



DAP-1360U

Wireless N300 Access Point & Router

Contents

Chapter 1. Introduction	4
Contents and Audience	4
Conventions	4
Document Structure	4
Chapter 2. Overview	5
General Information	5
Specifications	6
Product Appearance	9
Top Panel	9
Back and Bottom Panels	10
Delivery Package	11
Chapter 3. Installation and Connection	12
Before You Begin	12
Connecting to PC	13
PC with Ethernet Adapter	13
Configuring IP Address in OS Windows 7	14
PC with Wi-Fi Adapter	19
Configuring Wi-Fi Adapter in OS Windows 7	20
Connecting to Web-based Interface	23
Web-based Interface Structure	25
Summary Page	25
Home Page	27
Menu Sections	28
Notifications	29
Chapter 4. Configuring via Web-based Interface	30
Initial Configuration Wizard	30
Selecting Operation Mode	32
Configuring WDS Function	35
Changing LAN IPv4 Address	36
Wi-Fi Client	37
Configuring WAN Connection	39
<i>Static IPv4 Connection</i>	40
<i>PPPoE or PPPoE + Dynamic IP (PPPoE Dual Access) Connections</i>	41
<i>PPPoE + Static IP (PPPoE Dual Access) Connection</i>	42
<i>PPTP + Dynamic IP or L2TP + Dynamic IP Connection</i>	43
<i>PPTP + Static IP or L2TP + Static IP Connection</i>	44
Configuring Wireless Network	45
Configuring LAN Ports for IPTV/VoIP	47
Changing Web-based Interface Password	49
Connection of Multimedia Devices	51
Statistics	54
Network Statistics	54
DHCP	55
Routing Table	56
Clients and Session	57
Port Statistics	58
Multicast Groups	59

Connections Setup	60
WAN.....	60
<i>Creating Dynamic IPv4 or Static IPv4 WAN Connection</i>	62
<i>Creating PPPoE WAN Connection</i>	66
<i>Creating PPTP or L2TP WAN Connection</i>	71
LAN.....	75
Wi-Fi	79
Basic Settings.....	79
Client Management.....	87
WPS.....	88
<i>Using WPS Function via Web-based Interface</i>	90
<i>Using WPS Function without Web-based Interface</i>	91
WDS.....	92
WMM.....	94
Client.....	97
Client Shaping.....	100
Additional.....	102
MAC Filter.....	105
Roaming.....	107
Advanced	109
VLAN.....	110
DNS.....	112
DDNS.....	114
Ports Settings.....	116
Bandwidth Control.....	119
Routing.....	120
Remote Access.....	122
UPnP IGD.....	124
IGMP.....	125
ALG/Passthrough.....	126
Firewall	128
IP Filter.....	128
Virtual Servers.....	132
DMZ.....	135
MAC Filter.....	136
URL Filter.....	138
System	140
Configuration.....	141
Firmware Update.....	143
<i>Local Update</i>	144
<i>Remote Update</i>	145
Log.....	146
Ping.....	148
Traceroute.....	150
Telnet.....	152
System Time.....	153
Chapter 5. Operation Guidelines	155
Safety Rules and Conditions	155
Wireless Installation Considerations	156
Chapter 6. Abbreviations and Acronyms	157


CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the access point DAP-1360U and explains how to configure and operate it.

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

Conventions

Example	Description
text	The body text of the manual.
<i>Before You Begin</i>	A reference to a chapter or section of this manual.
<i>“Quick Installation Guide”</i>	A reference to a document.
Change	A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.).
192.168.0.51	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-1360U and configure a PC in order to access its web-based interface.

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

Chapter 5 includes safety instructions and tips for networking.

Chapter 6 introduces abbreviations and acronyms used in this manual.

CHAPTER 2. OVERVIEW

General Information

The DAP-1360U 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.

You are able to connect the wireless access point DAP-1360U switched to the router mode 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.

Using DAP-1360U, you are able to quickly create a wireless network and let your relatives or employees connect to 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, WDS, WMM.

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

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

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

In the router mode, the DAP-1360U device includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

You can configure the settings of the DAP-1360U device via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

The configuration wizard allows you to connect DAP-1360U 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).

Also DAP-1360U supports configuration and management via mobile application for Android and iPhone smartphones.

Now you can simply update the firmware: the access point itself finds approved firmware on D-Link update server and notifies when ready to install it.

Specifications*

Hardware	
Processor	<ul style="list-style-type: none"> RTL8196D (620MHz)
RAM	<ul style="list-style-type: none"> 32MB, SDRAM
Flash	<ul style="list-style-type: none"> 4MB, SPI
Interfaces	<ul style="list-style-type: none"> 10/100BASE-TX WAN port 4 10/100BASE-TX LAN ports
LEDs	<ul style="list-style-type: none"> POWER WLAN WPS INTERNET 4 LAN LEDS
Buttons	<ul style="list-style-type: none"> ON/OFF button to power on/power off RESET button to restore factory default settings WPS button to set up wireless connection and enable/disable wireless network
Antenna	<ul style="list-style-type: none"> Two detachable omnidirectional antennas (5dBi gain) RP-SMA connector
Power connector	<ul style="list-style-type: none"> Power input connector (DC)

Software	
WAN connection types	<ul style="list-style-type: none"> PPPoE Static IPv4 / Dynamic IPv4 PPPoE + Static IP (PPPoE Dual Access) PPPoE + Dynamic IP (PPPoE Dual Access) PPTP/L2TP PPTP/L2TP + Static IP PPTP/L2TP + Dynamic IP
Network functions	<ul style="list-style-type: none"> DHCP server/relay Automatic obtainment of LAN IP address (for access point/repeater/client/WDS modes) DNS relay Dynamic DNS Static IP routing IGMP Proxy RIP Support of UPnP IGD Support of VLAN WAN ping respond Support of SIP ALG Support of RTSP Autonegotiation of speed, duplex mode, and flow control/Manual speed and duplex mode setup for each Ethernet port Setup of maximum TX rate for each port of the access point
Firewall functions	<ul style="list-style-type: none"> Network Address Translation (NAT) Stateful Packet Inspection (SPI) IP filter MAC filter URL filter DMZ Prevention of ARP and DDoS attacks Virtual servers
VPN	<ul style="list-style-type: none"> IPsec/PPTP/L2TP/PPPoE pass-through

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

Software	
Management	<ul style="list-style-type: none"> · Local and remote access to settings through TELNET/WEB (HTTP/HTTPS) · Bilingual web-based interface for configuration and management (Russian/English) · Support of D-Link Assistant application for Android and iPhone smartphones · Firmware update via web-based interface · Automatic notification on new firmware version · Saving/restoring configuration to/from file · Support of logging to remote host · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility

Wireless Module Parameters	
Standards	<ul style="list-style-type: none"> · IEEE 802.11b/g/n
Frequency range	<ul style="list-style-type: none"> · 2400 ~ 2483.5MHz
Wireless connection security	<ul style="list-style-type: none"> · WEP · WPA/WPA2 (Personal/Enterprise) · MAC filter · WPS (PBC/PIN)
Advanced functions	<ul style="list-style-type: none"> · Support of client mode · WMM (Wi-Fi QoS) · Information on connected Wi-Fi clients · Advanced settings · Smart adjustment of Wi-Fi clients · Guest Wi-Fi / support of MBSSID · Rate limitation for wireless network/separate MAC addresses · Periodic scan of channels, automatic switch to least loaded channel · WDS · Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence)
Wireless connection rate	<ul style="list-style-type: none"> · IEEE 802.11b: 1, 2, 5.5, and 11Mbps · IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps · IEEE 802.11n: from 6.5 to 300Mbps (from MCS0 to MCS15)
Transmitter output power <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"> · 802.11b (typical at room temperature 25 °C) 15dBm (+/-1.5dB) at 1, 2, 5.5, 11Mbps · 802.11g (typical at room temperature 25 °C) 15dBm (+/-1.5dB) at 6, 9, 12, 18, 24, 36, 48, 54Mbps · 802.11n (typical at room temperature 25 °C) HT20 15dBm (+/-1.5dB) at MCS0/1/2/3/4/5/6/8/9/10/11/12/13/14 14dBm (+/-1.5dB) at MCS7/15 HT40 15dBm (+/-1.5dB) at MCS0/1/2/3/4/5/6/8/9/10/11/12/13/14 14dBm (+/-1.5dB) at MCS7/15

Wireless Module Parameters	
Receiver sensitivity	<ul style="list-style-type: none"> · 802.11b (typical at PER = 8% at room temperature 25 °C) <ul style="list-style-type: none"> -82dBm at 1Mbps -80dBm at 2Mbps -78dBm at 5.5Mbps -76dBm at 11Mbps · 802.11g (typical at PER = 10% at room temperature 25 °C) <ul style="list-style-type: none"> -85dBm at 6Mbps -84dBm at 9Mbps -82dBm at 12Mbps -80dBm at 18Mbps -77dBm at 24Mbps -73dBm at 36Mbps -69dBm at 48Mbps -68dBm at 54Mbps · 802.11n (typical at PER = 10% at room temperature 25 °C) <ul style="list-style-type: none"> HT20 <ul style="list-style-type: none"> -82dBm at MCS0/8 -79dBm at MCS1/9 -77dBm at MCS2/10 -74dBm at MCS3/11 -70dBm at MCS4/12 -66dBm at MCS5/13 -65dBm at MCS6/14 -64dBm at MCS7/15 HT40 <ul style="list-style-type: none"> -79dBm at MCS0/8 -76dBm at MCS1/9 -74dBm at MCS2/10 -71dBm at MCS3/11 -67dBm at MCS4/12 -63dBm at MCS5/13 -62dBm at MCS6/14 -61dBm at MCS7/15
Modulation schemes	<ul style="list-style-type: none"> · 802.11b: DQPSK, DBPSK, DSSS, CCK · 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM · 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM

Physical Parameters	
Dimensions	· 174 x 115 x 30 mm (7 x 4.5 x 1.2 in)
Weight	· 248 g (0.55 lb)

Operating Environment	
Power	· Output: 12V DC, 0.5A
Temperature	<ul style="list-style-type: none"> · Operating: from 0 to 40 °C · Storage: from -20 to 65 °C
Humidity	<ul style="list-style-type: none"> · Operating: from 10% to 90% (non-condensing) · Storage: from 5% to 95% (non-condensing)

Product Appearance

Top Panel



Figure 1. Top panel view.

LED	Mode	Description
POWER	<i>Solid green</i>	The device is powered on.
	<i>No light</i>	The device is powered off.
WLAN	<i>Solid green</i>	The device's WLAN is on.
	<i>Blinking green</i>	Data transfer through the Wi-Fi network.
	<i>No light</i>	The device's WLAN is off.
WPS	<i>Blinking green</i>	Attempting to add a wireless device via the WPS function.
	<i>No light</i>	The WPS function is not in use.
INTERNET	<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.
LAN 1-4	<i>Solid green</i>	A device (computer) is connected to the relevant port, the connection is on.
	<i>Blinking green</i>	Data transfer through the relevant LAN port. When the access point is being loaded, the LEDs are blinking one at a time. When the firmware is being upgraded, the LEDs are blinking two at a time.
	<i>No light</i>	The cable is not connected to the relevant port.

Back and Bottom Panels

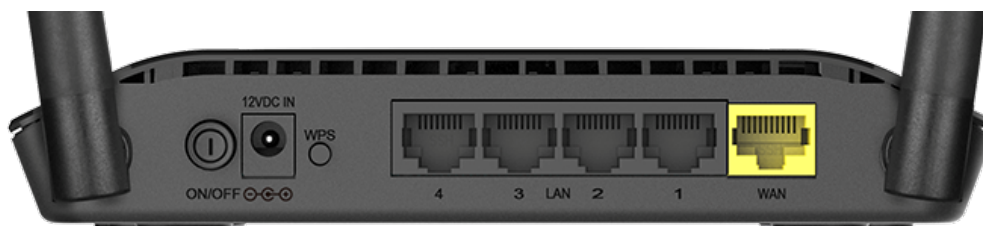


Figure 2. Back panel view.

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

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

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

Delivery Package

The following should be included:

- Access point DAP-1360U
- Power adapter DC 12V/0.5A
- Ethernet cable
- Two detachable antennas
- “***Quick Installation Guide***” (brochure).

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



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

CHAPTER 3. INSTALLATION AND CONNECTION

Before You Begin

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

Operating System

Configuration of the access point DAP-1360U 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.

Web Browser

The following web browsers are recommended:

- Apple Safari 8 and later
- Google Chrome 48 and later
- Microsoft Internet Explorer 10 and later
- Microsoft Edge 20.10240 and later
- Mozilla Firefox 44 and later
- Opera 35 and later.

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

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

Any computer that uses the 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 PC

PC with Ethernet Adapter

1. Connect an Ethernet cable between any of LAN ports located on the back panel of the access point and the Ethernet port of your PC.
2. Connect the power cord 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.
3. Turn on the access point by pressing the **ON/OFF** button on its back panel.

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.)

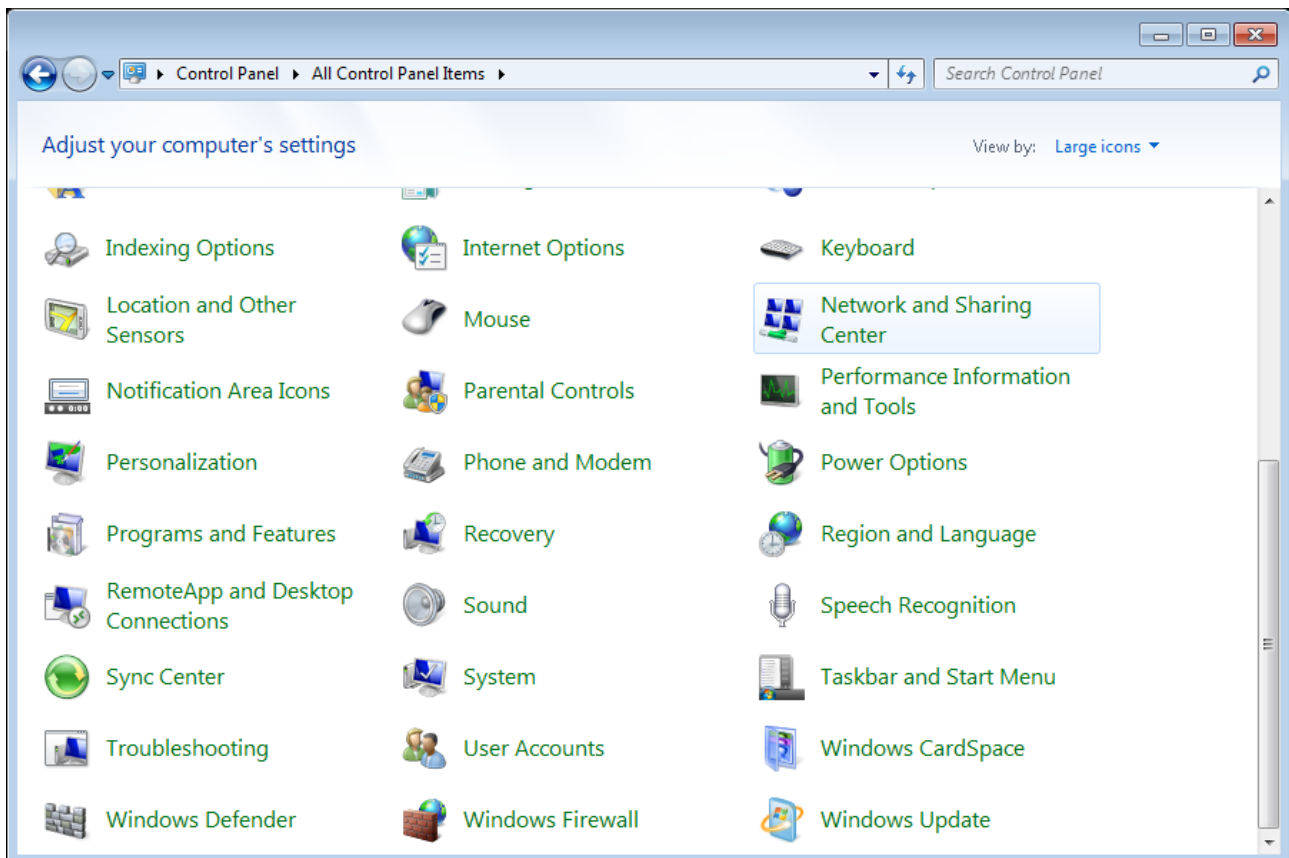


Figure 3. The **Control Panel** window.

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

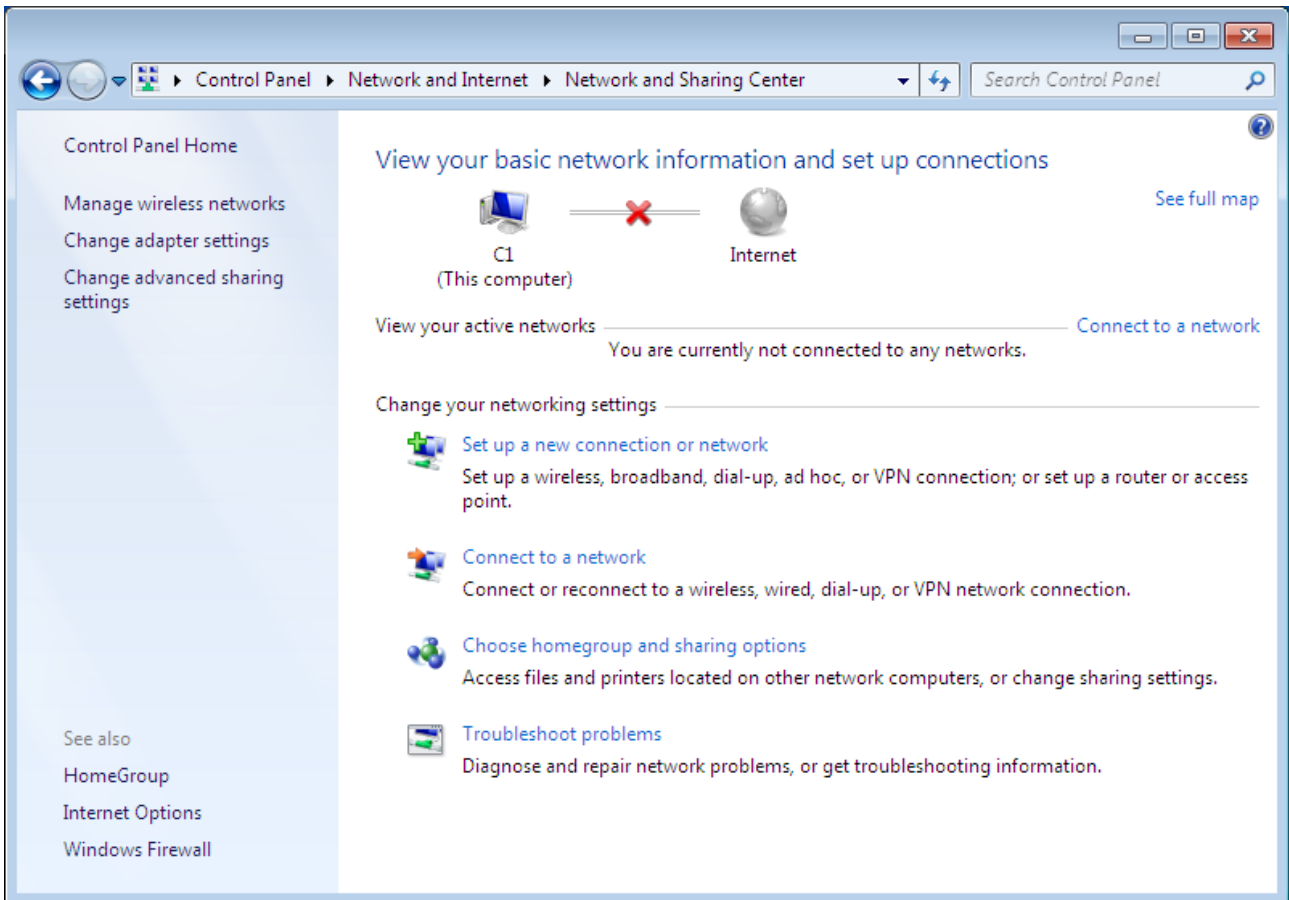


Figure 4. The **Network and Sharing Center** window.

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

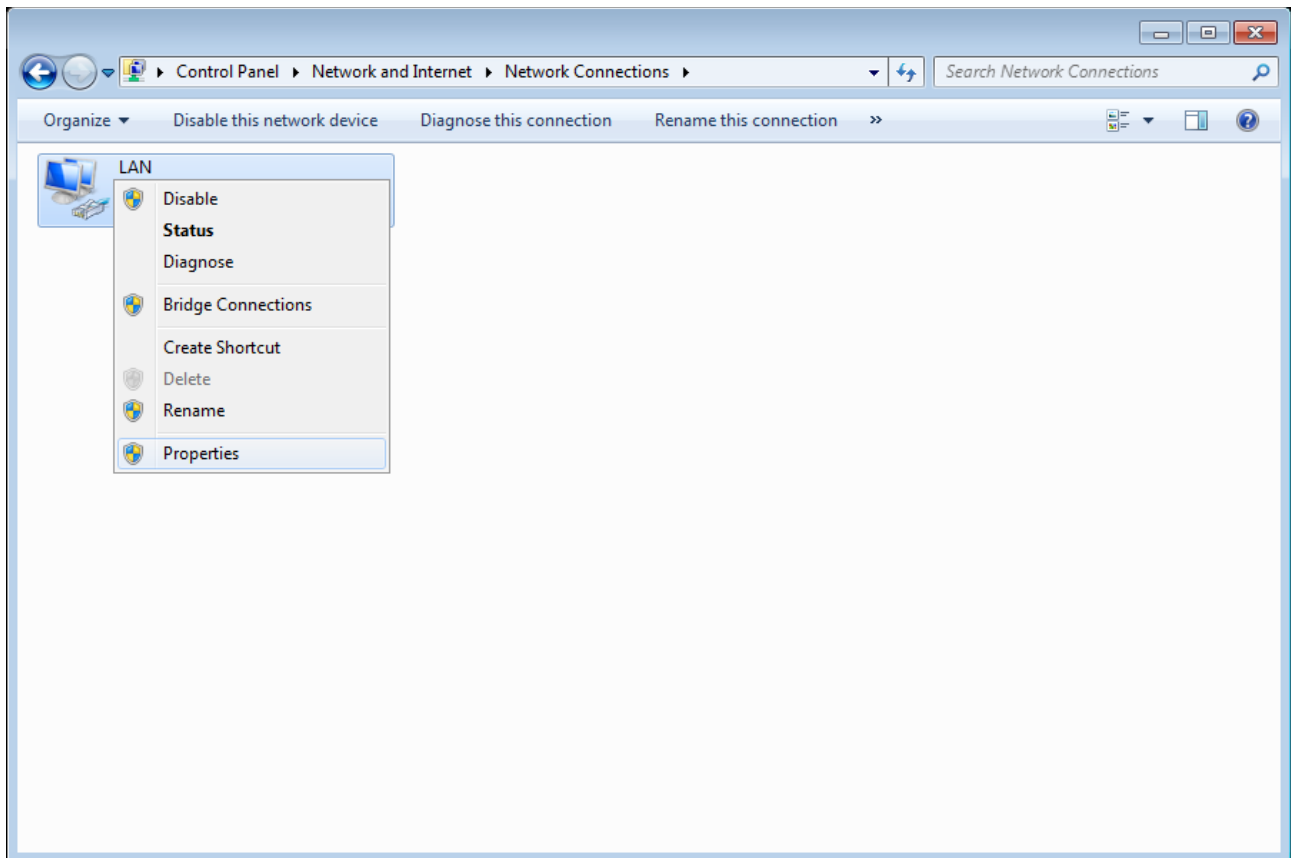


Figure 5. The **Network Connections** window.

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

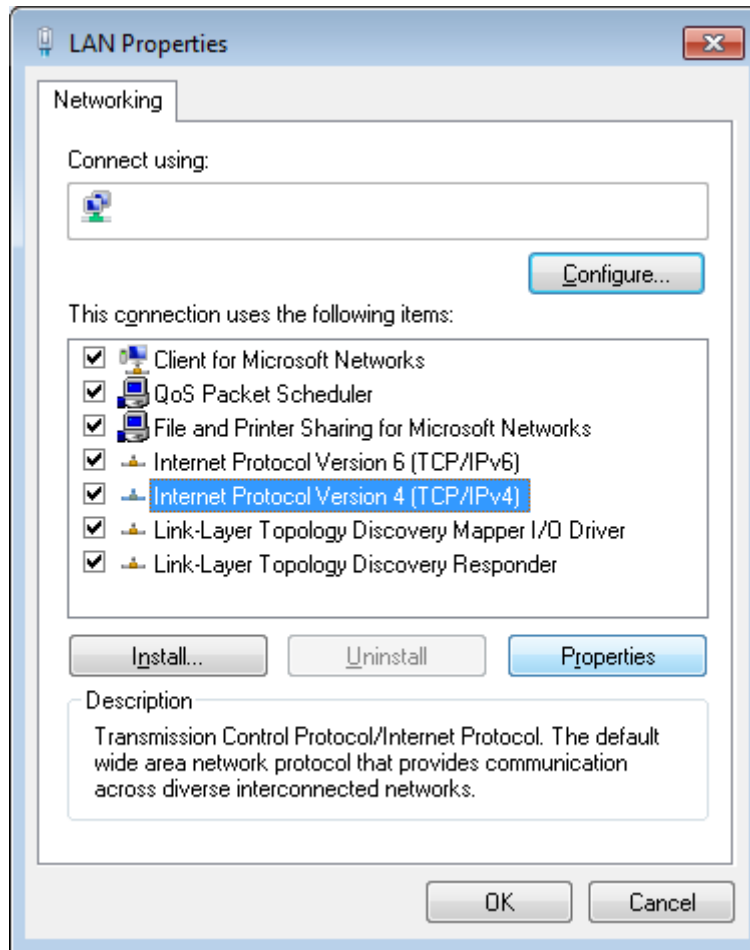


Figure 6. The **Local Area Connection Properties** window.

6. 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.

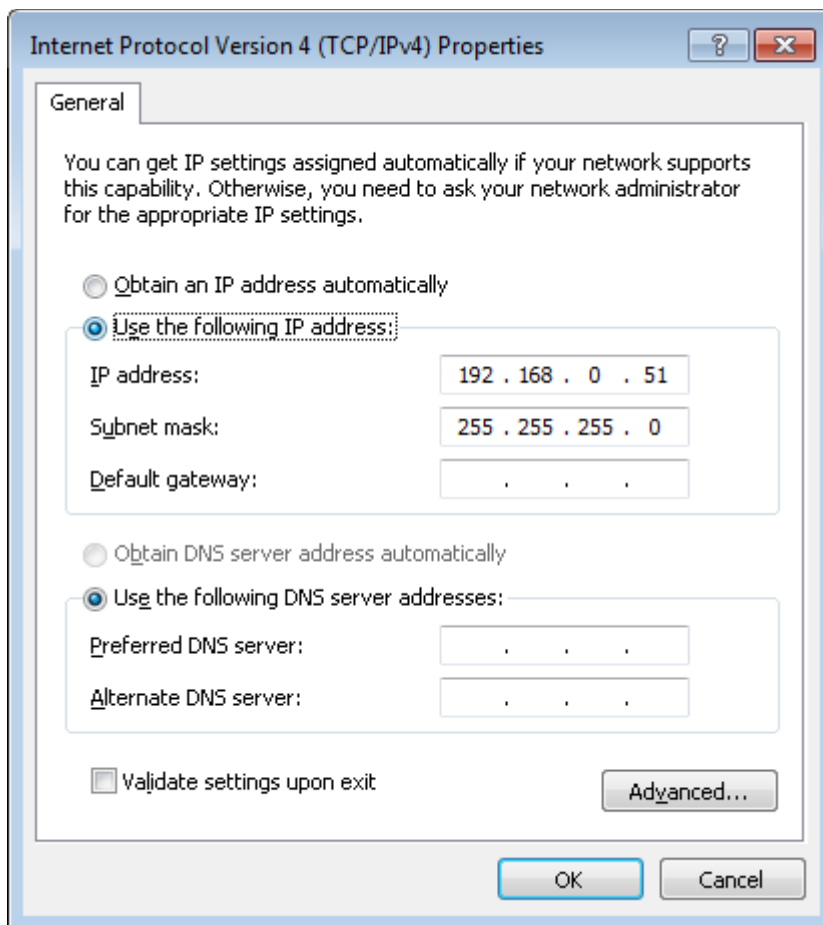


Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now you can connect to the web-based interface of DAP-1360U 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. Attach the antennas from the delivery package. To do this, remove the antennas from their wrapper, attach them to the relevant connectors on the back panel of the access point, and then screw the antennas in a clockwise direction to the back panel. Position the antennas upward at their connecting joints. This will ensure optimal operation of your wireless network.
2. Connect the power cord 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.
3. Turn on the access point by pressing the **ON/OFF** button on its back panel.
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.)

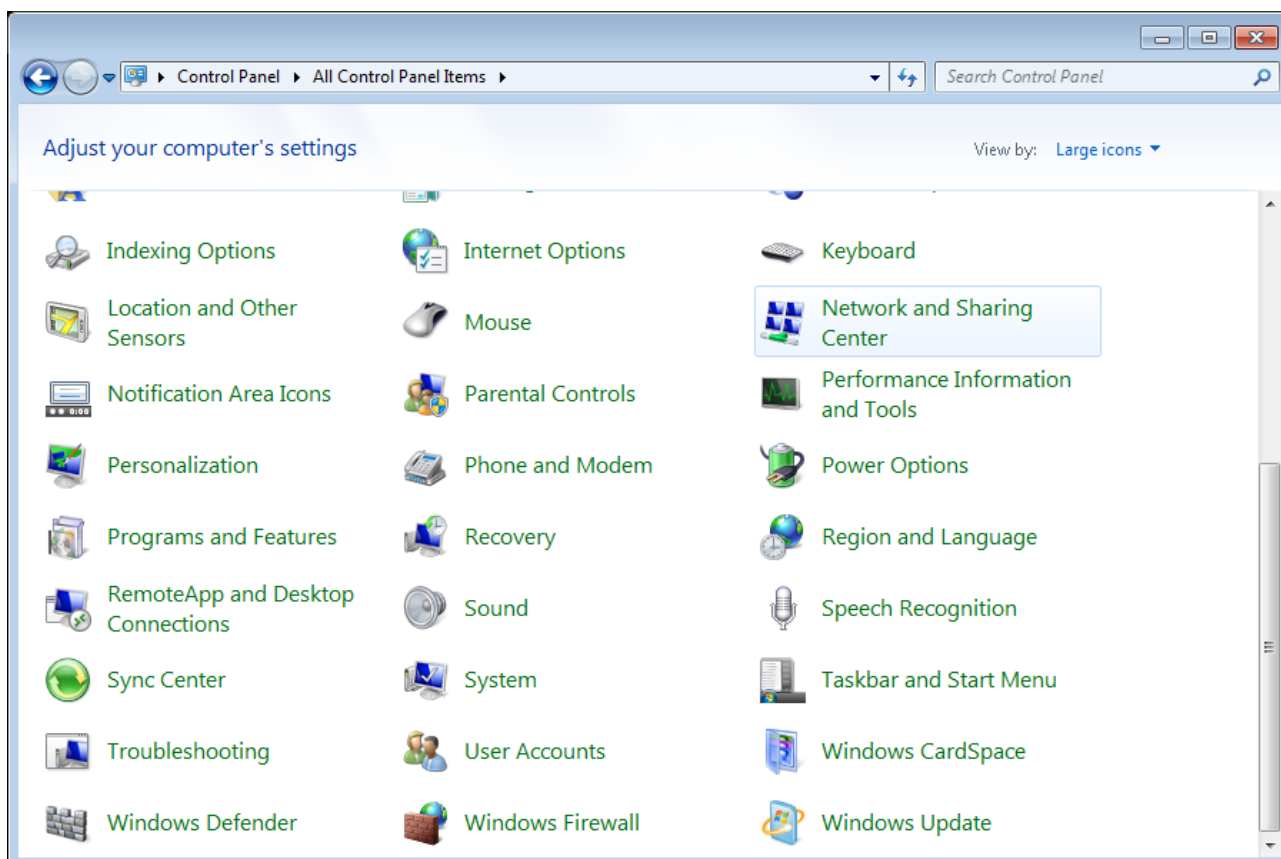


Figure 8. The **Control Panel** window.

3. In the menu located on the left part of the window, select the **Change adapter settings** line.
4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.

5. In the **Wireless Network Connection Properties** window, on the **Networking** tab, select the **Internet Protocol Version 4 (TCP/IPv4)** line. Click the **Properties** button.
6. 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.

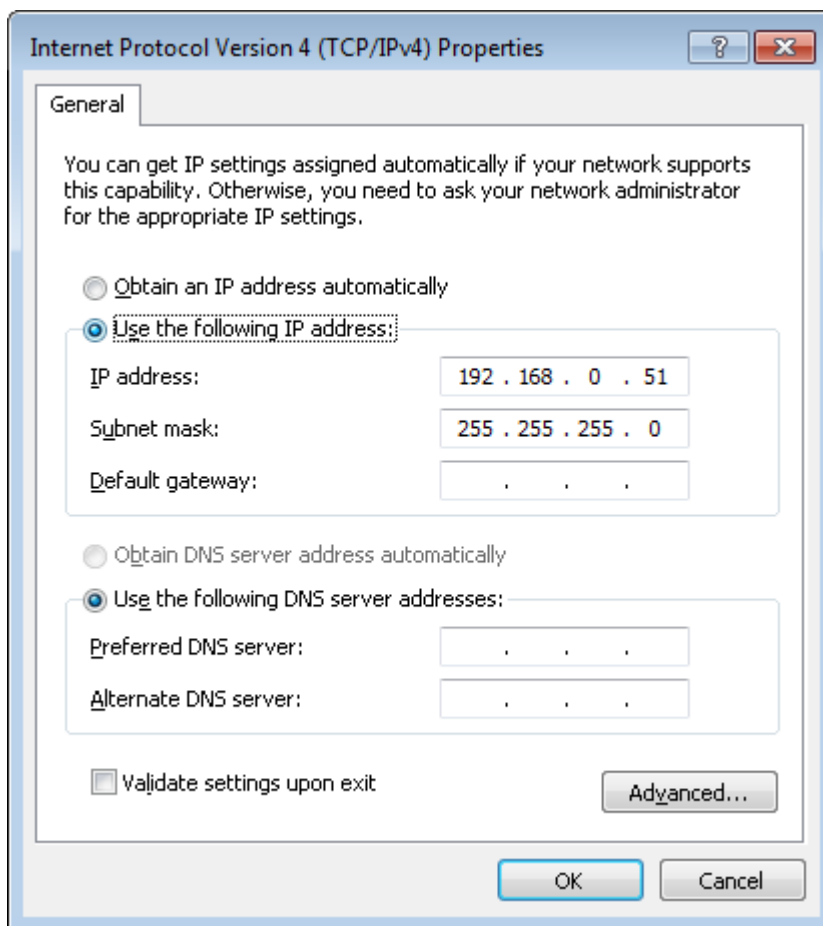


Figure 9. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

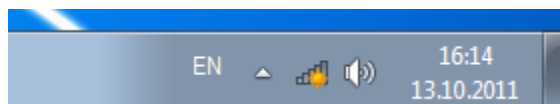


Figure 10. The notification area of the taskbar.

- In the opened window, in the list of available wireless networks, select the wireless network **DAP-1360** and click the **Connect** button.

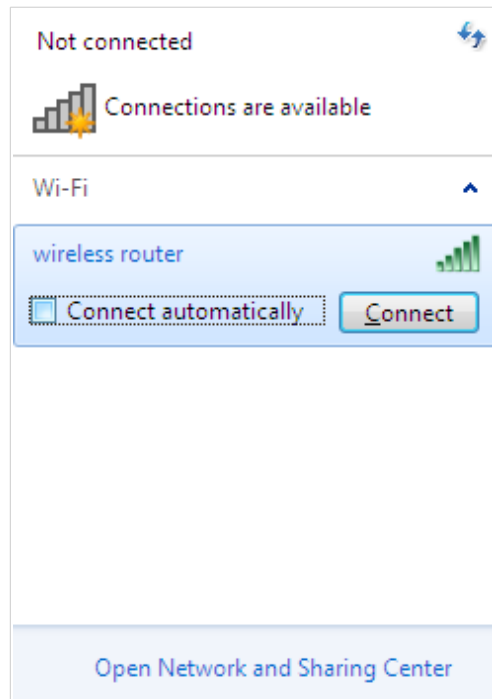


Figure 11. The list of available networks.

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

Now you can connect to the web-based interface of DAP-1360U 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 12). In the address bar of the web browser, enter the domain name of the access point (by default, **dlinkap.local**) with a dot at the end and press the **Enter** key. Also you can enter the IP address of the device (by default, **192.168.0.50**).

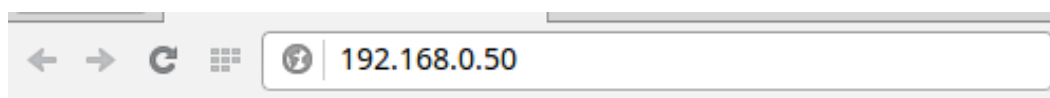


Figure 12. Connecting to the web-based interface of the DAP-1360U device.



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 30).

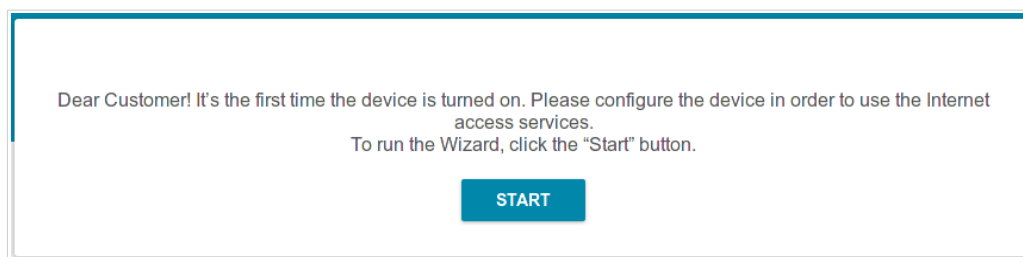
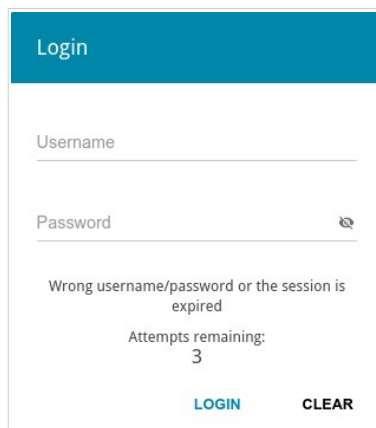


Figure 13. The page for running the Initial Configuration Wizard.

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



The screenshot shows a web-based login interface. At the top, there is a teal header with the word "Login" in white. Below the header, there are two input fields: "Username" and "Password". The "Password" field has a small eye icon to its right. Below the input fields, there is a message: "Wrong username/password or the session is expired". Underneath this message, it says "Attempts remaining: 3". At the bottom of the form, there are two buttons: "LOGIN" in teal and "CLEAR" in black.

Figure 14. 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.

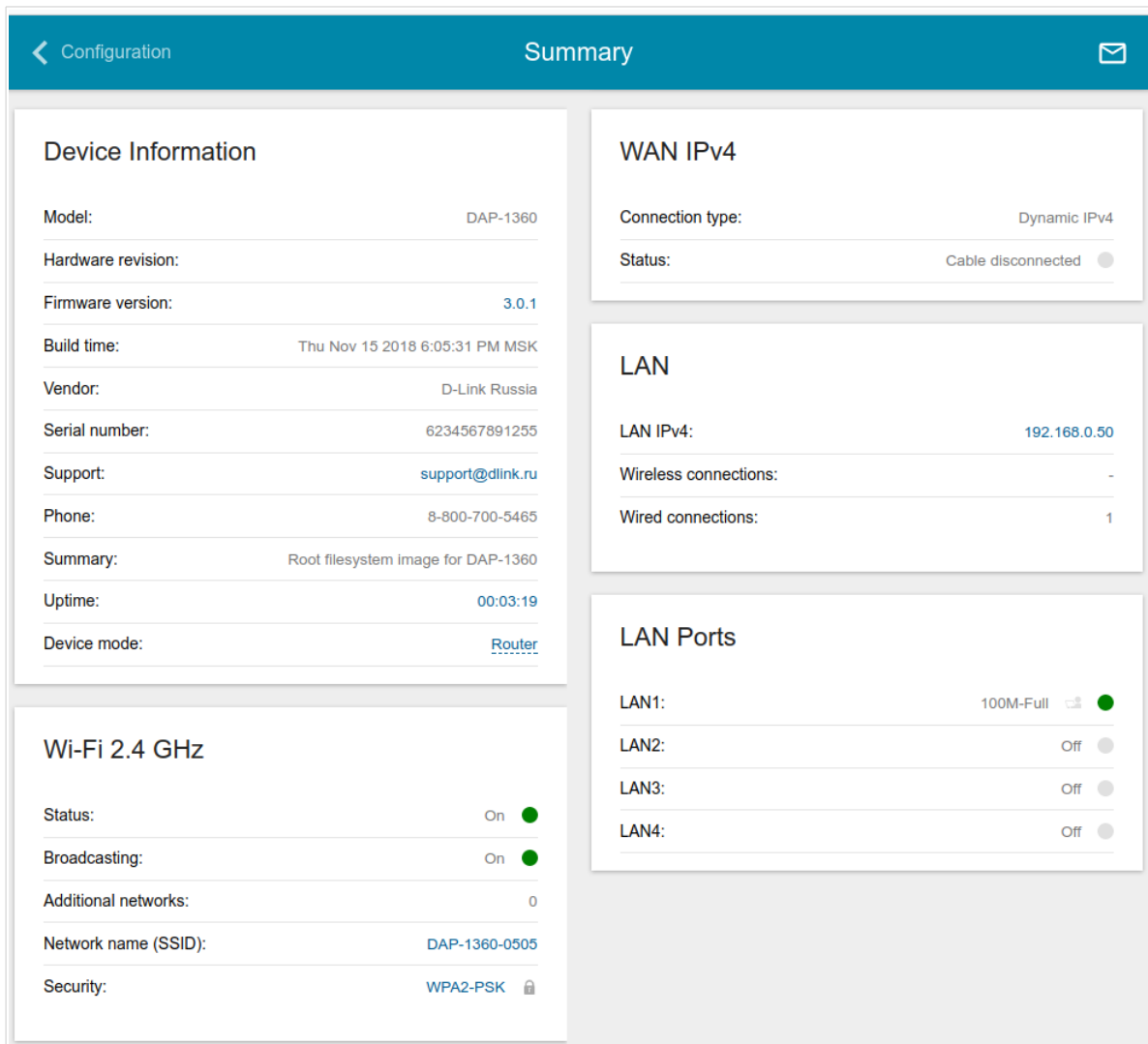


Figure 15. The summary page in the router mode.

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

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

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **initial setup wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 30).

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 **WDS** section, the MAC addresses of devices connected to the access point via the WDS function are displayed.

In the **LAN** section, the IPv4 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 ports and data transfer mode of active ports.

Home Page

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

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

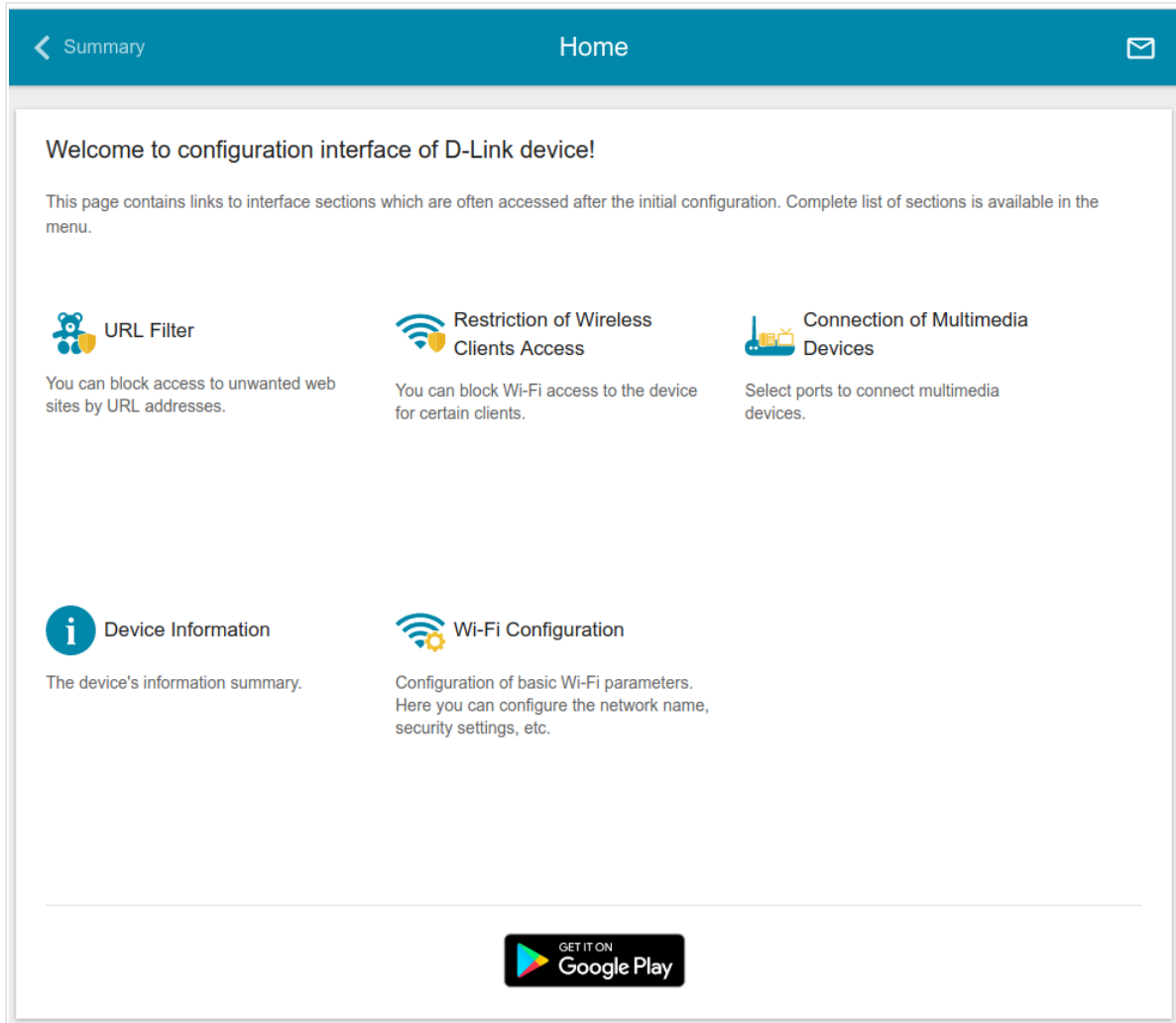


Figure 16. The **Home** page.

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 30).

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 54).

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 60).

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 79).

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 109).

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 128).

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 140).

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.

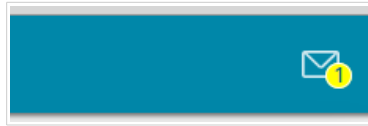


Figure 17. The web-based interface notifications.

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

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration 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.

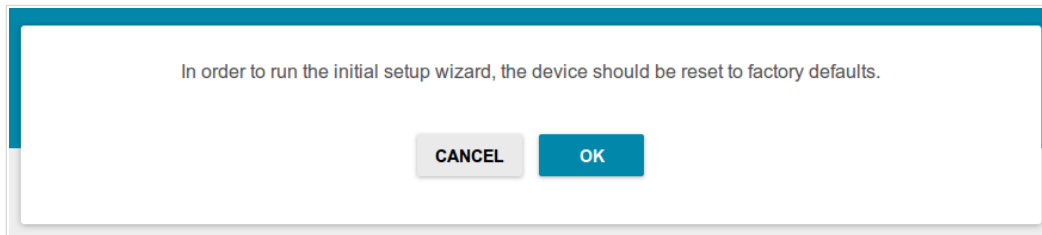


Figure 18. Restoring the default settings in the Wizard.

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-1360U (see the WLAN name (SSID) on the barcode label on the bottom panel of the device) and click the **NEXT** button.

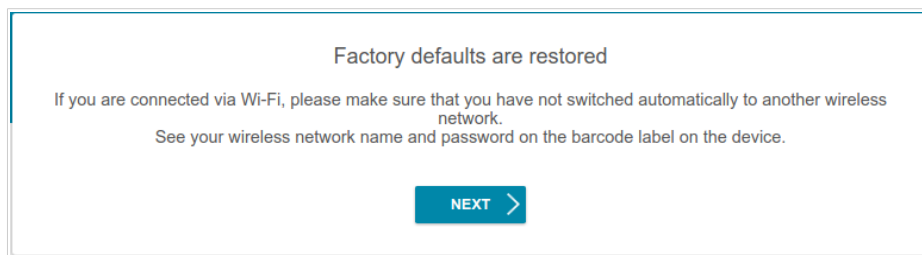


Figure 19. Checking connection to the wireless network.

Click the **START** button.

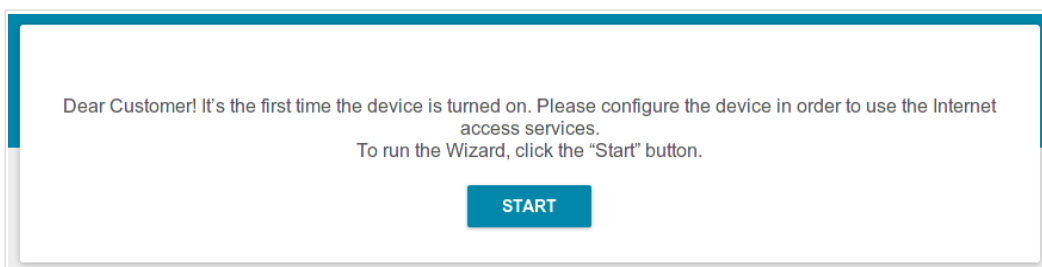


Figure 20. Starting the Wizard.

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

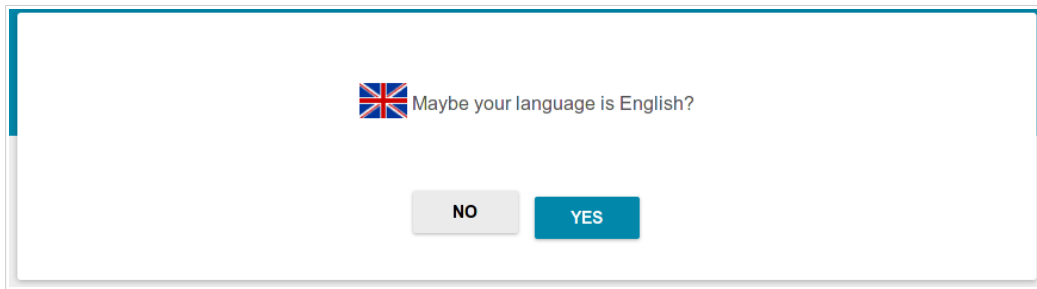


Figure 21. Selecting a language.

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

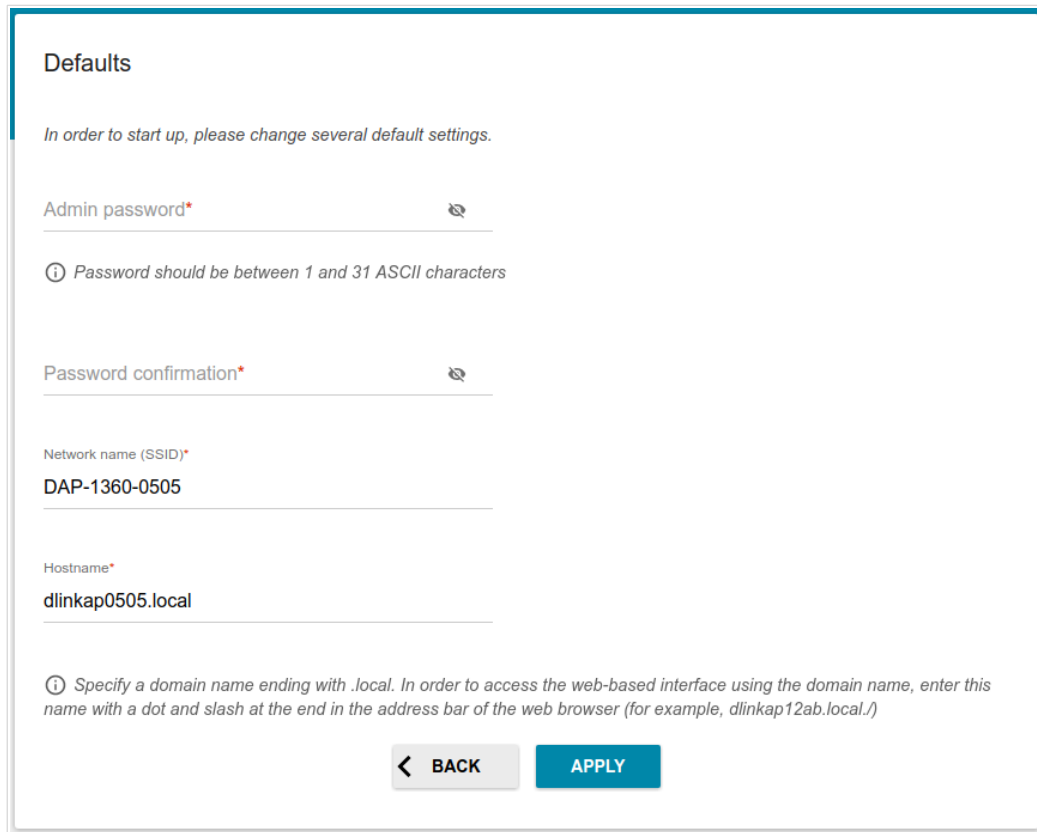


Figure 22. Changing the default settings.

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

Selecting Operation Mode

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

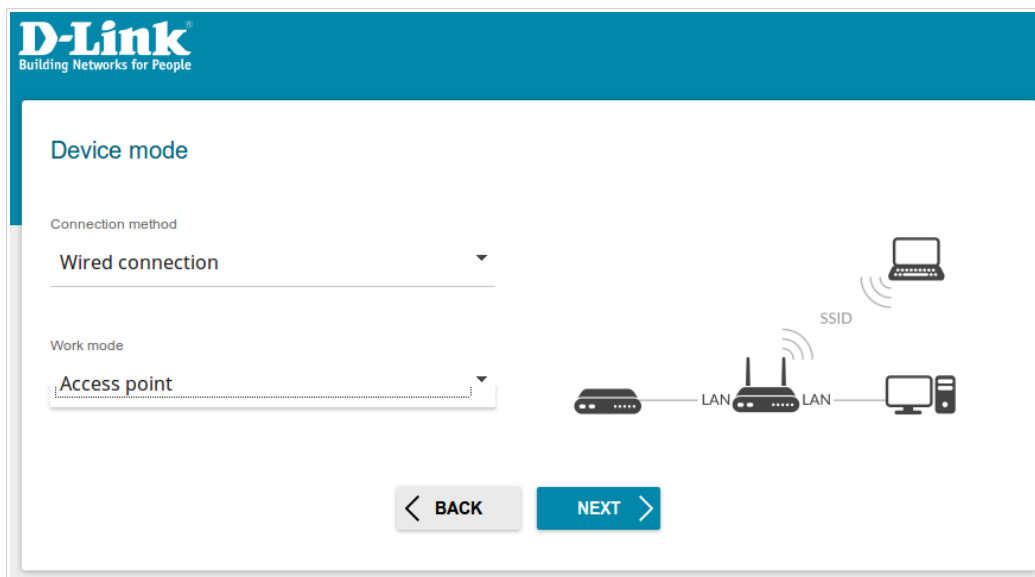


Figure 23. Selecting an operation mode. The **Access point** mode.

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.

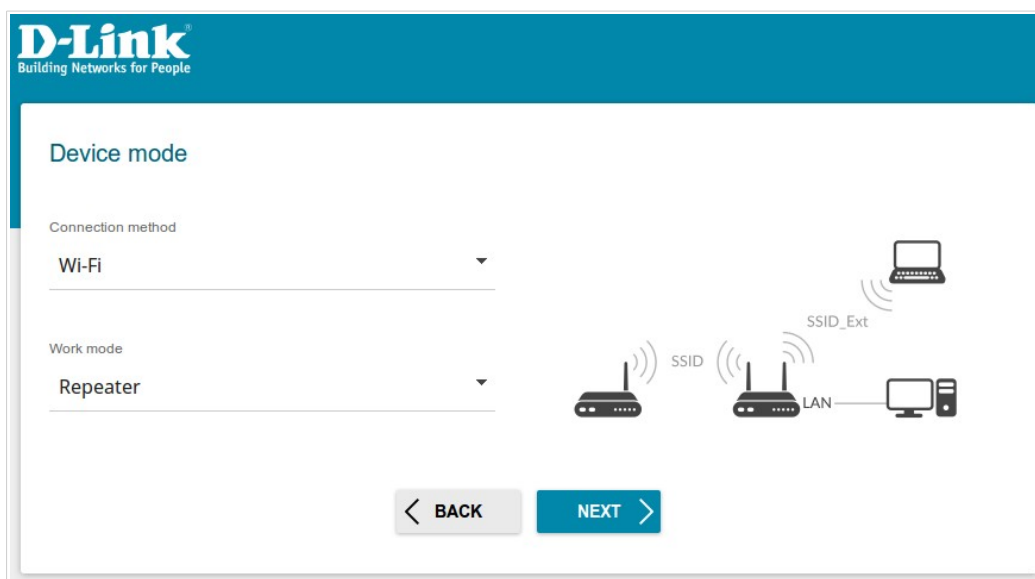


Figure 24. Selecting an operation mode. The **Repeater** mode.

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.

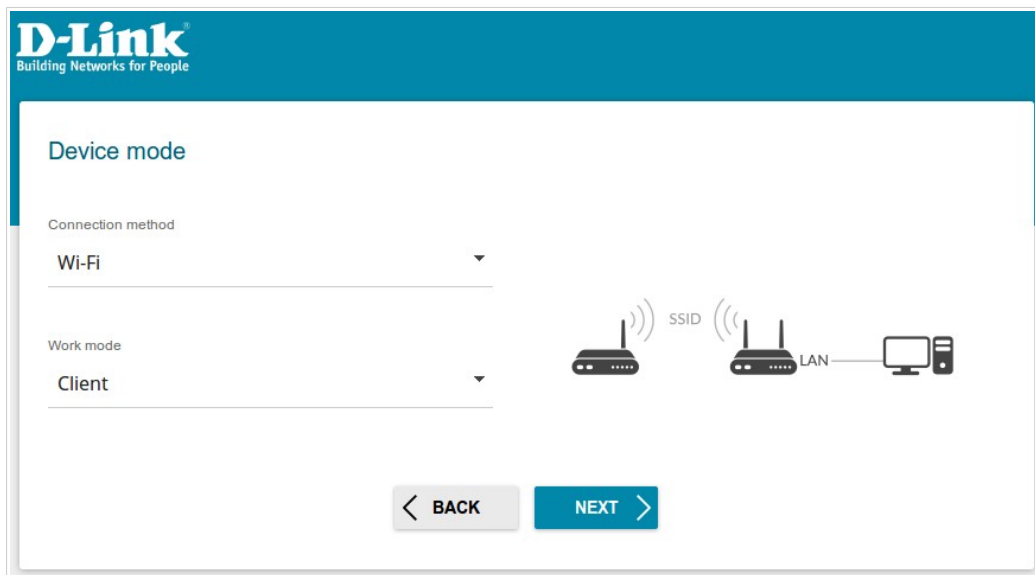


Figure 25. Selecting an operation mode. The **Client** mode.

Also you can enable the WDS function via the Initial Configuration Wizard. To do this, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **WDS** value. In this mode you can specify the WDS function parameters, 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.

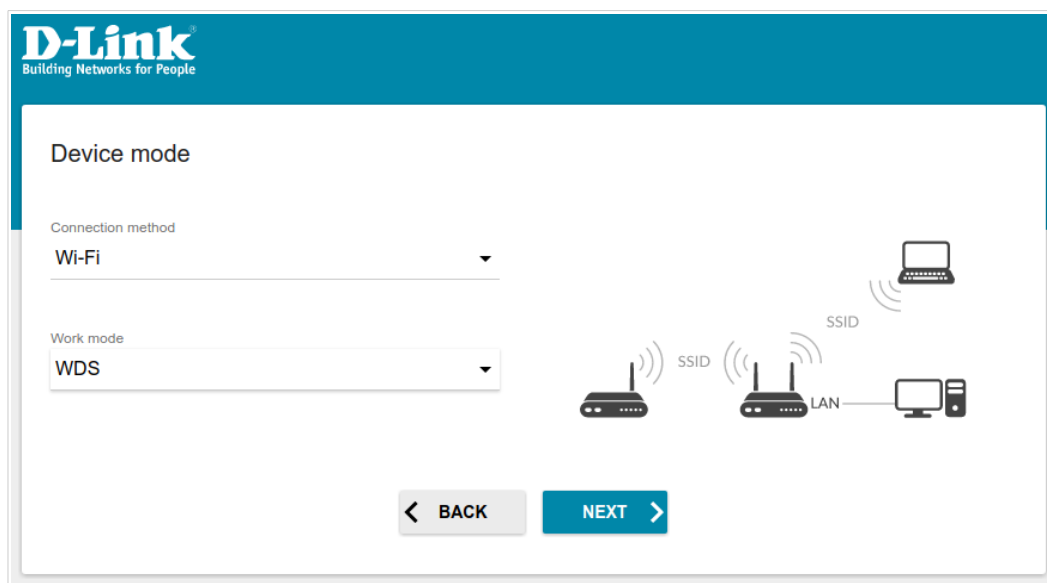


Figure 26. Selecting an operation mode. The **WDS** mode.

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

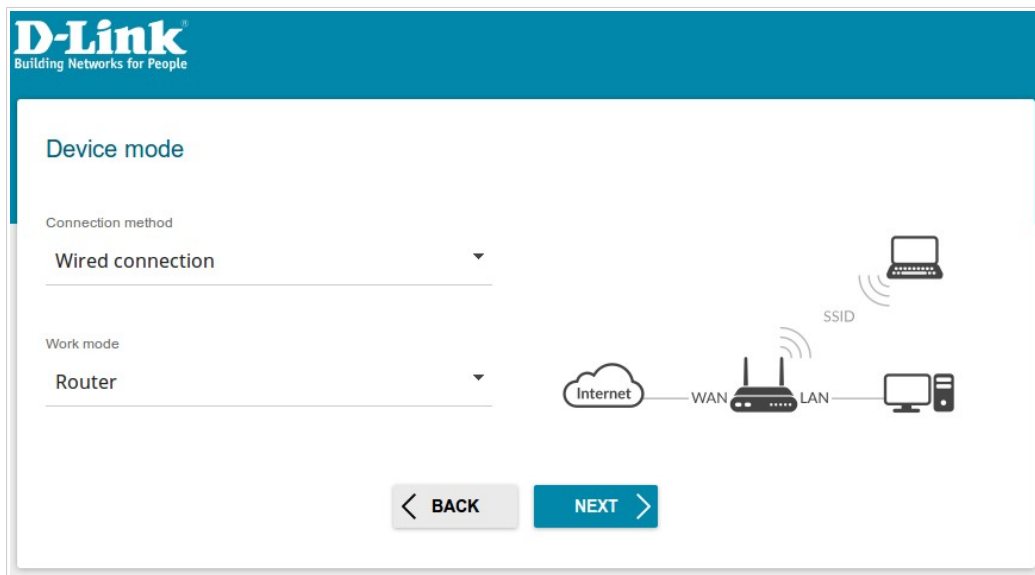


Figure 27. Selecting an operation mode. The **Router** mode.

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

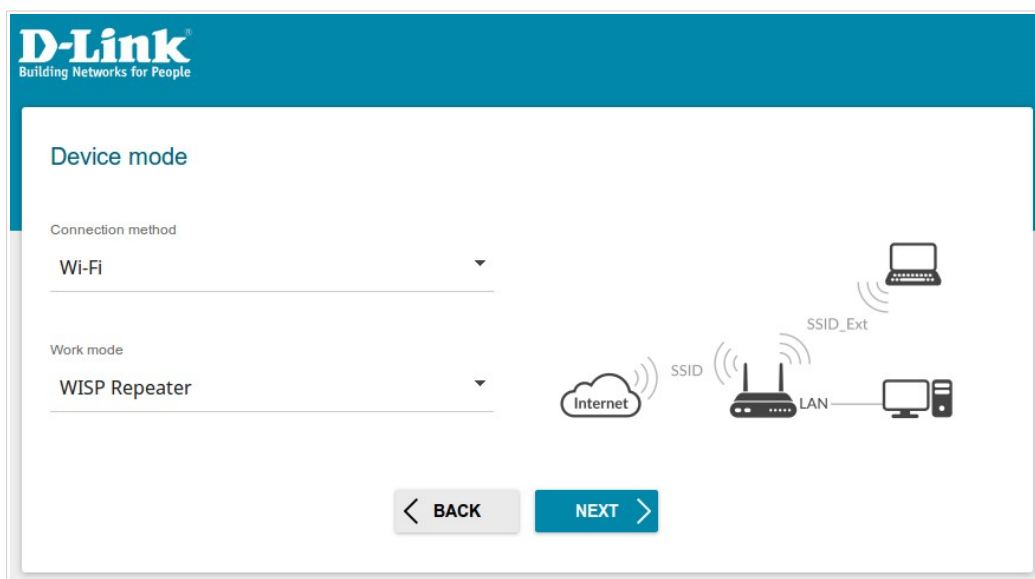


Figure 28. Selecting an operation mode. The **WISP Repeater** mode.

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

Configuring WDS Function

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

1. On the **WDS** page, in the **WDS Mode** list, select the WDS function mode.

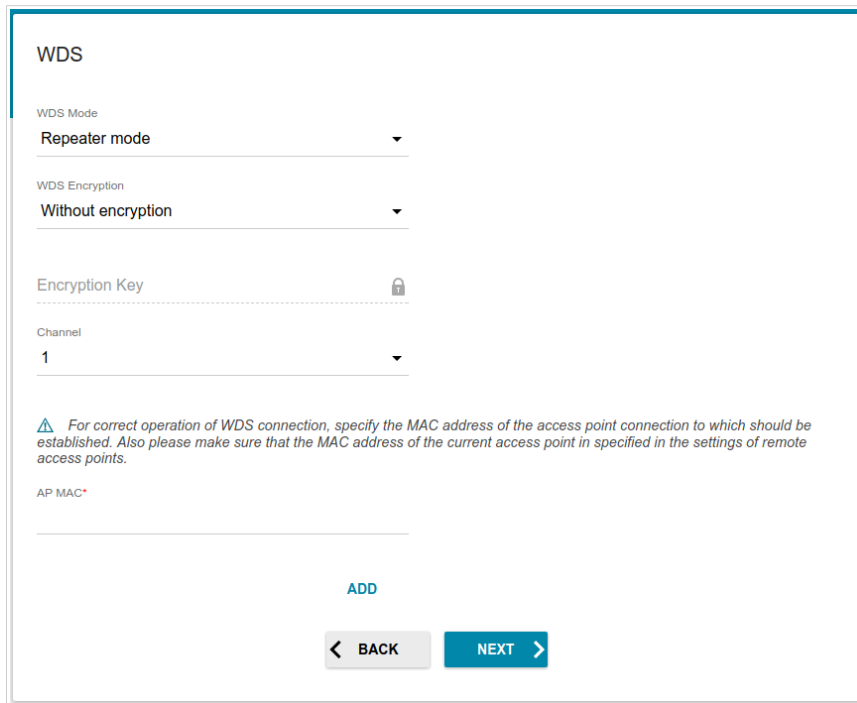


Figure 29. The page for configuring the WDS function.

2. In the **WDS Encryption** list, select a type of encryption for data transfer between access points interconnected via the WDS function. Then enter a key for the specified type of encryption in the **Encryption Key** field (a password that will be used to access the wireless network between the interconnected access points). When the **Without encryption** value is selected, traffic between the access points will not be secured.
3. In the **Channel** list, select the wireless channel number. The same wireless channel for the interconnected access points should be specified.
4. In the **AP MAC** field, specify the MAC address of a device connected to the access point via the WDS function. To specify several MAC addresses, click the **ADD** button, and in the line displayed, enter a MAC address.



The WDS function parameters must be the same for all interconnected devices.

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

Changing LAN IPv4 Address

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

1. Select the **Automatic obtainment of IPv4 address** to let DAP-1360U automatically obtain the LAN IPv4 address.
2. In the **Hostname** field, you should specify a domain name of the access point using which you can access the web-based interface after finishing the Wizard. Enter a new domain name of the access point ending with **.local** or leave the value suggested by the access point.

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

If you want to manually assign the LAN IPv4 address for DAP-1360U, do not select the **Automatic obtainment of IPv4 address** checkbox and fill in the **IP address**, **Netmask**, **Hostname** fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.

LAN

Automatic obtainment of IPv4 address

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

IP address*

192.168.0.50

Subnet mask*

255.255.255.0

Gateway IP address

Hostname*

dlinkap0505.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 30. The page for changing the LAN IPv4 address.


3. After changing the LAN IPv4 address of the device, make sure that the network adapter settings correspond to the new parameters.
4. 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.

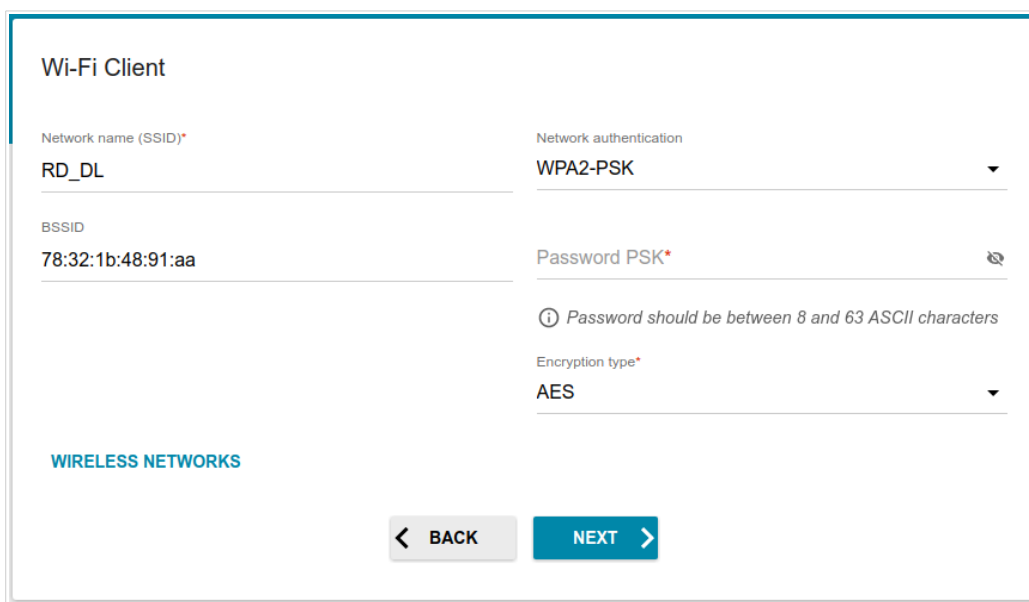


Figure 31. The page for configuring the Wi-Fi client.

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

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

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

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

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

Configuring WAN Connection

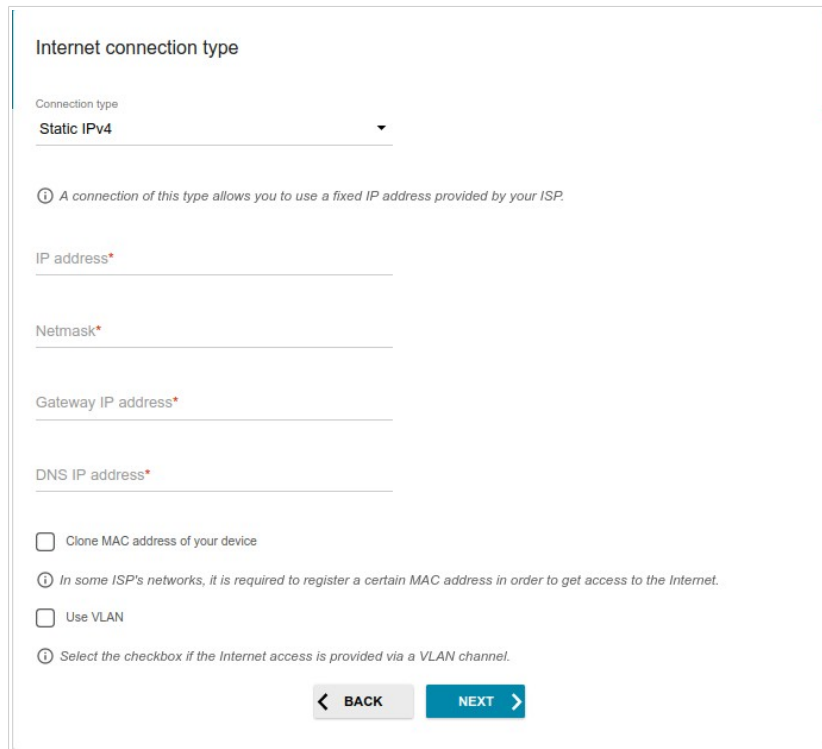
This configuration step is available for the **Router** and **WISP Repeater** modes.



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

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

Static IPv4 Connection

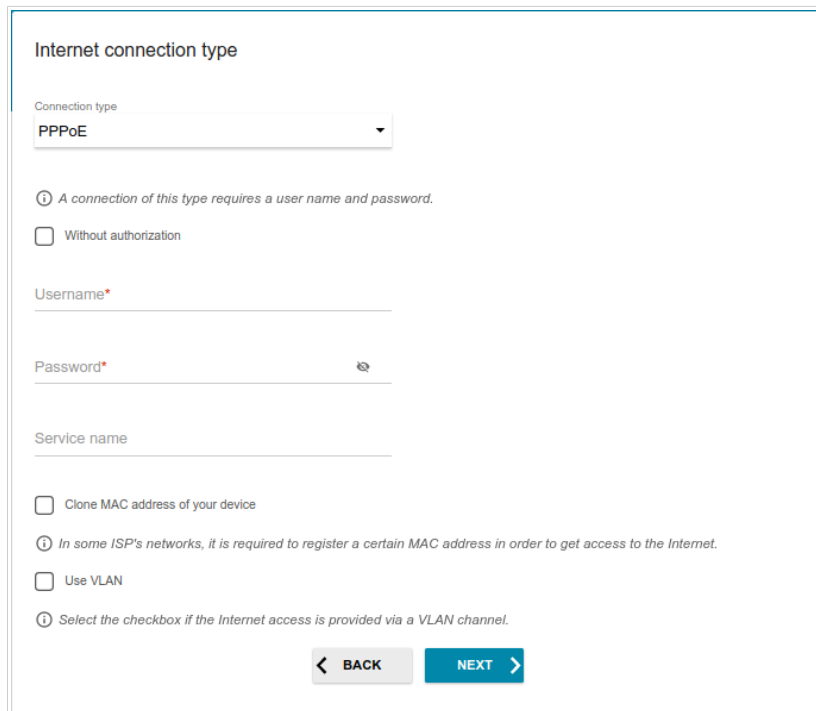


The screenshot shows a web-based configuration interface for a Static IPv4 connection. The title is "Internet connection type". Below the title, there is a dropdown menu labeled "Connection type" with "Static IPv4" selected. A help icon (i) is followed by the text: "A connection of this type allows you to use a fixed IP address provided by your ISP." Below this are four text input fields, each with a red asterisk indicating it is required: "IP address*", "Netmask*", "Gateway IP address*", and "DNS IP address*". There are two checkboxes: "Clone MAC address of your device" and "Use VLAN". A second help icon (i) is followed by the text: "In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet." Below the "Use VLAN" checkbox, another help icon (i) is followed by the text: "Select the checkbox if the Internet access is provided via a VLAN channel." At the bottom, there are two buttons: a grey "BACK" button with a left arrow and a blue "NEXT" button with a right arrow.

Figure 32. The page for configuring Static IPv4 WAN connection.

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

PPPoE or PPPoE + Dynamic IP (PPPoE Dual Access) Connections

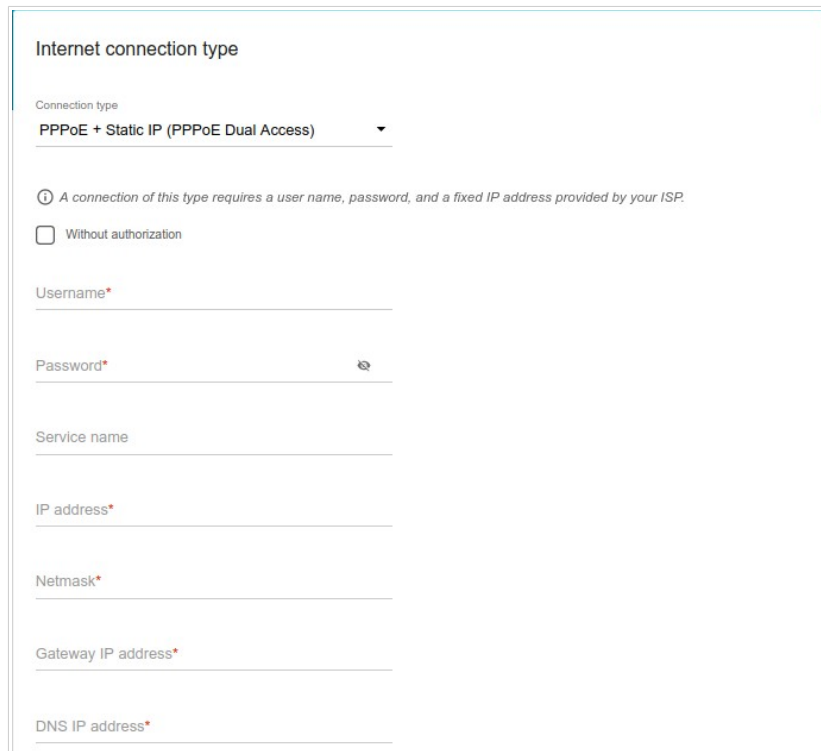


The screenshot shows a web-based configuration page titled "Internet connection type". At the top, there is a dropdown menu for "Connection type" with "PPPoE" selected. Below this, there is an information icon and a note: "A connection of this type requires a user name and password." There are two checkboxes: "Without authorization" (unchecked) and "Clone MAC address of your device" (unchecked). Below these are three text input fields: "Username*", "Password*" (with a "Show" icon), and "Service name". At the bottom, there are two more checkboxes: "Use VLAN" (unchecked) and "Select the checkbox if the Internet access is provided via a VLAN channel." (unchecked). At the very bottom, there are two buttons: "BACK" and "NEXT".

Figure 33. 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.

Without authorization

Username*

Password* 

Service name


IP address*

Netmask*

Gateway IP address*

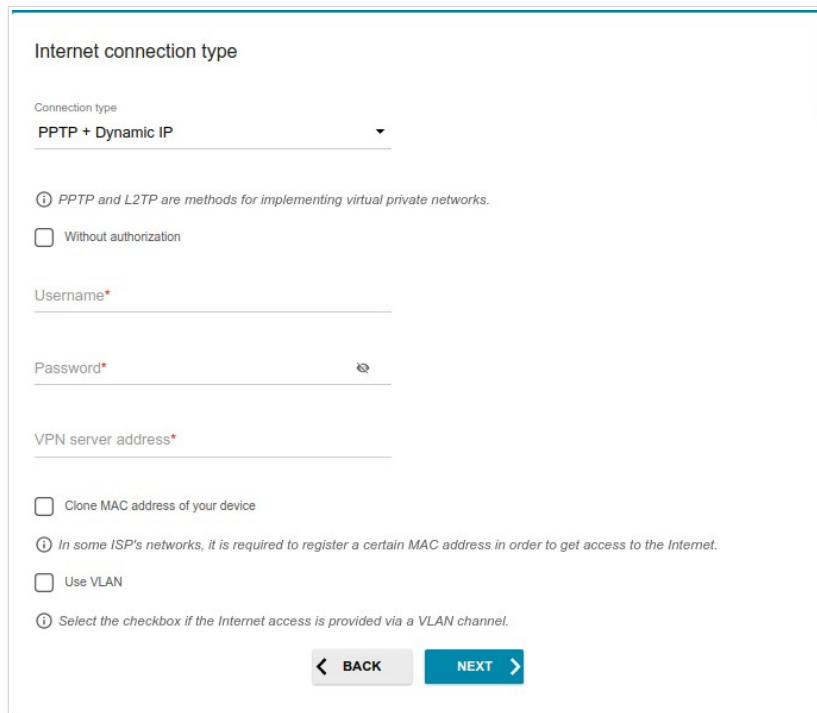
DNS IP address*

Figure 34. The page for configuring PPPoE + Static IP (PPPoE Dual Access) WAN connection.

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

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

PPTP + Dynamic IP or L2TP + Dynamic IP Connection



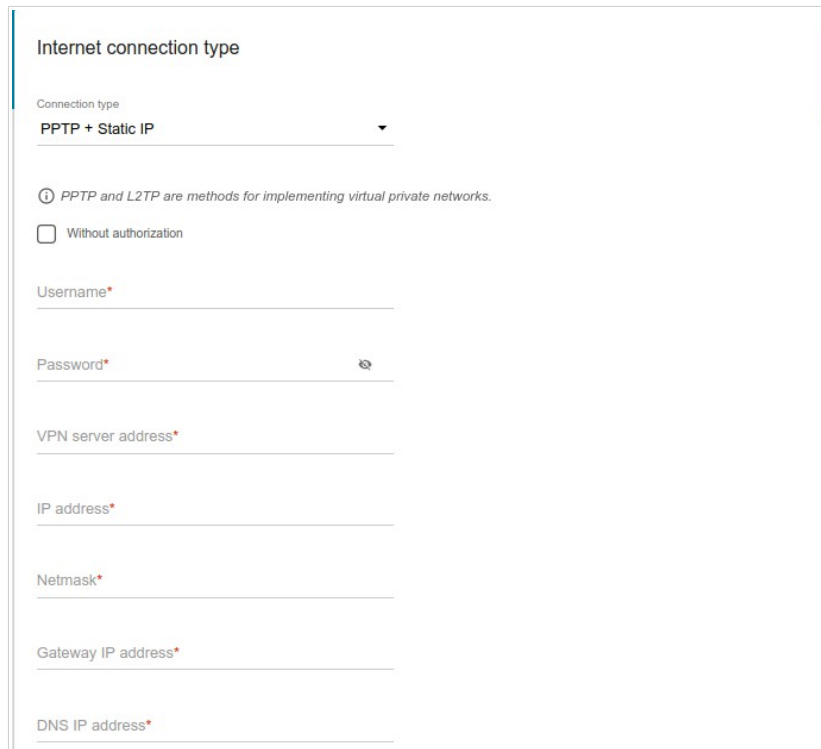
The screenshot shows a configuration page titled "Internet connection type". The "Connection type" dropdown menu is set to "PPTP + Dynamic IP". Below this, there is an information icon and the text "PPTP and L2TP are methods for implementing virtual private networks." There are two checkboxes: "Without authorization" (unchecked) and "Clone MAC address of your device" (unchecked). Below these are three text input fields: "Username*", "Password*" (with a "Show" icon), and "VPN server address*". At the bottom, there are two more checkboxes: "Use VLAN" (unchecked) and "Select the checkbox if the Internet access is provided via a VLAN channel." (unchecked). At the very bottom, there are two buttons: "BACK" and "NEXT".

Figure 35. The page for configuring PPTP + Dynamic IP WAN connection.

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

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

PPTP + Static IP or L2TP + Static IP Connection



The screenshot shows a web-based configuration interface for setting up a PPTP + Static IP WAN connection. The page is titled "Internet connection type" and features a dropdown menu currently set to "PPTP + Static IP". Below the dropdown is a help icon and a note: "PPTP and L2TP are methods for implementing virtual private networks." There is a checkbox labeled "Without authorization". The form includes several text input fields, each with a red asterisk indicating it is required: "Username*", "Password*" (with a "Show" icon to its right), "VPN server address*", "IP address*", "Netmask*", "Gateway IP address*", and "DNS IP address*".

Figure 36. The page for configuring PPTP + Static IP WAN connection.

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

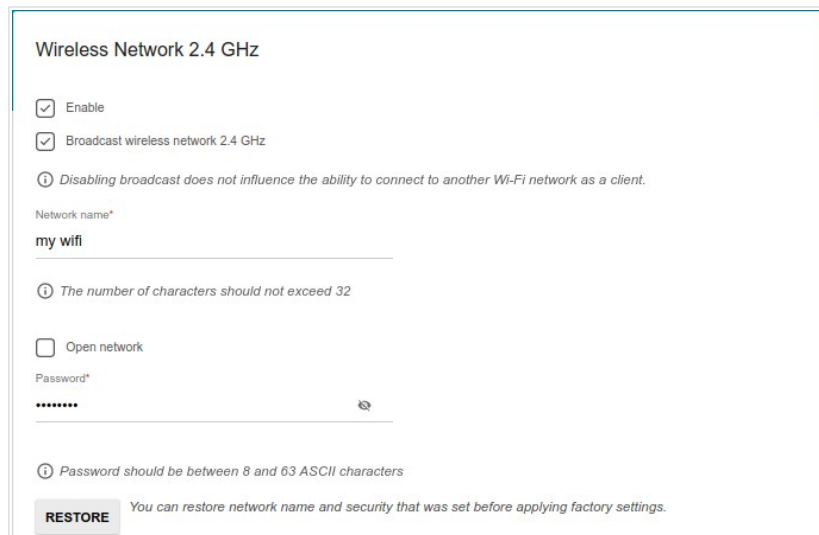
In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

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

Configuring Wireless Network

This configuration step is available for the **Router**, **Access point**, **WISP Repeater**, **Repeater**, and **WDS** 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 **Repeater** mode 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 wifi

The number of characters should not exceed 32

Open network

Password*

.....

Password should be between 8 and 63 ASCII characters

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

Figure 37. 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).

Enable guest network

i 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.

Network name*

my wifi

i The number of characters should not exceed 32

Open network

Max associated clients*

0

Enable shaping

Shaping (Mbit/s)*

0

Figure 38. The page for configuring the wireless network.

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

Configuring LAN Ports for IPTV/VoIP

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

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

The screenshot shows the IPTV configuration page. It includes the following elements:

- IPTV** section header.
- Two checked checkboxes: **Is an STB connected to the device?** and **Use VLAN ID**.
- A help icon and text: *Information about the VLAN ID can be found in the contract.*
- A text input field labeled **VLAN ID***.
- A diagram of a router's LAN ports: port 4 (with a TV icon), port 3 (labeled LAN), port 2 (with a person icon), port 1 (labeled Internet), and an unlabeled port to the right.
- Navigation buttons: **BACK** and **NEXT**.

Figure 39. The page for selecting a LAN port to connect an IPTV set-top box.

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

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

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.

4 3 LAN 2 1 Internet

Figure 40. The page for selecting a LAN port to connect an VoIP phone.

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

Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **Admin password** and **Password confirmation** fields. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.¹

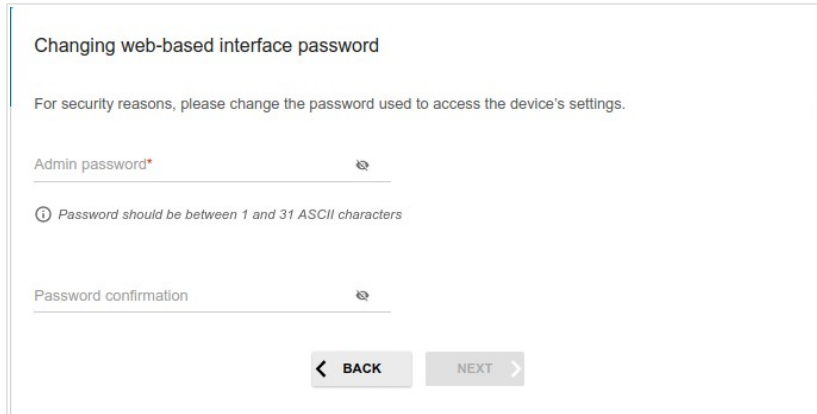


Figure 41. The page for changing the web-based interface password.

! 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 router.

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

On the next page, check all specified settings.

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

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

¹ 0-9, A-Z, a-z, space, !"#%&'()*+,-./:;<=>?@[\\]^_`{|}~.

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

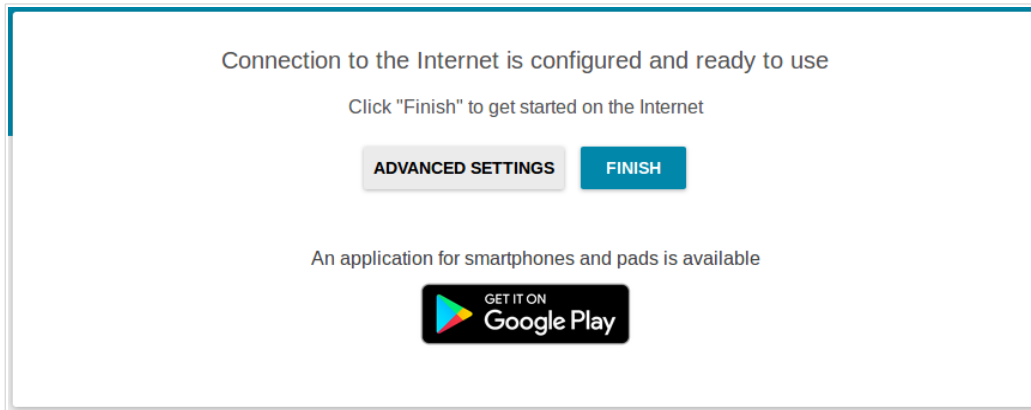


Figure 42. Checking the Internet availability.

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 is displayed on the **Summary** page).

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 27).

Connection of Multimedia Devices

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

The Multimedia Devices Connection Wizard helps to configure LAN ports 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-1360U in order to use these devices.

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

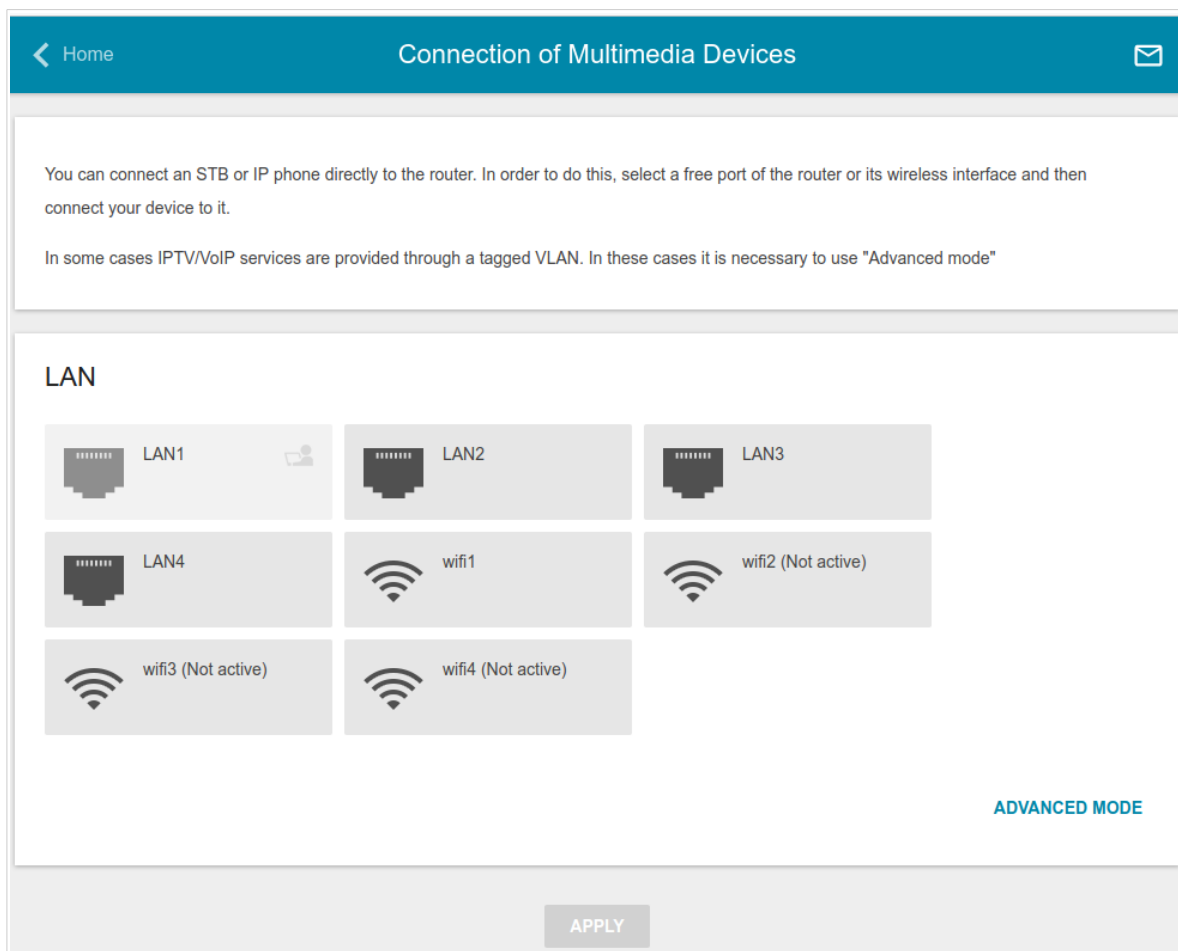


Figure 43. The Multimedia Devices Connection Wizard. The simple mode.

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

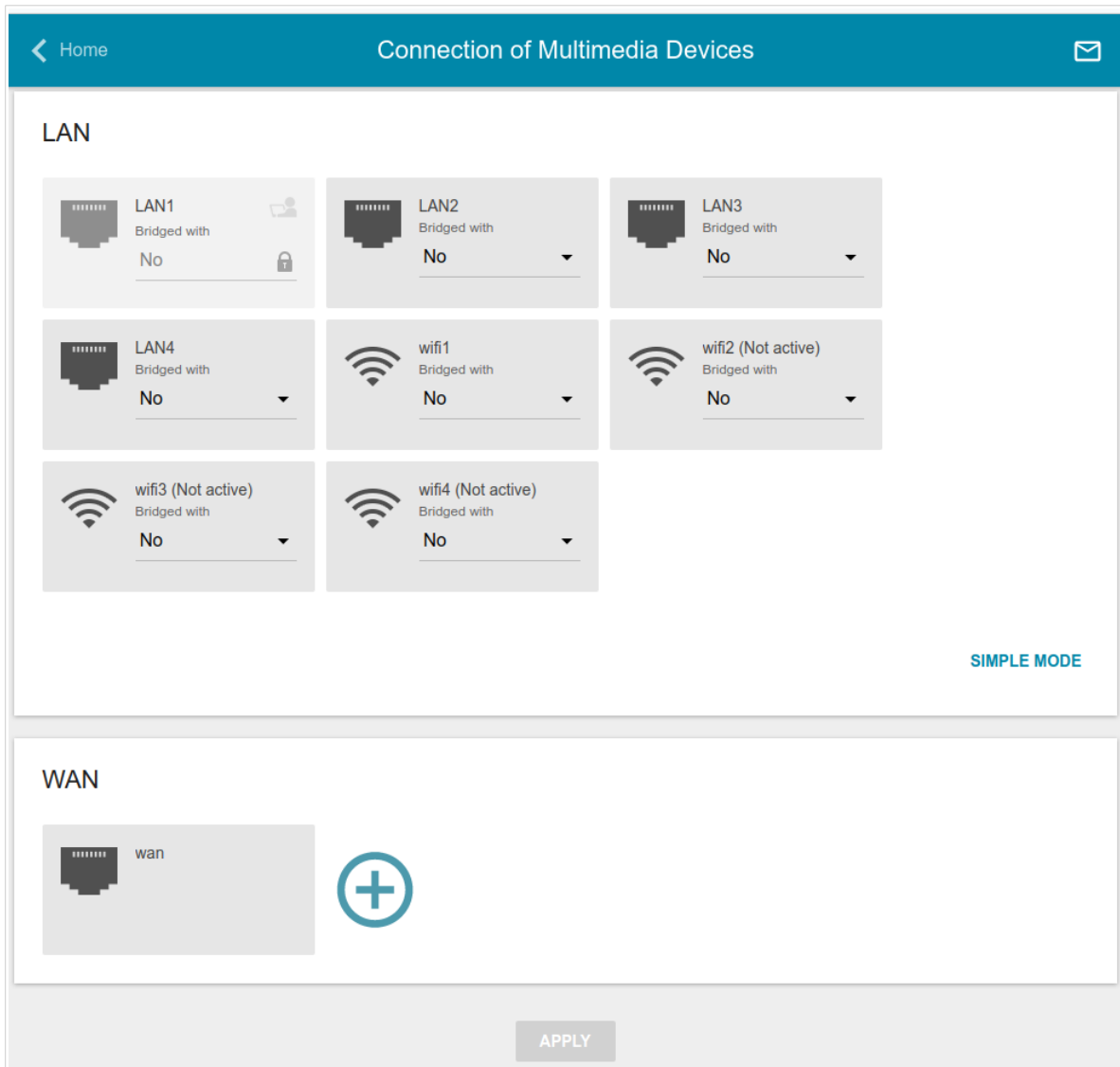


Figure 44. The Multimedia Devices Connection Wizard. The advanced mode.

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

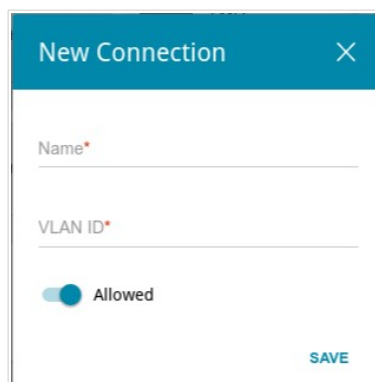


Figure 45. Adding a connection.

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

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

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

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

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

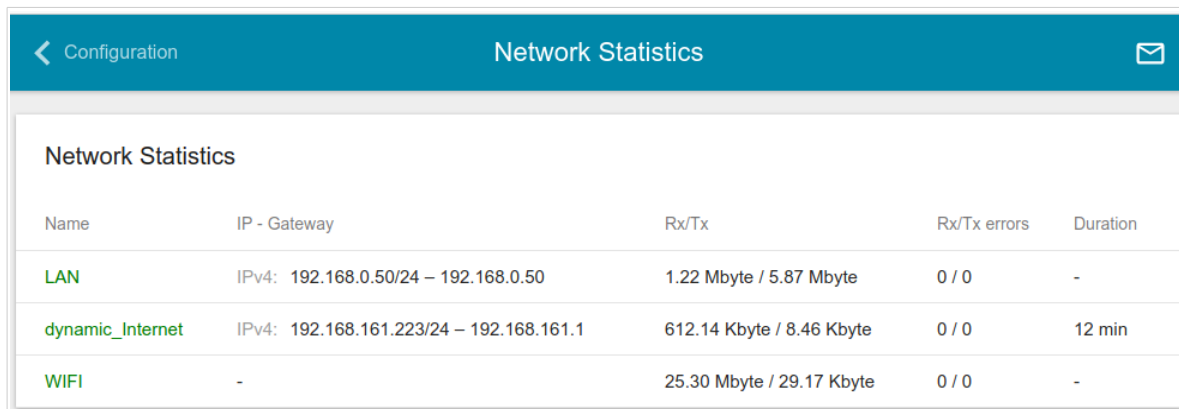
Statistics

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

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

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).



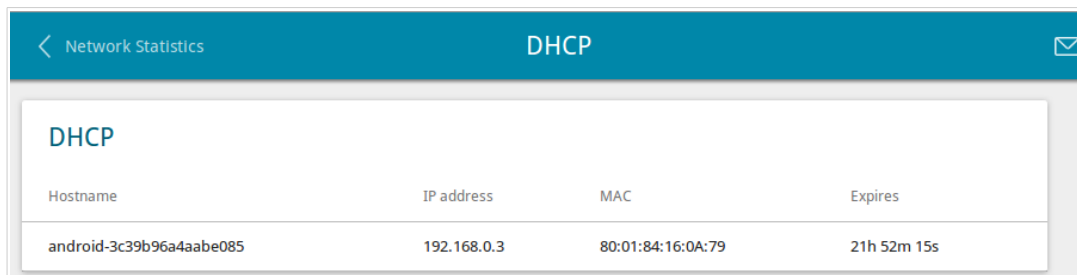
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.50/24 – 192.168.0.50	1.22 Mbyte / 5.87 Mbyte	0 / 0	-
dynamic_Internet	IPv4: 192.168.161.223/24 – 192.168.161.1	612.14 Kbyte / 8.46 Kbyte	0 / 0	12 min
WIFI	-	25.30 Mbyte / 29.17 Kbyte	0 / 0	-

Figure 46. The **Statistics / Network Statistics** page.

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

DHCP

The **Statistics / DHCP** page displays the information on computers that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the device, as well as the IP address expiration periods (the lease time).



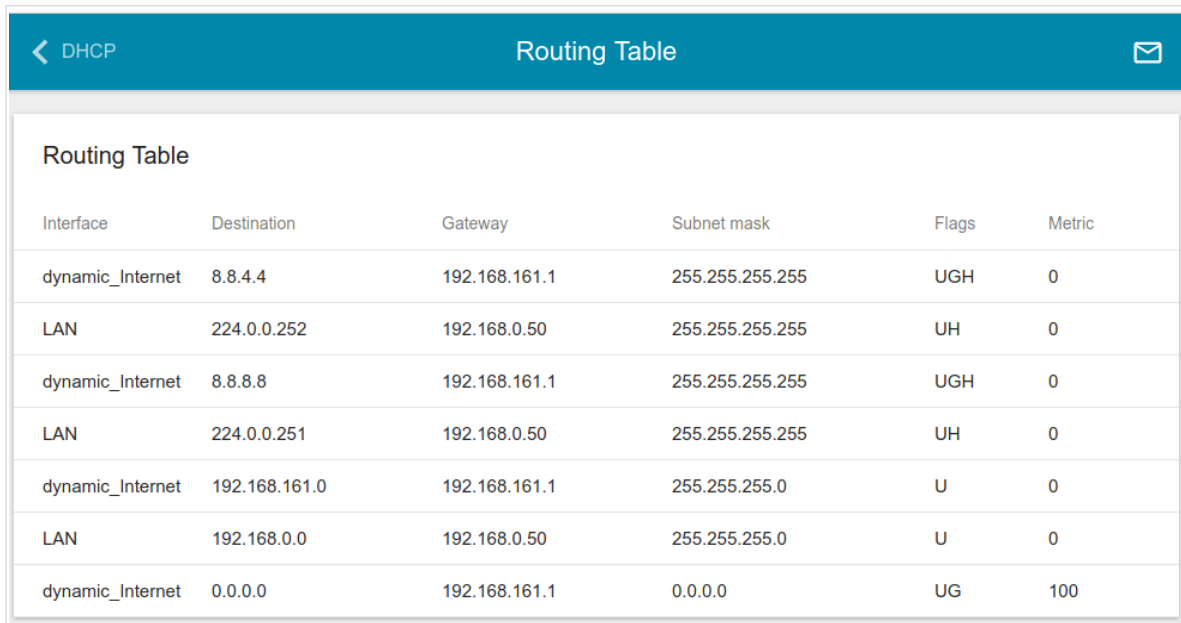
Hostname	IP address	MAC	Expires
android-3c39b96a4aabe085	192.168.0.3	80:01:84:16:0A:79	21h 52m 15s

Figure 47. The **Statistics / DHCP** page.

Routing Table

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

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

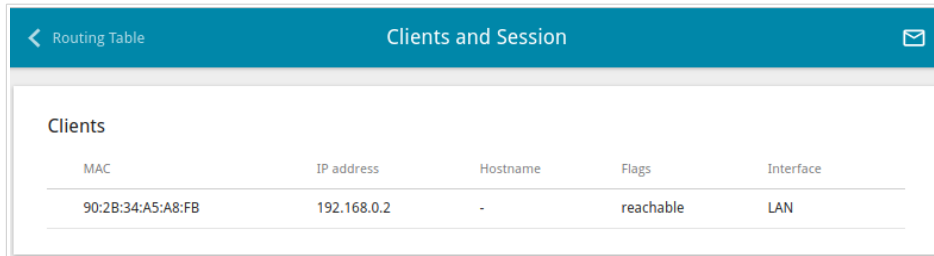


Interface	Destination	Gateway	Subnet mask	Flags	Metric
dynamic_Internet	8.8.4.4	192.168.161.1	255.255.255.255	UGH	0
LAN	224.0.0.252	192.168.0.50	255.255.255.255	UH	0
dynamic_Internet	8.8.8.8	192.168.161.1	255.255.255.255	UGH	0
LAN	224.0.0.251	192.168.0.50	255.255.255.255	UH	0
dynamic_Internet	192.168.161.0	192.168.161.1	255.255.255.0	U	0
LAN	192.168.0.0	192.168.0.50	255.255.255.0	U	0
dynamic_Internet	0.0.0.0	192.168.161.1	0.0.0.0	UG	100

Figure 48. The **Statistics / Routing Table** page.

Clients and Session

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



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

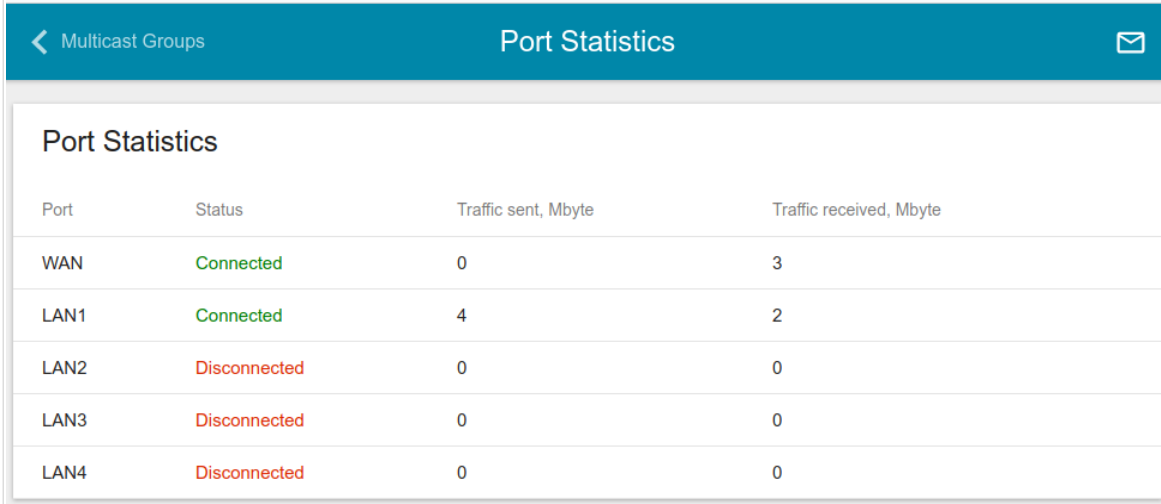
*Figure 49. The **Statistics / Clients and Session** page.*

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

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

Port Statistics

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



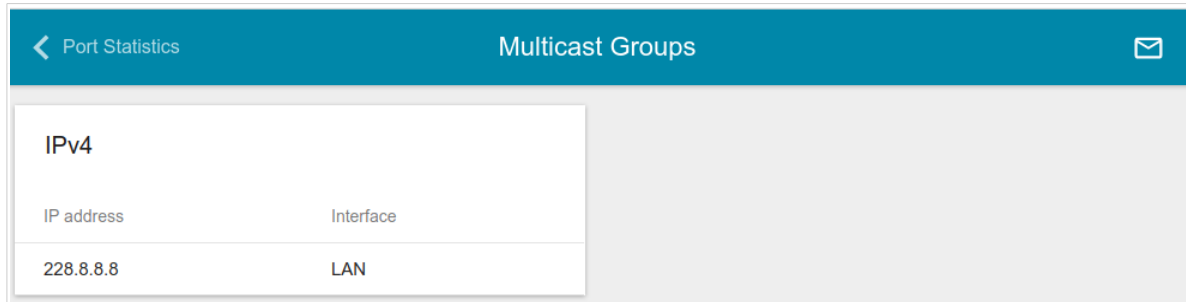
Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte
WAN	Connected	0	3
LAN1	Connected	4	2
LAN2	Disconnected	0	0
LAN3	Disconnected	0	0
LAN4	Disconnected	0	0

Figure 50. The **Statistics / Port Statistics** page.

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

Multicast Groups

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



IPv4	
IP address	Interface
228.8.8.8	LAN

Figure 51. 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).

WAN

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

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

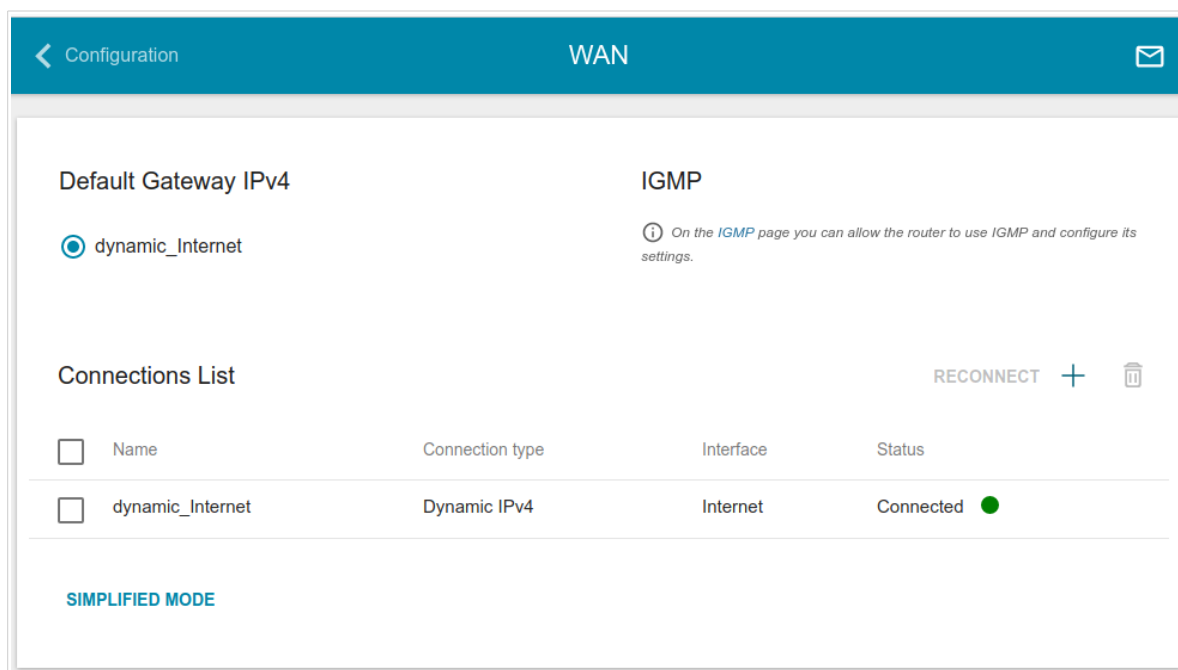



Figure 52. The **Connections Setup / WAN** page. The advanced mode.

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

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

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

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

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP** link (for the description of the page, see the **IGMP** section, page 125).

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

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

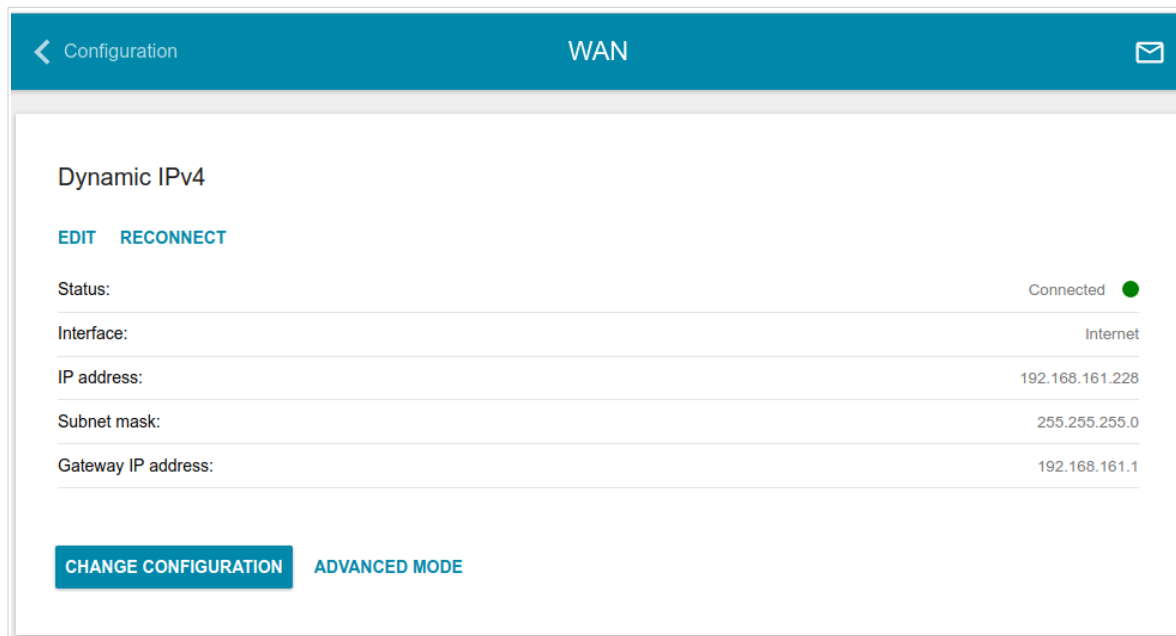


Figure 53. The **Connections Setup / WAN** page. The simplified mode.

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

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

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

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

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

Creating Dynamic IPv4 or Static IPv4 WAN Connection

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

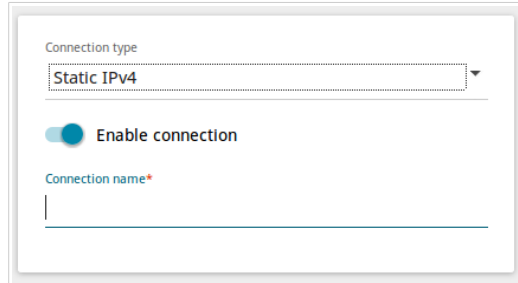


Figure 54. The page for creating a new **Static IPv4** connection. Selecting a connection type.

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

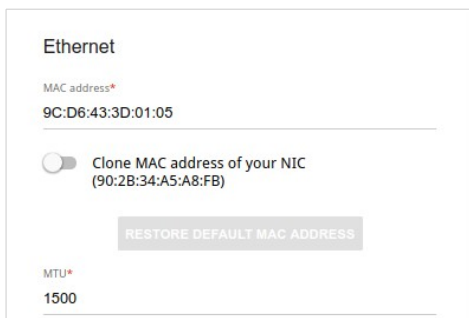


Figure 55. The page for creating a new **Static IPv4** connection. The **Ethernet** section.

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

IPv4

IP address*
192.168.161.240

Subnet mask*
255.255.255.0

Gateway IP address*
192.168.161.1

Primary DNS*
8.8.8.8

Secondary DNS
8.8.4.4

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

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

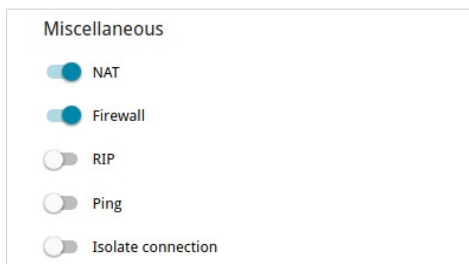


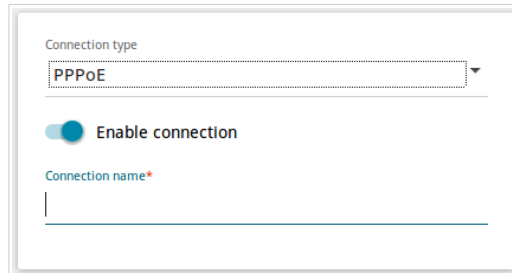
Figure 57. The page for creating a new **Static IPv4** connection. The **Miscellaneous** section.

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

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

Creating PPPoE WAN Connection

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



The screenshot shows a configuration form for a new PPPoE connection. At the top, there is a label 'Connection type' above a dropdown menu that currently displays 'PPPoE'. Below this is a toggle switch labeled 'Enable connection', which is currently turned on (indicated by a blue circle). At the bottom, there is a text input field labeled 'Connection name*' with a red asterisk indicating it is a required field.

Figure 58. The page for creating a new **PPPoE** connection. Selecting a connection type.

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



Figure 59. The page for creating a new **PPPoE** connection. The **Ethernet** section.

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

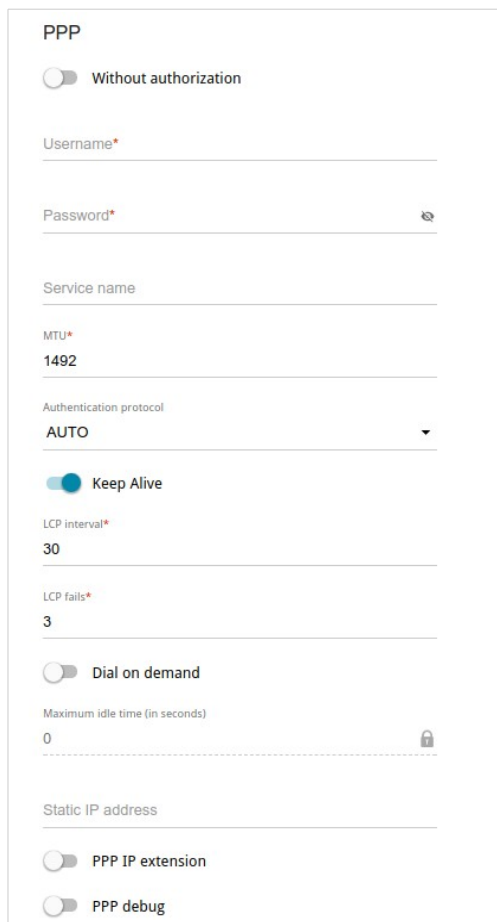


Figure 60. The page for creating a new **PPPoE** connection. The **PPP** section.

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

Parameter	Description
Dial on demand	Move the switch to the right if you want the access point to establish connection to the Internet on demand. In the Maximum idle time field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

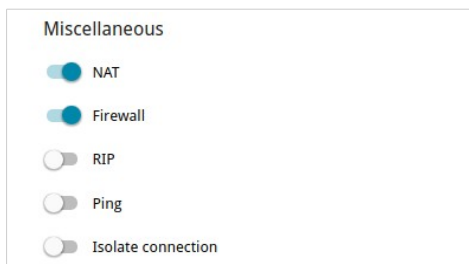


Figure 61. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.

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

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

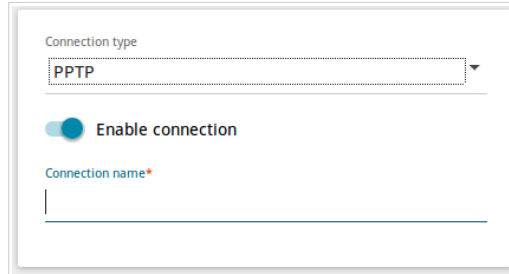
After clicking the button, the window for creating an additional connection opens.

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

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

Creating PPTP or L2TP WAN Connection

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



The screenshot shows a web interface for creating a connection. It features a dropdown menu labeled 'Connection type' with 'PPTP' selected. Below it is a toggle switch labeled 'Enable connection' which is currently turned on. At the bottom, there is a text input field labeled 'Connection name*'.


Figure 62. The page for creating a new **PPTP** connection. Selecting a connection type.

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

PPP

Without authorization

Username*

Password* 

VPN server address*

MTU*
1456

Authentication protocol
AUTO ▼


Encryption protocol
No encryption ▼

Keep Alive

LCP interval*
30

LCP fails*
3

Dial on demand

Maximum idle time (in seconds)
0 


Extra options

Static IP address

PPP debug

Enable MPPC

Figure 63. The page for creating a new PPTP connection. The PPP section.

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

Parameter	Description
Encryption protocol	Select a method of MPPE encryption. <ul style="list-style-type: none"> • No encryption: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. MPPE encryption can be applied only if the MS-CHAP , MS-CHAPV2 , or AUTO value is selected from the Authentication protocol drop-down list.
Keep Alive	Move the switch to the right if you want the access point to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the LCP interval and LCP fails fields are available. Specify the required values.
Dial on demand	Move the switch to the right if you want the access point to establish connection to the Internet on demand. In the Maximum idle time field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Extra options	Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional.</i>
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.
Enable MPPC	(<i>Microsoft Point-to-Point Compression</i>) For the PPTP type only. 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.

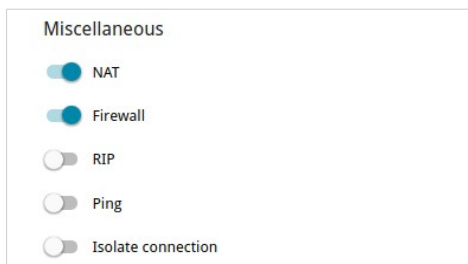


Figure 64. The page for creating a new PPTP connection. The **Miscellaneous** section.

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

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

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

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

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

Click the **OK** button.

LAN

To configure the router's local interface, go to the **Connections Setup / LAN** page. On this page, you can change IPv4 address, configure the built-in DHCP server, or specify MAC address and IP address pairs.

Local IP Address

IP address*
192.168.0.50

Mask*
255.255.255.0

Hostname
dlinkap.local

Figure 65. Configuring the local interface. The IPv4 tab. The **Local IP Address** section.

Parameter	Description
Local IP Address	
Mode of local IP address assignment	<p><i>For the Access point, Repeater, WDS, and Client modes only.</i></p> <p>Select the needed value from the drop-down list.</p> <p>Static: the IP address, subnet mask, and the gateway IP address are assigned manually.</p> <p>Dynamic: the access point automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.</p>
IP address	The IP address of the access point in the local subnet. By default, the following value is specified: 192 . 168 . 0 . 50 .
Mask	The mask of the local subnet. By default, the following value is specified: 255 . 255 . 255 . 0 .
Gateway IP address	<p><i>For the Access point, Repeater, WDS, and Client modes only.</i></p> <p>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></p>
Hostname	The name of the device assigned to its IP address in the local subnet.

Dynamic IP Addresses

Mode of dynamic IP address assignment

DHCP server ▼

Start IP*

192.168.0.100

End IP*

192.168.0.200

Lease time (in minutes)*

1440

DNS relay

Figure 66. Configuring the local interface. The IPv4 tab. The **Dynamic IP Addresses** section.

Parameter	Description
Dynamic IP Addresses	
Mode of dynamic IP address assignment	<p>An operating mode of the access point's DHCP server.</p> <p>Disable: the access point's DHCP server is disabled, clients' IP addresses are assigned manually.</p> <p>DHCP server: the access point assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the Start IP, End IP, Lease time fields and the DNS relay switch are displayed on the tab.</p> <p>DHCP relay: an external DHCP server is used to assign IP addresses to clients. When this value is selected, the External DHCP server IP and Option 82 Remote ID fields are displayed on the tab. <i>For the Router and WISP Repeater modes only.</i></p>
Start IP	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.

Parameter	Description
DNS relay	<p>Move the switch to the right so that the devices connected to the access point obtain the address of the access point as the DNS server address.</p> <p>Move the switch to the left so that the devices connected to the access point obtain the address transmitted by the ISP or specified on the Advanced / DNS page as the DNS server address.</p>
External DHCP server IP	<p>The IP address of the external DHCP server which assigns IP addresses to the access point's clients.</p> <p>To specify several IP addresses, click the ADD button, and in the line displayed, enter an IP address.</p> <p>To remove the IP address, click the Delete icon (✕) in the line of the address.</p>
Option 82 Remote ID	<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 **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 server** value is selected from the **Mode of dynamic IP address assignment** drop-down list).

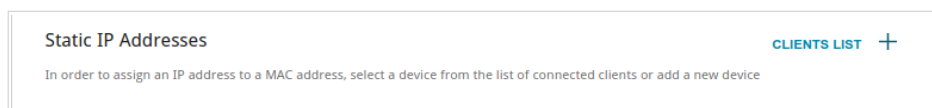



Figure 67. The section for creating MAC-IPv4 pairs.

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

In order to view MAC addresses of the devices connected to the access point at the moment, click the **CLIENTS LIST** button. In the opened window, select the needed device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

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

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

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.

The screenshot shows the 'Basic Settings' page for the Wi-Fi network configuration. The page is divided into two main sections: 'General Settings' and 'Wi-Fi Network'. The 'General Settings' section includes options to 'Enable Wireless', 'Country' (RUSSIAN FEDERATION), 'Wireless mode' (802.11 B), 'Select channel automatically', 'Enable additional channels', 'Channel' (auto (channel 13)), 'Enable periodic scanning', and 'Scanning period (in seconds)' (60). The 'Wi-Fi Network' section includes 'Network name (SSID)*' (DAP-1360-0505), 'Hide SSID', 'Max associated clients*' (0), 'Enable shaping', 'Broadcast wireless network', and 'Clients isolation'. Below these sections is the 'Security Settings' section, which includes 'Network authentication' (WPA2-PSK), 'Password PSK*', 'Encryption type*' (AES), and 'Group key update interval (in seconds)*' (3600). At the bottom of the page, there are two buttons: 'APPLY' and 'ADD WI-FI NETWORK'.

Figure 68. Basic settings of the wireless LAN.

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

Parameter	Description
Enable Wireless	To enable Wi-Fi connection, move the switch to the right. To disable Wi-Fi connection, move the switch to the left.
Country	The country you are in. Select a value from the drop-down list.
Wireless mode	Operating mode of the wireless network of the 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.
Select channel automatically	Move the switch to the right to let the access point itself choose the channel with the least interference.
Enable additional channels	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.
Channel	The wireless channel number. Left-click to open the window for selecting a channel (the action is available, when the Select channel automatically switch is moved to the left).
Enable periodic scanning	Move the switch to the right to let the access point search for a free channel in certain periods of time. When the switch is moved to the right, the Scanning period field is available for editing.
Scanning period	Specify a period of time (in seconds) after which the access point rescans channels.

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

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

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

The screenshot shows the 'Add Wi-Fi Network' configuration page. The page has a teal header with a back arrow, 'Basic Settings', 'Add Wi-Fi Network', and an envelope icon. The main content is split into two columns: 'Wi-Fi Network' and 'Security Settings'.
Wi-Fi Network
Network name (SSID)*: DAP-1360-0505.2
The number of characters should not exceed 32
 Hide SSID
Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point
Max associated clients*: 0
 Enable shaping
 Broadcast wireless network
Allows you to enable/disable broadcast of this SSID without disconnecting the wireless module of the router. Can be used with the mode "Wi-Fi Client"
 Clients isolation
Block traffic between devices connected to the access point
 Enable guest network
Enable the guest network in order to isolate Wi-Fi clients from the LAN network
Security Settings
Network authentication: WPA2-PSK
Password PSK*: [masked]
Password should be between 8 and 63 ASCII characters
Encryption type*: AES
Group key update interval (in seconds)*: 3600
An **APPLY** button is at the bottom left.

Figure 69. Creating a wireless network.

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

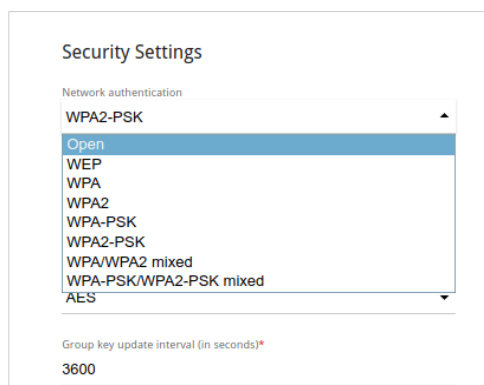


Figure 70. Network authentication types supported by the access point.

The access point supports the following authentication types:

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

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

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

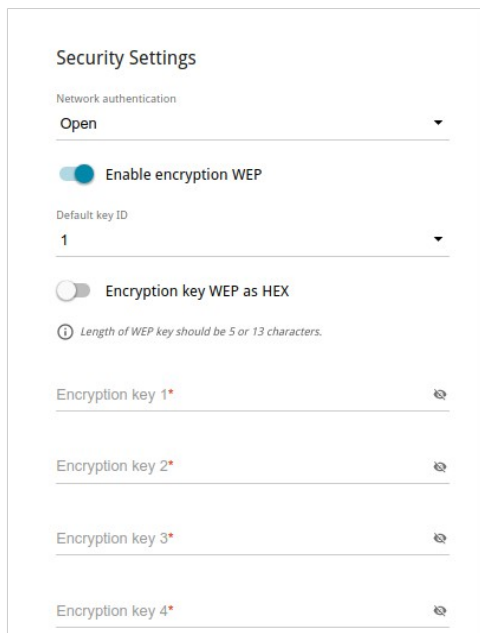



Figure 71. The **Open** value is selected from the **Network authentication** drop-down list.

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

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

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

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

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


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

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

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

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

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

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

Client Management

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

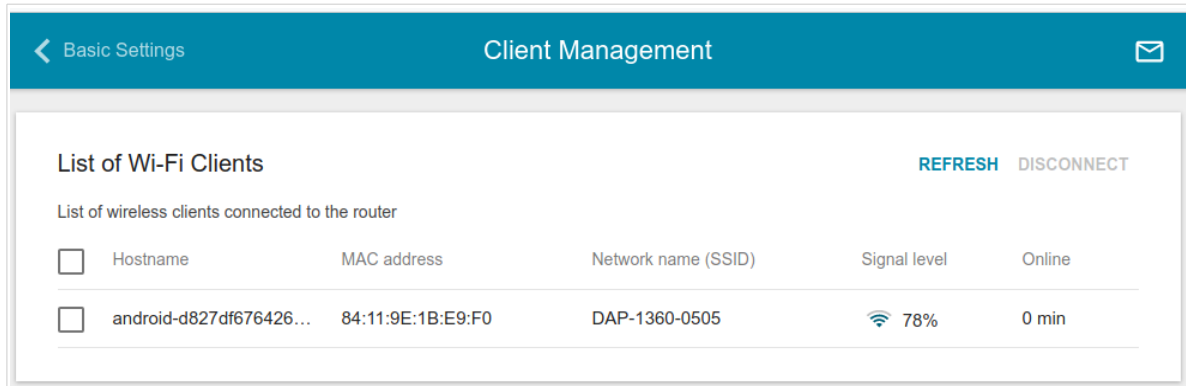


Figure 74. The page for managing the wireless clients.

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

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

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

WPS

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

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

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

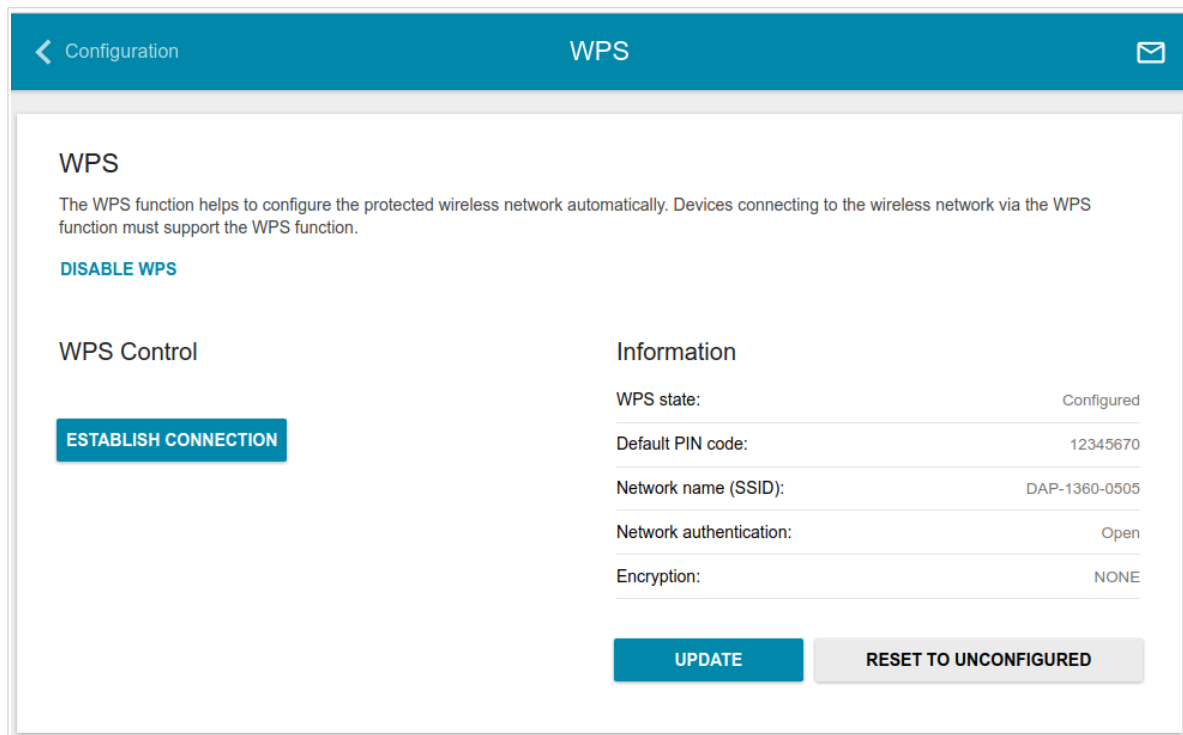


Figure 75. The page for configuring the WPS function.

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

Using WPS Function via Web-based Interface

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

1. 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.

Using WPS Function without Web-based Interface

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

1. Specify relevant security settings for the wireless network of the access point.
2. Click the **ENABLE WPS** button.
3. Save the settings and close the web-based interface (click the **Logout** line of the menu).

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

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

WDS

This page is available for the **Access point**, **Repeater**, **WDS**, and **Client** modes.

On the **Wi-Fi / WDS** page, you can enable the WDS function and select a mode of this function.

The WDS function allows joining local area networks together via a wireless connection of access points.

Figure 76. The page for configuring the WDS function.

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

- **Disable**: The function is disabled.
- **Bridge mode**: Access points communicate to each other only, wireless devices cannot connect to them.
- **Repeater mode**: Access points communicate to each other, wireless clients can connect to the WLAN created by interconnected access points.

You can specify the following parameters:

Parameter	Description
WDS Encryption	A type of encryption for data transfer between access points interconnected via the WDS function. Without encryption : No encryption. WEP . TKIP . AES .
Encryption Key	A key for the specified type of encryption. If the Without encryption value is selected from the WDS Encryption drop-down list, the field is not editable.

Parameter	Description
The MAC address of this point in 2.4 GHz	The MAC address of the access point.
AP MAC	<p>The MAC addresses of devices connected to the access point via the WDS function.</p> <p>To specify several MAC addresses, click the ADD button, and in the line displayed, enter a MAC address.</p> <p>To remove the MAC address, click the Delete icon (×) in the line of the address.</p>



The WDS function parameters specified on the page must be the same for all interconnected devices. In addition, it is required to set the same channel (on the **Wi-Fi / Basic settings** page).

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

WMM

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

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

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

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

The screenshot shows the WMM configuration page. At the top, there is a navigation bar with a back arrow, the text 'Configuration', the title 'WMM', and a mail icon. Below the navigation bar, the main content area is titled 'Wi-Fi Multimedia' and includes a descriptive sentence: 'The mechanism for improving Wi-Fi network performance. It is recommended for users not to change the specified values'. Underneath, there is a 'Work mode' section with a dropdown menu currently set to 'Manual'. The page is divided into two columns: 'Access Point' and 'Station'. Each column contains a table with the following parameters: AC, AIFSN, CWMin, CWMax, TXOP, ACM, and ACK. The values for these parameters are as follows:

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 77. 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.

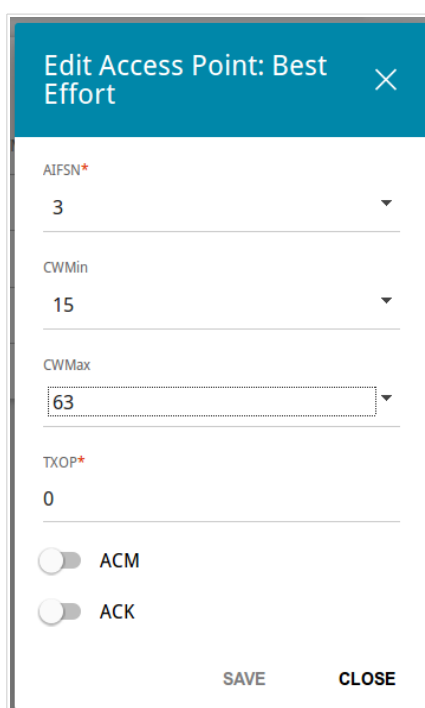


Figure 78. The window for changing parameters of the WMM function.

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

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

Click the **SAVE** button.

Client

This page is available for the **Router**, **Access point**, **WISP Repeater**, **Repeater**, and **Client** modes.

On the **Wi-Fi / Client** page, you can configure the device as a client to connect to a wireless access point or to a WISP.

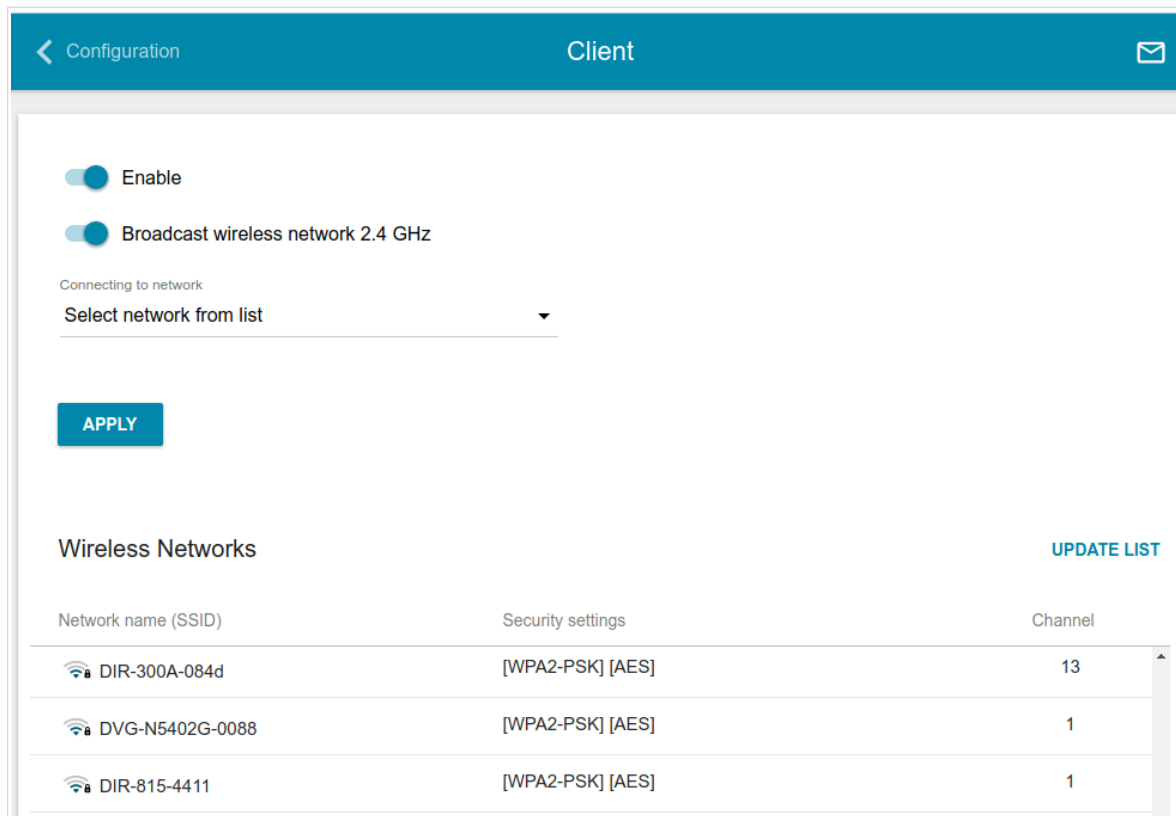


Figure 79. The page for configuring the client mode.

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


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

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

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

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

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

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

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

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

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

When connecting to a wireless access point, the wireless channel of DAP-1360U will switch to the channel of the access point to which you have connected.

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

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

Client Shaping

On the **Wi-Fi / Client Shaping** page, you can limit the maximum bandwidth of upstream and downstream traffic for each wireless client of the access point by its MAC address.

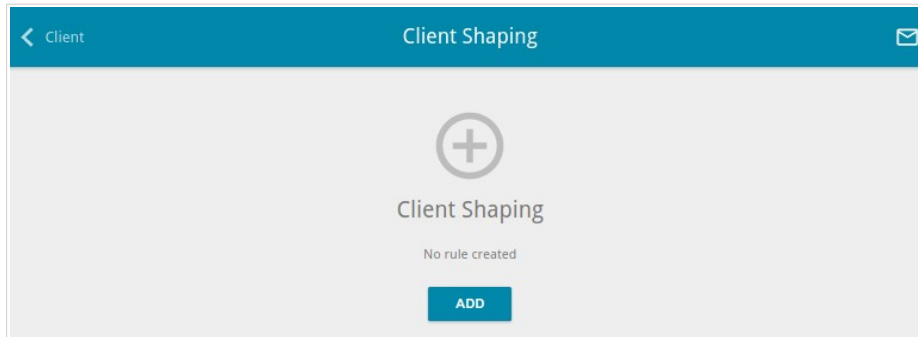


Figure 80. The **Wi-Fi / Client Shaping** page.

If you want to limit the maximum bandwidth of traffic for the access point's wireless client, create a relevant rule. To do this, click the **ADD** button (**+**).

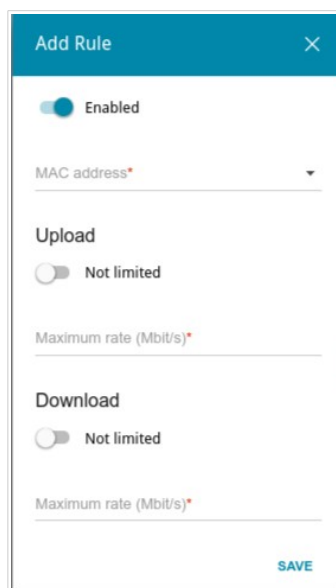



Figure 81. The window for setting up rate limit.

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

Parameter	Description
Enabled	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.
MAC address	In the field, enter the MAC address to which the rule will be applied. You can enter the MAC address of a device connected to the access point's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Upload	
Maximum rate	Specify the maximum value of the upstream traffic rate (Mbps) or move the Not limited switch to the right not to limit the maximum bandwidth of upstream traffic.
Download	
Maximum rate	Specify the maximum value of the downstream traffic rate (Mbps) or move the Not limited switch to the right not to limit the maximum bandwidth of downstream traffic.

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

To edit a rule, left-click the relevant rule. 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 in the table and click the **DELETE** button ().

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' configuration page for WLAN settings. The page has a teal header with a back arrow, 'Configuration', and 'Additional' text, and an envelope icon. The settings are organized into two columns:

- Left Column:**
 - Bandwidth: 20/40 MHz (dropdown)
 - Current bandwidth: 40 MHz (info icon)
 - Autonegotiation 20/40 (Coexistence):
 - TX power (in percent): 100 (dropdown)
 - B/G protection: Auto (dropdown)
 - Short GI: Enable (dropdown)
 - Drop multicast:
 - Adaptivity mode:
- Right Column:**
 - Beacon period (in milliseconds)*: 100
 - RTS threshold (in bytes)*: 2347
 - Frag threshold (in bytes)*: 2346
 - DTIM period (in beacon frames)*: 1
 - Station Keep Alive (in seconds)*: 0

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

Figure 82. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	<p>The channel bandwidth for 802.11n standard in the 2.4GHz band.</p> <p>20 MHz: 802.11n clients operate at 20MHz channels.</p> <p>20/40 MHz: 802.11n clients operate at 20MHz or 40MHz channels.</p>
Autonegotiation 20/40 (Coexistence)	<p>Move the switch to the right to let the access point to automatically choose the most suitable channel bandwidth (20MHz or 40MHz) for the connected devices (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the 20/40 MHz value is selected from the Bandwidth drop-down list.</p>
TX power	<p>The transmit power (in percentage terms) of the access point.</p>
B/G protection	<p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <p>Auto: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices).</p> <p>Always On: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</p> <p>Always Off: The protection function is always disabled.</p>
Short GI	<p>Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the access point is communicating to wireless devices.</p> <p>Enable: 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 Wireless mode drop-down list on the Wi-Fi / Basic Settings page).</p> <p>Disable: the access point uses the 800 ns standard guard interval.</p>
Drop multicast	<p>Move the switch to the right to disable multicasting for the access point's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected on the Advanced / IGMP page.</p>
Adaptivity mode	<p>Move the switch to the right to prevent your wireless network from interfering with radars and other mobile or stationary radio systems. Such a setting can slow down the access point's WLAN.</p>

Parameter	Description
Beacon period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS threshold	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.
Frag threshold	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).
DTIM period	The time period (in seconds) between sending a DTIM (a message notifying on broadcast or multicast transmission) and data transmission.
Station Keep Alive	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value 0 is specified, the checking is disabled.

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

MAC Filter

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

! It is recommended to configure the Wi-Fi MAC filter through a wired connection to DAP-1360U.

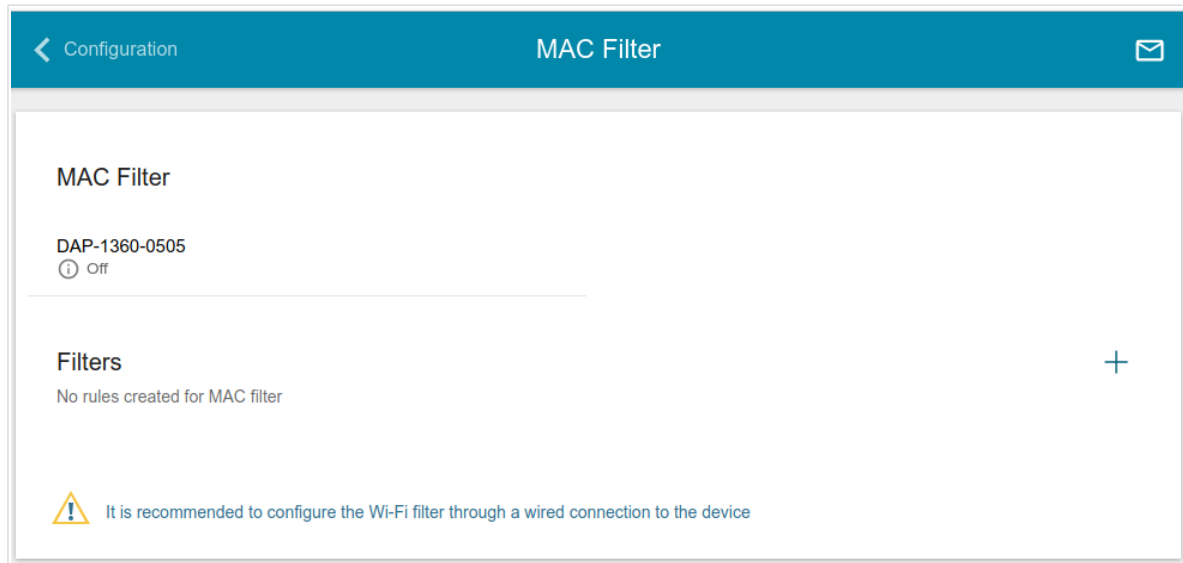


Figure 83. The page for configuring the MAC filter for the wireless network.

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 (**+**).

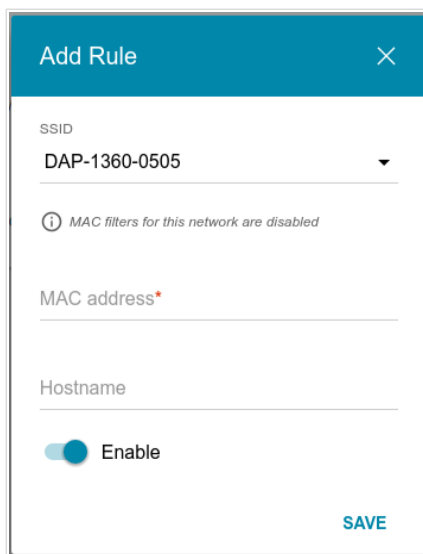



Figure 84. The window for adding a rule for the MAC filter.

You can specify the following parameters:

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

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

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

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

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, 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.

Roaming

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

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

Figure 85. The **Wi-Fi / Roaming** page.

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

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

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

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

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

Advanced

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

- create groups of ports for VLANs
- add name servers
- configure a DDNS service
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the access point
- setup the rate limit for traffic transmitted from every port of the access point
- define static routes
- create rules for remote access to the web-based interface
- enable the UPnP IGD protocol
- allow the access point to use IGMP
- allow the access point to use RTSP, enable the SIP ALG, the PPPoE/PPTP/L2TP/IPsec pass through functions for the access point.

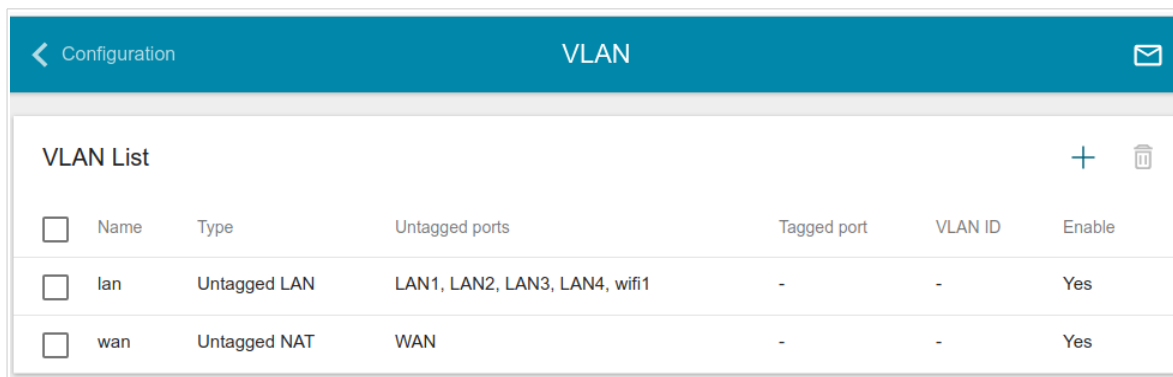
VLAN

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

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

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

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

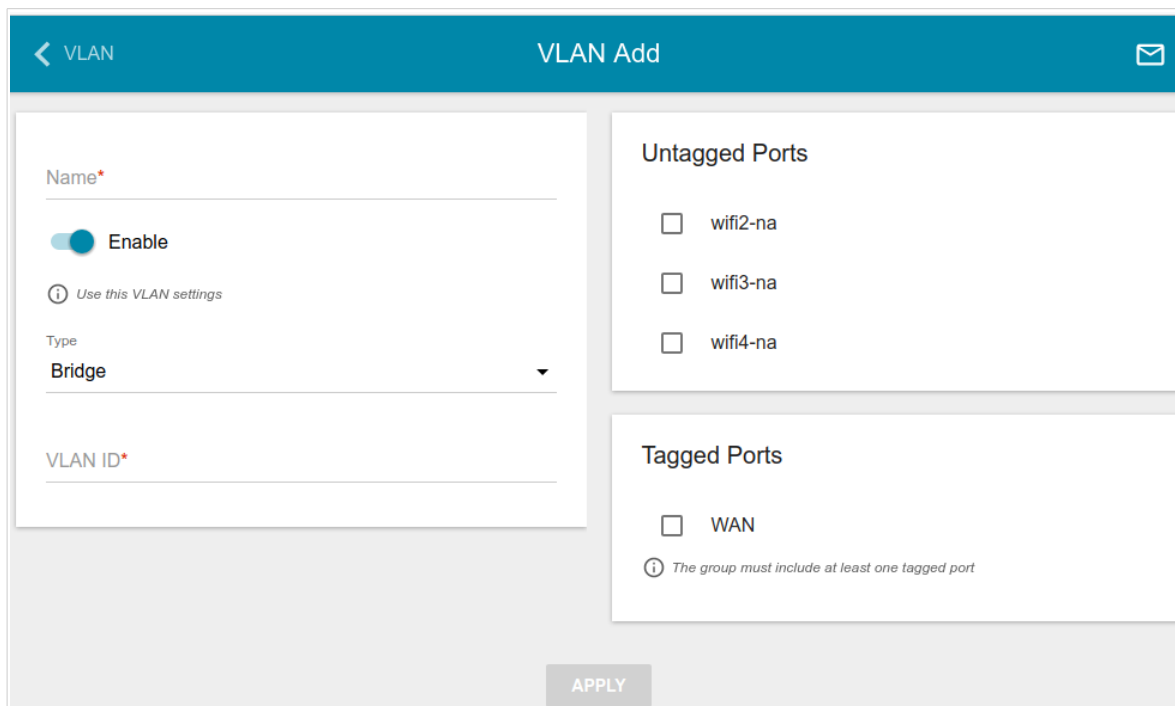


<input type="checkbox"/>	Name	Type	Untagged ports	Tagged port	VLAN ID	Enable
<input type="checkbox"/>	lan	Untagged LAN	LAN1, LAN2, LAN3, LAN4, wifi1	-	-	Yes
<input type="checkbox"/>	wan	Untagged NAT	WAN	-	-	Yes

Figure 86. The **Advanced / VLAN** page.

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

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



VLAN Add

Name*

Enable

Use this VLAN settings

Type
Bridge

VLAN ID*

Untagged Ports

wifi2-na

wifi3-na

wifi4-na

Tagged Ports

WAN

The group must include at least one tagged port

APPLY


Figure 87. The page for adding a group of ports for VLAN.

You can specify the following parameters:

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

Click the **APPLY** button.

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

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

DNS

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

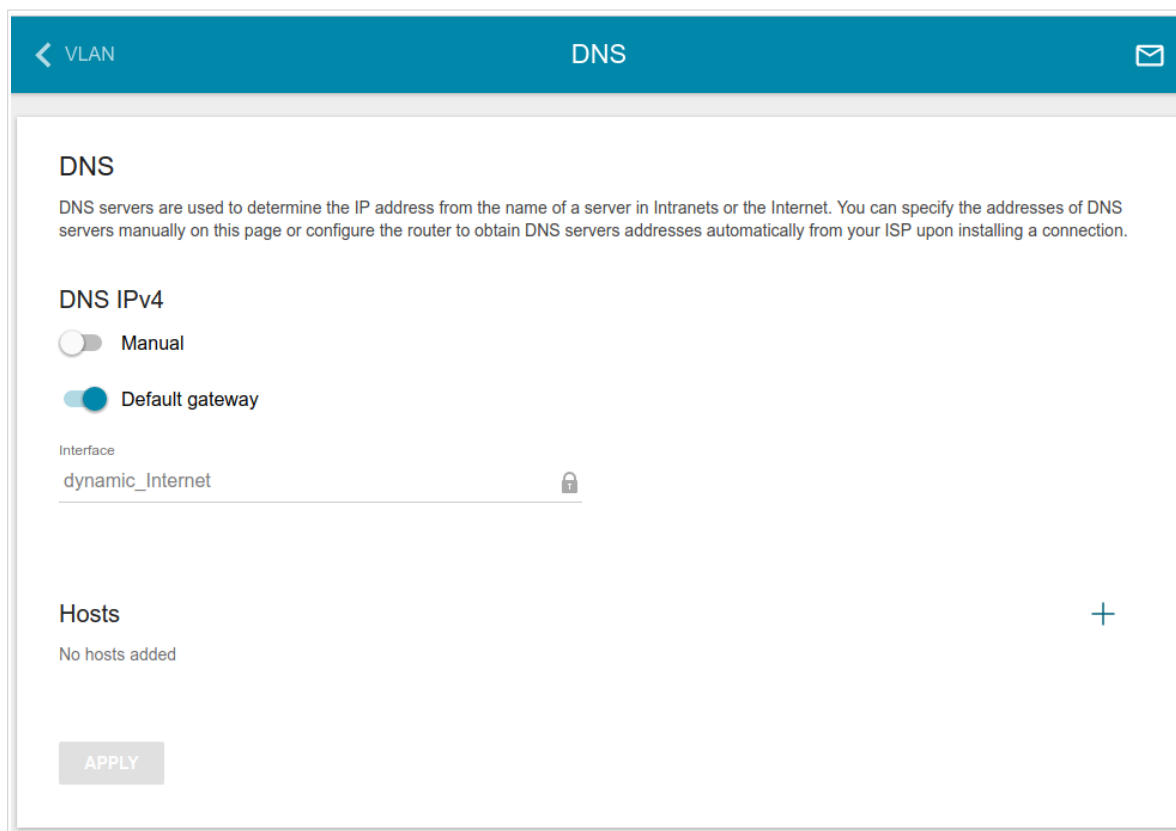


Figure 88. The **Advanced / DNS** page.

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.

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 IPv4** section, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server. Then click the **APPLY** button.

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

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

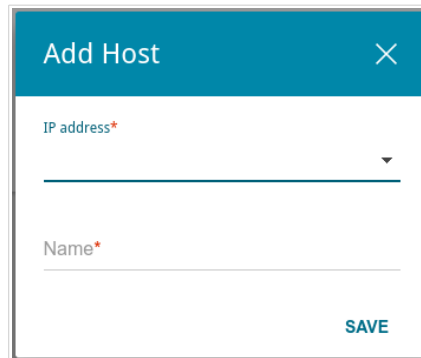



Figure 89. The window for adding a DNS record.

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

To edit an existing record, 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.

DDNS

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

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

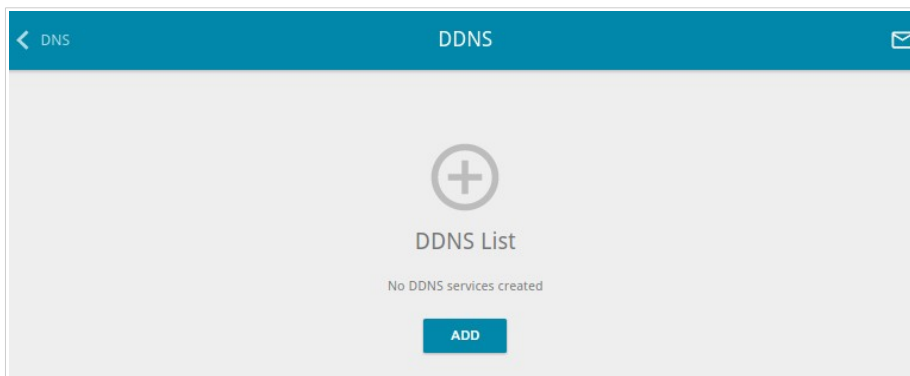



Figure 90. The **Advanced / DDNS** page.

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


Figure 91. The page for adding a DDNS service.

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

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

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

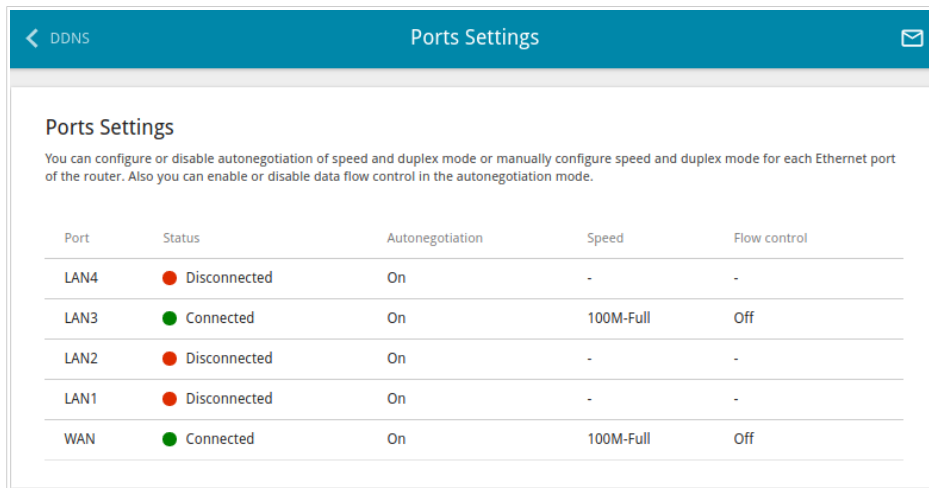
To edit parameters of the existing DDNS service, select the relevant line in the table. On the opened page, change the needed parameters and click the **SAVE** button.

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 ()

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
LAN4	Disconnected	On	-	-
LAN3	Connected	On	100M-Full	Off
LAN2	Disconnected	On	-	-
LAN1	Disconnected	On	-	-
WAN	Connected	On	100M-Full	Off

Figure 92. 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.

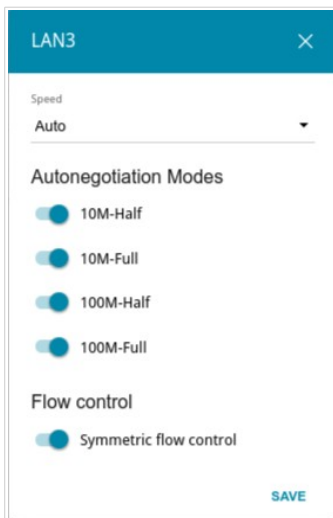


Figure 93. The window for changing the settings of the access point's port.

In the opened window, specify the needed parameters:

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

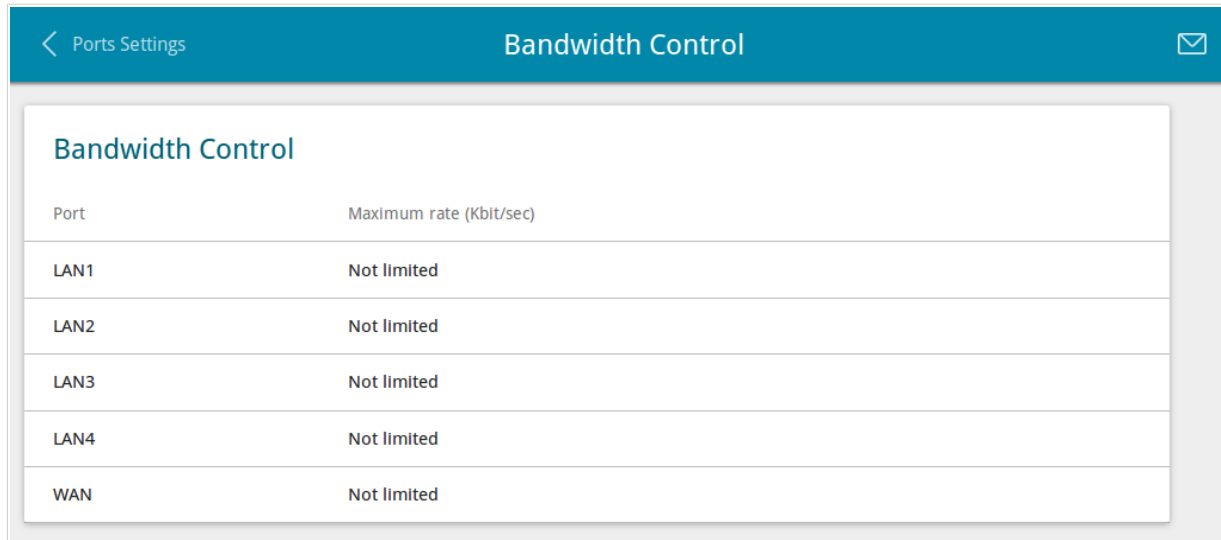
Parameter	Description
Flow control	
Symmetric flow control	Move the switch to the right to enable the flow control function for the port. Move the switch to the left to disable the flow control function for the port.

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

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

Bandwidth Control

On the **Advanced / Bandwidth Control** page, you can setup the rate limit for traffic transmitted from every port of the access point.



Port	Maximum rate (Kbit/sec)
LAN1	Not limited
LAN2	Not limited
LAN3	Not limited
LAN4	Not limited
WAN	Not limited

Figure 94. The **Advanced / Bandwidth Control** page.

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

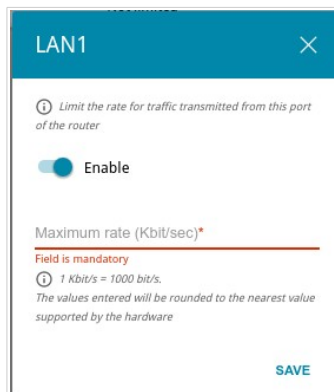


Figure 95. The window for setting up rate limit.

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

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

Routing

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

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

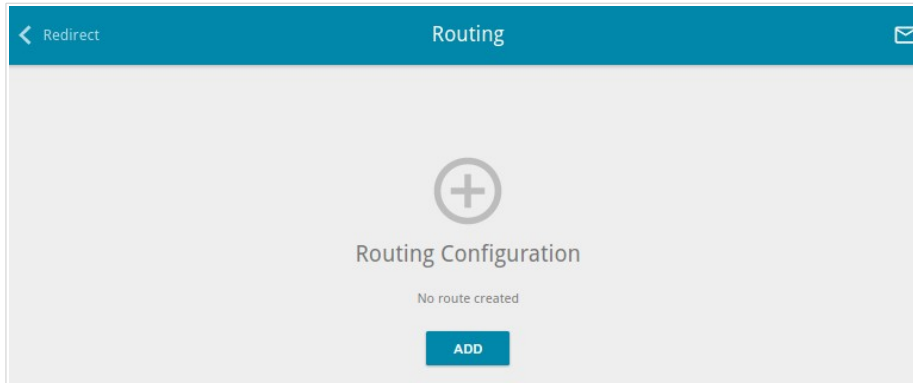


Figure 96. The **Advanced / Routing** page.

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

A screenshot of the 'Add route' dialog window. The window has a teal header with the title 'Add route' and a close 'X' button. The form contains five input fields: 'Interface*' with a dropdown menu showing 'Auto'; 'Destination network*'; 'Destination netmask*'; 'Gateway*'; and 'Metric'. A teal 'SAVE' button is located at the bottom right of the form.


Figure 97. The window for adding a new route.

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

Parameter	Description
Interface	From the drop-down list, select an interface through which the destination network can be accessed. If you have selected the Auto value, the access point itself sets the interface on the basis of data on connected networks.
Destination network	A destination network to which this route is assigned.
Destination netmask	The destination network mask.
Gateway	An IP address through which the destination network can be accessed.
Metric	A metric for the route. The lower the value, the higher is the route priority. <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 ().

Remote Access

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

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

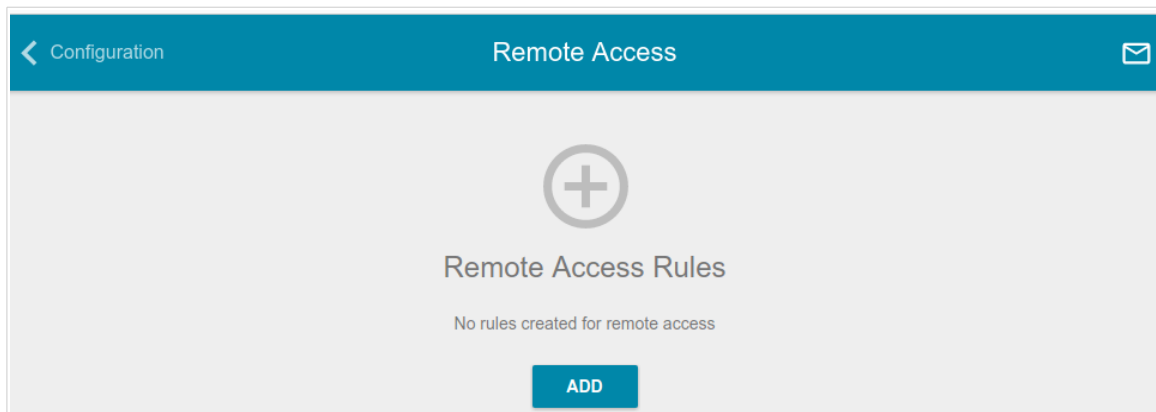


Figure 98. The **Advanced / Remote Access** page.

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

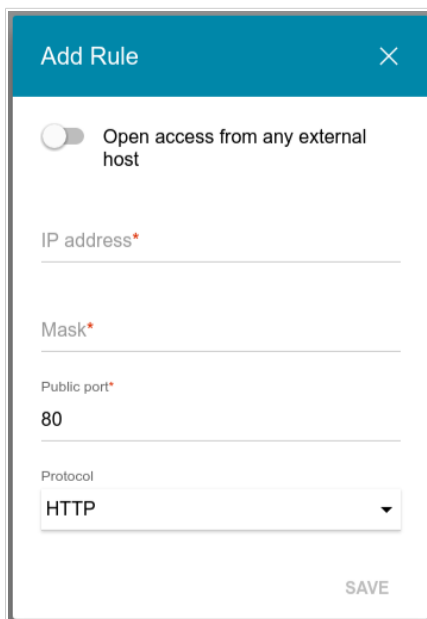


Figure 99. The window for adding a rule for remote management.


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

Parameter	Description
Open access from any external host	Move the switch to the right to allow access to the access point for any host. Upon that the IP address and Mask fields are not displayed.
IP address	A host or a subnet to which the rule is applied.

Parameter	Description
Mask	The mask of the subnet.
Public port	An external port of the access point. You can specify only one port.
Protocol	The protocol available for remote management of the access point.

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

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

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

UPnP IGD

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

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

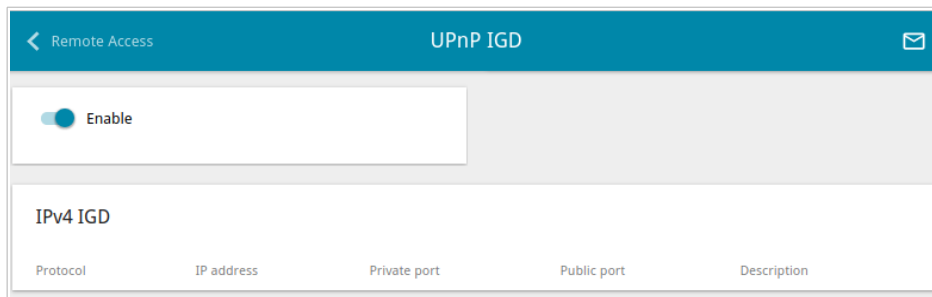


Figure 100. The **Advanced / UPnP IGD** page.

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

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

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

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

IGMP

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

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.

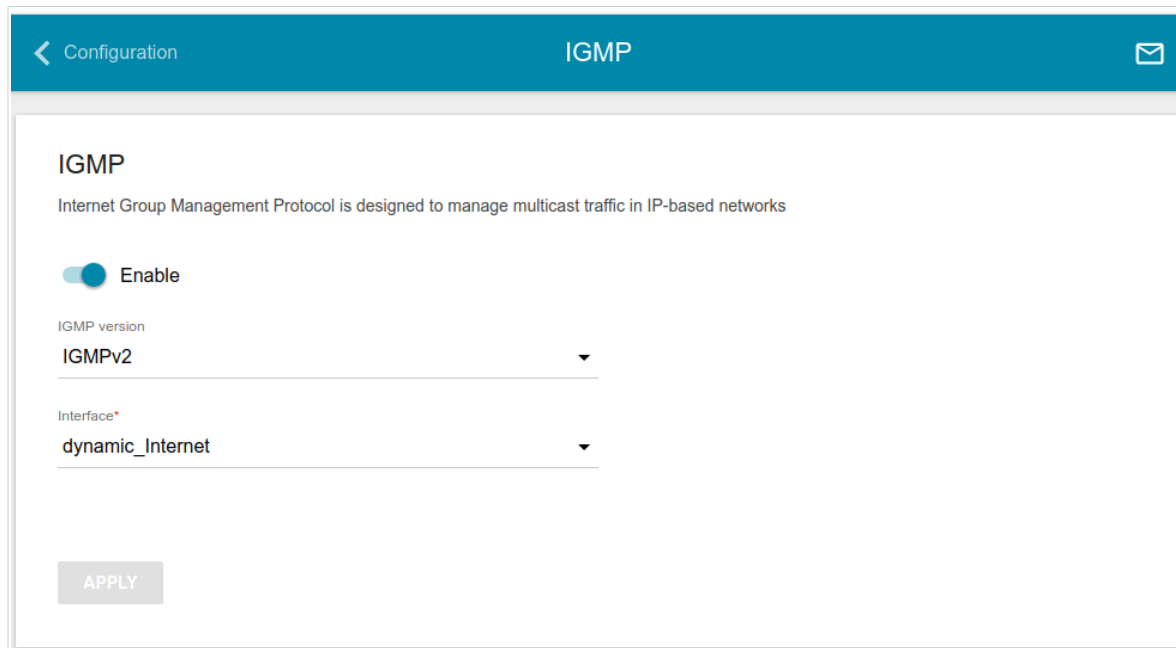


Figure 101. The **Advanced / IGMP** page.

The following elements are available on the page:

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

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

ALG/Passthrough

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

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

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

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

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

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

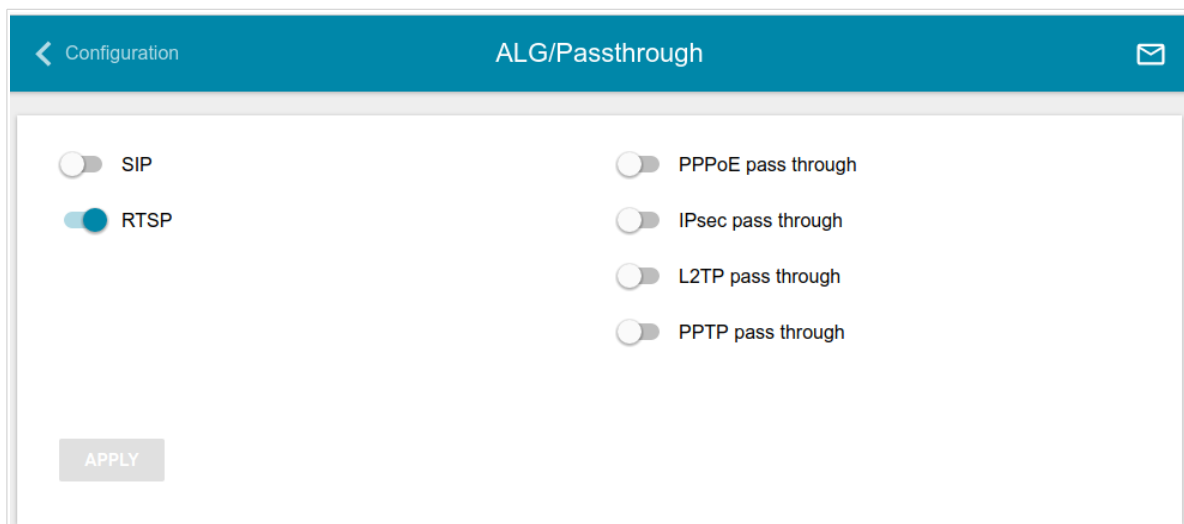


Figure 102. The **Advanced / ALG/Passthrough** page.

The following elements are available on the page:

Parameter	Description
SIP	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled access point. ³
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.

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

³ On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / 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 for the **Router** and **WISP Repeater** modes.

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

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

IP Filter

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

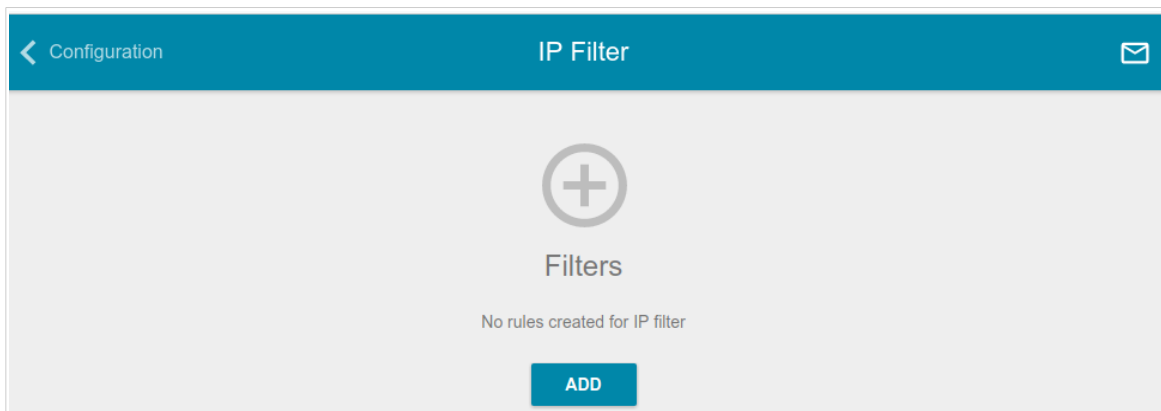


Figure 103. The **Firewall / IP Filter** page.

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

Figure 104. The page for adding a rule for IP filtering.


You can specify the following parameters:

Parameter	Description
General settings	
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Name	A name for the rule for easier identification. You can specify any name.
Action	Select an action for the rule. Allow: Allows packet transmission in accordance with the criteria specified by the rule. Deny: Denies packet transmission in accordance with the criteria specified by the rule.

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

Click the **APPLY** button.

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

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

Virtual Servers

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

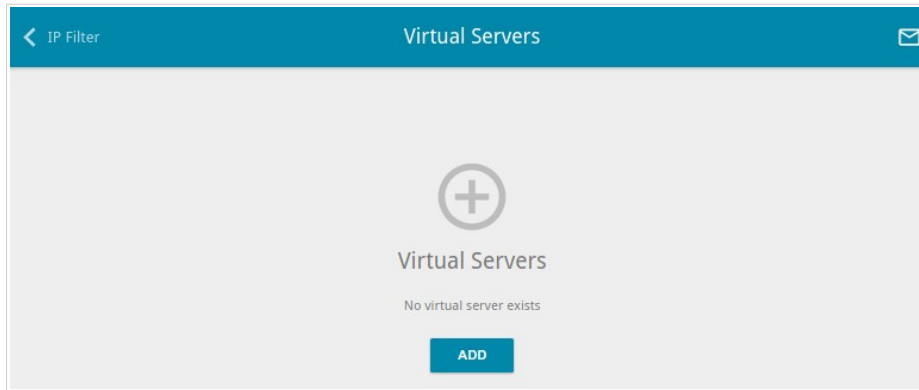



Figure 105. The **Firewall / Virtual Servers** page.

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

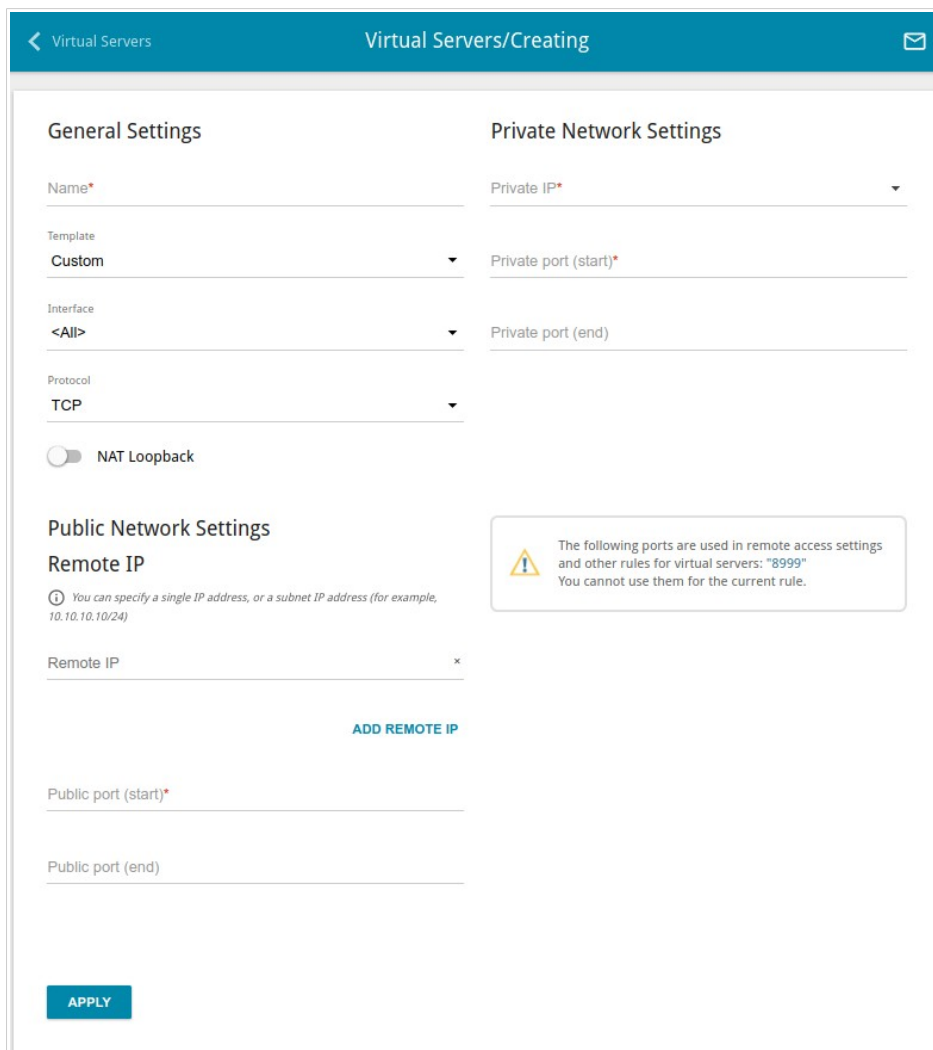


Figure 106. The page for adding a virtual server.


You can specify the following parameters:

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

Parameter	Description
Private port (start)/ Private port (end)	A port of the IP address specified in the Private IP field to which traffic is directed from the Public port . Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the Private port (start) field and leave the Private port (end) field blank.

Click the **APPLY** button.

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

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

DMZ

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

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

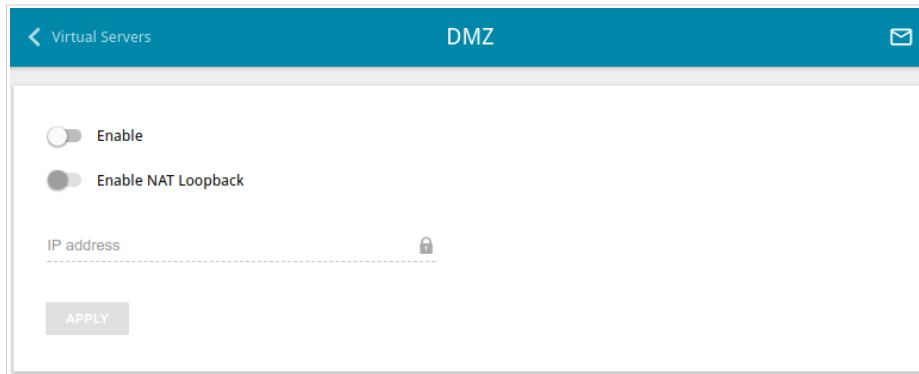


Figure 107. The **Firewall / DMZ** page.

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.

MAC Filter

On the **Firewall / MAC Filter** page, you can configure MAC-address-based filtering for computers of the access point's LAN.

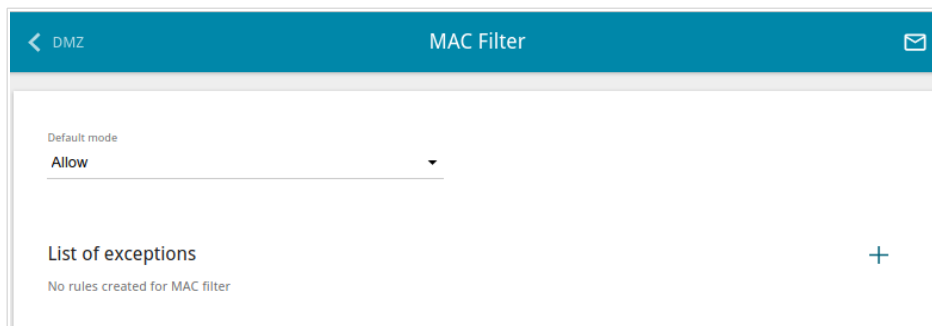


Figure 108. The **Firewall / MAC Filter** page.

Select the needed action from the drop-down list in the **Default mode** section to configure filtering for all devices of the 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 (**+**).

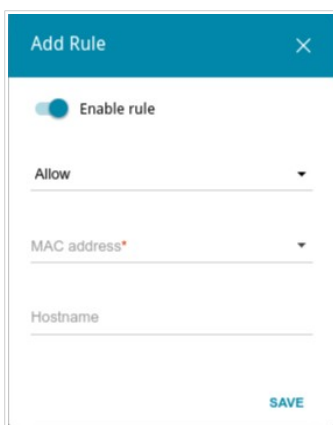



Figure 109. The window for adding a rule for the MAC filter.

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

Parameter	Description
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. Deny: Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices. Allow: Allows access to the access point's network and to the Internet for the device with the specified MAC address even if the default mode denies access for all devices.
MAC address	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).
Hostname	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.

URL Filter

On the **Firewall / URL Filter** page, you can specify restrictions on access to certain web sites and define devices to which the specified restrictions will be applied.

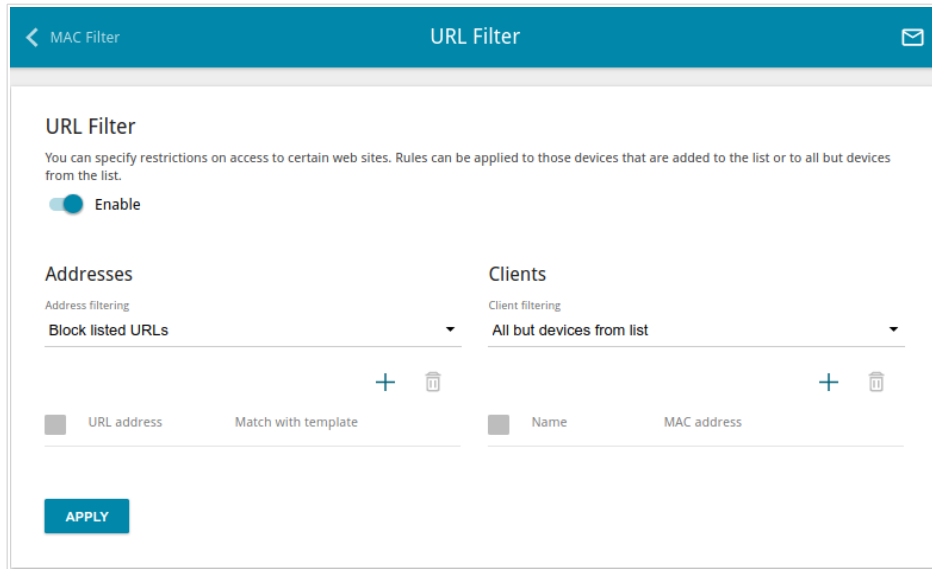




Figure 110. The **Firewall / URL Filter** page.

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

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


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


Parameter	Description
URL address	A URL address, a part of URL address, or a keyword.
Match with template	<p>Select a value from the drop-down list.</p> <p>Full: The request address should exactly match the value specified in the field above.</p> <p>Begin: The request address should begin with the value specified in the field above.</p> <p>End: The request address should end with the value specified in the field above.</p> <p>Partly: The request address should contain the value specified in the field above in any part of it.</p>

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

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

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

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

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

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

System

In this menu you can do the following:

- change the password used to access the access point's settings
- restore the factory default settings
- create a backup of the access point's configuration
- restore the access point's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the access point
- change the web-based interface language
- update the firmware of the access point
- configure automatic notification on new firmware version
- view the system log; configure sending the system log to a remote host
- check availability of a host on the Internet through the web-based interface of the access point
- trace the route to a host
- allow or forbid access to the access point via TELNET
- 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, or change the web-based interface language.

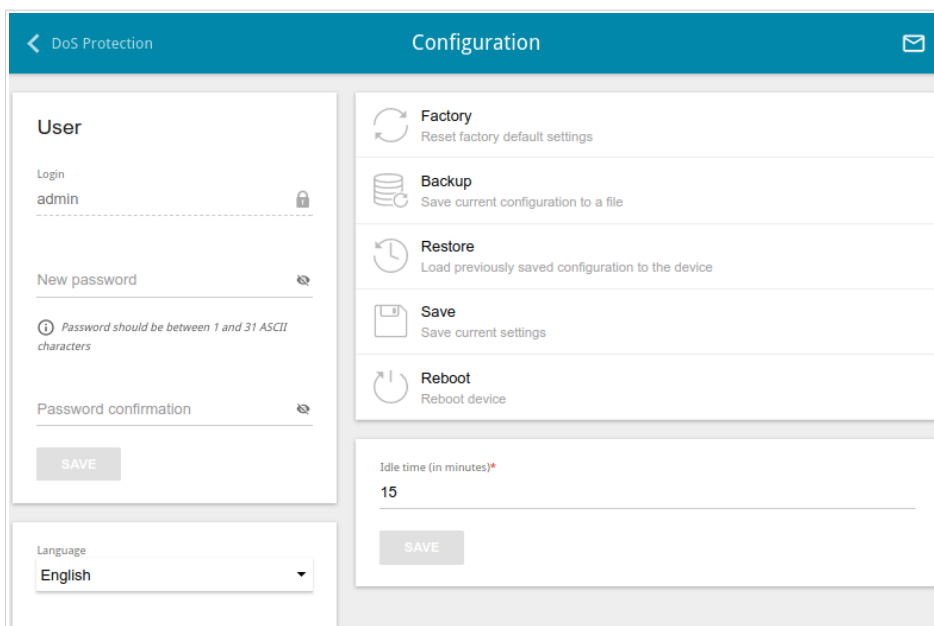


Figure 111. The **System / Configuration** page.

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.⁴ Click the **Show** icon (👁) to display the entered values. Then click the **SAVE** button.



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

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

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

The following buttons are also available on the page:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button (see the <i>Back and Bottom Panels</i> section, page 10).
Backup	Click the button to save the configuration (all settings of the access point) to your PC. The configuration backup will be stored in the download location of your web browser.
Restore	Click the button and follow the dialog box appeared to select a previously saved configuration file (all settings of the access point) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The access point saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

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

Firmware Update

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

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

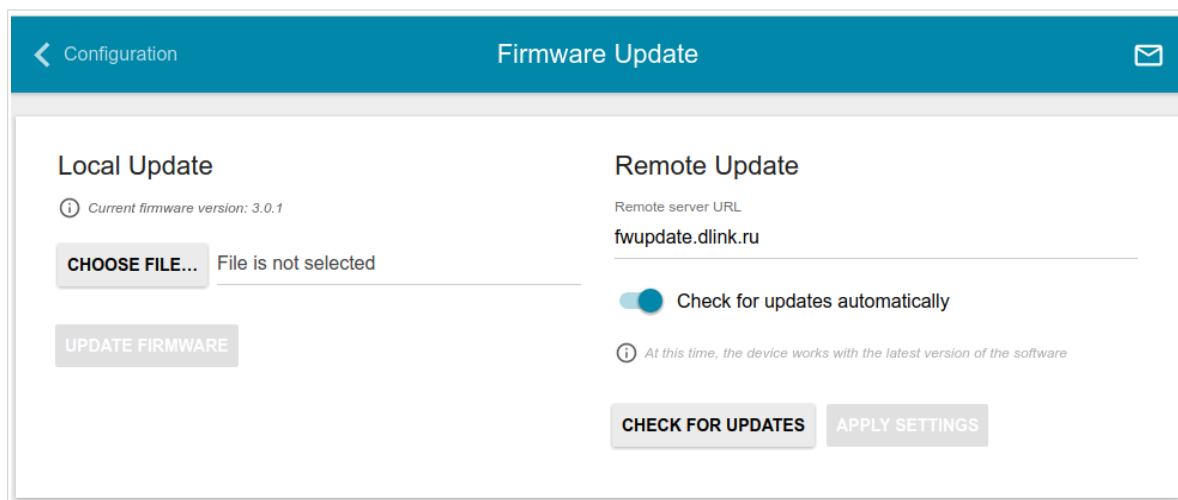


Figure 112. The **System / Firmware Update** page.

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.
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.

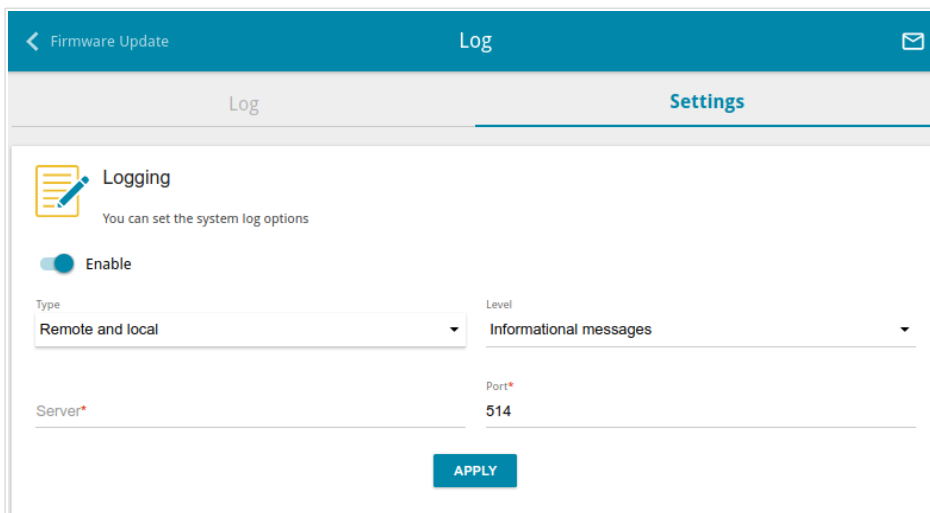


Figure 113. The **System / Log** page. The **Settings** tab.

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

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

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

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

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

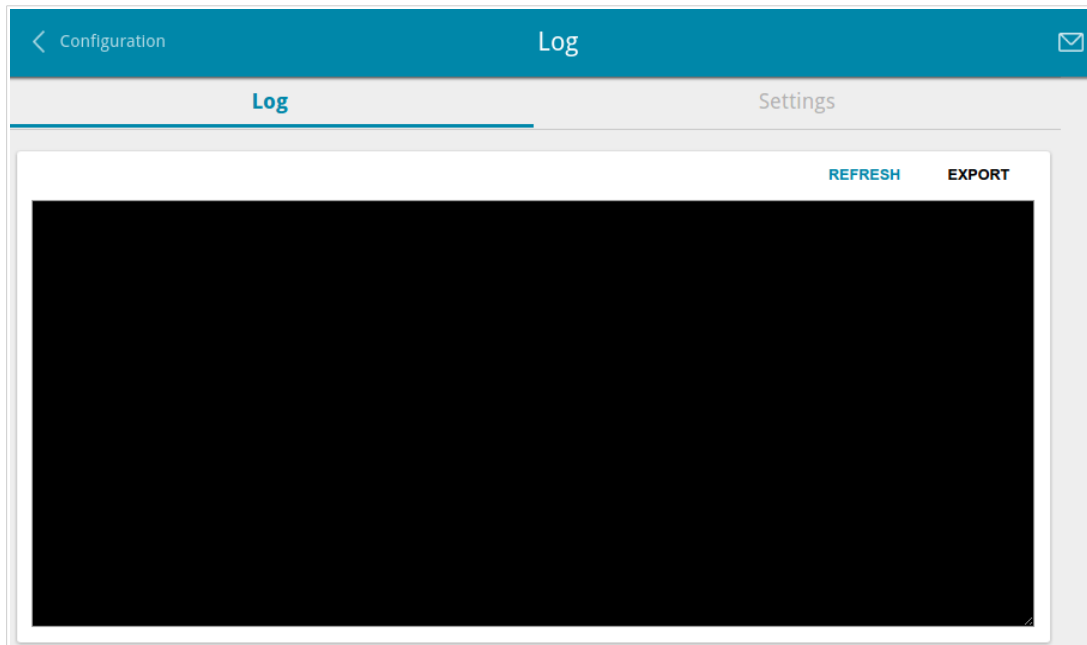


Figure 114. The **System / Log** page. The **Log** tab.

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.

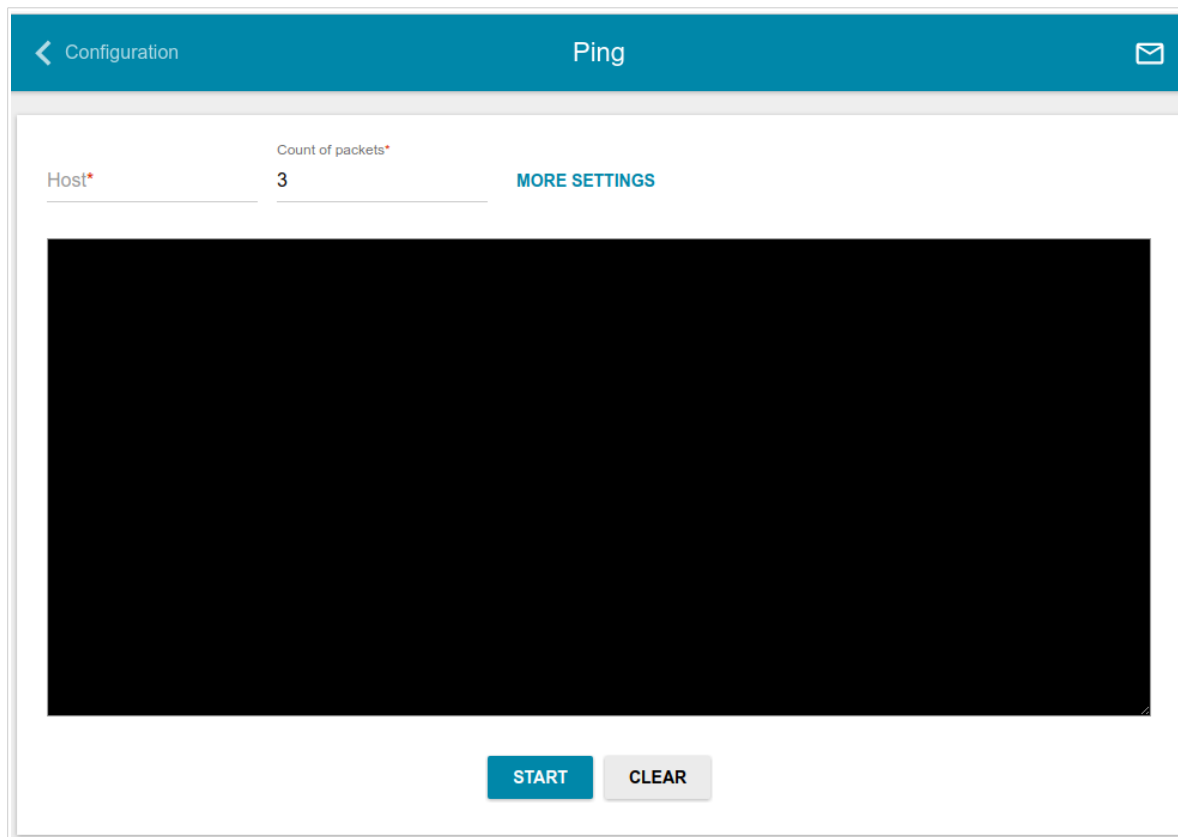


Figure 115. The **System / Ping** page.

To check availability of a host, enter the IP address or name of this host in the **Hostname** field and specify a number of requests that will be sent in order to check its availability in the **Count of packets** field.

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

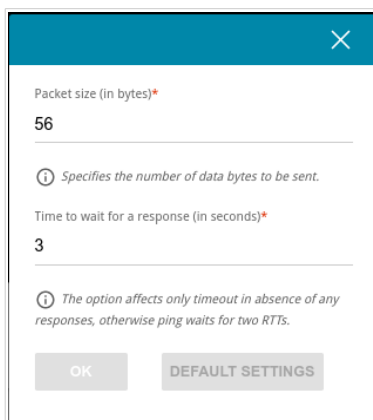


Figure 116. The **System / Ping** page. The additional settings window.

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

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

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

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

Traceroute

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

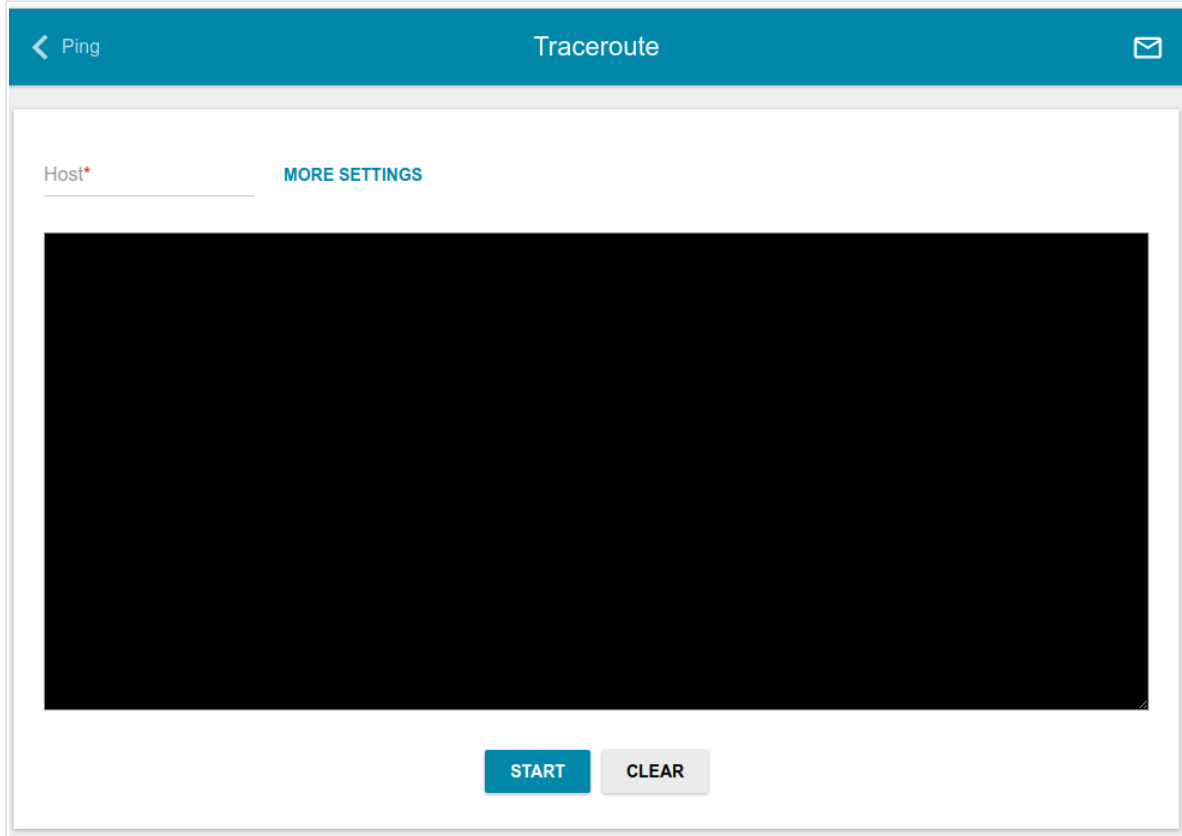
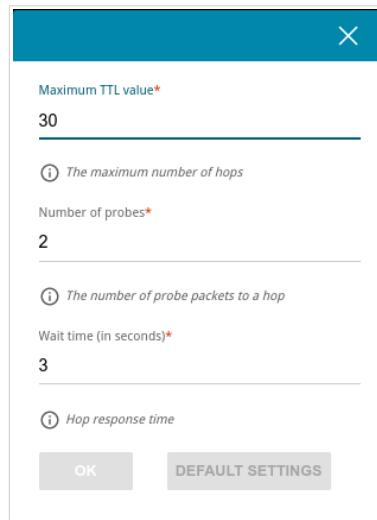


Figure 117. The **System / Traceroute** page.

To determine the route, enter the name or IP address of a host in the **Hostname** field.

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



Maximum TTL value*
30
 ⓘ The maximum number of hops

Number of probes*
2
 ⓘ The number of probe packets to a hop

Wait time (in seconds)*
3
 ⓘ Hop response time

OK DEFAULT SETTINGS

Figure 118. The **System / Traceroute** page. The additional settings window.

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

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

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

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

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

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.

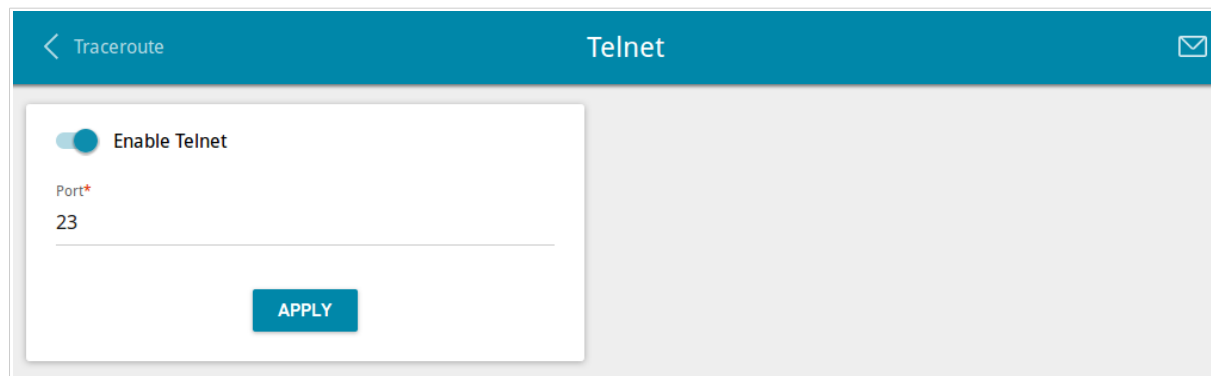


Figure 119. The **System / Telnet** page.

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.

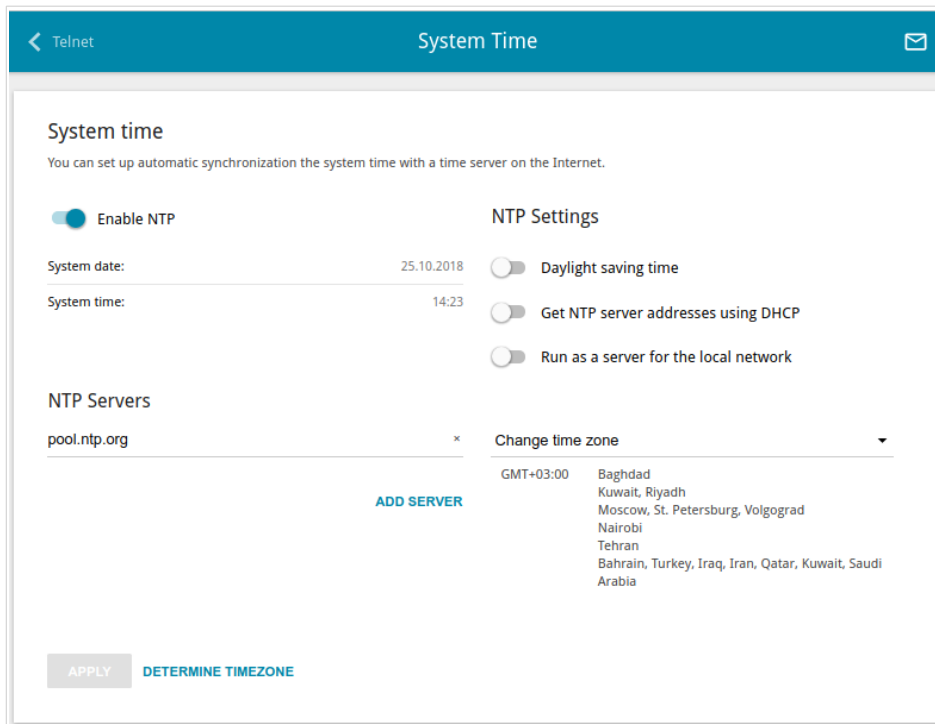


Figure 120. The **System / System Time** page.

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 **Change time zone** drop-down list in the **NTP Settings** section. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.
4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

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

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

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



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

CHAPTER 5. OPERATION GUIDELINES

Safety Rules and Conditions

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

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

Plug the device only into working electrical outlets with parameters indicated on the device.

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

The service life of the device is 2 years.

Wireless Installation Considerations

The DAP-1360U 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-1360U device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).
2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your access point and wireless network devices so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your access point away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone is not in use.

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

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

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