User Manual

# DAP-1150

## Wireless Access Point Supporting Router Mode

December 2011

# Contents

**Chapter 1. Introduction........................................5**
**Contents and Audience........................................5**
**Conventions........................................5**
**Document Structure........................................5**
**Chapter 2. Overview........................................6**
**General Information........................................6**
**Specifications........................................7**
**Product Appearance........................................10**
Front Panel........................................10
Back Panel........................................11
**Delivery Package........................................12**
**Chapter 3. Installation and Connection........................................13**
**Before You Begin........................................13**
**Connecting to PC........................................14**
PC with Ethernet Adapter........................................14
Obtaining IP Address Automatically in OS Windows XP........................................14
Obtaining IP Address Automatically in OS Windows 7........................................17
PC with Wi-Fi Adapter........................................21
Configuring Wi-Fi Adapter in OS Windows XP........................................22
Configuring Wi-Fi Adapter in OS Windows 7........................................23
**Connecting to Web-based Interface........................................25**
**Saving and Restoring Settings........................................29**
**Device Operation Modes........................................30**
Access Point Mode........................................30
Router Mode........................................30
**Chapter 4. Configuring Device (Access Point Mode)........................................31**
**Setup Wizard........................................31**
Wi-Fi Setup Wizard........................................31
**Status........................................37**
Network Statistics........................................37
LAN Clients........................................38
**Net........................................39**
LAN........................................39

**Wi-Fi**......................................................................**41**
Common settings..............................................................41
Basic Settings...............................................................42
Security Settings............................................................43
MAC Filter...................................................................48
Station List.................................................................50
WPS..........................................................................51
WDS..........................................................................54
Additional Settings..........................................................56
WMM..........................................................................58
Client.......................................................................60
**Advanced**...................................................................**63**
Device mode..................................................................63
**Firewall**...................................................................**64**
MAC Filter...................................................................64
**System**.....................................................................**65**
Administrator Password.......................................................65
Configuration................................................................66
System Log...................................................................67
Firmware Upgrade.............................................................69
Telnet.......................................................................70
**Chapter 5. Configuring Device (Router Mode)**....................**71**
**Setup Wizards**..............................................................**71**
Internet Setup Wizard........................................................71
*PPPoE Connection*...........................................................*73*
*Static IP Connection*.......................................................*77*
*Dynamic IP Connection*......................................................*80*
*PPTP + Static IP or L2TP + Static IP Connection*............................*82*
*PPTP + Dynamic IP or L2TP + Dynamic IP Connection*..........................*88*
Site Setup Wizard............................................................93
Wi-Fi Setup Wizard...........................................................94
**Status**....................................................................**100**
Network Statistics..........................................................100
Routing Table...............................................................101
LAN Clients.................................................................102
**Net**.......................................................................**103**
WAN.........................................................................103
*Creating PPPoE WAN Connection*.............................................*104*
*Creating Static IP WAN Connection*.........................................*107*
*Creating Dynamic IP WAN Connection*........................................*110*
*Creating PPTP + Static IP or L2TP + Static IP WAN Connection*..............*113*
*Creating PPTP + Dynamic IP or L2TP + Dynamic IP WAN Connection*............*118*
LAN.........................................................................123

**Wi-Fi**......125
Common settings......125
Basic Settings......126
Security Settings......127
MAC Filter......132
Station List......134
WPS......135
WDS......138
Additional Settings......140
WMM......142
Client......144
**Advanced**......147
UPnP......147
DDNS......148
DNS......150
Routing......151
Device mode......153
Remote Access......154
IGMP......156
**Firewall**......157
IP Filters......157
Virtual Servers......160
DMZ......162
MAC Filter......163
**Control**......164
URL Filter......164
**System**......166
Administrator Password......166
Configuration......167
System Log......168
Firmware Upgrade......170
NTP Client......171
Telnet......172
**Chapter 6. Operation Guidelines**......173
**Safety Instructions**......173
**Wireless Installation Considerations**......173
**Chapter 7. Abbreviations and Acronyms**......174

# CHAPTER 1. INTRODUCTION

## *Contents and Audience*

This manual describes the access point DAP-1150 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. |
| ***Before You Begin*** | A reference to a chapter or section of this manual. |
| ***"Quick Installation Guide"*** | A reference to a document. |
| **Change** | A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.). |
| `192.168.0.50` | Data that you should enter in the specified field. |
| ! Information | 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-1150 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-1150 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-1150, 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, WPS, WDS, WMM.

You are able to connect the wireless access point DAP-1150 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-1150 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-1150 device via the user-friendly web-based interface (the interface is available in several languages).

# *Specifications*[*]

**LAN Interface:**

- 1 10/100BASE-TX Ethernet port with auto MDI/MDIX.

**WLAN Interface:**

- IEEE 802.11b/g/n.

**Operation Mode:**

- 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.

[*] 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
    - WPA/WPA2 Enterprise
- 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).

**LEDs:**

- Power
- LAN/WAN
- WLAN.

**Power:**

- External power adapter DC 5V/1.2A
- RESET to Factory Defaults button.

**Operating Temperature:**

- from 0 to 55 $^0$C (from 32 to 131 $^0$F).

**Operating Humidity:**

- from 10% to 90% non-condensing.

**Certification:**

- CE
- FCC Class B
- C-Tick
- Wi-Fi.

## *Product Appearance*

### Front Panel

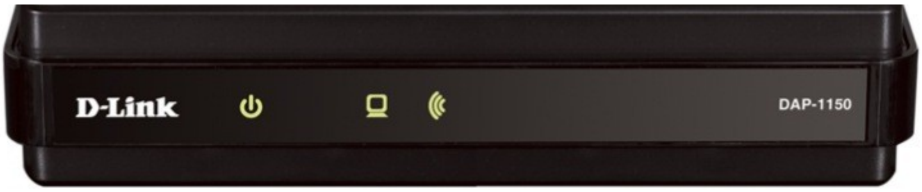


*Figure 1. Front panel view.*

| LED | Mode | Description |
|---|---|---|
| ⏻<br>**Power** | *Solid green* | The device is powered on. |
| | *No light* | The device is powered off. |
| | *Solid yellow* | When powered on: the device is being loaded; when loaded: a malfunction of the device. |
| 🖥<br>**LAN/WAN** | *Solid green* | Access point mode: the device has an IP address and is available for configuration.<br>Router mode: a WAN connection is established. |
| | *Blinking green* | The port is active (upstream or downstream traffic). |
| | *Solid yellow* | When powered on: the device is being loaded; when loaded in the router mode: no WAN connection is established. |
| 📶<br>**WLAN** | *Solid green* | The device's WLAN is on. |
| | *Blinking green* | The WLAN interface is active (upstream or downstream traffic). |

## Back Panel

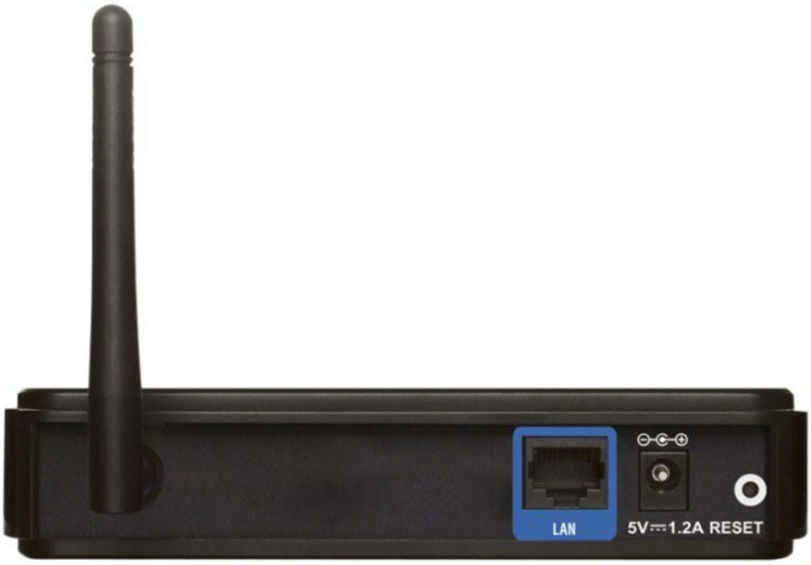


*Figure 2. Back panel view.*

| Port | Description |
|---|---|
| **LAN** | Access point mode: an Ethernet port to connect to a computer.<br>Router mode: an Ethernet 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). |
| **5V=1.2A** | Power connector. |
| **RESET** | A button to restore the factory default settings.<br>Power off the device. Push the RESET button. Power on the device keeping the RESET button pushed, and after 5 seconds release the button. |

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

## *Delivery Package*

The following should be included:

- Access point DAP-1150
- Power adapter 5V/1.2A
- Ethernet cable (CAT 5E)
- CD-ROM with "***User Manual***" and "***Quick Installation Guide***"
- "***Quick Installation Guide***" (brochure).

**!** 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-1150 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.

## Obtaining IP Address Automatically 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.

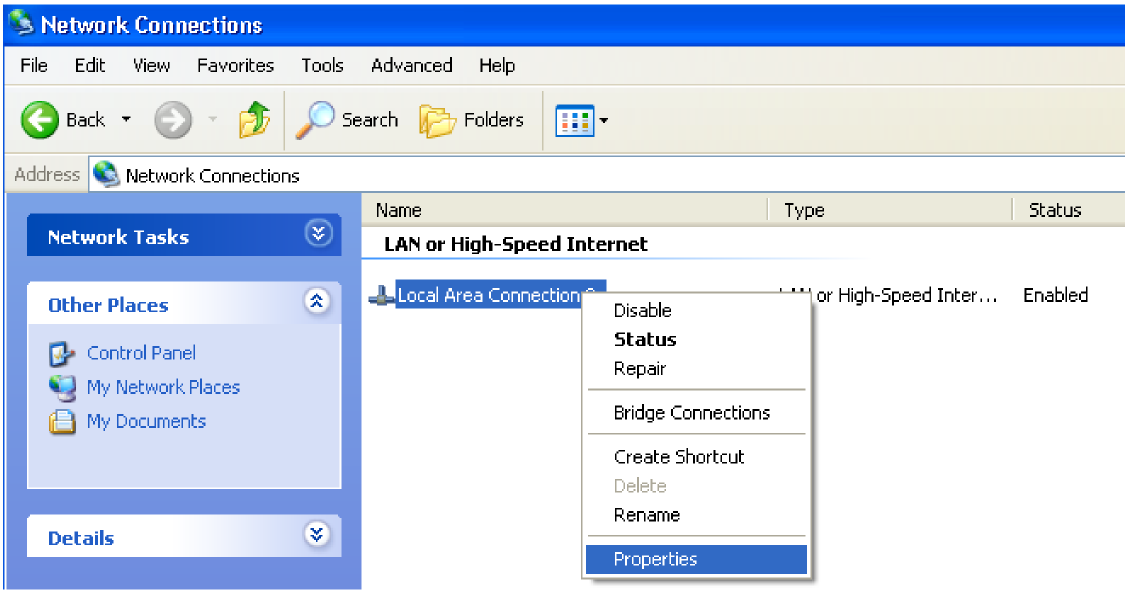
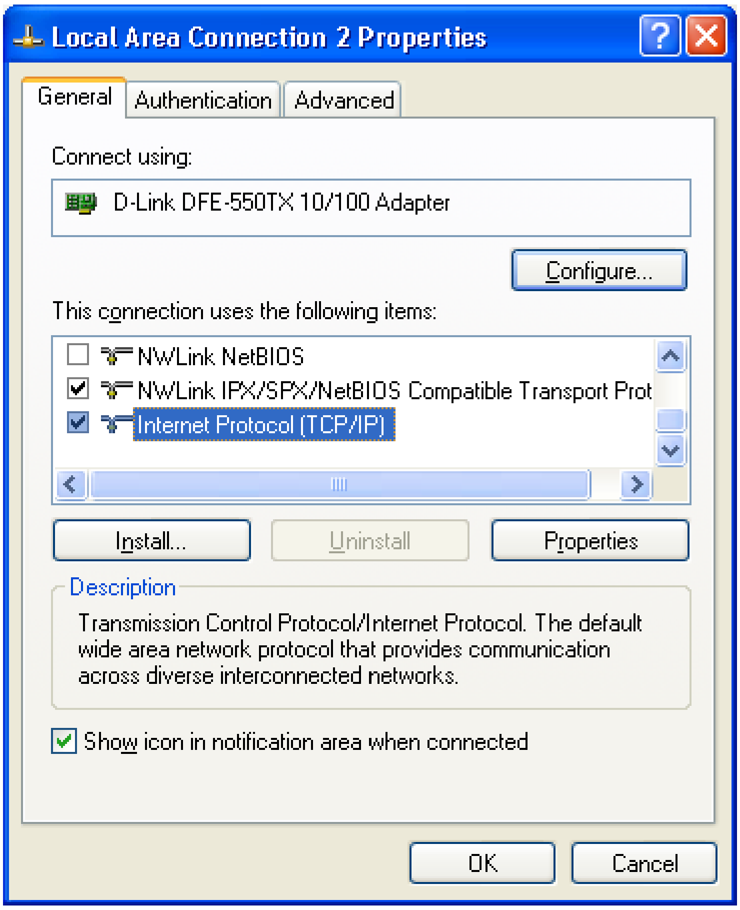


*Figure 3. The **Network Connections** window.*

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



Local Area Connection 2 Properties

Connect using:

D-Link DFE-550TX 10/100 Adapter

This connection uses the following items:

- □ NWLink NetBIOS
- ☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot
- ☑ Internet Protocol (TCP/IP)

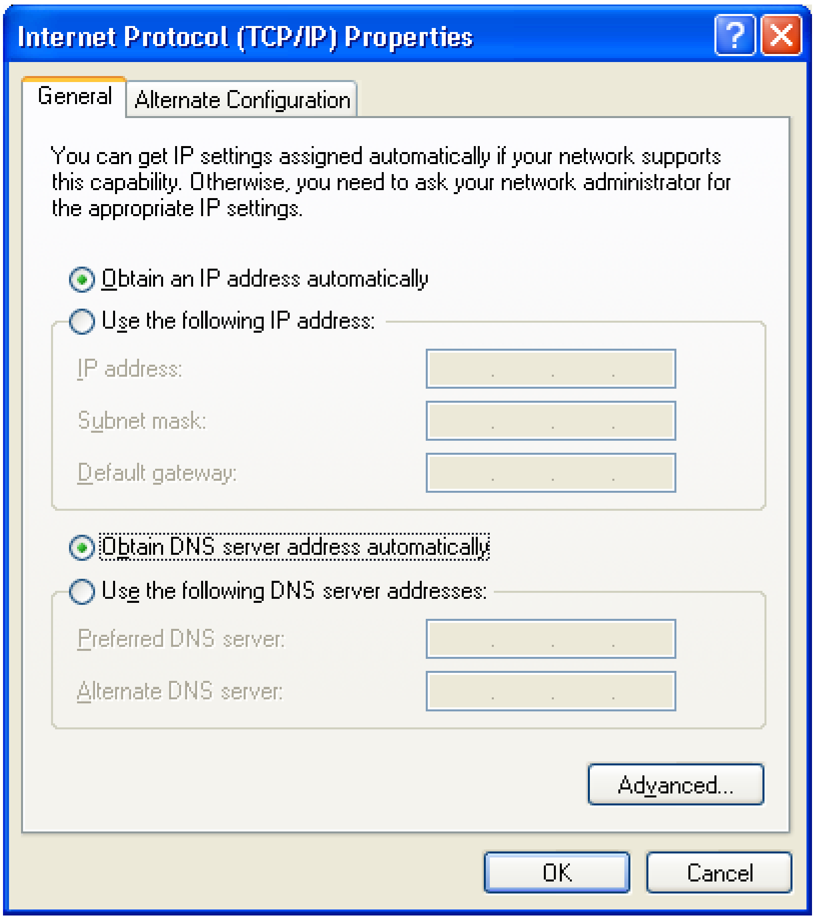
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

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

4. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. Click the **OK** button.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

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

Now your computer is configured to obtain an IP address automatically.

## Obtaining IP Address Automatically 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.)

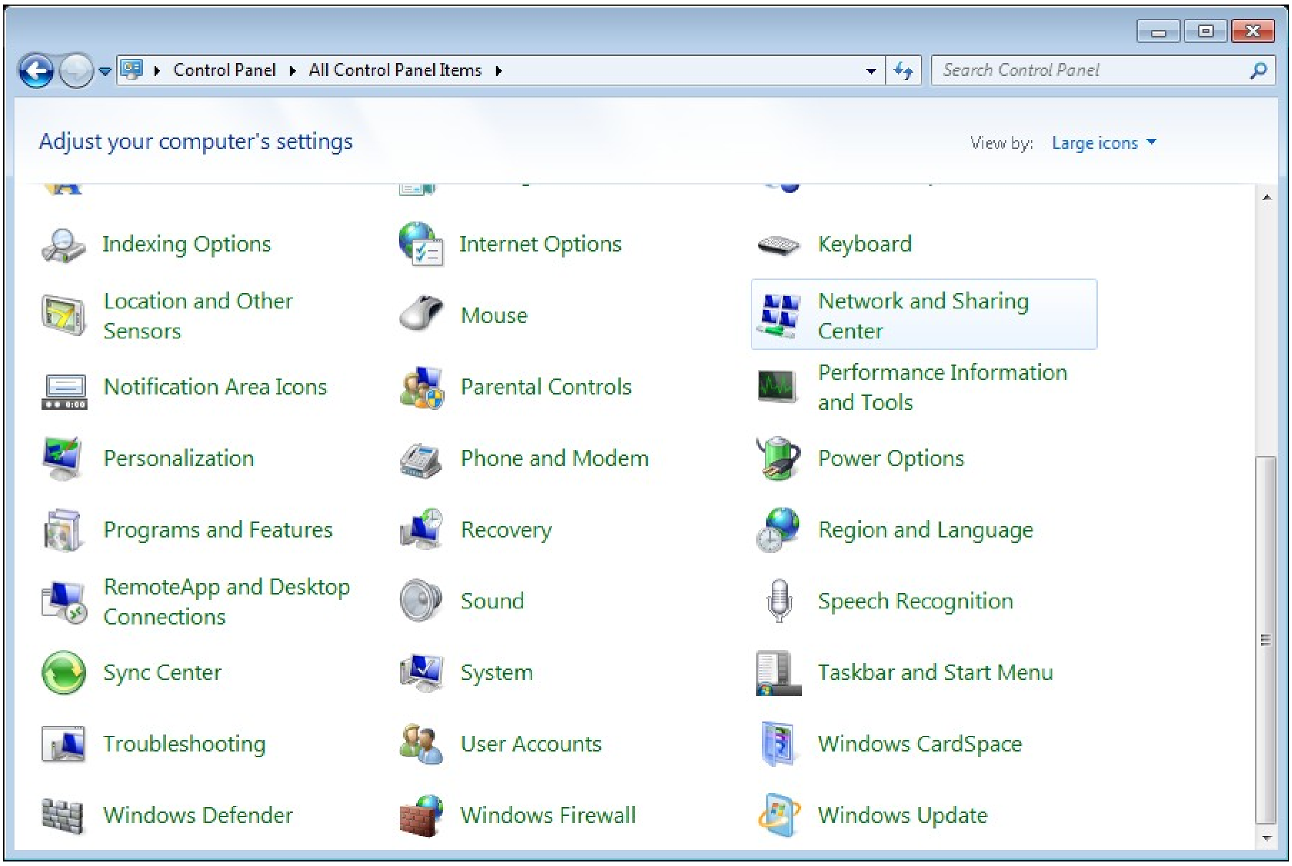
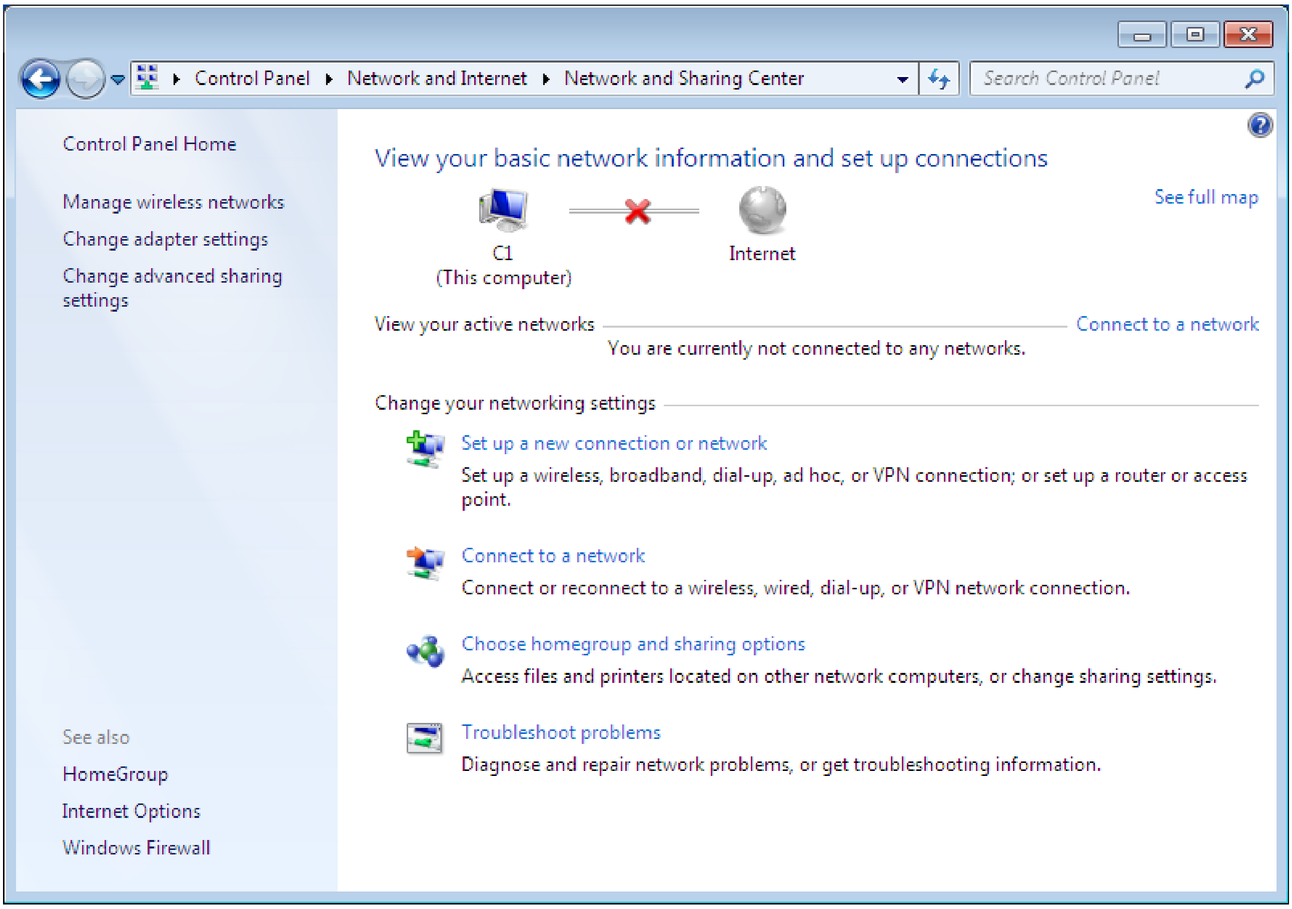


*Figure 6. The **Control Panel** window.*

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



Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

See full map

C1
(This computer)

Internet

View your active networks

Connect to a network

You are currently not connected to any networks.

Change your networking settings

Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options

Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

*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.

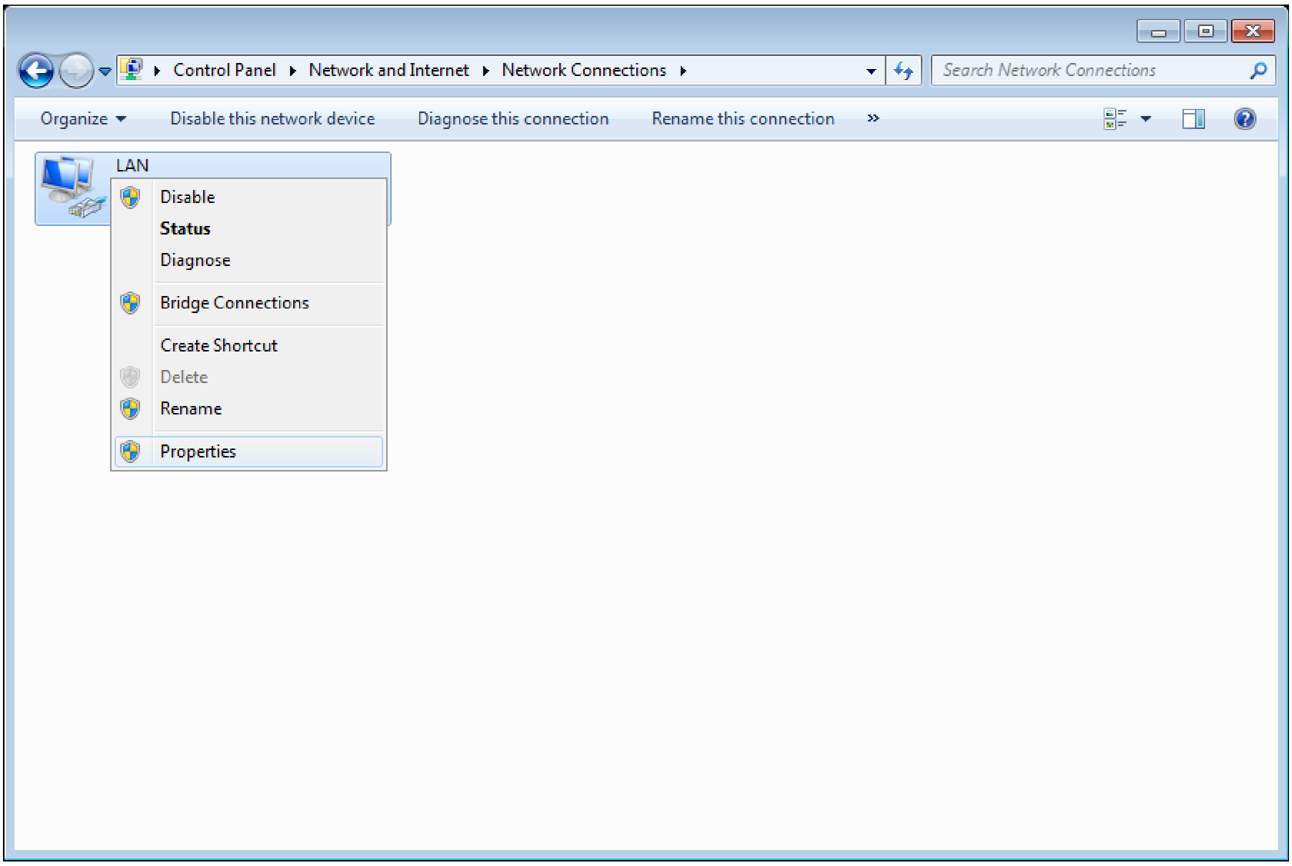
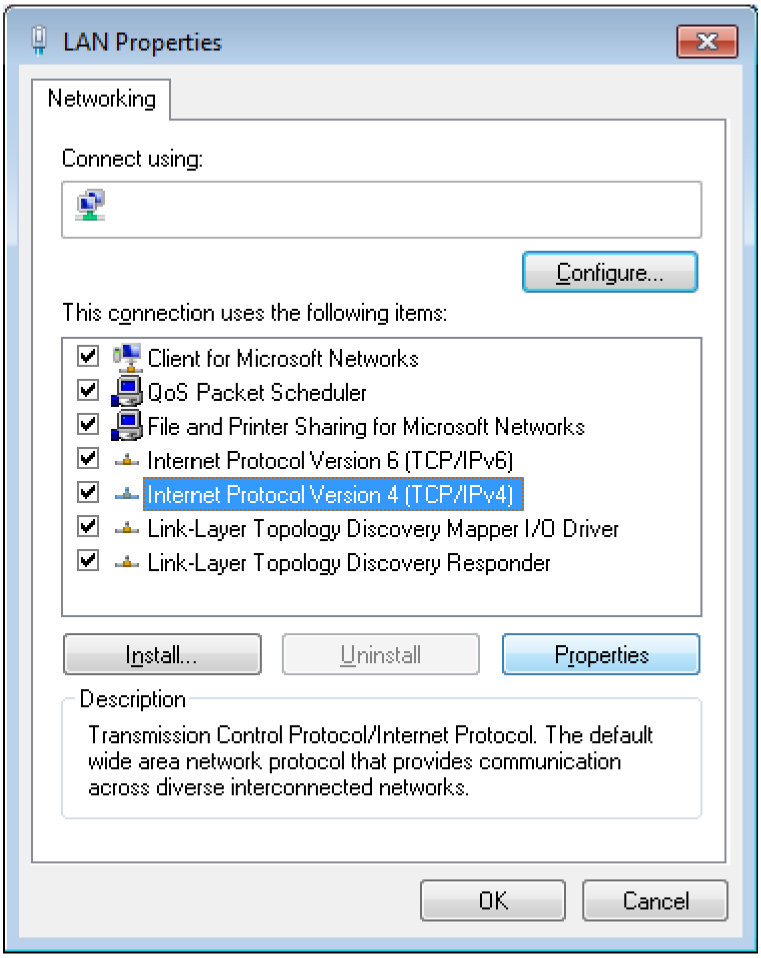


*Figure 8. The **Network Connections** window.*

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.



LAN Properties

Networking

Connect using:

Configure...

This connection uses the following items:

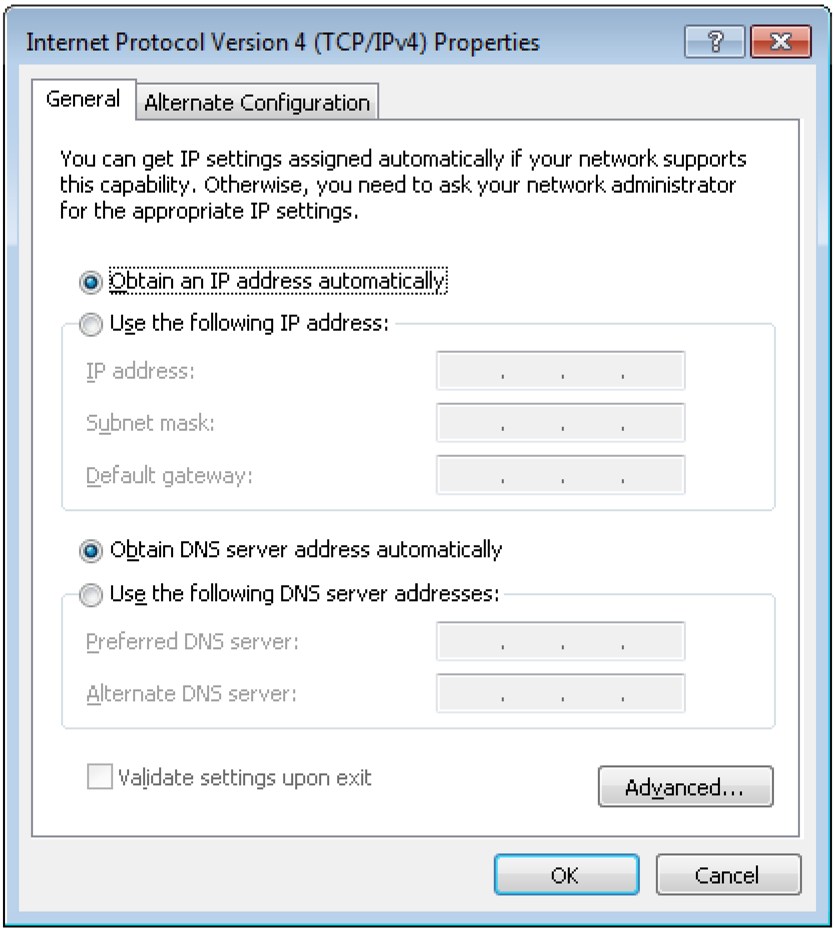
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

6. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. Click the **OK** button.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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

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

Now your computer is configured to obtain an IP address automatically.

## 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. Select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.

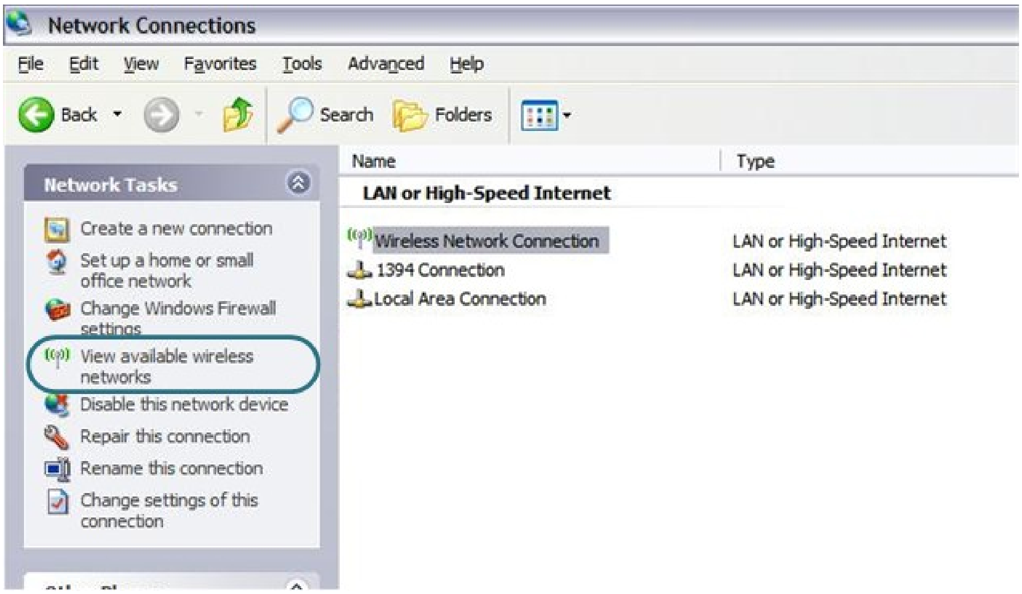

Network Connections
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Search
Folders
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
View available wireless networks
Disable this network device
Repair this connection
Rename this connection
Change settings of this connection
Name
Type
LAN or High-Speed Internet
Wireless Network Connection
LAN or High-Speed Internet
1394 Connection
LAN or High-Speed Internet
Local Area Connection
LAN or High-Speed Internet

*Figure 11. The* ***Network Connections*** *window.*

3. Search for available wireless networks.
4. In the opened **Wireless Network Connection** window, select the wireless network `DAP-1150` and click the **Connect** button.

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

! 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.)

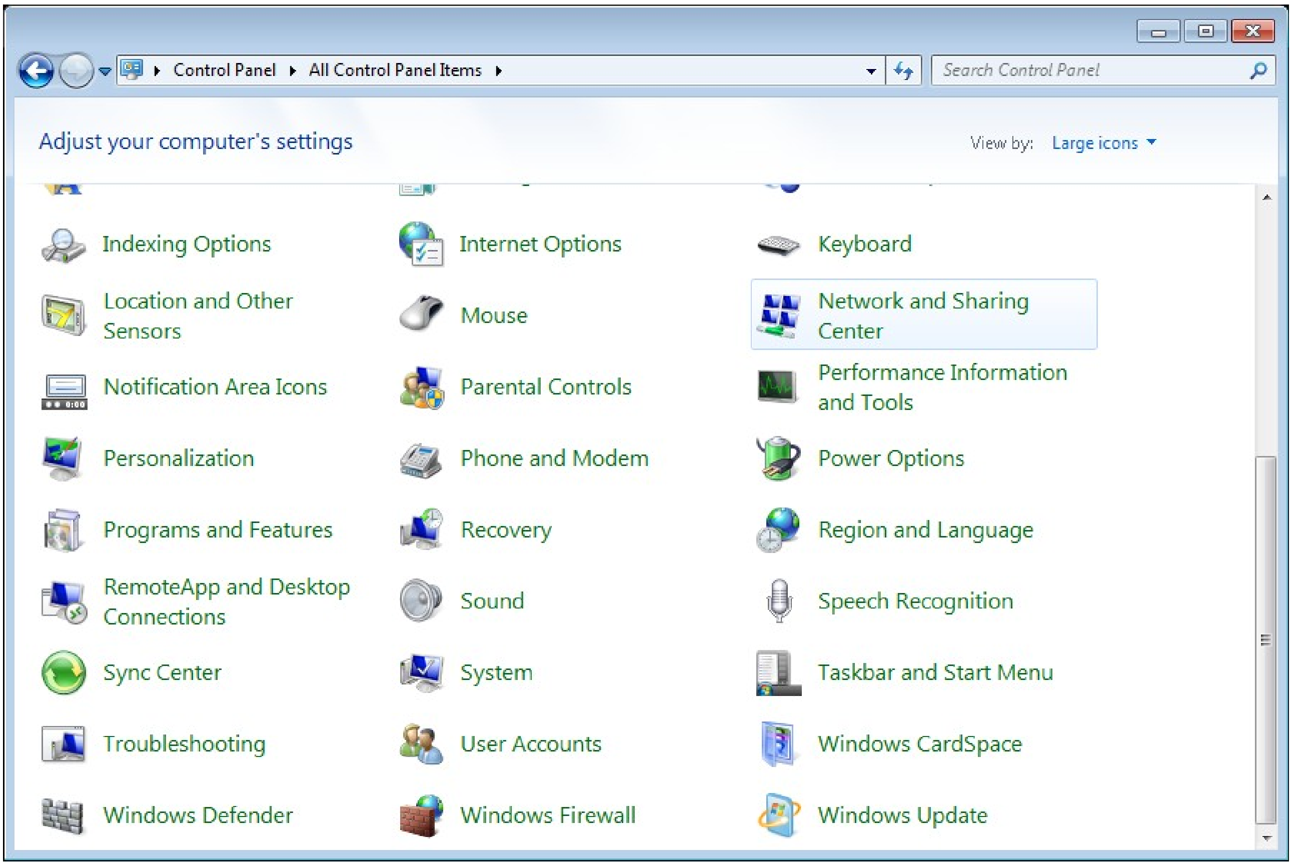


*Figure 12. The **Control Panel** window.*

3. In the menu located on the left part of the window, select the **Change adapter settings** line.
4. In the opened window, select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.
5. 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.

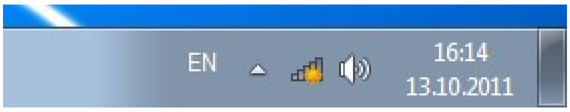


*Figure 13. The notification area of the taskbar.*

6. In the opened window, in the list of available wireless networks, select the wireless network **`DAP-1150`** and click the **Connect** button.

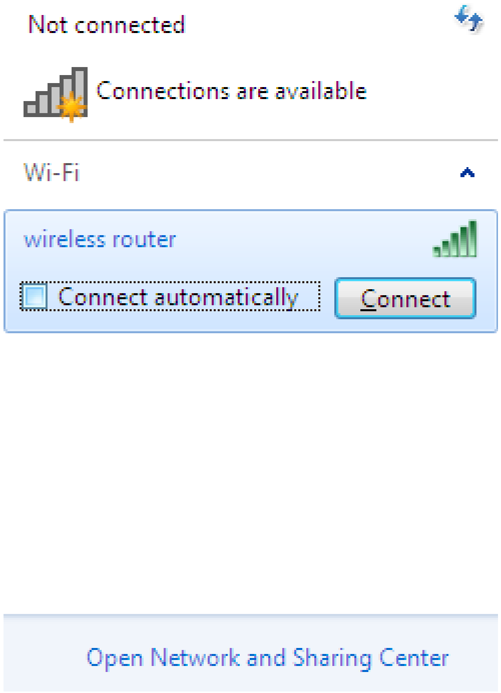


*Figure 14. The list of available networks.*

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

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

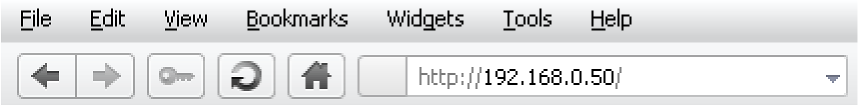
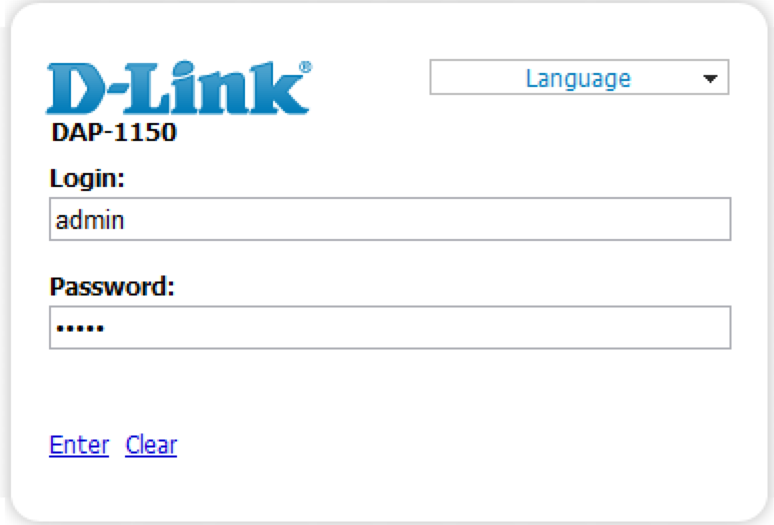


*Figure 15. Connecting to the web-based interface of the DAP-1150 device.*

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



DAP-1150

Login:

admin

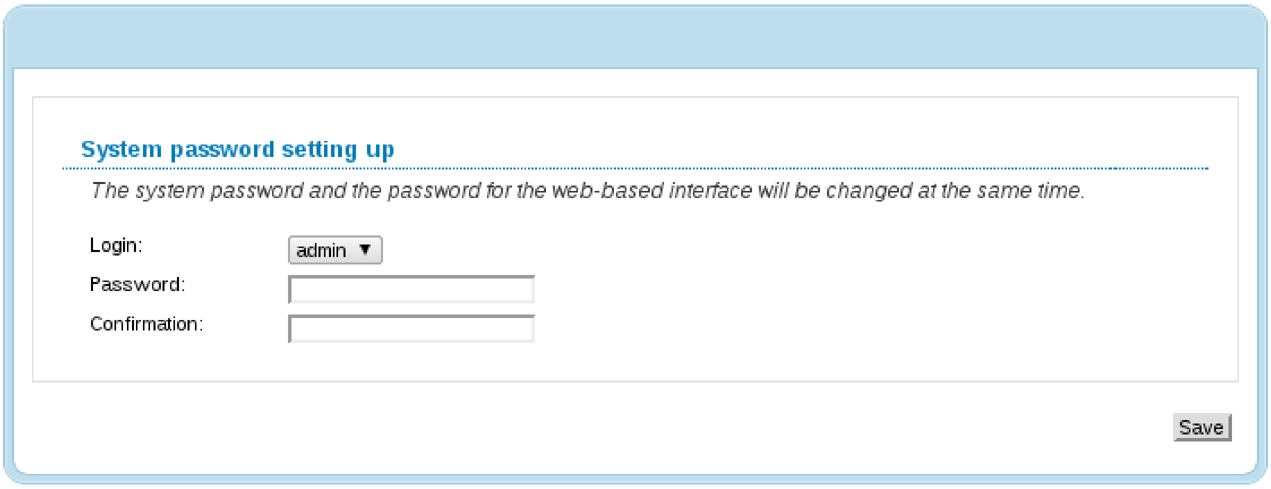
Password:

•••••

*Figure 16. The login page.*

**!** <u>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.</u>

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



System password setting up

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

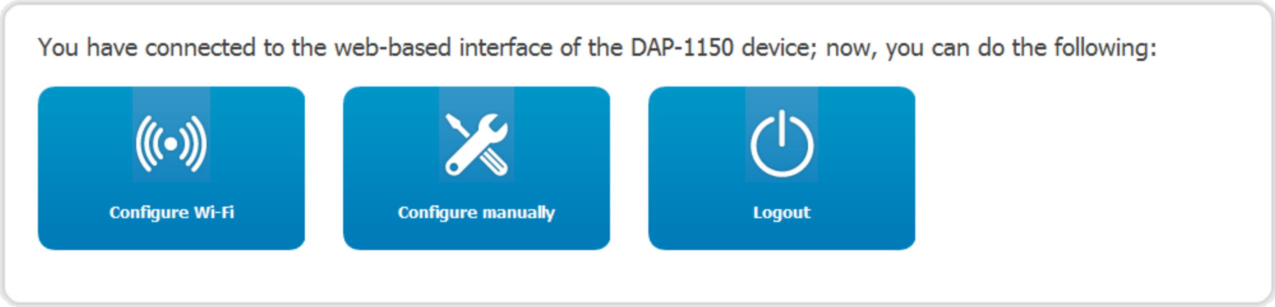
|  |  |
|---|---|
| Login: | admin ▼ |
| Password: |  |
| Confirmation: |  |

*Figure 17. The page for changing the default administrator password.*

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

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

After successful registration the access point's quick settings page opens. When the device is switched to the access point mode, the **Configure Wi-Fi**, **Configure manually**, **Logout** buttons are available on the page.



You have connected to the web-based interface of the DAP-1150 device; now, you can do the following:

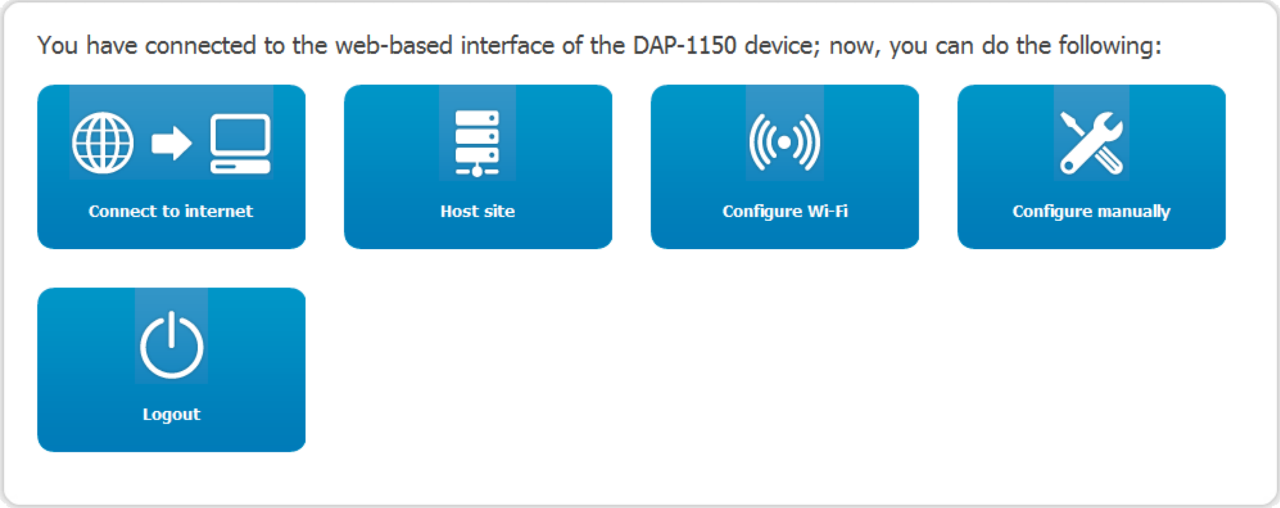
*Figure 18. The quick settings page in the access point mode.*

To configure the access point's wireless network, click the **Configure Wi-Fi** button. After clicking the button, the Wi-Fi Setup Wizard opens (see the ***Wi-Fi Setup Wizard*** section, page 31).

To get back to the quick settings page from the Wi-Fi Setup Wizard or any web-based interface menu section, left-click the D-Link logo in the top left corner of the page.

To configure all parameters of the access point independently without the Wizard, click the **Configure manually** button.

When the device is switched to the router mode, the **Connect to internet**, **Host site**, **Configure Wi-Fi**, **Configure manually**, and **Logout** buttons are available on the page.



You have connected to the web-based interface of the DAP-1150 device; now, you can do the following:

*Figure 19. The quick settings page in the router mode.*

To configure connection to the Internet, click the **Connect to internet** button. After clicking the button, the Internet Setup Wizard opens (see the ***Internet Setup Wizard*** section, page 71).

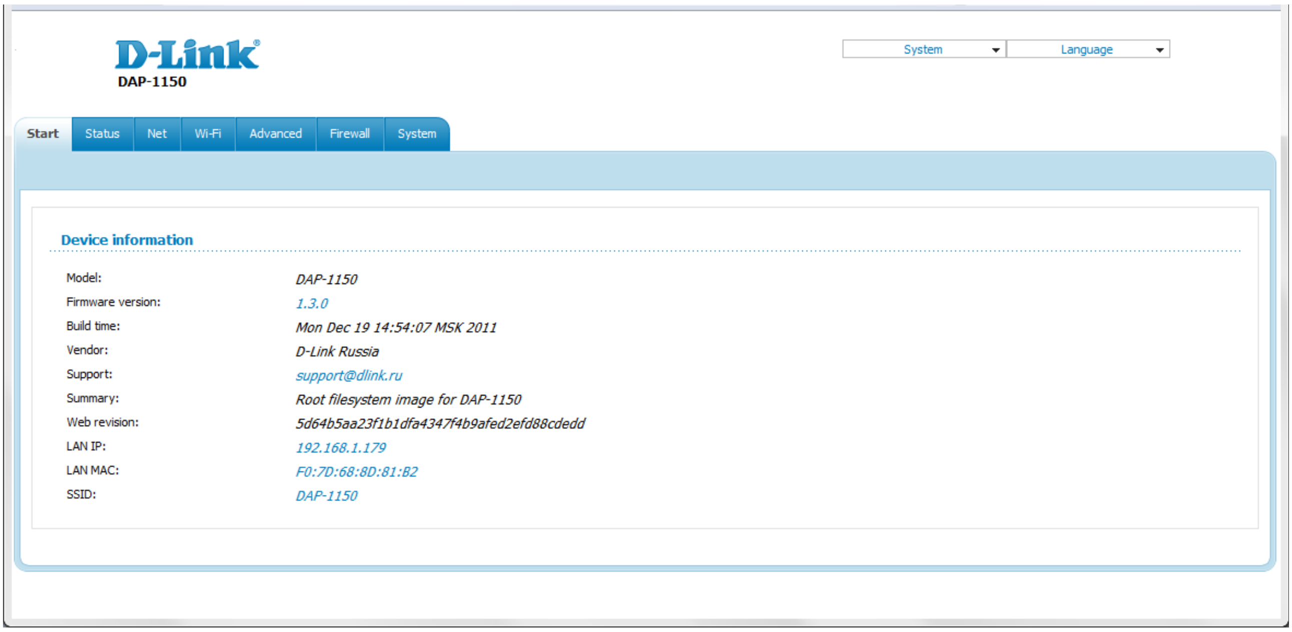
To configure access from the Internet to a web server located in your LAN, click the **Host site** button. After clicking the button, the Site Setup Wizard opens (see the ***Site Setup Wizard*** section, page 93).

To configure the access point's wireless network, click the **Configure Wi-Fi** button. After clicking the button, the Wi-Fi Setup Wizard opens (see the ***Wi-Fi Setup Wizard*** section, page 94).

To get back to the quick settings page from any Wizard or web-based interface menu section, left-click the D-Link logo in the top left corner of the page.

To configure all parameters of the access point independently without the Wizards, click the **Configure manually** button.

After clicking the **Configure manually** button the system statistics page opens. The 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.).



Device information

| | |
|---|---|
| Model: | DAP-1150 |
| Firmware version: | 1.3.0 |
| Build time: | Mon Dec 19 14:54:07 MSK 2011 |
| Vendor: | D-Link Russia |
| Support: | support@dlink.ru |
| Summary: | Root filesystem image for DAP-1150 |
| Web revision: | 5d64b5aa23f1b1dfa4347f4b9afed2efd88cdedd |
| LAN IP: | 192.168.1.179 |
| LAN MAC: | F0:7D:68:8D:81:B2 |
| SSID: | DAP-1150 |

*Figure 20. The system statistics page.*

From the system statistics page you can proceed to the page for upgrading the access point's firmware, contact the technical support group, and proceed to the settings of the local interface or the device's WLAN.

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 (see the ***Firmware Upgrade*** section, page 69).

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 (see the ***LAN*** section, page 39).

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 (see the ***Basic Settings*** section, page 42).

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.

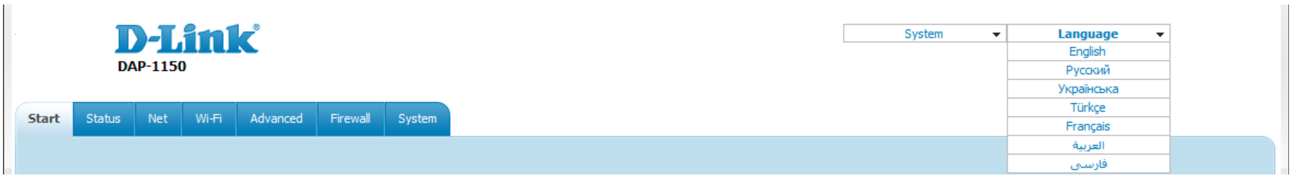


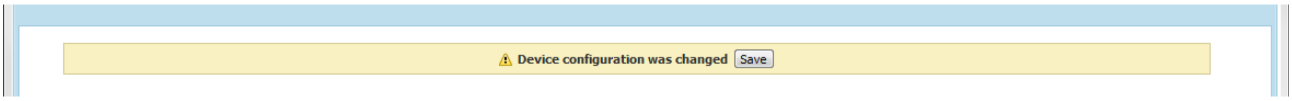
*Figure 21. Changing the language of the web-based interface.*

After selecting the language, the notification on unsaved changes will be displayed. Click the **Save** button to save the current language of the web-based interface as the default language.

## *Saving and Restoring Settings*

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

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



⚠ Device configuration was changed Save

*Figure 22. The notification on unsaved changes.*

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

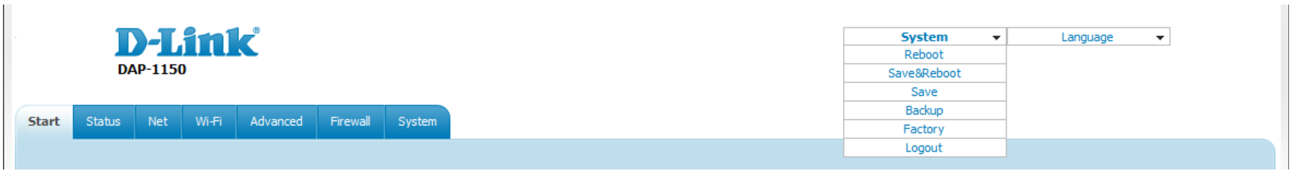


*Figure 23. The top-page menu.*

Click the **Reboot** line if you have already saved the device'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 device'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 RESET button. The button is located on the back panel of the access point next to the power connector.

To restore the factory default settings, do the following:

1. Power off the device.
2. Insert a small paperclip into the hole of the RESET button and push.
3. Power on the device keeping the button pushed.
4. After 5 seconds, release the button.

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 keep the button pushed for more than 8 seconds, the access point switches to crash recovery mode. To restore normal operation of the access point, please, contact the Technical Support Service.

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 devices equipped with a wireless interface 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.

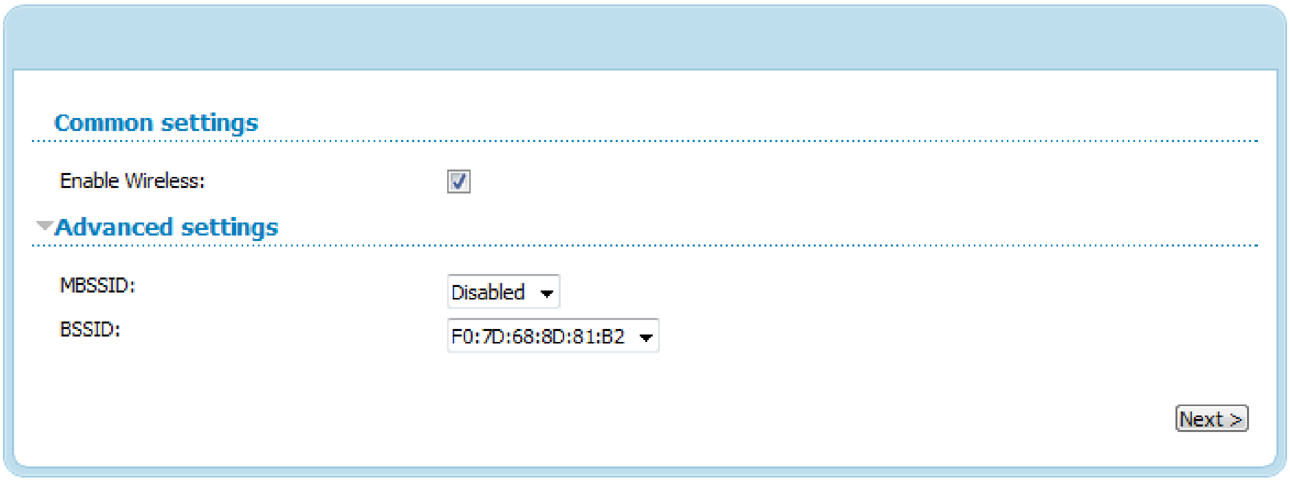
**!** When the device is switched to the router mode, the LAN port is used as the WAN port, therefore you cannot connect to it via a wired connection.

# CHAPTER 4. CONFIGURING DEVICE (ACCESS POINT MODE)

## *Setup Wizard*

### Wi-Fi Setup Wizard

To specify all needed settings for your wireless network, click the **Configure Wi-Fi** button.



Common settings

Enable Wireless: ☑

Advanced settings

MBSSID: Disabled

BSSID: F0:7D:68:8D:81:B2

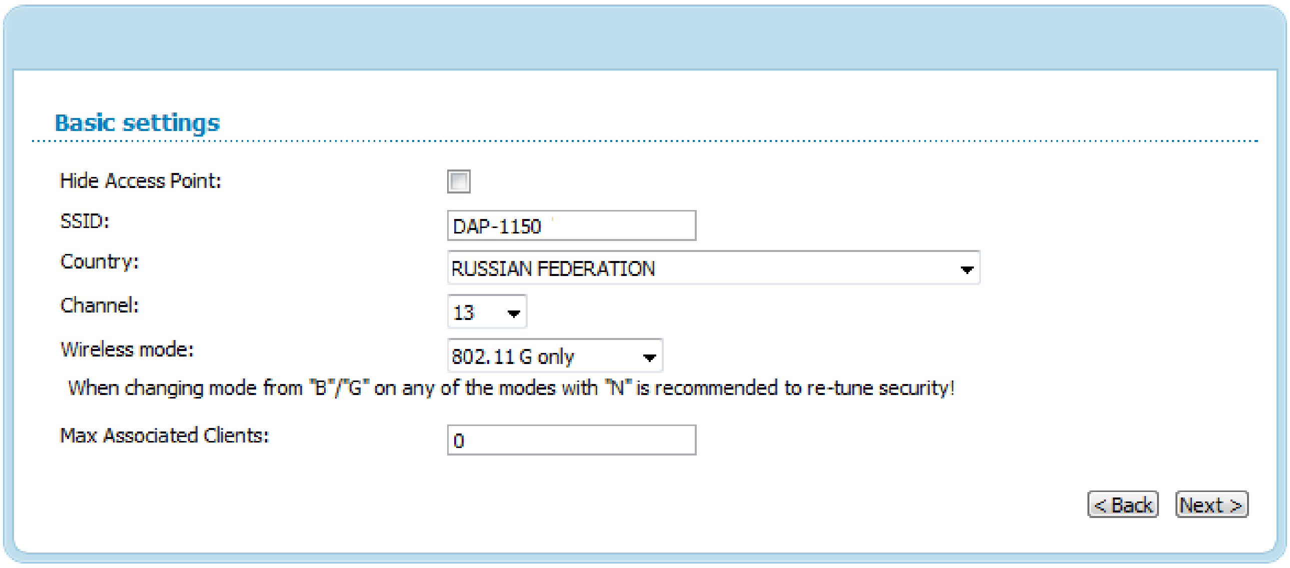
*Figure 24. Common and advanced settings of the wireless LAN.*

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**).



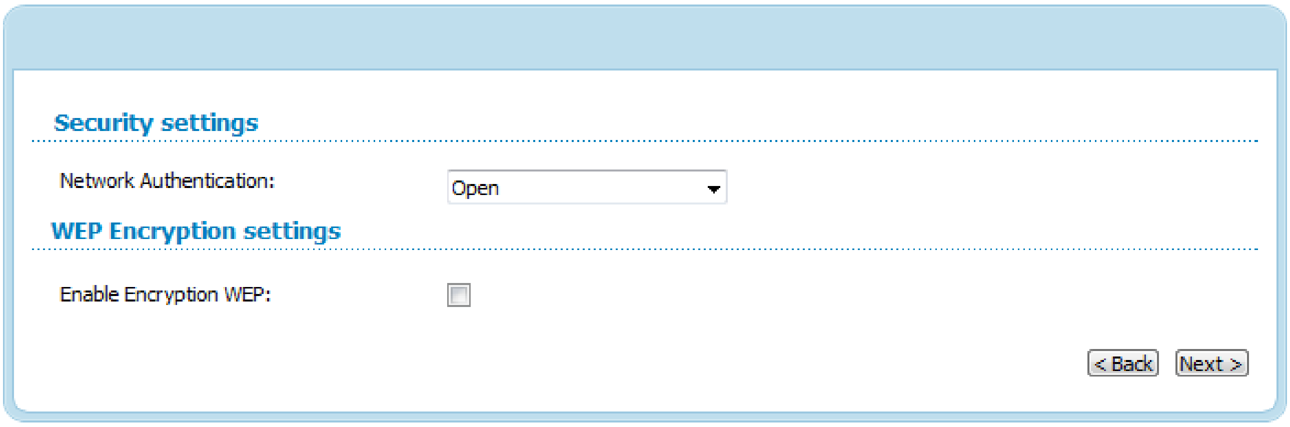
Basic settings

Hide Access Point: □
SSID: DAP-1150
Country: RUSSIAN FEDERATION
Channel: 13
Wireless mode: 802.11 G only
When changing mode from "B"/"G" on any of the modes with "N" is recommended to re-tune security!
Max Associated Clients: 0

*Figure 25. 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.



Security settings

Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP: □

*Figure 26. 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).

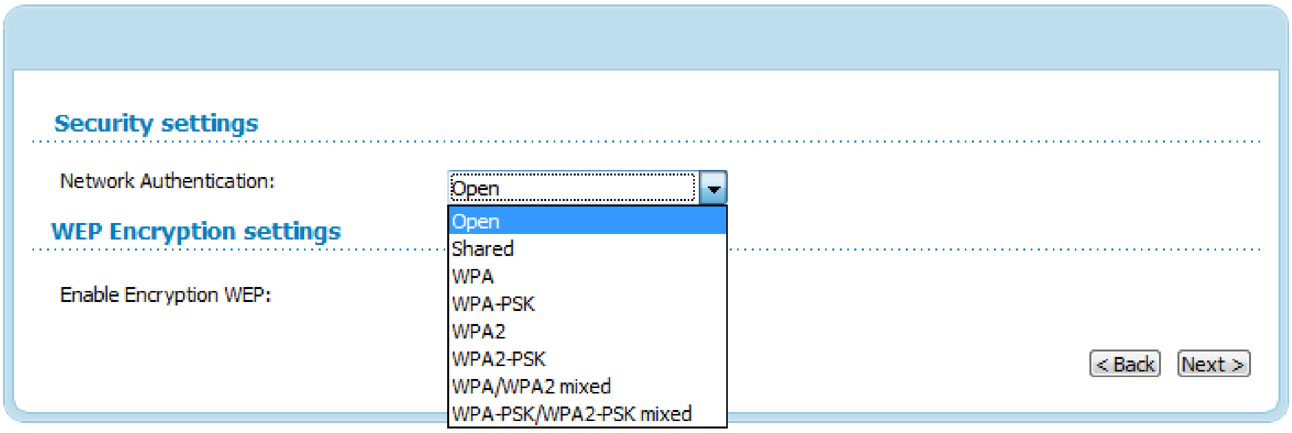


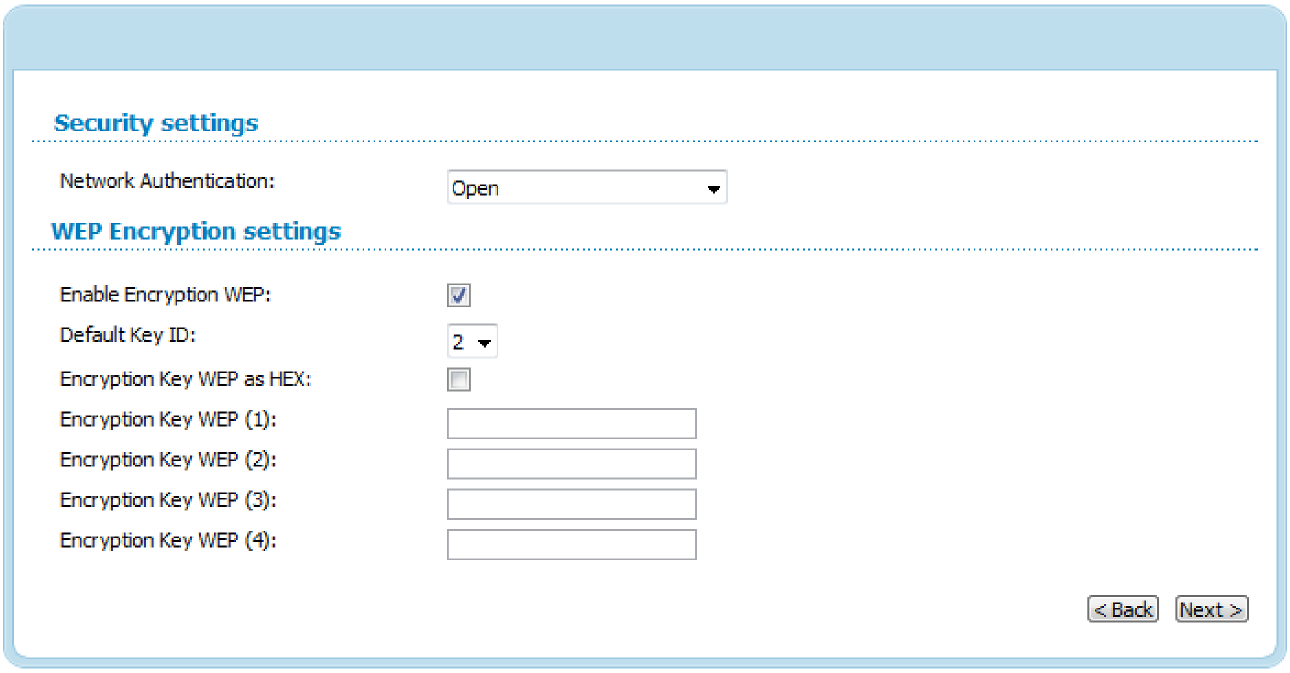
*Figure 27. Network authentication types supported by the access point.*

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** | WPA-based authentication using a RADIUS server. |
| **WPA-PSK** | WPA-based authentication using a PSK. |
| **WPA2** | WPA2-based authentication using a RADIUS server. |
| **WPA2-PSK** | WPA2-based authentication using a PSK. |
| **WPA/WPA2 mixed** | A mixed type of authentication. When this value is selected, devices using the **WPA** authentication type and devices using the **WPA2** authentication type can connect to the WLAN of the access point. |
| **WPA-PSK/WPA2-PSK mixed** | A mixed type of authentication. When this value is selected, devices using the **WPA-PSK** authentication type and devices using the **WPA2-PSK** authentication type can connect to the WLAN of the access point. |

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

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



Security settings

Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP: ☑

Default Key ID: 2

Encryption Key WEP as HEX: □

Encryption Key WEP (1):

Encryption Key WEP (2):

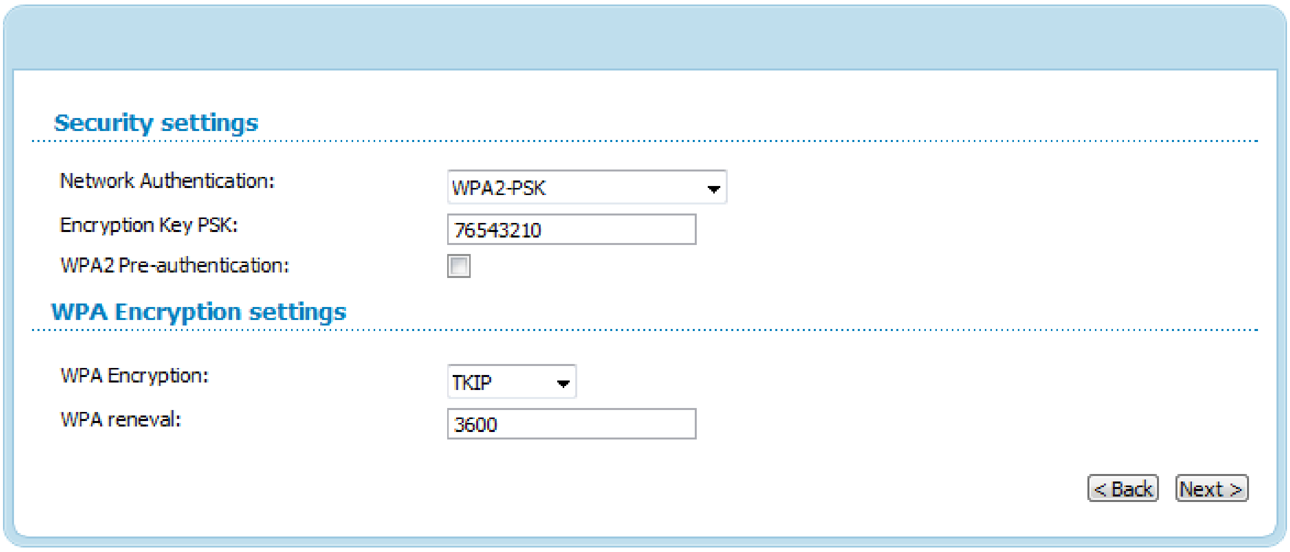
Encryption Key WEP (3):

Encryption Key WEP (4):

*Figure 28. 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.<br>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**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the **WPA Encryption settings** section is displayed:



**Security settings**

Network Authentication: WPA2-PSK

Encryption Key PSK: 76543210

WPA2 Pre-authentication: □

**WPA Encryption settings**

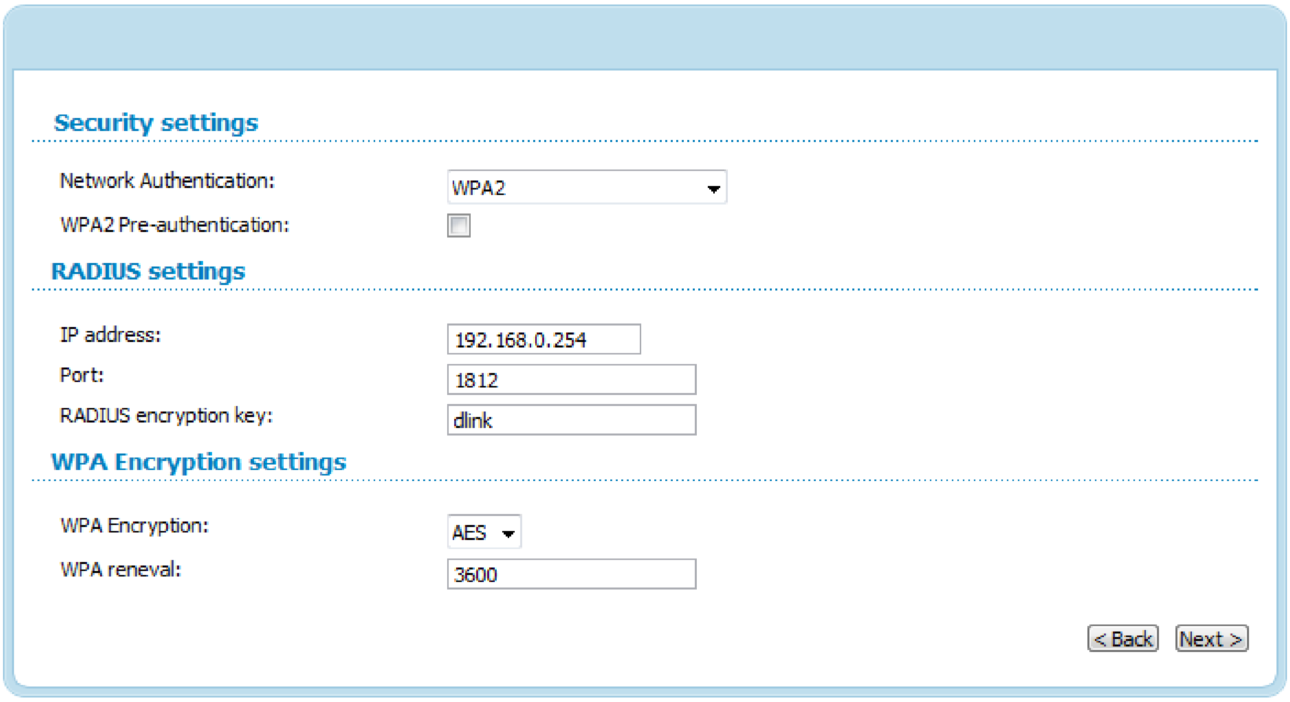
WPA Encryption: TKIP

WPA reneval: 3600

*Figure 29. 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** and **WPA-PSK/WPA2-PSK mixed** authentication types). |
| **WPA Encryption** | An encryption method: **TKIP**, **AES**, or **TKIP+AES**. |
| **WPA renewal** | The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed. |

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the **RADIUS settings** and **WPA Encryption settings** sections are available:



Security settings

Network Authentication: WPA2

WPA2 Pre-authentication: □

RADIUS settings

IP address: 192.168.0.254

Port: 1812

RADIUS encryption key: dlink

WPA Encryption settings

WPA Encryption: AES

WPA reneval: 3600

*Figure 30. The **WPA2** value is selected from the **Network Authentication** drop-down list.*

| Parameter | Description |
|---|---|
| **WPA2 Pre-authentication** | The checkbox activating preliminary authentication (displayed only for the **WPA2** and **WPA/WPA2 mixed** authentication types. |
| **IP address** | The IP address of the RADIUS server. |
| **Port** | A port of the RADIUS server. |
| **RADIUS encryption key** | The password which the access point uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings). |
| **WPA Encryption** | An encryption method: **TKIP** (available only for the **WPA** authentication type), **AES** (available only for the **WPA2** and **WPA/WPA2 mixed** authentication types). |
| **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.

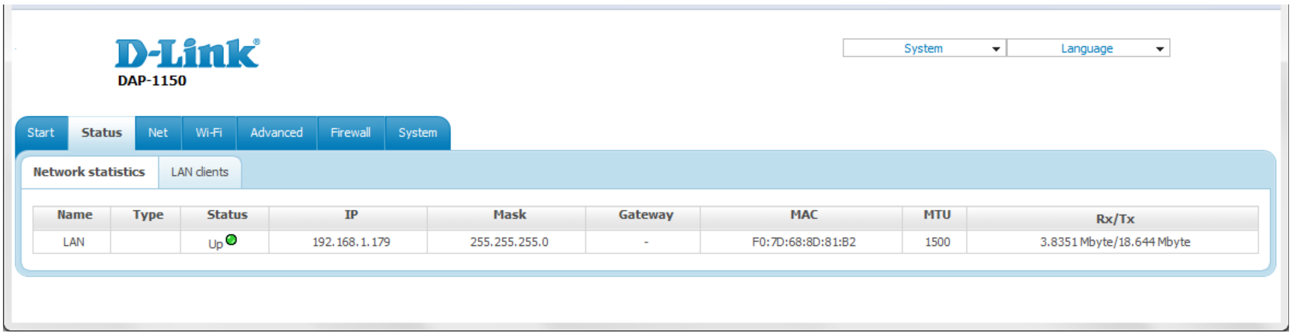
## *Status*

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

- network statistics
- 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 the local interface. On the page, the following data are displayed: IP address, subnet mask, 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).

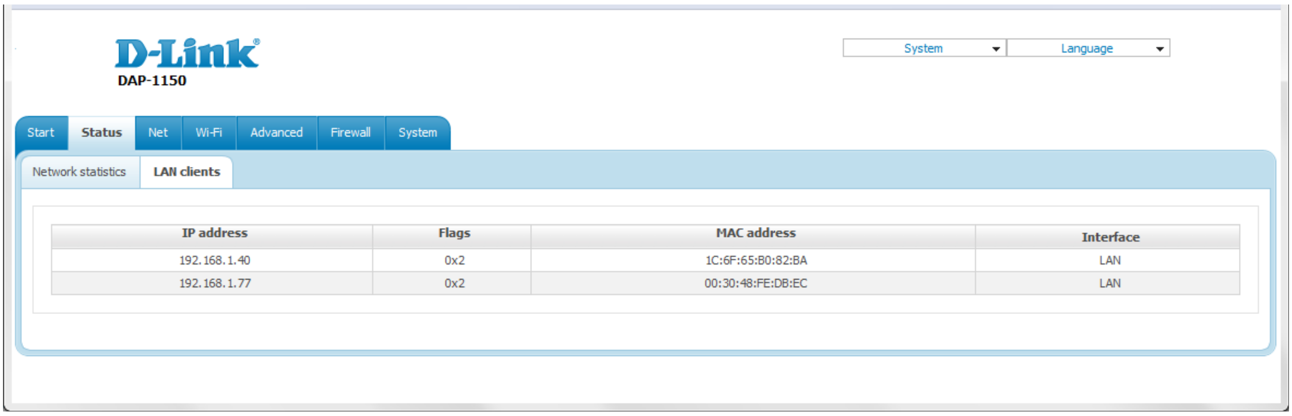


| Name | Type | Status | IP | Mask | Gateway | MAC | MTU | Rx/Tx |
|---|---|---|---|---|---|---|---|---|
| LAN | | Up ● | 192.168.1.179 | 255.255.255.0 | - | F0:7D:68:8D:81:B2 | 1500 | 3.8351 Mbyte/18.644 Mbyte |

*Figure 31. The **Status / Network statistics** 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.



| IP address | Flags | MAC address | Interface |
|---|---|---|---|
| 192.168.1.40 | 0x2 | 1C:6F:65:B0:82:BA | LAN |
| 192.168.1.77 | 0x2 | 00:30:48:FE:DB:EC | LAN |

*Figure 32. The **Status / LAN clients** page.*

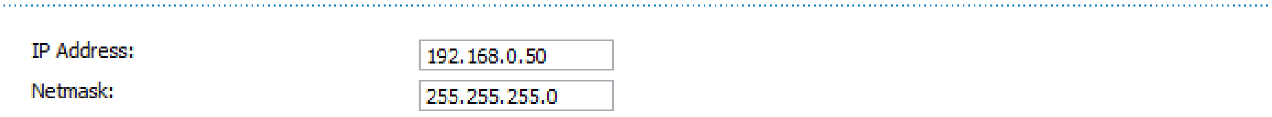
For each device the following data are displayed: the IP address, the MAC address, and the interface to which the device is connected.

## *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.



IP Address: 192.168.0.50

Netmask: 255.255.255.0

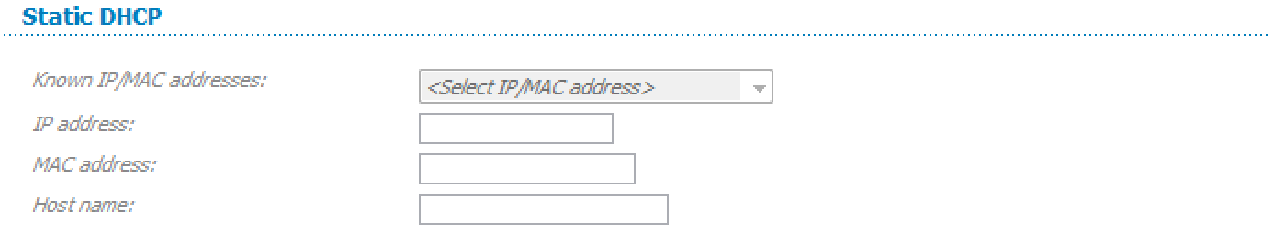
*Figure 33. Basic settings of the local interface.*

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 **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: <Select IP/MAC address>

IP address:

MAC address:

Host name:

*Figure 34. The section for creating MAC-IP pairs.*

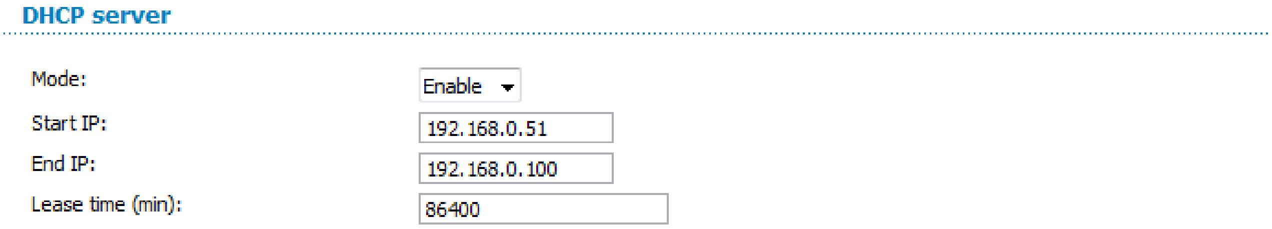
To create a MAC-IP pair, click the **Add** button. Enter the MAC address of the device from the LAN in the **MAC address** field and an IP address which will be assigned to this device in the **IP address** field. In the **Host name** field, specify a network name of the device for easier identification (*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 address** and **MAC address** 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 relevant line in the table and click the **Remove** button. Then click the **Save** button.

In the **DHCP server** section, you can configure the built-in DHCP sever of the access point.



DHCP server

| | |
|---|---|
| Mode: | Enable |
| Start IP: | 192.168.0.51 |
| End IP: | 192.168.0.100 |
| Lease time (min): | 86400 |

*Figure 35. The section for configuring the DHCP server.*

| Parameter | Description |
|---|---|
| **Mode** | An operating mode of the access point's DHCP server.<br>**Enable**: the access point assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the **Start IP**, **End IP**, and the **Lease time** fields are displayed on the page.<br>**Disable**: the access point's DHCP server is disabled, clients' IP addresses are assigned manually.<br>**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. |
| **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. |

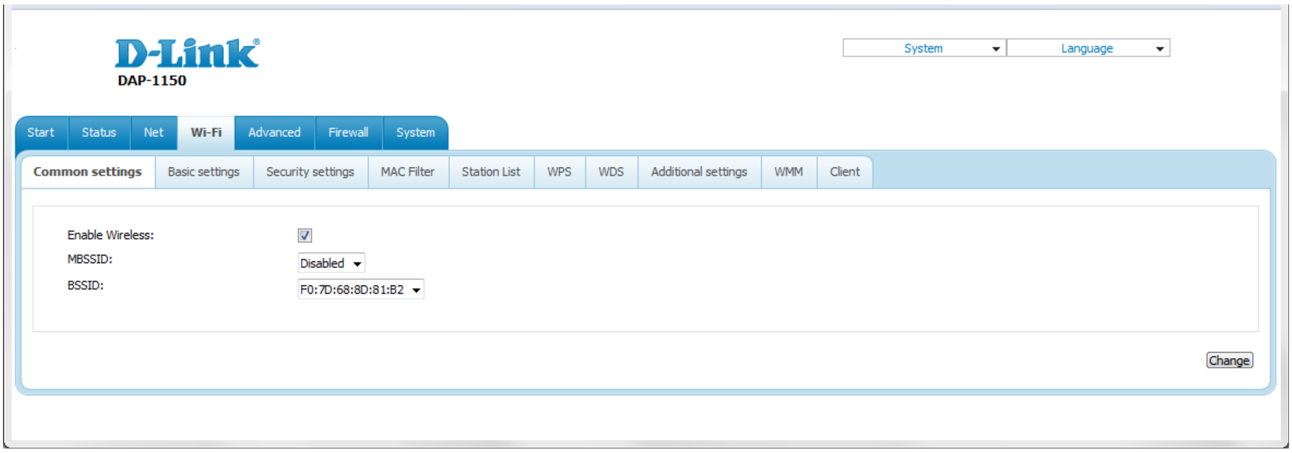
When all needed settings are configured, click the **Save** button.

## *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.



Enable Wireless: ☑
MBSSID: Disabled
BSSID: F0:7D:68:8D:81:B2

*Figure 36. 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).

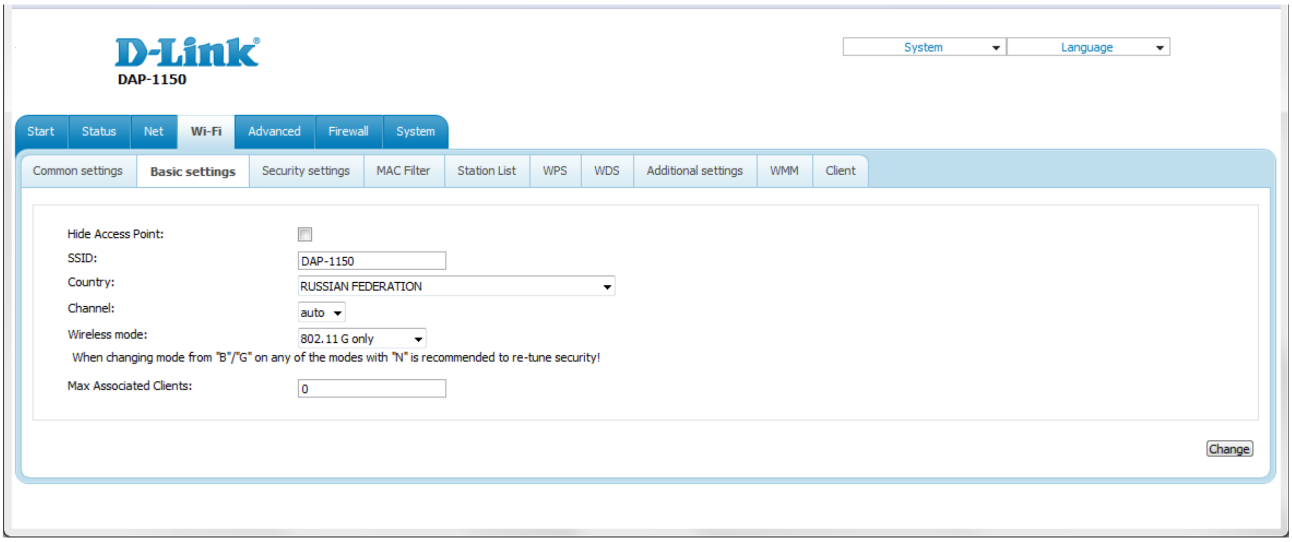
The value from the **BSSID** drop-down list is the unique identifier for your Wi-Fi network. You cannot change the value of this parameter, it is determined in the device's internal settings.

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.



Hide Access Point: □
SSID: DAP-1150
Country: RUSSIAN FEDERATION
Channel: auto
Wireless mode: 802.11 G only
When changing mode from "B"/"G" on any of the modes with "N" is recommended to re-tune security!
Max Associated Clients: 0

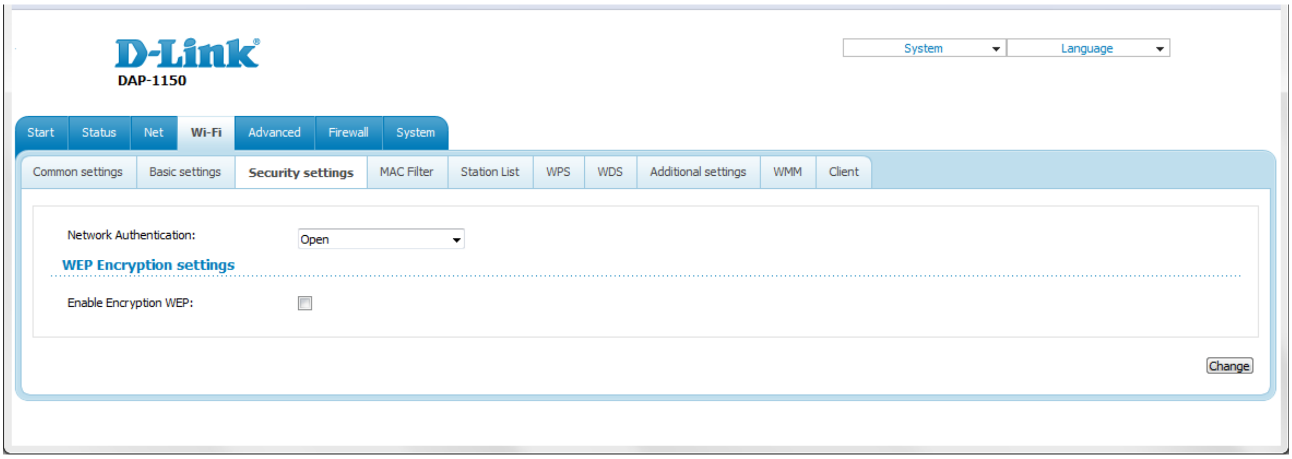
*Figure 37. Basic settings of the wireless LAN.*

| 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-1150** is specified. If your network is splitted into parts, each part has the default name (**DAP-1150.2**, **DAP-1150.3**, and **DAP-1150.4**). 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.



Network Authentication: Open

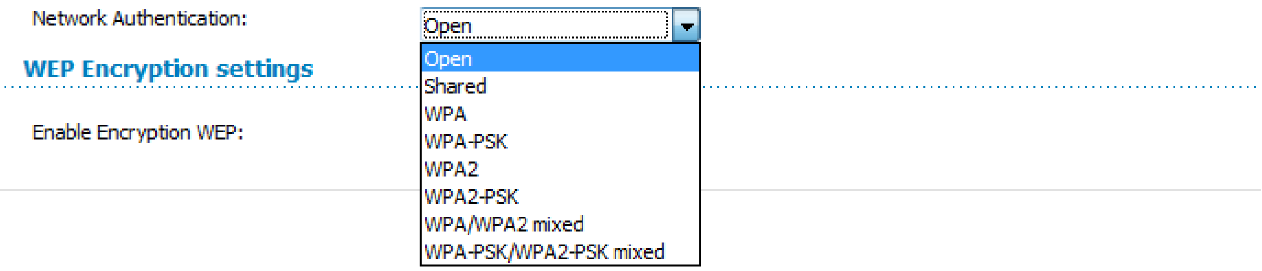
WEP Encryption settings

Enable Encryption WEP: □

*Figure 38. 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).



Network Authentication: Open

**WEP Encryption settings**

Enable Encryption WEP:

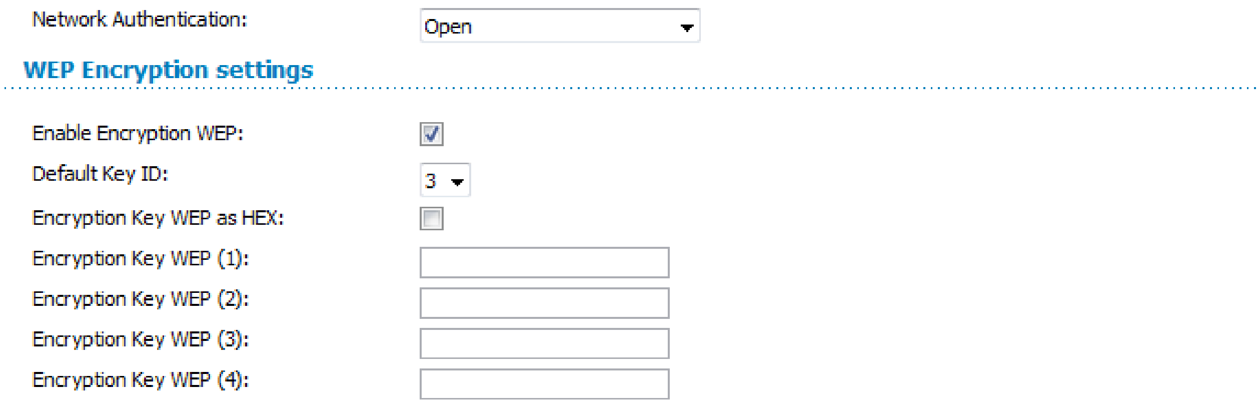
*Figure 39. Network authentication types supported by the access point.*

The access point supports the following authentication types:

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

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

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



Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP: ☑

Default Key ID: 3

Encryption Key WEP as HEX: □

Encryption Key WEP (1):

Encryption Key WEP (2):

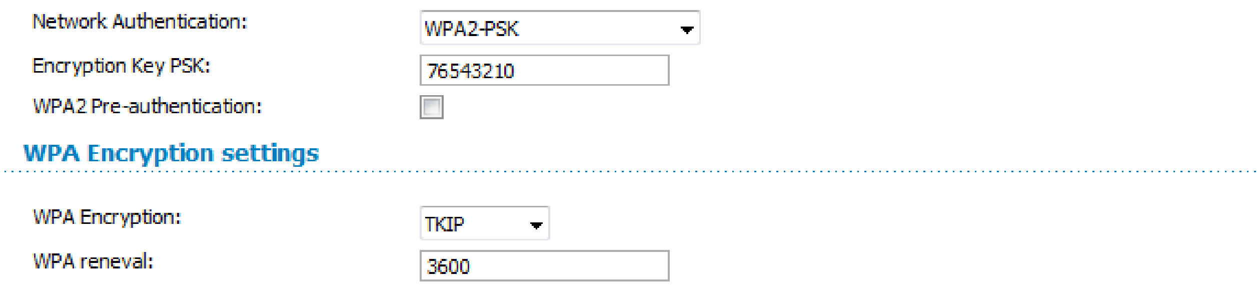
Encryption Key WEP (3):

Encryption Key WEP (4):

*Figure 40. 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.<br>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**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the **WPA Encryption settings** section is displayed:



Network Authentication: WPA2-PSK
Encryption Key PSK: 76543210
WPA2 Pre-authentication: □

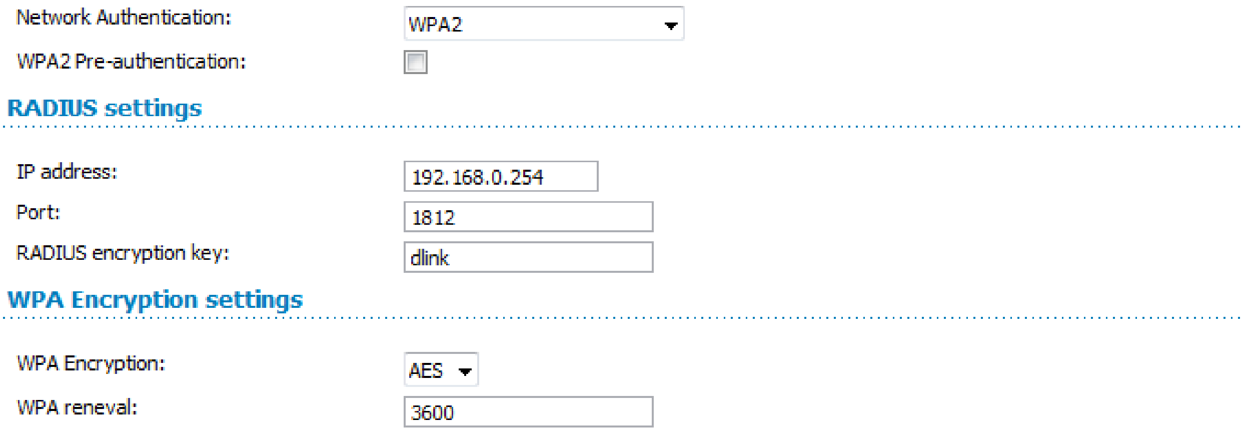
WPA Encryption settings

WPA Encryption: TKIP
WPA reneval: 3600

*Figure 41. 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** and **WPA-PSK/WPA2-PSK mixed** authentication types). |
| **WPA Encryption** | An encryption method: **TKIP**, **AES**, or **TKIP+AES**. |
| **WPA renewal** | The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed. |

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the **RADIUS settings** and **WPA Encryption settings** sections are available:



Network Authentication: WPA2

WPA2 Pre-authentication: □

RADIUS settings

IP address: 192.168.0.254

Port: 1812

RADIUS encryption key: dlink

WPA Encryption settings

WPA Encryption: AES

WPA renewal: 3600

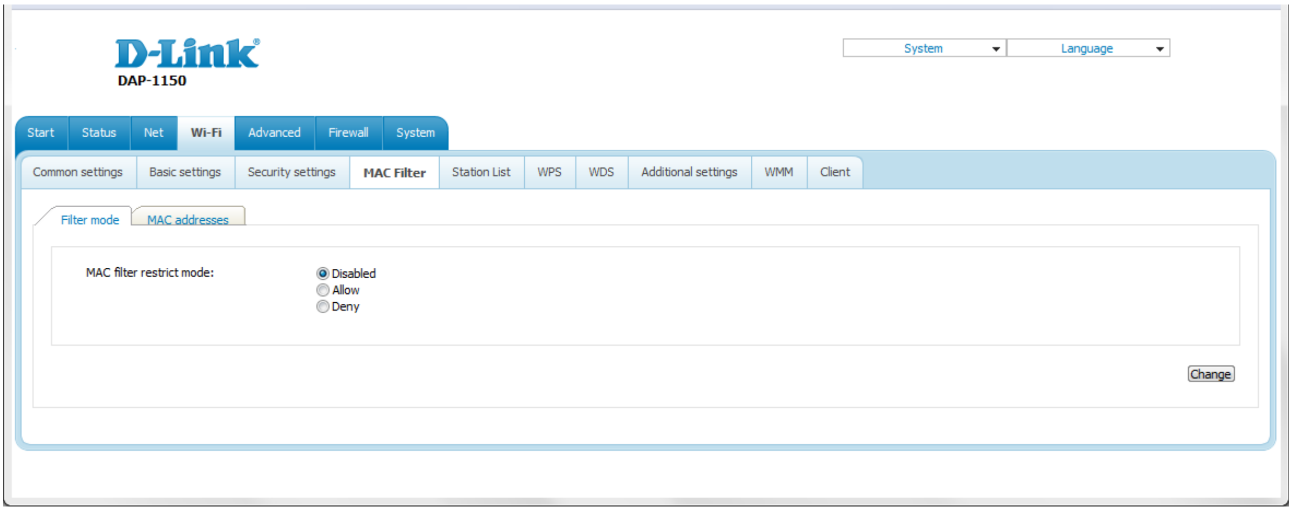
*Figure 42. The **WPA2** value is selected from the **Network Authentication** drop-down list.*

| Parameter | Description |
|---|---|
| **WPA2 Pre-authentication** | The checkbox activating preliminary authentication (displayed only for the **WPA2** and **WPA/WPA2 mixed** authentication types. |
| **IP address** | The IP address of the RADIUS server. |
| **Port** | A port of the RADIUS server. |
| **RADIUS encryption key** | The password which the access point uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings). |
| **WPA Encryption** | An encryption method: **TKIP** (available only for the **WPA** authentication type), **AES** (available only for the **WPA2** and **WPA/WPA2 mixed** authentication types). |
| **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.



MAC filter restrict mode:
● Disabled
○ Allow
○ Deny

*Figure 43. 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.

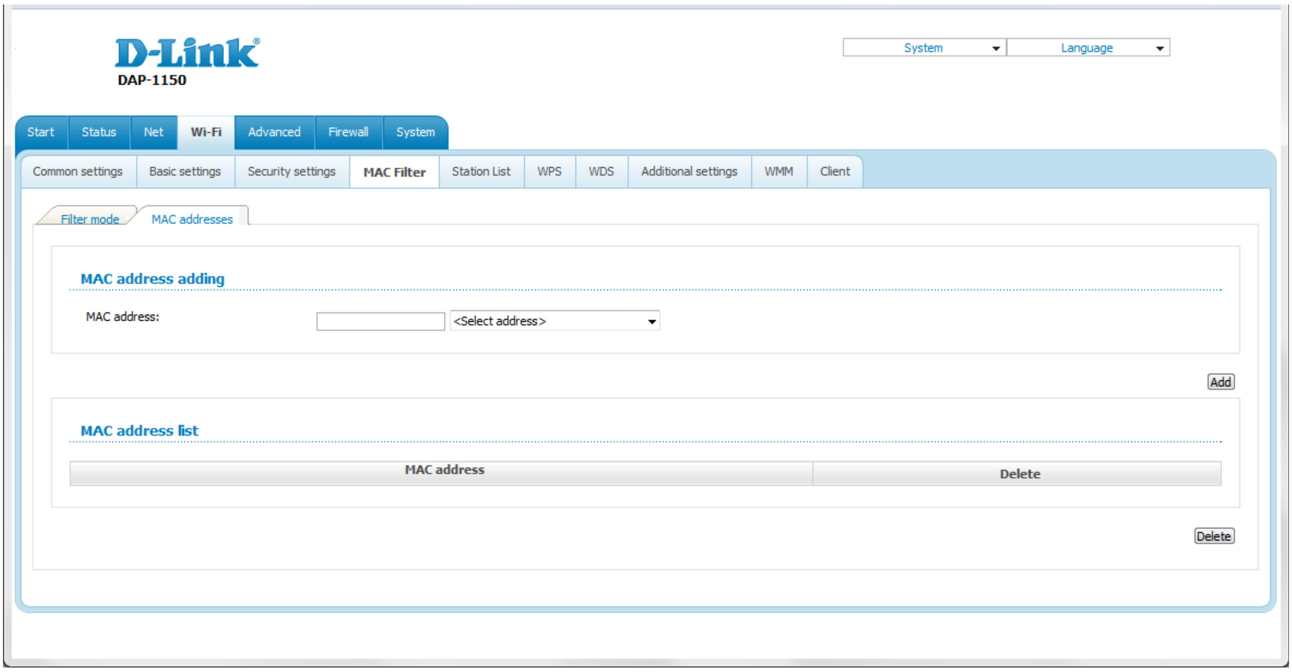


*Figure 44. The tab for adding a MAC address.*

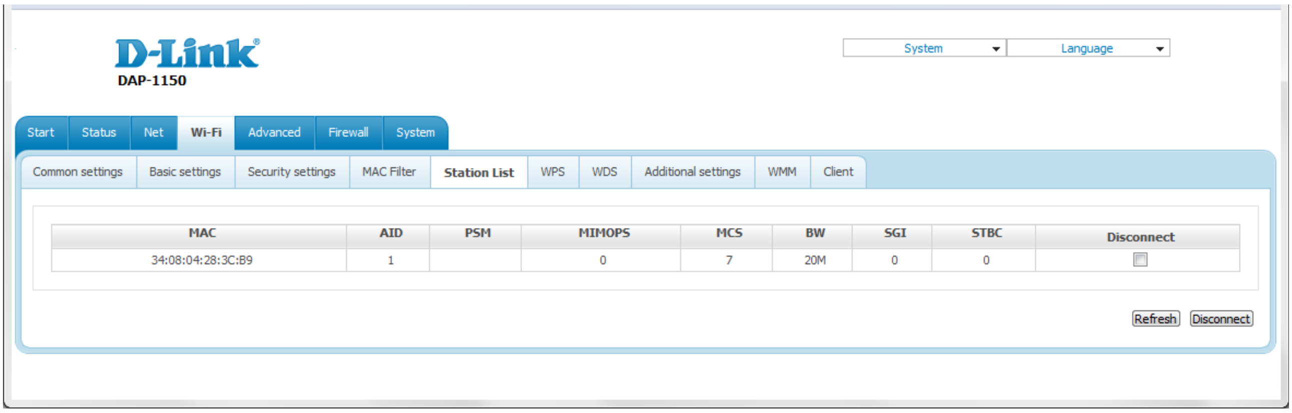
Enter an address in the **MAC address** field of the **MAC address adding** section and click the **Add** button.

To add the MAC address of a device connected to the access point's LAN at the moment, select the value containing the MAC and IP address of this device from the drop-down list located to the right of the **MAC address** field (the field will be filled in automatically) 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.



| MAC | AID | PSM | MIMOPS | MCS | BW | SGI | STBC | Disconnect |
|---|---|---|---|---|---|---|---|---|
| 34:08:04:28:3C:B9 | 1 |  | 0 | 7 | 20M | 0 | 0 | □ |

*Figure 45. The list of the wireless clients.*

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

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

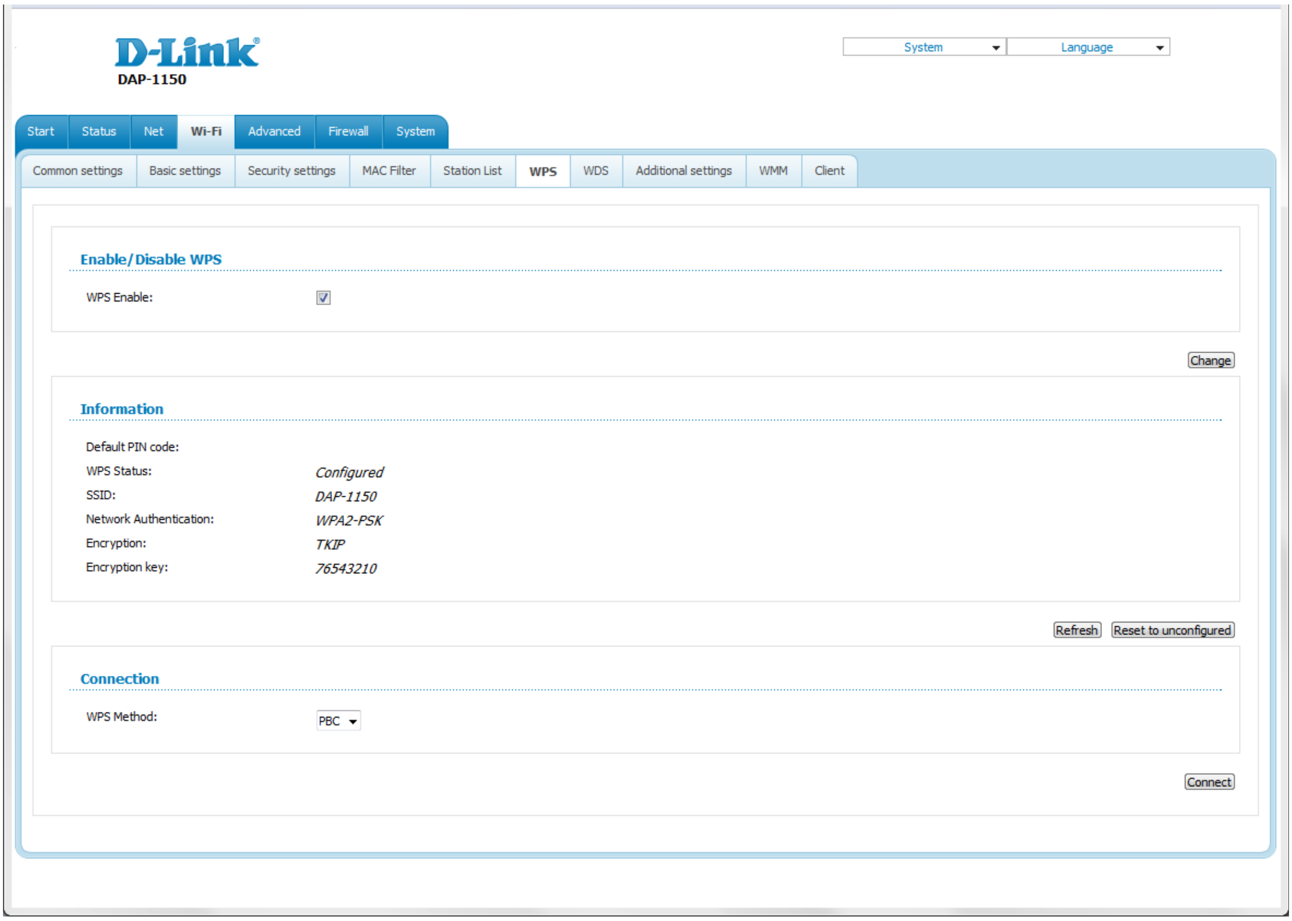
## WPS

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

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

! If the device's WLAN is 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 WPS function it is required to configure a type of WPA encryption.



**Enable/Disable WPS**

WPS Enable: ☑

**Information**

Default PIN code:
WPS Status: *Configured*
SSID: *DAP-1150*
Network Authentication: *WPA2-PSK*
Encryption: *TKIP*
Encryption key: *76543210*

**Connection**

WPS Method: PBC

*Figure 46. 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:<br>• **Configured** (all needed settings are specified)<br>• **Unconfigured** (you need to specify the relevant settings). |
| **SSID** | The name of the device'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 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 view the latest data on the state of connecting the wireless device via the WPS function. |
| **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.<br>**PIN**: Connecting the device via the PIN code.<br>**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.<br>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 WLAN of the access point via the WPS function. |

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 WLAN of the access point.
5. Click the relevant button in the software or on the cover 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.

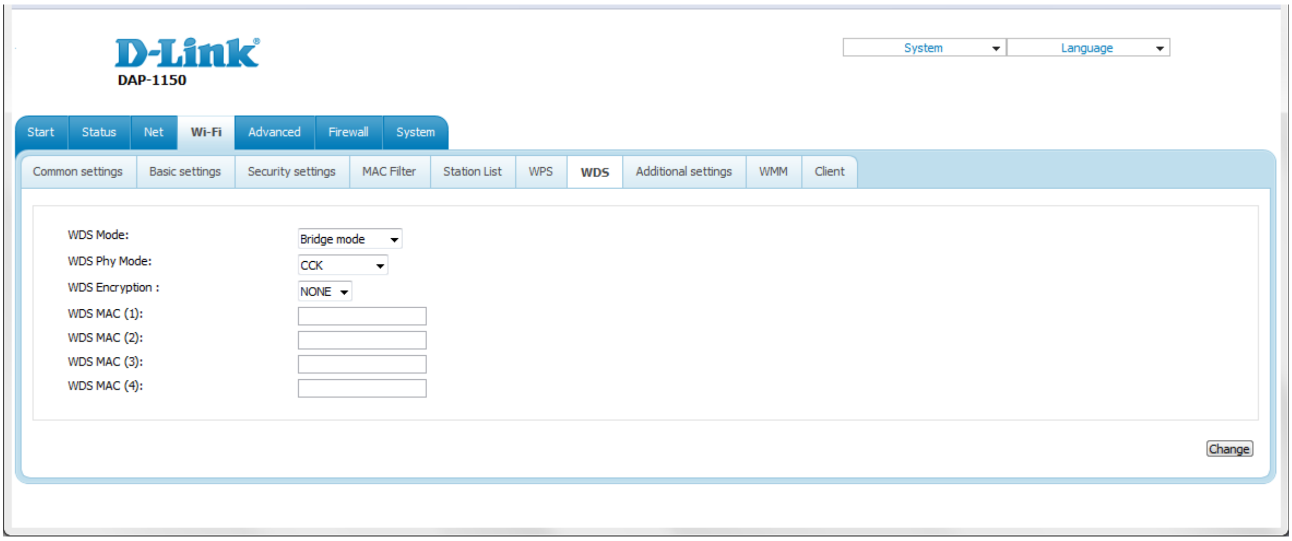
To add a wireless device via the PBC method of the WPS function, follow the next steps:

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 WLAN of the access point.
5. Click the relevant button in the software or 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.

## 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.



WDS Mode: Bridge mode
WDS Phy Mode: CCK
WDS Encryption : NONE
WDS MAC (1):
WDS MAC (2):
WDS MAC (3):
WDS MAC (4):

*Figure 47. The page for configuring the WDS function.*

The following fields are available on the page:

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

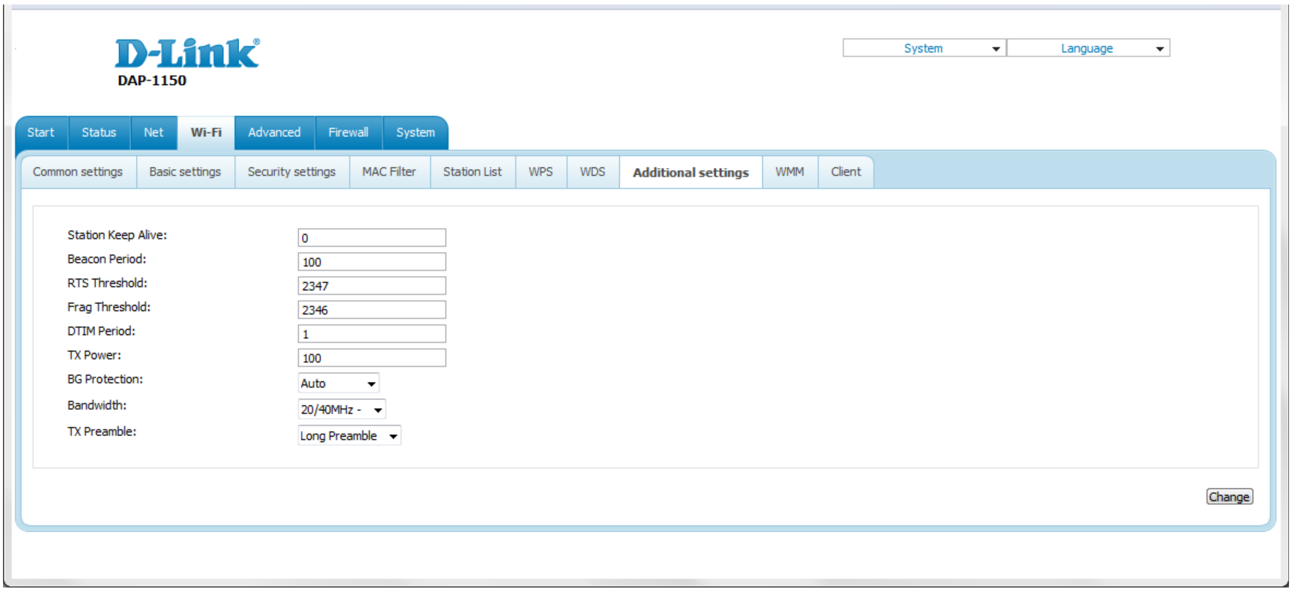
! The WDS function parameters specified on the page must be the same for all interconnected devices. In addition, it is required to set the same channel (on the **Wi-Fi / Basic settings** page).

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



Station Keep Alive: 0
Beacon Period: 100
RTS Threshold: 2347
Frag Threshold: 2346
DTIM Period: 1
TX Power: 100
BG Protection: Auto
Bandwidth: 20/40MHz -
TX Preamble: Long Preamble

*Figure 48. 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. |
| **TX Power** | The transmit power (in percentage terms) of the access point. |

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

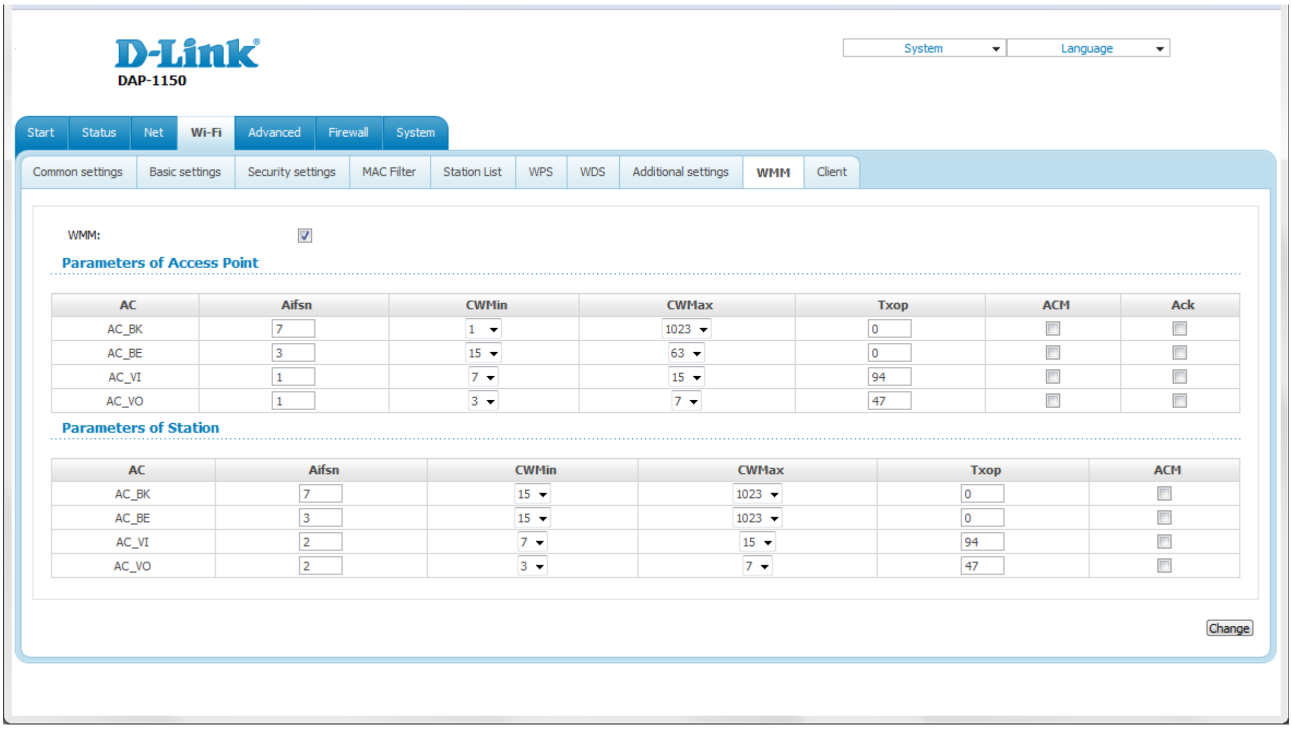
When you have configured the parameters, click the **Change** button.

# 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.



WMM: ☑

Parameters of Access Point

| AC | Aifsn | CWMin | CWMax | Txop | ACM | Ack |
|---|---|---|---|---|---|---|
| AC_BK | 7 | 1 | 1023 | 0 | □ | □ |
| AC_BE | 3 | 15 | 63 | 0 | □ | □ |
| AC_VI | 1 | 7 | 15 | 94 | □ | □ |
| AC_VO | 1 | 3 | 7 | 47 | □ | □ |

Parameters of Station

| AC | Aifsn | CWMin | CWMax | Txop | ACM |
|---|---|---|---|---|---|
| AC_BK | 7 | 15 | 1023 | 0 | □ |
| AC_BE | 3 | 15 | 1023 | 0 | □ |
| AC_VI | 2 | 7 | 15 | 94 | □ |
| AC_VO | 2 | 3 | 7 | 47 | □ |

*Figure 49. 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** | *Arbitrary Inter-Frame Space Number.* This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority. |
| **CWMin/CWMax** | *Contention Window Minimum/Contention Window Maximum*. 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** | *Transmission Opportunity*. The higher the value, the higher is the Access Category priority. |
| **ACM** | *Admission Control Mandatory.*<br>If selected, prevents from using the relevant Access Category. |
| **Ack** | *Acknowledgment*. Answering response requests while transmitting. Displayed only in the **Parameters of Access Point** section.<br>If not selected, the access point answers requests.<br>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-1150 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-1150 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-1150 and the remote access point. Other parameters of the wireless network of DAP-1150 do not depend upon the settings of the remote access point.

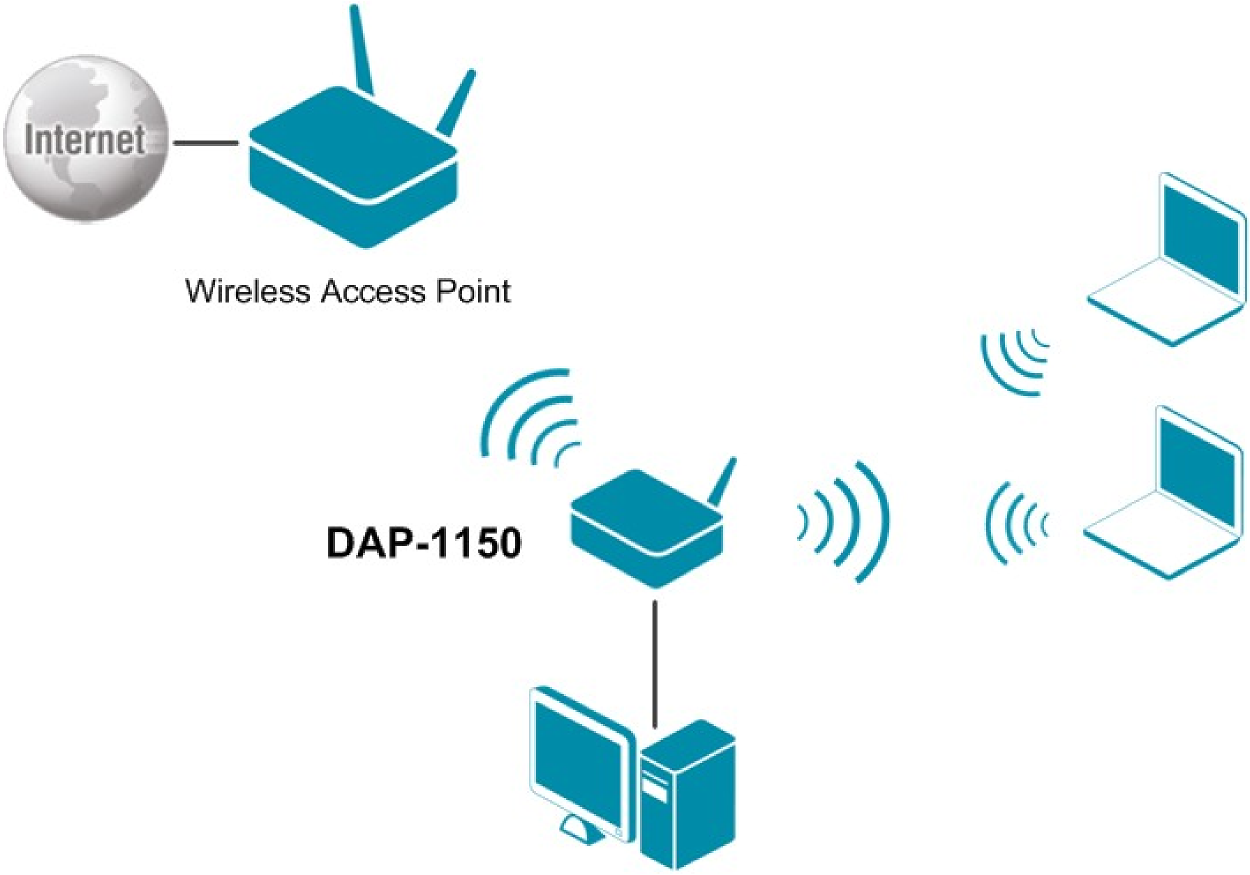
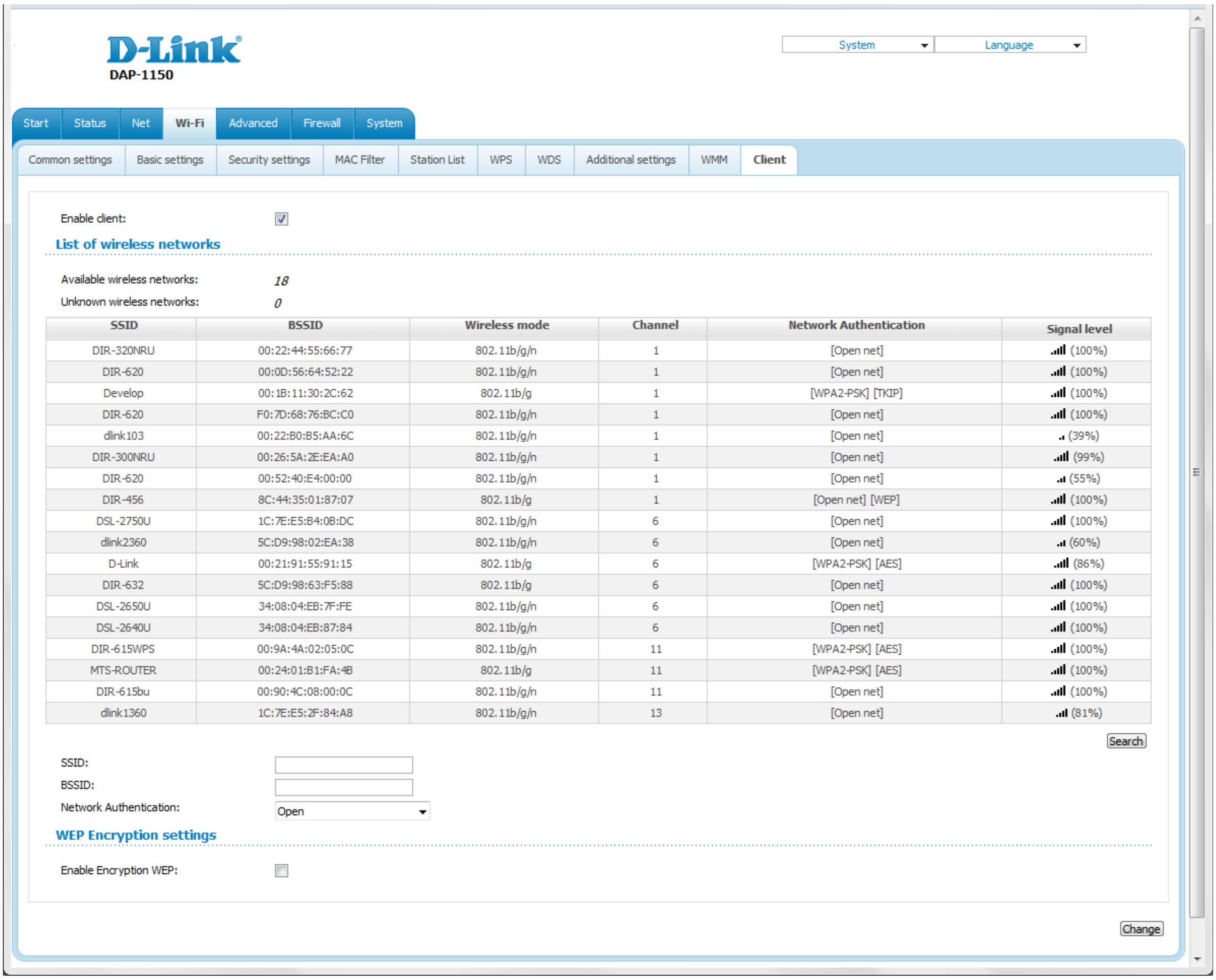


*Figure 50. Connecting DAP-1150 in the access point mode as a client.*

To allow the devices from the LAN of DAP-1150 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.



Enable client: ☑

**List of wireless networks**

Available wireless networks: *18*

Unknown wireless networks: *0*

| SSID | BSSID | Wireless mode | Channel | Network Authentication | Signal level |
|---|---|---|---|---|---|
| DIR-320NRU | 00:22:44:55:66:77 | 802.11b/g/n | 1 | [Open net] | (100%) |
| DIR-620 | 00:0D:56:64:52:22 | 802.11b/g/n | 1 | [Open net] | (100%) |
| Develop | 00:1B:11:30:2C:62 | 802.11b/g | 1 | [WPA2-PSK] [TKIP] | (100%) |
| DIR-620 | F0:7D:68:76:BC:C0 | 802.11b/g/n | 1 | [Open net] | (100%) |
| dlink103 | 00:22:B0:B5:AA:6C | 802.11b/g/n | 1 | [Open net] | (39%) |
| DIR-300NRU | 00:26:5A:2E:EA:A0 | 802.11b/g/n | 1 | [Open net] | (99%) |
| DIR-620 | 00:52:40:E4:00:00 | 802.11b/g/n | 1 | [Open net] | (55%) |
| DIR-456 | 8C:44:35:01:87:07 | 802.11b/g | 1 | [Open net] [WEP] | (100%) |
| DSL-2750U | 1C:7E:E5:B4:0B:DC | 802.11b/g/n | 6 | [Open net] | (100%) |
| dlink2360 | 5C:D9:98:02:EA:38 | 802.11b/g/n | 6 | [Open net] | (60%) |
| D-Link | 00:21:91:55:91:15 | 802.11b/g | 6 | [WPA2-PSK] [AES] | (86%) |
| DIR-632 | 5C:D9:98:63:F5:88 | 802.11b/g | 6 | [Open net] | (100%) |
| DSL-2650U | 34:08:04:EB:7F:FE | 802.11b/g/n | 6 | [Open net] | (100%) |
| DSL-2640U | 34:08:04:EB:87:84 | 802.11b/g/n | 6 | [Open net] | (100%) |
| DIR-615WPS | 00:9A:4A:02:05:0C | 802.11b/g/n | 11 | [WPA2-PSK] [AES] | (100%) |
| MTS-ROUTER | 00:24:01:B1:FA:4B | 802.11b/g | 11 | [WPA2-PSK] [AES] | (100%) |
| DIR-615bu | 00:90:4C:08:00:0C | 802.11b/g/n | 11 | [Open net] | (100%) |
| dlink1360 | 1C:7E:E5:2F:84:A8 | 802.11b/g/n | 13 | [Open net] | (81%) |

SSID:

BSSID:

Network Authentication: Open

**WEP Encryption settings**

Enable Encryption WEP: □

*Figure 51. 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-1150 will switch to the channel of the wireless access point to which you have connected.

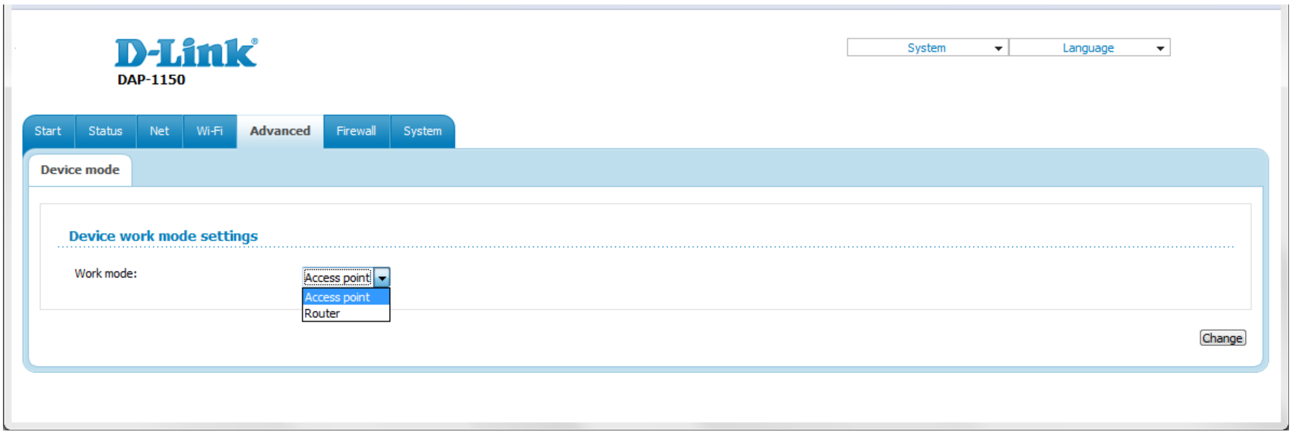
If the access point is connected to the selected network successfully, the green indicator appears to the right of the network's SSID in the table.

# *Advanced*

This menu is designed for switching the operating modes of the device.

## Device mode

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



Device work mode settings

Work mode: Access point

Access point
Router

*Figure 52. 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. Then select the **Save&Reboot** value from the top-page menu displayed when the mouse pointer is over the **System** caption and wait until the device is rebooted.

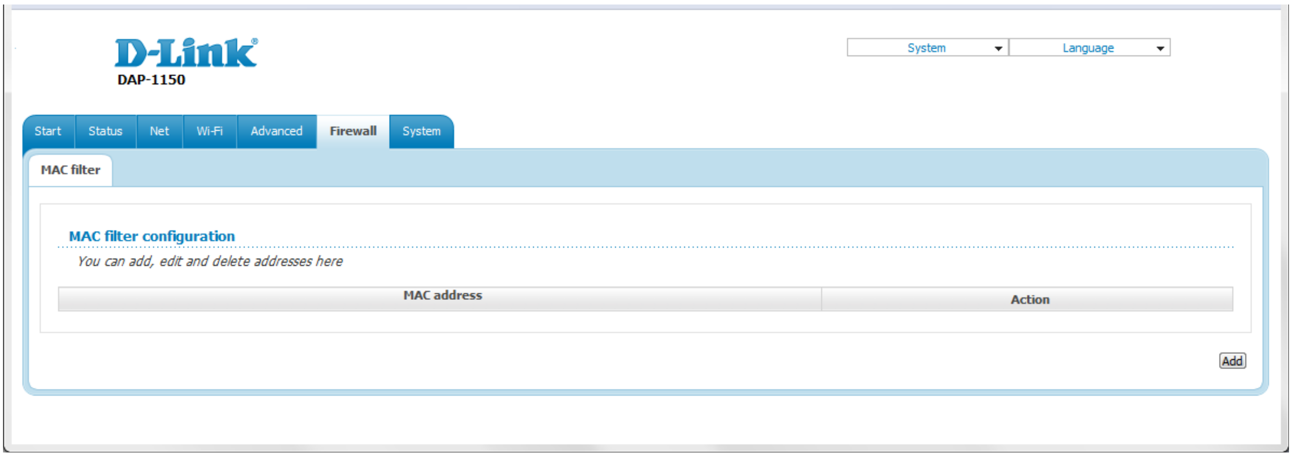
! When the device is switched to the router mode, you cannot connect to it via a wired connection.

## *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.



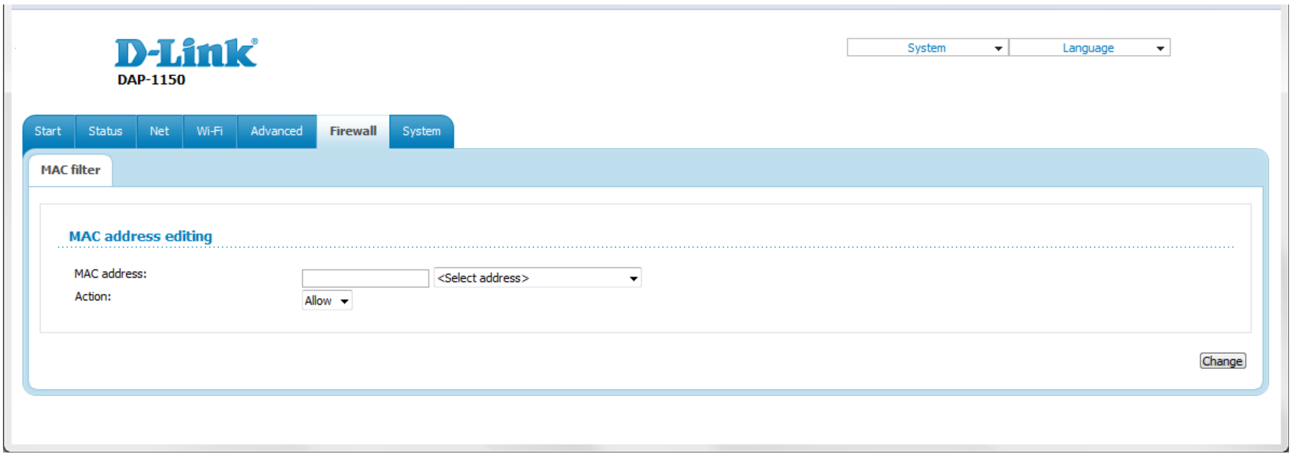
MAC filter configuration

*You can add, edit and delete addresses here*

| MAC address | Action |
|---|---|

*Figure 53. The **Firewall / MAC filter** page.*

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



MAC address editing

MAC address: <Select address>

Action: Allow

*Figure 54. 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 located to the right of the field (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*

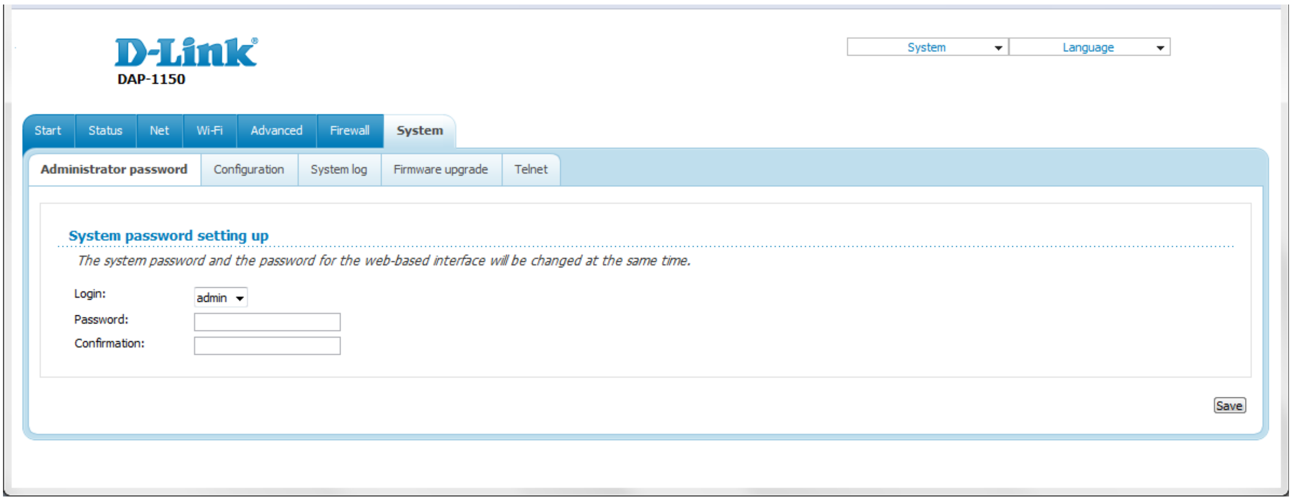
In this menu you can do the following:

- 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
- allow or forbid access to the access point via TELNET.

## 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.



System password setting up

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

Login: admin

Password:

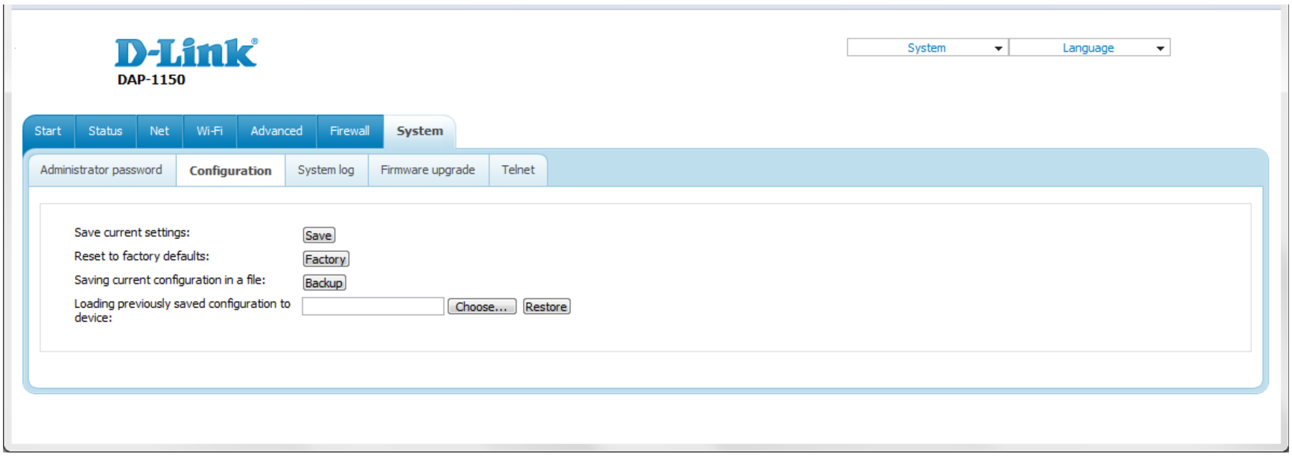
Confirmation:

*Figure 55. 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.



Save current settings: Save

Reset to factory defaults: Factory

Saving current configuration in a file: Backup

Loading previously saved configuration to device: Choose... Restore

*Figure 56. The **System / Configuration** page.*

The following buttons are available on the page:

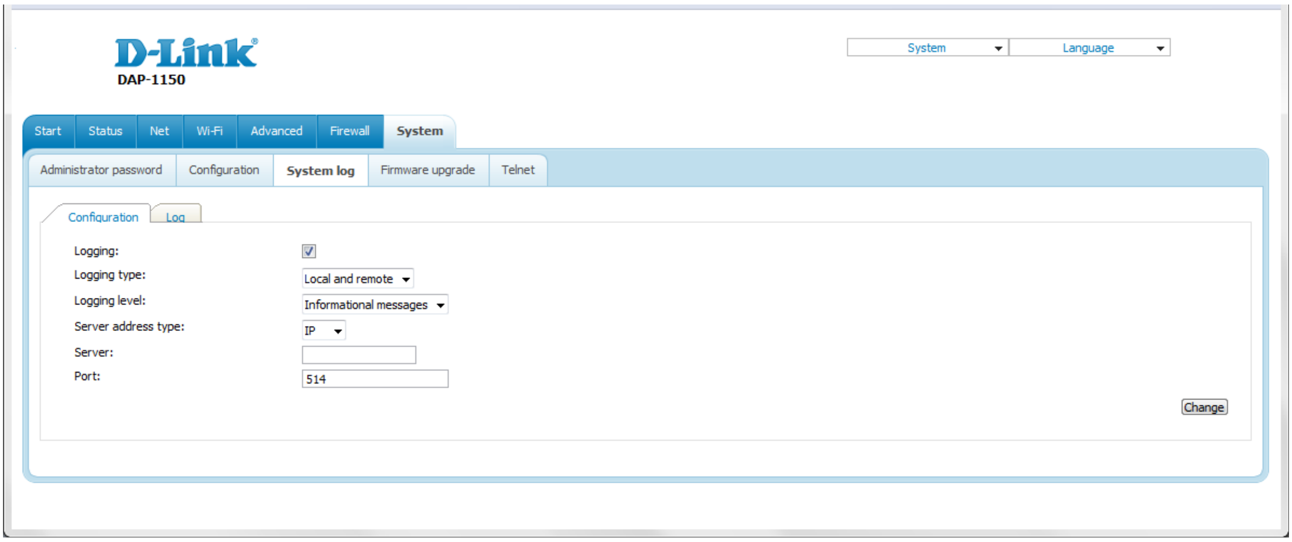
| Control | Description |
|---|---|
| **Save** | Click the button to save settings to the non-volatile memory. Please, save settings every time you change the device's parameters. Otherwise the changes will be lost upon hardware reboot of the access point. |
| **Factory** | Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button (see the ***Saving and Restoring Settings*** section, page 29). |
| **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.



Logging: ☑
Logging type: Local and remote
Logging level: Informational messages
Server address type: IP
Server:
Port: 514

*Figure 57. The **System / System log** page. The **Configuration** tab.*

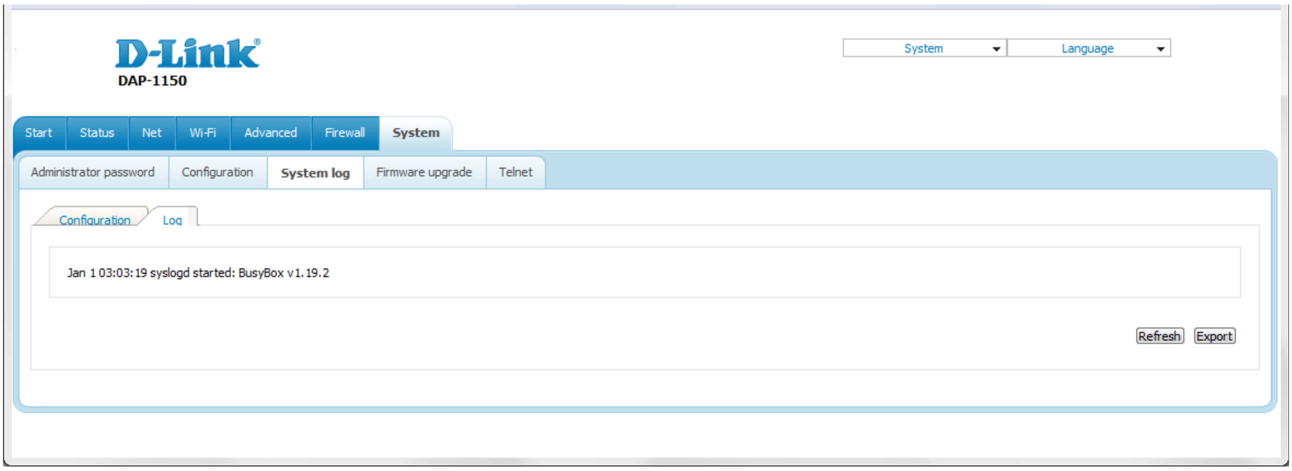
To enable logging of the system events, select the **Logging** checkbox on the **Configuration** tab. Then specify the needed parameters.

| Control | Description |
|---|---|
| **Logging type** | Select a type of logging from the drop-down list.<br>• **Local**: the system log is stored in the device's memory (and displayed on the **Log** tab). When this value is selected, the **Server address type**, **Server**, and **Port** fields are not displayed.<br>• **Remote**: the system log is sent to the remote host specified in the **Server** field.<br>• **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 address type** | From the drop-down list, select the **IP** value to specify an IP address of a host from the local or global network, or the **URL** value to specify a URL address of a remote server. |
| **Server** | The IP or URL address of the host from the local or global network, to which the system log will be sent. |
| **Port** | A port of the host specified in the **Server** field. By default, the value **514** is specified. |

After specifying the needed parameters, click the **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.



```
Jan 1 03:03:19 syslogd started: BusyBox v1.19.2
```

*Figure 58. 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 (available only in the access point mode).

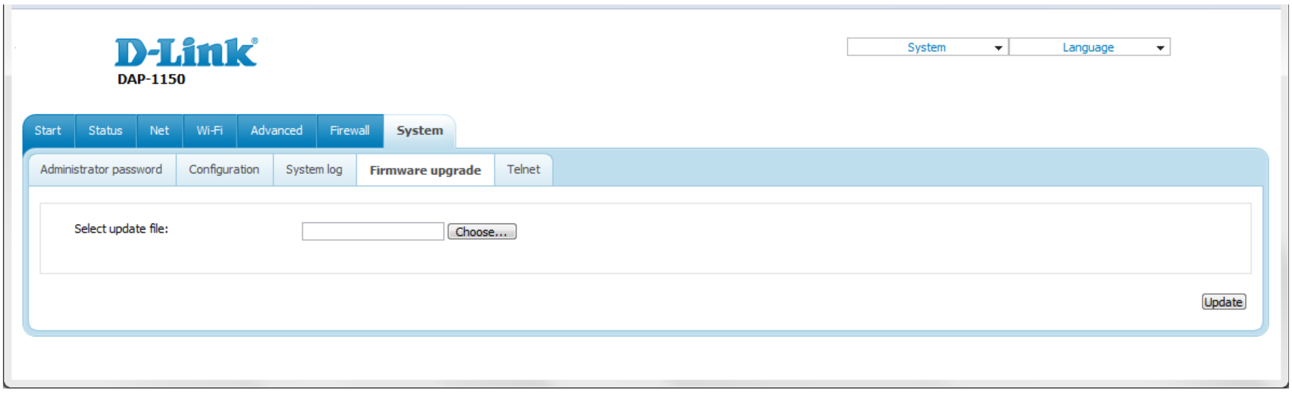


*Figure 59. The **System / Firmware upgrade** page.*

The current version of the device's firmware is displayed in the **Firmware version** field on the **Start** page. If you need to install a newer version of the firmware, follow the next steps:

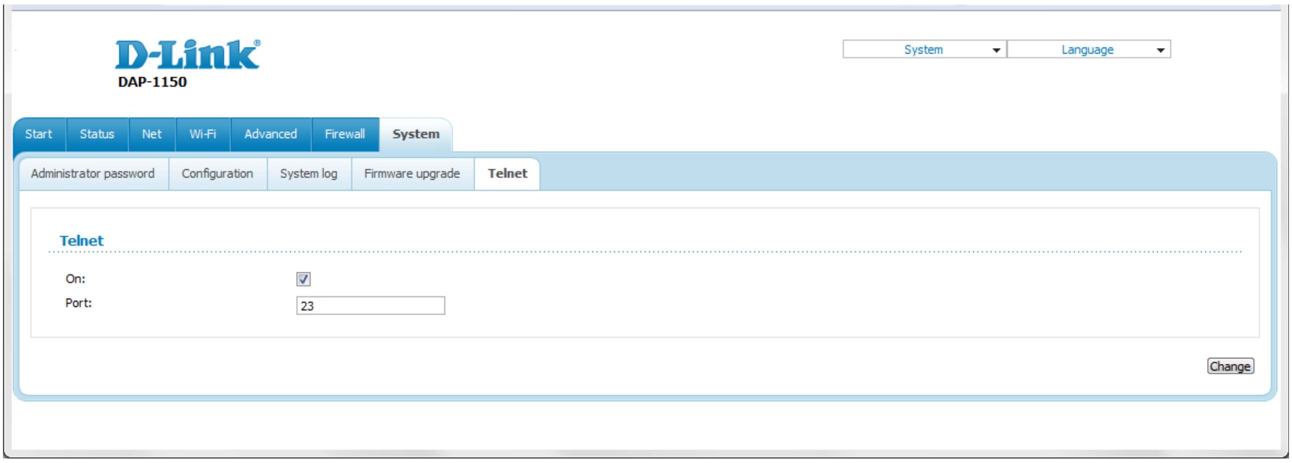
**!** Attention! Do not turn off the access point before the firmware upgrade is completed. This may cause the device breakdown.

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.
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`).

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

# 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.



Telnet

On: ☑

Port: 23

*Figure 60. The **System / Telnet** page.*

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

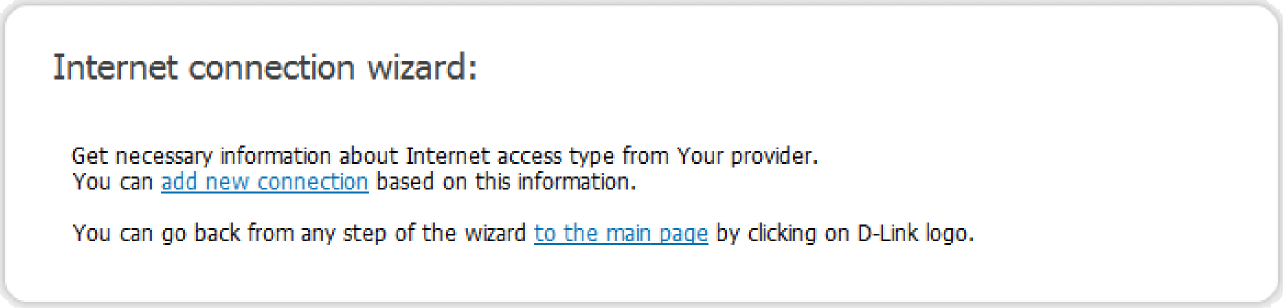
To enable access via TELNET again, select the **On** checkbox. In the **Port** field, enter the number of the access point's port through which access will be allowed (by default, the port `23` is specified). Then click the **Change** button.

# CHAPTER 5. CONFIGURING DEVICE (ROUTER MODE)

## *Setup Wizards*

### Internet Setup Wizard

To configure connection to the Internet, click the **Connect to internet** button.



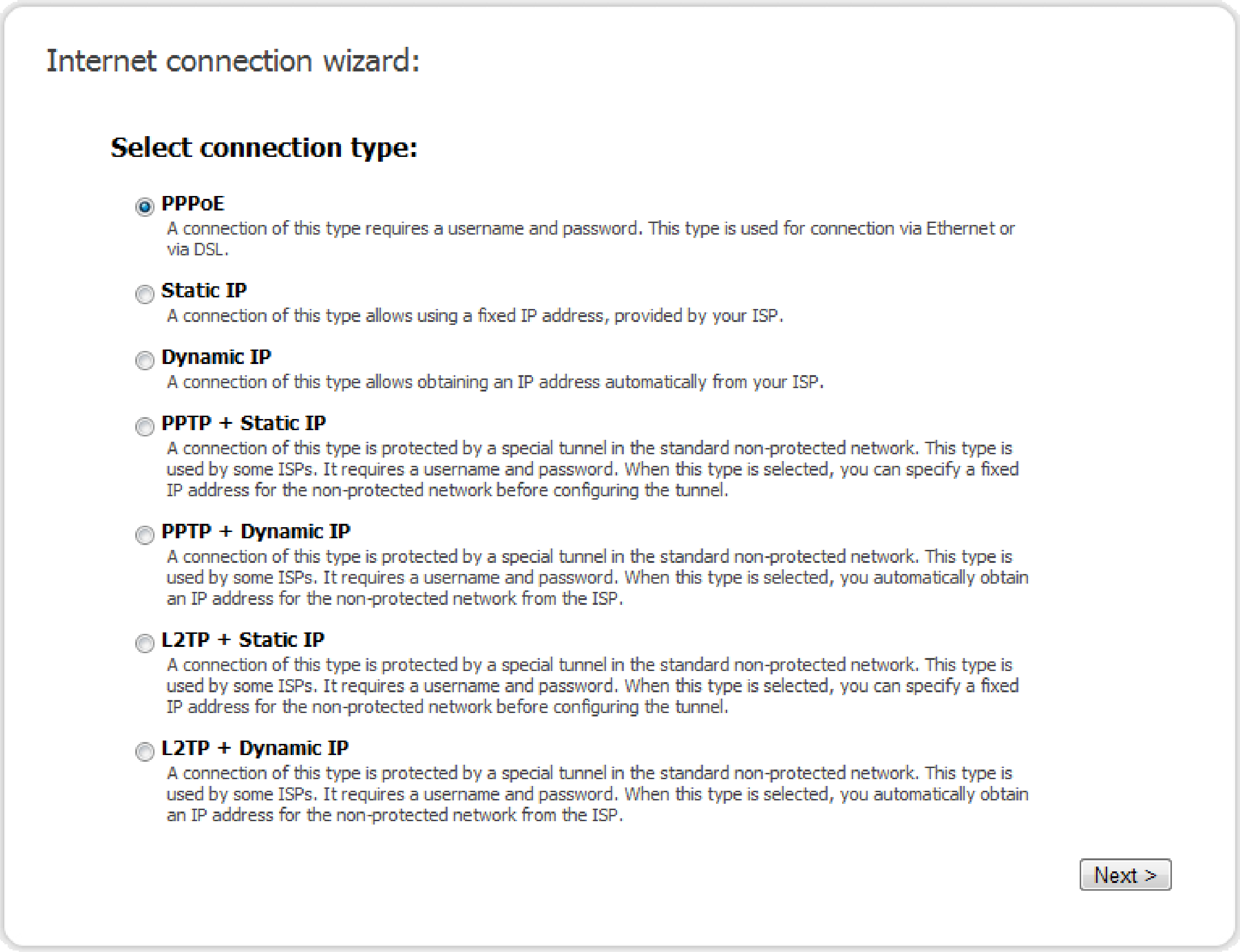
Internet connection wizard:

Get necessary information about Internet access type from Your provider.
You can add new connection based on this information.

You can go back from any step of the wizard to the main page by clicking on D-Link logo.

*Figure 61. Configuring connection to the Internet.*

To create a new WAN connection, click the **add new connection** link.



Internet connection wizard:

**Select connection type:**

● **PPPoE**
A connection of this type requires a username and password. This type is used for connection via Ethernet or via DSL.

○ **Static IP**
A connection of this type allows using a fixed IP address, provided by your ISP.

○ **Dynamic IP**
A connection of this type allows obtaining an IP address automatically from your ISP.

○ **PPTP + Static IP**
A connection of this type is protected by a special tunnel in the standard non-protected network. This type is used by some ISPs. It requires a username and password. When this type is selected, you can specify a fixed IP address for the non-protected network before configuring the tunnel.

○ **PPTP + Dynamic IP**
A connection of this type is protected by a special tunnel in the standard non-protected network. This type is used by some ISPs. It requires a username and password. When this type is selected, you automatically obtain an IP address for the non-protected network from the ISP.

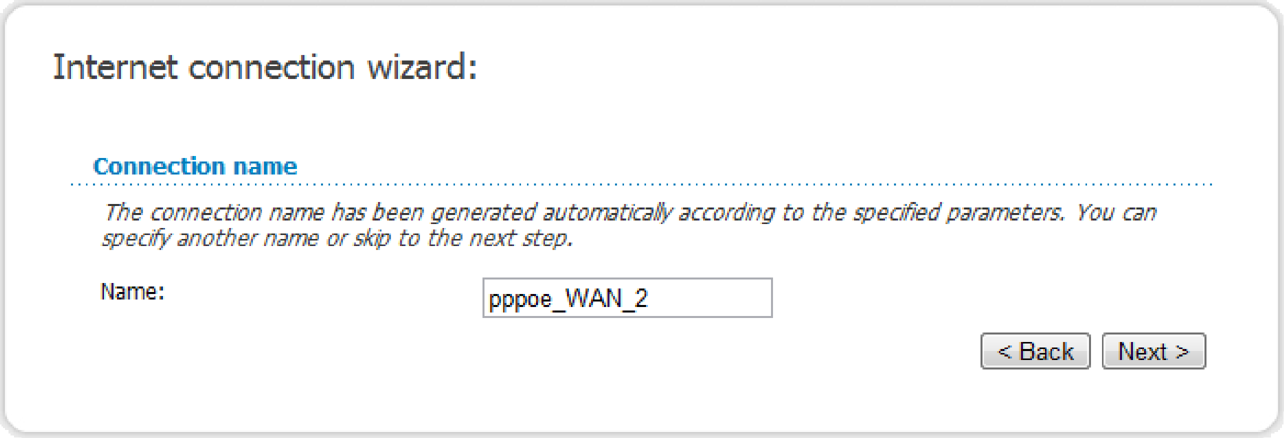
○ **L2TP + Static IP**
A connection of this type is protected by a special tunnel in the standard non-protected network. This type is used by some ISPs. It requires a username and password. When this type is selected, you can specify a fixed IP address for the non-protected network before configuring the tunnel.

○ **L2TP + Dynamic IP**
A connection of this type is protected by a special tunnel in the standard non-protected network. This type is used by some ISPs. It requires a username and password. When this type is selected, you automatically obtain an IP address for the non-protected network from the ISP.

*Figure 62. The page for selecting the connection type.*

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

### *PPPoE Connection*



Internet connection wizard:

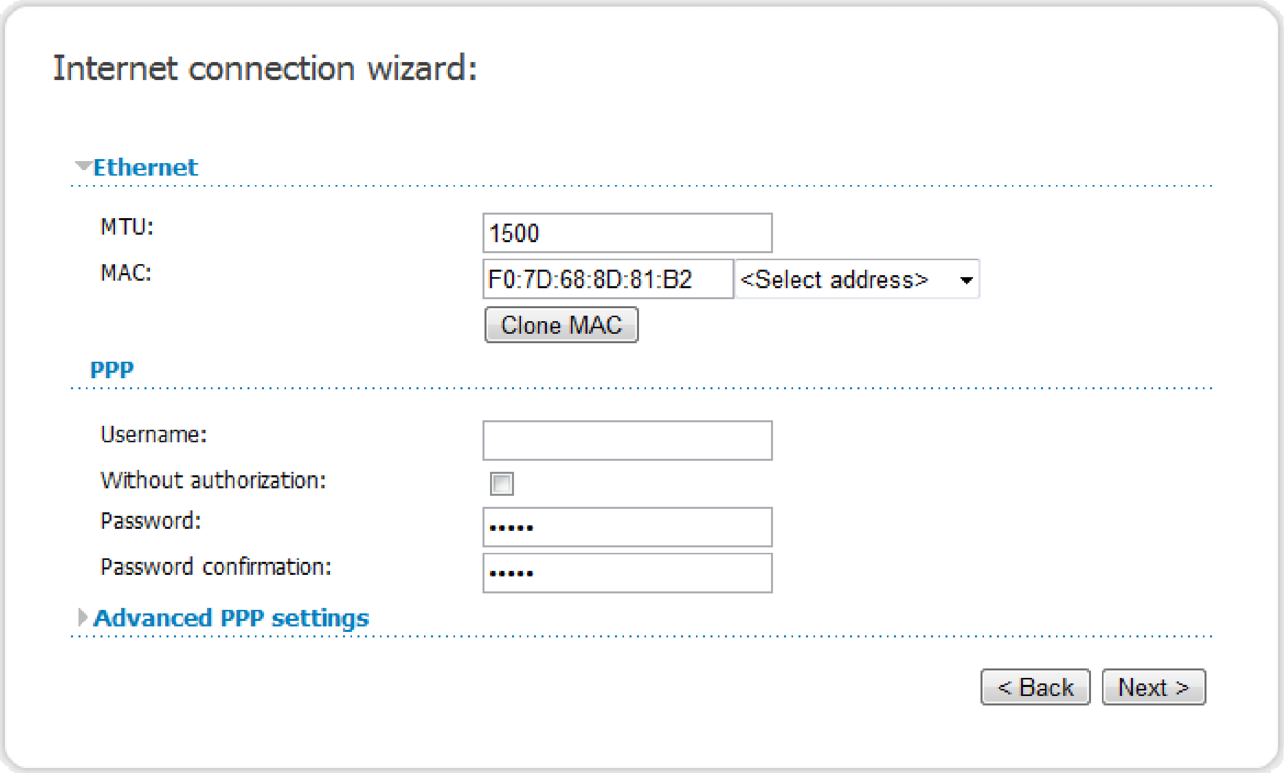
Connection name

*The connection name has been generated automatically according to the specified parameters. You can specify another name or skip to the next step.*

Name: pppoe_WAN_2

*Figure 63. Configuring PPPoE WAN connection.*

In the **Name** field, specify a name for the connection for easier identification and click the **Next** button.



Internet connection wizard:

Ethernet

MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

PPP

Username:

Without authorization: □

Password: •••••

Password confirmation: •••••

*Figure 64. Configuring PPPoE WAN connection.*

If needed, in the **MTU** field, change the maximum size of units transmitted by the interface.

If your ISP uses MAC address binding, in the **MAC** field, enter the MAC address registered by your ISP upon concluding the agreement.

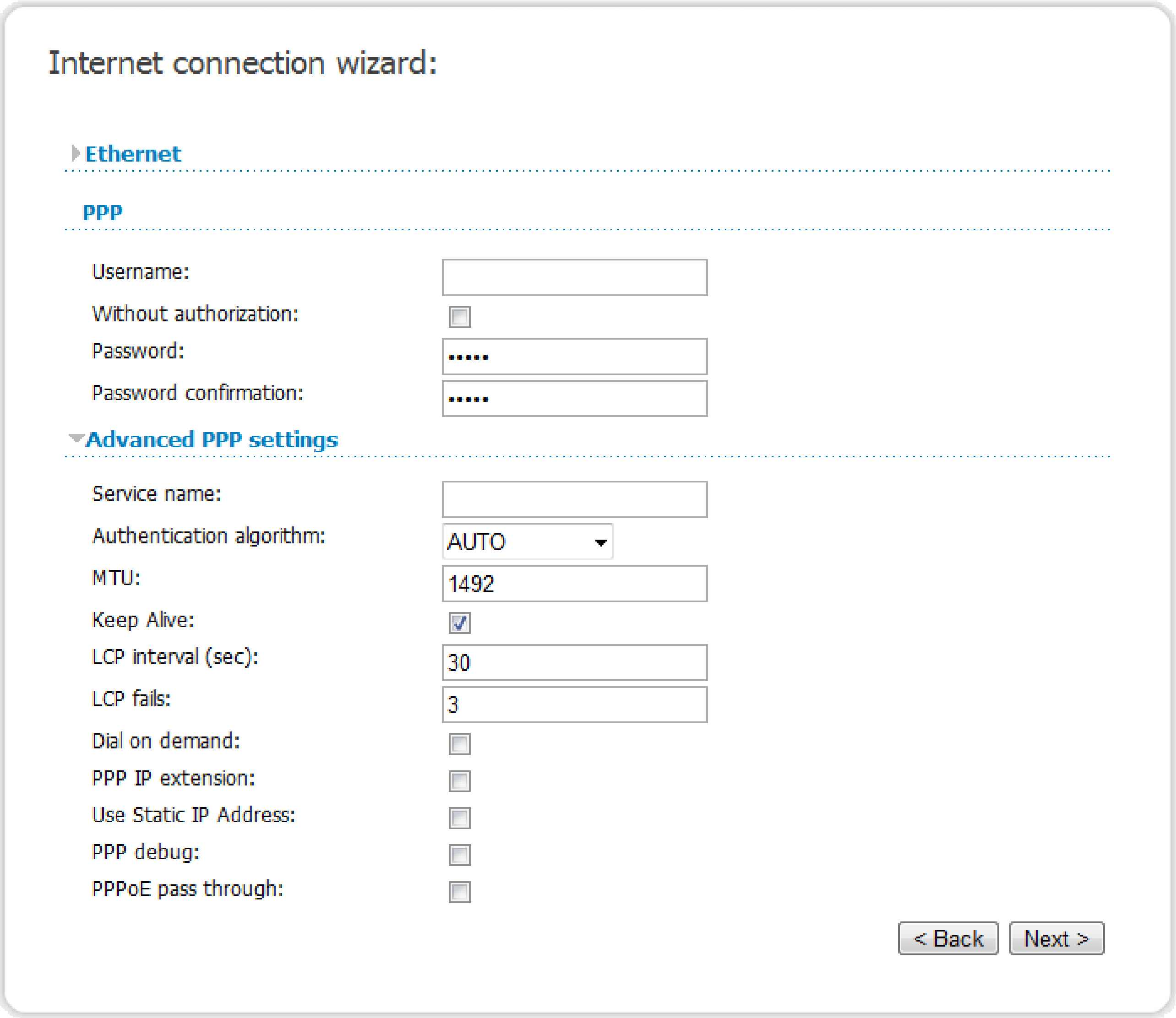
You can click the **Clone MAC** button to set the MAC address of the network interface card (of the computer that is being used to configure the access point at the moment).

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 located to the right of the field (the field will be filled in automatically).

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

If authorization is not required, select the **Without authorization** checkbox.

If needed, specify additional settings for your PPPoE WAN connection.



Internet connection wizard:

▸ Ethernet

PPP

| | |
|---|---|
| Username: | |
| Without authorization: | □ |
| Password: | ••••• |
| Password confirmation: | ••••• |

▾ Advanced PPP settings

| | |
|---|---|
| Service name: | |
| Authentication algorithm: | AUTO |
| MTU: | 1492 |
| Keep Alive: | ☑ |
| LCP interval (sec): | 30 |
| LCP fails: | 3 |
| Dial on demand: | □ |
| PPP IP extension: | □ |
| Use Static IP Address: | □ |
| PPP debug: | □ |
| PPPoE pass through: | □ |

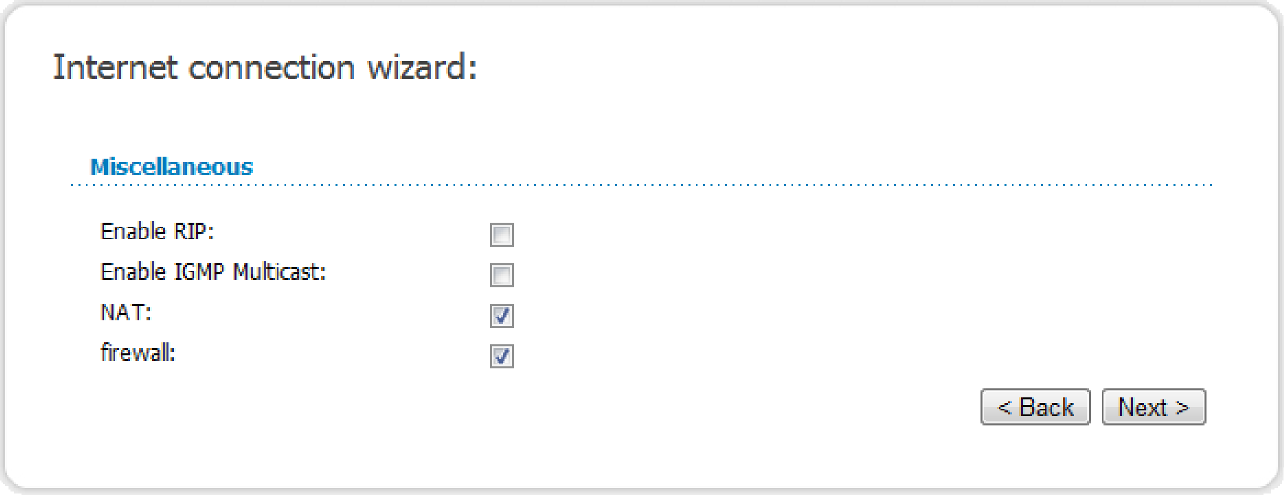
*Figure 65. Configuring PPPoE WAN connection.*

| Parameter | Description |
|---|---|
| **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. |

| Parameter | Description |
|---|---|
| **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. |
| **Use Static IP Address** | Select the checkbox if you want to use a static IP address to access the Internet. In the **IP Address** field displayed when the checkbox is selected, specify a static IP address. |
| **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. |

Click the **Next** button to continue.

If needed, change the connection settings available in the **Miscellaneous** section.



Internet connection wizard:

Miscellaneous

Enable RIP: □
Enable IGMP Multicast: □
NAT: ☑
firewall: ☑

*Figure 66. Configuring PPPoE WAN connection.*

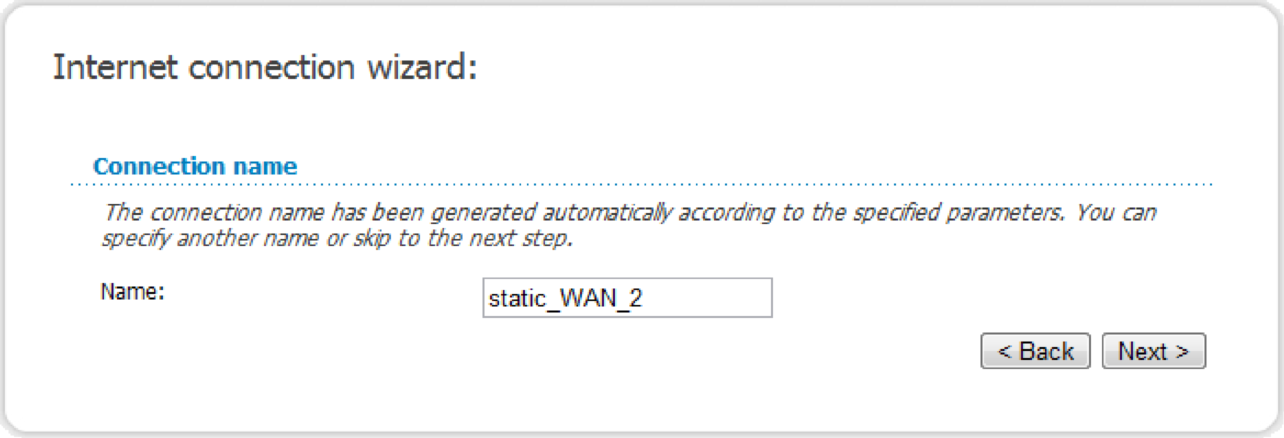
| Parameter | Description |
|---|---|
| **Enable RIP** | Select the checkbox to allow using RIP for this connection. |
| **Enable IGMP Multicast** | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |
| **NAT** | Select the checkbox if you 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. |

Click the **Next** button to continue.

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

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

### *Static IP Connection*



Internet connection wizard:

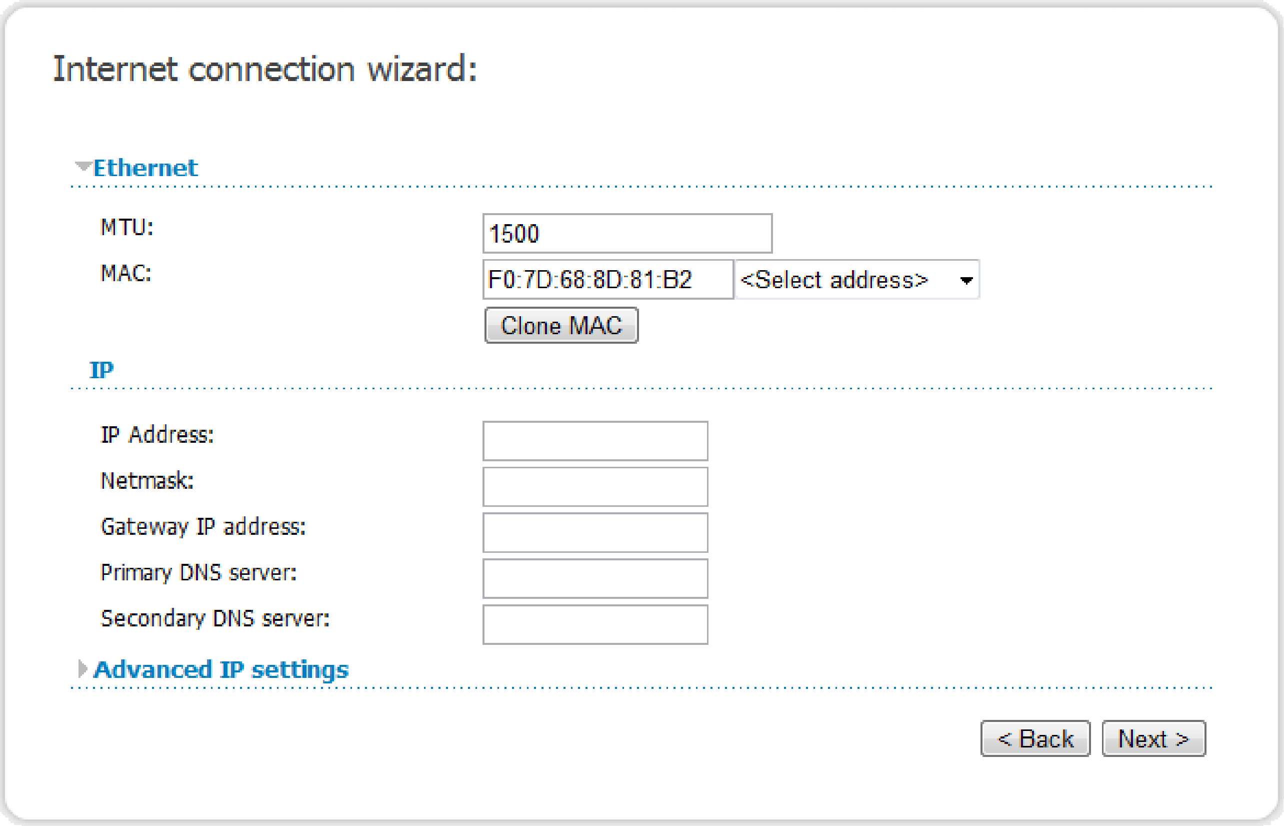
Connection name

*The connection name has been generated automatically according to the specified parameters. You can specify another name or skip to the next step.*

Name: static_WAN_2

*Figure 67. Configuring Static IP WAN connection.*

In the **Name** field, specify a name for the connection for easier identification and click the **Next** button.



Internet connection wizard:

Ethernet

MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

IP

IP Address:

Netmask:

Gateway IP address:

Primary DNS server:

Secondary DNS server:

*Figure 68. Configuring Static IP WAN connection.*

If needed, in the **MTU** field, change the maximum size of units transmitted by the interface.

If your ISP uses MAC address binding, in the **MAC** field, enter the MAC address registered by your ISP upon concluding the agreement.

You can click the **Clone MAC** 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).

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 located to the right of the field (the field will be filled in automatically).

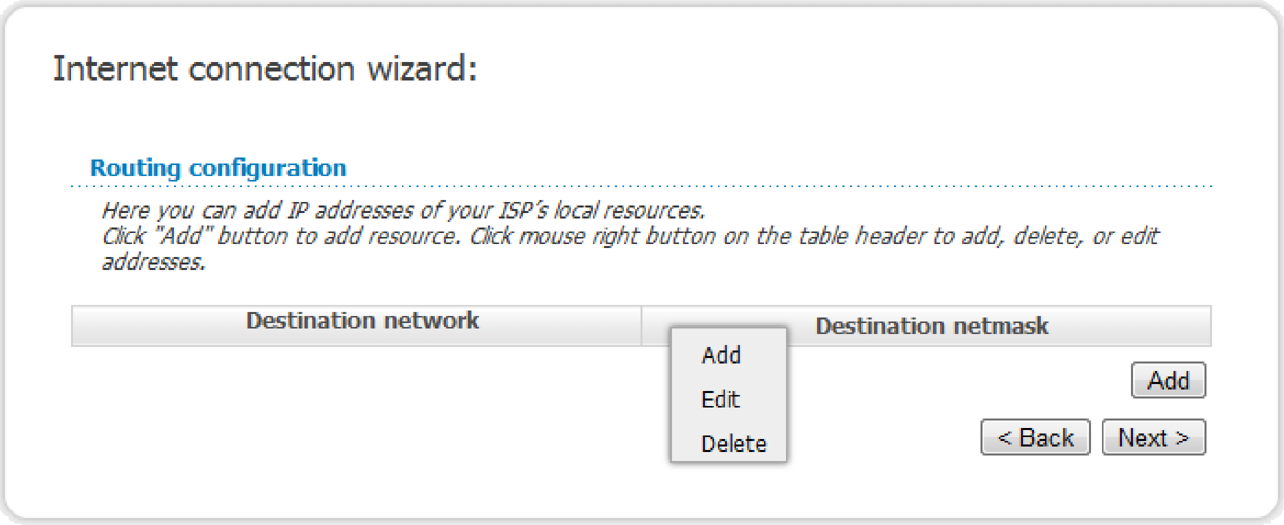
Fill in the **IP address** and **Netmask** fields.

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

In the **Primary DNS server** and **Secondary DNS server** fields, enter the addresses of the primary and secondary DNS servers.

Click the **Next** button to continue.

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



Internet connection wizard:

Routing configuration

*Here you can add IP addresses of your ISP's local resources.*
*Click "Add" button to add resource. Click mouse right button on the table header to add, delete, or edit addresses.*

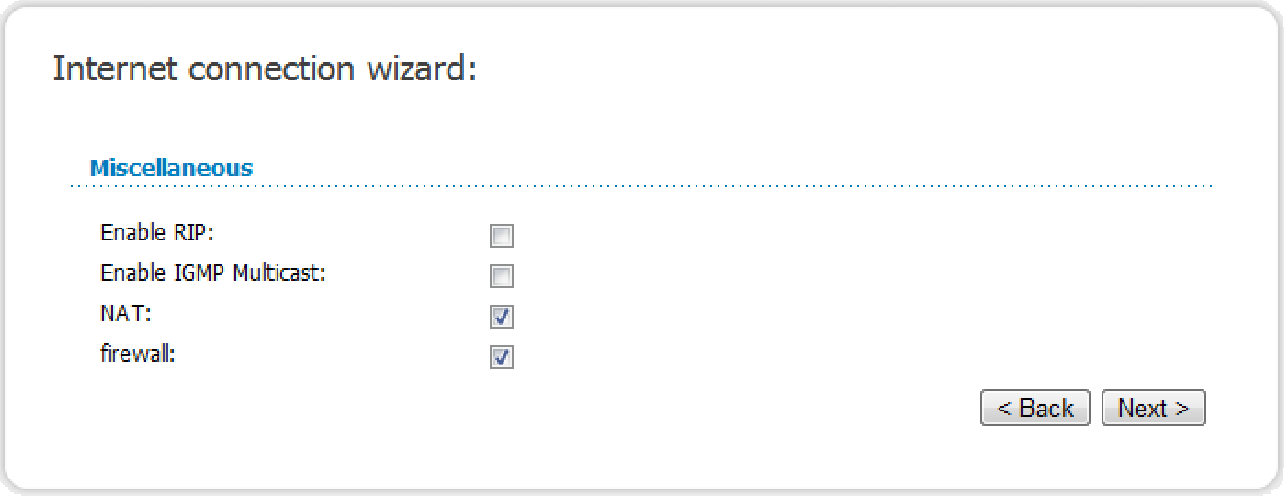
| Destination network | Destination netmask |
|---|---|

*Figure 69. Configuring Static IP WAN connection.*

To add a route, click the **Add** button or right-click the routing table heading and select the **Add** line from the shortcut menu displayed.

Click the **Next** button to continue.

If needed, change the connection settings available in the **Miscellaneous** section.



Internet connection wizard:

Miscellaneous

Enable RIP: □

Enable IGMP Multicast: □

NAT: ☑

firewall: ☑

*Figure 70. Configuring Static IP WAN connection.*

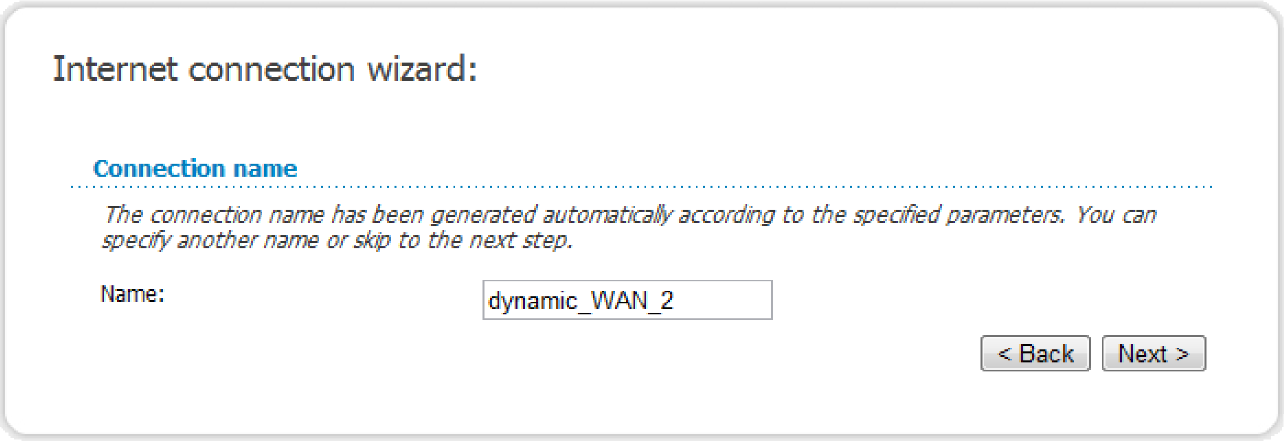
| Parameter | Description |
|---|---|
| **Enable RIP** | Select the checkbox to allow using RIP for this connection. |
| **Enable IGMP Multicast** | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |
| **NAT** | Select the checkbox if you 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. |

Click the **Next** button to continue.

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

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

## *Dynamic IP Connection*



Internet connection wizard:

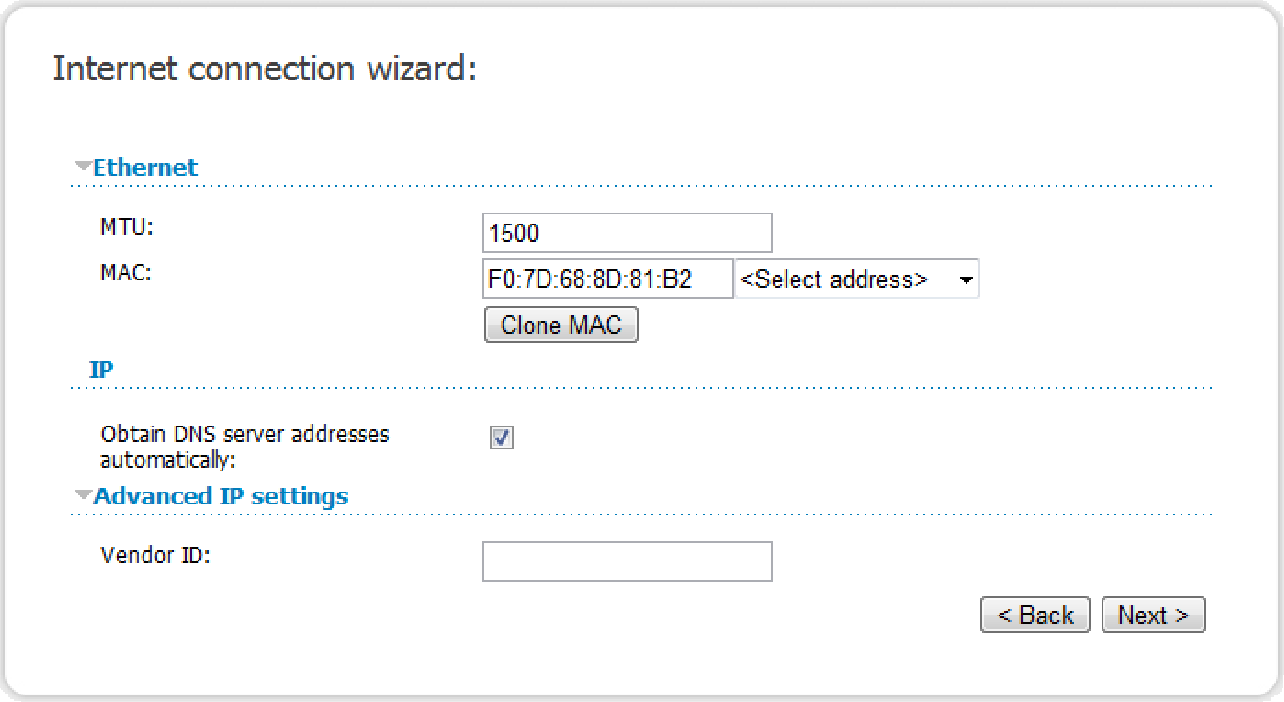
**Connection name**

*The connection name has been generated automatically according to the specified parameters. You can specify another name or skip to the next step.*

Name: dynamic_WAN_2

*Figure 71. Configuring Dynamic IP WAN connection.*

In the **Name** field, specify a name for the connection for easier identification and click the **Next** button.



Internet connection wizard:

**Ethernet**

MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

**IP**

Obtain DNS server addresses automatically: ☑

**Advanced IP settings**

Vendor ID:

*Figure 72. Configuring Dynamic IP WAN connection.*

If needed, in the **MTU** field, change the maximum size of units transmitted by the interface.

If your ISP uses MAC address binding, in the **MAC** field, enter the MAC address registered by your ISP upon concluding the agreement.

You can click the **Clone MAC** 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).

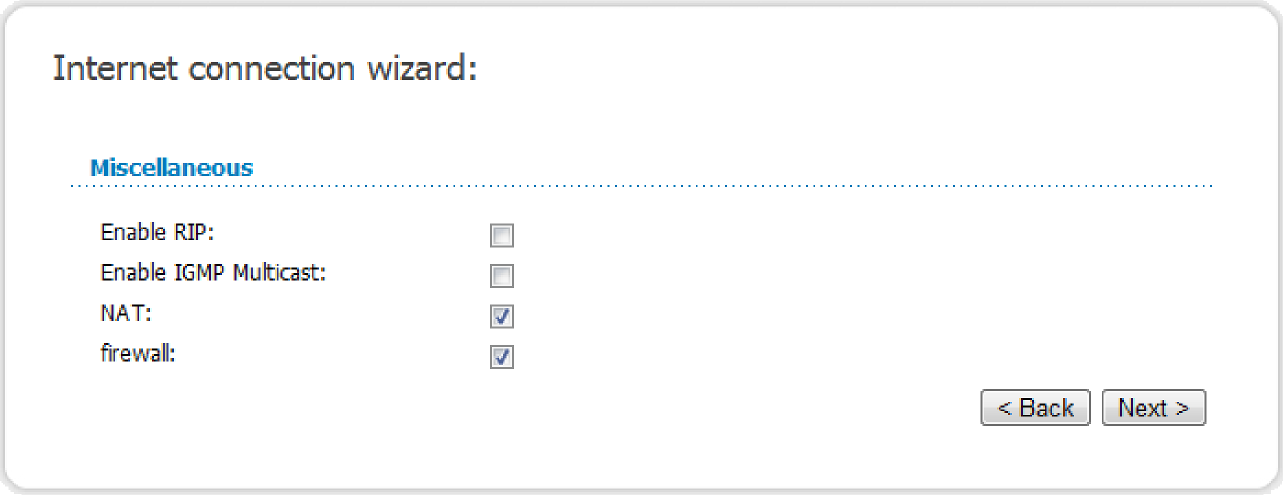
Also you can set the address of a device connected to the access point's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).

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** and **Secondary DNS server** fields.

If your ISP has provided its identifier, fill in the **Vendor ID** field.

Click the **Next** button to continue.

If needed, change the connection settings available in the **Miscellaneous** section.



Internet connection wizard:

Miscellaneous

Enable RIP: □

Enable IGMP Multicast: □

NAT: ☑

firewall: ☑

*Figure 73. Configuring Dynamic IP WAN connection.*

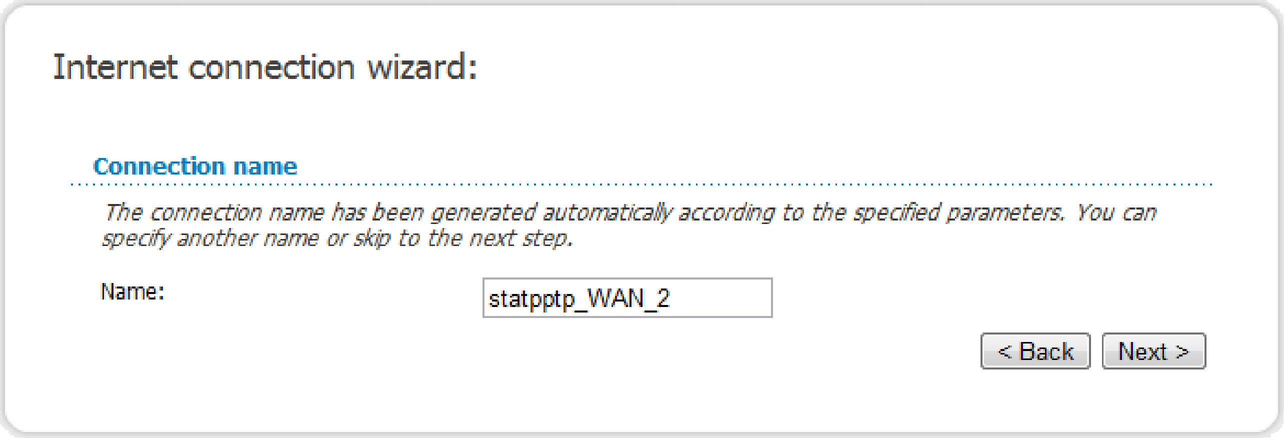
| Parameter | Description |
|---|---|
| **Enable RIP** | Select the checkbox to allow using RIP for this connection. |
| **Enable IGMP Multicast** | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |
| **NAT** | Select the checkbox if you 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. |

Click the **Next** button to continue.

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

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

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



Internet connection wizard:

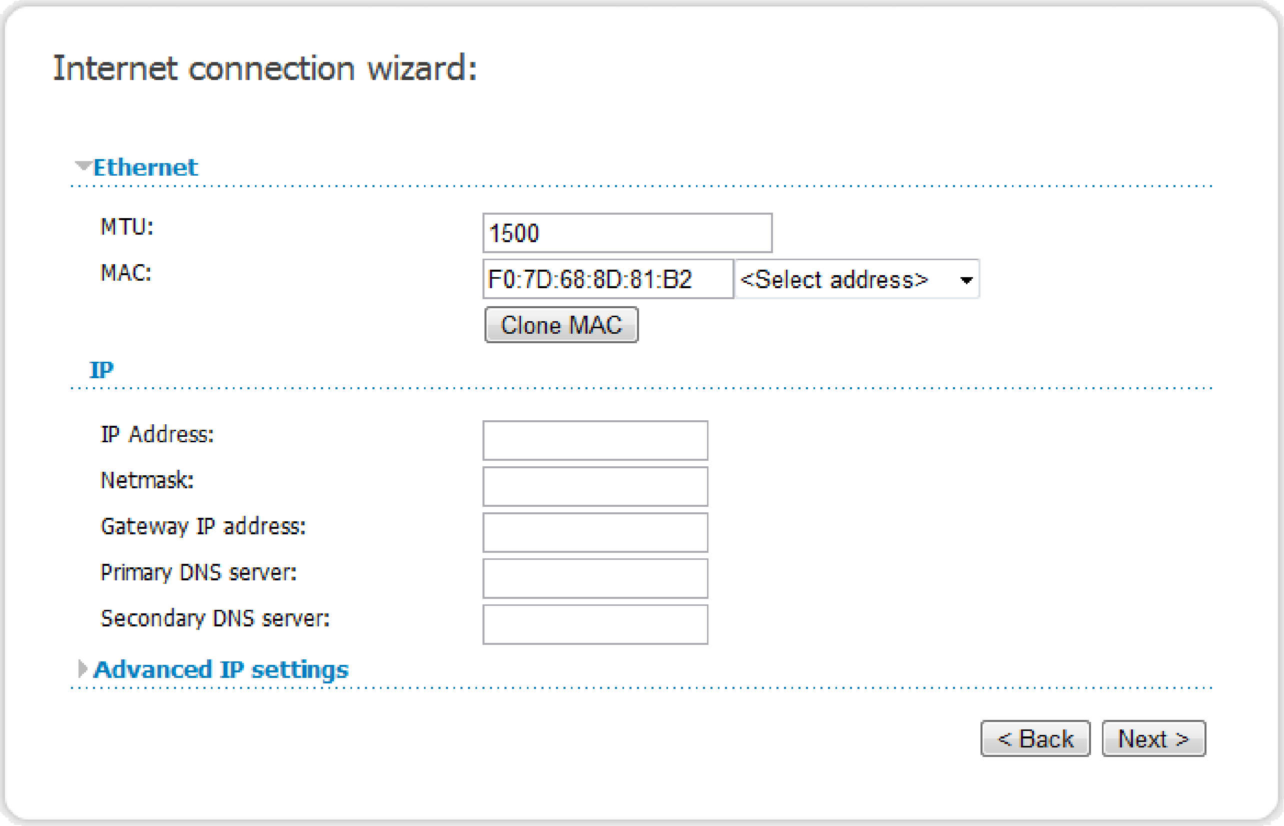
Connection name

*The connection name has been generated automatically according to the specified parameters. You can specify another name or skip to the next step.*

Name: statpptp_WAN_2

*Figure 74. Configuring PPTP + Static IP WAN connection.*

In the **Name** field, specify a name for the connection for easier identification and click the **Next** button.



Internet connection wizard:

Ethernet

MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

IP

IP Address:

Netmask:

Gateway IP address:

Primary DNS server:

Secondary DNS server:

Advanced IP settings

*Figure 75. Configuring PPTP + Static IP WAN connection.*

If needed, in the **MTU** field, change the maximum size of units transmitted by the interface.

If your ISP uses MAC address binding, in the **MAC** field, enter the MAC address registered by your ISP upon concluding the agreement.

You can click the **Clone MAC** 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).

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 located to the right of the field (the field will be filled in automatically).

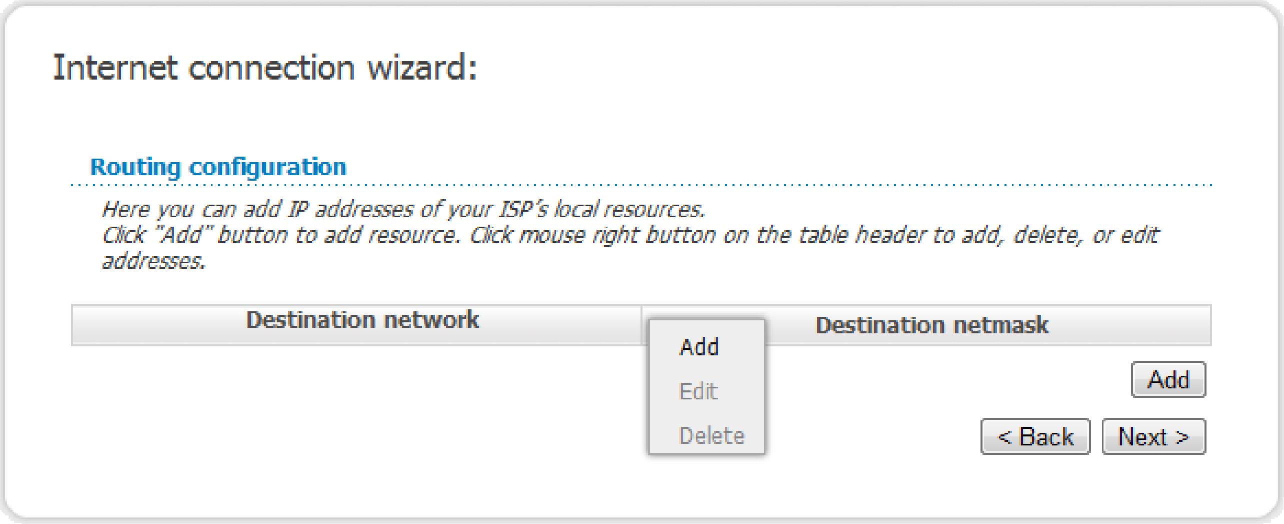
Fill in the **IP address** and **Netmask** fields.

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

In the **Primary DNS server** and **Secondary DNS server** fields, enter the addresses of the primary and secondary DNS servers.

Click the **Next** button to continue.

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


Internet connection wizard:

Routing configuration

*Here you can add IP addresses of your ISP's local resources.*
*Click "Add" button to add resource. Click mouse right button on the table header to add, delete, or edit addresses.*

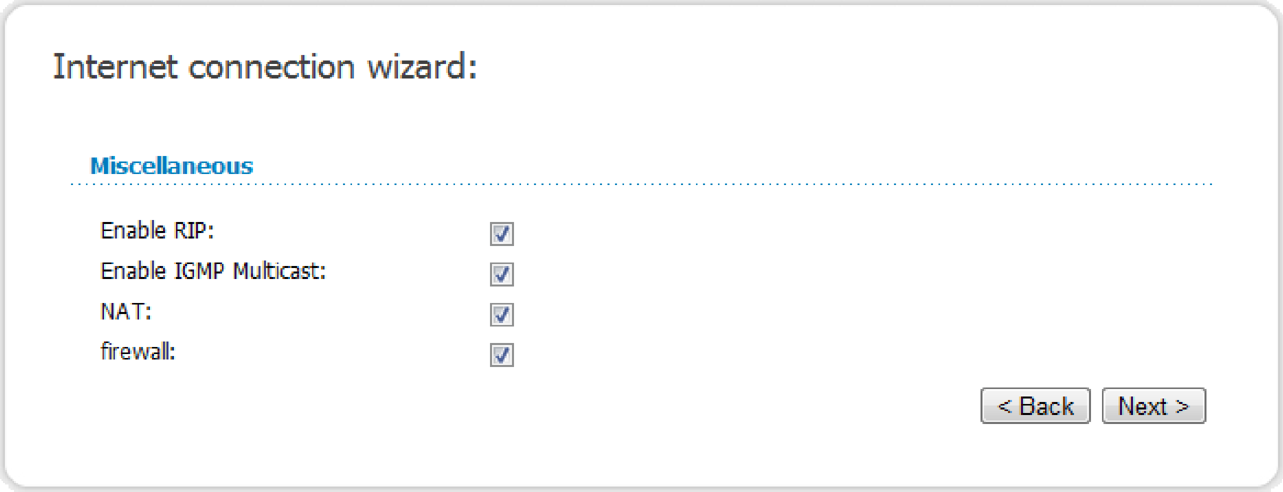
| Destination network | Destination netmask |
|---|---|

*Figure 76. Configuring PPTP + Static IP WAN connection.*

To add a route, click the **Add** button or right-click the routing table heading and select the **Add** line from the shortcut menu displayed.

Click the **Next** button to continue.

If needed, change the connection settings available in the **Miscellaneous** section.



Internet connection wizard:

Miscellaneous

Enable RIP: ☑

Enable IGMP Multicast: ☑

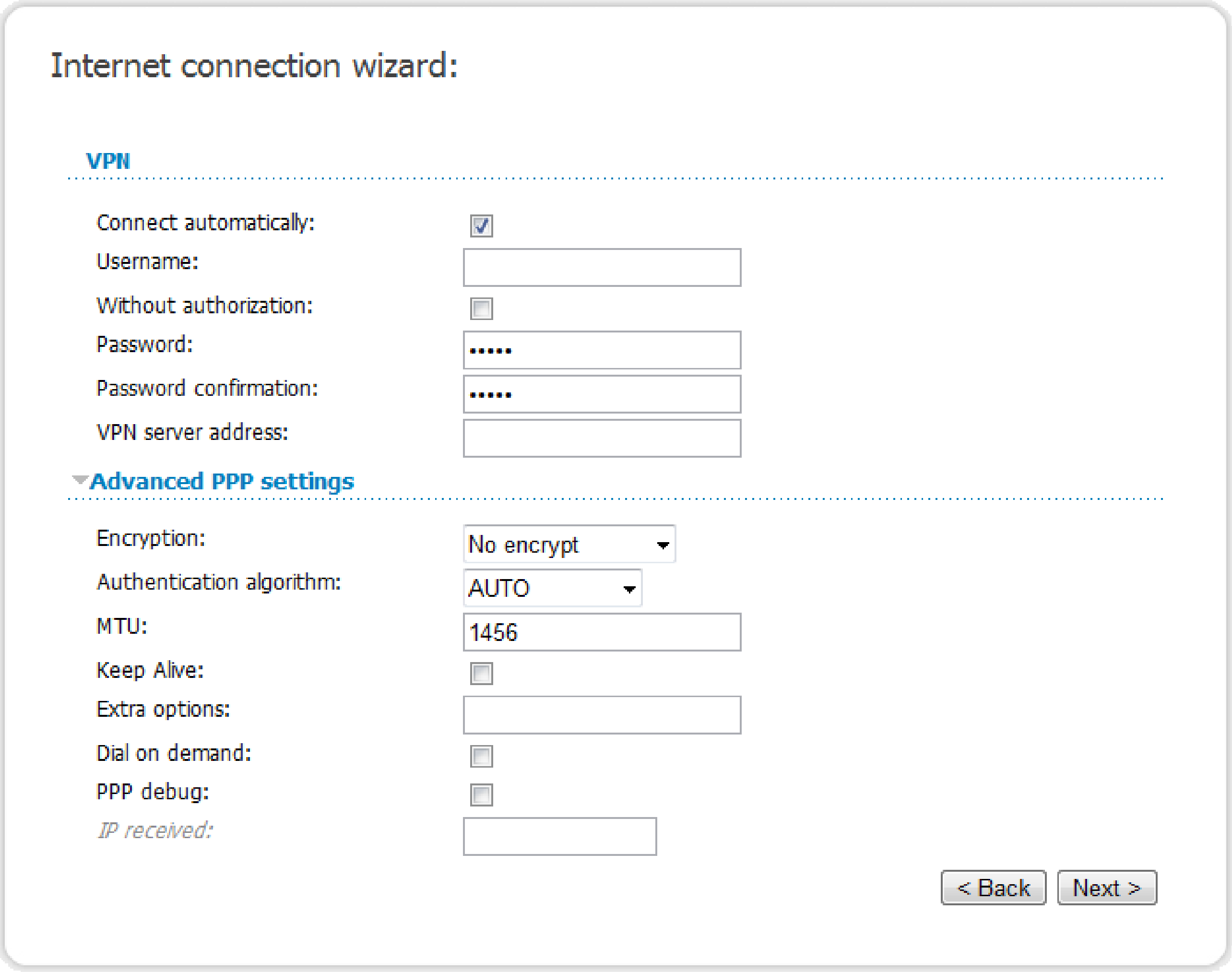
NAT: ☑

firewall: ☑

*Figure 77. Configuring PPTP + Static IP WAN connection.*

| Parameter | Description |
|---|---|
| **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. |

Click the **Next** button to continue.



Internet connection wizard:

VPN

|  |  |
|---|---|
| Connect automatically: | ☑ |
| Username: |  |
| Without authorization: | □ |
| Password: | ••••• |
| Password confirmation: | ••••• |
| VPN server address: |  |

Advanced PPP settings

|  |  |
|---|---|
| Encryption: | No encrypt |
| Authentication algorithm: | AUTO |
| MTU: | 1456 |
| Keep Alive: | □ |
| Extra options: |  |
| Dial on demand: | □ |
| PPP debug: | □ |
| IP received: |  |

*Figure 78. Configuring PPTP + Static IP WAN connection.*

Leave the **Connect automatically** checkbox selected to allow automatic start of the connection upon the load of the access point.

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

If authorization is not required, select the **Without authorization** checkbox.

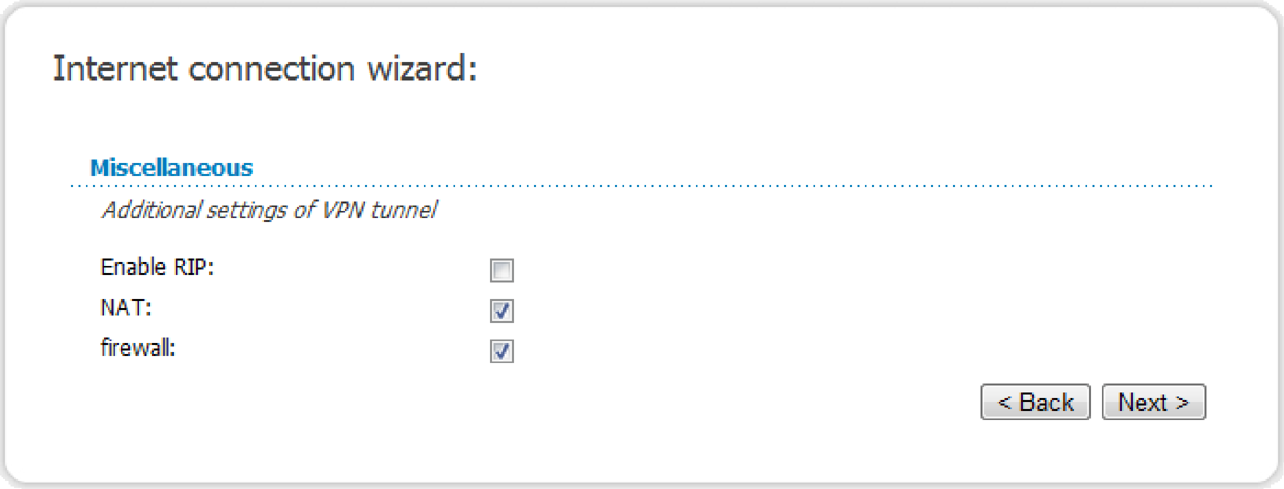
In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

If needed, specify additional settings for your PPTP + Static IP or L2TP + Static IP WAN connection.

| Parameter | Description |
|---|---|
| **Encryption** | Select a method of MPPE encryption.<br>• **No encrypt**: MPPE encryption is not applied.<br>• **MPPE 40/128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied.<br>• **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied.<br>• **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied.<br>MPPE encryption can be applied only if the **MSCHAP**, **MACHAPv2**, or **AUTO** value is selected from the **Authentication algorithm** drop-down list. |
| **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. *Optional*. |
| **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 debug** | Select the checkbox if you want to log all data on PPP connection debugging. |
| **IP received** | The IP address assigned by the ISP. |

Click the **Next** button to continue.

If needed, change the settings of the VPN tunnel available in the **Miscellaneous** section.



Internet connection wizard:

Miscellaneous

*Additional settings of VPN tunnel*

Enable RIP: □

NAT: ☑

firewall: ☑

*Figure 79. Configuring PPTP + Static IP WAN connection.*

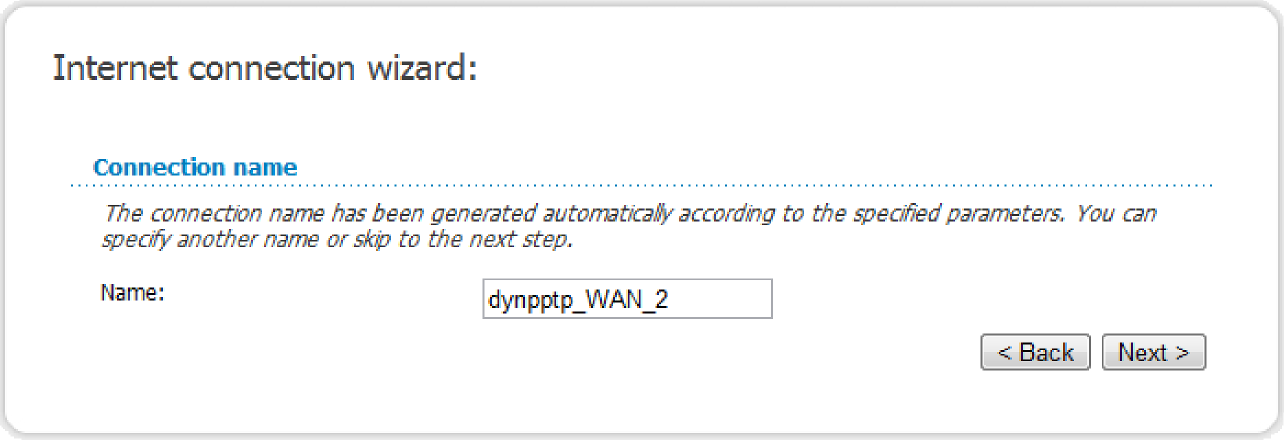
| Parameter | Description |
|---|---|
| **Enable RIP** | Select the checkbox to allow using RIP for this connection. |
| **NAT** | Select the checkbox if you want one WAN IP address to be used for all computers of your LAN. |
| **Firewall** | Select the checkbox to enable protection against ARP and DDoS attacks. |

Click the **Next** button to continue.

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

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

### *PPTP + Dynamic IP or L2TP + Dynamic IP Connection*



Internet connection wizard:

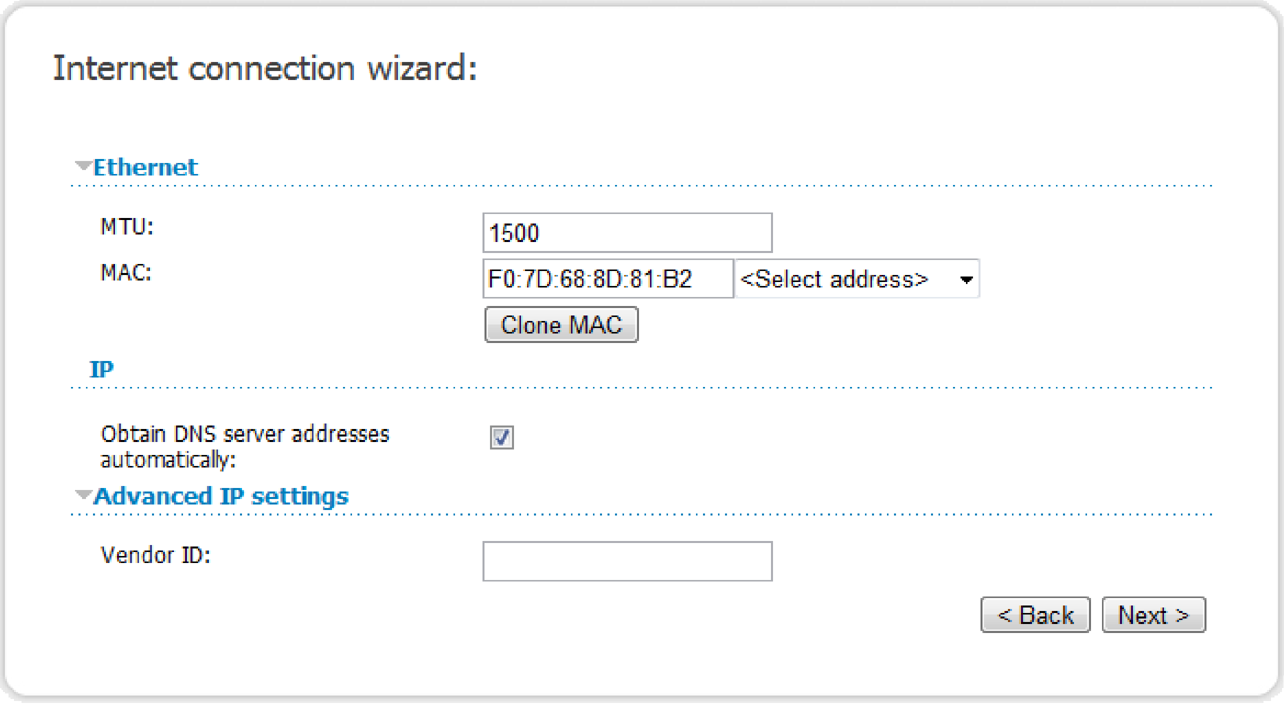
Connection name

*The connection name has been generated automatically according to the specified parameters. You can specify another name or skip to the next step.*

Name: dynpptp_WAN_2

*Figure 80. Configuring PPTP + Dynamic IP WAN connection.*

In the **Name** field, specify a name for the connection for easier identification and click the **Next** button.



Internet connection wizard:

Ethernet

MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

IP

Obtain DNS server addresses automatically: ☑

Advanced IP settings

Vendor ID:

*Figure 81. Configuring PPTP + Dynamic IP WAN connection.*

If needed, in the **MTU** field, change the maximum size of units transmitted by the interface.

If your ISP uses MAC address binding, in the **MAC** field, enter the MAC address registered by your ISP upon concluding the agreement.

You can click the **Clone MAC** 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).

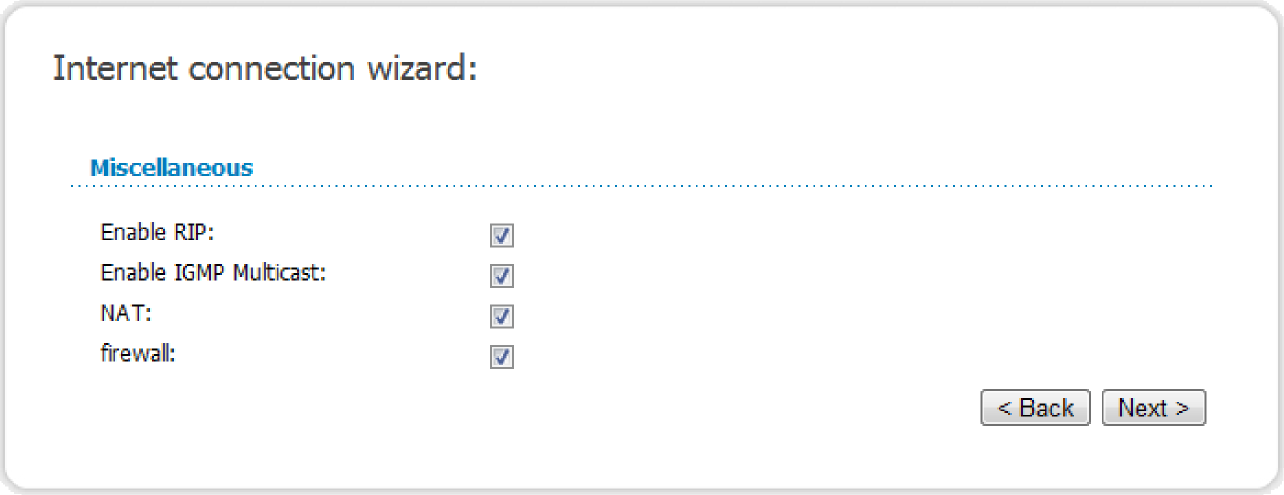
Also you can set the address of a device connected to the access point's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).

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** and **Secondary DNS server** fields.

If your ISP has provided its identifier, fill in the **Vendor ID** field.

Click the **Next** button to continue.

If needed, change the connection settings available in the **Miscellaneous** section.



Internet connection wizard:

Miscellaneous

Enable RIP: ☑

Enable IGMP Multicast: ☑

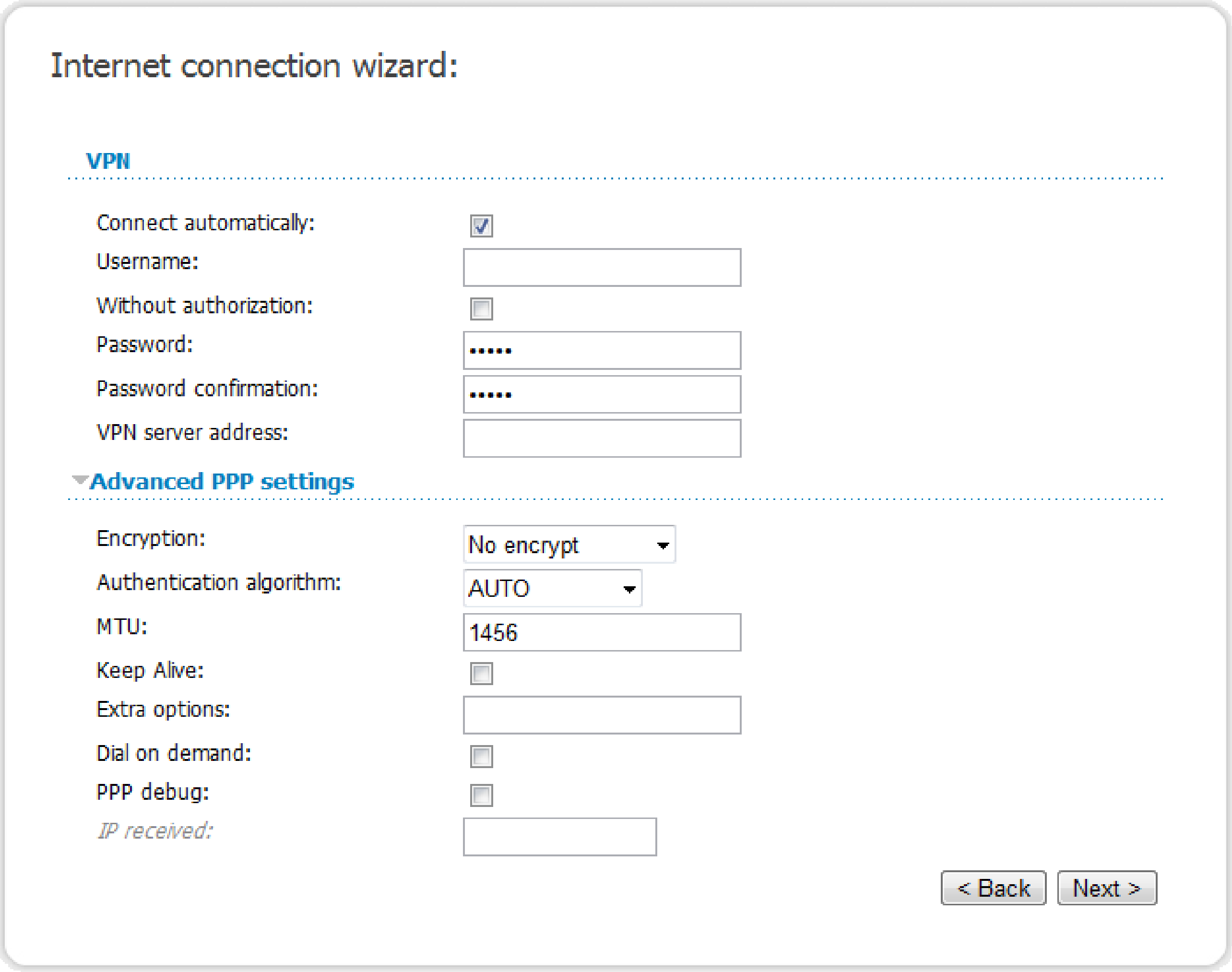
NAT: ☑

firewall: ☑

*Figure 82. Configuring PPTP + Dynamic IP WAN connection.*

| Parameter | Description |
|---|---|
| **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. |

Click the **Next** button to continue.



Internet connection wizard:

VPN

|  |  |
|---|---|
| Connect automatically: | ☑ |
| Username: |  |
| Without authorization: | □ |
| Password: | ••••• |
| Password confirmation: | ••••• |
| VPN server address: |  |

Advanced PPP settings

|  |  |
|---|---|
| Encryption: | No encrypt |
| Authentication algorithm: | AUTO |
| MTU: | 1456 |
| Keep Alive: | □ |
| Extra options: |  |
| Dial on demand: | □ |
| PPP debug: | □ |
| *IP received:* |  |

*Figure 83. Configuring PPTP + Dynamic IP WAN connection.*

Leave the **Connect automatically** checkbox selected to allow automatic start of the connection upon the load of the access point.

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

If authorization is not required, select the **Without authorization** checkbox.

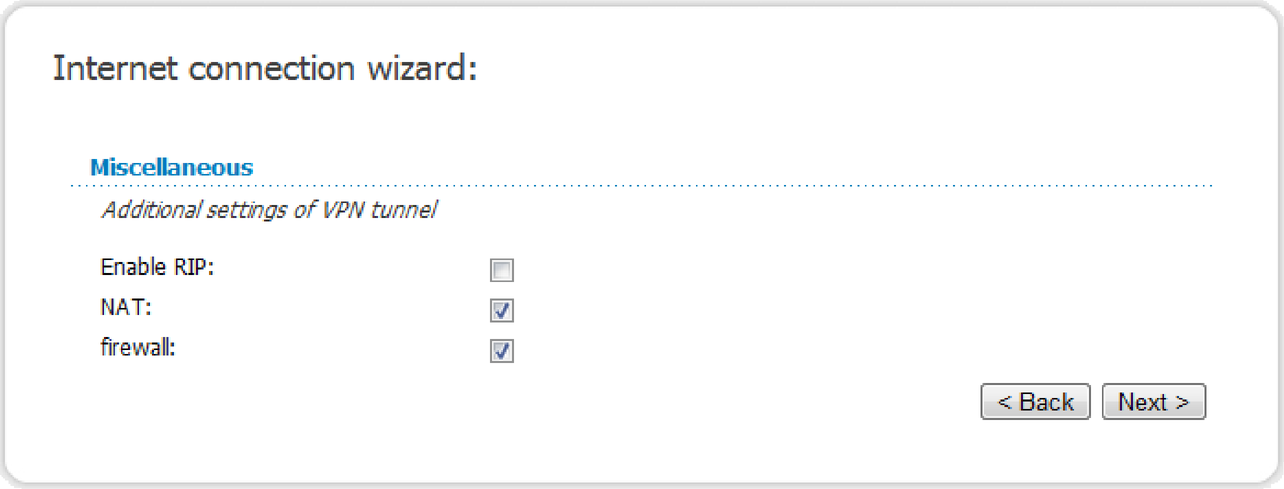
In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

If needed, specify additional settings for your PPTP + Dynamic IP or L2TP + Dynamic IP WAN connection.

| Parameter | Description |
|---|---|
| **Encryption** | Select a method of MPPE encryption.<br>• **No encrypt**: MPPE encryption is not applied.<br>• **MPPE 40/128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied.<br>• **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied.<br>• **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied.<br>MPPE encryption can be applied only if the **MSCHAP**, **MACHAPv2**, or **AUTO** value is selected from the **Authentication algorithm** drop-down list. |
| **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. *Optional*. |
| **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 debug** | Select the checkbox if you want to log all data on PPP connection debugging. |
| **IP received** | The IP address assigned by the ISP. |

Click the **Next** button to continue.

If needed, change the settings of the VPN tunnel available in the **Miscellaneous** section.



Internet connection wizard:

Miscellaneous

*Additional settings of VPN tunnel*

Enable RIP: ☐
NAT: ☑
firewall: ☑

*Figure 84. Configuring PPTP + Dynamic IP WAN connection.*

| Parameter | Description |
|---|---|
| **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. |

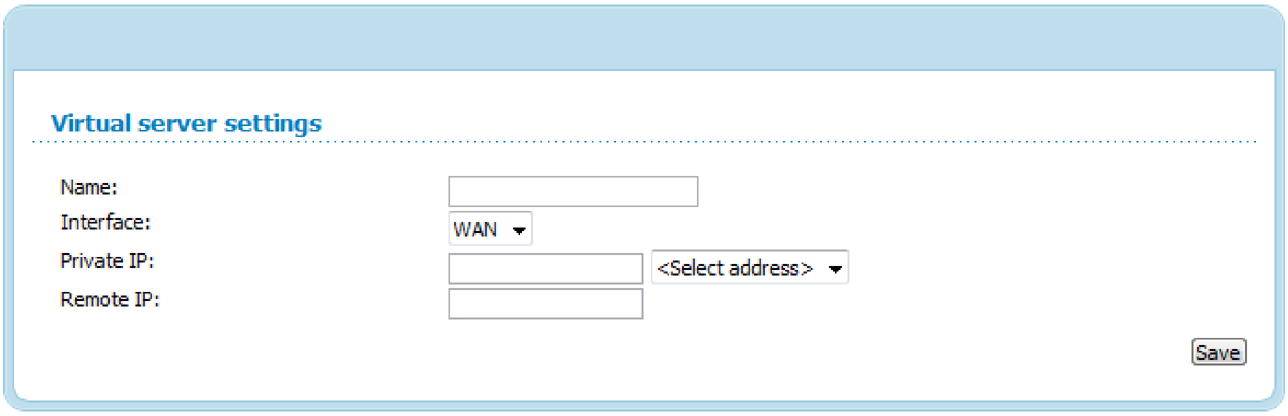
Click the **Next** button to continue.

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

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

## Site Setup Wizard

To create a virtual server for redirecting incoming Internet traffic to a specified IP address in the LAN, click the **Host site** button.



Virtual server settings

| | |
|---|---|
| Name: | |
| Interface: | WAN |
| Private IP: | <Select address> |
| Remote IP: | |

*Figure 85. The page for adding a virtual server.*

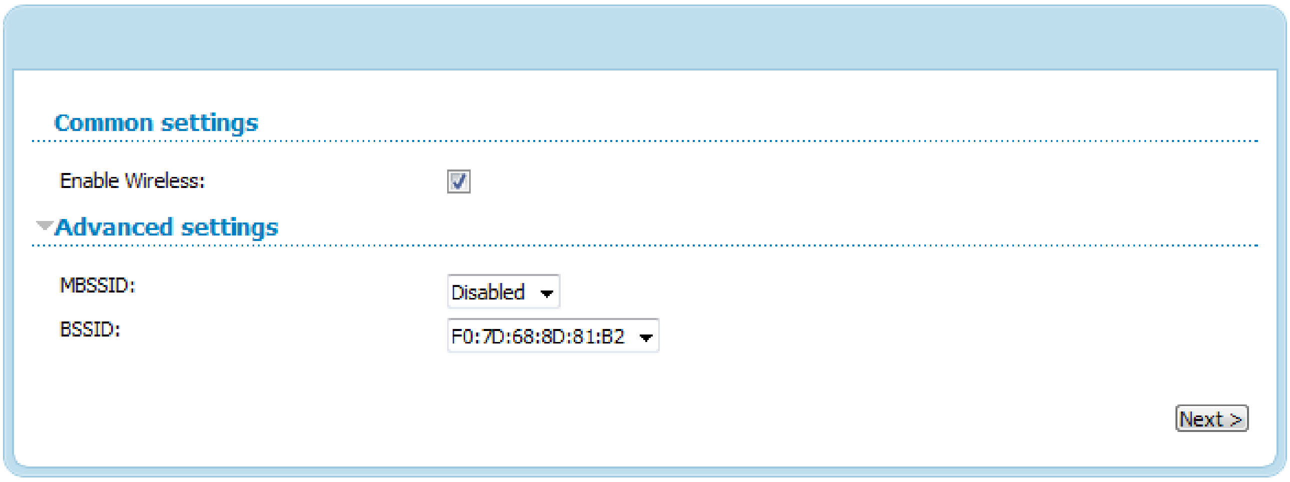
On the opened page, you can specify the following parameters:

| Parameter | Description |
|---|---|
| **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 located to the right of the **Private IP** field (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.

## Wi-Fi Setup Wizard

To specify all needed settings for your wireless network, click the **Configure Wi-Fi** button.



Common settings

Enable Wireless: ☑

Advanced settings

MBSSID: Disabled

BSSID: F0:7D:68:8D:81:B2

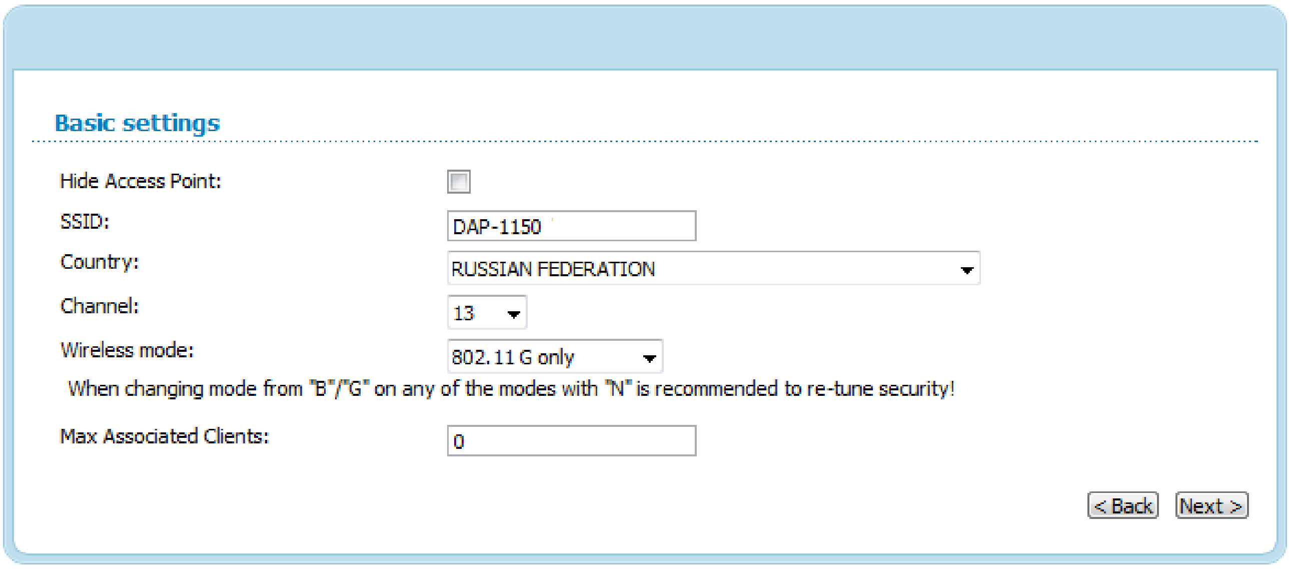
*Figure 86. Common and advanced settings of the wireless LAN.*

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**).



Basic settings

Hide Access Point: □

SSID: DAP-1150

Country: RUSSIAN FEDERATION

Channel: 13

Wireless mode: 802.11 G only

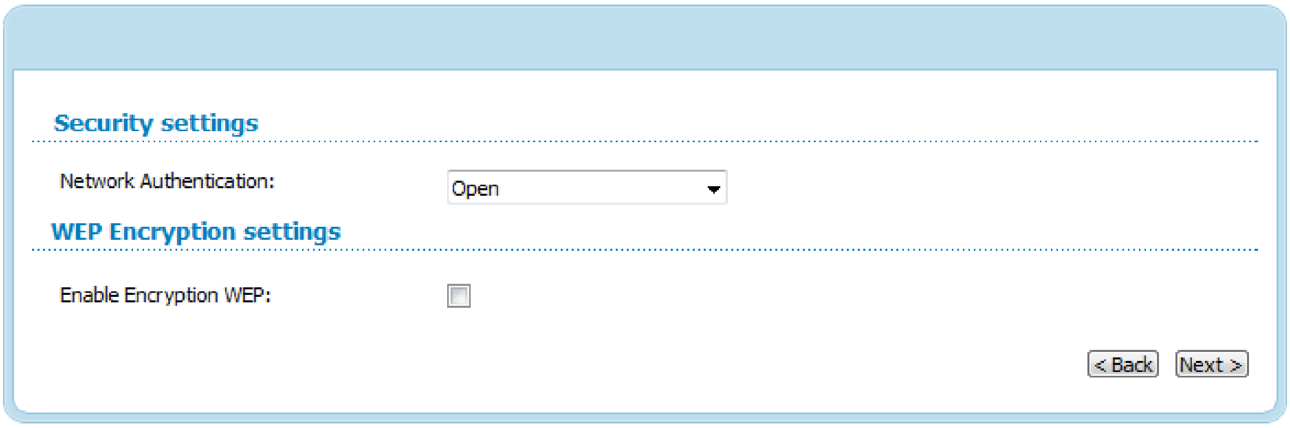
When changing mode from "B"/"G" on any of the modes with "N" is recommended to re-tune security!

Max Associated Clients: 0

*Figure 87. 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.



Security settings

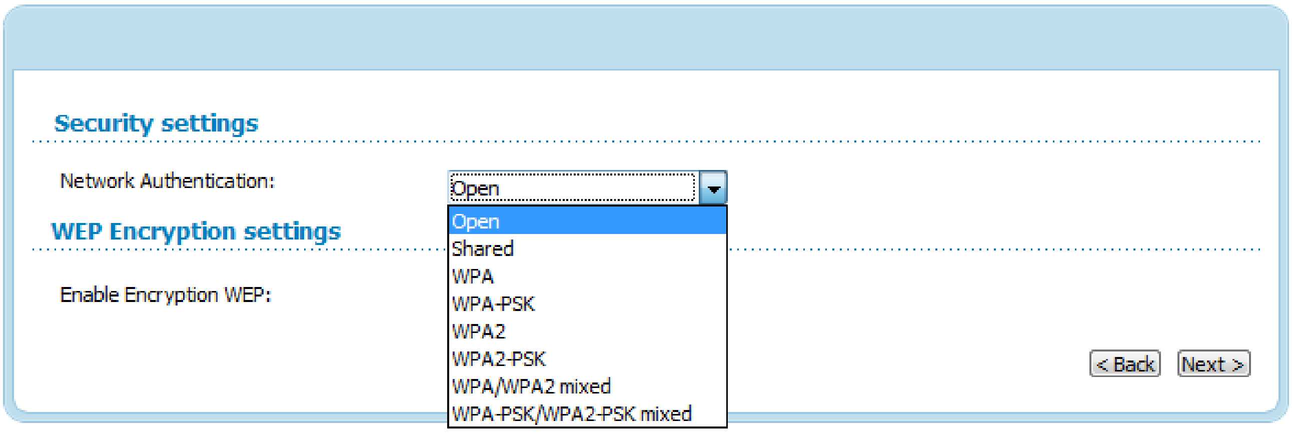
Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP: □

*Figure 88. 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).



Security settings

Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP:

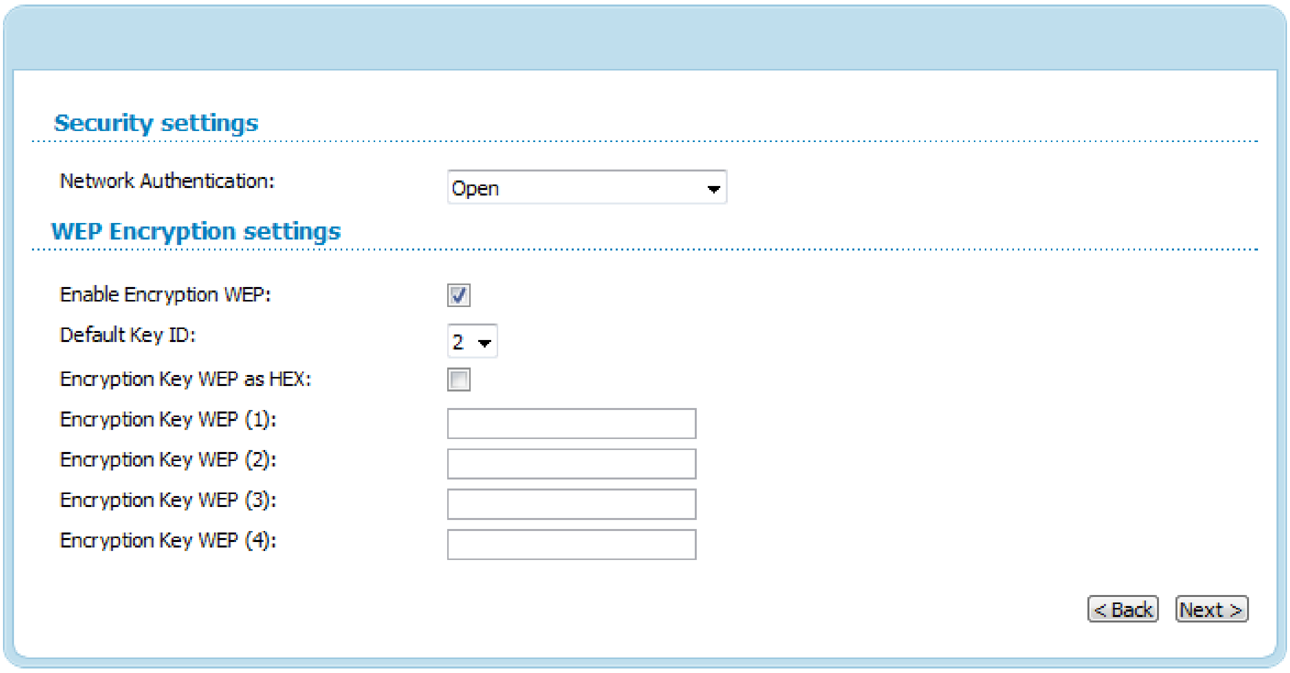
*Figure 89. Network authentication types supported by the access point.*

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** | WPA-based authentication using a RADIUS server. |
| **WPA-PSK** | WPA-based authentication using a PSK. |
| **WPA2** | WPA2-based authentication using a RADIUS server. |
| **WPA2-PSK** | WPA2-based authentication using a PSK. |
| **WPA/WPA2 mixed** | A mixed type of authentication. When this value is selected, devices using the **WPA** authentication type and devices using the **WPA2** authentication type can connect to the WLAN of the access point. |
| **WPA-PSK/WPA2-PSK mixed** | A mixed type of authentication. When this value is selected, devices using the **WPA-PSK** authentication type and devices using the **WPA2-PSK** authentication type can connect to the WLAN of the access point. |

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

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



Security settings

Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP: ☑

Default Key ID: 2

Encryption Key WEP as HEX: □

Encryption Key WEP (1):

Encryption Key WEP (2):

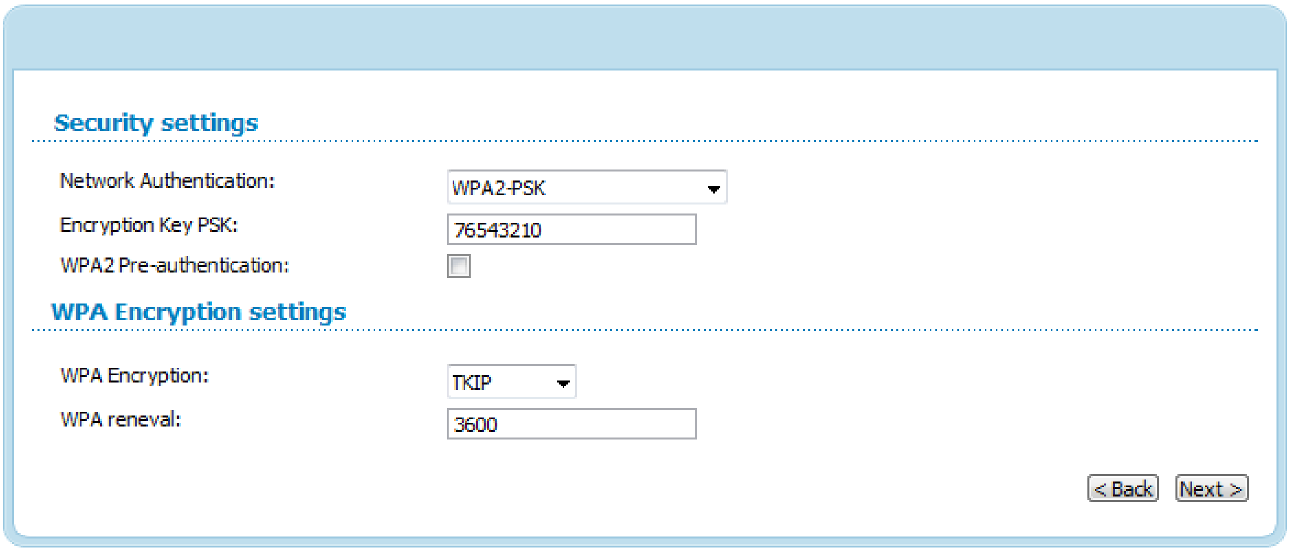
Encryption Key WEP (3):

Encryption Key WEP (4):

*Figure 90. 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.<br>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**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the **WPA Encryption settings** section is displayed:



Security settings

Network Authentication: WPA2-PSK

Encryption Key PSK: 76543210

WPA2 Pre-authentication: □

WPA Encryption settings

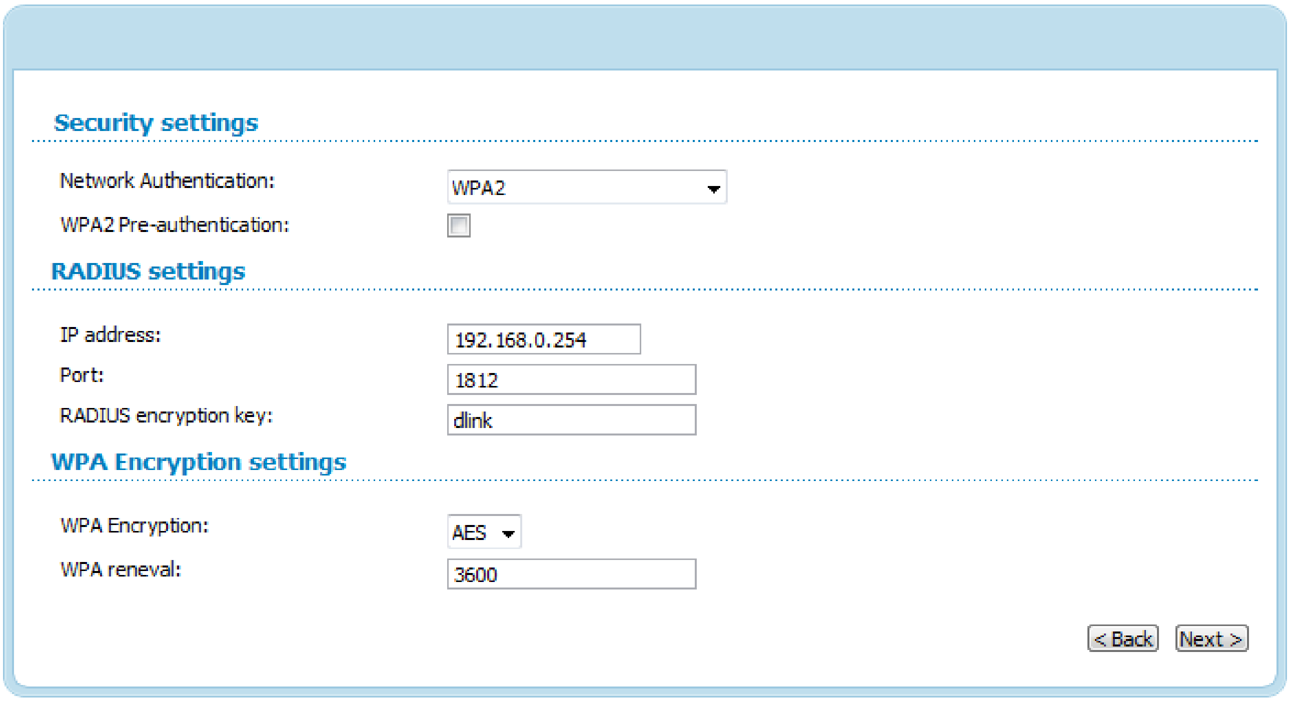
WPA Encryption: TKIP

WPA reneval: 3600

*Figure 91. 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** and **WPA-PSK/WPA2-PSK mixed** authentication types). |
| **WPA Encryption** | An encryption method: **TKIP**, **AES**, or **TKIP+AES**. |
| **WPA renewal** | The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value **0** is specified for this field, the key is not renewed. |

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the **RADIUS settings** and **WPA Encryption settings** sections are available:



Security settings

Network Authentication: WPA2

WPA2 Pre-authentication: □

RADIUS settings

IP address: 192.168.0.254

Port: 1812

RADIUS encryption key: dlink

WPA Encryption settings

WPA Encryption: AES

WPA reneval: 3600

*Figure 92. The **WPA2** value is selected from the **Network Authentication** drop-down list.*

| Parameter | Description |
|---|---|
| **WPA2 Pre-authentication** | The checkbox activating preliminary authentication (displayed only for the **WPA2** and **WPA/WPA2 mixed** authentication types. |
| **IP address** | The IP address of the RADIUS server. |
| **Port** | A port of the RADIUS server. |
| **RADIUS encryption key** | The password which the access point uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings). |
| **WPA Encryption** | An encryption method: **TKIP** (available only for the **WPA** authentication type), **AES** (available only for the **WPA2** and **WPA/WPA2 mixed** authentication types). |
| **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.

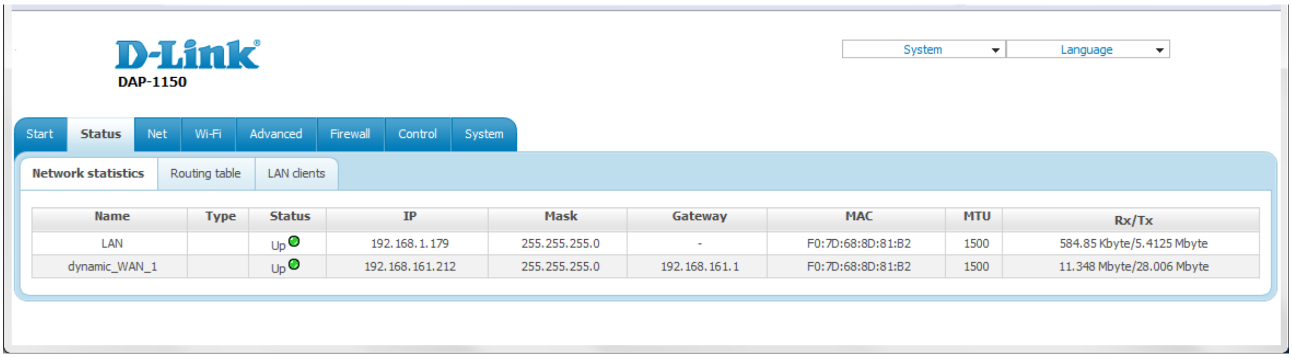
## *Status*

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

- network statistics
- 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 interfaces (connections) existing in the system. For each connection the following data are displayed: state, IP address, subnet mask and 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).

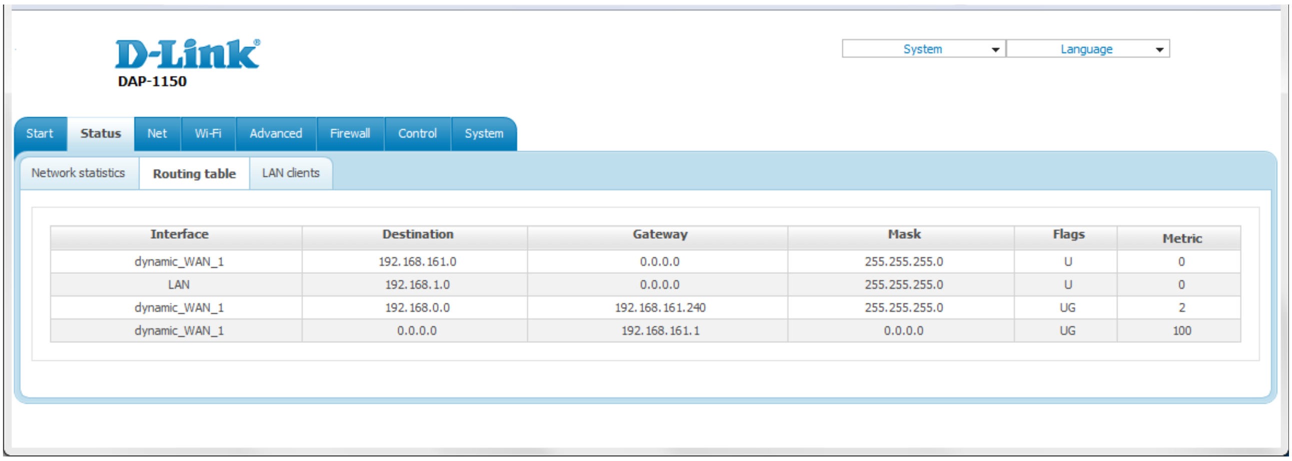


| Name | Type | Status | IP | Mask | Gateway | MAC | MTU | Rx/Tx |
|---|---|---|---|---|---|---|---|---|
| LAN | | Up ● | 192.168.1.179 | 255.255.255.0 | - | F0:7D:68:8D:81:B2 | 1500 | 584.85 Kbyte/5.4125 Mbyte |
| dynamic_WAN_1 | | Up ● | 192.168.161.212 | 255.255.255.0 | 192.168.161.1 | F0:7D:68:8D:81:B2 | 1500 | 11.348 Mbyte/28.006 Mbyte |

*Figure 93. The* ***Status / Network statistics*** *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.

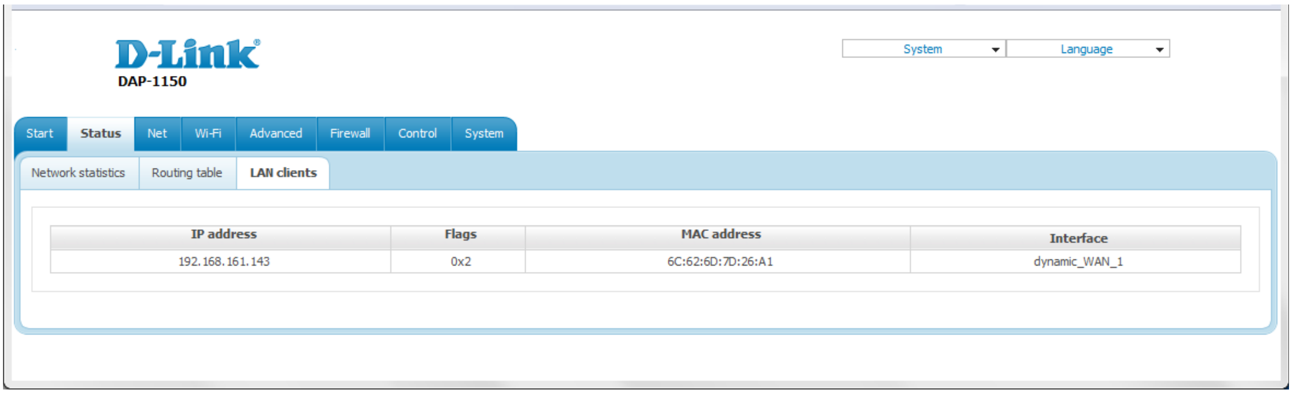


| Interface | Destination | Gateway | Mask | Flags | Metric |
|---|---|---|---|---|---|
| dynamic_WAN_1 | 192.168.161.0 | 0.0.0.0 | 255.255.255.0 | U | 0 |
| LAN | 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U | 0 |
| dynamic_WAN_1 | 192.168.0.0 | 192.168.161.240 | 255.255.255.0 | UG | 2 |
| dynamic_WAN_1 | 0.0.0.0 | 192.168.161.1 | 0.0.0.0 | UG | 100 |

*Figure 94. 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.



| IP address | Flags | MAC address | Interface |
|---|---|---|---|
| 192.168.161.143 | 0x2 | 6C:62:6D:7D:26:A1 | dynamic_WAN_1 |

*Figure 95. The **Status / LAN clients** page.*

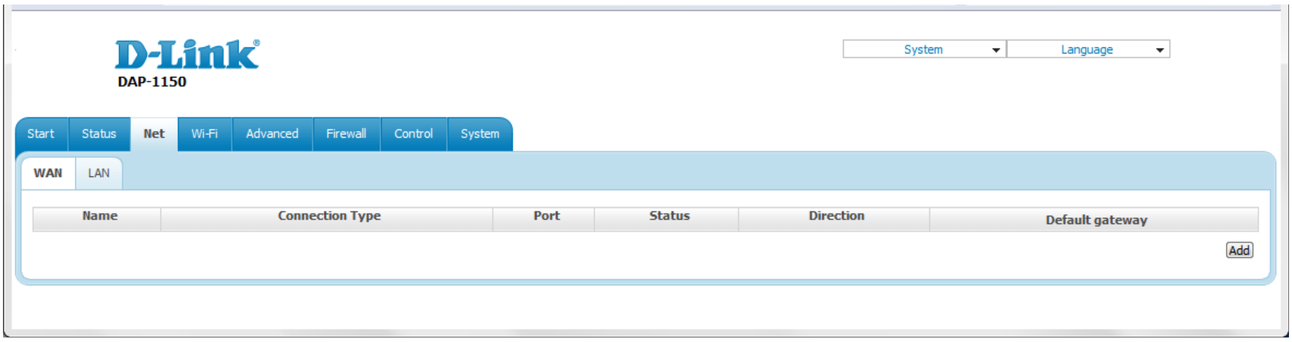
For each device the following data are displayed: the IP address, the MAC address, and the interface to which the device is connected.

# *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.



| Name | Connection Type | Port | Status | Direction | Default gateway |
|---|---|---|---|---|---|

*Figure 96. The* ***Net / WAN*** *page.*

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

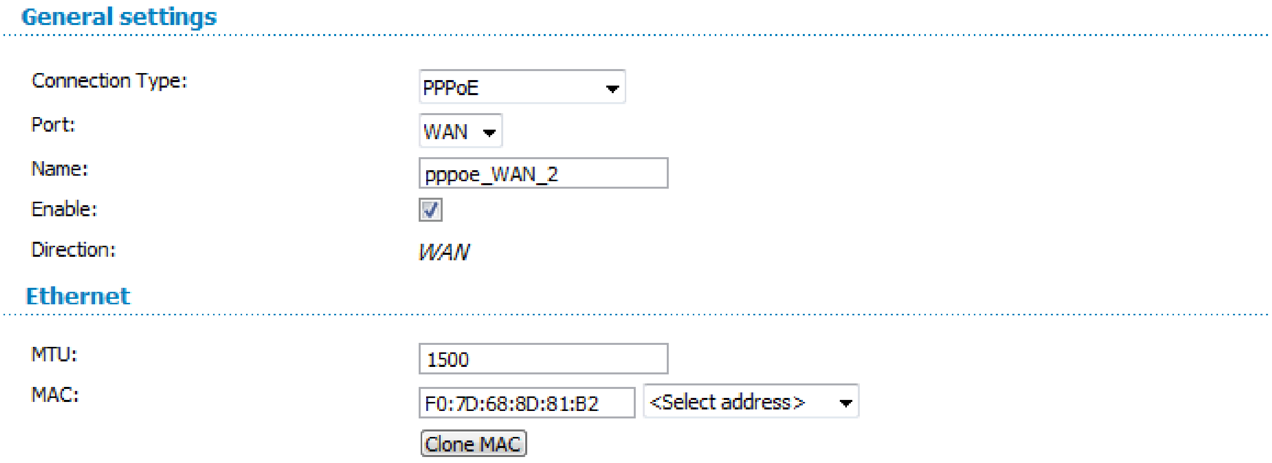
To edit an existing connection, left-click the relevant line in the table. On the page displayed, change the parameters and click the **Save** button.

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.



General settings

Connection Type: PPPoE

Port: WAN

Name: pppoe_WAN_2

Enable: ☑

Direction: WAN

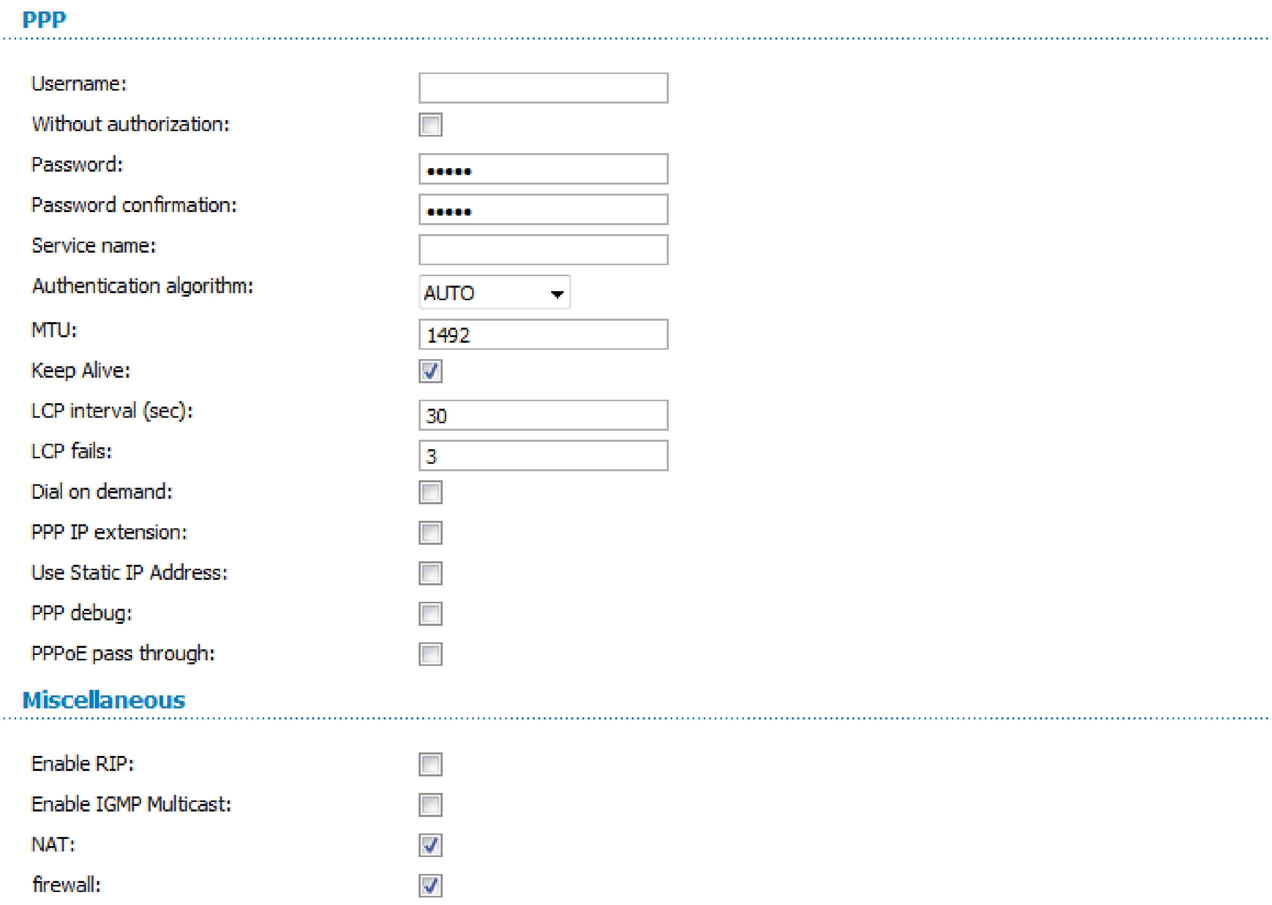
Ethernet

MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

*Figure 97. 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. |
| **MAC** | 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.<br>You can click the **Clone MAC** 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.<br>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 located to the right of the field (the field will be filled in automatically). |



PPP

| | |
|---|---|
| Username: | |
| Without authorization: | □ |
| Password: | ••••• |
| Password confirmation: | ••••• |
| Service name: | |
| Authentication algorithm: | AUTO |
| MTU: | 1492 |
| Keep Alive: | ☑ |
| LCP interval (sec): | 30 |
| LCP fails: | 3 |
| Dial on demand: | □ |
| PPP IP extension: | □ |
| Use Static IP Address: | □ |
| PPP debug: | □ |
| PPPoE pass through: | □ |

Miscellaneous

| | |
|---|---|
| Enable RIP: | □ |
| Enable IGMP Multicast: | □ |
| NAT: | ☑ |
| firewall: | ☑ |

*Figure 98. The page for creating a new connection. The **PPP** and **Miscellaneous** sections.*

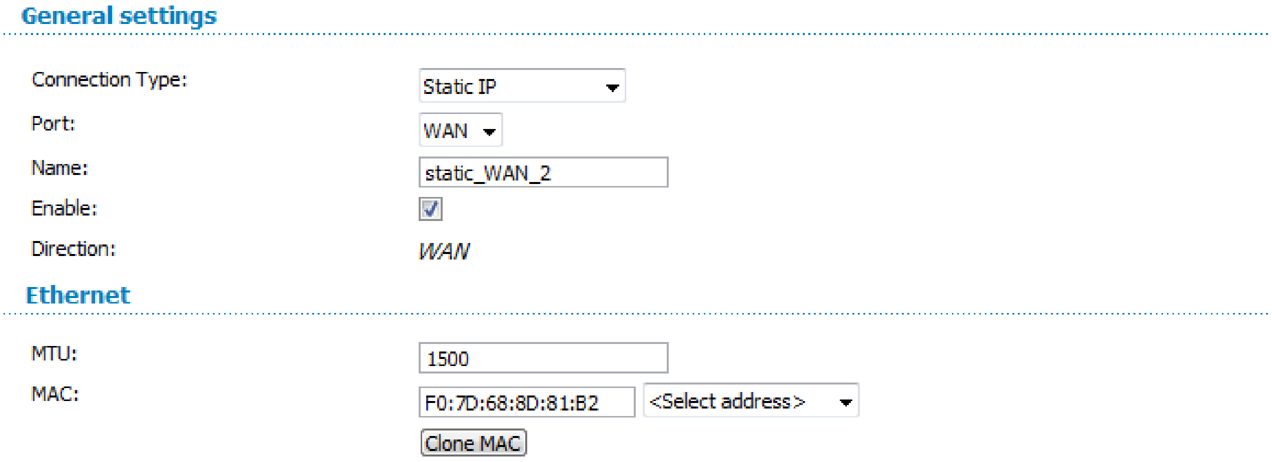
| Parameter | Description |
|---|---|
| **PPP** | |
| **Username** | A username (login) to access the Internet. |
| **Without authorization** | Select the checkbox if you don't need to enter a username and password to access the Internet. |
| **Password** | A password to access the Internet. |
| **Password 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. |

| Parameter | Description |
|---|---|
| **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. |
| **Use Static IP Address** | Select the checkbox if you want to use a static IP address to access the Internet. In the **IP Address** field displayed when the checkbox is selected, specify a static IP address. |
| **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. |
| **Enable IGMP Multicast** | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |
| **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. |

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.



General settings

Connection Type: Static IP

Port: WAN

Name: static_WAN_2

Enable: ☑

Direction: *WAN*

Ethernet

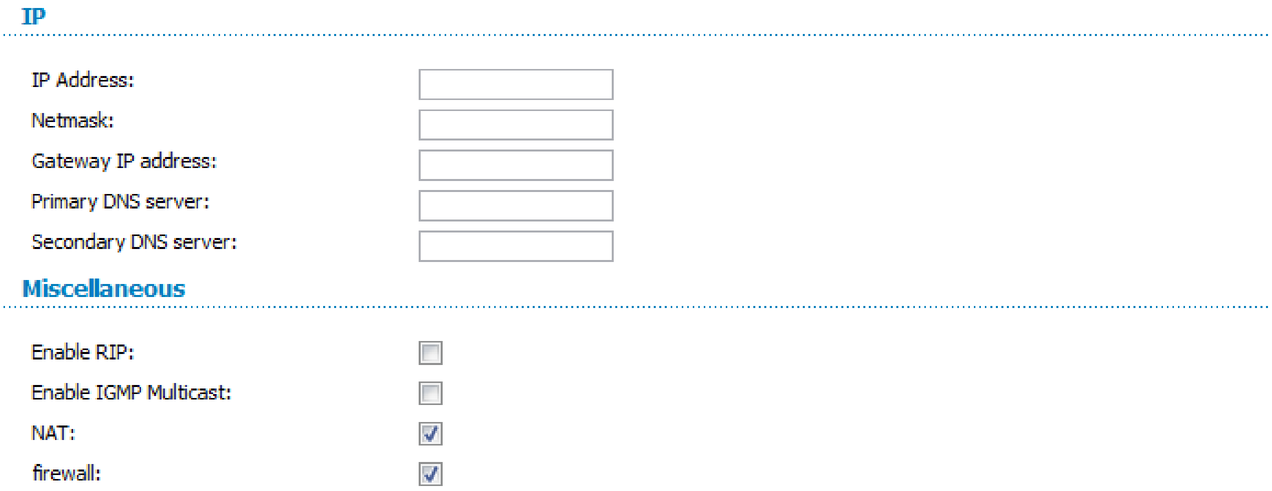
MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

*Figure 99. 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** | 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.<br>You can click the **Clone MAC** 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.<br>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 located to the right of the field (the field will be filled in automatically). |



IP

IP Address:

Netmask:

Gateway IP address:

Primary DNS server:

Secondary DNS server:

Miscellaneous

Enable RIP: □

Enable IGMP Multicast: □

NAT: ☑

firewall: ☑

*Figure 100. The page for creating a new connection. The **IP** and **Miscellaneous** sections.*

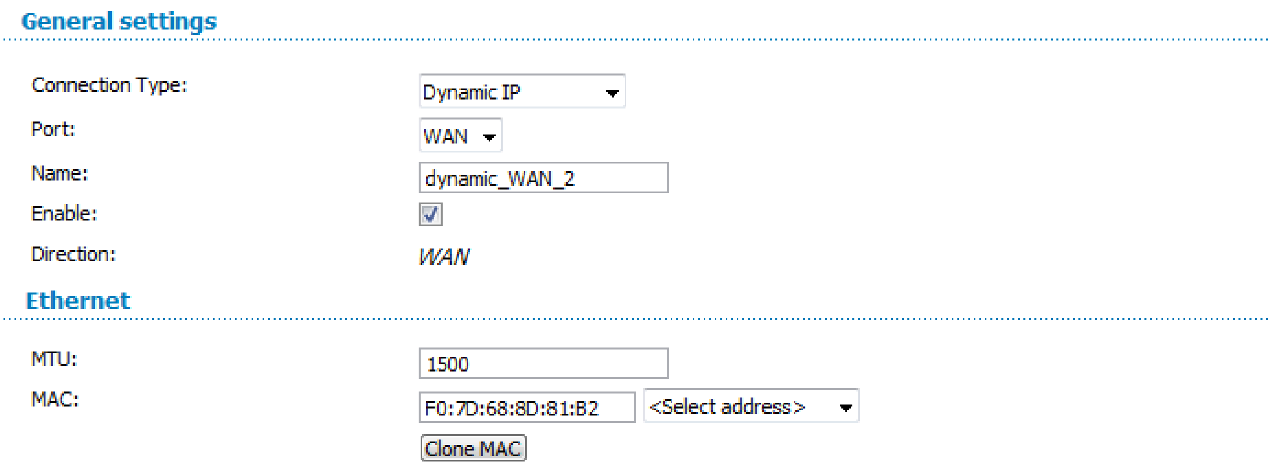
| Parameter | Description |
|---|---|
| **IP** | |
| **IP Address** | Enter an IP address for this WAN connection. |
| **Netmask** | Enter a subnet mask for this WAN connection. |
| **Gateway IP Address** | Enter an IP address of the gateway used by this WAN connection. |
| **Primary DNS server/ Secondary 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. |

| 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. |

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.



General settings

Connection Type: Dynamic IP

Port: WAN

Name: dynamic_WAN_2

Enable: ☑

Direction: WAN

Ethernet

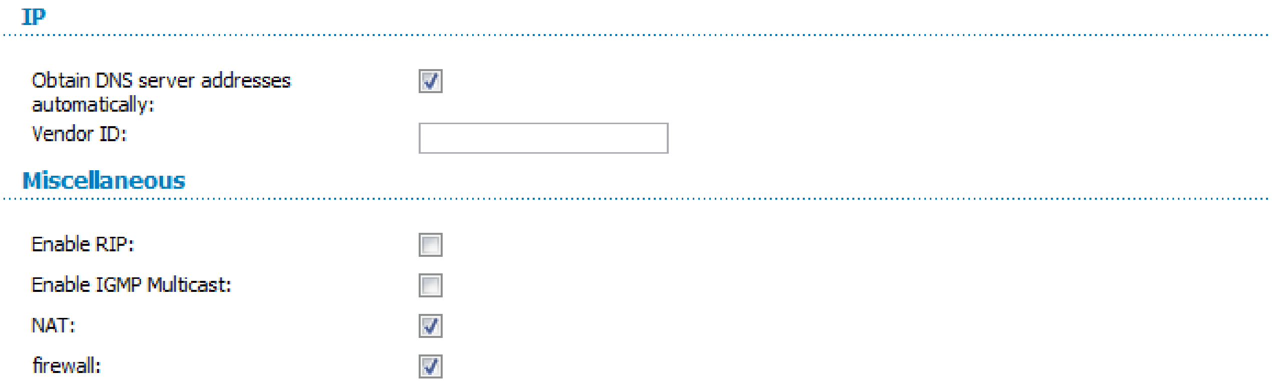
MTU: 1500

MAC: F0:7D:68:8D:81:B2 <Select address>

*Figure 101. 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** | 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.<br>You can click the **Clone MAC** 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.<br>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 located to the right of the field (the field will be filled in automatically). |


IP

Obtain DNS server addresses automatically: ☑
Vendor ID:

Miscellaneous

Enable RIP: □
Enable IGMP Multicast: □
NAT: ☑
firewall: ☑

*Figure 102. The page for creating a new connection. The **IP** and **Miscellaneous** sections.*

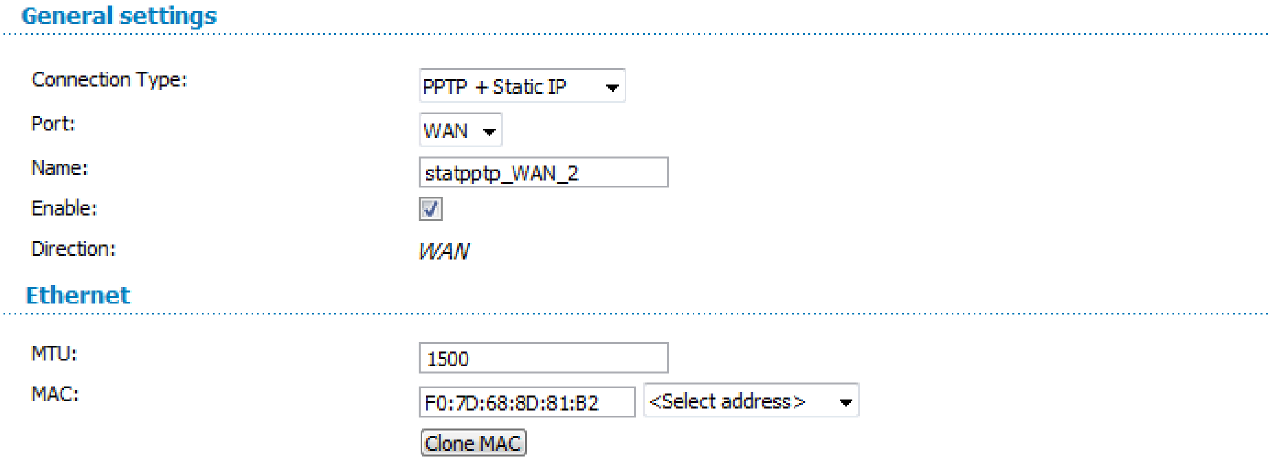
| Parameter | Description |
|---|---|
| **IP** | |
| **Obtain DNS server addresses automatically** | Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the **Primary DNS server** and **Secondary DNS server** fields are not displayed. |
| **Primary 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. *Optional*. |
| **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. |

| Parameter | Description |
|---|---|
| **NAT** | Select the checkbox if you want one WAN IP address to be used for all computers of your LAN. |
| **Firewall** | Select the checkbox to enable protection against ARP and DDoS attacks. |

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.



General settings

Connection Type: PPTP + Static IP
Port: WAN
Name: statpptp_WAN_2
Enable: ☑
Direction: WAN

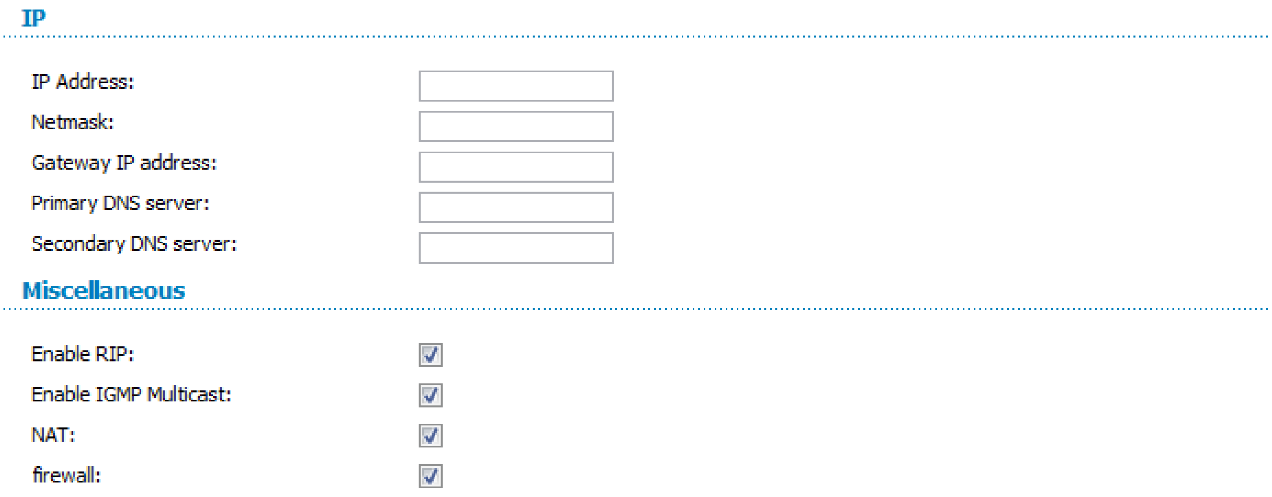
Ethernet

MTU: 1500
MAC: F0:7D:68:8D:81:B2 <Select address>

*Figure 103. 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** | 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.<br>You can click the **Clone MAC** 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.<br>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 located to the right of the field (the field will be filled in automatically). |



IP

| | |
|---|---|
| IP Address: | |
| Netmask: | |
| Gateway IP address: | |
| Primary DNS server: | |
| Secondary DNS server: | |

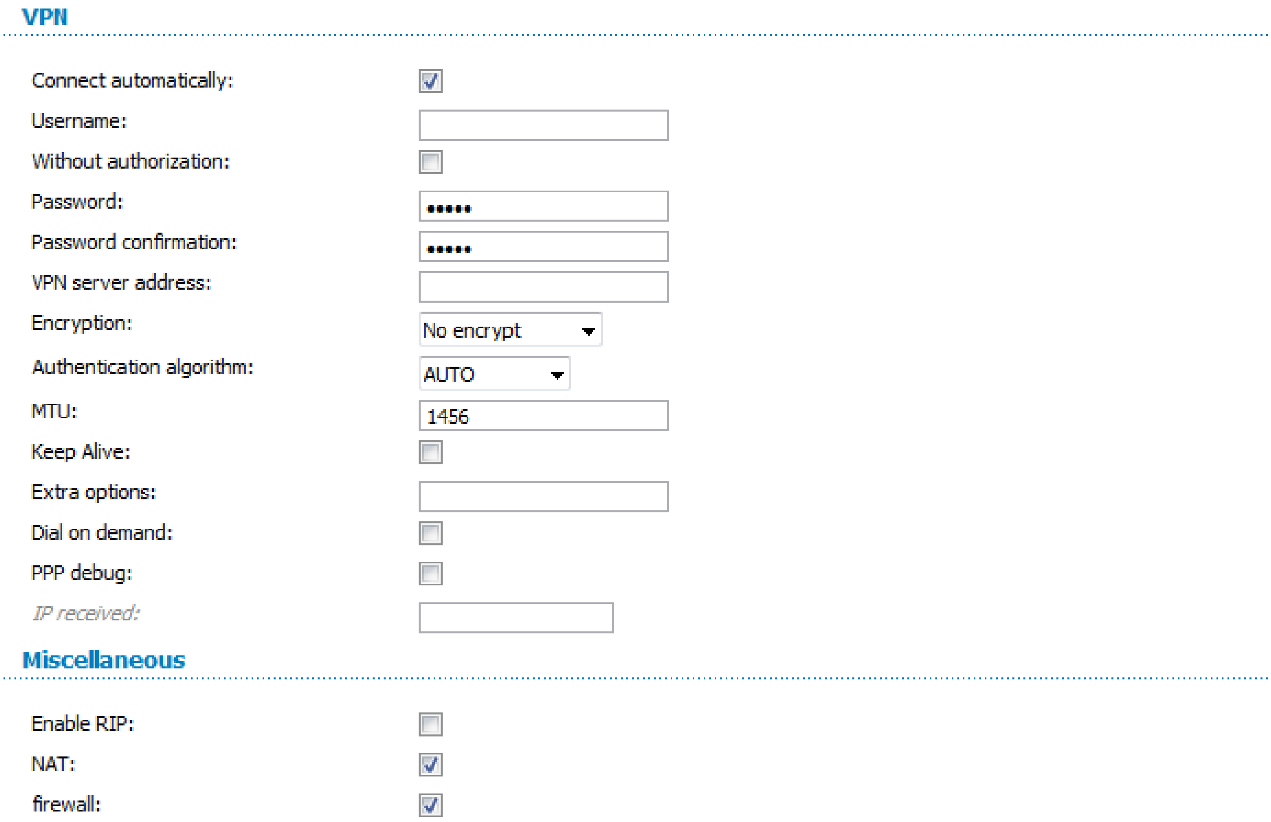
Miscellaneous

| | |
|---|---|
| Enable RIP: | ☑ |
| Enable IGMP Multicast: | ☑ |
| NAT: | ☑ |
| firewall: | ☑ |

*Figure 104. 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. |

| 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. |



VPN

| | |
|---|---|
| Connect automatically: | ☑ |
| Username: | |
| Without authorization: | □ |
| Password: | ••••• |
| Password confirmation: | ••••• |
| VPN server address: | |
| Encryption: | No encrypt |
| Authentication algorithm: | AUTO |
| MTU: | 1456 |
| Keep Alive: | □ |
| Extra options: | |
| Dial on demand: | □ |
| PPP debug: | □ |
| *IP received:* | |

Miscellaneous

| | |
|---|---|
| Enable RIP: | □ |
| NAT: | ☑ |
| firewall: | ☑ |

*Figure 105. The page for creating a new connection. The **VPN** and **Miscellaneous** sections.*

| 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). |

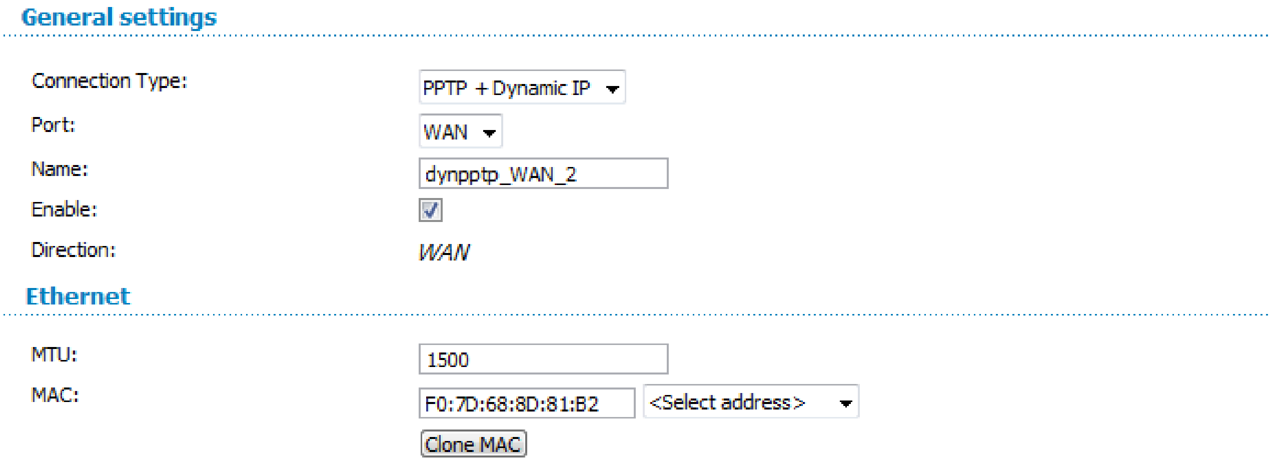
| Parameter | Description |
|---|---|
| **VPN server address** | The IP or URL address of the PPTP or L2TP authentication server. |
| **Encryption** | Select a method of MPPE encryption.<br>• **No encrypt**: MPPE encryption is not applied.<br>• **MPPE 40/128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied.<br>• **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied.<br>• **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied.<br>MPPE encryption can be applied only if the **MSCHAP**, **MACHAPv2**, or **AUTO** value is selected from the **Authentication algorithm** drop-down list. |
| **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. *Optional*. |
| **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 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** | 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. |

| Parameter | Description |
|---|---|
| **Firewall** | Select the checkbox to enable protection against ARP and DDoS attacks. |

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.



General settings

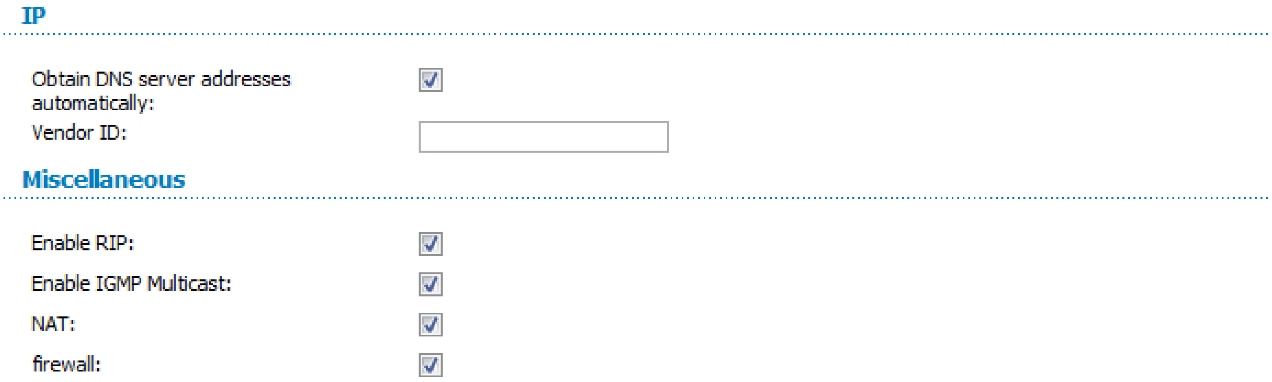
Connection Type: PPTP + Dynamic IP
Port: WAN
Name: dynpptp_WAN_2
Enable: ☑
Direction: WAN

Ethernet

MTU: 1500
MAC: F0:7D:68:8D:81:B2 <Select address>

*Figure 106. 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. |
| **MAC** | 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.<br>You can click the **Clone MAC** 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.<br>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 located to the right of the field (the field will be filled in automatically). |



IP

Obtain DNS server addresses automatically: ☑

Vendor ID:

Miscellaneous

Enable RIP: ☑

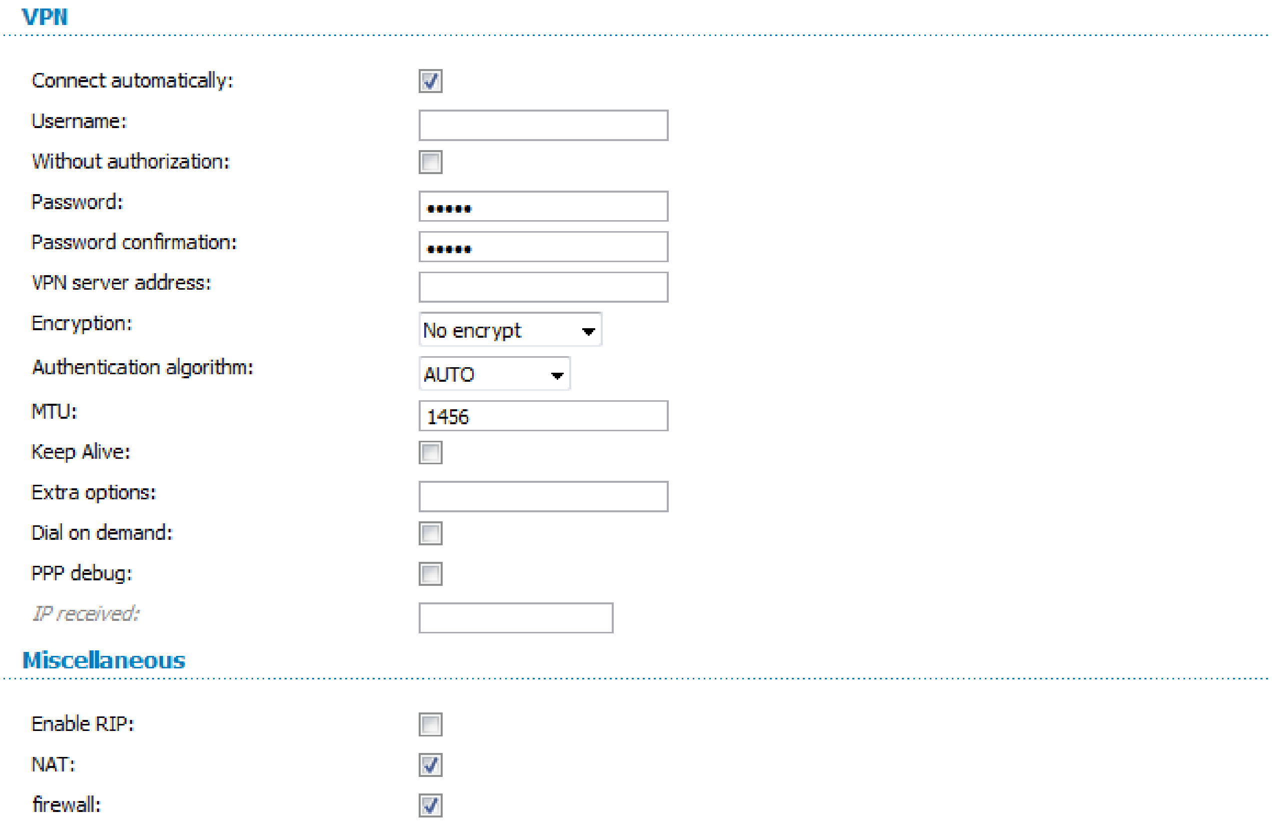
Enable IGMP Multicast: ☑

NAT: ☑

firewall: ☑

*Figure 107. 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/**<br>**Secondary DNS server** | Enter addresses of the primary and secondary DNS servers in the relevant fields. |
| **Vendor ID** | The identifier of your ISP. *Optional*. |
| **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. |



VPN

| | |
|---|---|
| Connect automatically: | ☑ |
| Username: | |
| Without authorization: | □ |
| Password: | ••••• |
| Password confirmation: | ••••• |
| VPN server address: | |
| Encryption: | No encrypt |
| Authentication algorithm: | AUTO |
| MTU: | 1456 |
| Keep Alive: | □ |
| Extra options: | |
| Dial on demand: | □ |
| PPP debug: | □ |
| *IP received:* | |

Miscellaneous

| | |
|---|---|
| Enable RIP: | □ |
| NAT: | ☑ |
| firewall: | ☑ |

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

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

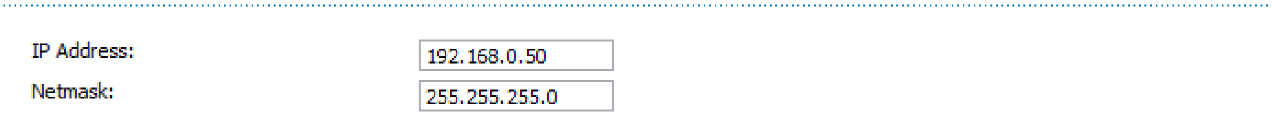
| Parameter | Description |
|---|---|
| **Encryption** | Select a method of MPPE encryption.<br>• **No encrypt**: MPPE encryption is not applied.<br>• **MPPE 40/128 bit**: MPPE encryption with a 40-bit or 128-bit key is applied.<br>• **MPPE 40 bit**: MPPE encryption with a 40-bit key is applied.<br>• **MPPE 128 bit**: MPPE encryption with a 128-bit key is applied.<br>MPPE encryption can be applied only if the **MSCHAP**, **MACHAPv2**, or **AUTO** value is selected from the **Authentication algorithm** drop-down list. |
| **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. *Optional*. |
| **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 debug** | Select the checkbox if you want to log all data on PPP connection debugging. |
| **IP received** | The IP address assigned by the ISP. |

| 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. |

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.



IP Address: 192.168.0.50
Netmask: 255.255.255.0

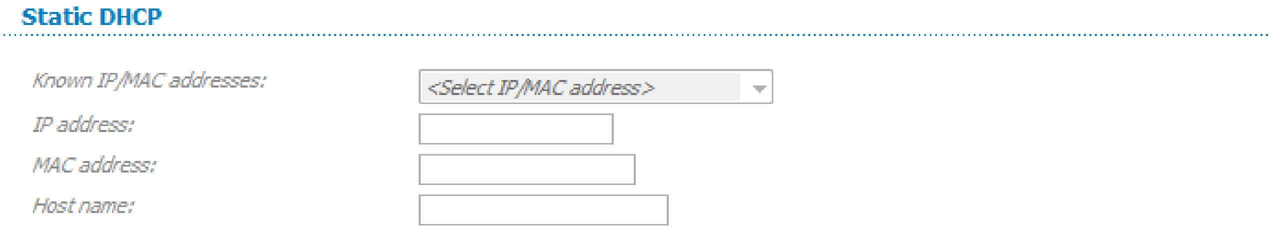
*Figure 109. Basic settings of the local interface.*

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 **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: <Select IP/MAC address>
IP address:
MAC address:
Host name:

*Figure 110. The section for creating MAC-IP pairs.*

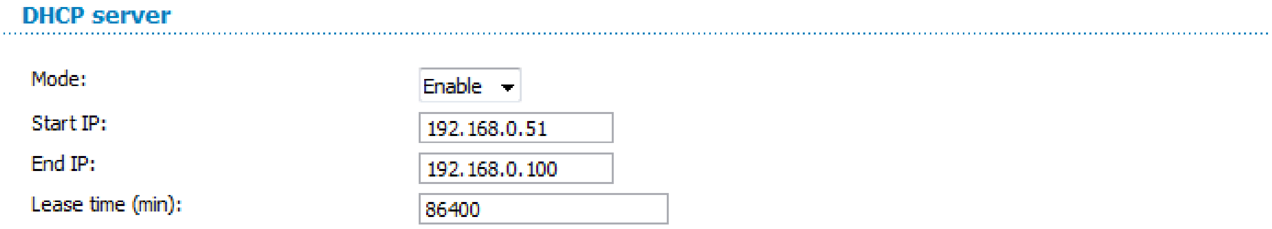
To create a MAC-IP pair, click the **Add** button. Enter the MAC address of the device from the LAN in the **MAC address** field and an IP address which will be assigned to this device in the **IP address** field. In the **Host name** field, specify a network name of the device for easier identification (*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 address** and **MAC address** 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 relevant line in the table and click the **Remove** button. Then click the **Save** button.

In the **DHCP server** section, you can configure the built-in DHCP sever of the access point.



DHCP server

Mode: Enable

Start IP: 192.168.0.51

End IP: 192.168.0.100

Lease time (min): 86400

*Figure 111. The section for configuring the DHCP server.*

| Parameter | Description |
|---|---|
| **Mode** | An operating mode of the access point's DHCP server.<br>**Enable**: the access point assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the **Start IP**, **End IP**, and the **Lease time** fields are displayed on the page.<br>**Disable**: the access point's DHCP server is disabled, clients' IP addresses are assigned manually.<br>**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. |
| **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. |

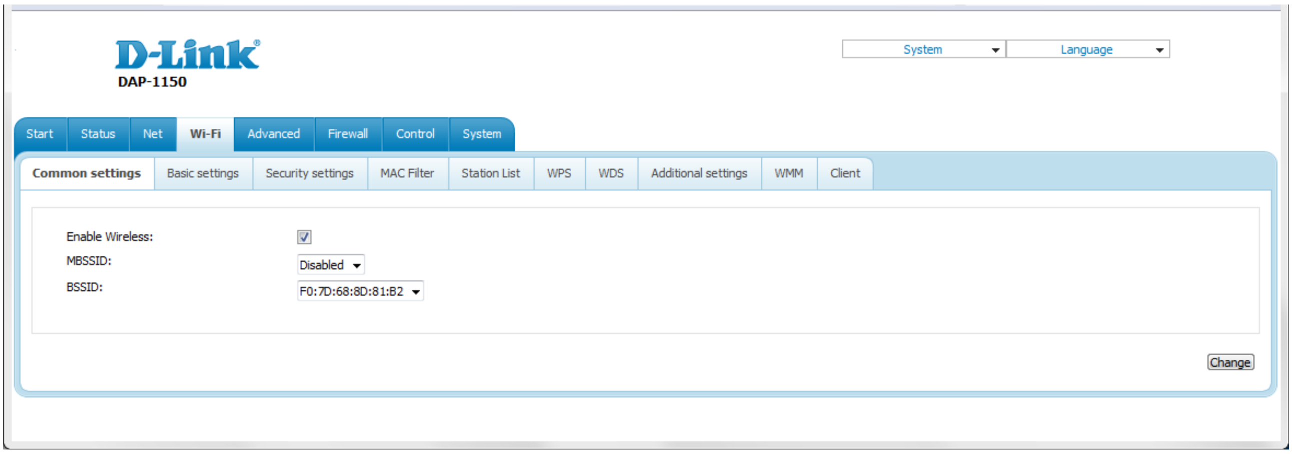
When all needed settings are configured, click the **Save** button.

# *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.



Enable Wireless: ☑
MBSSID: Disabled
BSSID: F0:7D:68:8D:81:B2

*Figure 112. 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).

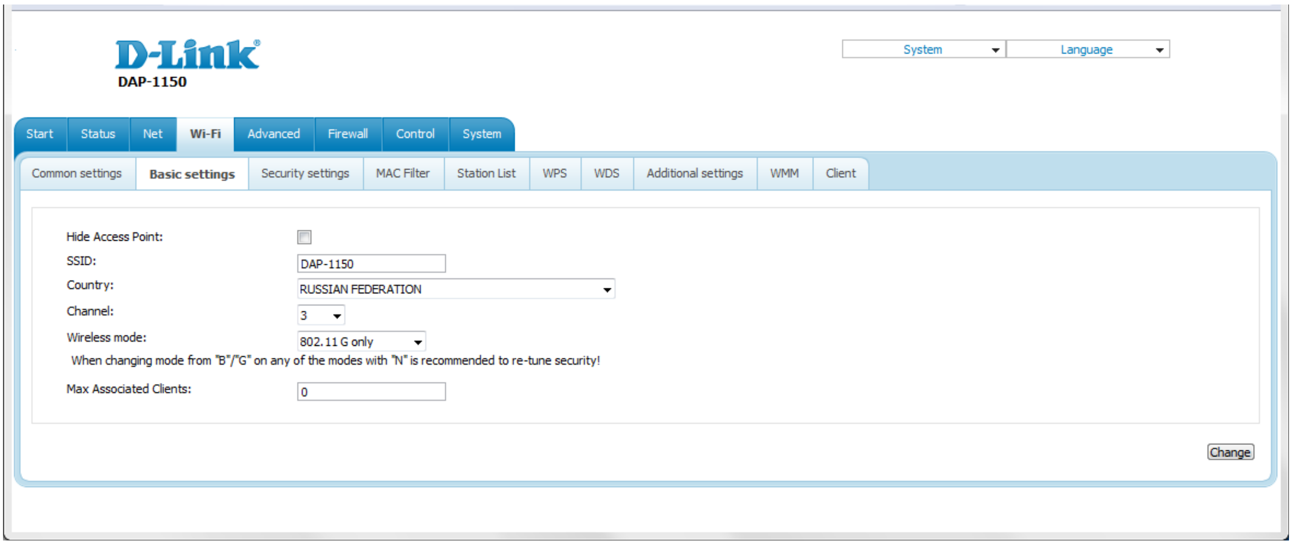
The value from the **BSSID** drop-down list is the unique identifier for your Wi-Fi network. You cannot change the value of this parameter, it is determined in the device's internal settings.

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.



Hide Access Point: □

SSID: DAP-1150

Country: RUSSIAN FEDERATION

Channel: 3

Wireless mode: 802.11 G only

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

Max Associated Clients: 0

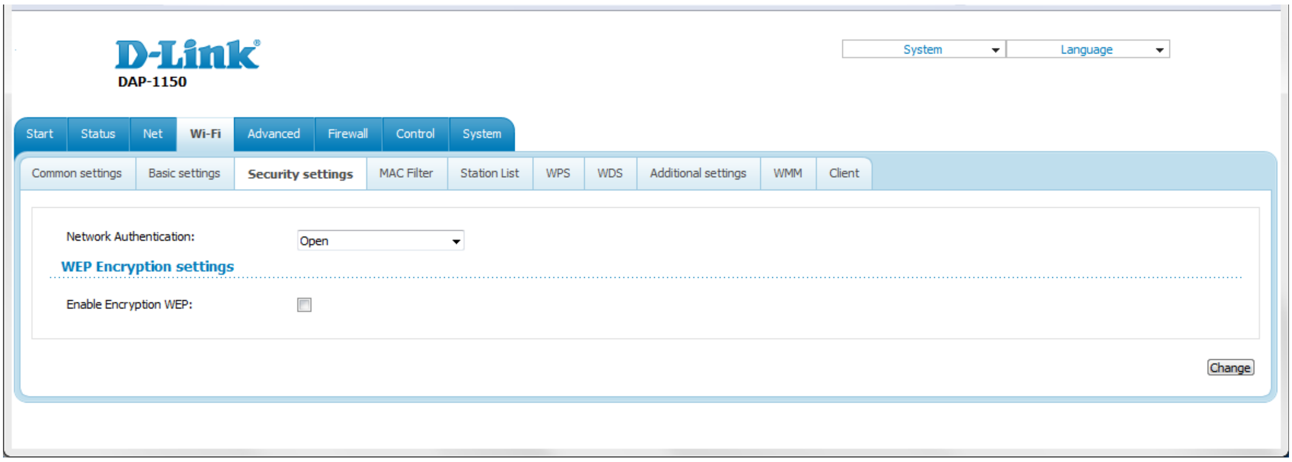
*Figure 113. Basic settings of the wireless LAN.*

| 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-1150` is specified. If your network is splitted into parts, each part has the default name (`DAP-1150.2`, `DAP-1150.3`, and `DAP-1150.4`). 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.



Network Authentication: Open

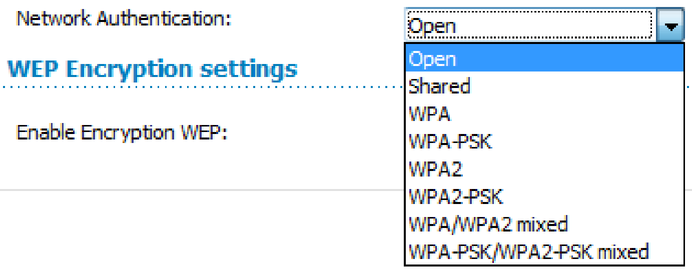
WEP Encryption settings

Enable Encryption WEP: □

*Figure 114. 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).



Network Authentication: Open

**WEP Encryption settings**

Enable Encryption WEP:

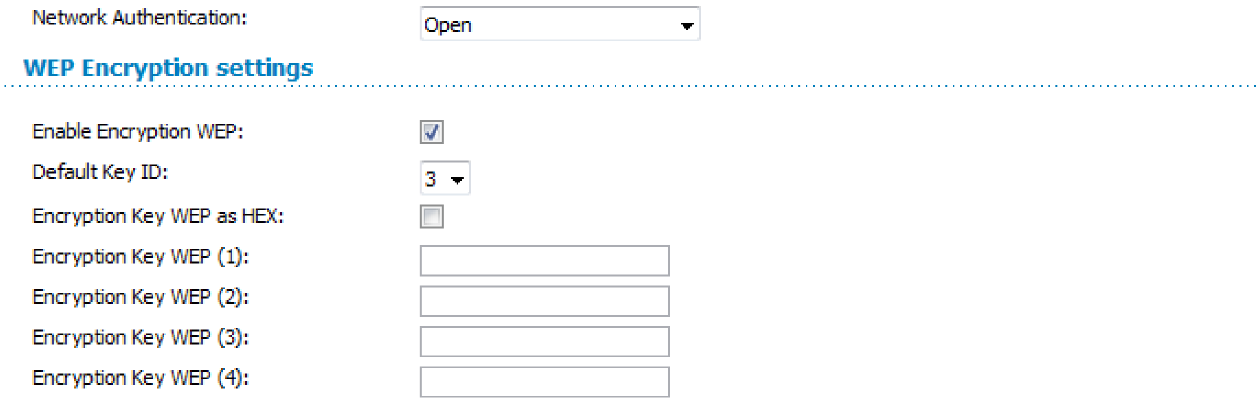
*Figure 115. Network authentication types supported by the access point.*

The access point supports the following authentication types:

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

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

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



Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP: ☑

Default Key ID: 3

Encryption Key WEP as HEX: □

Encryption Key WEP (1):

Encryption Key WEP (2):

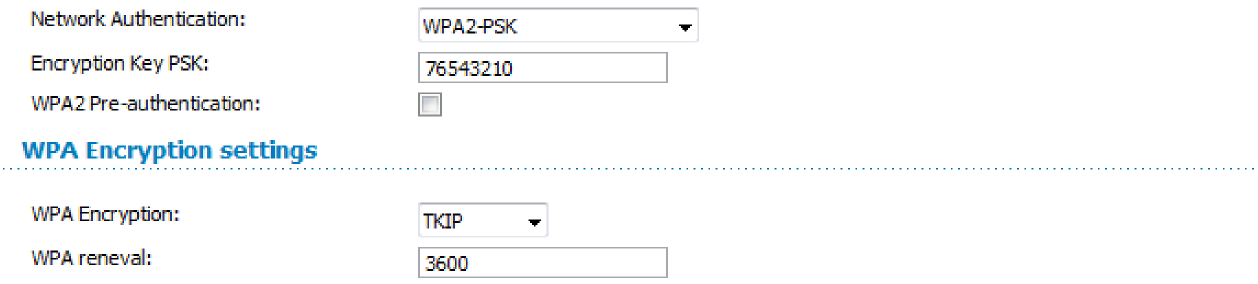
Encryption Key WEP (3):

Encryption Key WEP (4):

*Figure 116. 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.<br>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**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** value is selected, the **WPA Encryption settings** section is displayed:



Network Authentication: WPA2-PSK
Encryption Key PSK: 76543210
WPA2 Pre-authentication: □

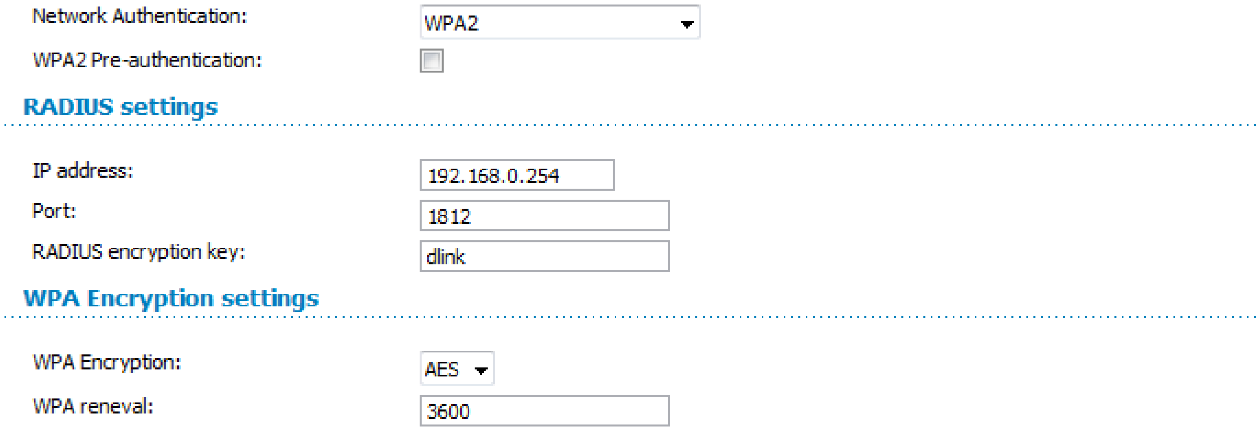
WPA Encryption settings

WPA Encryption: TKIP
WPA reneval: 3600

*Figure 117. 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** and **WPA-PSK/WPA2-PSK mixed** authentication types). |
| **WPA Encryption** | An encryption method: **TKIP**, **AES**, or **TKIP+AES**. |
| **WPA renewal** | The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed. |

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the **RADIUS settings** and **WPA Encryption settings** sections are available:



Network Authentication: WPA2

WPA2 Pre-authentication: □

RADIUS settings

IP address: 192.168.0.254

Port: 1812

RADIUS encryption key: dlink

WPA Encryption settings

WPA Encryption: AES

WPA renewal: 3600

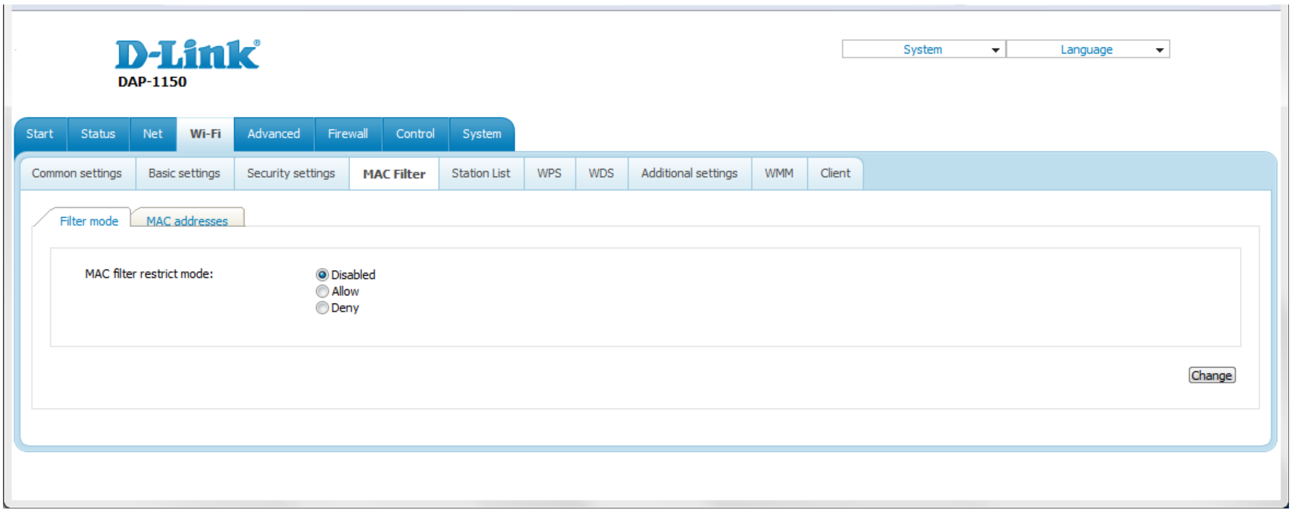
*Figure 118. The **WPA2** value is selected from the **Network Authentication** drop-down list.*

| Parameter | Description |
|---|---|
| **WPA2 Pre-authentication** | The checkbox activating preliminary authentication (displayed only for the **WPA2** and **WPA/WPA2 mixed** authentication types). |
| **IP address** | The IP address of the RADIUS server. |
| **Port** | A port of the RADIUS server. |
| **RADIUS encryption key** | The password which the access point uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings). |
| **WPA Encryption** | An encryption method: **TKIP** (available only for the **WPA** authentication type), **AES** (available only for the **WPA2** and **WPA/WPA2 mixed** authentication types). |
| **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.



MAC filter restrict mode: ● Disabled ○ Allow ○ Deny

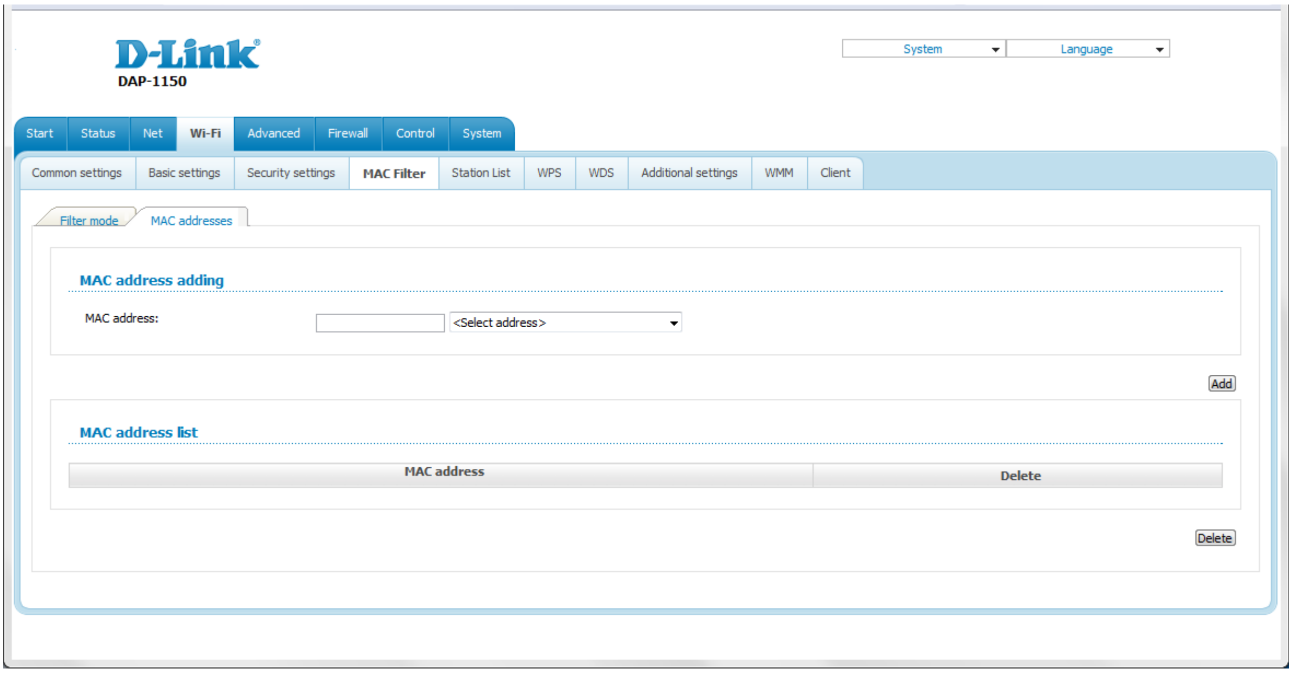
*Figure 119. MAC filters for the wireless network.*

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.



MAC address adding

MAC address: <Select address>

MAC address list

| MAC address | Delete |
|---|---|

*Figure 120. The tab for adding a MAC address.*

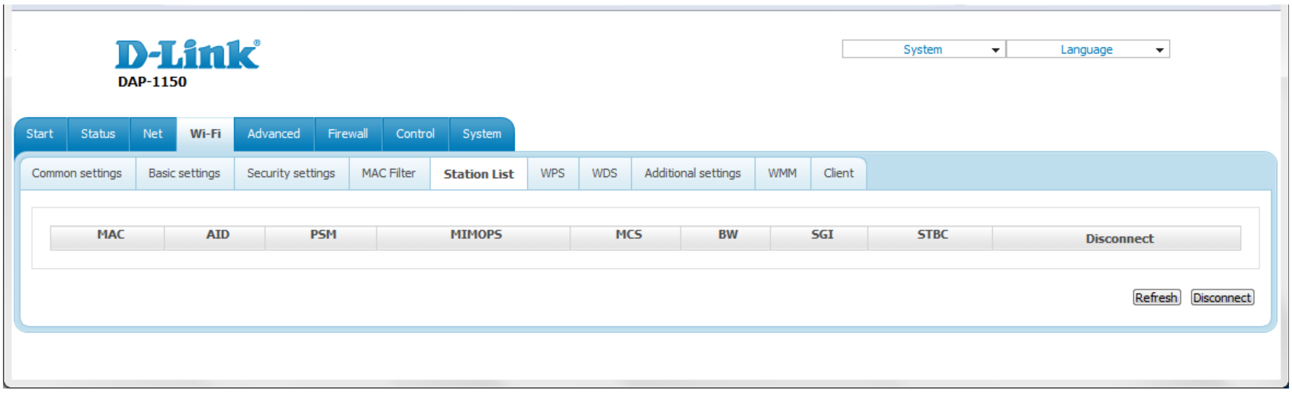
Enter an address in the **MAC address** field of the **MAC address adding** section and click the **Add** button.

To add the MAC address of a device connected to the access point's LAN at the moment, select the value containing the MAC and IP address of this device from the drop-down list located to the right of the **MAC address** field (the field will be filled in automatically) 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.



| MAC | AID | PSM | MIMOPS | MCS | BW | SGI | STBC | Disconnect |
|---|---|---|---|---|---|---|---|---|

*Figure 121. The list of the wireless clients.*

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

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

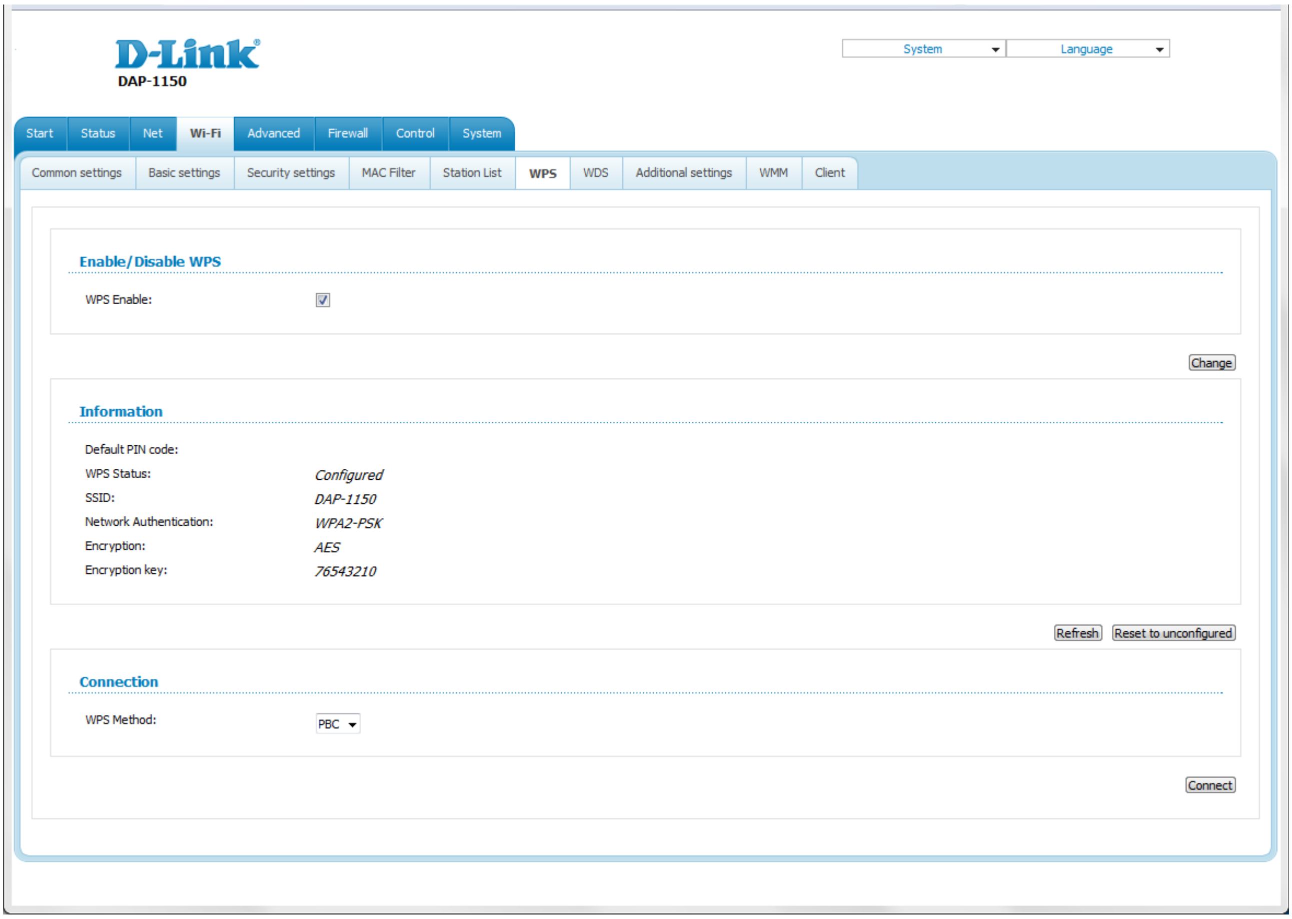
## WPS

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

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

! If the device's WLAN is 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 WPS function it is required to configure a type of WPA encryption.



Enable/Disable WPS

WPS Enable: ☑

Information

Default PIN code:
WPS Status: *Configured*
SSID: *DAP-1150*
Network Authentication: *WPA2-PSK*
Encryption: *AES*
Encryption key: *76543210*

Connection

WPS Method: PBC

*Figure 122. 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:<br>• **Configured** (all needed settings are specified)<br>• **Unconfigured** (you need to specify the relevant settings). |
| **SSID** | The name of the device'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 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 view the latest data on the state of connecting the wireless device via the WPS function. |
| **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.<br>**PIN**: Connecting the device via the PIN code.<br>**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.<br>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 WLAN of the access point via the WPS function. |

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 WLAN of the access point.
5. Click the relevant button in the software or on the cover 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.

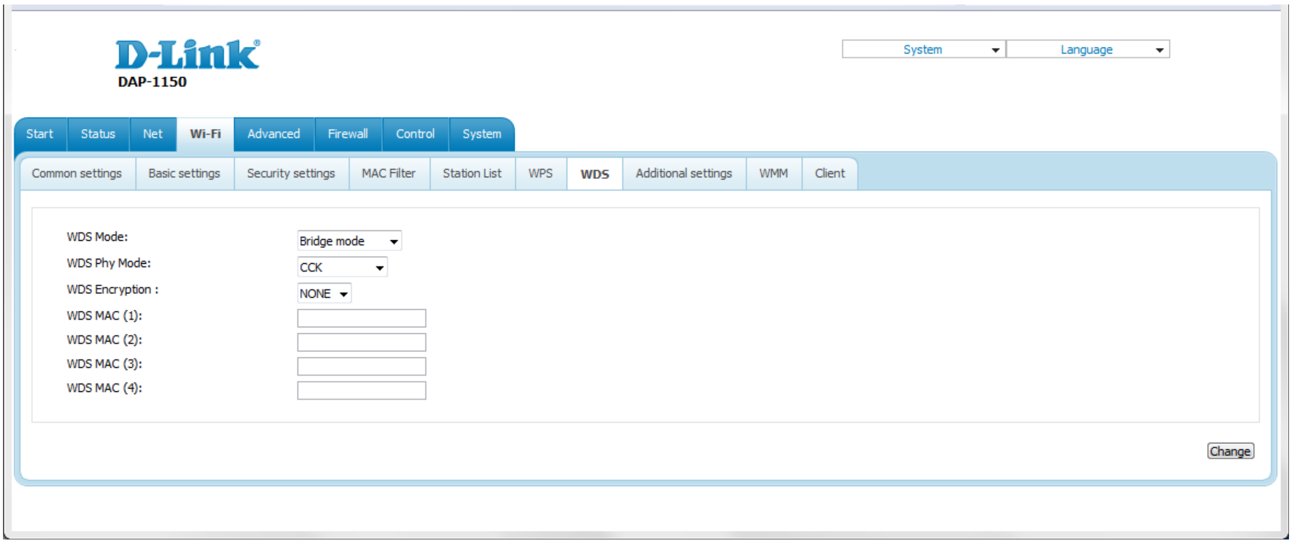
To add a wireless device via the PBC method of the WPS function, follow the next steps:

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 WLAN of the access point.
5. Click the relevant button in the software or 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.

## 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.



| | |
|---|---|
| WDS Mode: | Bridge mode |
| WDS Phy Mode: | CCK |
| WDS Encryption : | NONE |
| WDS MAC (1): | |
| WDS MAC (2): | |
| WDS MAC (3): | |
| WDS MAC (4): | |

*Figure 123. The page for configuring the WDS function.*

The following fields are available on the page:

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

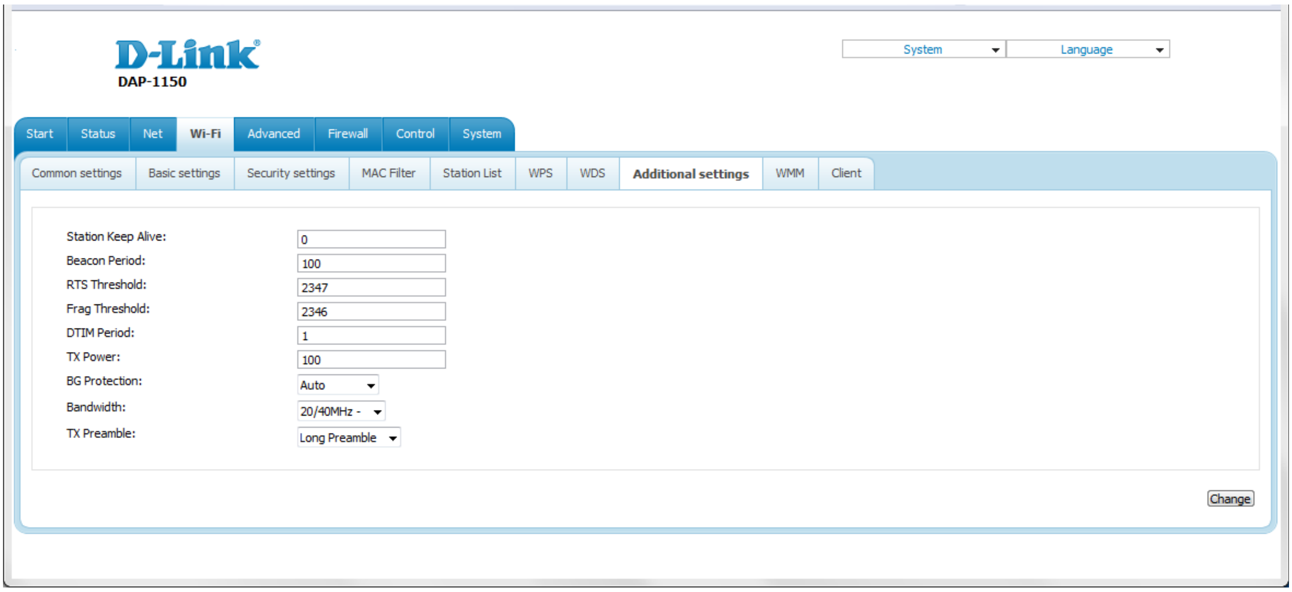
! The WDS function parameters specified on the page must be the same for all interconnected devices. In addition, it is required to set the same channel (on the **Wi-Fi / Basic settings** page).

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



Station Keep Alive: 0
Beacon Period: 100
RTS Threshold: 2347
Frag Threshold: 2346
DTIM Period: 1
TX Power: 100
BG Protection: Auto
Bandwidth: 20/40MHz -
TX Preamble: Long Preamble

*Figure 124. 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. |
| **TX Power** | The transmit power (in percentage terms) of the access point. |

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

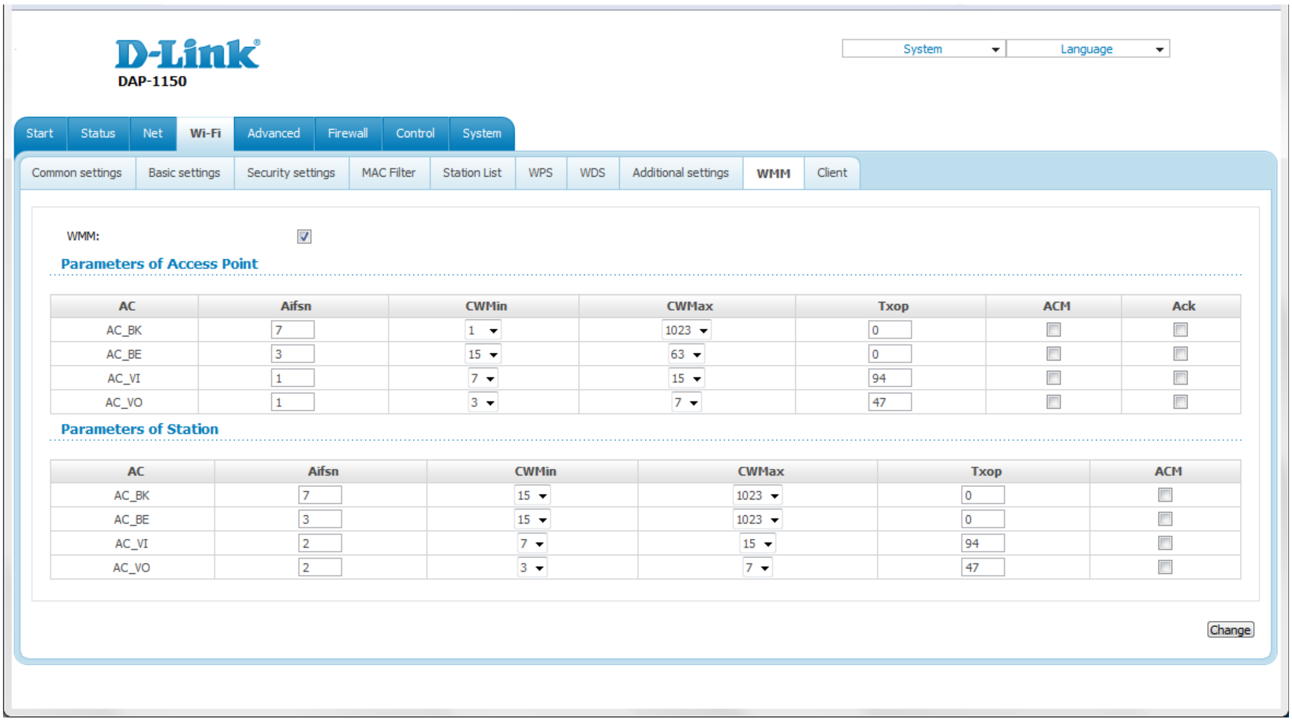
When you have configured the parameters, click the **Change** button.

## 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.



WMM: ☑

**Parameters of Access Point**

| AC | Aifsn | CWMin | CWMax | Txop | ACM | Ack |
|---|---|---|---|---|---|---|
| AC_BK | 7 | 1 | 1023 | 0 | □ | □ |
| AC_BE | 3 | 15 | 63 | 0 | □ | □ |
| AC_VI | 1 | 7 | 15 | 94 | □ | □ |
| AC_VO | 1 | 3 | 7 | 47 | □ | □ |

**Parameters of Station**

| AC | Aifsn | CWMin | CWMax | Txop | ACM |
|---|---|---|---|---|---|
| AC_BK | 7 | 15 | 1023 | 0 | □ |
| AC_BE | 3 | 15 | 1023 | 0 | □ |
| AC_VI | 2 | 7 | 15 | 94 | □ |
| AC_VO | 2 | 3 | 7 | 47 | □ |

*Figure 125. 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** | *Arbitrary Inter-Frame Space Number*. This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority. |
| **CWMin/CWMax** | *Contention Window Minimum/Contention Window Maximum*. 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** | *Transmission Opportunity*. The higher the value, the higher is the Access Category priority. |
| **ACM** | *Admission Control Mandatory*.<br>If selected, prevents from using the relevant Access Category. |
| **Ack** | *Acknowledgment*. Answering response requests while transmitting. Displayed only in the **Parameters of Access Point** section.<br>If not selected, the access point answers requests.<br>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-1150 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-1150 and the WISP access point. Other parameters of the wireless network of DAP-1150 do not depend upon the settings of the WISP access point.

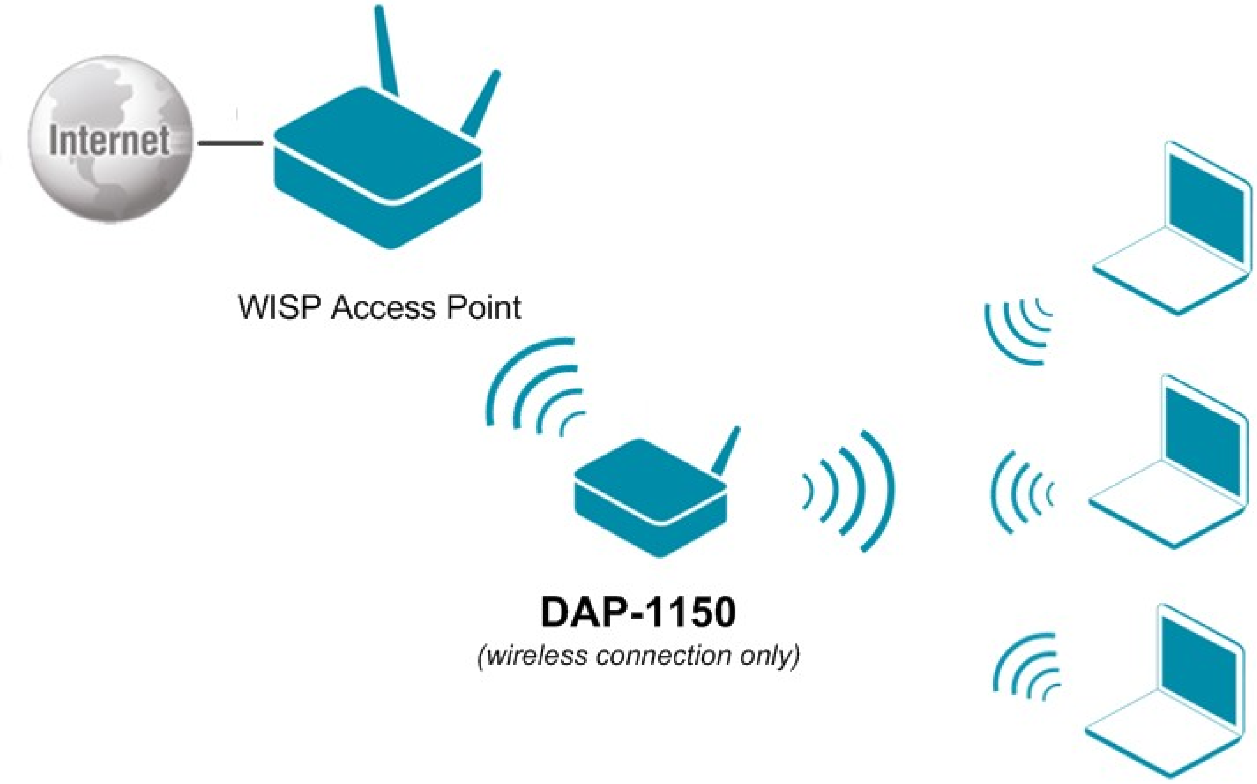
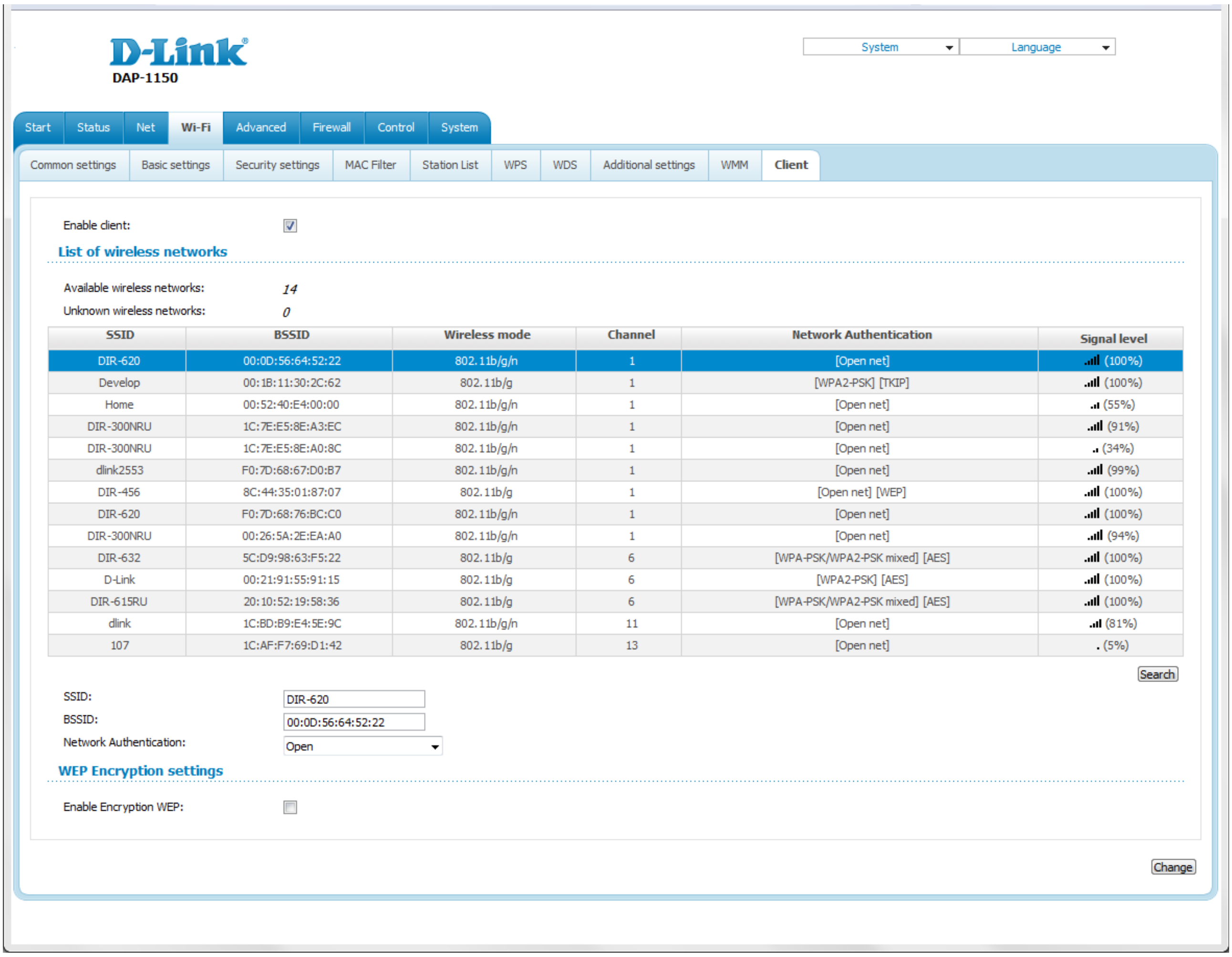


*Figure 126. Connecting DAP-1150 in the router mode as a client.*

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



Enable client: ☑

List of wireless networks

Available wireless networks: 14

Unknown wireless networks: 0

| SSID | BSSID | Wireless mode | Channel | Network Authentication | Signal level |
|---|---|---|---|---|---|
| DIR-620 | 00:0D:56:64:52:22 | 802.11b/g/n | 1 | [Open net] | (100%) |
| Develop | 00:1B:11:30:2C:62 | 802.11b/g | 1 | [WPA2-PSK] [TKIP] | (100%) |
| Home | 00:52:40:E4:00:00 | 802.11b/g/n | 1 | [Open net] | (55%) |
| DIR-300NRU | 1C:7E:E5:8E:A3:EC | 802.11b/g/n | 1 | [Open net] | (91%) |
| DIR-300NRU | 1C:7E:E5:8E:A0:8C | 802.11b/g/n | 1 | [Open net] | (34%) |
| dlink2553 | F0:7D:68:67:D0:B7 | 802.11b/g/n | 1 | [Open net] | (99%) |
| DIR-456 | 8C:44:35:01:87:07 | 802.11b/g | 1 | [Open net] [WEP] | (100%) |
| DIR-620 | F0:7D:68:76:BC:C0 | 802.11b/g/n | 1 | [Open net] | (100%) |
| DIR-300NRU | 00:26:5A:2E:EA:A0 | 802.11b/g/n | 1 | [Open net] | (94%) |
| DIR-632 | 5C:D9:98:63:F5:22 | 802.11b/g | 6 | [WPA-PSK/WPA2-PSK mixed] [AES] | (100%) |
| D-Link | 00:21:91:55:91:15 | 802.11b/g | 6 | [WPA2-PSK] [AES] | (100%) |
| DIR-615RU | 20:10:52:19:58:36 | 802.11b/g | 6 | [WPA-PSK/WPA2-PSK mixed] [AES] | (100%) |
| dlink | 1C:BD:B9:E4:5E:9C | 802.11b/g/n | 11 | [Open net] | (81%) |
| 107 | 1C:AF:F7:69:D1:42 | 802.11b/g | 13 | [Open net] | (5%) |

SSID: DIR-620

BSSID: 00:0D:56:64:52:22

Network Authentication: Open

WEP Encryption settings

Enable Encryption WEP: □

*Figure 127. 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-1150 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*

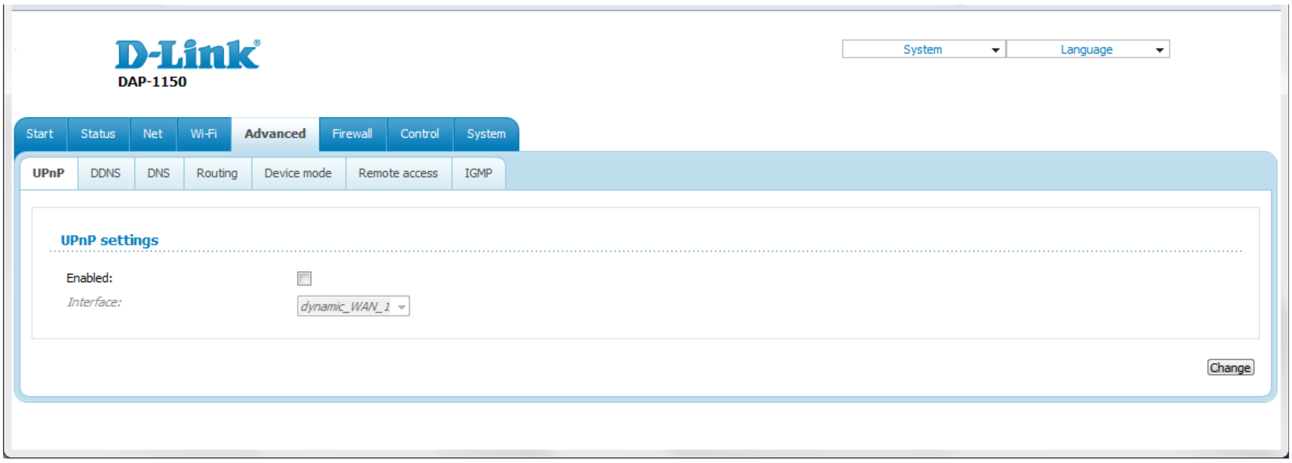
In this menu you can configure advanced settings of the access point switched to the router mode:

- enable the UPnP function
- configure a DDNS service
- add name servers
- define static routes
- switch the device to the other mode
- 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 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.



UPnP settings

Enabled: □

*Interface:* dynamic_WAN_1

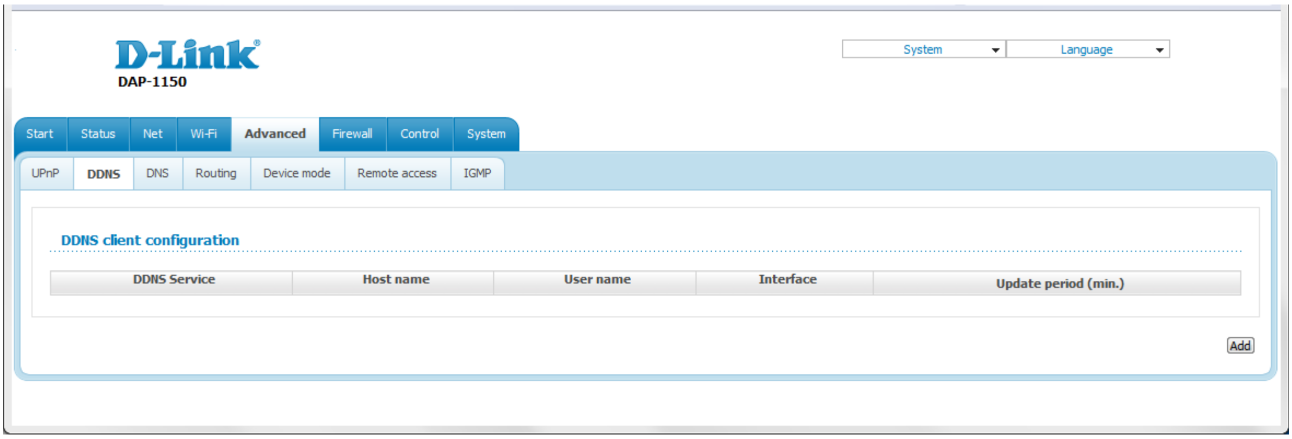
*Figure 128. The **Advanced / UPnP** page.*

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

If you want to enable the UPnP function in the access point, select the **Enabled** checkbox, select an interface for which the device's parameters will be automatically configured from the **Interface** drop-down list, 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.

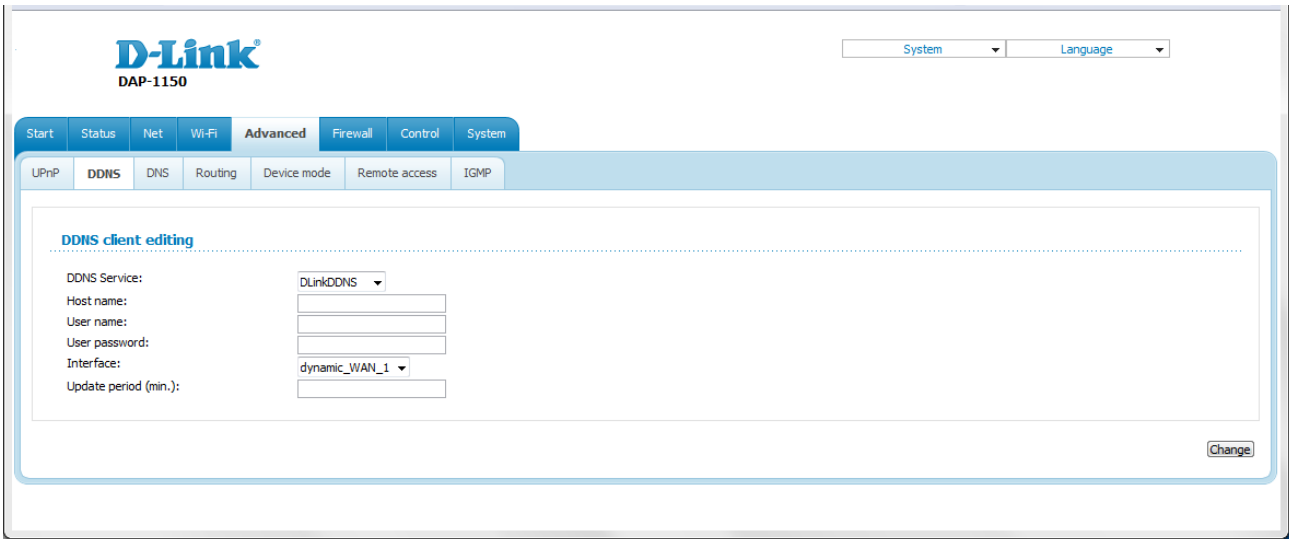


DDNS client configuration

| DDNS Service | Host name | User name | Interface | Update period (min.) |
|---|---|---|---|---|

*Figure 129. The* ***Advanced / DDNS*** *page.*

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



DDNS client editing

DDNS Service: DLinkDDNS
Host name:
User name:
User password:
Interface: dynamic_WAN_1
Update period (min.):

*Figure 130. The page for adding a 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. |

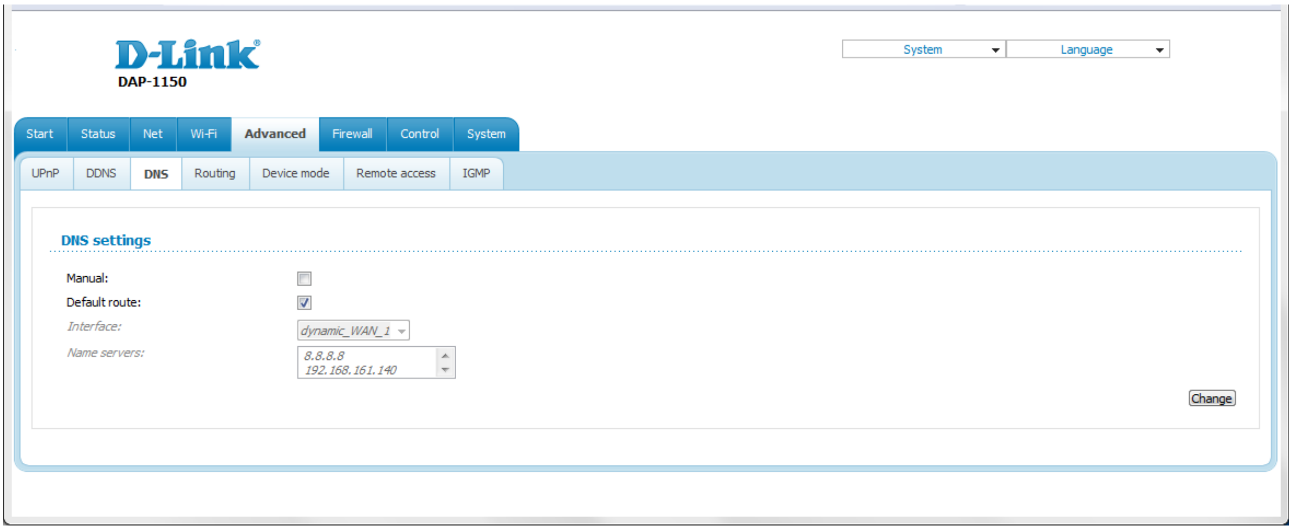
Click the **Change** button.

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.



DNS settings

Manual: □

Default route: ☑

*Interface:* dynamic_WAN_1

*Name servers:*
8.8.8.8
192.168.161.140

*Figure 131. 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.

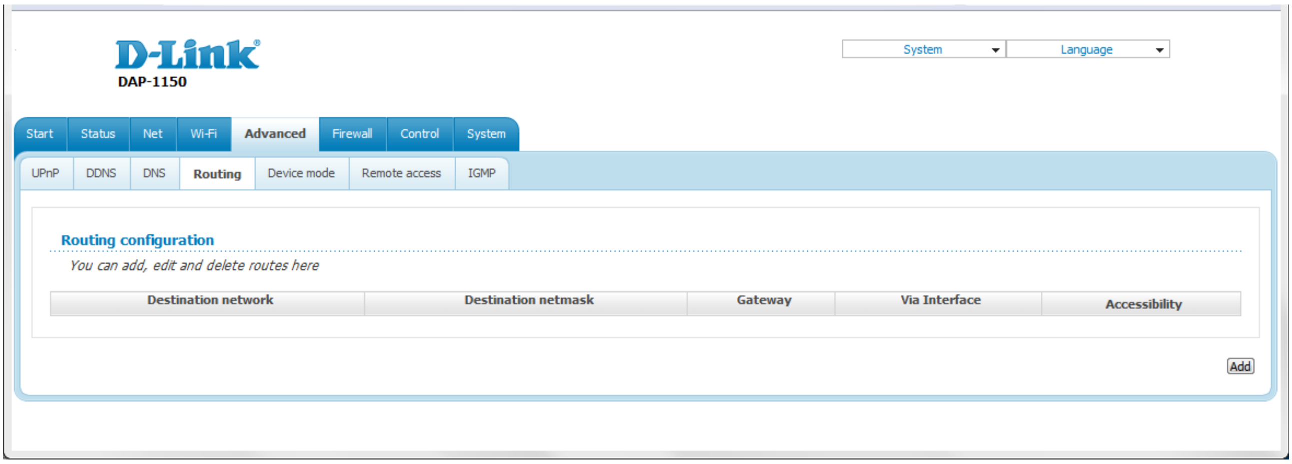
If you want to configure automatic obtainment of DNS servers addresses, deselect the **Manual** checkbox, select a WAN connection which will be used to obtain addresses of DNS servers automatically from the **Interface** drop-down list or select the **Default route** checkbox, so that the access point 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.



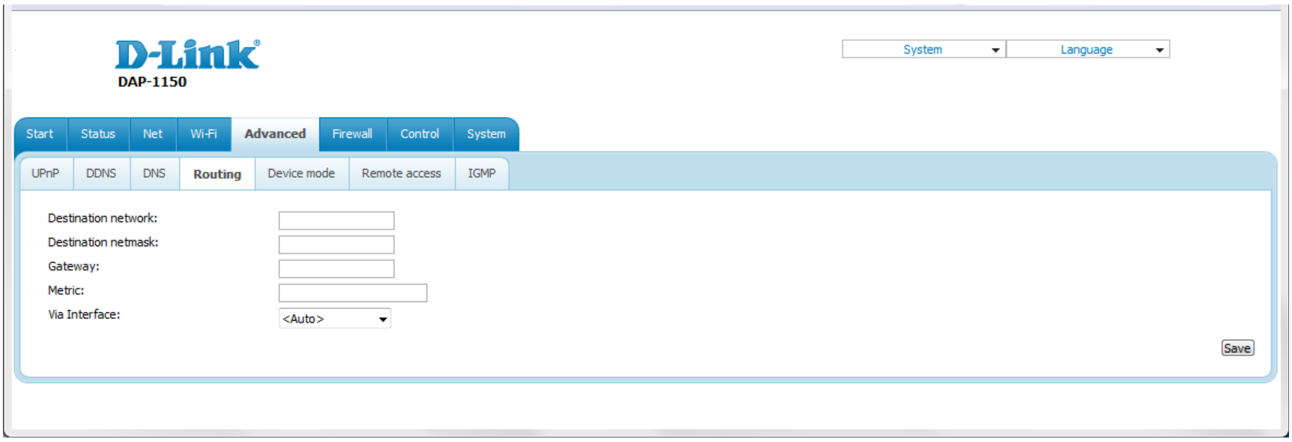
Routing configuration

You can add, edit and delete routes here

| Destination network | Destination netmask | Gateway | Via Interface | Accessibility |
|---|---|---|---|---|

*Figure 132. The **Advanced / Routing** page.*

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



Destination network:
Destination netmask:
Gateway:
Metric:
Via Interface: <Auto>

*Figure 133. 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 filed 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. *Optional*. |
| **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. |

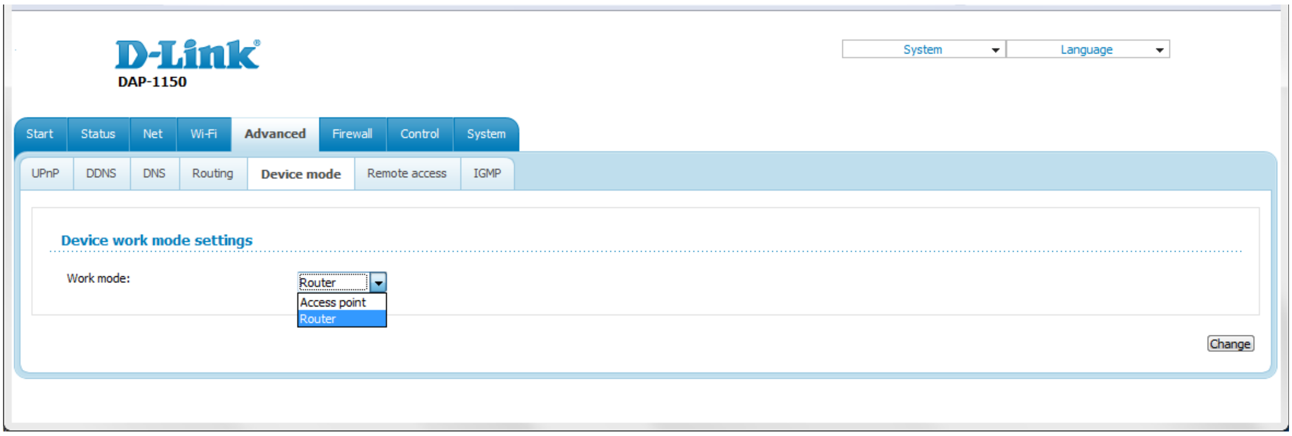
Click the **Save** button.

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.

## Device mode

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



Device work mode settings

Work mode: Router

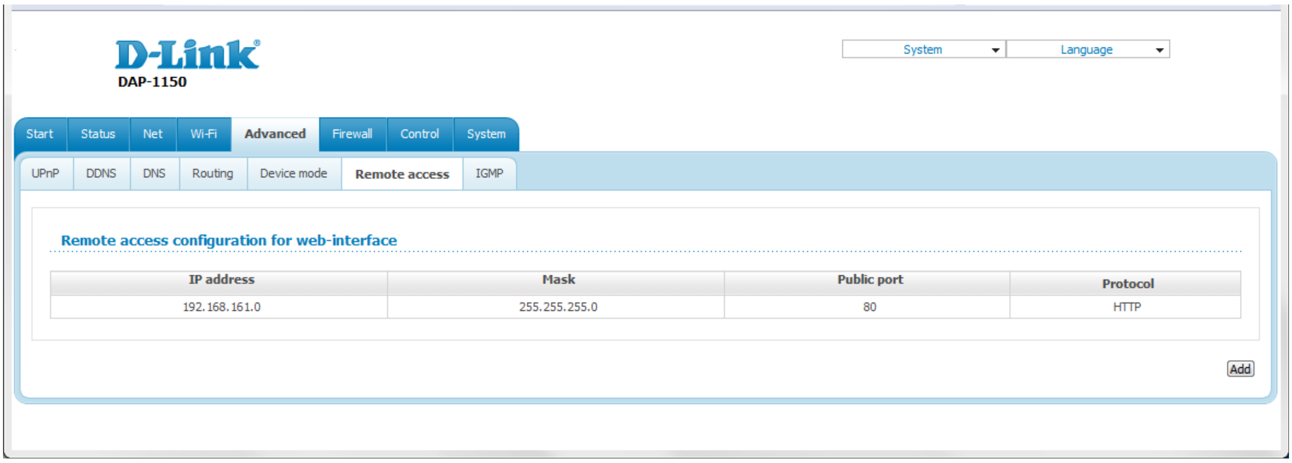
Access point
Router

*Figure 134. 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. Then select the **Save&Reboot** value from the top-page menu displayed when the mouse pointer is over the **System** caption and wait until the device is rebooted.

## 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.

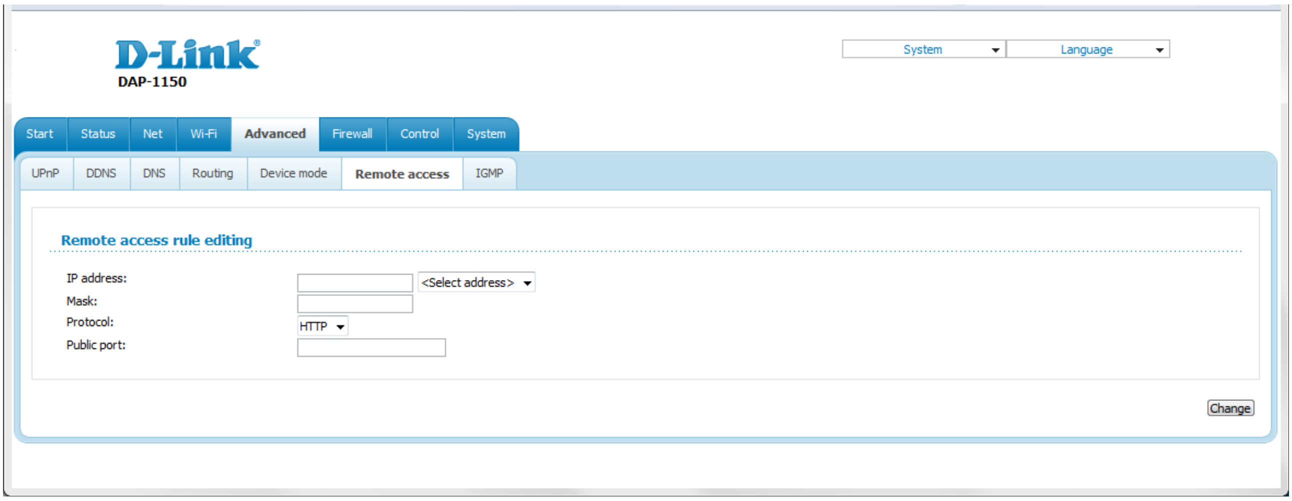


Remote access configuration for web-interface

| IP address | Mask | Public port | Protocol |
|---|---|---|---|
| 192.168.161.0 | 255.255.255.0 | 80 | HTTP |

*Figure 135. The **Advanced / Remote access** page.*

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



Remote access rule editing

IP address: <Select address>
Mask:
Protocol: HTTP
Public port:

*Figure 136. 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. |
| **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.

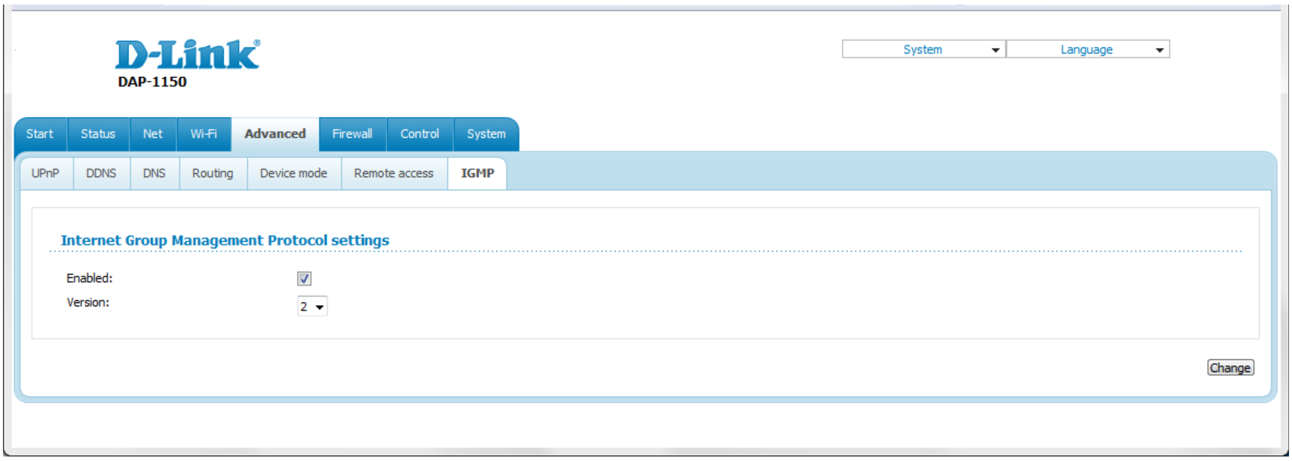
To edit a rule for remote access, click the relevant link. On the opened page, change the needed parameters and click the **Change** button.

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.



Internet Group Management Protocol settings

Enabled: ☑

Version: 2

*Figure 137. 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.

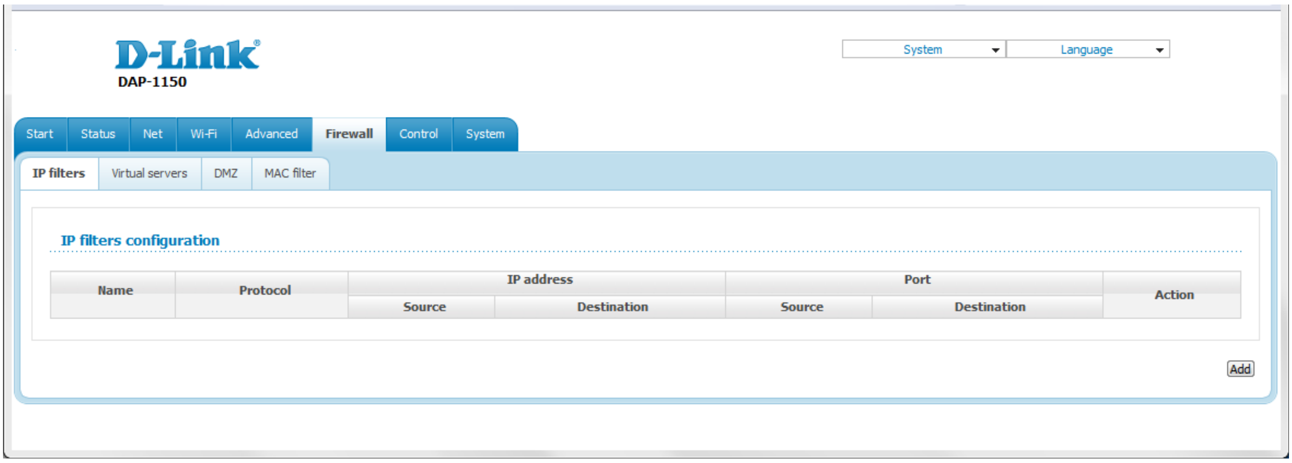
## *Firewall*

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.

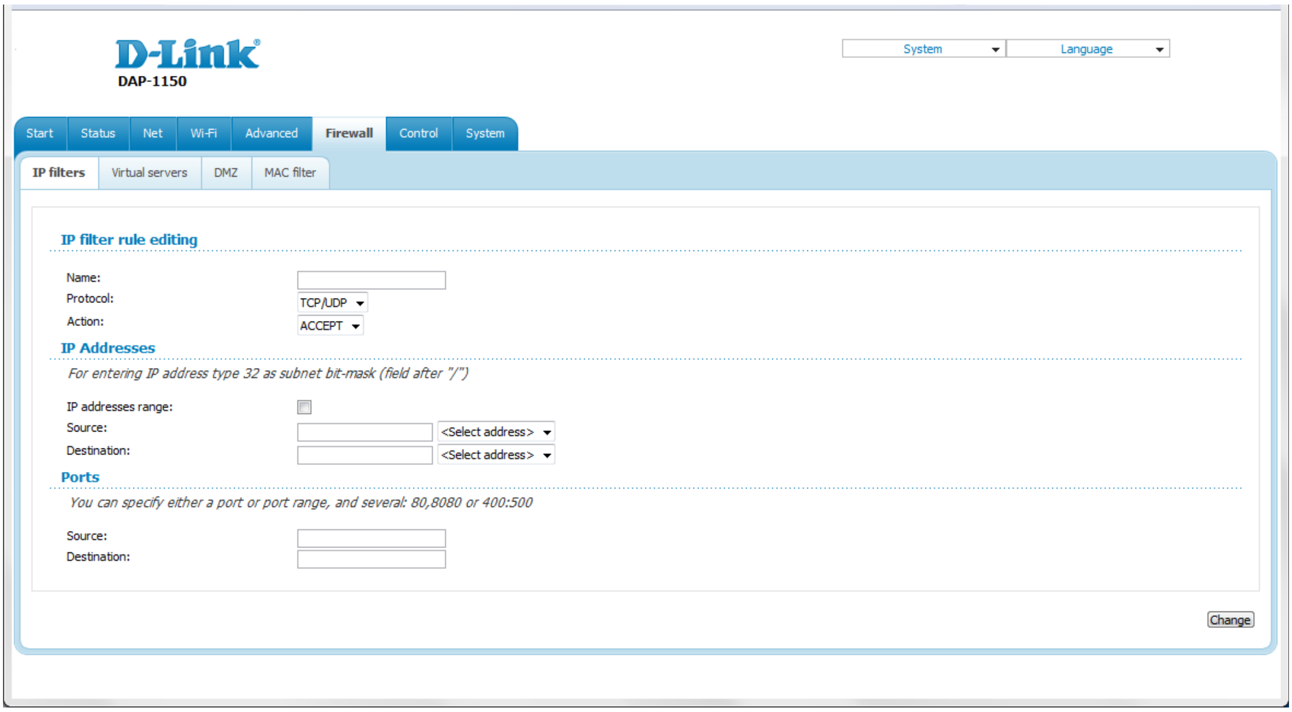


IP filters configuration

| Name | Protocol | IP address | | Port | | Action |
|---|---|---|---|---|---|---|
| | | Source | Destination | Source | Destination | |

*Figure 138. The **Firewall / IP filters** page.*

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



IP filter rule editing

Name:

Protocol: TCP/UDP

Action: ACCEPT

IP Addresses

*For entering IP address type 32 as subnet bit-mask (field after "/")*

IP addresses range: □

Source: <Select address>

Destination: <Select address>

Ports

*You can specify either a port or port range, and several: 80,8080 or 400:500*

Source:

Destination:

*Figure 139. 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.<br>**ACCEPT**: Allows packet transmission in accordance with the criteria specified by the rule.<br>**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** | The source host/subnet IP address.<br>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.<br>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`.<br>To choose a device connected to the access point's LAN at the moment, select the relevant IP address from the drop-down list located to the right of the field (the field will be filled in automatically). |
| **Destination** | The destination host/subnet IP address.<br>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.<br>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`.<br>To choose a device connected to the access point's LAN at the moment, select the relevant IP address from the drop-down list located to the right of the field (the field will be filled in automatically). |
| **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. |

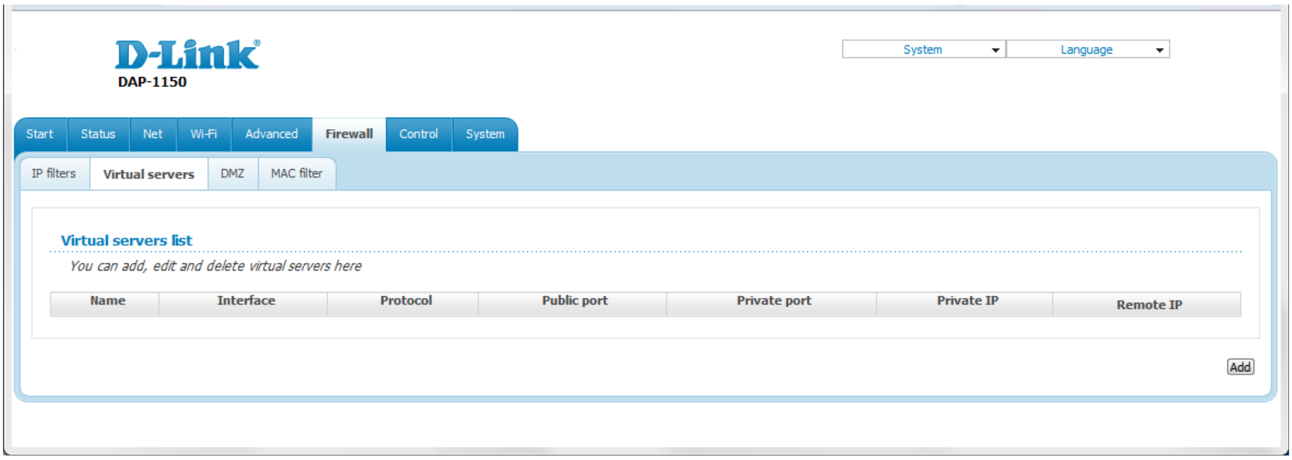
Click the **Change** button.

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.



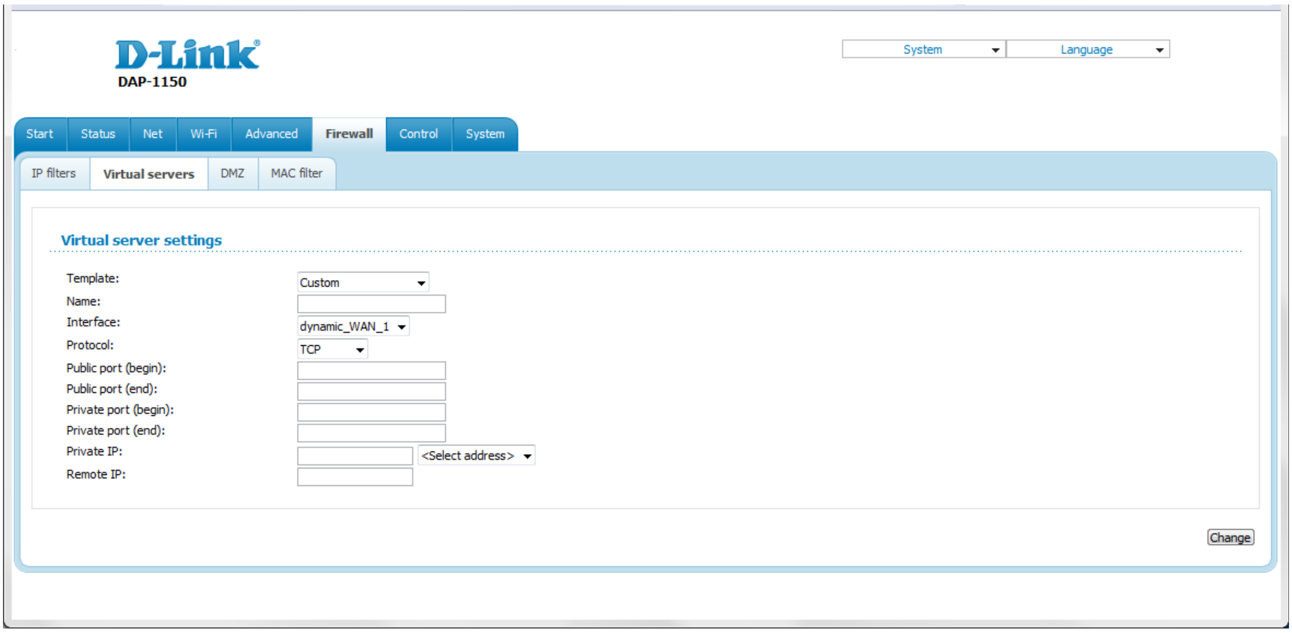
Virtual servers list

*You can add, edit and delete virtual servers here*

| Name | Interface | Protocol | Public port | Private port | Private IP | Remote IP |
|---|---|---|---|---|---|---|

*Figure 140. The **Firewall / Virtual servers** page.*

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



Virtual server settings

| | |
|---|---|
| Template: | Custom |
| Name: | |
| Interface: | dynamic_WAN_1 |
| Protocol: | TCP |
| Public port (begin): | |
| Public port (end): | |
| Private port (begin): | |
| Private port (end): | |
| Private IP: | <Select address> |
| Remote IP: | |

*Figure 141. 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)/**<br>**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)/**<br>**Private port (end)** | A port of the IP address specified in the **Private IP** field to which traffic is directed from the **Public port**. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the **Private port (begin)** field and leave the **Private port (end)** field blank. |
| **Private IP** | The IP address of the server from the local area network. To choose a device connected to the access point's LAN at the moment, select the relevant value from the drop-down list located to the right of the **Private IP** field (the field will be filled in automatically). |
| **Remote IP** | The IP address of the server from the external network. |

Click the **Change** button.

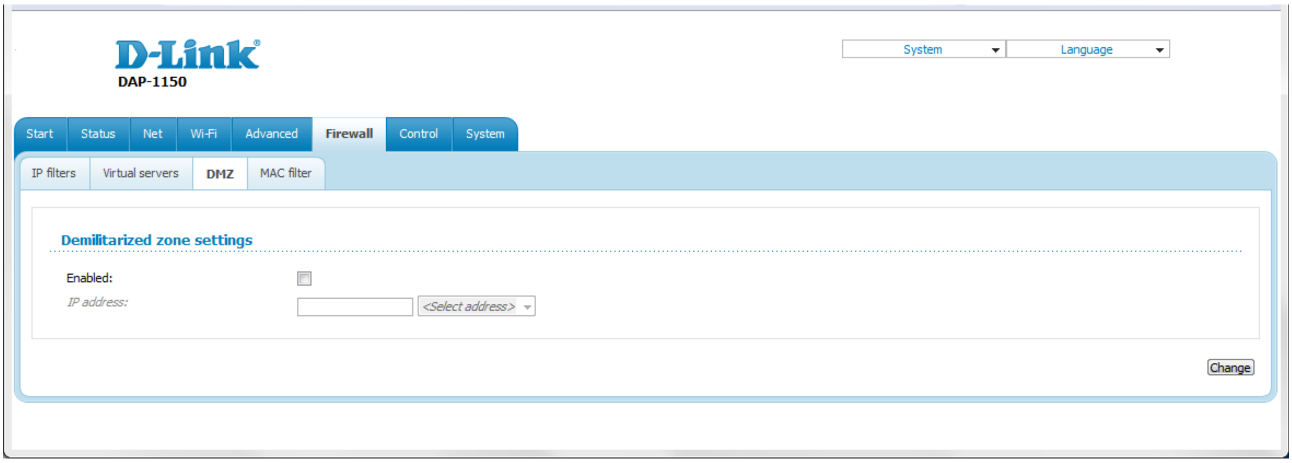
To edit the parameters of an existing server, follow the link with the name of the server. On the opened page, change the needed parameters and click the **Change** button.

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.



Demilitarized zone settings

Enabled: □

IP address: <Select address>

*Figure 142. The **Firewall / DMZ** page.*

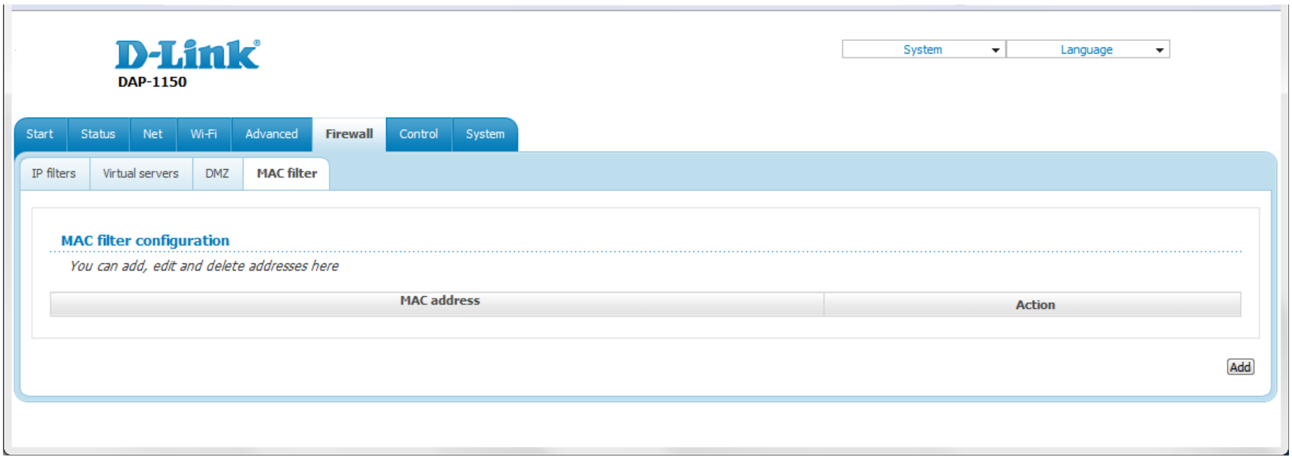
To enable the DMZ, select the **Enabled** checkbox, enter the IP address of a host from your network in the **IP address** field. To choose a device connected to the access point's LAN at the moment, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically) 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.



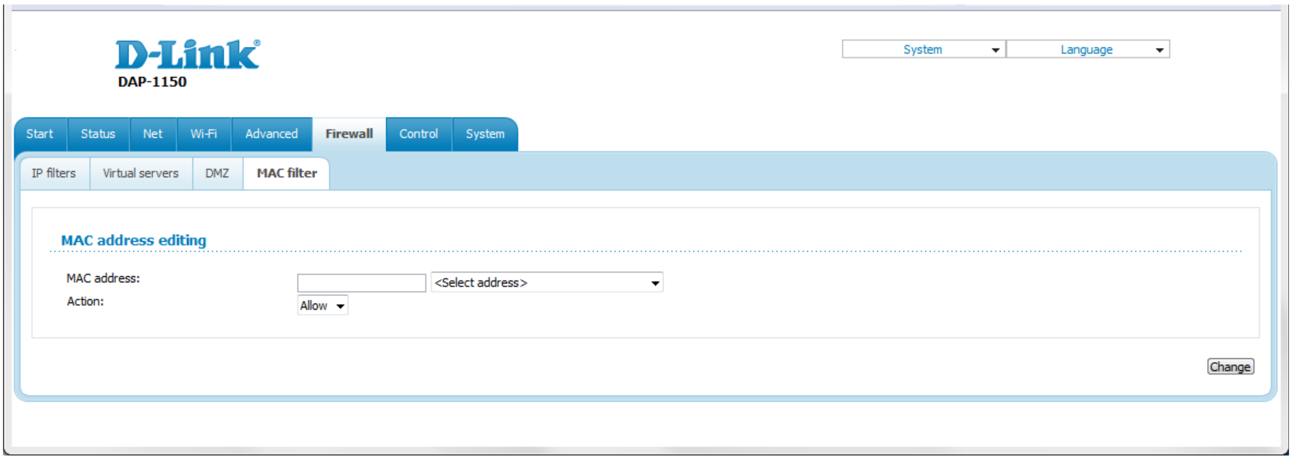
MAC filter configuration

*You can add, edit and delete addresses here*

| MAC address | Action |
|---|---|

*Figure 143. The **Firewall / MAC filter** page.*

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



MAC address editing

MAC address: <Select address>

Action: Allow

*Figure 144. 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 located to the right of the field (the field will be filled in automatically). Then select the **Deny** value from the **Action** drop-down list and click the **Change** button.

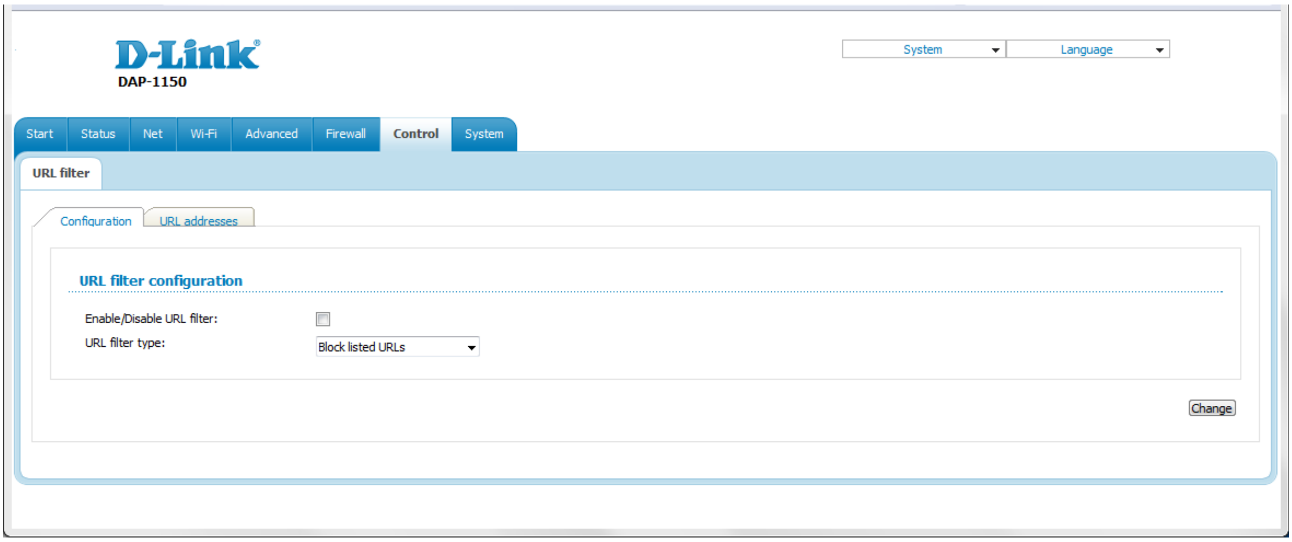
To remove an address from the list of MAC addresses for filtering, select the line with the relevant MAC address. On the opened page, click the **Delete** button.

# *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.



URL filter configuration

Enable/Disable URL filter: □

URL filter type: Block listed URLs

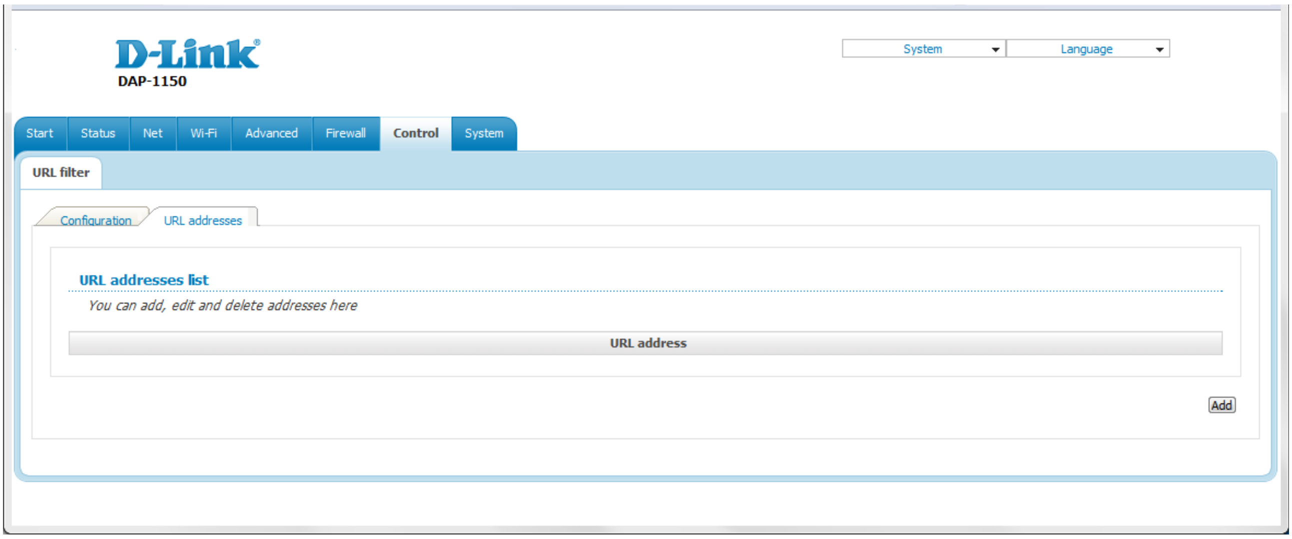
*Figure 145. The **Control / URL filter** page. The **Configuration** tab.*

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.



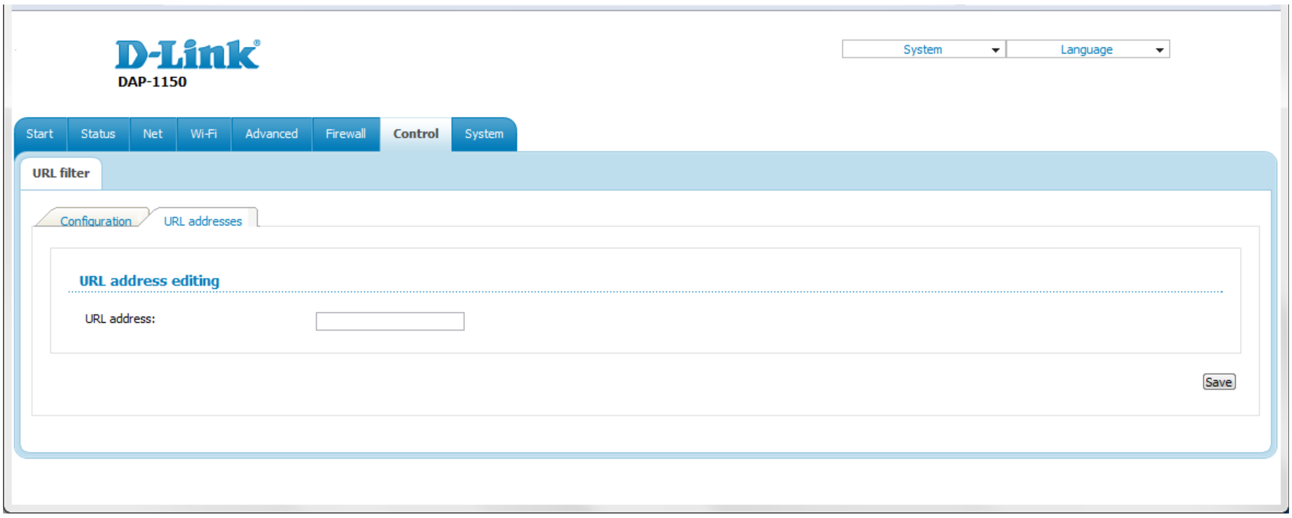
URL addresses list

*You can add, edit and delete addresses here*

| URL address |
|---|

*Figure 146. The **Control / URL filter** page. The **URL addresses** tab.*

On the opened page, specify the needed parameters.



URL address editing

URL address:

*Figure 147. 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*

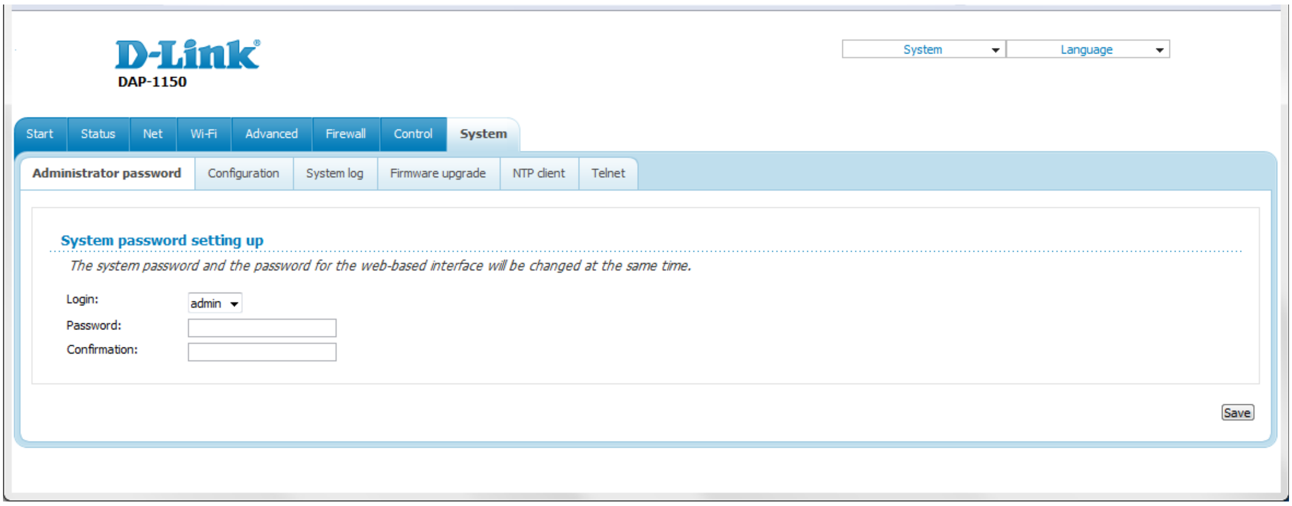
In this menu you can do the following:

- 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
- allow or forbid access to the access point via TELNET.

### 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.



System password setting up

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

Login: admin
Password:
Confirmation:

*Figure 148. 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.

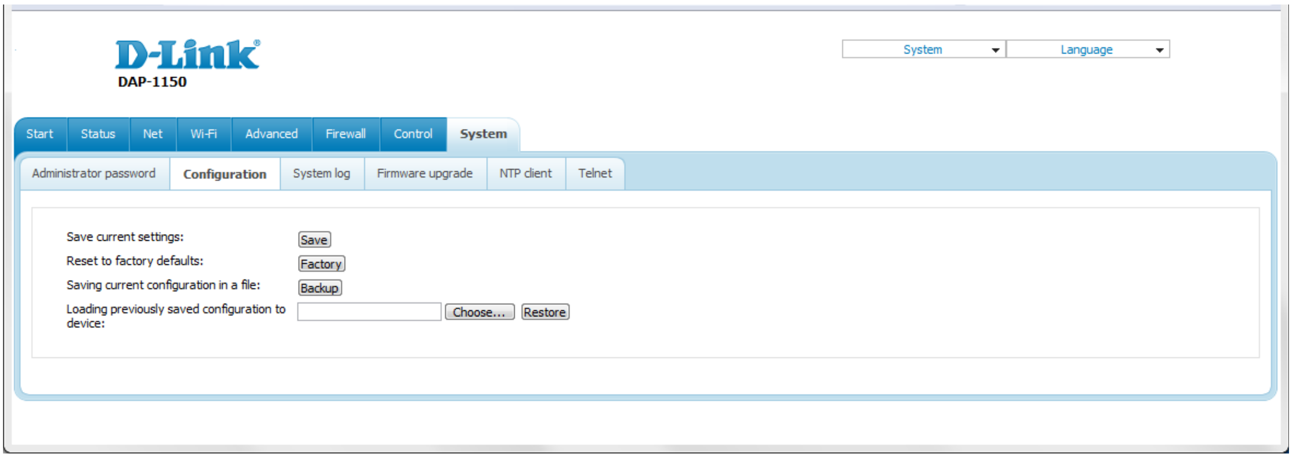


*Figure 149. The* ***System / Configuration*** *page.*

The following buttons are available on the page:

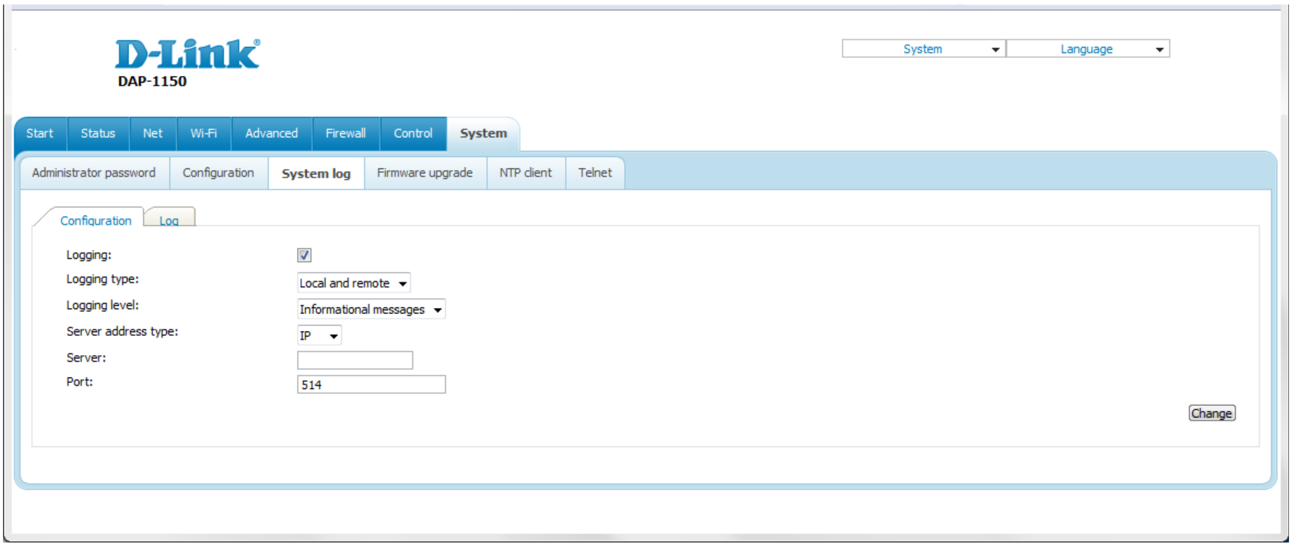
| Control | Description |
|---|---|
| **Save** | Click the button to save settings to the non-volatile memory. Please, save settings every time you change the device's parameters. Otherwise the changes will be lost upon hardware reboot of the access point. |
| **Factory** | Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button (see the ***Saving and Restoring Settings*** section, page 29). |
| **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.



Logging: ☑
Logging type: Local and remote
Logging level: Informational messages
Server address type: IP
Server:
Port: 514

*Figure 150. The **System / System log** page. The **Configuration** tab.*

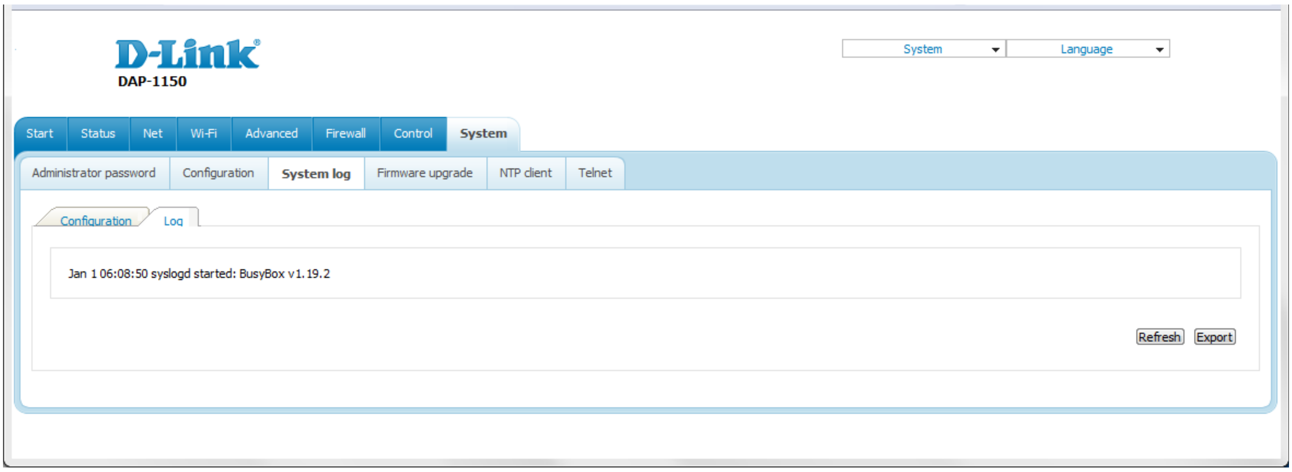
To enable logging of the system events, select the **Logging** checkbox on the **Configuration** tab. Then specify the needed parameters.

| Control | Description |
|---|---|
| **Logging type** | Select a type of logging from the drop-down list.<br>• **Local**: the system log is stored in the device's memory (and displayed on the **Log** tab). When this value is selected, the **Server address type**, **Server**, and **Port** fields are not displayed.<br>• **Remote**: the system log is sent to the remote host specified in the **Server** field.<br>• **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 address type** | From the drop-down list, select the **IP** value to specify an IP address of a host from the local or global network, or the **URL** value to specify a URL address of a remote server. |
| **Server** | The IP or URL address of the host from the local or global network, to which the system log will be sent. |
| **Port** | A port of the host specified in the **Server** field. By default, the value **514** is specified. |

After specifying the needed parameters, click the **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.



```
Jan 1 06:08:50 syslogd started: BusyBox v1.19.2
```

*Figure 151. 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 (available only in the access point mode).

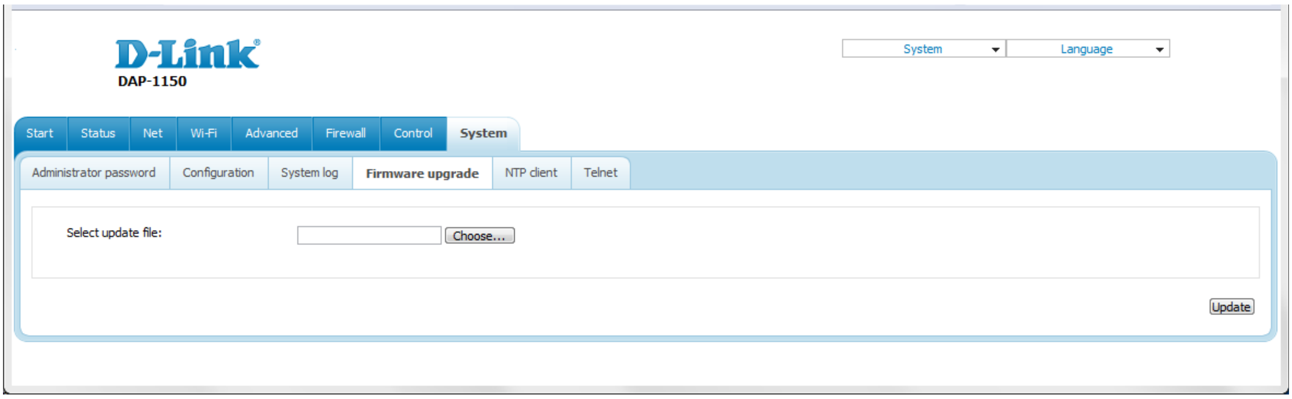


*Figure 152. The **System / Firmware upgrade** page.*

The current version of the device's firmware is displayed in the **Firmware version** field on the **Start** page. If you need to install a newer version of the firmware, follow the next steps:

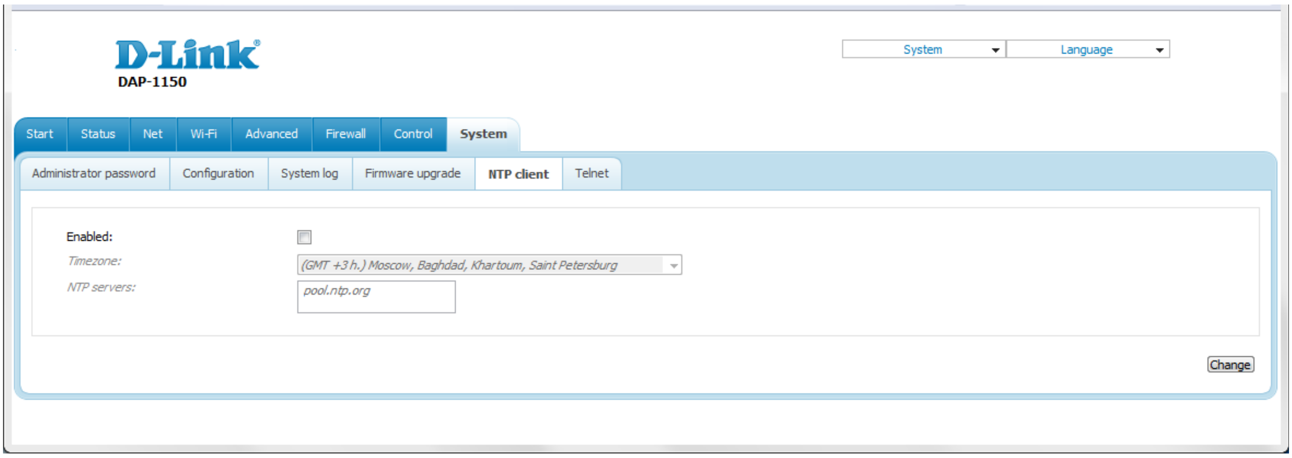
**!** Attention! Do not turn off the access point before the firmware upgrade is completed. This may cause the device breakdown.

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.
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**).

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

## NTP Client

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



Enabled: □
Timezone: (GMT +3 h.) Moscow, Baghdad, Khartoum, Saint Petersburg
NTP servers: pool.ntp.org

*Figure 153. The **System / NTP client** page.*

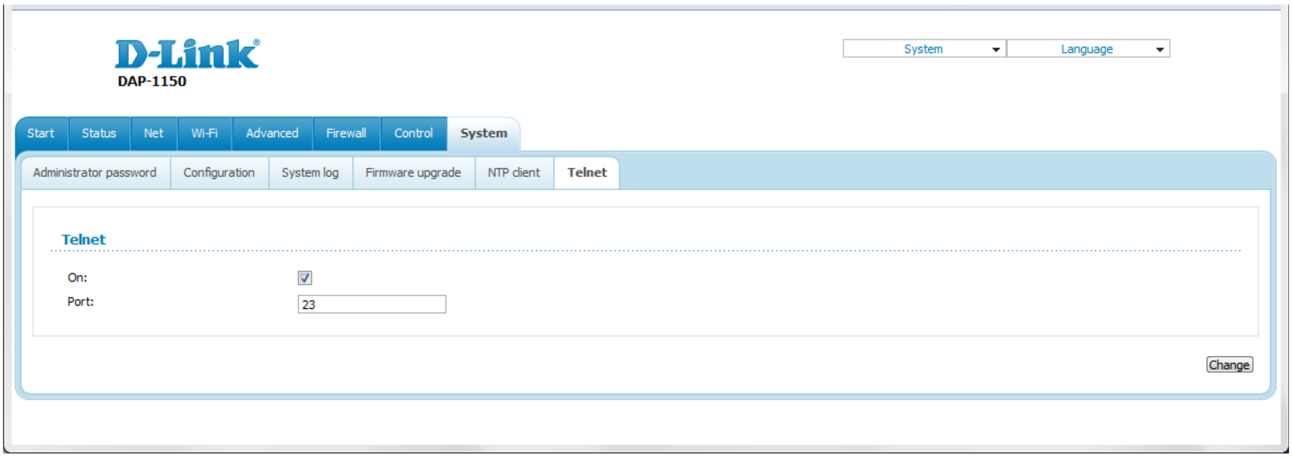
To enable automatic synchronization with a time server:

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.

## 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.



Telnet

On: ☑

Port: 23

*Figure 154. 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.

# 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-1150 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-1150 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 in 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 |