



DAP-1360U

Wireless N300 Access Point & Router

Contents

Chapter 1. Introduction	5
Contents and Audience	5
Conventions	5
Document Structure	5
Chapter 2. Overview	6
General Information	6
Specifications	7
Product Appearance	10
Top Panel	10
Back and Bottom Panels	11
Delivery Package	12
Chapter 3. Installation and Connection	13
Before You Begin	13
Connecting to PC	14
PC with Ethernet Adapter	14
Configuring IP Address in OS Windows XP	14
Configuring IP Address in OS Windows 7	17
PC with Wi-Fi Adapter	22
Configuring Wi-Fi Adapter in OS Windows XP	23
Configuring Wi-Fi Adapter in OS Windows 7	25
Connecting to Web-based Interface	28
Web-based Interface Structure	29
Access Point Mode	30
Router Mode	32
Notifications and System Drop-down Menu	34
Device Operation Modes	36
Access Point Mode	36
Router Mode	36
Chapter 4. Configuring Device (Access Point Mode)	37
Wireless Network Settings Wizard	37
Access Point Mode	38
Repeater Mode	40
Client Mode	43
Status	46
Network Statistics	46
DHCP	47
Clients	48
Multicast groups	49
Net	50
LAN	50
Wi-Fi	53
Basic Settings	53
Security Settings	55
MAC Filter	60
List of Wi-Fi Clients	62
WPS	63
<i>Using WPS Function via Web-based Interface</i>	<i>65</i>
<i>Using WPS Function without Web-based Interface</i>	<i>65</i>
WDS	67
Additional Settings	69
WMM	71
Client	73

Advanced	77
DNS.....	77
System	78
Administrator Password.....	79
Configuration.....	80
System Log.....	82
Firmware Upgrade.....	84
<i>Local Update</i>	85
<i>Remote Update</i>	86
System Time.....	87
Ping.....	88
Traceroute.....	89
Telnet.....	90
Device mode.....	91
Chapter 5. Configuring Device (Router Mode)	92
Monitoring	92
Click'n'Connect	96
Creating WAN Connection.....	98
<i>PPPoE Connection</i>	98
<i>Static IP Connection</i>	99
<i>Dynamic IP Connection</i>	100
<i>PPPoE + Static IP Connection</i>	101
<i>PPPoE + Dynamic IP Connection</i>	104
<i>PPTP + Static IP or L2TP + Static IP Connection</i>	106
<i>PPTP + Dynamic IP or L2TP + Dynamic IP Connection</i>	109
Checking Internet Availability.....	111
Configuring Wireless Connection.....	112
<i>Access Point Mode</i>	113
<i>Repeater Mode</i>	115
Wireless Network Settings Wizard	118
Access Point Mode.....	119
Repeater Mode.....	121
Client Mode.....	124
Virtual Server Settings Wizard	127
Status	129
Network Statistics.....	129
DHCP.....	130
Routing Table.....	131
Clients.....	132
Multicast groups.....	133
Net	134
WAN.....	134
<i>Creating PPPoE WAN Connection</i>	135
<i>Creating Static IP or Dynamic IP WAN Connection</i>	139
<i>Creating PPPoE + Static IP or PPPoE + Dynamic IP WAN Connection</i>	143
<i>Creating PPTP/L2TP + Static IP or PPTP/L2TP + Dynamic IP WAN Connection</i>	149
LAN.....	156

Wi-Fi	158
Basic Settings.....	158
Security Settings.....	160
MAC Filter.....	165
List of Wi-Fi Clients.....	167
WPS.....	168
<i>Using WPS Function via Web-based Interface</i>	170
<i>Using WPS Function without Web-based Interface</i>	170
WDS.....	172
Additional Settings.....	174
WMM.....	176
Client.....	178
Advanced	182
UPnP IGD.....	183
DDNS.....	184
DNS.....	186
Routing.....	187
Remote Access to Device.....	188
Miscellaneous.....	190
Firewall	192
IP Filters.....	192
Virtual Servers.....	195
DMZ.....	198
MAC Filter.....	199
Control	201
URL Filter.....	201
System	203
Administrator Password.....	204
Configuration.....	205
System Log.....	207
Firmware Upgrade.....	209
<i>Local Update</i>	210
<i>Remote Update</i>	211
System Time.....	212
Ping.....	213
Traceroute.....	214
Telnet.....	215
Device mode.....	216
Chapter 6. Operation Guidelines	217
Safety Instructions	217
Wireless Installation Considerations	217
Chapter 7. Abbreviations and Acronyms	218


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 DAP-1360U device and configure a PC in order to access its web-based interface.

Chapter 4 describes all pages of the web-based interface for the device in the access point mode.

Chapter 5 describes all pages of the web-based interface for the device in the router mode.

Chapter 6 includes safety instructions and tips for networking.

Chapter 7 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.

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.

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.

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 several languages).

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	
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 secure 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	
Operation Modes	<ul style="list-style-type: none"> · Access point mode · Router mode
WAN connection types	<ul style="list-style-type: none"> · PPPoE · Static IP / Dynamic IP · PPPoE + Static IP · PPPoE + Dynamic IP · PPTP/L2TP + Static IP · PPTP/L2TP + Dynamic IP
Network functions	<ul style="list-style-type: none"> · DHCP server/relay · DNS relay · Dynamic DNS · Static IP routing · IGMP Proxy · RIP · Support of UPnP IGD · WAN ping respond · Support of SIP ALG · Support of RTSP
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) · Multilingual web-based interface for configuration and management · Firmware update via web-based interface · Automatic notification on new firmware version · Saving/restoring configuration to/from file · Support of remote logging · Automatic synchronization of system time with NTP server and manual time/date setup · Ping function · 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"> · "Client" function (access point mode) Wireless network client Wireless network repeater · "Client" function (router mode) WISP repeater · WMM (Wi-Fi QoS) · Managing connected stations · Advanced settings · WDS
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	<ul style="list-style-type: none"> · 174 x 115 x 30 mm (7 x 4.5 x 1.2 in)
Weight	<ul style="list-style-type: none"> · 248 g (0.55 lb)
Operating Environment	
Power	<ul style="list-style-type: none"> · 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>	The WLAN interface is active (upstream or downstream traffic).
	<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 Internet connection is on.
	<i>Blinking green</i>	The WAN interface is active (upstream or downstream traffic).
	<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>	The LAN port is active (upstream or downstream traffic).
	<i>No light</i>	The cable is not connected to the relevant port.

Back and Bottom Panels

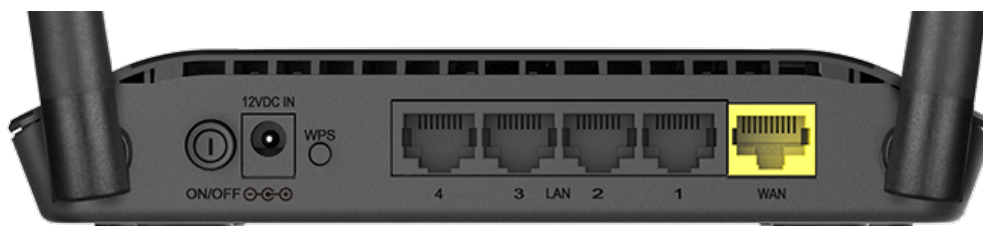


Figure 2. Back panel view.

Name	Description
ON/OFF	A button to turn the device on/off.
12VDC IN	Power connector.
WPS	<p>A button to set up a secure 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 5 and later
- Google Chrome 5 and later
- Microsoft Internet Explorer 8 and later
- Mozilla Firefox 5 and later
- Opera 10 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. Make sure that your PC is powered off.
2. Connect an Ethernet cable between any of LAN ports located on the back panel of the access point and the Ethernet port of your PC.
3. 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.
4. Turn on the access point by pressing the **ON/OFF** button on its back panel.
5. Turn on your PC and wait until your operating system is completely loaded.

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

Configuring IP Address in OS Windows XP

1. Click the **Start** button and proceed to the **Control Panel > Network and Internet Connections > Network Connections** window.
2. In the **Network Connections** window, right-click the relevant **Local Area Connection** icon and select the **Properties** line in the menu displayed.

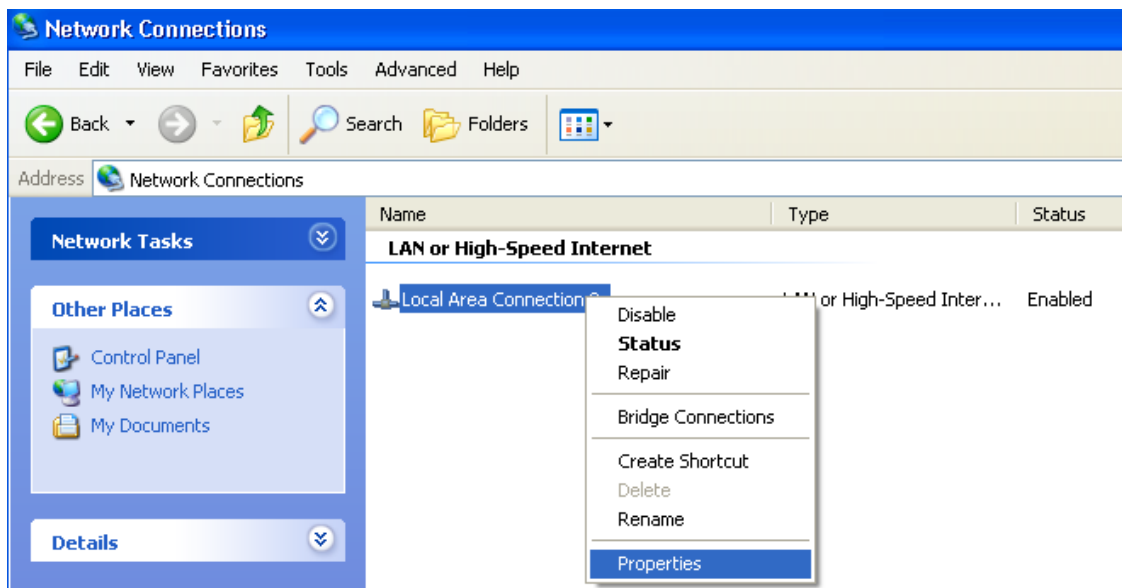


Figure 3. The **Network Connections** window.

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

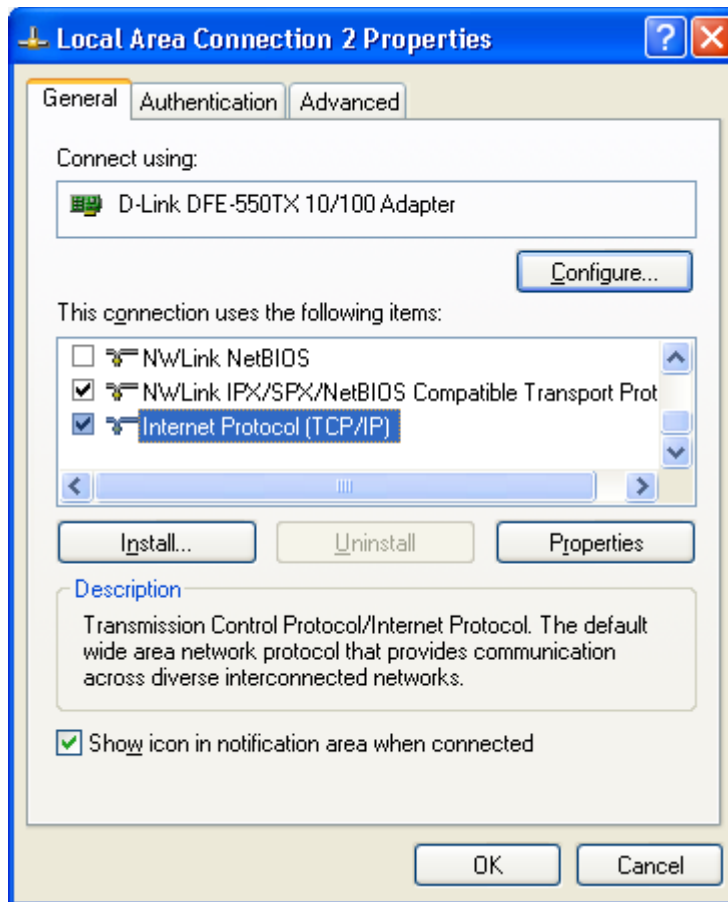


Figure 4. The **Local Area Connection Properties** window.

4. Select the **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.

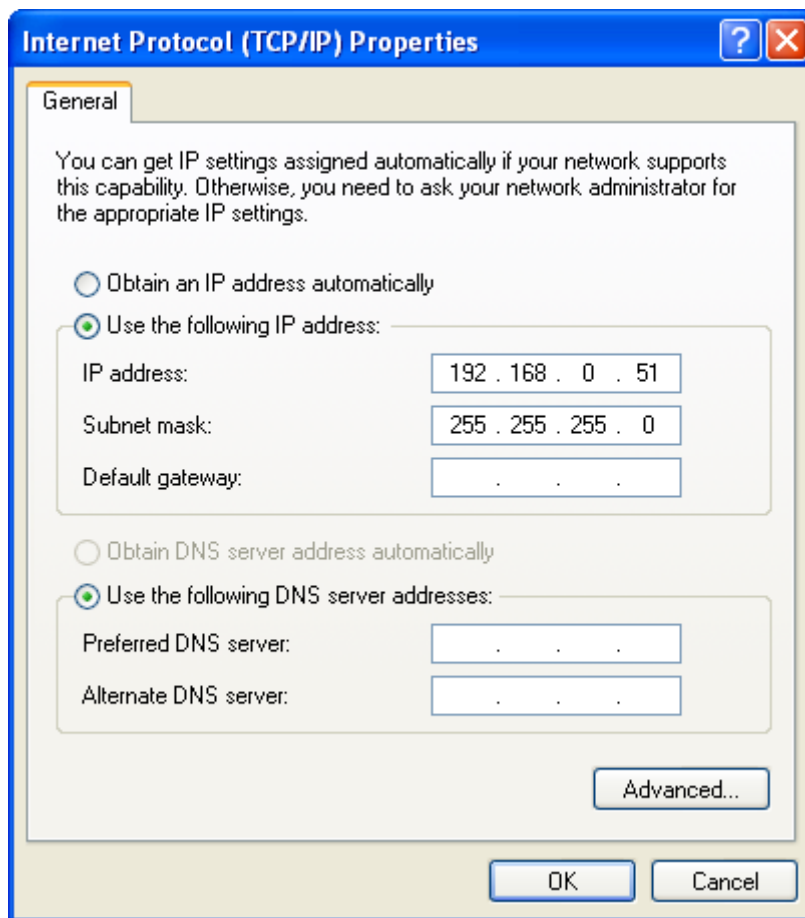


Figure 5. The **Internet Protocol (TCP/IP) Properties** window.

5. 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.

Configuring IP Address in OS Windows 7

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

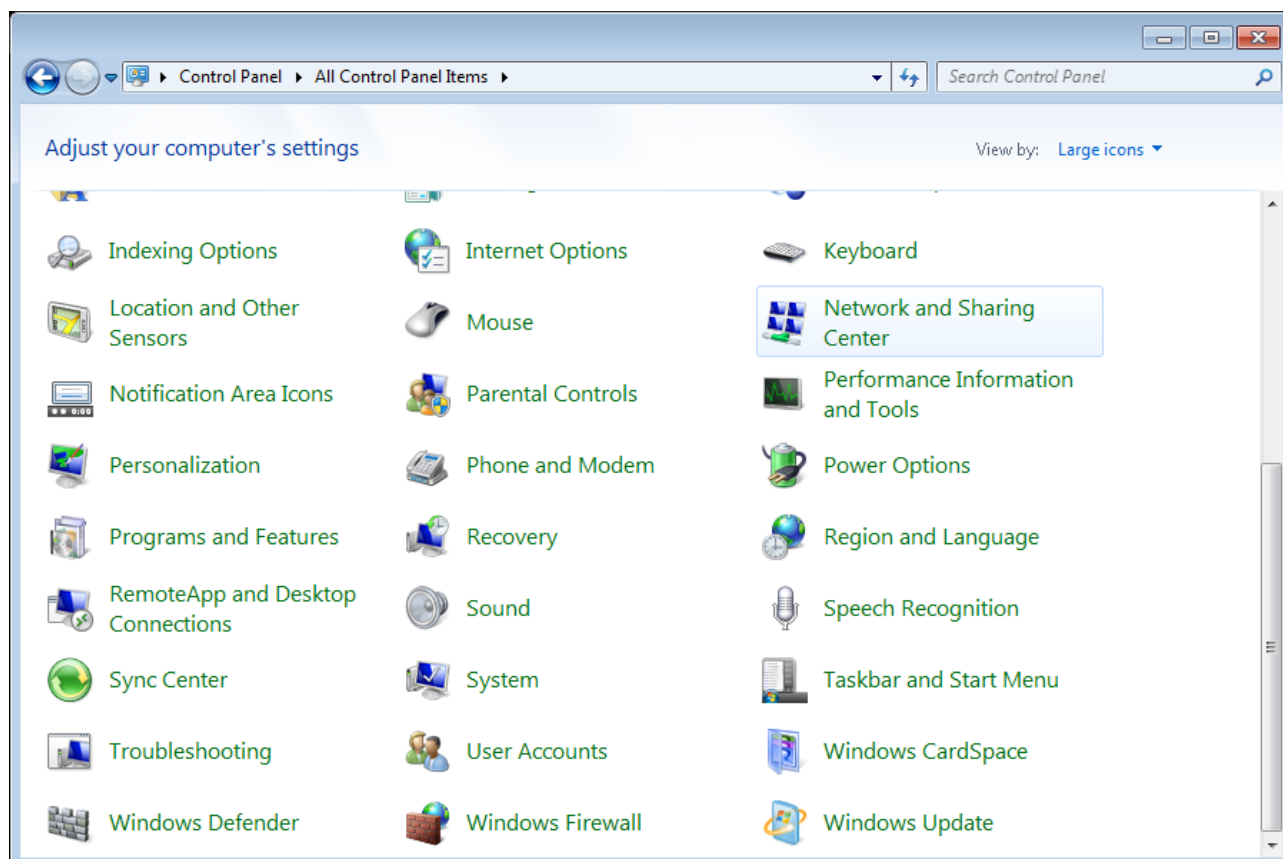


Figure 6. The **Control Panel** window.

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

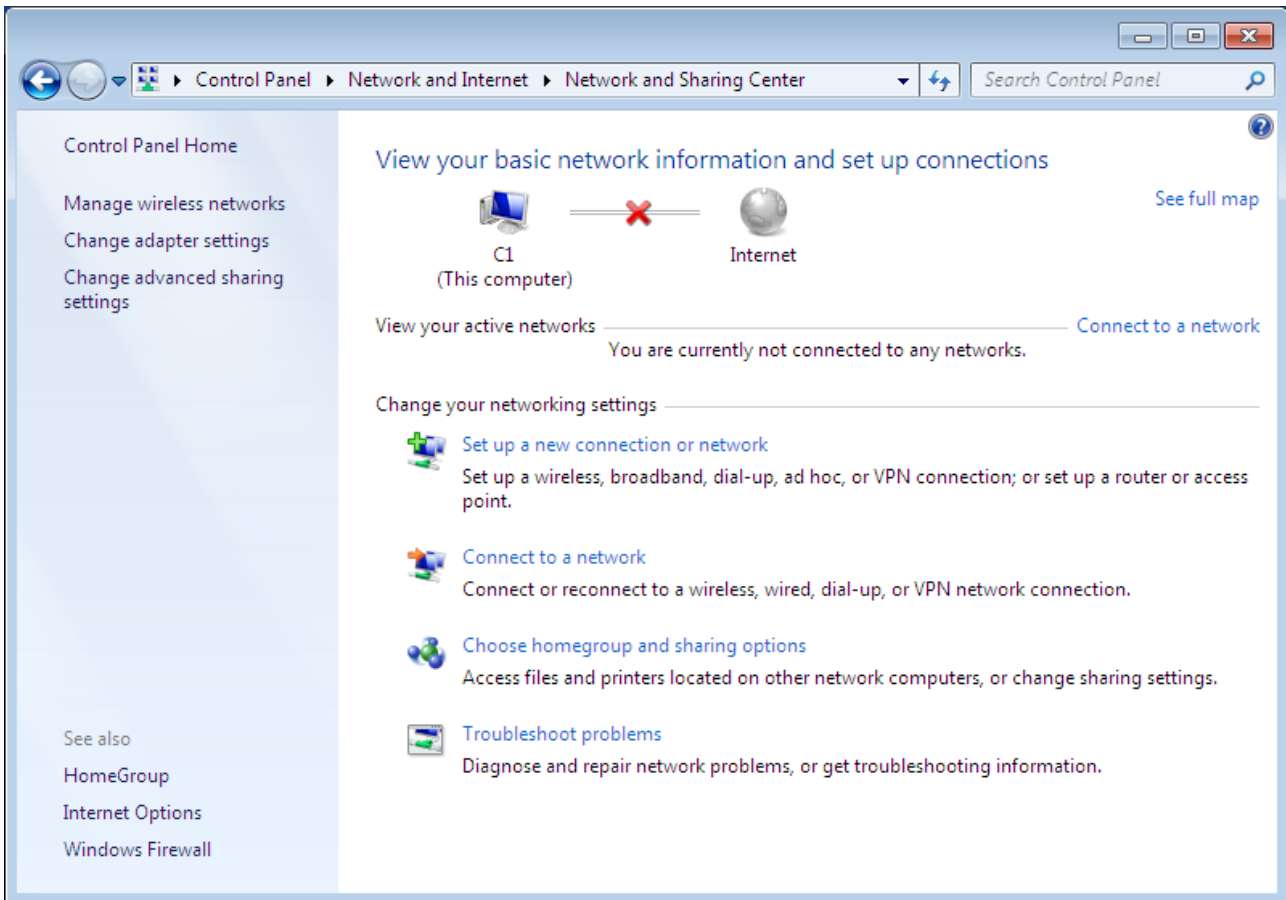


Figure 7. The **Network and Sharing Center** window.

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

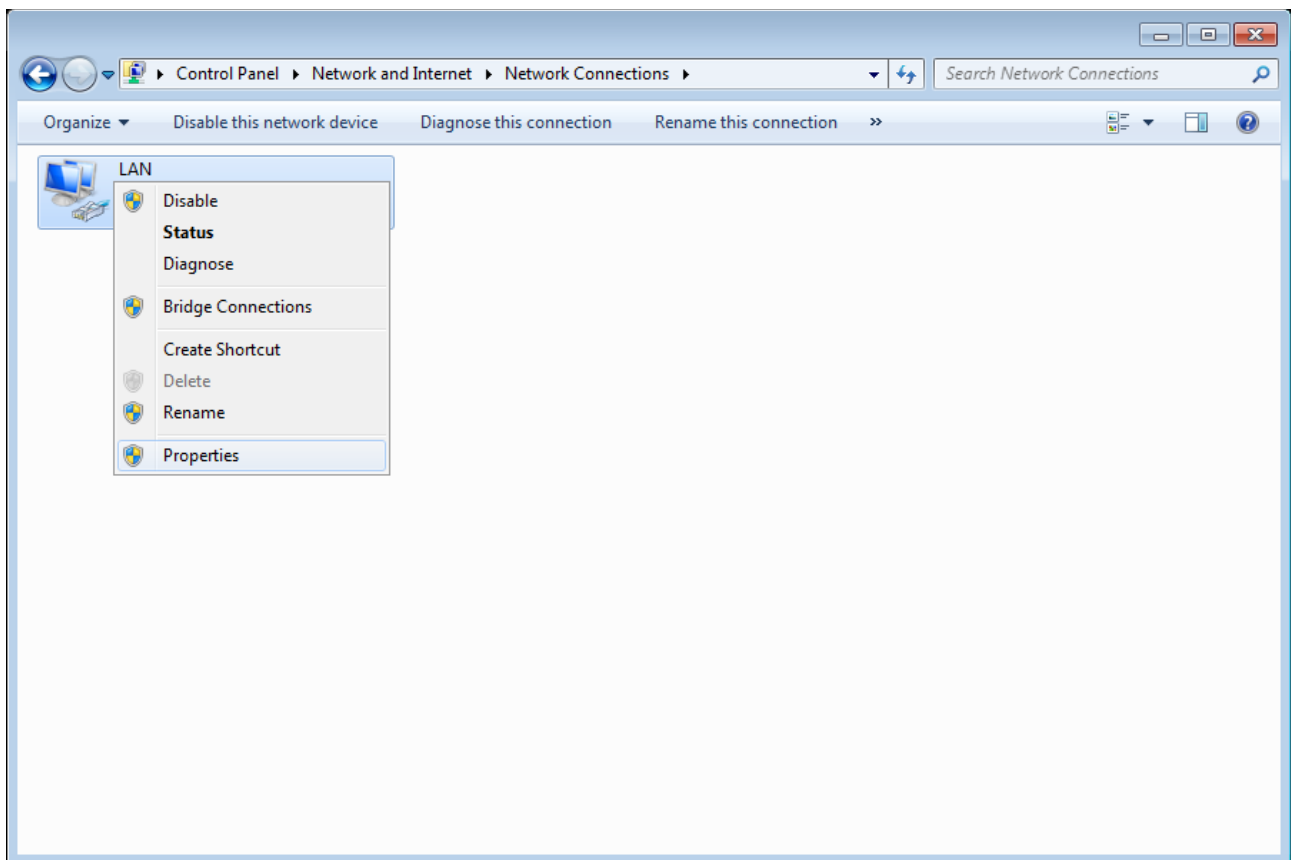


Figure 8. The **Network Connections** window.

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

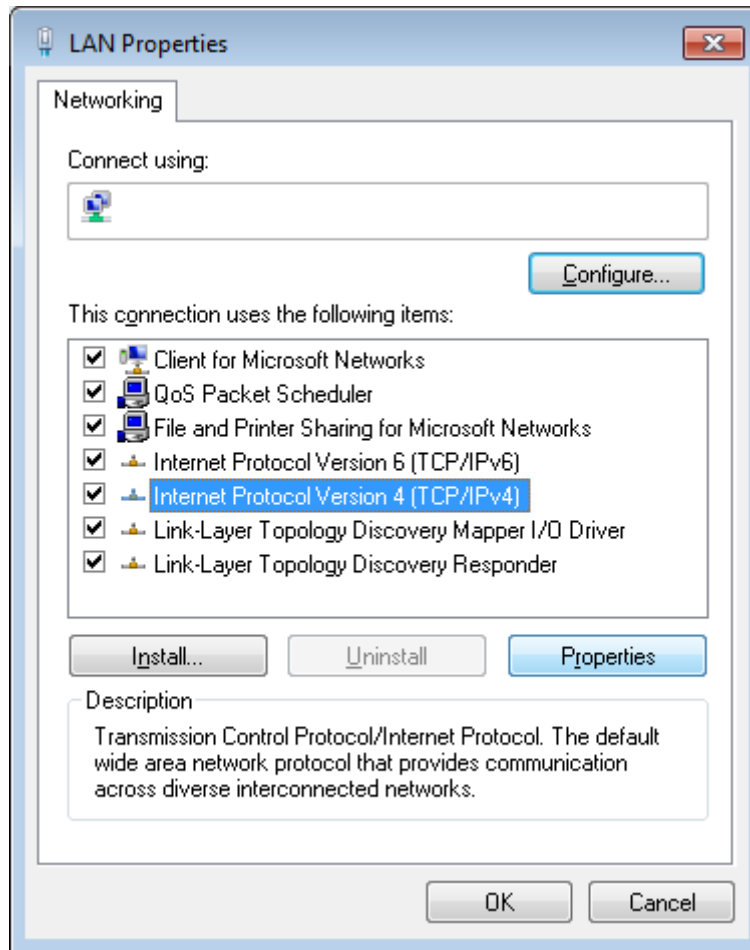


Figure 9. The **Local Area Connection Properties** window.

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

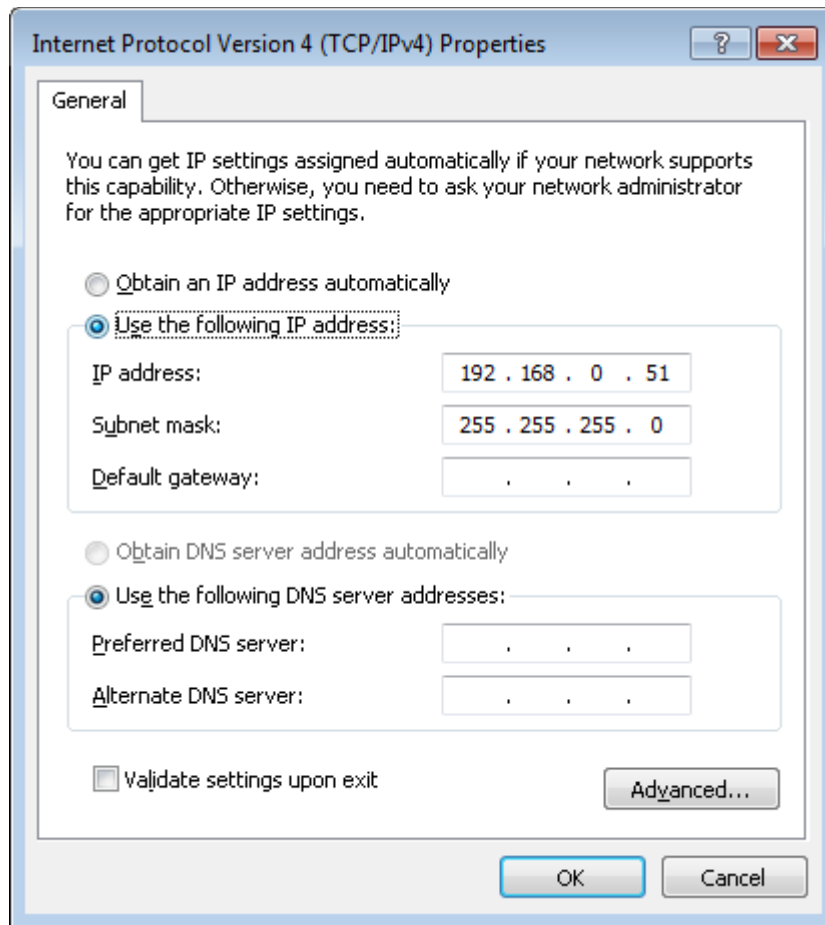


Figure 10. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now you can connect to the web-based interface of DAP-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. Turn on your PC and wait until your operating system is completely loaded.
5. Turn on your Wi-Fi adapter. As a rule, modern notebooks with built-in wireless NICs are equipped with a button or switch that turns on/off the wireless adapter (refer to your PC documents). If your PC is equipped with a pluggable wireless NIC, install the software provided with your Wi-Fi adapter.

Configuring Wi-Fi Adapter in OS Windows XP

1. Click the **Start** button and proceed to the **Control Panel > Network and Internet Connections > Network Connections** window.
2. In the **Network Connections** 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.
3. In the **Wireless Network Connection Properties** window, on the **General** tab, select the **Internet Protocol (TCP/IP)** line. Click the **Properties** button.
4. 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.

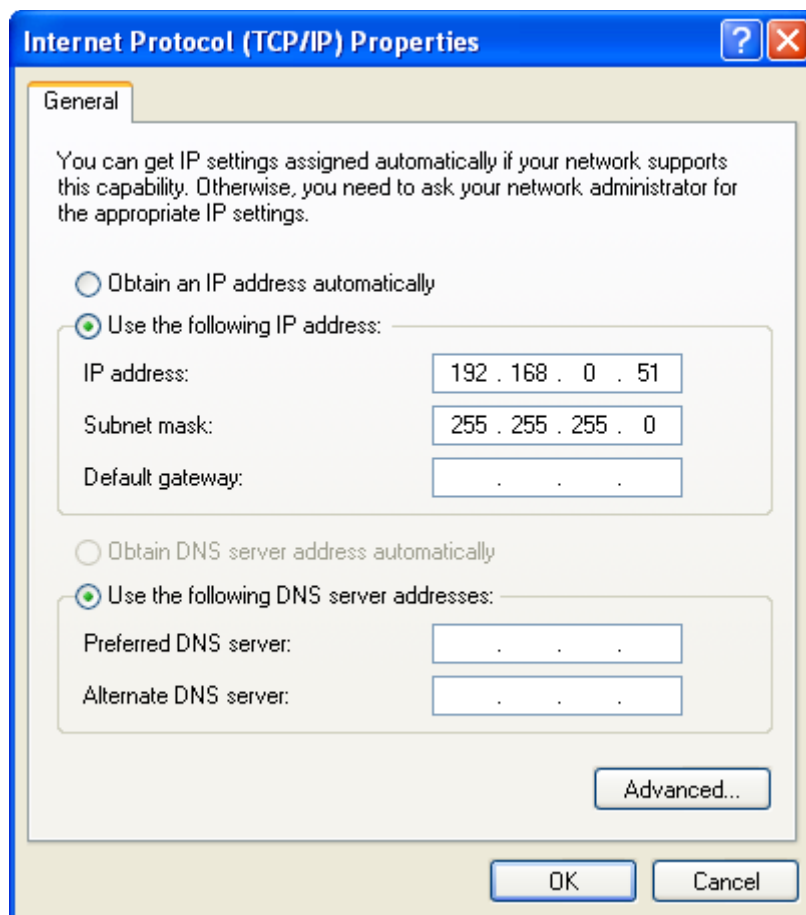


Figure 11. The **Internet Protocol (TCP/IP) Properties** window.

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

6. Search for available wireless networks.

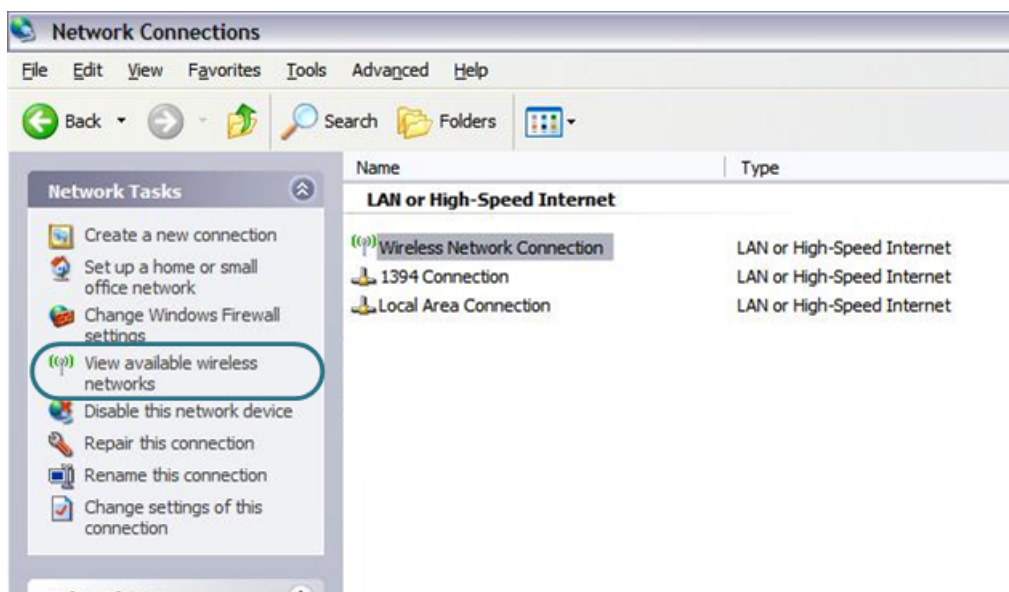


Figure 12. The **Network Connections** window.

7. In the opened **Wireless Network Connection** window, select the wireless network **DAP-1360** and click the **Connect** button.
8. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Network key** and **Confirm network key** fields and click the **Connect** button.

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

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.

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.)

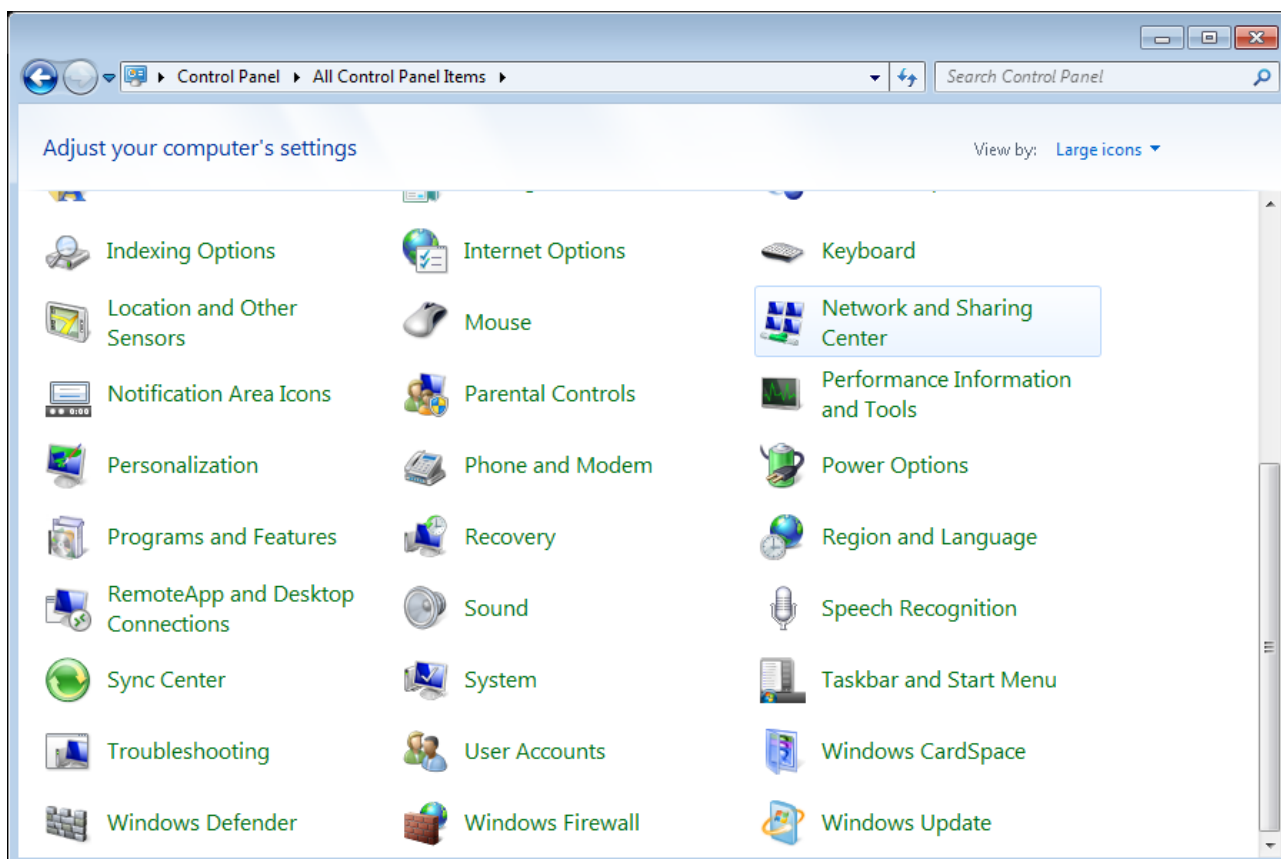


Figure 13. The **Control Panel** window.

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.

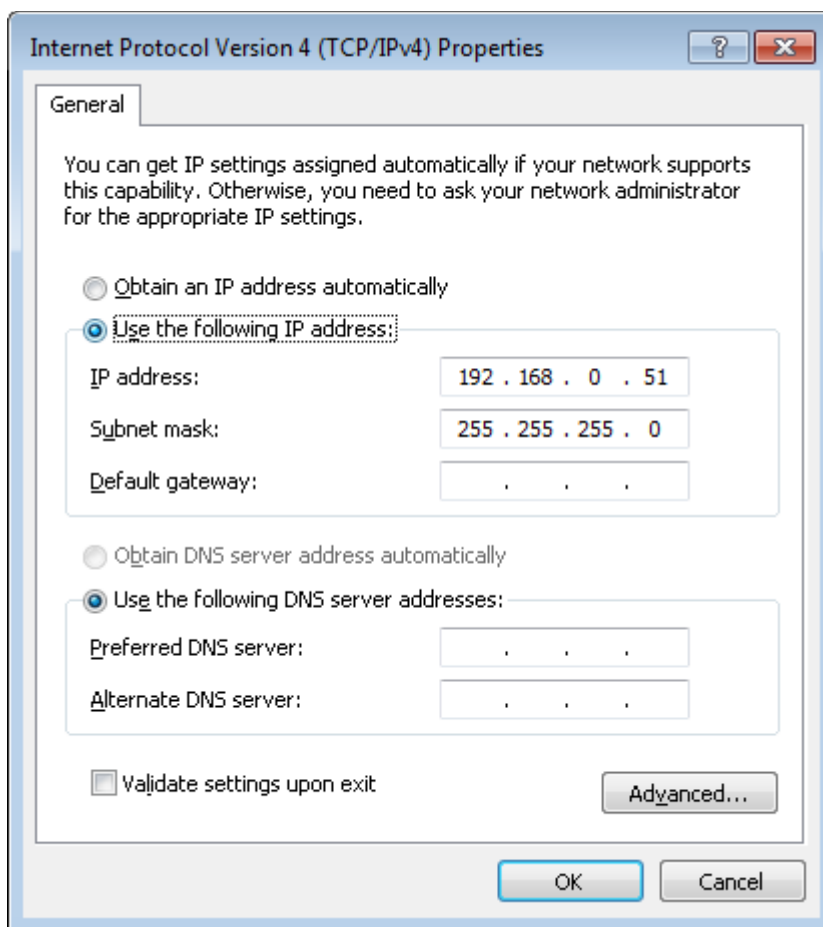


Figure 14. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

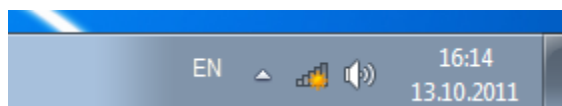


Figure 15. The notification area of the taskbar.

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

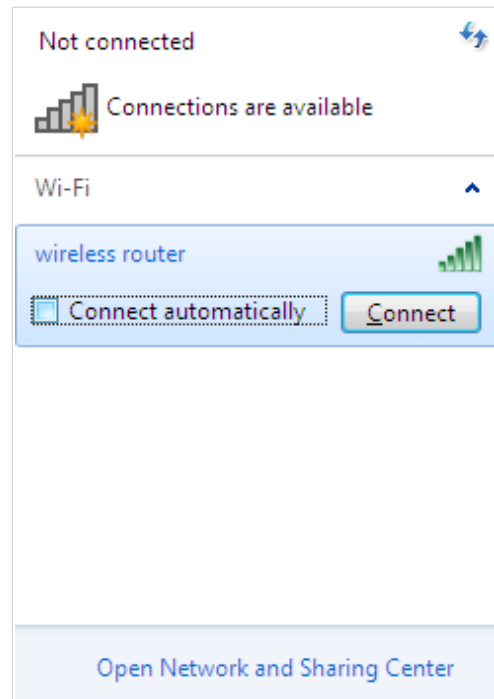


Figure 16. The list of available networks.

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

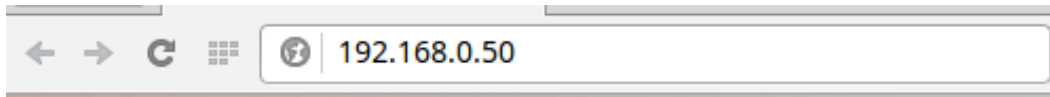


Figure 17. Connecting to the web-based interface of the DAP-1360U device.

! 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.

After the first access to the web-based interface you need to change the default administrator password. Enter the new password in the **Password** and **Confirmation** fields. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and characters available on the keyboard. Then click the **Apply** button.

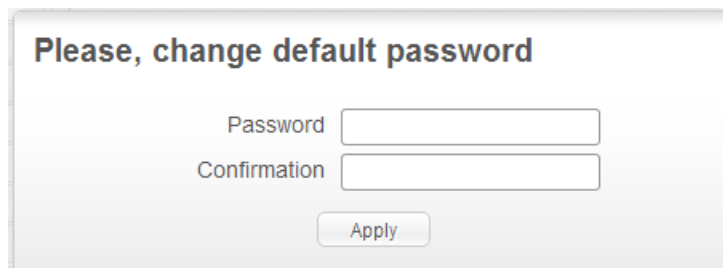
A screenshot of a web form titled "Please, change default password". The form has two input fields: "Password" and "Confirmation". Below these fields is an "Apply" button.

Figure 18. The page for changing the default administrator 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 device.

When the web-based interface is accessed the next time and after, the login page opens. Enter the username (**admin**) in the **Login** field and the password you specified in the **Password** field, then click the **Enter** button.

A screenshot of a login page titled "D-LINK DEVICE". The page has two input fields: "Login" and "Password". Below these fields are two buttons: "Clear" and "Enter".

Figure 19. The login page.

Web-based Interface Structure

After successful registration the **Home / Information** page opens. The selected operating mode defines the view of the page and the components of the web-based interface.

The web-based interface of the access point is multilingual. If you need to select another language for the web-based interface, place the mouse pointer over the **English** caption in the top part of the page and select a language from the menu displayed.



Figure 20. Changing the language of the web-based interface.

Also you can find a specific page via search. To do this, enter the name of the page, wholly or partly, in the search bar in the top part of the web-based interface page, and then select a needed link in the search results.

Access Point Mode

The **Home / Information** page displays general information on the access point and its software.

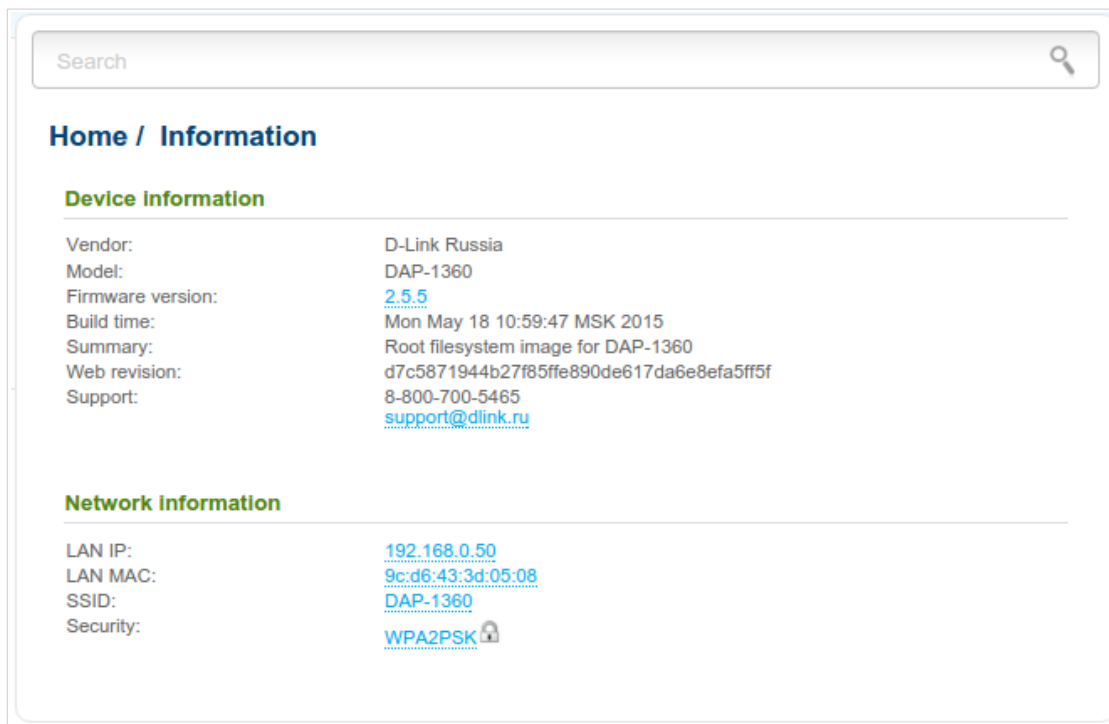


Figure 21. The general information page in the access point mode.

From the page you can quickly get to some pages of the web-based interface.

To upgrade the firmware of the access point, left-click the current firmware version (the right column of the **Firmware version** line) and follow the dialog box appeared.

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

To edit the access point's local interface parameters, left-click the IP or MAC address of the local interface (the right column of the **LAN IP** line or **LAN MAC** line correspondingly). After clicking the line, the page for editing the LAN interface opens (for the detailed description of the page, see the **LAN** section, page 50).

To configure the access point's WLAN parameters, left-click the SSID of the WLAN (the right column of the **SSID** line). After clicking the line, the **Wi-Fi / Basic settings** page opens (for the detailed description of the page, see the **Basic Settings** section, page 53).

To configure security settings of the WLAN, left-click the network authentication type (the right column of the **Security** line). After clicking the line, the **Wi-Fi / Security settings** page opens (for the detailed description of the page, see the **Security Settings** section, page 55).

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

In the **Home** section you can run the **Wireless network settings wizard** (for the detailed description of the Wizard, see the *Wireless Network Settings Wizard* section, page 37).

The pages of the **Status** section display data on the current state of the access point (for the description of the pages, see the *Status* section, page 46).

The page of the **Net** section is designed for configuring basic parameters of the LAN interface of the access point (for the description of the page, see the *Net* section, page 50).

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 53).

The page of the **Advanced** section is designed for adding DNS servers to the system (for the description of the page, see the *Advanced* section, page 77).

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 78).

Router Mode

The **Home / Information** page displays general information on the access point and its software.

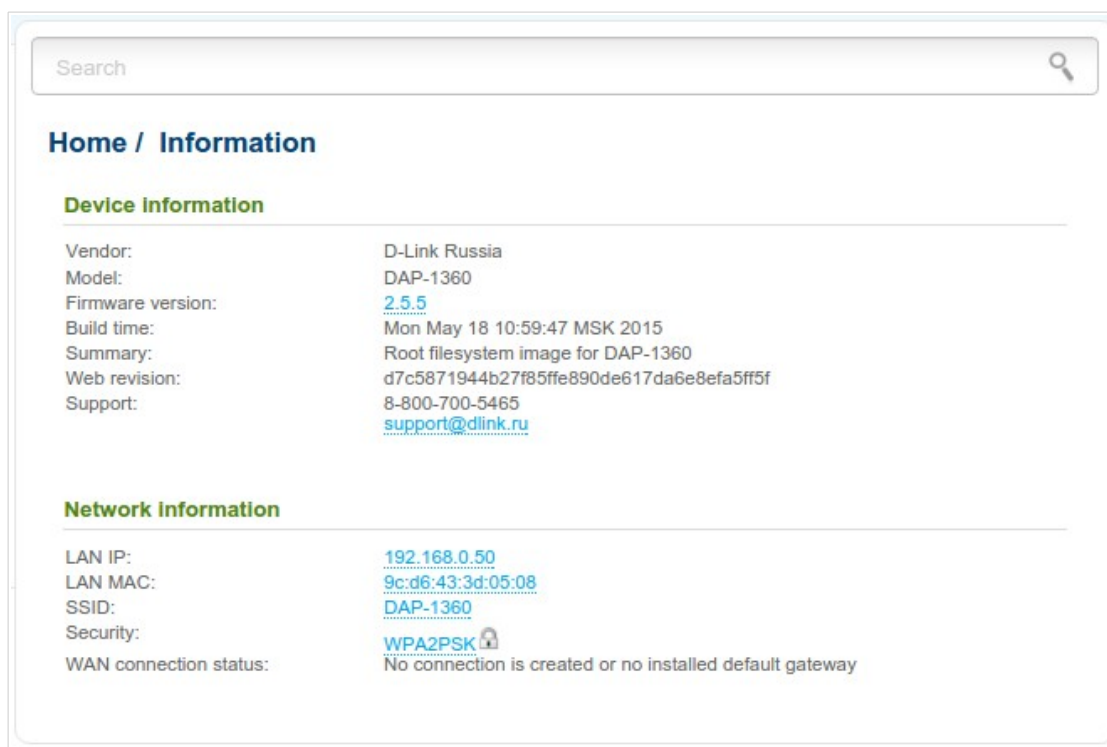


Figure 22. The general information page in the router mode.

From the page you can quickly get to some pages of the web-based interface.

To upgrade the firmware of the access point, left-click the current firmware version (the right column of the **Firmware version** line) and follow the dialog box appeared.

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

To edit the access point's local interface parameters, left-click the IP or MAC address of the local interface (the right column of the **LAN IP** line or **LAN MAC** line correspondingly). After clicking the line, the page for editing the LAN interface opens (for the detailed description of the page, see the **LAN** section, page 156).

To configure the access point's WLAN parameters, left-click the SSID of the WLAN (the right column of the **SSID** line). After clicking the line, the **Wi-Fi / Basic settings** page opens (for the detailed description of the page, see the **Basic Settings** section, page 158).

To configure security settings of the WLAN, left-click the network authentication type (the right column of the **Security** line). After clicking the line, the **Wi-Fi / Security settings** page opens (for the detailed description of the page, see the **Security Settings** section, page 160).

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

The **Monitoring** section provides an interactive scheme which illustrates the access point's settings and the LAN structure.

In the **Home** section you can run the needed Wizard.

To configure connection to the Internet, go to the **Click'n'Connect** page (for the detailed description of the Wizard, see the *Click'n'Connect* section, page 96).

To configure the access point's wireless network, go to the **Wireless network settings wizard** page (for the detailed description of the Wizard, see the *Wireless Network Settings Wizard* section, page 118).

To configure access from the Internet to a web server located in your LAN, go to the **Virtual server settings wizard** page (for the detailed description of the Wizard, see the *Virtual Server Settings Wizard* section, page 127).

The pages of the **Status** section display data on the current state of the access point (for the description of the pages, see the *Status* section, page 129).

The pages of the **Net** 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 *Net* section, page 134).

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 158).

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 182).

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 192).

The pages of the **Control** section are designed for creating restrictions on access to the Internet (for the description of the page, see the *Control* section, page 201).

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 203).

Notifications and System Drop-down Menu

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

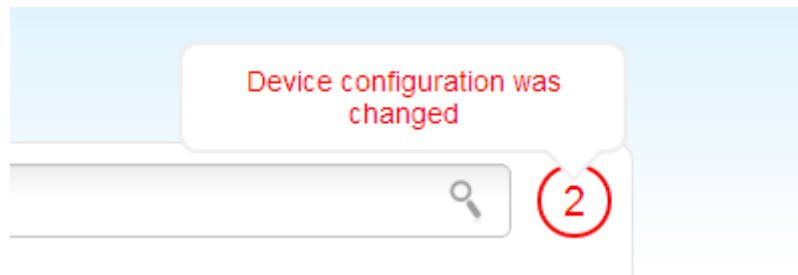


Figure 23. The web-based interface notifications.

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

! Note that you should regularly save the changes of the access point's settings to the non-volatile memory.

You can save the access point's settings via the menu displayed when the mouse pointer is over the **System** caption in the top left part of the page. Also the **System** menu allows you to reboot the device, create and load the configuration backup, restore the factory defaults, update the firmware, disable/enable the WLAN.

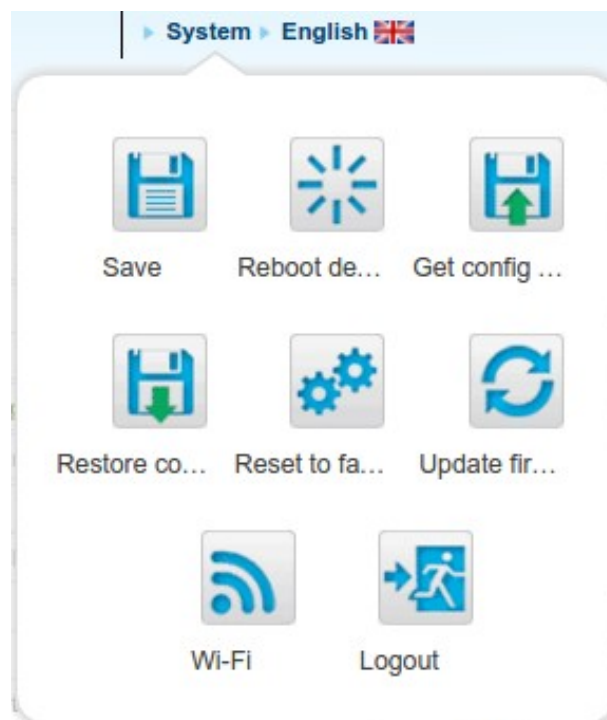










Figure 24. The **System** menu in the top part of the page.

Control	Description
 Save	<p>Click the icon to save new settings to the non-volatile memory.</p> <p>Also you can save the device's parameters via the Save button on the System / Configuration page.</p>
 Reboot device	<p>Click the icon to reboot the device. All unsaved changes will be lost after the device's reboot.</p>
 Get config backup	<p>Click the icon 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.</p> <p>Also you can create the configuration backup via the Backup button on the System / Configuration page.</p>
 Restore config	<p>Click the icon to go to the System / Configuration page.</p>
 Reset to factory	<p>Click the icon to restore the factory default settings. Also you can restore the factory defaults via the Factory button on the System / Configuration page.</p> <p>Also you can restore the factory default settings via the hardware RESET button which is located on the bottom panel of the access point. Push the button (with the access point powered on) and hold for 10 seconds. Then release the button.</p>
 Update firmware	<p>Click the icon to update the firmware of the access point.</p> <p>Also you can update the firmware on the System / Firmware upgrade page.</p>
 Wi-Fi	<p>Click the icon to disable or enable the device's WLAN.</p> <p>Also you can disable/enable the access point's WLAN on the Wi-Fi / Basic settings page.</p>
 Logout	<p>Click the icon to exit the web-based interface.</p>

Device Operation Modes

Access Point Mode

In the access point mode, the device is used to create a wireless local area network or to connect to a wired router.

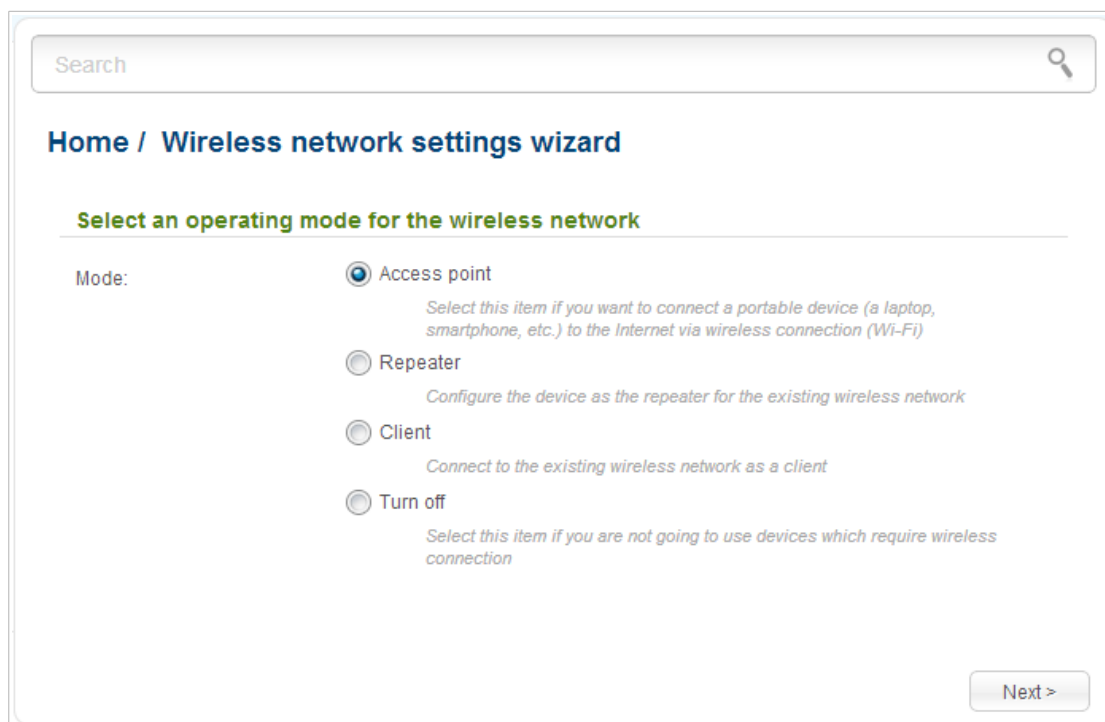
Router Mode

In the router mode, the device is used to connect to the Internet. You can connect the device to a cable or DSL modem or to a private Ethernet line and create a WAN connection. In addition, you can configure connection to a Wireless Internet Service Provider.

CHAPTER 4. CONFIGURING DEVICE (ACCESS POINT MODE)

Wireless Network Settings Wizard

To specify all needed settings for your wireless network, click the **Wireless network settings wizard** link in the **Home** section.



Search

Home / Wireless network settings wizard

Select an operating mode for the wireless network

Mode:

- Access point
Select this item if you want to connect a portable device (a laptop, smartphone, etc.) to the Internet via wireless connection (Wi-Fi)
- Repeater
Configure the device as the repeater for the existing wireless network
- Client
Connect to the existing wireless network as a client
- Turn off
Select this item if you are not going to use devices which require wireless connection

Next >

Figure 25. The page for selecting the operating mode for the wireless network.

If you are not going to use the wireless connection, select the **Turn off** choice of the **Mode** radio button. Click the **Next** button and then click the **Apply** button on the opened page. After clicking the button, the **Home / Information** page opens.

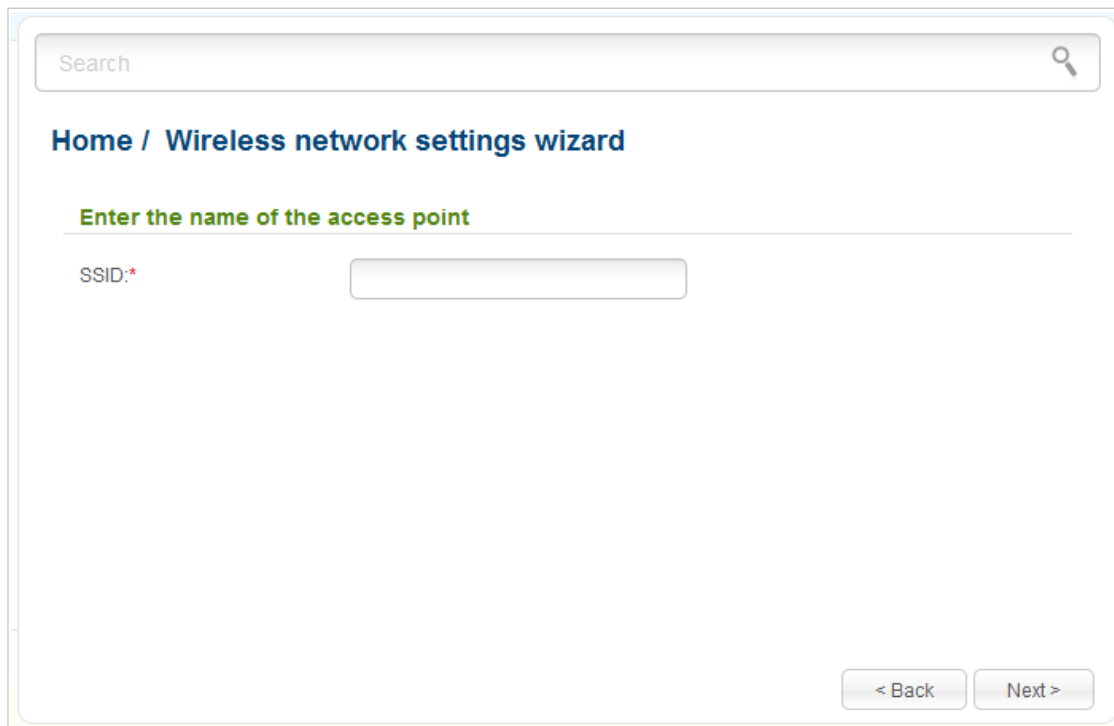
If you want to connect portable devices to the network of the access point via wireless connection, select the **Access point** choice of the **Mode** radio button. Click the **Next** button.

If you want to configure DAP-1360U as a repeater to connect to a wireless access point, select the **Repeater** choice of the **Mode** radio button. Click the **Next** button.

If you want to configure DAP-1360U as a client to connect to a wireless access point, select the **Client** choice of the **Mode** radio button. Click the **Next** button.

Access Point Mode

On the opened page, in the **SSID** field, specify a new name for the network (use digits and Latin characters).



The screenshot shows a web interface for configuring a wireless network. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar, the breadcrumb "Home / Wireless network settings wizard" is displayed. A green heading "Enter the name of the access point" is followed by a horizontal line. Underneath, the label "SSID:*" is positioned to the left of an empty text input field. At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 26. Page for changing the name of the wireless LAN.

Click the **Next** button to continue.

On the next page, you can modify security settings of the WLAN.

Select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the WLAN of the access point.

When the **Open** value is selected, the **Network key** field is unavailable. After applying this setting, the **Open** authentication type with no encryption is specified for the WLAN of the access point.

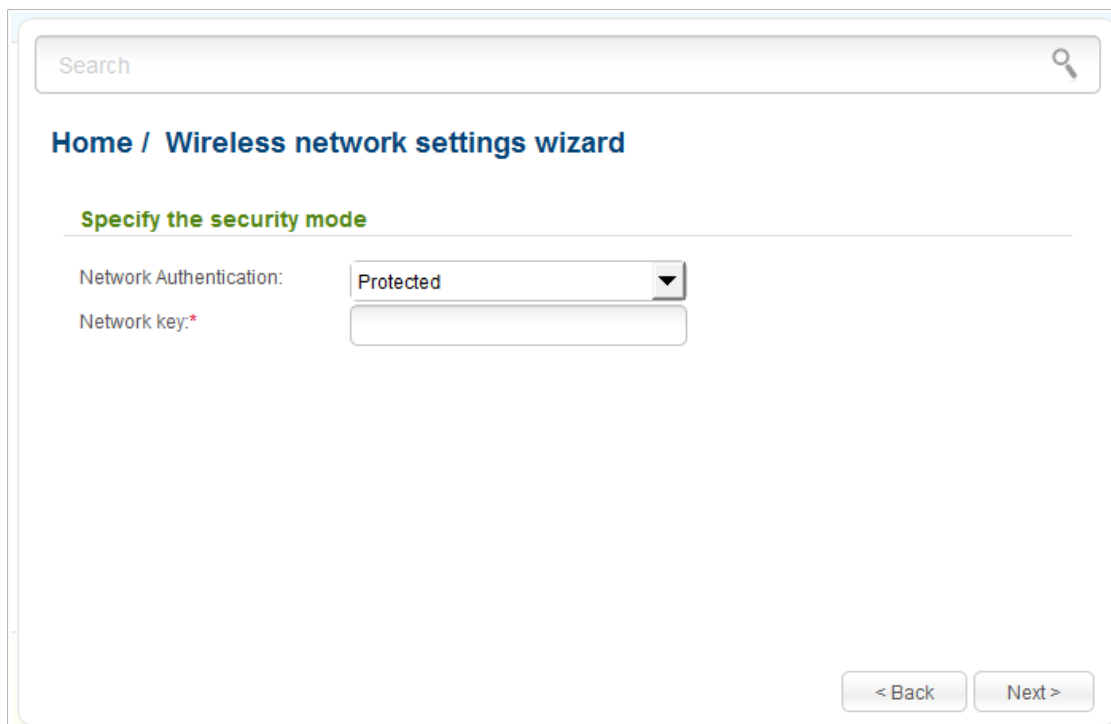


Figure 27. Page for selecting a security mode for the wireless network.

Click the **Next** button to continue.

On the next page, the specified settings are displayed. Make sure that they are correct and then click the **Apply** button. After clicking the button, the **Home / Information** page opens.

Repeater Mode

On the opened page, click the **Search** button.

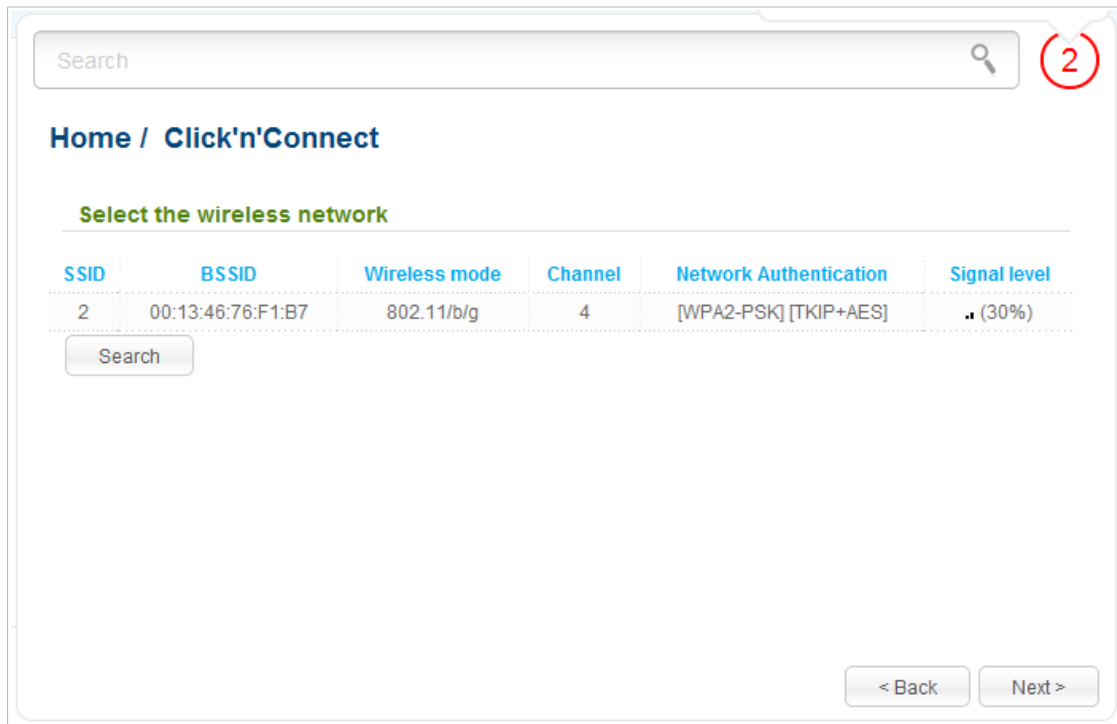
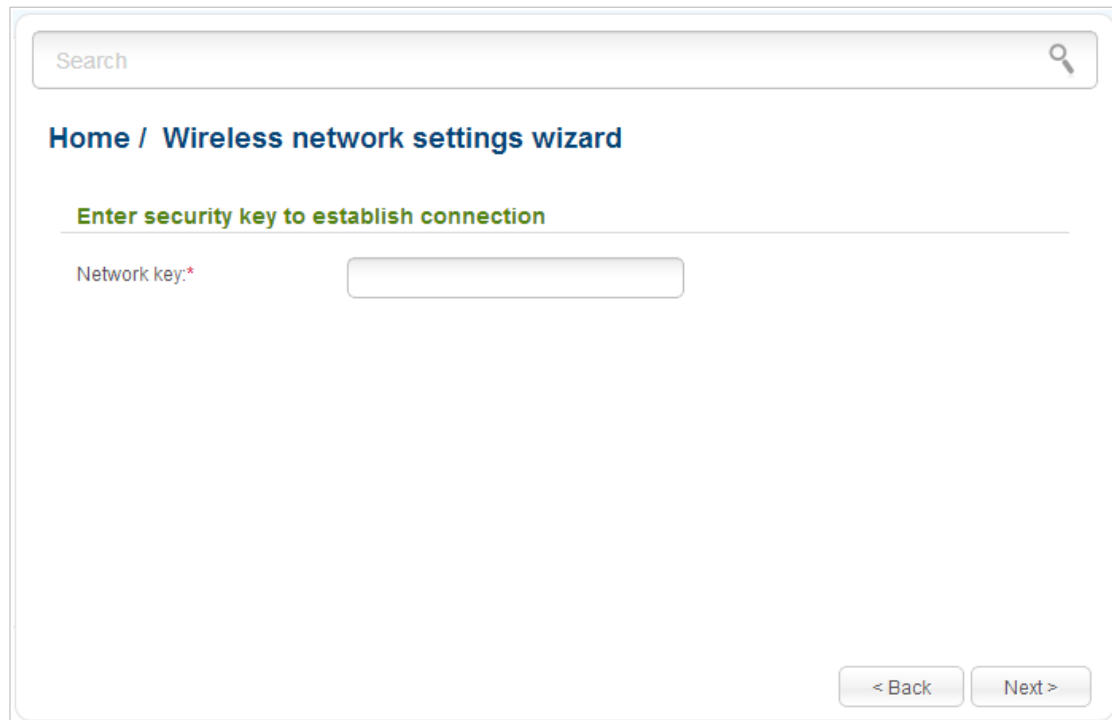


Figure 28. The page for selecting a network to connect.

Select the network to which you want to connect and click the **Next** button.



The screenshot shows a web interface for configuring a wireless network. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar, the breadcrumb "Home / Wireless network settings wizard" is displayed. A green heading reads "Enter security key to establish connection". Underneath, the label "Network key:" is followed by a text input field. At the bottom right, there are two buttons: "< Back" and "Next >".

Figure 29. The page for entering the password for connection to the wireless network.

If you need a password to connect to the selected network, enter the password in the **Network key** field and click the **Next** button.

On the next page, you can specify an individual name (SSID) and security settings for the access point or configure the parameters identical with the network to which you connect.

Search

Home / Wireless network settings wizard

Enter the settings for the extender network

SSID:*

Use the same security and network key as those for the exiting network:

Network Authentication:

Network key:*

< Back Next >

Figure 30. The page for changing the settings of the wireless local area network.

If you want to leave the name of the wireless network and security settings identical with the network to which you connect, click the **Next** button.

If you want to configure individual settings for the access point, deselect the **Use the same security and network key as those for the exiting network** checkbox and enter a name for the wireless network in the **SSID** field. It is strongly recommended to configure the secure wireless network of DAP-1360U. To do this, select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the WLAN of the access point. Click the **Next** button.

On the next page, the parameters of the network to which you want to connect, the entered password, and the settings of the wireless network of the access point are displayed. Make sure that the specified settings are correct and then click the **Apply** button. After that, the wireless channel of DAP-1360U will switch to the channel of the wireless access point to which you have connected.

After clicking the **Apply** button, the **Home / Information** page opens.

Client Mode

On the opened page, click the **Search** button.

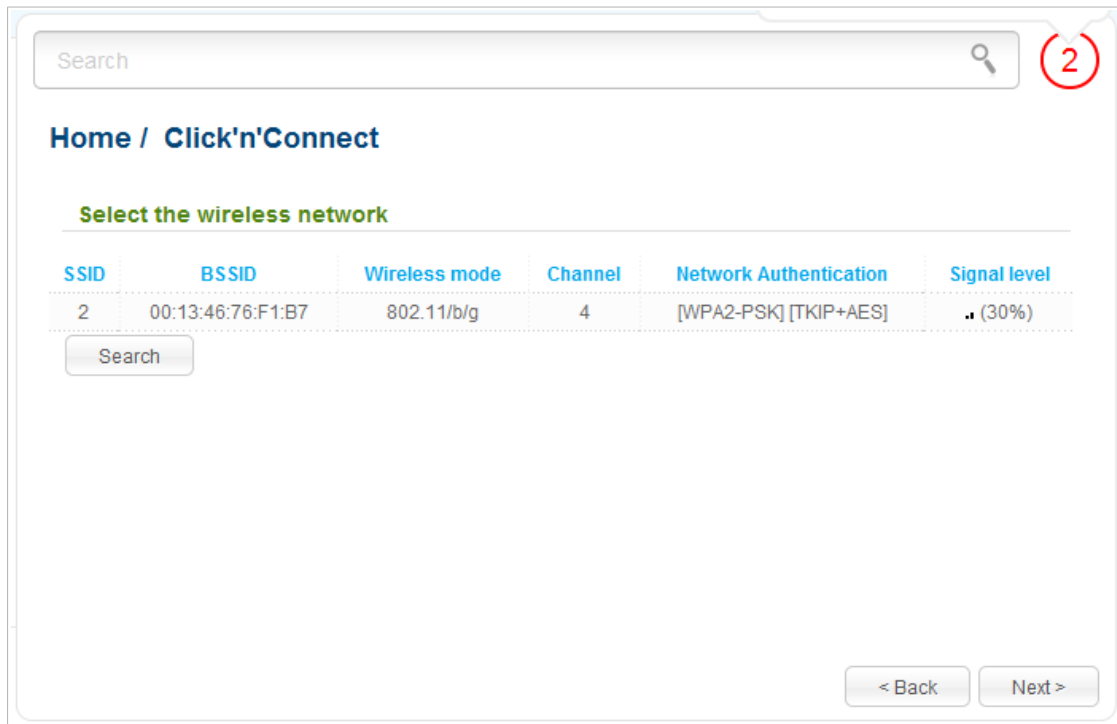
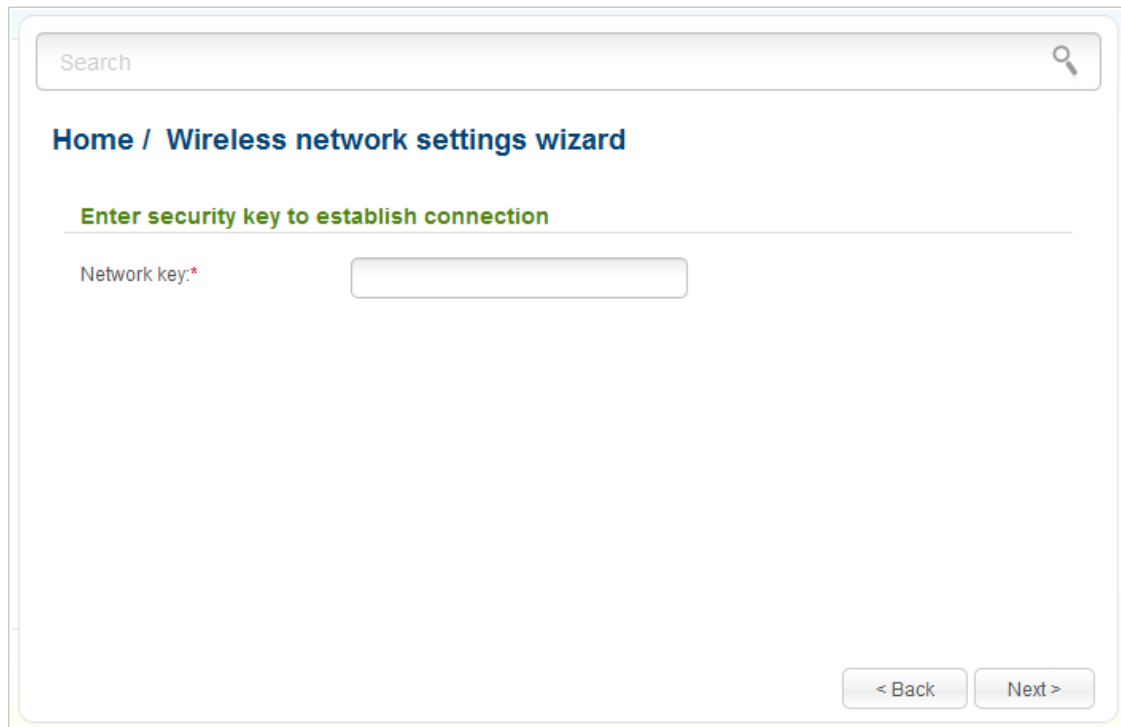


Figure 31. The page for selecting a network to connect.

Select the network to which you want to connect and click the **Next** button.



The screenshot shows a web interface for configuring a wireless network. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar, the breadcrumb "Home / Wireless network settings wizard" is displayed. A green heading reads "Enter security key to establish connection". Underneath, the label "Network key:" is followed by an empty text input field. At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 32. The page for entering the password for connection to the wireless network.

If you need a password to connect to the selected network, enter the password in the **Network key** field and click the **Next** button.

On the next page, you can specify an individual name (SSID) and security settings for the access point or disable the device's wireless network broadcast.

Search

Home / Wireless network settings wizard

Broadcasting their network

Enable:

SSID:*

Specify the security mode

Network Authentication: Protected ▼

Network key:*

< Back Next >

Figure 33. The page for changing the settings of the wireless local area network.

If you want to use the access point's wireless network to connect devices, leave the **Enable** checkbox selected. Then, if needed, specify another name for the network in the **SSID** field (use digits and Latin characters).

It is strongly recommended to configure the secure wireless network of DAP-1360U. To do this, select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the WLAN of the access point. Click the **Next** button.

On the next page, the parameters of the network to which you want to connect, the entered password, and the settings of the wireless network of the access point are displayed. Make sure that the specified settings are correct and then click the **Apply** button. After that, the wireless channel of DAP-1360U will switch to the channel of the wireless access point to which you have connected.

After clicking the **Apply** button, the **Home / Information** page opens.

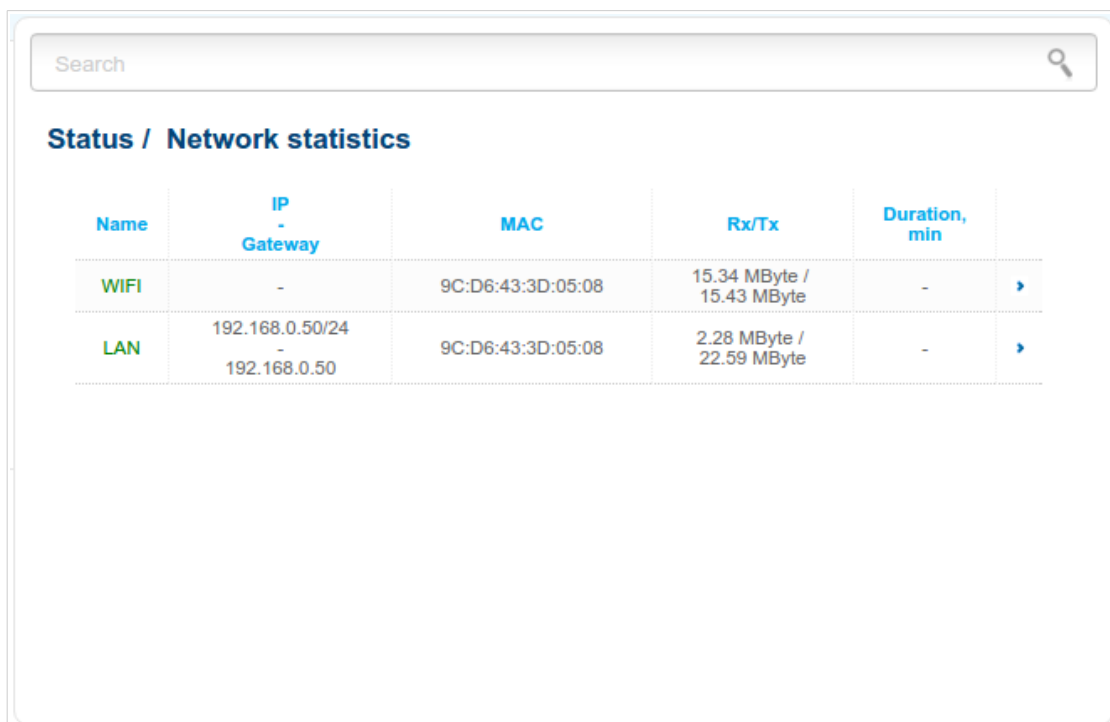
Status

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

- network statistics
- IP addresses leased by the DHCP server
- data on devices connected to the access point's network and its web-based interface
- addresses of active multicast groups.

Network Statistics

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



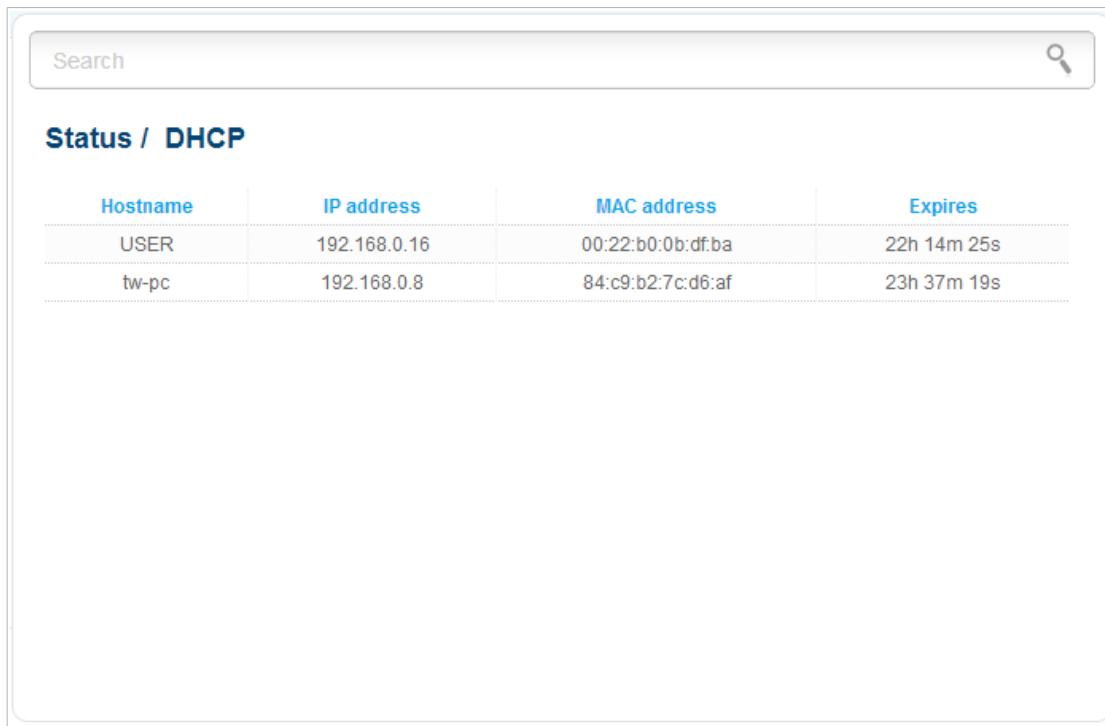
The screenshot shows the 'Status / Network statistics' page. At the top, there is a search bar. Below it, the title 'Status / Network statistics' is displayed. A table lists network connections with the following columns: Name, IP - Gateway, MAC, Rx/Tx, and Duration, min. The 'WIFI' connection is highlighted in green, and the 'LAN' connection is also highlighted in green. The 'LAN' connection shows two IP addresses: 192.168.0.50/24 and 192.168.0.50. The 'Rx/Tx' column shows data received and transmitted in MByte. The 'Duration, min' column shows a dash '-' for both connections. There are right-pointing arrows in the last column for each row.

Name	IP - Gateway	MAC	Rx/Tx	Duration, min
WIFI	-	9C:D6:43:3D:05:08	15.34 MByte / 15.43 MByte	-
LAN	192.168.0.50/24 192.168.0.50	9C:D6:43:3D:05:08	2.28 MByte / 22.59 MByte	-

Figure 34. The **Status / Network statistics** page.

DHCP

The **Status / 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).



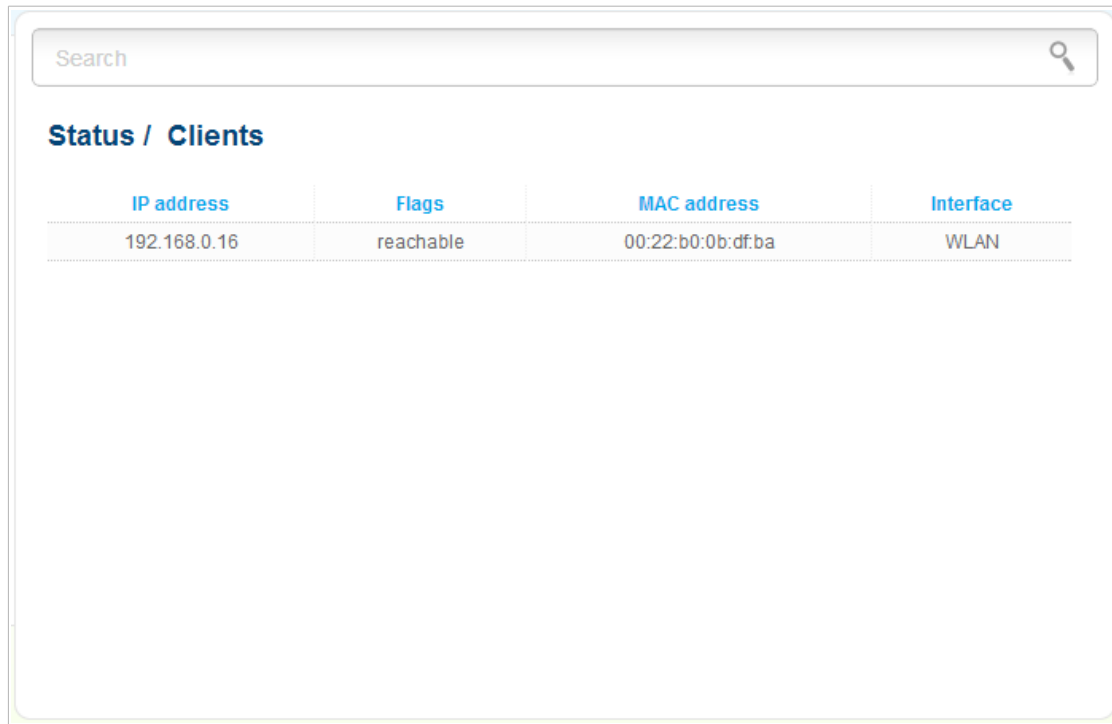
The screenshot shows a web interface for the DHCP status page. At the top, there is a search bar with the placeholder text "Search" and a magnifying glass icon. Below the search bar, the title "Status / DHCP" is displayed in blue. Underneath the title is a table with four columns: "Hostname", "IP address", "MAC address", and "Expires". The table contains two rows of data. The first row shows a hostname of "USER", an IP address of "192.168.0.16", a MAC address of "00:22:b0:0b:df:ba", and an expiration time of "22h 14m 25s". The second row shows a hostname of "tw-pc", an IP address of "192.168.0.8", a MAC address of "84:c9:b2:7c:d6:af", and an expiration time of "23h 37m 19s".

Hostname	IP address	MAC address	Expires
USER	192.168.0.16	00:22:b0:0b:df:ba	22h 14m 25s
tw-pc	192.168.0.8	84:c9:b2:7c:d6:af	23h 37m 19s

Figure 35. The **Status / DHCP** page.

Clients

On the **Status / Clients** page, you can view the list of devices connected to the access point and devices accessing its web-based interface.



The screenshot shows a web interface for the 'Status / Clients' page. At the top, there is a search bar with the placeholder text 'Search' and a magnifying glass icon. Below the search bar, the title 'Status / Clients' is displayed. Underneath the title is a table with four columns: 'IP address', 'Flags', 'MAC address', and 'Interface'. The table contains one row of data representing a connected client.

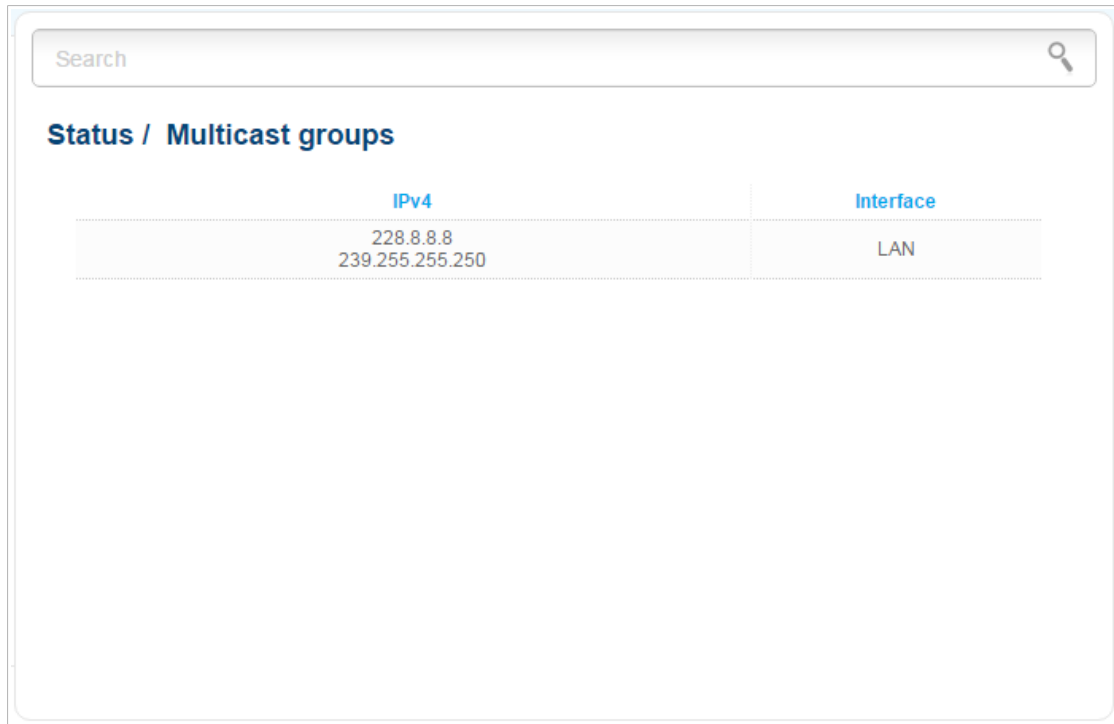
IP address	Flags	MAC address	Interface
192.168.0.16	reachable	00:22:b0:0b:df:ba	WLAN

Figure 36. The **Status / Clients** page.

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

Multicast groups

The **Status / 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.



The screenshot shows a web interface for 'Status / Multicast groups'. At the top is a search bar with the text 'Search' and a magnifying glass icon. Below the search bar is the title 'Status / Multicast groups'. Underneath is a table with two columns: 'IPv4' and 'Interface'. The table contains two rows of data.

IPv4	Interface
228.8.8.8	LAN
239.255.255.250	

Figure 37. The **Status / Multicast groups** page.

Net

In this menu you can configure basic parameters of the local area network of the access point.

LAN

To configure the access point's local interface, proceed to the **Net / LAN** page.

The screenshot shows a configuration form with the following fields and values:

- Name: LAN
- IP Address*: 192.168.0.50
- Netmask*: 255.255.255.0
- Gateway IP address: (empty)

Figure 38. Basic settings of the local interface.

If needed, edit the basic settings of the local interface.

Parameter	Description
IP Address	The IP address of the access point in the local subnet. By default, the following value is specified: 192 . 168 . 0 . 50 .
Netmask	The mask of the local subnet. By default, the following value is specified: 255 . 255 . 255 . 0 .
Gateway IP address	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> .

When needed settings are configured, click the **Apply** button.

In the **DHCP server** section, you can configure the built-in DHCP server of the access point. In the access point mode, the DHCP server is disabled by default.

The screenshot shows the DHCP server configuration section with the following fields and values:

- Mode: Enable
- Start IP*: 192.168.0.51
- End IP*: 192.168.0.100
- Gateway IP address: (empty)
- Primary DNS server: (empty)
- Secondary DNS server: (empty)
- Lease time (min)*: 1440

Figure 39. The section for configuring the DHCP server.

Parameter	Description
Mode	<p>An operating mode of the access point's DHCP server.</p> <p>Enable: 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, Gateway IP address, Primary DNS server, Secondary DNS server, and the Lease time fields are displayed on the page.</p> <p>Disable: the access point's DHCP server is disabled, clients' IP addresses are assigned manually.</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.
Gateway IP address	The gateway IP address for clients of the access point. When this field is left blank, clients use the IP address of the access point as the gateway address.
Primary DNS server/ Secondary DNS server	The IP addresses of the primary and secondary DNS servers for clients of the access point. When these fields are left blank, clients use the IP address of the access point as the addresses of the DNS servers.
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.

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

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

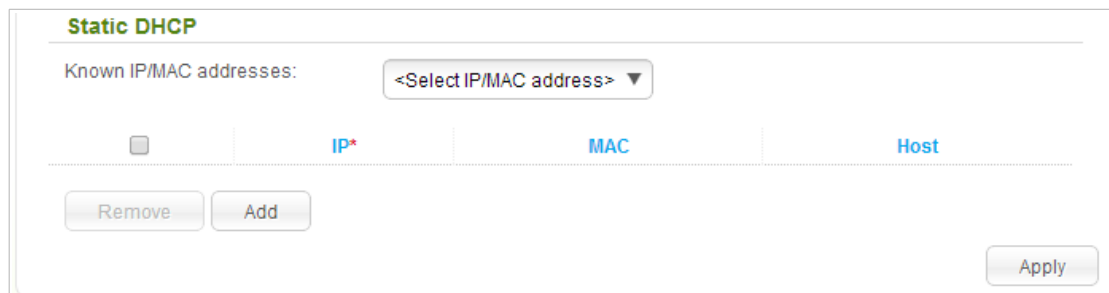


Figure 40. The section for creating MAC-IP pairs.

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

Also you can create a MAC-IP pair for a device connected to the access point's LAN at the moment. To do this, select the relevant value from the **Known IP/MAC addresses** drop-down list (the fields of the section will be filled in automatically).

When all needed MAC-IP pairs are specified, click the **Apply** button.

Existing MAC-IP pairs are displayed in the table of the **Static DHCP** section. To remove a pair, select the checkbox in the relevant line in the table and click the **Remove** button. Then click the **Apply** button.

Wi-Fi

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

Basic Settings

On the **Wi-Fi / Basic settings** page, you can enable the wireless local area network (WLAN) of the access point and configure its basic parameters.

Figure 41. Basic settings of the wireless LAN.

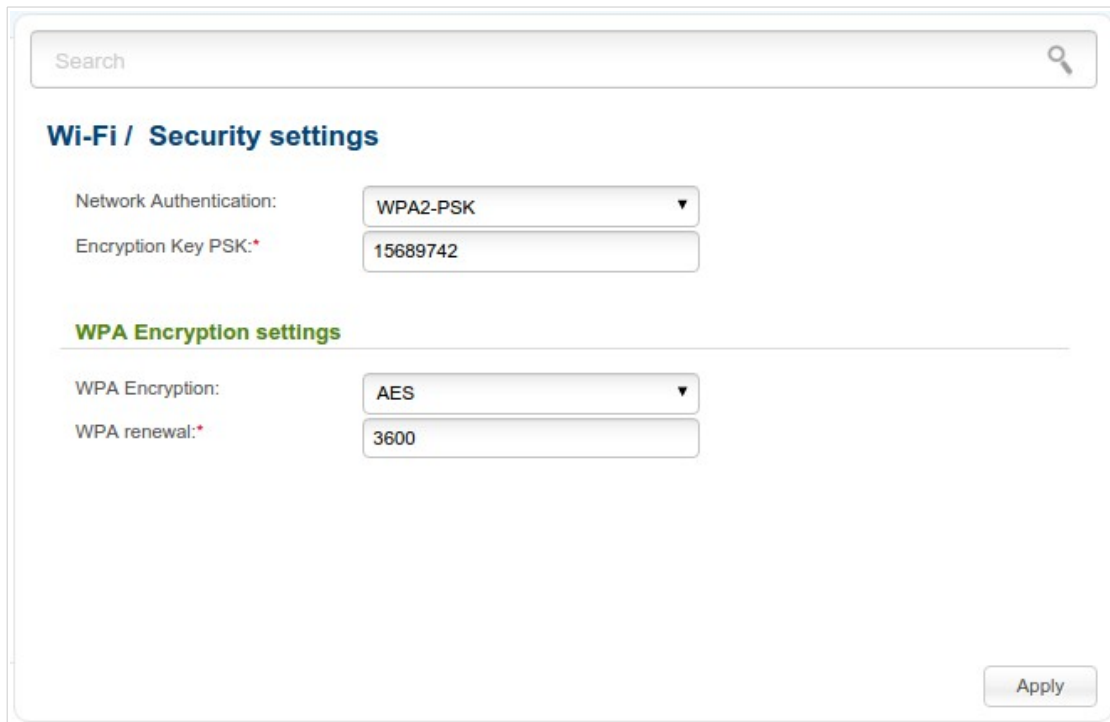
Parameter	Description
Enable Wireless	The checkbox enables Wi-Fi connections. If you want to disable your WLAN, deselect the checkbox.
Broadcast wireless network	If the checkbox is not selected, devices cannot connect to the access point's WLAN (or to the selected part of the WLAN if the network is split into parts). Upon that the device can connect to another access point as a wireless client.

Parameter	Description
MBSSID	<p>To split the network into several parts, select a relevant value (2, 3, or 4) from the drop-down list. By default, the wireless network is not split (the Disabled value is selected from the list).</p> <p>For every part of the WLAN you can specify a name (SSID), some parameters from the basic settings page, and security settings. To do this, select the needed part from the BSSID drop-down list and click the Apply button. Then specify needed parameters on the Wi-Fi / Basic settings page or proceed to the Wi-Fi / Security settings page.</p>
BSSID	<p>The unique identifier for your Wi-Fi network. You cannot change the value of this parameter, it is determined in the device's internal settings.</p> <p>If you have split your WLAN into parts, the drop-down list contains several values. Each identifier corresponds to a single part of the WLAN.</p>
Hide Access Point	<p>If the checkbox is selected, other users cannot see your Wi-Fi network. (It is recommended not to select this checkbox in order to simplify initial configuration of your WLAN.)</p>
SSID	<p>A name for the WLAN. By default, the value DAP-1360 is specified. If your network is split into parts, each part has the default name (DAP-1360.2, DAP-1360.3, and DAP-1360.4). It is recommended to specify another name for the network upon initial configuration (use digits and Latin characters).</p>
Country	<p>The country you are in. Select a value from the drop-down list.</p>
Channel	<p>The wireless channel number. When the auto value is selected, the access point itself chooses the channel with the least interference.</p>
Wireless mode	<p>Operating mode of the wireless network of the access point. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.</p>
Max Associated Clients	<p>The maximum number of devices connected to the wireless network of the access point (or to the selected part of the WLAN if the network is split into parts). When the value 0 is specified, the device does not limit the number of connected clients.</p>
Clients Isolation	<p>Select the checkbox to forbid wireless clients of your WLAN (or the selected part of the WLAN if the network is split into parts) to communicate to each other.</p>

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

Security Settings

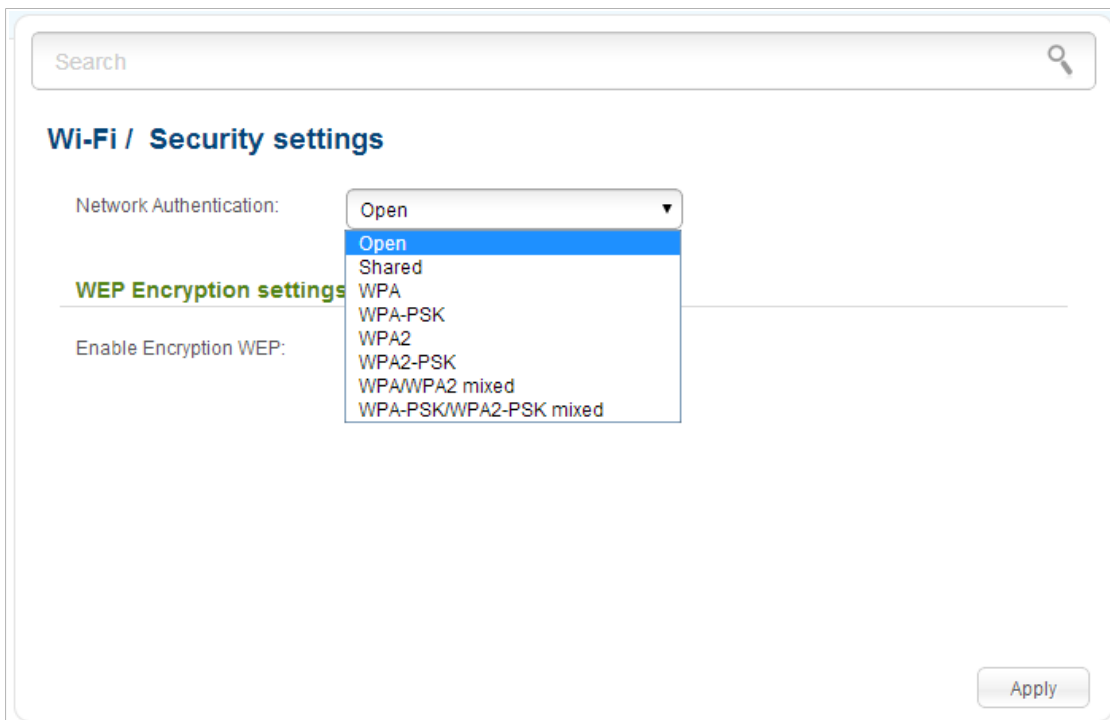
On the **Wi-Fi / Security settings** page, you can modify security settings of the WLAN.



The screenshot shows the 'Wi-Fi / Security settings' page. At the top is a search bar. Below it, the 'Network Authentication' dropdown is set to 'WPA2-PSK' and the 'Encryption Key PSK' field contains '15689742'. Under the 'WPA Encryption settings' section, the 'WPA Encryption' dropdown is set to 'AES' and the 'WPA renewal' field contains '3600'. An 'Apply' button is located at the bottom right.

Figure 42. The default security settings.

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



The screenshot shows the 'Wi-Fi / Security settings' page with the 'Network Authentication' dropdown menu open. The menu lists the following options: Open (highlighted), Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 mixed, and WPA-PSK/WPA2-PSK mixed. The 'Enable Encryption WEP' checkbox is visible below the dropdown. An 'Apply' button is at the bottom right.

Figure 43. 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).
Shared	Shared key authentication with WEP encryption. This authentication type is not available when on the Wi-Fi / Basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected.
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 WLAN of the access point.
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 WLAN of the access point.



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

When the **Open** or **Shared** value is selected, the **WEP Encryption settings** section is displayed (the section is unavailable for the wireless network operating modes which support the standard 802.11n):

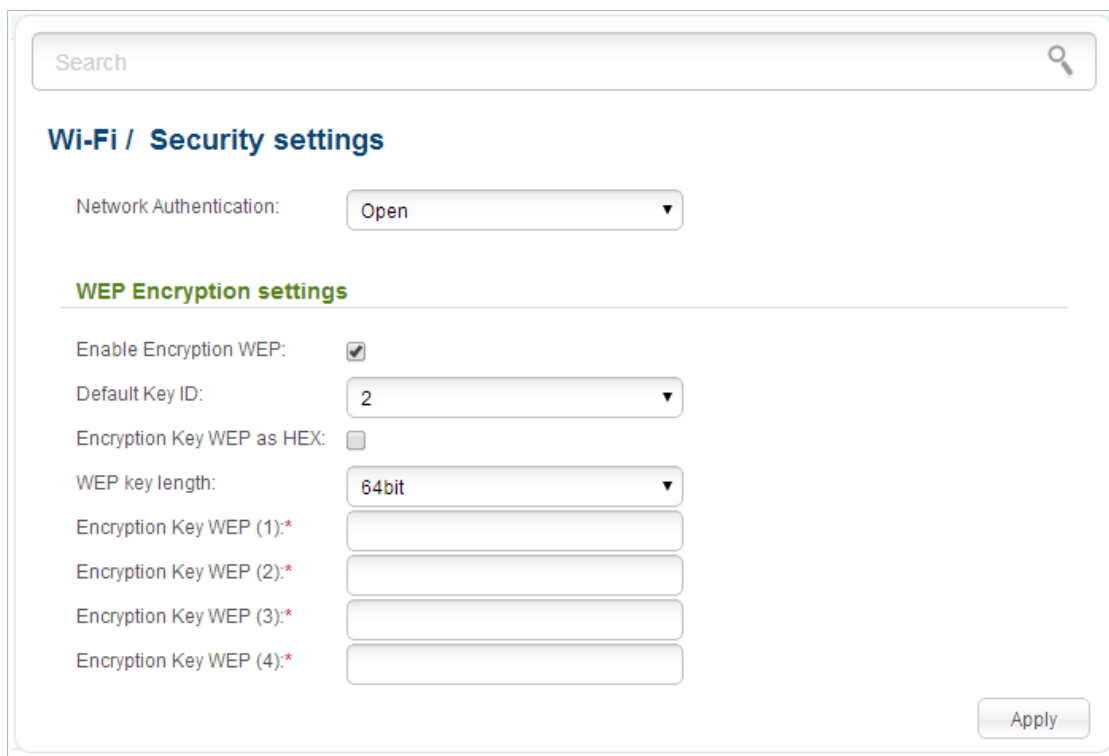


Figure 44. The **Open** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
Enable Encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the Default Key ID field, the Encryption Key WEP as HEX checkbox, the WEP key length drop-down list, and four Encryption Key WEP fields are displayed on the page. For the Shared authentication type the checkbox is always selected.
Default Key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption Key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.
WEP key length	The length of WEP encryption key. Select the value 64bit to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the value 128bit to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Encryption Key WEP (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.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the **WPA Encryption settings** section is displayed:

The screenshot shows a web interface for configuring Wi-Fi security. At the top is a search bar. Below it is the heading "Wi-Fi / Security settings". Under this heading, there are two main sections. The first section, "Network Authentication", has a dropdown menu currently showing "WPA2-PSK" and a text input field for "Encryption Key PSK" containing the value "15689742". The second section, "WPA Encryption settings", has a dropdown menu for "WPA Encryption" set to "AES" and a text input field for "WPA renewal" set to "3600". An "Apply" button is located at the bottom right of the settings area.

Figure 45. The **WPA-PSK/WPA2-PSK mixed** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
Encryption Key PSK	A key for WPA encryption. The key can contain digits and/or Latin characters.
WPA Encryption	An encryption method: TKIP , AES , or TKIP+AES .
WPA renewal	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 the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the **RADIUS settings** and **WPA Encryption settings** sections are available:

The screenshot shows the 'Wi-Fi / Security settings' interface. At the top, there is a search bar. Below it, the 'Network Authentication' dropdown menu is set to 'WPA/WPA2 mixed'. The 'WPA2 Pre-authentication' checkbox is currently unchecked. The 'RADIUS settings' section contains three input fields: 'IP address:*' with the value '192.168.0.254', 'Port:*' with the value '1812', and 'RADIUS encryption key:*' which is empty. The 'WPA Encryption settings' section has a 'WPA Encryption' dropdown set to 'AES' and a 'WPA renewal:*' field with the value '3600'. An 'Apply' button is located at the bottom right of the settings area.

Figure 46. The **WPA/WPA2 mixed** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
WPA2 Pre-authentication	The checkbox activating preliminary authentication (displayed only for the WPA2 and WPA/WPA2 mixed authentication types).
IP address	The IP address of the 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).
WPA Encryption	An encryption method: TKIP , AES , or TKIP+AES .
WPA renewal	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.

MAC Filter

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

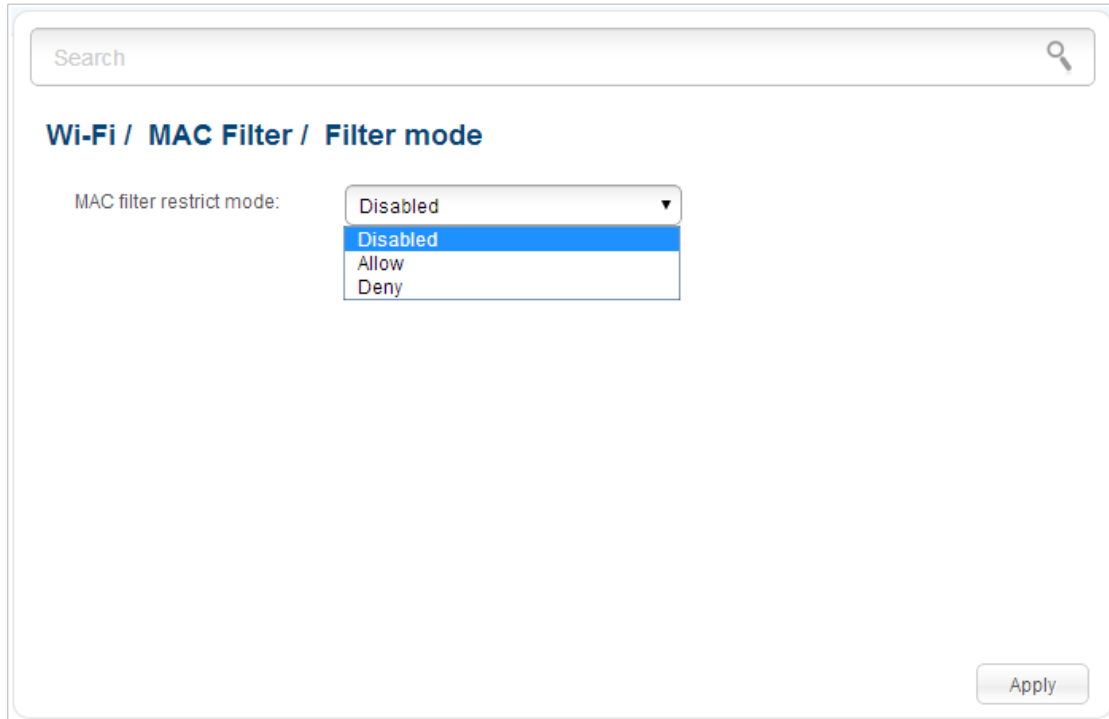


Figure 47. The page for configuring the MAC filter for the wireless network.

By default, MAC filtering is not active (the **Disabled** value is selected from the **MAC filter restrict mode** drop-down list on the **Wi-Fi / MAC Filter / Filter mode** page).

To open your wireless network for the devices which MAC addresses are specified on the **Wi-Fi / MAC Filter / MAC addresses** page and to close the wireless network for all other devices, select the **Allow** value from the **MAC filter restrict mode** drop-down list and click the **Apply** button.

To close your wireless network for the devices which MAC addresses are specified on the **Wi-Fi / MAC Filter / MAC addresses** page, select the **Deny** value from the **MAC filter restrict mode** drop-down list and click the **Apply** button.

To add a MAC address to which the selected filtering mode will be applied, proceed to the **Wi-Fi / MAC Filter / MAC addresses** page.

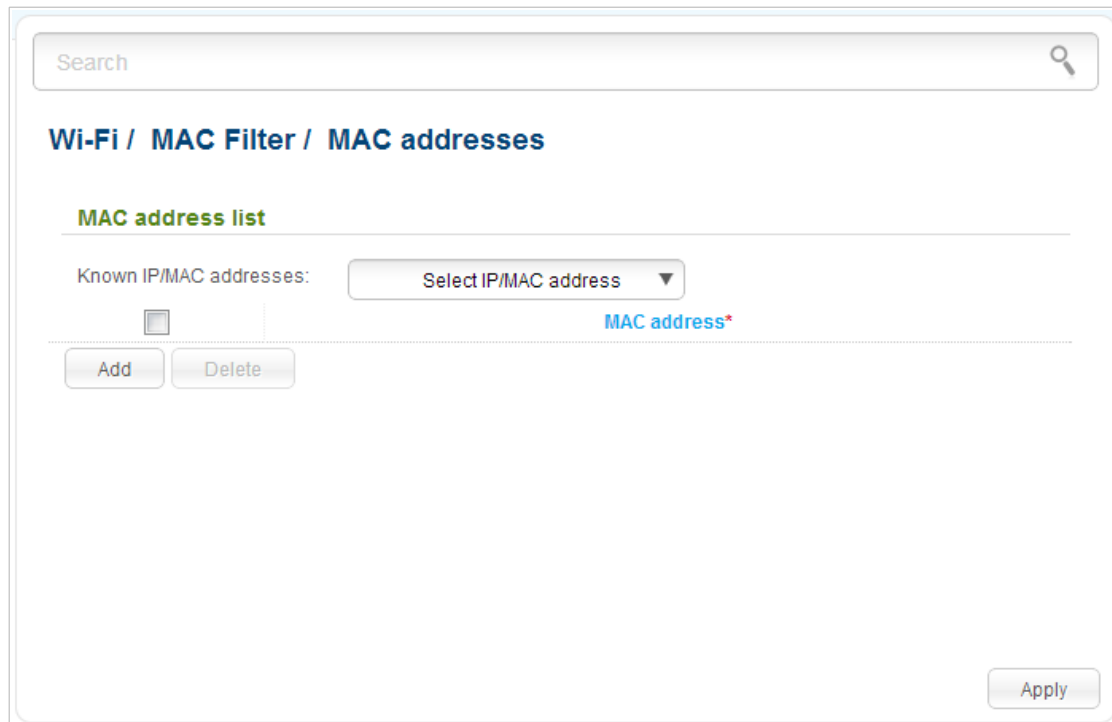


Figure 48. The page for adding a MAC address.

Click the **Add** button and enter an address in the field displayed. Also you can enter the MAC address of a device connected to the LAN of the access point at the moment. To do this, select the relevant device from the **Known IP/MAC addresses** drop-down list (the field will be filled in automatically). Then click the **Apply** button.

To remove a MAC address from the list of MAC addresses, select the checkbox located to the left of the relevant MAC address and click the **Delete** button. Then click the **Apply** button.

List of Wi-Fi Clients

On the **Wi-Fi / List of WiFi clients** page, you can view the list of wireless clients connected to the access point. Devices connected to the access point via the WDS function are not displayed in the list.

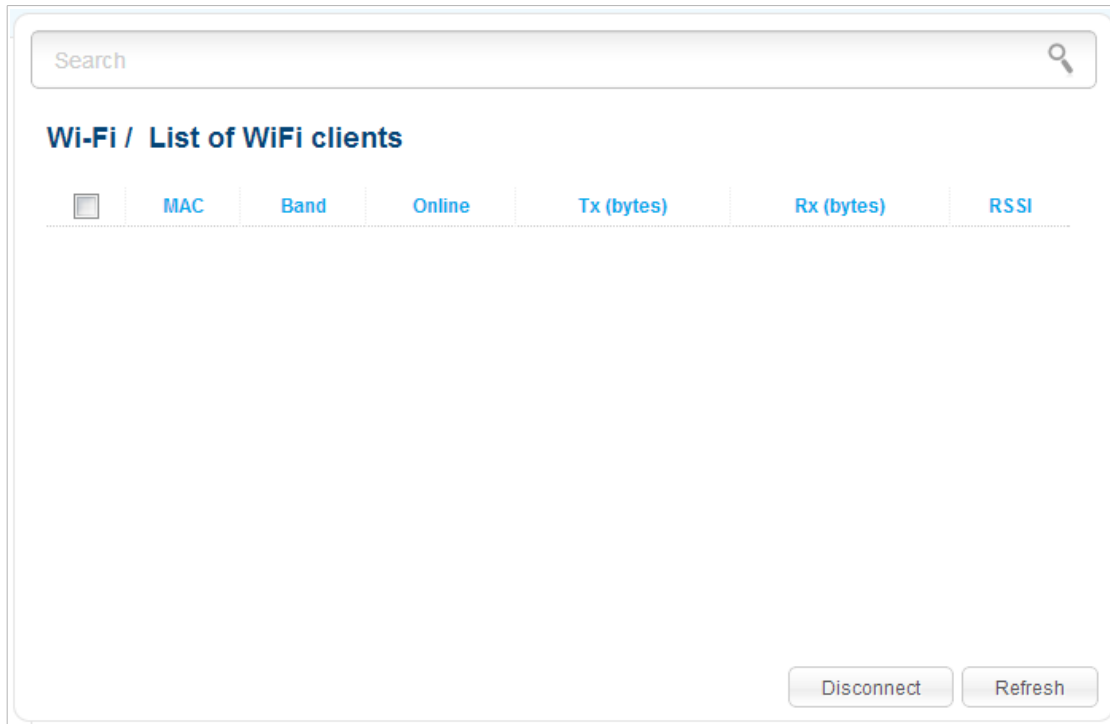


Figure 49. The list of the wireless clients.

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

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

WPS

On the **Wi-Fi / WPS** page, you can enable the function for secure configuration of the WLAN and select a method used to easily add wireless devices 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.

! If the device's WLAN is split into parts (the value **2**, **3**, or **4** is selected from the **MBSSID** drop-down list on the **Wi-Fi / Basic settings** page), the WPS function can be used only for the first part of the WLAN (the first value from the **BSSID** drop-down list).

! 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 (on the **Wi-Fi / Security settings** page). When other security settings are specified, controls of the **Wi-Fi / WPS** page are not available.

Search

Wi-Fi / WPS

Enable/Disable WPS

WPS Enable:

Apply

Information

Default PIN code:	12345670
WPS Status:	Configured
SSID:	DAP-1360
Network Authentication:	WPA2-PSK
Encryption:	AES
Encryption key:	76543210

Refresh Reset to unconfigured

Connection

WPS Method: PBC

Connect

Figure 50. The page for configuring the WPS function.

To activate the WPS function, select the **WPS Enable** checkbox and click the **Apply** button. When the checkbox is selected, the **Information** and **Connection** sections are available on the page.

Parameter	Description
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.
WPS Status	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).
SSID	The name of the access point's WLAN (or the first part of the WLAN if the network is split into parts).
Network Authentication	The network authentication type specified for the WLAN (or the first part of the WLAN).
Encryption	The encryption type specified for the WLAN (or the first part of the WLAN).
Encryption key	The encryption key specified for the WLAN (or the first part of the WLAN).
Refresh	Click the button to refresh the data on the page.
Reset to unconfigured	Click the button to reset the parameters of the WPS function.
WPS Method	A method of the WPS function. Select a value from the drop-down list. PIN : Connecting the device via the PIN code. PBC : Connecting the device via the push button (actual or virtual).
PIN Code	The PIN code of the WPS-enabled device that needs to be connected to the wireless network of the access point. The field is displayed only when the PIN value is selected from the WPS Method drop-down list.
Connect	Click the button to connect the wireless device to the access point's WLAN via the WPS function.

Using WPS Function via Web-based Interface

To add a wireless device via the PIN method of the WPS function, follow the next steps:

1. Select the **WPS Enable** checkbox.
2. Click the **Apply** button.
3. 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 add a wireless device via the PBC method of the WPS function, follow the next steps:


1. Select the **WPS Enable** checkbox.
2. Click the **Apply** button.
3. 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. Click the **Connect** button in the web-based interface of the access point.

Using WPS Function without Web-based Interface

You can add a wireless device to the access point's WLAN 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 corresponding security settings for the wireless network of the access point.
2. Select the **WPS Enable** checkbox.
3. Click the **Apply** button.

4. Save the settings and close the web-based interface (click the icon  (**Save**) in the menu displayed when the mouse pointer is over the **System** caption in the top left part of

the page, then click the icon  (**Logout**)).

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

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.

Search

Wi-Fi / WDS

WDS Mode: Bridge mode

WDS Encryption : NONE

Encryption Key:

WDS MAC (1):

WDS MAC (2):

WDS MAC (3):

WDS MAC (4):

Apply

Figure 51. The page for configuring the WDS function.

The following fields are available on the page:

Parameter	Description
WDS Mode	The WDS function mode. 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.
WDS Encryption	A type of encryption for data transfer between access points interconnected via the WDS function. NONE: No encryption. WEP. TKIP. AES.
Encryption Key	A key for the specified type of encryption. If the NONE value is selected from the WDS Encryption drop-down list, the field is not editable.
WDS MAC (1-4)	The MAC addresses of devices connected to the access point via the WDS function.

! 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.

Additional Settings

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

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

Figure 52. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
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.
Beacon Period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS Threshold	The minimum size (in bites) of a packet for which an RTS frame is transmitted.
Frag Threshold	The maximum size (in bites) 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.

Parameter	Description
TX Power	The transmit power (in percentage terms) of the access point.
Drop multicast	Select the checkbox to disable multicasting for the access point's WLAN. Deselect the checkbox to enable multicasting from WAN connections for which the Enable IGMP Multicast checkbox is selected.
Bandwidth	The channel bandwidth for 802.11n devices. 20MHz : 802.11n devices operate at 20MHz channels. 40MHz : 802.11n devices operate at 40MHz channels. 20/40MHz - : 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the previous adjacent channel). 20/40MHz + : 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the next adjacent channel).
Short GI	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the access point is communicating to wireless devices. Enable : the access point uses the 400 ns short guard interval. For the wireless network operating modes which support 802.11n standard only (see the value of the Wireless mode drop-down list on the Wi-Fi / Basic settings page). Disable : the access point uses the 800 ns standard guard interval.
Adaptivity Mode	Select the checkbox to prevent your wireless network from interfering with radars and other mobile or stationary radio systems. Such a setting can slow down the WLAN of the access point.

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.

To enable the function, select the **WMM** checkbox and click the **Apply** button.

Wi-Fi / WMM

WMM:

Parameters of Access Point

AC	Aifsn (1~15)*	CWMin	CWMax	Txop*	ACM	Ack
AC_BK	7	1	1023	0	Off	Off
AC_BE	3	15	63	0	Off	Off
AC_VI	1	7	15	94	Off	Off
AC_VO	1	3	7	47	Off	Off

Parameters of Station

AC	Aifsn (1~15)*	CWMin	CWMax	Txop*	ACM
AC_BK	7	15	1023	0	Off
AC_BE	3	15	1023	0	Off
AC_VI	2	7	15	94	Off
AC_VO	2	3	7	47	Off

Apply

Figure 53. The page for configuring the WMM function.

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

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

- **AC_BK** (*Background*), low priority traffic (print jobs, file downloads, etc.).
- **AC_BE** (*Best Effort*), traffic from legacy devices or devices/applications that do not support QoS.
- **AC_VI** (*Video*).
- **AC_VO** (*Voice*).

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

For every Access Category the following fields are available:

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.
Txop	<i>Transmission Opportunity.</i> The higher the value, the higher is the Access Category priority.
ACM	<i>Admission Control Mandatory.</i> If on, prevents from using the relevant Access Category.
Ack	<i>Acknowledgment.</i> Answering response requests while transmitting. Displayed only in the Parameters of Access Point section. If off, the access point answers requests. If on, the access point does not answer requests.

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

Client

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

The “client” function in the access point mode allows using DAP-1360U as a wireless client and a wireless repeater.

To use the access point as a wireless repeater, you need to configure the same parameters of the wireless connection (the name of the wireless network, encryption parameters, and the channel) for DAP-1360U and the remote access point.

To use the access point as a wireless client, you need to configure the same channel of the wireless connection for DAP-1360U and the remote access point. Other parameters of the wireless network of DAP-1360U do not depend upon the settings of the remote access point.

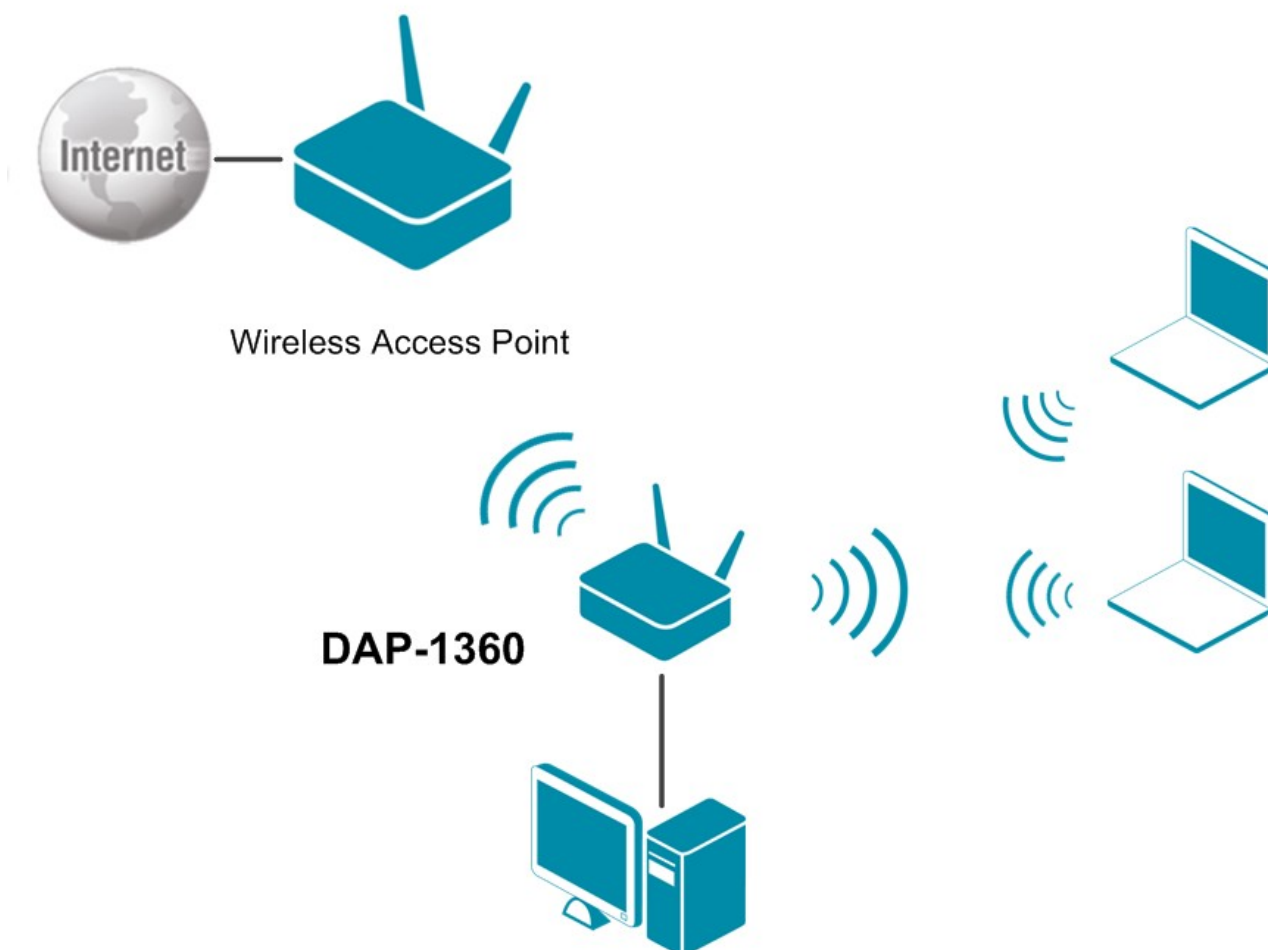


Figure 54. Connecting DAP-1360U in the access point mode as a client.

To allow the devices from the LAN of DAP-1360U to obtain the IP addresses from the DHCP server of the remote access point or network, it is necessary to disable the built-in DHCP server of the device. To do this, proceed to the **Net / LAN** page; then in the **DHCP server** section, in the **Mode** drop-down list, select the **Disable** value and click the **Apply** button.

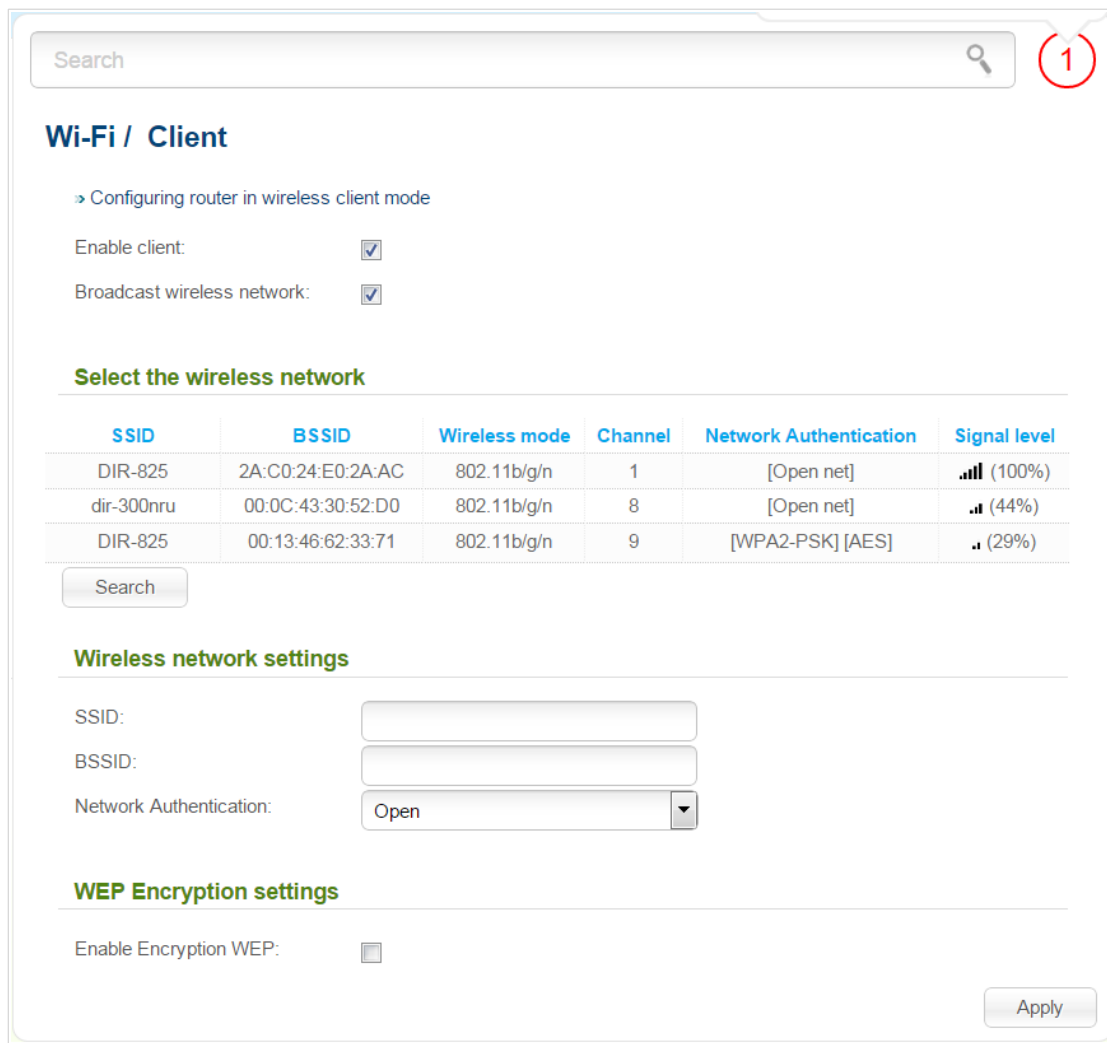


Figure 55. The page for configuring the client mode.

To configure the access point as a client, select the **Enable client** checkbox. When the checkbox is selected, the following fields are displayed on the page:

Parameter	Description
Broadcast wireless network	If the checkbox is not selected, devices cannot connect to the access point's WLAN. Upon that DAP-1360U can connect to another access point as a wireless client.
Wireless network settings	
SSID	The name of the network to which the access point connects.
BSSID	The unique identifier of the network to which the access point connects.
Network Authentication	The authentication type of the network to which the access point connects.

When the **Open** or **Shared** authentication type is selected, the following fields are available:

Parameter	Description
Enable Encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the Default Key ID field, the Encryption Key WEP as HEX checkbox, the WEP key length drop-down list, and four Encryption Key WEP fields are displayed on the page. For the Shared authentication type the checkbox is always selected.
Default Key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption Key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.
WEP key length	The length of WEP encryption key. Select the value 64bit to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the value 128bit to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Encryption Key WEP (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.

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

Parameter	Description
Encryption Key PSK	A key for WPA encryption. The key can contain digits and/or Latin characters.
WPA Encryption	An encryption method: TKIP , AES , or TKIP+AES .

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

In addition, when the **Enable client** checkbox is selected, the list of available wireless networks is displayed on the page.

To view the latest data on the available wireless networks, click the **Search** button.

To connect to a wireless network from the list, select the needed network. Upon that the relevant values are automatically inserted in the **SSID**, **BSSID**, and **Network Authentication** fields.

For the **Open** authentication type with no encryption, click the **Apply** button.

For the **Open** authentication type with encryption and the **Shared** authentication type, select a needed value from the **Default Key ID** drop-down list. If needed, select the **Encryption Key WEP as HEX** checkbox to set a hexadecimal number as a key for encryption. Then select a needed value in the **WEP key length** drop-down list, fill in 4 **Encryption Key WEP** fields, and click the **Apply** button.

For the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** authentication types, fill in the **Encryption Key PSK** field and click the **Apply** button.

After clicking the **Apply** button, the wireless channel of DAP-1360U will switch to the channel of the wireless access point to which you have connected.

If the access point is connected to the selected network successfully, the green indicator appears to the right of the network's SSID in the table.

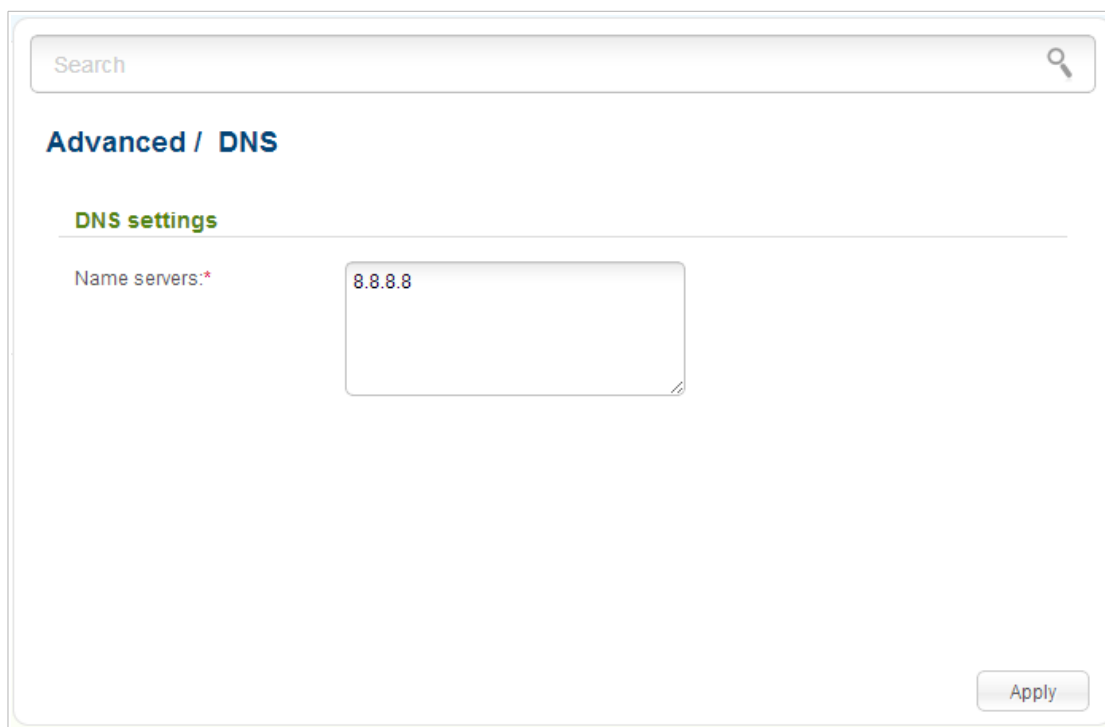
The step-by-step description of how to configure the access point as a wireless client is available on D-Link website. To access it, click the **Configuring router in wireless client mode** link in the top part of the page.

Advanced

In this menu you can add name servers.

DNS

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



The screenshot shows a web interface for configuring DNS settings. At the top, there is a search bar with the placeholder text "Search" and a magnifying glass icon. Below the search bar, the page title "Advanced / DNS" is displayed in blue. Underneath, the section "DNS settings" is highlighted in green. The main content area features a label "Name servers:*" followed by a text input field containing the IP address "8.8.8.8". At the bottom right of the page, there is an "Apply" button.

Figure 56. 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).

On this page, you can specify the addresses of DNS servers manually.



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

If you want to specify the DNS server, enter a DNS server address in the **Name servers** list. To specify several addresses, press the **Enter** key and enter a needed address in the next line. Then click the **Apply** button.

To remove a DNS server from the system, remove the relevant line from the **Name servers** field and click the **Apply** button.

System

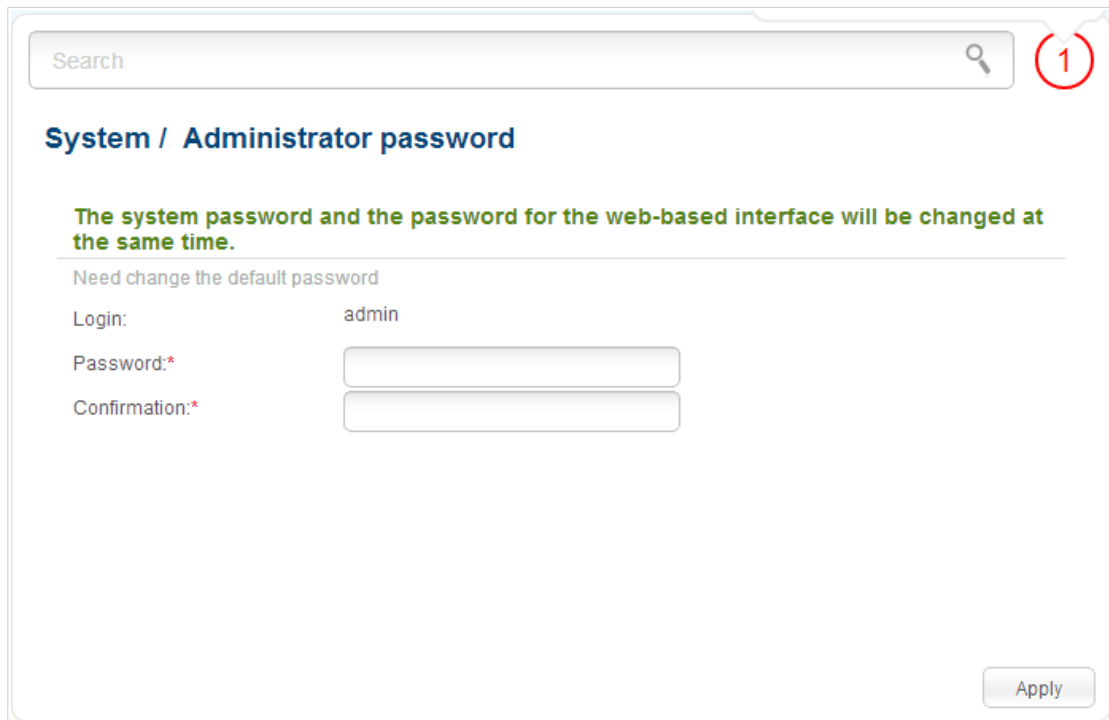
In this menu you can do the following:

- change the password used to access the access point's settings
- save the current settings to the non-volatile memory
- reboot the access point
- create a backup of the access point's configuration
- restore the access point's configuration from a previously saved file
- restore the factory default settings
- view the system log
- update the firmware of the access point
- configure automatic notification on new firmware version
- configure automatic synchronization of the system time or manually configure the date and time for the access point
- 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
- switch the device to the other mode.

Administrator Password

On the **System / Administrator password** 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.

! For security reasons, it is strongly recommended to change the administrator password upon initial configuration of the access point.



Search

System / Administrator password

The system password and the password for the web-based interface will be changed at the same time.

Need change the default password

Login: admin

Password:*

Confirmation:*

Apply

Figure 57. The page for modifying the administrator password.

Enter the new password in the **Password** and **Confirmation** fields and click the **Apply** button.

Configuration

On the **System / Configuration** page, you can reboot the device, save the changed settings to the non-volatile memory, restore the factory defaults, backup the current configuration, or restore the access point's configuration from a previously created file.

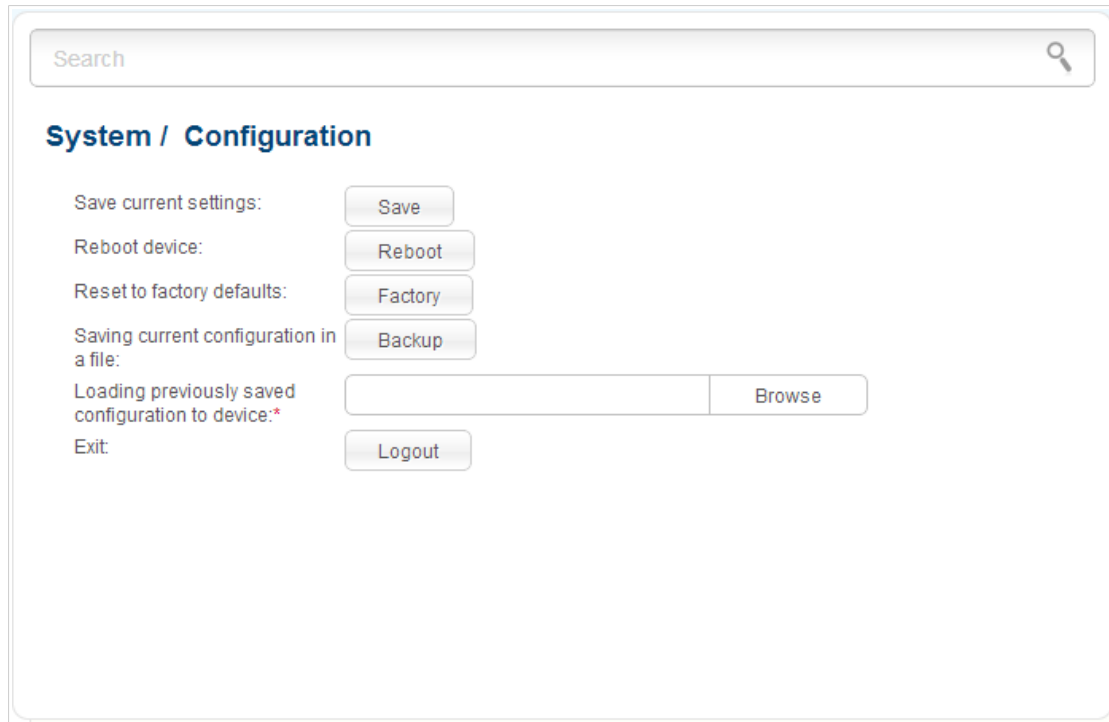


Figure 58. The **System / Configuration** page.

The following buttons are available on the page:

Control	Description
Save	Click the button to save settings to the non-volatile memory. Please, save settings every time you change the device's parameters. Otherwise the changes will be lost upon hardware reboot of the access point.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button located on the bottom panel of the access point (see the <i>Back and Bottom Panels</i> section, page 11).
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.
Browse	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.
Logout	Click the button to exit the web-based interface.

Actions of the **Save**, **Reboot**, **Factory**, **Backup**, and **Logout** buttons also can be performed via the top-page menu displayed when the mouse pointer is over the **System** caption.

System Log

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

Figure 59. The **System / System log / Configuration** page.

To enable logging of the system events, select the **Logging** checkbox. Then specify the needed parameters.

Control	Description
Logging 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 device's memory (and displayed on the System / System log / Log page). When this value is selected, the Server and Port fields are not displayed. • Remote: the system log is sent to the remote host specified in the Server field. • Local and remote: the system log is stored in the device's memory (and displayed on the System / System log / Log page) and sent to the remote host specified in the Server field.
Logging level	Select a type of messages and alerts/notifications to be logged.
Server	The IP or URL address of the host from the local or global network, to which the system log will be sent.

Control	Description
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, deselect the **Logging** checkbox and click the **Apply** button.

On the **System / System log / Log** page, the events specified in the **Logging level** list are displayed.

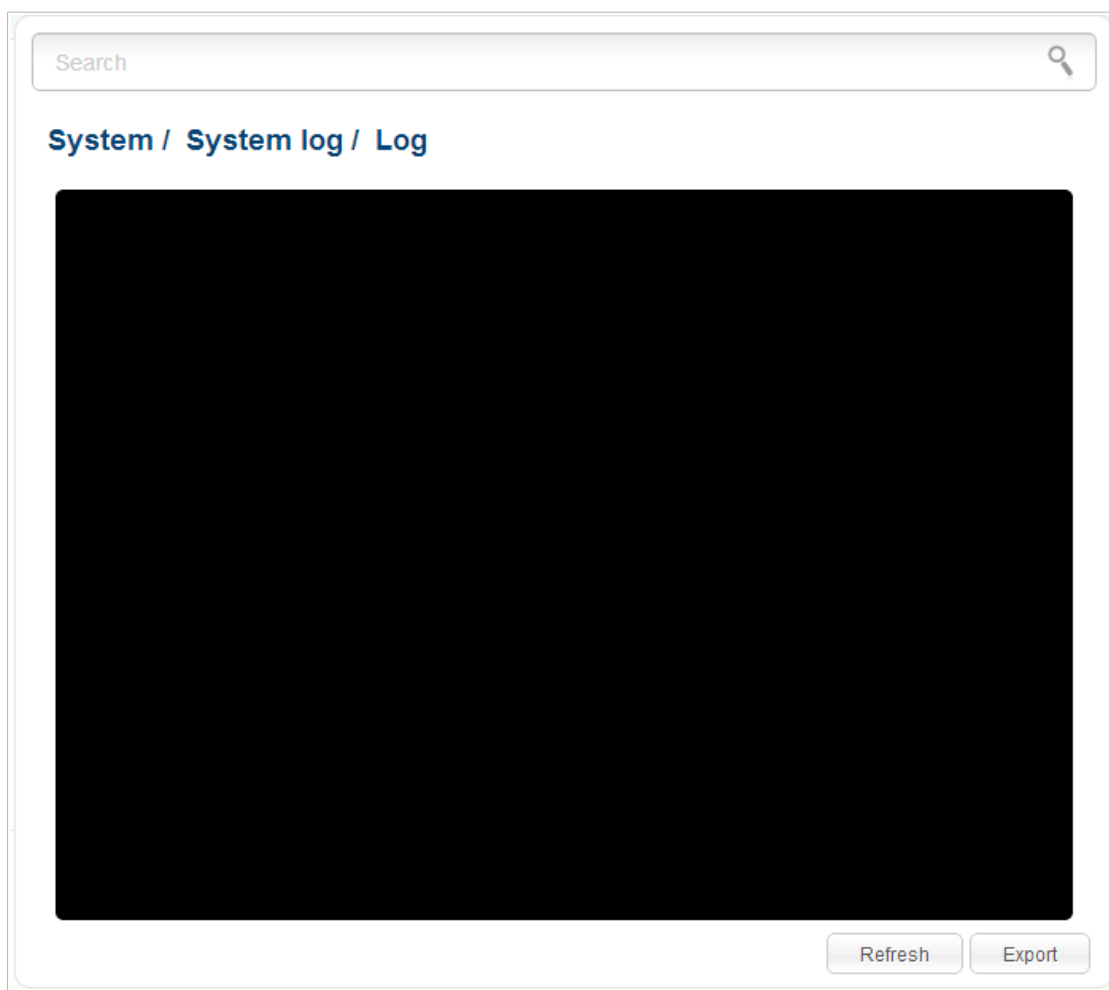


Figure 60. The **System / System log / Log** page.

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

To save the system log to your PC, click the **Export** button and follow the dialog box appeared.

Firmware Upgrade

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



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

Search

System / Firmware upgrade

Local update

Select update file:* Browse

Update

Remote update

Check for updates automatically:

Remote server URL:

Check for updates Apply settings

Figure 61. The **System / Firmware upgrade** page.

The current version of the access point's firmware is displayed next the D-Link logo in the top left corner of the page.

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, deselect the **Check for updates automatically** checkbox and click the **Apply settings** button.

To enable the automatic check for firmware updates, in the **Remote update** section, select the **Check for updates automatically** checkbox 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 upgrade 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 upgrade 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 **Browse** button on the **System / Firmware upgrade** page to locate the new firmware file.
3. Click the **Update** button to upgrade the firmware of the access point.
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.

After the upgrade is completed, the new version of the firmware will be displayed in the top left corner of the page.

If after updating the firmware the access point doesn't work correctly, please restore the factory default settings. To do this, place the mouse pointer over the **System** caption in the top left corner

of the page and click the  (**Reset to factory**) icon. Wait until the access point is rebooted.

Remote Update

! Attention! Do not turn off the access point before the firmware upgrade 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 upgrade** page, in the **Remote update** section, click the **Check for updates** button to check if a newer firmware version exists.
2. Click the **OK** button in the window displayed to upgrade the firmware of the access point. Also you can upgrade the firmware of the access point by clicking the **Remote update** 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.

After the upgrade is completed, the new version of the firmware will be displayed in the top left corner of the page.

If after updating the firmware the access point doesn't work correctly, please restore the factory default settings. To do this, place the mouse pointer over the **System** caption in the top left corner

of the page and click the  (**Reset to factory**) icon. Wait until the access point is rebooted.

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.

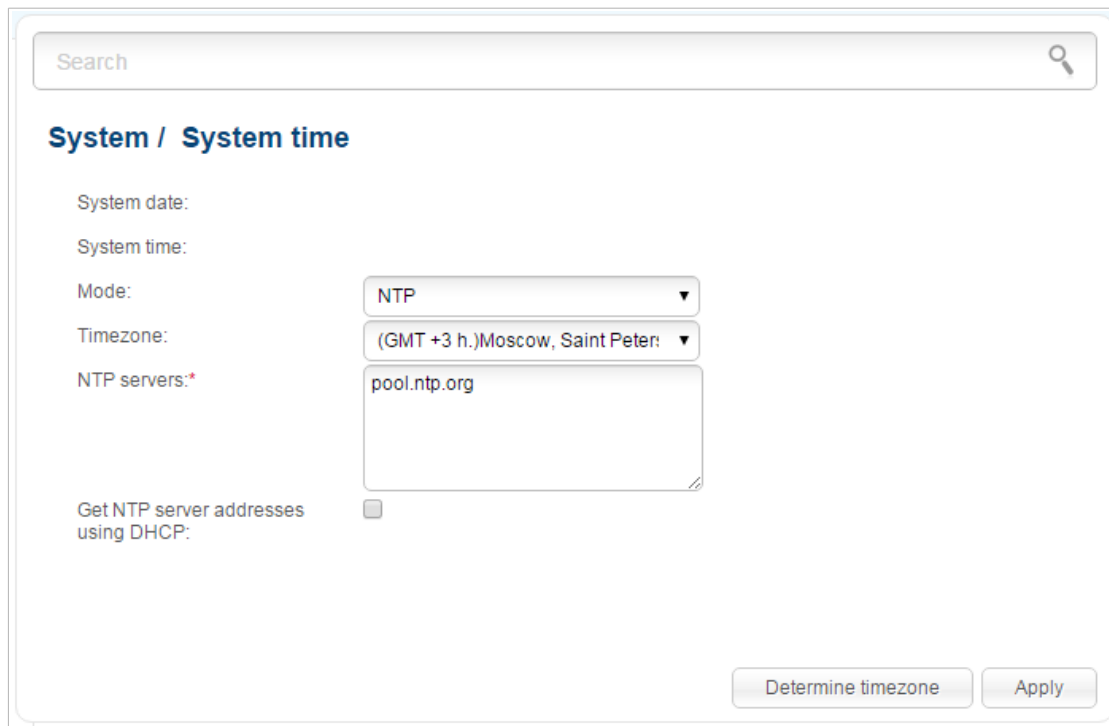


Figure 62. The **System / System time** page.

To set the system time manually, select the **Manual** value from the **Mode** drop-down list and set the time and date in the fields displayed. Then click the **Apply** button.

To enable automatic synchronization with a time server, follow the next steps:

1. Select the **NTP** value from the **Mode** drop-down list.
2. Select your time zone from the drop-down list. To set the time zone in accordance with the settings of your operating system, click the **Determine timezone** button in the bottom right corner of the page.
3. Specify the needed NTP server in the **NTP servers** field or leave the server specified by default.
4. Click the **Apply** button.

In some cases NTP servers addresses are provided by your ISP. In this case, you need to select the **Get NTP server addresses using DHCP** checkbox. Contact your ISP to clarify if this checkbox needs to be enabled. If the **Get NTP server addresses using DHCP** checkbox is selected, the **NTP servers** field is not available.

After clicking the **Apply** button, the date and time set for the access point will be displayed in the **System date** and **System time** fields.



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).

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.

The screenshot shows a web interface for the 'System / Ping' utility. At the top, there is a search bar with the placeholder text 'Search' and a magnifying glass icon. Below the search bar, the page title 'System / Ping' is displayed in a bold, blue font. Underneath the title, there are two input fields: 'Host*' (with an asterisk indicating it is required) and 'Count of packets:'. The 'Host*' field is a standard text input box, and the 'Count of packets:' field is a dropdown menu currently showing the value '1'. At the bottom right of the form area, there is a 'Start' button.

Figure 63. The **System / Ping** page.

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

Traceroute

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



Search

System / Traceroute

Traceroute

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

Host:*

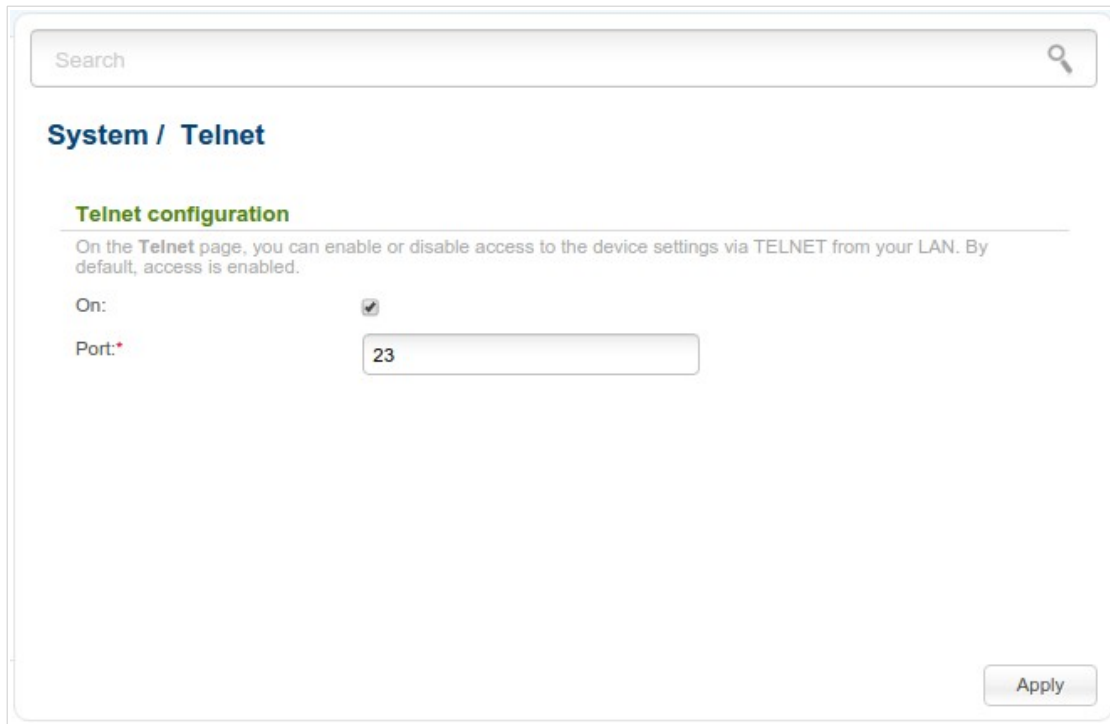
Start

Figure 64. The **System / Traceroute** page.

To define the route, enter the name or IP address of a host in the **Host** field and click the **Start** button. After a while, the results will be displayed on the page.

Telnet

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



Search

System / Telnet

Telnet configuration

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

On:

Port:*

Apply

Figure 65. The **System / Telnet** page.

To disable access via TELNET, deselect the **On** checkbox and click the **Apply** button.

To enable access via TELNET again, select the **On** checkbox. 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.

Device mode

On the **System / Device mode** page, you can change the operating mode of the device.

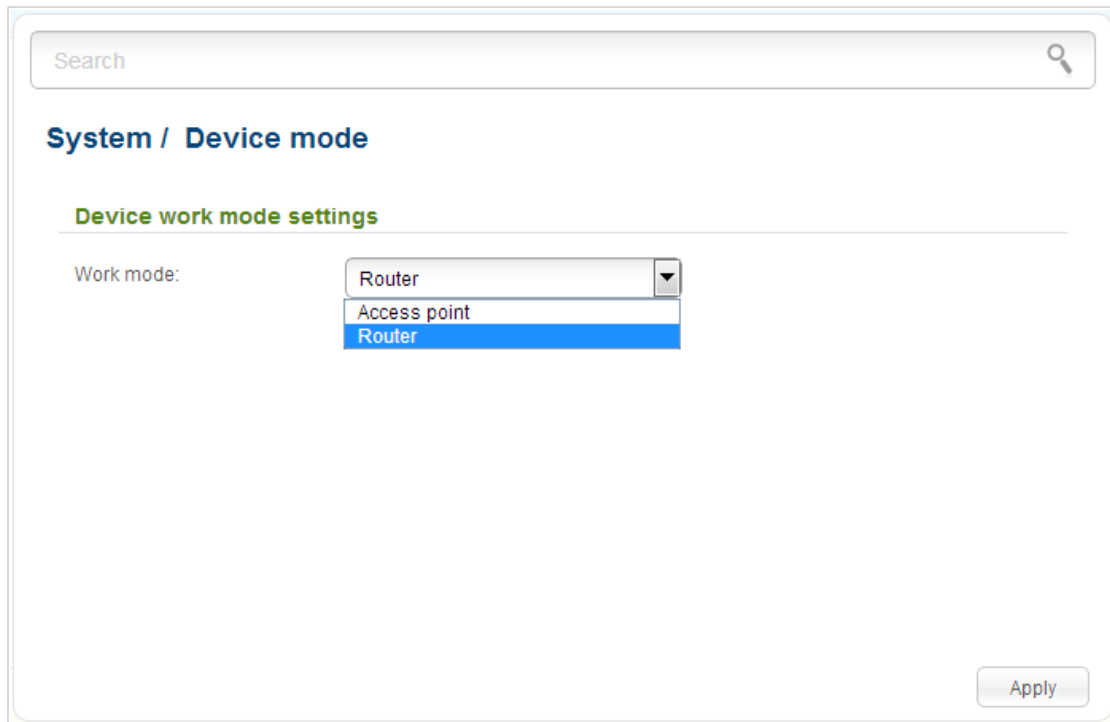


Figure 66. The page for changing the operating mode of the device.

To switch the device to the other mode, select the **Router** value from the **Work mode** drop-down list and click the **Apply** button. In the opened dialog box, click the **OK** button to save new settings and immediately reboot the access point.

CHAPTER 5. CONFIGURING DEVICE (ROUTER MODE)

Monitoring

The page displays an interactive scheme which illustrates the access point's settings and the LAN structure.

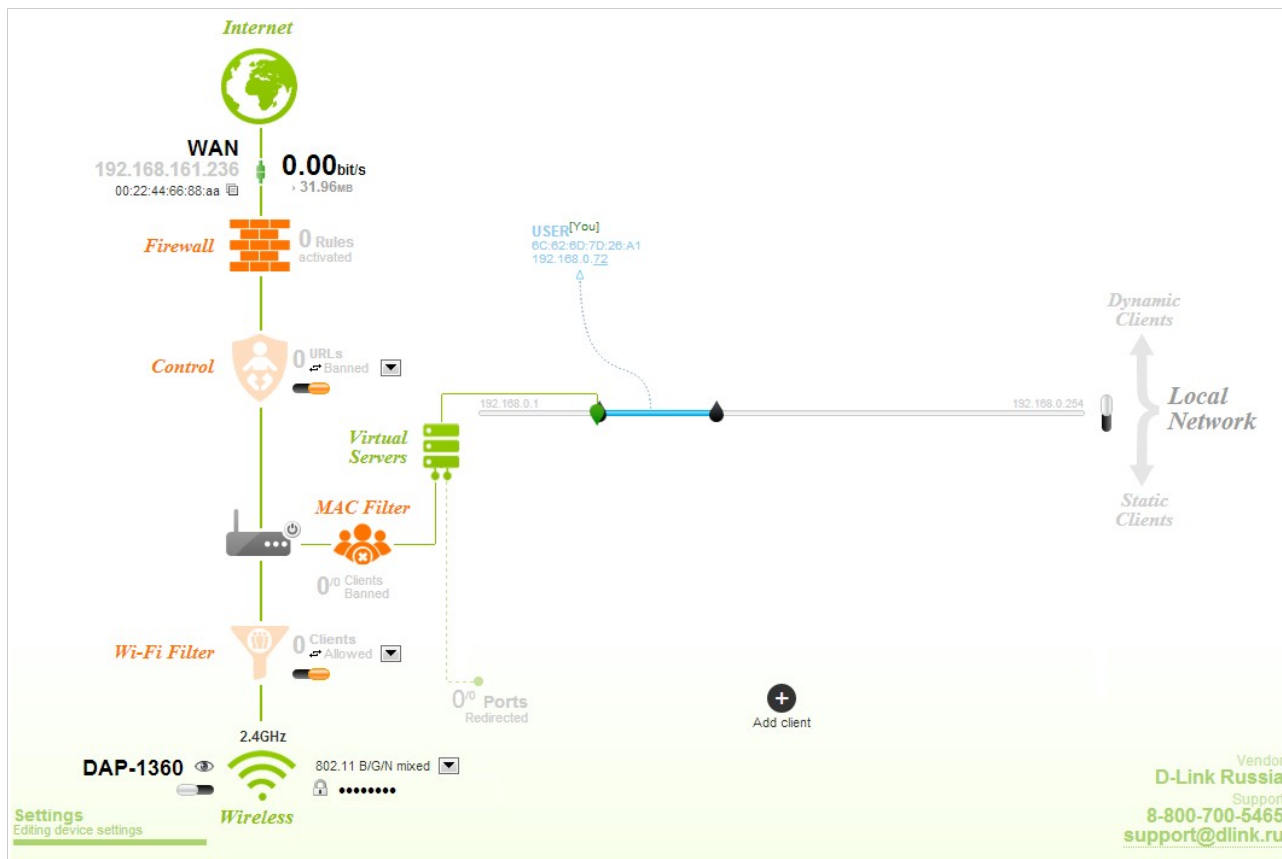











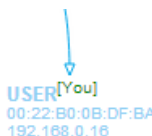


Figure 67. The Monitoring page.

Also you can modify the basic parameters of the access point on the **Monitoring** page. To access the access point's advanced settings, click the **Editing device settings** link in the bottom left corner of the page. For the detailed description of all the access point's functions, see the relevant section of this manual.

The interactive scheme displays the following elements:

Control	Description
 <p>Internet</p>	<p>The Internet element displays information on the active connection. Place the mouse pointer over the icon to switch to another connection, remove existing connections, or add new ones.</p> <p>If the Ethernet cable provided by your ISP is connected to the WAN port of the access point, to the left, the name of the active connection, received or specified IP address, and the MAC address of this connection are displayed. You can change the MAC address in the editing mode or clone the MAC address of a connected device by placing the mouse pointer over the Clone MAC address icon ().</p> <p>To the right, the approximate data transfer rate and the total value of the received data are displayed.</p>
 <p>Firewall</p>	<p>The Firewall element displays the number of the IP filter active rules. Place the mouse pointer over the icon to view the list of the IP filter rules, remove existing rules, add new ones, or quickly switch the filtering mode for a rule.</p>
 <p>Control</p>	<p>The Control element displays the number of blocked/allowed web sites. Place the mouse pointer over the icon to view the list of web sites, remove existing entries, or add new ones.</p> <p>Use the Enable/Disable URL-filter switch () to enable or disable the URL filter.</p> <p>Use the drop-down list to the right of the element to quickly change the operating mode: block access to web sites from the list or allow access to web sites from the list.</p>
 <p>Device</p>	<p>The Device element displays the layout of your device. Place the mouse pointer over the top right corner of this icon to display the system menu which helps you to reboot the device, save the configuration, restore the factory default settings, update the firmware, exit the web-based interface.</p>
 <p>MAC Filter</p>	<p>The MAC Filter element displays the total number of clients to which the filtering rules are applied and the number of blocked clients. Place the mouse pointer over the icon to view the list of filtered clients, remove existing clients, add new ones, or quickly switch the filtering mode for a client.</p>

Control	Description
 <p data-bbox="225 456 453 488">Virtual Servers</p>	<p>The Virtual Servers element is designed for redirecting incoming traffic to a specific IP address in the LAN. It displays the total number of rules for redirecting traffic and the number of rules active in this specific LAN. Place the mouse pointer over the icon to view the list of all rules for redirecting traffic, remove existing rules, or add new ones.</p>
 <p data-bbox="293 757 384 788">DHCP</p>	<p>The DHCP element is a scale where the range of the DHCP server addresses is placed. Dynamic clients receive IP addresses from this range.</p> <p>Use the Enable/Disable DHCP Server switch () to enable or disable DHCP server. If you want to change the range, enter a value from the keyboard in the editing mode or move the sliders. In the editing mode, you can specify the subnet mask.</p>
 <p data-bbox="213 1111 467 1142">Dynamic Clients</p>	<p>The Dynamic Clients area displays all connected dynamic clients. An icon of a client displays the name of a device, its MAC address, and received IP address. The list of actions available for each client is displayed when the mouse pointer is over an icon. If you want to assign the current IP address to the MAC address of the client, drag and drop its icon to the static clients area.</p>
 <p data-bbox="236 1413 443 1444">Static Clients</p>	<p>The Static Clients area displays all static clients. An icon of a client displays the name of a device, its MAC address, and received IP address. The list of actions available for each client is displayed when the mouse pointer is over an icon. If you want to break the binding between the MAC address of the client and its current IP address, drag and drop its icon to the dynamic clients area. Use the Add client button to add static clients.</p>

Control	Description
 <p>Wireless</p>	<p>The Wireless element displays information on Wi-Fi module operation. To the left, the name of the access point is displayed. You can change it in the editing mode.</p> <p>Use the Hide Access Point switch (/) to forbid or allow other users to see your wireless network.</p> <p>Use the Enable/Disable Wireless switch () to enable or disable your wireless network.</p> <p>To the right, the standards of devices which can connect to the access point are displayed. You can select other standards from the drop-down list.</p> <p>Use the Enable/Disable password protection switch (/) to modify security settings of your wireless network. If you want to view or change the password, switch to the editing mode of the relevant field.</p>
 <p>Wireless (Client Mode)</p>	<p>The Wireless (Client Mode) element displays operation of Wi-Fi module in the client mode. To the right of the graphical representation of another access point, its name and MAC address are displayed.</p> <p>Use the Disable client mode switch () to disable the client mode.</p>
 <p>Wi-Fi Filter</p>	<p>The Wi-Fi Filter element displays the number of MAC addresses specified in the MAC filter. The element is unavailable when the Wi-Fi module is in the client mode. Place the mouse pointer over the icon to view the list of MAC addresses, remove existing addresses, or add new ones.</p> <p>Use the Enable/Disable Wi-Fi filter switch () to enable or disable the Wi-Fi filter.</p> <p>Use the drop-down list to the right of the element to quickly change the mode of the filter (allow or forbid access to your wireless network).</p>

In this section, you can contact the technical support group (to send an e-mail). To do this, left-click the support e-mail address in the bottom right corner of the page. After clicking the line, the e-mail client window for sending a new letter to the specified address opens.

Click'n'Connect

To configure connection to the Internet, click the **Click'n'Connect** link in the **Home** section.



Figure 68. Configuring connection to the Internet.

Connect the Ethernet cable provided by your ISP to the WAN port of the access point. Verify the relevant LED (the **Internet** LED should be on).

Click the **Next** button to continue.

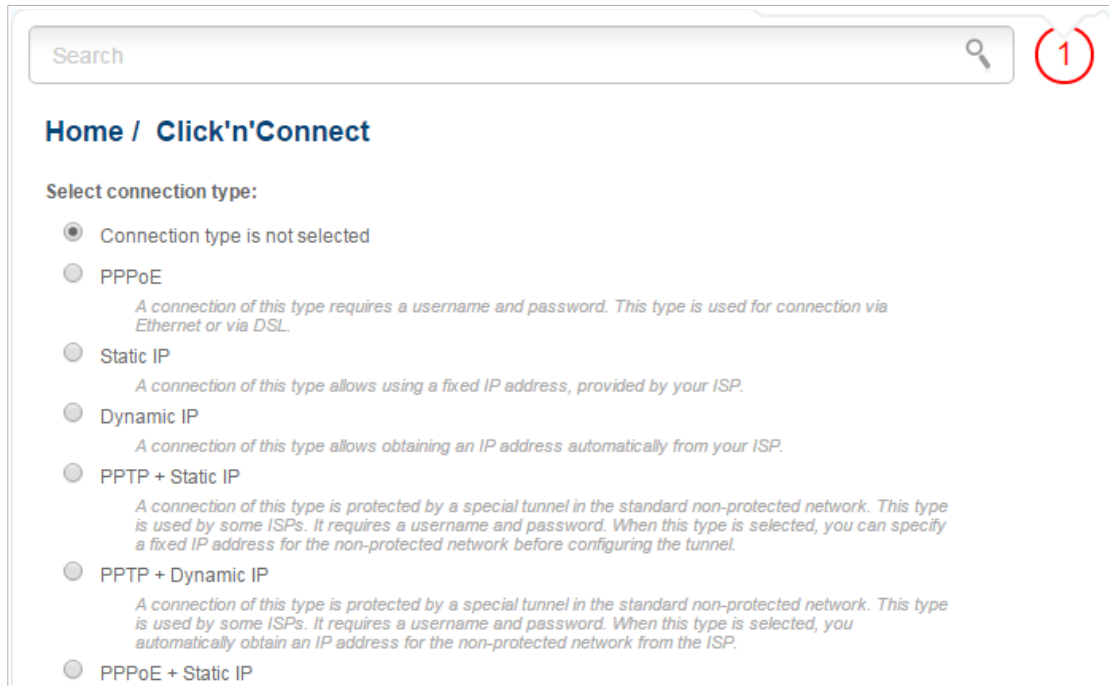


Figure 69. The page for selecting the connection type.

On the opened page, select the needed choice of the radio button and click the **Next** button.

Creating WAN Connection

PPPoE Connection

Search

Home / Click'n'Connect

Connection name:* pppoe

Username:*

Password:*

Password confirmation:*

Expert

< Back Next >

Figure 70. Configuring PPPoE WAN connection.

In the **Connection name** field, specify a name for the connection for easier identification.

In the **Username** field, enter your login, and in the **Password** and **Password confirmation** fields – the password provided by your ISP.

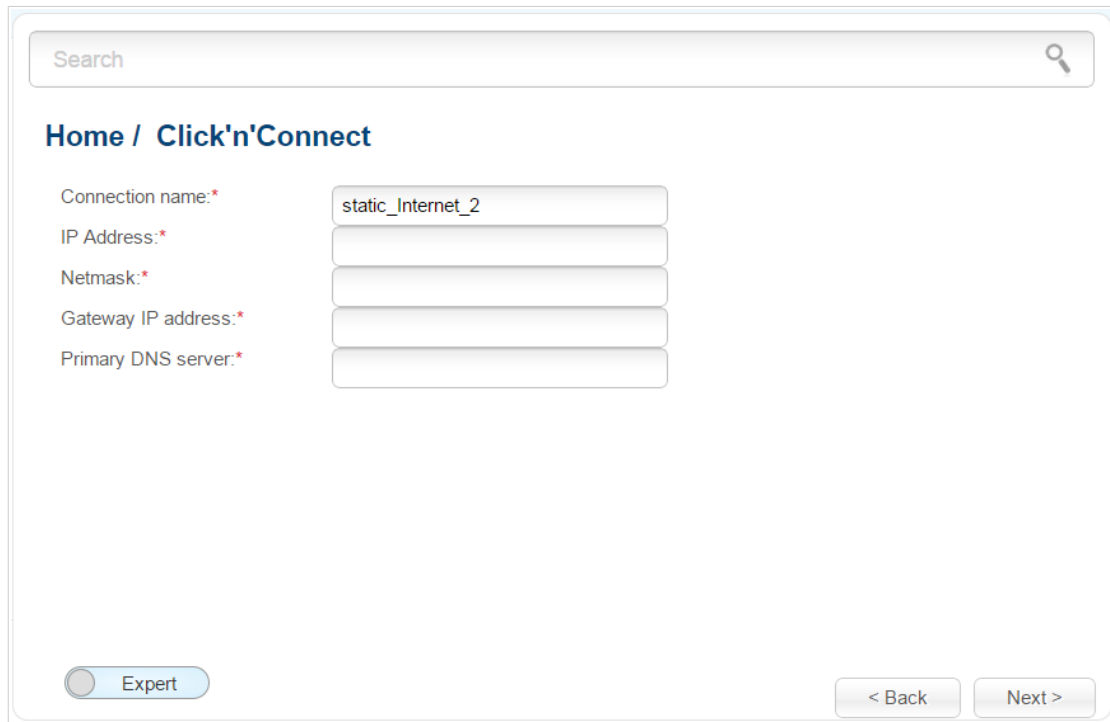
As a rule, the specified settings are enough to configure a connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPPoE WAN Connection* section, page 135).

Click the **Next** button to continue.

After that the page displaying all specified settings opens. Click the **Apply** button to create the connection or the **Back** button to specify other settings.

After clicking the **Apply** button, the page for checking the Internet availability opens (see the *Checking Internet Availability* section, page 111).

Static IP Connection



The screenshot shows a web interface for configuring a Static IP connection. At the top, there is a search bar. Below it, the breadcrumb navigation reads "Home / Click'n'Connect". The main configuration area contains five fields, each with a red asterisk indicating it is required: "Connection name:" (containing "static_Internet_2"), "IP Address:", "Netmask:", "Gateway IP address:", and "Primary DNS server:". At the bottom left, there is a radio button labeled "Expert" which is currently unselected. At the bottom right, there are two buttons: "< Back" and "Next >".

Figure 71. Configuring Static IP WAN connection.

In the **Connection name** field, specify a name for the connection for easier identification.

Fill in the **IP Address** and **Netmask** fields.

In the **Gateway IP address** field, enter the IP address of the gateway used by this WAN connection.

In the **Primary DNS server** field, enter the address of the primary DNS server.

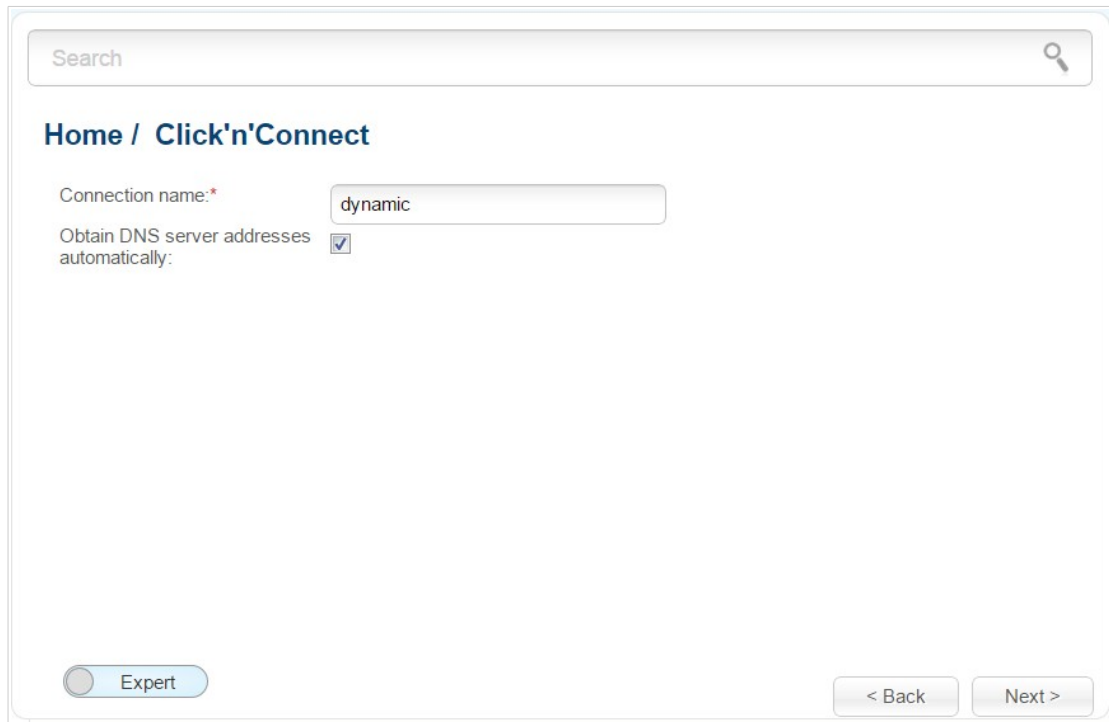
As a rule, the specified settings are enough to configure a connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating Static IP or Dynamic IP WAN Connection* section, page 139).

Click the **Next** button to continue.

After that the page displaying all specified settings opens. Click the **Apply** button to create the connection or the **Back** button to specify other settings.

After clicking the **Apply** button, the page for checking the Internet availability opens (see the *Checking Internet Availability* section, page 111).

Dynamic IP Connection



Search

Home / Click'n'Connect

Connection name:*

Obtain DNS server addresses automatically:

Expert

< Back Next >

Figure 72. Configuring Dynamic IP WAN connection.

In the **Connection name** field, specify a name for the connection for easier identification.

If your ISP has provided the addresses of the DNS servers, deselect the **Obtain DNS server addresses automatically** checkbox and fill in the **Primary DNS server** field.

As a rule, the specified settings are enough to configure a connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating Static IP or Dynamic IP WAN Connection* section, page 139).

Click the **Next** button to continue.

After that the page displaying all specified settings opens. Click the **Apply** button to create the connection or the **Back** button to specify other settings.

After clicking the **Apply** button, the page for checking the Internet availability opens (see the *Checking Internet Availability* section, page 111).

PPPoE + Static IP Connection

Search

Home / Click'n'Connect

IP Address:* 192.168.161.228

Netmask:* 255.255.255.0

Gateway IP address:* 192.168.161.1

Primary DNS server:* 192.168.161.140

Expert

< Back Next >

Figure 73. Configuring PPPoE + Static IP WAN connection.

Fill in the **IP Address** and **Netmask** fields.

In the **Gateway IP address** field, enter the IP address of the gateway used by this WAN connection.

In the **Primary DNS server** field, enter the address of the primary DNS server.

As a rule, the specified settings are enough at this step to configure a connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPPoE + Static IP or PPPoE + Dynamic IP WAN Connection* section, page 143).

Click the **Next** button to continue.

If needed, enter the IP addresses of the ISP's local resources.

The screenshot shows a web-based configuration interface. At the top, there is a search bar with the text 'Search' and a magnifying glass icon. Below the search bar is a breadcrumb trail: 'Home / Click'n'Connect'. A section header in green text reads 'IP addresses of your ISP's local resources'. Underneath this header, a line of text says 'Here the wizard can add IP addresses of your ISP's local resources.' This is followed by a vertical list of ten input fields, each preceded by a label: 'IP address 1:', 'IP address 2:', 'IP address 3:', 'IP address 4:', 'IP address 5:', 'IP address 6:', 'IP address 7:', 'IP address 8:', 'IP address 9:', and 'IP address 10:'. At the bottom right of the form area, there are two buttons: '< Back' and 'Next >'.

Figure 74. Configuring PPPoE + Static IP WAN connection.

Click the **Next** button to continue.

The screenshot shows a web interface for configuring a PPPoE connection. At the top, there is a search bar. Below it, the page title is "Home / Click'n'Connect". The main form contains four fields: "Connection name:*" with the value "pppoe", "Username:*", "Password:*" (masked with dots), and "Password confirmation:*" (masked with dots). At the bottom left, there is a toggle switch labeled "Expert" which is currently turned off. At the bottom right, there are two buttons: "< Back" and "Next >".

Figure 75. Configuring PPPoE + Static IP WAN connection.

In the **Connection name** field, specify a name for the connection for easier identification.

In the **Username** field, enter your login, and in the **Password** and **Password confirmation** fields – the password provided by your ISP.

As a rule, the specified settings are enough to configure a connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the **Creating PPPoE + Static IP or PPPoE + Dynamic IP WAN Connection** section, page 143).

Click the **Next** button to continue.

After that the page displaying all specified settings opens. Click the **Apply** button to create the connection or the **Back** button to specify other settings.

After clicking the **Apply** button, the page for checking the Internet availability opens (see the **Checking Internet Availability** section, page 111).

PPPoE + Dynamic IP Connection

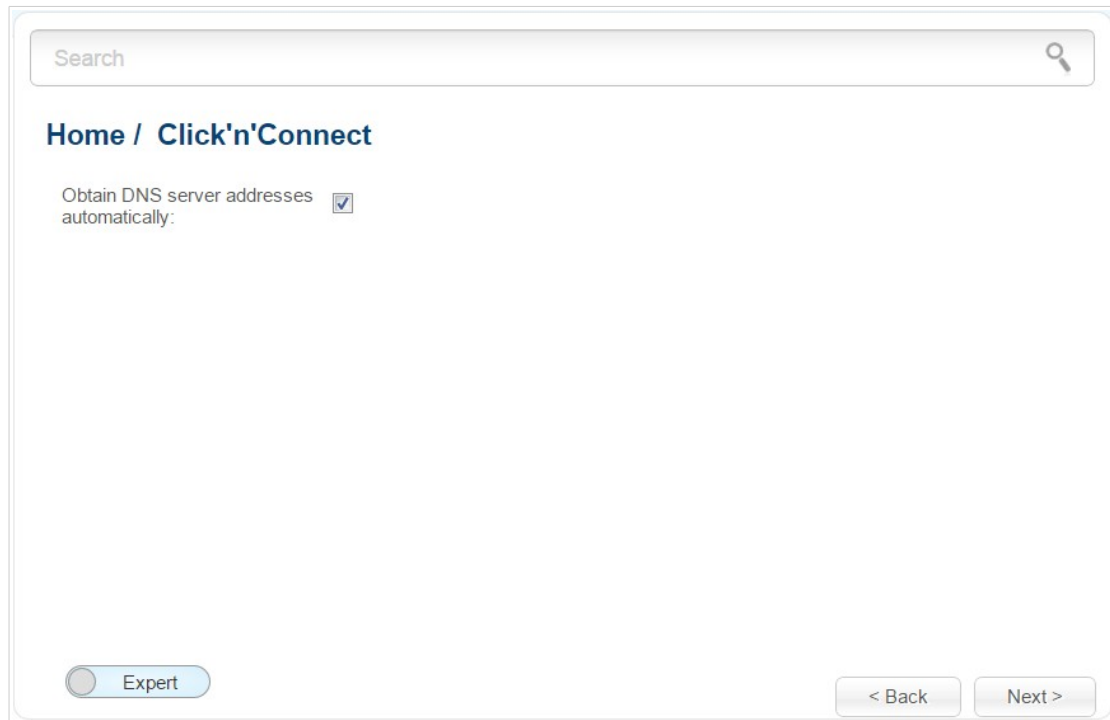


Figure 76. Configuring PPPoE + Dynamic IP WAN connection.

If your ISP has provided the addresses of the DNS servers, deselect the **Obtain DNS server addresses automatically** checkbox and fill in the **Primary DNS server** field.

As a rule, the specified settings are enough at this step to configure a connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPPoE + Static IP or PPPoE + Dynamic IP WAN Connection* section, page 143).

Click the **Next** button to continue.

The screenshot shows a web-based configuration interface. At the top, there is a search bar with the text 'Search' and a magnifying glass icon. Below the search bar, the breadcrumb 'Home / Click'n'Connect' is displayed. The main content area contains four labeled input fields: 'Connection name:*' with the value 'pppoe', 'Username:*', 'Password:*' (masked with dots), and 'Password confirmation:*' (masked with dots). At the bottom left, there is a radio button labeled 'Expert' which is currently unselected. At the bottom right, there are two buttons: '< Back' and 'Next >'. The entire interface is enclosed in a light blue border.

Figure 77. Configuring PPPoE + Dynamic IP WAN connection.

In the **Connection name** field, specify a name for the connection for easier identification.

In the **Username** field, enter your login, and in the **Password** and **Password confirmation** fields – the password provided by your ISP.

As a rule, the specified settings are enough to configure a connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPPoE + Static IP or PPPoE + Dynamic IP WAN Connection* section, page 143).

Click the **Next** button to continue.

After that the page displaying all specified settings opens. Click the **Apply** button to create the connection or the **Back** button to specify other settings.

After clicking the **Apply** button, the page for checking the Internet availability opens (see the *Checking Internet Availability* section, page 111).

PPTP + Static IP or L2TP + Static IP Connection

The screenshot shows a web-based configuration interface for a WAN connection. At the top, there is a search bar. Below it, the breadcrumb 'Home / Click'n'Connect' is visible. The main configuration area contains four rows of fields, each with a label and a text input box. The labels are 'IP Address:*', 'Netmask:*', 'Gateway IP address:*', and 'Primary DNS server:*'. The input boxes contain the values '192.168.161.228', '255.255.255.0', '192.168.161.1', and '192.168.161.140' respectively. At the bottom left, there is a toggle switch labeled 'Expert' which is currently turned off. At the bottom right, there are two buttons: '< Back' and 'Next >'.

Figure 78. Configuring PPTP + Static IP WAN connection.

Fill in the **IP Address** and **Netmask** fields.

In the **Gateway IP address** field, enter the IP address of the gateway used by this WAN connection.

In the **Primary DNS server** field, enter the address of the primary DNS server.

As a rule, the specified settings are enough to configure a non-protected connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPTP/L2TP + Static IP or PPTP/L2TP + Dynamic IP WAN Connection* section, page 149).

Click the **Next** button to continue.

If needed, enter the IP addresses of the ISP's local resources.

Search

Home / Click'n'Connect

IP addresses of your ISP's local resources

Here the wizard can add IP addresses of your ISP's local resources.

IP address 1:

IP address 2:

IP address 3:

IP address 4:

IP address 5:

IP address 6:

IP address 7:

IP address 8:

IP address 9:

IP address 10:

< Back Next >

Figure 79. Configuring PPTP + Static IP WAN connection.

Click the **Next** button to continue.

Search

Home / Click'n'Connect

Connection name:* statpptp

Username:*

Password:*

Password confirmation:*

VPN server address:*

Expert

< Back Next >

Figure 80. Configuring PPTP + Static IP WAN connection.

In the **Connection name** field, specify a name for the connection for easier identification.

In the **Username** field, enter your login, and in the **Password** and **Password confirmation** fields – the password provided by your ISP.

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

As a rule, the specified settings are enough to configure a protected connection (the VPN tunnel). If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPTP/L2TP + Static IP or PPTP/L2TP + Dynamic IP WAN Connection* section, page 149).

Click the **Next** button to continue.

After that the page displaying all specified settings opens. Click the **Apply** button to create the connection or the **Back** button to specify other settings.

After clicking the **Apply** button, the page for checking the Internet availability opens (see the *Checking Internet Availability* section, page 111).

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

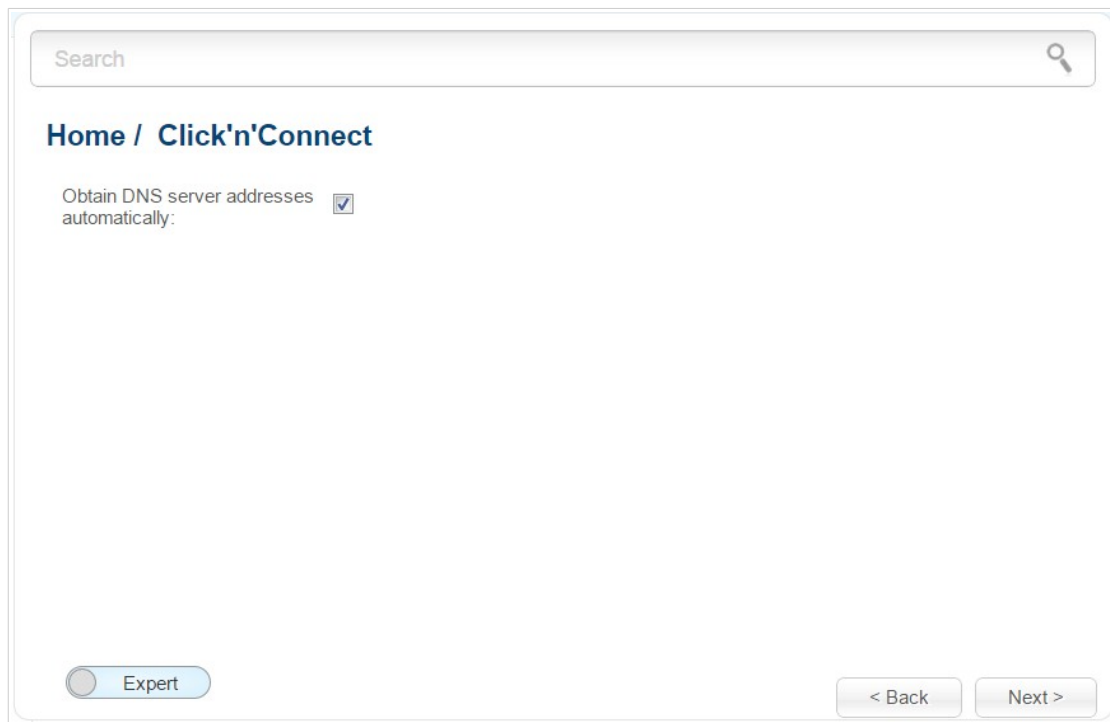


Figure 81. Configuring PPTP + Dynamic IP WAN connection.

If your ISP has provided the addresses of the DNS servers, deselect the **Obtain DNS server addresses automatically** checkbox and fill in the **Primary DNS server** field.

As a rule, the specified settings are enough to configure a non-protected connection of the selected type. If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPTP/L2TP + Static IP or PPTP/L2TP + Dynamic IP WAN Connection* section, page 149).

Click the **Next** button to continue.

Search

Home / Click'n'Connect

Connection name:* dynpptp

Username:*

Password:*

Password confirmation:*

VPN server address:*

Expert

< Back Next >

Figure 82. Configuring PPTP + Dynamic IP WAN connection.

In the **Connection name** field, specify a name for the connection for easier identification.

In the **Username** field, enter your login, and in the **Password** and **Password confirmation** fields – the password provided by your ISP.

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

As a rule, the specified settings are enough to configure a protected connection (the VPN tunnel). If you need to specify additional settings, open the expert settings mode. To do this, use the switch in the bottom left corner of the page (for a detailed description of all the connection's parameters, see the *Creating PPTP/L2TP + Static IP or PPTP/L2TP + Dynamic IP WAN Connection* section, page 149).

Click the **Next** button to continue.

After that the page displaying all specified settings opens. Click the **Apply** button to create the connection or the **Back** button to specify other settings.

After clicking the **Apply** button, the page for checking the Internet availability opens (see the *Checking Internet Availability* section, page 111).

Checking Internet Availability

On the page, you can check the WAN connection you have created.

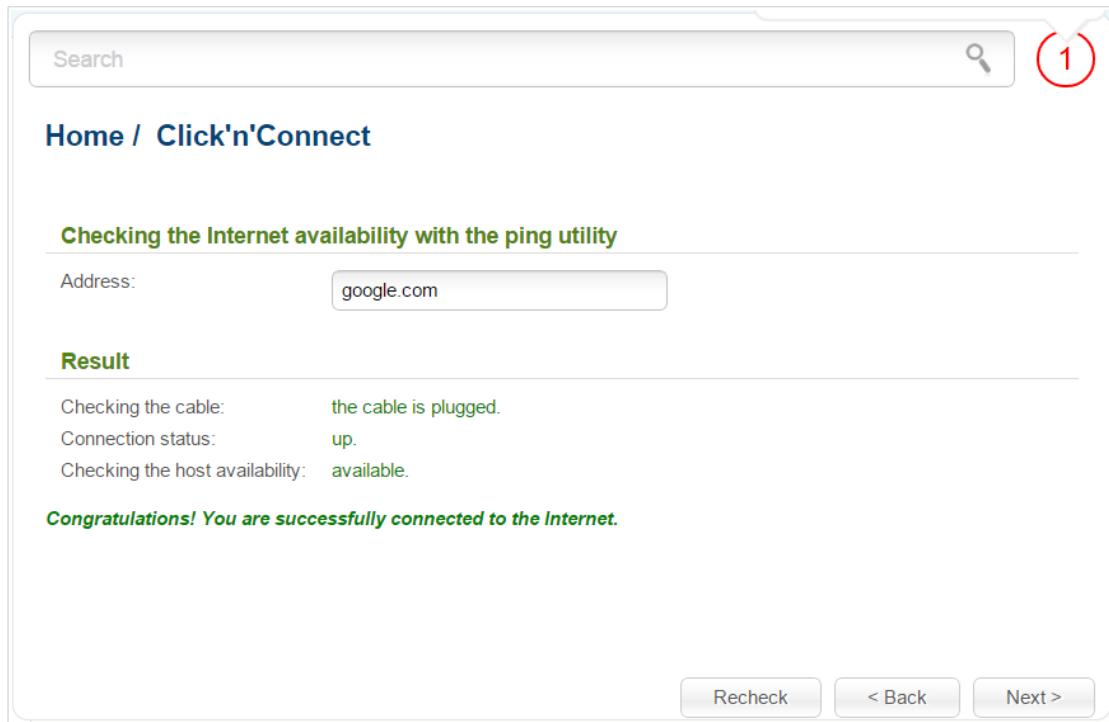


Figure 83. Checking the Internet availability.

In the **Result** section, the status of the WAN connection and possible causes of malfunctions are displayed. To recheck the status of the WAN connection, enter the IP address or name of a host in the **Address** field or leave the value specified by default (**google.com**). Then click the **Recheck** button.

Click the **Back** button to specify other settings.

Click the **Next** button to continue.

After clicking the **Next** button, the page for configuring wireless connection opens (see the *Configuring Wireless Connection* section, page 112).

Configuring Wireless Connection

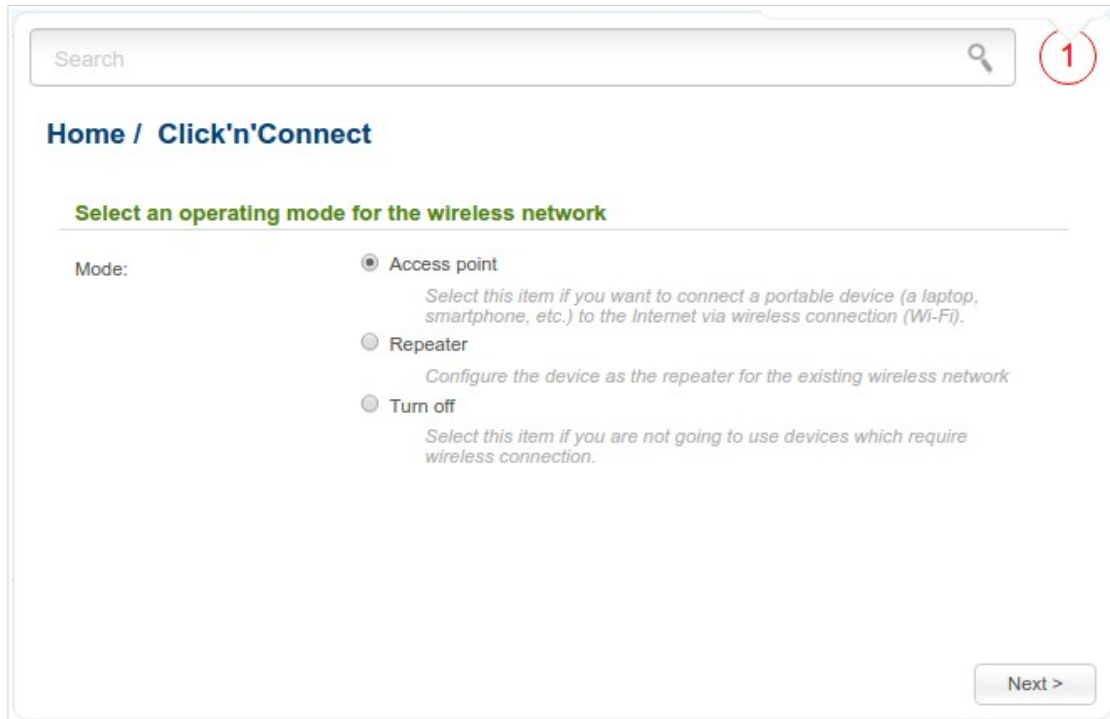


Figure 84. Selecting the operating mode for the wireless network.

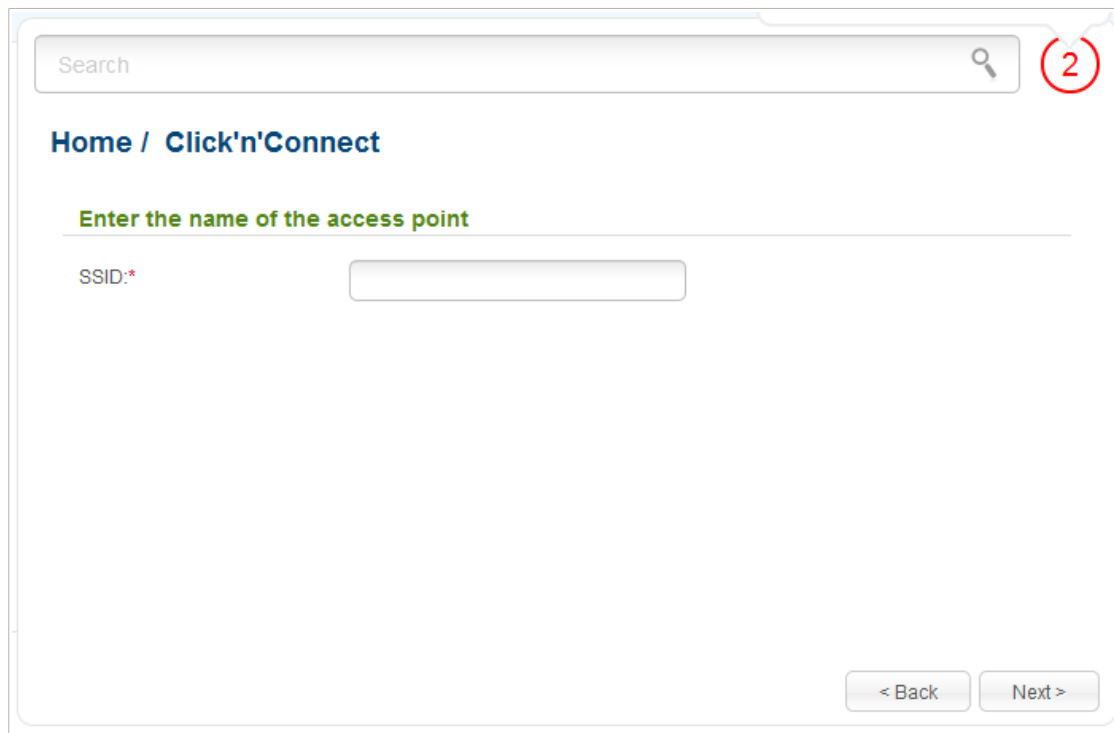
If you are not going to use the wireless connection, select the **Turn off** choice of the **Mode** radio button. Click the **Next** button and then click the **Apply** button on the opened page. After clicking the button, the **Home / Information** page opens.

If you want to connect portable devices to the network of the access point via wireless connection, select the **Access point** choice of the **Mode** radio button. Click the **Next** button.

If you want to configure DAP-1360U as a repeater to connect to a wireless access point, select the **Repeater** choice of the **Mode** radio button. Click the **Next** button.

Access Point Mode

On the opened page, in the **SSID** field, specify a new name for the network (use digits and Latin characters).



The screenshot shows a web interface for configuring the wireless LAN. At the top, there is a search bar with a magnifying glass icon and a red circle containing the number '2'. Below the search bar, the breadcrumb navigation reads 'Home / Click'n'Connect'. A green instruction line says 'Enter the name of the access point'. Underneath, the label 'SSID: *' is followed by an empty text input field. At the bottom right, there are two buttons: '< Back' and 'Next >'.

Figure 85. Changing the name of the wireless LAN.

Click the **Next** button to continue.

On the next page, you can modify security settings of the WLAN.

Select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the WLAN of the access point.

When the **Open** value is selected, the **Network key** field is unavailable. After applying this setting, the **Open** authentication type with no encryption is specified for the WLAN of the access point.

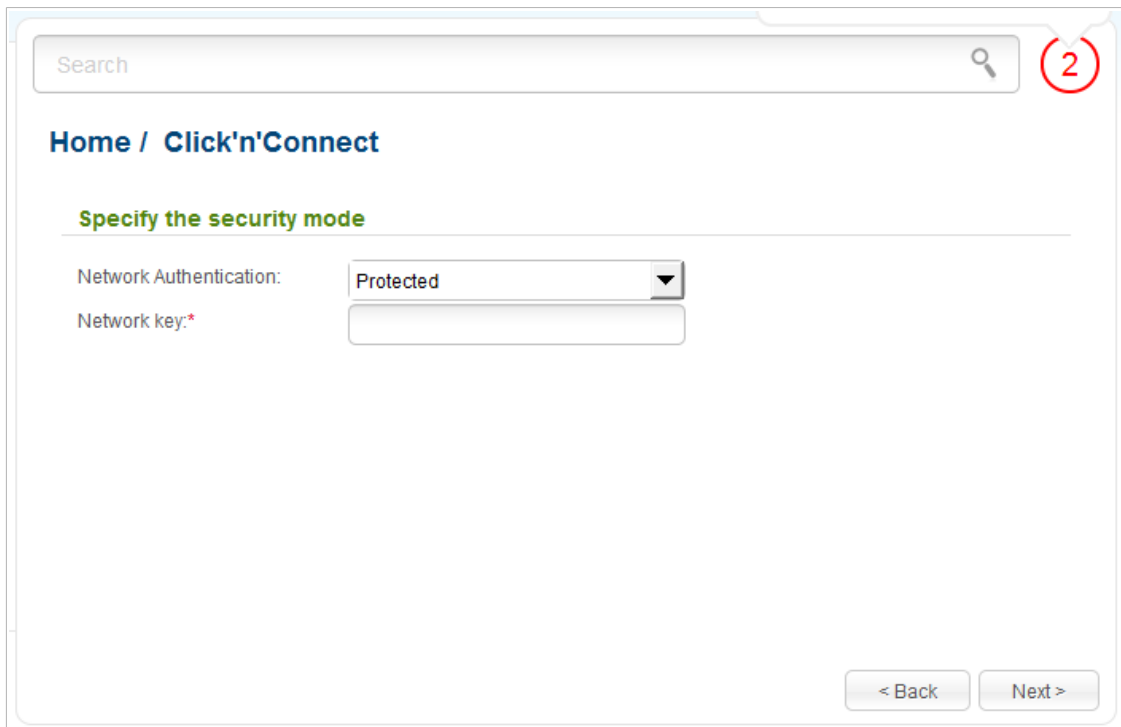


Figure 86. Selecting a security mode for the wireless network.

Click the **Next** button to continue.

On the next page, the specified settings are displayed. Make sure that they are correct and then click the **Apply** button. After clicking the button, the **Home / Information** page opens.

Repeater Mode

On the opened page, click the **Search** button.

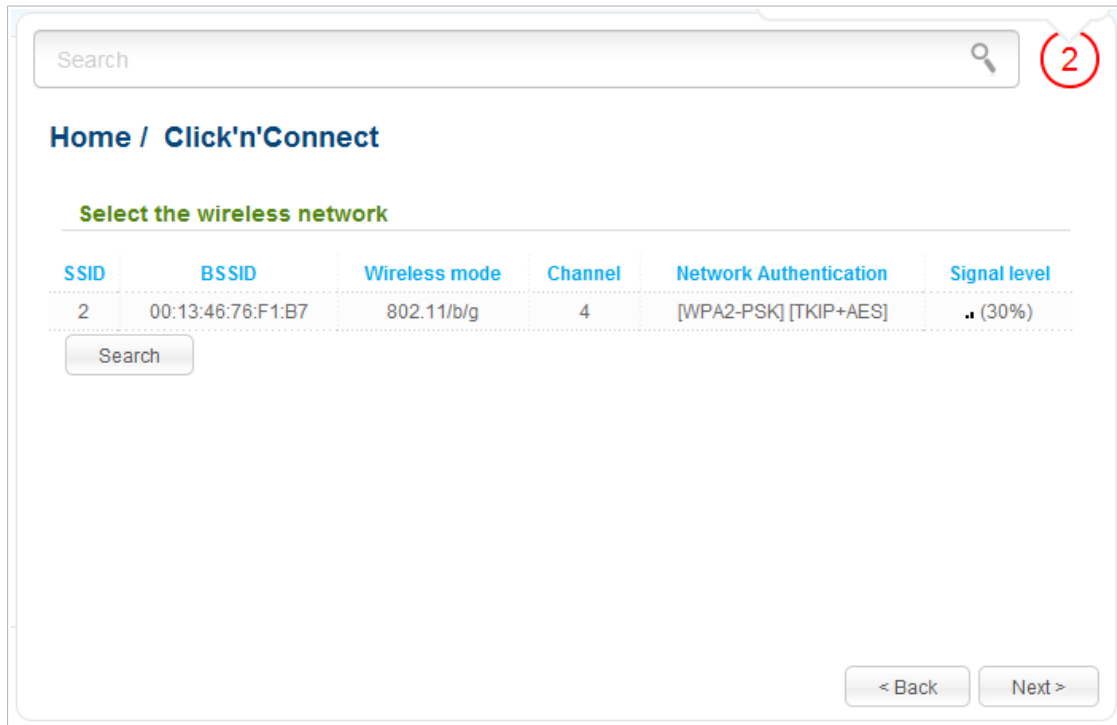


Figure 87. The page for selecting a network to connect.

Select the network to which you want to connect and click the **Next** button.

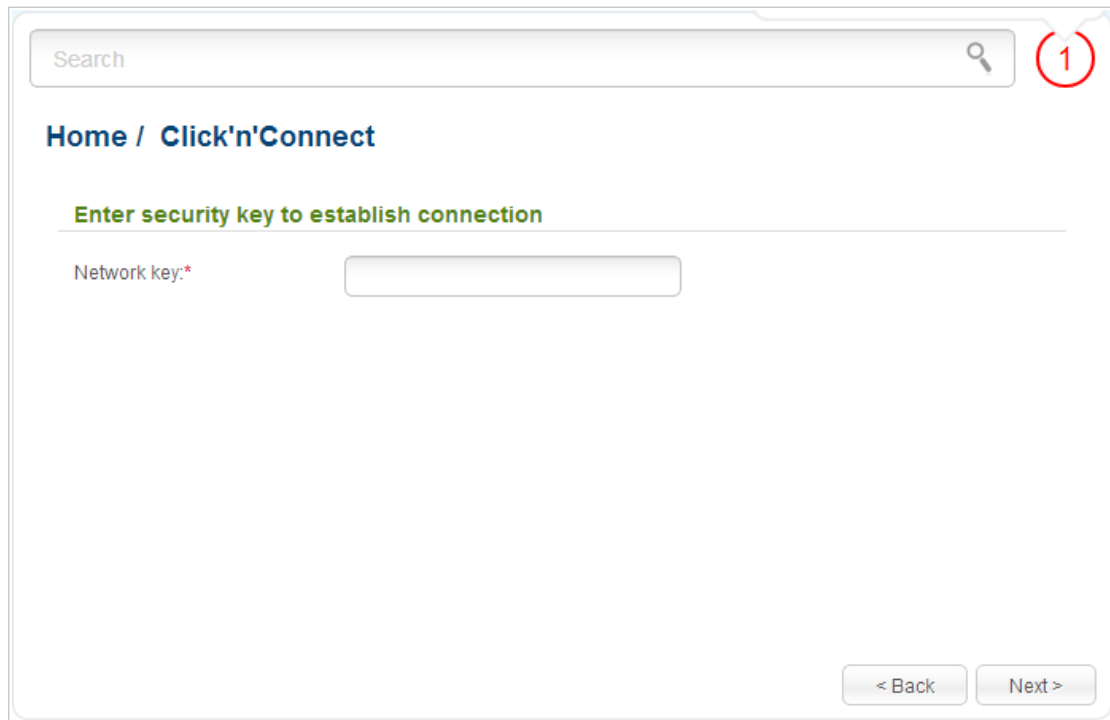


Figure 88. The page for entering the password for connection to the wireless network.

If you need a password to connect to the selected network, enter the password in the **Network key** field and click the **Next** button.

On the next page, you can specify an individual name (SSID) and security settings for the access point or configure the parameters identical with the network to which you connect.

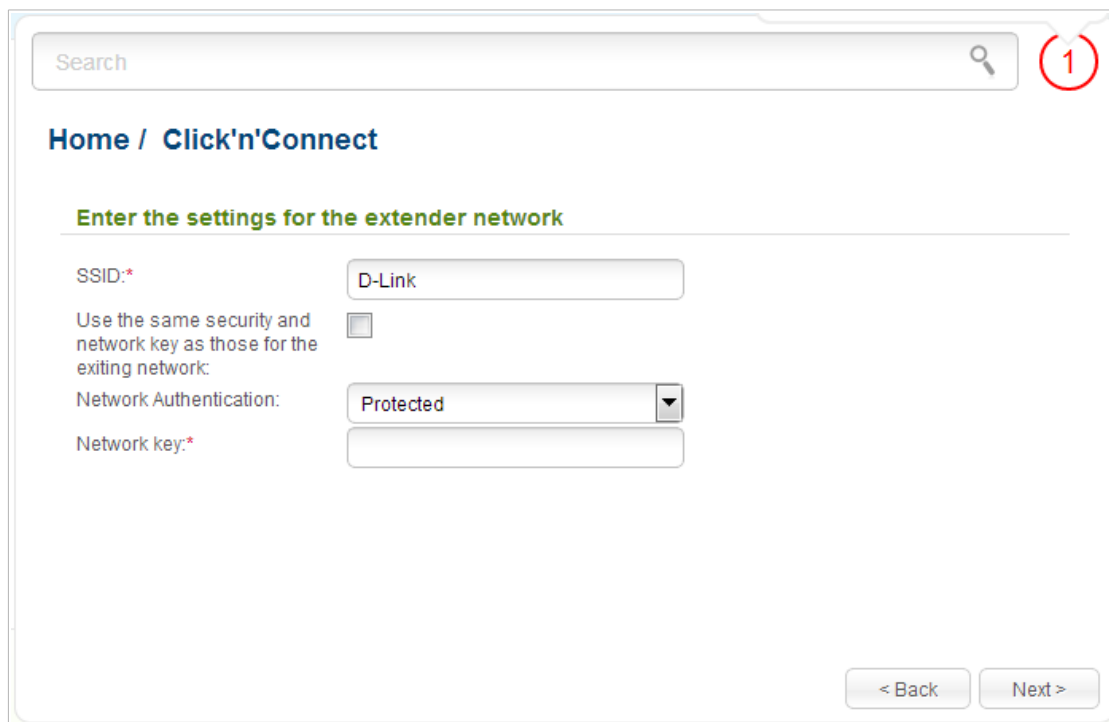


Figure 89. The page for changing the settings of the wireless local area network.

If you want to leave the name of the wireless network and security settings identical with the network to which you connect, click the **Next** button.

If you want to configure individual settings for the access point, deselect the **Use the same security and network key as those for the exiting network** checkbox and enter a name for the wireless network in the **SSID** field. It is strongly recommended to configure the secure wireless network of DAP-1360U. To do this, select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the WLAN of the access point. Click the **Next** button.

On the next page, the parameters of the network to which you want to connect, the entered password, and the settings of the wireless network of the access point are displayed. Make sure that the specified settings are correct and then click the **Apply** button. After that, the wireless channel of DAP-1360U will switch to the channel of the wireless access point to which you have connected.

After configuring the device as a repeater, you need to create a WAN connection with relevant parameters for the **WiFiClient** interface.

After clicking the **Apply** button, the **Home / Information** page opens.

Wireless Network Settings Wizard

To specify all needed settings for your wireless network, click the **Wireless network settings wizard** link in the **Home** section.

Search

Home / Wireless network settings wizard

Select an operating mode for the wireless network

Mode:

- Access point
Select this item if you want to connect a portable device (a laptop, smartphone, etc.) to the Internet via wireless connection (Wi-Fi)
- Repeater
Configure the device as the repeater for the existing wireless network
- Client
Connect to the existing wireless network as a client
- Turn off
Select this item if you are not going to use devices which require wireless connection

Next >

Figure 90. The page for selecting the operating mode for the wireless network.

If you are not going to use the wireless connection, select the **Turn off** choice of the **Mode** radio button. Click the **Next** button and then click the **Apply** button on the opened page. After clicking the button, the **Home / Information** page opens.

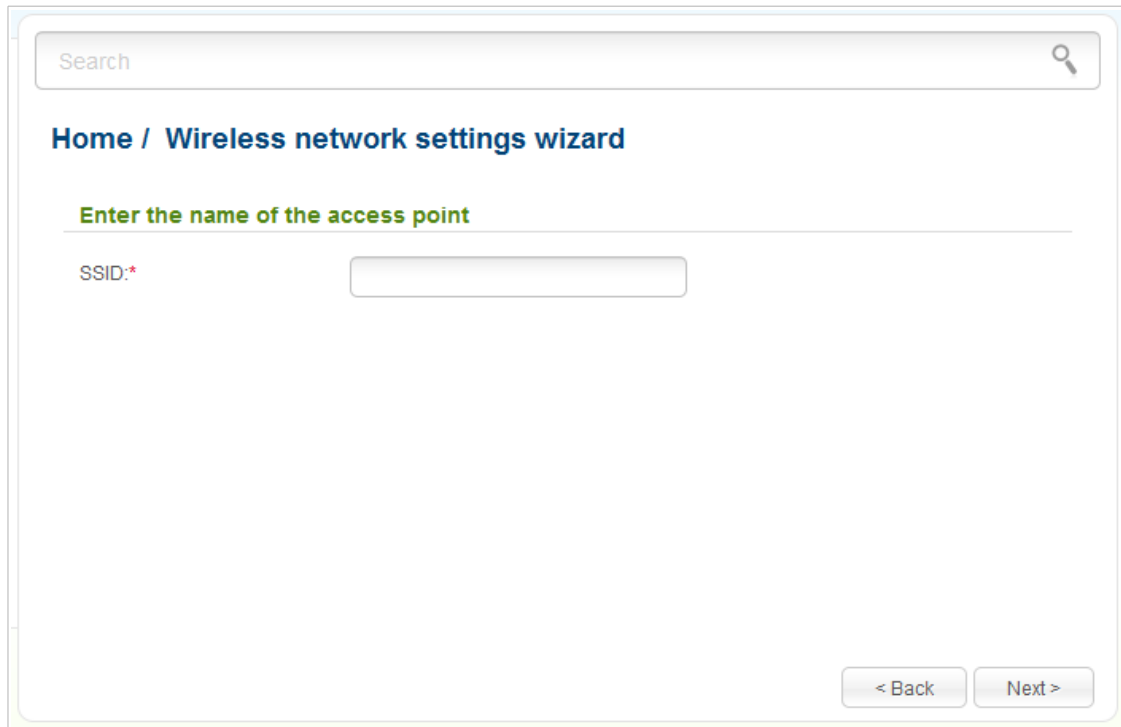
If you want to connect portable devices to the network of the access point via wireless connection, select the **Access point** choice of the **Mode** radio button. Click the **Next** button.

If you want to configure DAP-1360U as a repeater to connect to a wireless access point, select the **Repeater** choice of the **Mode** radio button. Click the **Next** button.

If you want to configure DAP-1360U as a client to connect to a wireless access point, select the **Client** choice of the **Mode** radio button. Click the **Next** button.

Access Point Mode

On the opened page, in the **SSID** field, specify a new name for the network (use digits and Latin characters).



The screenshot shows a web interface for configuring wireless network settings. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar, the breadcrumb "Home / Wireless network settings wizard" is displayed. A green heading "Enter the name of the access point" is followed by a horizontal line. Underneath, the label "SSID:*" is positioned to the left of an empty text input field. At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 91. Page for changing the name of the wireless LAN.

Click the **Next** button to continue.

On the next page, you can modify security settings of the WLAN.

Select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the WLAN of the access point.

When the **Open** value is selected, the **Network key** field is unavailable. After applying this setting, the **Open** authentication type with no encryption is specified for the WLAN of the access point.

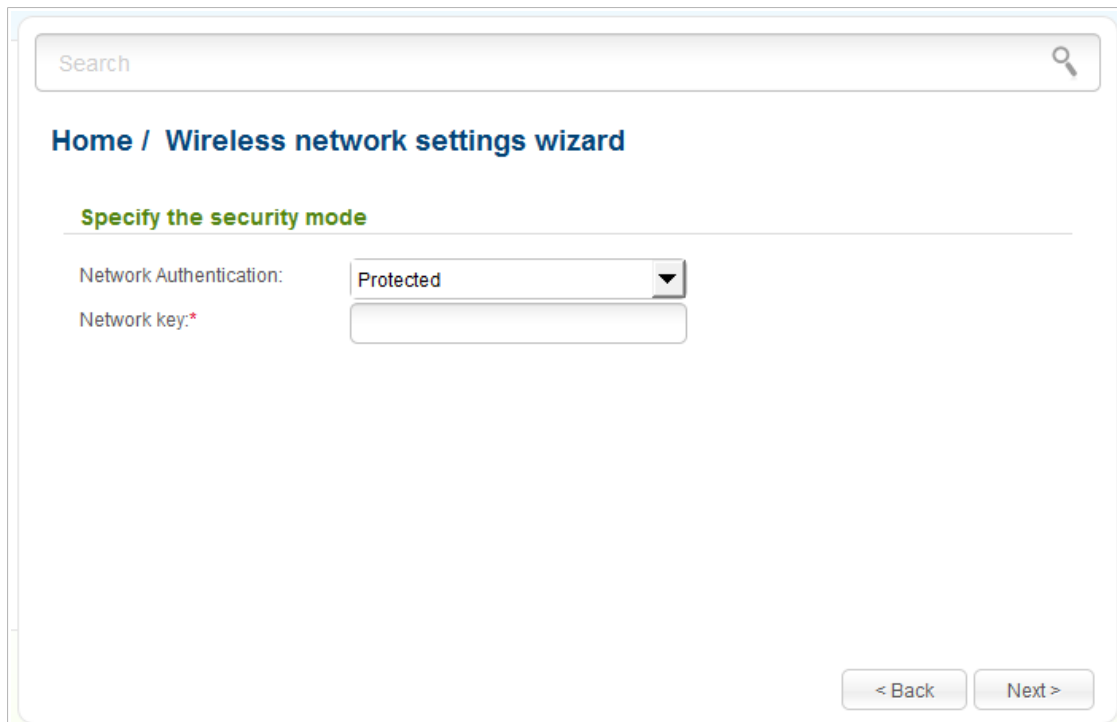


Figure 92. Page for selecting a security mode for the wireless network.

Click the **Next** button to continue.

On the next page, the specified settings are displayed. Make sure that they are correct and then click the **Apply** button. After clicking the button, the **Home / Information** page opens.

Repeater Mode

On the opened page, click the **Search** button.

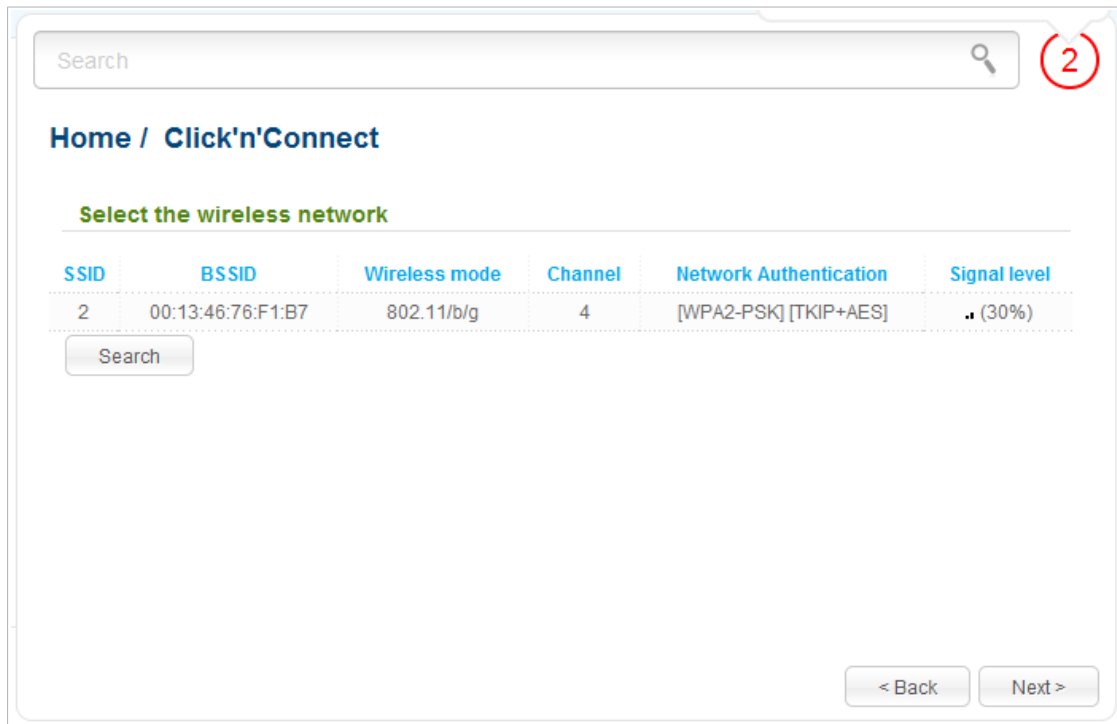
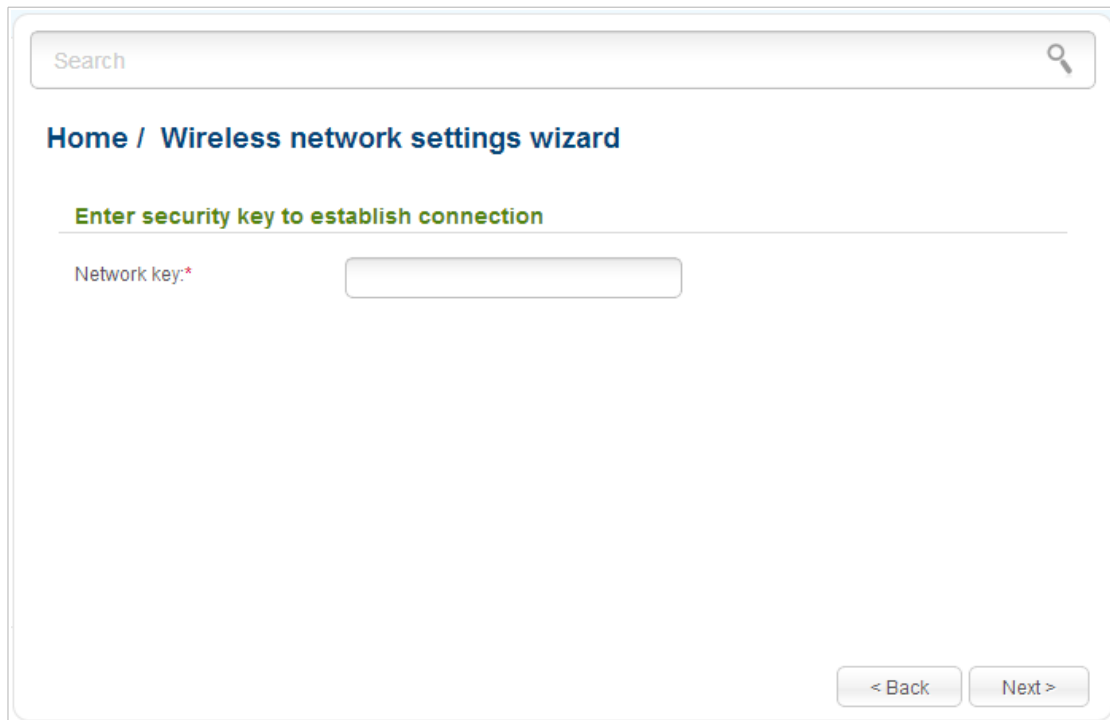


Figure 93. The page for selecting a network to connect.

Select the network to which you want to connect and click the **Next** button.



The screenshot shows a web interface for configuring a wireless network. At the top, there is a search bar with the word "Search" and a magnifying glass icon. Below the search bar, the breadcrumb "Home / Wireless network settings wizard" is displayed. A green heading reads "Enter security key to establish connection". Underneath, the label "Network key:" is followed by a red asterisk and an empty text input field. At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 94. The page for entering the password for connection to the wireless network.

If you need a password to connect to the selected network, enter the password in the **Network key** field and click the **Next** button.

On the next page, you can specify an individual name (SSID) and security settings for the access point or configure the parameters identical with the network to which you connect.

Search

Home / Wireless network settings wizard

Enter the settings for the extender network

SSID:*

Use the same security and network key as those for the exiting network:

Network Authentication:

Network key:*

< Back Next >

Figure 95. The page for changing the settings of the wireless local area network.

If you want to leave the name of the wireless network and security settings identical with the network to which you connect, click the **Next** button.

If you want to configure individual settings for the access point, deselect the **Use the same security and network key as those for the exiting network** checkbox and enter a name for the wireless network in the **SSID** field. It is strongly recommended to configure the secure wireless network of DAP-1360U. To do this, select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the WLAN of the access point. Click the **Next** button.

On the next page, the parameters of the network to which you want to connect, the entered password, and the settings of the wireless network of the access point are displayed. Make sure that the specified settings are correct and then click the **Apply** button. After that, the wireless channel of DAP-1360U will switch to the channel of the wireless access point to which you have connected.

After configuring the device as a repeater, you need to create a WAN connection with relevant parameters for the **WiFiClient** interface.

After clicking the **Apply** button, the **Home / Information** page opens.

Client Mode

On the opened page, click the **Search** button.

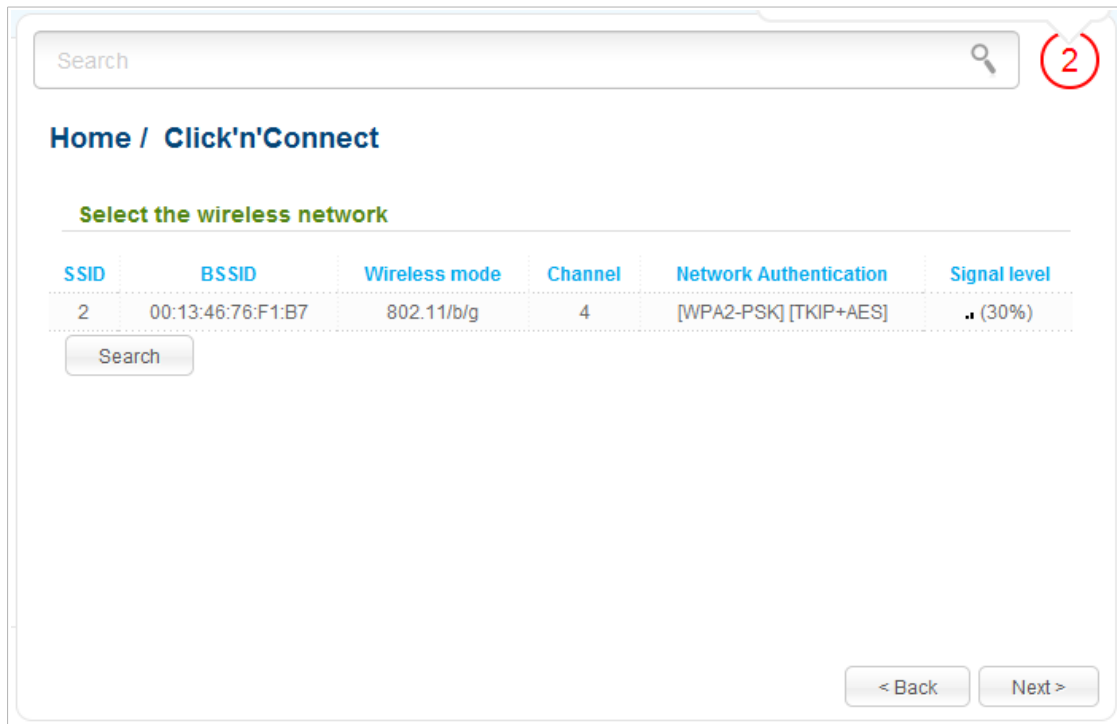
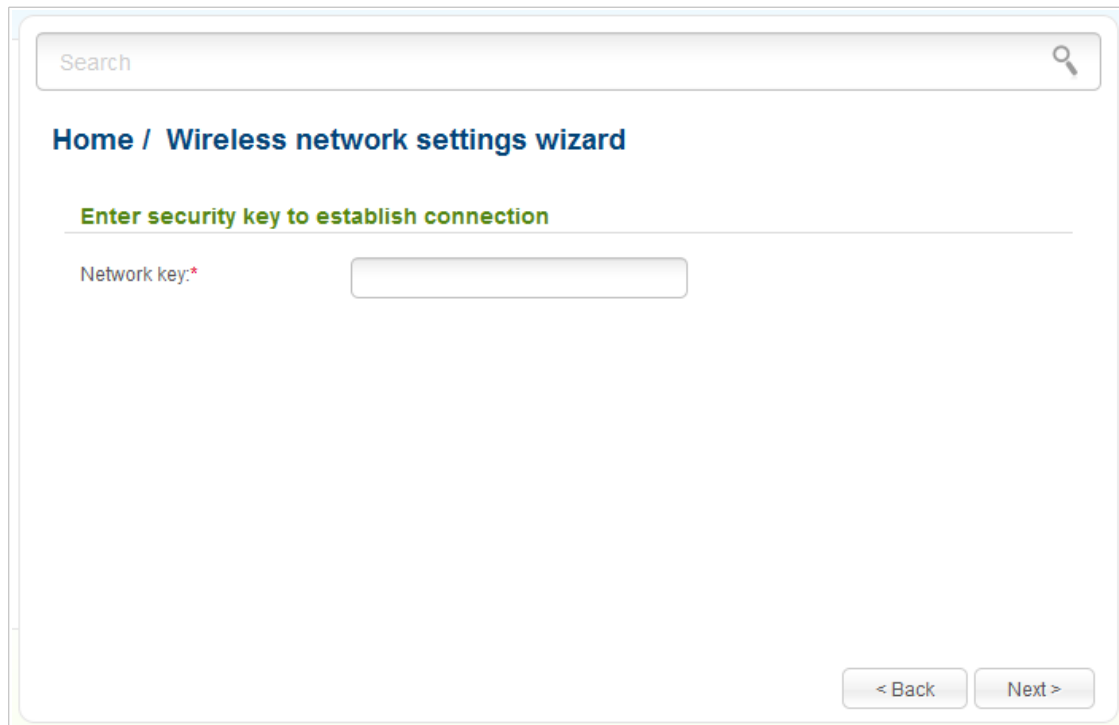


Figure 96. The page for selecting a network to connect.

Select the network to which you want to connect and click the **Next** button.



The screenshot shows a web interface for configuring a wireless network. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar, the breadcrumb "Home / Wireless network settings wizard" is displayed. A green heading reads "Enter security key to establish connection". Underneath, the label "Network key:" is followed by an empty text input field. At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 97. The page for entering the password for connection to the wireless network.

If you need a password to connect to the selected network, enter the password in the **Network key** field and click the **Next** button.

On the next page, you can specify an individual name (SSID) and security settings for the access point or disable the device's wireless network broadcast.

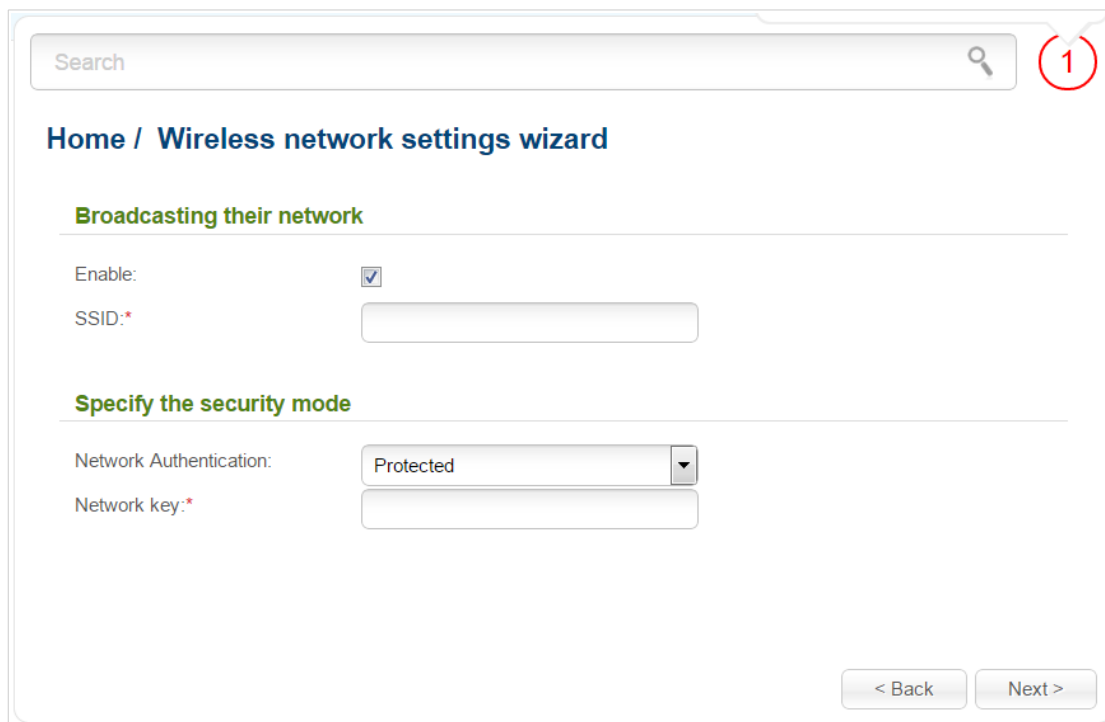


Figure 98. The page for changing the settings of the wireless local area network.

If you want to use the access point's wireless network to connect devices, leave the **Enable** checkbox selected. Then, if needed, specify another name for the network in the **SSID** field (use digits and Latin characters).

It is strongly recommended to configure the secure wireless network of DAP-1360U. To do this, select the **Protected** value from the **Network Authentication** drop-down list and enter a key (a password that will be used to access your wireless network) in the **Network key** field. Use digits and Latin characters. After applying this setting, the **WPA-PSK/WPA2-PSK mixed** authentication type is specified for the access point's WLAN. Click the **Next** button.

On the next page, the parameters of the network to which you want to connect, the entered password, and the settings of the wireless network of the access point are displayed. Make sure that the specified settings are correct and then click the **Apply** button. After that, the wireless channel of DAP-1360U will switch to the channel of the wireless access point to which you have connected.

After configuring the device as a client, you need to create a WAN connection with relevant parameters for the **WiFiClient** interface.

After clicking the **Apply** button, the **Home / Information** page opens.

Virtual Server Settings Wizard

To create a virtual server for redirecting incoming Internet traffic to a specified IP address in the LAN, click the **Virtual server settings wizard** link in the **Home** section.

Figure 99. The page for adding a virtual server.

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

Parameter	Description
Template	Select a virtual server template from the drop-down list, or select Custom to specify all parameters of the new virtual server manually.
Name	Enter a name for the virtual server for easier identification. You can specify any name.
Interface	Select a WAN connection to which this virtual server will be assigned.
Protocol	A protocol that will be used by the new virtual server. Select a value from the drop-down list.
Public port (begin)/ Public port (end)	A port of the access point from which traffic is directed to the IP address specified in the Private IP field. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the Public port (begin) field and leave the Public port (end) field blank.

Parameter	Description
Private port (begin)/ 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 (begin) field and leave the Private port (end) field blank.
Private IP	Enter 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).
Remote IP	Enter the IP address of the server from the external network.
Enable NAT Loopback	If the checkbox is selected, users of the access point's LAN can access the server, which IP address is specified in the Private IP field, using the access point's external IP address as the server's IP address. If a DDNS service is configured on the Advanced / DDNS page, the users can access the server via the device's domain name.

When needed settings are configured, click the **Apply** button.

After clicking the **Apply** button, a dialog box appears.

If you are going to create a new virtual server, click the **OK** button. After clicking the button, the **Firewall / Virtual servers** page opens (see the *Virtual Servers* section, page 195, for a detailed description of the elements from the page).

If you are not going to create a new virtual server, click the **Cancel** button. After clicking the button, the **Home / Information** page opens.

Status

The pages of this section display data on the current state of the access point switched to the router mode:

- 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
- addresses of active multicast groups.

Network Statistics

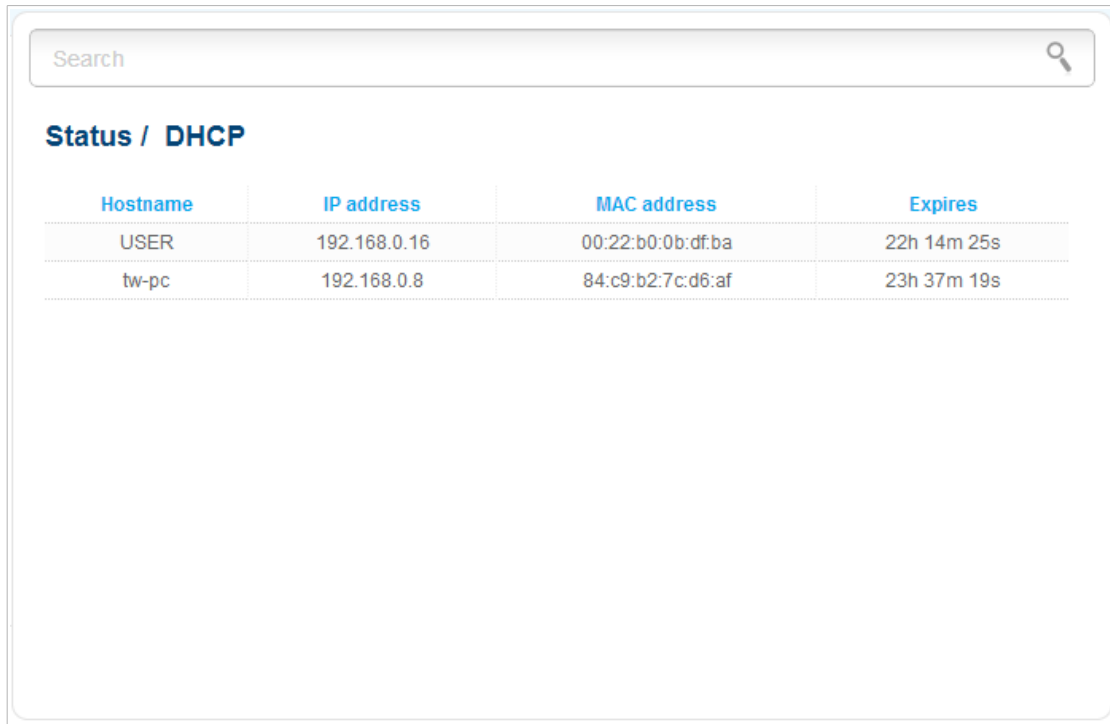
On the **Status / Network statistics** page, you can view statistics for all connections existing in the system (WAN connections, LAN, WLAN). For each connection the following data are displayed: name and state (when the connection is on, its name is highlighted in green, when the connection is off, its name is highlighted in red), IP address and subnet mask, gateway (if the connection is established), MAC address, MTU value, 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	MAC	Rx/Tx	Duration, min	
WIFI	-	9C:D6:43:3D:05:08	3.94 MByte / 2.62 MByte	-	▶
LAN	192.168.0.50/24 - 192.168.0.50	9C:D6:43:3D:05:08	1.74 MByte / 12.71 MByte	-	▶
internet	192.168.43.67/24 - 192.168.43.1	9C:D6:43:3D:05:08	5.48 KByte / 8.41 KByte	9.3	▶

Figure 100. The **Status / Network statistics** page.

DHCP

The **Status / 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).



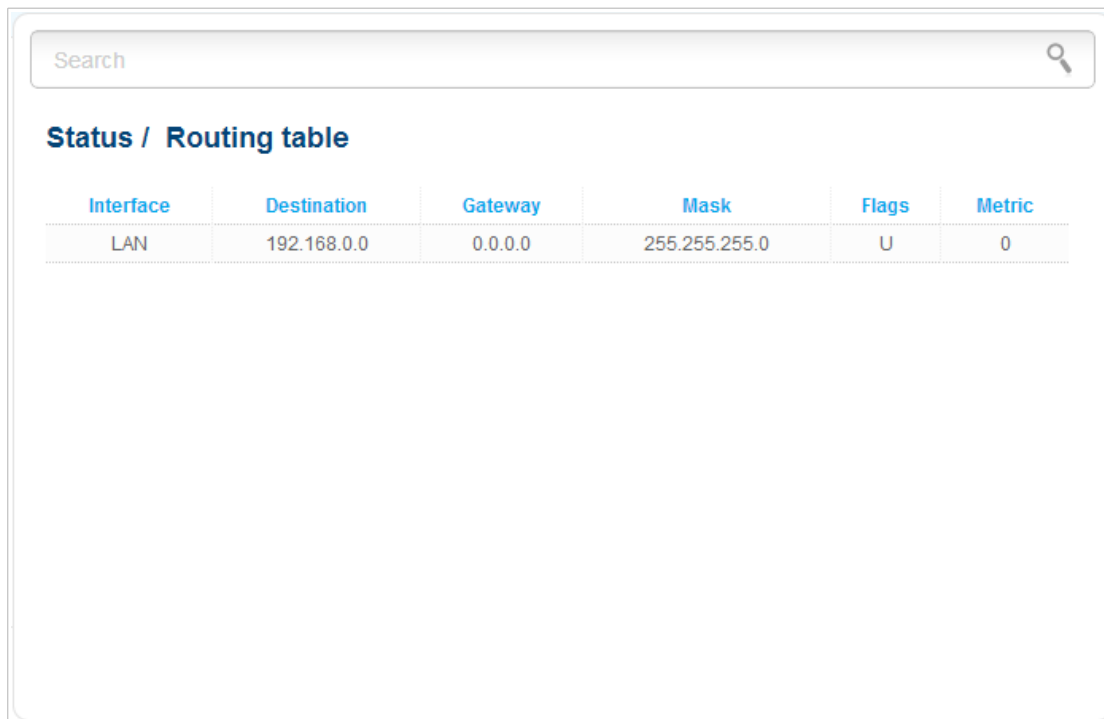
The screenshot shows a web interface for the DHCP status page. At the top, there is a search bar with the placeholder text "Search" and a magnifying glass icon. Below the search bar, the title "Status / DHCP" is displayed in blue. Underneath the title is a table with four columns: "Hostname", "IP address", "MAC address", and "Expires". The table contains two rows of data. The first row shows a hostname of "USER", an IP address of "192.168.0.16", a MAC address of "00:22:b0:0b:df:ba", and an expiration time of "22h 14m 25s". The second row shows a hostname of "tw-pc", an IP address of "192.168.0.8", a MAC address of "84:c9:b2:7c:d6:af", and an expiration time of "23h 37m 19s".

Hostname	IP address	MAC address	Expires
USER	192.168.0.16	00:22:b0:0b:df:ba	22h 14m 25s
tw-pc	192.168.0.8	84:c9:b2:7c:d6:af	23h 37m 19s

Figure 101. The **Status / DHCP** page.

Routing Table

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



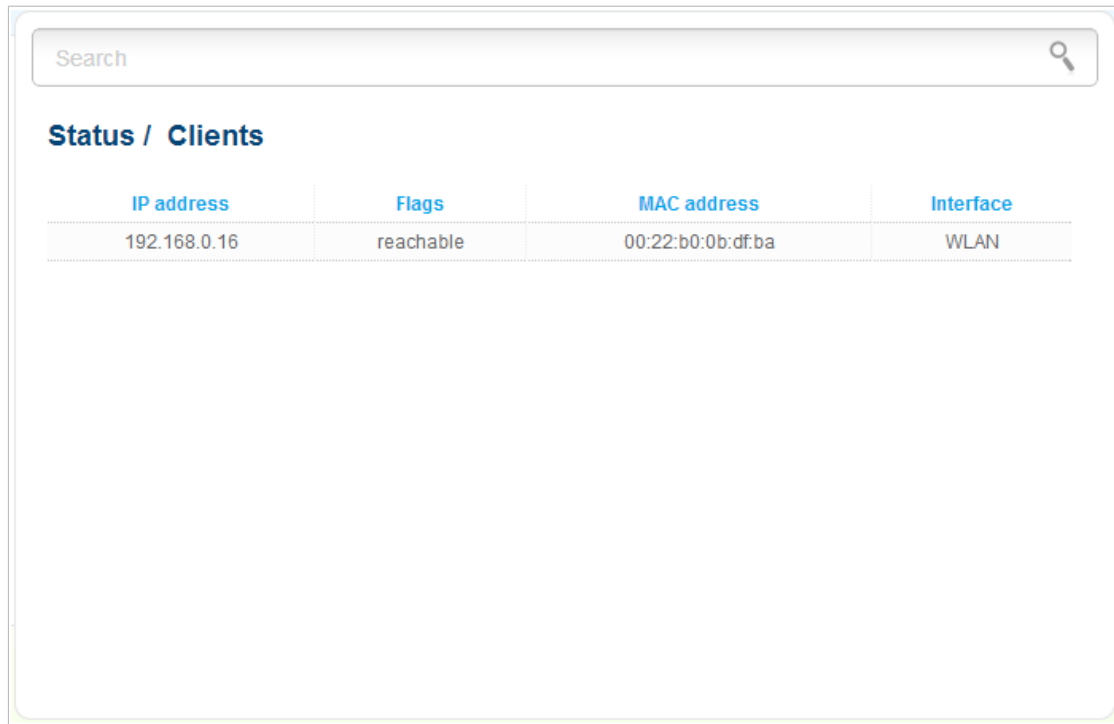
The screenshot shows a web interface for the routing table. At the top is a search bar with the text "Search" and a magnifying glass icon. Below the search bar is the heading "Status / Routing table". Underneath the heading is a table with six columns: Interface, Destination, Gateway, Mask, Flags, and Metric. The table contains one row of data: Interface: LAN, Destination: 192.168.0.0, Gateway: 0.0.0.0, Mask: 255.255.255.0, Flags: U, and Metric: 0.

Interface	Destination	Gateway	Mask	Flags	Metric
LAN	192.168.0.0	0.0.0.0	255.255.255.0	U	0

Figure 102. The **Status / Routing table** page.

Clients

On the **Status / Clients** page, you can view the list of devices connected to the access point and devices accessing its web-based interface.



The screenshot shows a web interface for the 'Status / Clients' page. At the top, there is a search bar with the text 'Search' and a magnifying glass icon. Below the search bar, the title 'Status / Clients' is displayed. Underneath the title is a table with four columns: 'IP address', 'Flags', 'MAC address', and 'Interface'. The table contains one row of data: IP address '192.168.0.16', Flags 'reachable', MAC address '00:22:b0:0b:df:ba', and Interface 'WLAN'.

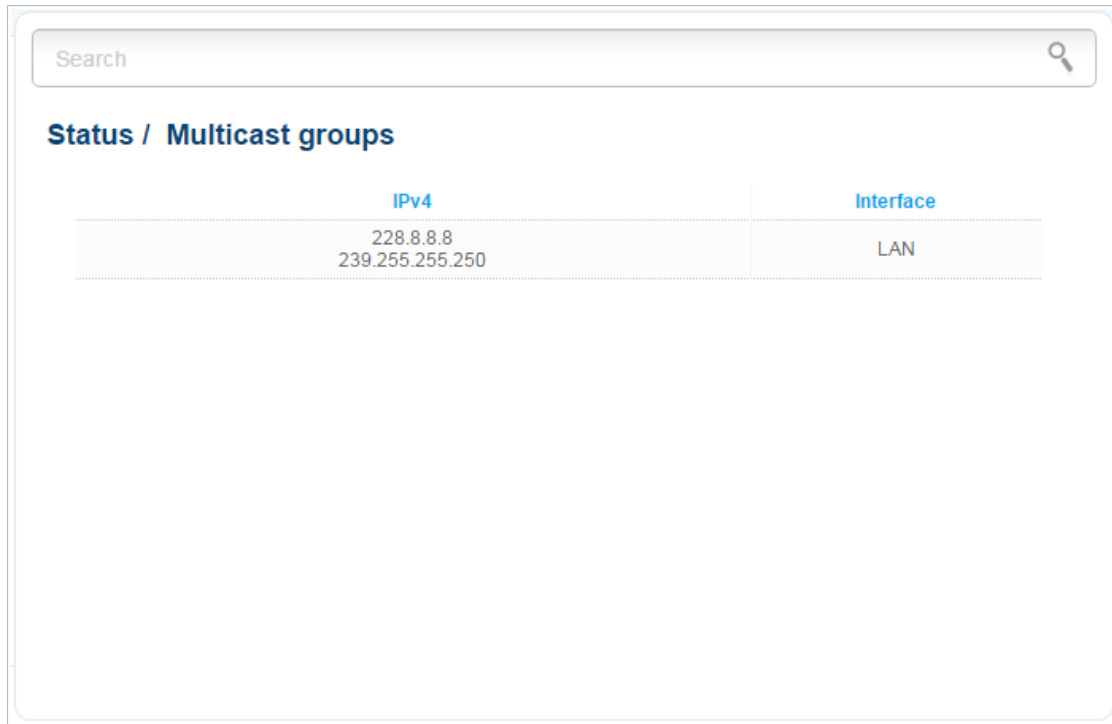
IP address	Flags	MAC address	Interface
192.168.0.16	reachable	00:22:b0:0b:df:ba	WLAN

Figure 103. The **Status / Clients** page.

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

Multicast groups

The **Status / 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.



The screenshot shows a web interface for 'Status / Multicast groups'. At the top is a search bar with the text 'Search' and a magnifying glass icon. Below the search bar is the title 'Status / Multicast groups'. Underneath is a table with two columns: 'IPv4' and 'Interface'. The table contains one row of data with the IPv4 addresses '228.8.8.8' and '239.255.255.250' in the first column, and 'LAN' in the second column.

IPv4	Interface
228.8.8.8 239.255.255.250	LAN

Figure 104. The **Status / Multicast groups** page.

Net

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

WAN

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

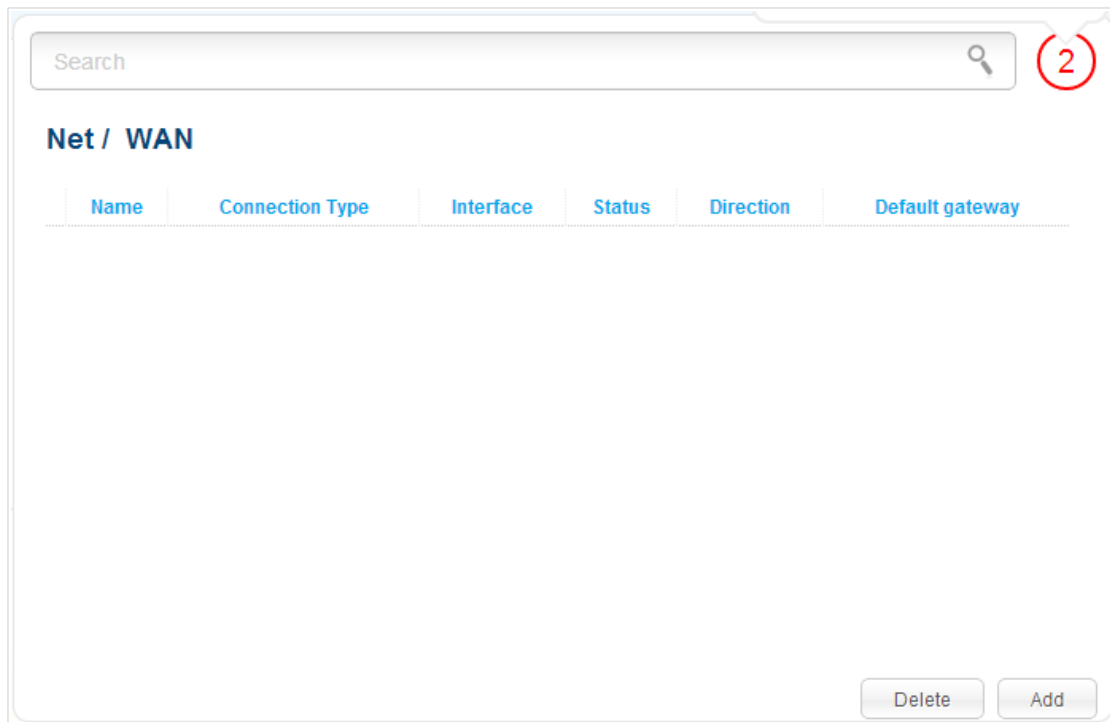


Figure 105. The **Net / WAN** page.

To create a new connection, click the **Add** button. On the page displayed, specify the relevant values.

To edit an existing connection, left-click the relevant line in the table. On the page displayed, change the parameters and click the **Apply** button.

To remove a connection, 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 use one of existing WAN connections as a default gateway, select the choice of the **Default gateway** radio button located in the line corresponding to this connection.

Creating PPPoE WAN Connection

To create a connection of the PPPoE type, click the **Add** button on the **Net / WAN** page. On the opened page, select the **PPPoE** value from the **Connection Type** drop-down list and specify the needed values.



General settings

Connection Type:

Interface:

Name:*

Enable:

Direction:

Figure 106. The page for creating a new **PPPoE** connection. The **General settings** section.

Parameter	Description
General settings	
Interface	A physical interface to which the new connection will be assigned.
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.

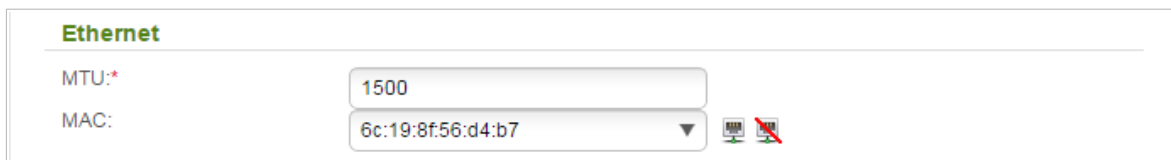


Figure 107. The page for creating a new PPPoE connection. The Ethernet section.



Parameter	Description
Ethernet	
MTU	The maximum size of units transmitted by the interface.
MAC	<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>You can click the Clone MAC address of your computer icon () 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.</p> <p>Also you can set the address of a device connected to the access point's LAN at the moment. To do this, select the relevant value from the drop-down list (the field will be filled in automatically).</p> <p>You can click the Restore default MAC address icon () to set the access point's MAC address.</p>

Figure 108. The page for creating a new PPPoE connection. The PPP section.

Parameter	Description
PPP	
Username	A username (login) to access the Internet.
Without authorization	Select the checkbox if you don't need to enter a username and password to access the Internet.
Password	A password to access the Internet.
Password confirmation	The confirmation of the entered password (to avoid mistypes).
Service name	The name of the PPPoE authentication server.
Authentication algorithm	Select a required authentication method from the drop-down list or leave the AUTO value.
MTU	The maximum size of units transmitted by the interface.
Keep Alive	Select the checkbox 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. When the checkbox is selected, the LCP interval and LCP fails fields are available. Specify the required values.
Dial on demand	Select the checkbox 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.

Parameter	Description
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this checkbox needs to be enabled.
Static IP Address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Select the checkbox if you want to log all data on PPP connection debugging.

Miscellaneous

Isolate connection:

Enable RIP:

Enable IGMP Multicast:

NAT:

Firewall:

Ping:

Figure 109. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
Isolate connection	When the checkbox is selected, the access point uses an alternate routing table for this connection. Select the checkbox only when your ISP requires this.
Enable RIP	Select the checkbox to allow using RIP for this connection.
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.
Ping	Select the checkbox to allow the access point to answer ping requests from the external network through this connection. For security reasons, it is recommended not to select this checkbox.

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

Creating Static IP or Dynamic IP WAN Connection

To create a connection of the Static IP or Dynamic IP type, click the **Add** button on the **Net / WAN** page. On the opened page, select the relevant value from the **Connection Type** drop-down list and specify the needed values.



The screenshot shows the 'General settings' section of a configuration page. It includes the following fields and controls:

- Connection Type:** A dropdown menu with 'Static IP' selected.
- Interface:** A dropdown menu with 'WAN' selected.
- Name:*** A text input field containing 'static'.
- Enable:** A checked checkbox.
- Direction:** A dropdown menu with 'WAN' selected.

Figure 110. The page for creating a new **Static IP** connection. The **General settings** section.

Parameter	Description
General settings	
Interface	A physical interface to which the new connection will be assigned.
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.

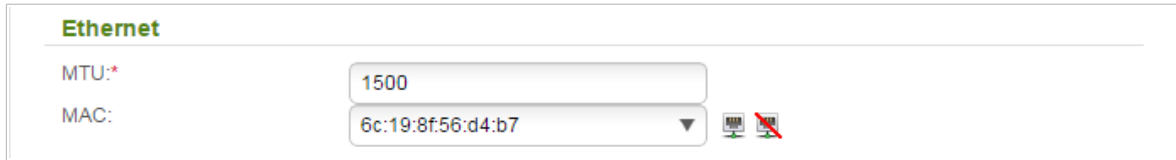




Figure 111. The page for creating a new **Static IP** connection. The **Ethernet** section.

Parameter	Description
Ethernet	
MTU	The maximum size of units transmitted by the interface.
MAC	<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>You can click the Clone MAC address of your computer icon () 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.</p> <p>Also you can set the address of a device connected to the access point's LAN at the moment. To do this, select the relevant value from the drop-down list (the field will be filled in automatically).</p> <p>You can click the Restore default MAC address icon () to set the access point's MAC address.</p>

IP

IP Address:*

Netmask:*

Gateway IP address:*

Primary DNS server:*

Secondary DNS server:

Figure 112. The page for creating a new **Static IP** connection. The **IP** section.

Parameter	Description
IP	
<i>For Static IP type</i>	
IP Address	Enter an IP address for this WAN connection.
Netmask	Enter a subnet mask for this WAN connection.
Gateway IP address	Enter an IP address of the gateway used by this WAN connection.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
<i>For Dynamic IP type</i>	
Obtain DNS server addresses automatically	Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the Primary DNS server and Secondary DNS server fields are not displayed.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. <i>Optional.</i>
Hostname	A name of the access point specified by your ISP. <i>Optional.</i>

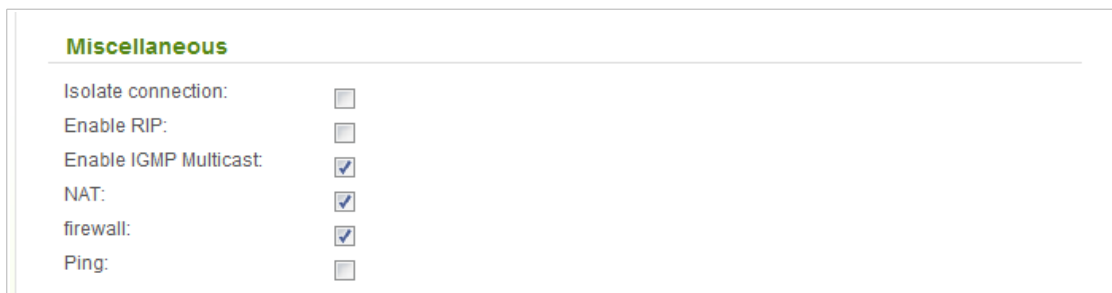


Figure 113. The page for creating a new **Static IP** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
Isolate connection	When the checkbox is selected, the access point uses an alternate routing table for this connection. Select the checkbox only when your ISP requires this.
Enable RIP	Select the checkbox to allow using RIP for this connection.
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.
Ping	Select the checkbox to allow the access point to answer ping requests from the external network through this connection. For security reasons, it is recommended not to select this checkbox.

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

Creating PPPoE + Static IP or PPPoE + Dynamic IP WAN Connection

To create a connection of the PPPoE + Static IP or PPPoE + Dynamic IP type, click the **Add** button on the **Net / WAN** page. On the opened page, select the relevant value from the **Connection Type** drop-down list and specify the needed values.

General settings

Connection Type: PPPoE + Static IP ▼

Interface: WAN ▼

Name: * pppoe_WAN_1

Enable:

Direction: WAN

Figure 114. The page for creating a new PPPoE + Static IP connection. The **General settings** section.

Parameter	Description
General settings	
Interface	A physical interface to which the new connection will be assigned.
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.

Ethernet

MTU:*





MAC:  

Figure 115. The page for creating a new PPPoE + Static IP connection. The Ethernet section.

Parameter	Description
Ethernet	
MTU	The maximum size of units transmitted by the interface.
MAC	<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>You can click the Clone MAC address of your computer icon () 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.</p> <p>Also you can set the address of a device connected to the access point's LAN at the moment. To do this, select the relevant value from the drop-down list (the field will be filled in automatically).</p> <p>You can click the Restore default MAC address icon () to set the access point's MAC address.</p>

IP

IP Address:*

Netmask:*

Gateway IP address:*

Primary DNS server:*

Secondary DNS server:

Figure 116. The page for creating a new PPPoE + Static IP connection. The IP section.

Parameter	Description
IP	
<i>For PPPoE + Static IP type</i>	
IP Address	Enter an IP address for this WAN connection.
Netmask	Enter a subnet mask for this WAN connection.
Gateway IP address	Enter an IP address of the gateway used by this WAN connection.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
<i>For PPPoE + Dynamic IP type</i>	
Obtain DNS server addresses automatically	Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the Primary DNS server and Secondary DNS server fields are not displayed.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. <i>Optional.</i>
Hostname	A name of the access point specified by your ISP. <i>Optional.</i>

Miscellaneous

Isolate connection:

Enable RIP:

Enable IGMP Multicast:

NAT:

Firewall:

Ping:

Figure 117. The page for creating a new **PPPoE + Static IP** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous (for IP section)	
Isolate connection	When the checkbox is selected, the access point uses an alternate routing table for this connection. Select the checkbox only when your ISP requires this.
Enable RIP	Select the checkbox to allow using RIP for this connection.
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.
Ping	Select the checkbox to allow the access point to answer ping requests from the external network through this connection. For security reasons, it is recommended not to select this checkbox.

PPP

Username:*

Without authorization:

Password:*

Password confirmation:*

Service name:

Authentication algorithm: AUTO ▼

MTU:*

Keep Alive:

LCP interval (sec):*

LCP fails:*

Dial on demand:

PPP IP extension:

Static IP Address:

PPP debug:

Figure 118. The page for creating a new **PPPoE + Static IP** connection. The **PPP** section.

Parameter	Description
PPP	
Username	A username (login) to access the Internet.
Without authorization	Select the checkbox if you don't need to enter a username and password to access the Internet.
Password	A password to access the Internet.
Password confirmation	The confirmation of the entered password (to avoid mistypes).
Service name	The name of the PPPoE authentication server.
Authentication algorithm	Select a required authentication method from the drop-down list or leave the AUTO value.
MTU	The maximum size of units transmitted by the interface.
Keep Alive	Select the checkbox 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. When the checkbox is selected, the LCP interval and LCP fails fields are available. Specify the required values.
Dial on demand	Select the checkbox 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.

Parameter	Description
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this checkbox needs to be enabled.
Static IP Address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Select the checkbox if you want to log all data on PPP connection debugging.

Miscellaneous

Isolate connection:

Enable RIP:

Enable IGMP Multicast:

NAT:

Firewall:

Ping:

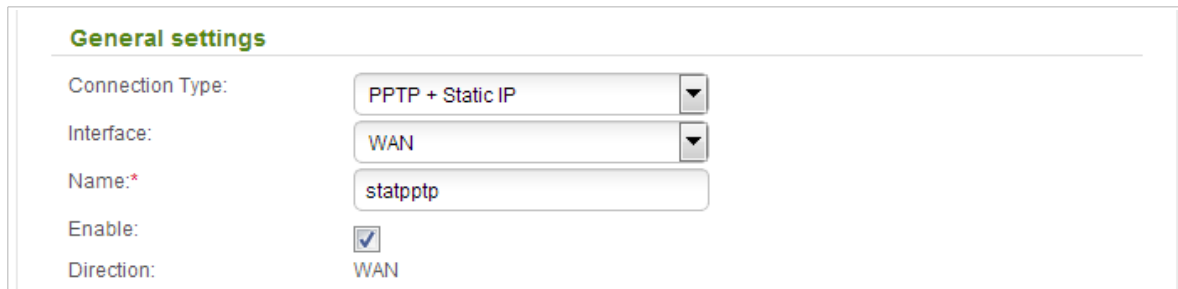
Figure 119. The page for creating a new **PPPoE + Static IP** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous (for PPP section)	
Isolate connection	When the checkbox is selected, the access point uses an alternate routing table for this connection. Select the checkbox only when your ISP requires this.
Enable RIP	Select the checkbox to allow using RIP for this connection.
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.
Ping	Select the checkbox to allow the access point to answer ping requests from the external network through this connection. For security reasons, it is recommended not to select this checkbox.

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

Creating PPTP/L2TP + Static IP or PPTP/L2TP + Dynamic IP WAN Connection

To create a connection of the PPTP + Static IP, L2TP + Static IP, PPTP + Dynamic IP, or L2TP + Dynamic IP type, click the **Add** button on the **Net / WAN** page. On the opened page, select the relevant value from the **Connection Type** drop-down list and specify the needed values.



General settings

Connection Type: PPTP + Static IP

Interface: WAN

Name:* statppt

Enable:

Direction: WAN

Figure 120. The page for creating a new **PPTP + Static IP** connection. The **General settings** section.

Parameter	Description
General settings	
Interface	A physical interface to which the new connection will be assigned.
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.

Ethernet

MTU:*





MAC:  

Figure 121. The page for creating a new **PPTP + Static IP** connection. The **Ethernet** section.

Parameter	Description
Ethernet	
MTU	The maximum size of units transmitted by the interface.
MAC	<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>You can click the Clone MAC address of your computer icon () 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.</p> <p>Also you can set the address of a device connected to the access point's LAN at the moment. To do this, select the relevant value from the drop-down list (the field will be filled in automatically).</p> <p>You can click the Restore default MAC address icon () to set the access point's MAC address.</p>

IP

IP Address:*

Netmask:*

Gateway IP address:*

Primary DNS server:*

Secondary DNS server:

Isolate connection:

Enable RIP:

Enable IGMP Multicast:

NAT:

Firewall:

Ping:

Figure 122. The page for creating a new **PPTP + Static IP** connection. The **IP** section.

Parameter	Description
IP	
<i>For PPTP + Static IP and L2TP + Static IP types</i>	
IP Address	Enter an IP address for this WAN connection.
Netmask	Enter a subnet mask for this WAN connection.
Gateway IP address	Enter an IP address of the gateway used by this WAN connection.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Isolate connection	When the checkbox is selected, the access point uses an alternate routing table for this connection. Select the checkbox only when your ISP requires this.
Enable RIP	Select the checkbox to allow using RIP for this connection.
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.
Ping	Select the checkbox to allow the access point to answer ping requests from the external network through this connection. For security reasons, it is recommended not to select this checkbox.

Parameter	Description
<i>For PPTP + Dynamic IP and L2TP + Dynamic IP types</i>	
Obtain DNS server addresses automatically	Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the Primary DNS server and Secondary DNS server fields are not displayed.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. <i>Optional.</i>
Hostname	A name of the access point specified by your ISP. <i>Optional.</i>
Isolate connection	When the checkbox is selected, the access point uses an alternate routing table for this connection. Select the checkbox only when your ISP requires this.
Enable RIP	Select the checkbox to allow using RIP for this connection.
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.
Ping	Select the checkbox to allow the access point to answer ping requests from the external network through this connection. For security reasons, it is recommended not to select this checkbox.

VPN

Connect automatically:

Username:*

Without authorization:

Password:*

Password confirmation:*

VPN server address:*

Encryption: No encrypt ▼

Authentication algorithm: AUTO ▼

MTU:*

Keep Alive:

LCP interval (sec):*

LCP fails:*

Extra options:

Dial on demand:

Static IP Address:

PPP debug:

IP received:

Isolate connection:

Enable RIP:

NAT:

Firewall:

Ping:

Figure 123. The page for creating a new **PPTP + Static IP** connection. The **VPN** section.

Parameter	Description
VPN	
Connect automatically	Select the checkbox to enable auto-start of the connection upon the boot-up of the access point.
Username	A username (login) to access the Internet.
Without authorization	Select the checkbox if you don't need to enter a username and password to access the Internet.
Password	A password to access the Internet.
Password confirmation	The confirmation of the entered password (to avoid mistypes).
VPN server address	The IP or URL address of the PPTP or L2TP authentication server.

Parameter	Description
Encryption	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encrypt: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP, MS-CHAP-V2, or AUTO value is selected from the Authentication algorithm drop-down list.</p>
Authentication algorithm	<p>Select a required authentication method from the drop-down list or leave the AUTO value.</p>
MTU	<p>The maximum size of units transmitted by the interface.</p>
Keep Alive	<p>Select the checkbox 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. When the checkbox is selected, the LCP interval and LCP fails fields are available. Specify the required values.</p>
Extra options	<p>Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional.</i></p>
Dial on demand	<p>Select the checkbox 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.</p>
Static IP Address	<p>Fill in the field if you want to use a static IP address to access the Internet.</p>
PPP debug	<p>Select the checkbox if you want to log all data on PPP connection debugging.</p>
IP received	<p>The IP address assigned by the ISP.</p>
Isolate connection	<p>When the checkbox is selected, the access point uses an alternate routing table for this connection. Select the checkbox only when your ISP requires this.</p>
Enable RIP	<p>Select the checkbox to allow using RIP for this connection.</p>

Parameter	Description
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.
Ping	Select the checkbox to allow the access point to answer ping requests from the external network through this connection. For security reasons, it is recommended not to select this checkbox.

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

LAN

To configure the access point's local interface, proceed to the **Net / LAN** page.

The screenshot shows a configuration form with two input fields. The first field is labeled 'IP Address:*' and contains the value '192.168.0.50'. The second field is labeled 'Netmask:*' and contains the value '255.255.255.0'.

Figure 124. Basic settings of the local interface.

If needed, edit the basic settings of the local interface.

Parameter	Description
IP Address	The IP address of the access point in the local subnet. By default, the following value is specified: 192 . 168 . 0 . 50 .
Netmask	The mask of the local subnet. By default, the following value is specified: 255 . 255 . 255 . 0 .

When needed settings are configured, click the **Apply** button.

In the **DHCP server** section, you can configure the built-in DHCP server of the access point. In the router mode, the DHCP server is enabled by default.

The screenshot shows the 'DHCP server' configuration section. It includes a 'Mode:' dropdown menu set to 'Enable', a 'DNS Relay:' checkbox that is checked, and three input fields: 'Start IP:*' with '192.168.0.51', 'End IP:*' with '192.168.0.100', and 'Lease time (min):*' with '1440'.

Figure 125. The section for configuring the DHCP server.

Parameter	Description
Mode	<p>An operating mode of the access point's DHCP server.</p> <p>Enable: the access point assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the DNS Relay, Start IP, End IP, and the Lease time fields are displayed on the page.</p> <p>Disable: the access point's DHCP server is disabled, clients' IP addresses are assigned manually.</p> <p>Relay: an external DHCP server is used to assign IP addresses to clients. When this value is selected, the External DHCP server IP field is displayed on the page.</p>

Parameter	Description
DNS Relay	Select the checkbox so that the devices connected to the access point obtain the address of the access point as the DNS server address. Deselect the checkbox 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.
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.
External DHCP server IP	The IP address of the external DHCP server which assigns IP addresses to the access point's clients.

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

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

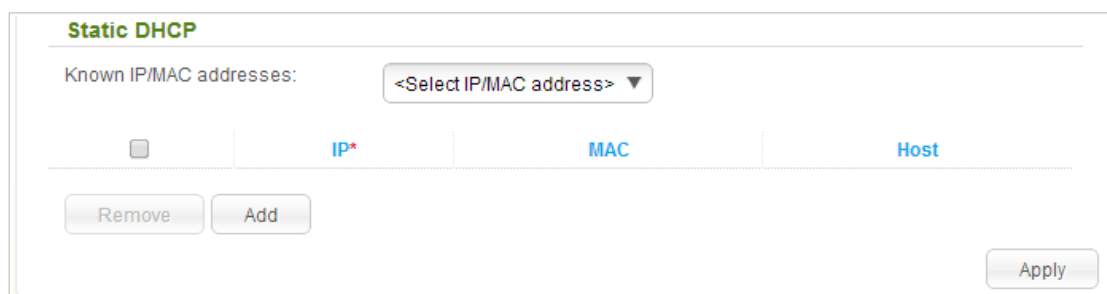


Figure 126. The section for creating MAC-IP pairs.

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

Also you can create a MAC-IP pair for a device connected to the access point's LAN at the moment. To do this, select the relevant value from the **Known IP/MAC addresses** drop-down list (the fields of the section will be filled in automatically).

When all needed MAC-IP pairs are specified, click the **Apply** button.

Existing MAC-IP pairs are displayed in the table of the **Static DHCP** section. To remove a pair, select the checkbox in the relevant line in the table and click the **Remove** button. Then click the **Apply** button.

Wi-Fi

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

Basic Settings

On the **Wi-Fi / Basic settings** page, you can enable the wireless local area network (WLAN) of the access point and configure its basic parameters.

Figure 127. Basic settings of the wireless LAN.

Parameter	Description
Enable Wireless	The checkbox enables Wi-Fi connections. If you want to disable your WLAN, deselect the checkbox.
Broadcast wireless network	If the checkbox is not selected, devices cannot connect to the access point's WLAN (or to the selected part of the WLAN if the network is split into parts). Upon that the device can connect to another access point as a wireless client.

Parameter	Description
MBSSID	<p>To split the network into several parts, select a relevant value (2, 3, or 4) from the drop-down list. By default, the wireless network is not split (the Disabled value is selected from the list).</p> <p>For every part of the WLAN you can specify a name (SSID), some parameters from the basic settings page, and security settings. To do this, select the needed part from the BSSID drop-down list and click the Apply button. Then specify needed parameters on the Wi-Fi / Basic settings page or proceed to the Wi-Fi / Security settings page.</p>
BSSID	<p>The unique identifier for your Wi-Fi network. You cannot change the value of this parameter, it is determined in the device's internal settings.</p> <p>If you have split your WLAN into parts, the drop-down list contains several values. Each identifier corresponds to a single part of the WLAN.</p>
Hide Access Point	<p>If the checkbox is selected, other users cannot see your Wi-Fi network. (It is recommended not to select this checkbox in order to simplify initial configuration of your WLAN.)</p>
SSID	<p>A name for the WLAN. By default, the value DAP-1360 is specified. If your network is split into parts, each part has the default name (DAP-1360.2, DAP-1360.3, and DAP-1360.4). It is recommended to specify another name for the network upon initial configuration (use digits and Latin characters).</p>
Country	<p>The country you are in. Select a value from the drop-down list.</p>
Channel	<p>The wireless channel number. When the auto value is selected, the access point itself chooses the channel with the least interference.</p>
Wireless mode	<p>Operating mode of the wireless network of the access point. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.</p>
Max Associated Clients	<p>The maximum number of devices connected to the wireless network of the access point (or to the selected part of the WLAN if the network is split into parts). When the value 0 is specified, the device does not limit the number of connected clients.</p>
Clients Isolation	<p>Select the checkbox to forbid wireless clients of your WLAN (or the selected part of the WLAN if the network is split into parts) to communicate to each other.</p>

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

Security Settings

On the **Wi-Fi / Security settings** page, you can modify security settings of the WLAN.

The screenshot shows the 'Wi-Fi / Security settings' page. At the top is a search bar. Below it, the title 'Wi-Fi / Security settings' is displayed. Under 'Network Authentication', a dropdown menu is set to 'WPA2-PSK'. Below that, the 'Encryption Key PSK' field contains the value '15689742'. A section titled 'WPA Encryption settings' is separated by a horizontal line. Under 'WPA Encryption', a dropdown menu is set to 'AES'. Below that, the 'WPA renewal' field contains the value '3600'. An 'Apply' button is located at the bottom right of the settings area.

Figure 128. The default security settings.

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

The screenshot shows the 'Wi-Fi / Security settings' page with the 'Network Authentication' dropdown menu open. The menu lists the following options: 'Open' (highlighted in blue), 'Shared', 'WPA', 'WPA-PSK', 'WPA2', 'WPA2-PSK', 'WPA/WPA2 mixed', and 'WPA-PSK/WPA2-PSK mixed'. The 'Enable Encryption WEP' field is currently empty. An 'Apply' button is located at the bottom right of the settings area.

Figure 129. 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).
Shared	Shared key authentication with WEP encryption. This authentication type is not available when on the Wi-Fi / Basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected.
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 WLAN of the access point.
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 WLAN of the access point.



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

When the **Open** or **Shared** value is selected, the **WEP Encryption settings** section is displayed (the section is unavailable for the wireless network operating modes which support the standard 802.11n):

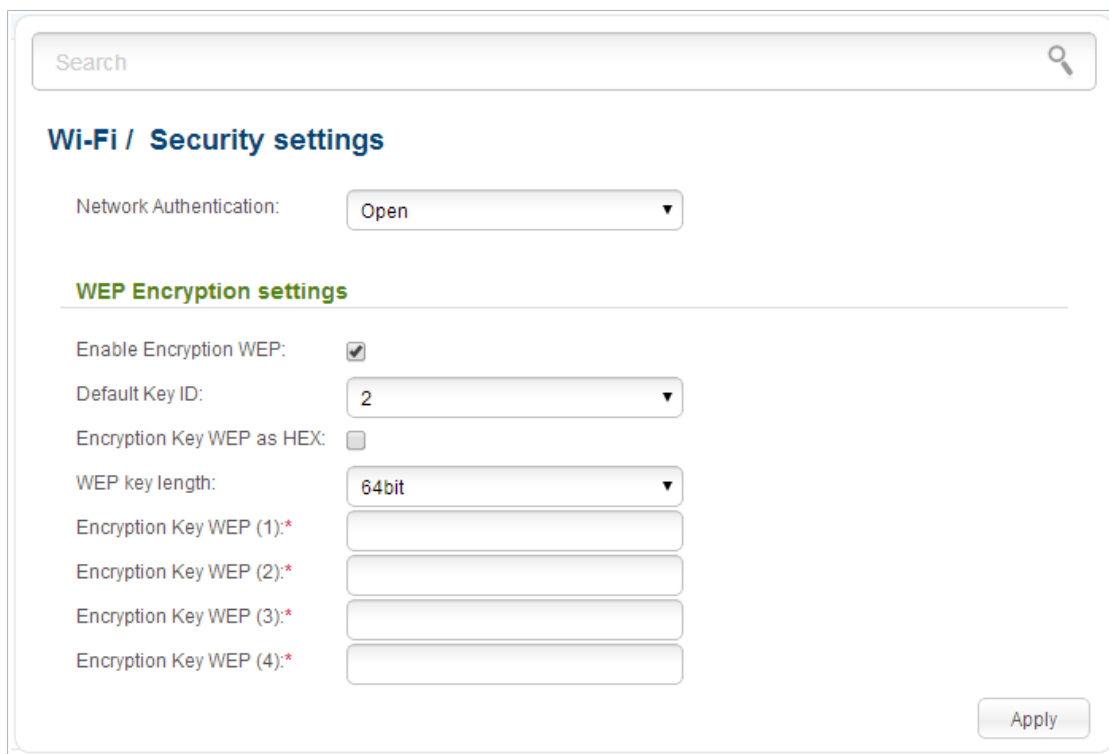


Figure 130. The **Open** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
Enable Encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the Default Key ID field, the Encryption Key WEP as HEX checkbox, the WEP key length drop-down list, and four Encryption Key WEP fields are displayed on the page. For the Shared authentication type the checkbox is always selected.
Default Key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption Key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.
WEP key length	The length of WEP encryption key. Select the value 64bit to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the value 128bit to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Encryption Key WEP (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.

When the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the **WPA Encryption settings** section is displayed:

The screenshot shows a web interface for configuring Wi-Fi security. At the top is a search bar. Below it is the heading 'Wi-Fi / Security settings'. Under this heading, there are two main sections. The first section, 'Network Authentication', has a dropdown menu currently showing 'WPA2-PSK' and a text input field for 'Encryption Key PSK' containing the value '15689742'. The second section, 'WPA Encryption settings', has a dropdown menu for 'WPA Encryption' set to 'AES' and a text input field for 'WPA renewal' set to '3600'. An 'Apply' button is located at the bottom right of the settings area.

Figure 131. The **WPA-PSK/WPA2-PSK mixed** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
Encryption Key PSK	A key for WPA encryption. The key can contain digits and/or Latin characters.
WPA Encryption	An encryption method: TKIP , AES , or TKIP+AES .
WPA renewal	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 the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the **RADIUS settings** and **WPA Encryption settings** sections are available:

Figure 132. The **WPA/WPA2 mixed** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
WPA2 Pre-authentication	The checkbox activating preliminary authentication (displayed only for the WPA2 and WPA/WPA2 mixed authentication types).
IP address	The IP address of the 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).
WPA Encryption	An encryption method: TKIP , AES , or TKIP+AES .
WPA renewal	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.

MAC Filter

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

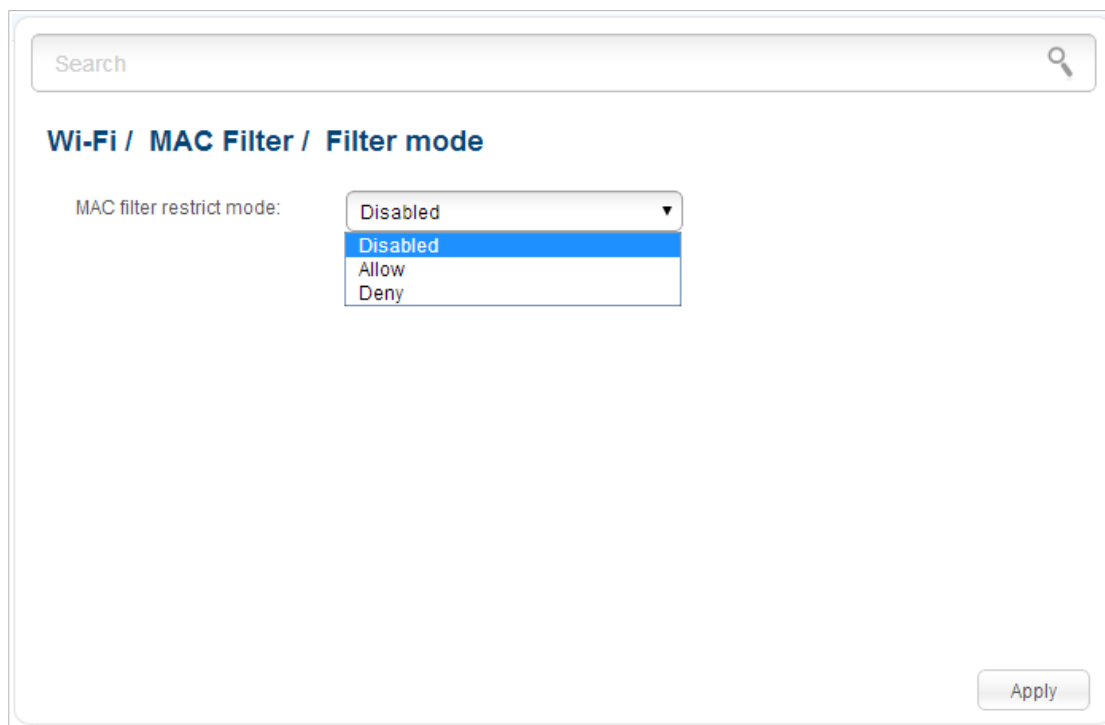


Figure 133. The page for configuring the MAC filter for the wireless network.

By default, MAC filtering is not active (the **Disabled** value is selected from the **MAC filter restrict mode** drop-down list on the **Wi-Fi / MAC Filter / Filter mode** page).

To open your wireless network for the devices which MAC addresses are specified on the **Wi-Fi / MAC Filter / MAC addresses** page and to close the wireless network for all other devices, select the **Allow** value from the **MAC filter restrict mode** drop-down list and click the **Apply** button.

To close your wireless network for the devices which MAC addresses are specified on the **Wi-Fi / MAC Filter / MAC addresses** page, select the **Deny** value from the **MAC filter restrict mode** drop-down list and click the **Apply** button.

To add a MAC address to which the selected filtering mode will be applied, proceed to the **Wi-Fi / MAC Filter / MAC addresses** page.

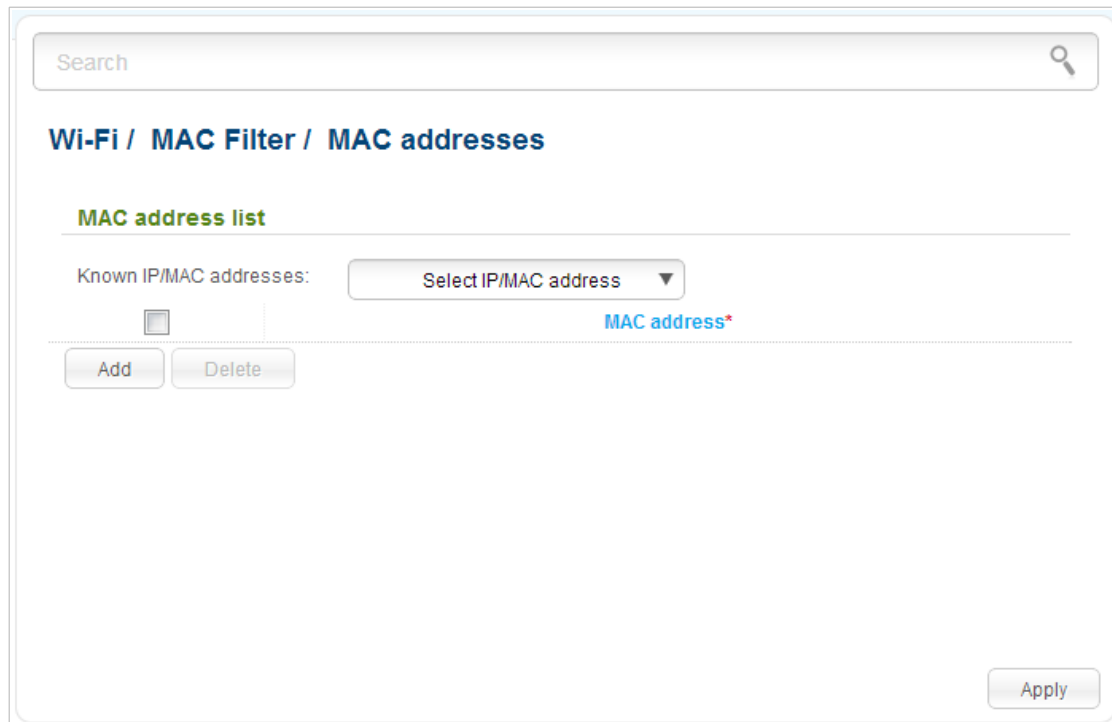


Figure 134. The page for adding a MAC address.

Click the **Add** button and enter an address in the field displayed. Also you can enter the MAC address of a device connected to the LAN of the access point at the moment. To do this, select the relevant device from the **Known IP/MAC addresses** drop-down list (the field will be filled in automatically). Then click the **Apply** button.

To remove a MAC address from the list of MAC addresses, select the checkbox located to the left of the relevant MAC address and click the **Delete** button. Then click the **Apply** button.

List of Wi-Fi Clients

On the **Wi-Fi / List of WiFi clients** page, you can view the list of wireless clients connected to the access point. Devices connected to the access point via the WDS function are not displayed in the list.

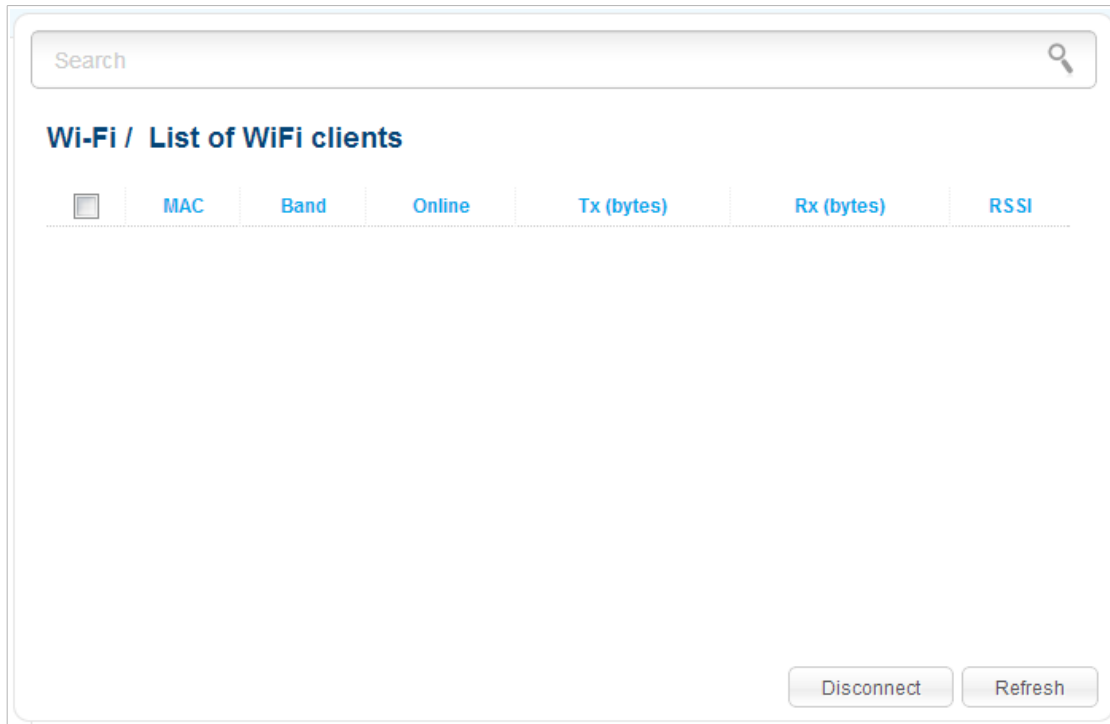


Figure 135. The list of the wireless clients.

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

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

WPS

On the **Wi-Fi / WPS** page, you can enable the function for secure configuration of the WLAN and select a method used to easily add wireless devices 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.

! If the device's WLAN is split into parts (the value **2**, **3**, or **4** is selected from the **MBSSID** drop-down list on the **Wi-Fi / Basic settings** page), the WPS function can be used only for the first part of the WLAN (the first value from the **BSSID** drop-down list).

! 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 (on the **Wi-Fi / Security settings** page). When other security settings are specified, controls of the **Wi-Fi / WPS** page are not available.

Search

Wi-Fi / WPS

Enable/Disable WPS

WPS Enable:

Apply

Information

Default PIN code:	12345670
WPS Status:	Configured
SSID:	DAP-1360
Network Authentication:	WPA2-PSK
Encryption:	AES
Encryption key:	76543210

Refresh Reset to unconfigured

Connection

WPS Method: PBC

Connect

Figure 136. The page for configuring the WPS function.

To activate the WPS function, select the **WPS Enable** checkbox and click the **Apply** button. When the checkbox is selected, the **Information** and **Connection** sections are available on the page.

Parameter	Description
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.
WPS Status	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).
SSID	The name of the access point's WLAN (or the first part of the WLAN if the network is split into parts).
Network Authentication	The network authentication type specified for the WLAN (or the first part of the WLAN).
Encryption	The encryption type specified for the WLAN (or the first part of the WLAN).
Encryption key	The encryption key specified for the WLAN (or the first part of the WLAN).
Refresh	Click the button to refresh the data on the page.
Reset to unconfigured	Click the button to reset the parameters of the WPS function.
WPS Method	A method of the WPS function. Select a value from the drop-down list. PIN : Connecting the device via the PIN code. PBC : Connecting the device via the push button (actual or virtual).
PIN Code	The PIN code of the WPS-enabled device that needs to be connected to the wireless network of the access point. The field is displayed only when the PIN value is selected from the WPS Method drop-down list.
Connect	Click the button to connect the wireless device to the access point's WLAN via the WPS function.

Using WPS Function via Web-based Interface

To add a wireless device via the PIN method of the WPS function, follow the next steps:

1. Select the **WPS Enable** checkbox.
2. Click the **Apply** button.
3. 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 add a wireless device via the PBC method of the WPS function, follow the next steps:


1. Select the **WPS Enable** checkbox.
2. Click the **Apply** button.
3. 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. Click the **Connect** button in the web-based interface of the access point.

Using WPS Function without Web-based Interface

You can add a wireless device to the access point's WLAN 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 corresponding security settings for the wireless network of the access point.
2. Select the **WPS Enable** checkbox.
3. Click the **Apply** button.

4. Save the settings and close the web-based interface (click the icon  (**Save**) in the menu displayed when the mouse pointer is over the **System** caption in the top left part of

the page, then click the icon  (**Logout**)).

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

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.

Search

Wi-Fi / WDS

WDS Mode: Bridge mode

WDS Encryption : NONE

Encryption Key:

WDS MAC (1):

WDS MAC (2):

WDS MAC (3):

WDS MAC (4):

Apply

Figure 137. The page for configuring the WDS function.

The following fields are available on the page:

Parameter	Description
WDS Mode	The WDS function mode. 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.
WDS Encryption	A type of encryption for data transfer between access points interconnected via the WDS function. NONE: No encryption. WEP. TKIP. AES.
Encryption Key	A key for the specified type of encryption. If the NONE value is selected from the WDS Encryption drop-down list, the field is not editable.
WDS MAC (1-4)	The MAC addresses of devices connected to the access point via the WDS function.



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.

Additional Settings

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

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

Figure 138. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
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.
Beacon Period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
RTS Threshold	The minimum size (in bites) of a packet for which an RTS frame is transmitted.
Frag Threshold	The maximum size (in bites) 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.

Parameter	Description
TX Power	The transmit power (in percentage terms) of the access point.
Drop multicast	Select the checkbox to disable multicasting for the access point's WLAN. Deselect the checkbox to enable multicasting from WAN connections for which the Enable IGMP Multicast checkbox is selected.
Bandwidth	The channel bandwidth for 802.11n devices. 20MHz : 802.11n devices operate at 20MHz channels. 40MHz : 802.11n devices operate at 40MHz channels. 20/40MHz - : 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the previous adjacent channel). 20/40MHz + : 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the next adjacent channel).
Short GI	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the access point is communicating to wireless devices. Enable : the access point uses the 400 ns short guard interval. For the wireless network operating modes which support 802.11n standard only (see the value of the Wireless mode drop-down list on the Wi-Fi / Basic settings page). Disable : the access point uses the 800 ns standard guard interval.
Adaptivity Mode	Select the checkbox to prevent your wireless network from interfering with radars and other mobile or stationary radio systems. Such a setting can slow down the WLAN of the access point.

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.

To enable the function, select the **WMM** checkbox and click the **Apply** button.

Wi-Fi / WMM

WMM:

Parameters of Access Point

AC	Aifsn (1~15)*	CWMin	CWMax	Txop*	ACM	Ack
AC_BK	7	1	1023	0	Off	Off
AC_BE	3	15	63	0	Off	Off
AC_VI	1	7	15	94	Off	Off
AC_VO	1	3	7	47	Off	Off

Parameters of Station

AC	Aifsn (1~15)*	CWMin	CWMax	Txop*	ACM
AC_BK	7	15	1023	0	Off
AC_BE	3	15	1023	0	Off
AC_VI	2	7	15	94	Off
AC_VO	2	3	7	47	Off

Apply

Figure 139. The page for configuring the WMM function.

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

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

- **AC_BK** (*Background*), low priority traffic (print jobs, file downloads, etc.).
- **AC_BE** (*Best Effort*), traffic from legacy devices or devices/applications that do not support QoS.
- **AC_VI** (*Video*).
- **AC_VO** (*Voice*).

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

For every Access Category the following fields are available:

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.
Txop	<i>Transmission Opportunity.</i> The higher the value, the higher is the Access Category priority.
ACM	<i>Admission Control Mandatory.</i> If on, prevents from using the relevant Access Category.
Ack	<i>Acknowledgment.</i> Answering response requests while transmitting. Displayed only in the Parameters of Access Point section. If off, the access point answers requests. If on, the access point does not answer requests.

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

Client

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

The “client” function in the router mode allows using DAP-1360U as a WISP repeater.

To use the access point as a WISP repeater, you need to configure the same channel of the wireless connection for DAP-1360U and the WISP access point. Other parameters of the wireless network of DAP-1360U do not depend upon the settings of the WISP access point.

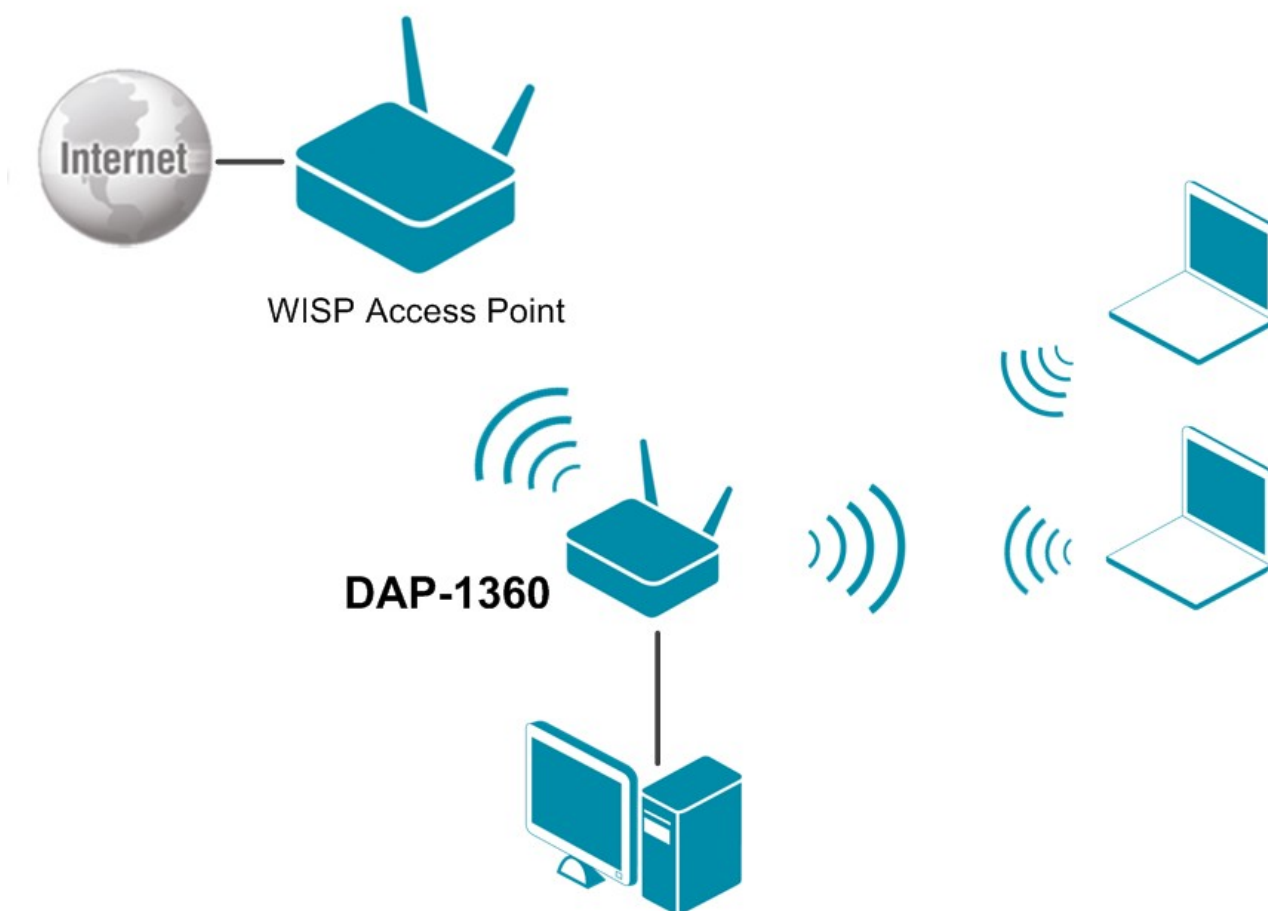


Figure 140. Connecting DAP-1360U in the router mode as a client.

After configuring the device as a client, you need to create a WAN connection with relevant parameters for the **WiFiClient** interface.

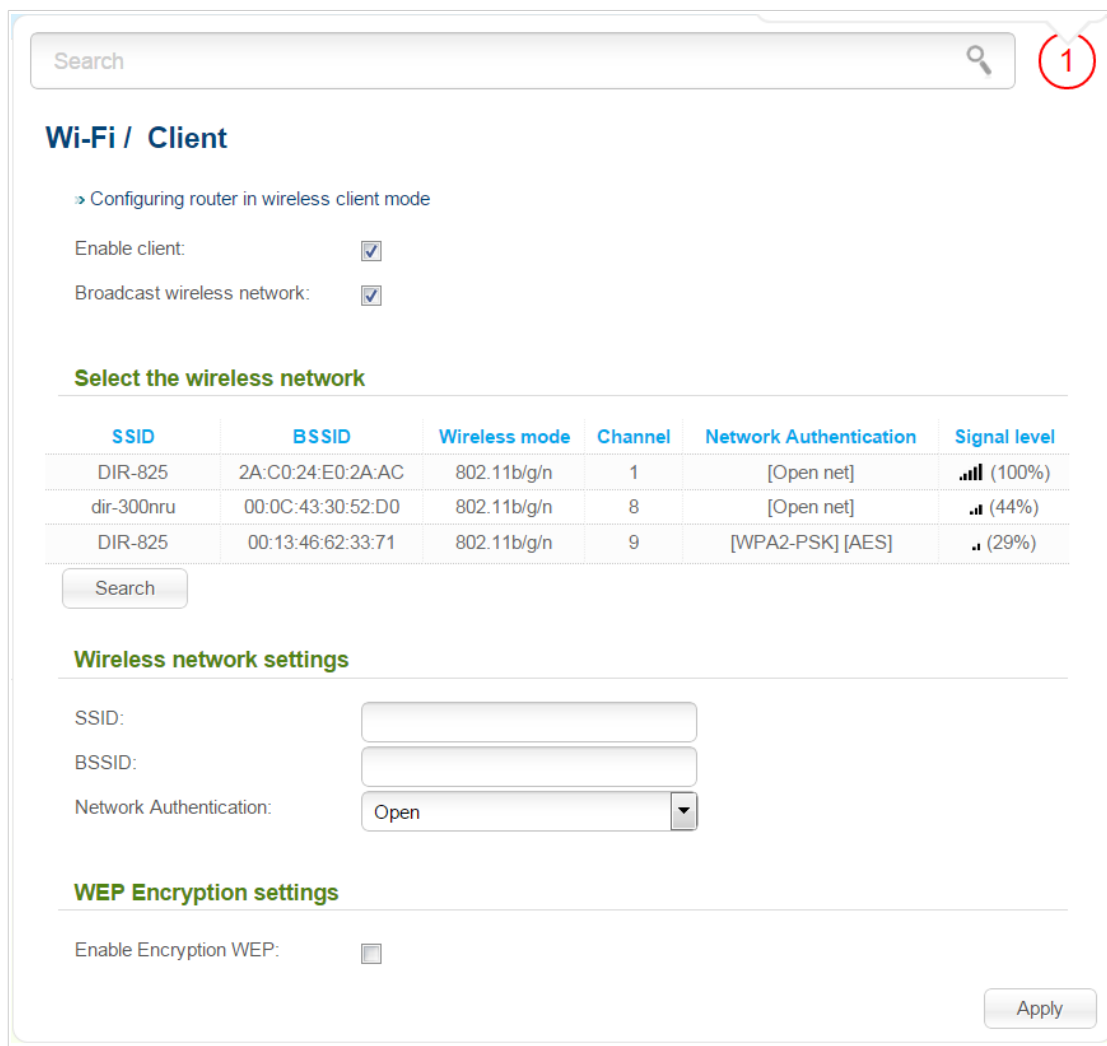


Figure 141. The page for configuring the client mode.

To configure the access point as a client, select the **Enable client** checkbox. When the checkbox is selected, the following fields are displayed on the page:

Parameter	Description
Broadcast wireless network	If the checkbox is not selected, devices cannot connect to the access point's WLAN. Upon that DAP-1360U can connect to another access point as a wireless client.
Wireless network settings	
SSID	The name of the network to which the access point connects.
BSSID	The unique identifier of the network to which the access point connects.
Network Authentication	The authentication type of the network to which the access point connects.

When the **Open** or **Shared** authentication type is selected, the following fields are available:

Parameter	Description
Enable Encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the Default Key ID field, the Encryption Key WEP as HEX checkbox, the WEP key length drop-down list, and four Encryption Key WEP fields are displayed on the page. For the Shared authentication type the checkbox is always selected.
Default Key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption Key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.
WEP key length	The length of WEP encryption key. Select the value 64bit to specify keys containing 5 ASCII symbols or 10 HEX symbols. Select the value 128bit to specify keys containing 13 ASCII symbols or 26 HEX symbols.
Encryption Key WEP (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.

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

Parameter	Description
Encryption Key PSK	A key for WPA encryption. The key can contain digits and/or Latin characters.
WPA Encryption	An encryption method: TKIP , AES , or TKIP+AES .

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

In addition, when the **Enable client** checkbox is selected, the list of available wireless networks is displayed on the page.

To view the latest data on the wireless networks, click the **Search** button.

To connect to a wireless network from the list, select the needed network. Upon that the relevant values are automatically inserted in the **SSID**, **BSSID**, and **Network Authentication** fields.

For the **Open** authentication type with no encryption, click the **Apply** button.

For the **Open** authentication type with encryption and the **Shared** authentication type, select a needed value from the **Default Key ID** drop-down list. If needed, select the **Encryption Key WEP as HEX** checkbox to set a hexadecimal number as a key for encryption. Then select a needed value in the **WEP key length** drop-down list, fill in 4 **Encryption Key WEP** fields, and click the **Apply** button.

For the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** authentication types, fill in the **Encryption Key PSK** field and click the **Apply** button.

After clicking the **Apply** button, the wireless channel of DAP-1360U will switch to the channel of the wireless access point to which you have connected.

If the access point is connected to the selected network successfully, the green indicator appears to the right of the network's SSID in the table.

The step-by-step description of how to configure the access point as a wireless client is available on D-Link website. To access it, click the **Configuring router in wireless client mode** link in the top part of the page.

Advanced

In this menu you can configure advanced settings of the access point switched to the router mode:

- enable the UPnP IGD protocol
- configure a DDNS service
- add name servers
- define static routes
- create rules for remote access to the web-based interface
- allow the access point to use IGMP, RTSP, enable the SIP ALG, PPPoE pass through, PPTP pass through, and L2TP pass through functions.

UPnP IGD

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 142. The **Advanced / UPnP IGD** page.

If you want to manually specify all parameters needed for network applications, deselect the **Enabled** checkbox and click the **Apply** button.

If you want to enable the UPnP IGD protocol in the access point, select the **Enabled** checkbox and click the **Apply** button.

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	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.
Comments	Information transmitted by a client's network application.

DDNS

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

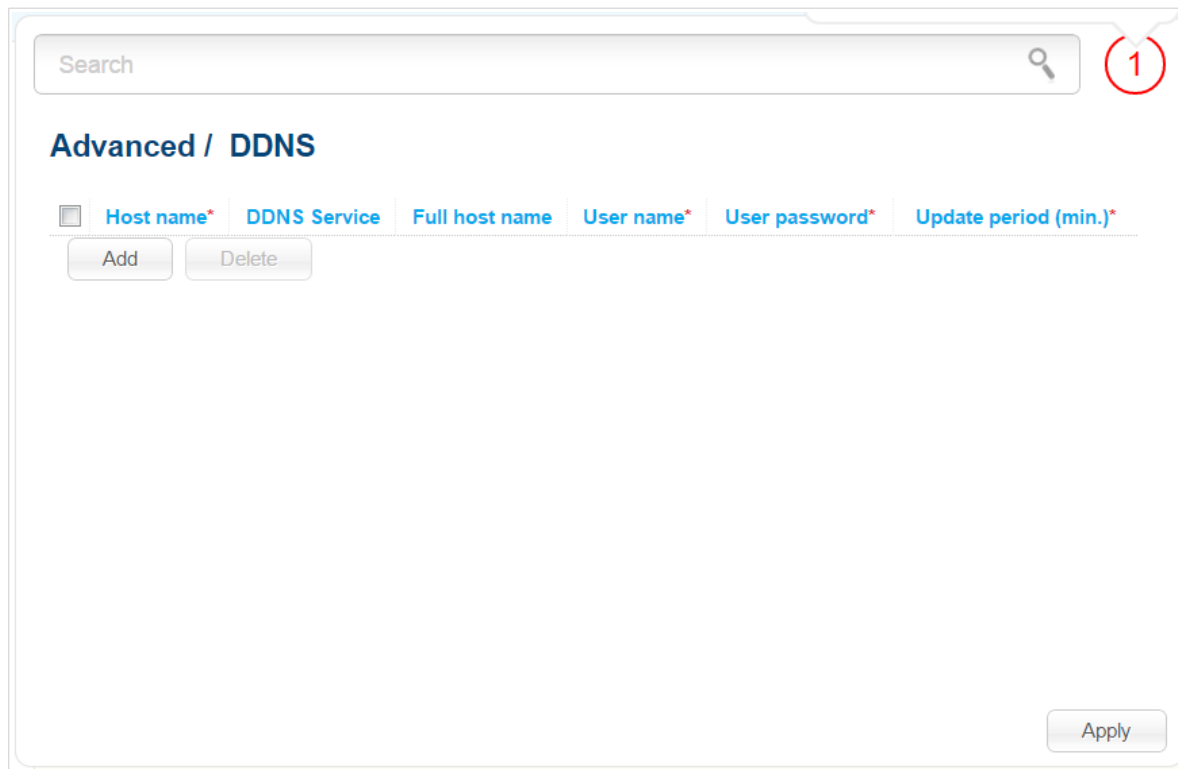


Figure 143. The **Advanced / DDNS** page.

To add a new DDNS service, click the **Add** button. In the line displayed, you can specify the following parameters:

Parameter	Description
Host name	The part of the domain name specified by a user while registering at a DDNS provider.
DDNS Service	Select a DDNS provider from the drop-down list.
Full host name	The domain name registered at your DDNS provider. The field will be filled in automatically.
User name	The username to authorize for your DDNS provider.
User password	The password to authorize for your DDNS provider.
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 **Apply** button.

To edit parameters of the existing DDNS service, select a needed field in the relevant line of the table, change its value, and click the **Apply** 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. Then click the **Apply** button.

DNS

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

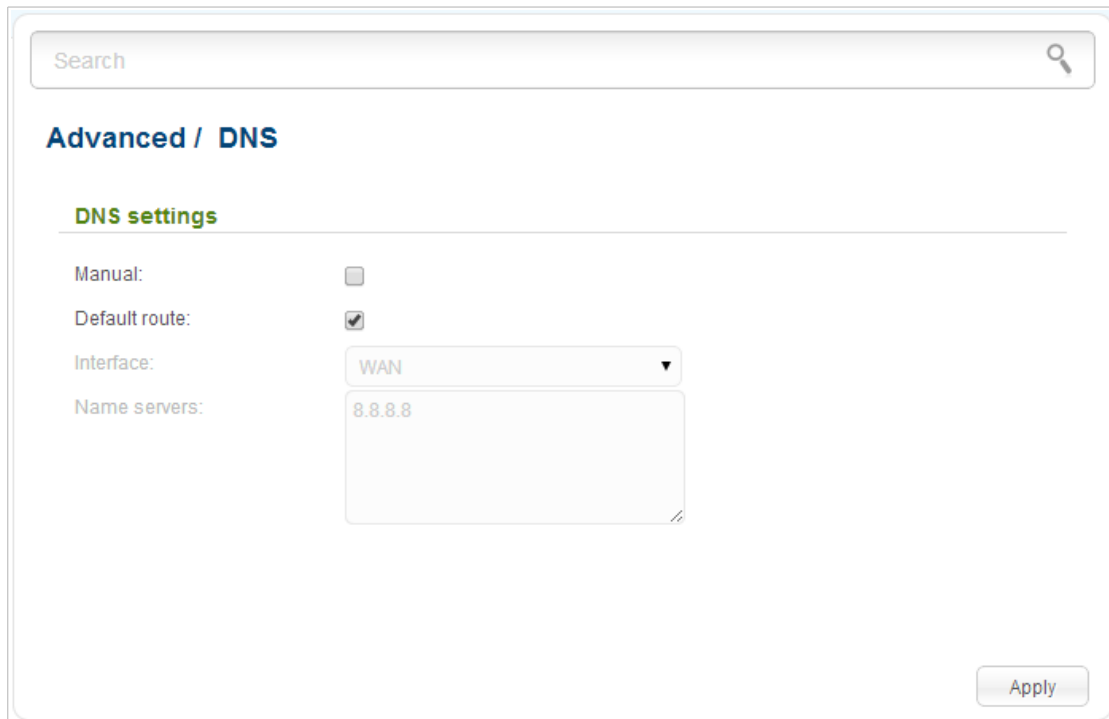


Figure 144. The **Advanced / DNS** page.

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, deselect the **Manual** checkbox, select a WAN connection which will be used to obtain addresses of DNS servers automatically from the **Interface** drop-down list or select the **Default route** checkbox, so that the access point could use the connection set as the default gateway (on the **Net / WAN** page) to obtain DNS server addresses, and click the **Apply** button.

If you want to specify the DNS server manually, select the **Manual** checkbox and enter a DNS server address in the **Name servers** list. To specify several addresses, press the **Enter** key and enter a needed address in the next line. Then click the **Apply** button.

To remove a DNS server from the system, remove the relevant line from the **Name servers** field and click the **Apply** button.

Routing

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

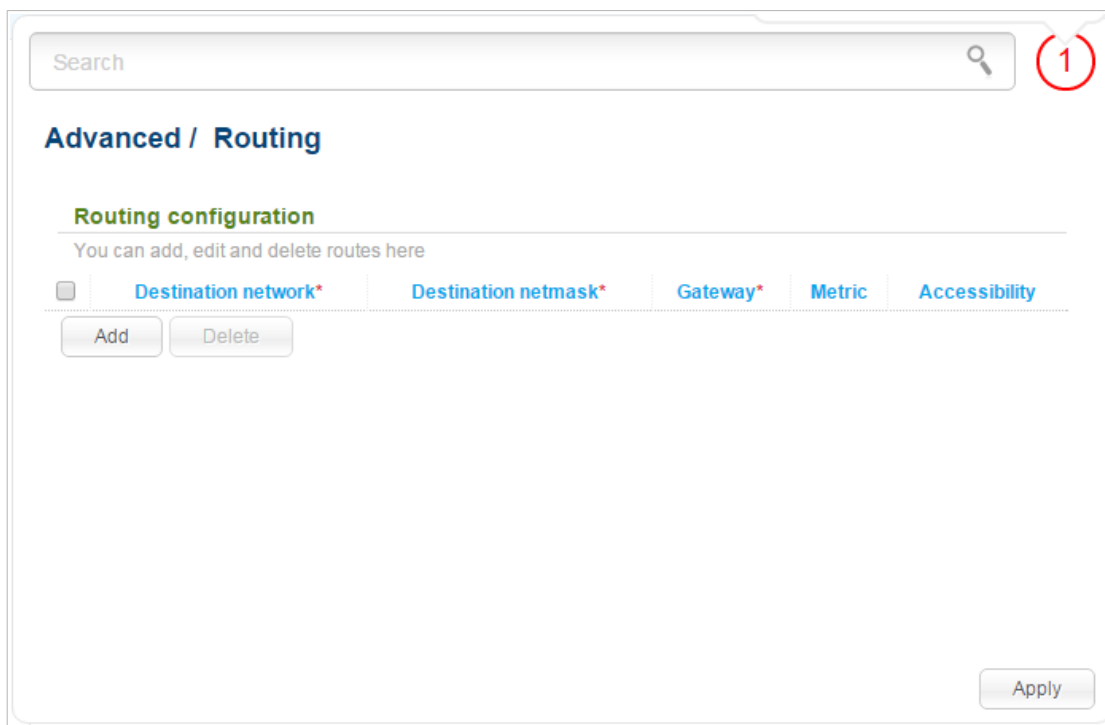


Figure 145. The **Advanced / Routing** page.

To create a new route, click the **Add** button. In the line displayed, you can specify the following parameters:

Parameter	Description
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. The field is available when the <Auto> value is selected from the Via Interface drop-down list of this line.
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 **Apply** button.

To edit an existing route, select a needed field in the relevant line of the table, change its value, and click the **Apply** 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. Then click the **Apply** button.

Remote Access to Device

On the **Advanced / Remote access to device** page, you can configure access to the web-based interface of the access point. By default, the access from external networks to the device is closed. If you need to allow access to DAP-1360U from the external network, create relevant rules.

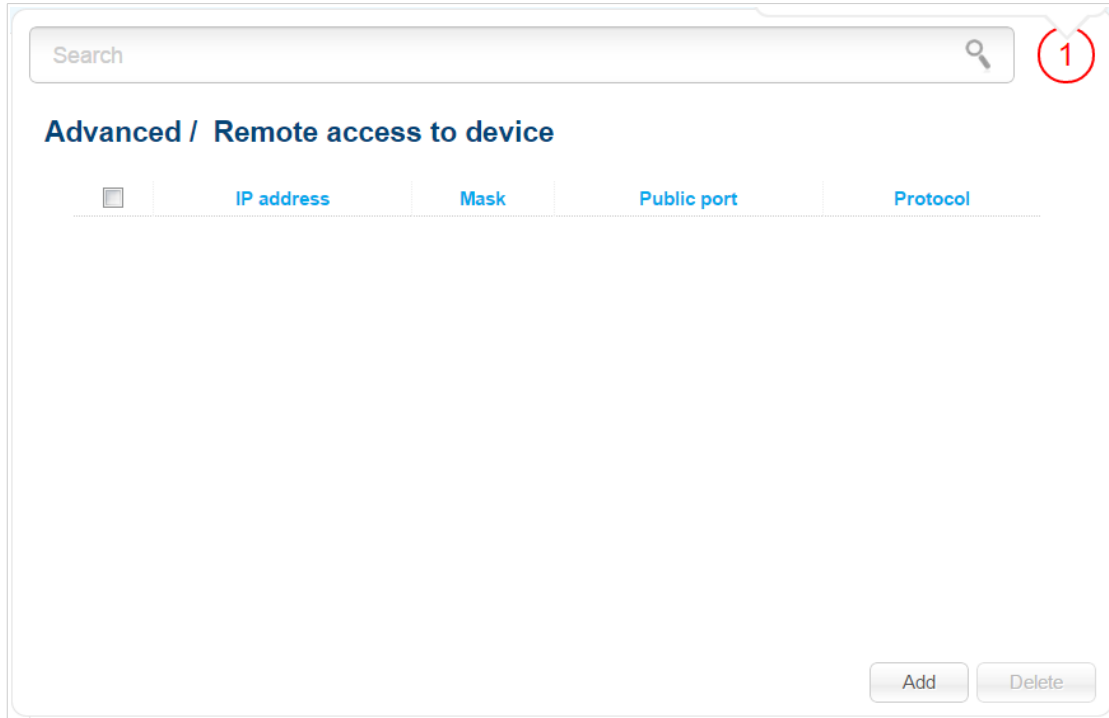


Figure 146. The **Advanced / Remote access to device** page.

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

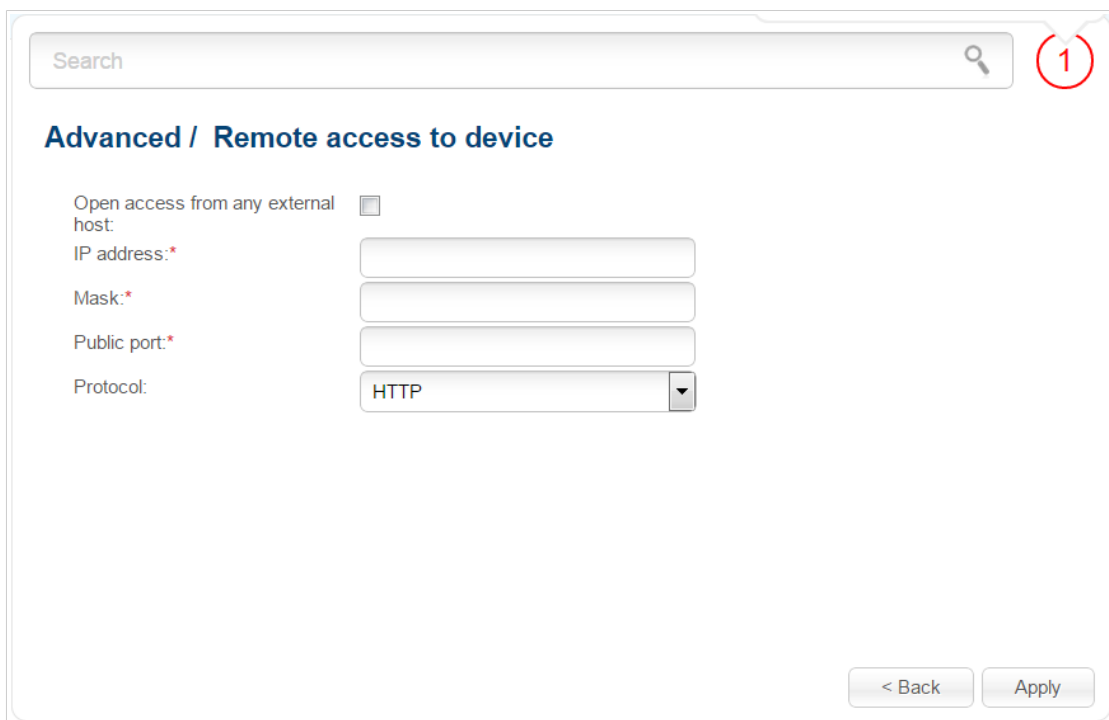


Figure 147. The page for adding a rule for remote management.

You can specify the following parameters:

Parameter	Description
Open access from any external host	Select the checkbox to allow access to the device for any host. When the checkbox is selected, the IP address and Mask fields are not available for editing.
IP address	A host or a subnet to which the rule is applied.
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 **Apply** button.

To edit a rule for remote access, click the link to the relevant rule. On the opened page, change the needed parameters and click the **Apply** 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. Also you can remove a rule on the editing page.

Miscellaneous

On the **Advanced / Miscellaneous** page, you can enable IGMP, RTSP, the SIP ALG function and the PPPoE pass through, PPTP pass through, and L2TP pass through functions.

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

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

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

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

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

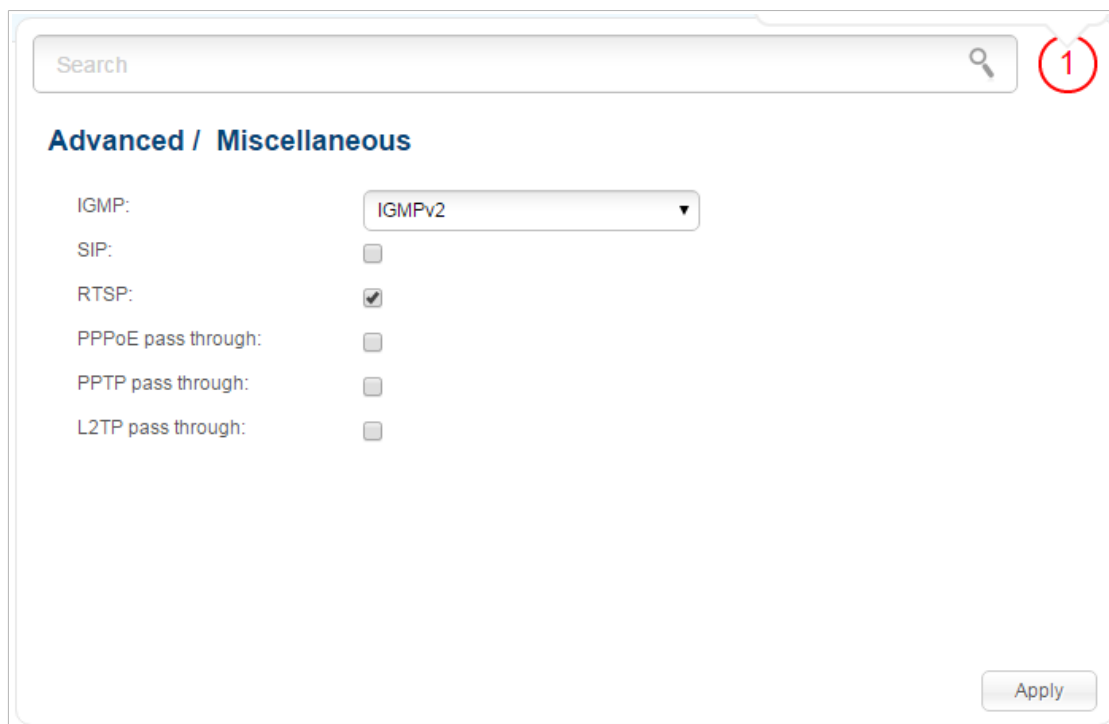


Figure 148. The **Advanced / Miscellaneous** page.

The following elements are available on the page:

Parameter	Description
IGMP	Select a version of IGMP from the drop-down list to enable IGMP. Such a setting allows using the IGMP Proxy function for all WAN connections for which the Enable IGMP Multicast checkbox is selected. To disable IGMP, select the Off value from the drop-down list.
SIP	Select the checkbox to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled device. ¹
RTSP	Select the checkbox to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Select the checkbox to enable the PPPoE pass through function.
PPTP pass through	Select the checkbox to enable the PPTP pass through function.
L2TP pass through	Select the checkbox to enable the L2TP pass through function.

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

¹ On the **Net / WAN** page, create a WAN connection, on the **Advanced / Miscellaneous** page, select the **SIP** checkbox, connect the phone 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

In this menu you can configure the firewall of the access point switched to the router mode:

- add rules for IP filtering
- create virtual servers
- define a DMZ
- configure the MAC filter.

IP Filters

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

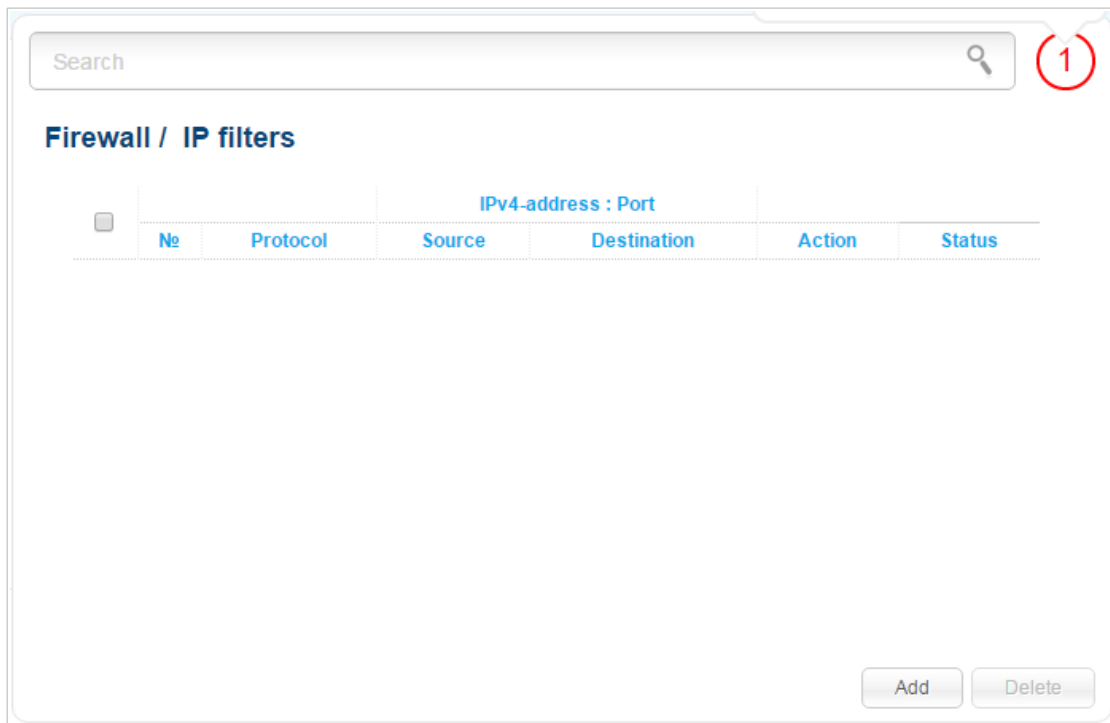


Figure 149. The **Firewall / IP filters** page.

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

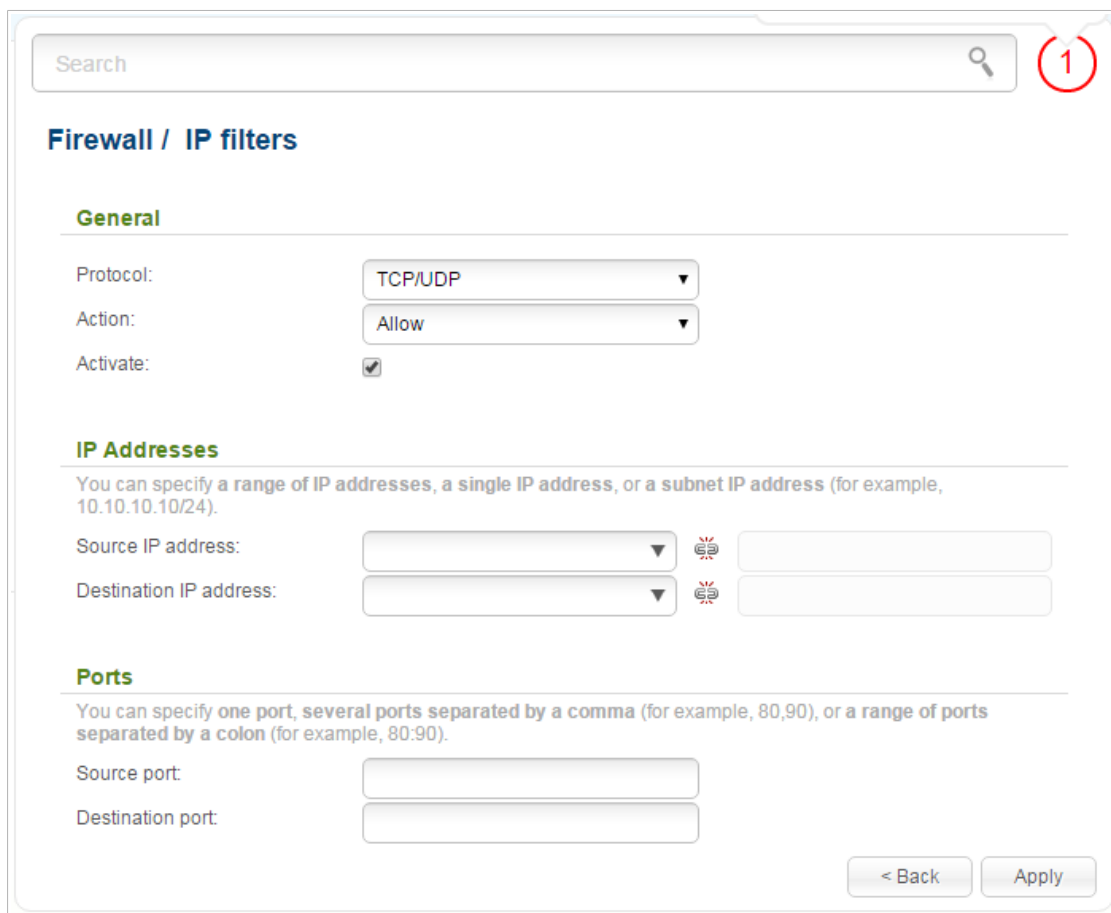




Figure 150. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
General	
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.
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.
Activate	If the checkbox is selected, the rule is enabled. Deselect the checkbox to disable the rule.
IP Addresses	

Parameter	Description
Source IP address	<p>The source host/subnet IP address.</p> <p>To choose a device connected to the access point's LAN at the moment, select the relevant IP address from the drop-down list (the field will be filled in automatically).</p> <p>If you want to specify a range of IP addresses, click the icon  (Range) and enter the starting and ending addresses in the left and right fields correspondingly.</p>
Destination IP address	<p>The destination host/subnet IP address.</p> <p>To choose a device connected to the access point's LAN at the moment, select the relevant IP address from the drop-down list (the field will be filled in automatically).</p> <p>If you want to specify a range of IP addresses, click the icon  (Range) and enter the starting and ending addresses in the left and right fields correspondingly.</p>
Ports	
Source port	<p>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.</p>
Destination port	<p>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.</p>

Click the **Apply** button.

To edit a rule for IP filtering, click the link to the relevant rule. 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 in 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.

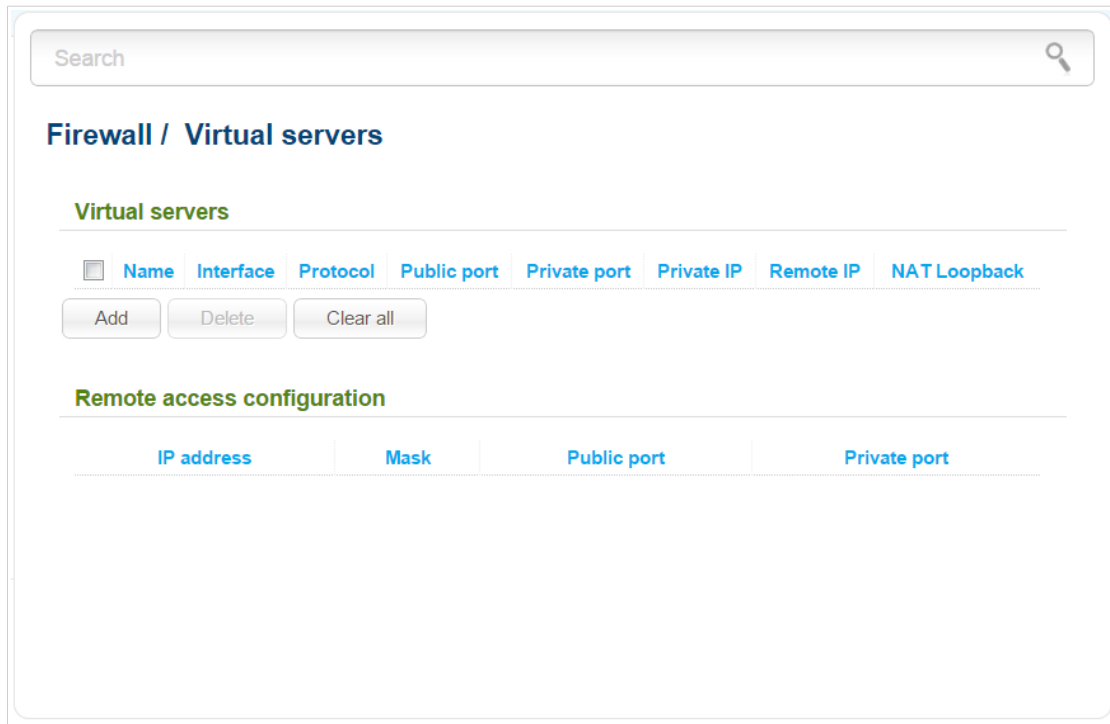


Figure 151. The **Firewall / Virtual servers** page.

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

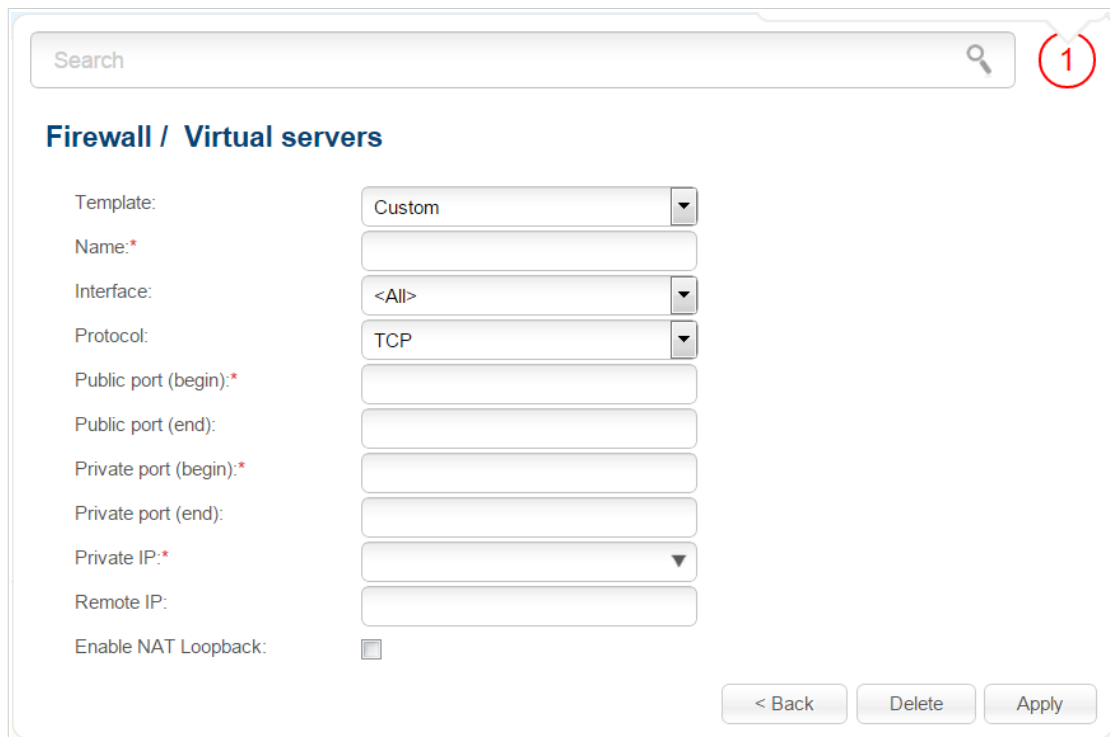


Figure 152. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
Template	Select a virtual server template from the drop-down list, or select Custom to specify all parameters of the new virtual server manually.
Name	A name for the virtual server for easier identification. You can specify any name.
Interface	A WAN connection to which this virtual server will be assigned.
Protocol	A protocol that will be used by the new virtual server. Select a value from the drop-down list.
Public port (begin)/ Public port (end)	A port of the access point from which traffic is directed to the IP address specified in the Private IP field. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the Public port (begin) field and leave the Public port (end) field blank.
Private port (begin)/ 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 (begin) field and leave the Private port (end) field blank.
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).
Remote IP	The IP address of the server from the external network.
Enable NAT Loopback	If the checkbox is selected, users of the access point's LAN can access the server, which IP address is specified in the Private IP field, using the access point's external IP address as the server's IP address. If a DDNS service is configured on the Advanced / DDNS page, the users can access the server via the device's domain name.

Click the **Apply** button.

To edit the parameters of an existing server, select the relevant server 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 in the table and click the **Delete** button. Also you can remove a server on the editing page.

To remove all servers from this page, click the **Clear all** button.

In the **Remote access configuration** section, rules created on the **Advanced / Remote access to device** page are displayed. If after creating virtual servers you need to edit rules for remote access, you can quickly get to the **Advanced / Remote access to device** page by clicking the link to the relevant rule.

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.

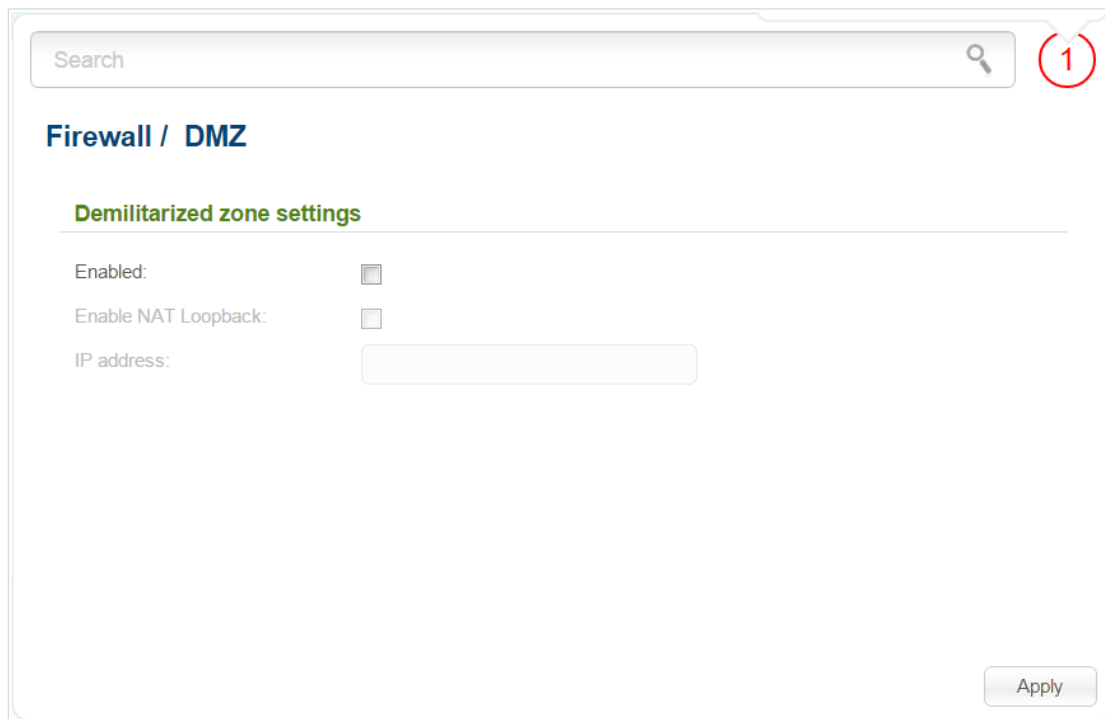


Figure 153. The **Firewall / DMZ** page.

To enable the DMZ, select the **Enabled** checkbox.

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).

If you want users of the access point's LAN to access the host using the external IP address of DAP-1360U, select the **Enable NAT Loopback** checkbox. If a DDNS service is configured on the **Advanced / DDNS** page, also the users can access the host via the device's domain 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, deselect the **Enabled** checkbox 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.

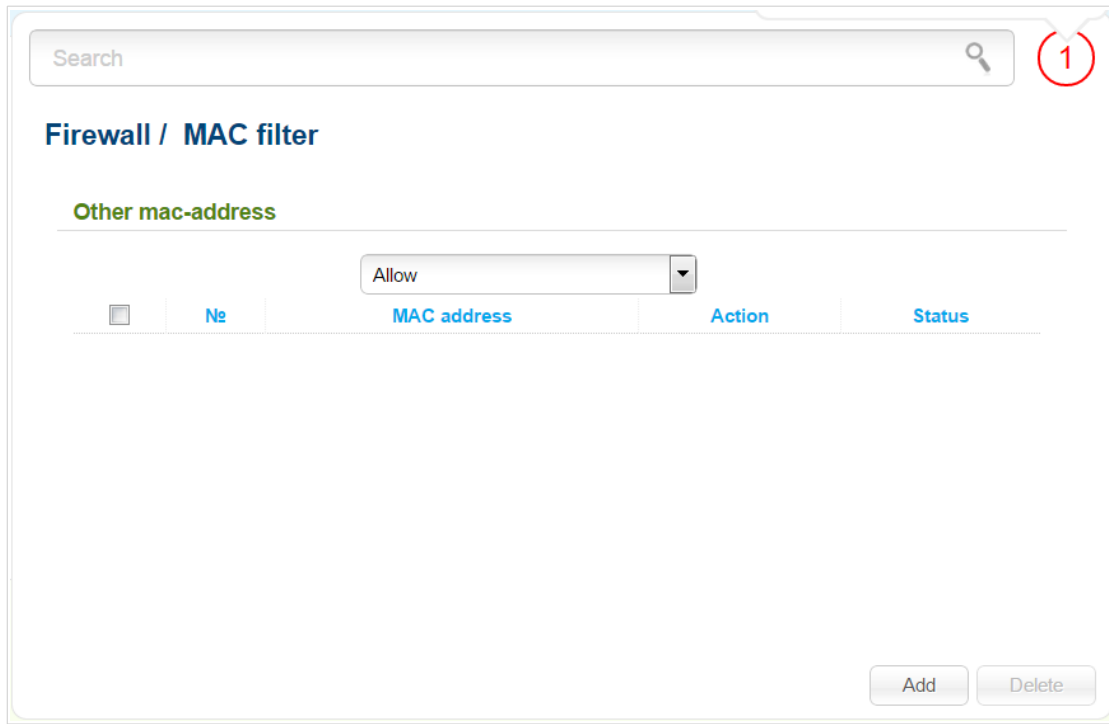


Figure 154. The **Firewall / MAC filter** page.

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

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

If you need to specify a filtering mode for each device separately, create relevant rules. To do this, click the **Add** button.

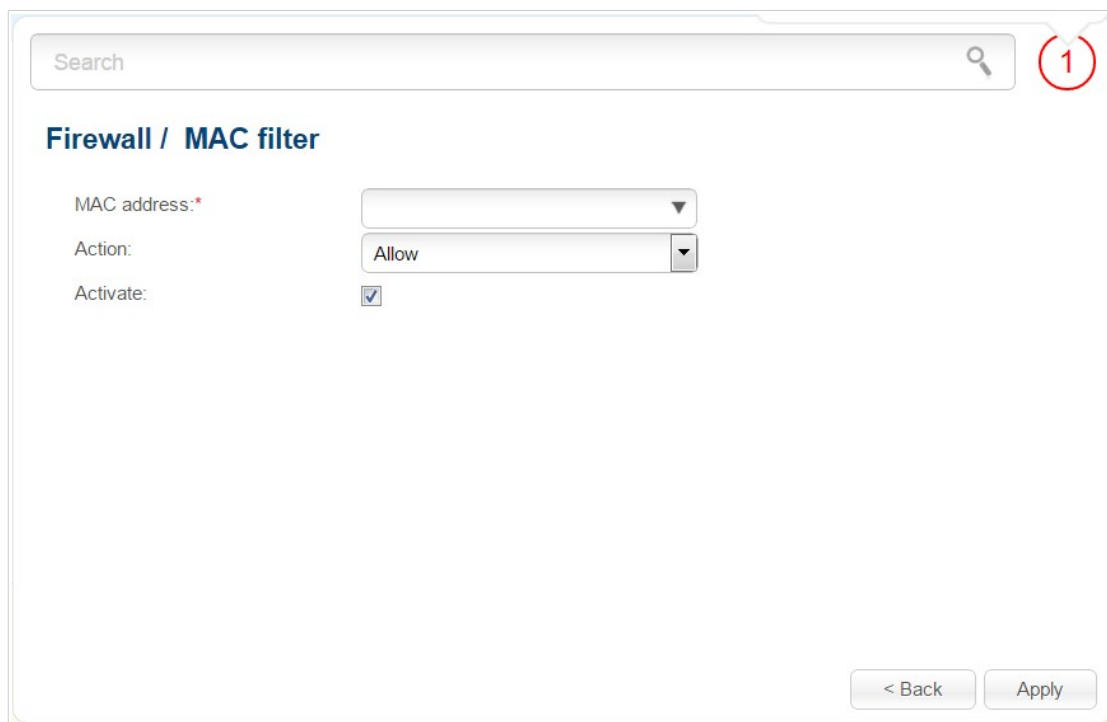


Figure 155. The page for adding a rule for the MAC filter.

You can specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the access point's LAN. You can enter the MAC address of a device connected to the access point's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Action	Select an action for the rule. Deny: Blocks access to the access point's network for the device with the specified MAC address. Allow: Allows access to the access point's network and to the Internet for the device with the specified MAC address when the rules on the Firewall / IP filters page block access for this device.
Activate	If the checkbox is selected, the rule is enabled. Deselect the checkbox to disable the rule.

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

To edit a rule for filtering, click the link to the relevant rule. 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 in the table and click the **Delete** button. Also you can remove a rule on the editing page.

Control

This menu is designed to create restrictions on access to certain web sites.

URL Filter

On the pages of the **Control / URL filter** section, you can specify restrictions on access to certain web sites.

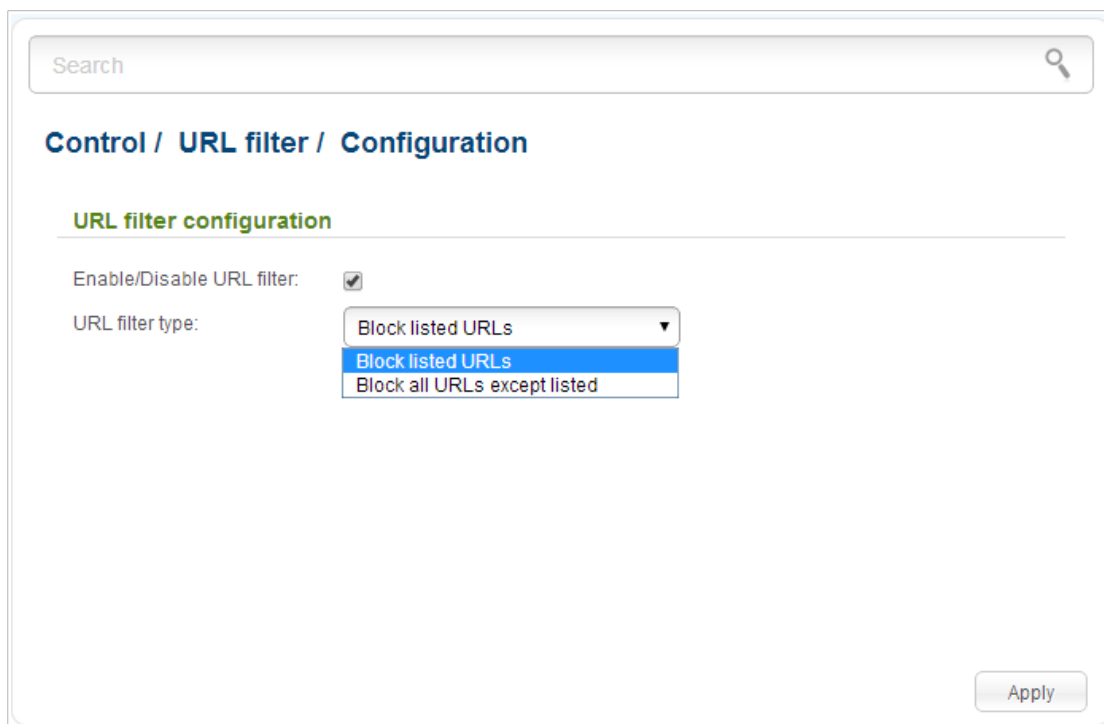


Figure 156. The **Control / URL filter / Configuration** page.

To enable the URL filter, select the **Enable/Disable URL filter** checkbox on the **Control / URL filter / Configuration** page, then select a needed mode from the **URL filter type** drop-down list:

- **Block listed URLs:** when this value is selected, the access point blocks access to all addresses specified on the **Control / URL filter / Configuration** page;
- **Block all URLs except listed:** when this value is selected, the access point allows access to addresses specified on the **Control / URL filter / Configuration** page and blocks access to all other web sites.

Click the **Apply** button.

To specify URL addresses to which the selected filtering will be applied, go to the **Control / URL filter / URL addresses** page.

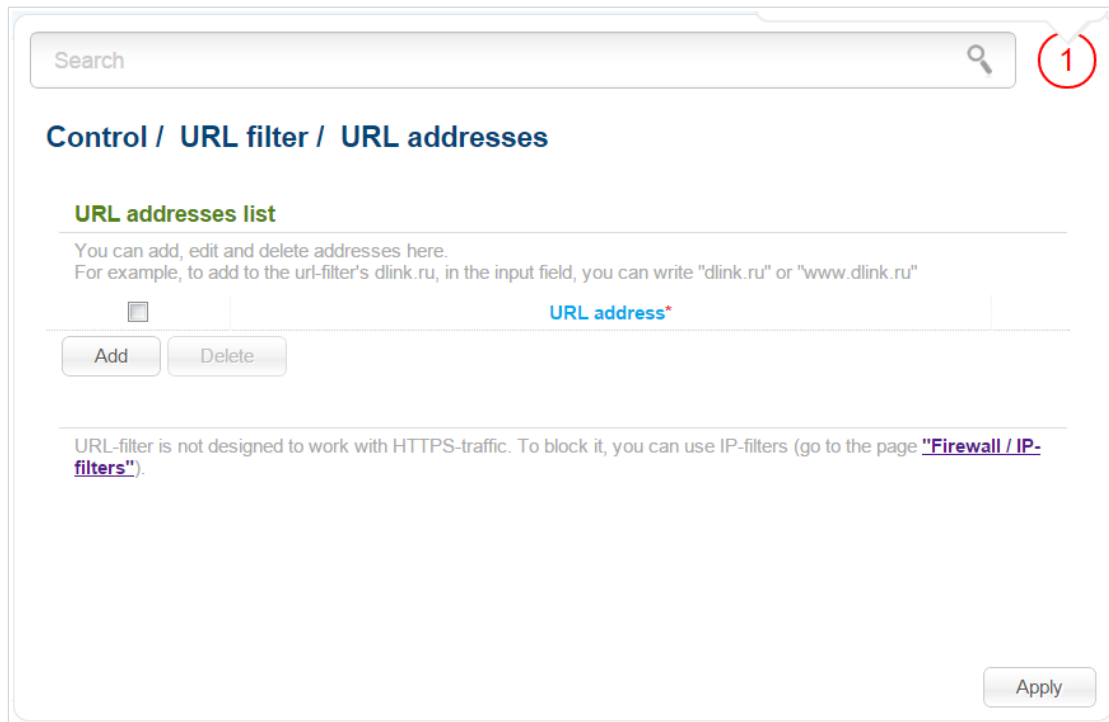


Figure 157. The **Control / URL filter / URL addresses** page.

Click the **Add** button and enter an address in the field displayed. Then click the **Apply** button.

To remove an address from the list of URL addresses, select the checkbox located to the left of the relevant URL address and click the **Delete** button. Then click the **Apply** button.

System

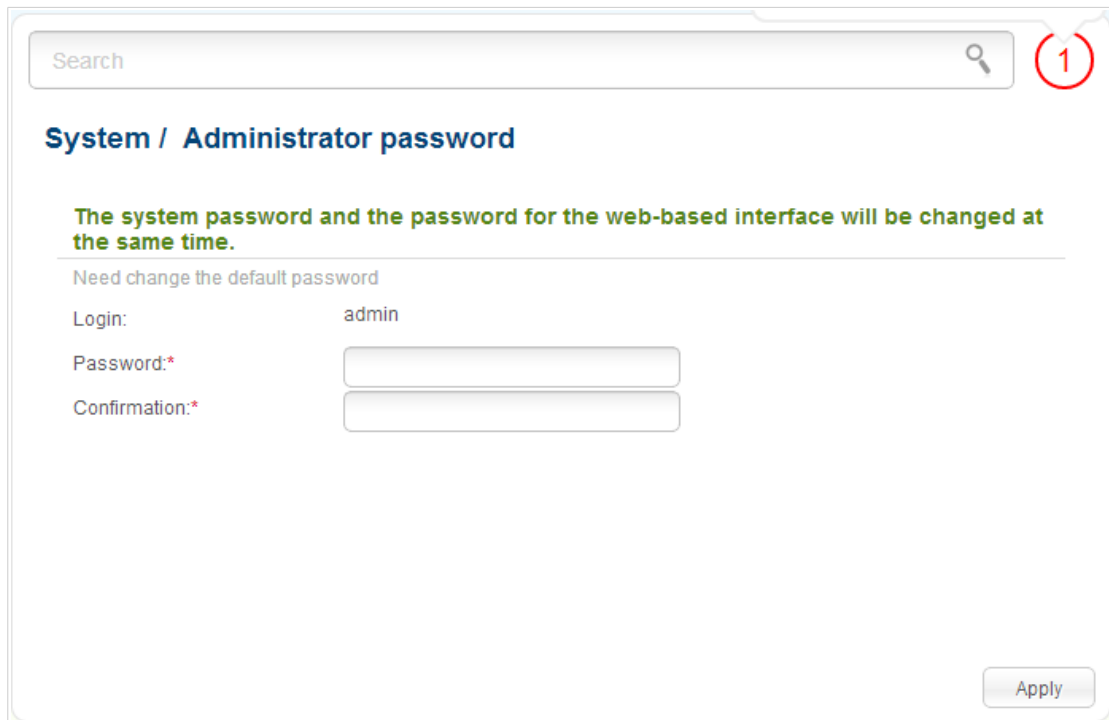
In this menu you can do the following:

- change the password used to access the access point's settings
- save the current settings to the non-volatile memory
- reboot the access point
- create a backup of the access point's configuration
- restore the access point's configuration from a previously saved file
- restore the factory default settings
- view the system log
- update the firmware of the access point
- configure automatic notification on new firmware version
- configure automatic synchronization of the system time or manually configure the date and time for the access point
- 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
- switch the device to the other mode.

Administrator Password

On the **System / Administrator password** 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.

! For security reasons, it is strongly recommended to change the administrator password upon initial configuration of the access point.



Search

System / Administrator password

The system password and the password for the web-based interface will be changed at the same time.

Need change the default password

Login: admin

Password:*

Confirmation:*

Apply

Figure 158. The page for modifying the administrator password.

Enter the new password in the **Password** and **Confirmation** fields and click the **Apply** button.

Configuration

On the **System / Configuration** page, you can reboot the device, save the changed settings to the non-volatile memory, restore the factory defaults, backup the current configuration, or restore the access point's configuration from a previously created file.

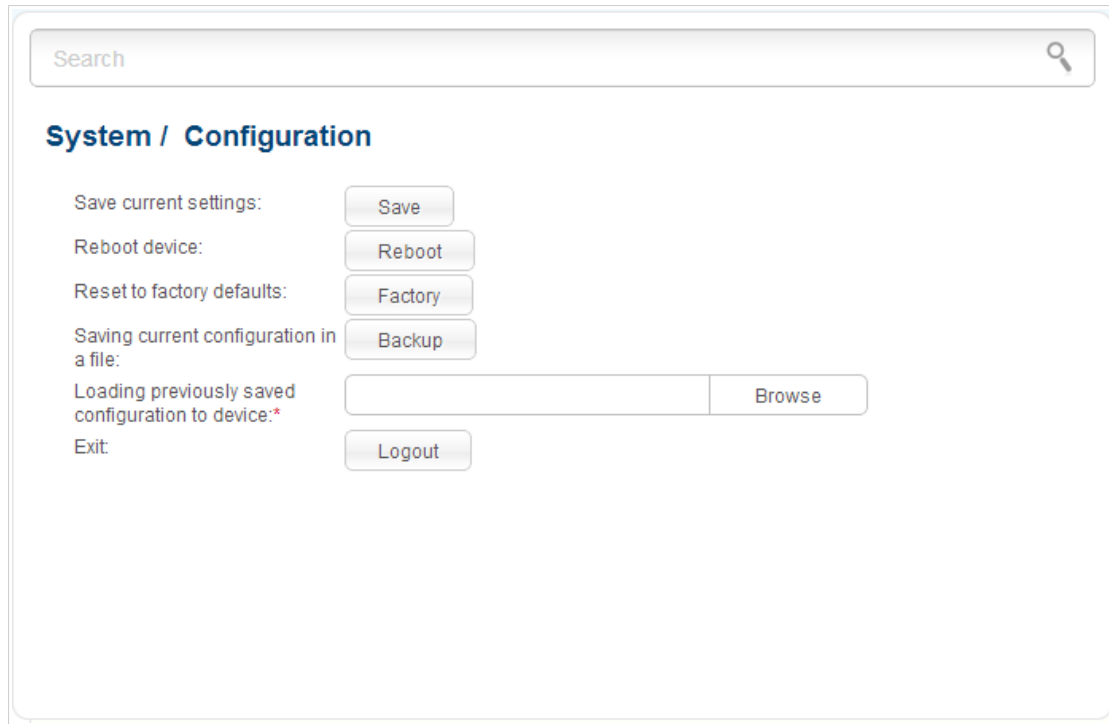


Figure 159. The **System / Configuration** page.

The following buttons are available on the page:

Control	Description
Save	Click the button to save settings to the non-volatile memory. Please, save settings every time you change the device's parameters. Otherwise the changes will be lost upon hardware reboot of the access point.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button located on the bottom panel of the access point (see the <i>Back and Bottom Panels</i> section, page 11).
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.
Browse	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.
Logout	Click the button to exit the web-based interface.

Actions of the **Save**, **Reboot**, **Factory**, **Backup**, and **Logout** buttons also can be performed via the top-page menu displayed when the mouse pointer is over the **System** caption.

System Log

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

Figure 160. The **System / System log / Configuration** page.

To enable logging of the system events, select the **Logging** checkbox. Then specify the needed parameters.

Control	Description
Logging 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 device's memory (and displayed on the System / System log / Log page). When this value is selected, the Server and Port fields are not displayed. • Remote: the system log is sent to the remote host specified in the Server field. • Local and remote: the system log is stored in the device's memory (and displayed on the System / System log / Log page) and sent to the remote host specified in the Server field.
Logging level	Select a type of messages and alerts/notifications to be logged.
Server	The IP or URL address of the host from the local or global network, to which the system log will be sent.

Control	Description
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, deselect the **Logging** checkbox and click the **Apply** button.

On the **System / System log / Log** page, the events specified in the **Logging level** list are displayed.

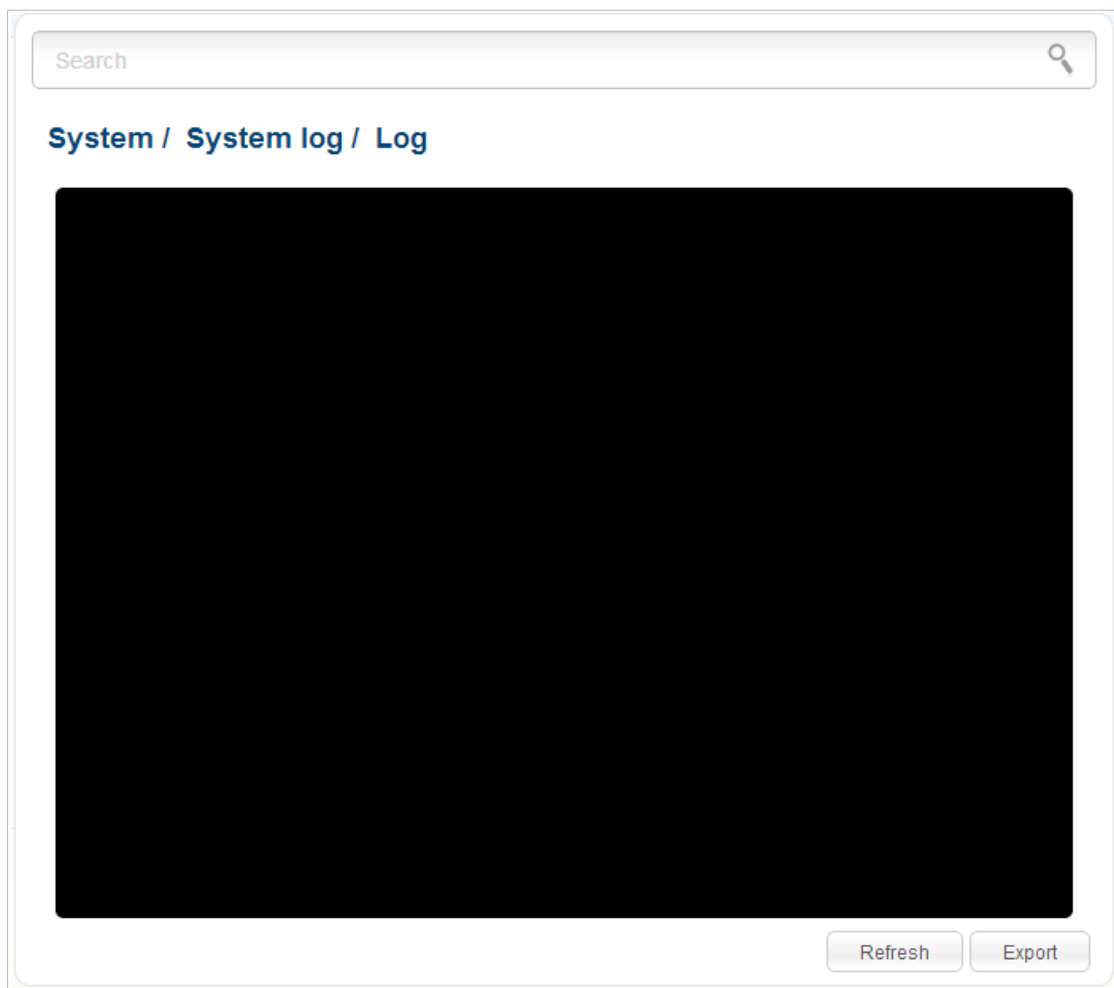


Figure 161. The **System / System log / Log** page.

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

To save the system log to your PC, click the **Export** button and follow the dialog box appeared.

Firmware Upgrade

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



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

The screenshot shows the 'System / Firmware upgrade' page. At the top is a search bar. Below it is the page title 'System / Firmware upgrade'. The page is divided into two sections: 'Local update' and 'Remote update'. In the 'Local update' section, there is a label 'Select update file:*', an empty text input field, a 'Browse' button, and an 'Update' button. In the 'Remote update' section, there is a label 'Check for updates automatically:' with a checked checkbox, a label 'Remote server URL:', a text input field containing 'fwupdate.dlink.ru', a 'Check for updates' button, and an 'Apply settings' button.

Figure 162. The **System / Firmware upgrade** page.

The current version of the access point's firmware is displayed next the D-Link logo in the top left corner of the page.

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, deselect the **Check for updates automatically** checkbox and click the **Apply settings** button.

To enable the automatic check for firmware updates, in the **Remote update** section, select the **Check for updates automatically** checkbox 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 upgrade 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 upgrade 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 **Browse** button on the **System / Firmware upgrade** page to locate the new firmware file.
3. Click the **Update** button to upgrade the firmware of the access point.
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.

After the upgrade is completed, the new version of the firmware will be displayed in the top left corner of the page.

If after updating the firmware the access point doesn't work correctly, please restore the factory default settings. To do this, place the mouse pointer over the **System** caption in the top left corner

of the page and click the  (**Reset to factory**) icon. Wait until the access point is rebooted.

Remote Update

! Attention! Do not turn off the access point before the firmware upgrade 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 upgrade** page, in the **Remote update** section, click the **Check for updates** button to check if a newer firmware version exists.
2. Click the **OK** button in the window displayed to upgrade the firmware of the access point. Also you can upgrade the firmware of the access point by clicking the **Remote update** 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.

After the upgrade is completed, the new version of the firmware will be displayed in the top left corner of the page.

If after updating the firmware the access point doesn't work correctly, please restore the factory default settings. To do this, place the mouse pointer over the **System** caption in the top left corner

of the page and click the  (**Reset to factory**) icon. Wait until the access point is rebooted.

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.

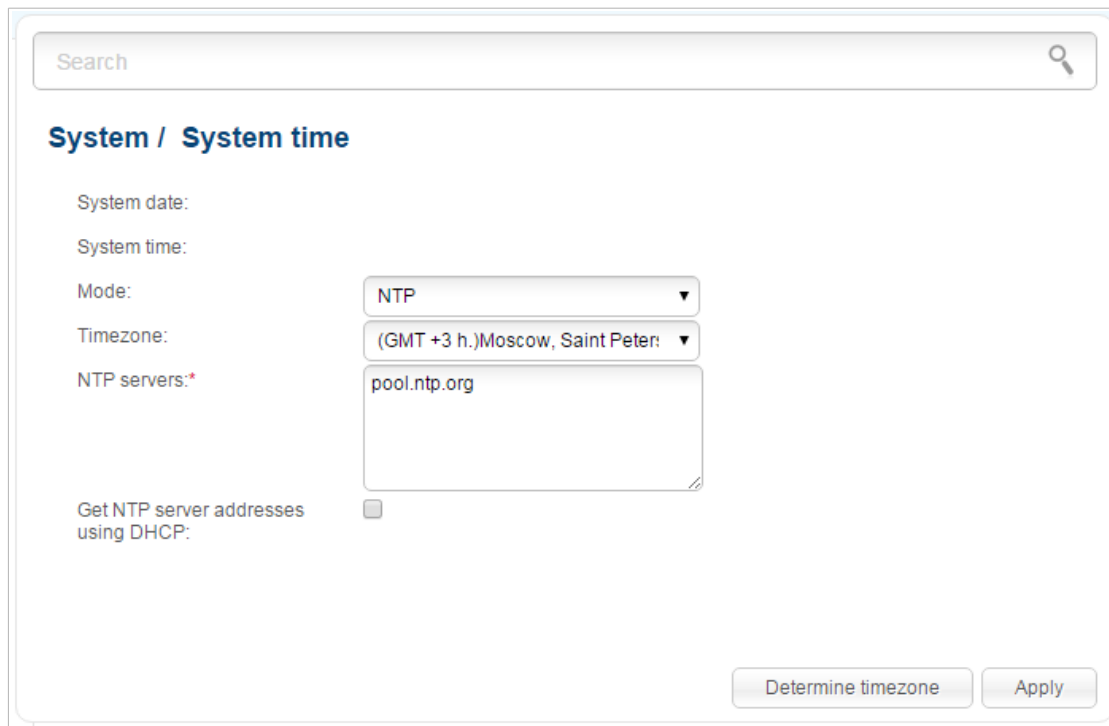


Figure 163. The **System / System time** page.

To set the system time manually, select the **Manual** value from the **Mode** drop-down list and set the time and date in the fields displayed. Then click the **Apply** button.

To enable automatic synchronization with a time server, follow the next steps:

1. Select the **NTP** value from the **Mode** drop-down list.
2. Select your time zone from the drop-down list. To set the time zone in accordance with the settings of your operating system, click the **Determine timezone** button in the bottom right corner of the page.
3. Specify the needed NTP server in the **NTP servers** field or leave the server specified by default.
4. Click the **Apply** button.

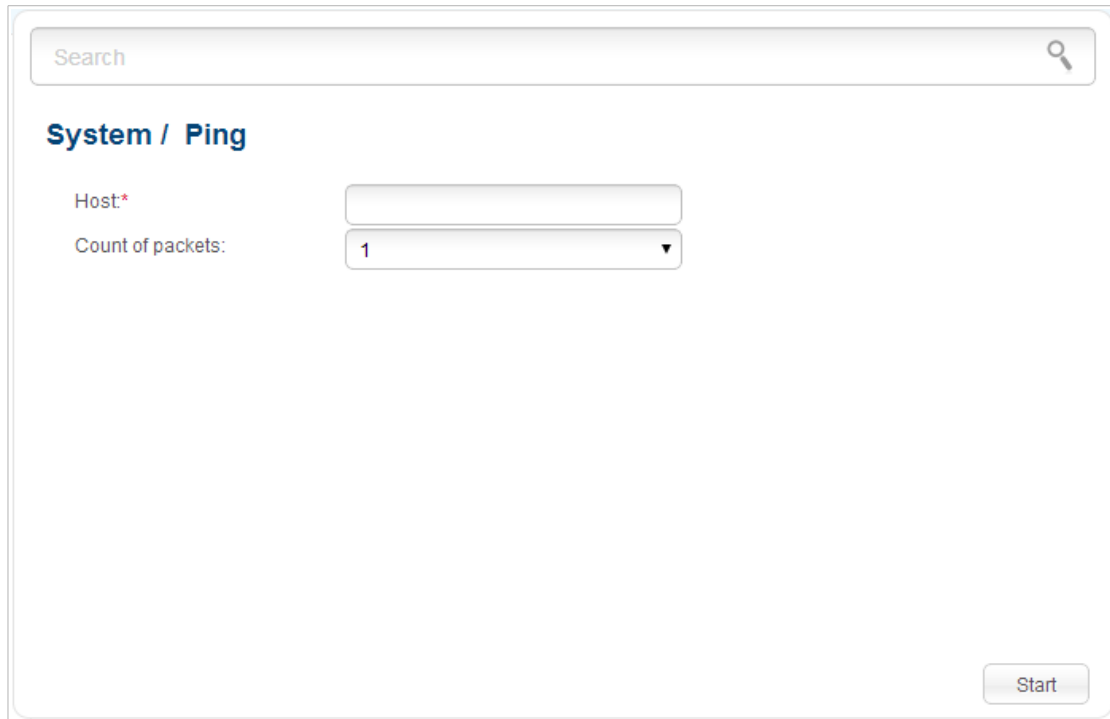
In some cases NTP servers addresses are provided by your ISP. In this case, you need to select the **Get NTP server addresses using DHCP** checkbox. Contact your ISP to clarify if this checkbox needs to be enabled. If the **Get NTP server addresses using DHCP** checkbox is selected, the **NTP servers** field is not available.

! 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).

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.



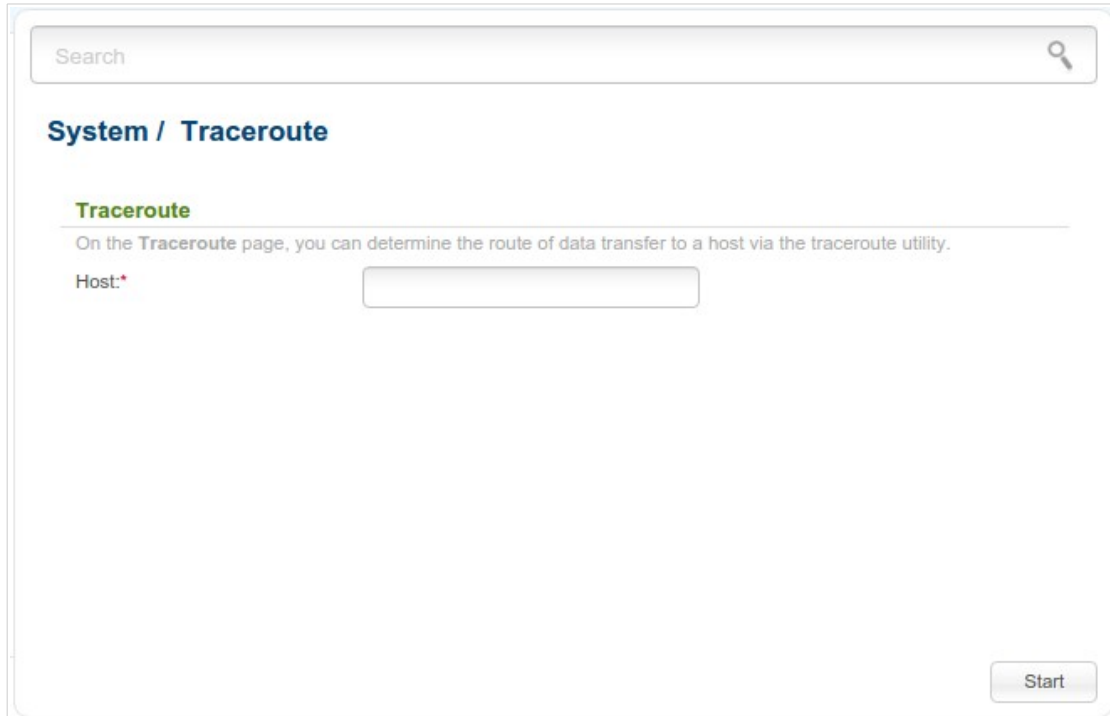
The screenshot shows a web interface for the 'System / Ping' utility. At the top, there is a search bar with the placeholder text 'Search' and a magnifying glass icon. Below the search bar, the page title 'System / Ping' is displayed in a bold, blue font. Underneath the title, there are two input fields: 'Host*' is a text input field, and 'Count of packets:' is a dropdown menu currently showing the value '1'. At the bottom right of the form area, there is a 'Start' button.

Figure 164. The **System / Ping** page.

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

Traceroute

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



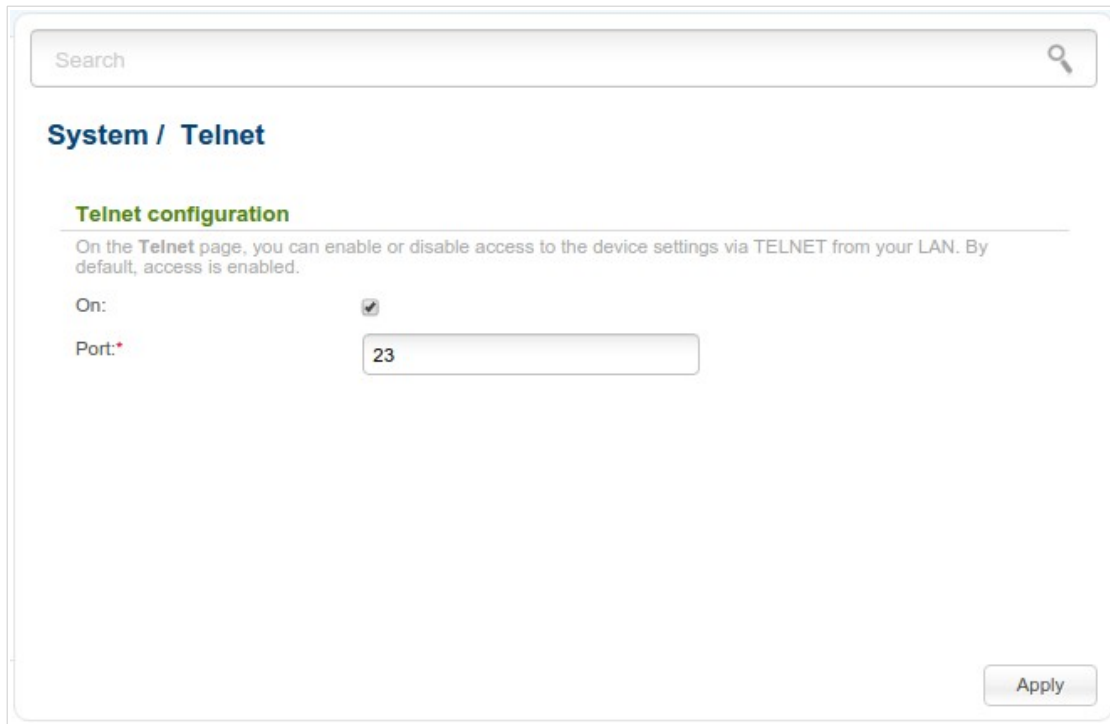
The screenshot shows a web interface for the 'System / Traceroute' page. At the top, there is a search bar with the placeholder text 'Search' and a magnifying glass icon. Below the search bar, the page title 'System / Traceroute' is displayed in a blue font. Underneath, the word 'Traceroute' is written in green. A horizontal line separates the title from the main content area. Below the line, there is a descriptive sentence: 'On the Traceroute page, you can determine the route of data transfer to a host via the traceroute utility.' Below this sentence, there is a label 'Host:' followed by a red asterisk, and an empty text input field. At the bottom right of the page, there is a 'Start' button.

Figure 165. The **System / Traceroute** page.

To define the route, enter the name or IP address of a host in the **Host** field and click the **Start** button. After a while, the results will be displayed on the page.

Telnet

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



Search

System / Telnet

Telnet configuration

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

On:

Port:*

Apply

Figure 166. The **System / Telnet** page.

To disable access via TELNET, deselect the **On** checkbox and click the **Apply** button.

To enable access via TELNET again, select the **On** checkbox. 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.

Device mode

On the **System / Device mode** page, you can change the operating mode of the device.

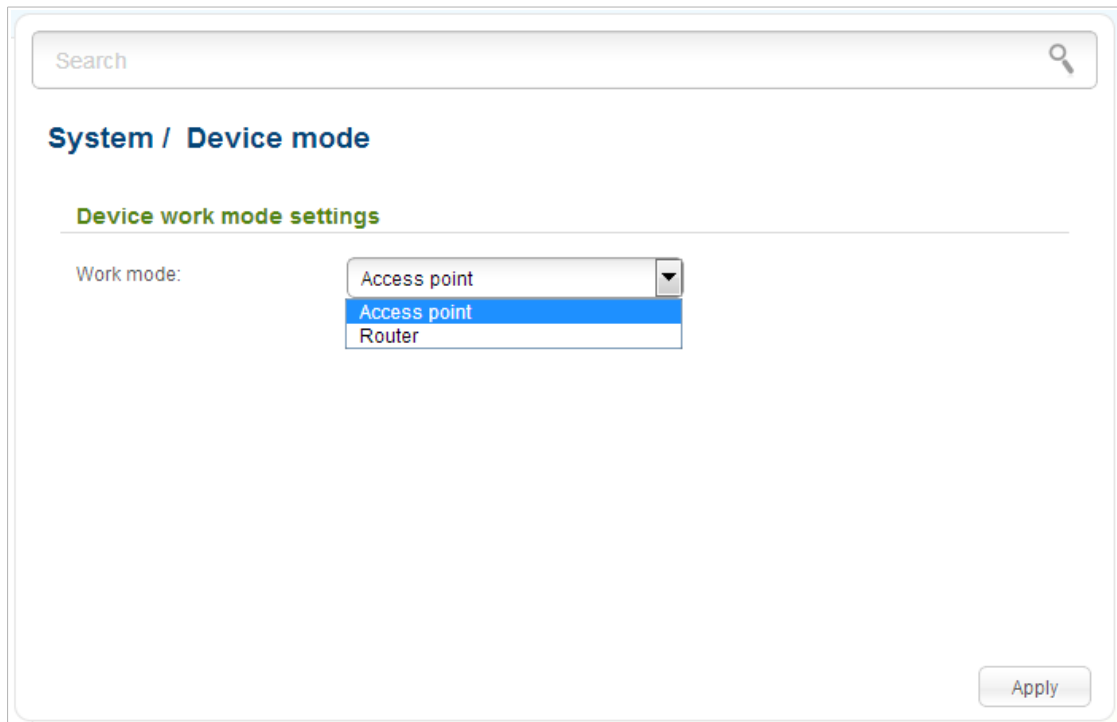


Figure 167. The page for changing the operating mode of the device.

To switch the device to the other mode, select the **Access point** value from the **Work mode** drop-down list and click the **Apply** button. In the opened dialog box, click the **OK** button to save new settings and immediately reboot the access point.

CHAPTER 6. OPERATION GUIDELINES

Safety Instructions

Place your access point on a flat horizontal surface or mount the access point on the wall (the mounting holes are located on the bottom panel of the device). Make sure that the access point is provided with sufficient ventilation.

To prevent overheating, do not obstruct the ventilation openings of the access point.

Plug the access point into a surge protector to reduce the risk of damage from power surges and lightning strikes.

Operate the access point only from an electrical outlet with the correct power source as indicated on the adapter.

Do not open the cover of the access point. Otherwise any warranty will be invalidated.

Unplug the equipment before dusting and cleaning. Use a damp cloth to clean the equipment. Do not use liquid/aerosol cleaners or magnetic/static cleaning devices.

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 7. 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