



DAP-1155

Wireless N 150 Access Point & Router

Contents

Chapter 1. Introduction.....	6
Contents and Audience.....	6
Conventions.....	6
Document Structure.....	6
Chapter 2. Overview.....	7
General Information.....	7
Specifications.....	8
Product Appearance.....	11
Front Panel.....	11
Back Panel.....	12
Delivery Package.....	13
Chapter 3. Installation and Connection.....	14
Before You Begin.....	14
Connecting to PC.....	15
PC with Ethernet Adapter.....	15
Configuring IP Address in OS Windows XP.....	15
Configuring IP Address in OS Windows 7.....	18
PC with Wi-Fi Adapter.....	23
Configuring Wi-Fi Adapter in OS Windows XP.....	24
Configuring Wi-Fi Adapter in OS Windows 7.....	26
Connecting to Web-based Interface.....	29
Web-based Interface Structure.....	31
Access Point Mode.....	33
Router Mode.....	35
Saving and Restoring Settings.....	37
Device Operation Modes.....	39
Access Point Mode.....	39
Router Mode.....	39
Chapter 4. Configuring Device (Access Point Mode).....	40
Wireless Network Settings Wizard.....	40
Status.....	46
Network Statistics.....	46
DHCP.....	47
LAN Clients.....	48
Net.....	49
LAN.....	49

Wi-Fi	52
Common settings.....	52
Basic Settings.....	53
Security Settings.....	55
MAC Filter.....	59
Station List.....	61
WPS.....	62
<i>Using WPS Function via Web-based Interface</i>	64
<i>Using WPS Function without Web-based Interface</i>	64
WDS.....	66
Additional Settings.....	68
WMM.....	70
Client.....	72
Firewall	75
MAC Filter.....	75
System	77
Administrator Password.....	78
Configuration.....	79
System Log.....	81
Firmware Upgrade.....	83
Ping.....	85
Telnet.....	86
Device mode.....	87
Chapter 5. Configuring Device (Router Mode)	88
Click'n'Connect	88
Creating WAN Connection.....	90
<i>PPPoE Connection</i>	90
<i>Static IP Connection</i>	95
<i>Dynamic IP Connection</i>	99
<i>PPTP + Static IP or L2TP + Static IP Connection</i>	103
<i>PPTP + Dynamic IP or L2TP + Dynamic IP Connection</i>	111
Checking Internet Availability.....	118
Configuring Wireless Connection.....	119
Wireless Network Settings Wizard	120
Virtual Server Settings Wizard	126
Status	127
Network Statistics.....	127
DHCP.....	128
Routing Table.....	129
LAN Clients.....	130

Net	131
WAN.....	131
<i>Creating PPPoE WAN Connection</i>	132
<i>Creating Static IP WAN Connection</i>	136
<i>Creating Dynamic IP WAN Connection</i>	139
<i>Creating PPTP + Static IP or L2TP + Static IP WAN Connection</i>	142
<i>Creating PPTP + Dynamic IP or L2TP + Dynamic IP WAN Connection</i>	147
LAN.....	152
Wi-Fi	155
Common settings.....	155
Basic Settings.....	156
Security Settings.....	158
MAC Filter.....	162
Station List.....	164
WPS.....	165
<i>Using WPS Function via Web-based Interface</i>	167
<i>Using WPS Function without Web-based Interface</i>	167
WDS.....	169
Additional Settings.....	171
WMM.....	173
Client.....	175
Advanced	178
UPnP.....	179
DDNS.....	180
DNS.....	182
Routing.....	183
Remote Access.....	185
IGMP.....	187
Firewall	188
IP Filters.....	188
Virtual Servers.....	191
DMZ.....	194
MAC Filter.....	195
Control	197
URL Filter.....	197
System	200
Administrator Password.....	201
Configuration.....	202
System Log.....	204
Firmware Upgrade.....	206
NTP Client.....	208
Ping.....	209
Traceroute.....	210
Telnet.....	211
Device mode.....	212

Chapter 6. Operation Guidelines.....	213
Safety Instructions.....	213
Wireless Installation Considerations.....	213
Chapter 7. Abbreviations and Acronyms.....	214


CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the access point DAP-1155 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-1155 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-1155 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-1155, 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 150Mbps).

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-1155 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-1155 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 and manage the settings of the DAP-1155 device via the user-friendly web-based interface (the interface is available in several languages).

Specifications*

WAN Interface:

- 1 10/100BASE-TX Ethernet port for cable or DSL modem or private Ethernet line.

LAN Interface:

- 1 10/100BASE-TX Ethernet port.

WLAN Interface:

- IEEE 802.11n (up to 150Mbps)
- IEEE 802.11b/g.

Operation Modes:

- Access point mode
- Router mode.

Network Functions:

- WAN connection types:
 - PPPoE
 - Static IP
 - Dynamic IP
 - PPTP/L2TP + Static IP
 - PPTP/L2TP + Dynamic IP
- DHCP server and client
- DNS relay
- VPN pass-through (PPTP/L2TP)
- Dynamic DNS
- Static IP routing
- Remote management
- Network statistics for each interface
- IGMP Proxy
- RIP
- UPnP
- WAN ping respond.

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

Wireless Connection:

- WLAN splitting (up to 4 SSIDs)
- Supported security settings:
 - WEP
 - WPA/WPA2 Personal
- MAC filter
- Managing connected stations
- PIN and PBC methods of WPS
- WMM (Wi-Fi QoS)
- Advanced settings
- WDS
- “Client” function (access point mode):
 - Wireless network client
 - Wireless network repeater
- “Client” function (router mode):
 - WISP repeater.

Firewall Functions:

- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)
- IP filters
- URL filter
- MAC filter
- DMZ
- Prevention of ARP and DDoS attacks
- Virtual servers.

Configuration and Management:

- Multilingual web-based interface for configuration and management
- Access via TELNET
- Firmware update via web-based interface
- Saving/restoring configuration to/from file
- Support of remote logging
- Automatic synchronization of system time with NTP server (router mode)
- Ping function
- Traceroute utility (router mode).

LEDs:

- Power
- WLAN
- WPS
- LAN
- Internet.

Power:

- External power adapter DC 12V
- Reset to Factory Defaults button
- WPS button.

Operating Temperature:

- from 0 to 40 °C (from 32 to 104 °F).

Storage Temperature:

- from -20 to 65 °C (from -4 to 149 °F).

Operating Humidity:

- from 10% to 90% non-condensing.

Storage Humidity:






- from 5% to 95% non-condensing.

Product Appearance

Front Panel



Figure 1. Front 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).
 WPS	<i>Solid green</i>	The wireless device is connected to the access point's WLAN (lights for several minutes).
	<i>Blinking green</i>	Attempting to add a wireless device via the WPS function.
 LAN	<i>Solid green</i>	A device (computer) is connected to the relevant port, the connection is on.
	<i>Blinking green</i>	The port is active (upstream or downstream traffic).
 Internet	<i>Solid green</i>	The Internet connection is on.
	<i>Blinking green</i>	The WAN interface is active (upstream or downstream traffic).

Back Panel

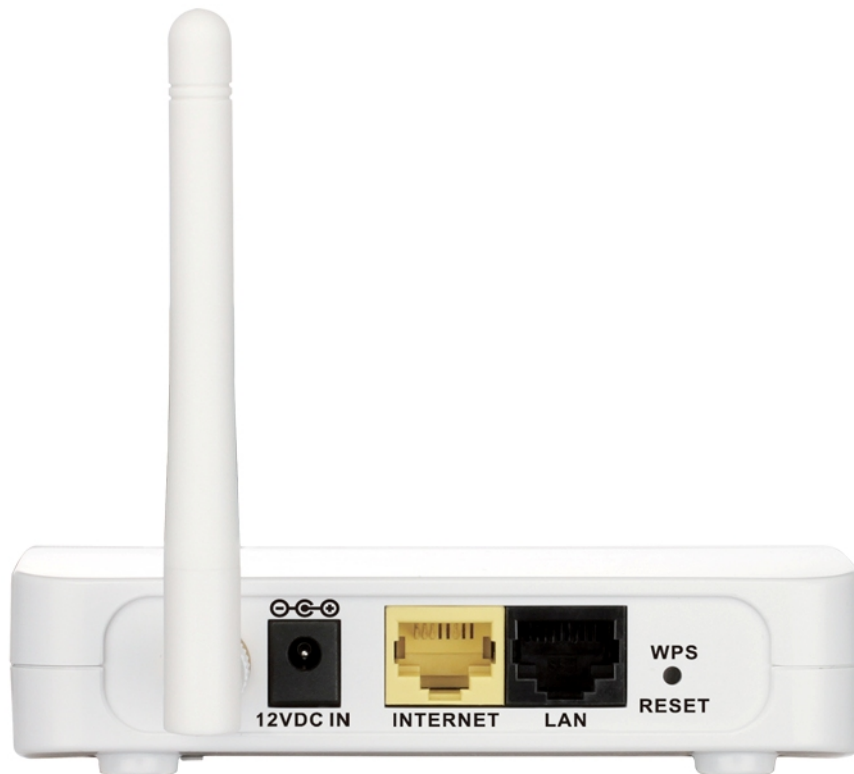


Figure 2. Back panel view.

Port	Description
12 VDC IN	Power connector.
INTERNET	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).
LAN	An Ethernet port to connect to a computer.
WPS RESET	A button to restore the factory default settings and to quickly add wireless devices to the access point's WLAN (the WPS function). To use the WPS function: with the device turned on, push the button and immediately release it. To restore the factory defaults: with the device turned on, push the button, hold it for 3 seconds, then release it.

The device is equipped with a detachable antenna (Reverse SMA).

Delivery Package

The following should be included:

- Access point DAP-1155
- Power adapter DC 12V
- Ethernet cable (CAT 5E)
- “***Quick Installation Guide***” (brochure).

The “***User Manual***” and “***Quick Installation Guide***” documents in Russian and English are available on D-Link website (see <ftp.dlink.ru/pub/Wireless/DAP-1155/Description/Rev.B/>).



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-1155 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: Windows Internet Explorer, Mozilla Firefox, or Opera.

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 the LAN port 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 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.

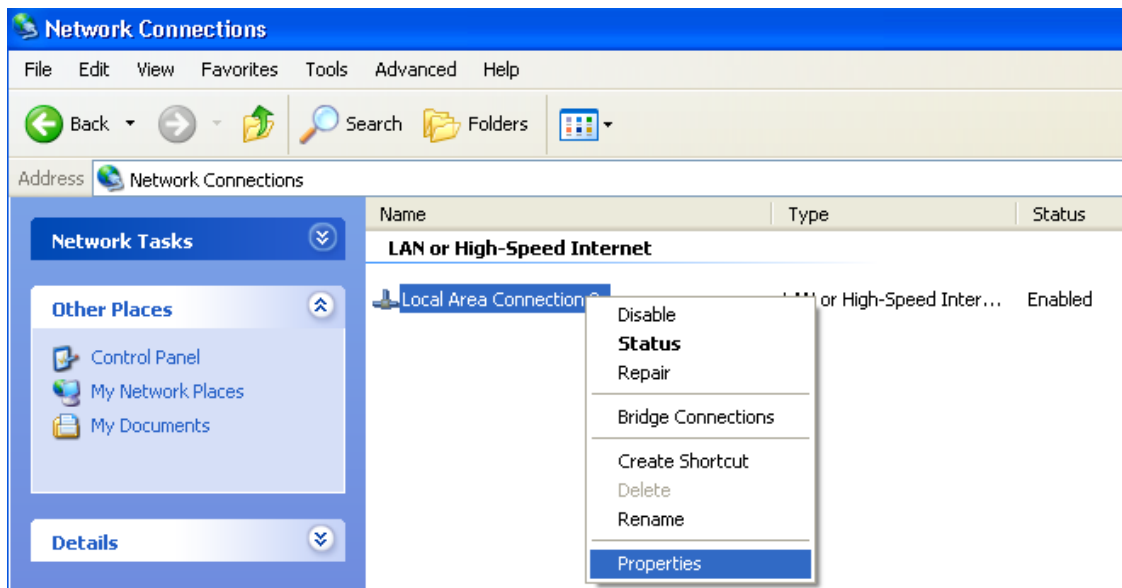


Figure 3. The **Network Connections** window.

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

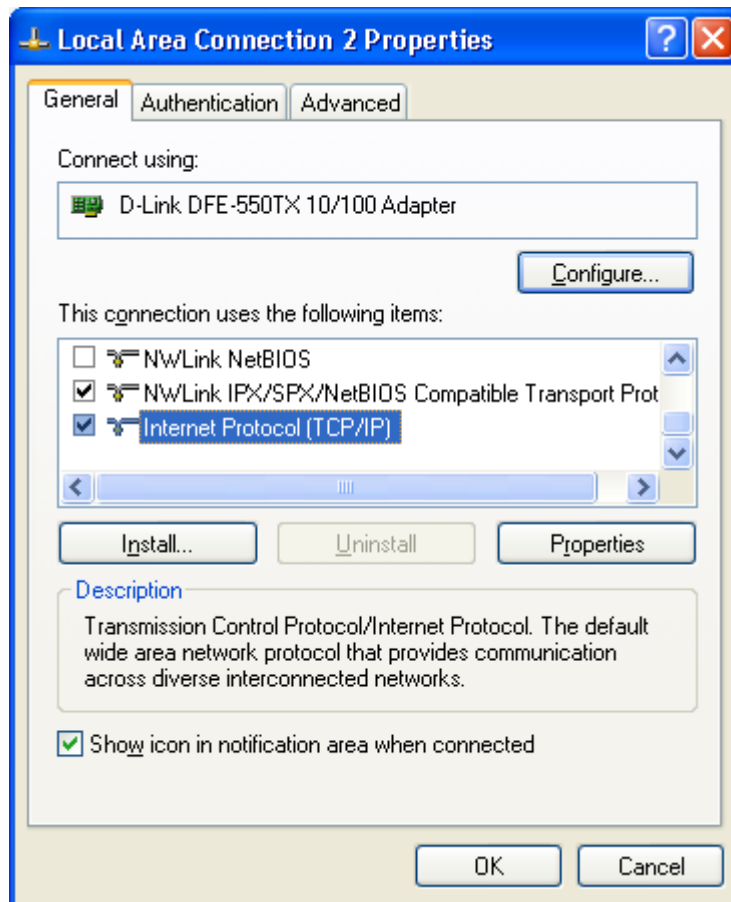


Figure 4. The **Local Area Connection Properties** window.

4. Select the **Use the following IP address** radio button and enter the value **198.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

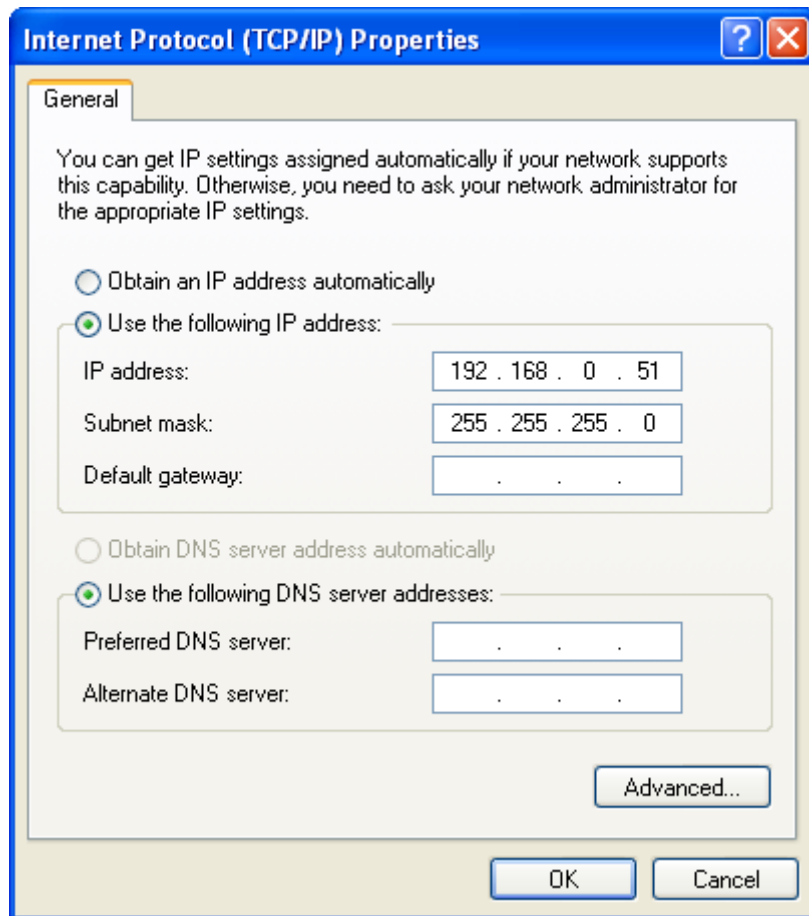


Figure 5. The **Internet Protocol (TCP/IP) Properties** window.

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

Now you can connect to the web-based interface of DAP-1155 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.)

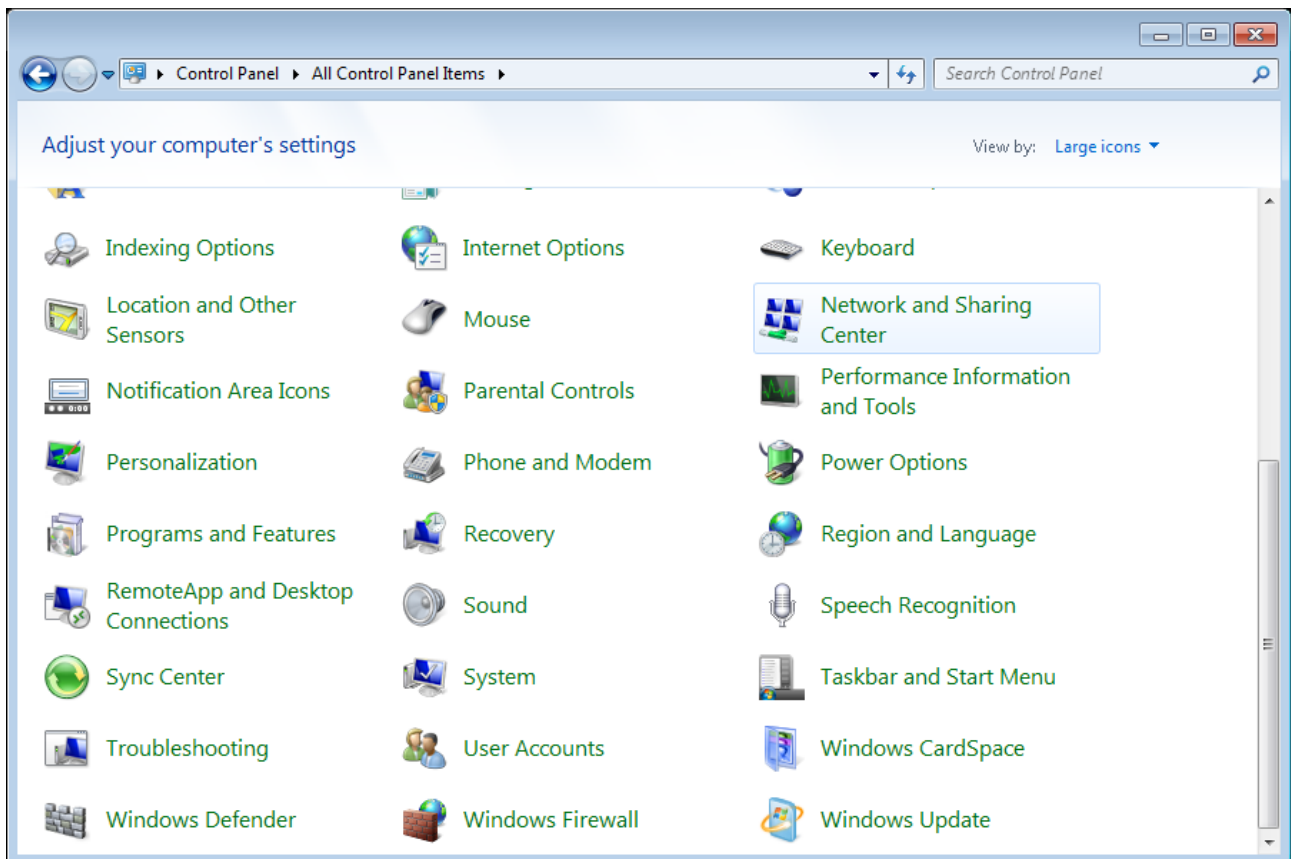


Figure 6. The **Control Panel** window.

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

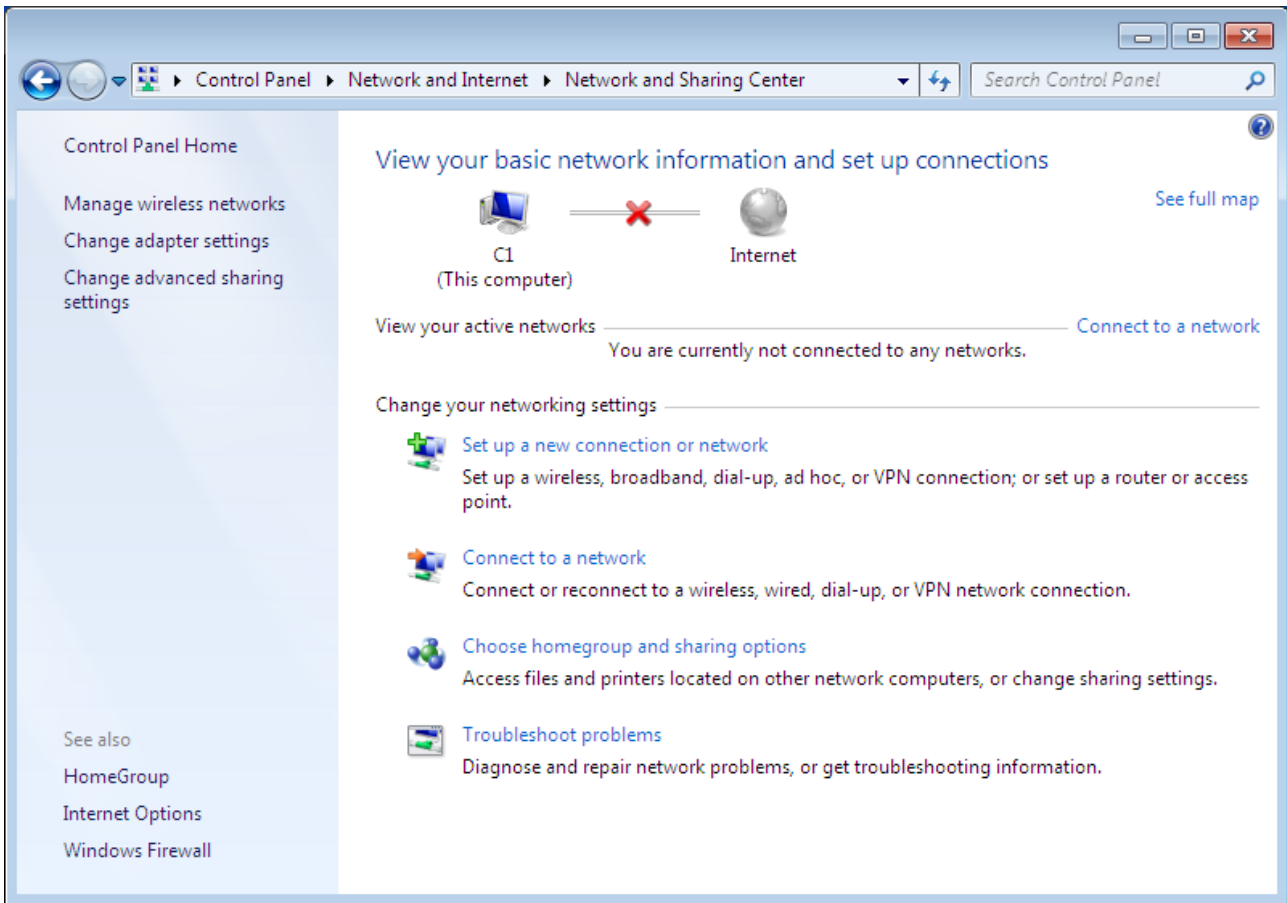


Figure 7. The **Network and Sharing Center** window.

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

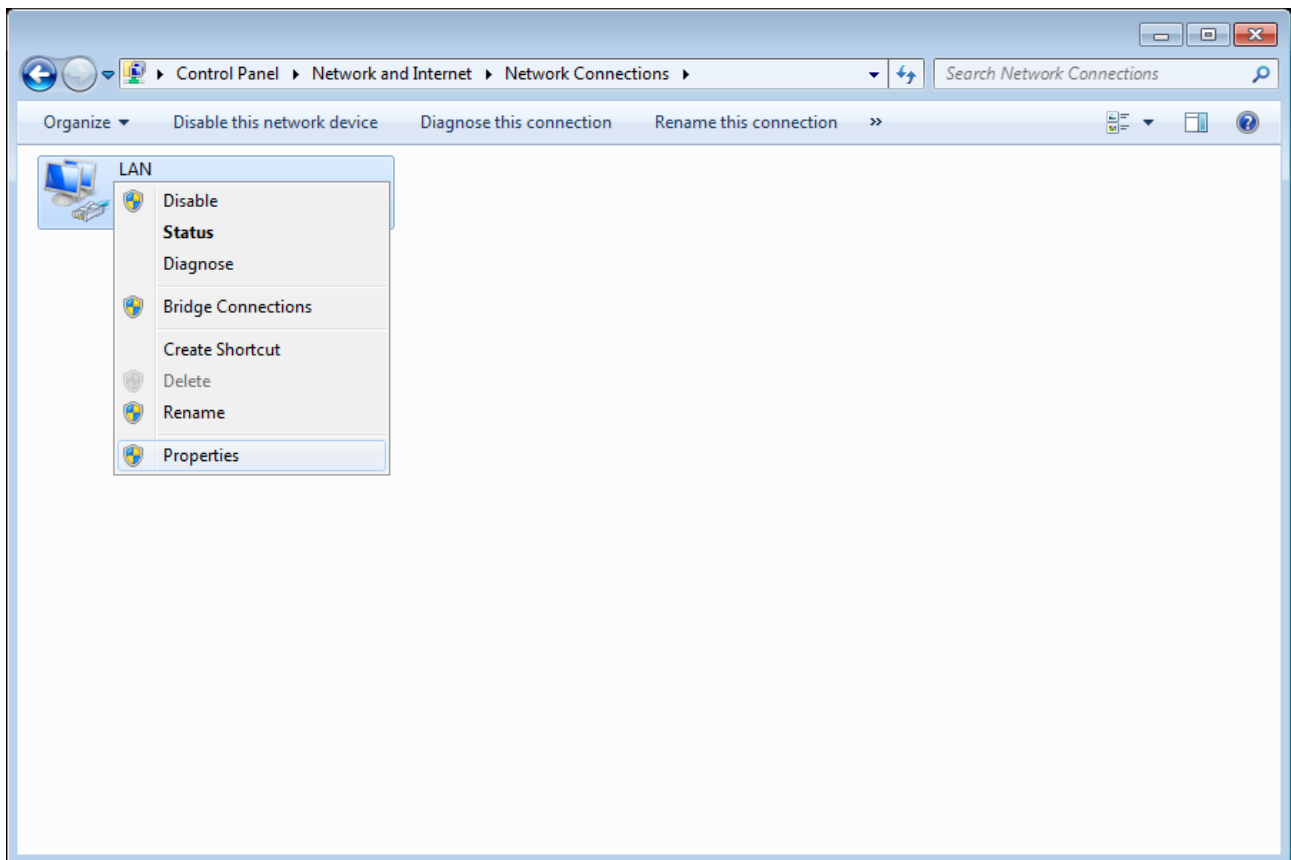


Figure 8. The **Network Connections** window.

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.

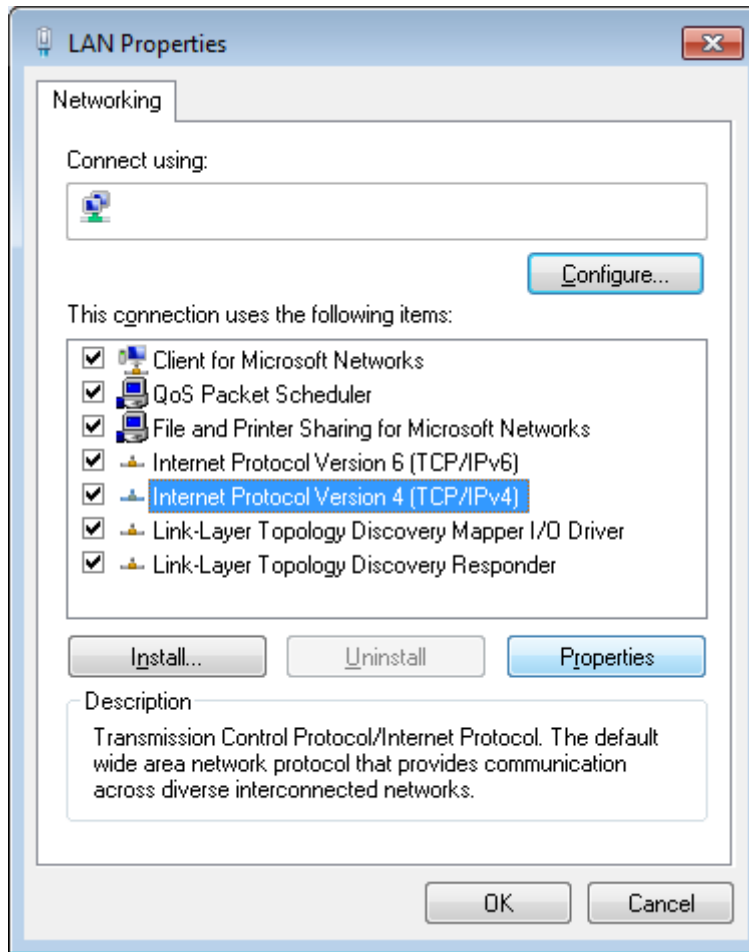


Figure 9. The **Local Area Connection Properties** window.

6. Select the **Use the following IP address** radio button and enter the value **198.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

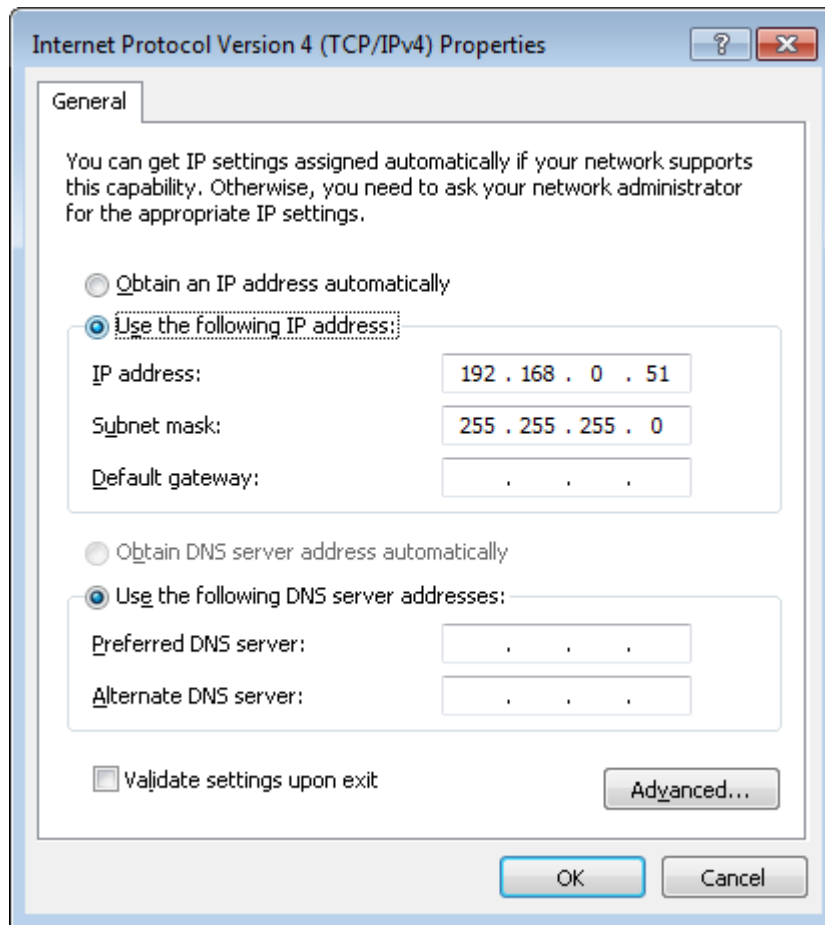


Figure 10. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now you can connect to the web-based interface of DAP-1155 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. 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.
2. Turn on your PC and wait until your operating system is completely loaded.
3. 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 **198.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

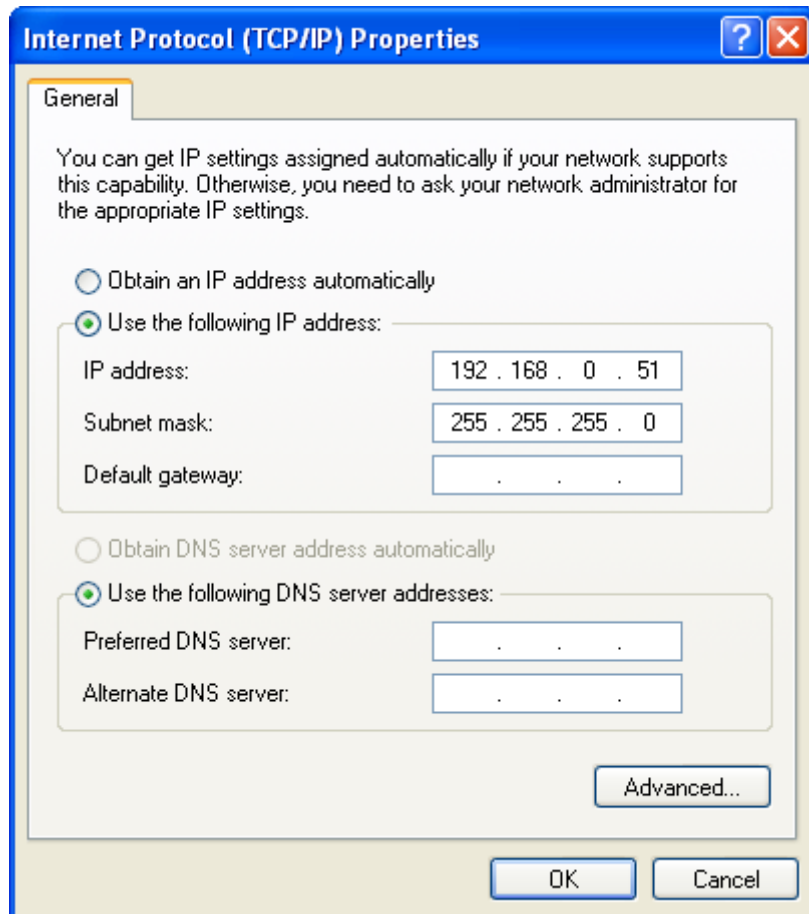


Figure 11. The **Internet Protocol (TCP/IP) Properties** window.

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

6. Search for available wireless networks.

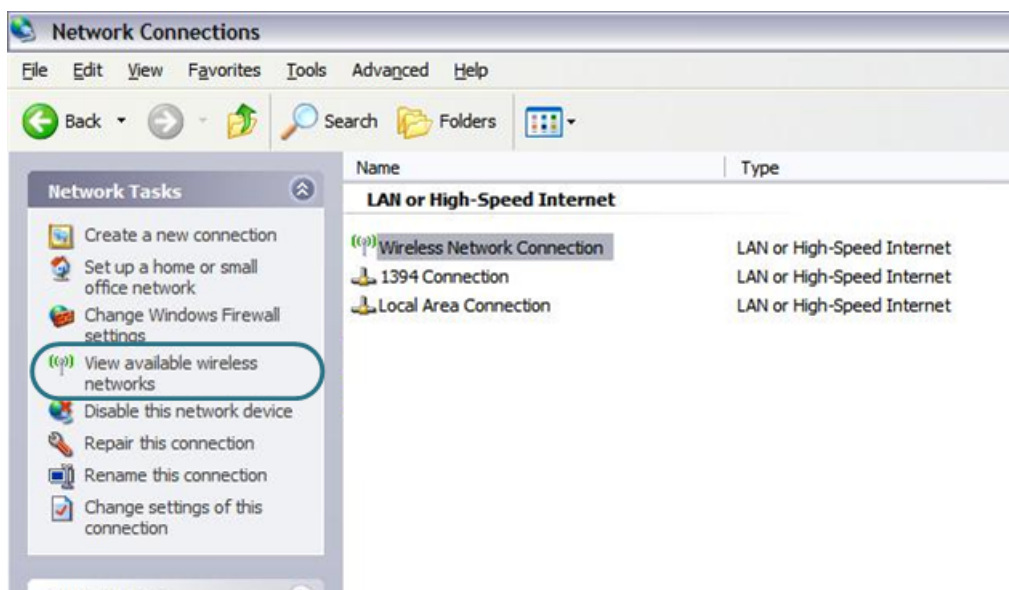


Figure 12. The **Network Connections** window.

7. In the opened **Wireless Network Connection** window, select the wireless network **DAP-1155** 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-1155 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.)

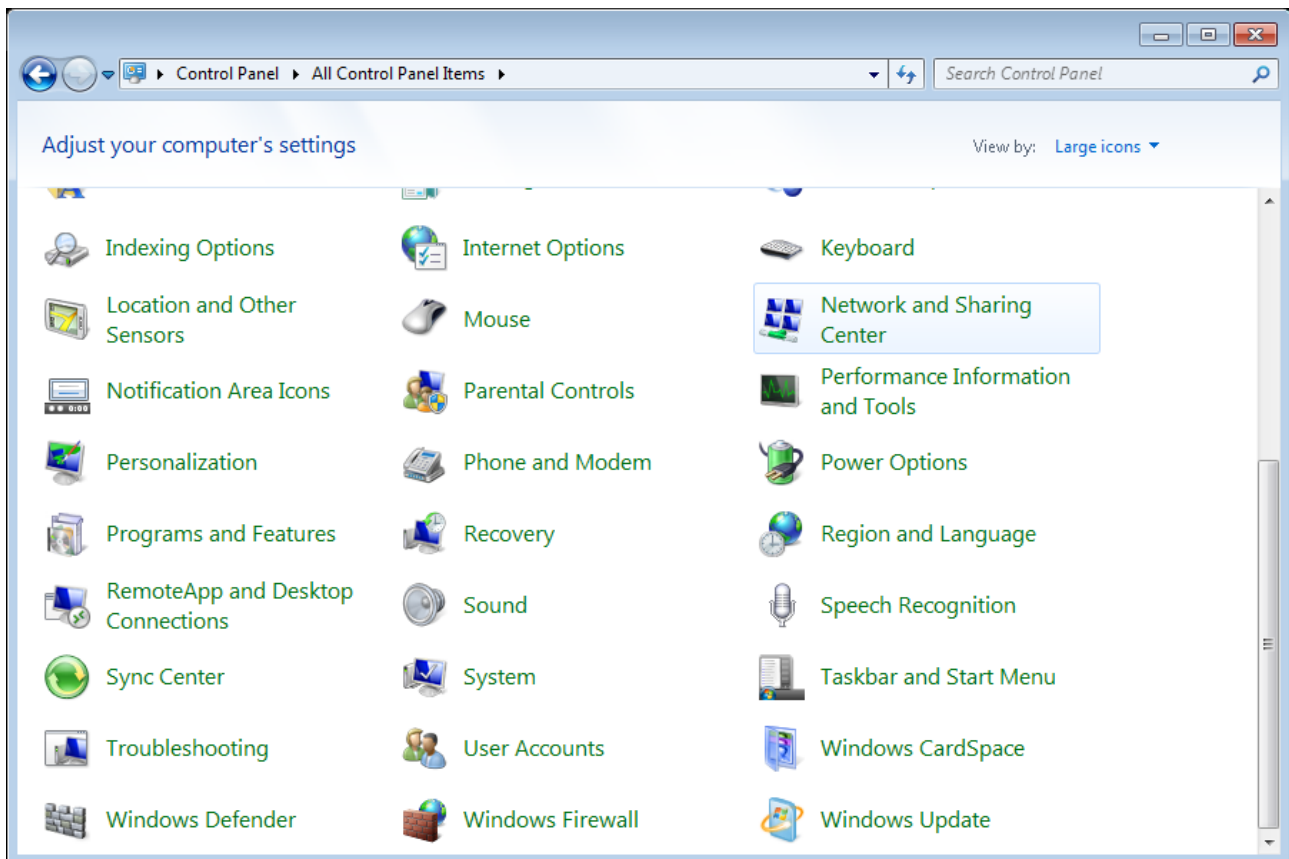


Figure 13. The **Control Panel** window.

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 **198.168.0.51** in the **IP address** field. The **Subnet mask** field will be filled in automatically. Click the **OK** button.

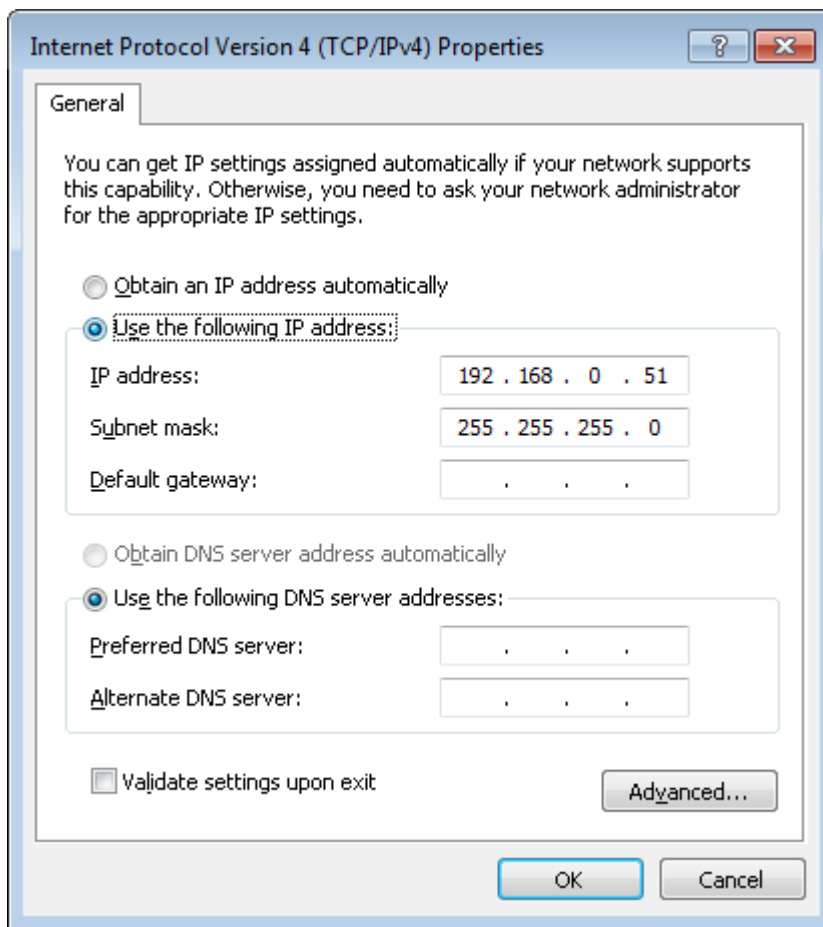


Figure 14. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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.

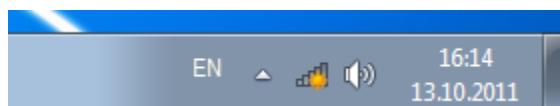


Figure 15. The notification area of the taskbar.

9. In the opened window, in the list of available wireless networks, select the wireless network **DAP-1155** and click the **Connect** button.

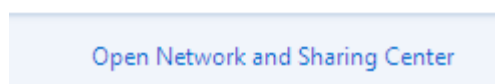
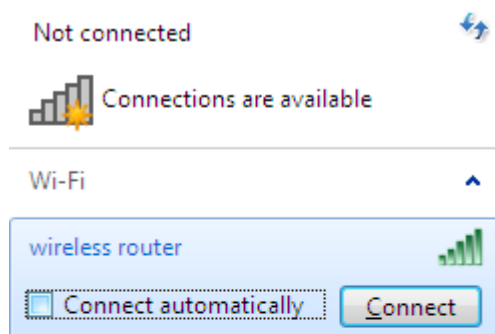


Figure 16. The list of available networks.

10. 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-1155 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.).

1. Start a web browser (see the *Before You Begin* section, page 14).
2. In the address bar of the web browser, enter **http://dlinkap/** or **http://192.168.0.50/** (the default IP address of the access point). Press the **Enter** key.



Figure 17. Connecting to the web-based interface of the DAP-1155 device.

3. On the opened page, enter the username and password for the administrator account in the **Login** and **Password** fields correspondingly (by default, the following username and password are specified: **admin**, **admin**). Then click the **Enter** link.

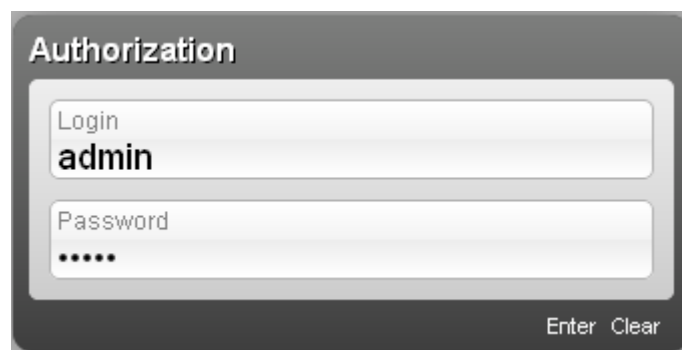


Figure 18. The login page.

! 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.

Right after the first access to the web-based interface you are forwarded to the page for changing the administrator password specified by default.

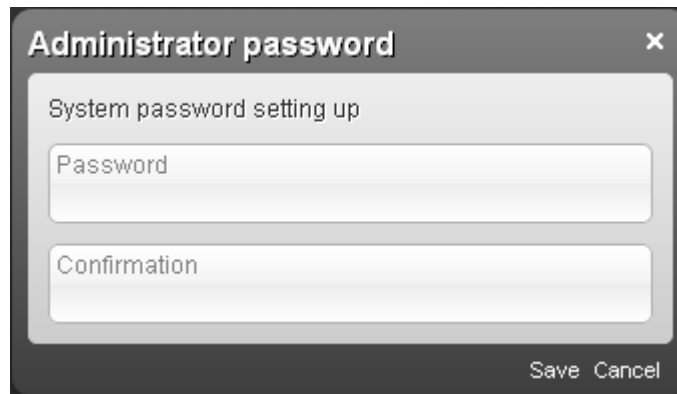


Figure 19. The page for changing the default administrator password.

Enter a new password in the **Password** and **Confirmation** fields (you may use digits, Latin letters (uppercase and/or lowercase), and characters available on the keyboard), then click the **Save** link.



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 **WPS/RESET** button. This procedure wipes out all settings that you have configured for your device.

Web-based Interface Structure

After successful registration the access point's quick settings page opens. The selected operating mode defines the view of the quick settings page and the components of the web-based interface.

The web-based interface of the access point is multilingual. Select a needed language from the menu displayed when the mouse pointer is over the **Language** caption. You can change the language of the web-based interface in any menu item.

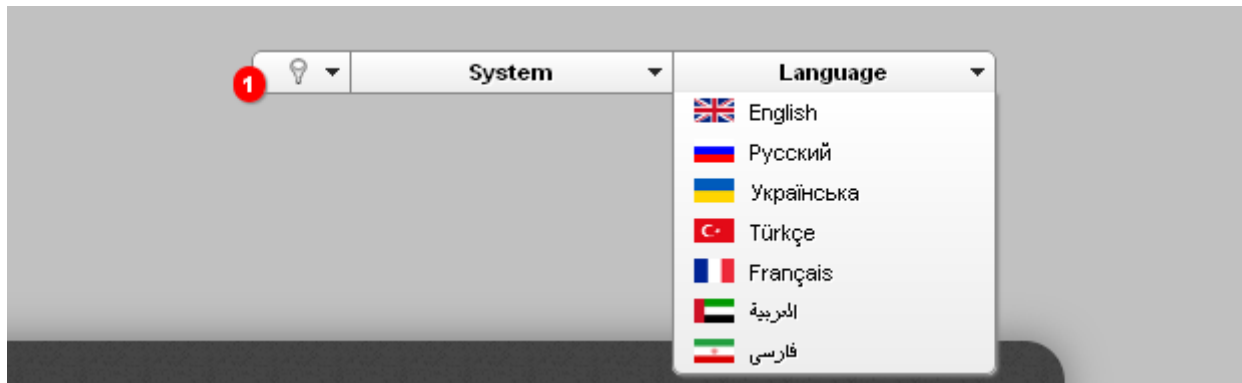



Figure 20. Changing the language of the web-based interface.

After selecting the language, the notification on unsaved changes will be displayed. Click the **Save**

icon () to save the current language of the web-based interface as the default language.

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.

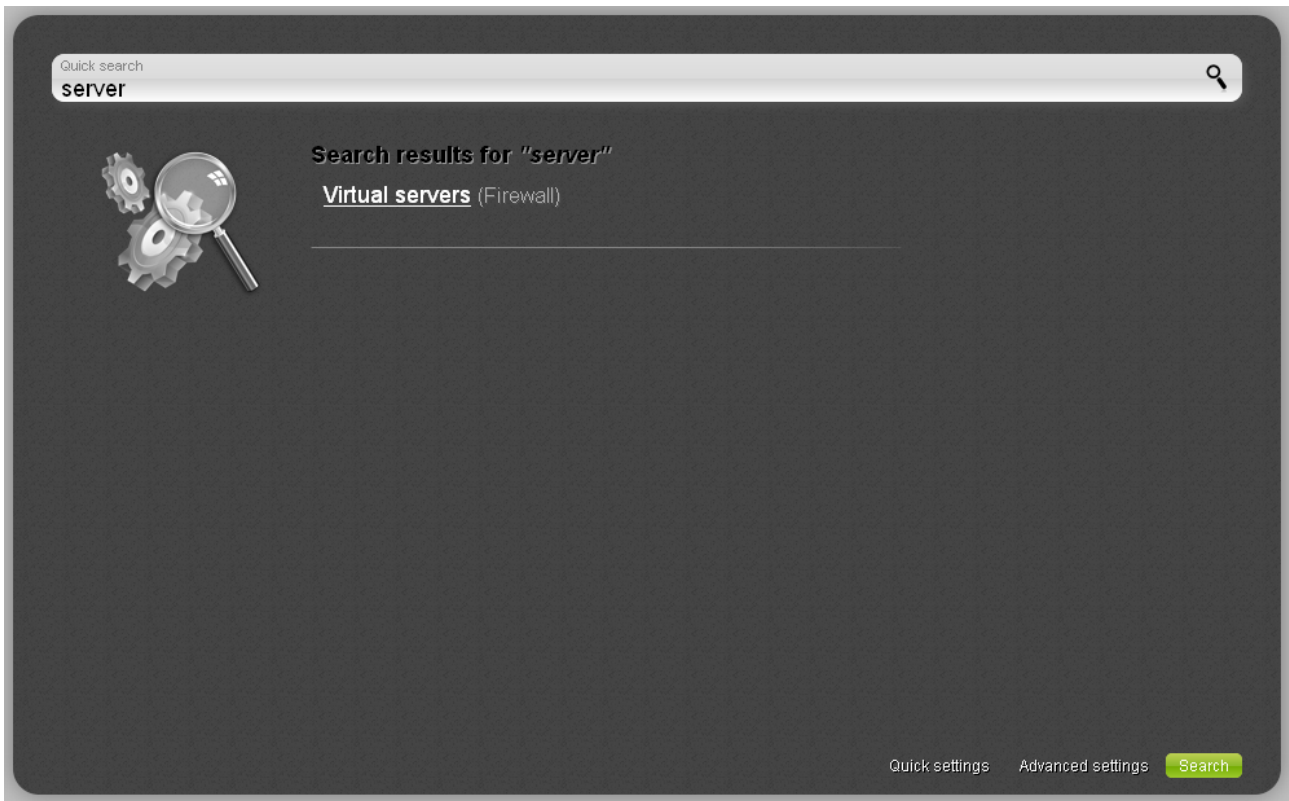


Figure 21. The page displaying the search results.

Access Point Mode

The quick settings page displays general information on the access point and its software (the version and the date of the firmware, the IP address of the device, the name of the WLAN, etc.).



Figure 22. The quick settings page in the access point mode.

On the page you can run the Wi-Fi Wizard, quickly get to some pages of the web-based interface, search for a specific page, or switch to the advanced settings section.

To upgrade the firmware of the access point, left-click the current firmware version (the right column of the **Firmware version** line). After clicking the line, the **System / Firmware upgrade** page opens (for the detailed description of the page, see the *Firmware Upgrade* section, page 83).

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 49).

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 the access point's wireless network, click the **Wireless network settings wizard** link in the **Wi-Fi** section (for the detailed description of the Wizard, see the *Wireless Network Settings Wizard* section, page 40).

To configure all parameters of the access point independently without the Wizard, click the **Advanced settings** link in the bottom right corner of the page.

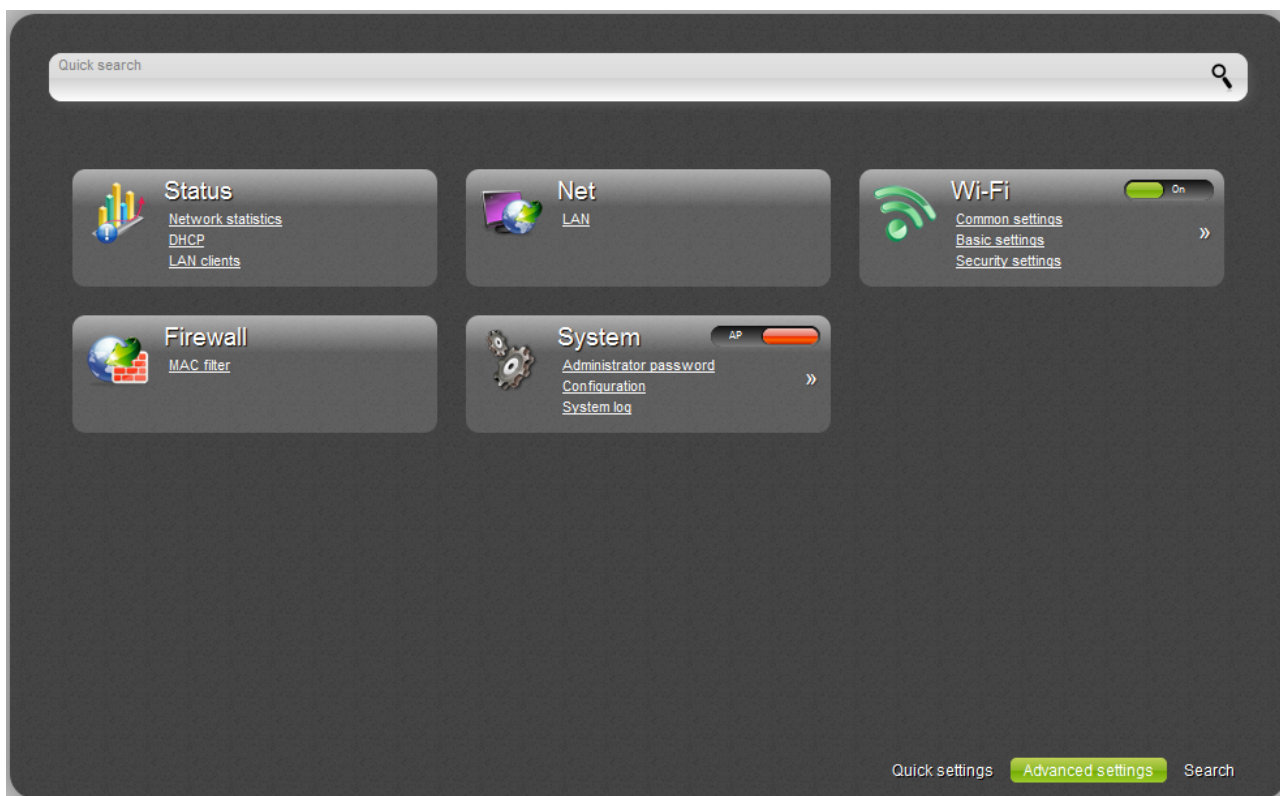
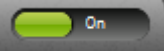



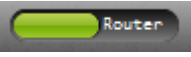

Figure 23. The advanced settings page in the access point mode.

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 49).

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 52). Also you can enable or disable the device's WLAN directly from the advanced settings page. To enable the WLAN, select the **On** position () of the **Enable/Disable Wi-Fi** switch. To disable the WLAN, select the **Off** position () of the **Enable/Disable Wi-Fi** switch.

The page of the **Firewall** section is designed for configuring MAC-address-based filtering for computers of the access point's LAN (for the description of the page, see the *Firewall* section, page 75).

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 77). Also you can change the operating mode of the device directly from the advanced settings page. To switch the device to the router mode, select the **Router** position () of the **Switch device mode** switch. In the opened dialog box, click the **OK** button to save new settings and immediately reboot the access point. To switch the device to the access point mode, select the **AP** position () of the **Switch device mode** switch. In the opened dialog box, click the **OK** button and wait until the device is rebooted.

Router Mode

The quick settings page displays general information on the access point and its software (the version and the date of the firmware, the IP address of the device, the name of the WLAN, etc.).



Figure 24. The quick settings page in the router mode.

On the page you can run a needed Wizard, quickly get to some pages of the web-based interface, search for a specific page, or switch to the advanced settings section.

To upgrade the firmware of the access point, left-click the current firmware version (the right column of the **Firmware version** line). After clicking the line, the **System / Firmware upgrade** page opens (for the detailed description of the page, see the **Firmware Upgrade** section, page 206).

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 152).

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 156).

To configure connection to the Internet, click the **Click'n'Connect** link in the **Net** section (for the detailed description of the Wizard, see the *Click'n'Connect* section, page 88).

To configure the access point's wireless network, click the **Wireless network settings wizard** link in the **Wi-Fi** section (for the detailed description of the Wizard, see the *Wireless Network Settings Wizard* section, page 120).

To configure access from the Internet to a web server located in your LAN, click the **Virtual server settings wizard** link in the **Firewall** section (for the detailed description of the Wizard, see the *Virtual Server Settings Wizard* section, page 126).

To configure all parameters of the access point independently without the Wizards, click the **Advanced settings** link in the bottom right corner of the page.

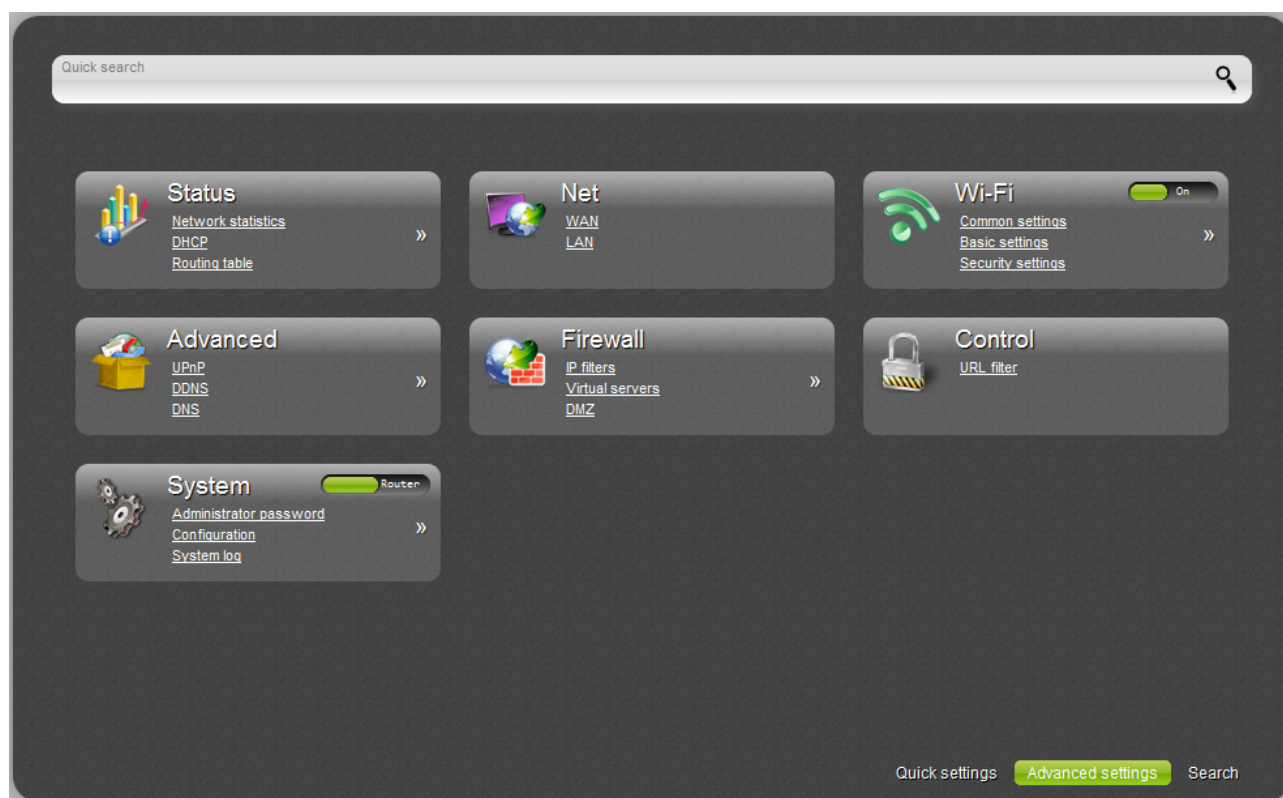
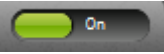



Figure 25. The advanced settings page in the router mode.

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 127).

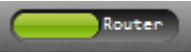

The pages of the **Net** section are designed for configuring basic parameters of the LAN interface of the access point and creating a connection to the Internet (for the description of the pages, see the *Net* section, page 131).

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 155). Also you can enable or disable the device's WLAN directly from the advanced settings page. To enable the WLAN, select the **On** position () of the **Enable/Disable Wi-Fi** switch. To disable the WLAN, select the **Off** position () of the **Enable/Disable Wi-Fi** switch.


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 178).

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 188).

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 197).

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 200). Also you can change the operating mode of the device directly from the advanced settings page. To switch the device to the router mode, select the **Router** position () of the **Switch device mode** switch. In the opened dialog box, click the **OK** button to save new settings and immediately reboot the access point. To switch the device to the access point mode, select the **AP** position () of the **Switch device mode** switch. In the opened dialog box, click the **OK** button and wait until the device is rebooted.

Saving and Restoring Settings

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

The access point's web-based interface displays the notification on unsaved changes at the top of the page.

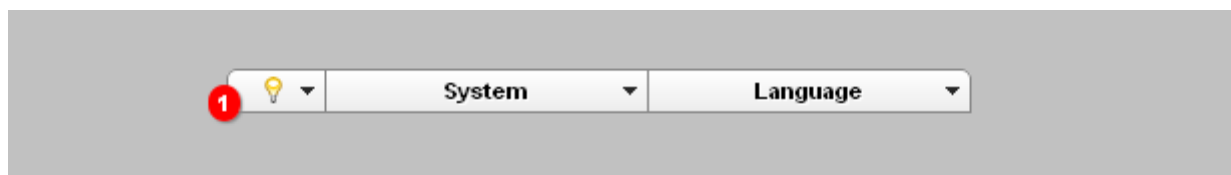



Figure 26. The notification on unsaved changes.

Place the mouse pointer on the **Notifications** icon () to view the list of unsaved changes and click the relevant link.

You can save the access point's settings via the top-page menu displayed when the mouse pointer is over the **System** caption.

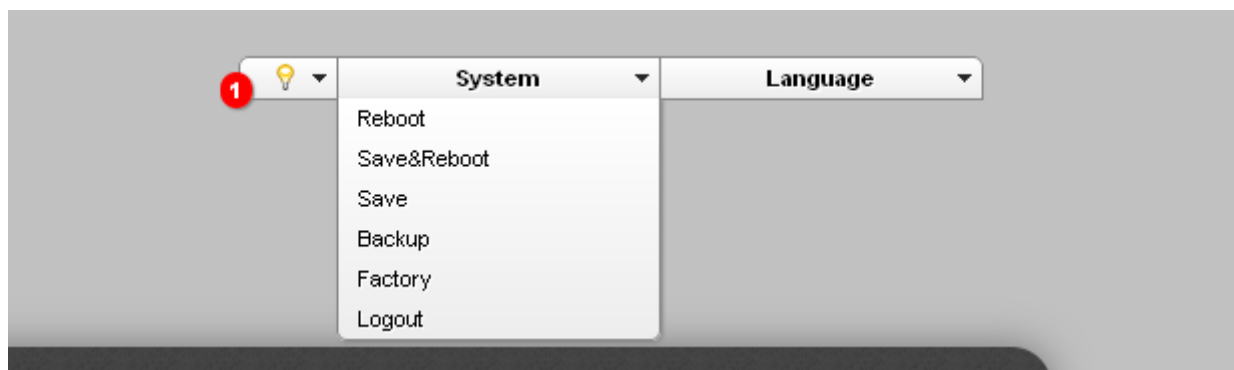


Figure 27. The top-page menu.

Click the **Reboot** line if you have already saved the access point's settings.

Click the **Save&Reboot** line to save new settings and immediately reboot the access point.

Click the **Save** line to save new settings to the non-volatile memory and continue configuring the device. Also you can save the device's parameters via the **Save** button on the **System / Configuration** page.

Click the **Backup** line and follow the dialog box appeared to save the configuration (all settings of the access point) to your PC. Also you can save the access point's configuration to your PC via the **Backup** button on the **System / Configuration** page.

Click the **Factory** line to restore the factory default settings. Also you can restore the factory defaults via the **Factory** button on the **System / Configuration** page.

Also you can restore the factory default settings via the hardware **WPS/RESET** button. The button is located on the back panel of the access point. Use a small paperclip to activate the button; insert it into the hole (with the access point turned on), push, and hold for 3 seconds. Then remove the paperclip. Wait for about 30 seconds. Now you can access the web-based interface of the access point using the default IP address, username and password.

When you have configured all needed settings, click the **Logout** line.

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 **Wi-Fi** section.

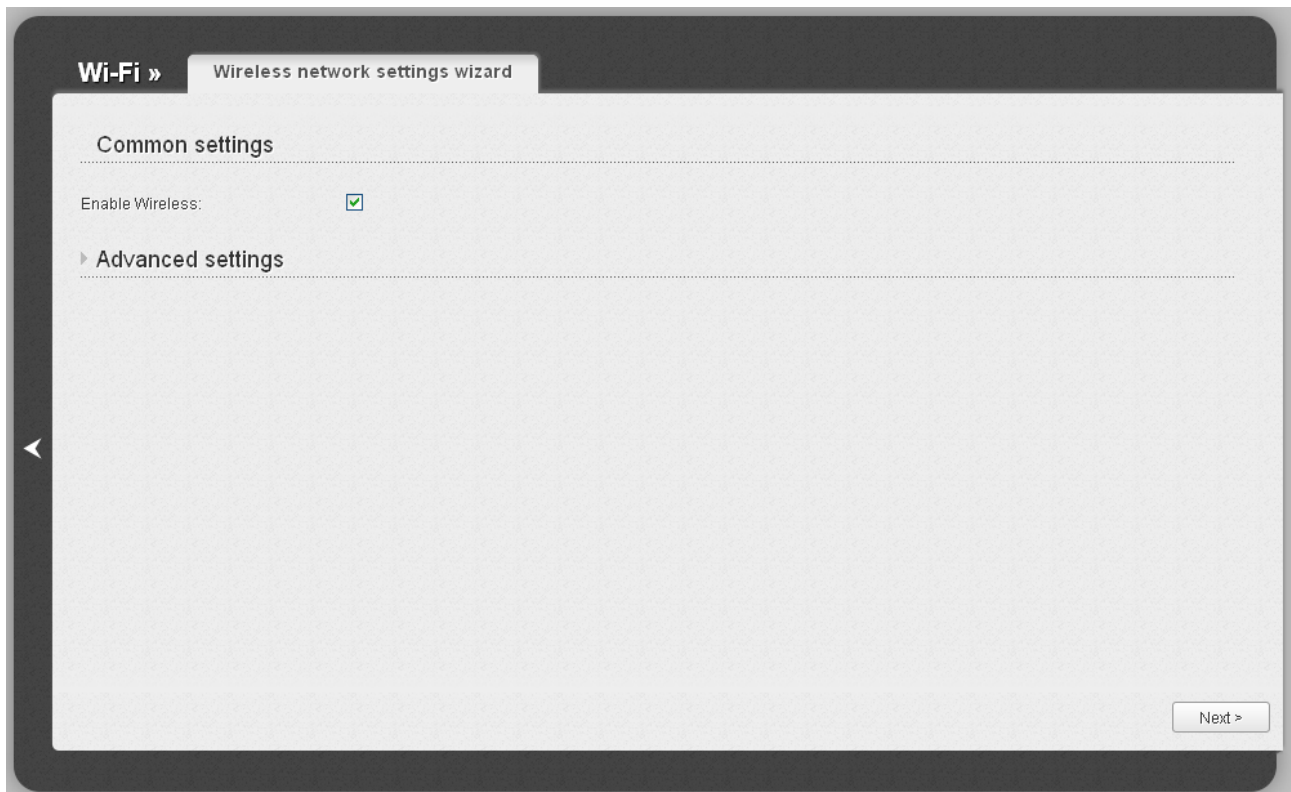


Figure 28. Common and advanced settings of the wireless LAN.

On the opened page, in the **Common settings** section, select the **Enable Wireless** checkbox (if it was deselected before) to enable Wi-Fi connections.

In the **Advanced settings** section, you can split your network into several parts. To do this, select the relevant value (**2**, **3**, or **4**) from the **MBSSID** drop-down list.

Click the **Next** button to continue.

In the **Basic settings** section, you can change the basic parameters of your access point's WLAN: “hide” your wireless network (**Hide Access Point**), specify a name for the network (**SSID**), select your location (**Country**) and the wireless channel number (**Channel**), specify the operating mode (**Wireless Mode**) and the maximum number of devices connected to the wireless network (**Max Associated Clients**).

Wi-Fi » Wireless network settings wizard

Basic settings

Hide Access Point

SSID:

Country:

Channel:

Wireless mode:

When changing mode from "B/G" on any of the modes with "N" is recommended to re-tune security!

Max Associated Clients:

< Back Next >

Figure 29. Basic settings of the wireless LAN.

Click the **Next** button to continue.

On the next page, you can modify security settings of the WLAN. By default, the **Open** network authentication type with no encryption is specified for the WLAN.

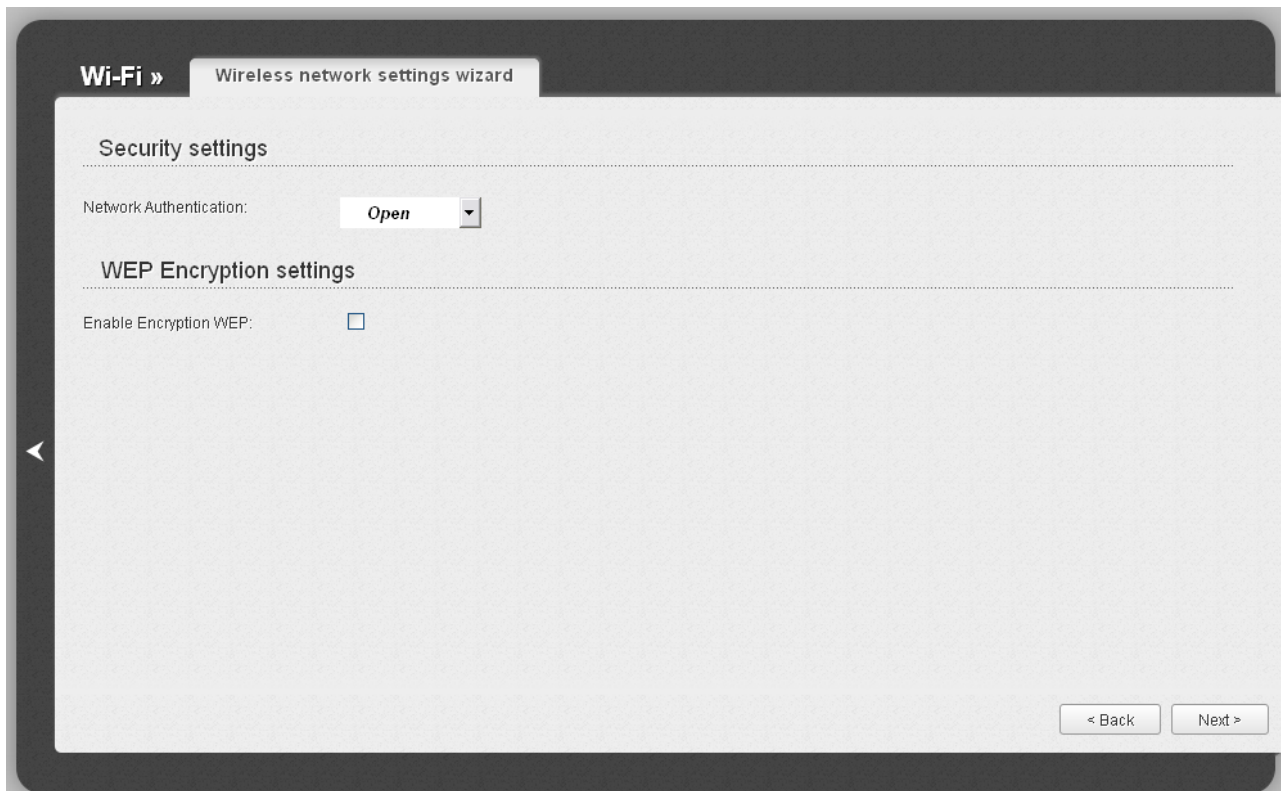


Figure 30. The default security settings.



The default security settings do not provide sufficient protection for the WLAN. Please specify your own security settings for the WLAN (or each part of the WLAN if the network was splitted into parts).

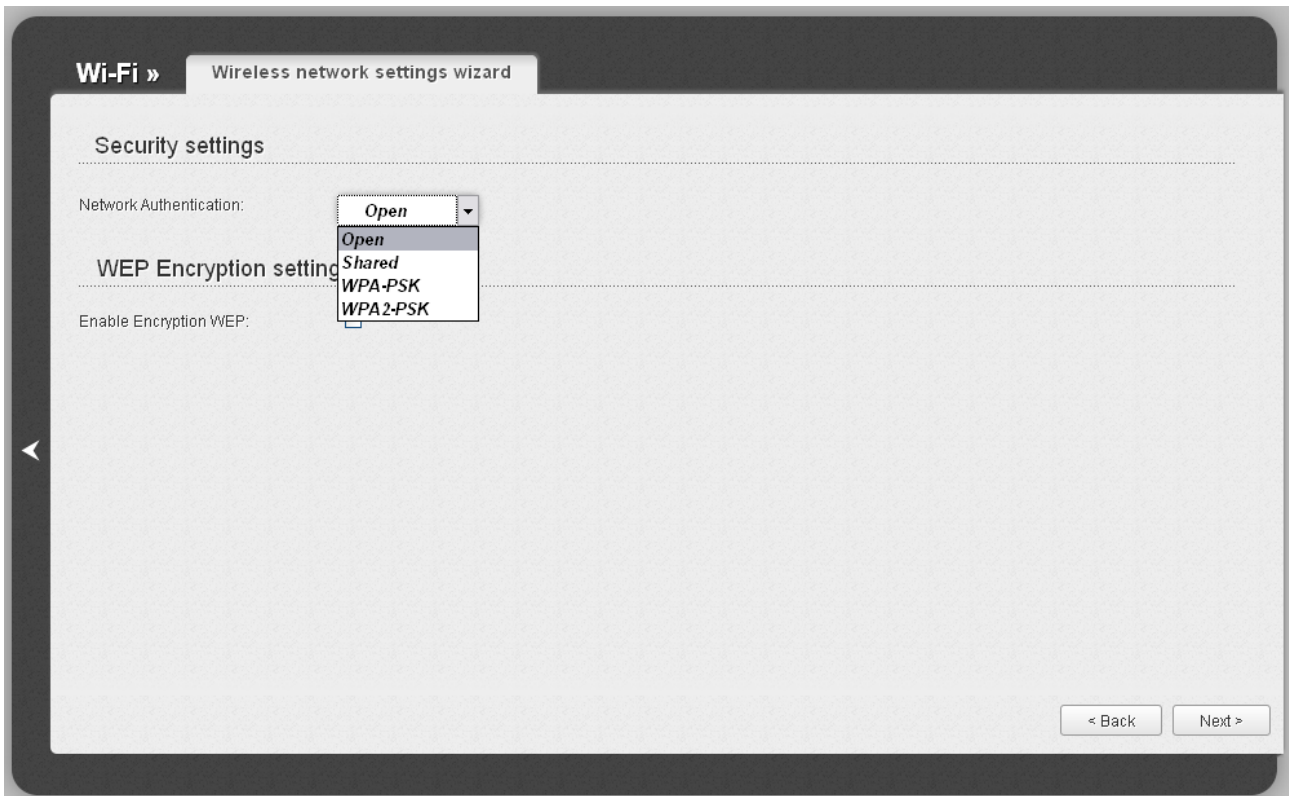


Figure 31. Network authentication types supported by the access point.

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 basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected.
WPA-PSK	WPA-based authentication using a PSK.
WPA2-PSK	WPA2-based authentication using a PSK.

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):

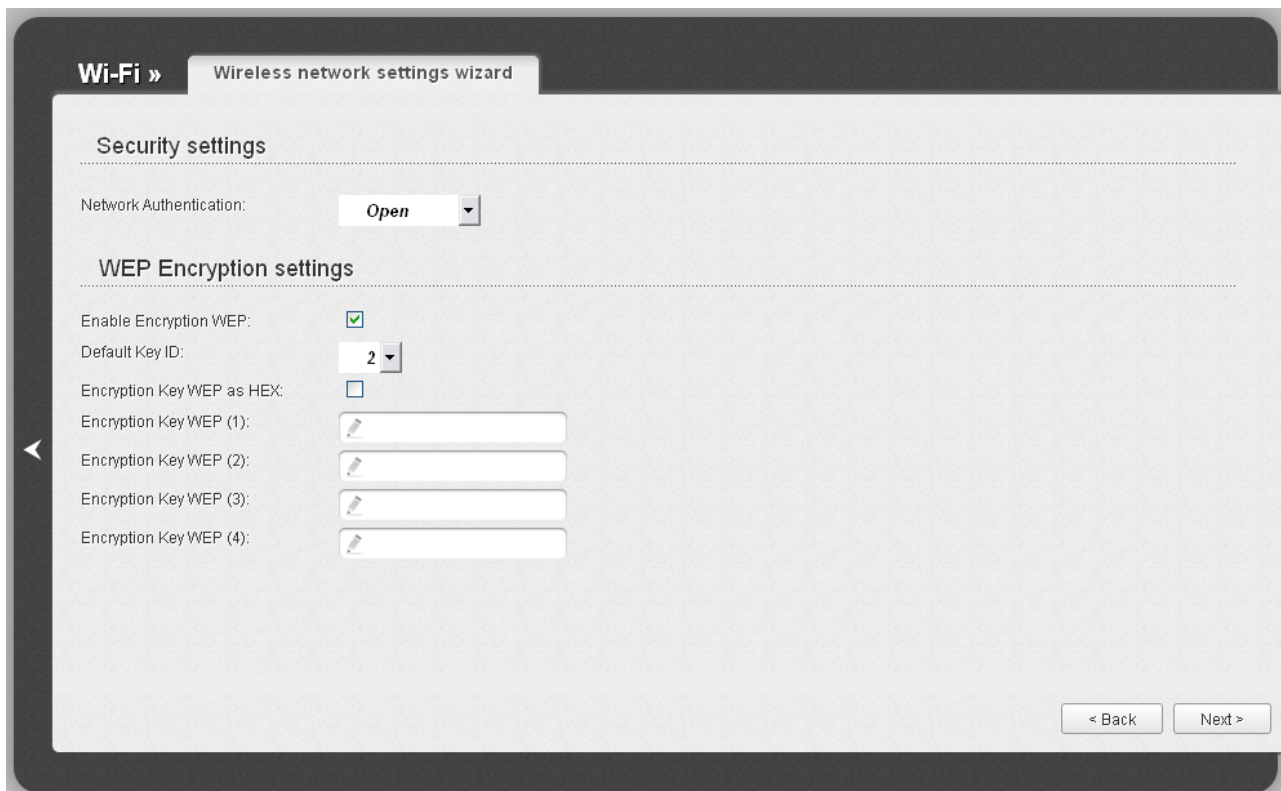


Figure 32. The **Open** value is selected from the **Network Authentication** drop-down list.

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, 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.
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. You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters). If the Encryption Key WEP as HEX checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F).

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



Figure 33. The **WPA2-PSK** 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.
WPA2 Pre-authentication	The checkbox activating preliminary authentication (displayed only for the WPA2-PSK authentication type).
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.

Click the **Next** button to continue.

When all the steps of configuring the WLAN are completed, the specified settings are displayed on the page. Check their correctness and then click the **Save** button. After that you get to the quick settings page.

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.

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).



Name	IP	Gateway	MAC	MTU	Rx/Tx
WIFI	-	-	00:12:34:56:79:22	1500	3.42 Mbyte/60.3 Kbyte
LAN	192.168.0.50/24	-	00:12:34:56:78:22	1500	119 Kbyte/1.34 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).

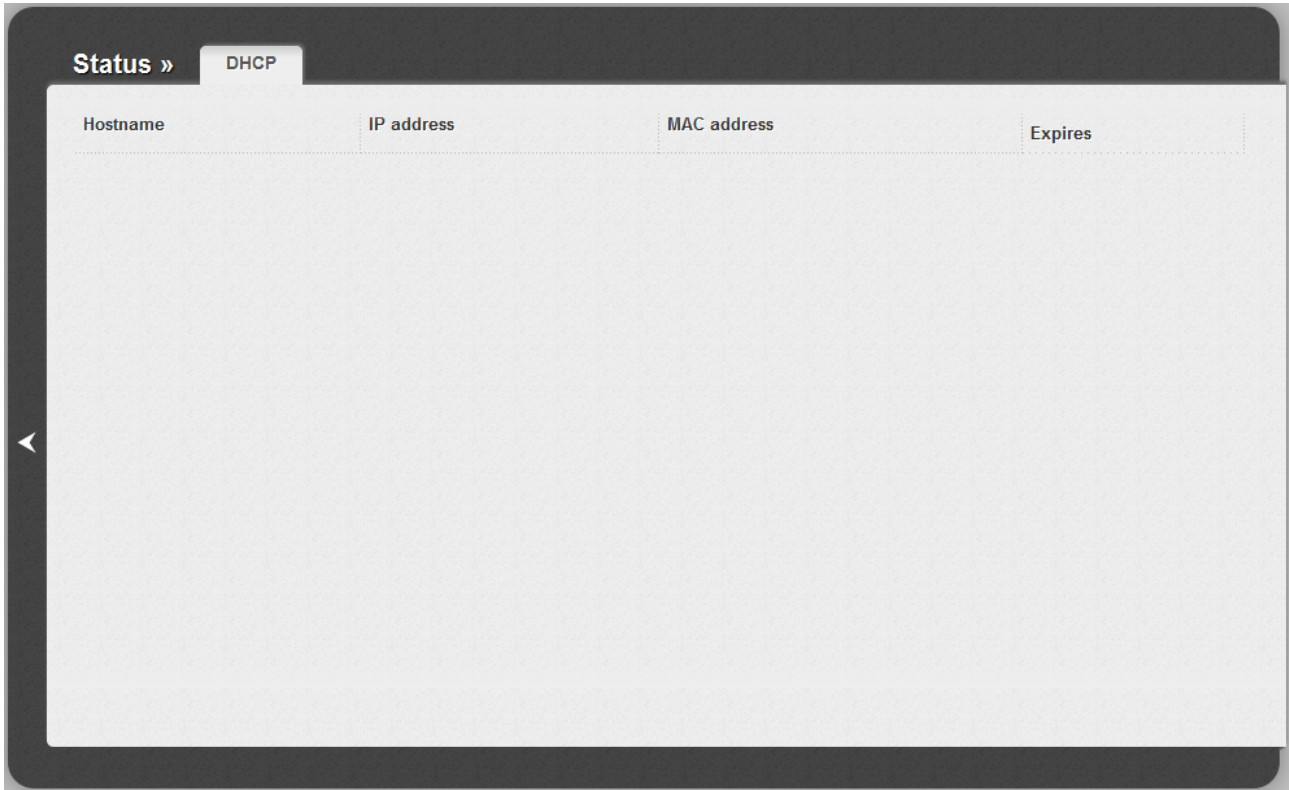


Figure 35. The **Status / DHCP** page.

LAN Clients

On the **Status / LAN 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 with a dark header. On the left, there is a navigation menu with a left-pointing arrow. The main content area has a dark background with a light-colored table. The table has four columns: IP address, Flags, MAC address, and Interface. There are three rows of data. The first row shows IP address 192.168.1.77, Flags 0x2, MAC address 00:30:48:fe:db:ec, and Interface LAN. The second row shows IP address 192.168.1.40, Flags 0x2, MAC address 1c:6f:65:b0:82:ba, and Interface LAN. The third row shows IP address 192.168.161.1, Flags 0x2, MAC address 1c:6f:65:b0:82:ba, and Interface WAN.

IP address	Flags	MAC address	Interface
192.168.1.77	0x2	00:30:48:fe:db:ec	LAN
192.168.1.40	0x2	1c:6f:65:b0:82:ba	LAN
192.168.161.1	0x2	1c:6f:65:b0:82:ba	WAN

Figure 36. The **Status / LAN 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.

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 the LAN configuration interface. It features two input fields: 'IP Address:*' with a pencil icon and the value '192.168.0.50', and 'Netmask:*' with a pencil icon and the value '255.255.255.0'. The fields are set against a light gray background with a dotted line above them.

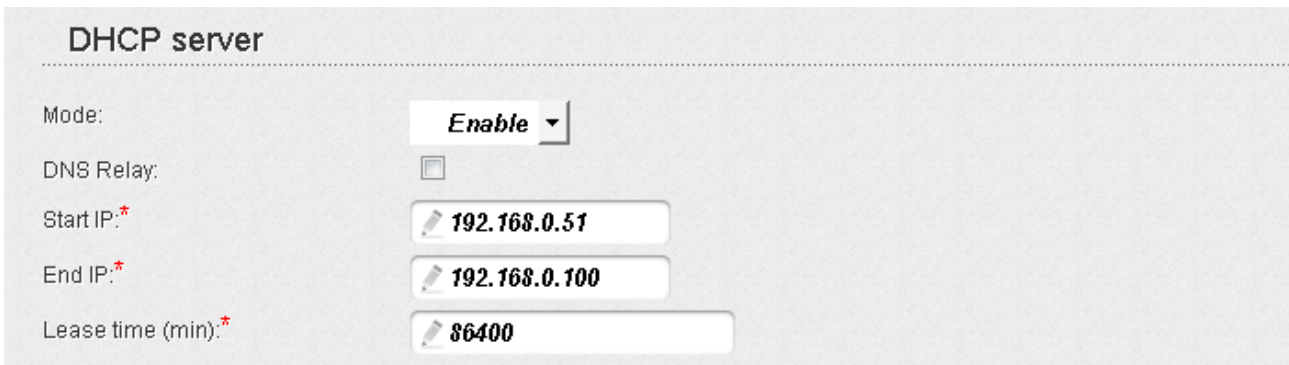
Figure 37. Basic settings of the local interface.

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 **Save** 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. It is titled 'DHCP server' and includes the following settings: 'Mode:' set to a dropdown menu with 'Enable' selected; 'DNS Relay:' with an unchecked checkbox; 'Start IP:*' with a pencil icon and the value '192.168.0.51'; 'End IP:*' with a pencil icon and the value '192.168.0.100'; and 'Lease time (min):*' with a pencil icon and the value '86400'. The background is light gray with a dotted line above the title.

Figure 38. 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. <i>Available in the router mode only.</i></p>
DNS Relay	<p><i>Available in the router mode only.</i></p> <p>Select the checkbox so that the devices connected to the access point obtain the address transmitted by the ISP as the DNS server address.</p> <p>Deselect the checkbox so that the devices connected to the access point obtain the address of the access point as the DNS server address.</p>
Start IP	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
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 **Save** 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).

Static DHCP

Known IP/MAC addresses:

	IP	MAC	Host
<input type="checkbox"/>			

Figure 39. 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 **IP** and **MAC** fields will be filled in automatically).

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

Wi-Fi

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

Common settings

On the **Wi-Fi / Common settings** page, you can enable your wireless local area network (WLAN) and split it into parts.

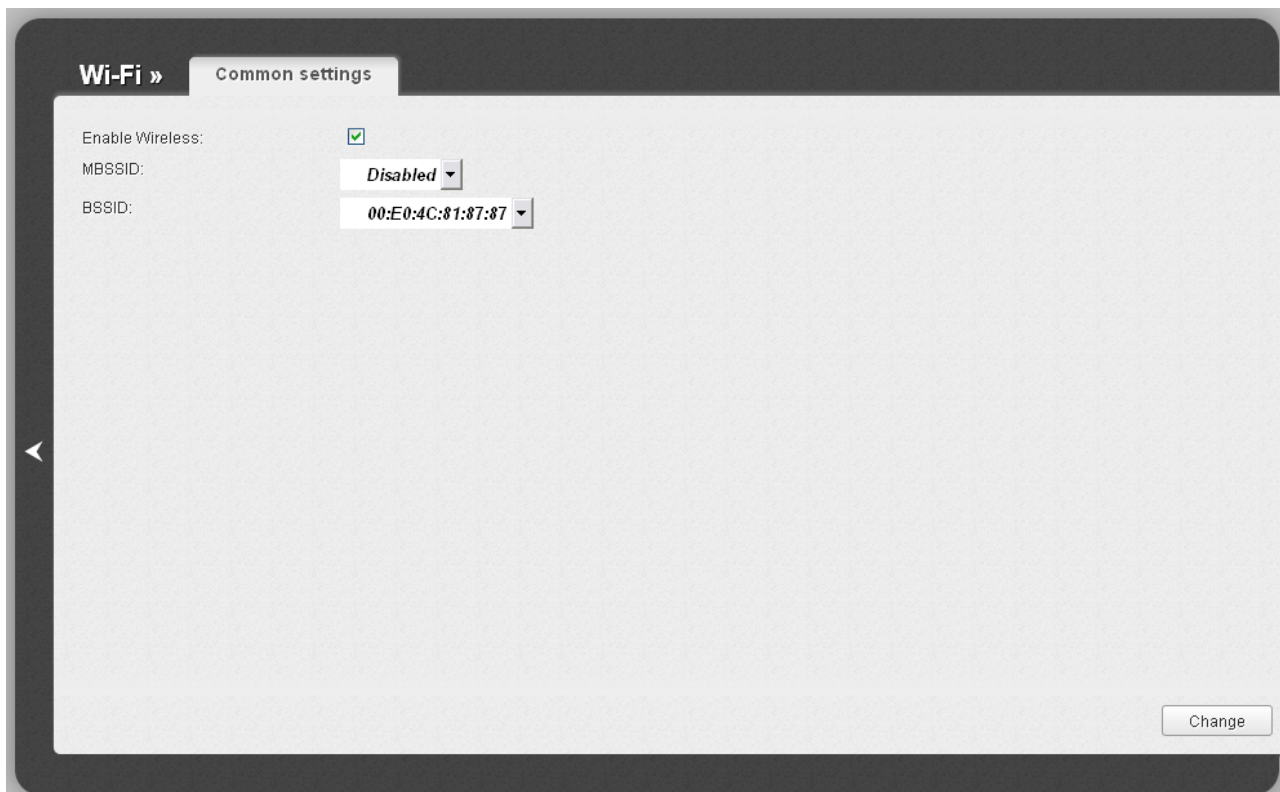


Figure 40. Common settings of the wireless LAN.

The **Enable Wireless** checkbox enables Wi-Fi connections. By default, the checkbox is selected. If you want to disable your WLAN, deselect the **Enable Wireless** checkbox.

The access point allows splitting your WLAN into several parts (up to four) with their own names (SSIDs) and unique identifiers (BSSIDs). To split the network into several parts, select a relevant value (**2**, **3**, or **4**) from the **MBSSID** drop-down list. By default, the wireless network is not splitted (the **Disabled** value is selected from the list).

The value from the **BSSID** drop-down list is 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.

If you have splitted your WLAN into parts, the **BSSID** drop-down list contains several values. Each identifier corresponds to a single part of the WLAN.

For every part of the WLAN you can specify a name (SSID), security settings, rules for MAC filtering, and enable the WMM function (if needed). To specify these values, select the needed part from the **BSSID** drop-down list and click the **Change** button. Then proceed to the relevant page of the **Wi-Fi** menu section.

Basic Settings

On the **Wi-Fi / Basic settings** page, you can configure basic parameters of the device's WLAN.

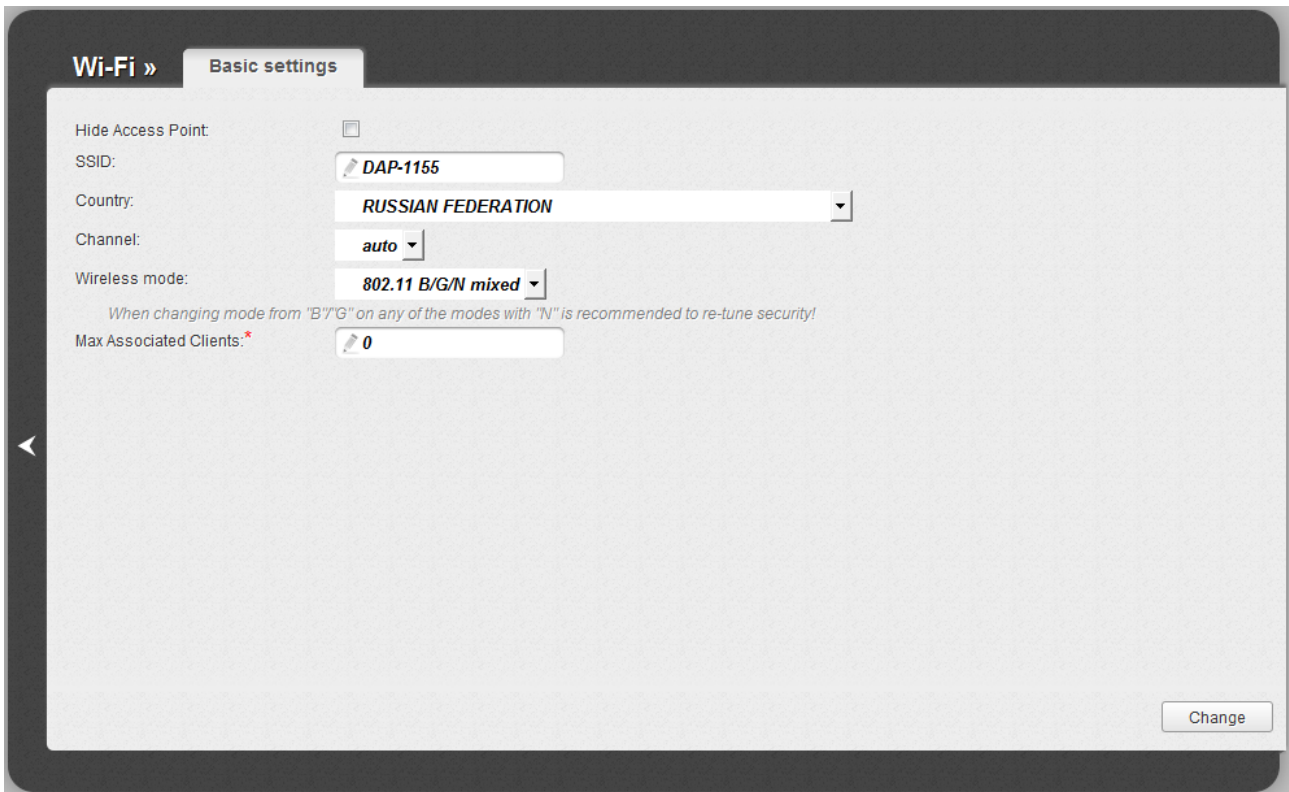


Figure 41. Basic settings of the wireless LAN.

Parameter	Description
Hide Access Point	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.)
SSID	A name for the WLAN. By default, the value DAP-1155 is specified. If your network is splitted into parts, each part has the default name (DAP-1155.2 , DAP-1155.3 , and DAP-1155.4). It is recommended to specify another name for the network upon initial configuration (use digits and Latin characters).
Country	The country you are in. Select a value from the drop-down list.
Channel	The wireless channel number. When the auto value is selected, the access point itself chooses the channel with the least interference.
Wireless mode	Operating mode of the wireless network of the access point. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
Max Associated Clients	The maximum number of devices connected to the wireless network of the access point. When the value 0 is specified, the device does not limit the number of connected clients.

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

Security Settings

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

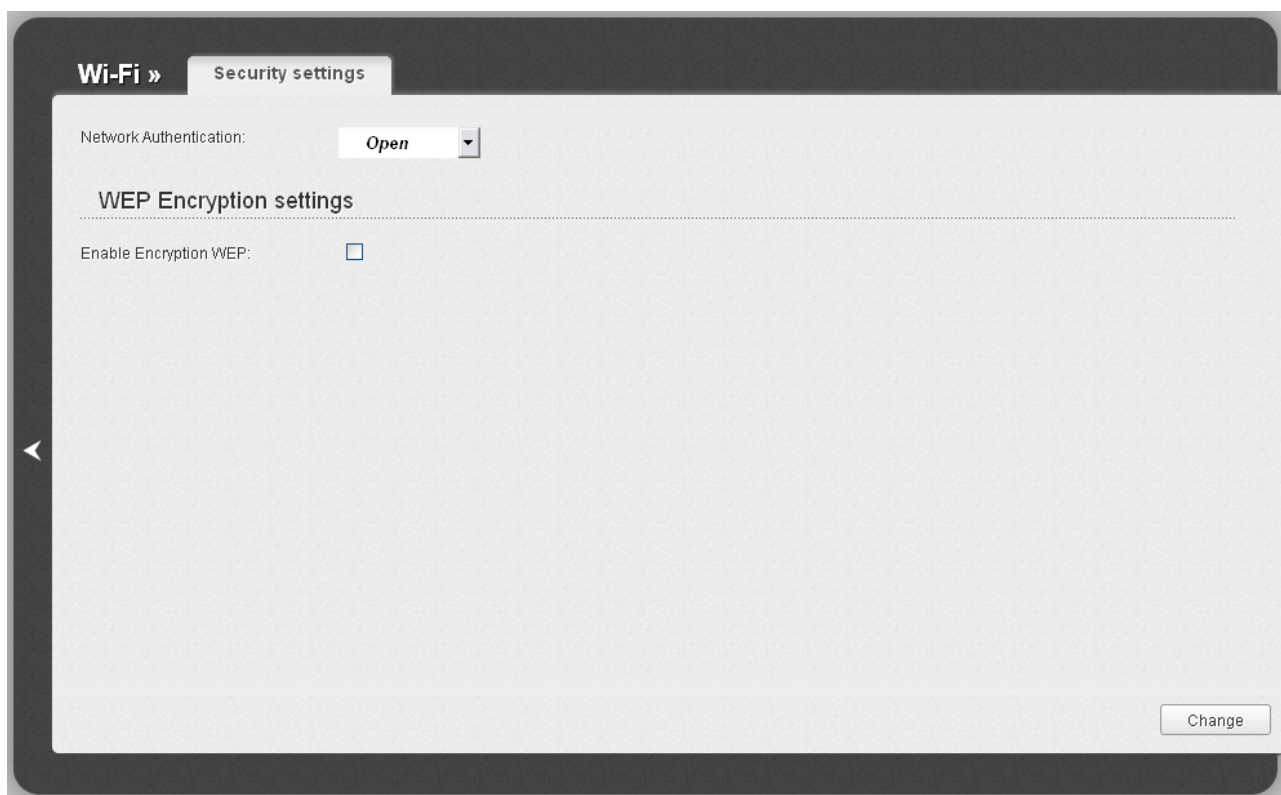


Figure 42. The default security settings.

By default, the **Open** network authentication type with no encryption is specified for the WLAN.

! The default security settings do not provide sufficient protection for the WLAN. Please, specify your own security settings for the WLAN (or each part of the WLAN if the network was splitted into parts).

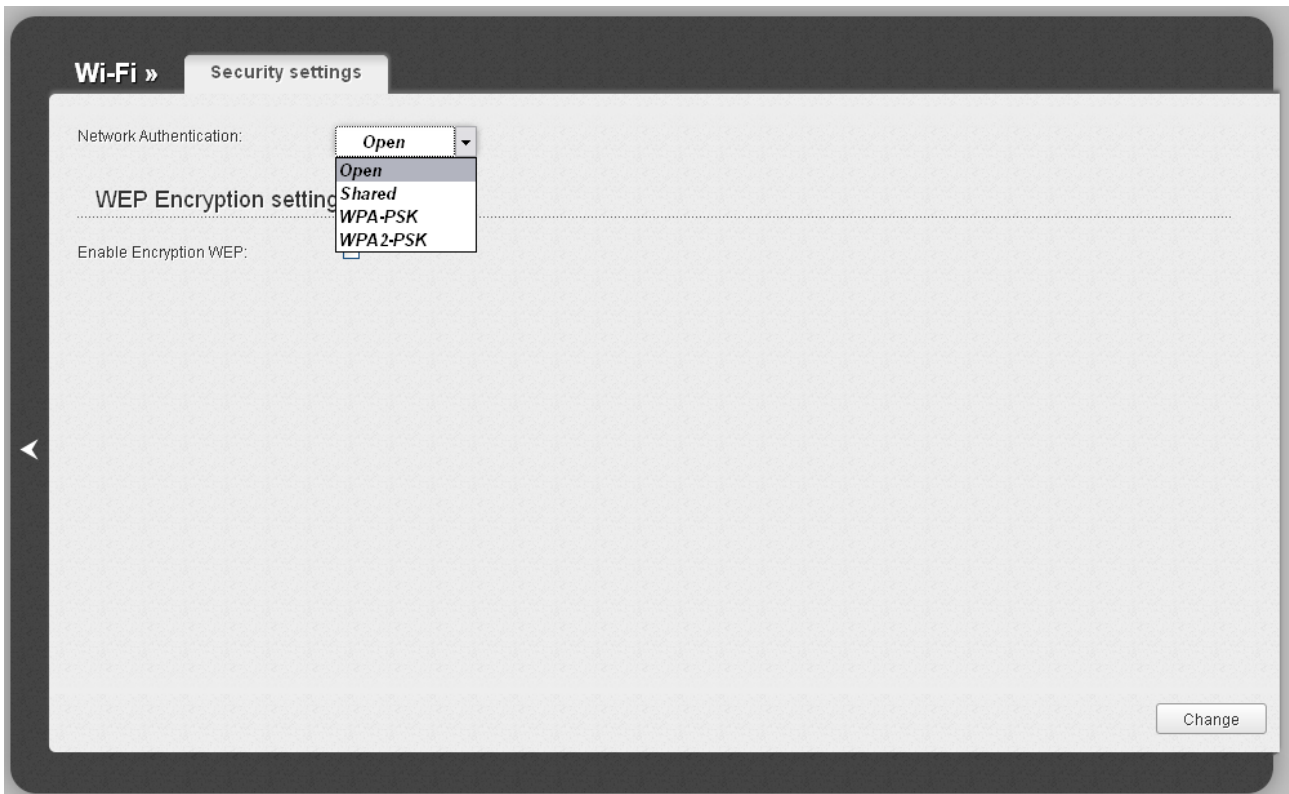


Figure 43. Network authentication types supported by the access point.

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-PSK	WPA-based authentication using a PSK.
WPA2-PSK	WPA2-based authentication using a PSK.

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):

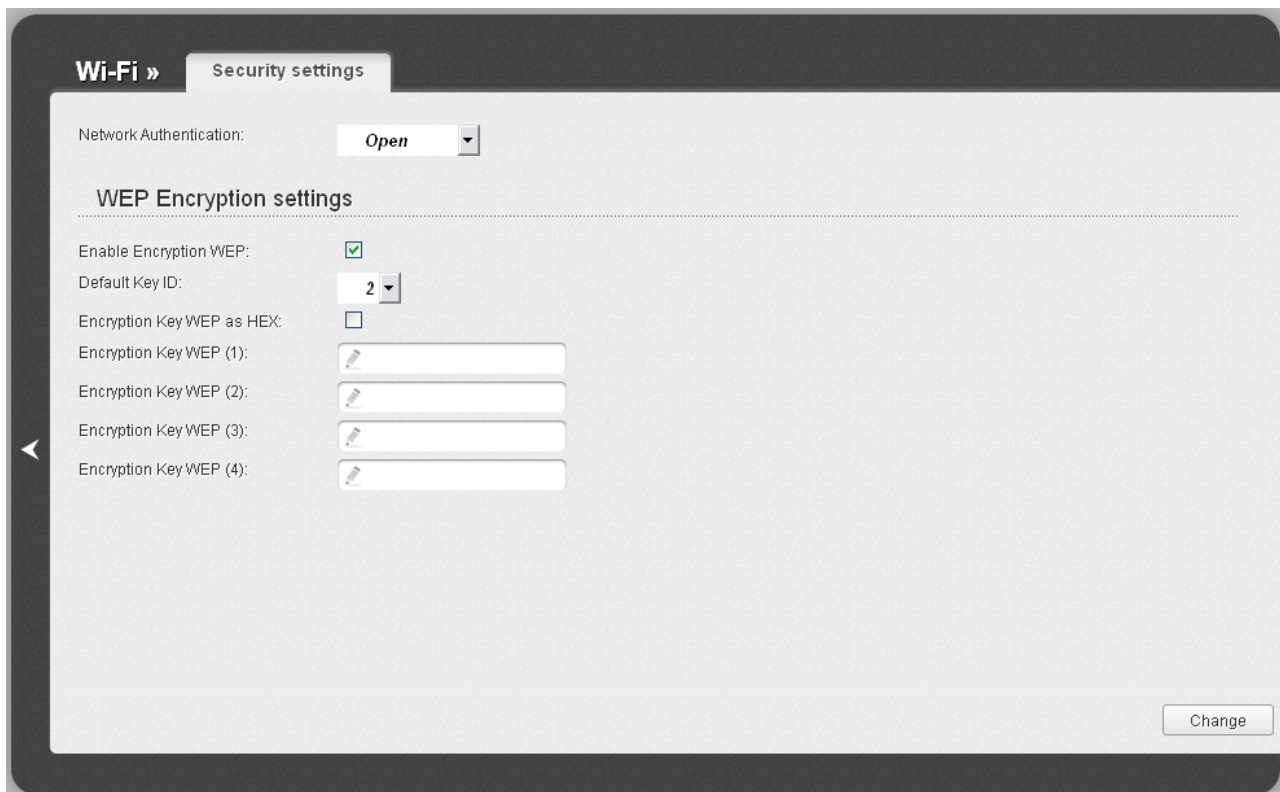


Figure 44. The **Open** value is selected from the **Network Authentication** drop-down list.

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, 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.
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. You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters). If the Encryption Key WEP as HEX checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F).

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

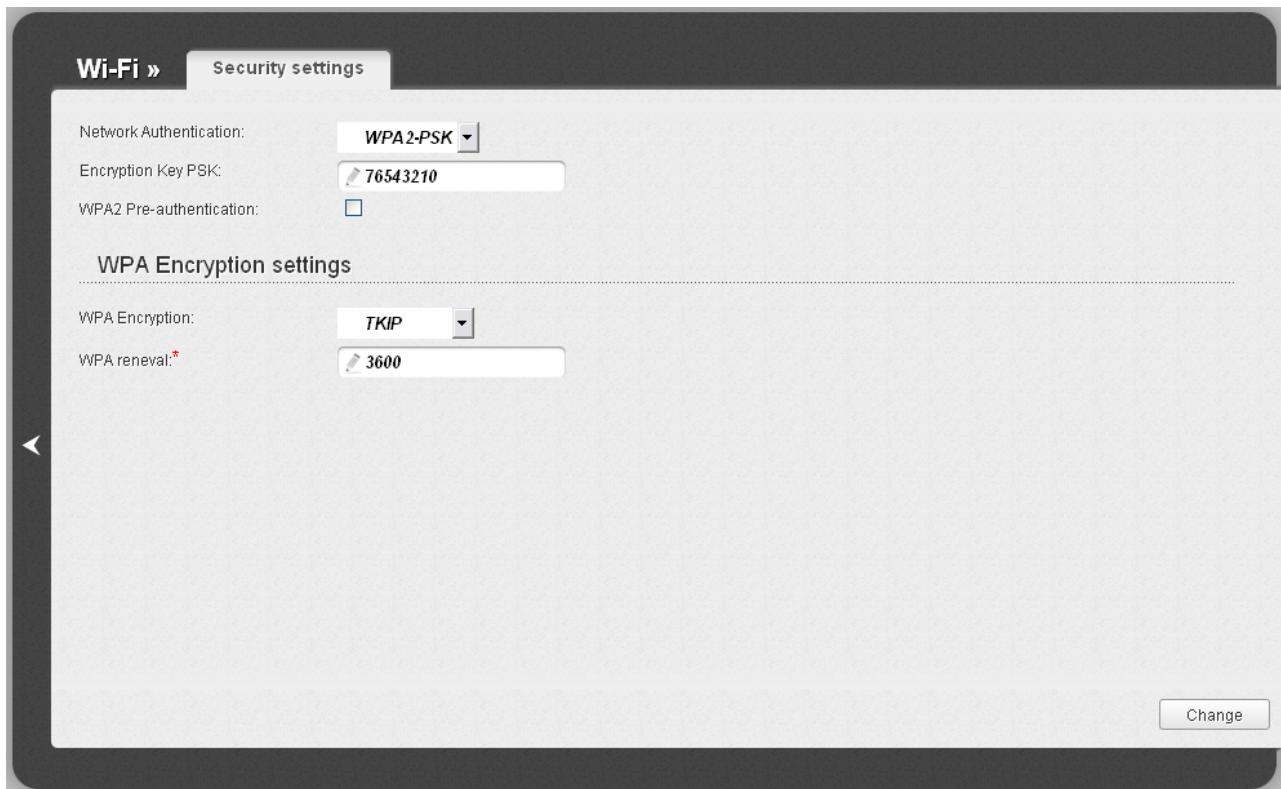


Figure 45. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
Encryption Key PSK	A key for WPA encryption. The key can contain digits and/or Latin characters.
WPA2 Pre-authentication	The checkbox activating preliminary authentication (displayed only for the WPA2-PSK authentication type).
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 **Change** button.

MAC Filter

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



Figure 46. The MAC filter for the wireless network.

By default, MAC filtering is not active (the **Disabled** choice of the **MAC filter restrict mode** radio button is selected).

To open your wireless network for the devices which MAC addresses are specified on the **MAC addresses** tab and to close the wireless network for all other devices, select the **Allow** choice of the **MAC filter restrict mode** radio button and click the **Change** button.

To close your wireless network for the devices which MAC addresses are specified on the **MAC addresses** tab, select the **Deny** choice of the **MAC filter restrict mode** radio button and click the **Change** button.

To add a MAC address to which the selected filtering mode will be applied, proceed to the **MAC addresses** tab.

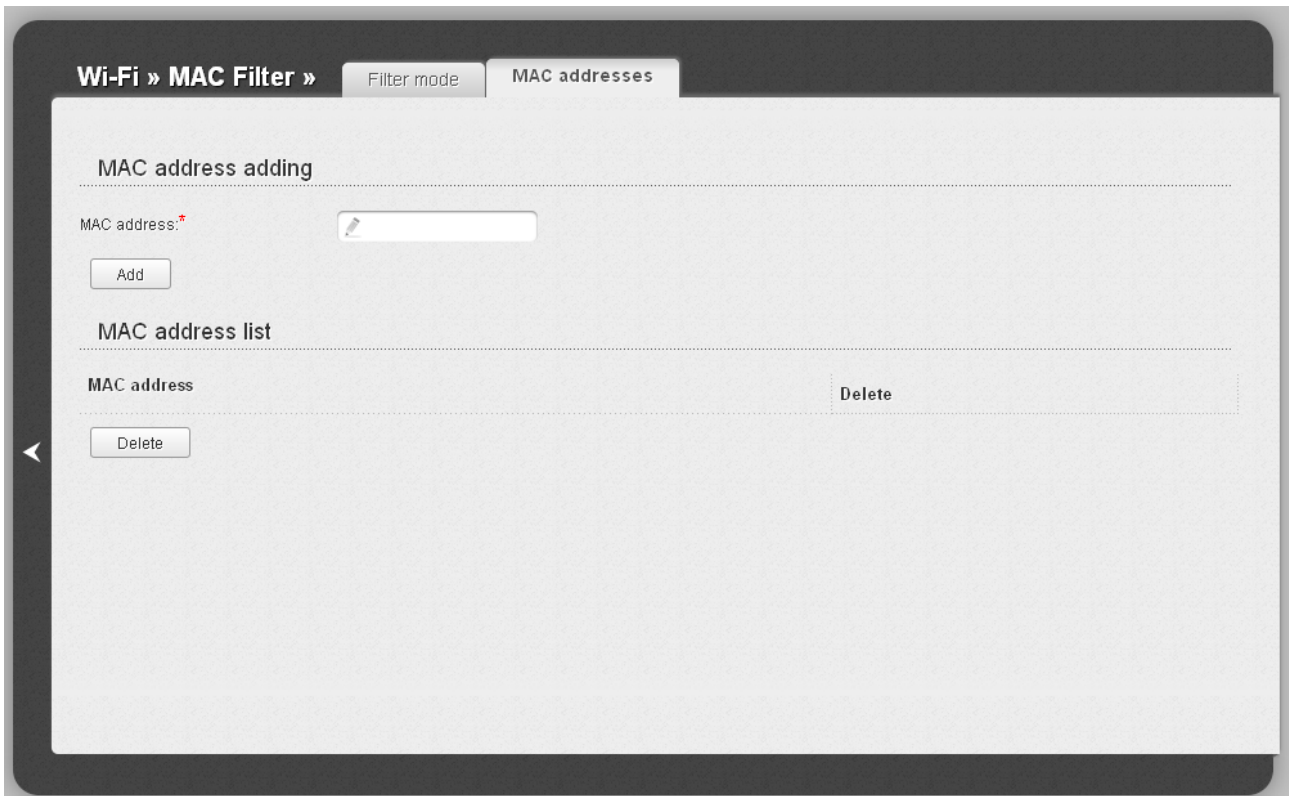


Figure 47. The tab for adding a MAC address.

Enter an address in the **MAC address** field of the **MAC address adding** section and click the **Add** button.

To remove a MAC address from the list of MAC addresses, select the checkbox located to the right of the relevant MAC address in the **MAC address list** section and click the **Delete** button.

Station List

On the **Wi-Fi / Station List** 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.

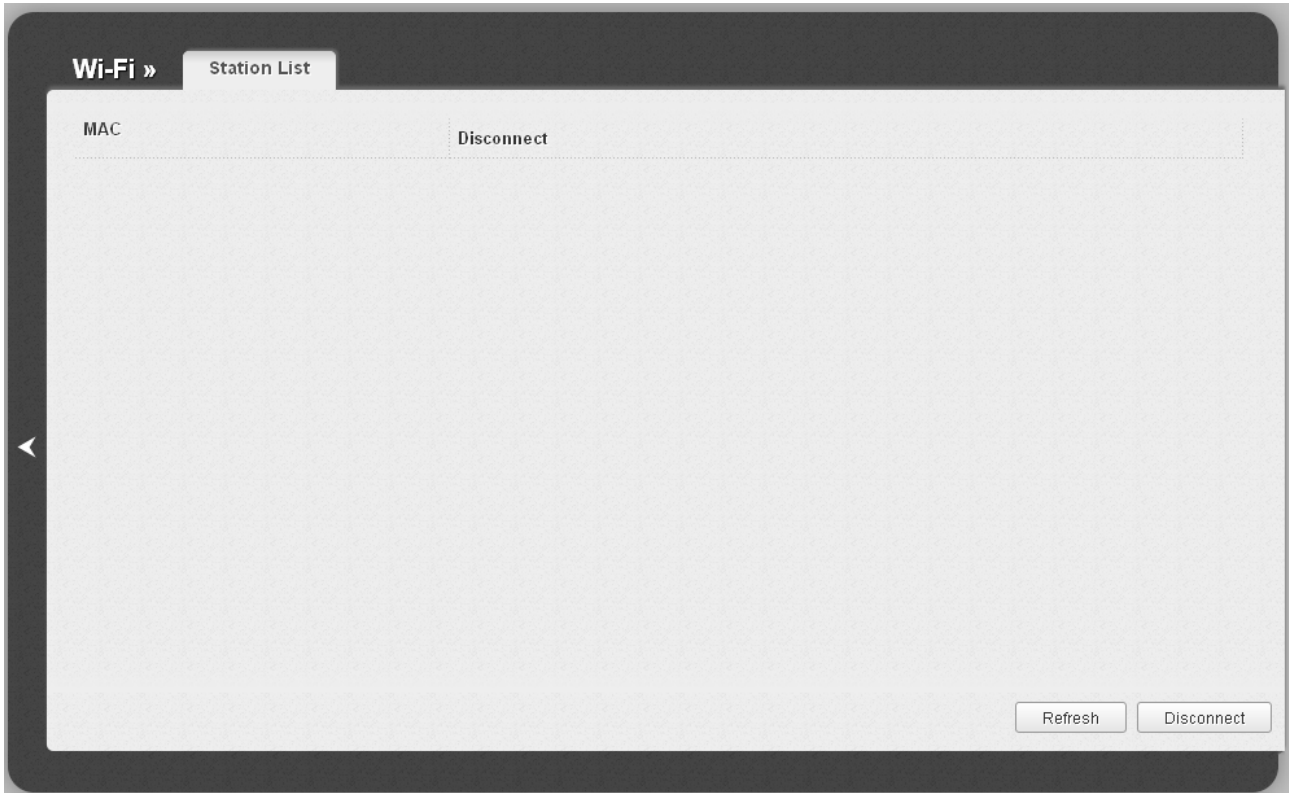


Figure 48. The list of the wireless clients.

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 access point's WLAN is splitted into parts (the value **2**, **3**, or **4** is selected from the **MBSSID** drop-down list on the **Wi-Fi / Common 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, **WPA-PSK** or **WPA2-PSK** with the **AES** or **TKIP+AES** encryption method (on the **Wi-Fi / Security settings** page).

Wi-Fi » WPS

Enable/Disable WPS

WPS Enable:

Change

Information

Default PIN code:

WPS Status: *Configured*

SSID: *DAP-1155*

Network Authentication: *WPAPSK*

Encryption: *AES*

Encryption key: *76543210*

Refresh Reset to unconfigured

Connection

WPS Method: **PBC**

Connect

Figure 49. The page for configuring the WPS function.

To activate the WPS function, select the **WPS Enable** checkbox and click the **Change** 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) • Unconfigured (you need to specify the relevant settings).
SSID	The name of the access point's WLAN (or the first part of the WLAN if the network is splitted 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 **Change** 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 **Change** 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 **Change** button.
4. Save the settings and close the web-based interface (click the **Save** line in the top-page menu displayed when the mouse pointer is over the **System** caption, then click the **Logout** line).

Later you will be able to add wireless devices to the WLAN by pressing the **WPS/RESET** 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/RESET** button of the access point and immediately release it.

After clicking the button the **WPS** LED blinks green. If the wireless device has been successfully connected to the WLAN, the LED stops blinking and lights green for several minutes.

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.

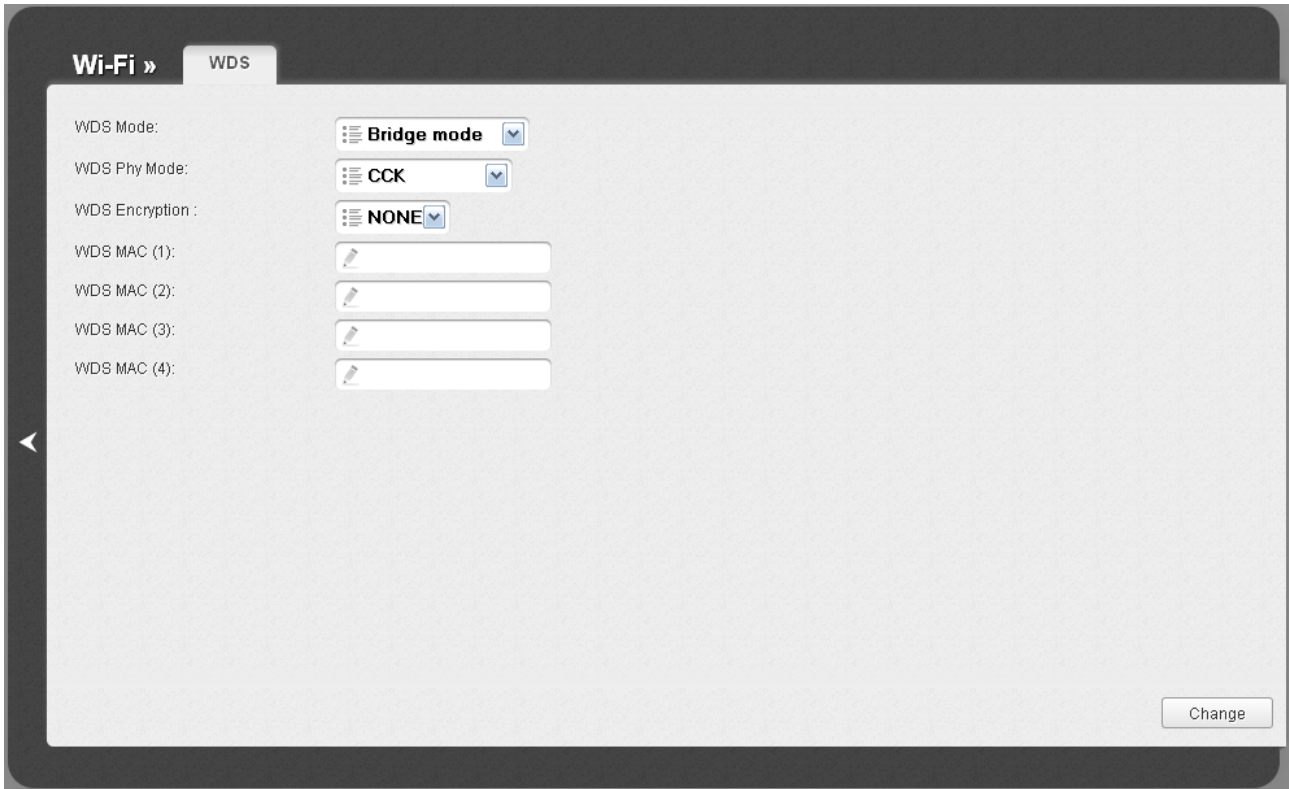


Figure 50. The page for configuring the WDS function.

The following fields are available on the page:

Parameter	Description
WDS Mode	<p>The WDS function mode.</p> <p>Disable: The function is disabled.</p> <p>Bridge mode: Access points communicate to each other only, wireless devices cannot connect to them.</p> <p>Repeater mode: Access points communicate to each other, wireless clients can connect to the WLAN created by interconnected access points.</p>
WDS Phy Mode	<p>A physical mode of data transfer between access points interconnected via the WDS function.</p> <p>CCK: 802.11b devices only.</p> <p>OFDM: 802.11g devices only.</p> <p>HTMIX: 802.11g and 802.11n devices.</p> <p>GREENFIELD: 802.11n devices only.</p>
WDS Encryption	<p>A type of encryption for data transfer between access points interconnected via the WDS function.</p> <p>NONE: No encryption.</p> <p>WEP.</p> <p>TKIP.</p> <p>AES.</p>
Encryption Key	<p>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 displayed.</p>
WDS MAC (1-4)	<p>The MAC addresses of devices connected to the access point via the WDS function.</p>



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

When you have configured the parameters, click the **Change** 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 51. 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.
BG Protection	<p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <p>Auto: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices).</p> <p>Always On: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</p> <p>Always Off: The protection function is always disabled.</p>
Bandwidth	<p>The channel bandwidth for 802.11n devices.</p> <p>20MHz: 802.11n devices operate at 20MHz channels.</p> <p>40MHz: 802.11n devices operate at 40MHz channels.</p> <p>20/40MHz -: 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the previous adjacent channel).</p> <p>20/40MHz +: 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the next adjacent channel).</p>
TX Preamble	<p>This parameter defines the length of the CRC block sent by the access point when communicating to wireless devices.</p> <p>Select a value from the drop-down list.</p> <p>Long Preamble.</p> <p>Short Preamble (this value is recommended for networks with high-volume traffic).</p>

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

The screenshot shows the WMM configuration interface. At the top, 'WMM' is checked. Below are two sections: 'Parameters of Access Point' and 'Parameters of Station'. Each section contains a table with columns for AC, Aifsn, CWMin, CWMax, Txop, ACM, and Ack. The 'Change' button is at the bottom right.

Parameters of Access Point						
AC	Aifsn	CWMin	CWMax	Txop	ACM	Ack
AC_BK	7	1	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

Parameters of Station					
AC	Aifsn	CWMin	CWMax	Txop	ACM
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

Figure 52. 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 selected, 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 not selected, the access point answers requests. If selected, the access point does not answer requests.

When you have configured the parameters, click the **Change** 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-1155 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-1155 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-1155 and the remote access point. Other parameters of the wireless network of DAP-1155 do not depend upon the settings of the remote access point.

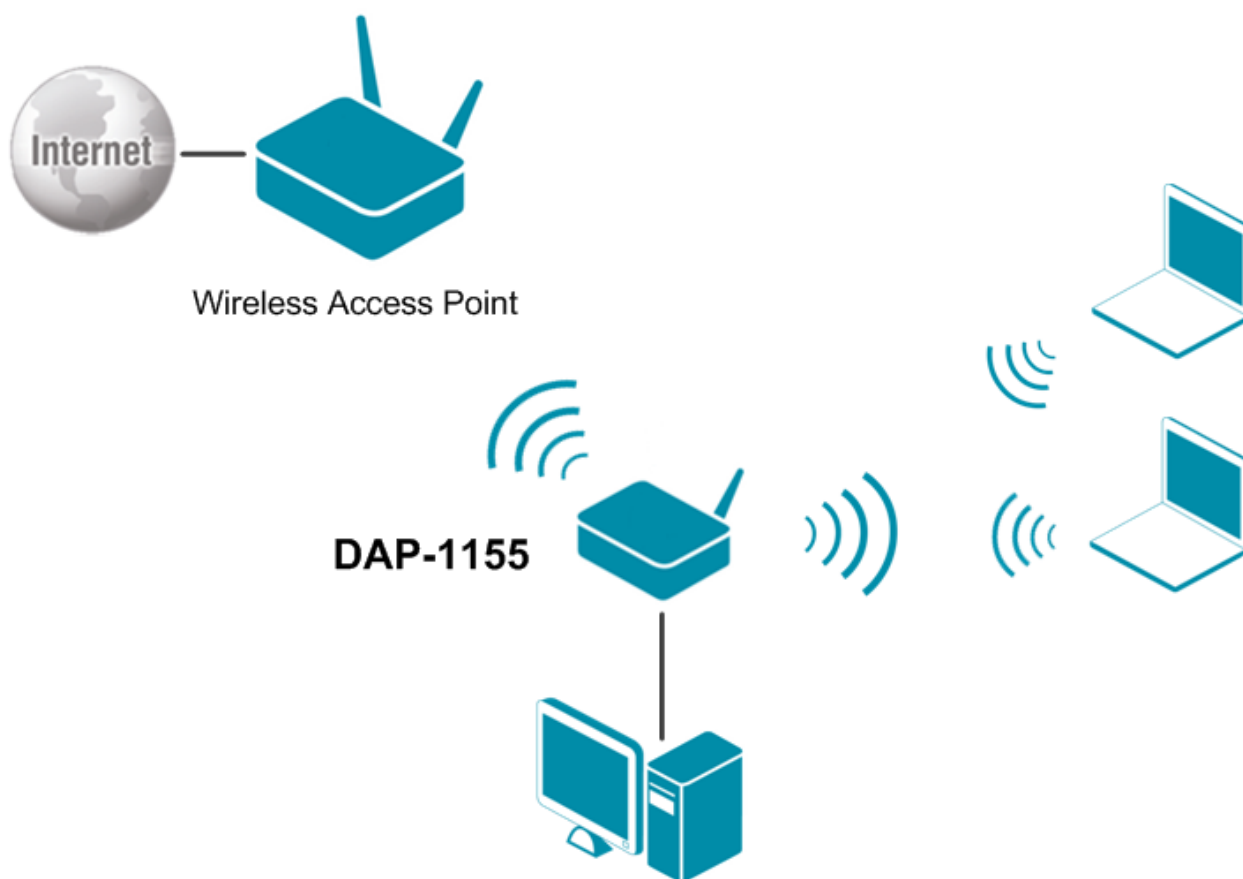


Figure 53. Connecting DAP-1155 in the access point mode as a client.

To allow the devices from the LAN of DAP-1155 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 **Save** button.

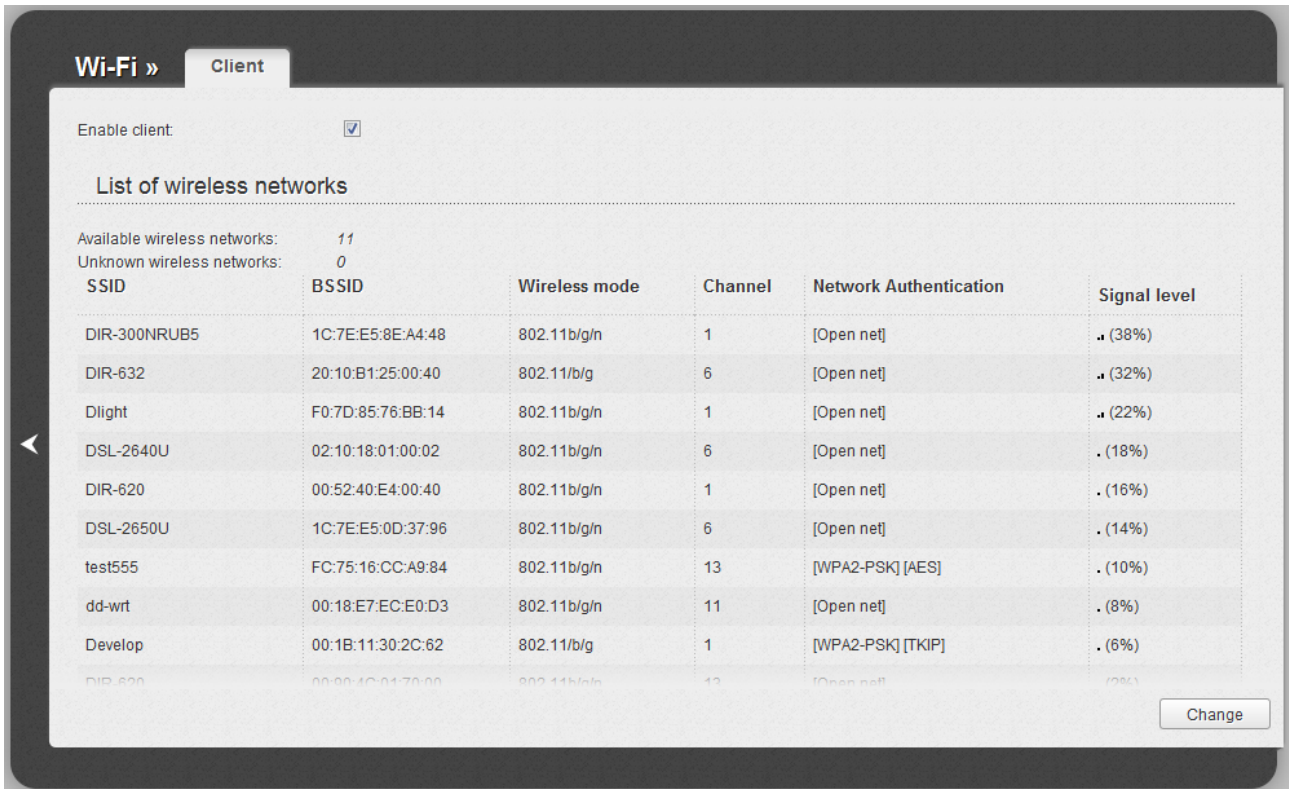


Figure 54. The page for configuring the client mode.

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
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 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 (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. You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters).

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

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

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

In addition, when the **Enable client** checkbox is selected, the list of available wireless networks is displayed on the page. The **Unknown wireless networks** field shows the number of hidden wireless networks.

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 **Change** 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, fill in 4 **Encryption Key WEP** fields, and click the **Change** 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 **Change** button.

After clicking the **Change** button, the wireless channel of DAP-1155 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.

Firewall

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

MAC Filter

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

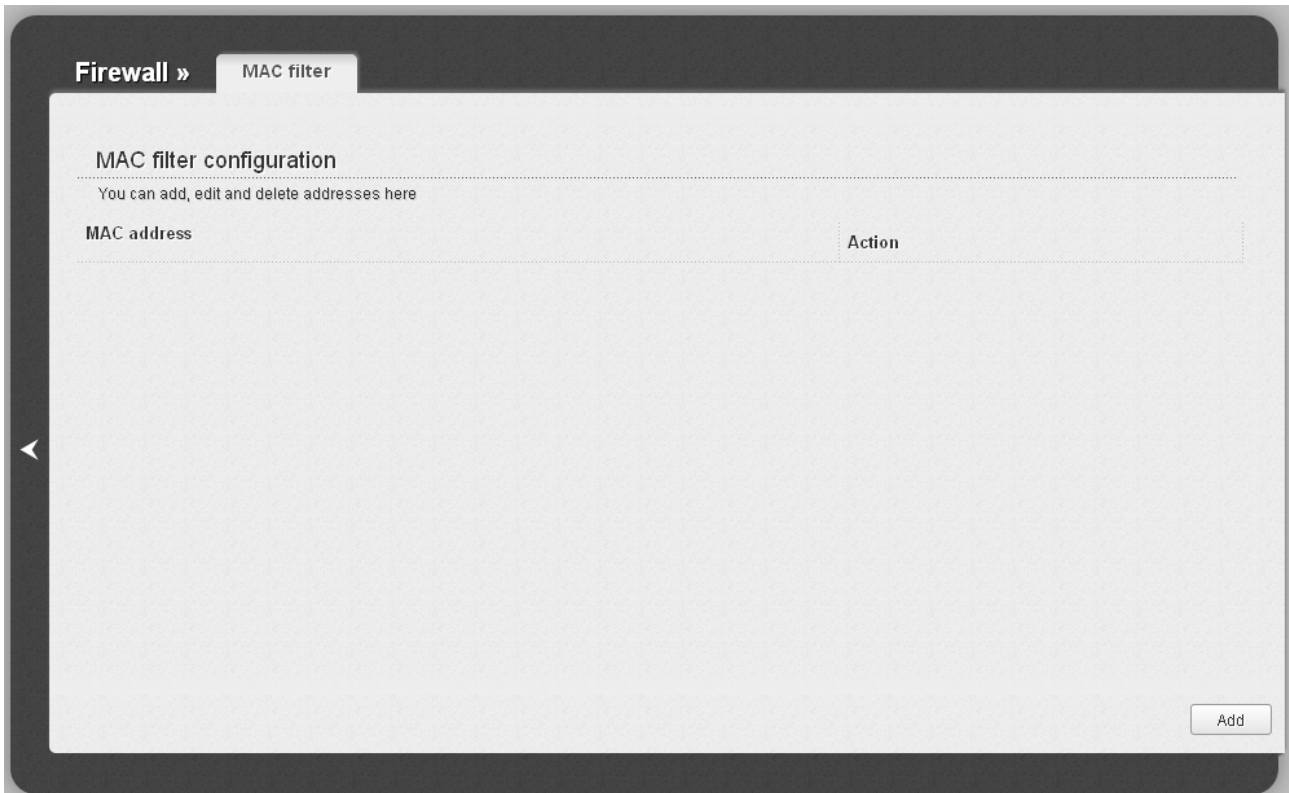


Figure 55. The **Firewall / MAC filter** page.

To specify a new address for the MAC filter, click the **Add** button.

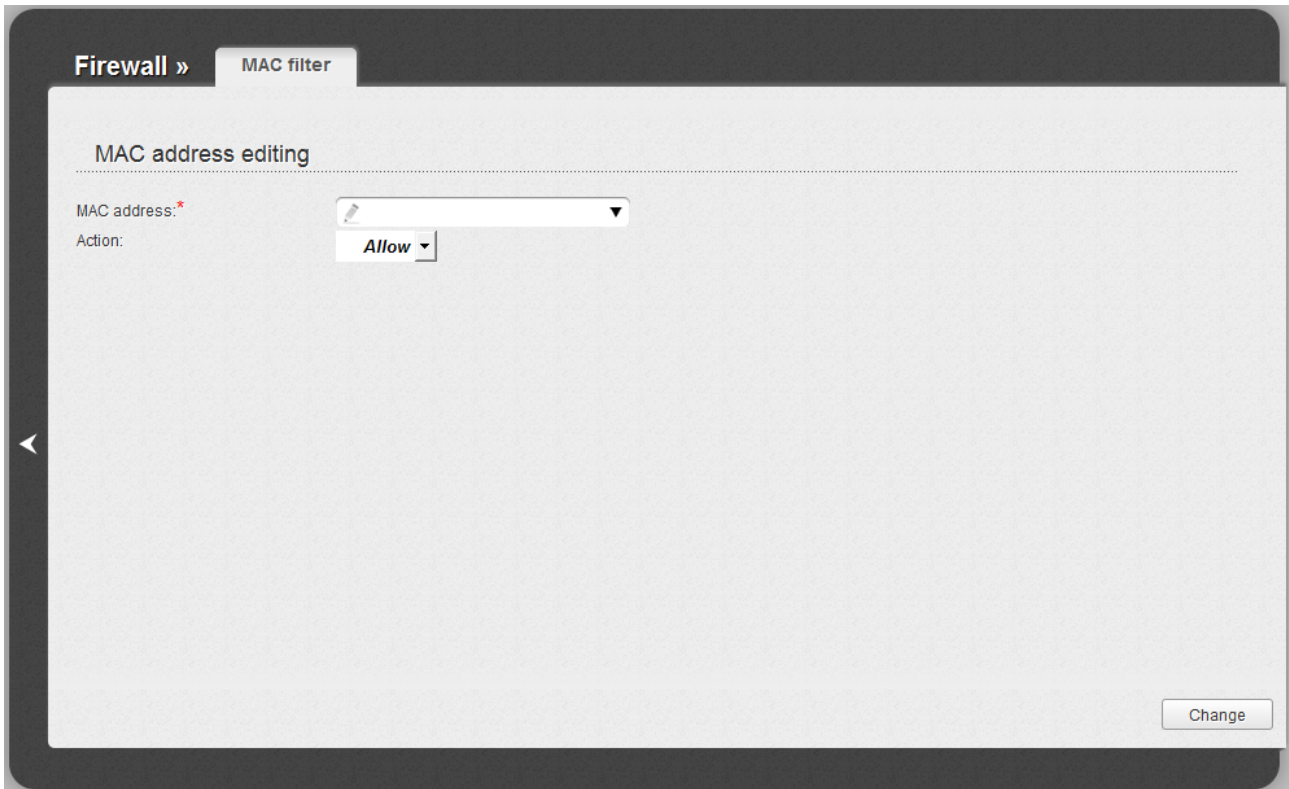


Figure 56. The page for adding an address for the MAC filter.

On the opened page, enter the MAC address of the device from the access point's LAN in the **MAC 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). Then select the **Deny** value from the **Action** drop-down list and click the **Change** button.

To remove an address from the list of MAC addresses for filtering, select the line with the relevant MAC address. On the opened page, click the **Delete** button.

System

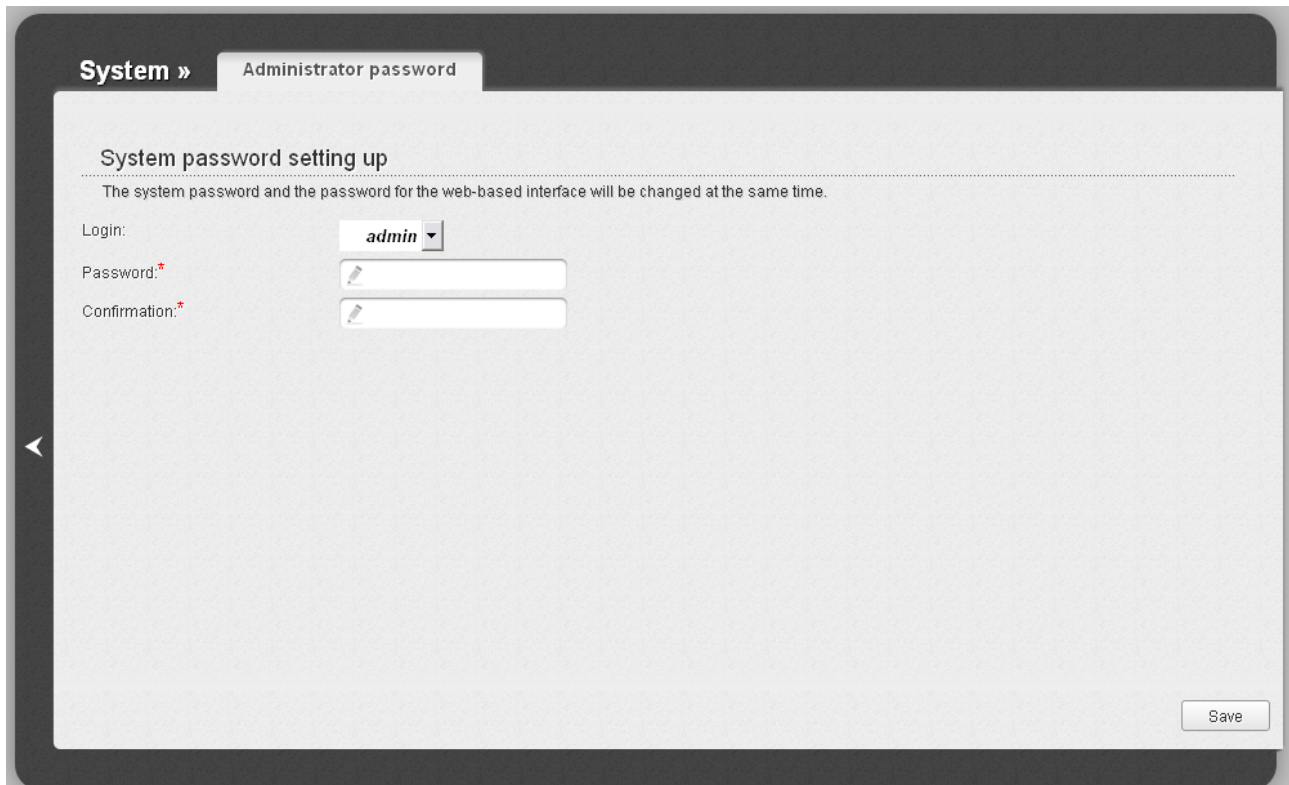
In this menu you can do the following:

- change the password used to access the access point's settings
- save the current settings to the non-volatile memory
- 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
- check availability of a host on the Internet through the web-based interface of the access point
- 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.



The screenshot shows a web-based configuration page for the administrator password. The page has a dark header with 'System »' and 'Administrator password'. The main content area is light gray and contains the following elements:

- System password setting up**: A section header.
- The system password and the password for the web-based interface will be changed at the same time.**: A note.
- Login:**: A dropdown menu with 'admin' selected.
- Password:***: A text input field with a password icon.
- Confirmation:***: A text input field with a password icon.
- Save**: A button in the bottom right corner.

Figure 57. The page for modifying the administrator password.

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

Configuration

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

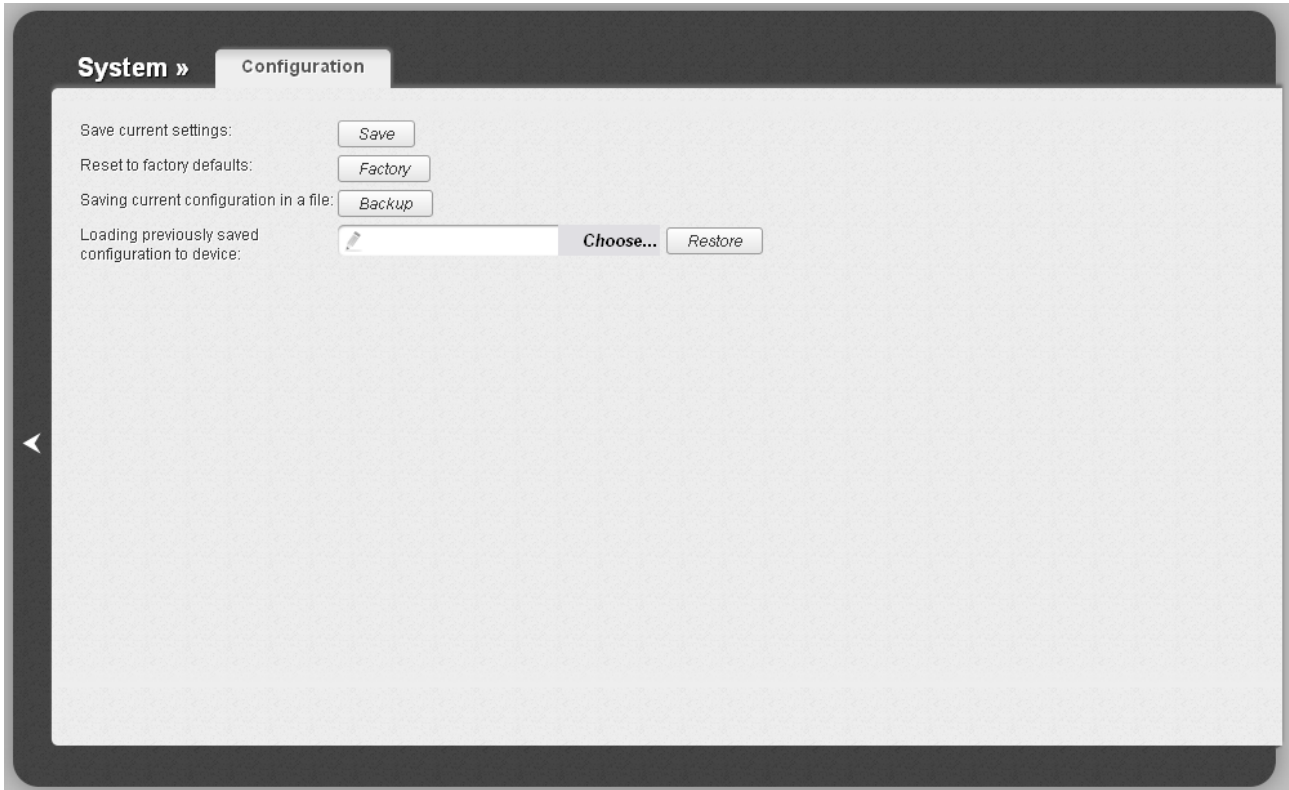


Figure 58. The **System / Configuration** page.

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.
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware WPS/RESET button (see the <i>Saving and Restoring Settings</i> section, page 37).
Backup	Click the button and follow the dialog box appeared to save the configuration (all settings of the access point) to your PC.
Restore	Click the button to upload a previously saved configuration (all settings of the access point) from a file on your PC. Click the Choose/Browse ¹ button to select a previously saved configuration file located on your PC.

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

¹ The name of the button depends upon the web browser that you use.

System Log

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

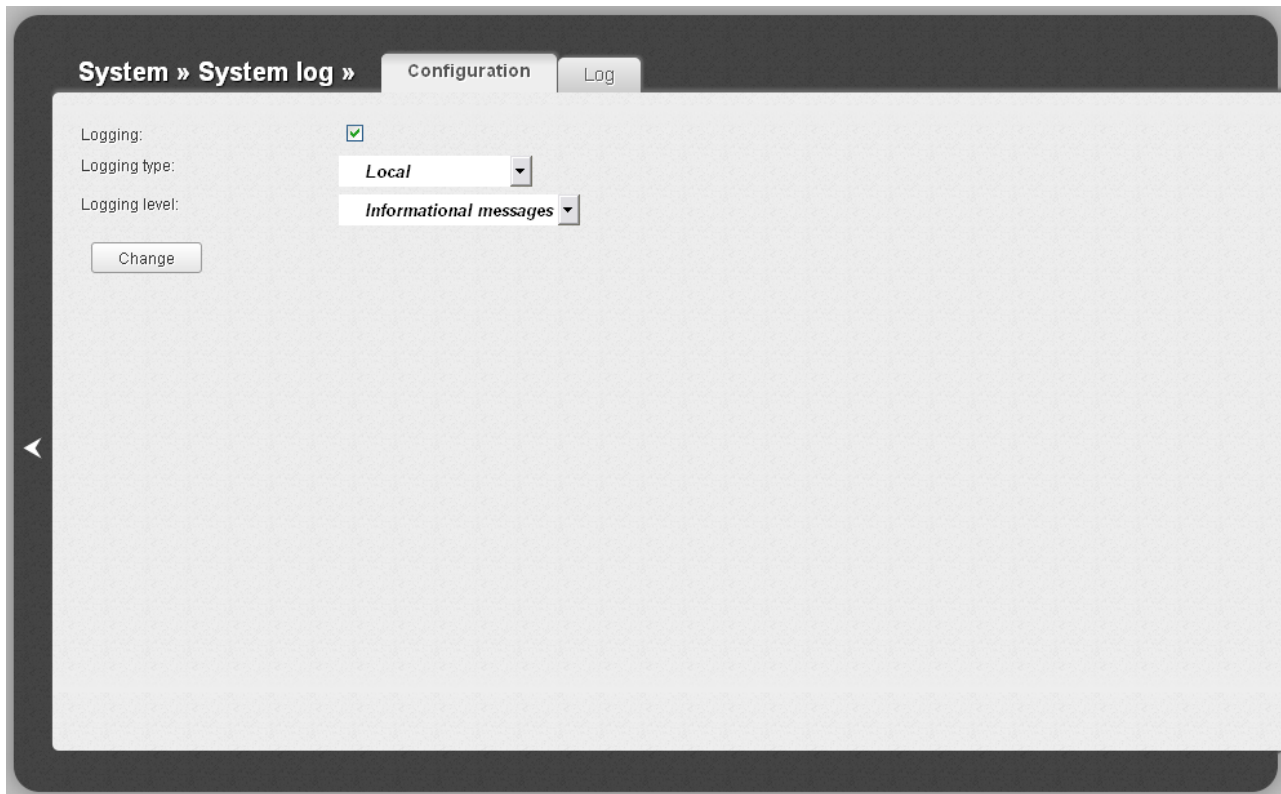


Figure 59. The **System / System log** page. The **Configuration** tab.

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

Control	Description
Logging type	Select a type of logging from the drop-down list. <ul style="list-style-type: none"> • Local: the system log is stored in the device's memory (and displayed on the Log tab). 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 Log tab) 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 **Change** button.

To disable logging of the system events, deselect the **Logging** checkbox and click the **Change** button.

On the **Log** tab, the events specified in the **Logging level** list are displayed.

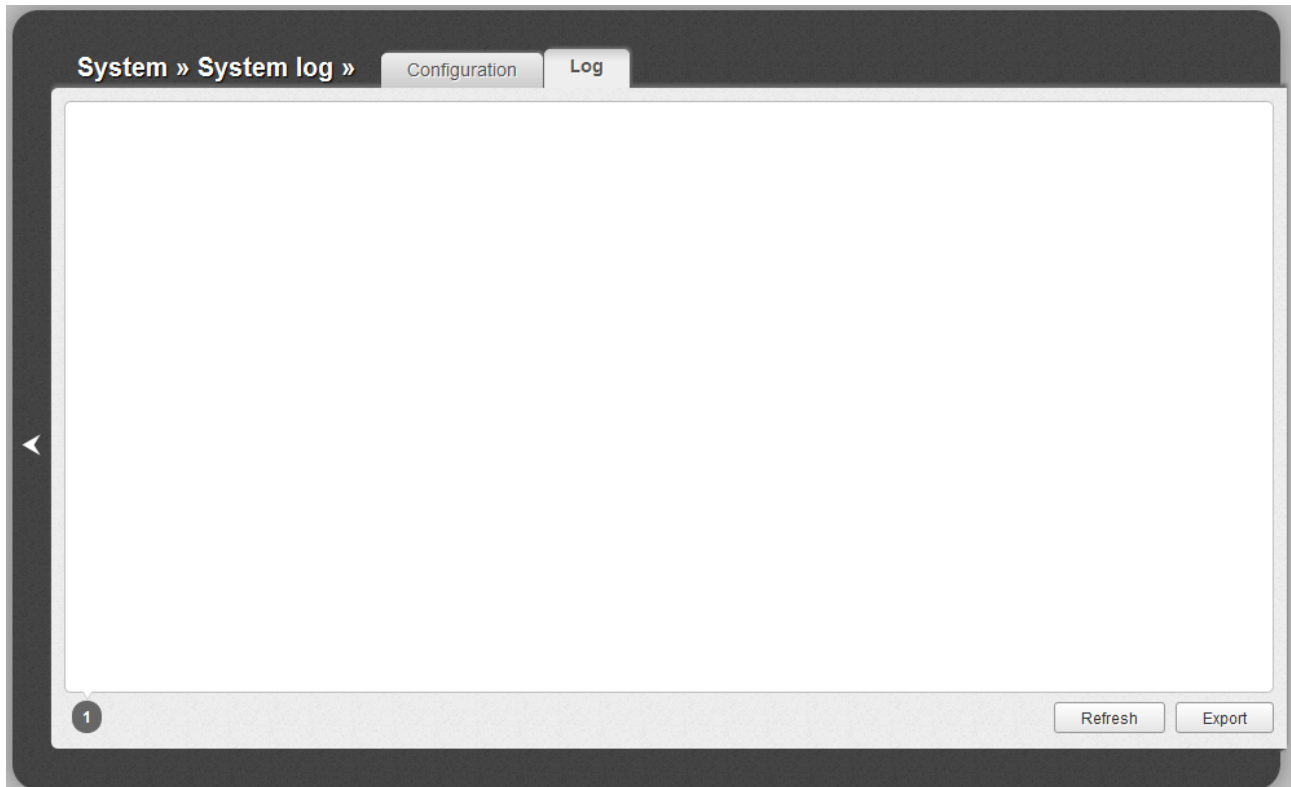


Figure 60. The **System / System log** page. The **Log** tab.

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

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

Firmware Upgrade

On the **System / Firmware upgrade** page, you can upgrade the firmware of the access point.

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

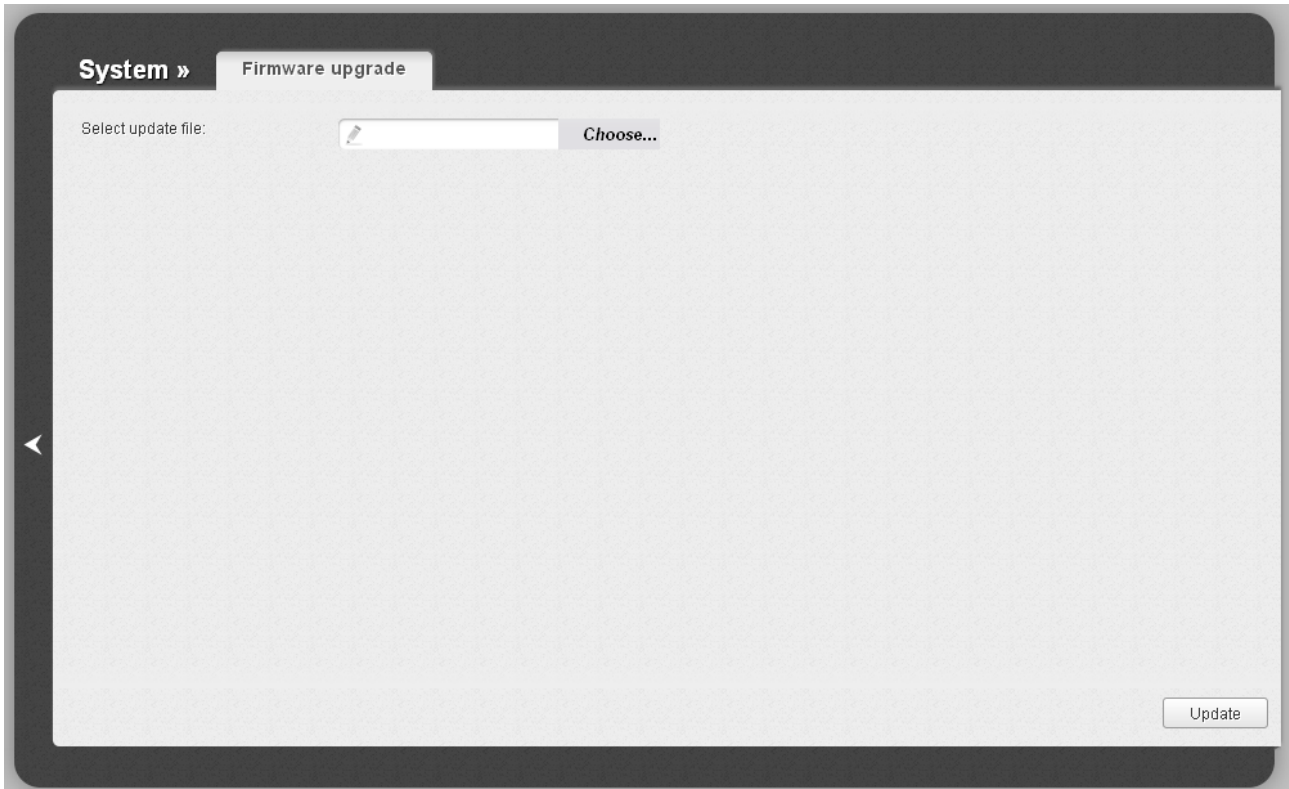


Figure 61. The **System / Firmware upgrade** page.

The current version of the access point's firmware is displayed in the **Firmware version** field located next the D-Link logo in the top left corner of the page. If you need to install a newer version of the firmware, follow the next steps:

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

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **Choose/Browse**² 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.

² The name of the button depends upon the web browser that you use.

6. Select the **Factory** line in the top-page menu displayed when the mouse pointer is over the **System** caption.
7. Wait until the access point is rebooted. Log into the web-based interface, using the default IP address, login and password (**192.168.0.50**, **admin**, **admin**).

Ping

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

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



Figure 62. 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 **Ping** button. The check results will be displayed in the **Log** field.

Also you can run the Ping function in the background mode. To do this, select the **Background ping** checkbox. Then enter the IP address or name of a host in the **Host** field and click the **Ping** button. When this mode is selected, the **Count of packets** and **Log** fields are not displayed.

In the background mode, the Ping utility sends requests to the host specified in the **Host** field every 40 seconds. The **Background ping status** light shows the status of the Ping function (green light: the function is running, red light: the function is not running).

To stop running the Ping function in the background mode, deselect the **Background ping** checkbox, enter the IP address or name of a host in the **Host** field, and click the **Ping** button.

Telnet

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



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

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

Device mode

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

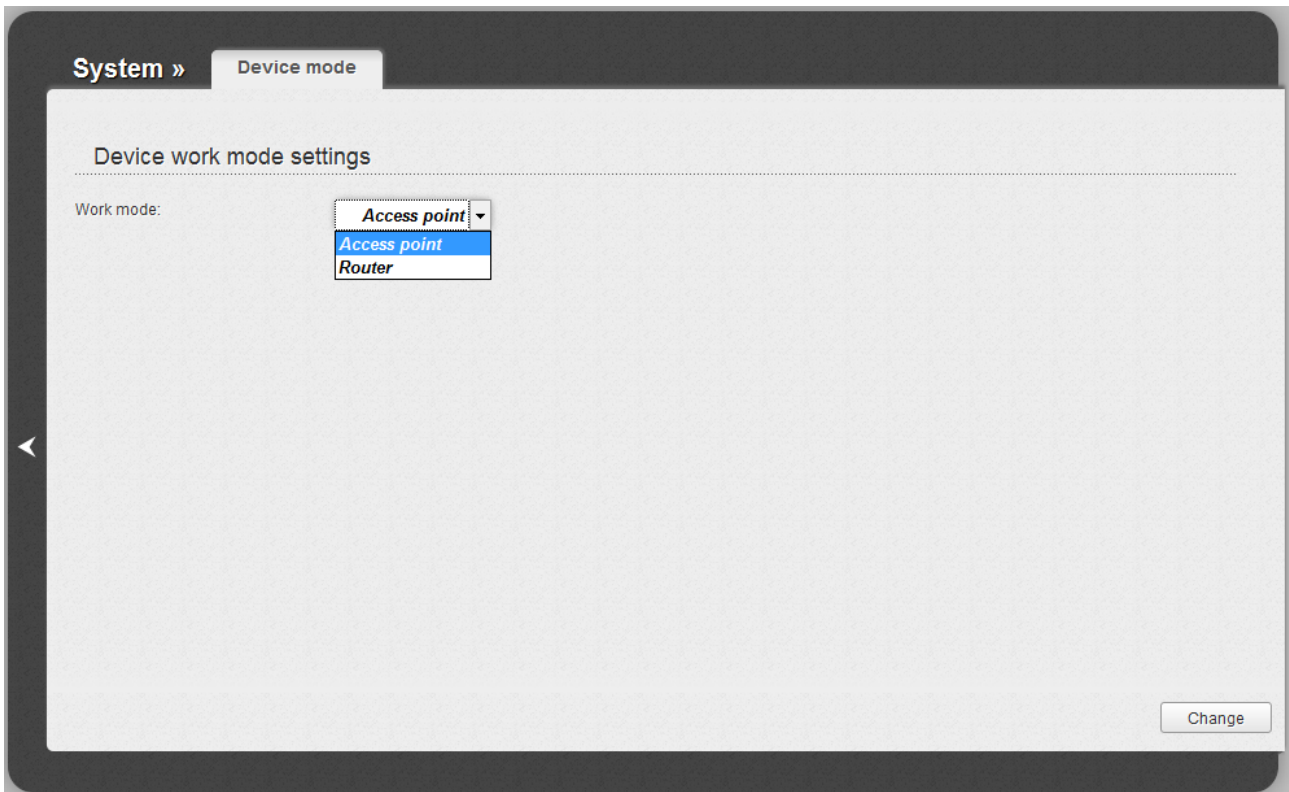


Figure 64. The page for changing the operating mode of the device.

To switch the device to the other mode, select the **Router** value from the **Work mode** drop-down list and click the **Change** 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)

Click'n'Connect

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

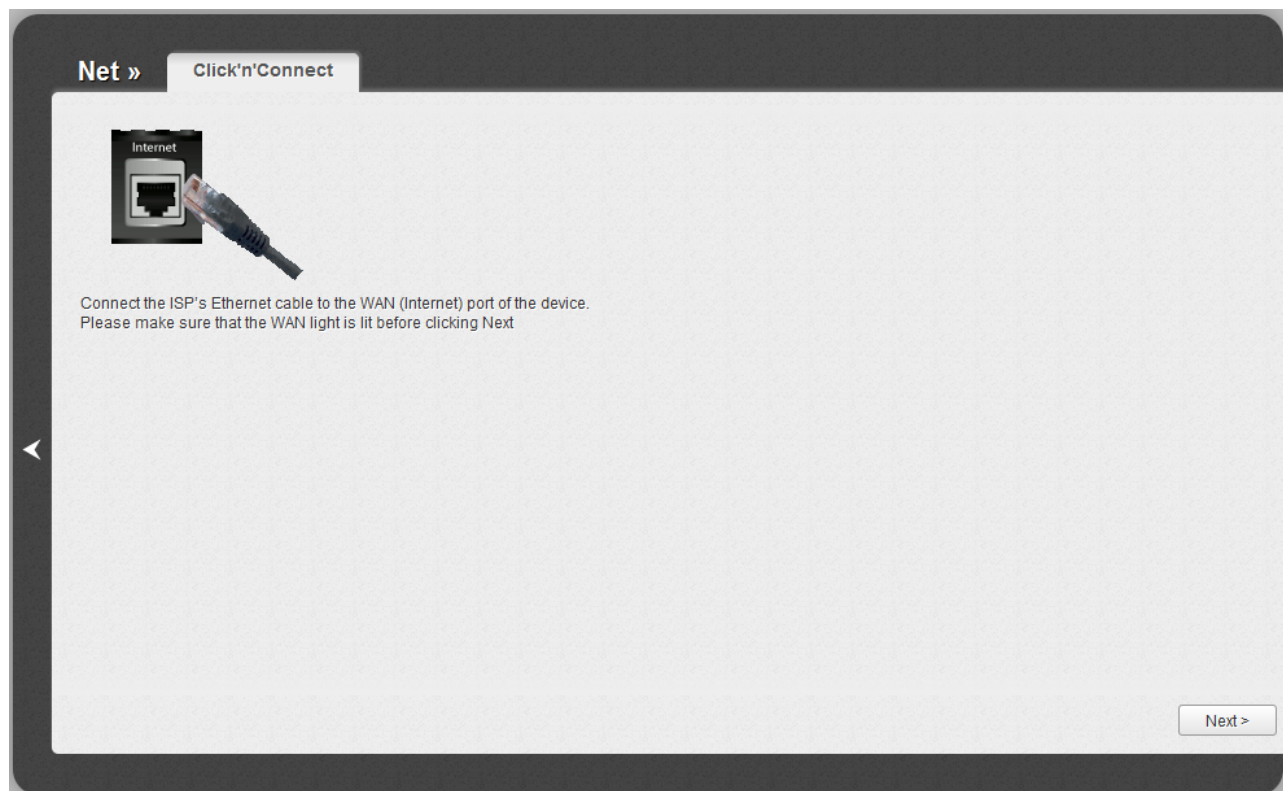


Figure 65. Configuring connection to the Internet.

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.

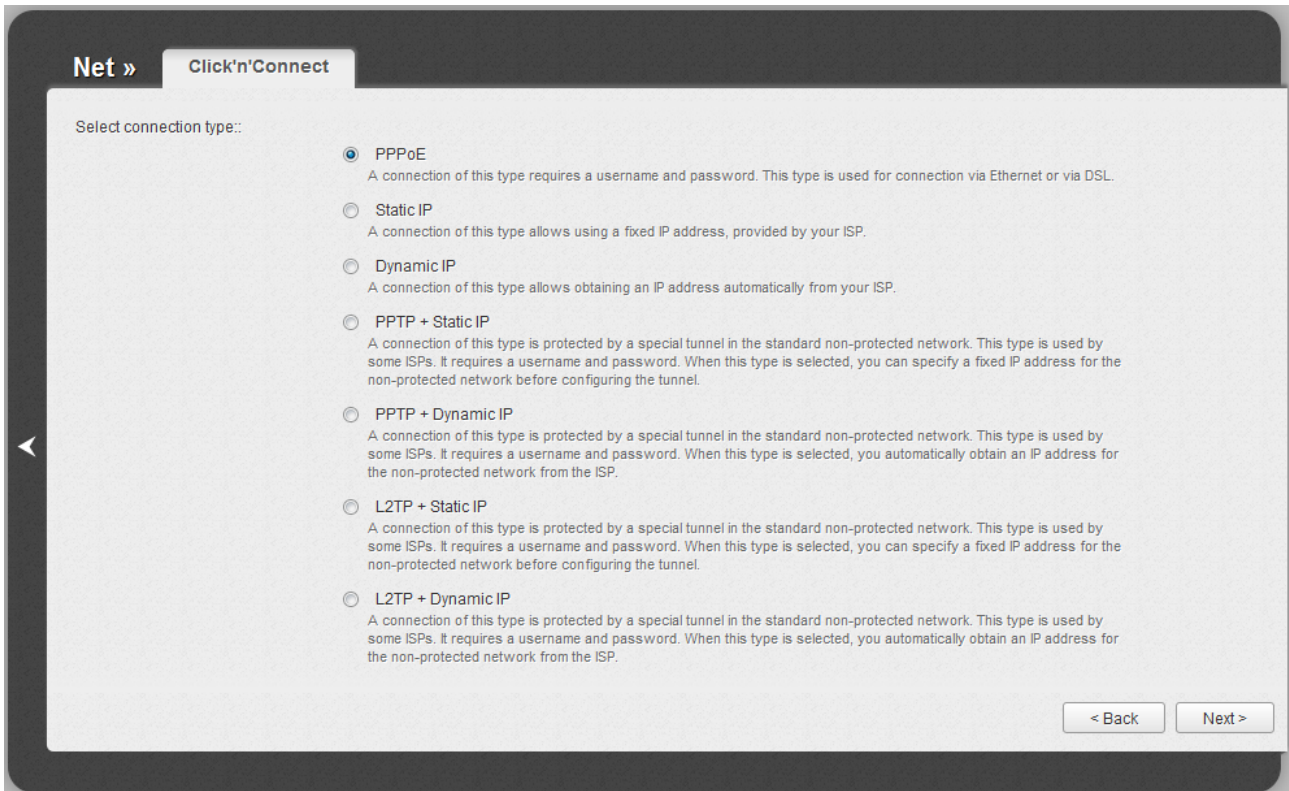


Figure 66. The page for selecting the connection type.

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

Creating WAN Connection

PPPoE Connection

The screenshot shows a web-based configuration interface for creating a WAN connection. At the top, there is a breadcrumb 'Net »' and a tab 'Click'n'Connect'. Below this, there are four input fields: 'Connection name:*' with the value 'pppoe_WAN_1', 'Username:*', 'Password:*', and 'Password confirmation:*'. Each field has a small icon to its left. At the bottom left, there is a switch labeled 'Brief' and a yellow tooltip that says 'Use this switch to enter or exit the expert mode.' At the bottom right, there are two buttons: '< Back' and 'Next >'. A left-pointing arrow is visible on the left side of the interface.

Figure 67. 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.

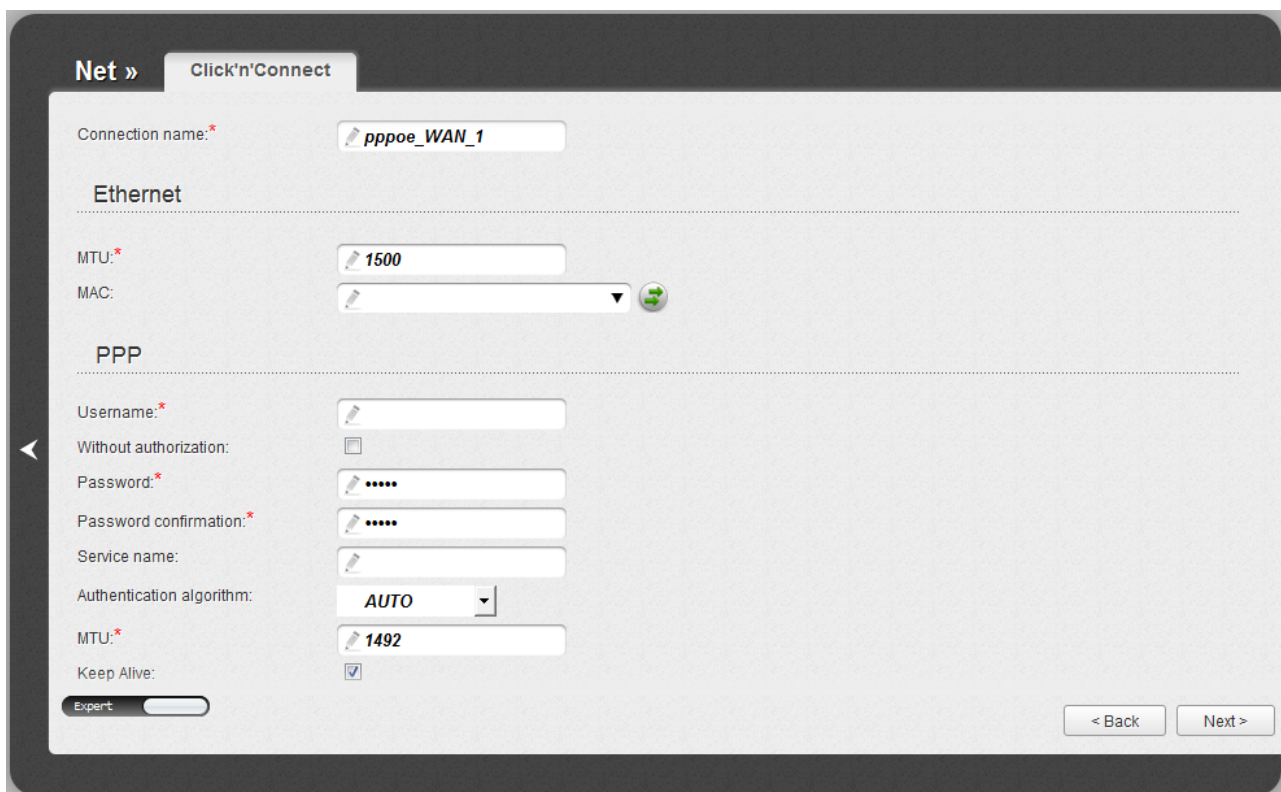



Figure 68. Configuring PPPoE WAN connection. The expert settings mode. The **Ethernet** section.

Parameter	Description
Connection name	A name for connection for easier identification.
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 button () 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>

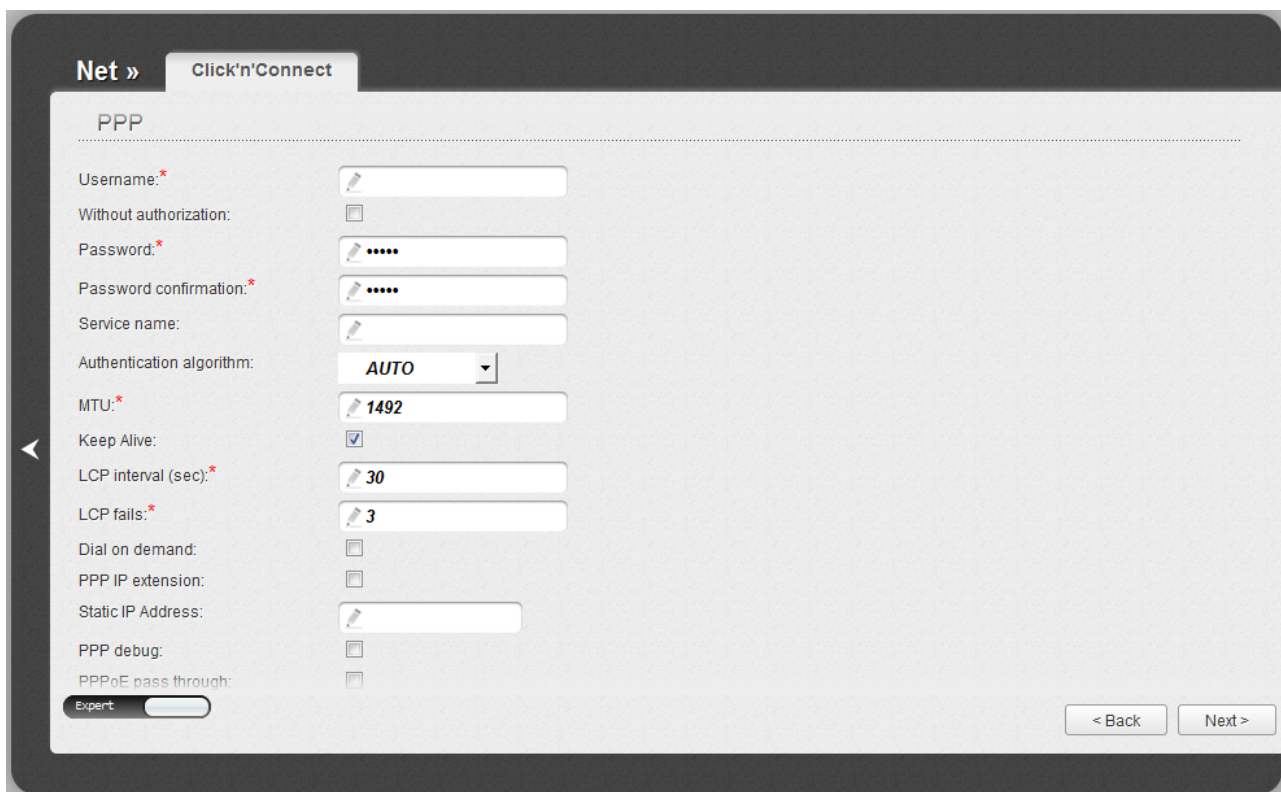


Figure 69. Configuring PPPoE WAN connection. The expert settings mode. The **PPP** section.

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.

Parameter	Description
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.
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.
PPPoE pass through	Select the checkbox if you want to allow PPPoE clients of computers from your LAN to connect to the Internet through this PPPoE connection of the access point.

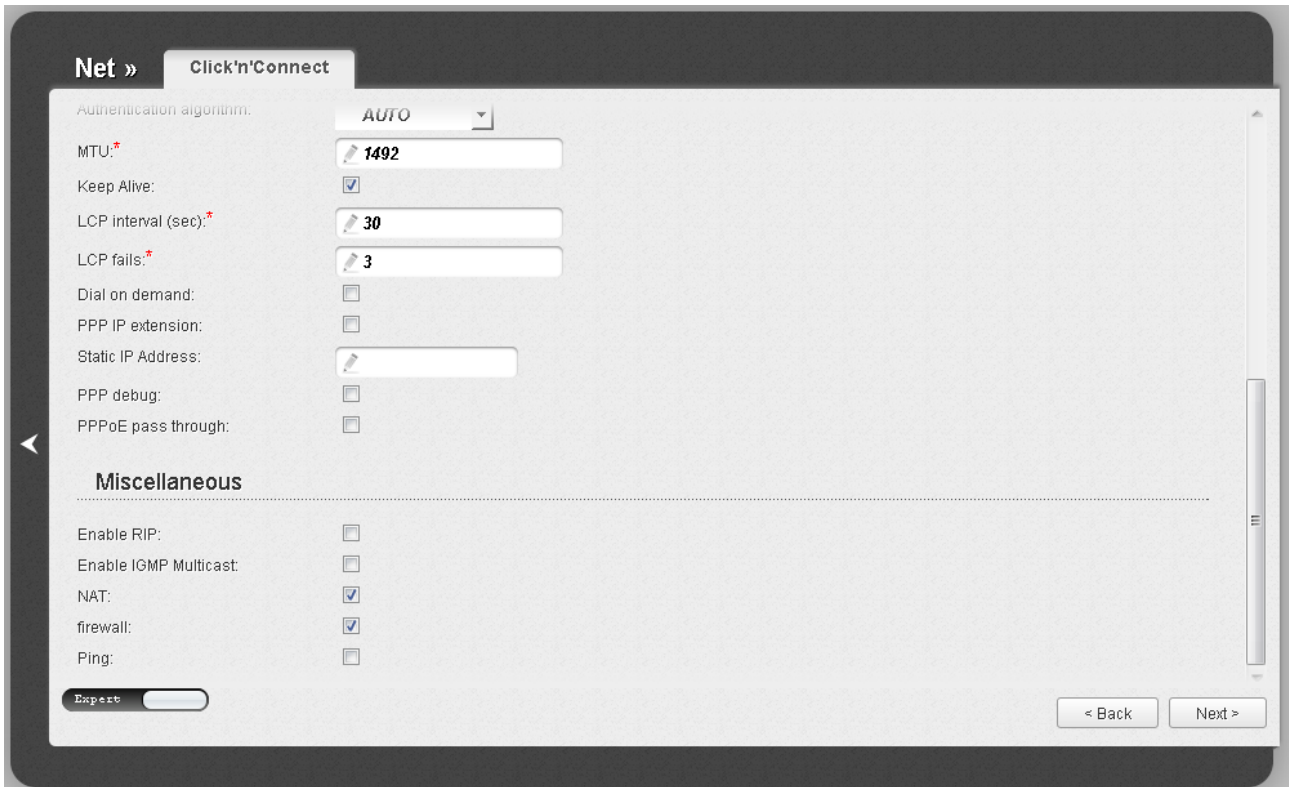


Figure 70. Configuring PPPoE WAN connection. The expert settings mode. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
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.

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 118).

Static IP Connection

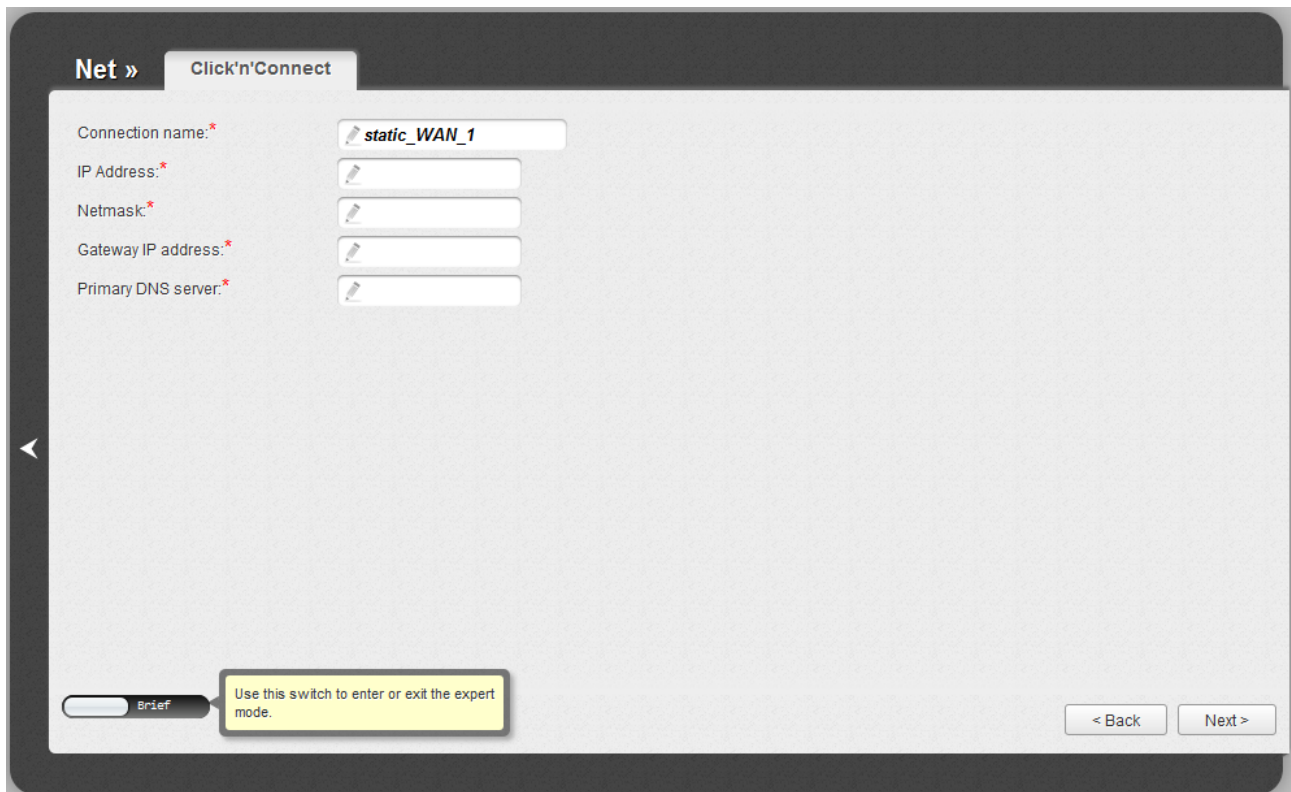


Figure 71. Configuring Static IP WAN connection.

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.

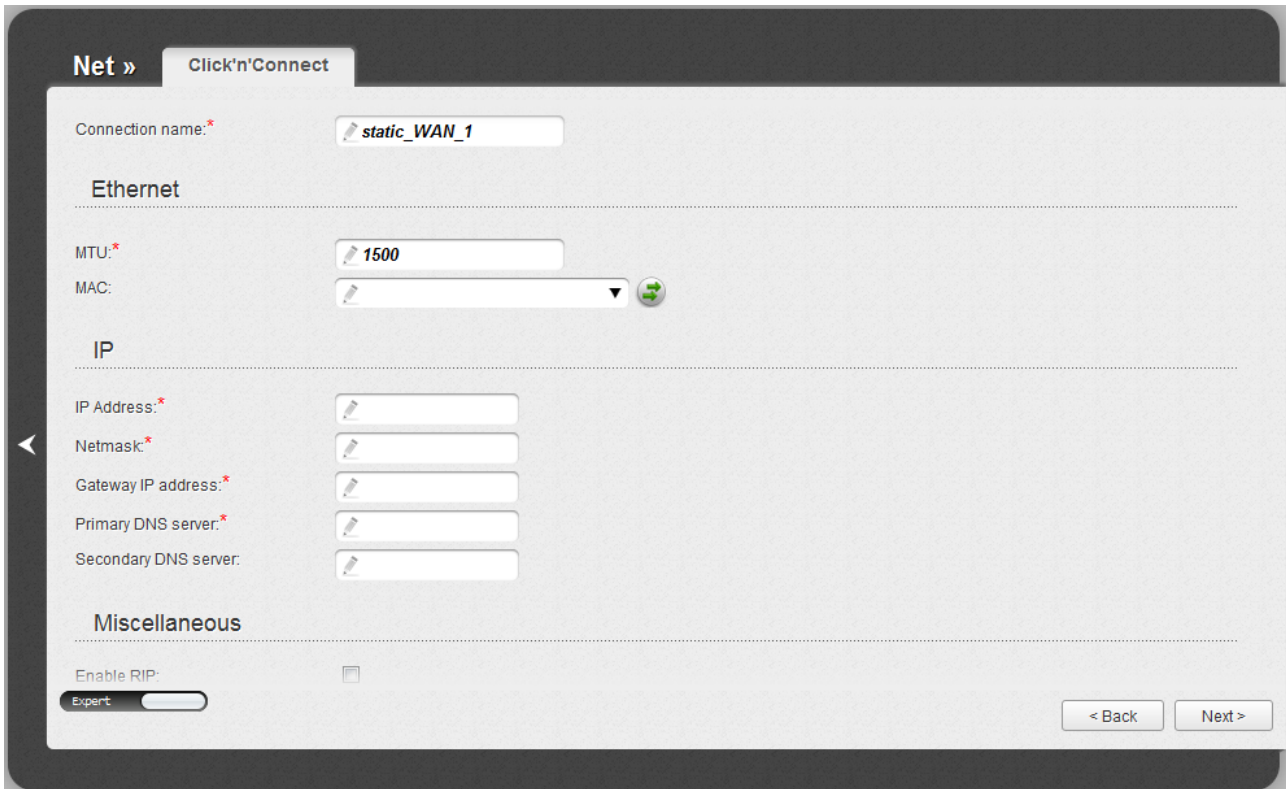



Figure 72. Configuring Static IP WAN connection. The expert settings mode. The **Ethernet** section.

Parameter	Description
Connection name	A name for connection for easier identification.
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 button () 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>

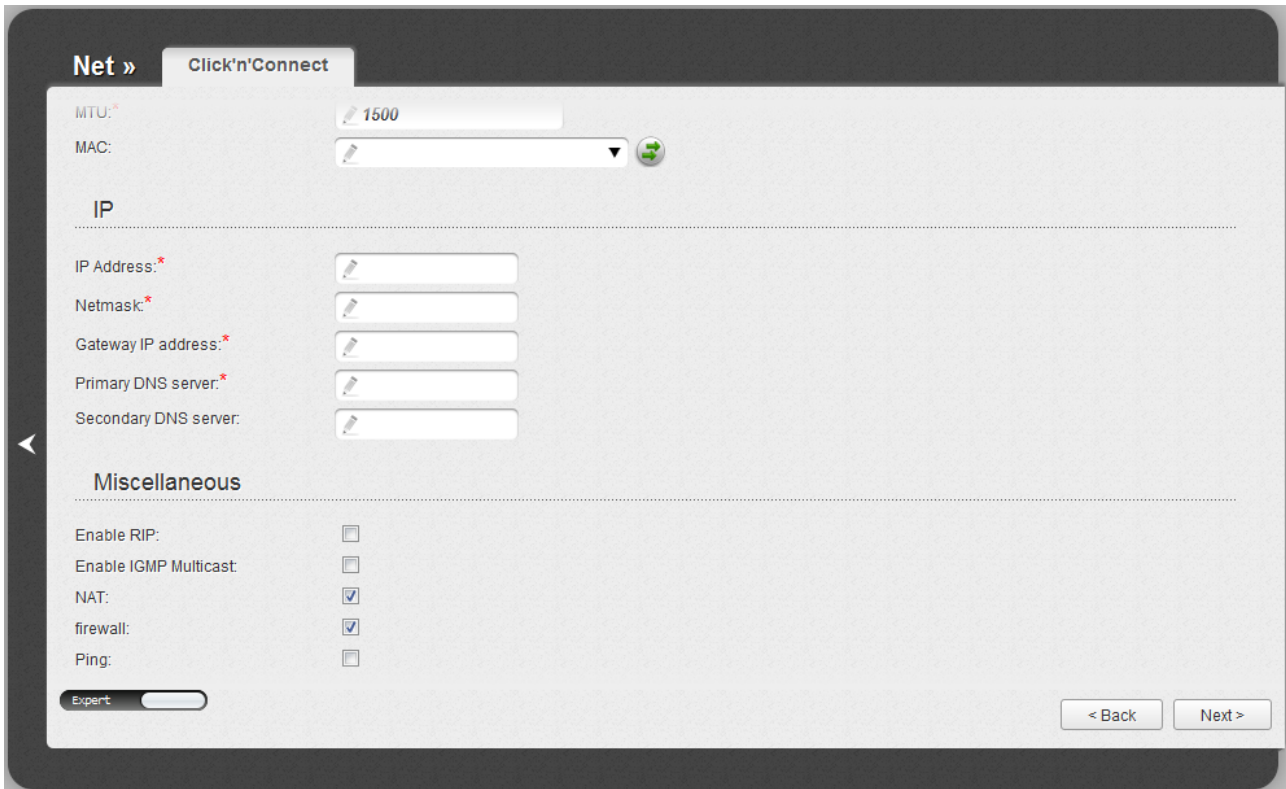


Figure 73. Configuring Static IP WAN connection. The expert settings mode. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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.
Miscellaneous	
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.

Parameter	Description
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.

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 118).

Dynamic IP Connection

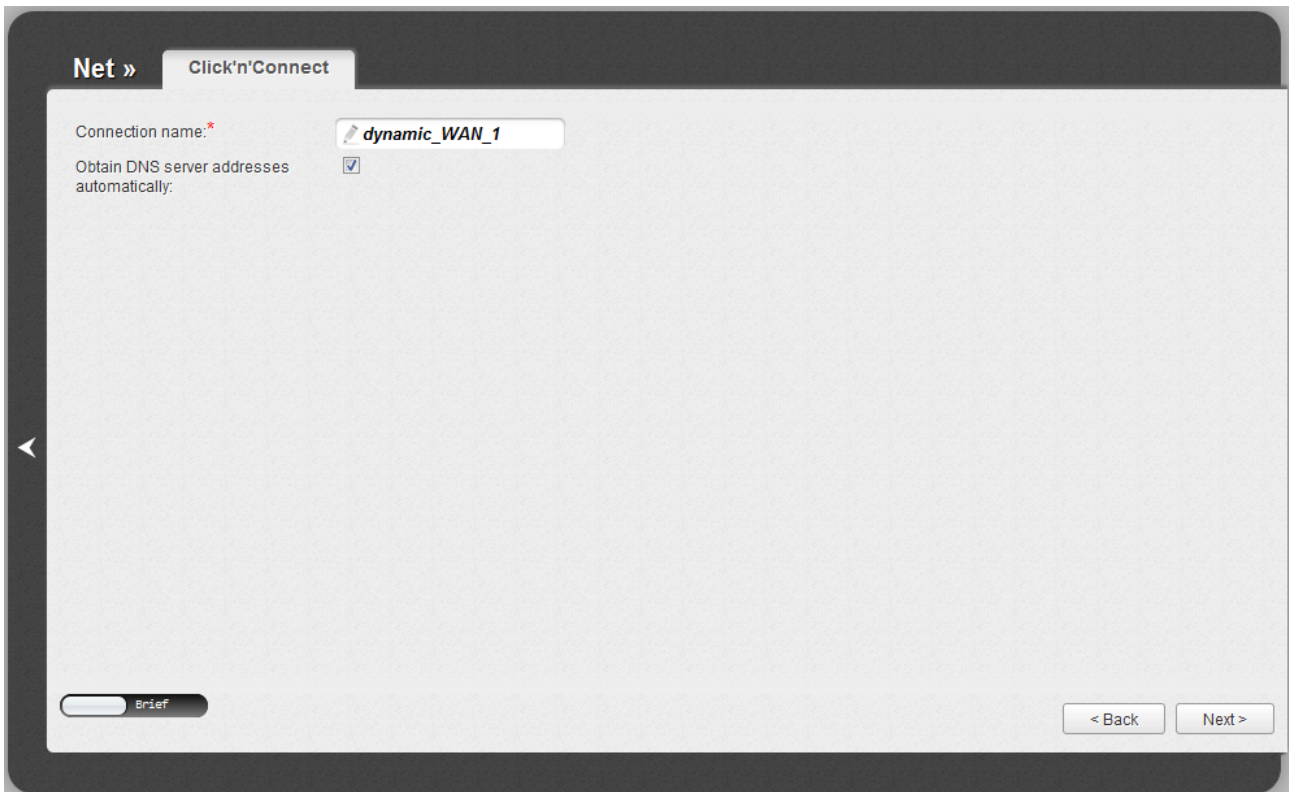


Figure 74. Configuring Dynamic IP WAN connection.

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.

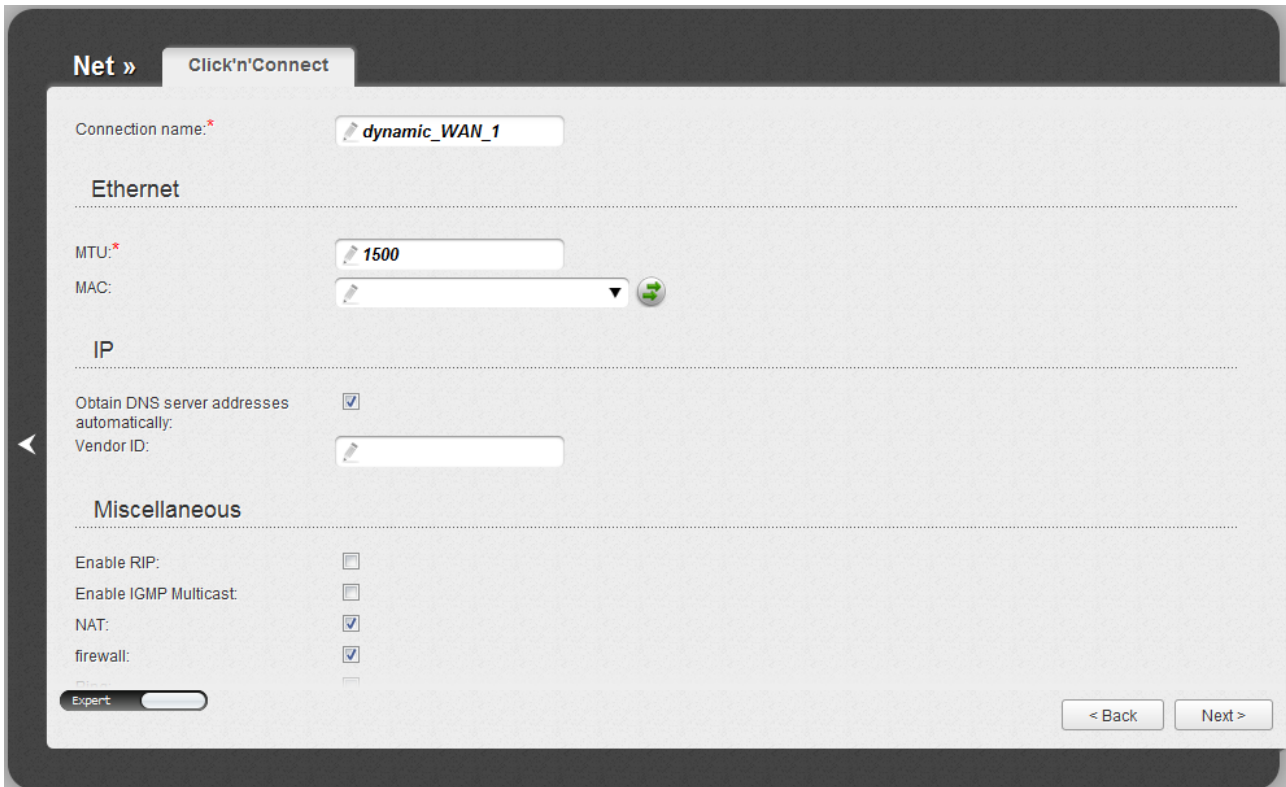



Figure 75. Configuring Dynamic IP WAN connection. The expert settings mode. The **Ethernet** section.

Parameter	Description
Connection name	A name for connection for easier identification.
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 button () 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>

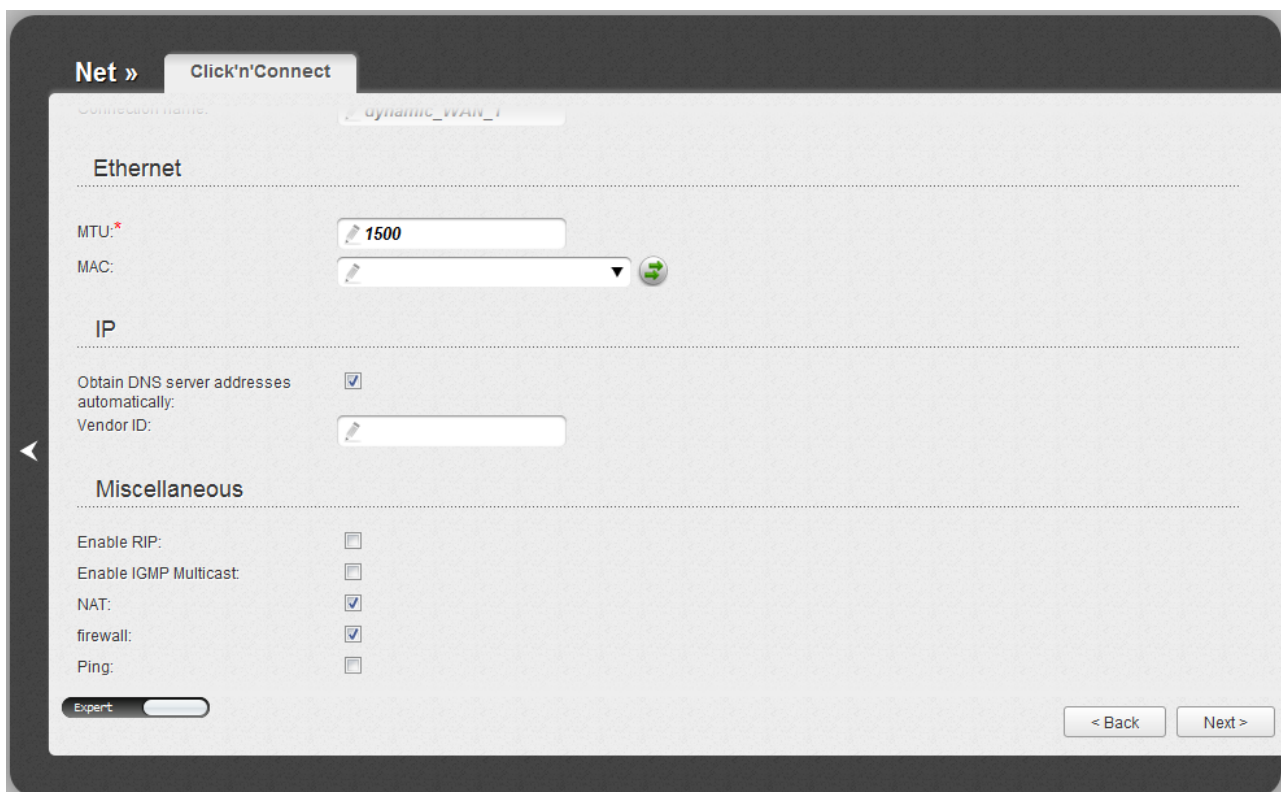


Figure 76. Configuring Dynamic IP WAN connection. The expert settings mode. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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>
Miscellaneous	
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.

Parameter	Description
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.

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 118).

PPTP + Static IP or L2TP + Static IP Connection

The screenshot shows a web-based configuration interface for a router. At the top left, there is a breadcrumb trail: "Net »" followed by a tab labeled "Click'n'Connect". Below this, there are four input fields, each with a red asterisk indicating a required field. The fields are labeled "IP Address:", "Netmask:", "Gateway IP address:", and "Primary DNS server:". Each field has a small pencil icon to its right, suggesting an edit function. At the bottom left, there is a toggle switch labeled "Brief". At the bottom right, there are two buttons: "< Back" and "Next >".

Figure 77. 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.

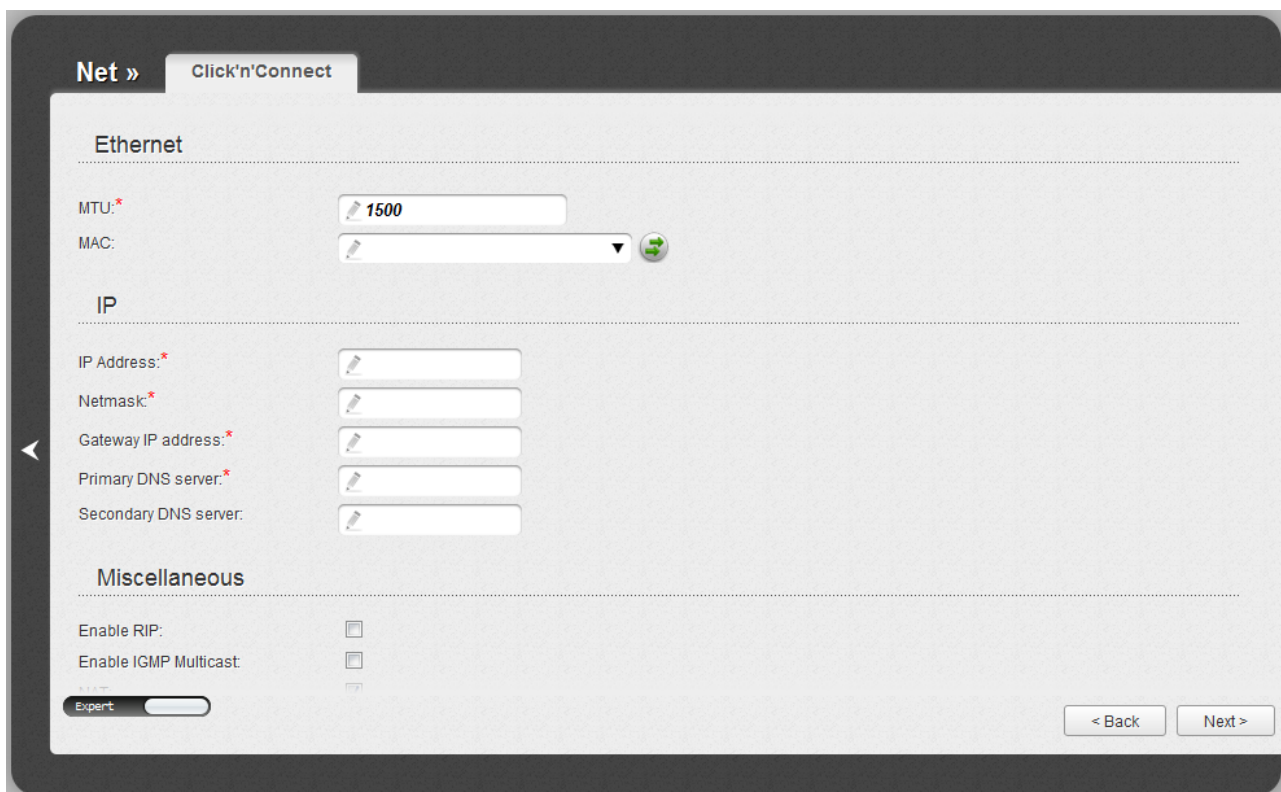



Figure 78. Configuring PPTP + Static IP WAN connection. The expert settings mode. The **Ethernet** section.

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 button () 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>

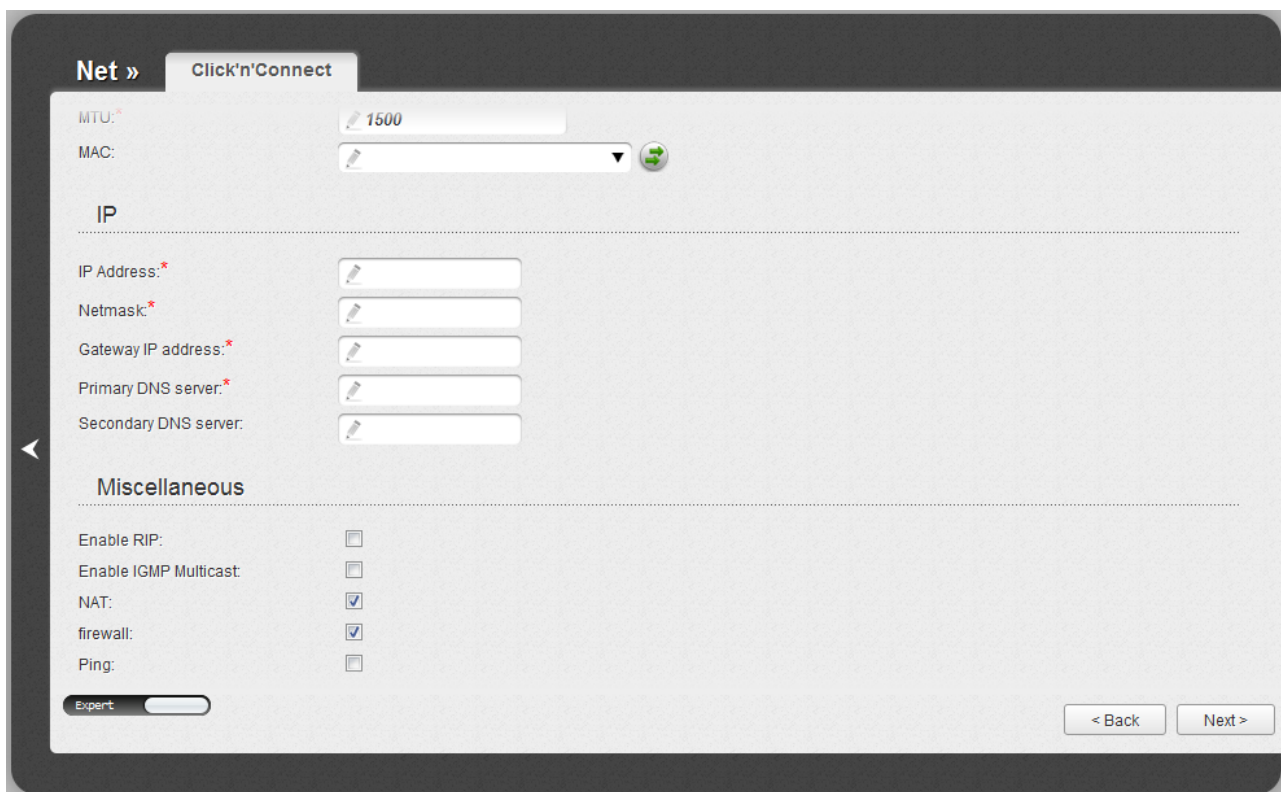


Figure 79. Configuring PPTP + Static IP WAN connection. The expert settings mode. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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.
Miscellaneous	
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.

Parameter	Description
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.

Click the **Next** button to continue.

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

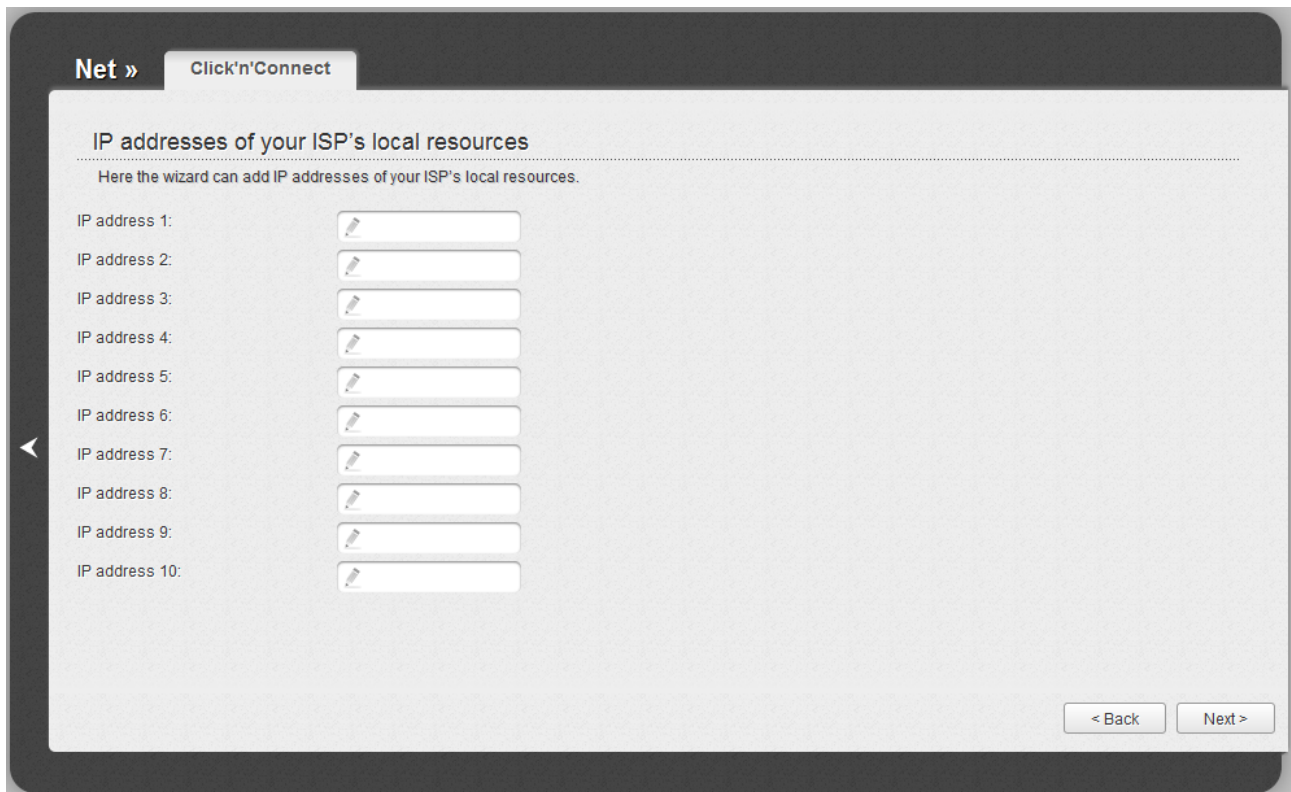


Figure 80. Configuring PPTP + Static IP WAN connection.

Click the **Next** button to continue.

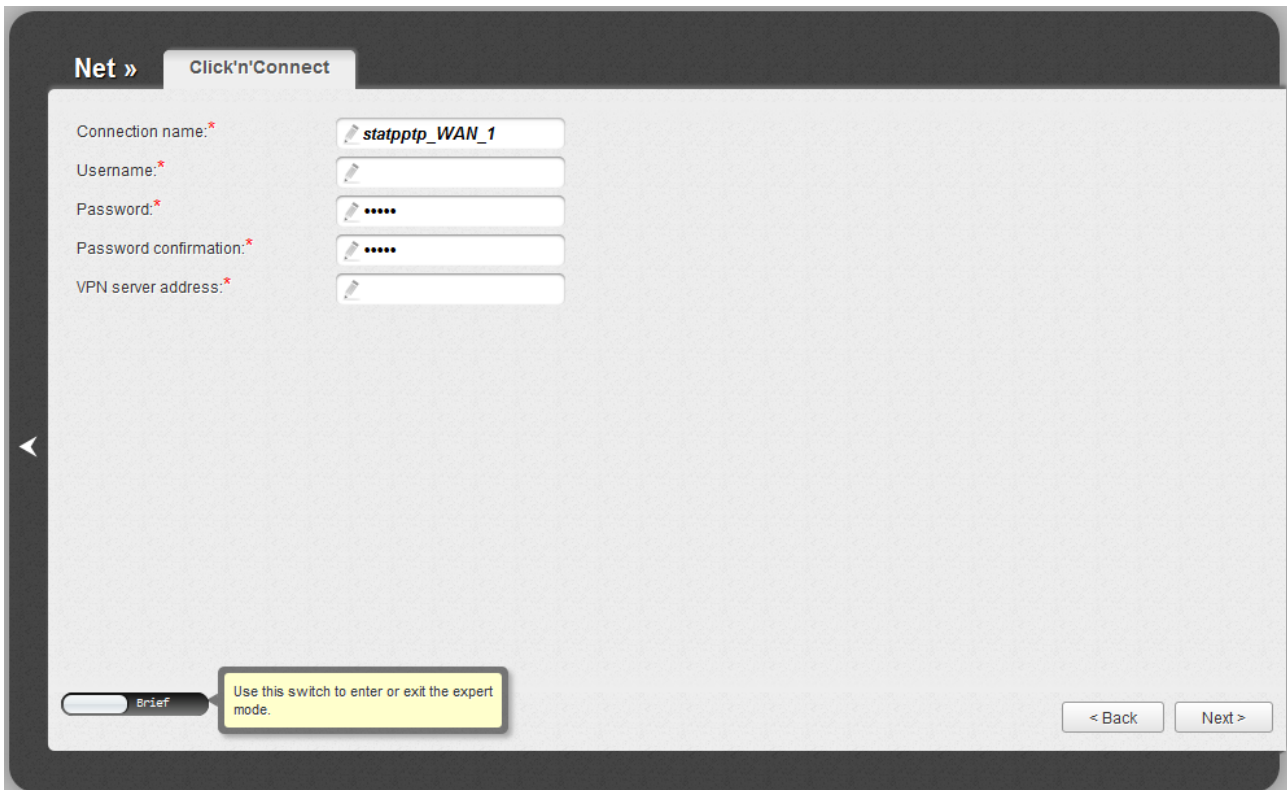


Figure 81. Configuring PPTP + Static IP WAN connection.

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.

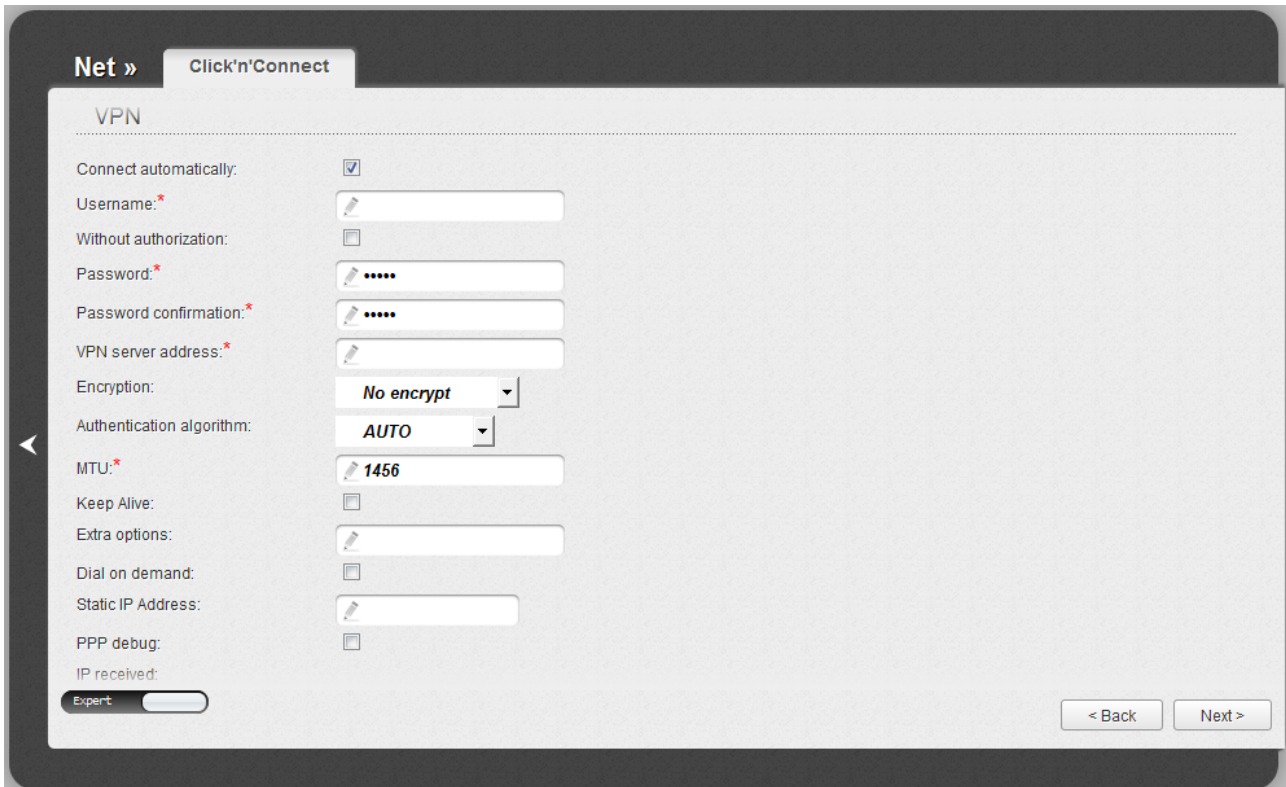


Figure 82. Configuring PPTP + Static IP WAN connection. The expert settings mode. The VPN section.

Parameter	Description
Connection name	A name for connection for easier identification.
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>

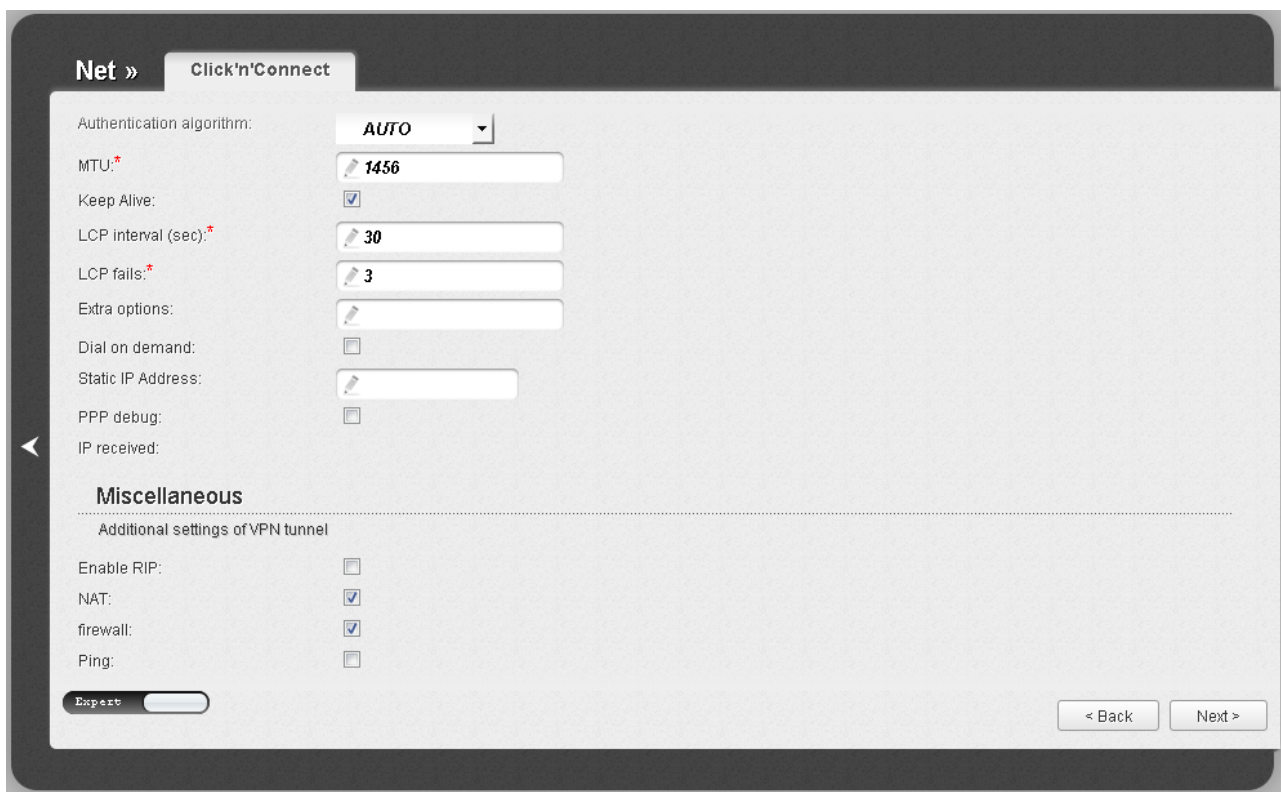


Figure 83. Configuring PPTP + Static IP WAN connection. The expert settings mode. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
Enable RIP	Select the checkbox to allow using RIP for this connection.
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.

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 118).

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

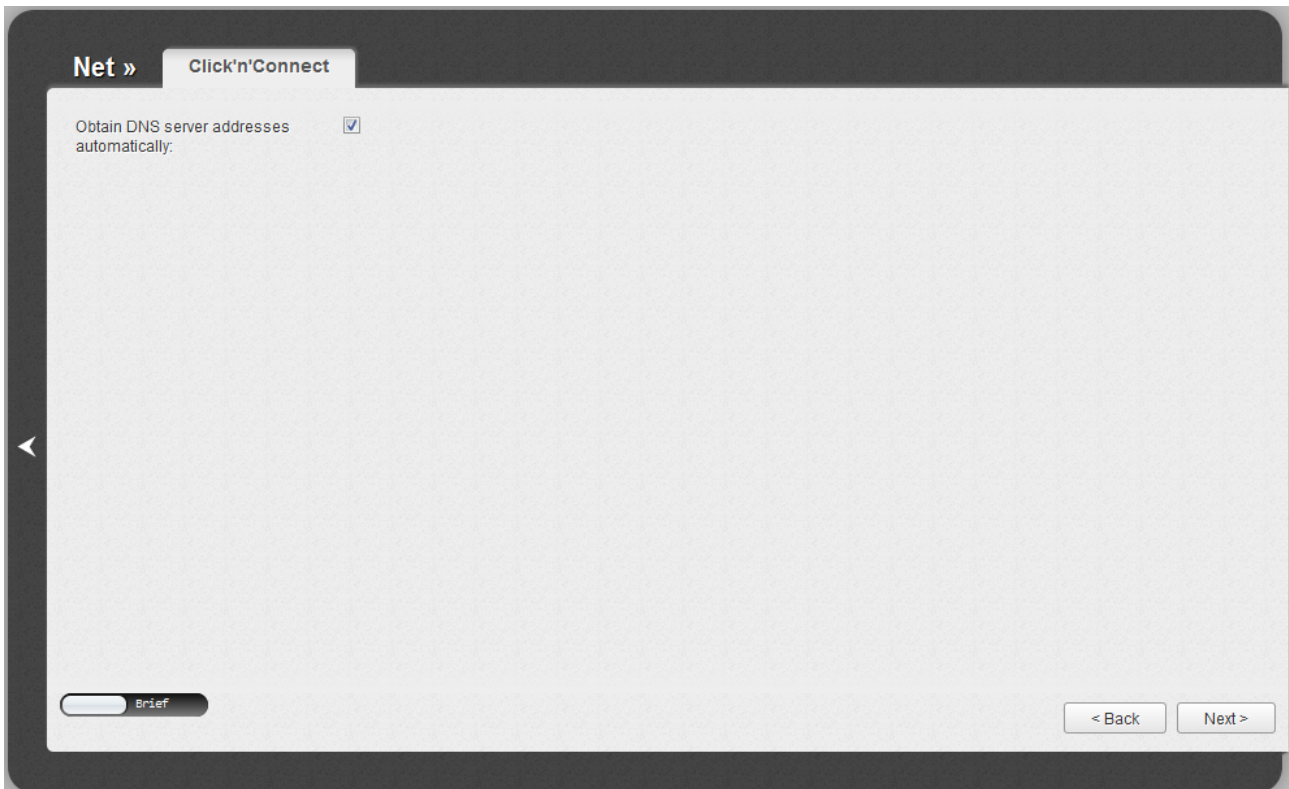


Figure 84. Configuring PPTP + Dynamic IP WAN connection.

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.

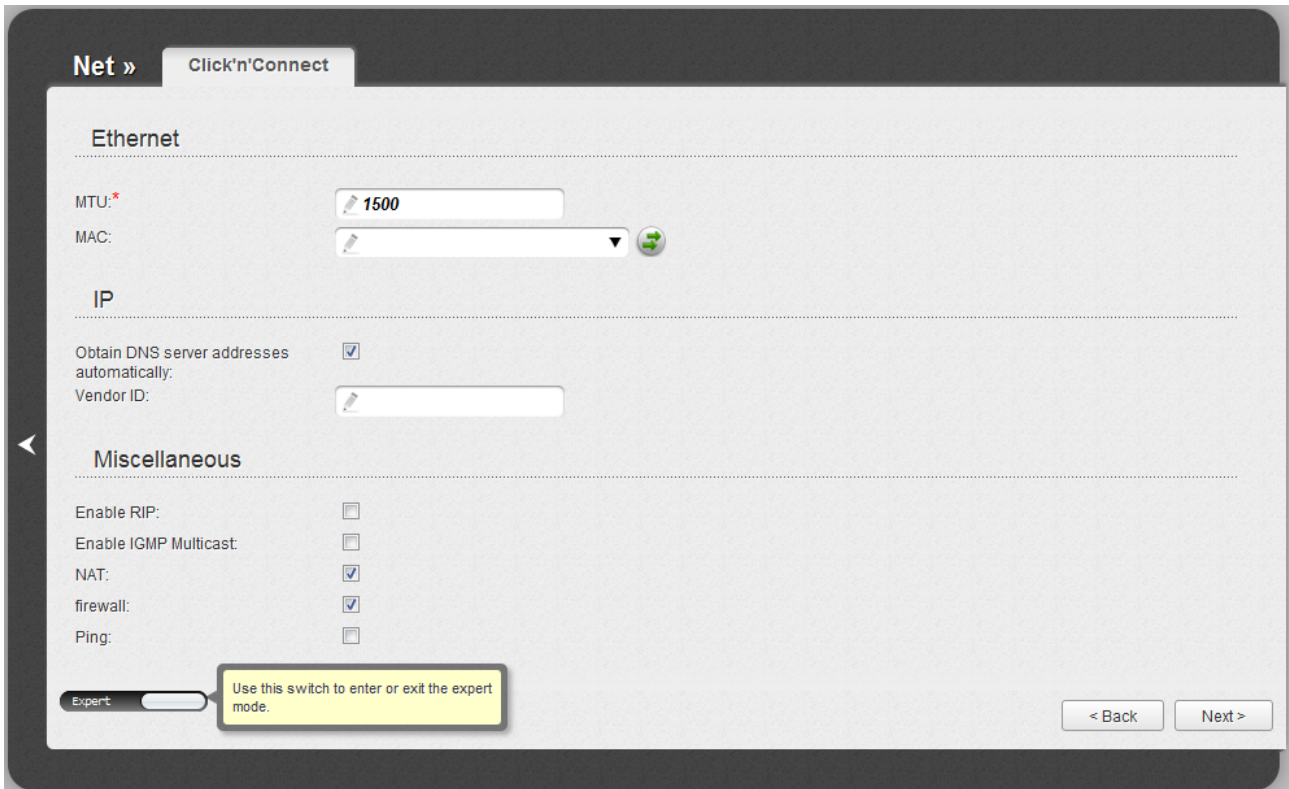



Figure 85. Configuring PPTP + Dynamic IP WAN connection. The expert settings mode. The **Ethernet** section.

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 button () 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>

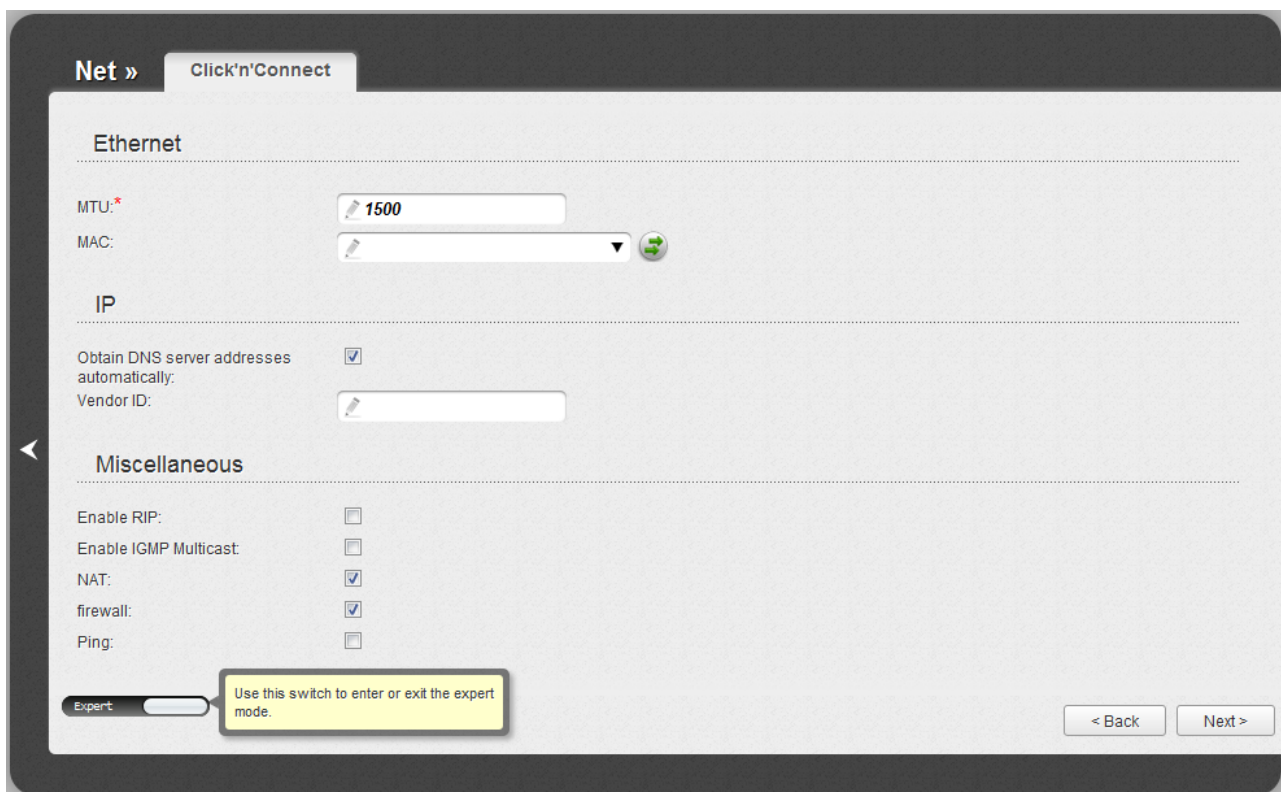


Figure 86. Configuring PPTP + Dynamic IP WAN connection. The expert settings mode. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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>
Miscellaneous	
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.

Parameter	Description
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.

Click the **Next** button to continue.

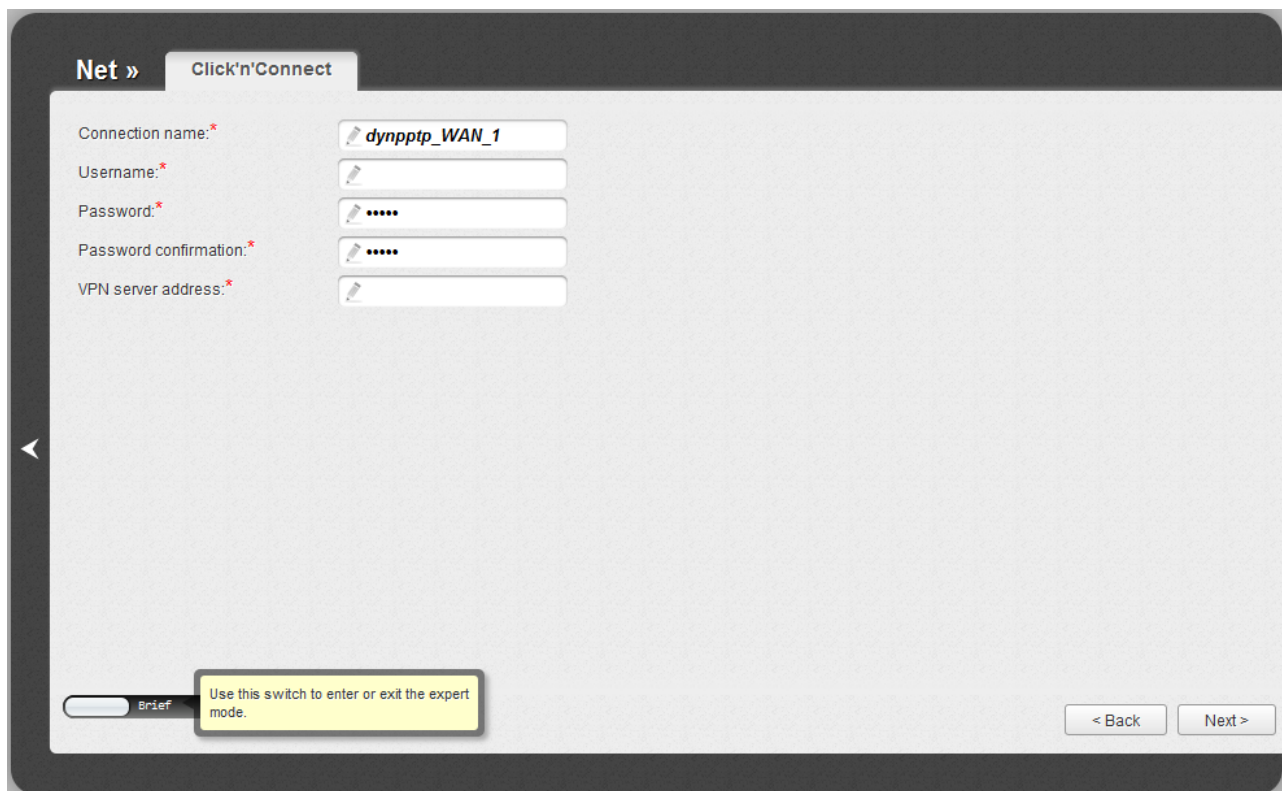


Figure 87. Configuring PPTP + Dynamic IP WAN connection.

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.

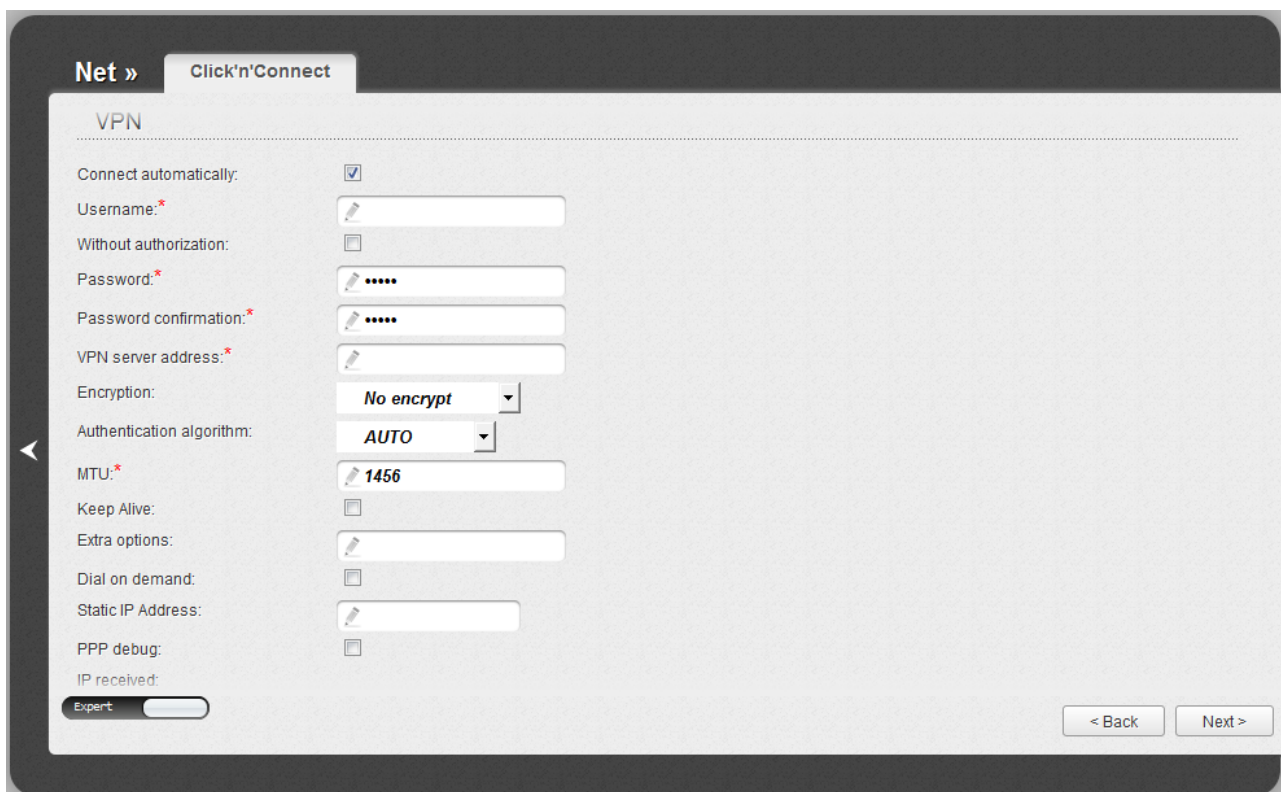


Figure 88. Configuring PPTP + Dynamic IP WAN connection. The expert settings mode. The **VPN** section.

Parameter	Description
Connection name	A name for connection for easier identification.
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>

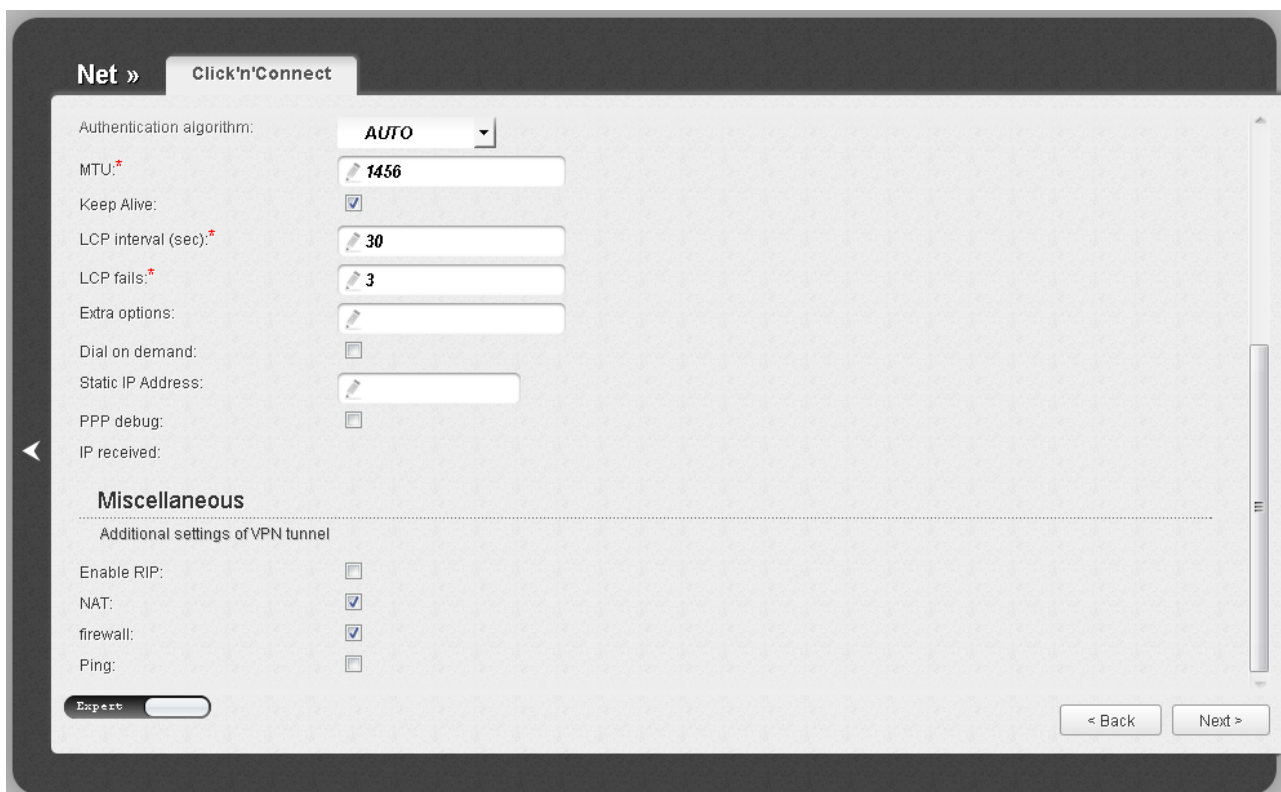


Figure 89. Configuring PPTP + Dynamic IP WAN connection. The expert settings mode. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
Enable RIP	Select the checkbox to allow using RIP for this connection.
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.

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 118).

Checking Internet Availability

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

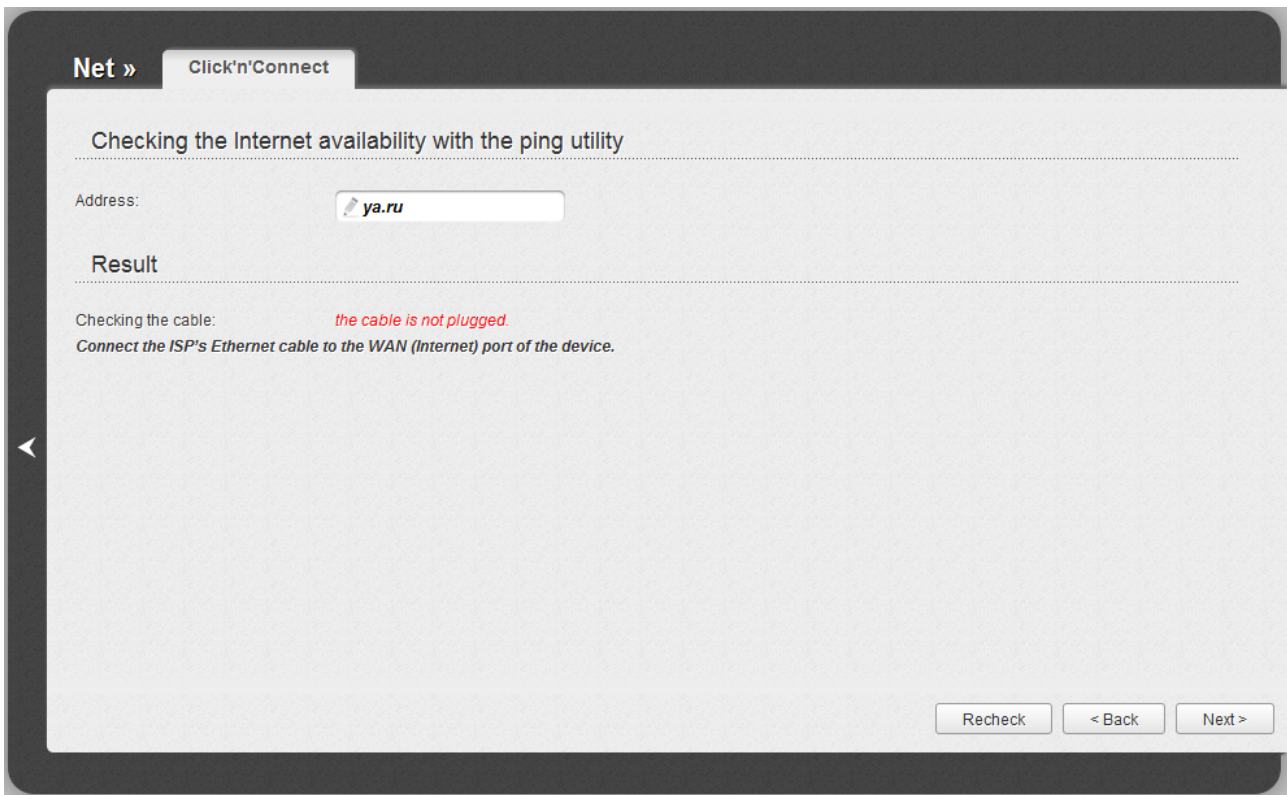


Figure 90. Checking the Internet availability.

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 (**ya.ru**). 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 119).

Configuring Wireless Connection

On the page, you can change the name of your wireless network, specify a password to it, or disable Wi-Fi connections.

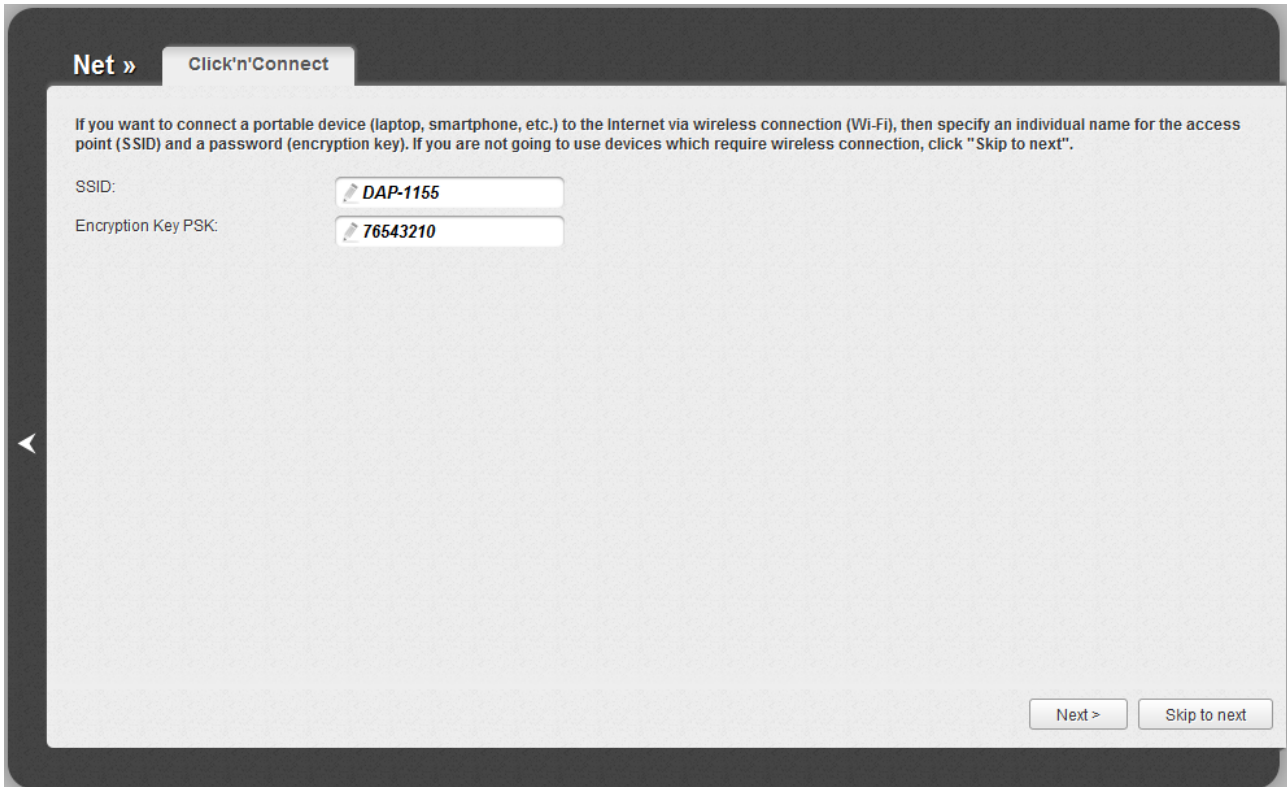


Figure 91. Configuring the wireless connection.

In the **SSID** field, specify a new name for the network (use digits and Latin characters).

In the **Encryption Key PSK** field, enter a key (a password that will be used to access your wireless network). Use digits and Latin characters.

Click the **Next** button to continue.

Click the **Skip to next** button to disable Wi-Fi connections.

On the opened page, click the **Back** button to specify other settings for your wireless network.

Click the **Save** button to save the specified settings.

After clicking the **Save** button, the quick settings page opens.

Wireless Network Settings Wizard

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

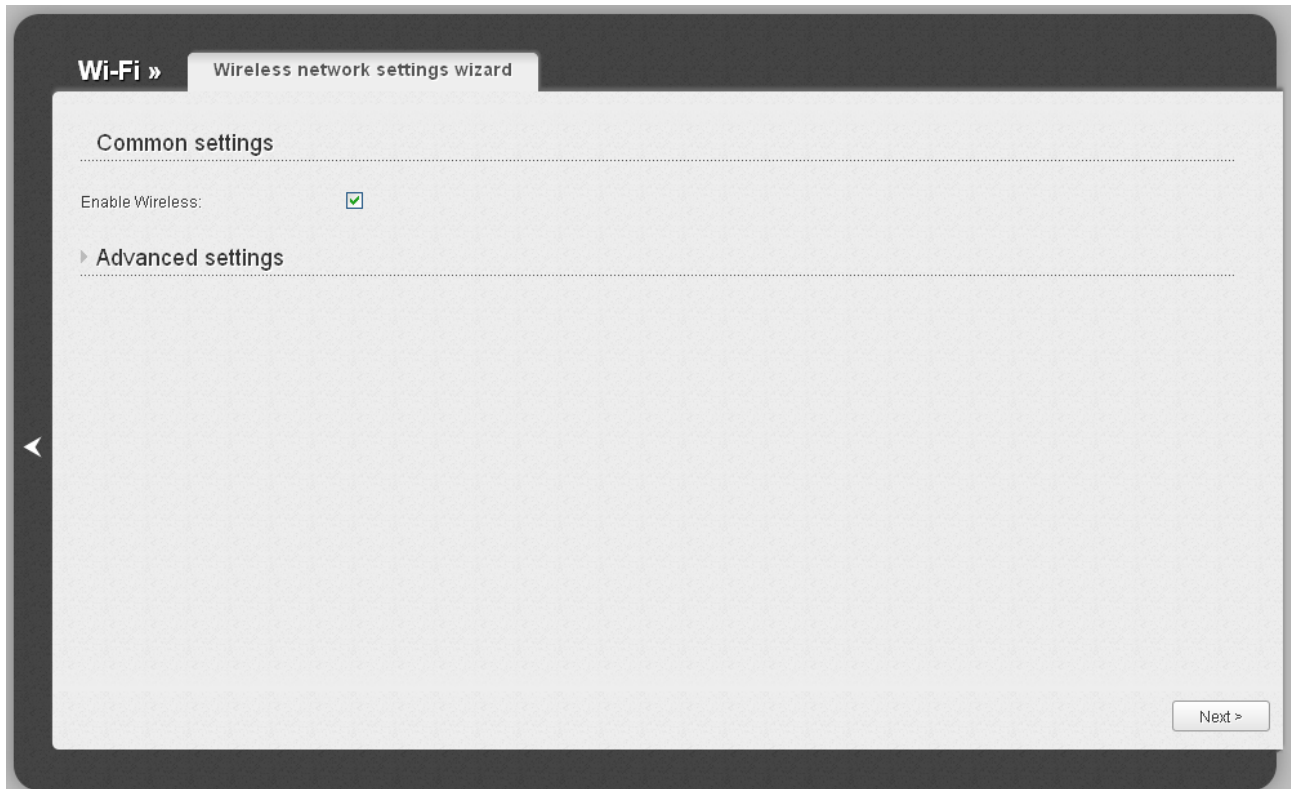


Figure 92. Common and advanced settings of the wireless LAN.

On the opened page, in the **Common settings** section, select the **Enable Wireless** checkbox (if it was deselected before) to enable Wi-Fi connections.

In the **Advanced settings** section, you can split your network into several parts. To do this, select the relevant value (**2**, **3**, or **4**) from the **MBSSID** drop-down list.

Click the **Next** button to continue.

In the **Basic settings** section, you can change the basic parameters of your access point's WLAN: “hide” your wireless network (**Hide Access Point**), specify a name for the network (**SSID**), select your location (**Country**) and the wireless channel number (**Channel**), specify the operating mode (**Wireless Mode**) and the maximum number of devices connected to the wireless network (**Max Associated Clients**).

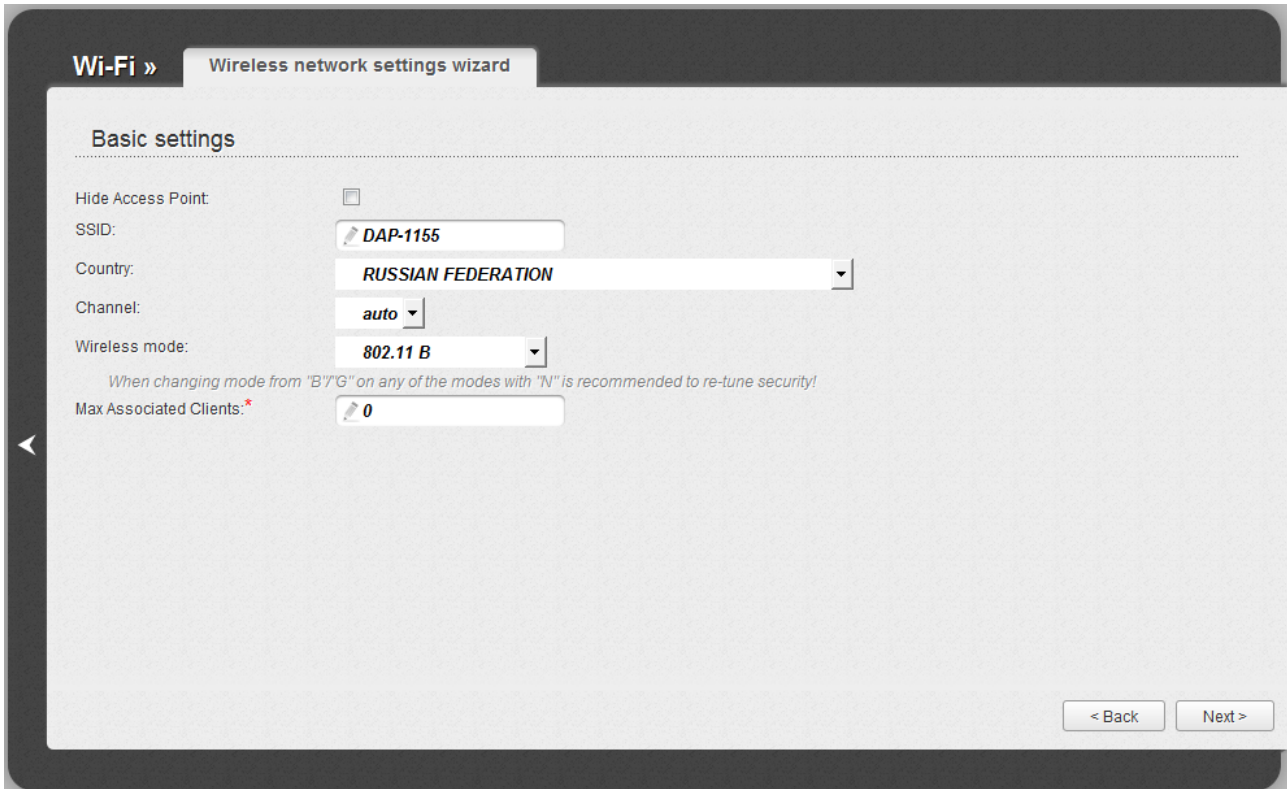


Figure 93. Basic settings of the wireless LAN.

Click the **Next** button to continue.

On the next page, you can modify security settings of the WLAN. By default, the **Open** network authentication type with no encryption is specified for the WLAN.

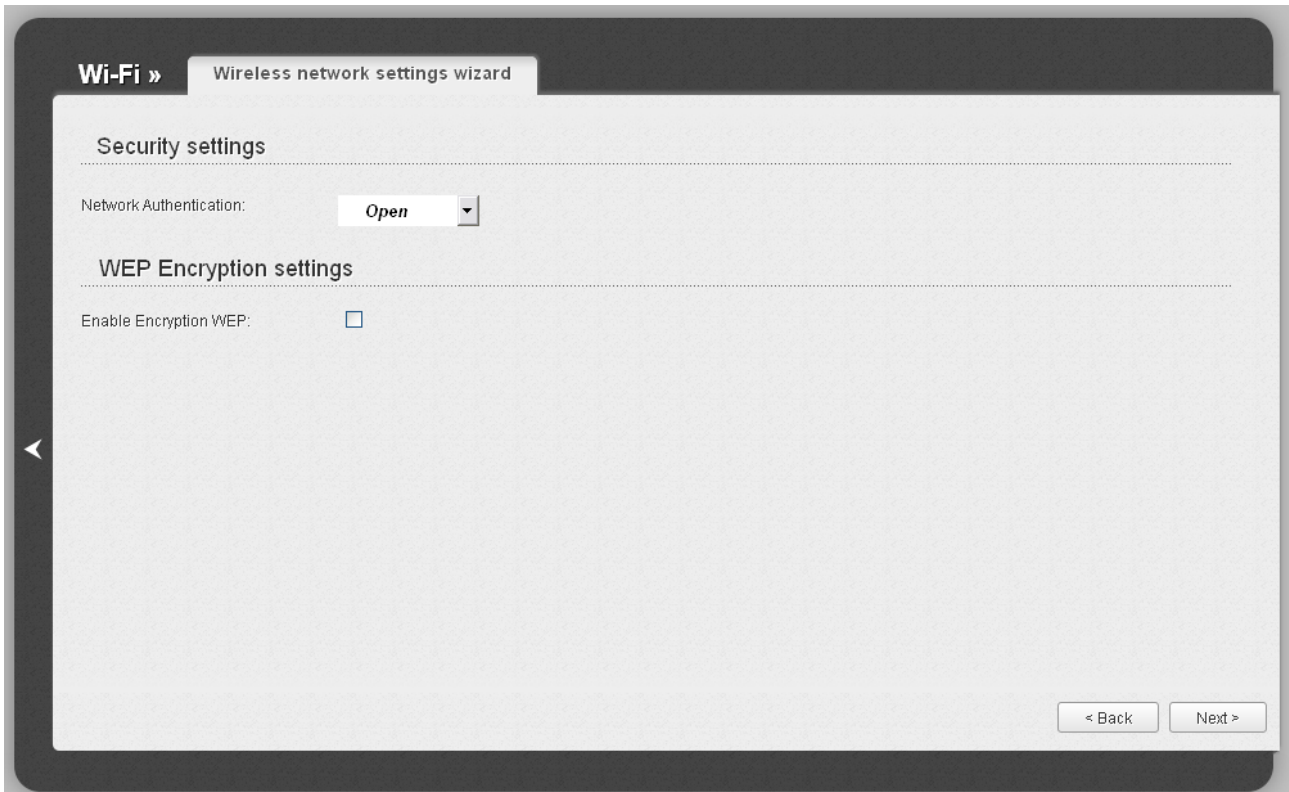


Figure 94. The default security settings.



The default security settings do not provide sufficient protection for the WLAN. Please, specify your own security settings for the WLAN (or each part of the WLAN if the network was splitted into parts).

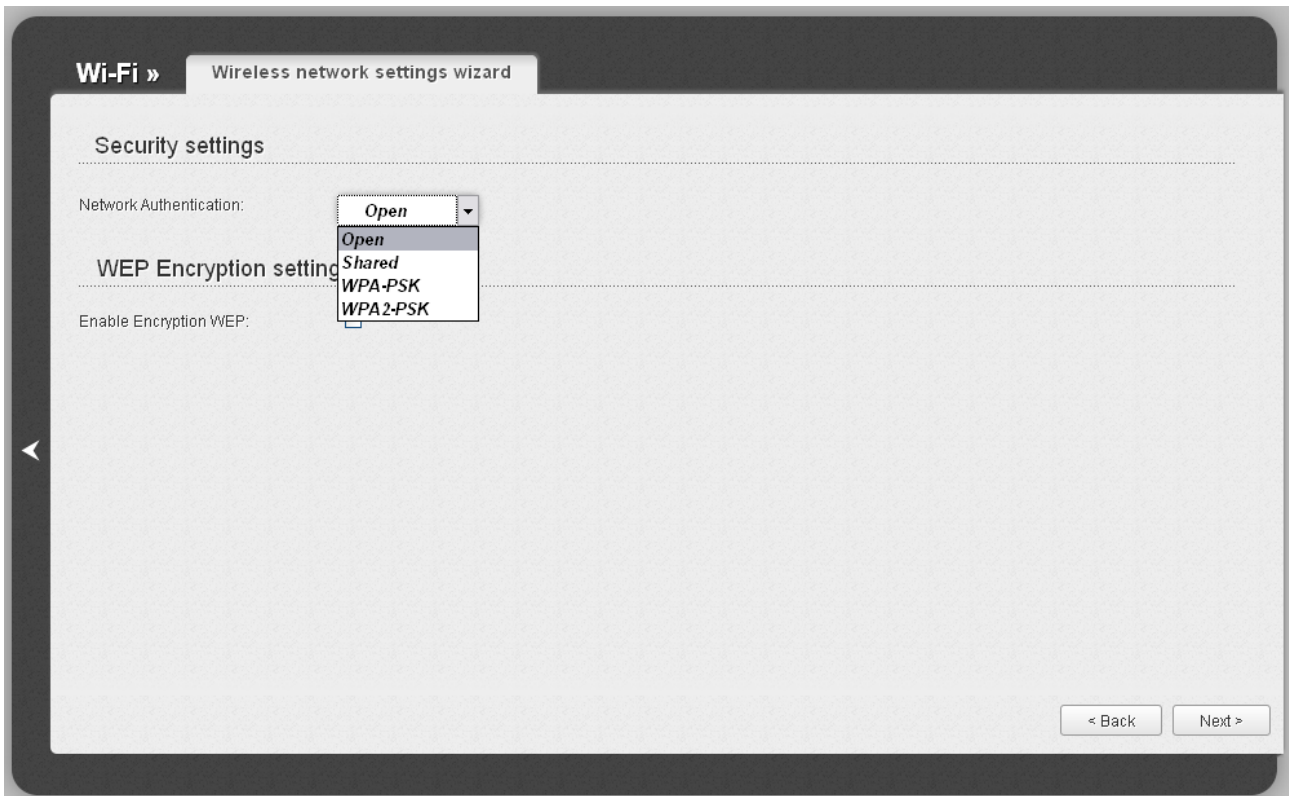


Figure 95. Network authentication types supported by the access point.

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 basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected.
WPA-PSK	WPA-based authentication using a PSK.
WPA2-PSK	WPA2-based authentication using a PSK.

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):

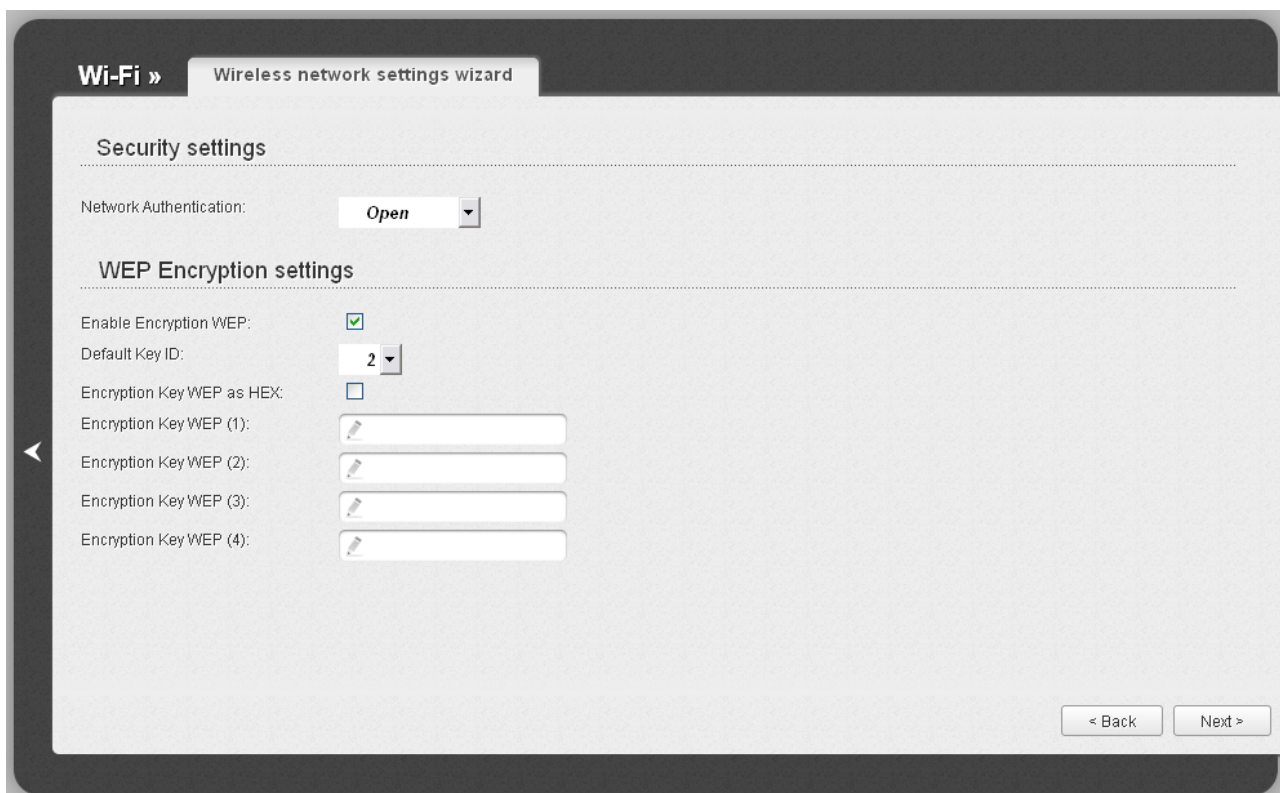


Figure 96. The **Open** value is selected from the **Network Authentication** drop-down list.

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, 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.
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. You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters). If the Encryption Key WEP as HEX checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F).

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

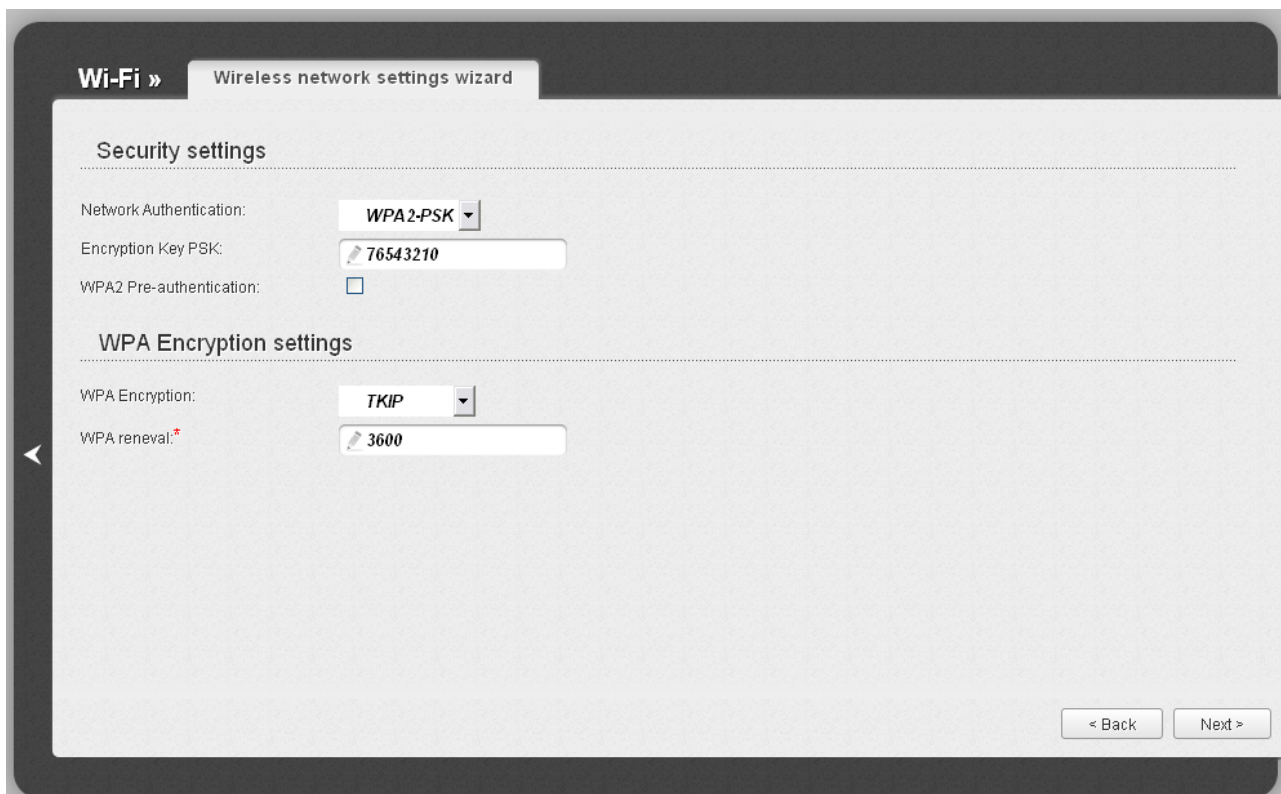


Figure 97. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
Encryption Key PSK	A key for WPA encryption. The key can contain digits and/or Latin characters.
WPA2 Pre-authentication	The checkbox activating preliminary authentication (displayed only for the WPA2-PSK authentication type).
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.

Click the **Next** button to continue.

When all the steps of configuring the WLAN are completed, the specified settings are displayed on the page. Check their correctness and then click the **Save** button. After that you get to the quick settings page.

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 **Firewall** section.

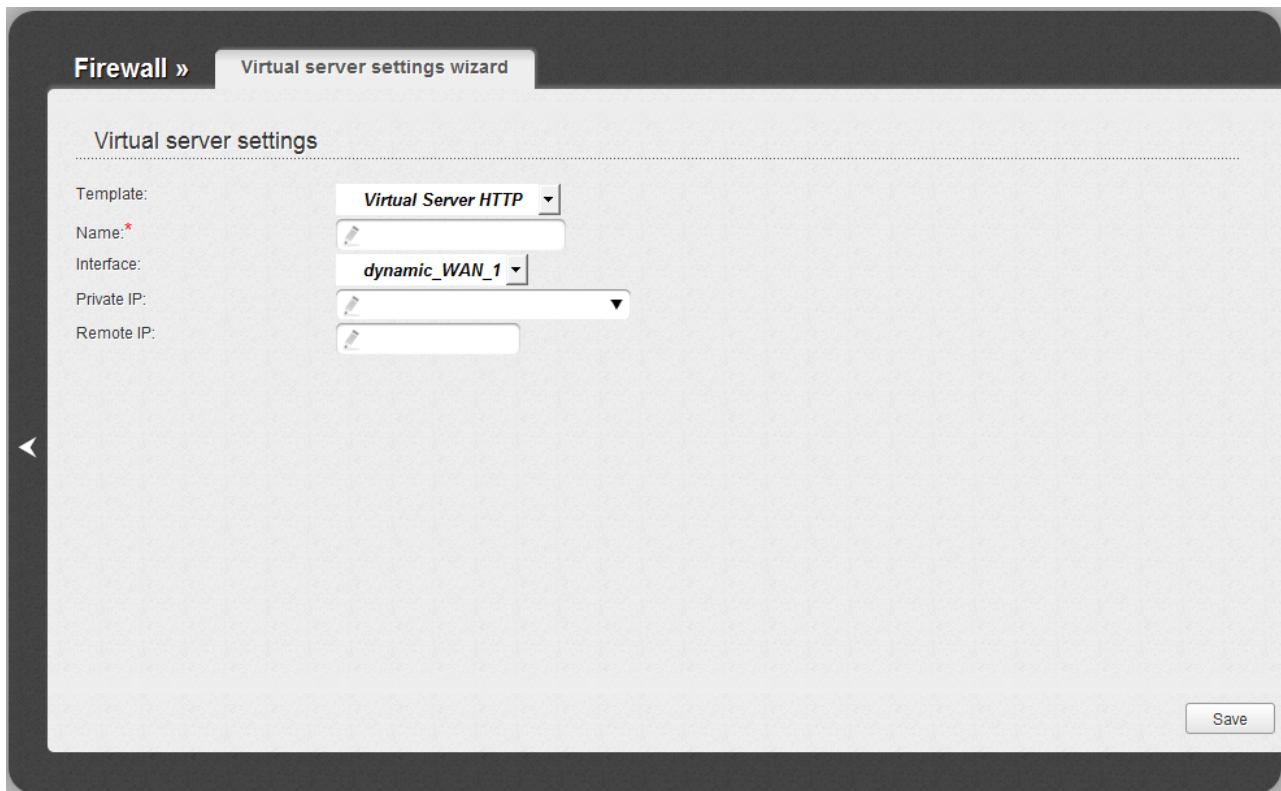


Figure 98. The page for adding a virtual server.

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.
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.

When needed settings are configured, click the **Save** button. After that you get to the quick settings page.

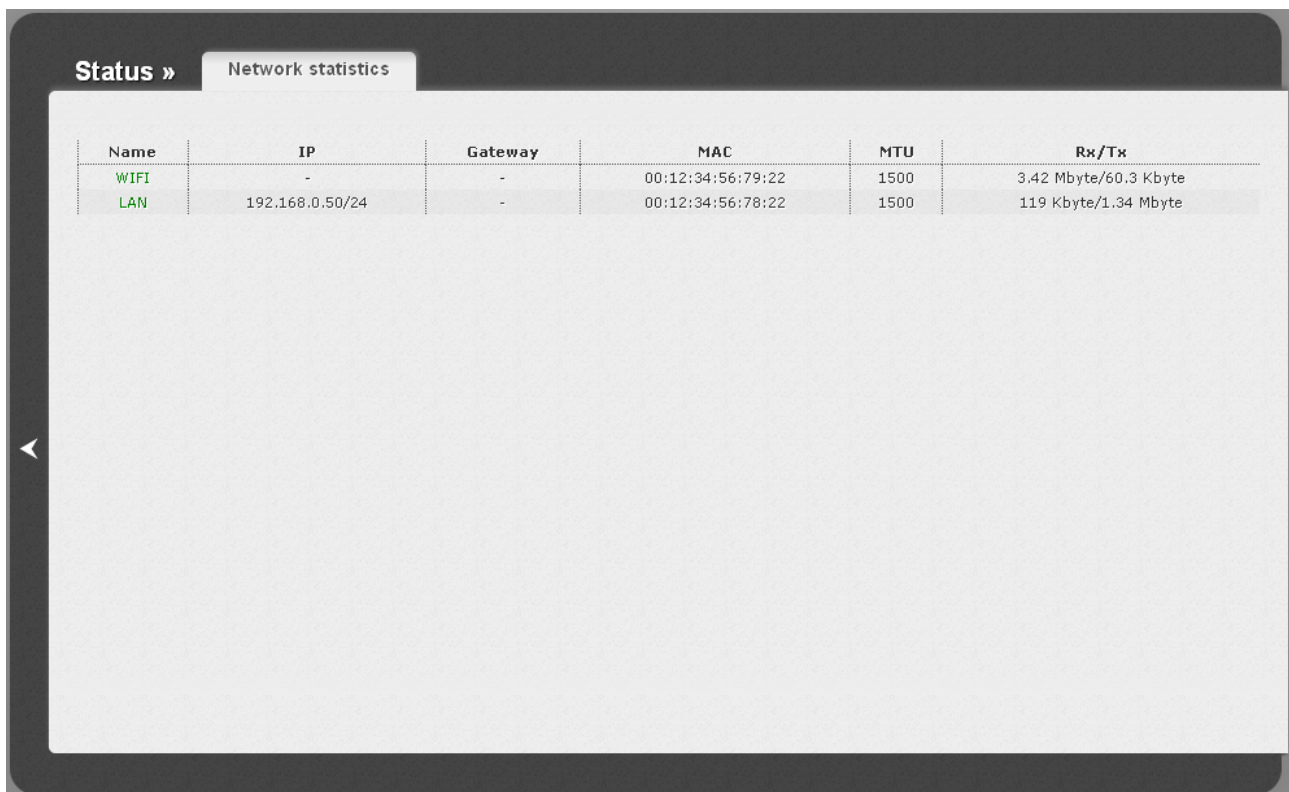
Status

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 device's network and its web-based interface.

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	MTU	Rx/Tx
WIFI	-	-	00:12:34:56:79:22	1500	3.42 Mbyte/60.3 Kbyte
LAN	192.168.0.50/24	-	00:12:34:56:78:22	1500	119 Kbyte/1.34 Mbyte

Figure 99. 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).

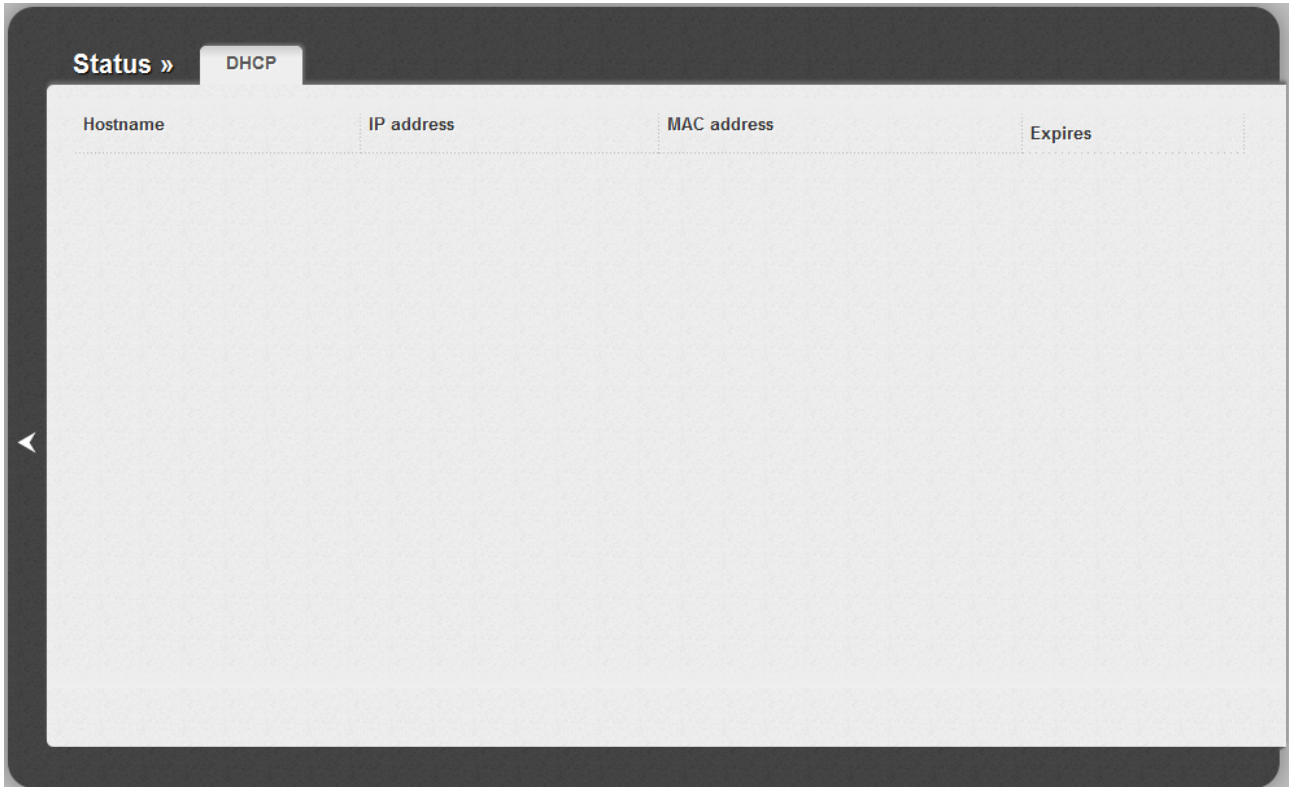
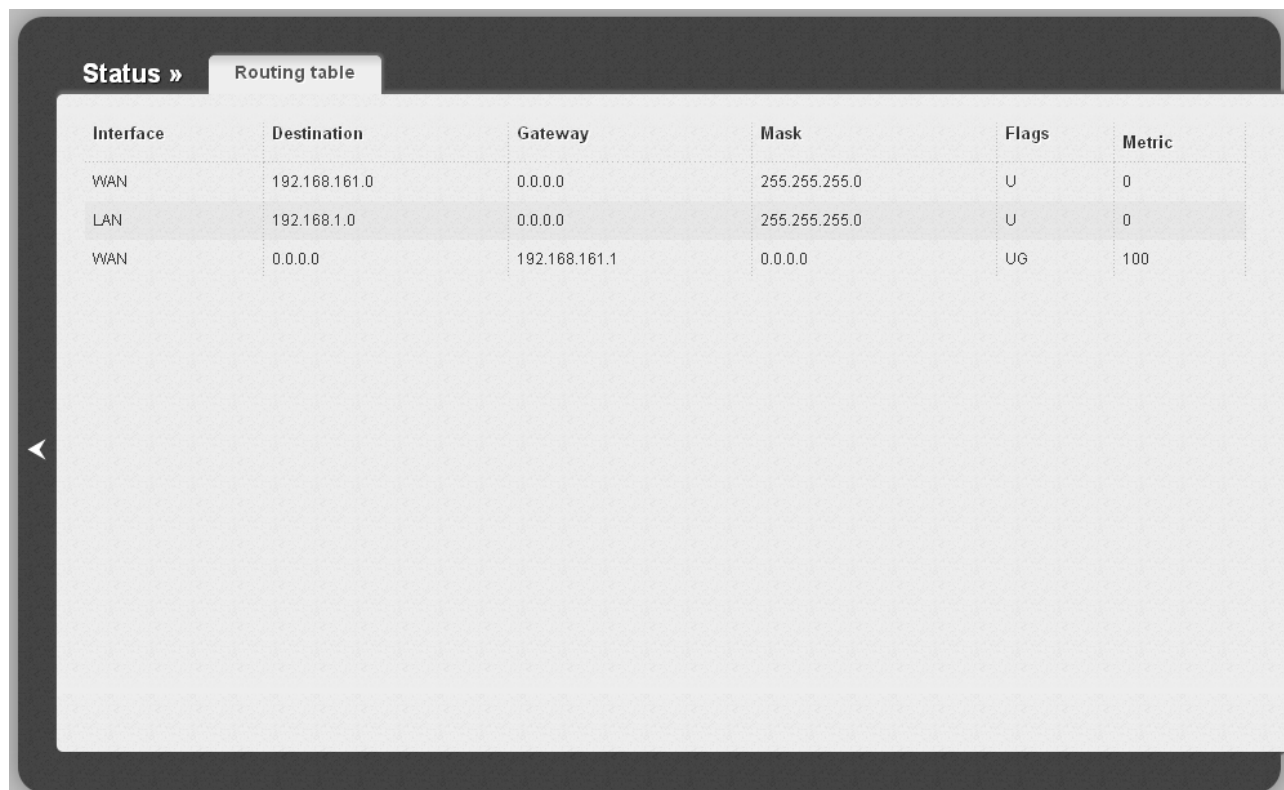


Figure 100. The **Status / DHCP** page.

Routing Table

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



Interface	Destination	Gateway	Mask	Flags	Metric
WAN	192.168.161.0	0.0.0.0	255.255.255.0	U	0
LAN	192.168.1.0	0.0.0.0	255.255.255.0	U	0
WAN	0.0.0.0	192.168.161.1	0.0.0.0	UG	100

Figure 101. The **Status / Routing table** page.

LAN Clients

On the **Status / LAN 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 with a dark header. On the left, there is a navigation menu with a left-pointing arrow. The main content area has a light background and contains a table with the following data:

IP address	Flags	MAC address	Interface
192.168.1.77	0x2	00:30:48:fe:db:ec	LAN
192.168.1.40	0x2	1c:6f:65:b0:82:ba	LAN
192.168.161.1	0x2	1c:6f:65:b0:82:ba	WAN

Figure 102. The **Status / LAN 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.

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.

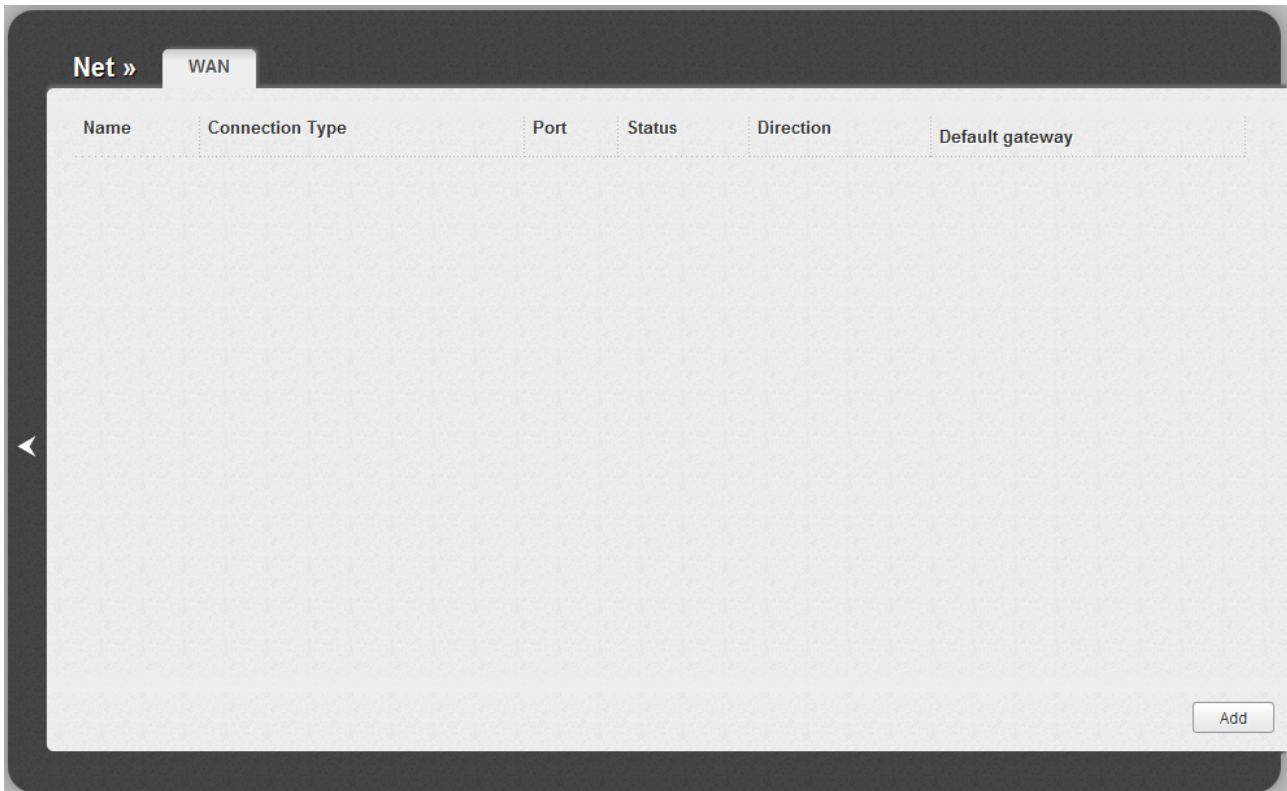


Figure 103. The **Net / WAN** page.

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 **Save** button.

To delete an existing connection, left-click the relevant line in the table. On the page displayed, click the **Delete** button.

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.

The screenshot shows a configuration interface with two main sections: **General settings** and **Ethernet**.
 Under **General settings**, the following fields are visible:
 - **Connection Type:** A dropdown menu with 'PPPoE' selected.
 - **Port:** A dropdown menu with 'WAN' selected.
 - **Name:*** A text input field containing 'pppoe_WAN_1'.
 - **Enable:** A checked checkbox.
 - **Direction:** A text field containing 'WAN'.
 Under **Ethernet**, the following fields are visible:
 - **MTU:*** A text input field containing '1500'.
 - **MAC:** A dropdown menu that is currently empty, with a green refresh icon to its right.

Figure 104. The page for creating a new connection. The **General settings** and **Ethernet** sections.

Parameter	Description
General settings	
Port	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	The maximum size of units transmitted by the interface.

Parameter	Description
<p style="text-align: center;">MAC</p>	<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 button () 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>

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:

PPPoE pass through:

Figure 105. The page for creating a new 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.
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.
PPPoE pass through	Select the checkbox if you want to allow PPPoE clients of computers from your LAN to connect to the Internet through this PPPoE connection of the access point.

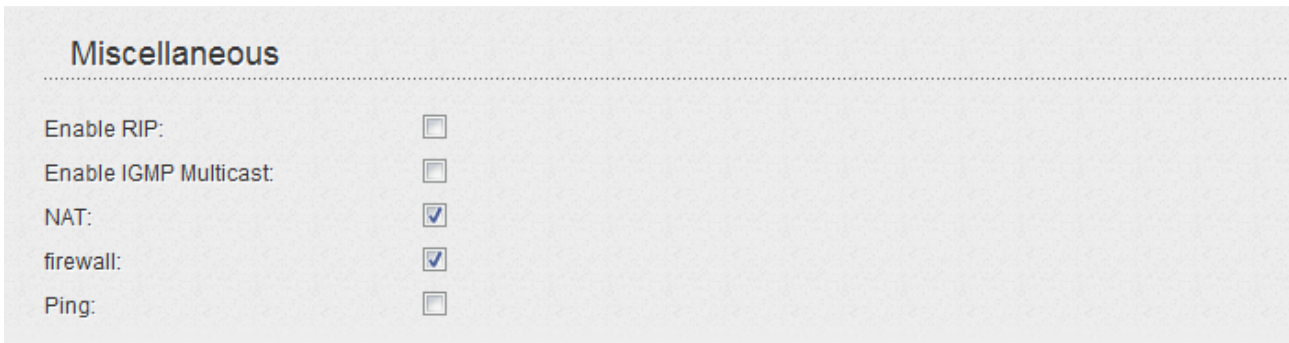


Figure 106. The page for creating a new connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
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 **Save** button.


Creating Static IP WAN Connection

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

The screenshot shows a configuration interface with two main sections: **General settings** and **Ethernet**.
General settings includes:
 - Connection Type: Static IP (dropdown)
 - Port: WAN (dropdown)
 - Name: static_WAN_1 (text input)
 - Enable:
 - Direction: WAN
Ethernet section includes:
 - MTU: 1500 (text input)
 - MAC: (empty dropdown menu)

Figure 107. The page for creating a new connection. The **General settings** and **Ethernet** sections.

Parameter	Description
General settings	
Port	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	The maximum size of units transmitted by the interface.

Parameter	Description
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 button () 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>

IP

IP Address:^{*}

Netmask:^{*}

Gateway IP address:^{*}

Primary DNS server:^{*}

Secondary DNS server:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Ping:

Figure 108. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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.
Miscellaneous	
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 **Save** button.


Creating Dynamic IP WAN Connection

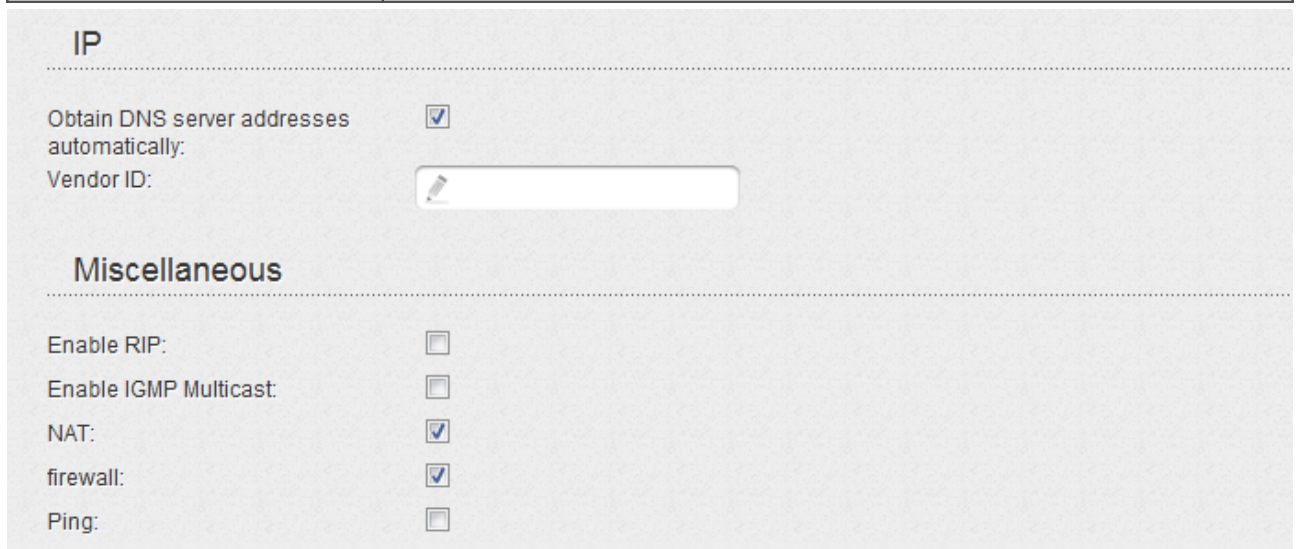
To create a connection of the Dynamic IP type, click the **Add** button on the **Net / WAN** page. On the opened page, select the **Dynamic IP** value from the **Connection Type** drop-down list and specify the needed values.

The screenshot shows a configuration interface with two main sections: **General settings** and **Ethernet**.
General settings includes:
 - Connection Type: Dynamic IP (dropdown)
 - Port: WAN (dropdown)
 - Name: dynamic_WAN_1 (text input with edit icon)
 - Enable:
 - Direction: WAN
Ethernet section includes:
 - MTU: 1500 (text input with edit icon)
 - MAC: (empty dropdown menu with edit icon and refresh icon)

Figure 109. The page for creating a new connection. The **General settings** and **Ethernet** sections.

Parameter	Description
General settings	
Port	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	The maximum size of units transmitted by the interface.

Parameter	Description
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 button () 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>



The screenshot shows a configuration page with two main sections: **IP** and **Miscellaneous**. The **IP** section includes a checkbox for "Obtain DNS server addresses automatically:" which is checked, and a "Vendor ID:" field with a text input box and a pencil icon. The **Miscellaneous** section includes five checkboxes: "Enable RIP:" (unchecked), "Enable IGMP Multicast:" (unchecked), "NAT:" (checked), "firewall:" (checked), and "Ping:" (unchecked).

Figure 110. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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>
Miscellaneous	
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 **Save** button.


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

To create a connection of the PPTP + Static IP or L2TP + Static 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 a configuration interface with two main sections: **General settings** and **Ethernet**.
General settings includes:
 - Connection Type: PPTP + Static IP (dropdown)
 - Port: WAN (dropdown)
 - Name: statpptp_WAN_1 (text input)
 - Enable:
 - Direction: WAN
Ethernet section includes:
 - MTU: 1500 (text input)
 - MAC: (empty dropdown menu)

Figure 111. The page for creating a new connection. The **General settings** and **Ethernet** sections.

Parameter	Description
General settings	
Port	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	The maximum size of units transmitted by the interface.

Parameter	Description
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 button () 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>

IP

IP Address:*

Netmask:*

Gateway IP address:*

Primary DNS server:*

Secondary DNS server:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Ping:

Figure 112. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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.

Parameter	Description
Miscellaneous	
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:

Extra options:

Dial on demand:

Static IP Address:

PPP debug:

IP received:

Figure 113. The page for creating a new 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.
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	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.
Extra options	Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional</i> .
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
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.
IP received	The IP address assigned by the ISP.

Miscellaneous

Enable RIP:

NAT:

firewall:

Ping:

Figure 114. The page for creating a new connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
Enable RIP	Select the checkbox to allow using RIP for this connection.
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 **Save** button.


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

To create a connection of the 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.

The screenshot shows a configuration interface with two main sections: **General settings** and **Ethernet**.
General settings includes:
 - Connection Type: PPTP + Dynamic IP (dropdown)
 - Port: WAN (dropdown)
 - Name: dynpptp_WAN_1 (text input with edit icon)
 - Enable:
 - Direction: WAN
Ethernet section includes:
 - MTU: 1500 (text input with edit icon)
 - MAC: (dropdown menu with edit icon and refresh icon)

Figure 115. The page for creating a new connection. The **General settings** and **Ethernet** sections.

Parameter	Description
General settings	
Port	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	The maximum size of units transmitted by the interface.

Parameter	Description
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 button () 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>

IP

Obtain DNS server addresses automatically:

Vendor ID:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Ping:

Figure 116. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

Parameter	Description
IP	
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>
Miscellaneous	
Enable RIP	Select the checkbox to allow using RIP for this connection.

Parameter	Description
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:

Extra options:

Dial on demand:

Static IP Address:

PPP debug:

IP received:

Figure 117. The page for creating a new 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.
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	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.
Extra options	Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional.</i>
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
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.
IP received	The IP address assigned by the ISP.

Miscellaneous

Enable RIP:

NAT:

firewall:

Ping:

Figure 118. The page for creating a new connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
Enable RIP	Select the checkbox to allow using RIP for this connection.
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 **Save** button.

LAN

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

The screenshot shows the LAN configuration interface. It features two input fields: 'IP Address:*' with the value '192.168.0.50' and 'Netmask:*' with the value '255.255.255.0'. Each field has a small edit icon to its left.

Figure 119. 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 **Save** 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 which is unchecked, and three input fields: 'Start IP:*' with '192.168.0.51', 'End IP:*' with '192.168.0.100', and 'Lease time (min):*' with '86400'. Each input field has an edit icon.

Figure 120. 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 transmitted by the ISP or specified on the Advanced / DNS page as the DNS server address. Deselect the checkbox so that the devices connected to the access point obtain the address of the access point 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 **Save** 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).

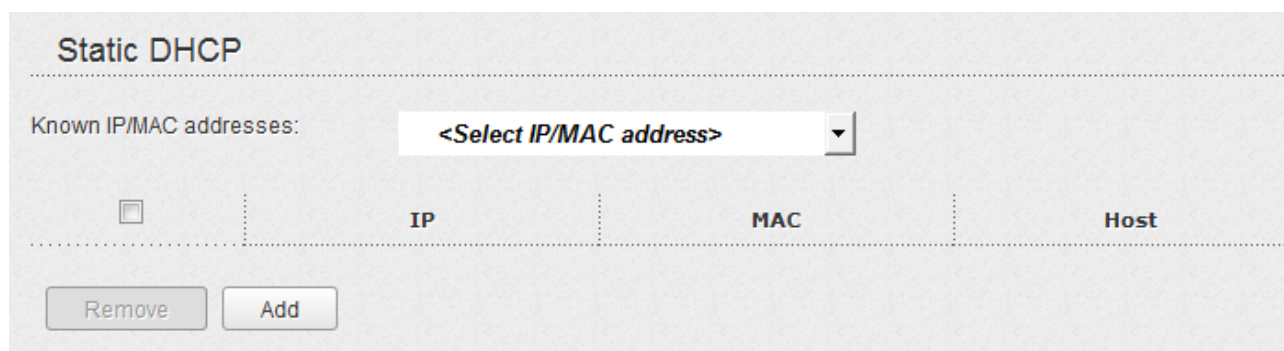


Figure 121. The section for creating MAC-IP pairs.

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 **IP** and **MAC** fields will be filled in automatically).

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

Wi-Fi

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

Common settings

On the **Wi-Fi / Common settings** page, you can enable your wireless local area network (WLAN) and split it into parts.



Figure 122. Common settings of the wireless LAN.

The **Enable Wireless** checkbox enables Wi-Fi connections. By default, the checkbox is selected. If you want to disable your WLAN, deselect the **Enable Wireless** checkbox.

The access point allows splitting your WLAN into several parts (up to four) with their own names (SSIDs) and unique identifiers (BSSIDs). To split the network into several parts, select a relevant value (**2**, **3**, or **4**) from the **MBSSID** drop-down list. By default, the wireless network is not splitted (the **Disabled** value is selected from the list).

The value from the **BSSID** drop-down list is 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.

If you have splitted your WLAN into parts, the **BSSID** drop-down list contains several values. Each identifier corresponds to a single part of the WLAN.

For every part of the WLAN you can specify a name (SSID), security settings, rules for MAC filtering, and enable the WMM function (if needed). To specify these values, select the needed part from the **BSSID** drop-down list and click the **Change** button. Then proceed to the relevant page of the **Wi-Fi** menu section.

Basic Settings

On the **Wi-Fi / Basic settings** page, you can configure basic parameters of the device's WLAN.

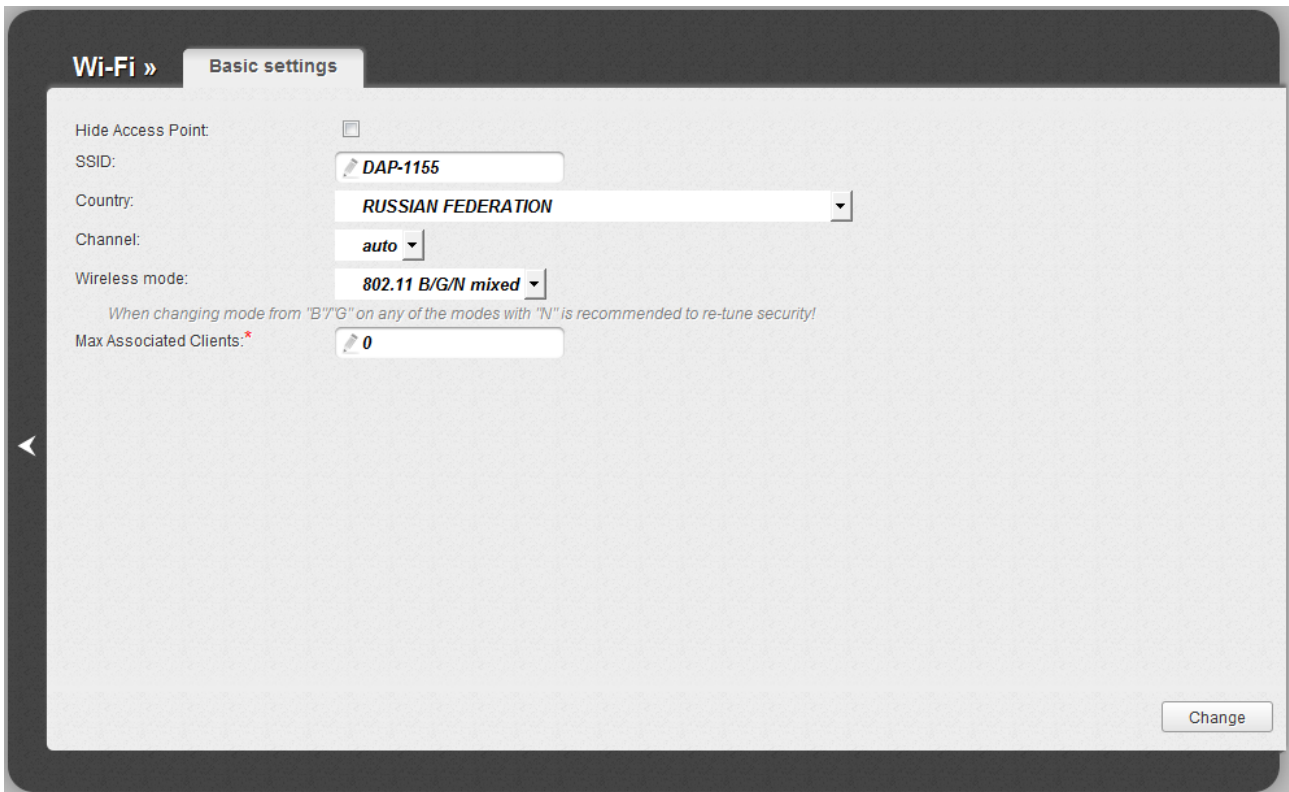


Figure 123. Basic settings of the wireless LAN.

Parameter	Description
Hide Access Point	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.)
SSID	A name for the WLAN. By default, the value DAP-1155 is specified. If your network is splitted into parts, each part has the default name (DAP-1155.2 , DAP-1155.3 , and DAP-1155.4). It is recommended to specify another name for the network upon initial configuration (use digits and Latin characters).
Country	The country you are in. Select a value from the drop-down list.
Channel	The wireless channel number. When the auto value is selected, the access point itself chooses the channel with the least interference.
Wireless mode	Operating mode of the wireless network of the access point. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
Max Associated Clients	The maximum number of devices connected to the wireless network of the access point. When the value 0 is specified, the device does not limit the number of connected clients.

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

Security Settings

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

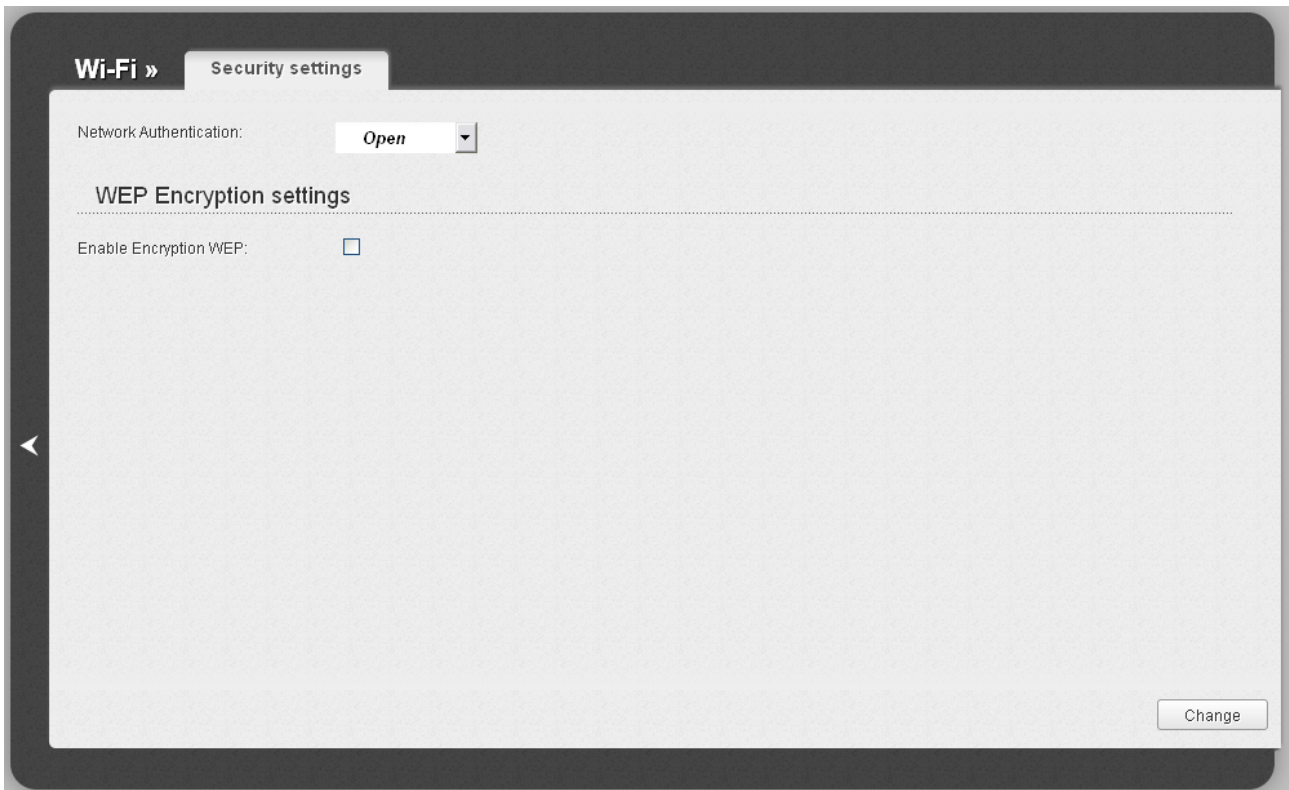


Figure 124. The default security settings.

By default, the **Open** network authentication type with no encryption is specified for the WLAN.

! The default security settings do not provide sufficient protection for the WLAN. Please, specify your own security settings for the WLAN (or each part of the WLAN if the network was splitted into parts).

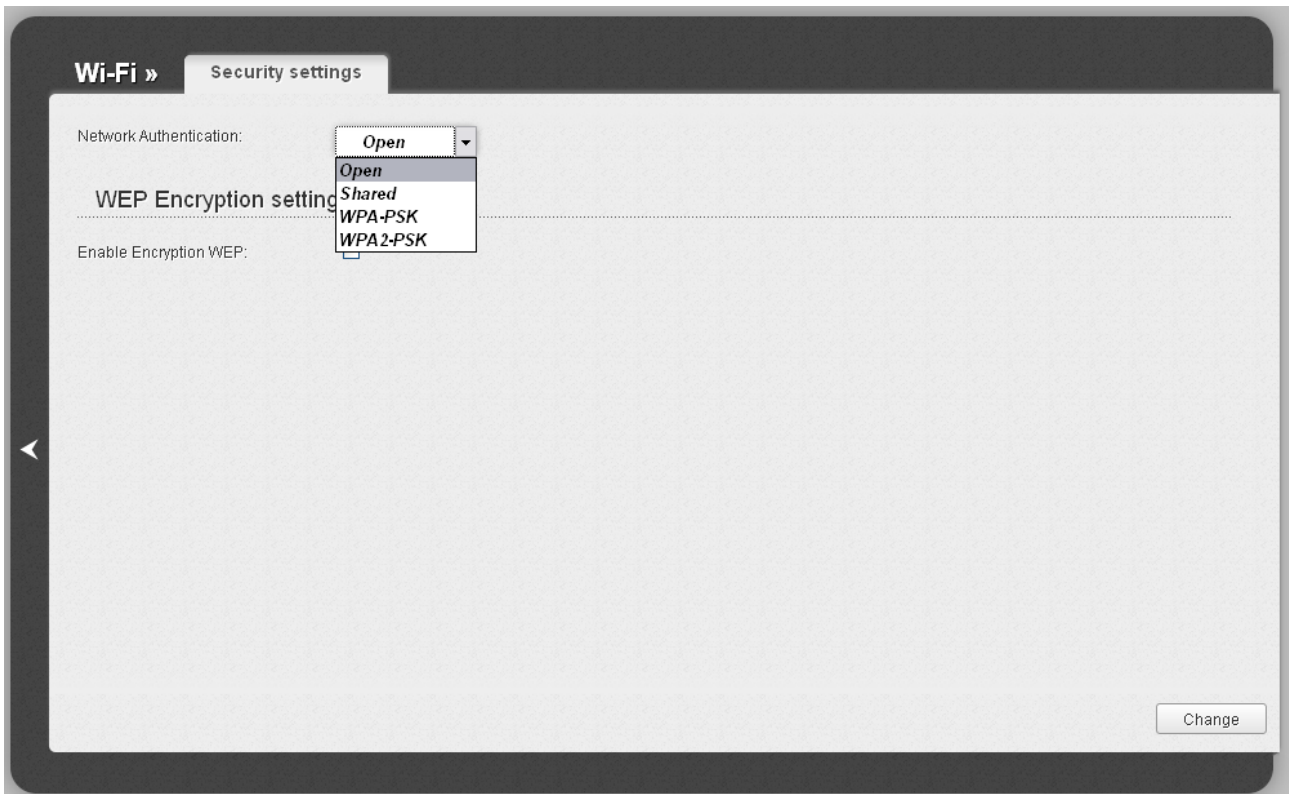


Figure 125. Network authentication types supported by the access point.

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-PSK	WPA-based authentication using a PSK.
WPA2-PSK	WPA2-based authentication using a PSK.

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):

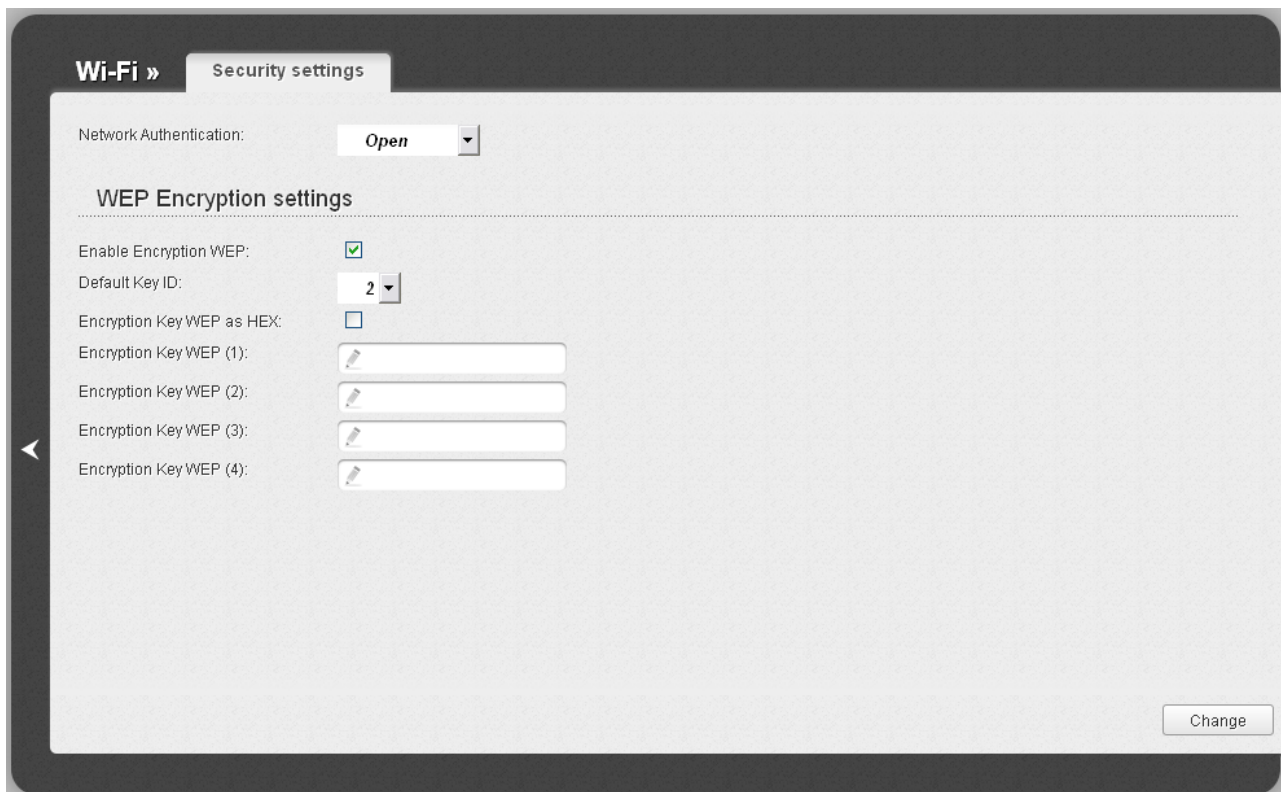


Figure 126. The **Open** value is selected from the **Network Authentication** drop-down list.

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, 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.
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. You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters). If the Encryption Key WEP as HEX checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F).

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

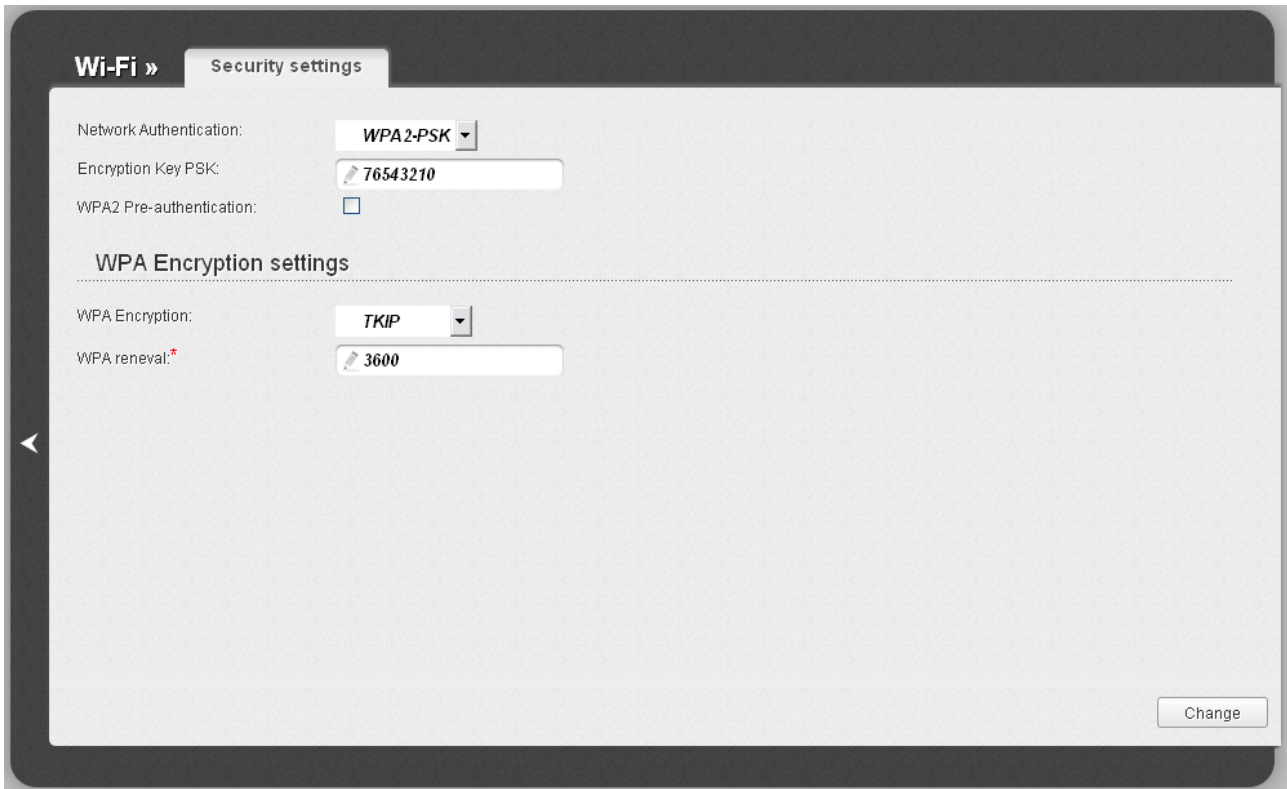


Figure 127. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
Encryption Key PSK	A key for WPA encryption. The key can contain digits and/or Latin characters.
WPA2 Pre-authentication	The checkbox activating preliminary authentication (displayed only for the WPA2-PSK authentication type).
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 **Change** button.

MAC Filter

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



Figure 128. MAC filters for the wireless network.

By default, MAC filtering is not active (the **Disabled** choice of the **MAC filter restrict mode** radio button is selected).

To open your wireless network for the devices which MAC addresses are specified on the **MAC addresses** tab and to close the wireless network for all other devices, select the **Allow** choice of the **MAC filter restrict mode** radio button and click the **Change** button.

To close your wireless network for the devices which MAC addresses are specified on the **MAC addresses** tab, select the **Deny** choice of the **MAC filter restrict mode** radio button and click the **Change** button.

To add a MAC address to which the selected filtering mode will be applied, proceed to the **MAC addresses** tab.



Figure 129. The tab for adding a MAC address.

Enter an address in the **MAC address** field of the **MAC address adding** section and click the **Add** button.

To remove a MAC address from the list of MAC addresses, select the checkbox located to the right of the relevant MAC address in the MAC address list section and click the **Delete** button.

Station List

On the **Wi-Fi / Station List** 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.

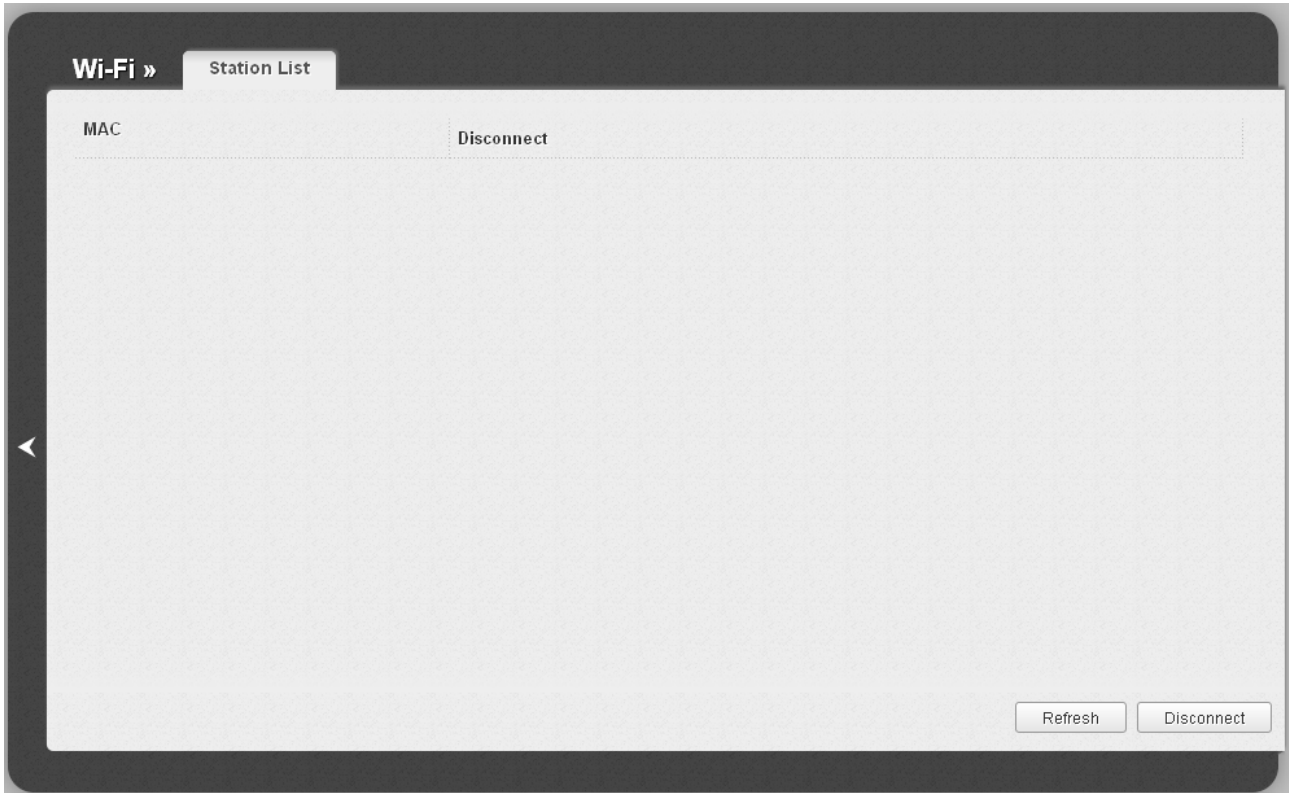


Figure 130. The list of the wireless clients.

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 access point's WLAN is splitted into parts (the value **2**, **3**, or **4** is selected from the **MBSSID** drop-down list on the **Wi-Fi / Common 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, **WPA-PSK** or **WPA2-PSK** with the **AES** or **TKIP+AES** encryption method (on the **Wi-Fi / Security settings** page).

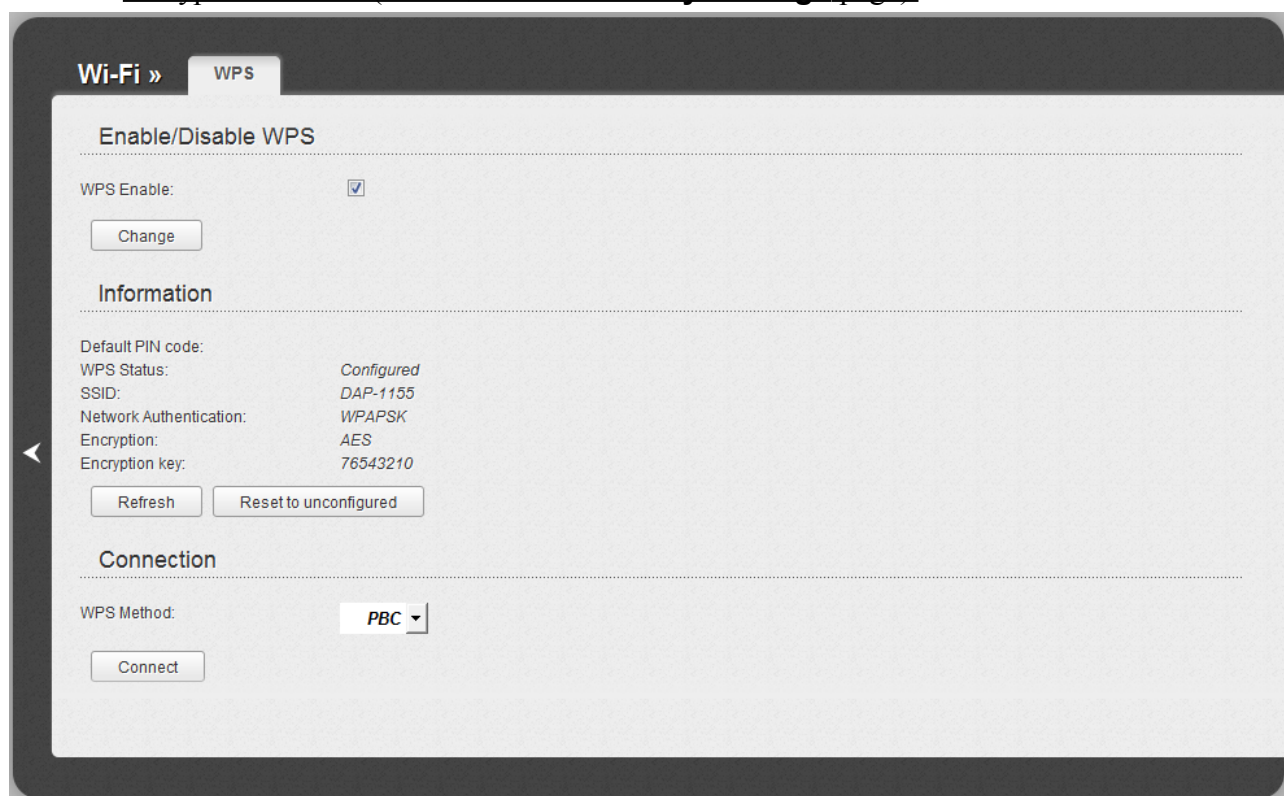


Figure 131. The page for configuring the WPS function.

To activate the WPS function, select the **WPS Enable** checkbox and click the **Change** 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) • Unconfigured (you need to specify the relevant settings).
SSID	The name of the access point's WLAN (or the first part of the WLAN if the network is splitted 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 **Change** 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 **Change** 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:

6. Specify corresponding security settings for the wireless network of the access point.
7. Select the **WPS Enable** checkbox.
8. Click the **Change** button.
9. Save the settings and close the web-based interface (click the **Save** line in the top-page menu displayed when the mouse pointer is over the **System** caption, then click the **Logout** line).

Later you will be able to add wireless devices to the WLAN by pressing the **WPS/RESET** 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/RESET** button of the access point and immediately release it.

After clicking the button the **WPS** LED blinks green. If the wireless device has been successfully connected to the WLAN, the LED stops blinking and lights green for several minutes.

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.

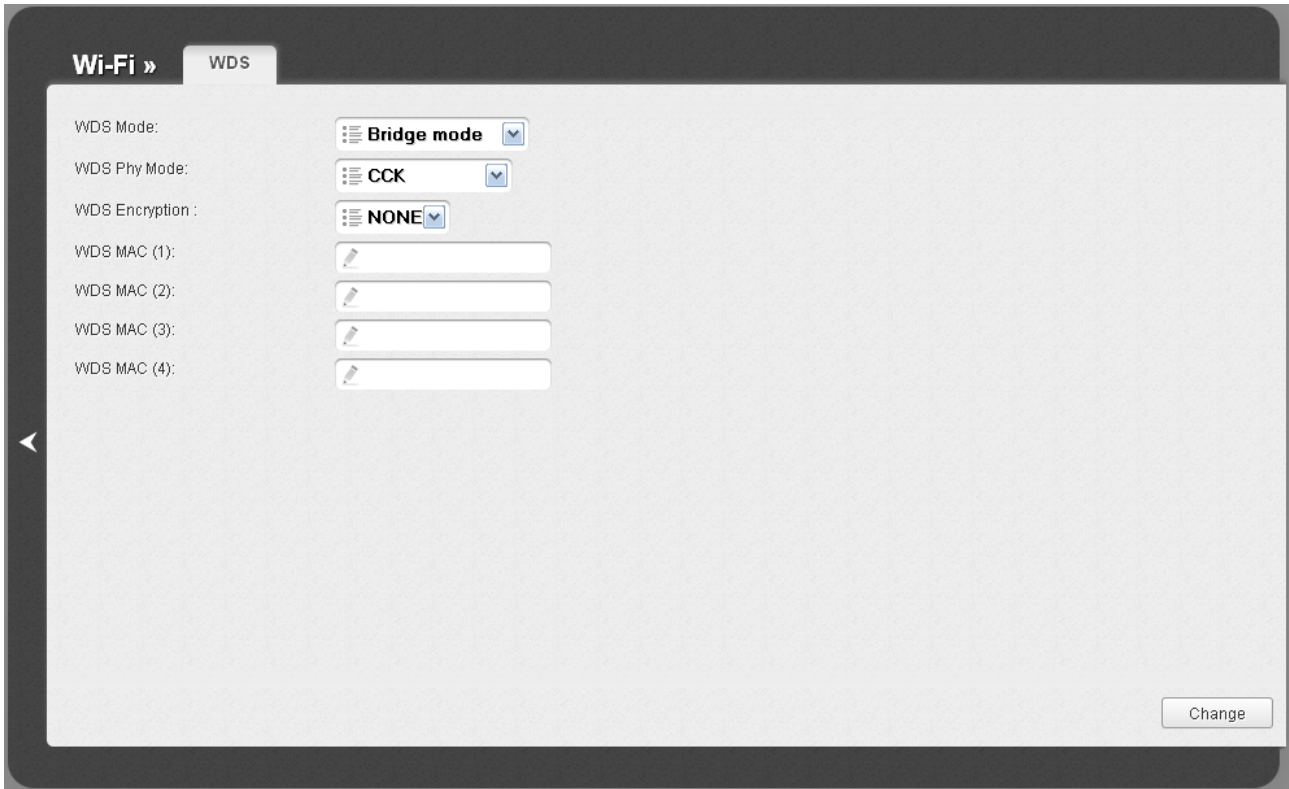


Figure 132. The page for configuring the WDS function.

The following fields are available on the page:

Parameter	Description
WDS Mode	<p>The WDS function mode.</p> <p>Disable: The function is disabled.</p> <p>Bridge mode: Access points communicate to each other only, wireless devices cannot connect to them.</p> <p>Repeater mode: Access points communicate to each other, wireless clients can connect to the WLAN created by interconnected access points.</p>
WDS Phy Mode	<p>A physical mode of data transfer between access points interconnected via the WDS function.</p> <p>CCK: 802.11b devices only.</p> <p>OFDM: 802.11g devices only.</p> <p>HTMIX: 802.11g and 802.11n devices.</p> <p>GREENFIELD: 802.11n devices only.</p>
WDS Encryption	<p>A type of encryption for data transfer between access points interconnected via the WDS function.</p> <p>NONE: No encryption.</p> <p>WEP.</p> <p>TKIP.</p> <p>AES.</p>
Encryption Key	<p>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 displayed.</p>
WDS MAC (1-4)	<p>The MAC addresses of devices connected to the access point via the WDS function.</p>



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

When you have configured the parameters, click the **Change** 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!

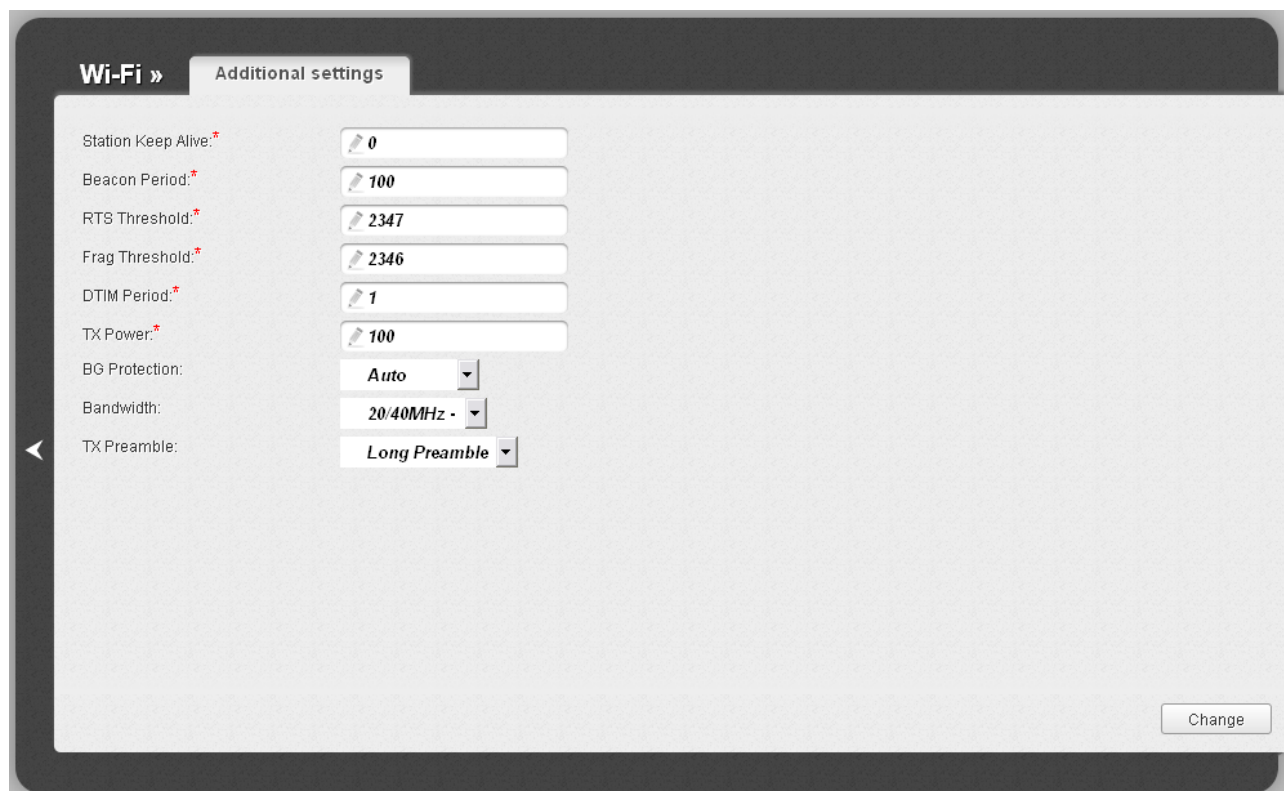


Figure 133. Additional settings of the WLAN.

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.
BG Protection	<p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <p>Auto: The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices).</p> <p>Always On: The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</p> <p>Always Off: The protection function is always disabled.</p>
Bandwidth	<p>The channel bandwidth for 802.11n devices.</p> <p>20MHz: 802.11n devices operate at 20MHz channels.</p> <p>40MHz: 802.11n devices operate at 40MHz channels.</p> <p>20/40MHz -: 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the previous adjacent channel).</p> <p>20/40MHz +: 802.11n devices operate at 20MHz and 40MHz channels (the channel is combined with the next adjacent channel).</p>
TX Preamble	<p>This parameter defines the length of the CRC block sent by the access point when communicating to wireless devices.</p> <p>Select a value from the drop-down list.</p> <p>Long Preamble.</p> <p>Short Preamble (this value is recommended for networks with high-volume traffic).</p>

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

The screenshot shows the WMM configuration interface. At the top, 'WMM' is checked. Below are two sections: 'Parameters of Access Point' and 'Parameters of Station'. Each section contains a table with columns for AC, Aifsn, CWMin, CWMax, Txop, ACM, and Ack. The 'Change' button is at the bottom right.

Parameters of Access Point						
AC	Aifsn	CWMin	CWMax	Txop	ACM	Ack
AC_BK	7	1	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

Parameters of Station						
AC	Aifsn	CWMin	CWMax	Txop	ACM	
AC_BK	7	15	1023	0	<input type="checkbox"/>	
AC_BE	3	15	1023	0	<input type="checkbox"/>	
AC_VI	2	7	15	94	<input type="checkbox"/>	
AC_VO	2	3	7	47	<input type="checkbox"/>	

Figure 134. 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 selected, 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 not selected, the access point answers requests. If selected, the access point does not answer requests.

When you have configured the parameters, click the **Change** 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-1155 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-1155 and the WISP access point. Other parameters of the wireless network of DAP-1155 do not depend upon the settings of the WISP access point.

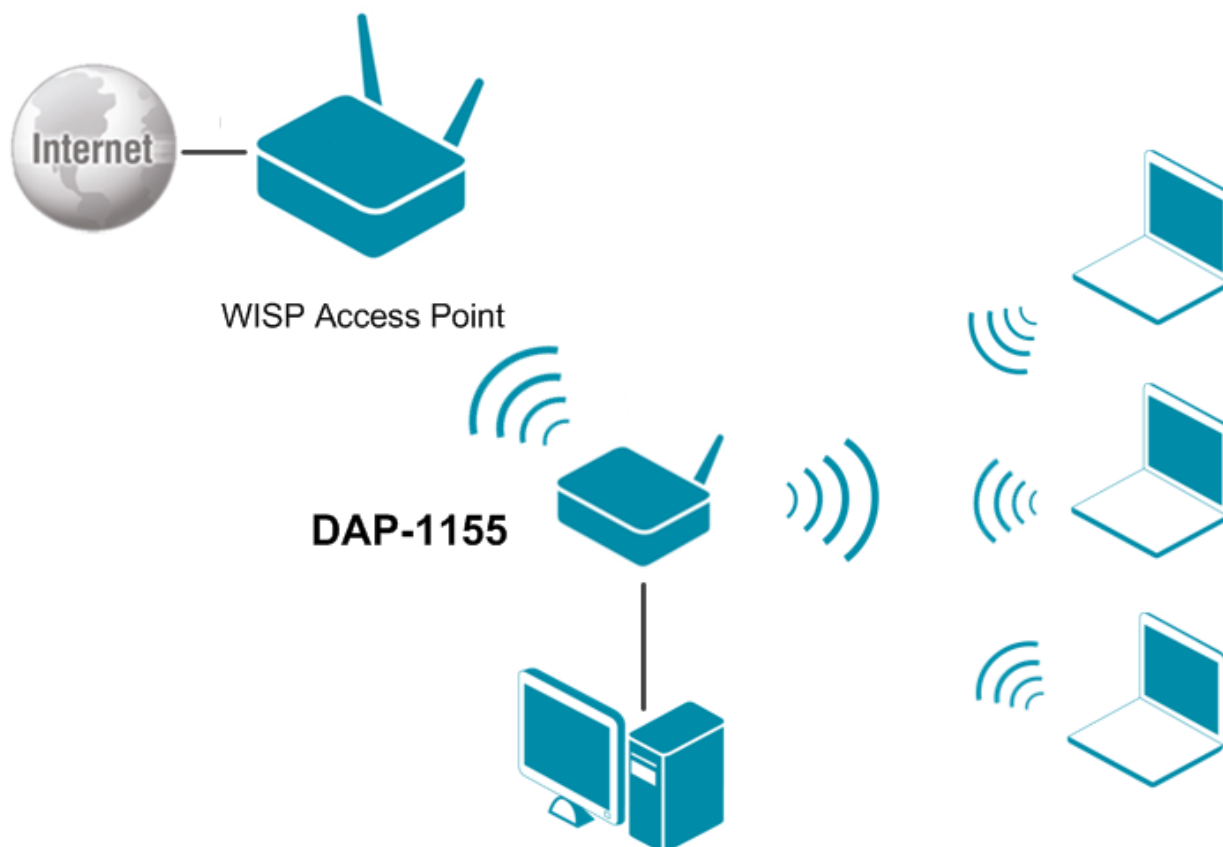


Figure 135. Connecting DAP-1155 in the router mode as a client.

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

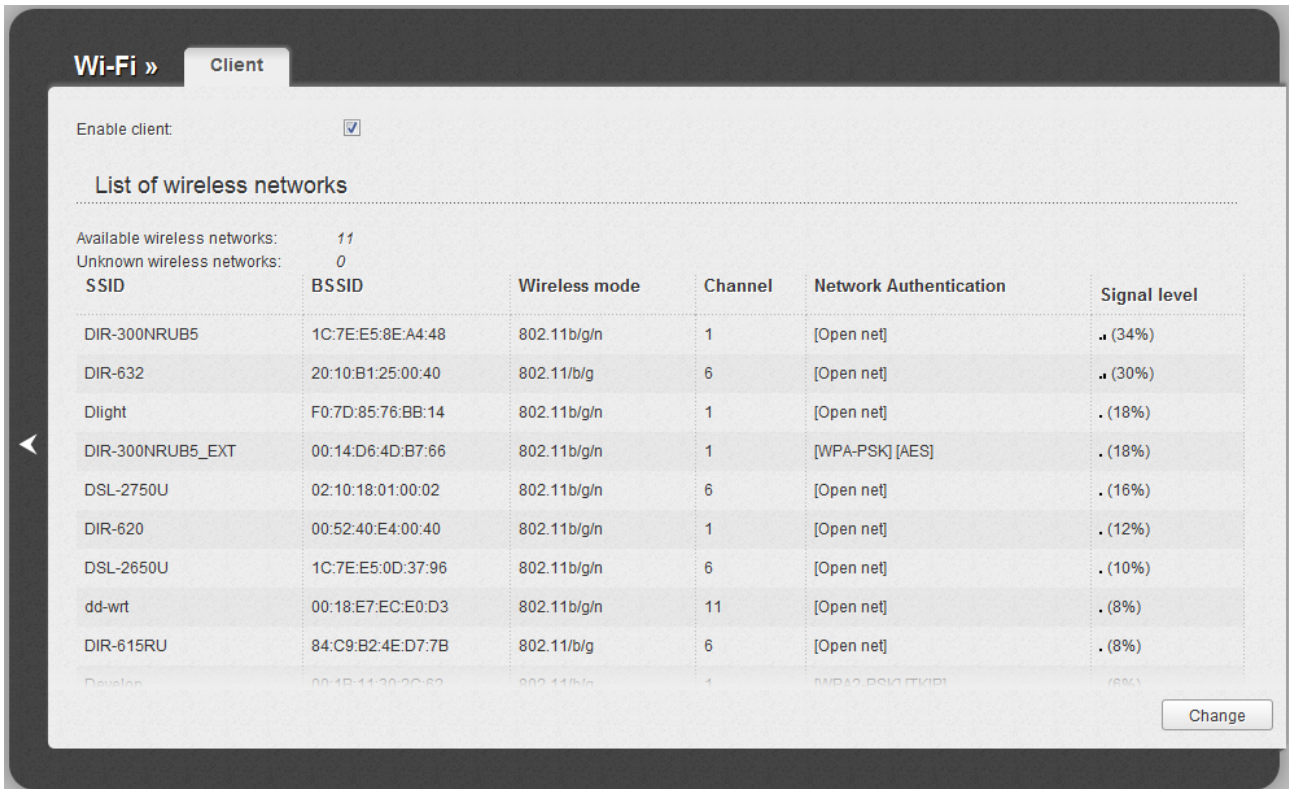


Figure 136. The page for configuring the client mode.

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
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 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 (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. You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters).

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

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

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

In addition, when the **Enable client** checkbox is selected, the list of available wireless networks is displayed on the page. The **Unknown wireless networks** field shows the number of hidden wireless networks.

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 **Change** 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, fill in 4 **Encryption Key WEP** fields, and click the **Change** 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 **Change** button.

After clicking the **Change** button, the wireless channel of DAP-1155 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.

Advanced

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

- enable the UPnP function
- 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.

UPnP

On the **Advanced / UPnP** page, you can enable and disable the UPnP function.

UPnP is a set of networking protocols designed for automatic configuration of network devices. The UPnP function performs automatic configuration of the device's parameters for network applications requiring an incoming connection to the access point.

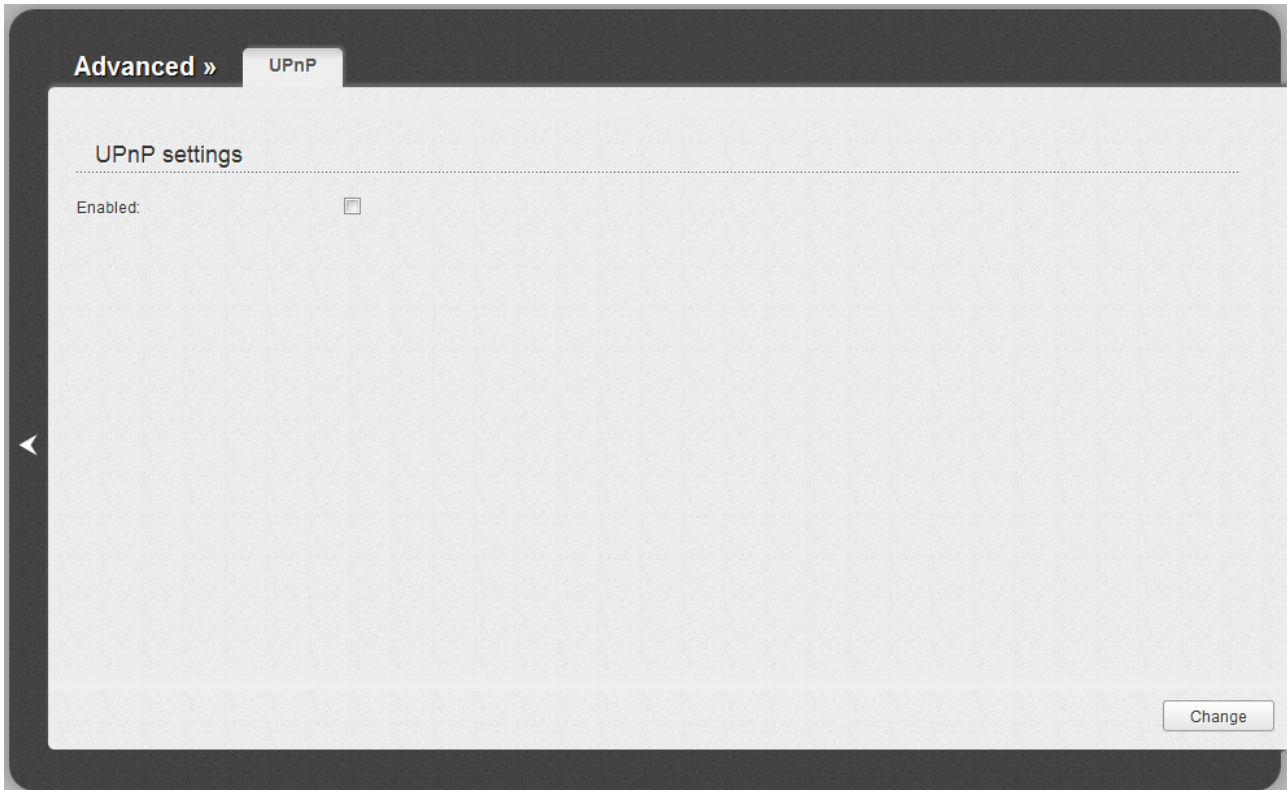


Figure 137. The **Advanced / UPnP** page.

If you want to enable the UPnP function in the access point, select the **Enabled** checkbox and click the **Change** button.

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

DDNS

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

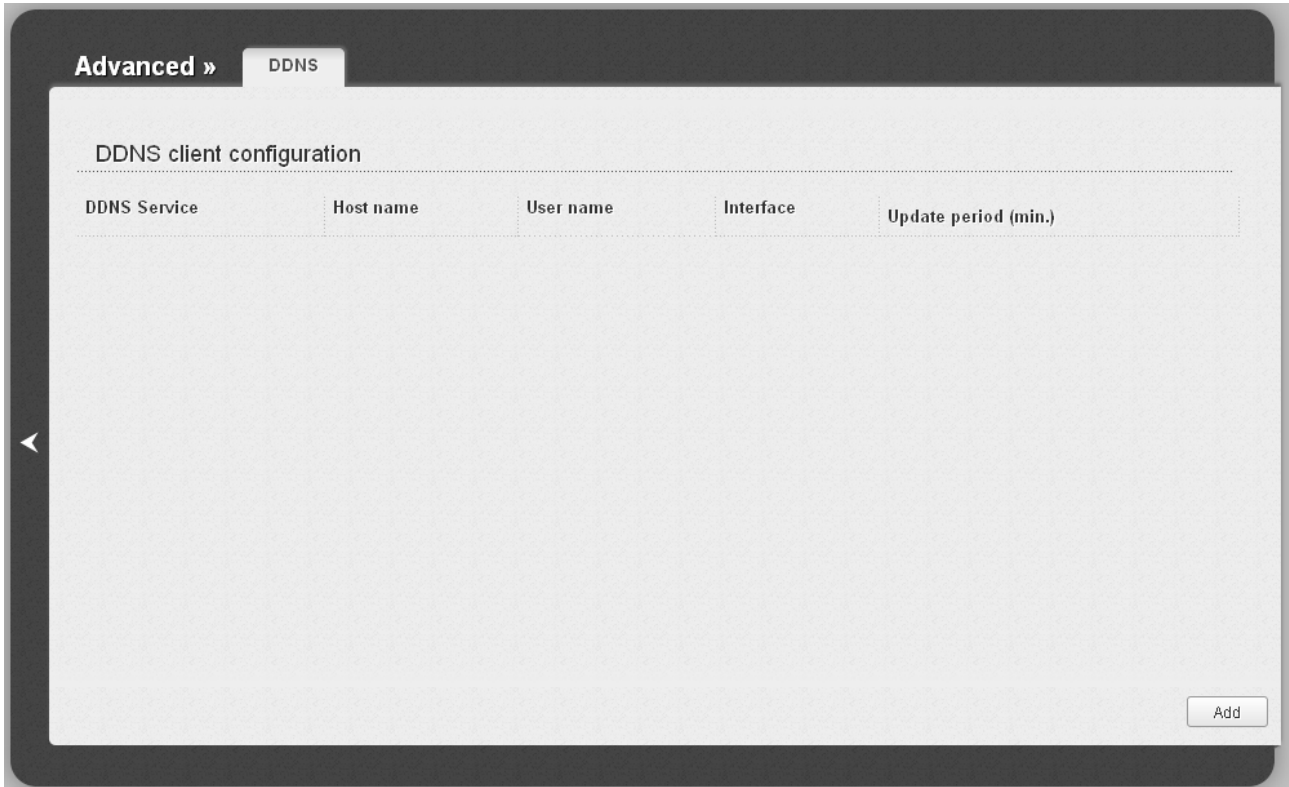


Figure 138. The **Advanced / DDNS** page.

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

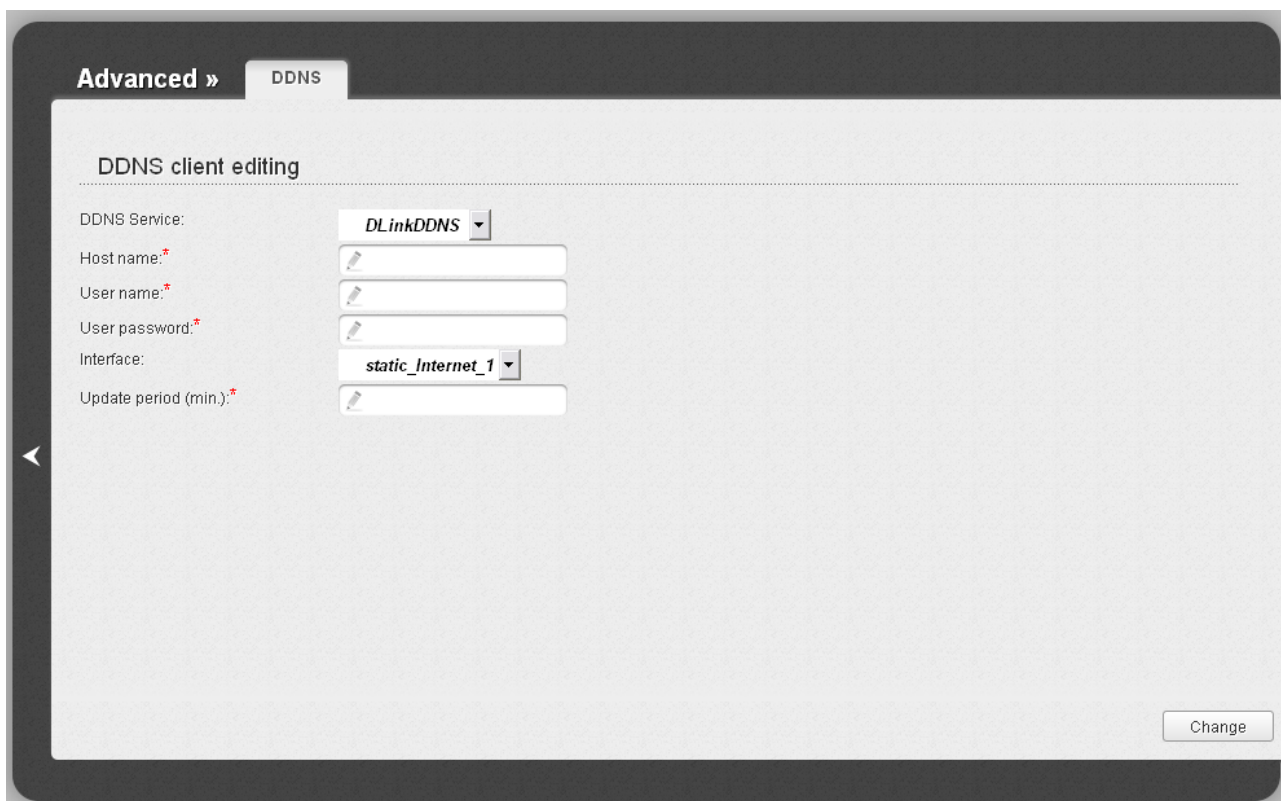


Figure 139. The page for editing the DDNS service.

You can specify the following parameters:

Parameter	Description
DDNS Service	Select a DDNS provider from the drop-down list.
Host name	The domain name registered at your DDNS provider.
User name	The username to authorize for your DDNS provider.
User password	The password to authorize for your DDNS provider.
Interface	Select a WAN connection which IP address will be used to access the DDNS service.
Update period	An interval (in minutes) between sending data with the IP address of the interface specified in the field above to the relevant DDNS service.

Click the **Change** button.

To edit parameters of the existing DDNS service, click the relevant service link. On the opened page, change the needed parameters and click the **Change** button.

To remove an existing DDNS service, click the relevant service link. On the opened page, click the **Delete** button.

DNS

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

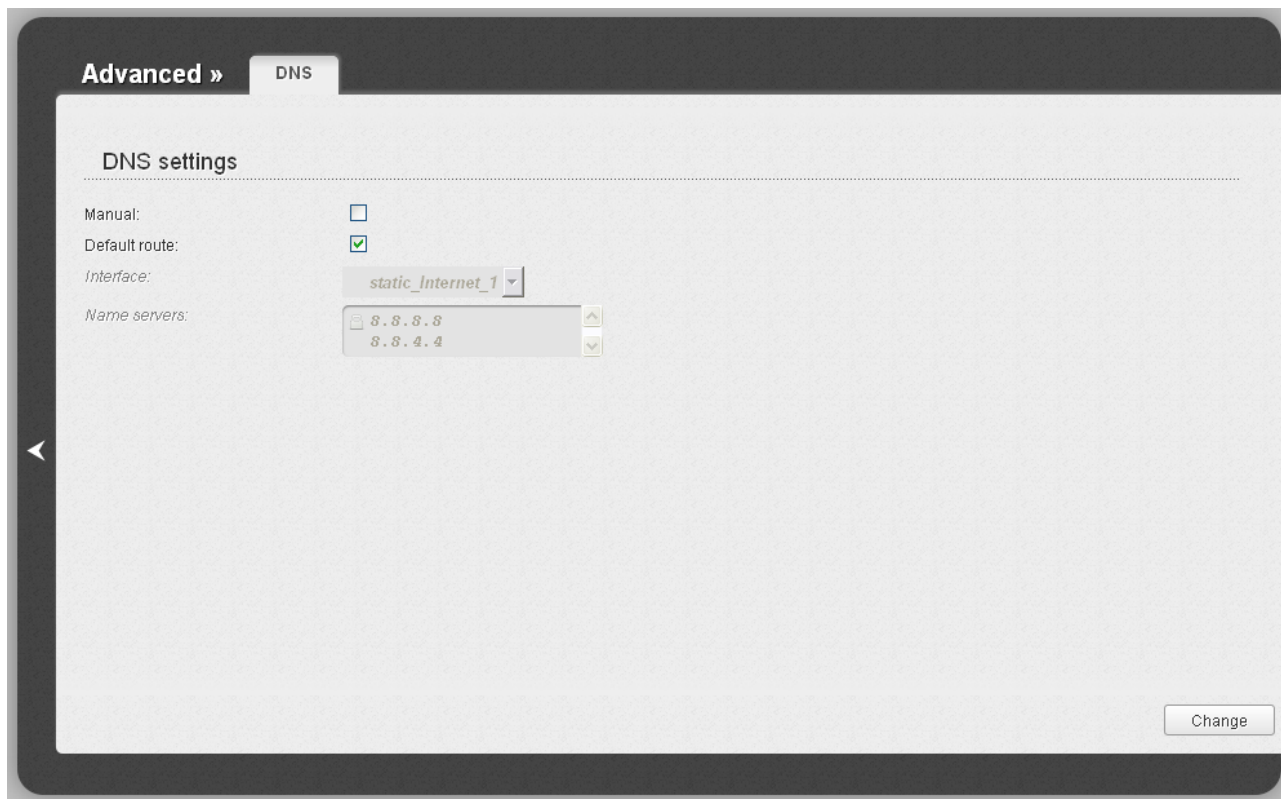


Figure 140. The **Advanced / DNS** page.

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).

The device performs the DNS relay function, i.e., it redirects the DNS requests of users to external DNS servers. 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 **Change** 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 **Change** button.

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

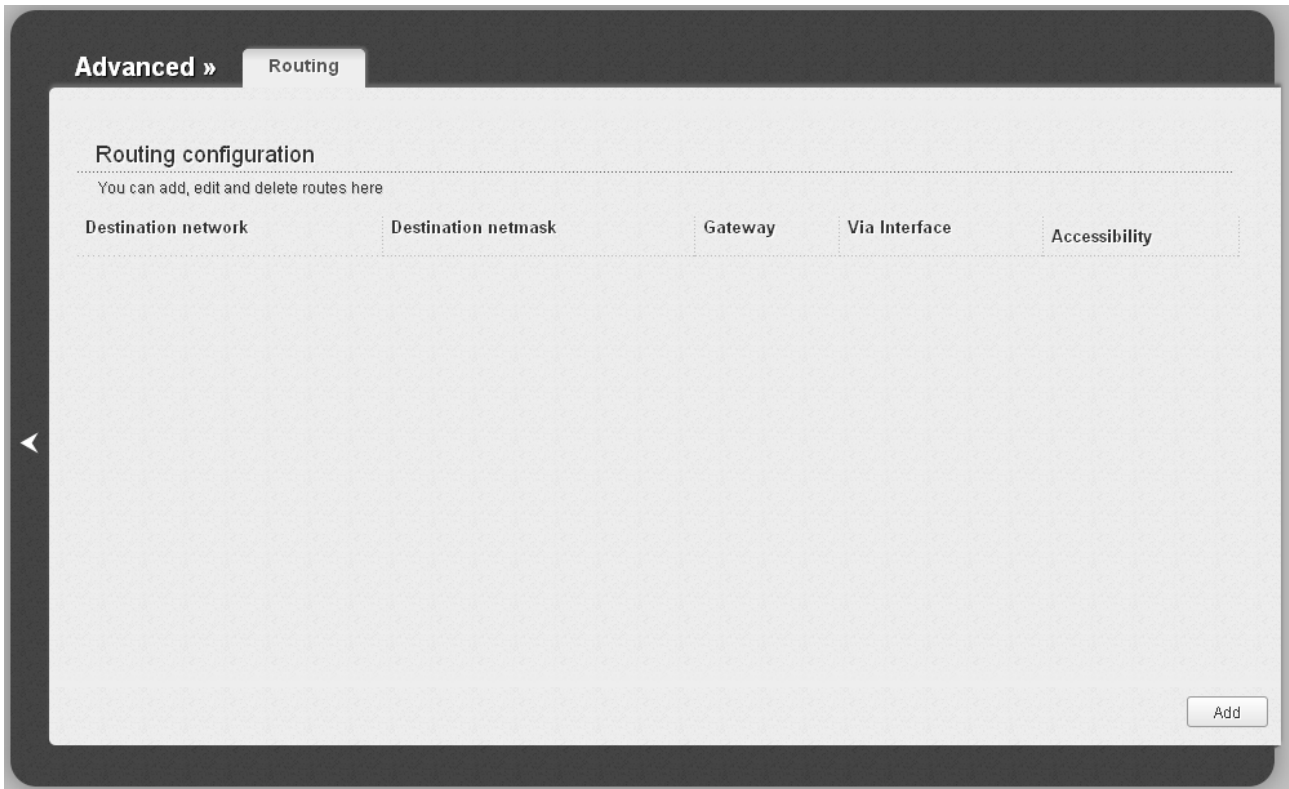


Figure 141. The **Advanced / Routing** page.

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

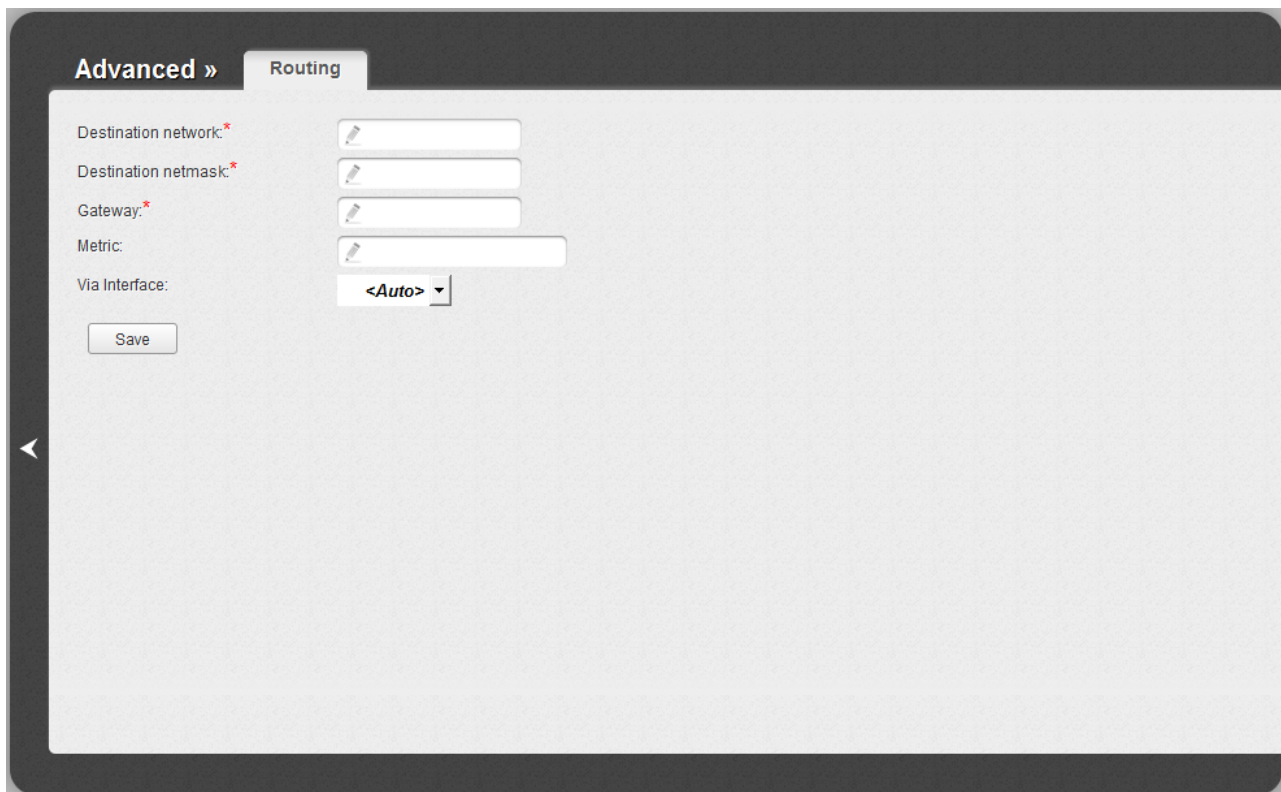


Figure 142. The page for adding a static route.

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 displayed when the <Auto> value is selected from the Via Interface drop-down list.
Metric	A metric for the route. The lower the value, the higher is the route priority. <i>Optional.</i>
Via Interface	Select an interface through which the destination network can be accessed from the drop-down list. If you have selected the <Auto> value of this drop-down list, the access point itself sets the interface on the basis of data on connected networks.

Click the **Save** button.

To edit an existing route, click the relevant route link. On the opened page, change the needed parameters and click the **Save** button.

To remove an existing route, click the relevant route link. On the opened page, click the **Delete** button.

Remote Access

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



Figure 143. The **Advanced / Remote access** page.

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



Figure 144. The page for adding a rule for remote management.

You can specify the following parameters:

Parameter	Description
IP address	A host or a subnet to which the rule is applied. 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).
Mask	The mask of the subnet.
Protocol	The protocol available for remote management of the access point.
Public port	An external port of the access point. You can specify only one port.

Click the **Change** button.

To edit a rule for remote access, click the relevant link. On the opened page, change the needed parameters and click the **Change** button.

To remove a rule for remote access, click the relevant link. On the opened page, click the **Delete** button.

IGMP

On the **Advanced / IGMP** page, you can enable IGMP for the access point.

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

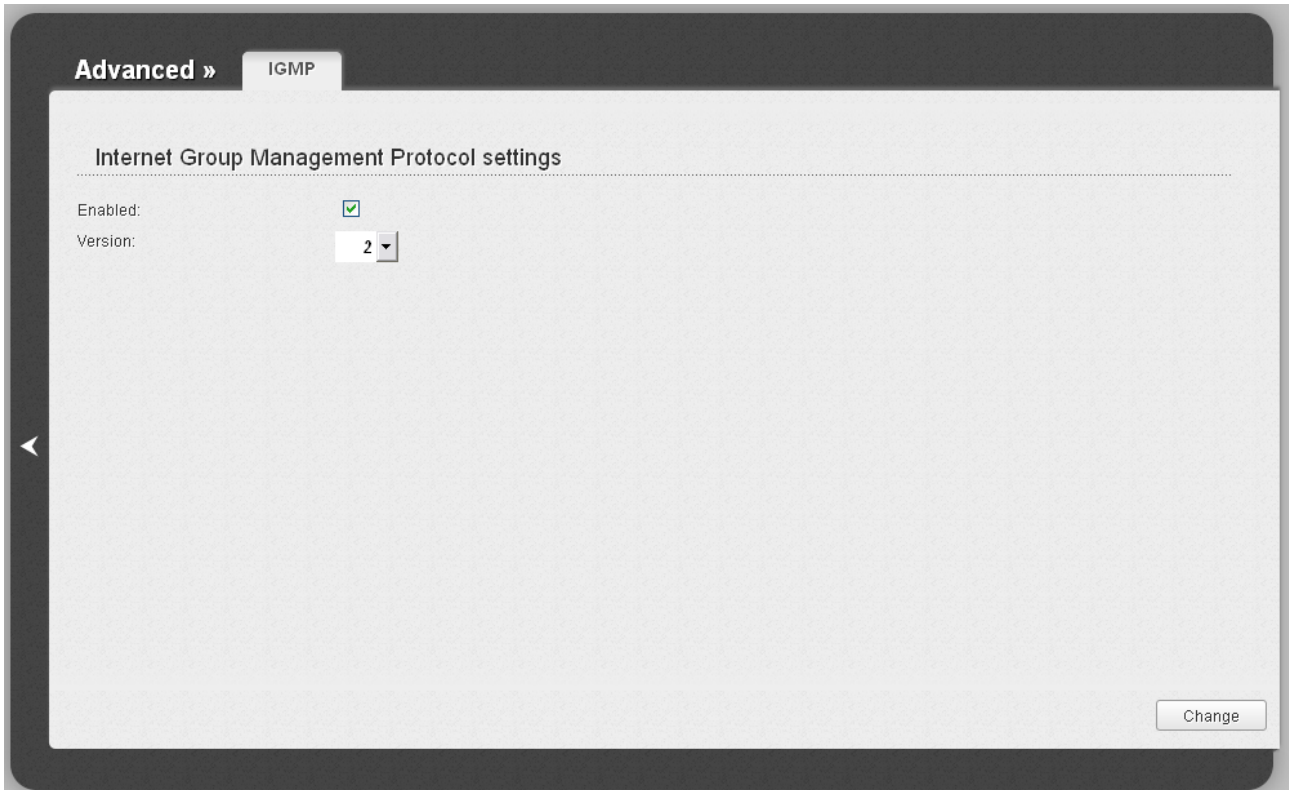


Figure 145. The **Advanced / IGMP** page.

To enable IGMP, select the **Enabled** checkbox. From the **Version** drop-down list, select a version of IGMP. Then click the **Change** button. 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, deselect the **Enabled** checkbox and click the **Change** button.

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.

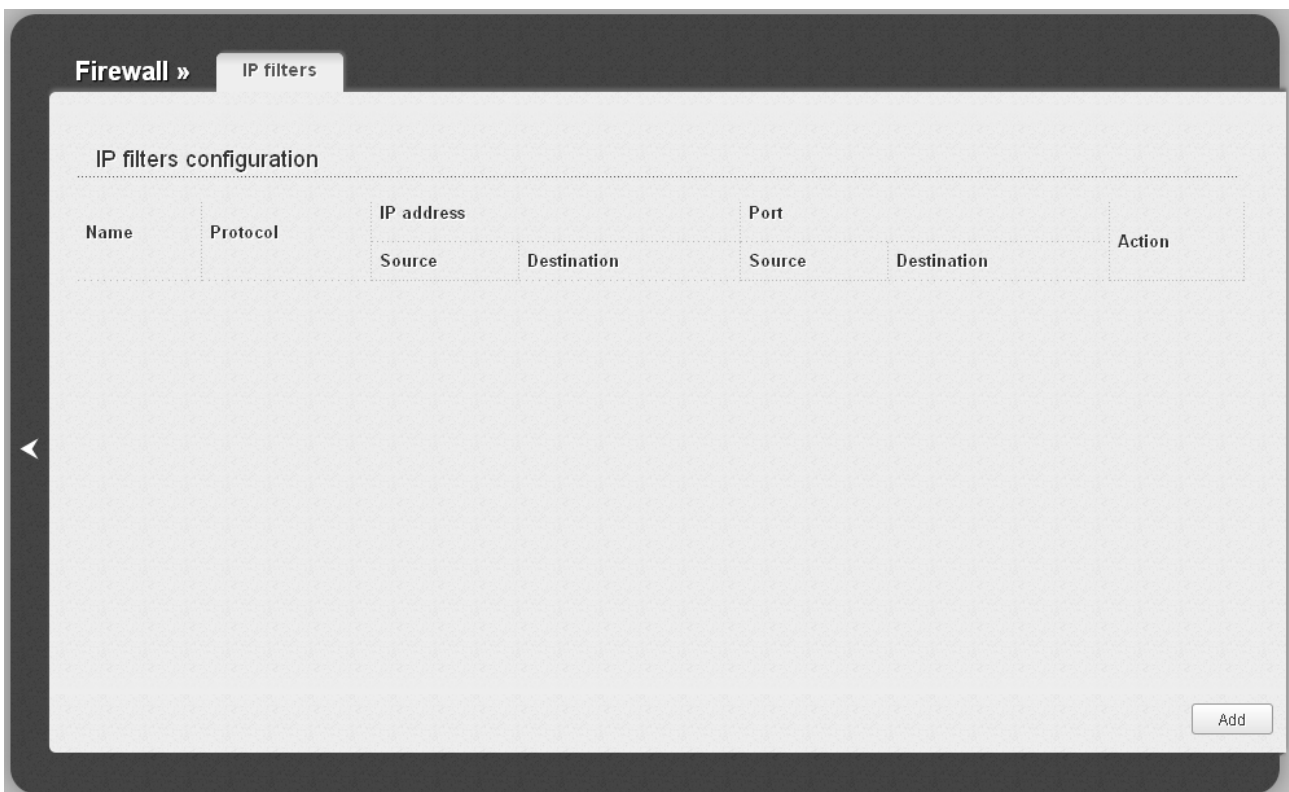


Figure 146. The **Firewall / IP filters** page.

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

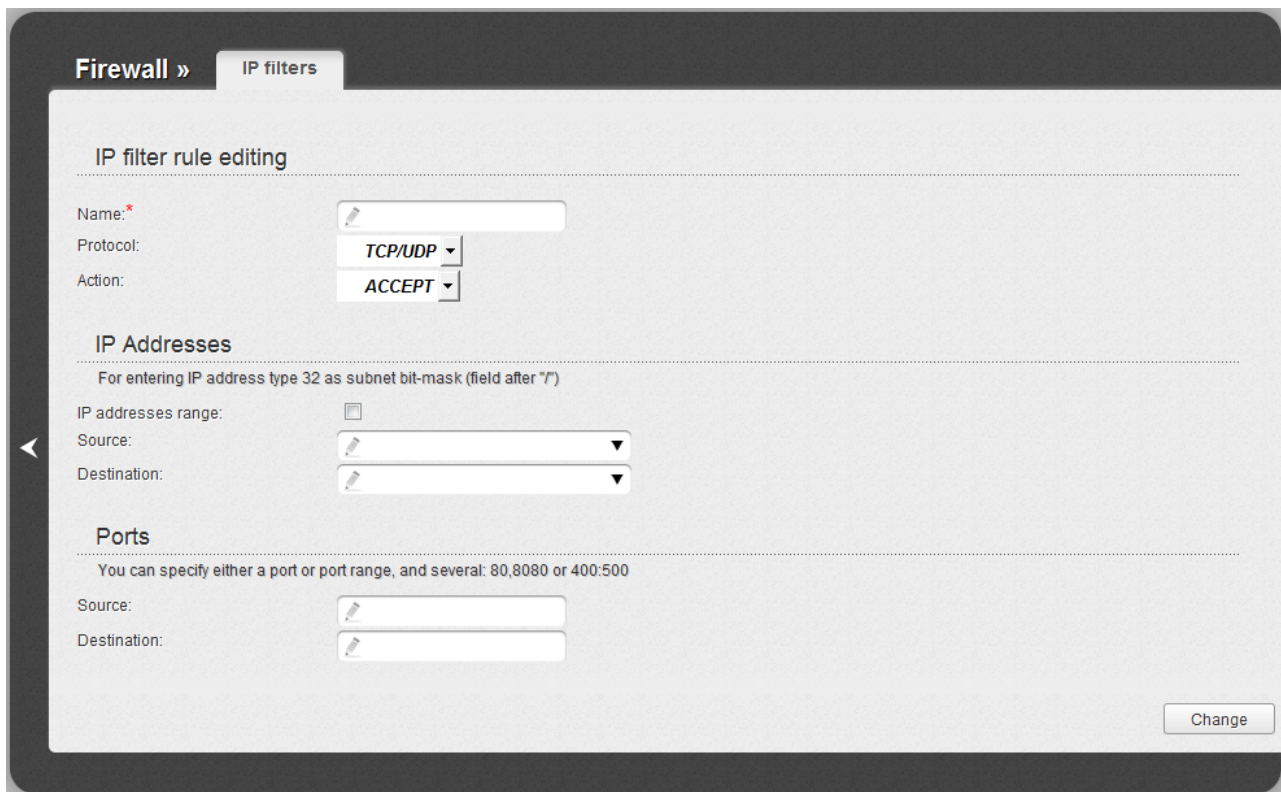


Figure 147. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
IP filter rule editing	
Name	A name for the rule for easier identification.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.
Action	Select an action for the rule. ACCEPT: Allows packet transmission in accordance with the criteria specified by the rule. DROP: Denies packet transmission in accordance with the criteria specified by the rule.
IP Addresses	
IP address range	Select the checkbox if you want to specify a range of IP addresses as the source or destination IP address.

Parameter	Description
Source	<p>The source host/subnet IP address.</p> <p>If the IP address range checkbox is selected, specify the starting IP address of the range in the Source (first) field and the ending IP address in the Source (last) field.</p> <p>If the IP address range checkbox is not selected, specify the IP address of the host or subnet in the Source field. To specify an IP address add /32.</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>
Destination	<p>The destination host/subnet IP address.</p> <p>If the IP address range checkbox is selected, specify the starting IP address of the range in the Destination (first) field and the ending IP address in the Destination (last) field.</p> <p>If the IP address range checkbox is not selected, specify the starting IP address of the host or subnet in the Destination field. To specify an IP address add /32.</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>
Ports	
Source	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.
Destination	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.

Click the **Change** 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 **Change** button.

To remove a rule for IP filtering, click the link to the relevant rule. On the opened page, click the **Delete** button.

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.

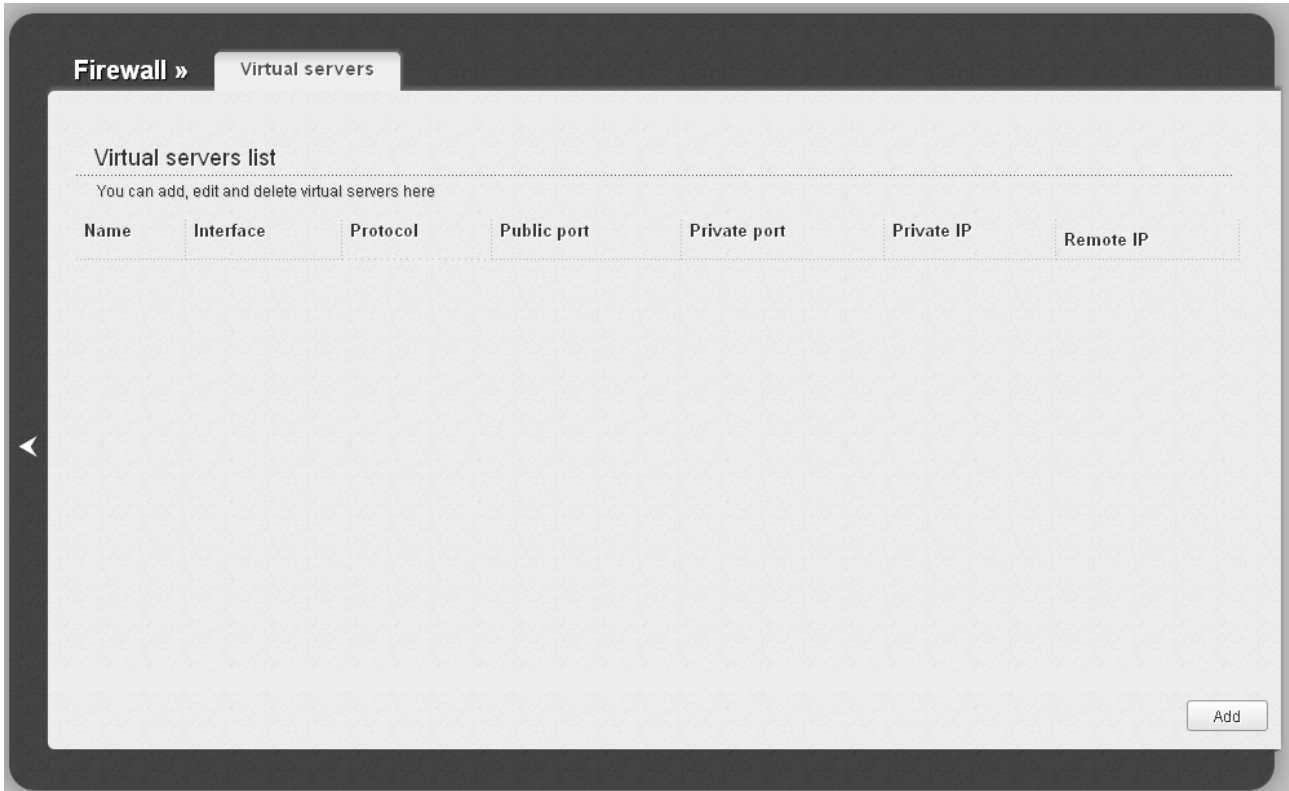


Figure 148. The **Firewall / Virtual servers** page.

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

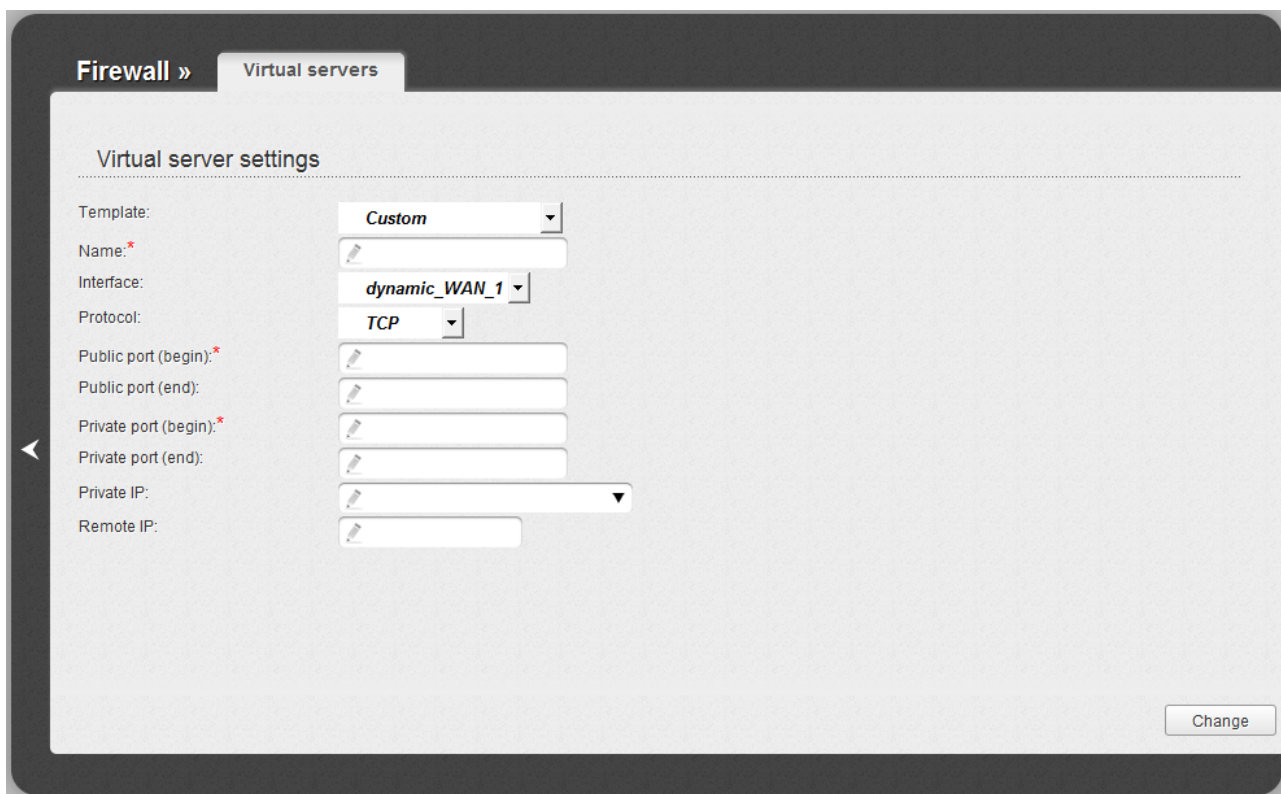


Figure 149. The page for adding a virtual server.

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.

Parameter	Description
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.

Click the **Change** button.

To edit the parameters of an existing server, follow the link with the name of the server. On the opened page, change the needed parameters and click the **Change** button.

To remove an existing server, follow the link with the name of the server. On the opened page, click the **Delete** button.

DMZ

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

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

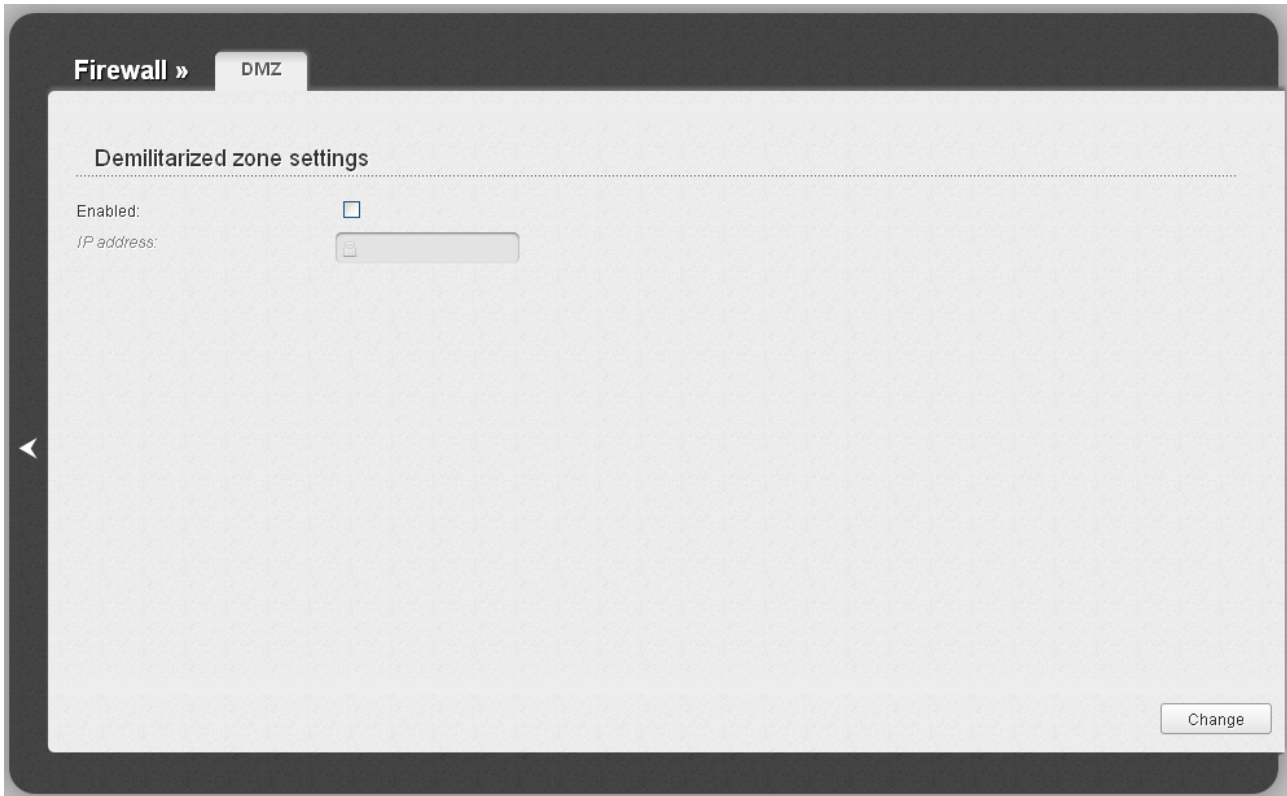


Figure 150. The **Firewall / DMZ** page.

To enable the DMZ, select the **Enabled** checkbox, enter the IP address of a host from your network in the **IP address** field, and click the **Change** 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 local network of the access point, then entering `http://access_point_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 **Change** button.

MAC Filter

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

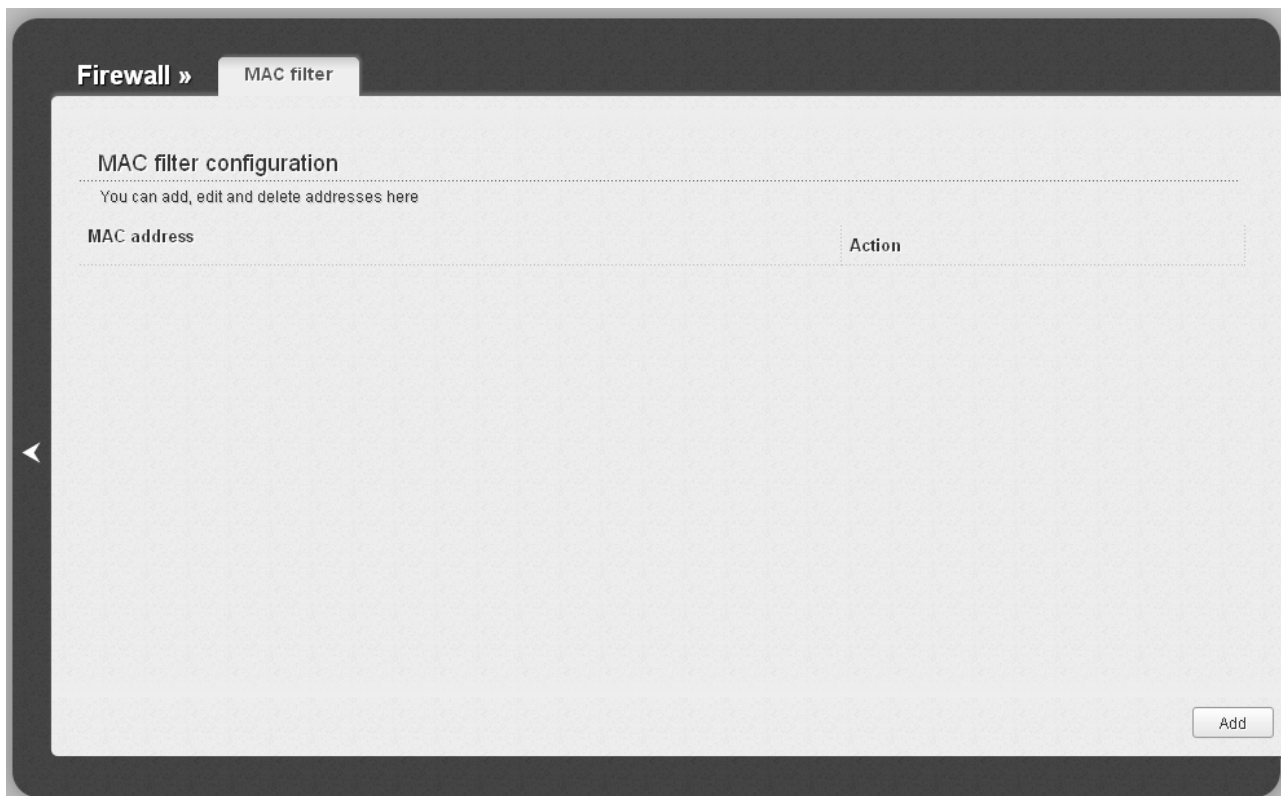


Figure 151. The **Firewall / MAC filter** page.

To specify a new address for the MAC filter, click the **Add** button.

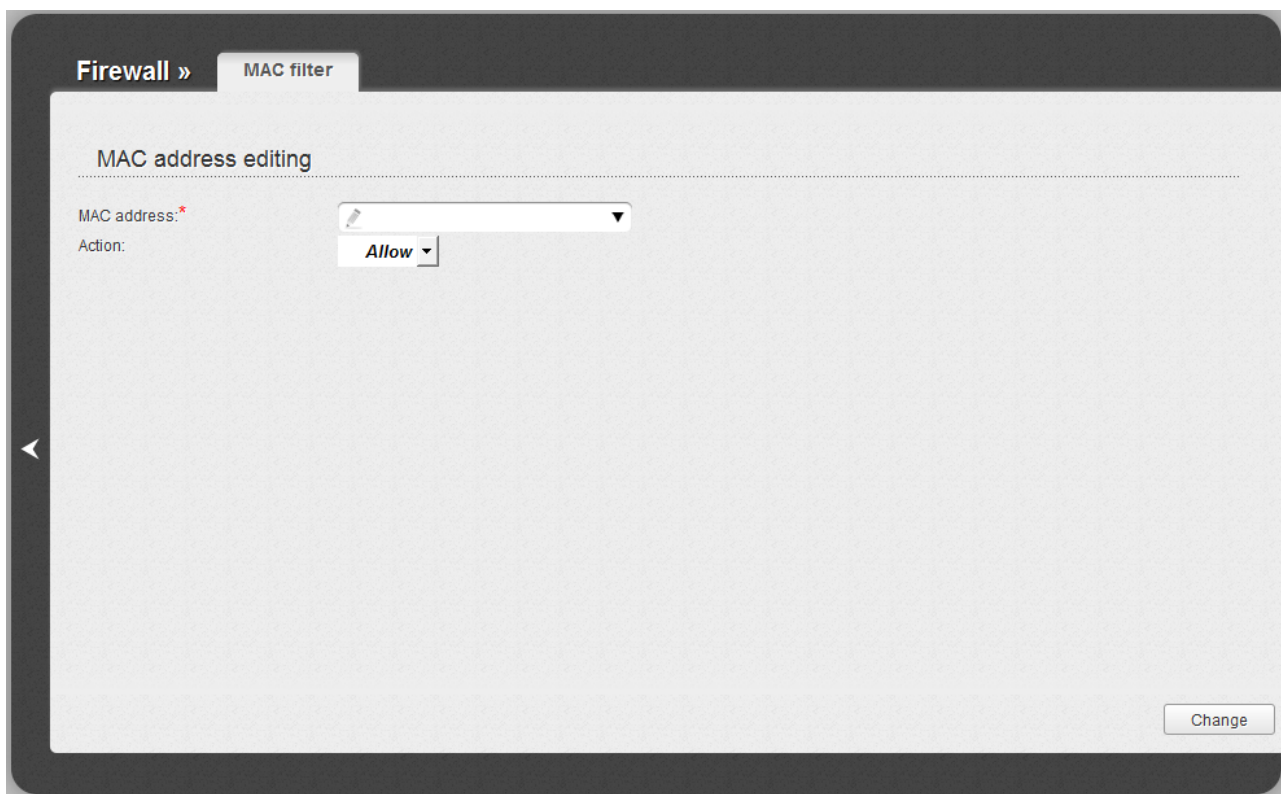


Figure 152. The page for adding an address for the MAC filter.

On the opened page, enter the MAC address of the device from the access point's LAN in the **MAC 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). Then select the **Deny** value from the **Action** drop-down list and click the **Change** button.

To remove an address from the list of MAC addresses for filtering, select the line with the relevant MAC address. On the opened page, click the **Delete** button.

Control

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

URL Filter

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

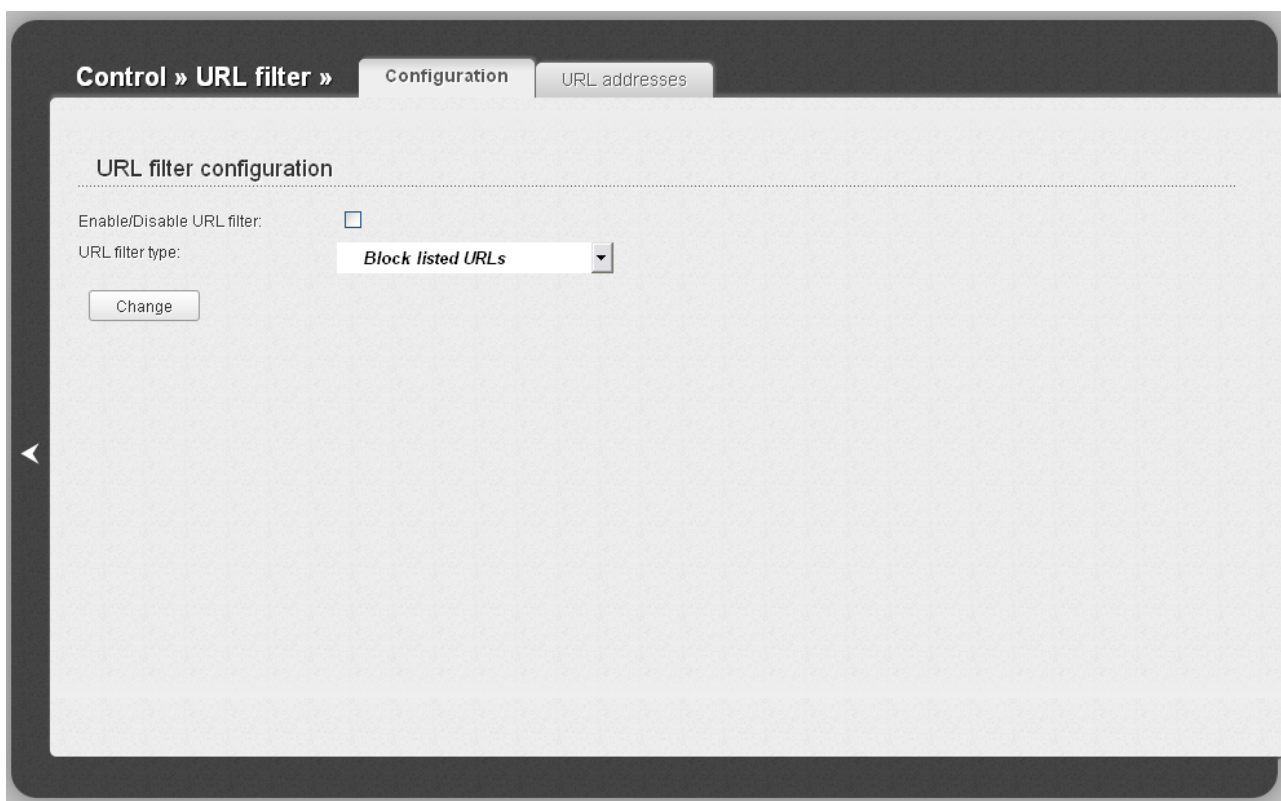


Figure 153. The **Control / URL filter** page. The **Configuration** tab.

To enable the URL filter, select the **Enable/Disable URL filter** checkbox on the **Configuration** tab, 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 **URL addresses** tab;
- **Block all URLs except listed:** when this value is selected, the access point allows access to addresses specified on the **URL addresses** tab and blocks access to all other web sites.

Click the **Change** button.

To specify URL addresses to which the selected filtering will be applied, go to the **URL addresses** tab and click the **Add** button.

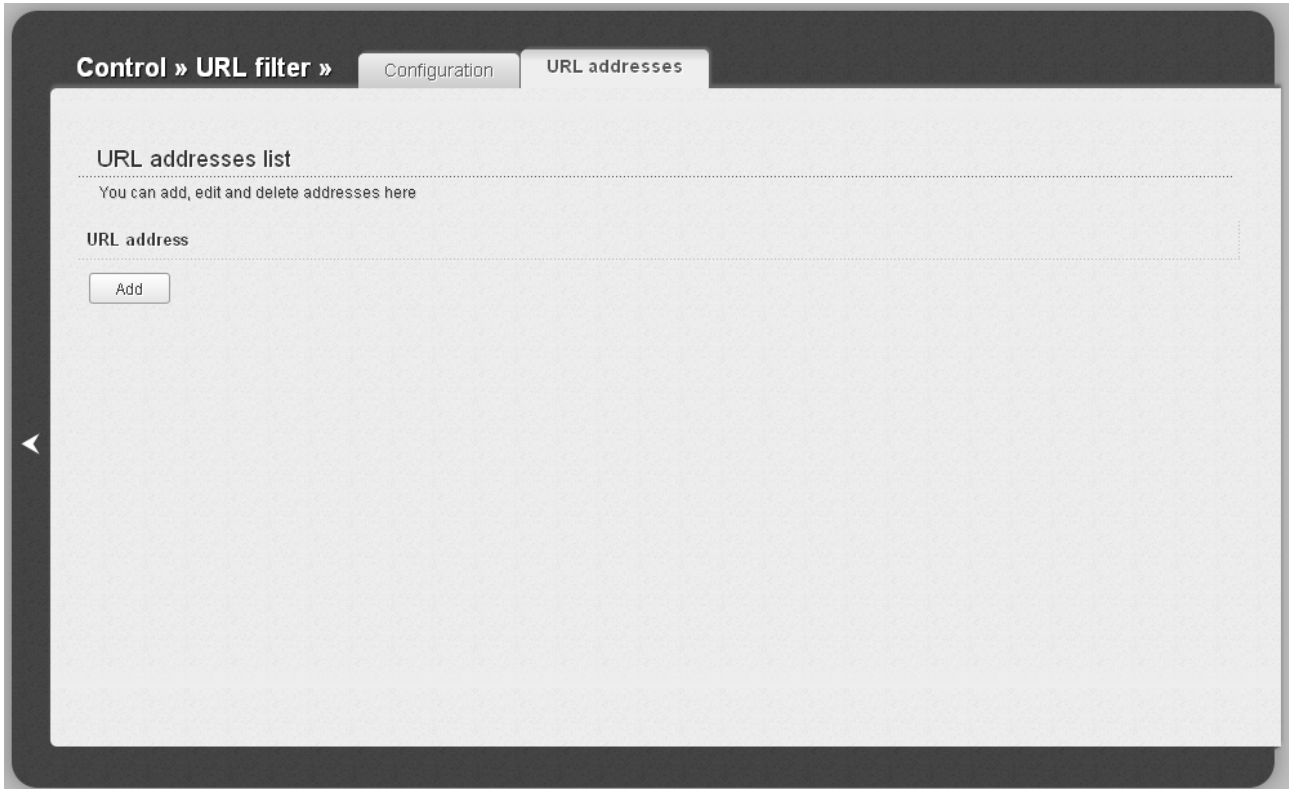


Figure 154. The **Control / URL filter** page. The **URL addresses** tab.

On the opened page, specify the needed parameters.

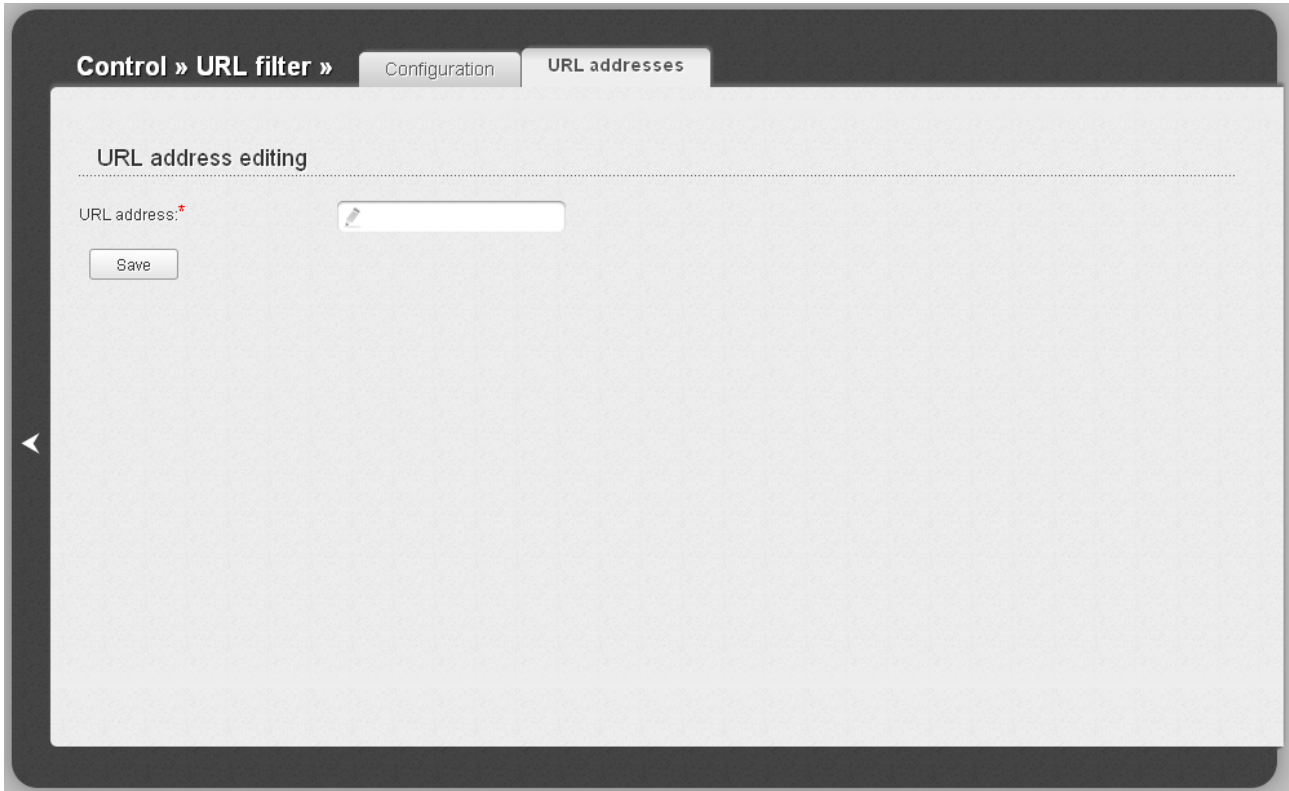


Figure 155. The page for adding an address for the URL filter.

Enter a URL address in the **URL address** field and click the **Save** button.

To remove an address from the list of URL addresses, select the relevant address in the table on the **URL addresses** tab and click the **Delete** button.

To disable the URL filter, deselect the **Enable/Disable URL filter** checkbox on the **Configuration** tab, then click the **Change** button.

System

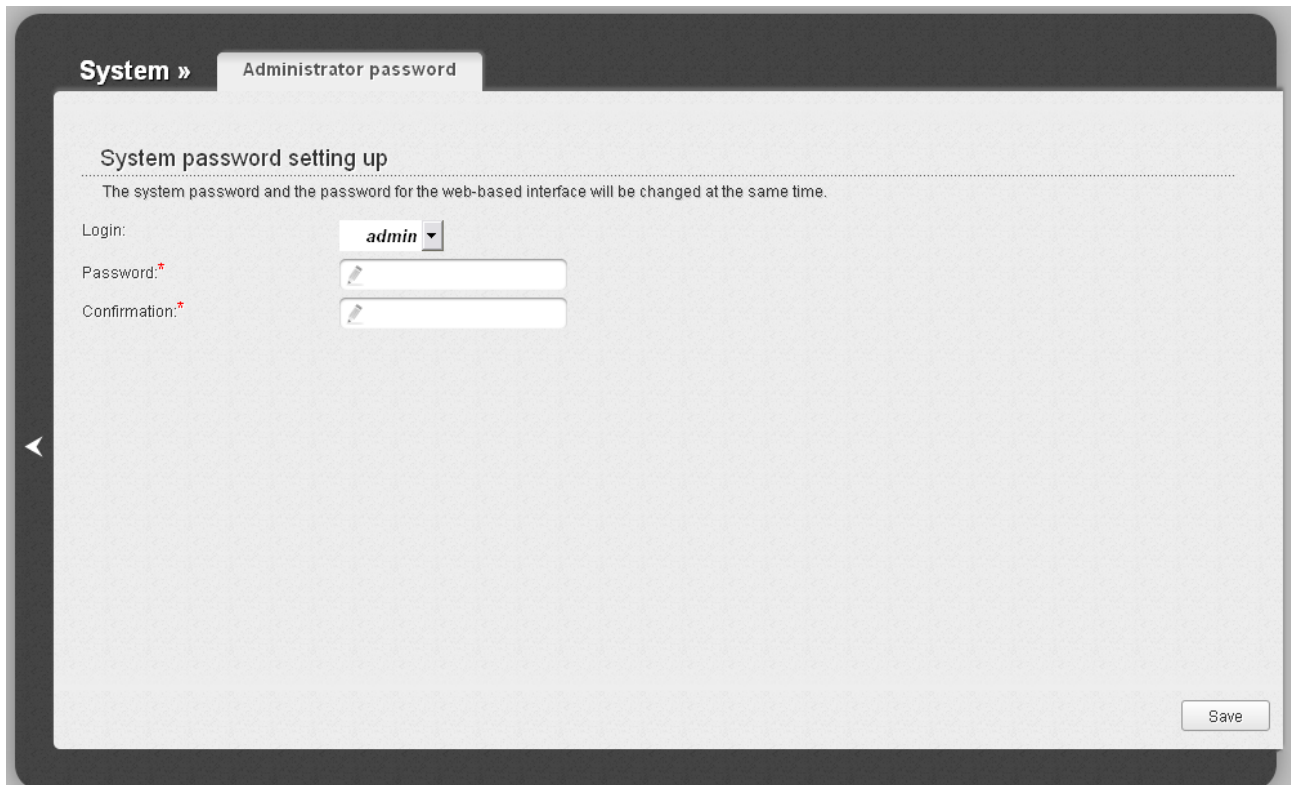
In this menu you can do the following:

- change the password used to access the access point's settings
- save the current settings to the non-volatile memory
- 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 synchronization of the system time
- 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.



The screenshot shows a web-based configuration page for the administrator password. The page has a dark header with 'System »' and 'Administrator password'. The main content area is light gray and contains the following elements:

- System password setting up**: A section header.
- The system password and the password for the web-based interface will be changed at the same time.**: A note below the header.
- Login:**: A dropdown menu with 'admin' selected.
- Password:***: A text input field with a password icon.
- Confirmation:***: A text input field with a password icon.
- Save**: A button at the bottom right of the form area.

Figure 156. The page for modifying the administrator password.

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

Configuration

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

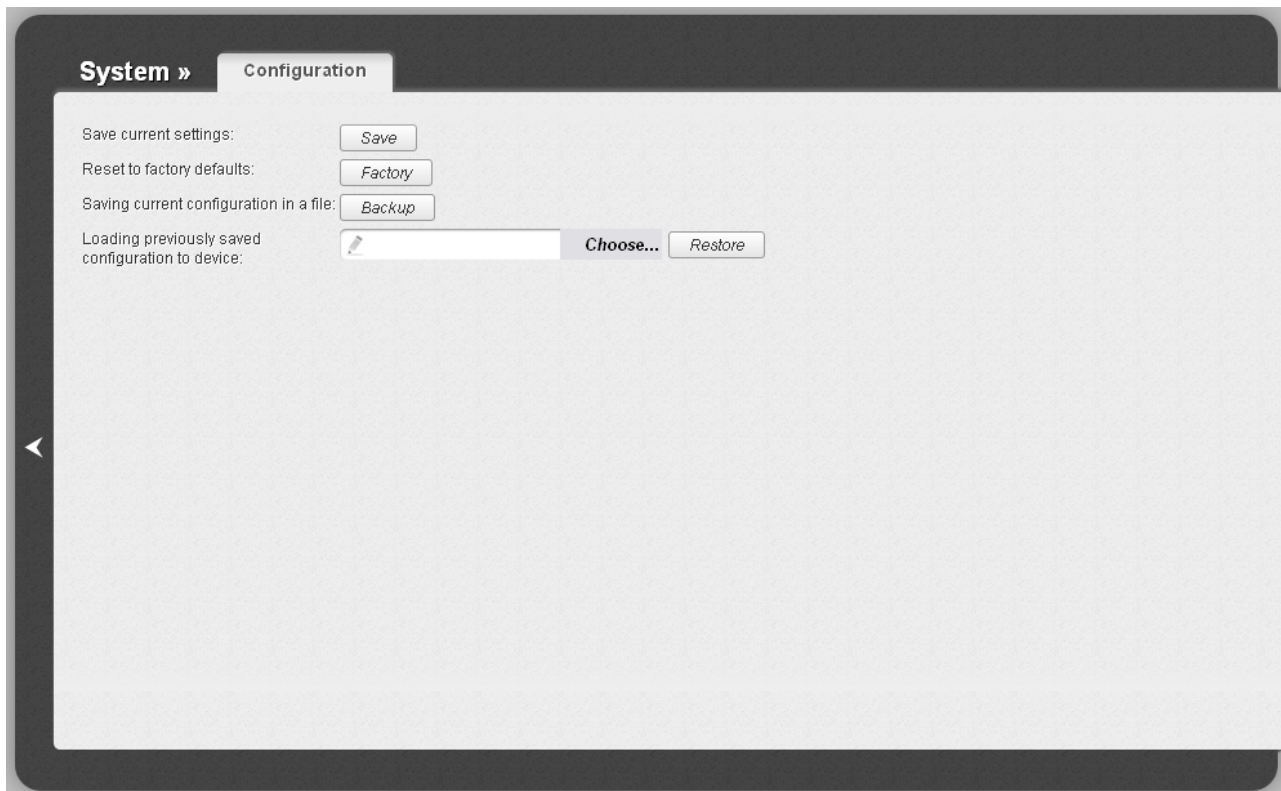


Figure 157. The **System / Configuration** page.

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.
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware WPS/RESET button (see the <i>Saving and Restoring Settings</i> section, page 37).
Backup	Click the button and follow the dialog box appeared to save the configuration (all settings of the access point) to your PC.
Restore	Click the button to upload a previously saved configuration (all settings of the access point) from a file on your PC. Click the Choose/Browse ³ button to select a previously saved configuration file located on your PC.

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

³ The name of the button depends upon the web browser that you use.

System Log

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

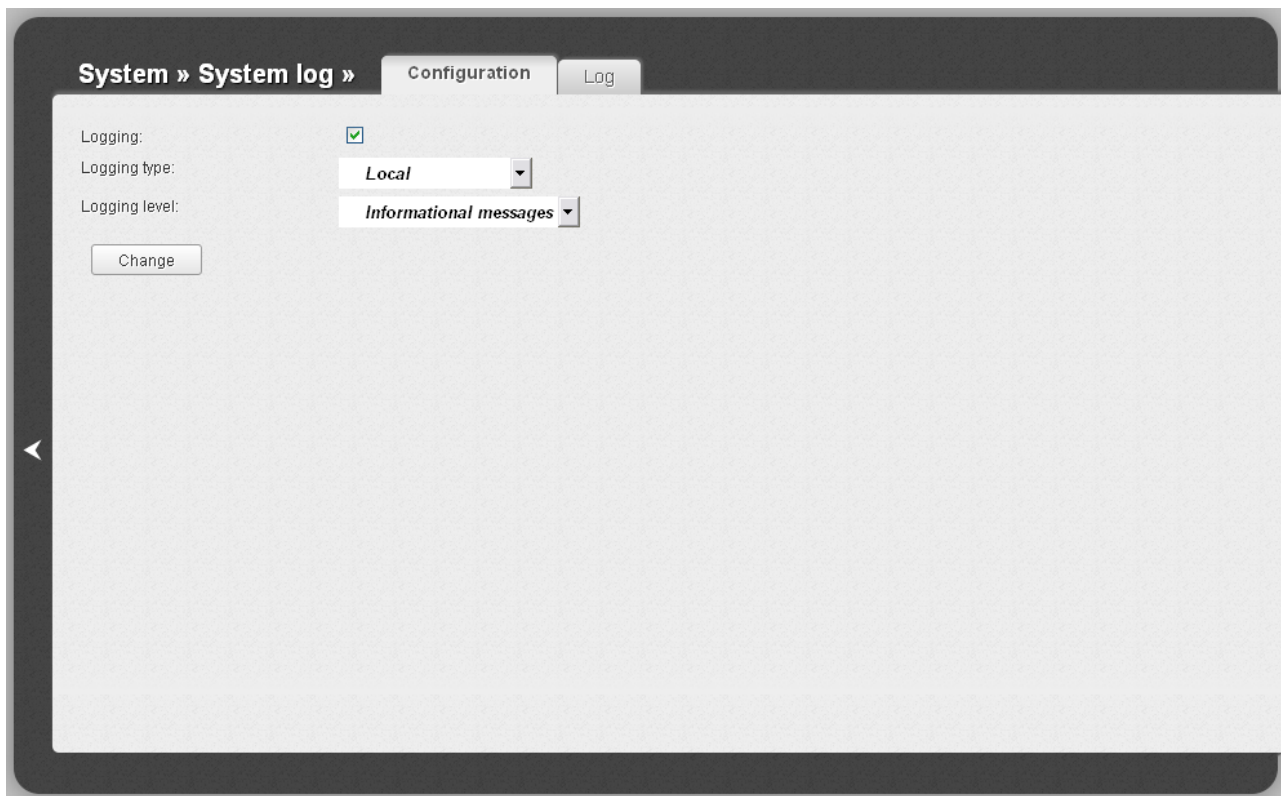


Figure 158. The **System / System log** page. The **Configuration** tab.

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

Control	Description
Logging type	Select a type of logging from the drop-down list. <ul style="list-style-type: none"> • Local: the system log is stored in the device's memory (and displayed on the Log tab). 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 Log tab) 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 **Change** button.

To disable logging of the system events, deselect the **Logging** checkbox and click the **Change** button.

On the **Log** tab, the events specified in the **Logging level** list are displayed.

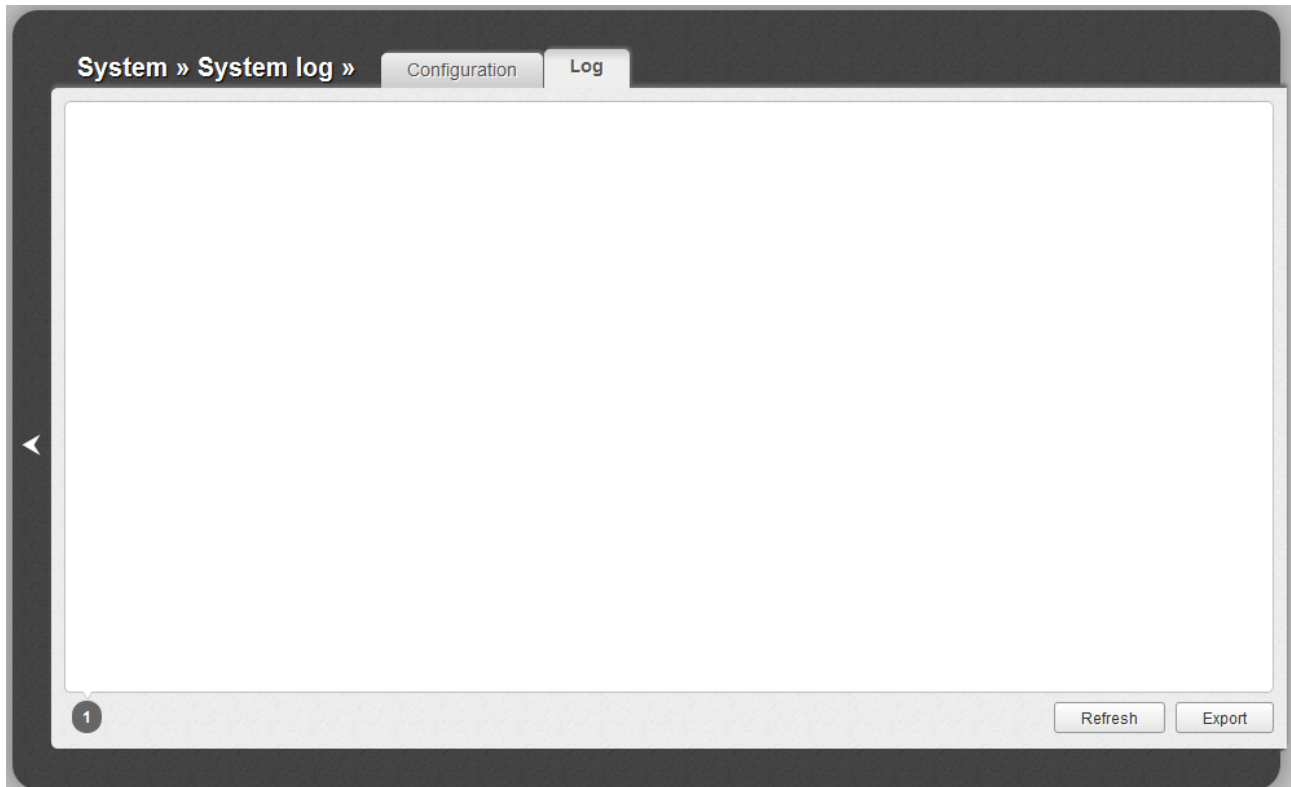


Figure 159. The **System / System log** page. The **Log** tab.

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

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

Firmware Upgrade

On the **System / Firmware upgrade** page, you can upgrade the firmware of the access point.

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

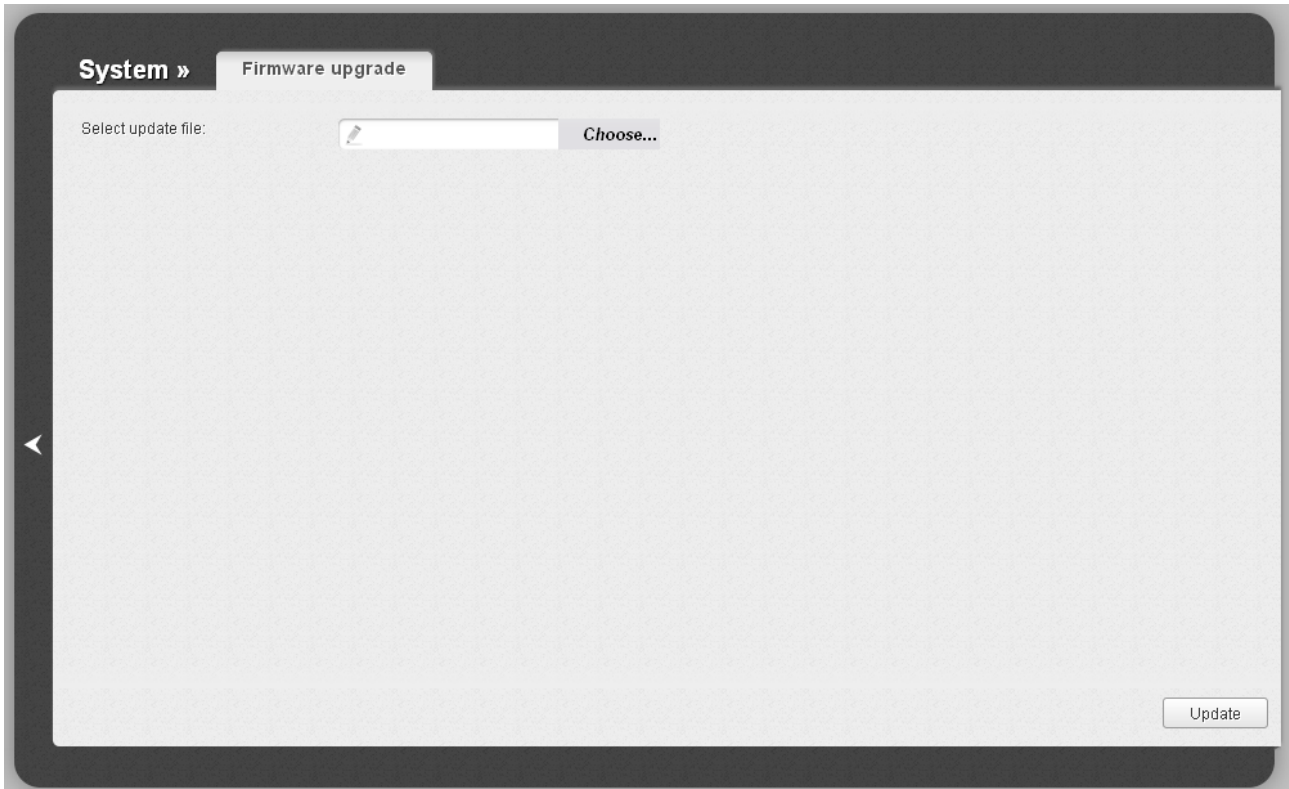


Figure 160. The **System / Firmware upgrade** page.

The current version of the access point's firmware is displayed in the **Firmware version** field located next the D-Link logo in the top left corner of the page. If you need to install a newer version of the firmware, follow the next steps:

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

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **Choose/Browse**⁴ 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.

⁴ The name of the button depends upon the web browser that you use.

6. Select the **Factory** line in the top-page menu displayed when the mouse pointer is over the **System** caption.
7. Wait until the access point is rebooted. Log into the web-based interface, using the default IP address, login and password (**192.168.0.50**, **admin**, **admin**).

NTP Client

On the **System / NTP client** page, you can configure automatic synchronization of the system time with a time server on the Internet.

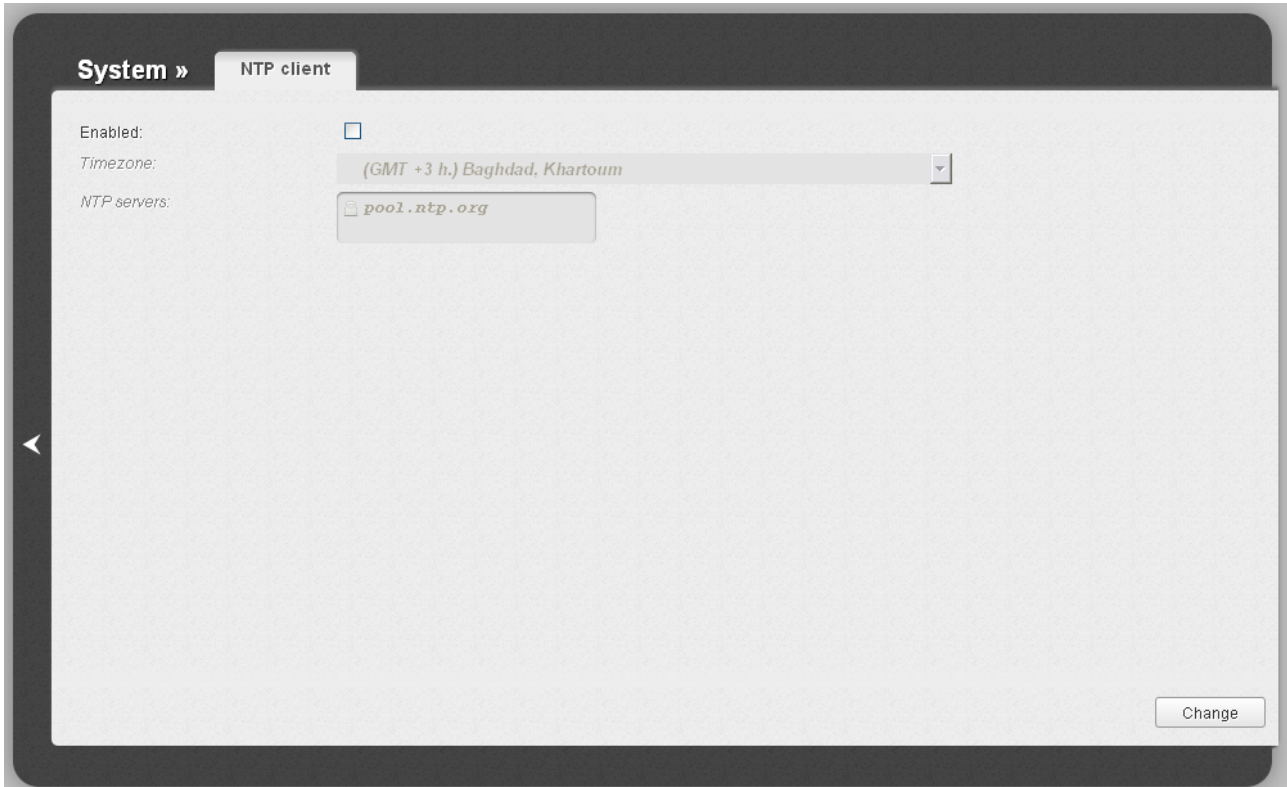


Figure 161. The **System / NTP client** page.

To enable automatic synchronization with a time server:

1. Select the **Enabled** checkbox.
2. Select your time zone.
3. Specify the needed NTP server in the **NTP servers** field or leave the server specified by default.
4. Click the **Change** button.



When the access point is powered off or rebooted, the system time is reset to the default value. If you have set automatic synchronization for the system time, the internal clock of the device will be configured after connecting to the Internet.

Ping

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

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



Figure 162. 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 **Ping** button. The check results will be displayed in the **Log** field.

Also you can run the Ping function in the background mode. To do this, select the **Background ping** checkbox. Then enter the IP address or name of a host in the **Host** field and click the **Ping** button. When this mode is selected, the **Count of packets** and **Log** fields are not displayed.

In the background mode, the Ping utility sends requests to the host specified in the **Host** field every 40 seconds. The **Background ping status** light shows the status of the Ping function (green light: the function is running, red light: the function is not running).

To stop running the Ping function in the background mode, deselect the **Background ping** checkbox, enter the IP address or name of a host in the **Host** field, and click the **Ping** button.

Traceroute

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

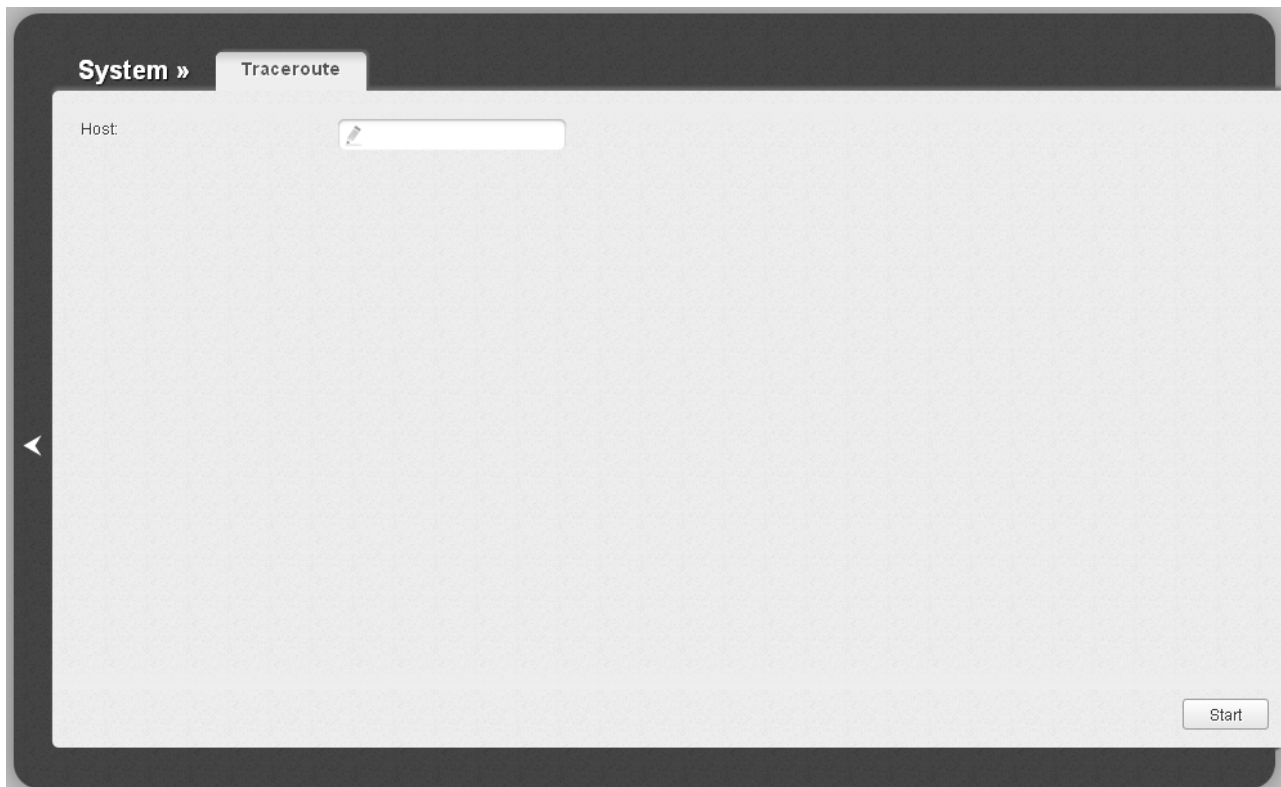


Figure 163. The **System / Traceroute** page.

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.



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

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

Device mode

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

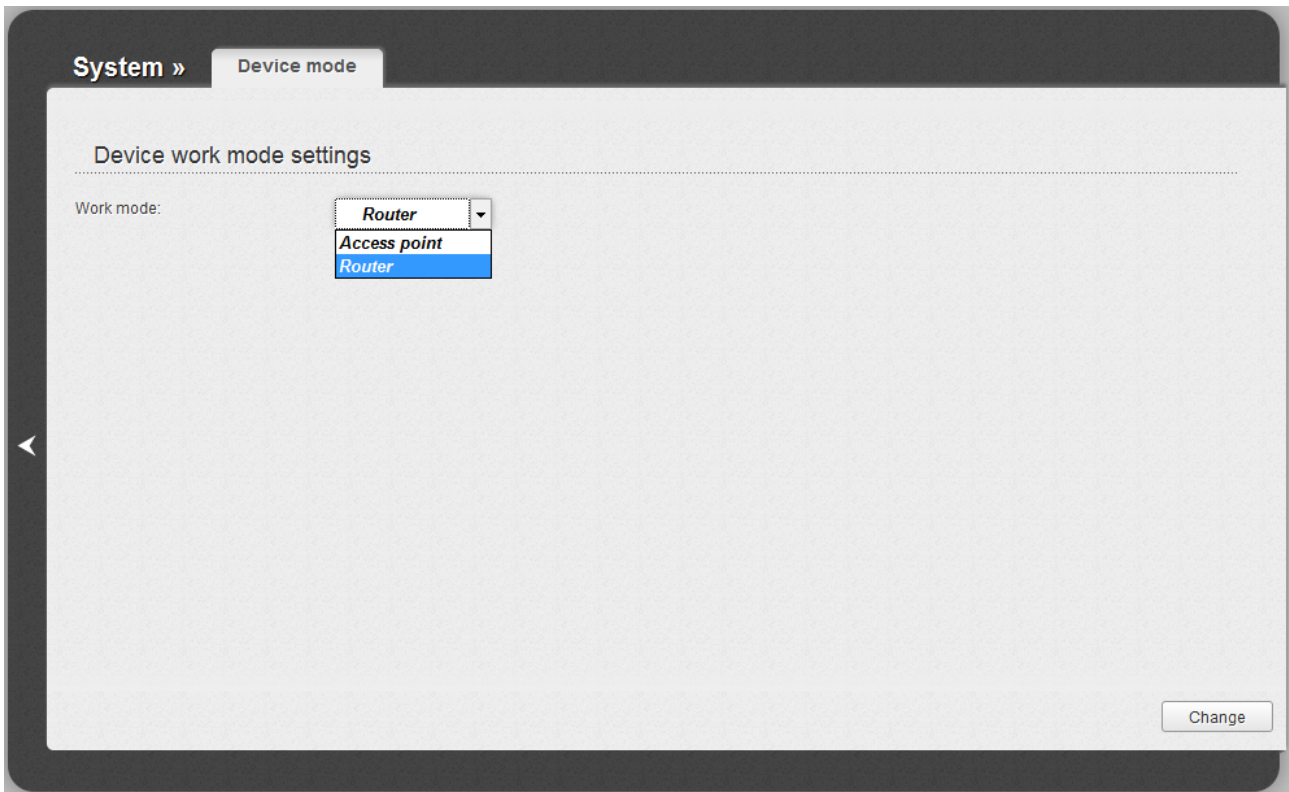


Figure 165. The page for changing the operating mode of the device.

To switch the device to the other mode, select the **Access point** value from the **Work mode** drop-down list and click the **Change** 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-1155 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-1155 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
HTMIX	High Throughput Mixed
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
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
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