/14</li> <li>-64dBm at MCS7/15</li> </ul> </li> <li>HT40                                     <ul style="list-style-type: none"> <li>-79dBm at MCS0/8</li> <li>-76dBm at MCS1/9</li> <li>-74dBm at MCS2/10</li> <li>-71dBm at MCS3/11</li> <li>-67dBm at MCS4/12</li> <li>-63dBm at MCS5/13</li> <li>-62dBm at MCS6/14</li> <li>-61dBm at MCS7/15</li> </ul> </li> </ul> </li> </ul>
<b>Modulation schemes</b>	<ul style="list-style-type: none"> <li>· 802.11b: DQPSK, DBPSK, DSSS, CCK</li> <li>· 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM</li> <li>· 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM (HT20 and HT40)</li> </ul>

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

Operating Environment	
<b>Power</b>	<ul style="list-style-type: none"> <li>· External DC power adapter 12V/0.5A (not included in the delivery package)</li> <li>· PoE: 802.3af (8W), 48V/0.5A</li> </ul>
<b>Temperature</b>	<ul style="list-style-type: none"> <li>· Operating: from 0 to 40 °C</li> <li>· Storage: from -20 to 65 °C</li> </ul>
<b>Humidity</b>	<ul style="list-style-type: none"> <li>· Operating: from 10% to 90% (non-condensing)</li> <li>· Storage: from 5% to 95% (non-condensing)</li> </ul>

## 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 is off.
	<i>Slow blinking red</i>	The firmware is being updated.
	<i>Solid blue</i>	The device's WLAN is on.
	<i>Blinking blue</i>	Data transfer through the Wi-Fi network.
	<i>Blinking yellow</i>	Attempting to add a wireless device via the WPS function.
	<i>No light</i>	The device is powered off.

## Back Panel

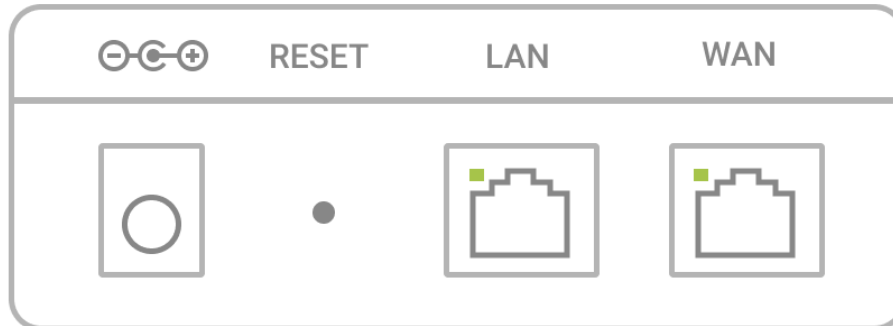


Figure 2. Back panel view.

Name	Description	
<b>RESET</b>	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.	
<b>LAN</b>	An Ethernet port to connect a computer or network device. A <b>LAN</b> 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.
<b>WAN (PoE)</b>	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 <b>INTERNET</b> 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 also equipped with two internal Wi-Fi antennas.

## ***Delivery Package***

The following should be included:

- Access point DAP-300P
- 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](http://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-300P 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 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 802.11b, g, or n NIC (Wi-Fi adapter). In addition, you should specify the values of SSID, channel number and security settings defined in the web-based interface of the access point for all these wireless workstations.

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

1. Connect the power adapter (12V DC, 0.5A, 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-300P**.
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-300P.
5. In the settings of the wireless network **DAP-300P** on your mobile device, in the **IP Settings** field, select the **Static** value.<sup>1</sup>
6. Enter the value **192.168.0.51** in the **IP address** field. Confirm the changed settings.
7. Launch D-Link Assistant application on your mobile device. The application is available for Android smartphones in Google Play.



*D-Link Assistant for Android*

---

<sup>1</sup> 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.

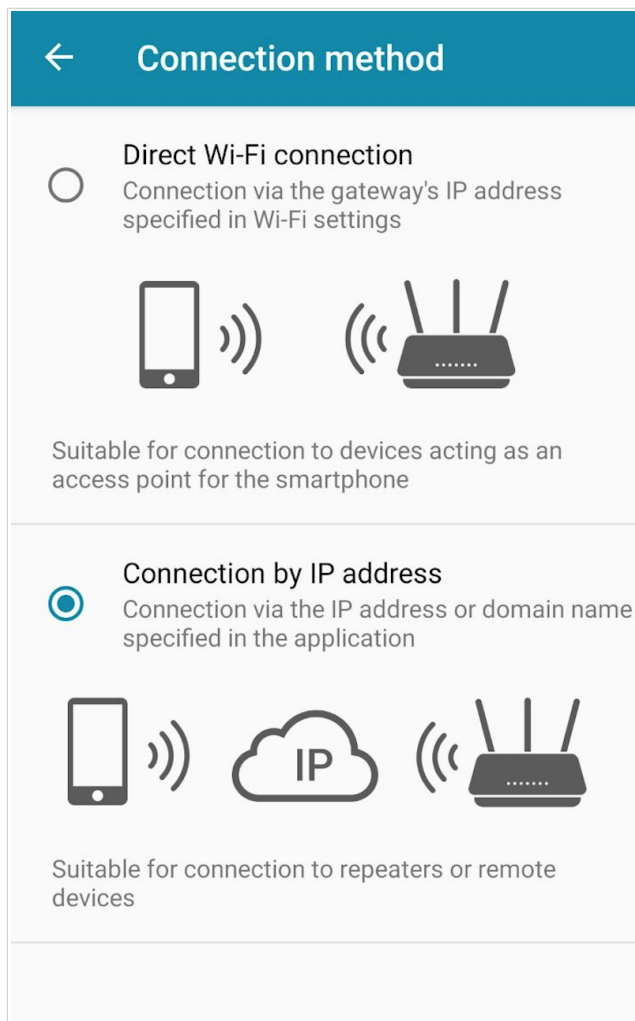


Figure 3. The **Connection method** section.

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

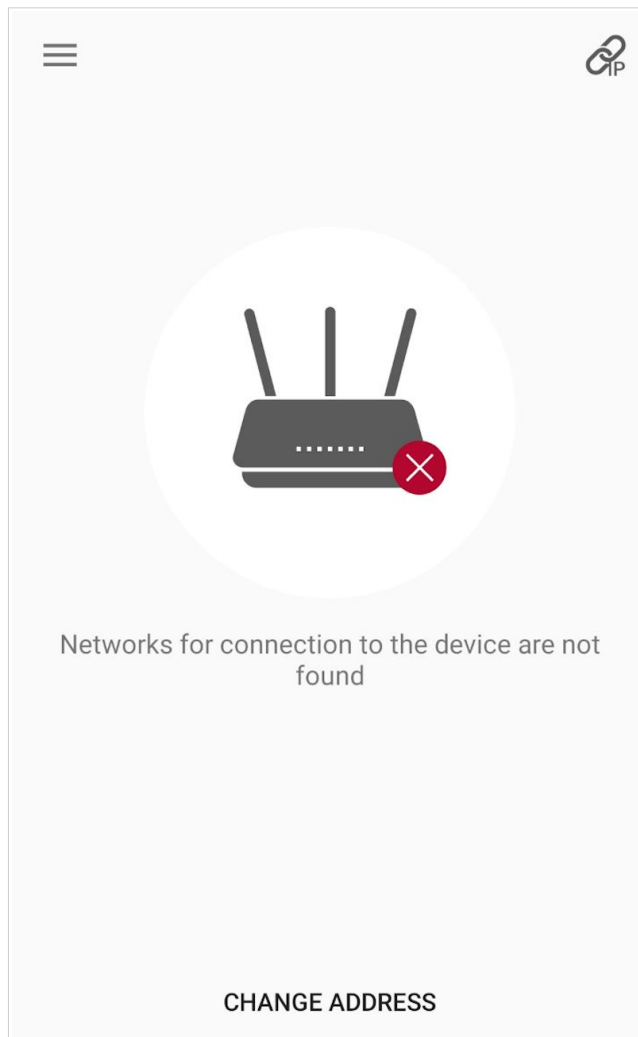


Figure 4. The application main page.



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 (✓).

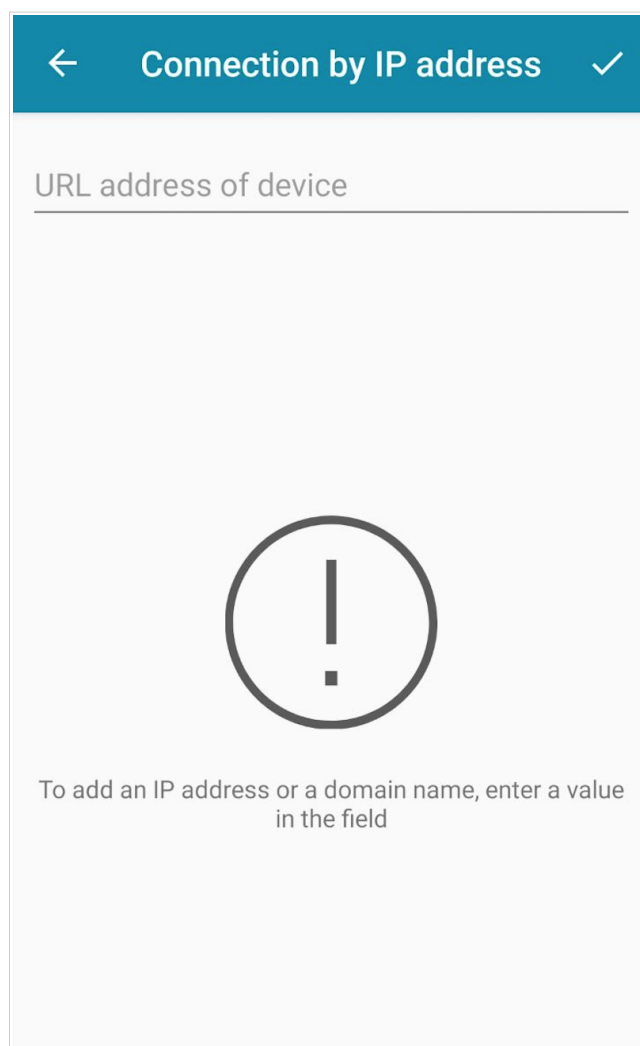


Figure 5. The page for entering the IP address of the device.

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

**!** As you perform initial configuration of the 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.

If you changed the administrator password via the web-based interface, when DAP-300P is accessed with the application the next time, click the **ENTER LOGIN/PASSWORD** button. Enter the username (**admin**) and the password you specified.

## Connecting to PC

### PC with Ethernet Adapter

1. Connect an Ethernet cable between 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 (12V DC, 0.5A, 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.)

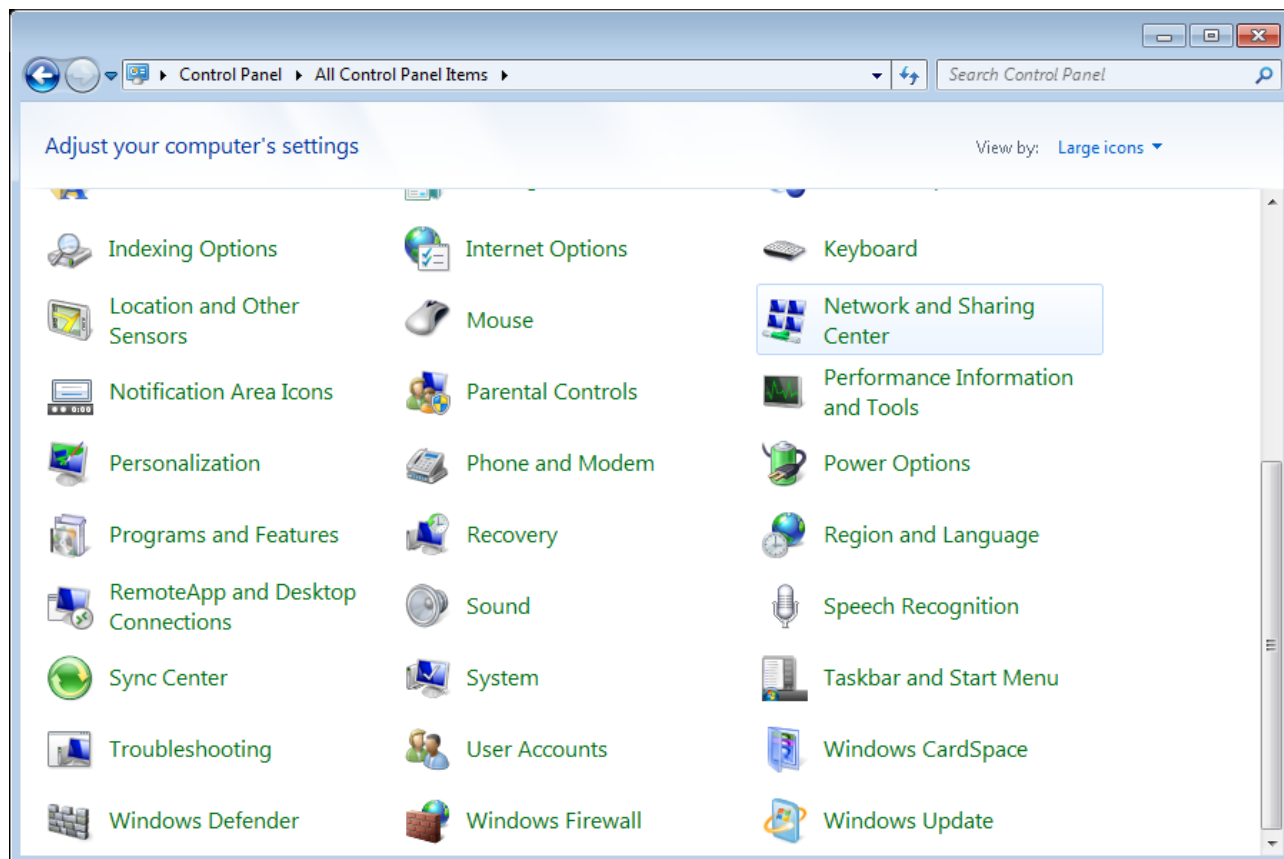


Figure 6. The **Control Panel** window.

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

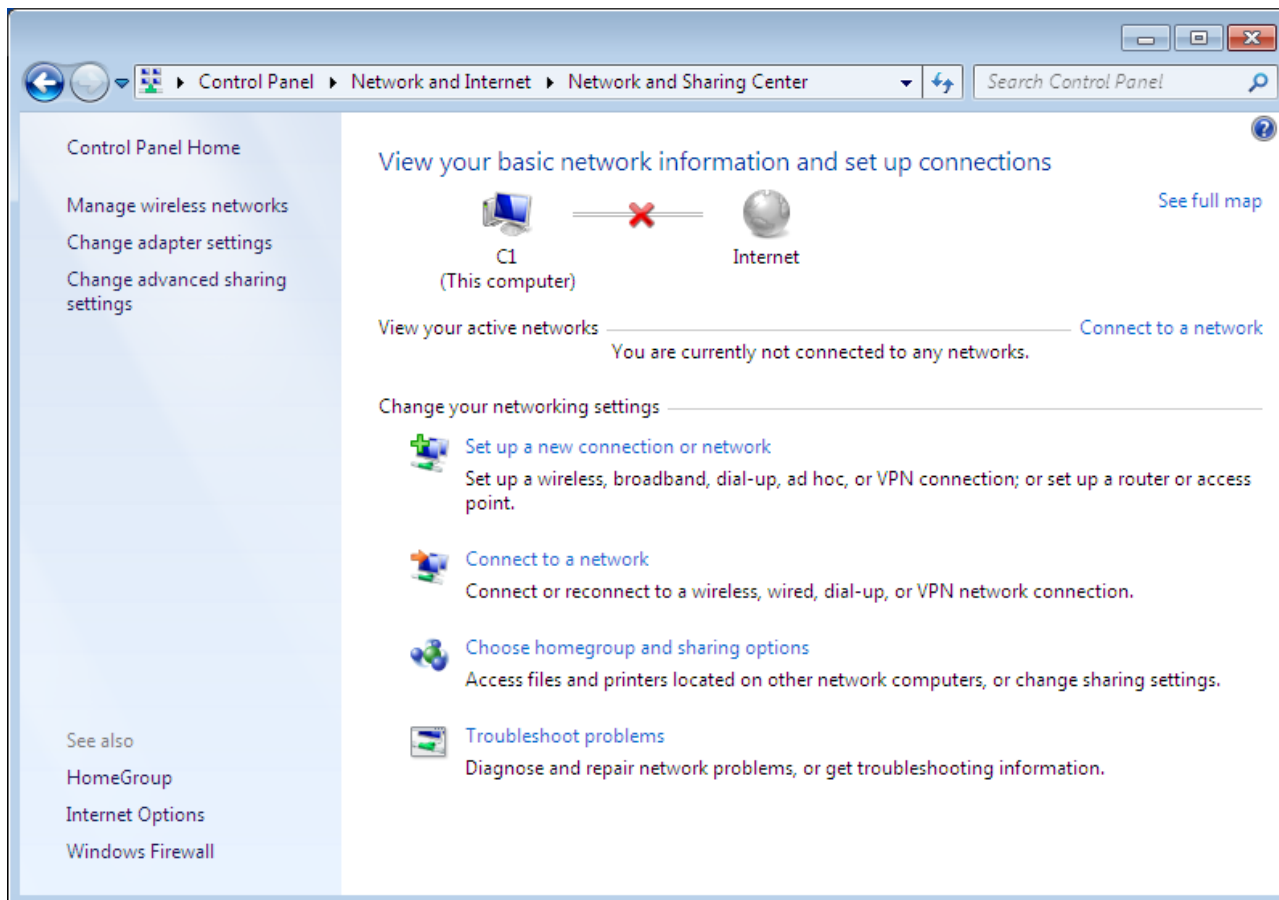


Figure 7. The **Network and Sharing Center** window.

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

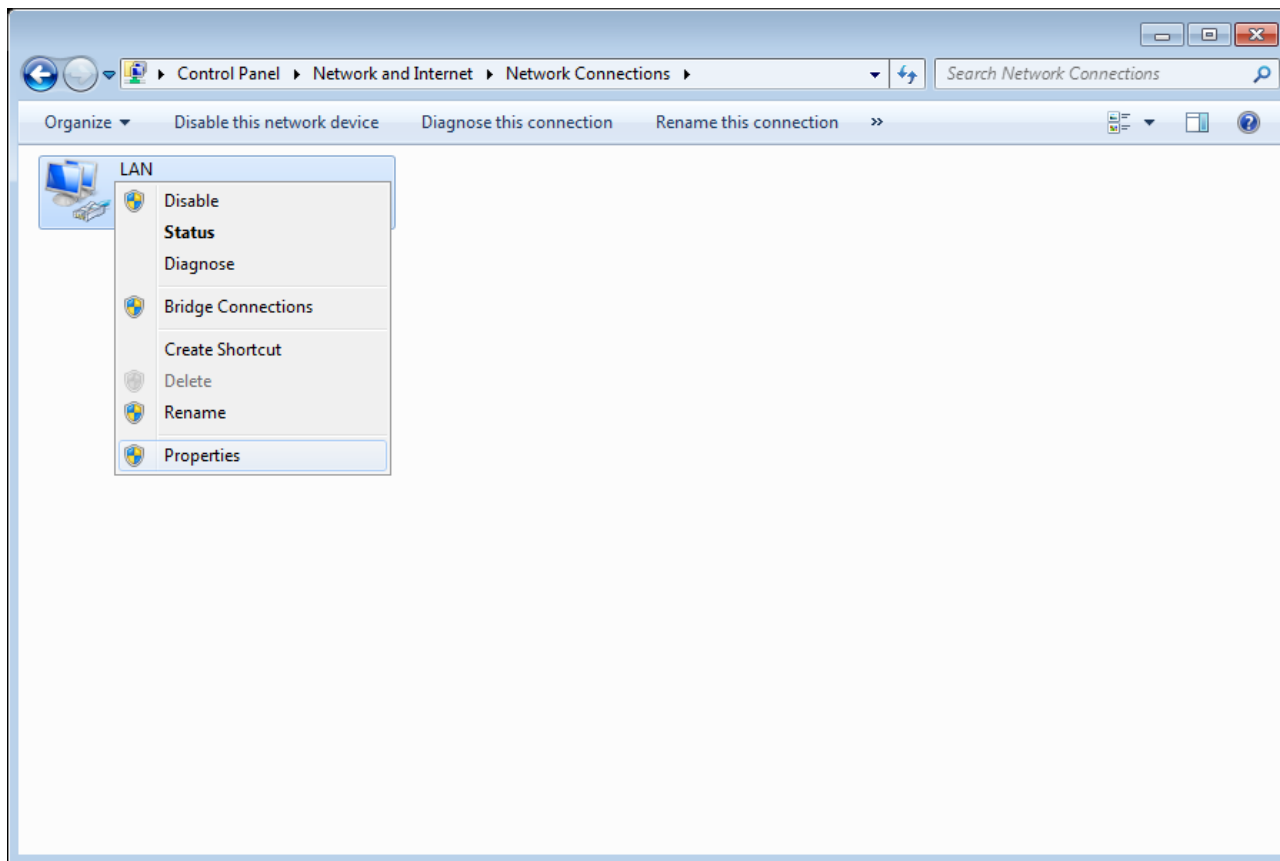


Figure 8. The **Network Connections** window.

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.

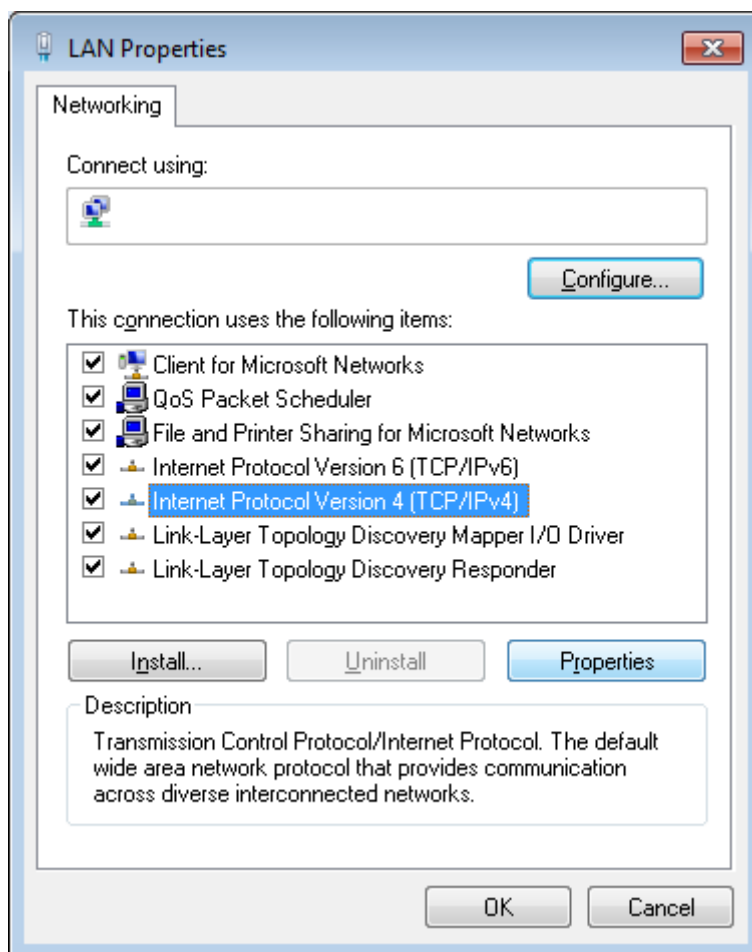


Figure 9. The **Local Area Connection Properties** window.

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.

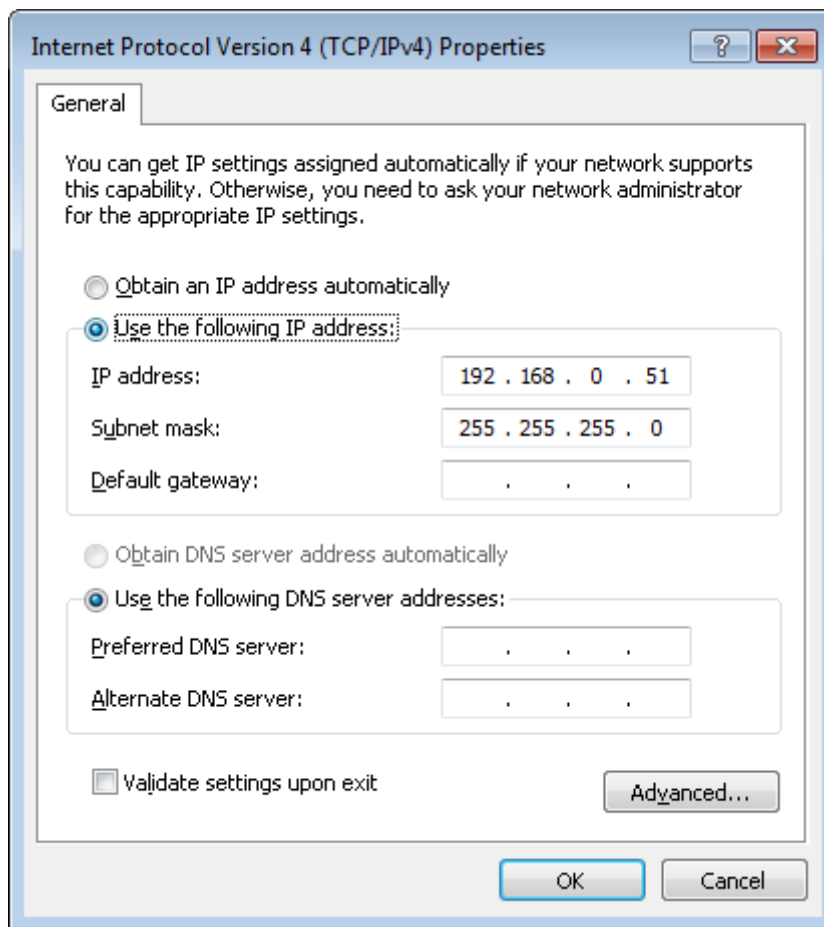


Figure 10. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now you can connect to the web-based interface of DAP-300P 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.

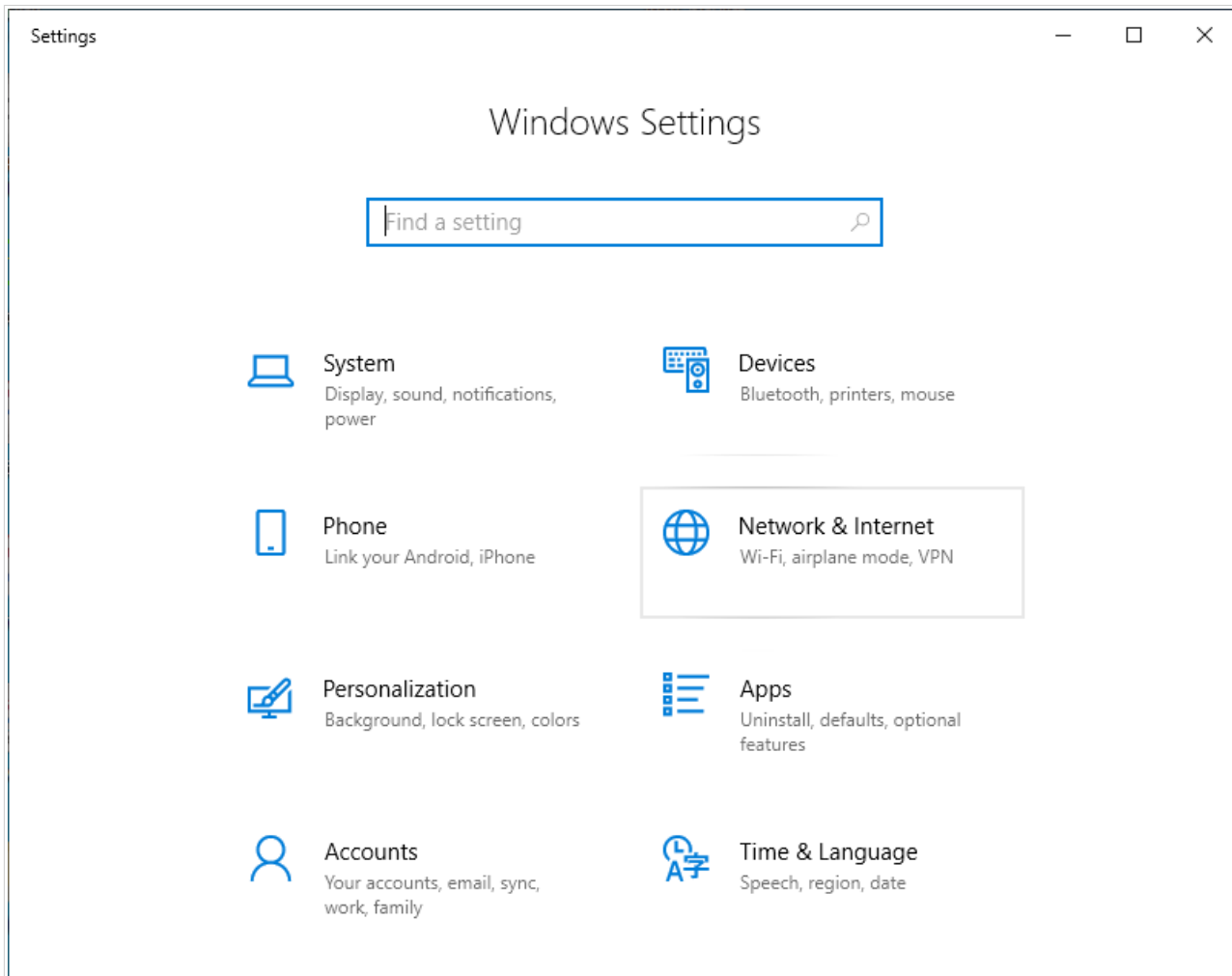


Figure 11. The **Windows Settings** window.



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

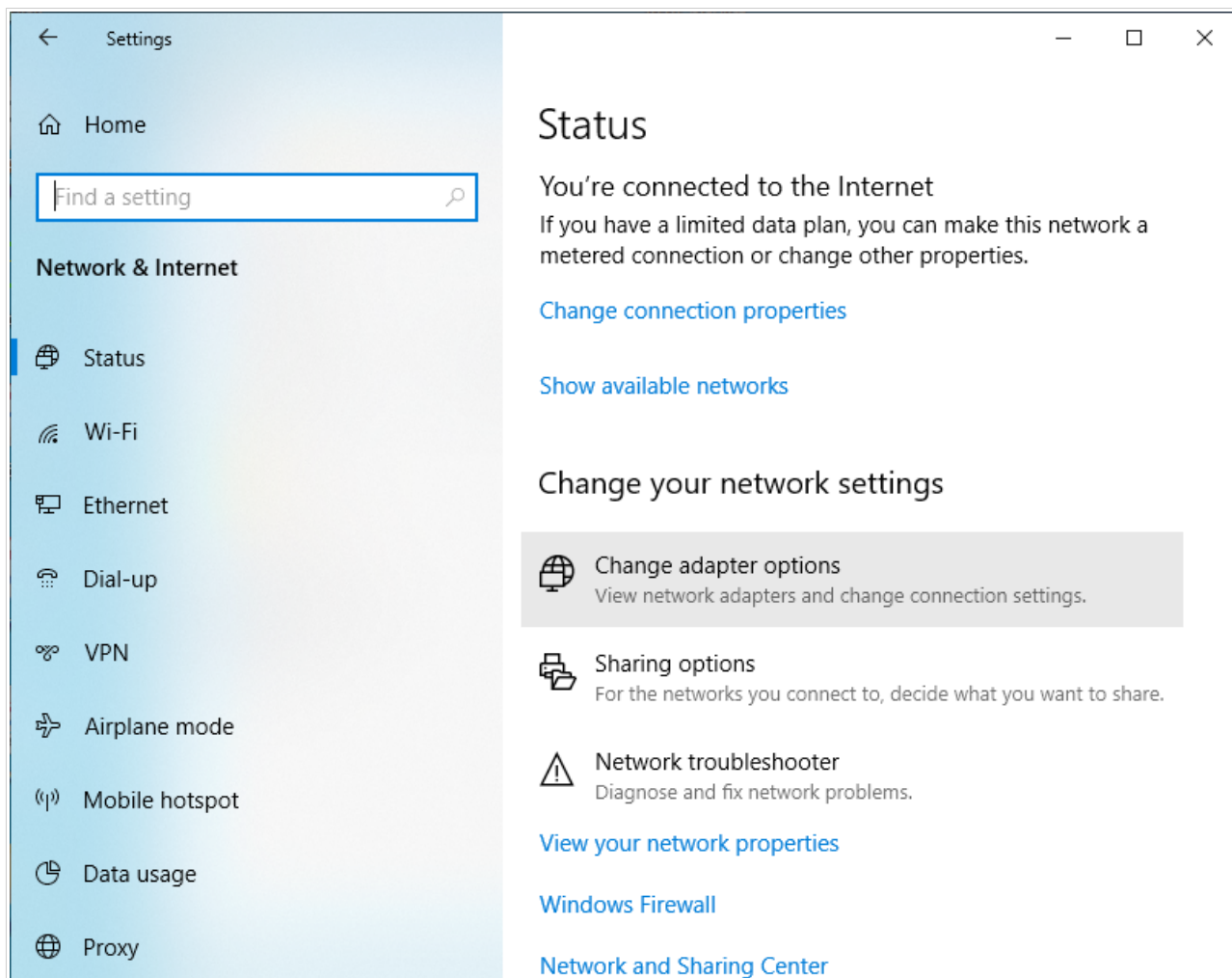


Figure 12. The **Network & Internet** window.

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

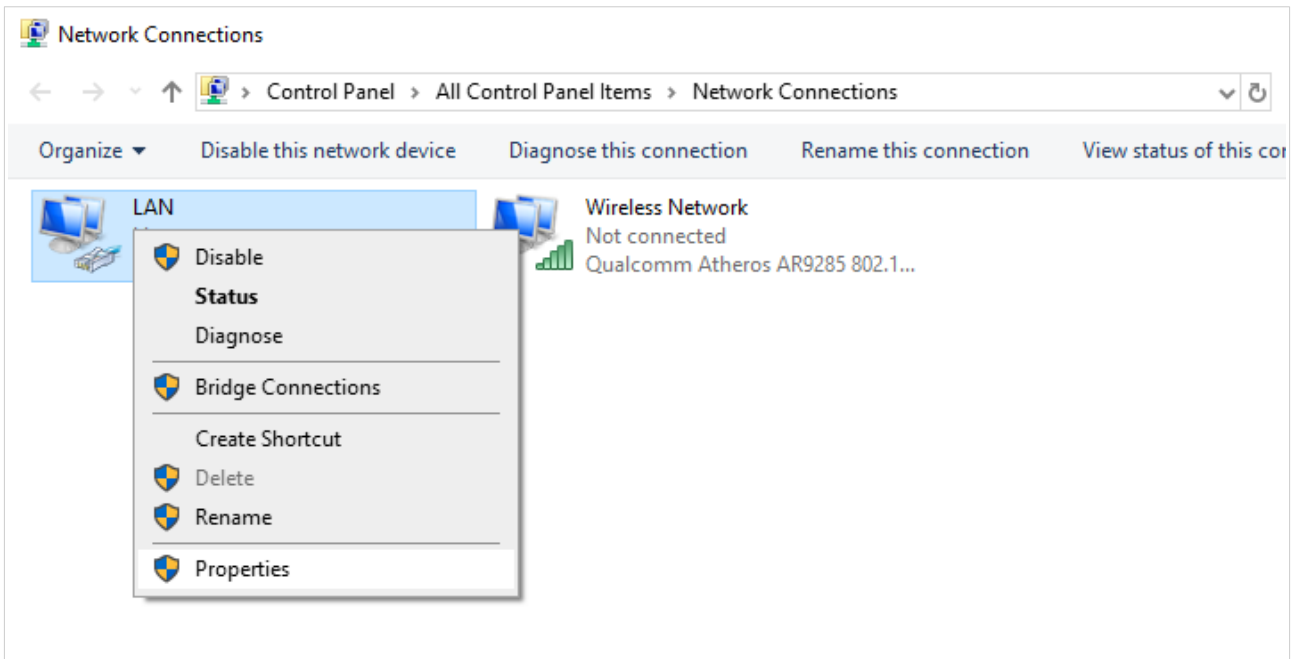


Figure 13. The **Network Connections** window.

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.

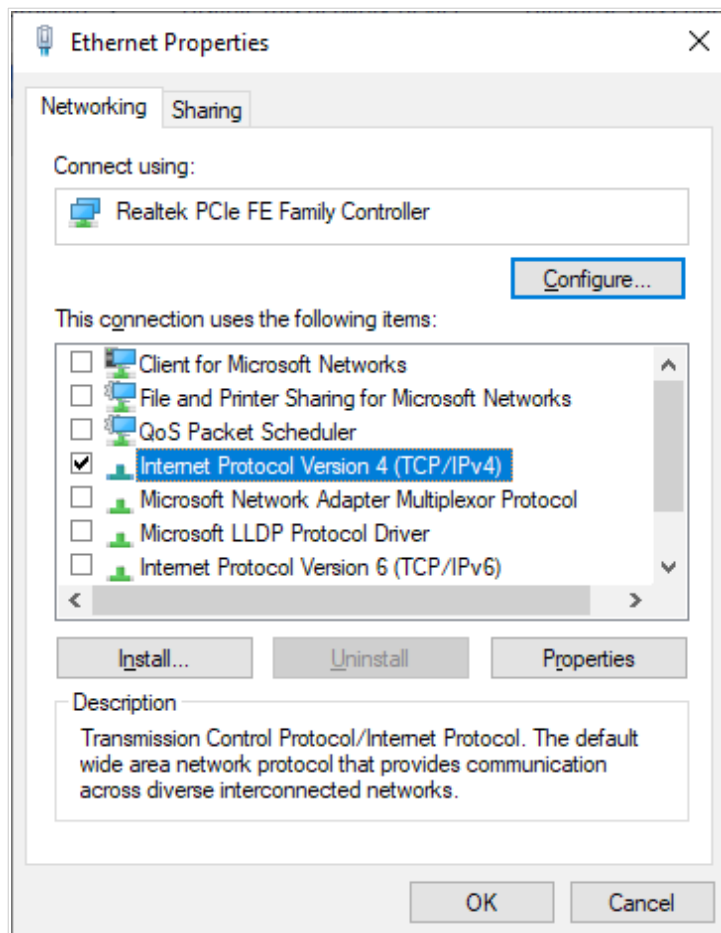


Figure 14. The local area connection properties window.

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.

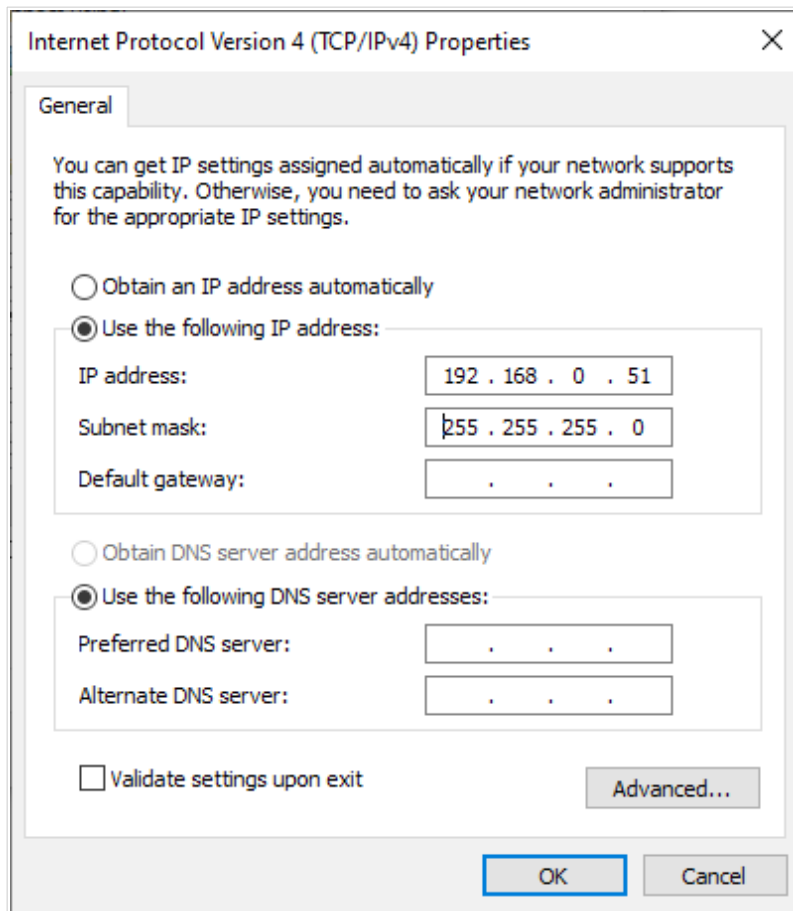


Figure 15. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now you can connect to the web-based interface of DAP-300P 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 (12V DC, 0.5A, 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.)

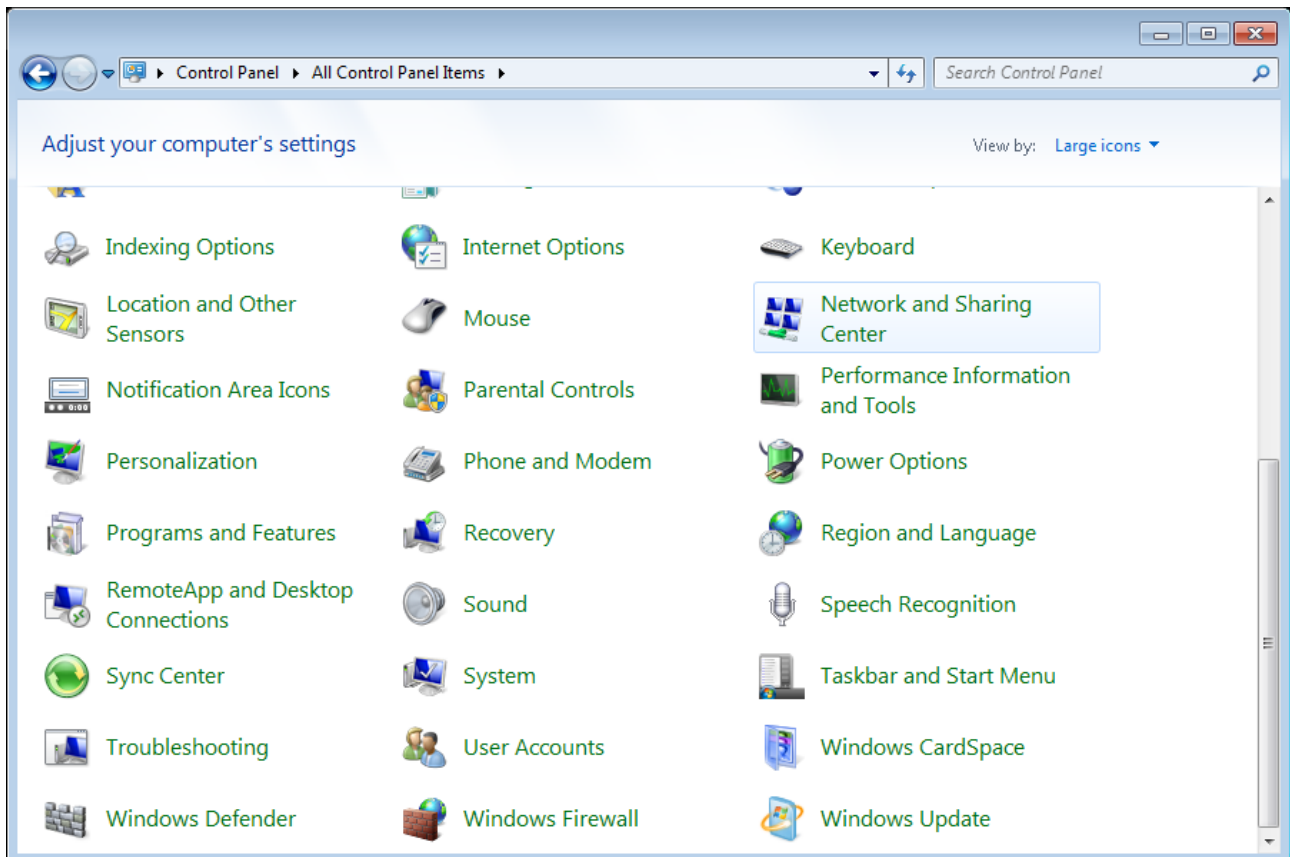


Figure 16. The Control Panel window.

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.

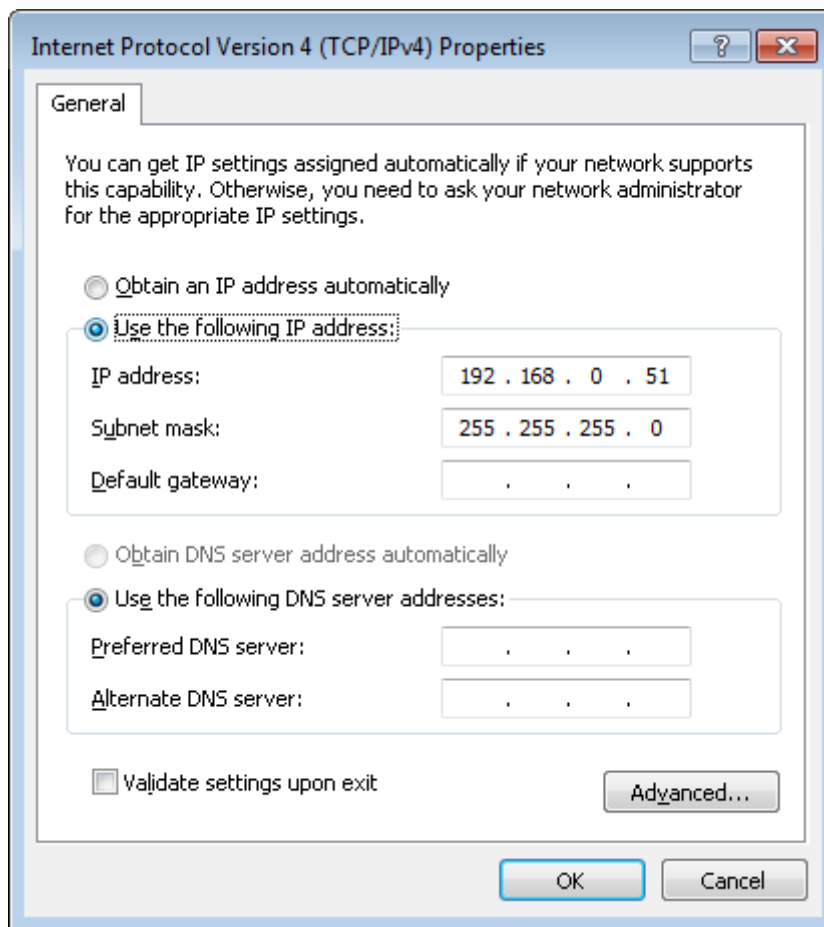


Figure 17. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

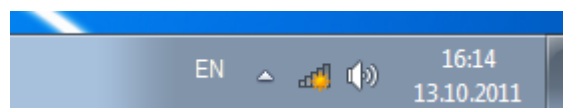


Figure 18. The notification area of the taskbar.

9. In the opened window, in the list of available wireless networks, select the wireless network **DAP-300P** and click the **Connect** button.

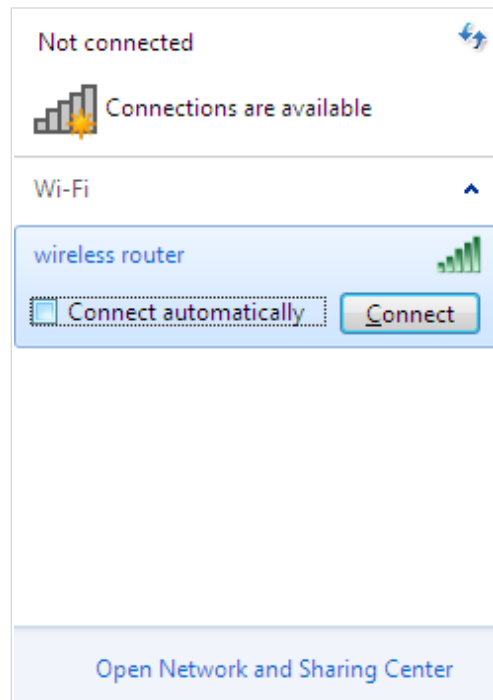


Figure 19. The list of available networks.

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

Now you can connect to the web-based interface of DAP-300P 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.

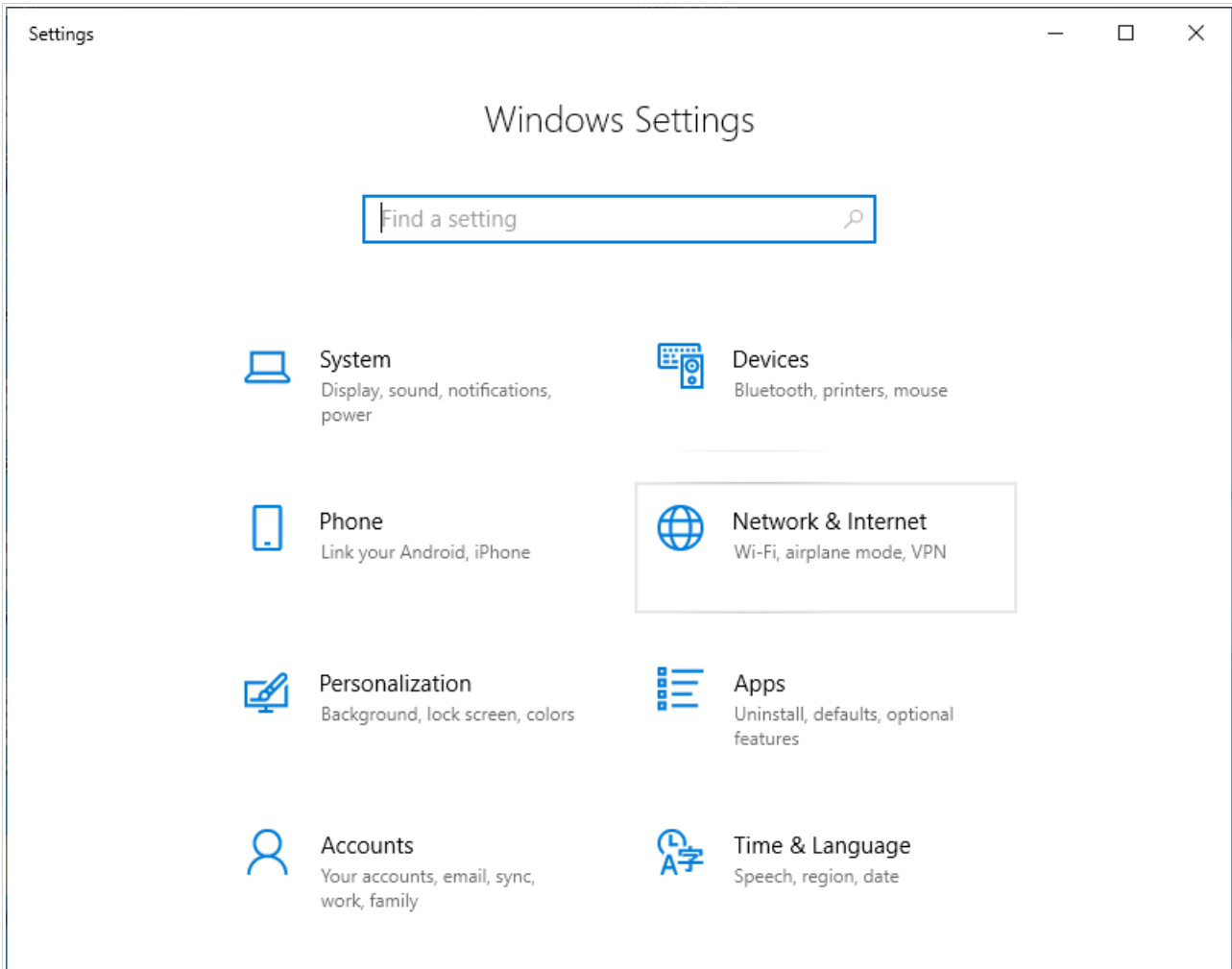


Figure 20. The **Windows Settings** window.

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.

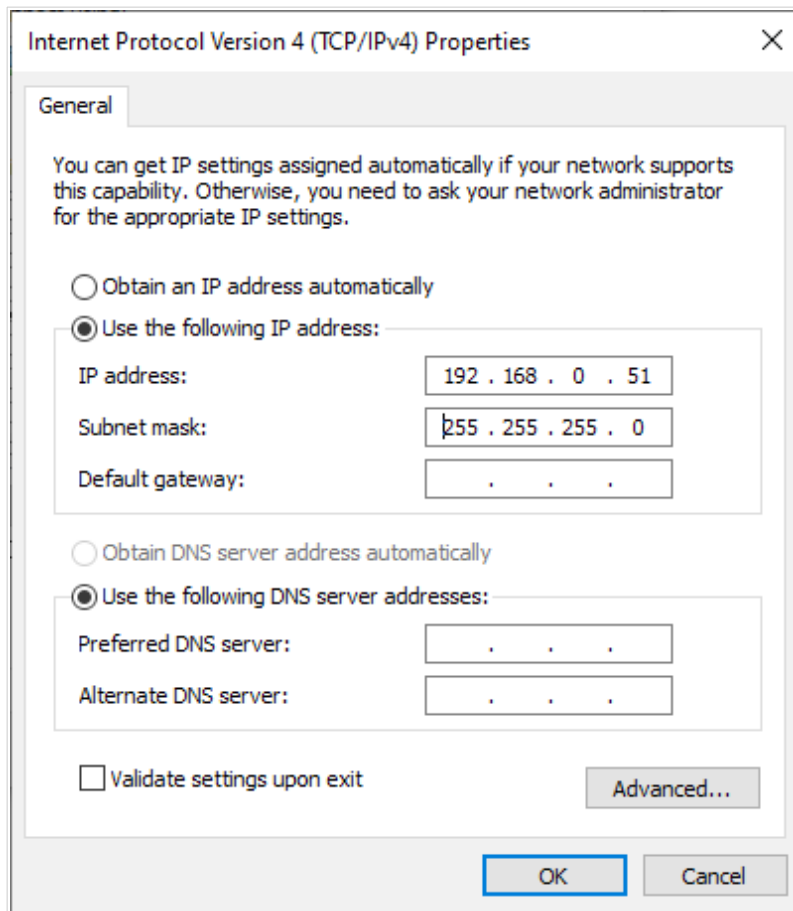


Figure 21. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

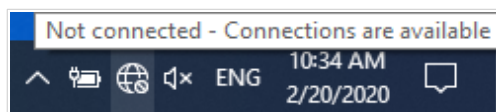


Figure 22. The notification area of the taskbar.

- In the opened **Wireless Network Connection** window, select the wireless network **DAP-300P** and click the **Connect** button.

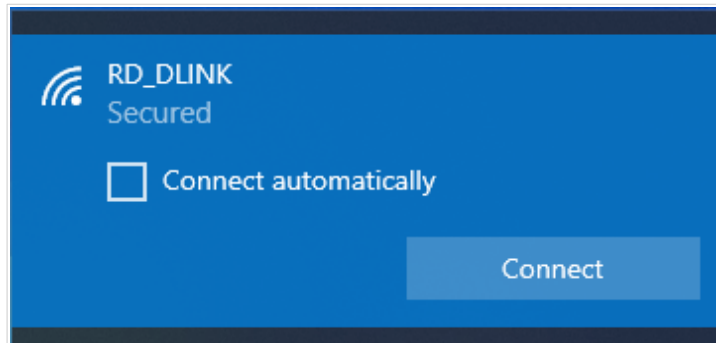


Figure 23. The list of available networks.

- 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**).

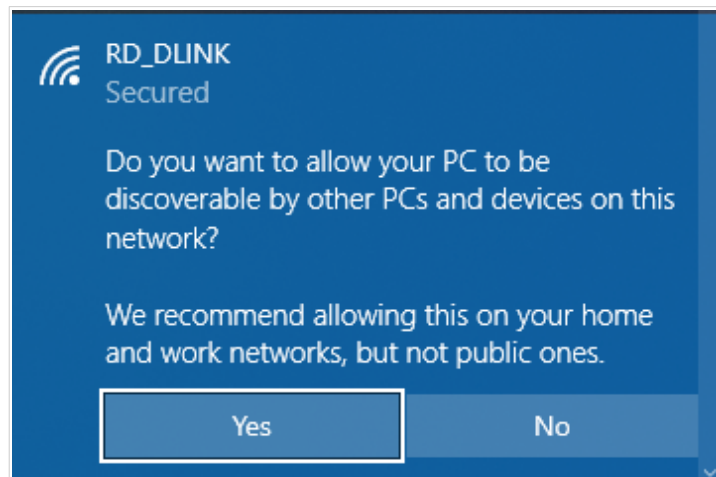


Figure 24. PC discovery settings.

- 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-300P 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 13). In the address bar of the web browser, enter the IP address of the access point (by default, **192.168.0.50**). Press the **Enter** key.

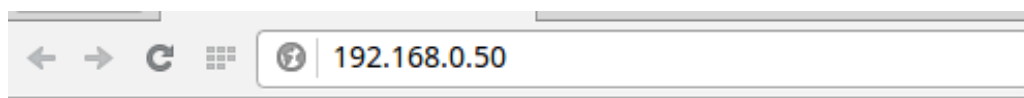


Figure 25. Connecting to the web-based interface of the DAP-300P device.

**!** 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 42).

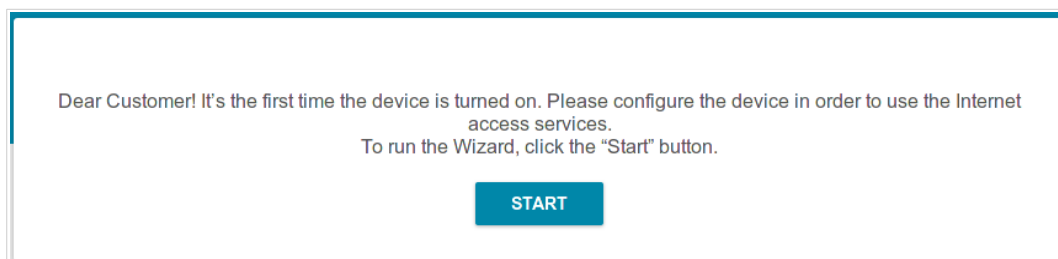
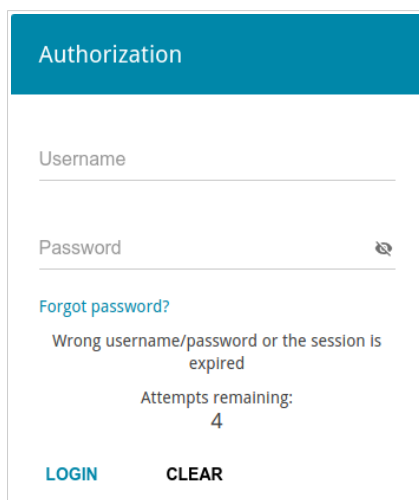


Figure 26. The page for running the Initial Configuration Wizard.

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

Password

[Forgot password?](#)

Wrong username/password or the session is expired

Attempts remaining:  
4

[LOGIN](#) [CLEAR](#)

Figure 27. The login page.

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

## Web-based Interface Structure

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.

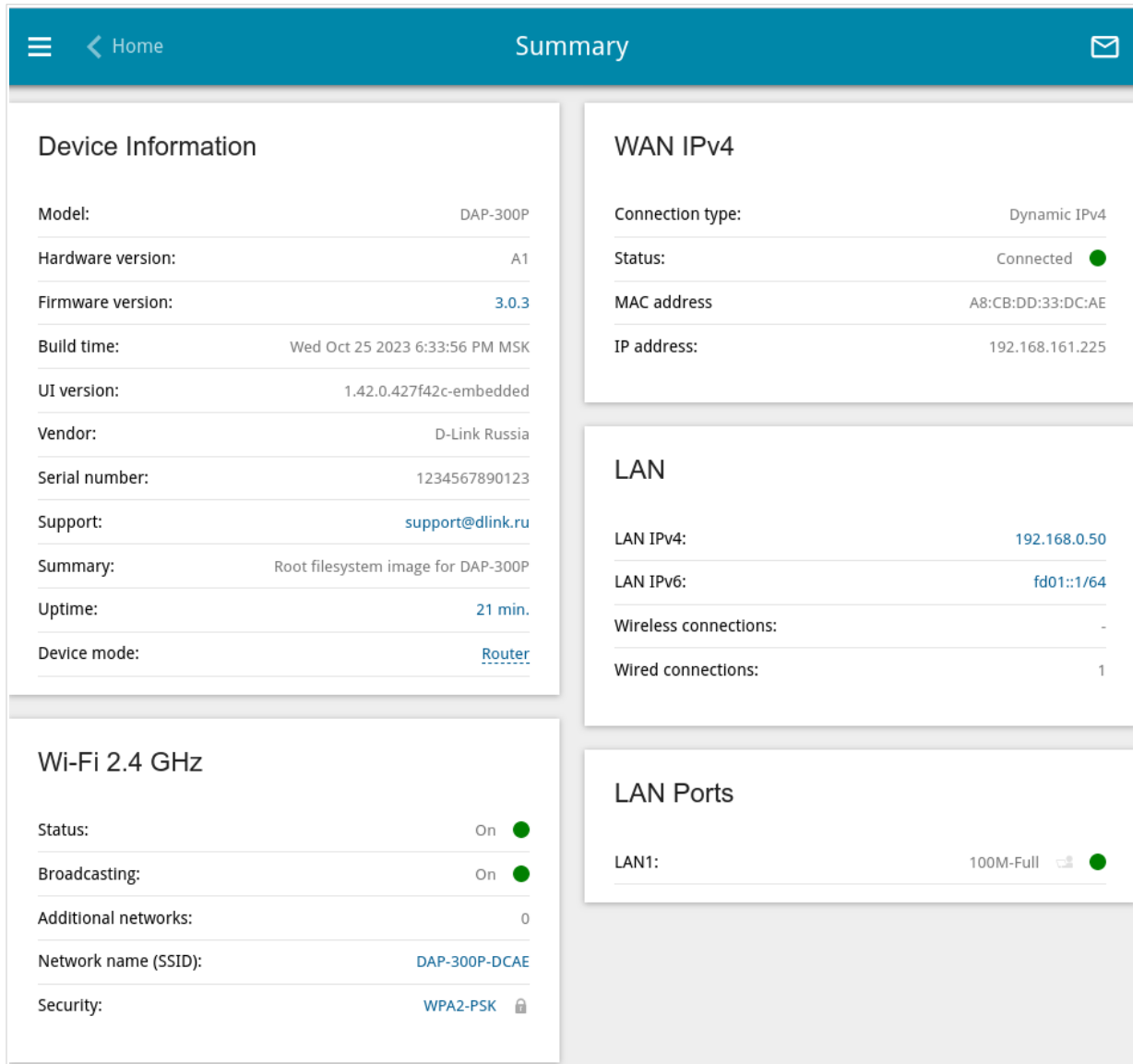


Figure 28. The summary page in the router mode.

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 Configuration Wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 42).

The **Wi-Fi 2.4 GHz** section displays 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 **WAN** section, data on the type and status of the existing WAN connection are displayed.

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

## 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.

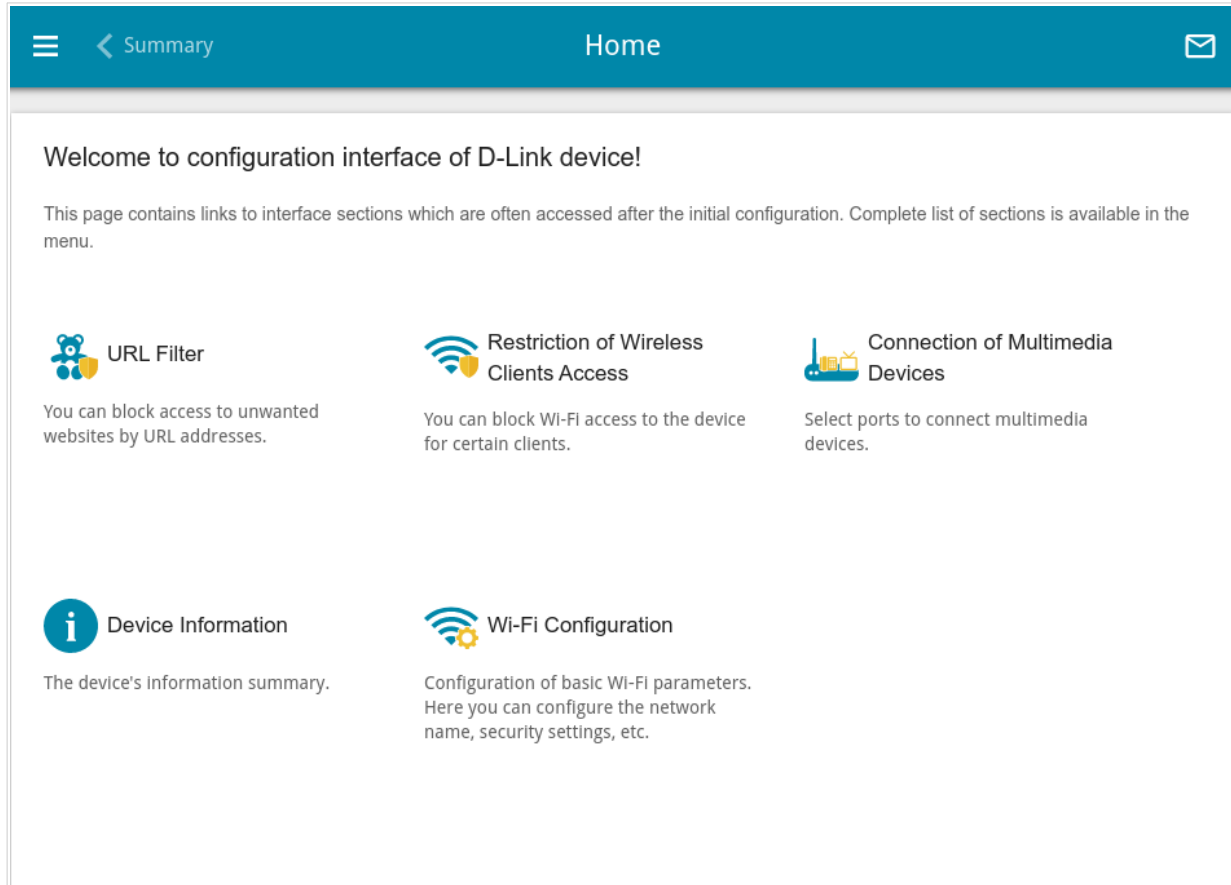


Figure 29. The **Home** page.

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 42).

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 67).

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 72).

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 104).

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 125).

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 149).

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 160).

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.

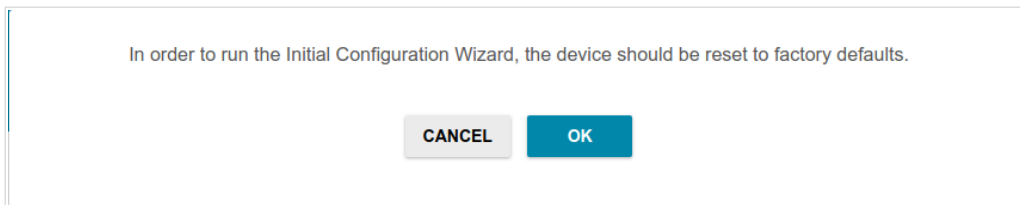


Figure 31. Restoring the default settings in the Wizard.

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-300P** (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

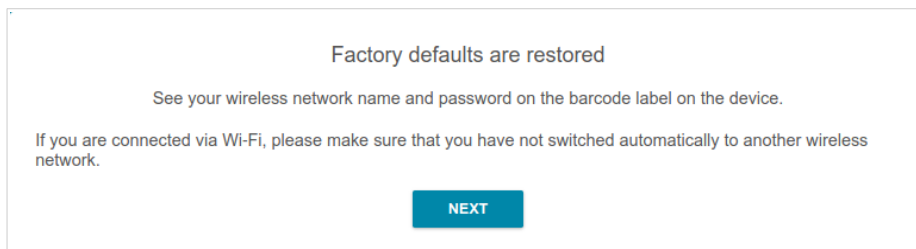


Figure 32. Checking connection to the wireless network.

Click the **START** button.

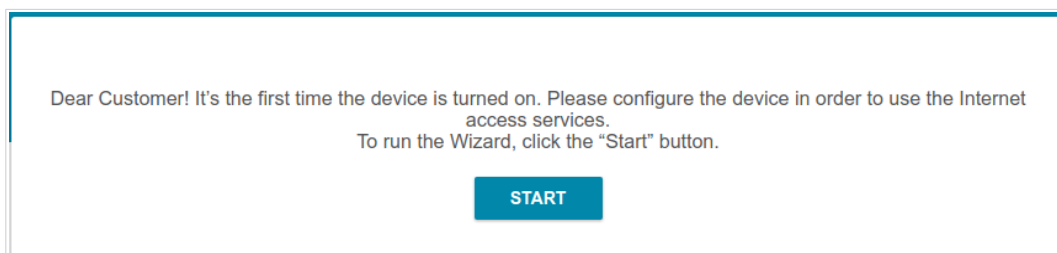


Figure 33. Starting the Wizard.

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

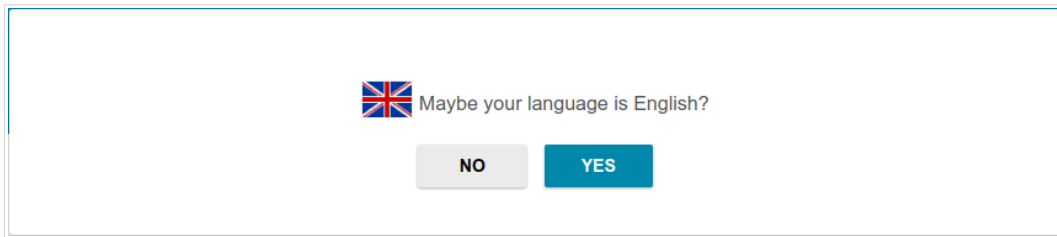


Figure 34. Selecting a language.

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 **User's interface password** and **Password confirmation** fields and the name of the wireless network in the **Network name (SSID)** field. Then click the **APPLY** button.

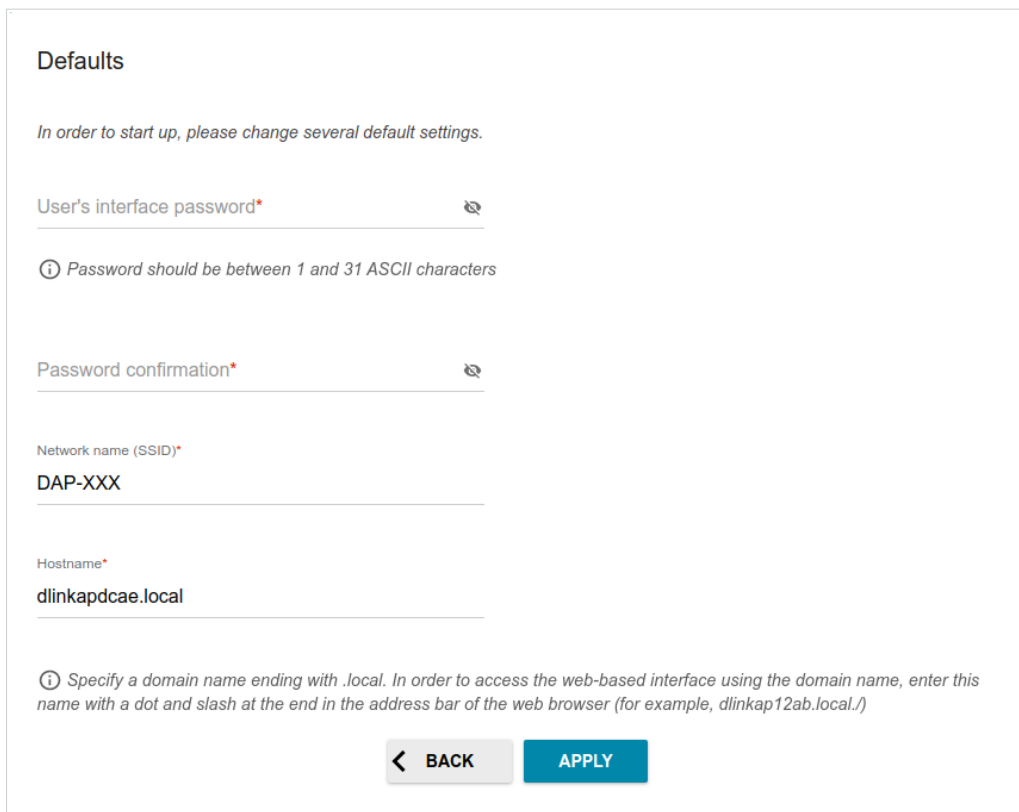


Figure 35. Changing the default settings.

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

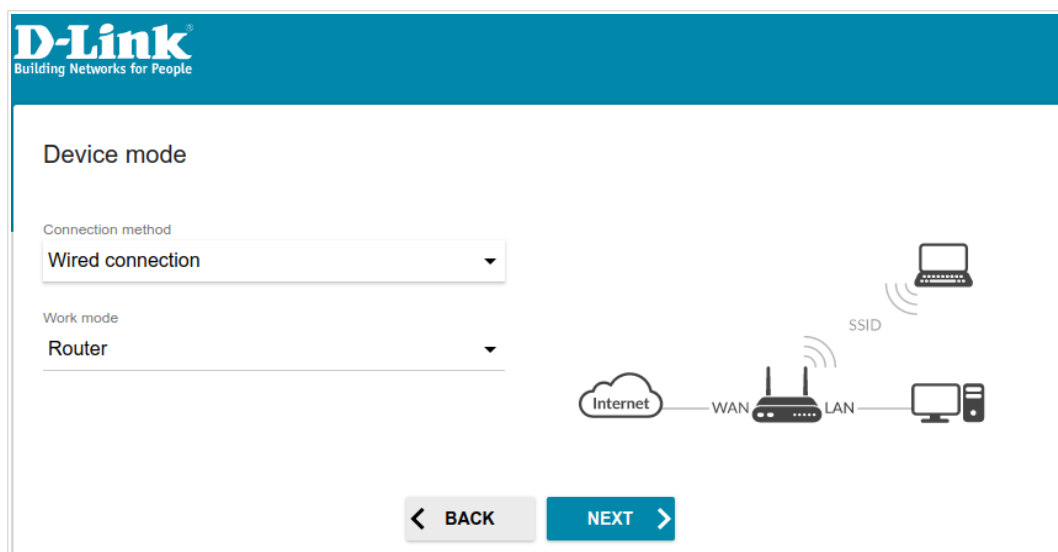


Figure 36. Selecting an operation mode. The **Router** mode.

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

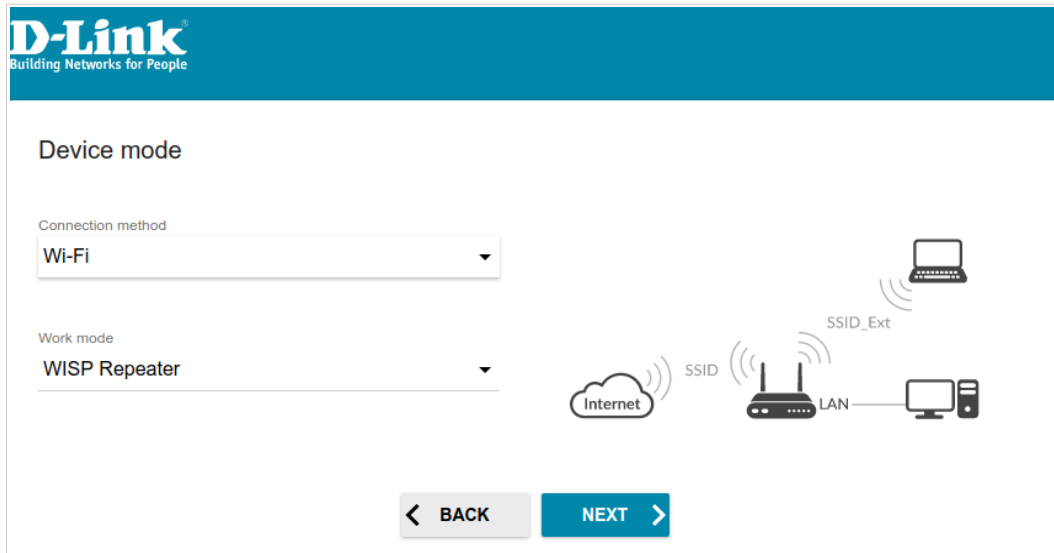


Figure 37. Selecting an operation mode. The **WISP Repeater** mode.

## 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 **Wired connection** value. Then from the **Work mode** list select the **Access point** value. In this mode you can change the LAN IP address, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.

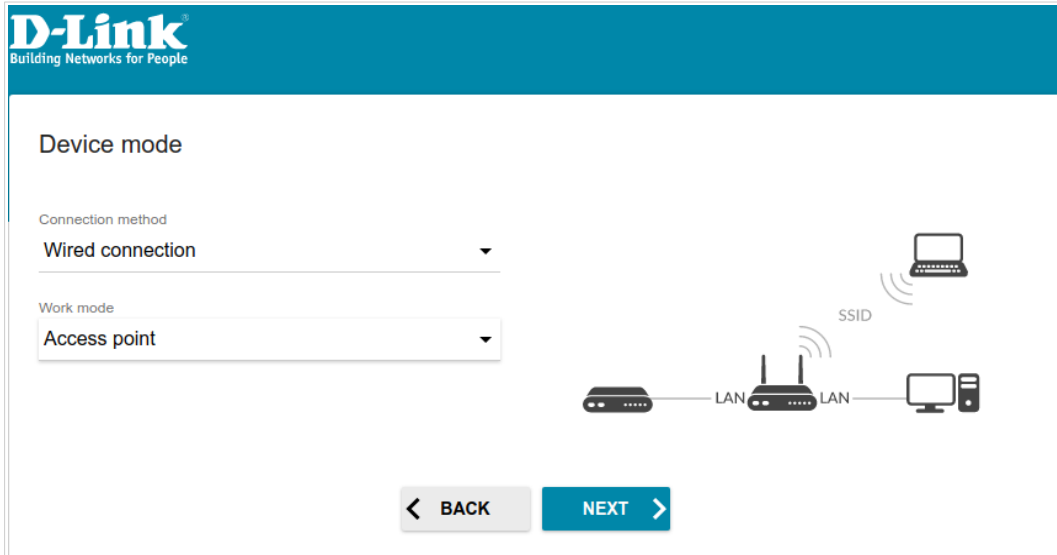


Figure 38. Selecting an operation mode. The **Access point** mode.

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 **Wi-Fi** value. Then from the **Work mode** list select the **Repeater** value. In this mode you can change the LAN IP address, connect your device to another access point, set your own settings for the wireless network, and set your own password for access to the web-based interface of the device.

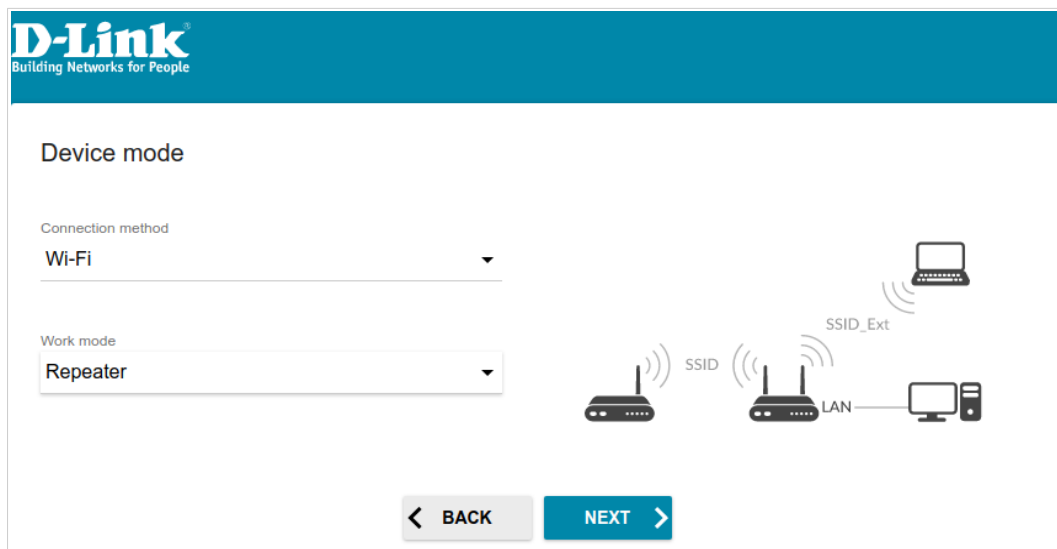


Figure 39. Selecting an operation mode. The **Repeater** mode.

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

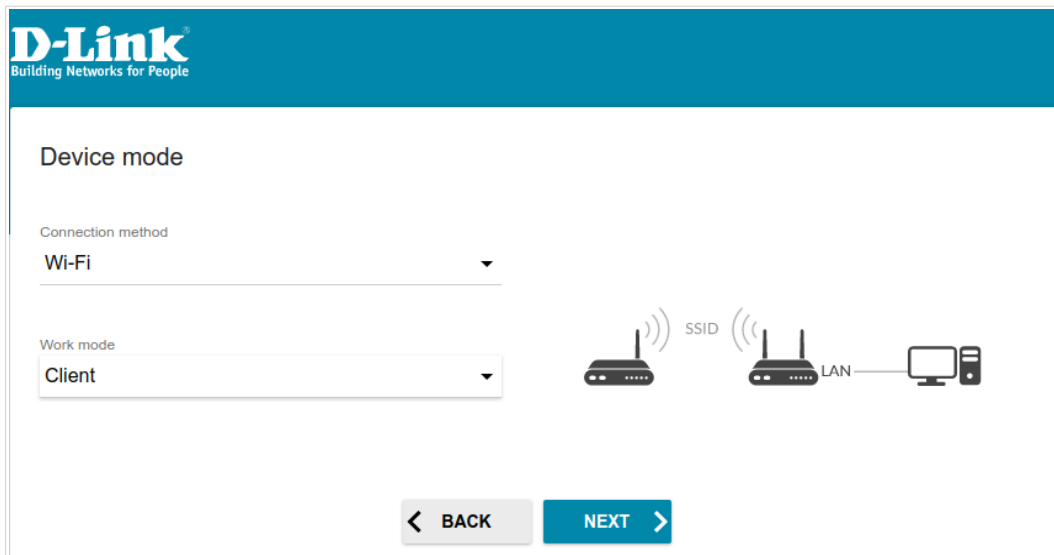


Figure 40. Selecting an operation mode. The **Client** mode.

## Changing LAN IPv4 Address

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

1. Select the **Automatic obtainment of IPv4 address** to let the device automatically obtain the LAN IPv4 address.

If you want to manually assign the LAN IPv4 address for DAP-300P, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Subnet mask**, **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-300P 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

Hostname\*

dlinkap986a.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 41. The page for changing the LAN IPv4 address.

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




## Wi-Fi Client

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

1. On the **Wi-Fi Client** page, 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.

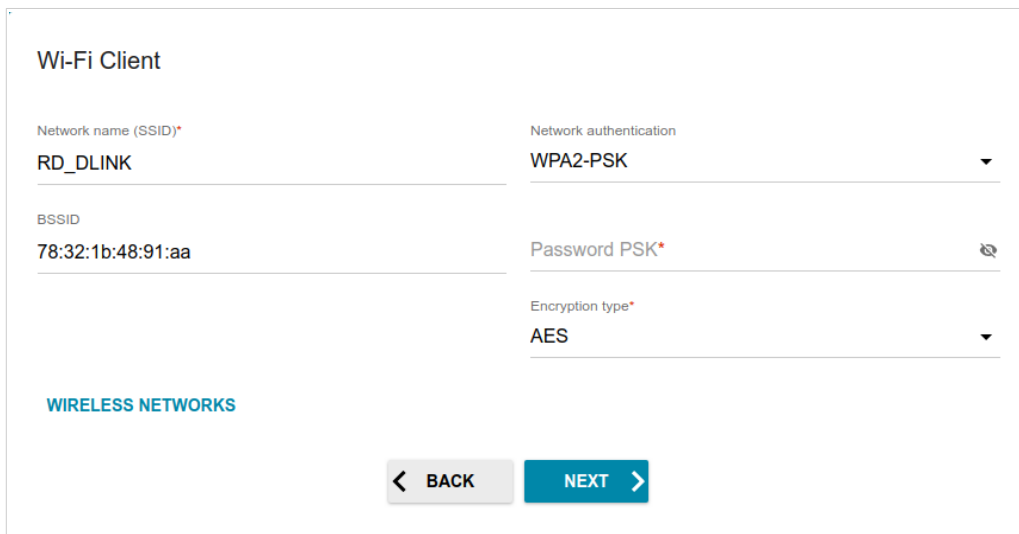


Figure 42. The page for configuring the Wi-Fi client.

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

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

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

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


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

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

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 a particular MAC address was registered by your ISP upon concluding the agreement, from the **MAC address assignment method** drop-down list, select the **Manual** value and enter this address in the **MAC address** field. Choose the **Clone MAC address of your device** value to place the MAC address of your network interface card in the field, or leave the **Default MAC address** value to place the access point's WAN interface MAC address in the field.
4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field.
5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

## Static IPv4 Connection

**Internet connection type**

Connection type  
Static IPv4

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

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

IP address\*

Subnet mask\*

Gateway IP address\*

DNS IP address\*

MAC address assignment method  
Default MAC address

MAC address  
A8:CB:DD:33:DC:AE

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

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

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

Ping

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

Figure 43. The page for configuring Static IPv4 WAN connection.

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

## Static IPv6 Connection

### Internet connection type

Connection type  
Static IPv6

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

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

IP address\*

Prefix\*

Gateway IP address\*

DNS IP address\*

MAC address assignment method  
Default MAC address

MAC address  
A8:CB:DD:33:DC:AE

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

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

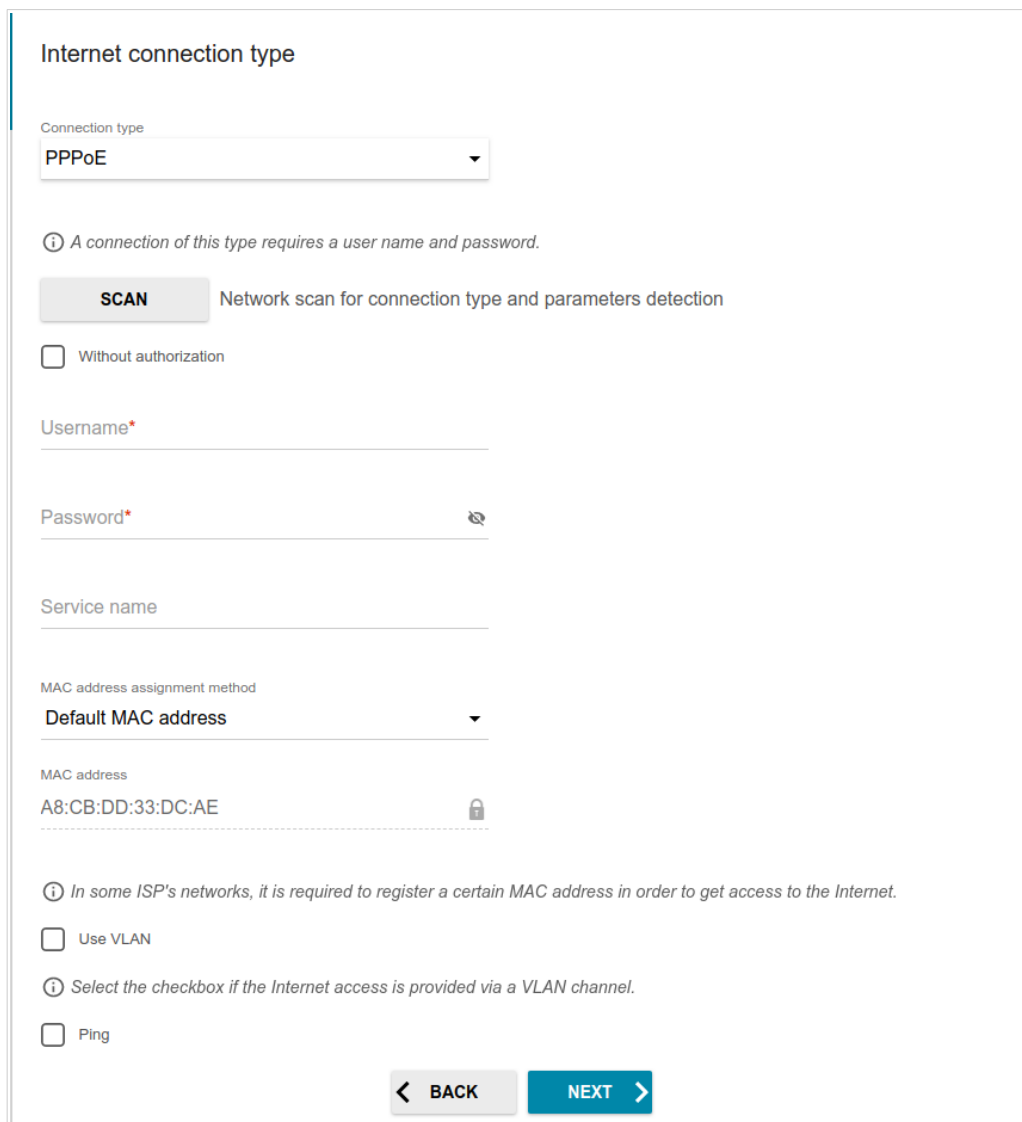
Ping

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

Figure 44. 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 configuration page titled "Internet connection type". The "Connection type" dropdown menu is set to "PPPoE". Below this, there is an information icon and a note: "A connection of this type requires a user name and password." 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 "Username\*" field is empty. The "Password\*" field contains a masked password and has a "Show" icon (an eye with a slash) to its right. The "Service name" field is empty. The "MAC address assignment method" dropdown menu is set to "Default MAC address". The "MAC address" field contains "A8:CB:DD:33:DC:AE" and has a lock icon to its right. Below this, there is another information icon and a note: "In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet." There are three checkboxes: "Use VLAN" (unchecked), "Select the checkbox if the Internet access is provided via a VLAN channel." (unchecked), and "Ping" (unchecked). At the bottom, there are "BACK" and "NEXT" navigation buttons.


Figure 45. 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

Internet connection type


Connection type  
PPPoE + Static IP (PPPoE Dual Access) ▼

 A connection of this type requires a user name, password, and a fixed IP address provided by your ISP.

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

Without authorization

Username\*

Password\* 

Service name

IP address\*

Subnet mask\*

Gateway IP address\*

DNS IP address\*

MAC address assignment method  
Default MAC address ▼



MAC address  
A8:CB:DD:33:DC:AE 

Figure 46. 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, a dropdown menu is set to "PPTP + Dynamic IP". Below this is an information icon and text: "PPTP and L2TP are methods for implementing virtual private networks." A "SCAN" button is followed by the text "Network scan for connection type and parameters detection". There is a checkbox labeled "Without authorization" which is currently unchecked. Below are input fields for "Username\*", "Password\*" (with a show/hide icon), and "VPN server address\*". A dropdown menu for "MAC address assignment method" is set to "Default MAC address". Below that is a "MAC address" field containing "A8:CB:DD:33:DC:AE" with a lock icon. Another information icon and text: "In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet." There are three checkboxes: "Use VLAN" (unchecked), "Use IGMP" (checked), and "Ping" (unchecked). Below "Use IGMP" is an information icon and text: "Internet Group Management Protocol is designed to manage multicast traffic in IP-based networks." At the bottom are "BACK" and "NEXT" navigation buttons.

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

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

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



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

Internet connection type


Connection type  
PPTP + Static IP

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

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

Without authorization

Username\*

Password\* 

VPN server address\*

IP address\*

Subnet mask\*

Gateway IP address\*

DNS IP address\*

MAC address assignment method  
Default MAC address



MAC address  
A8:CB:DD:33:DC:AE 

Figure 48. The page for configuring PPTP + Static IP WAN connection.

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

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

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

## Configuring Wireless Network

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

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

Open network

Password\*

.....

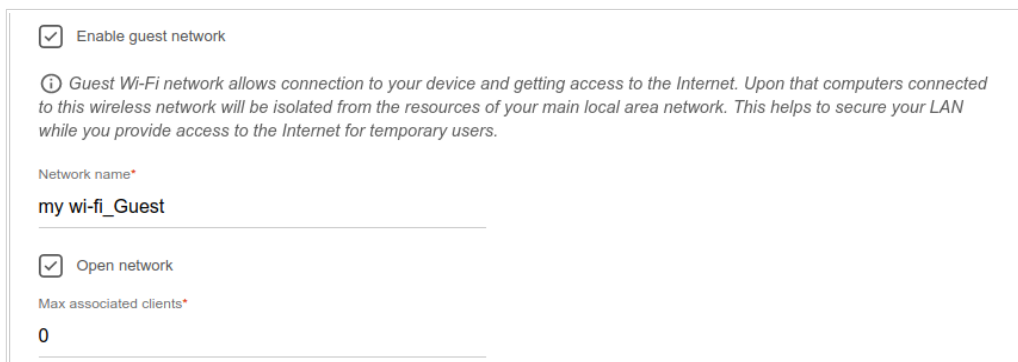
*Password should be between 8 and 63 ASCII characters*

**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 49. The page for configuring the wireless network.

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



The screenshot shows a configuration form for a wireless network. At the top, there is a checked checkbox labeled 'Enable guest network'. Below this is an information icon followed by a paragraph: '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.' Underneath is a text input field for 'Network name\*' with the value 'my wi-fi\_Guest'. Below that is another checked checkbox labeled 'Open network'. At the bottom, there is a text input field for 'Max associated clients\*' with the value '0'.

Figure 50. 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. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

## Configuring LAN Port for IPTV/VoIP

This configuration step is available for the **Router** mode. Configuration of the LAN port is available only via Wi-Fi connection to DAP-300P.

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

IPTV

Is an STB connected to the device?

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

Use VLAN ID

VLAN ID\*

*ⓘ Information about the VLAN ID can be found in the contract.*

WAN

Figure 51. The page for selecting a LAN port to connect an IPTV set-top box.

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

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

VoIP

Is an IP phone connected to the device?

*ⓘ If your ISP provides VoIP service, you can connect an IP phone directly to the router without additional equipment*

Use VLAN ID

VLAN ID\*

*ⓘ Information about the VLAN ID can be found in the contract.*

WAN

Figure 52. The page for selecting a LAN port to connect a VoIP phone.

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

## Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **User's interface password** and **Password confirmation** fields. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.<sup>2</sup>

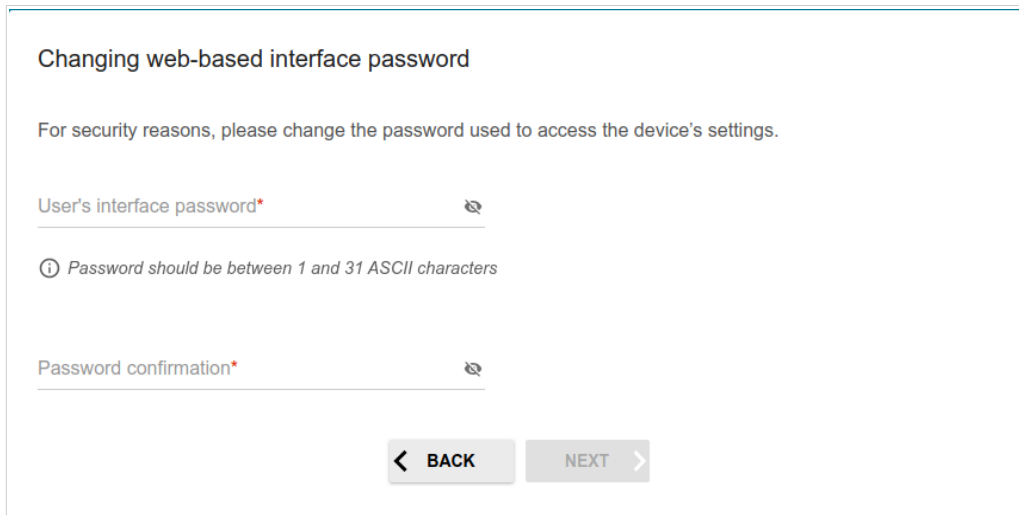


Figure 53. The page for changing the web-based interface password.



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.

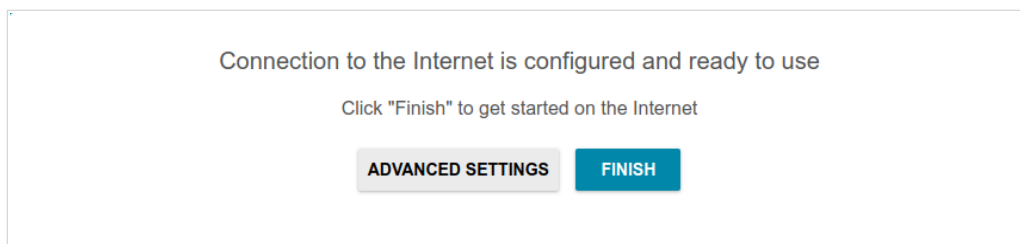
On the next page, check all specified settings.

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.

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

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



*Figure 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 39).

## 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 or available wireless interfaces 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-300P in order to use these devices.

**!** Configuration of the LAN port is available only via Wi-Fi connection to DAP-300P.

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

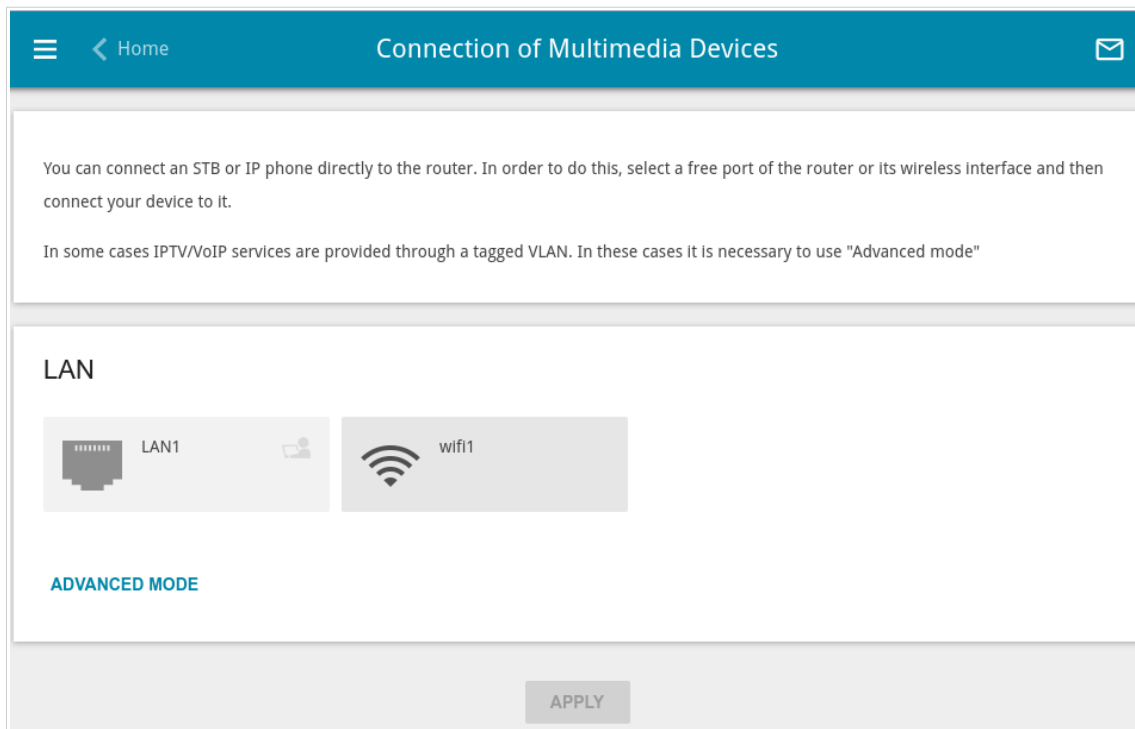


Figure 55. The Multimedia Devices Connection Wizard. The simplified mode.



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 (  ).

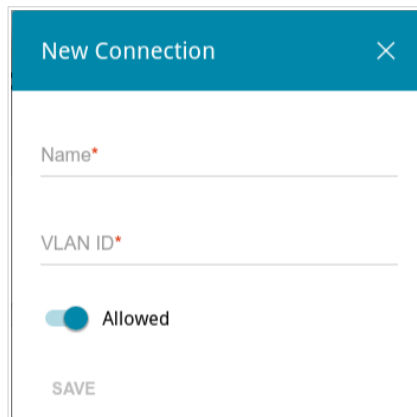



Figure 57. Adding a connection.

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 element corresponding to the LAN port or wireless interface to which the additional device is connected, select the created connection. Click the **APPLY** button.

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

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

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

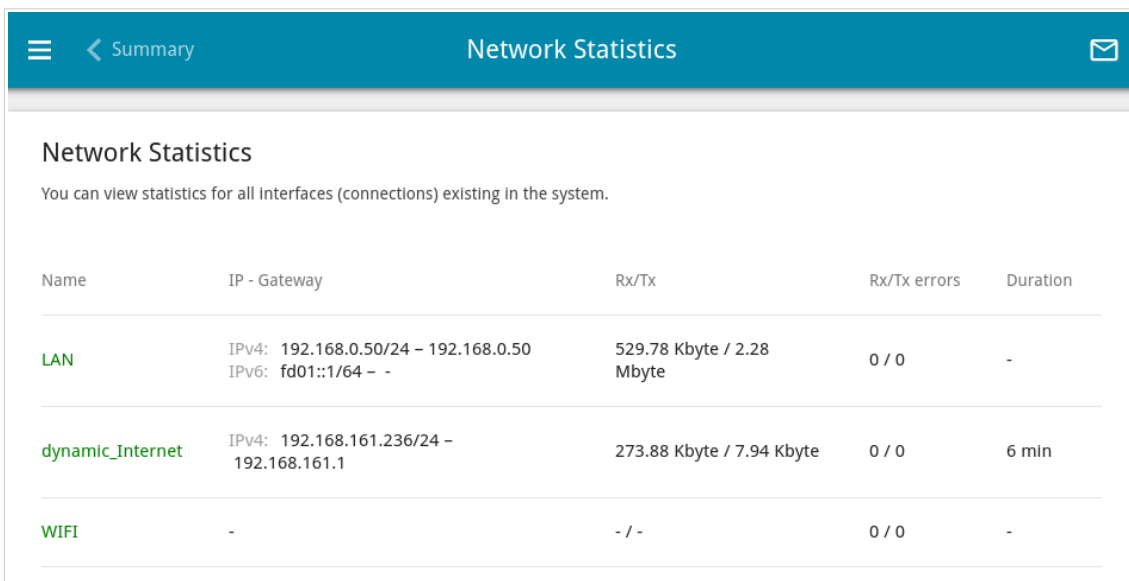
## Statistics

The pages of this section display data on the current state of the 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
- the routing table
- addresses of active multicast groups.

## Network Statistics

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



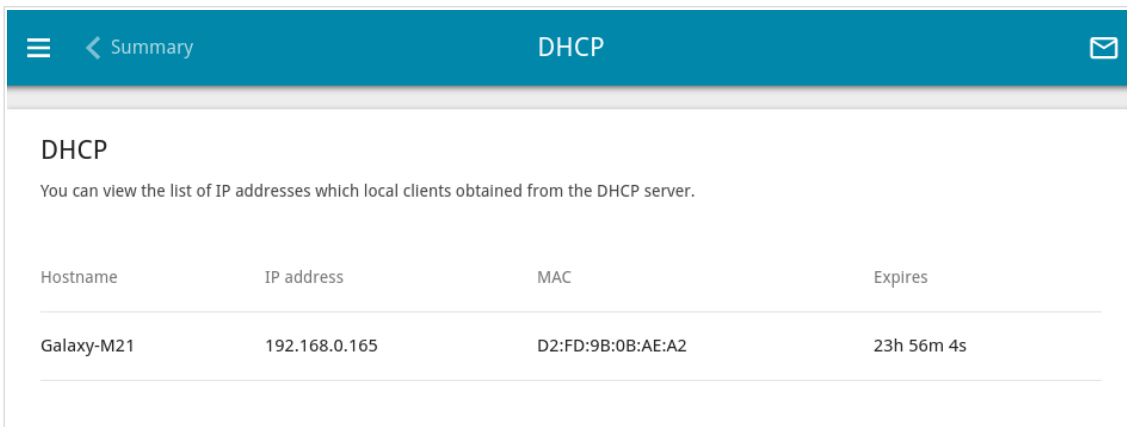
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.50/24 – 192.168.0.50 IPv6: fd01::1/64 – -	529.78 Kbyte / 2.28 Mbyte	0 / 0	-
dynamic_Internet	IPv4: 192.168.161.236/24 – 192.168.161.1	273.88 Kbyte / 7.94 Kbyte	0 / 0	6 min
WIFI	-	- / -	0 / 0	-

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 devices that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the device.

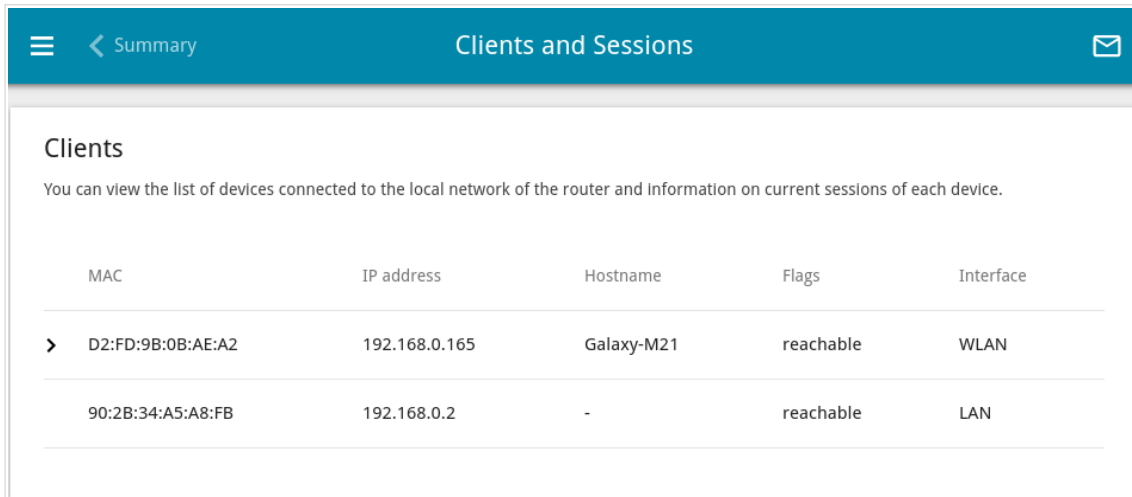


Hostname	IP address	MAC	Expires
Galaxy-M21	192.168.0.165	D2:FD:9B:0B:AE:A2	23h 56m 4s

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

## Clients and Sessions

On the **Statistics / Clients and Sessions** 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
> D2:FD:9B:0B:AE:A2	192.168.0.165	Galaxy-M21	reachable	WLAN
90:2B:34:A5:A8:FB	192.168.0.2	-	reachable	LAN

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

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

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

## 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
dynamic_Inter...	0.0.0.0	0.0.0.0	192.168.155.15	UG	100
dynamic_Inter...	8.8.4.4	255.255.255.255	192.168.155.15	UGH	0
LAN	192.168.0.0	255.255.255.0	0.0.0.0	U	0
dynamic_Inter...	192.168.155.0	255.255.255.0	0.0.0.0	U	0
dynamic_Inter...	192.168.161.140	255.255.255.255	192.168.155.15	UGH	0
LAN	224.0.0.251	255.255.255.255	0.0.0.0	UH	0
LAN	224.0.0.252	255.255.255.255	0.0.0.0	UH	0
LAN	fd01::/64		::	U	256
LAN	fd00::/8		::	U	256

Figure 61. The **Statistics / Routing Table** page.

## Multicast Groups

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

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

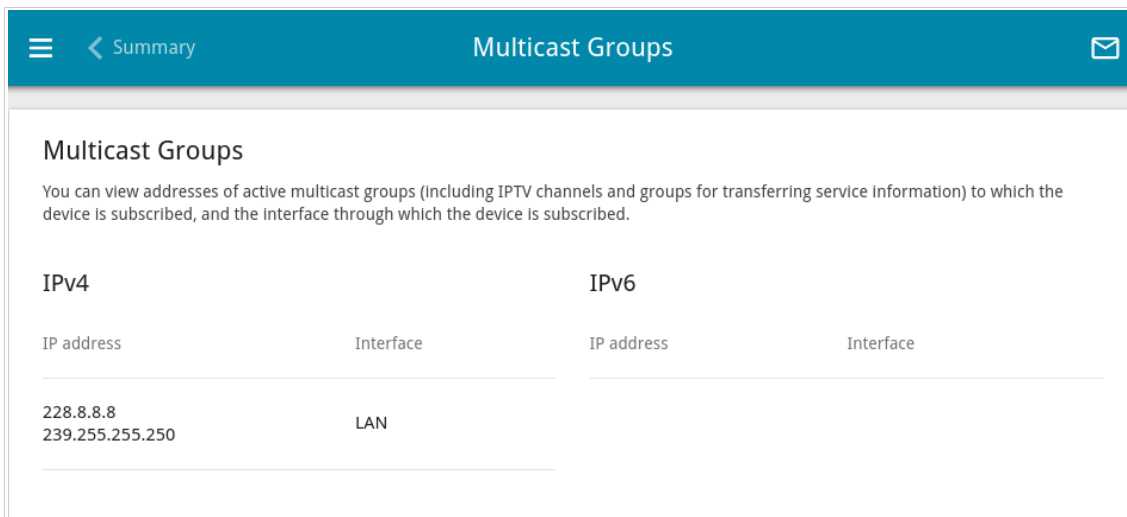


Figure 62. The **Statistics / Multicast Groups** page.

## Connections Setup

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

### LAN

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

#### IPv4

Go to the **IPv4** tab to change IPv4 address, configure IPv4 addresses assignment settings, or specify MAC address and IP address pairs.

**Local IP Address**

Mode of local IP address assignment  
 Static

IP address\*  
 192.168.0.50

Mask\*  
 255.255.255.0

Gateway IP address

Hostname  
 dlinkap986a.local

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

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

Parameter	Description
<b>Local IP Address</b>	
<b>Mode of local IP address assignment</b>	<p>For the <b>Access point, Repeater, and Client</b> modes only.</p> <p>Select the needed value from the drop-down list.</p> <ul style="list-style-type: none"> <li><b>Static:</b> The IP address, subnet mask, and the gateway IP address are assigned manually.</li> <li><b>Dynamic:</b> The access point automatically obtains these parameters from the LAN DHCP server or from the router to which it connects. When this value is selected, the controls of the <b>Dynamic IP Addresses</b> section are not available.</li> </ul>
<b>IP address</b>	The IP address of the access point in the local subnet. By default, the following value is specified: <b>192.168.0.50</b> .



Parameter	Description
<b>Mask</b>	The mask of the local subnet. By default, the following value is specified: <b>255 . 255 . 255 . 0</b> .
<b>Gateway IP address</b>	<i>For the <b>Access point, Repeater, and Client</b> modes only.</i> The gateway IP 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>
<b>Hostname</b>	The name of the device assigned to its IP address in the local subnet.

**Dynamic IP Addresses**

Mode of IPv4 address assignment  
 DHCP ▼

---

Start IP\*  
 192.168.0.100

---

End IP\*  
 192.168.0.200

---

**SELECT ADDRESS RANGE**

Lease time (in minutes)\*  
 1440


---

DNS relay

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

Figure 64. Configuring the local interface. The **IPv4** tab. The **Dynamic IP Addresses** section.

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

Parameter	Description
<b>External DHCP server IP</b>	<p>The IPv4 address of the external DHCP server which assigns IPv4 addresses to the access point's clients.</p> <p>To specify several IPv4 addresses, click the <b>ADD</b> button, and in the line displayed, enter an IPv4 address.</p> <p>To remove the IPv4 address, click the <b>Delete</b> button (  ) in the line of the address.</p>
<b>Option 82 Remote ID</b>	<p>The value of the Remote ID field of DHCP option 82 in accordance with RFC3046.</p> <p>Do not fill in the field unless your ISP or the administrator of the external DHCP server provided this value.</p>

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

In the **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 65. The section for configuring DHCP options.

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

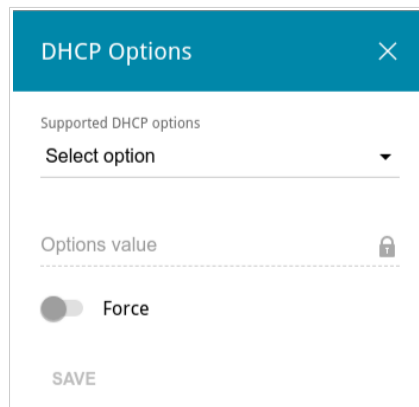



Figure 66. The window for configuring a DHCP option.

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

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

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

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

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

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

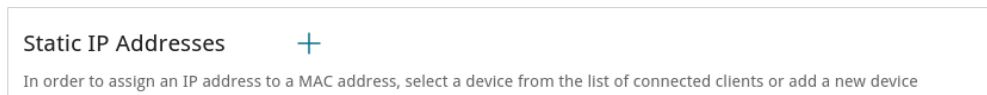




Figure 67. The section for creating MAC-IPv4 pairs.

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. To limit the time of the specified IPv4 address assignment, specify the required value in the **Lease time** field. Click the **SAVE** button.

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

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

## IPv6

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

**Local IPv6 Address**

Mode of local IP address assignment  
**Static** ▼

---

IPv6 address\*  
**fd01::1/64**

---

Gateway IPv6 address  
 For example: fd00::2

---

Hostname  
**dlinkapdcae.local**

---

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

Figure 68. Configuring the local interface. The **IPv6** tab. The **Local IPv6 Address** section.

Parameter	Description
<b>Local IPv6 Address</b>	
<b>Mode of local IP address assignment</b>	<p>Select the needed value from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Static:</b> An IPv6 address and a prefix are specified manually.</li> <li>• <b>Dynamic:</b> The access point automatically obtains these parameters from the LAN DHCPv6 server or from the router to which it connects. When this value is selected, the controls of the <b>Dynamic IP Addresses</b> section are not available. <i>Available if the <b>Access point, Repeater, or Client</b> mode was selected in the Initial Configuration Wizard.</i></li> <li>• <b>Prefix delegation:</b> The access point requests a prefix to configure an IPv6 address from a delegating router. <i>Available if the <b>Router</b> or <b>WISP Repeater</b> mode was selected in the Initial Configuration Wizard.</i></li> </ul>

Parameter	Description
<b>IPv6 address</b>	The IPv6 address of the access point in the local subnet. By default, the following value is specified: <b>fd01::1</b> . The field is available for editing if the <b>Static</b> value is selected from the <b>Mode of local IP address assignment</b> drop-down list.
<b>Gateway IPv6 address</b>	<i>Available if the <b>Access point, Repeater, or Client</b> 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>
<b>Hostname</b>	The name of the device assigned to its IPv6 address in the local subnet.

Dynamic IP Addresses

Mode of IPv6 address assignment  
Stateful ▼

---

Start IP\*

---

End IP\*

SELECT ADDRESS RANGE

---

Lease time (in minutes)\*

---

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

DNS relay

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

Figure 69. Configuring the local interface. The IPv6 tab. The **Dynamic IP Addresses** section.

Parameter	Description
<b>Dynamic IP Addresses</b>	
<b>Mode of IPv6 address assignment</b>	Select the needed value from the drop-down list. <ul style="list-style-type: none"> <li>• <b>Disable:</b> Clients' IPv6 addresses are assigned manually.</li> <li>• <b>Stateless:</b> Clients themselves configure IPv6 addresses using the prefix.</li> <li>• <b>Stateful:</b> The built-in DHCPv6 server of the access point allocates addresses from the range specified in the <b>Start IP</b> and <b>End IP</b> fields. Also when this value is selected, the <b>Static IP Addresses</b> section is displayed on the tab.</li> </ul>

Parameter	Description
<b>Start IP</b>	The start IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
<b>End IP</b>	The end IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
<b>SELECT ADDRESS RANGE</b>	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the <b>SAVE</b> button to automatically fill in the <b>Start IP</b> and <b>End IP</b> fields.
<b>Lease time</b>	The lifetime of IPv6 addresses provided to clients.
<b>DNS relay</b>	<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 <b>Advanced / DNS</b> page as the DNS server address.</p>

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

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

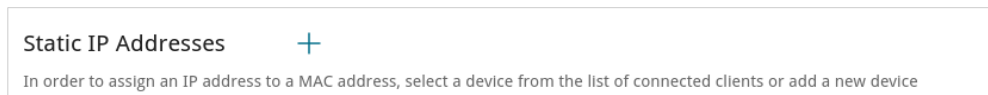




Figure 70. The section for creating MAC-IPv6 pairs.

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. To limit the time of the specified IPv6 address assignment, specify the required value in the **Lease time** field. Click the **SAVE** button.

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

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

## 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.

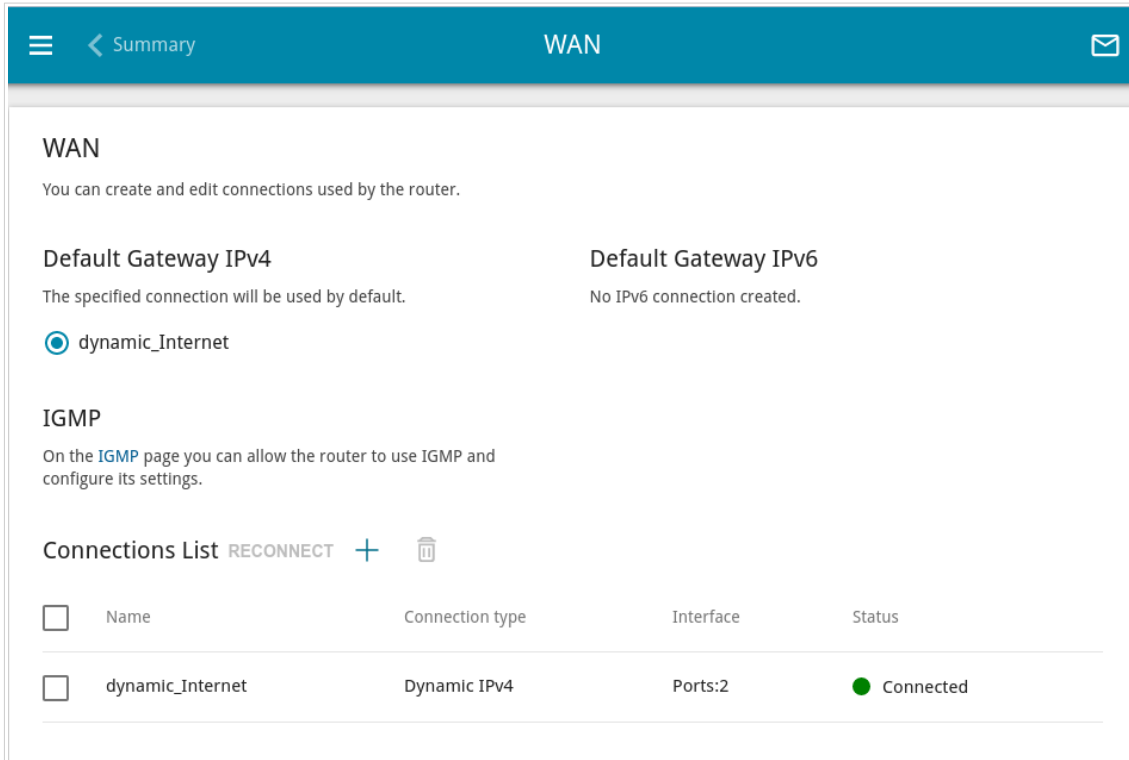



Figure 71. The **Connections Setup / WAN** page.

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

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

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

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

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP** link (for the description of the page, see the **IGMP** section, page 146).

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



## Creating Dynamic IPv4 or Static IPv4 WAN Connection

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

**General Settings**

Connection type  
Static IPv4

---

Interface  
Ports:2

---

Connection name\*  
statip\_29

---

Enable connection

NAT

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

Firewall

*ⓘ Protection against external connections for the LAN devices. For security reasons, it is recommended not to disable.*

Ping

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

RIP

Isolate connection

*ⓘ Use of an alternate routing table for this connection. It is recommended not to enable unless your ISP requires it.*

Figure 72. The page for creating a new **Static IPv4** connection. The **General Settings** section.

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

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

Ethernet

MAC address\*

A8:CB:DD:33:DC:AE

---

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

**RESTORE DEFAULT MAC ADDRESS**

MTU\*

1500

Figure 73. The page for creating a new **Static IPv4** connection. The **Ethernet** section.

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

**IPv4**

IP address\*

---

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

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

The screenshot shows a configuration window titled "Authorization via 802.1x Protocol". At the top, there is a toggle switch labeled "Enable authorization via 802.1x protocol". Below this, the "Authentication method" is set to "EAP-MD5" with a lock icon. There are two input fields: "Username" and "Password", both with lock icons. The "Password" field has a "Show" icon (an eye) to its right.

Figure 75. The page for creating a new **Static IPv4** connection. The **Authorization via 802.1x Protocol** section.

Parameter	Description
<b>Authorization via 802.1x Protocol</b>	
<b>Enable authorization via 802.1x protocol</b>	Move the switch to the right to allow authorization in the ISP's network via the 802.1x protocol.
<b>Authentication method</b>	Select a needed authentication method from the drop-down list.
<b>Username</b>	Enter the username provided by your ISP.
<b>Password</b>	Enter the password provided by your ISP. Click the <b>Show</b> icon (👁) to display the entered password.

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

## Creating Dynamic IPv6 or Static IPv6 WAN Connection

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

General Settings

Connection type  
 Static IPv6

Interface  
 Ports:2

Connection name\*  
 statipv6\_1

Enable connection

Firewall

*Protection against external connections for the LAN devices. For security reasons, it is recommended not to disable.*

Ping

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

RIP

Isolate connection

*Use of an alternate routing table for this connection. It is recommended not to enable unless your ISP requires it.*

Figure 76. The page for creating a new **Static IPv6** connection. The **General Settings** section.

Parameter	Description
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>Firewall</b>	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
<b>Ping</b>	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.
<b>RIP</b>	Move the switch to the right to allow using RIP for this connection.

Parameter	Description
<b>Isolate connection</b>	If the switch is moved to the right, the access point uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

Ethernet

MAC address\*

A8:CB:DD:33:DC:AE

---

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

**RESTORE DEFAULT MAC ADDRESS**

MTU\*

1500

Figure 77. The page for creating a new **Static IPv6** connection. The **Ethernet** section.

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

IPv6

IPv6 address\*

---

Prefix\*

---

Gateway IPv6 address\*

---

Primary IPv6 DNS server\*

---

Secondary IPv6 DNS server

---

Figure 78. The page for creating a new **Static IPv6** connection. The **IPv6** section.

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

Parameter	Description
<b>Primary IPv6 DNS server/Secondary IPv6 DNS server</b>	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.

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



## Creating PPPoE WAN Connection

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

**General Settings**

Connection type  
PPPoE

---

Interface  
Ports:2

---

Connection name\*  
pppoe\_24

---

Enable connection

NAT

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

Firewall

*ⓘ Protection against external connections for the LAN devices. For security reasons, it is recommended not to disable.*

Ping

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

RIP

Isolate connection

*ⓘ Use of an alternate routing table for this connection. It is recommended not to enable unless your ISP requires it.*

Figure 79. The page for creating a new PPPoE connection. The **General Settings** section.

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

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

Figure 80. The page for creating a new **PPPoE** connection. The **Ethernet** section.

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

**PPP**

Without authorization

Username\*

---

Password\* 🔍

---

Service name

---

MTU\*

1492

---

Authentication protocol

AUTO ▼

---

Keep Alive

LCP interval (in seconds)\*

30

---

LCP failures\*

3

---

Dial on demand

Maximum idle time (in seconds)

30 🔒

---

PPP IP extension

PPP debug

Figure 81. The page for creating a new **PPPoE** connection. The **PPP** section.

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

Parameter	Description
<b>Keep Alive</b>	If the switch is moved to the right, the access point sends echo requests in order to check the connection state. After several consecutive unanswered requests the access point restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the <b>LCP interval</b> and <b>LCP failures</b> fields correspondingly or leave the default values.
<b>Dial on demand</b>	Move the switch to the right if you want the access point to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.
<b>PPP IP extension</b>	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
<b>PPP debug</b>	Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list on the <b>System / Log</b> page (see the <i>Log</i> section, page 166).

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

## Creating PPTP or L2TP WAN Connection

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

**General Settings**

Connection type  
PPTP

---

Connection name\*  
pptp\_92

---

Enable connection

NAT

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

Firewall

*ⓘ Protection against external connections for the LAN devices. For security reasons, it is recommended not to disable.*

Ping

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

RIP

Isolate connection

*ⓘ Use of an alternate routing table for this connection. It is recommended not to enable unless your ISP requires it.*

Figure 82. The page for creating a new PPTP connection. The **General Settings** section.


Parameter	Description
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	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.
<b>Firewall</b>	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.

Parameter	Description
<b>Ping</b>	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.
<b>RIP</b>	Move the switch to the right to allow using RIP for this connection.
<b>Isolate connection</b>	If the switch is moved to the right, the access point uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

PPP

Without authorization

Username\*

Password\* 

VPN server address\*

MTU\*  
1456

Encryption protocol  
No encryption ▼


Authentication protocol  
AUTO ▼

Keep Alive

LCP interval (in seconds)\*  
30

LCP failures\*  
3

Dial on demand

Maximum idle time (in seconds)  
30 

Extra options

PPP debug

Enable MPPC

Figure 83. The page for creating a new PPTP connection. The PPP section.

Parameter	Description
<b>PPP</b>	
<b>Without authorization</b>	Move the switch to the right if you don't need to enter a username and password to access the Internet.

Parameter	Description
<b>Username</b>	A username (login) to access the Internet.
<b>Password</b>	A password to access the Internet. Click the <b>Show</b> icon (🔍) to display the entered password.
<b>VPN server address</b>	The IP address or full domain name of the PPTP or L2TP authentication server.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>Encryption protocol</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encryption</b>: MPPE encryption is not applied.</li> <li>• <b>MPPE 40 128 bit</b>: MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit</b>: MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit</b>: MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MS-CHAP</b>, <b>MS-CHAPv2</b>, or <b>AUTO</b> value is selected from the <b>Authentication protocol</b> drop-down list.</p>
<b>Authentication protocol</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.
<b>Keep Alive</b>	If the switch is moved to the right, the access point sends echo requests in order to check the connection state. After several consecutive unanswered requests the access point restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the <b>LCP interval</b> and <b>LCP failures</b> fields correspondingly or leave the default values.
<b>Dial on demand</b>	Move the switch to the right if you want the access point to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.
<b>Extra options</b>	Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional</i> .
<b>PPP debug</b>	Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list on the <b>System / Log</b> page (see the <i>Log</i> section, page 166).

Parameter	Description
<b>Enable MPPC</b>	<i>(Microsoft Point-to-Point Compression)</i> <i>For the <b>PPTP</b> type only.</i> Move the switch to the right if it is necessary to use the data compression function in order to configure the connection. Move the switch to the left to disable the 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 an existing connection which will be used to access the PPTP/L2TP server and click the **CONTINUE** button; or select the **create a new connection** choice of the radio button and click the **CREATE CONNECTION** button.

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



## Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

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

General Settings

Connection type  
 PPPoE IPv6

Interface  
 Ports:2

Connection name\*  
 pppoev6\_25

Enable connection

Firewall  
Protection against external connections for the LAN devices. For security reasons, it is recommended not to disable.

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

RIP

Isolate connection  
Use of an alternate routing table for this connection. It is recommended not to enable unless your ISP requires it.

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

Parameter	Description
<b>Interface</b>	A physical or virtual WAN interface to which the new connection will be assigned.
<b>Connection name</b>	A name for the connection for easier identification.
<b>Enable connection</b>	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
<b>NAT</b>	<i>For the <b>PPPoE Dual Stack</b> type only.</i> If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
<b>Firewall</b>	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.

Parameter	Description
<b>Ping</b>	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.
<b>RIP</b>	Move the switch to the right to allow using RIP for this connection.
<b>Isolate connection</b>	If the switch is moved to the right, the access point uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

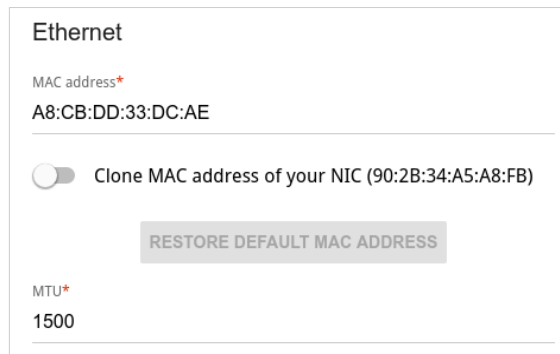


Figure 85. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.

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

**PPP**

Without authorization

Username\*

---

Password\* 🔒

---

Service name

---

MTU\*

1492

---

Authentication protocol

AUTO ▼

---

Keep Alive

LCP interval (in seconds)\*

30

---

LCP failures\*

3

---

Dial on demand

Maximum idle time (in seconds)

30 🔒

---

PPP IP extension

PPP debug

Figure 86. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.

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

Parameter	Description
<p><b>Keep Alive</b></p>	<p>If the switch is moved to the right, the access point sends echo requests in order to check the connection state. After several consecutive unanswered requests the access point restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the <b>LCP interval</b> and <b>LCP failures</b> fields correspondingly or leave the default values.</p>
<p><b>Dial on demand</b></p>	<p>Move the switch to the right if you want the access point to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.</p>
<p><b>PPP IP extension</b></p>	<p>This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.</p>
<p><b>PPP debug</b></p>	<p>Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the <b>Debugging messages</b> value should be selected from the <b>Level</b> drop-down list on the <b>System / Log</b> page (see the <i>Log</i> section, page 166).</p>

Figure 87. The page for creating a new PPPoE Pv6 connection. The IPv6 section.

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

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

## WAN Failover

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

On the **Connections Setup / WAN Failover** page, you can enable the WAN backup function, which provides you with uninterrupted access to the Internet. When your main connection breaks down, the 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 88. The **Connections Setup / WAN Failover** page.

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

Parameter	Description
<b>Basic connection</b>	From the drop-down list, select a WAN connection which will be used as the main one.
<b>Backup connection</b>	From the drop-down list, select a WAN connection which will be used as the reserve one.
<b>Test host</b>	An IP address that the access point will check for availability via ICMP ping mechanism.
<b>Interval between checks</b>	A time period (in seconds) between attempts to check the status of the main connection. By default, the value <b>10</b> is specified.

Parameter	Description
<b>Timeout check</b>	A time period (in seconds) for an attempt to check the status of the main connection. At the end of this period the access point's internal system makes a decision to enable/disable the reserve channel. By default, the value <b>3</b> is specified.
<b>Number of inspections of active connection</b>	A number of requests that will be sent in order to analyze the status of the main connection when the connection is active (the access point uses the main connection as a default gateway).
<b>Number of inspections of inactive connection</b>	A number of requests that will be sent in order to analyze the status of the main connection when the connection is inactive (the access point uses the reserve connection as a default gateway).

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

## Wi-Fi

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

### Basic Settings

In the **Wi-Fi / Basic Settings** section, you can change basic parameters for the wireless interface of the access point and configure the basic and additional wireless networks.

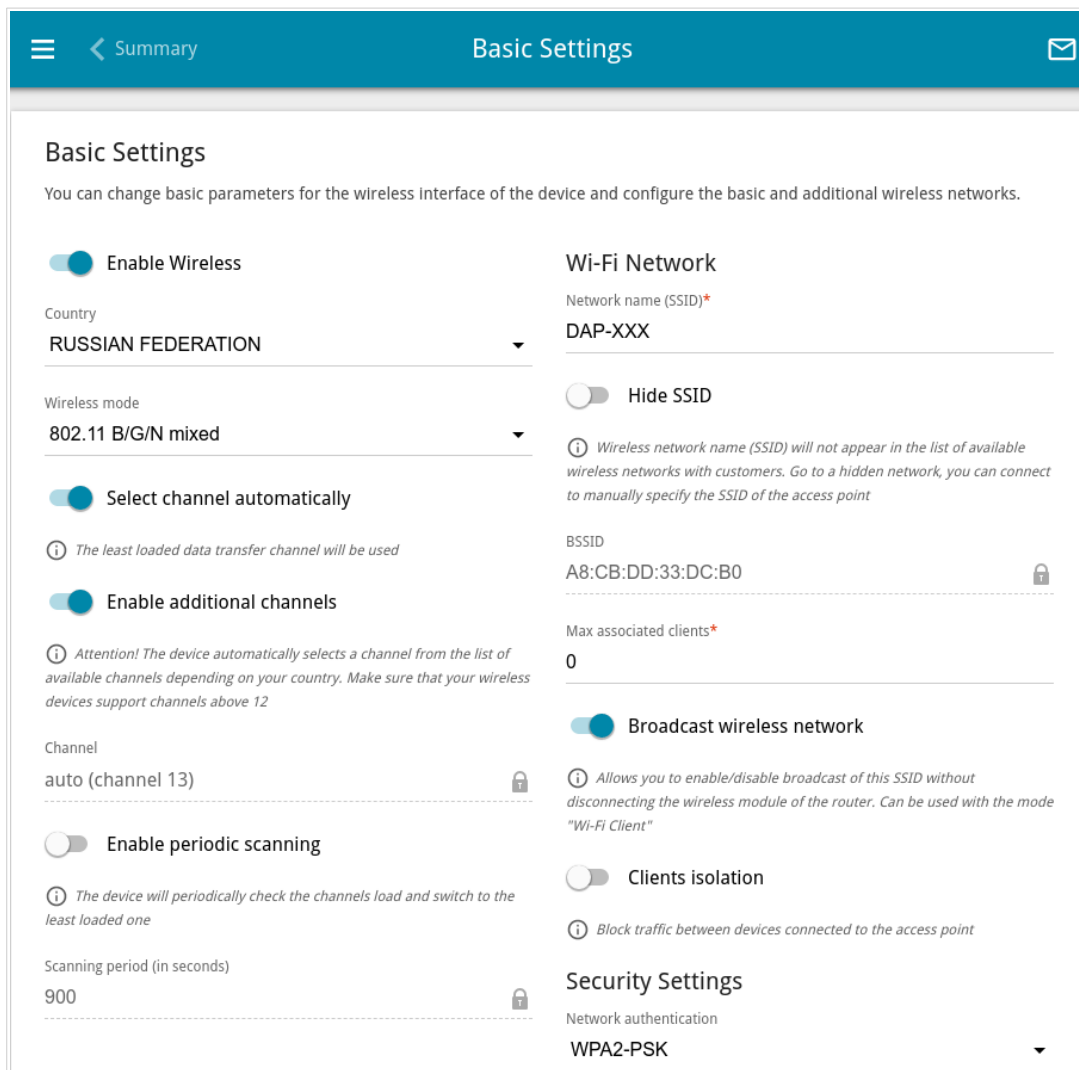


Figure 89. Basic settings of the wireless LAN.

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

Parameter	Description
<b>Enable Wireless</b>	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left.
<b>Country</b>	The country you are in. Select a value from the drop-down list.
<b>Wireless mode</b>	Operating mode of the wireless network of the 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.



Parameter	Description
<b>Select channel automatically</b>	Move the switch to the right to let the access point itself choose the channel with the least interference.
<b>Enable additional channels</b>	If the switch is moved to the left, the device automatically selects one of available standard channels. To use additional channels (the 12th and 13th), move the switch to the right.
<b>Channel</b>	The wireless channel number. To select a channel manually, left-click; in the opened window, select a channel and click the <b>SAVE</b> button. The action is available, when the <b>Select channel automatically</b> switch is moved to the left.
<b>Enable periodic scanning</b>	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 <b>Scanning period</b> field is available for editing.
<b>Scanning period</b>	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.

Figure 90. Creating a wireless network.

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

Parameter	Description
<b>Broadcast wireless network</b>	If the switch is moved to the left, devices cannot connect to the wireless network. Upon that the access point can connect to another access point as a wireless client.
<b>Clients isolation</b>	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
<b>Enable guest network</b>	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.

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

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

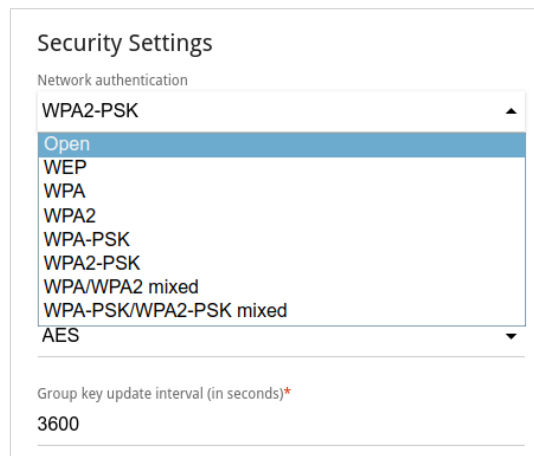


Figure 91. Network authentication types supported by the access point.

The access point supports the following authentication types:

Authentication type	Description
<b>Open</b>	Open authentication (with WEP encryption for wireless network modes not supporting 802.11n devices).
<b>WEP</b>	Authentication with a shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n devices is selected from the <b>Wireless mode</b> drop-down list on the <b>Wi-Fi / Basic Settings</b> page.
<b>WPA</b>	WPA-based authentication using a RADIUS server.
<b>WPA-PSK</b>	WPA-based authentication using a PSK.
<b>WPA2</b>	WPA2-based authentication using a RADIUS server.
<b>WPA2-PSK</b>	WPA2-based authentication using a PSK.

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

**!** 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):

The screenshot shows the 'Security Settings' page. At the top, 'Network authentication' is set to 'Open'. Below this, there is a toggle for 'Enable encryption WEP' which is turned on. A 'Default key ID' dropdown is set to '1'. A note states: 'It is recommended to use the first key by default to ensure compatibility with many devices.' There is also a toggle for 'Encryption key WEP as HEX' which is turned off. A note says: '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 clear button.

Figure 92. The **Open** value is selected from the **Network authentication** drop-down list.

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

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

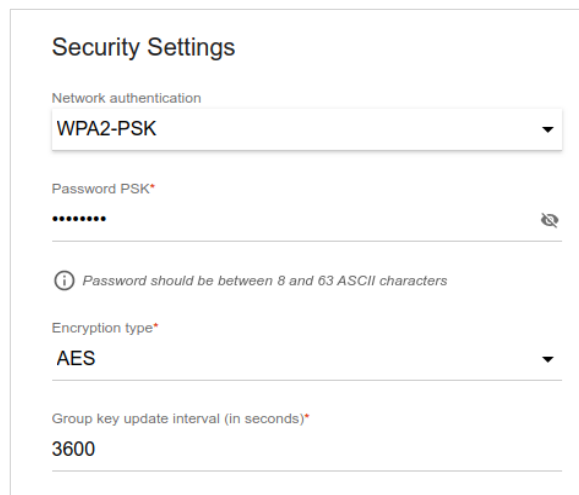
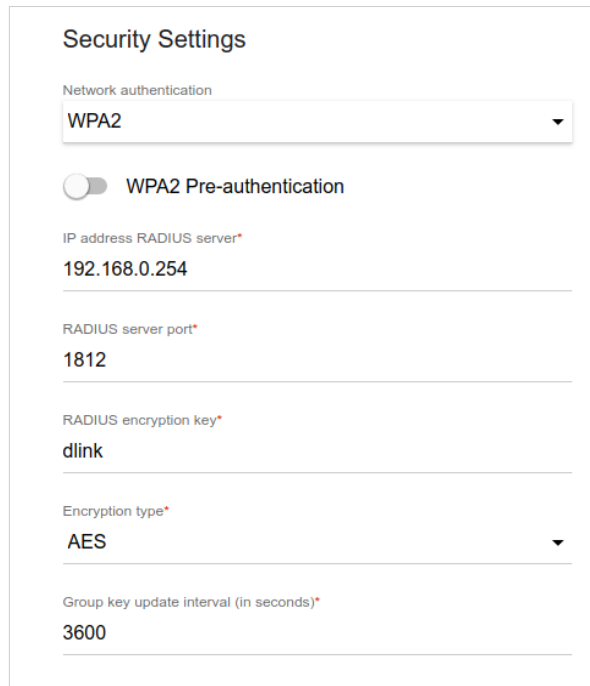


Figure 93. The **WPA2-PSK** value is selected from the **Network authentication** drop-down list.

Parameter	Description
<b>Password PSK</b>	A password for WPA encryption. The password can contain digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout. <sup>3</sup> Click the <b>Show</b> icon (🔍) to display the entered password.
<b>Encryption type</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> .
<b>Group key update interval</b>	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value <b>0</b> is specified for this field, the key is not renewed.

<sup>3</sup> 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' configuration page. At the top, 'Network authentication' is set to 'WPA2'. Below this, the 'WPA2 Pre-authentication' toggle is turned off. The 'IP address RADIUS server\*' field contains '192.168.0.254'. The 'RADIUS server port\*' field contains '1812'. The 'RADIUS encryption key\*' field contains 'dlink'. The 'Encryption type\*' dropdown menu is set to 'AES'. The 'Group key update interval (in seconds)\*' field contains '3600'.

Figure 94. The **WPA2** value is selected from the **Network authentication** drop-down list.

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

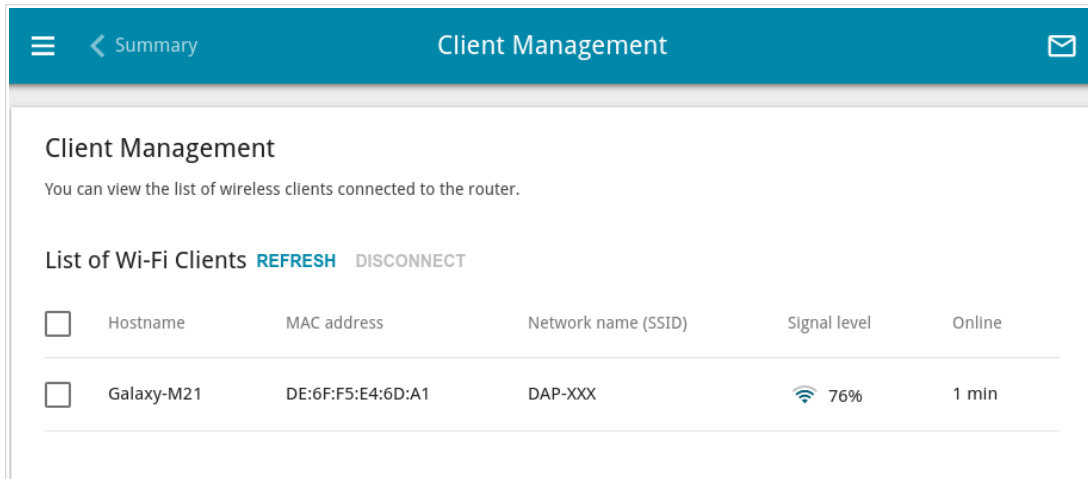
When you have configured the parameters, click the **APPLY** button.

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

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

## Client Management

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



*Figure 95. 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 are not available.

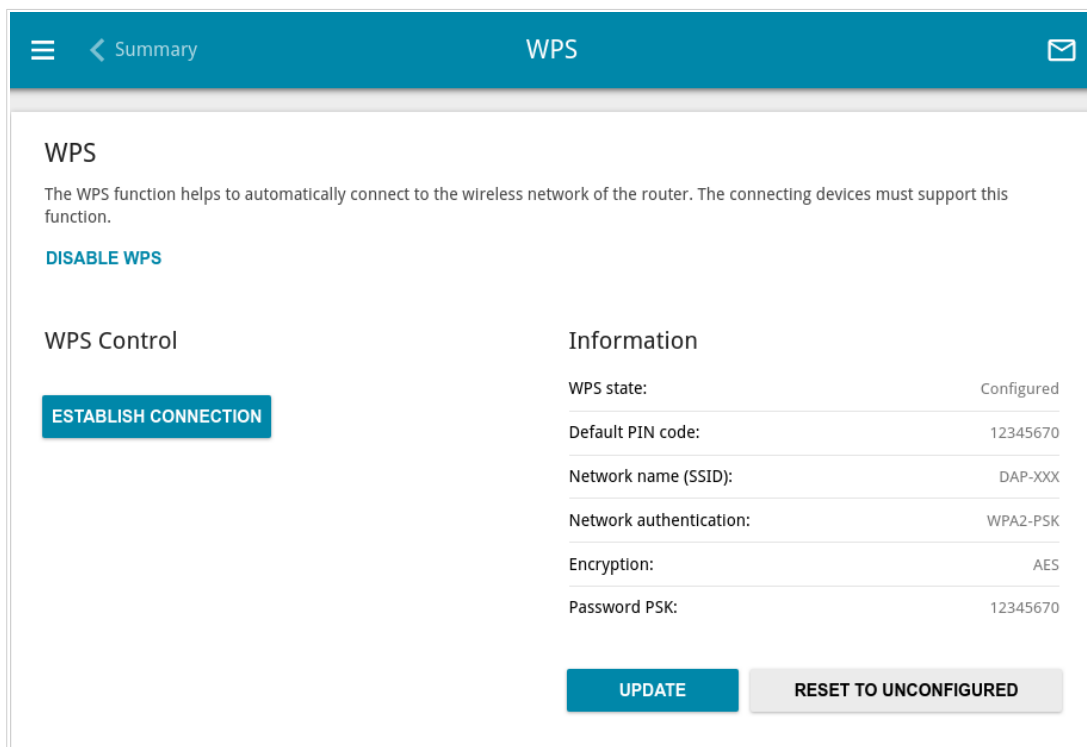


Figure 96. The page for configuring the WPS function.

To activate the WPS function, click the **ENABLE WPS** button.



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

Parameter	Description
<b>WPS state</b>	The state of the WPS function: <ul style="list-style-type: none"> <li>• <b>Configured</b> (all needed settings are specified; these settings will be used upon establishing the wireless connection)</li> <li>• <b>Unconfigured</b> (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).</li> </ul>
<b>Default PIN code</b>	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.
<b>Network name (SSID)</b>	The name of the access point's wireless network.
<b>Network authentication</b>	The network authentication type specified for the wireless network.
<b>Encryption</b>	The encryption type specified for the wireless network.
<b>Password PSK</b>	The encryption password specified for the wireless network.
<b>UPDATE</b>	Click the button to update the data on the page.
<b>RESET TO UNCONFIGURED</b>	Click the button to reset the parameters of the WPS function.

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

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

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

To enable the WMM function, click the **ENABLE** button. When the WMM function is enabled, the **Access Point** and **Station** sections are displayed on the page.

Configuration WMM

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

**DISABLE**

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

Figure 97. 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.

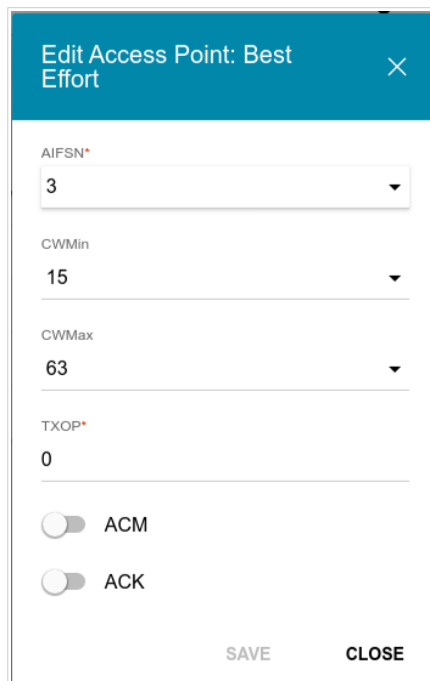


Figure 98. The window for changing parameters of the WMM function.

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

Parameter	Description
<b>ACM</b>	<i>Admission Control Mandatory.</i> If the switch is moved to the right, the device cannot use the relevant Access Category.
<b>ACK</b>	<i>Acknowledgment.</i> Answering response requests while transmitting. Displayed only in the <b>Access Point</b> section. If the switch is moved to the left, the 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 access point as a client to connect to a wireless access point or to a WISP.

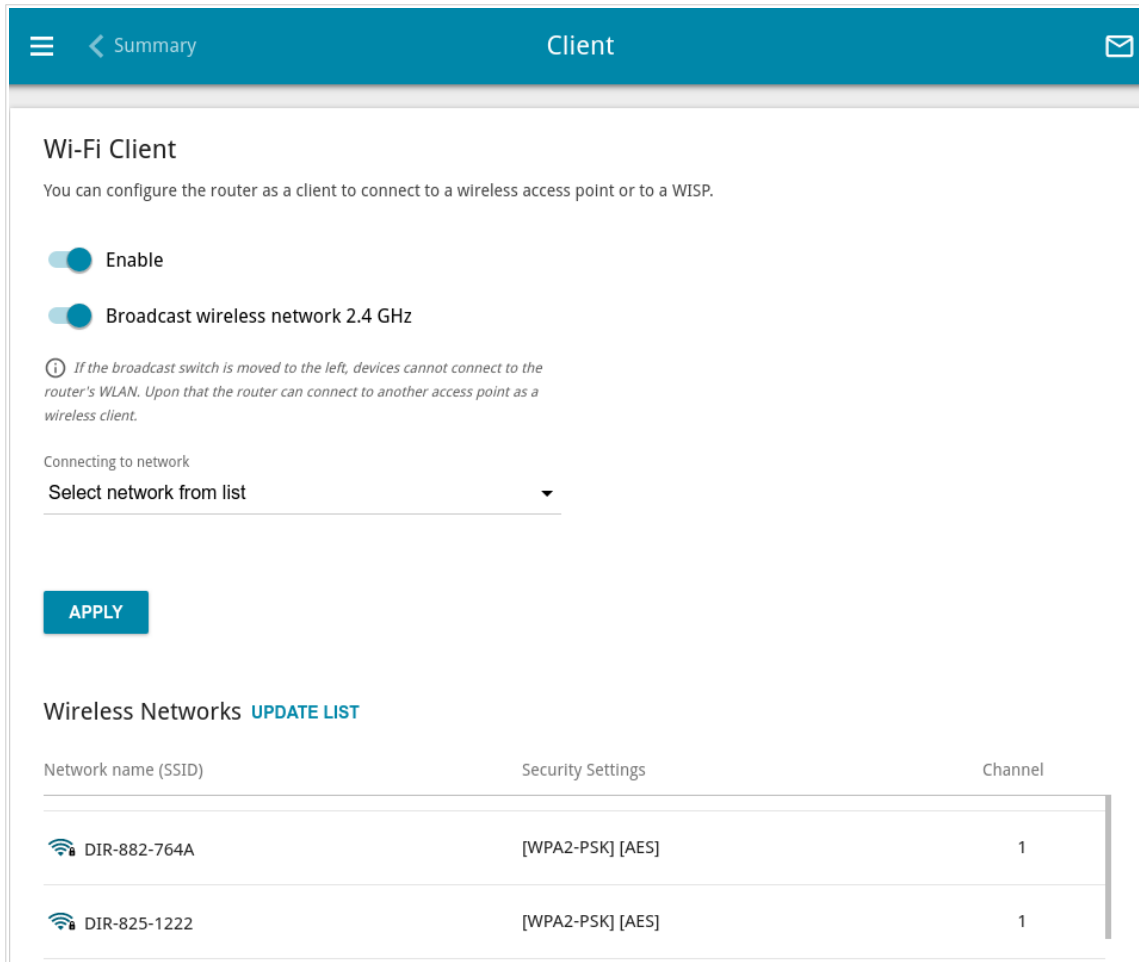


Figure 99. The page for configuring the client mode.

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
<b>Broadcast wireless network 2.4 GHz</b>	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.
<b>Connecting to network</b>	A method for connecting to another access point.

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

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

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

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

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

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

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

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

## Additional

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

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

The screenshot shows the 'Additional' settings page for Wi-Fi. The page has a blue header with a menu icon, a back arrow labeled 'Summary', the title 'Additional', and an envelope icon. Below the header, the section is titled 'Wi-Fi Additional Settings' with a subtitle 'You can define additional parameters for the WLAN of the router.' The settings are organized into two columns. The left column includes: Bandwidth (20/40 MHz), a help icon with text 'Using bandwidth of one or several channels of the wireless network simultaneously', 'Current bandwidth: 40 MHz', an 'Autonegotiation 20/40 (Coexistence)' toggle (off), a help icon with text 'Automatic change of bandwidth in the loaded environment', TX power (in percent) (100), a 'Drop multicast' toggle (on), a help icon with text 'Disables multicasting (IGMP, SSDP, etc.) for the wireless network. In some cases this helps to improve performance', an 'Adaptivity mode' toggle (on), a help icon with text 'Reduces influence on operation of other wireless devices in the loaded environment. This can lower performance of your wireless network', and an 'STBC' toggle (off). 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 100. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
<b>Bandwidth</b>	<p>The channel bandwidth for 802.11n standard.</p> <ul style="list-style-type: none"> <li>• <b>20 MHz:</b> 802.11n clients operate at 20MHz channels.</li> <li>• <b>20/40 MHz:</b> 802.11n clients operate at 20MHz or 40MHz channels.</li> </ul>



Parameter	Description
<b>Autonegotiation 20/40 (Coexistence)</b>	Move the switch to the right to let the access point automatically choose the most suitable channel bandwidth (20MHz or 40MHz) for the connected devices (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the <b>20/40 MHz</b> value is selected from the <b>Bandwidth</b> drop-down list.
<b>TX power</b>	The transmit power (in percentage terms) of the access point.
<b>Drop multicast</b>	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 <b>Advanced / IGMP</b> page.
<b>Adaptivity mode</b>	Move the switch to the right to let the access point switch from the channels at which radars and other mobile or stationary radio systems operate in case it interferes with these devices. Such a setting can slow down the access point's WLAN. In order to use the adaptivity mode, the automatic channel selection should be enabled (on the <b>Wi-Fi / Basic Settings</b> page).
<b>STBC</b>	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. Move the switch to the right if you need to use the STBC technique.
<b>B/G protection</b>	The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Select a value from the drop-down list. <ul style="list-style-type: none"> <li>• <b>Auto:</b> The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices).</li> <li>• <b>Always On:</b> The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</li> <li>• <b>Always Off:</b> The protection function is always disabled.</li> </ul>

Parameter	Description
<b>Short GI</b>	<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"> <li>• <b>Enable:</b> The access point uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n standard (see the value of the <b>Wireless mode</b> drop-down list on the <b>Wi-Fi / Basic Settings</b> page).</li> <li>• <b>Disable:</b> The access point uses the 800 ns standard guard interval.</li> </ul>
<b>Beacon period</b>	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
<b>RTS threshold</b>	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
<b>Frag threshold</b>	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).
<b>DTIM period</b>	The number of beacon frames between sending DTIM messages (messages notifying on broadcast or multicast transmission).
<b>Station Keep Alive</b>	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value <b>0</b> is specified, the checking is disabled.

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

## MAC Filter

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

**!** It is recommended to configure the Wi-Fi MAC filter through a wired connection to DAP-300P.

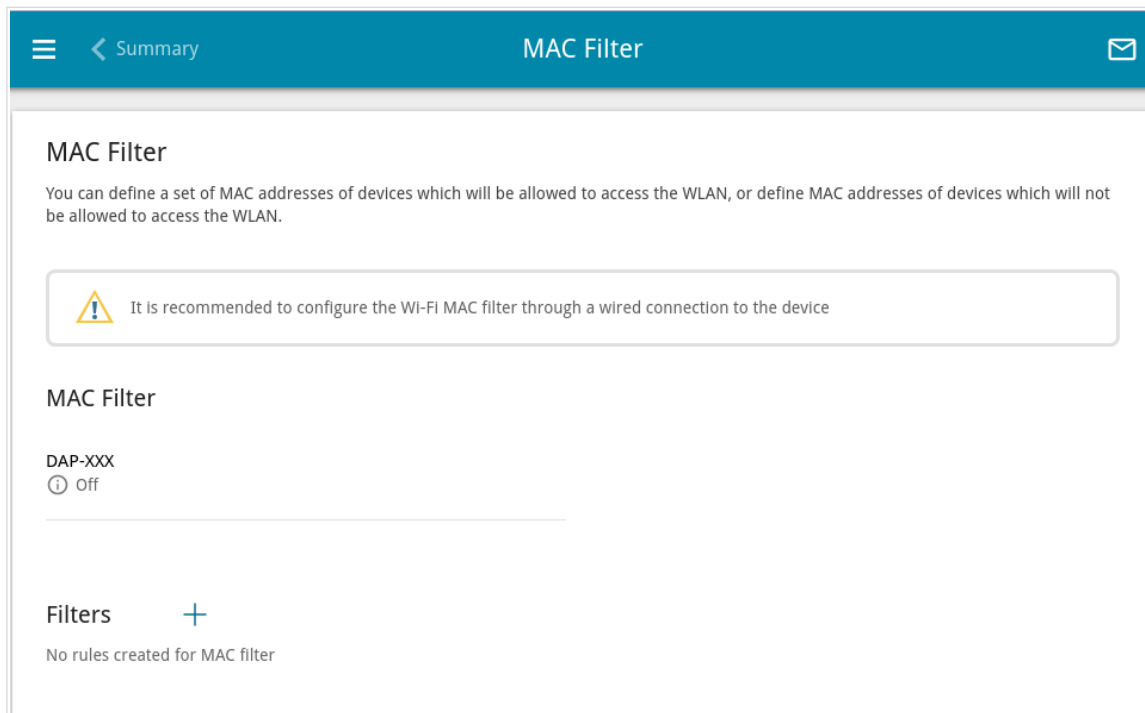


Figure 101. The page for configuring the MAC filter for the wireless network.

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 ( **+** ).

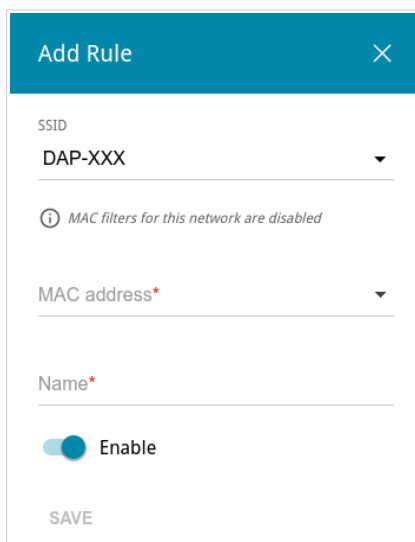


Figure 102. The window for adding a rule for the MAC filter.

You can specify the following parameters:

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

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

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

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

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

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

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

## ***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 VLANs
- configure a DDNS service
- configure notifications on the reason of the Internet connection failure
- define static routes
- configure TR-069 client
- enable the UPnP IGD function
- enable the built-in UDPXY application for the access point
- allow the access point to use IGMP
- enable the RTSP, SIP ALG mechanisms, and PPPoE/PPTP/L2TP/IPsec pass through functions.

## DNS

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

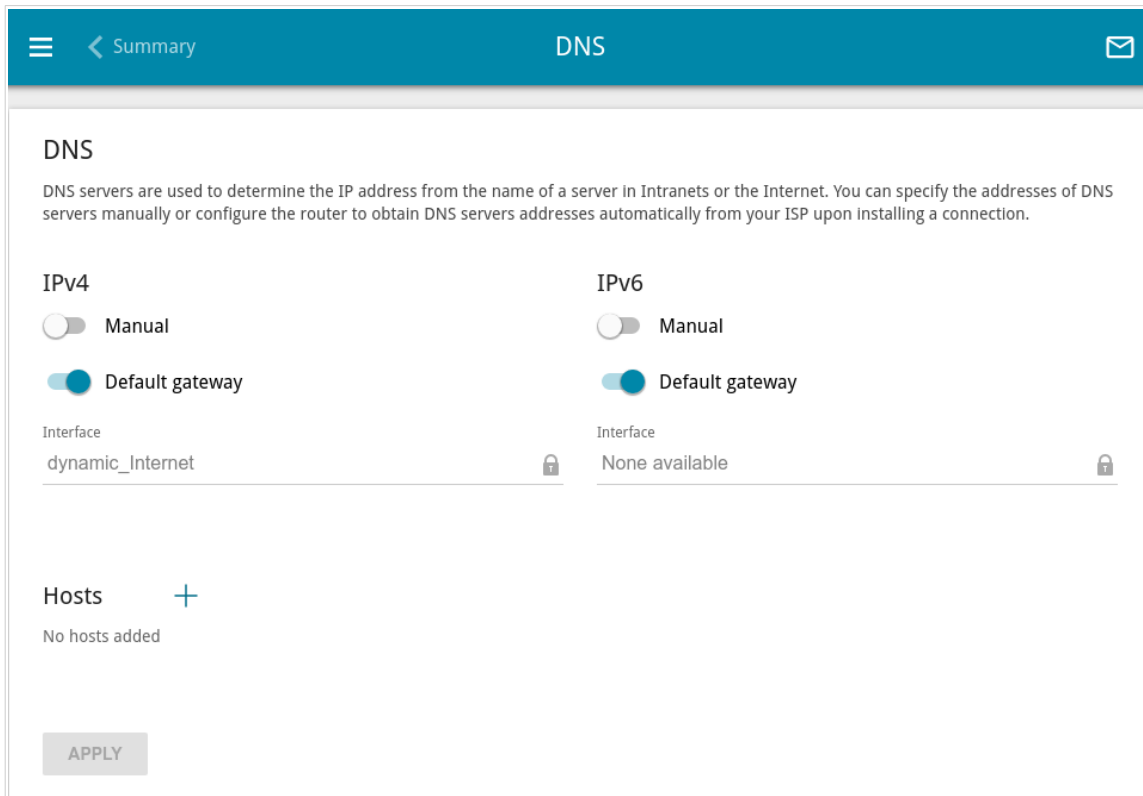


Figure 103. The **Advanced / DNS** page.

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.




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

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

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

To specify a DNS server manually, move the **Manual** switch to the right. 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 remove a DNS server from the page, click the **Delete** button (  ) in the line of the address and then click the **APPLY** button.

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

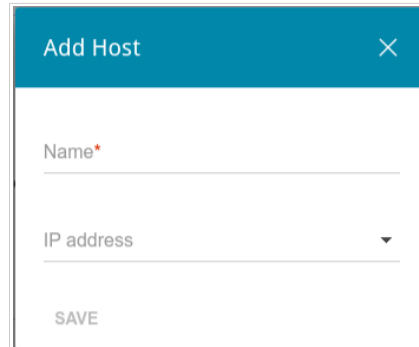



Figure 104. The window for adding a DNS record.

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

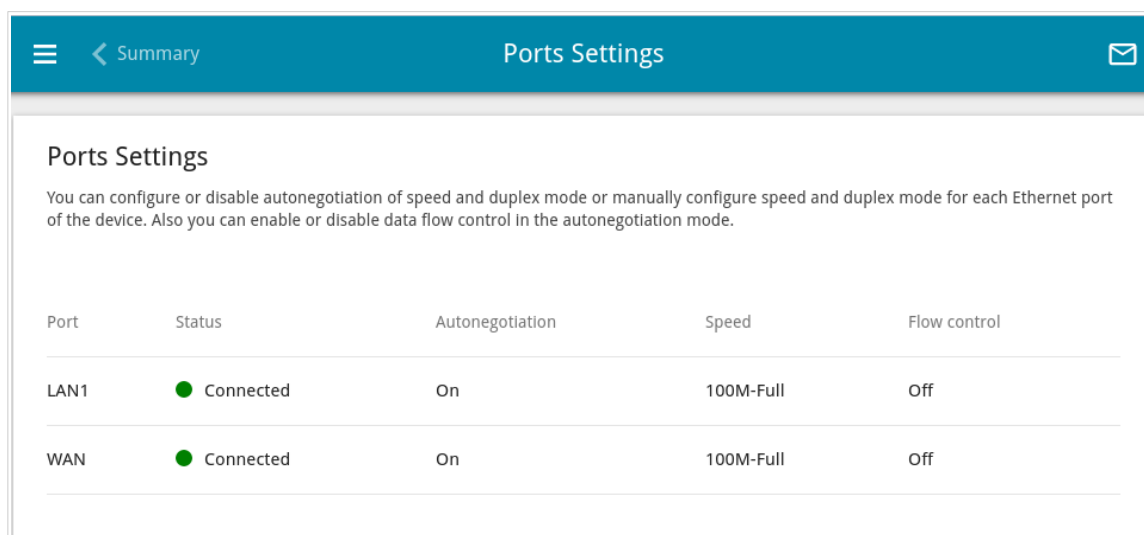
To remove a record, in the **Hosts** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button (  ).

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

## 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	100M-Full	Off
WAN	● Connected	On	100M-Full	Off

Figure 105. 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.



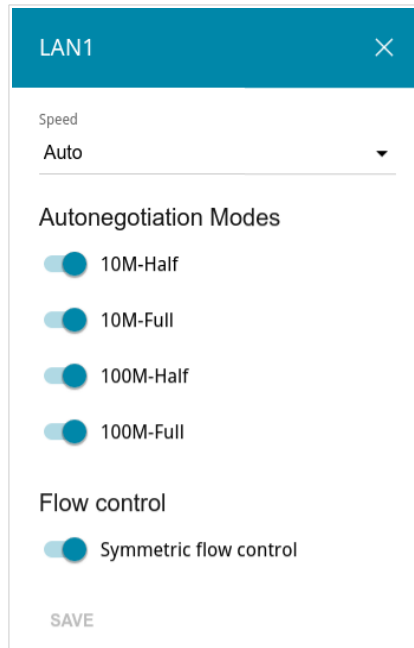


Figure 106. The window for changing the settings of the access point's port.

In the opened window, specify the needed parameters:

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

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

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

If in the future you need to edit the parameters of the 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.

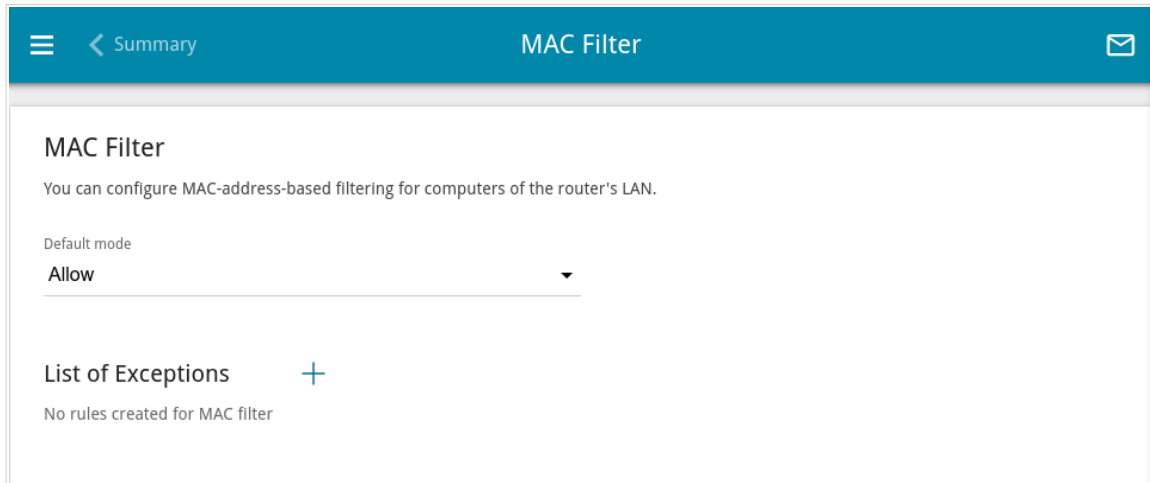


Figure 107. The **Advanced / MAC Filter** page.

Select the needed action from the drop-down list in the **Default mode** section to configure filtering for all devices of the 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 the specified filtering mode will be applied), click the **ADD** button ( **+** ).

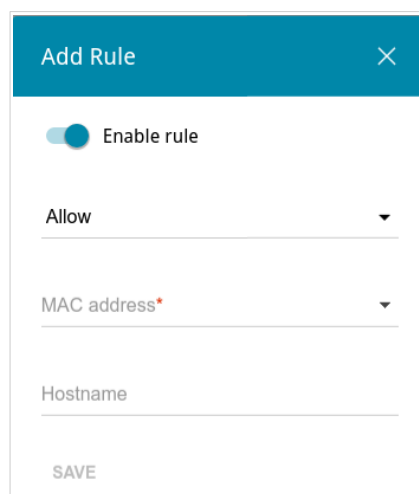



Figure 108. The window for adding a rule for the MAC filter.

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

Parameter	Description
<b>Enable rule</b>	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
<b>Action</b>	Select an action for the rule. <ul style="list-style-type: none"> <li>• <b>Deny:</b> Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices.</li> <li>• <b>Allow:</b> Allows access to the 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.</li> </ul>
<b>MAC address</b>	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).
<b>Hostname</b>	The name of the device for easier identification. You can specify any name.

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

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

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

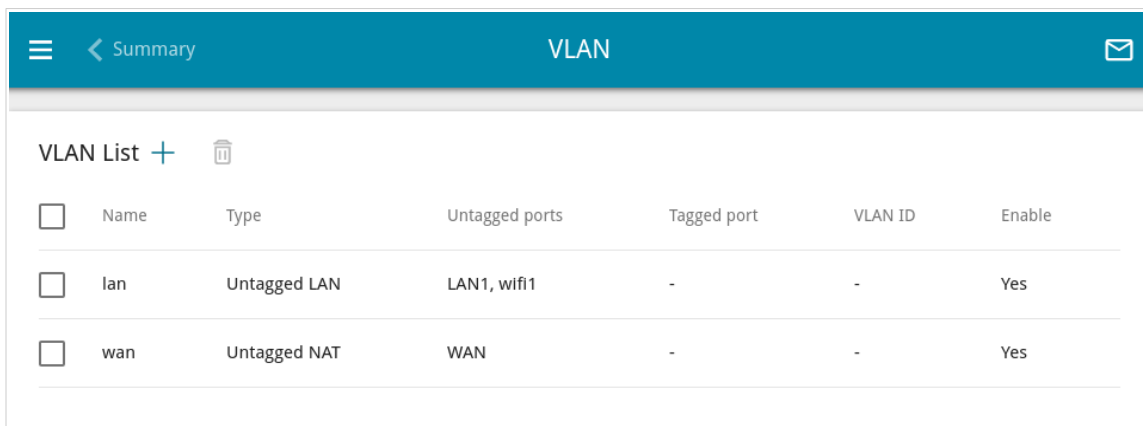
## VLAN

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"/>	Name	Type	Untagged ports	Tagged port	VLAN ID	Enable
<input type="checkbox"/>	lan	Untagged LAN	LAN1, wifi1	-	-	Yes
<input type="checkbox"/>	wan	Untagged NAT	WAN	-	-	Yes

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

If you want to create a VLAN including the LAN port or available Wi-Fi networks of the access point, first delete relevant records from the **lan** network on this page. To do this, select the **lan** line. On the opened page, in the **Untagged Ports** section, deselect the checkbox located to the left of the relevant element, and click the **APPLY** button.

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

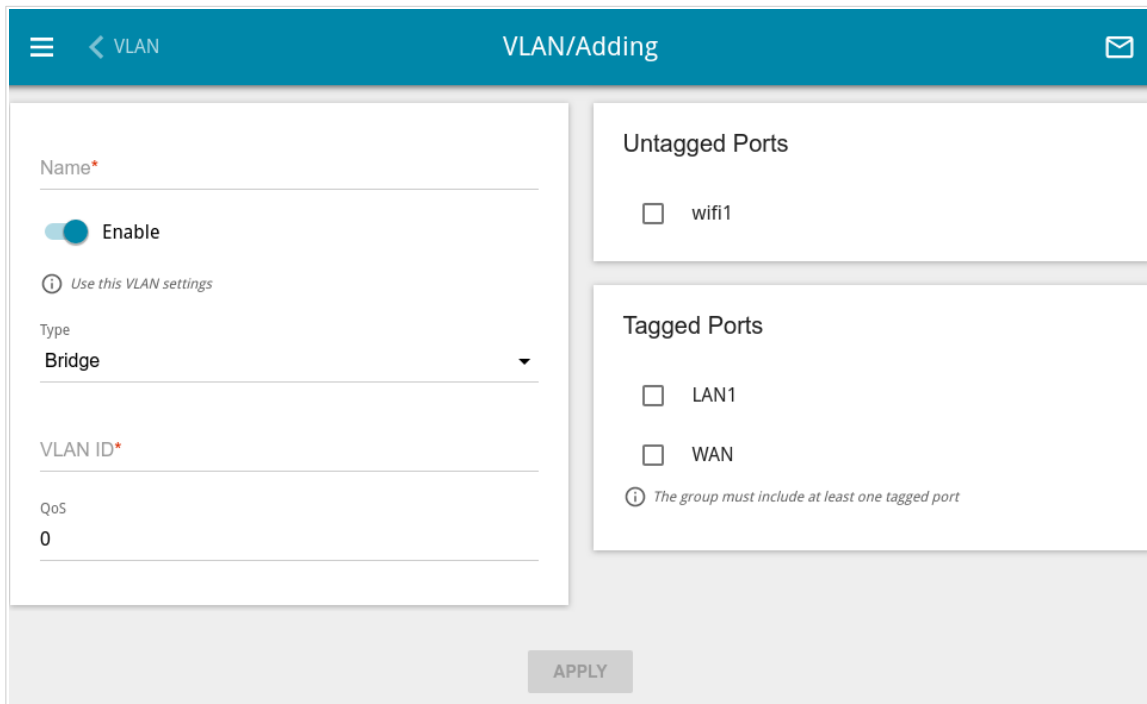


Figure 110. The page for adding a VLAN.


You can specify the following parameters:

Parameter	Description
<b>Name</b>	A name for the VLAN for easier identification.
<b>Enable</b>	Move the switch to the right to allow using this VLAN.
<b>Type</b>	<p>The type of the VLAN.</p> <ul style="list-style-type: none"> <li>• <b>Untagged NAT:</b> The VLAN of this type is an external connection with address translation. It is mostly used to transmit untagged traffic. When this value is selected, the <b>VLAN ID</b> field and the <b>Tagged Ports</b> section are not displayed. Only one VLAN of this type can exist in the system.</li> <li>• <b>Tagged NAT:</b> The VLAN of this type is an external connection with address translation. It is mostly used to connect to the Internet. Later the network which identifier is specified in the <b>VLAN ID</b> field is used as an interface to create a WAN connection (on the <b>Connections Setup / WAN</b> page). When this value is selected, the <b>Untagged Ports</b> section is not displayed.</li> <li>• <b>Bridge:</b> The VLAN of this type is a transparent connection between an internal port and an external connection. It is mostly used to connect IPTV set-top boxes.</li> </ul>

Parameter	Description
<b>VLAN ID</b>	An identifier of the VLAN.
<b>QoS</b>	A priority tag for the transmitted traffic.
<b>Untagged Ports</b>	The section includes the ports and Wi-Fi networks that can be added to the VLAN. To add an element, select the checkbox located to the left of it. To remove an element, deselect the checkbox located to the left of it.
<b>Tagged Ports</b>	Select an available value to assign it to this VLAN. To do this, select the checkbox located to the left of the relevant port.

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 (  ).

## 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 a DDNS service.

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.

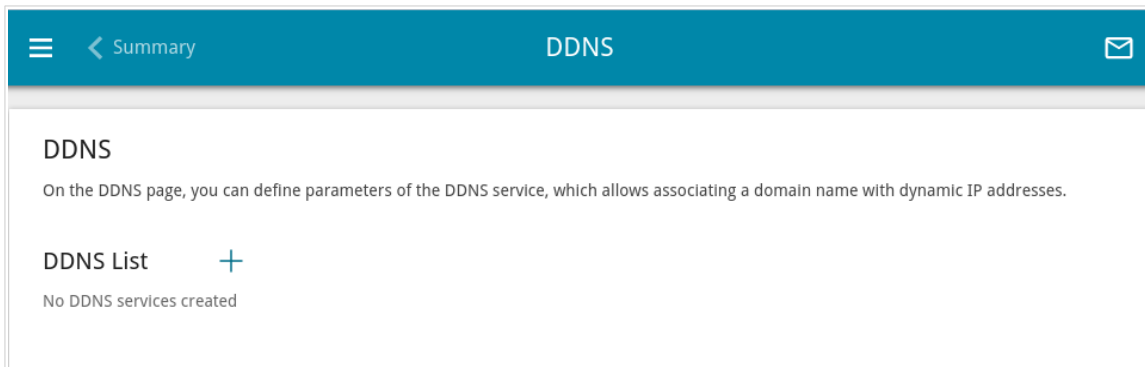


Figure 111. The **Advanced / DDNS** page.

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

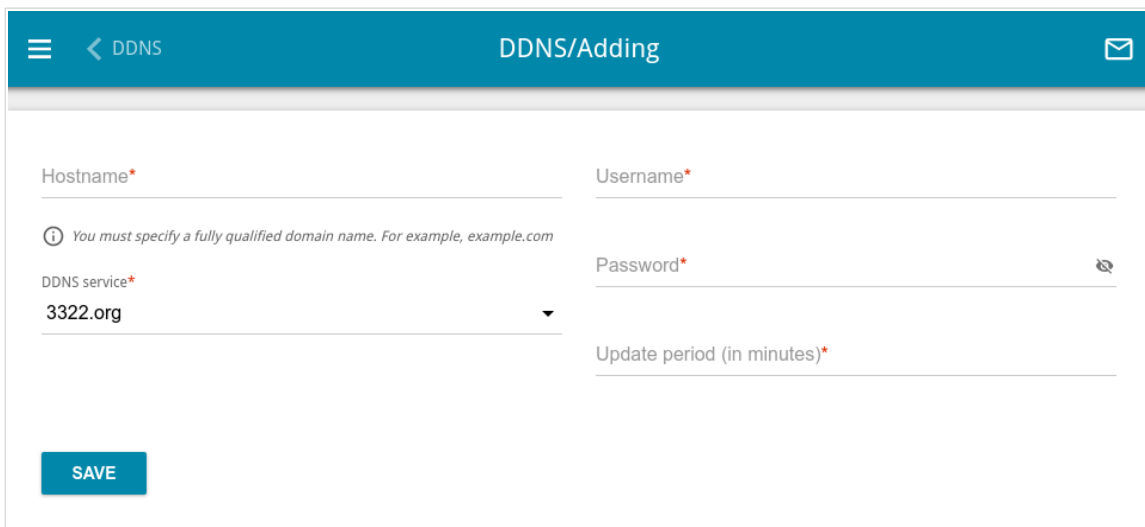



Figure 112. The page for configuring the access point to use a DDNS service.




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

Parameter	Description
<b>Hostname</b>	The full domain name registered at your DDNS provider.
<b>DDNS service</b>	Select a DDNS provider from the drop-down list.
<b>Username</b>	The username to authorize for your DDNS provider.
<b>Password</b>	The password to authorize for your DDNS provider. Click the <b>Show</b> icon (  ) to display the entered password.
<b>Update period</b>	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 edit parameters of the existing DDNS service, select the relevant line in the table. On the opened page, change the needed parameters and click the **SAVE** button.

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

## 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.

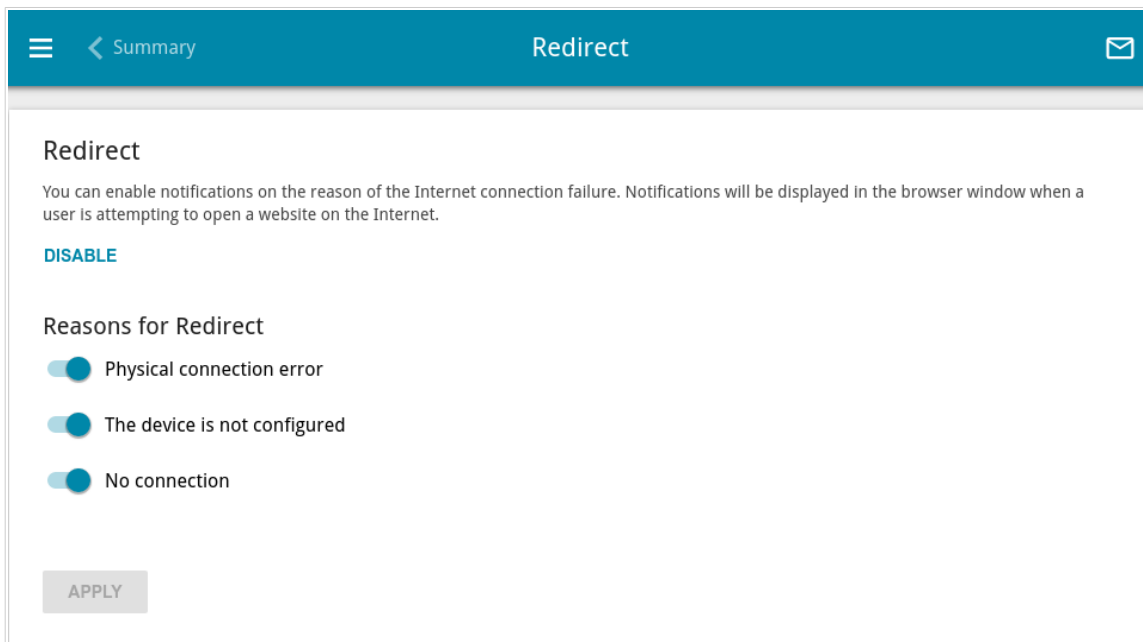


Figure 113. The **Advanced / Redirect** page.

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

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

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.

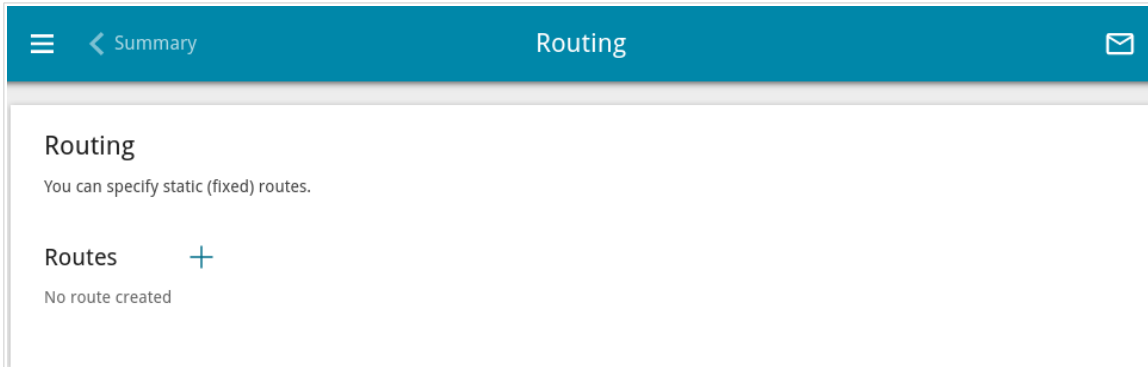


Figure 114. The **Advanced / Routing** page.

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

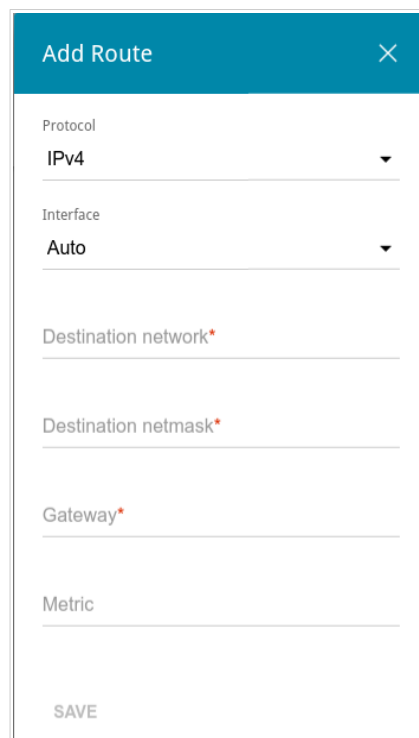
The screenshot shows a modal dialog box titled 'Add Route' with a close button (X) in the top right corner. The form contains several fields: 'Protocol' with a dropdown menu showing 'IPv4'; 'Interface' with a dropdown menu showing 'Auto'; 'Destination network\*' with a text input field; 'Destination netmask\*' with a text input field; 'Gateway\*' with a text input field; and 'Metric' with a text input field. At the bottom of the dialog is a 'SAVE' button.


Figure 115. The window for adding a new route.

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

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

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 116. The page for configuring the TR-069 client.

You can specify the following parameters:

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

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

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

## 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 function. The UPnP function allows to automatically create port forwarding rules for applications in the access point's LAN requiring a connection from an external network.

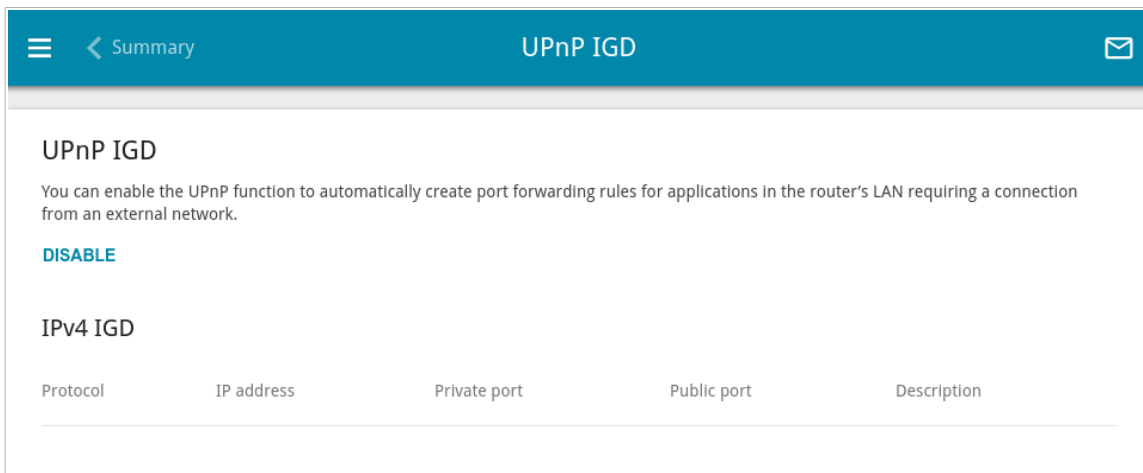


Figure 117. The **Advanced / UPnP IGD** page.

By default, the UPnP function is enabled. You can also manually add port forwarding rules for network applications on the **Firewall / Virtual Servers** page.

**!** Port forwarding rules will be automatically created only in case the access point's default WAN connection uses a public IP address.

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

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

If you want to disable the UPnP function, click the **DISABLE** button.

## 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 118. The **Advanced / UDPXY** page.

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

Upon that the following fields are displayed on the page:

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

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



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

**udpxy status:**

Server Process ID	Accepting clients on	Multicast address	Active clients
2599	192.168.0.50:4022	192.168.155.143	0

**Available HTTP requests:**

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

udpxy v. 1.0 (Build 23) standard - [Mon Mar 16 17:34:44 2020]  
udpxy and udpxrec are Copyright (C) 2008-2013 Pavel V. Cherenkov and licensed under GNU GPLv3

Figure 119. 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 120. The **Advanced / IGMP** page.

The following elements are available on the page:

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

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 enable the RTSP, SIP ALG mechanisms, and PPPoE/PPTP/L2TP/IPsec pass through functions.

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

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

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

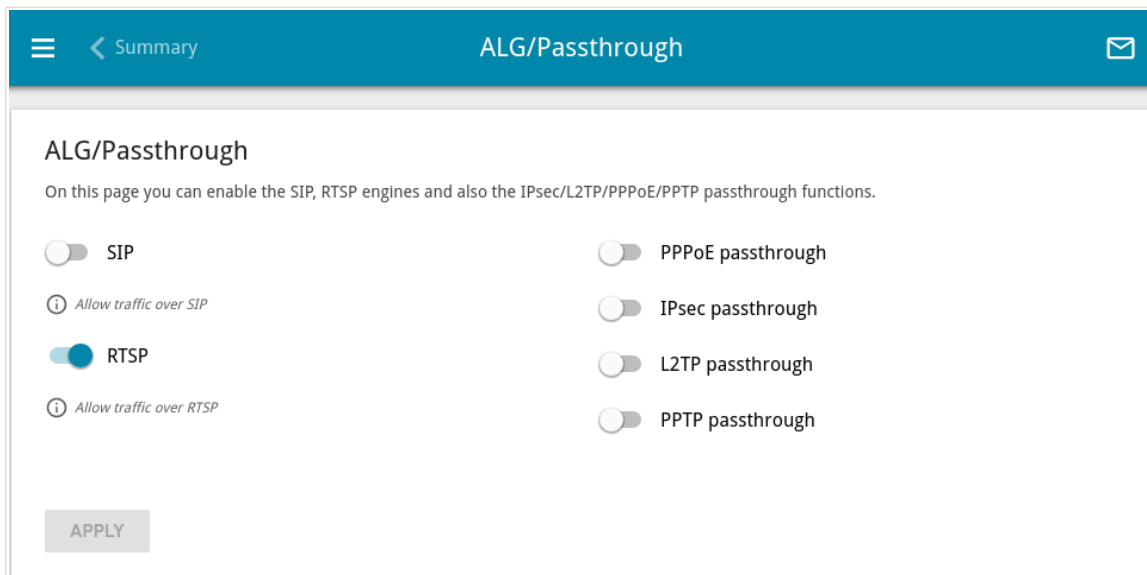


Figure 121. The **Advanced / ALG/Passthrough** page.

The following elements are available on the page:

Parameter	Description
<b>SIP</b>	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled access point. <sup>4</sup>
<b>RTSP</b>	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
<b>PPPoE pass through</b>	Move the switch to the right to enable the PPPoE pass through function.
<b>IPsec pass through</b>	Move the switch to the right to enable the IPsec pass through function.
<b>L2TP pass through</b>	Move the switch to the right to enable the L2TP pass through function.
<b>PPTP pass through</b>	Move the switch to the right to enable the PPTP pass through function.

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

---

4 On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / ALG/Passthrough** page, connect an Ethernet cable between a LAN port of the 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).

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

## IP Filter

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

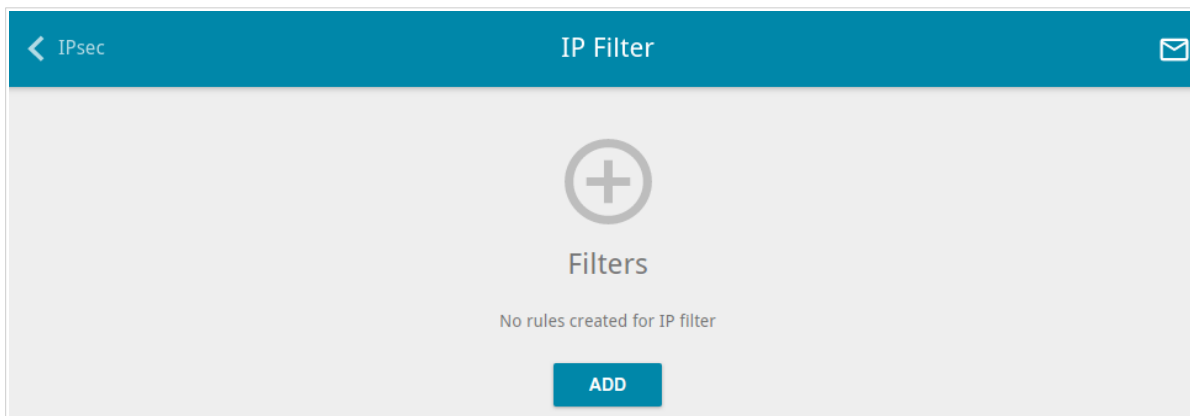


Figure 122. The **Firewall / IP Filter** page.

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

Figure 123. The page for adding a rule for IP filtering.

You can specify the following parameters:


Parameter	Description
<b>General Settings</b>	
<b>Enable rule</b>	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
<b>Name</b>	A name for the rule for easier identification. You can specify any name.
<b>Priority</b>	The priority level of the rule. In the field, enter the needed value. The lower the value, the higher is the priority of the rule. You can specify a value from <b>0</b> to <b>5000</b> .

Parameter	Description
<b>Action</b>	Select an action for the rule. <ul style="list-style-type: none"> <li>• <b>Allow</b>: Allows packet transmission in accordance with the criteria specified by the rule.</li> <li>• <b>Deny</b>: Denies packet transmission in accordance with the criteria specified by the rule.</li> </ul>
<b>Protocol</b>	A protocol for network packet transmission. Select a value from the drop-down list.
<b>IP version</b>	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
<b>Source IP address</b>	
<b>Set as</b>	Select the needed value from the drop-down list.
<b>Start IPv4 address / Start IPv6 address</b>	The source host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the <b>End IPv4 address / End IPv6 address</b> field blank. You can choose a device connected to the 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).
<b>End IPv4 address / End IPv6 address</b>	The source host end IPv4 or IPv6 address.
<b>Subnet IPv4 address / Subnet IPv6 address</b>	The source subnet IPv4 or IPv6 address. The field is displayed when the <b>Subnet</b> value is selected from the <b>Set as</b> drop-down list.
<b>Destination IP address</b>	
<b>Set as</b>	Select the needed value from the drop-down list.
<b>Start IPv4 address / Start IPv6 address</b>	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the <b>End IPv4 address / End IPv6 address</b> field blank. You can choose a device connected to the 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).
<b>End IPv4 address / End IPv6 address</b>	The destination host end IPv4 or IPv6 address.
<b>Subnet IPv4 address / Subnet IPv6 address</b>	The destination subnet IPv4 or IPv6 address. The field is displayed when the <b>Subnet</b> value is selected from the <b>Set as</b> drop-down list.

Parameter	Description
<b>Ports</b>	
<b>Destination port</b>	A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.
<b>Set source port manually</b>	Move the switch to the right to specify a port of the source IP address manually. Upon that the <b>Source port</b> field is displayed.
<b>Source port</b>	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

Click the **APPLY** button.

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

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



## Virtual Servers

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

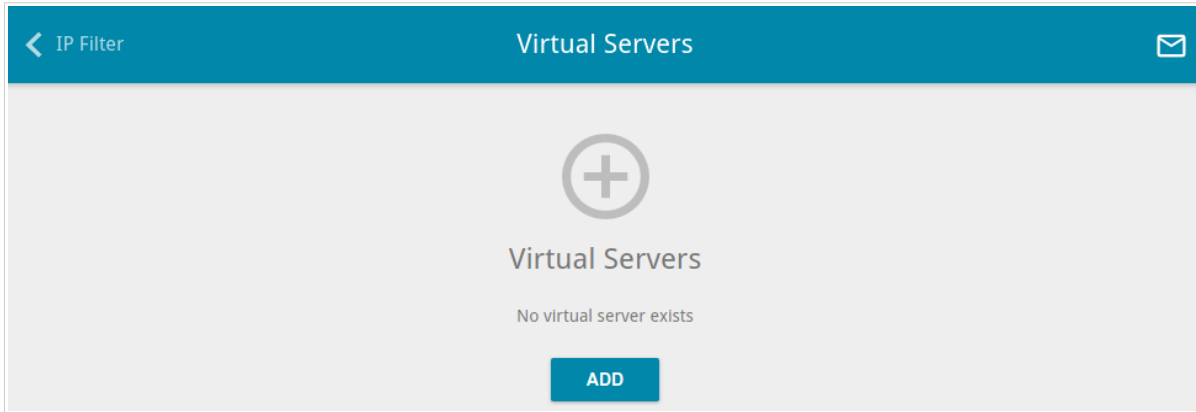


Figure 124. The **Firewall / Virtual Servers** page.

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

Figure 125. The page for adding a virtual server.


You can specify the following parameters:

Parameter	Description
<b>General Settings</b>	
<b>Name</b>	A name for the virtual server for easier identification. You can specify any name.
<b>Template</b>	Select a virtual server template from the drop-down list, or select <b>Custom</b> to specify all parameters of the new virtual server manually.
<b>Interface</b>	A WAN connection to which this virtual server will be assigned.
<b>Protocol</b>	A protocol that will be used by the new virtual server. Select a value from the drop-down list.

Parameter	Description
<b>NAT Loopback</b>	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).
<b>Public Network Settings</b>	
<b>Remote IP address</b>	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 <b>ADD REMOTE IP</b> button and enter the address in the displayed line. To remove the IP address, click the <b>Delete</b> icon (✕) in the line of the address.
<b>Public port</b>	A port of the access point from which traffic is directed to the IP address specified in the <b>Private IP</b> field in the <b>Private Network Settings</b> section. You can specify one port or several ports separated by a comma.
<b>Private Network Settings</b>	
<b>Private IP</b>	The IP address of the server from the local area network. To choose a device connected to the access point's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).
<b>Private port</b>	A port of the IP address specified in the <b>Private IP</b> field to which traffic is directed from the <b>Public port</b> . You can specify one port or several ports separated by a comma.

Click the **APPLY** button.

To 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 access point, 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.

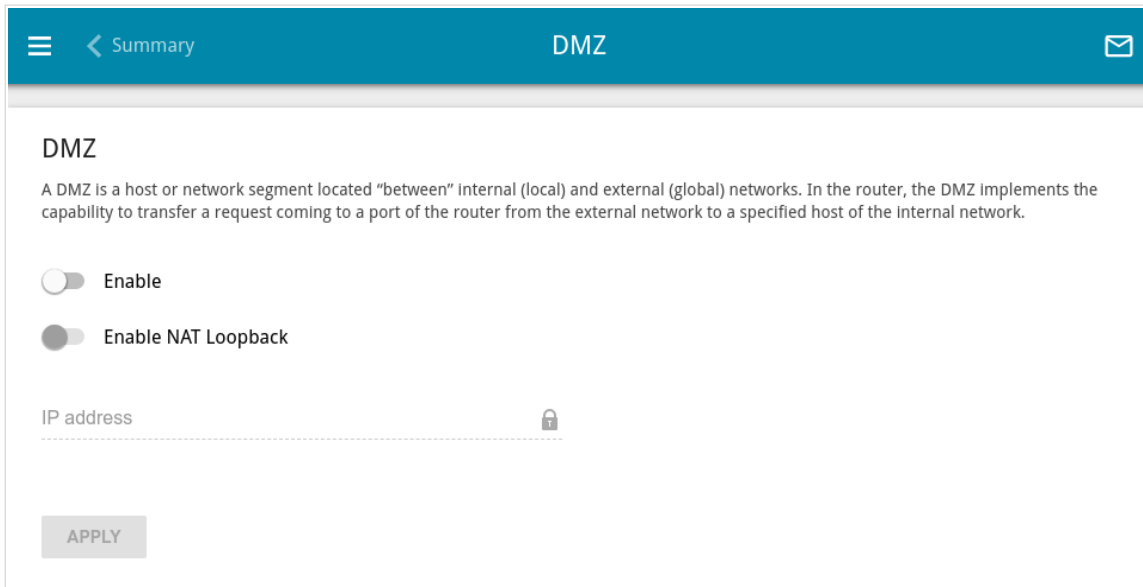


Figure 126. The **Firewall / DMZ** page.

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.

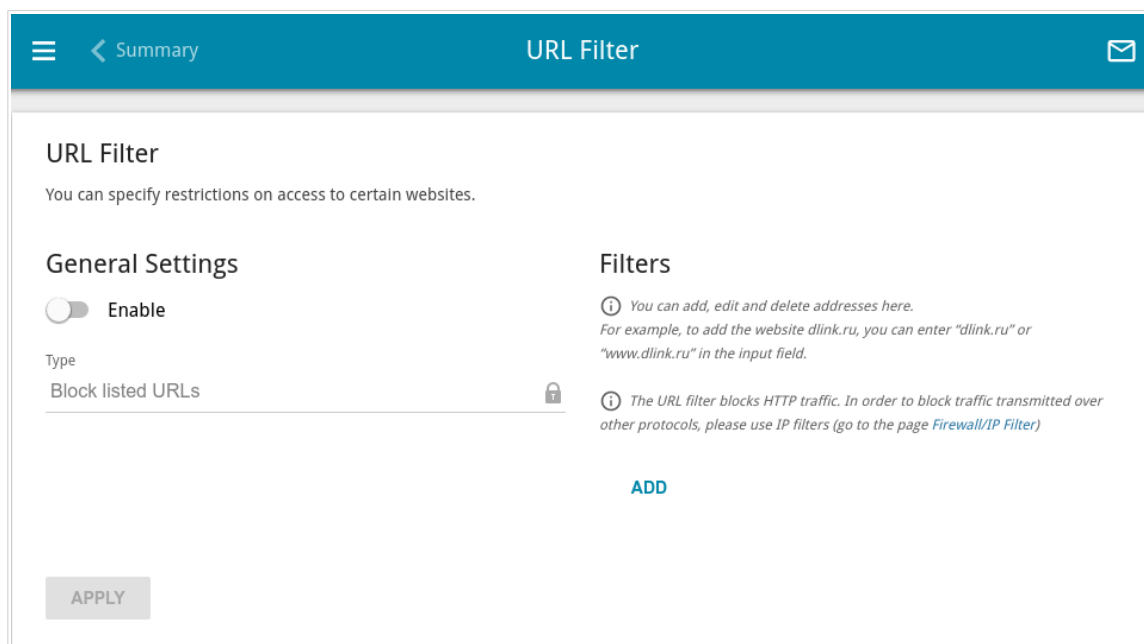


Figure 127. The **Firewall / URL Filter** page.

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

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

Click the **APPLY** button.

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

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

## Remote Access

On the **Firewall / 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.

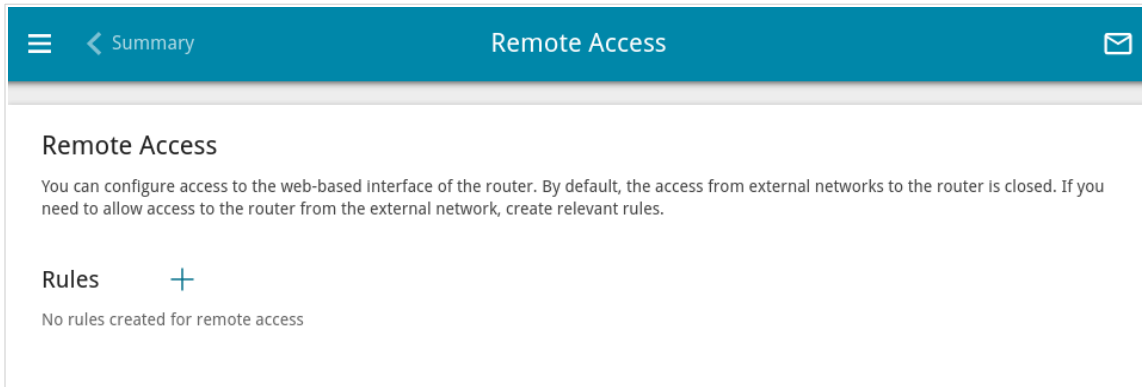


Figure 128. The **Advanced / Remote Access** page.

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

The screenshot shows the 'Add Rule' configuration window. It has a teal header with the title 'Add Rule' and a close icon. The form contains several fields: 'Name\*' (text input), 'Interface' (dropdown menu with 'Automatic' selected), 'IP version' (dropdown menu with 'IPv4' selected), a toggle switch for 'Open access from any external host' (currently off), 'IP address\*' (text input), 'Mask\*' (text input), 'Public port\*' (text input with '80' entered), and 'Protocol' (dropdown menu with 'HTTP' selected). At the bottom, there is a 'SAVE' button.


Figure 129. The window for adding a rule for remote management.

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

Parameter	Description
<b>Name</b>	A name for the rule for easier identification. You can specify any name.
<b>Interface</b>	From the drop-down list, select an interface (WAN connection) through which remote access to the access point will operate. Leave the <b>Automatic</b> value to allow remote access to operate through all created WAN connections.
<b>IP version</b>	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
<b>Open access from any external host</b>	Move the switch to the right to allow access to the access point for any host. Upon that the <b>IP address</b> and <b>Mask</b> fields are not displayed.
<b>IP address</b>	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.
<b>Mask</b>	<i>For the IPv4-based network only.</i> The mask of the subnet.
<b>Public port</b>	<i>For the IPv4-based network only.</i> An external port of the access point. You can specify only one port.
<b>Protocol</b>	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 (  ).

## 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 or configure automatic reboot on a schedule
- change the web-based interface language
- update the firmware of the access point
- configure automatic notification on new firmware version
- view the system log; configure sending the system log to a remote host
- check availability of a host on the Internet through the web-based interface of the access point
- trace the route to a host
- enable or disable access to the access point via TELNET
- configure automatic synchronization of the system time or manually configure the date and time for the access point.



## 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, 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, change the web-based interface language, or configure automatic reboot of the device on a schedule.

The screenshot shows the 'Configuration' page with a teal header. Below the header, there are three main sections: 'User', 'Miscellaneous', and 'Automatic Reboot'. The 'User' section includes fields for 'admin', 'New password', and 'Password confirmation', each with a 'Show' icon. A 'SAVE' button is below these fields. The 'Miscellaneous' section includes a 'Language' dropdown set to 'English' and an 'Idle time (in minutes)\*' field set to '10', with a 'SAVE' button below. The 'Automatic Reboot' section has a toggle switch for 'Enable' and a 'SAVE' button below. On the right side, there is an 'Action' column with five options: 'Factory' (Reset factory default settings), 'Backup' (Save current configuration to a file), 'Restore' (Load previously saved configuration to the device), 'Save' (Save current settings), and 'Reboot' (Reboot device).

Figure 130. The **System / Configuration** page.

In order to change the password for the administrator account, in the **User** section, enter a new password in the **New password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.<sup>5</sup> Click the **Show** icon (👁) to display the entered values. Then click the **SAVE** button.

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

**!** Remember or write down the new password for the administrator account. In case of losing the new password, you can access the settings of the 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, in the **Miscellaneous** section, select the needed value from the **Language** drop-down list.

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

The following buttons are available in the **Action** section:

Control	Description
<b>Factory</b>	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware <b>RESET</b> button (see the <i>Back Panel</i> section, page 11).
<b>Backup</b>	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.
<b>Restore</b>	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.
<b>Save</b>	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.
<b>Reboot</b>	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

To configure automatic reboot of the device on a schedule, in the **Automatic Reboot** section, move the **Enable** switch to the right and specify the time period for the device's reboot (in seconds) in the **Period** field. Click the **SAVE** button.

To disable automatic reboot of the device on a schedule, in the **Automatic Reboot** section, move the **Enable** switch to the left and 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.

**!** Update the firmware only when the access point is connected to your PC via a wired connection.

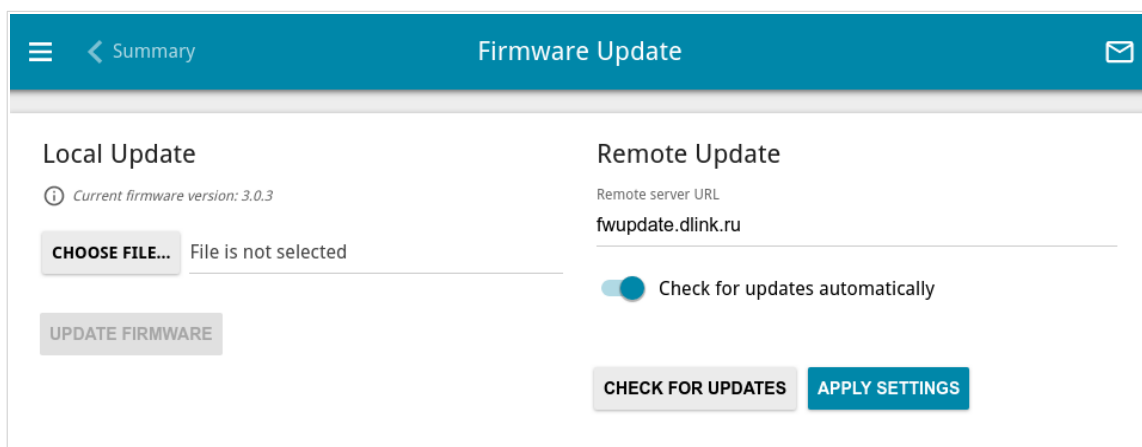


Figure 131. The **System / Firmware Update** page.

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

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

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

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

If after updating the firmware the 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.

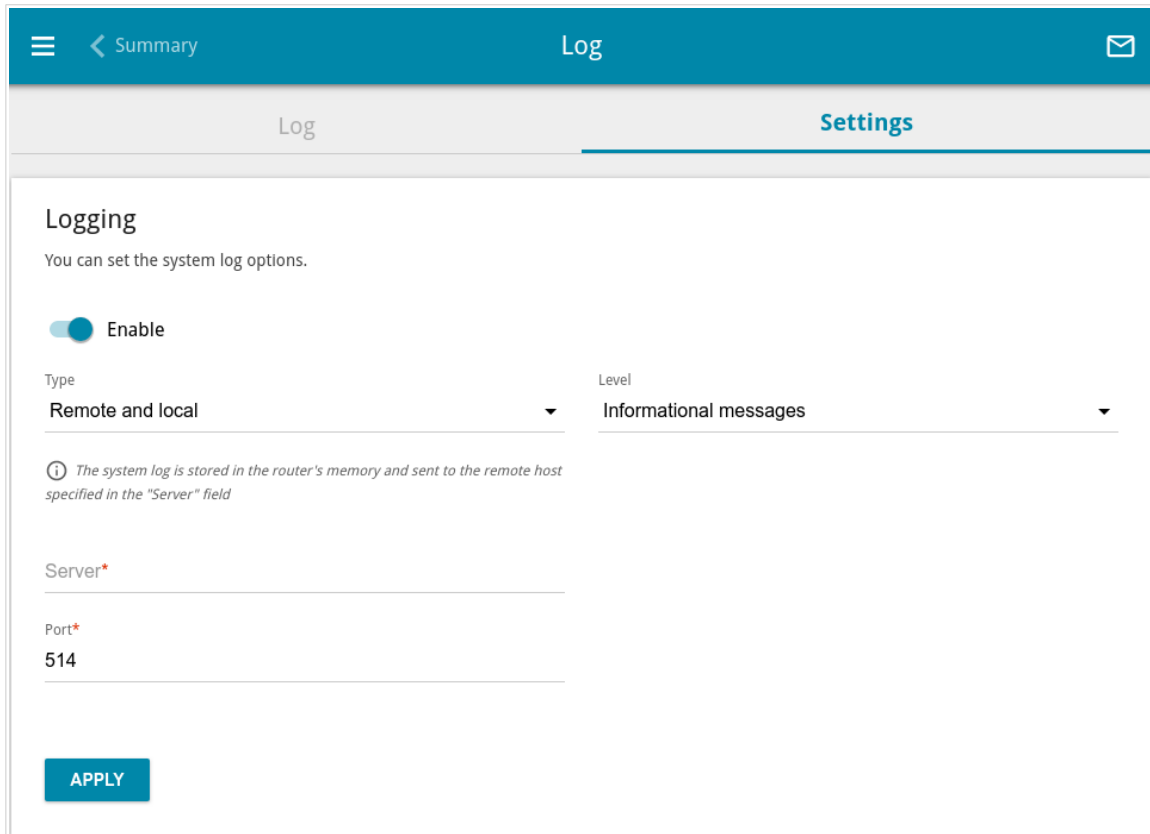
To update the firmware of the access point remotely, follow the next steps:

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.

## Log

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



The screenshot shows the 'Log' settings page in a web interface. The page has a teal header with a menu icon, a back arrow labeled 'Summary', the title 'Log', and an envelope icon. Below the header, there are two tabs: 'Log' and 'Settings', with 'Settings' being the active tab. The main content area is titled 'Logging' and contains the following elements:

- A sub-header 'Logging' followed by the text 'You can set the system log options.'
- An 'Enable' toggle switch that is currently turned on.
- Two dropdown menus: 'Type' set to 'Remote and local' and 'Level' set to 'Informational messages'.
- An information icon with the text: 'The system log is stored in the router's memory and sent to the remote host specified in the "Server" field'.
- A 'Server\*' text input field.
- A 'Port\*' text input field with the value '514'.
- An 'APPLY' button at the bottom left.

Figure 132. 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
<b>Logging</b>	
<b>Type</b>	Select a type of logging from the drop-down list. <ul style="list-style-type: none"> <li>• <b>Local:</b> The system log is stored in the access point's memory. When this value is selected, the <b>Server</b> and <b>Port</b> fields are not displayed.</li> <li>• <b>Remote:</b> The system log is sent to the remote host specified in the <b>Server</b> field.</li> <li>• <b>Remote and local:</b> The system log is stored in the access point's memory and sent to the remote host specified in the <b>Server</b> field.</li> </ul>
<b>Level</b>	Select a type of messages and alerts/notifications to be logged.
<b>Server</b>	The IP address or full domain name of the host from the local or global network, to which the system log will be sent.
<b>Port</b>	A port of the host specified in the <b>Server</b> field. By default, the value <b>514</b> is specified.

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

To 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.

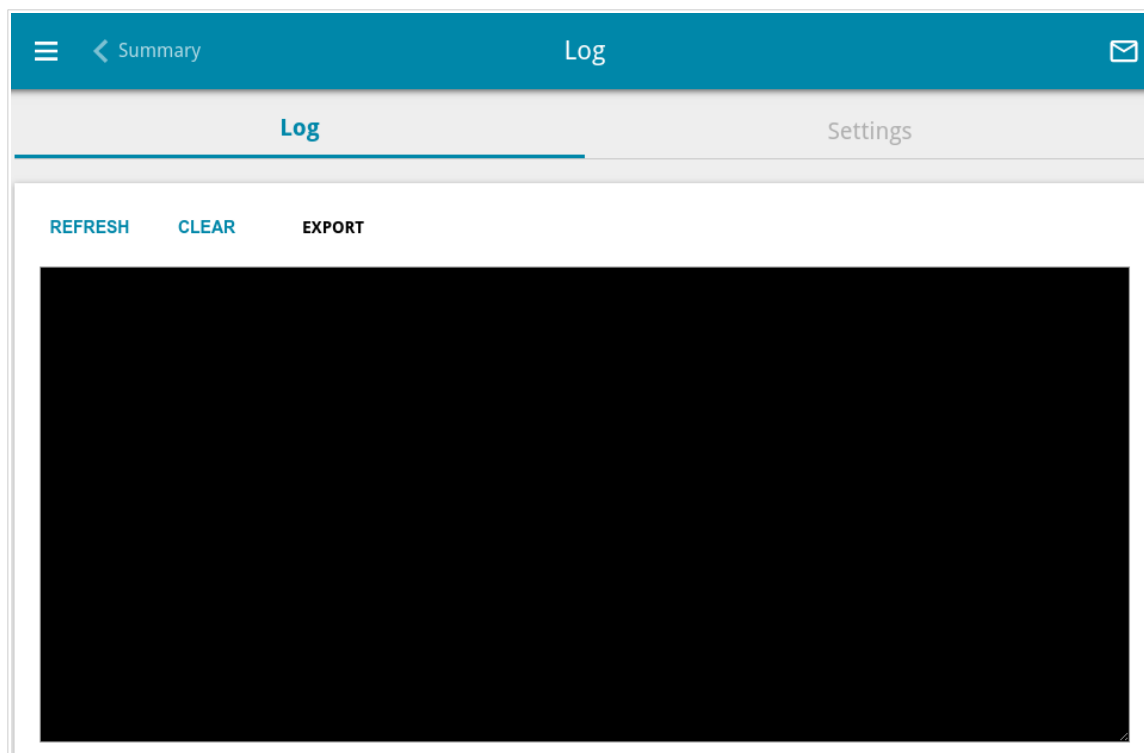


Figure 133. The **System / Log** page. The **Log** tab.

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.

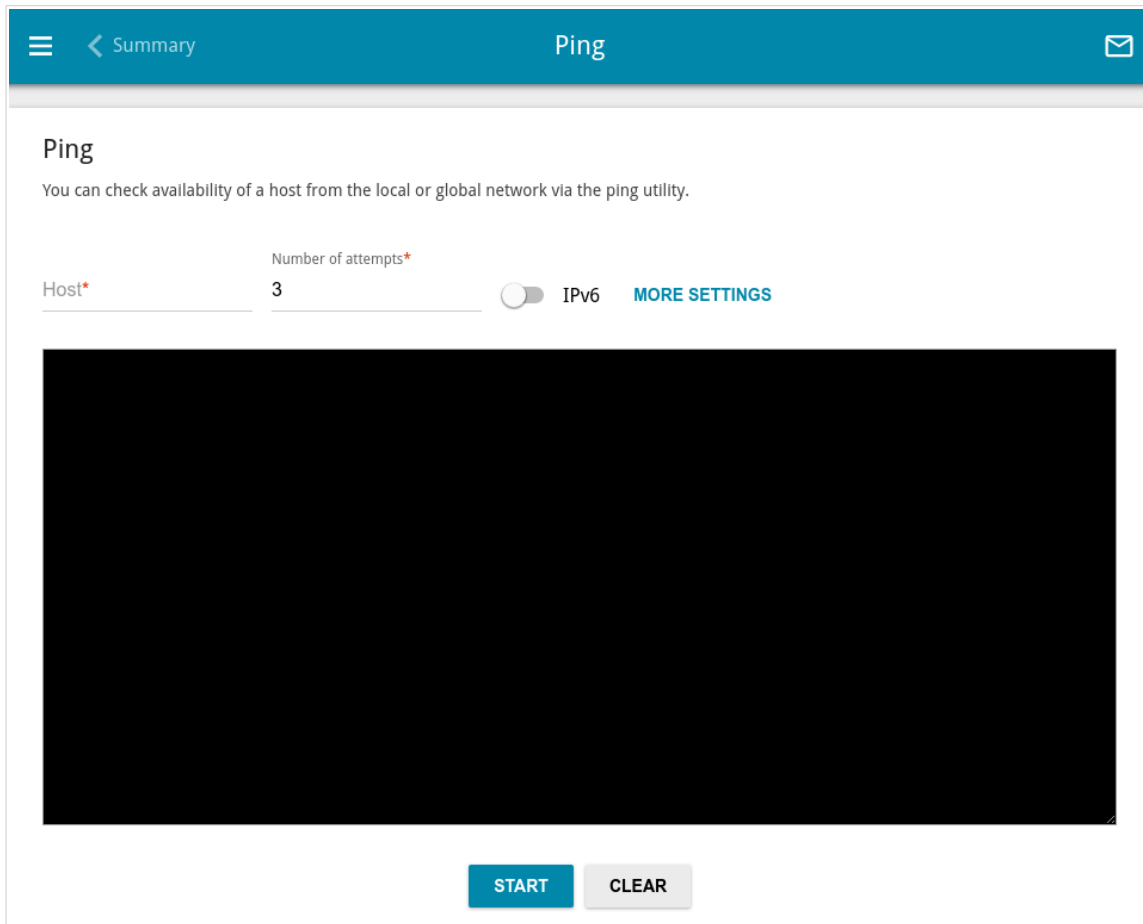


Figure 134. The **System / Ping** page.

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

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

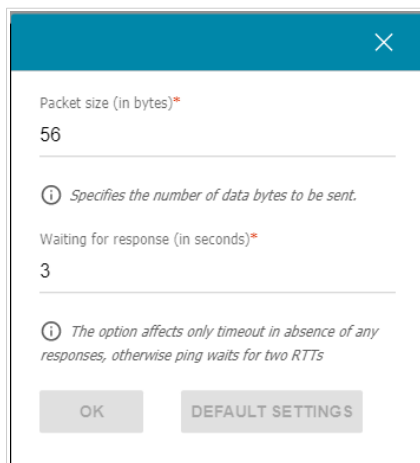


Figure 135. The **System / Ping** page. The additional settings window.

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

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

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

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

## Traceroute

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

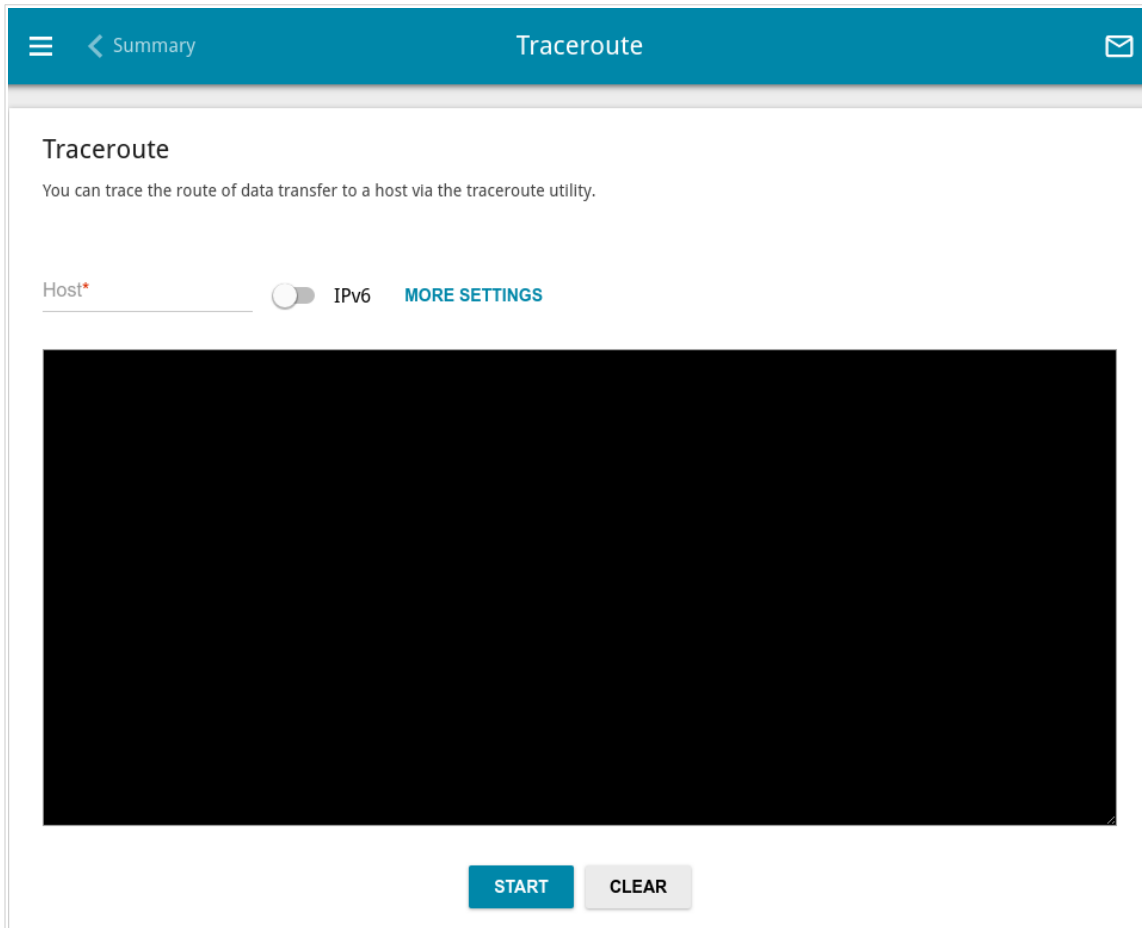


Figure 136. The **System / Traceroute** page.

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

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

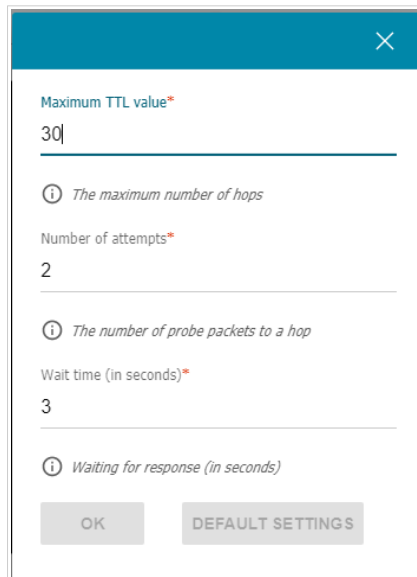


Figure 137. The **System / Traceroute** page. The additional settings window.

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

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

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

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

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

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

## Telnet

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

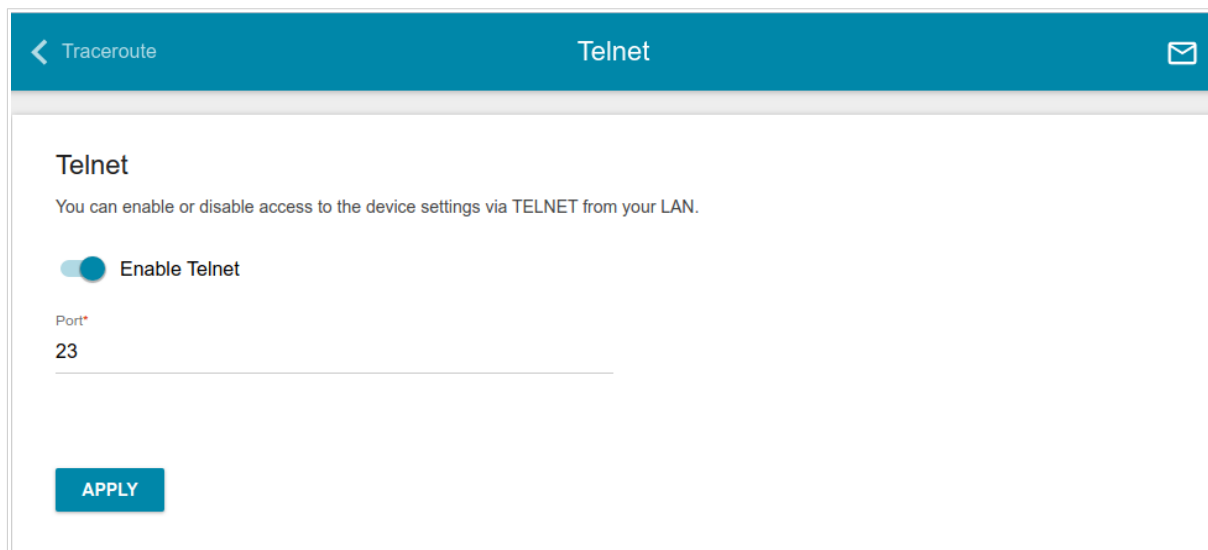


Figure 138. The **System / Telnet** page.

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

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

## System Time

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

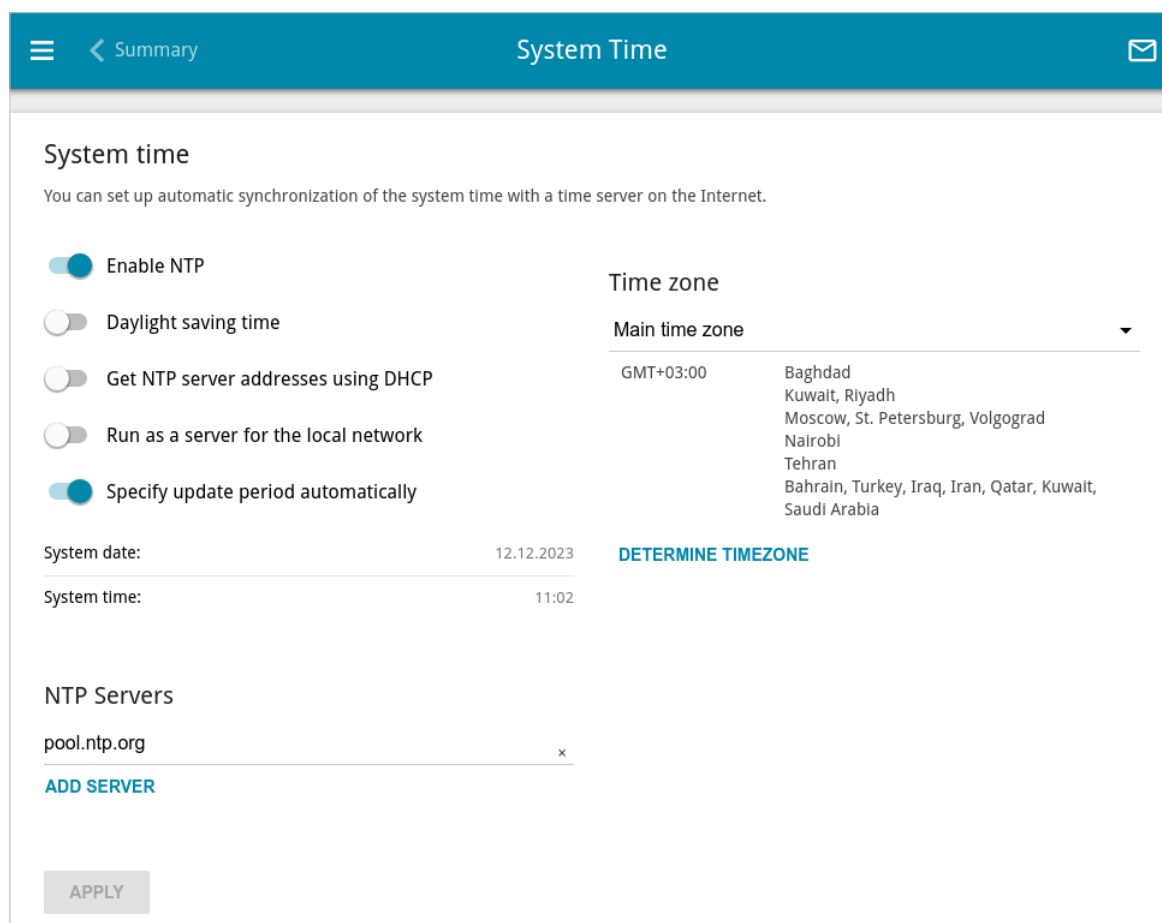


Figure 139. The **System / System Time** page.

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.

To enable the access point to automatically adjust to daylight saving time, move the **Daylight saving time** switch to the right. From the **Daylight saving time zone** drop-down list, select the time zone that will be used during summer time and specify the needed values in the **Beginning of daylight saving time** and **End of daylight saving time** sections. Click the **APPLY** button.

In some cases NTP servers addresses are provided by your ISP. In this case, you need to move the **Get NTP server addresses using DHCP** switch 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.

By default, the system is configured to automatically determine the system time synchronization interval. Upon that the **Specify update period automatically** switch is moved to the right. To configure the synchronization interval of the system time manually, move the **Specify update period automatically** switch to the left, and in the **Update period** field, specify the needed value (in minutes). 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).

## CHAPTER 5. OPERATION GUIDELINES

### ***Terms and Conditions for Installation, Safe Operation, Storage, Transportation, and Disposal***

Please carefully read this section before installation and connection of the device. Make sure that the device and cables are not damaged. The device should be used only as intended (reception/transmission of data in computer networks); installation should be performed in accordance with the documents available on the official website.

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

The power supply must correspond to the power options from the device specifications list. When a power adapter (not included in the delivery package) is used, the electrical outlet must be installed near the equipment and must be easily accessible.

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

The device may be stored and transported only in the original packaging at the temperature and humidity indicated in the specifications. No restrictions apply to sales. Please contact an authorized distributor to dispose of the equipment upon the end of its operation.

The service life of the device is 2 years.

The warranty period starts on the date of purchase from an authorized distributor within Russia or the CIS countries and extends for one year.

Irrespective of the date of purchase, the warranty period cannot exceed 2 years from the date of manufacture, which is determined by 6<sup>th</sup> (year) and 7<sup>th</sup> (month) digit in the serial number printed on the device label.

*Year: E – 2014, F – 2015, G – 2016, H – 2017, I – 2018, J – 2019, 0 – 2020, 1 – 2021, 2 – 2022, 3 – 2023.*

*Month: 1 – January, 2 – February, ..., 9 – September, A – October, B – November, C – December.*

If a fault is detected, please contact D-Link service center or technical support group.



## ***Wireless Installation Considerations***

The DAP-300P 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-300P 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

<b>3G</b>	Third Generation
<b>AC</b>	Access Category
<b>AES</b>	Advanced Encryption Standard
<b>AP</b>	Access Point
<b>ARP</b>	Address Resolution Protocol
<b>BPSK</b>	Binary Phase-shift Keying
<b>BSSID</b>	Basic Service Set Identifier
<b>CCK</b>	Complementary Code Keying
<b>CHAP</b>	Challenge Handshake Authentication Protocol
<b>CoS</b>	Class of Service
<b>DBSK</b>	Differential Binary Phase-shift Keying
<b>DDNS</b>	Dynamic Domain Name System
<b>DDoS</b>	Distributed Denial of Service
<b>DES</b>	Data Encryption Standard
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DMZ</b>	DeMilitarized Zone
<b>DNS</b>	Domain Name System
<b>DPD</b>	Dead Peer Detection
<b>DQPSK</b>	Differential Quadrature Phase-shift Keying
<b>DSL</b>	Digital Subscriber Line
<b>DSSS</b>	Direct-sequence Spread Spectrum
<b>DTIM</b>	Delivery Traffic Indication Message
<b>EoGRE</b>	Ethernet over Generic Routing Encapsulation
<b>GMT</b>	Greenwich Mean Time
<b>GRE</b>	Generic Routing Encapsulation
<b>GSM</b>	Global System for Mobile Communications

<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>ICMP</b>	Internet Control Message Protocol
<b>ID</b>	Identifier
<b>IGD</b>	Internet Gateway Device
<b>IGMP</b>	Internet Group Management Protocol
<b>IKE</b>	Internet Key Exchange
<b>IMEI</b>	International Mobile Equipment Identity
<b>IMSI</b>	International Mobile Subscriber Identity
<b>IP</b>	Internet Protocol
<b>IPTV</b>	Internet Protocol Television
<b>IPsec</b>	Internet Protocol Security
<b>ISP</b>	Internet Service Provider
<b>L2TP</b>	Layer 2 Tunneling Protocol
<b>LAN</b>	Local Area Network
<b>LCP</b>	Link Control Protocol
<b>LED</b>	Light-emitting diode
<b>LTE</b>	Long Term Evolution
<b>MAC</b>	Media Access Control
<b>MBSSID</b>	Multiple Basic Service Set Identifier
<b>MIB</b>	Management Information Base
<b>MIMO</b>	Multiple Input Multiple Output
<b>MPPE</b>	Microsoft Point-to-Point Encryption
<b>MPU</b>	Maximum Packet Unit
<b>MS-CHAP</b>	Microsoft Challenge Handshake Authentication Protocol
<b>MTU</b>	Maximum Transmission Unit
<b>NAT</b>	Network Address Translation
<b>NIC</b>	Network Interface Controller

<b>NTP</b>	Network Time Protocol
<b>OFDM</b>	Orthogonal Frequency Division Multiplexing
<b>PAP</b>	Password Authentication Protocol
<b>PBC</b>	Push Button Configuration
<b>PCP</b>	Port Control Protocol
<b>PFS</b>	Perfect Forward Secrecy
<b>PIN</b>	Personal Identification Number
<b>PMP</b>	Port Mapping Protocol
<b>PoE</b>	Power over Ethernet
<b>PPP</b>	Point-to-Point Protocol
<b>pppd</b>	Point-to-Point Protocol Daemon
<b>PPPoE</b>	Point-to-point protocol over Ethernet
<b>PPTP</b>	Point-to-point tunneling protocol
<b>PSK</b>	Pre-shared key
<b>PUK</b>	PIN Unlock Key
<b>QAM</b>	Quadrature Amplitude Modulation
<b>QoS</b>	Quality of Service
<b>QPSK</b>	Quadrature Phase-shift Keying
<b>RADIUS</b>	Remote Authentication in Dial-In User Service
<b>RIP</b>	Routing Information Protocol
<b>RIPng</b>	Next Generation Routing Information Protocol
<b>RTS</b>	Request To Send
<b>RTSP</b>	Real Time Streaming Protocol
<b>SA</b>	Security Association
<b>SAE</b>	Simultaneous Authentication of Equals
<b>SIM</b>	Subscriber Identification Module
<b>SIP</b>	Session Initiation Protocol
<b>SMB</b>	Server Message Block

<b>SNMP</b>	Simple Network Management Protocol
<b>SSH</b>	Secure Shell
<b>SSID</b>	Service Set Identifier
<b>STBC</b>	Space-time block coding
<b>TCP</b>	Transmission Control Protocol
<b>TKIP</b>	Temporal Key Integrity Protocol
<b>TLS</b>	Transport Layer Security
<b>ToS</b>	Type of Service
<b>UAM</b>	Universal Access Method
<b>UDP</b>	User Datagram Protocol
<b>UPnP</b>	Universal Plug and Play
<b>URL</b>	Uniform Resource Locator
<b>USB</b>	Universal Serial Bus
<b>VLAN</b>	Virtual Local Area Network
<b>VPN</b>	Virtual Private Network
<b>VRID</b>	Virtual Router Identifier
<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>WAN</b>	Wide Area Network
<b>WEP</b>	Wired Equivalent Privacy
<b>Wi-Fi</b>	Wireless Fidelity
<b>WISP</b>	Wireless Internet Service Provider
<b>WLAN</b>	Wireless Local Area Network
<b>WMM</b>	Wi-Fi Multimedia
<b>WPA</b>	Wi-Fi Protected Access
<b>WPS</b>	Wi-Fi Protected Setup