



## **DIR-300N**

### **Wireless Router with Built-in 4-port Switch**

# Contents

<b>Chapter 1. Introduction</b> .....	<b>4</b>
<b>Contents and Audience</b> .....	<b>4</b>
<b>Conventions</b> .....	<b>4</b>
<b>Document Structure</b> .....	<b>4</b>
<b>Chapter 2. Overview</b> .....	<b>5</b>
<b>General Information</b> .....	<b>5</b>
<b>Specifications</b> .....	<b>6</b>
<b>Product Appearance</b> .....	<b>11</b>
Front Panel and Right Side Panel.....	11
Back Panel.....	12
<b>Delivery Package</b> .....	<b>13</b>
<b>Chapter 3. Installation and Connection</b> .....	<b>14</b>
<b>Before You Begin</b> .....	<b>14</b>
<b>Connecting to PC (in OS Windows XP)</b> .....	<b>15</b>
PC with Ethernet Adapter.....	15
Obtaining IP Address Automatically.....	15
PC with Wi-Fi Adapter.....	18
Configuring Wi-Fi Adapter.....	18
<b>Connecting to Web-based Interface</b> .....	<b>19</b>
<b>Saving and Restoring Settings</b> .....	<b>21</b>
<b>Chapter 4. Configuring via Web-based Interface</b> .....	<b>23</b>
<b>Status</b> .....	<b>23</b>
Network Statistics.....	23
Routing Table.....	24
LAN Clients.....	25
<b>Net</b> .....	<b>26</b>
Connections.....	26
<i>Editing Local Interface Parameters</i> .....	27
<i>Creating PPPoE WAN Connection</i> .....	31
<i>Creating IPoE WAN Connection</i> .....	35
<i>Creating PPTP or L2TP WAN Connection</i> .....	38
<b>Wi-Fi</b> .....	<b>41</b>
Common settings.....	41
Basic Settings.....	42
Security Settings.....	44
MAC Filter.....	51
Station List.....	53
WPS.....	54
<i>Using WPS Function via Web-based Interface</i> .....	56
<i>Using WPS Function without Web-based Interface</i> .....	56
WDS.....	57

Additional Settings.....	59
WMM.....	61
Client.....	63
<b>Advanced.....</b>	<b>65</b>
VLAN.....	65
UPnP.....	68
DDNS.....	69
DNS.....	71
Routing.....	72
Remote Access.....	74
IGMP.....	76
<b>Firewall.....</b>	<b>77</b>
IP Filters.....	77
Virtual Servers.....	79
DMZ.....	81
MAC Filter.....	82
<b>Control.....</b>	<b>83</b>
URL Filter.....	83
<b>System.....</b>	<b>84</b>
Administrator Password.....	84
Configuration.....	85
System Log.....	86
Firmware Upgrade.....	88
NTP Client.....	89
<b>Chapter 5. Operation Guidelines.....</b>	<b>90</b>
<b>Safety Instructions.....</b>	<b>90</b>
<b>Wireless Installation Considerations.....</b>	<b>90</b>
<b>Connecting to Cable or DSL Modem.....</b>	<b>91</b>
<b>Chapter 6. Abbreviations and Acronyms.....</b>	<b>92</b>


# CHAPTER 1. INTRODUCTION

## Contents and Audience

This manual describes the router DIR-300NRU and explains how to configure and operate it.

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

## Conventions

Example	Description
text	The body text of the manual.
<i>Before You Begin</i>	A reference to a chapter or section of this manual.
<i>“Quick Installation Guide”</i>	A reference to a document.
<b>Change</b>	A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.).
192.168.0.1	Data that you should enter in the specified field.
 <u>Information</u>	An important note.

## Document Structure

*Chapter 1* describes the purpose and structure of the document.

*Chapter 2* gives an overview of the router's hardware and software features, describes its appearance and the package contents.

*Chapter 3* explains how to install the router DIR-300NRU and configure a PC in order to access its web-based interface.

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

*Chapter 5* includes safety instructions and tips for networking and connecting additional equipment.

*Chapter 6* introduces abbreviations and acronyms used in this manual.

## CHAPTER 2. OVERVIEW

### ***General Information***

The DIR-300NRU device is a wireless router with a built-in 4-port switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

You are able to connect the wireless router DIR-300NRU to a cable or DSL modem or to a private Ethernet line and use a high-speed Internet connection to successfully fulfill a wide range of professional tasks. The built-in 4-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network.

Using the DIR-300NRU device, you are able to quickly create a wireless network at home or in your office, which lets your relatives or employees connect to your wireless network virtually anywhere (within the operational range of your wireless network). The router is designed to work with 802.11n wireless devices (at the rate up to 150Mbps) and supports 802.11b/g wireless devices.

The router supports multiple functions for the wireless interface: several security standards (WEP, WPA/WPA2, IEEE 802.1X), MAC address filtering, different operation modes (access point, client, bridge), WPS, WMM.

The wireless router DIR-300NRU 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 wireless router DIR-300NRU via the user-friendly web-based interface (the interface is available in several languages).

## ***Specifications***

### **WAN Interface:**

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

### **LAN Interface:**

- 4 10/100BASE-TX Ethernet ports.

### **WLAN Interface:**

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

### **Network Functions:**

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

## Wireless Connection:

- WLAN splitting (up to 4 SSIDs)
- Supported security settings:
  - WEP
  - WPA/WPA2 Personal
  - WPA/WPA2 Enterprise
  - IEEE 802.1X
- MAC filter
- Managing connected stations
- PIN and PBC methods of WPS
- WMM (Wi-Fi QoS)
- Advanced settings
- WDS
- Support of client mode.

## Frequency Range:

- 2.4~2.497MHz ISM band.

## Data Rate:

- 802.11b:
  - 11, 5.5, 2, and 1Mbps
- 802.11g:
  - 54, 48, 36, 24, 18, 12, 9, and 6Mbps
- 802.11n:
  - 6.5~150Mbps.

### Transmitter Output Power:

- 802.11b:
  - typical 17dBm (+/-2dB) at 11, 5.5, 2, and 1Mbps at 25 °C
- 802.11g:
  - typical 17dBm (+/-2dB) at 6 to 36Mbps at 25 °C
  - typical 16dBm (+/-2dB) at 48Mbps at 25 °C
  - typical 15dBm (+/-2dB) at 54Mbps at 25 °C
- 802.11n:
  - typical 16dBm (+/-2dB) at MCS0 to MCS2 at 25 °C
  - typical 15dBm (+/-2dB) at MCS3 to MCS4 at 25 °C
  - typical 13dBm (+/-2dB) at MCS5 and MCS7 at 25 °C.

### EIRP (Effective Isotropic Radiated Power)

- 802.11b:
  - 17dBm
- 802.11g:
  - 16dBm
- 802.11n:
  - 19dBm.

### Receiver Sensitivity:

- 802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature):
  - -86dBm at 11Mbps
  - -87dBm at 5.5Mbps
  - -88dBm at 2Mbps
  - -90dBm at 1Mbps



- 802.11g (typical at PER = 10% (1000-byte PDUs) at room temperature):
  - -84dBm at 6Mbps
  - -82dBm at 9Mbps
  - -80dBm at 12Mbps
  - -78dBm at 18Mbps
  - -77dBm at 24Mbps
  - -74dBm at 36Mbps
  - -70dBm at 48Mbps
  - -68dBm at 54Mbps
- 802.11n (typical at PER < 10% (1000-byte PDUs) at room temperature):
  - **HT20:**
    - -93dBm at BPSK, coding rate 1/2 (MCS-0)
    - -90dBm at QPSK, coding rate 1/2 (MCS-1)
    - -88dBm at QPSK, coding rate 3/4 (MCS-2)
    - -85dBm at 16-QAM, coding rate 1/2 (MCS-3)
    - -82dBm at 16-QAM, coding rate 3/4 (MCS-4)
    - -78dBm at 64-QAM, coding rate 2/3 (MCS-5)
    - -77dBm at 64-QAM, coding rate 3/4 (MCS-6)
    - -76dBm at 64-QAM, coding rate 5/6 (MCS-7)
  - **HT40:**
    - -90dBm at BPSK, coding rate 1/2 (MCS-0)
    - -87dBm at QPSK, coding rate 1/2 (MCS-1)
    - -85dBm at QPSK, coding rate 3/4 (MCS-2)
    - -82dBm at 16-QAM, coding rate 1/2 (MCS-3)
    - -79dBm at 16-QAM, coding rate 3/4 (MCS-4)
    - -75dBm at 64-QAM, coding rate 2/3 (MCS-5)
    - -74dBm at 64-QAM, coding rate 3/4 (MCS-6)
    - -73dBm at 64-QAM, coding rate 5/6 (MCS-7).

### **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.

### **LEDs:**

- Power
- Internet
- WLAN
- 4 LAN LEDs
- WPS.

### **Power:**

- External power adapter DC 5V/1A
- Reset to Factory Defaults button.

### **Operating Temperature:**

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

### **Operating Humidity:**

- from 10% to 90% non-condensing.

## Product Appearance

### Front Panel and Right Side Panel

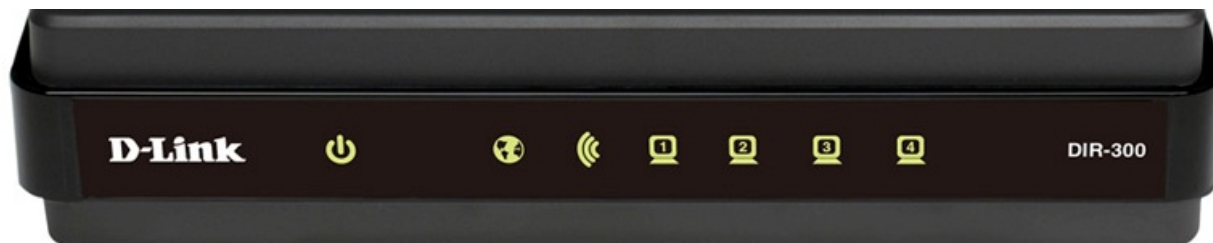






Figure 1. Front panel view.

LED	Mode	Description
 <b>Power</b>	<i>Solid green</i>	The router is powered on.
	<i>No light</i>	The router is powered off.
 <b>Internet</b>	<i>Solid green</i>	The Internet connection is on.
	<i>Blinking green</i>	The WAN interface is active (upstream or downstream traffic).
 <b>WLAN</b>	<i>Solid green</i>	The router's WLAN is on.
	<i>Blinking green</i>	The WLAN interface is active (upstream or downstream traffic).
 <b>LAN 1-4</b>	<i>Solid green</i>	A device (computer) is connected to the relevant port, the connection is on.
	<i>Blinking green</i>	The LAN port is active (upstream or downstream traffic).

The WPS button located on the right side panel of the router is designed to quickly add wireless devices to the router's WLAN. A separate LED is located on the WPS button.

Mode	Description
<i>Blinking blue</i>	Attempting to add a wireless device via the WPS function.
<i>Solid blue</i>	The wireless device is connected to the router's WLAN (lights for several minutes).

## Back Panel



Figure 2. Back panel view.

Port	Description
<b>LAN 1-4</b>	4 Ethernet ports to connect computers or network devices.
<b>INTERNET</b>	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).
<b>5V-1A</b>	Power connector.
<b>RESET</b>	A button to restore the factory default settings. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.

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

## ***Delivery Package***

The following should be included:

- Wireless router DIR-300NRU
- Power adapter 5V/1A
- 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 wireless router DIR-300NRU with a built-in 4-port switch (hereinafter referred to as “the router”) 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 router 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 router.

#### **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 router for all these wireless workstations.

## Connecting to PC (in OS Windows XP)

### PC with Ethernet Adapter

1. Make sure that your PC is powered off.
2. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
3. Connect the power cord to the power connector port on the back panel of the router, 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

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.

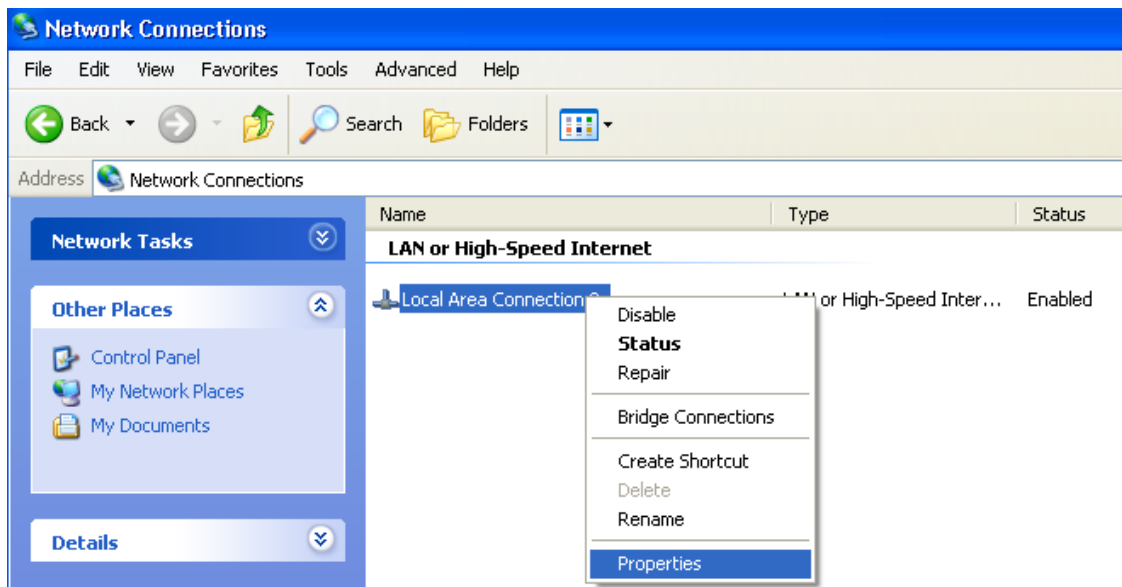


Figure 3. The **Network Connections** window.

3. In the **Local Area Connection Properties** window, on the **General** tab, in the **This connection uses the following items** section, select the **Internet Protocol (TCP/IP)** line. Click the **Properties** button.

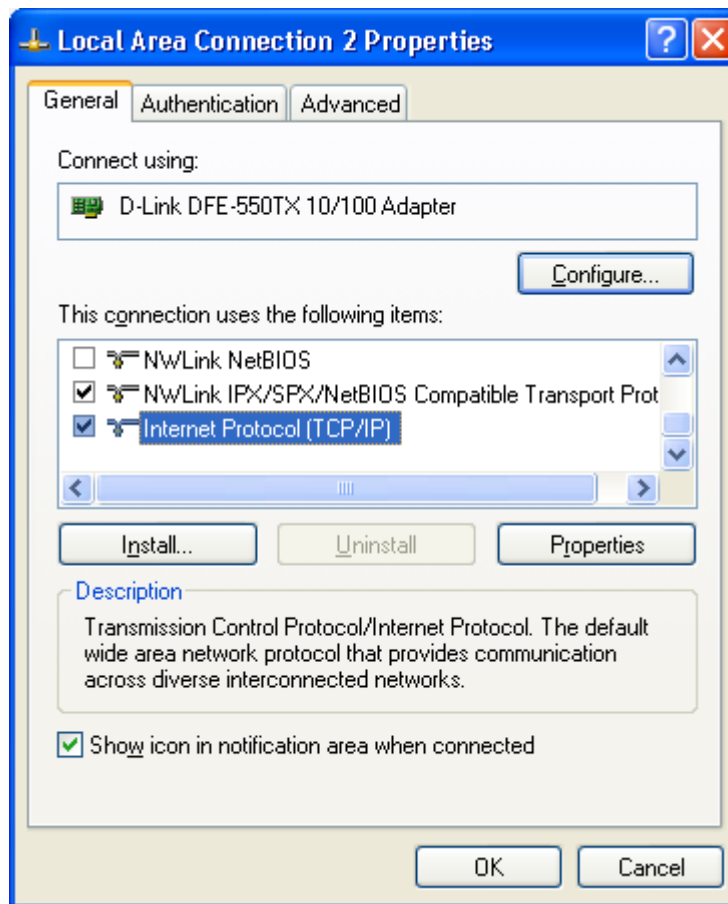


Figure 4. The **Local Area Connection Properties** window.



4. Select the **Obtain an IP address automatically** radio button. Click the **OK** button.

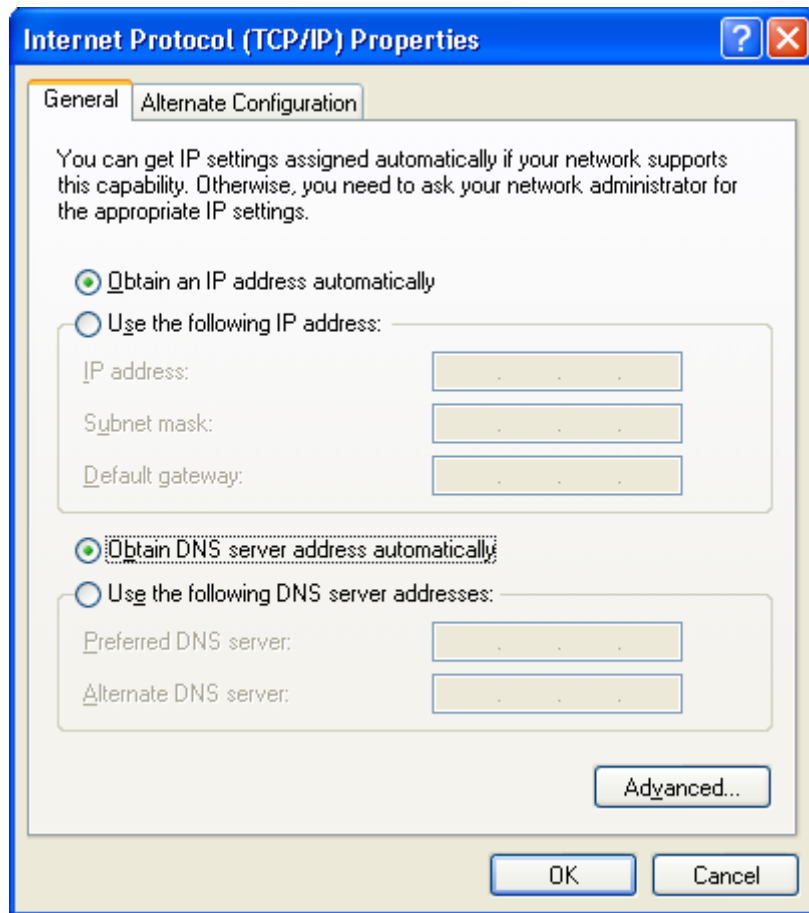


Figure 5. The **Internet Protocol (TCP/IP) Properties** window.

Click the **OK** button. 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 router, 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

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 connection and make sure that your Wi-Fi adapter is on.

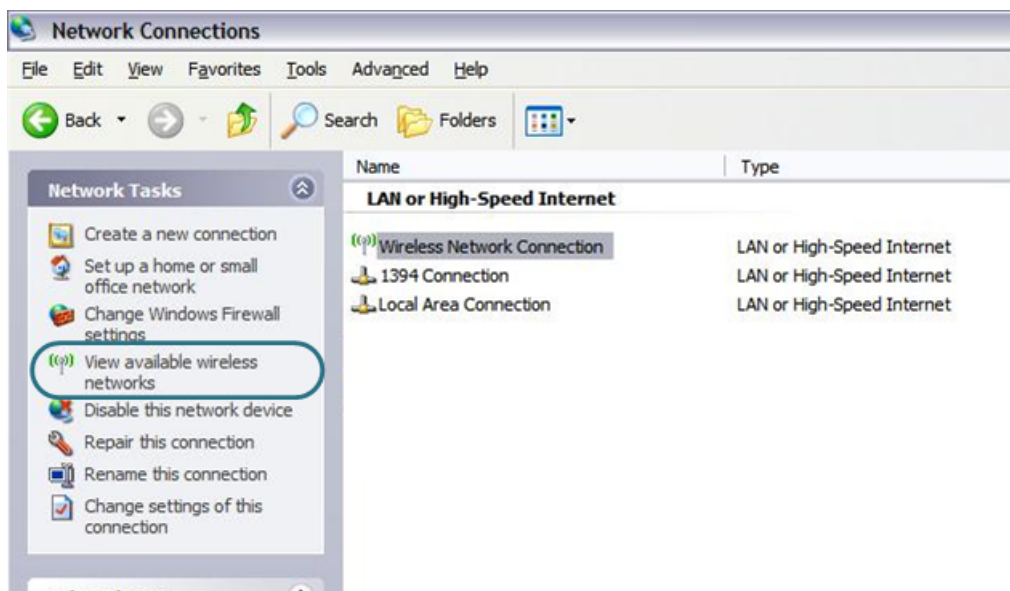


Figure 6. The **Network Connections** window.

3. Search for available wireless networks.
4. In the opened **Wireless Network Connection** window, select the needed wireless network (**DIR-300NRU**) and click the **Connect** button.

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

**!** If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings 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 (create a WAN connection, change the parameters of the wireless network, specify the settings of the firewall, etc.).

1. Start a web browser (see the *Before You Begin* section, page 14).
2. In the address bar of the web browser, enter the IP address of the router (by default, the following IP address is specified: **192.168.0.1**). Press the **Enter** key.



Figure 7. Connecting to the web-based interface of the DIR-300NRU 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** button.

A screenshot of the login page for the DIR-300NRU device. The page has a teal header with the text 'DIR\_300NRUB5'. Below the header, there are two input fields: 'Login:' and 'Password:'. At the bottom of the form, there are two buttons: 'Clear' and 'Enter'.

Figure 8. The login page.

**!** If the error “The page cannot be displayed” (or “Unable to display the page”/“Could not connect to remote server”) occurs upon connecting to the web-based interface of the router, make sure that you have properly connected the router to your computer.

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



Figure 9. 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 router only after restoring the factory default settings via the hardware Reset button. This procedure wipes out all settings that you have configured for your router.

After successful registration the system statistics page opens. The page displays general information on the router and its software.

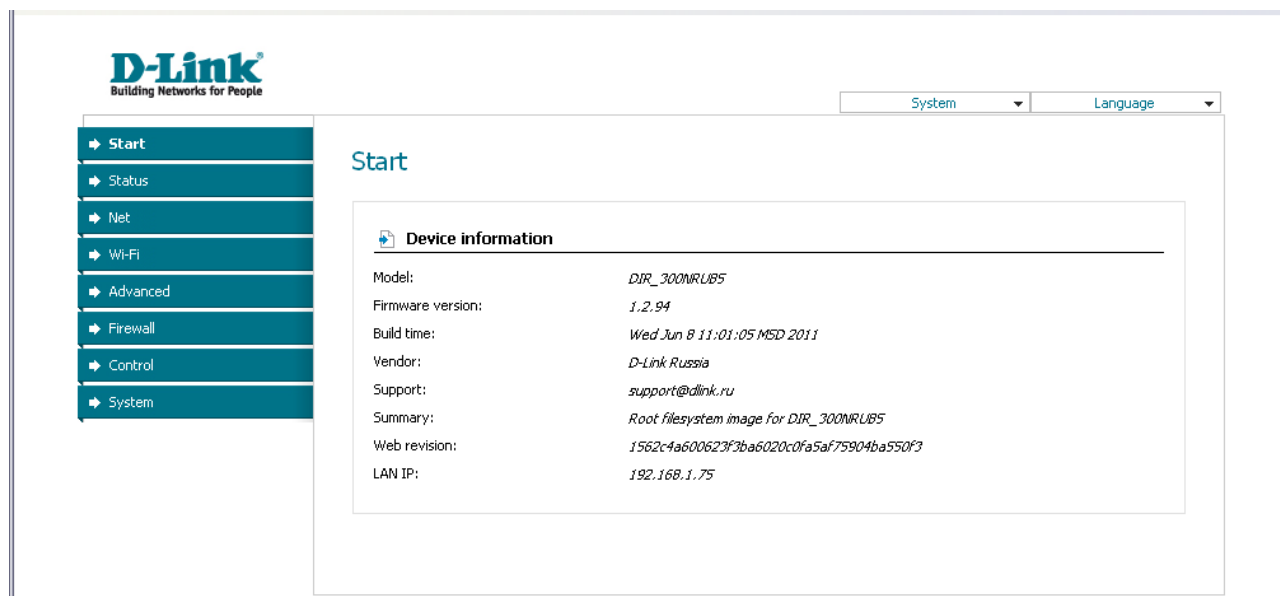


Figure 10. The system statistics page.

The web-based interface of the router 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.

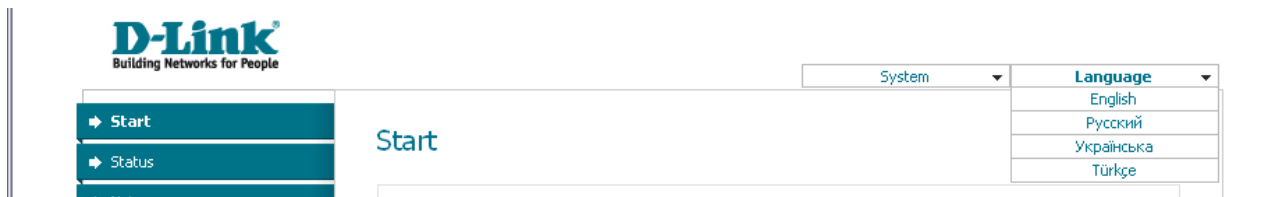


Figure 11. Changing the language of the web-based interface.

## Saving and Restoring Settings

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

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



Figure 12. The notification on unsaved changes.

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

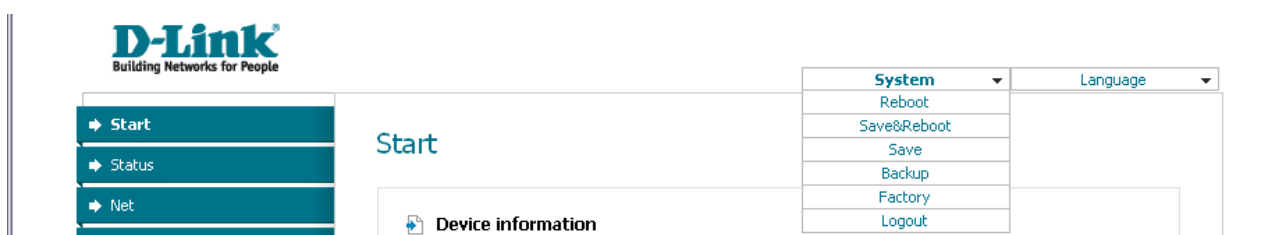


Figure 13. The top-page menu.

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

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

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 router) to your PC. Also you can save the router'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 hole of the button is located on the back panel of the router next to the power connector. Use a small paperclip to activate the button; insert it into the hole (with the router turned on), push, and hold for 10 seconds. Then remove the paperclip. Wait for about 30 seconds. Now you can access the web-based interface of the router using the default IP address, username and password.

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

# CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

## Status

This menu displays data on the current state of the router. The following are represented: statistics for every active interface, data on devices connected to the router's network and its web-based interface, and the routing table.

## 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).

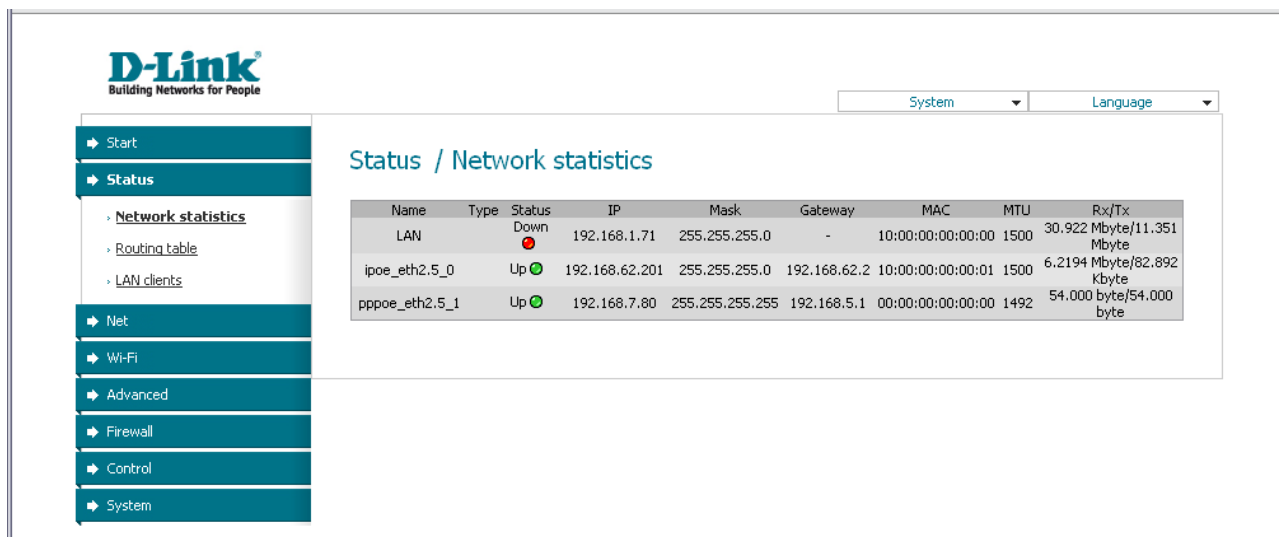
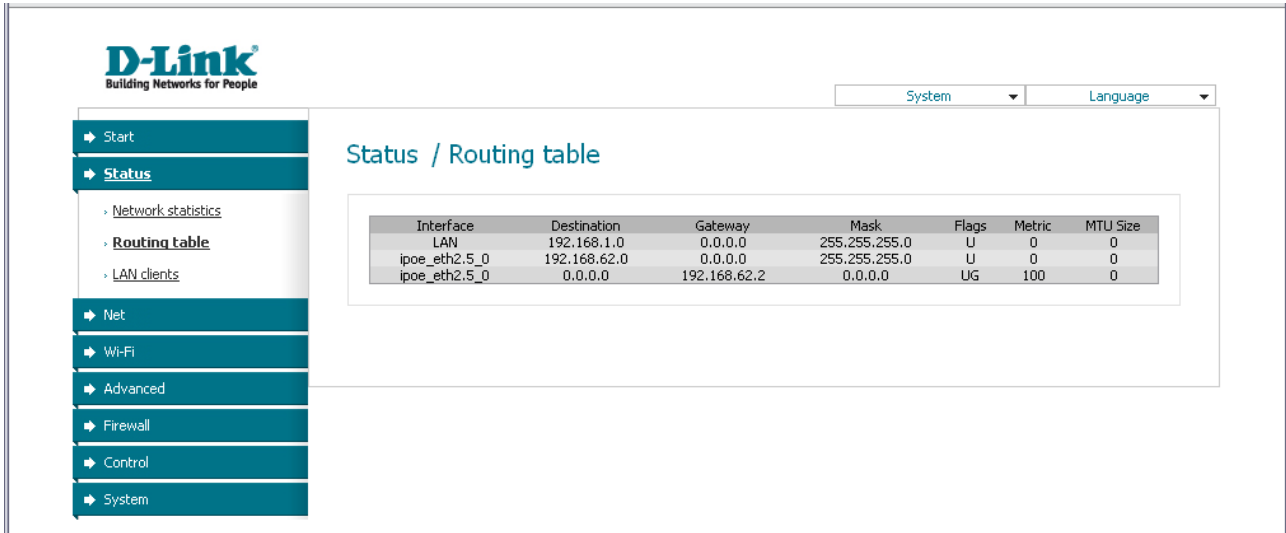


Figure 14. The Status / Network statistics page.

## Routing Table

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



The screenshot shows the D-Link web interface. The top left features the D-Link logo and tagline 'Building Networks for People'. Below it is a navigation menu with items: Start, Status (selected), Network statistics, Routing table (selected), LAN clients, Net, Wi-Fi, Advanced, Firewall, Control, and System. The main content area is titled 'Status / Routing table' and contains a table with the following data:

Interface	Destination	Gateway	Mask	Flags	Metric	MTU Size
LAN	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0
ipoe_eth2.5_0	192.168.62.0	0.0.0.0	255.255.255.0	U	0	0
ipoe_eth2.5_0	0.0.0.0	192.168.62.2	0.0.0.0	UG	100	0

Figure 15. The **Status / Routing table** page.



## LAN Clients

On the **Status / LAN clients** page, you can view data on network devices connected to the router. The page displays devices connected to the wireless network of the router, devices connected to the built-in switch of the router, and devices accessing the web-based interface of the router.

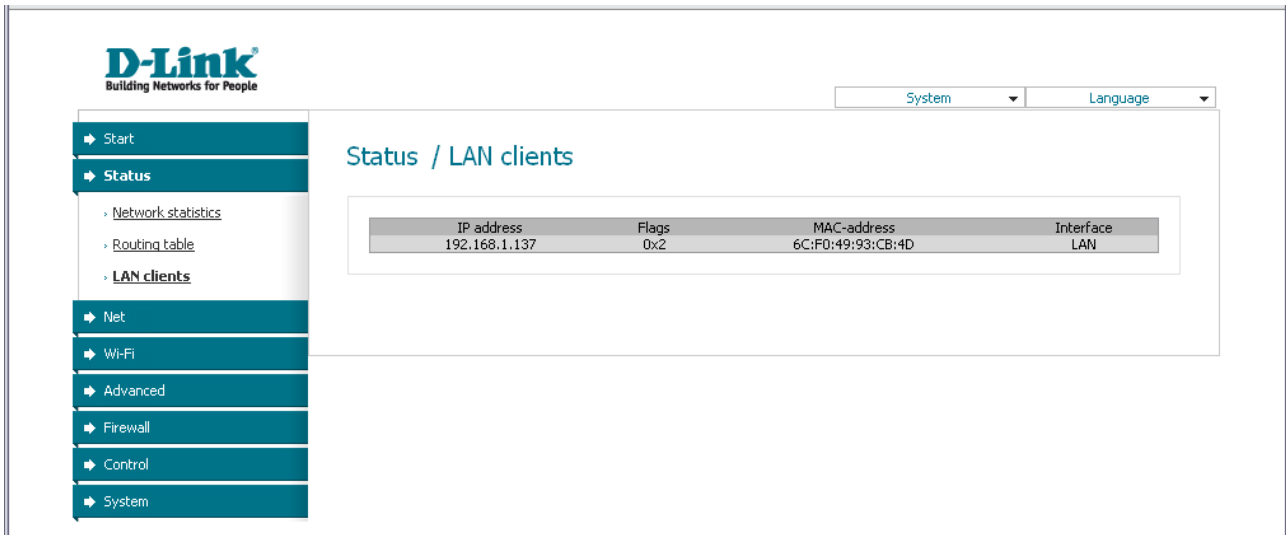


Figure 16. The **Status / LAN clients** page.

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 router's local area network and configure connection to the Internet (a WAN connection).

## Connections

On the **Net / Connections** page, you can create and edit connections used by the router.

By default, two connections are configured in the system:

- **LAN**: corresponds to the local interface of the router. The connection is represented by the ports of the built-in switch (ports 1-4) and the wireless interface of the router. You cannot delete this connection.
- **WAN**: connection to the Internet. This connection is assigned to the INTERNET port of the router (**port 5**). You can edit this connection or delete it.

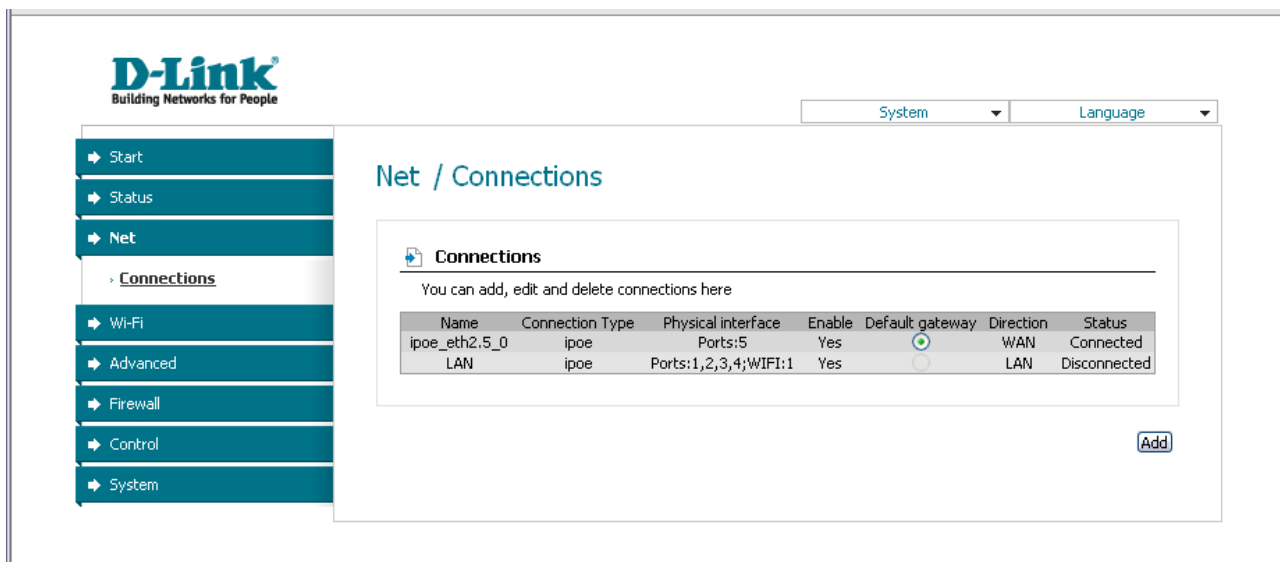


Figure 17. The **Net / Connections** page.

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.

## Editing Local Interface Parameters

To edit the parameters of the router's local area network, left-click the **LAN** connection on the **Net / Connections** page.

On the **Main** tab, you can configure basic parameters of the router's LAN.

### Net / Connections

The screenshot displays the 'Net / Connections' web interface. At the top, there are three tabs: 'Main' (selected), 'DHCP server', and 'Static DHCP'. Below the tabs, the 'General settings' section is expanded, showing 'Connection type and common settings'. The 'Name' field is set to 'LAN', 'Connection Type' is 'IPoE', 'Enable' is checked, and 'Direction' is 'LAN'. The 'Physical layer' section is also expanded, showing 'Physical interface selection and tuning' with 'Physical interface' set to 'Ports:1,2,3,4;WIFI:1'. The 'IP settings' section is expanded, showing 'Internet Protocol settings' with 'IP Address' set to '192.168.0.1' and 'Netmask' set to '255.255.255.0'. At the bottom, the 'Interface' field is set to 'br0'. A 'Save' button is located at the bottom right of the form.

Name:	LAN
Connection Type:	IPoE
Enable:	<input checked="" type="checkbox"/>
Direction:	LAN
Physical interface:	Ports:1,2,3,4;WIFI:1
IP Address:	192.168.0.1
Netmask:	255.255.255.0
Interface:	br0

Save

Figure 18. Basic parameters of the router's LAN.

Parameter	Description
<b>General settings</b>	
<b>Name</b>	A name for this connection.
<b>Connection Type</b>	The type of network protocol used by this connection – <b>IPoE</b> .
<b>Enable</b>	The checkbox enabling this connection.
<b>Direction</b>	The direction of this connection.
<b>Physical layer</b>	
<b>Physical interface</b>	The physical interface to which this connection is assigned.
<b>IP settings</b>	
<b>IP Address</b>	The router's IP address. By default, the following value is specified: <b>192.168.0.1</b> .
<b>Netmask</b>	The subnet mask. By default, the following value is specified: <b>255.255.255.0</b> .
<b>Interface</b>	The name assigned to the connection by the system.

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

On the **DHCP server** tab, you can configure the built-in DHCP sever of the router.

## Net / Connections

The screenshot shows the DHCP server configuration interface. At the top, there are three tabs: 'Main', 'DHCP server', and 'Static DHCP'. The 'DHCP server' tab is active. Below the tabs, there are four configuration fields:

- Mode:** A dropdown menu with 'Enable' selected.
- Start IP:** A text input field containing '192.168.0.2'.
- End IP:** A text input field containing '192.168.0.254'.
- Lease time (min):** A text input field containing '6400'.

A 'Save' button is located at the bottom right of the configuration area.

Figure 19. The tab for configuring the DHCP server.

Parameter	Description
<b>Mode</b>	<p>An operating mode of the router's DHCP server.</p> <p><b>Enable:</b> the router assigns IP addresses to clients automatically in accordance with specified parameters. When this value is selected, the <b>Start IP</b>, <b>End IP</b>, and the <b>Lease time</b> fields are displayed on the tab. If the DHCP server is enabled, you can also specify MAC-IP pairs on the <b>Static DHCP</b> tab.</p> <p><b>Disable:</b> the router's DHCP server is disabled, clients' IP addresses are assigned manually.</p> <p><b>Relay:</b> an external DHCP server is used to assign IP addresses to clients. When this value is selected, the <b>External DHCP server IP</b> field is displayed on the tab.</p>
<b>Start IP</b>	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
<b>End IP</b>	The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
<b>Lease time</b>	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
<b>External DHCP server IP</b>	The IP address of the external DHCP server which assigns IP addresses to the router's clients.

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

On the **Static DHCP** tab, you can specify MAC address and IP address pairs. The tab is active when the router's DHCP server is enabled.

## Net / Connections

The screenshot shows the 'Static DHCP' configuration page. At the top, there are three tabs: 'Main', 'DHCP server', and 'Static DHCP'. The 'Static DHCP' tab is selected. Below the tabs, there are three input fields: 'IP address' with the value '192.168.1.34', 'MAC address' with the value '00:11:22:33:44:55', and 'Host name' with the value 'moi'. Below these fields is a table with three columns: 'IP address', 'MAC address', and 'Host name'. The table contains one row with the values '192.168.1.34', '00:11:22:33:44:55', and 'moi'. To the right of the table are 'Remove' and 'Add' buttons. At the bottom right of the page is a 'Save' button.

Figure 20. The tab for configuring MAC-IP pairs.

To create a MAC-IP pair (set a fixed IP address in the local area network for a device with a certain MAC address), click the **Add** button.

You can specify the following parameters:

Parameter	Description
<b>IP address</b>	An IP address which will be assigned to the device with the specified MAC address.
<b>MAC address</b>	The MAC address of the device from the LAN.
<b>Host name</b>	A network name of the device for easier identification. <i>Optional.</i>

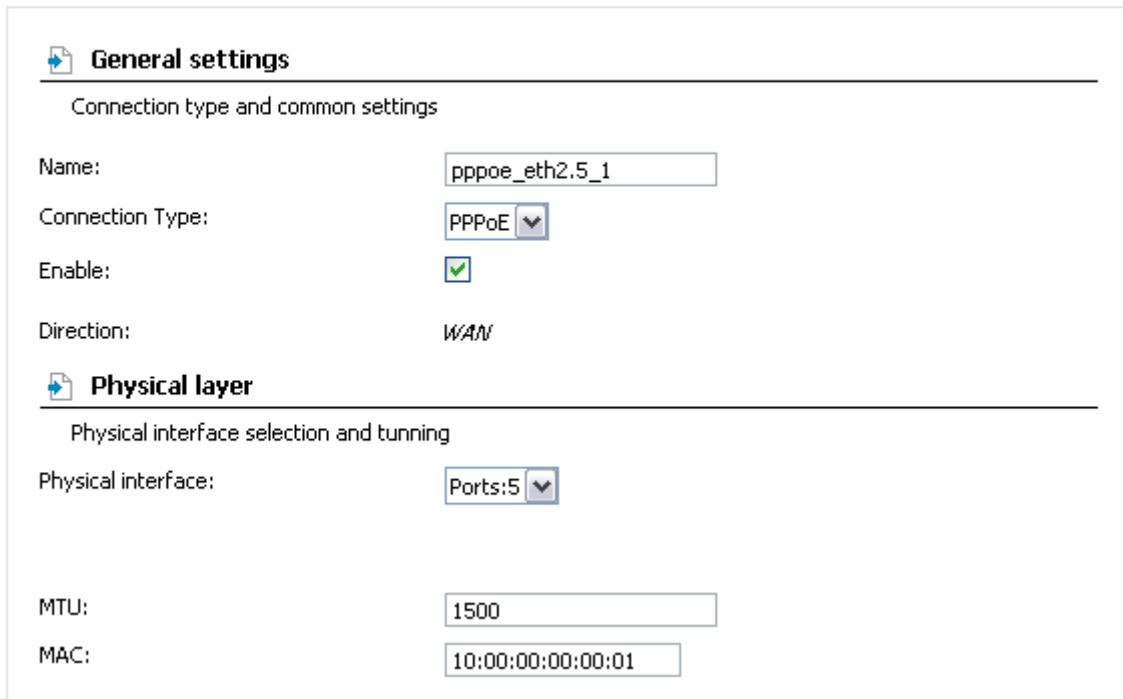
Click the **Save** button.

Existing MAC-IP pairs are displayed on the **Static DHCP** tab. To remove a pair, select the relevant line in the table and click the **Remove** button. Then click the **Save** button.

## Creating PPPoE WAN Connection

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

### Net / Connections



The screenshot displays the configuration interface for a new connection. It is divided into two main sections: **General settings** and **Physical layer**.

**General settings** section includes the following fields:

- Name:** A text input field containing the value "pppoe\_eth2.5\_1".
- Connection Type:** A dropdown menu with "PPPoE" selected.
- Enable:** A checkbox that is checked.
- Direction:** A text input field containing the value "WAN".

**Physical layer** section includes the following fields:

- Physical interface:** A dropdown menu with "Ports:5" selected.
- MTU:** A text input field containing the value "1500".
- MAC:** A text input field containing the value "10:00:00:00:00:01".

Figure 21. The page for creating a new connection. The **General settings** and **Physical layer** sections.

Parameter	Description
<b>General settings</b>	
<b>Name</b>	A name for connection for easier identification.
<b>Enable</b>	Select the checkbox to enable the connection.
<b>Direction</b>	The direction of this connection.
<b>Physical layer</b>	
<b>Physical interface</b>	A physical or virtual interface to which the new connection will be assigned.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>MAC</b>	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. By default, the router's MAC address is specified in the field.



PPP settings

Enter the username, password, and other settings provided by the ISP. Leave the default values for the remaining fields.

PPP Username:

Without authorization:

Password:

Password confirmation:

Authentication algorithm: AUTO ▼

Service name:

Dial on demand:

MTU:

PPP IP extension:

Keep Alive:

Use Static IP Address:

PPP debug:

PPPoE pass through:

Interface:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Figure 22. The page for creating a new connection. The **PPP settings** and **Miscellaneous** sections.

Parameter	Description
<b>PPP settings</b>	
<b>PPP Username</b>	A username (login) to access the Internet.
<b>Without authorization</b>	Select the checkbox if you don't need to enter a username and password to access the Internet.
<b>Password</b>	A password to access the Internet.
<b>Password confirmation</b>	The confirmation of the entered password (to avoid mistypes).
<b>Authentication algorithm</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.

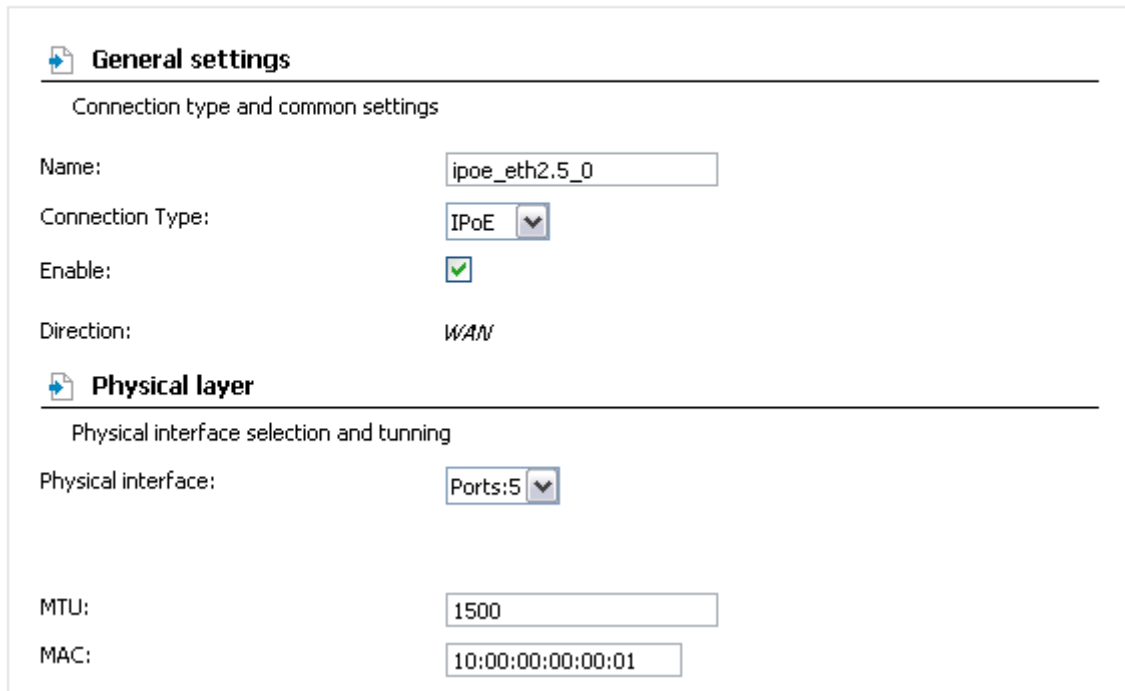
Parameter	Description
<b>Service name</b>	The name of the PPPoE authentication server.
<b>Dial on demand</b>	Select the checkbox if you want the router to establish connection to the Internet on demand. In the <b>Maximum idle time</b> field, specify a period of inactivity (in seconds) after which the connection should be terminated.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>PPP IP extension</b>	This option is used by some ISPs. Contact your ISP to clarify if this checkbox needs to be enabled.
<b>Keep Alive</b>	Select the checkbox if you want the router 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 <b>LCP interval</b> and <b>LCP fails</b> fields are available. Specify the required values.
<b>Use Static IP Address</b>	Select the checkbox if you want to use a static IP address to access the Internet. In the <b>IP Address</b> field displayed when the checkbox is selected, specify a static IP address.
<b>PPP debug</b>	Select the checkbox if you want to log all data on PPP connection debugging.
<b>PPPoE pass through</b>	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 router.
<b>Interface</b>	The name assigned to the connection by the system.
<b>Miscellaneous</b>	
<b>Enable RIP</b>	Select the checkbox to allow using RIP for this connection.
<b>Enable IGMP Multicast</b>	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
<b>NAT</b>	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
<b>Firewall</b>	Select the checkbox to enable protection against ARP and DDoS attacks.

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

## Creating IPoE WAN Connection

To create a connection of this type, select the **WAN** connection on the **Net / Connections** page. On the opened page, select the **IPoE** value from the **Connection type** drop-down list and specify the needed values.

### Net / Connections



The screenshot displays the configuration interface for a new connection. It is divided into two main sections: **General settings** and **Physical layer**.

**General settings** (Connection type and common settings):


- Name: ipoe\_eth2.5\_0
- Connection Type: IPoE (selected from a dropdown menu)
- Enable:
- Direction: WAN

**Physical layer** (Physical interface selection and tuning):

- Physical interface: Ports:5 (selected from a dropdown menu)
- MTU: 1500
- MAC: 10:00:00:00:00:01

Figure 23. The page for creating a new connection. The **General settings** and **Physical layer** sections.

Parameter	Description
<b>General settings</b>	
<b>Name</b>	A name for connection for easier identification.
<b>Enable</b>	Select the checkbox to enable the connection.
<b>Direction</b>	The direction of this connection.
<b>Physical layer</b>	
<b>Physical interface</b>	A physical or virtual interface to which the new connection will be assigned.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>MAC</b>	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. By default, the router's MAC address is specified in the field.

 **IP settings**


Internet Protocol settings

Obtain an IP address automatically:

Obtain DNS server addresses automatically:

Vendor ID:

Interface:

 **Miscellaneous**

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Figure 24. The page for creating a new connection. The **IP settings** and **Miscellaneous** sections.

Parameter	Description
<b>IP settings</b>	
<b>Obtain an IP address automatically</b>	Select the checkbox to configure automatic IP address assignment for this connection. When the checkbox is selected, the <b>IP Address</b> , <b>Netmask</b> , and <b>Gateway IP Address</b> fields are not displayed.
<b>IP Address</b>	Enter an IP address for this WAN connection.
<b>Netmask</b>	Enter a subnet mask for this WAN connection.
<b>Gateway IP Address</b>	Enter an IP address of the gateway used by this WAN connection.
<b>Obtain DNS server addresses automatically</b>	Displayed when the <b>Obtain an IP address automatically</b> checkbox is selected.  Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the <b>Primary DNS server</b> and <b>Secondary DNS server</b> fields are not displayed.
<b>Primary DNS server/ Secondary DNS server</b>	Enter addresses of the primary and secondary DNS servers in the relevant fields.
<b>Vendor ID</b>	The identifier of your ISP. This field is specified when the ISP assigns an IP address automatically (the <b>Obtain an IP address automatically</b> checkbox is selected). <i>Optional</i> .
<b>Interface</b>	The name assigned to the connection by the system.
<b>Miscellaneous</b>	
<b>Enable RIP</b>	Select the checkbox to allow using RIP for this connection.
<b>Enable IGMP Multicast</b>	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
<b>NAT</b>	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
<b>Firewall</b>	Select the checkbox to enable protection against ARP and DDoS attacks.

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

## Creating PPTP or L2TP WAN Connection

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

### Net / Connections

The screenshot shows the configuration page for a new connection. It is divided into two main sections: **General settings** and **Physical layer**.

**General settings** (Connection type and common settings):

- Name: l2tp\_eth2.5\_0
- Connection Type: L2TP
- Enable:
- Direction: WAN

**Physical layer** (Physical interface selection and tuning):

- Physical interface: ipoe\_eth2.5\_0

Figure 25. The page for creating a new connection. The **General settings** and **Physical layer** sections.

Parameter	Description
<b>General settings</b>	
<b>Name</b>	A name for connection for easier identification.
<b>Enable</b>	Select the checkbox to enable the connection.
<b>Direction</b>	The direction of this connection.
<b>Physical layer</b>	
<b>Physical interface</b>	An existing PPPoE or IPoE interface (connection) to which the new connection will be assigned.

**PPTP/L2TP settings**

PPTP and L2TP are methods for implementing virtual private networks.

Connect automatically:

A way of specifying the service name: URL ▾

Service name:

Without authorization:

PPP Username:

Password:

Password confirmation:

Encryption: No encrypt ▾

Authentication algorithm: AUTO ▾

Keep Alive:

Extra options:

*IP received:*

MTU:

*Interface:*

---

**Miscellaneous**

Enable RIP:

NAT:

firewall:

Figure 26. The page for creating a new connection. The **PPTP/L2TP settings** and **Miscellaneous** sections.

Parameter	Description
<b>PPTP/L2TP settings</b>	
<b>Connect automatically</b>	Select the checkbox to enable auto-start of the connection upon the boot-up of the router.
<b>A way of specifying the service name</b>	Select a way of specifying the address of the PPTP or L2TP server.
<b>Service name</b>	The IP or URL address of the PPTP or L2TP server.
<b>Without authorization</b>	Select the checkbox if you don't need to enter a username and password to access the Internet.
<b>PPP Username</b>	A username (login) to access the Internet.
<b>Password</b>	A password to access the Internet.
<b>Password confirmation</b>	The confirmation of the entered password (to avoid mistypes).

Parameter	Description
<b>Encryption</b>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> <li>• <b>No encrypt</b>: MPPE encryption is not applied.</li> <li>• <b>MPPE 40/128 bit</b>: MPPE encryption with a 40-bit or 128-bit key is applied.</li> <li>• <b>MPPE 40 bit</b>: MPPE encryption with a 40-bit key is applied.</li> <li>• <b>MPPE 128 bit</b>: MPPE encryption with a 128-bit key is applied.</li> </ul> <p>MPPE encryption can be applied only if the <b>MSCHAP</b>, <b>MACHAPv2</b>, or <b>AUTO</b> value is selected from the <b>Authentication algorithm</b> drop-down list.</p>
<b>Authentication algorithm</b>	Select a required authentication method from the drop-down list or leave the <b>AUTO</b> value.
<b>Keep Alive</b>	Select the checkbox if you want the router 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 <b>LCP interval</b> and <b>LCP fails</b> fields are available. Specify the required values.
<b>Extra options</b>	Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional</i> .
<b>IP received</b>	The IP address assigned by the ISP.
<b>MTU</b>	The maximum size of units transmitted by the interface.
<b>Interface</b>	The name assigned to the connection by the system.
<b>Miscellaneous</b>	
<b>Enable RIP</b>	Select the checkbox to allow using RIP for this connection.
<b>NAT</b>	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
<b>Firewall</b>	Select the checkbox to enable protection against ARP and DDoS attacks.

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.

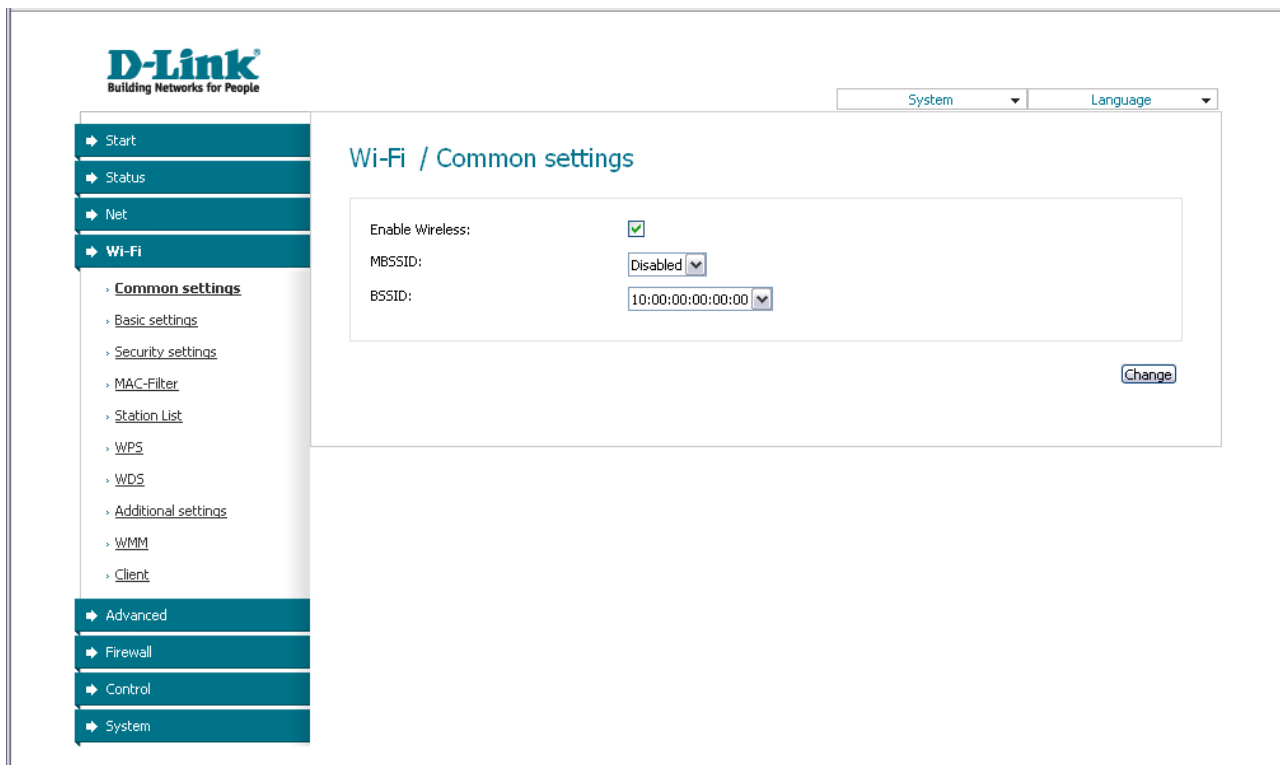


Figure 27. Common settings of the wireless LAN.

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 router 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 router'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 router's WLAN.

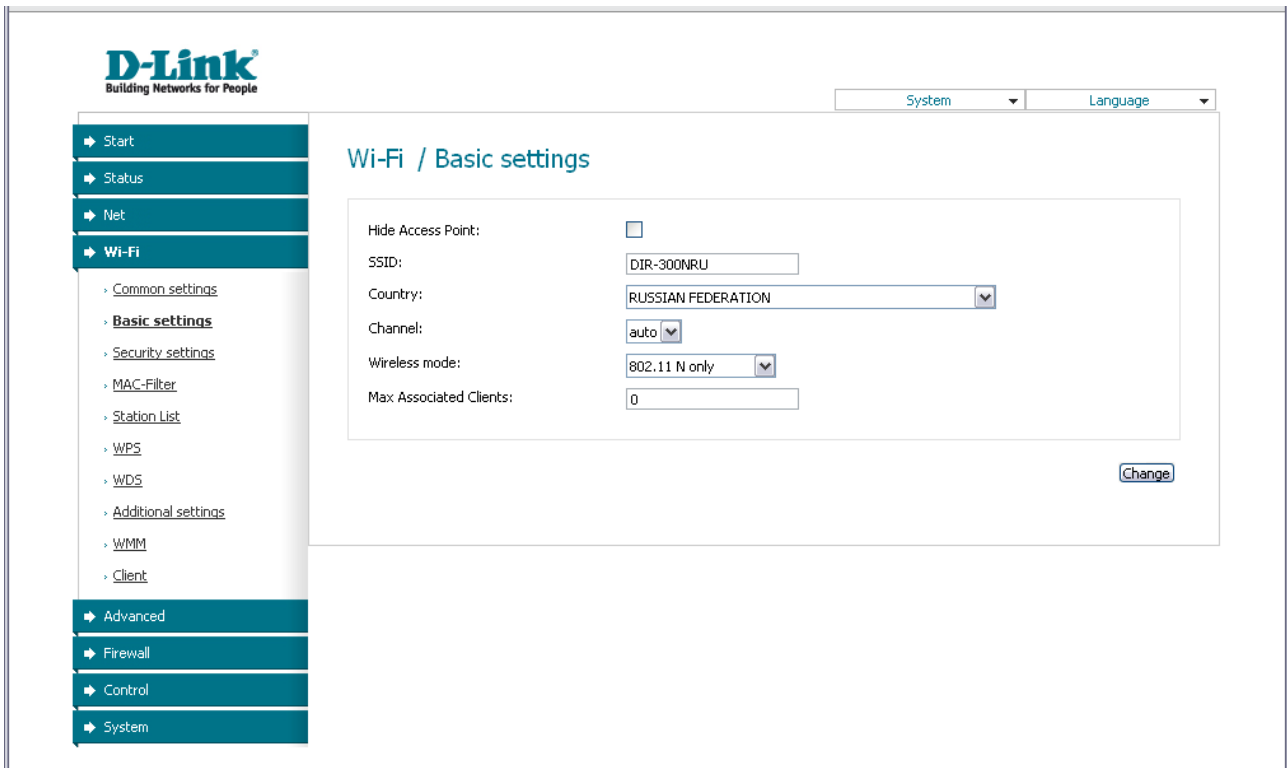


Figure 28. Basic settings of the wireless LAN.

Parameter	Description
<b>Hide Access Point</b>	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.)
<b>SSID</b>	A name for the WLAN. By default, the value <b>DIR-300NRU</b> is specified. If your network is splitted into parts, each part has the default name ( <b>DIR-300NRU.2</b> , <b>DIR-300NRU.3</b> , and <b>DIR-300NRU.4</b> ). It is recommended to specify another name for the network upon initial configuration (use digits and Latin characters).
<b>Country</b>	The country you are in. Select a value from the drop-down list.
<b>Channel</b>	The wireless channel number. When the <b>auto</b> value is selected, the router itself chooses the channel with the least interference.
<b>Wireless mode</b>	Operating mode of the router's wireless network. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
<b>Max Associated Clients</b>	The maximum number of devices connected to the wireless network of the router. When the value <b>0</b> is specified, the router does not limit the number of connected clients.

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

## Security Settings

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

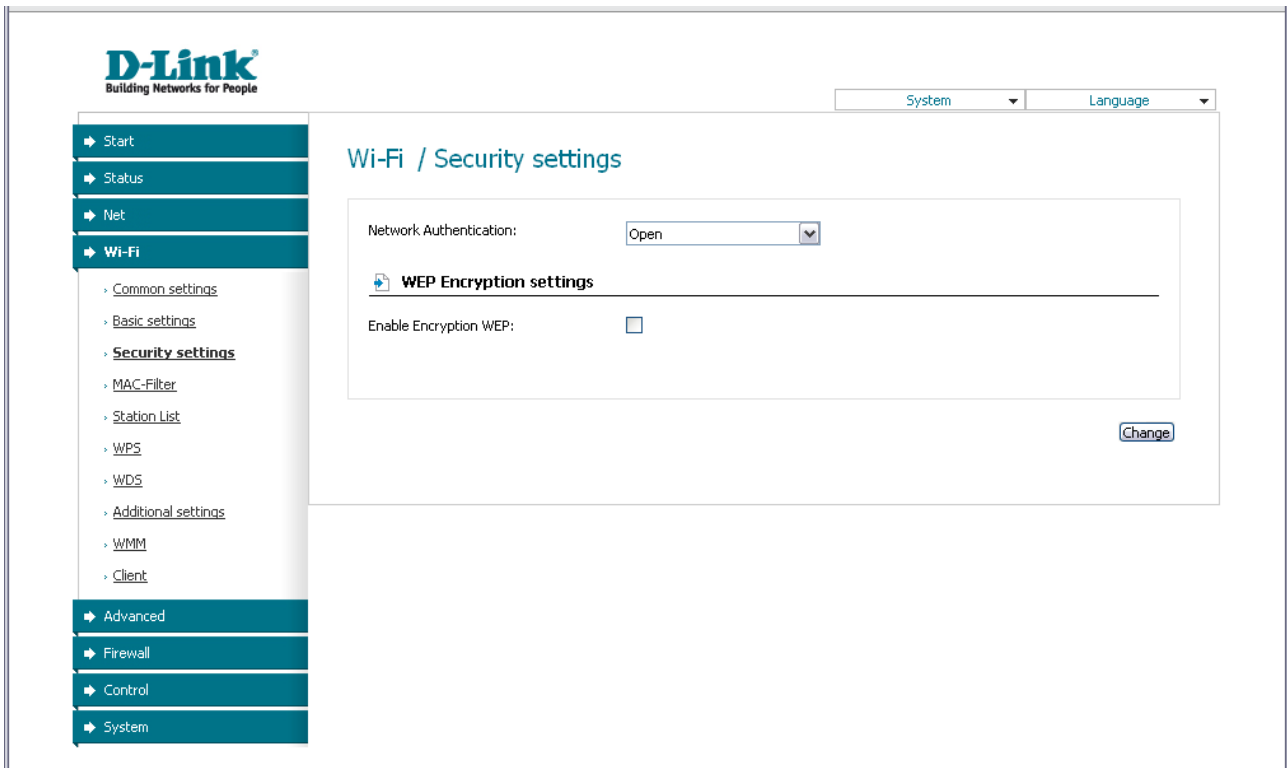


Figure 29. The default security settings.

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).

## Wi-Fi / Security settings

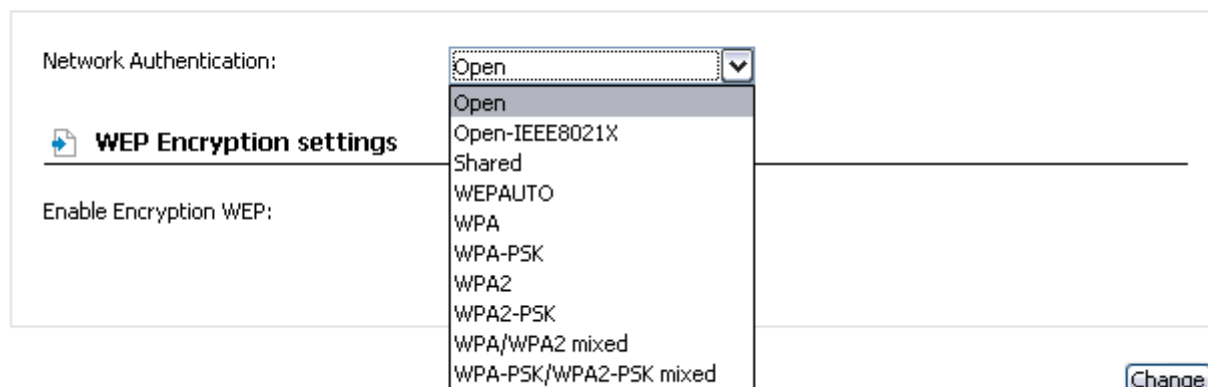


Figure 30. Network authentication types supported by the router.

The router supports the following authentication types:

Authentication type	Description
<b>Open</b>	Open authentication (with or without WEP encryption).
<b>Open-IEEE8021X</b>	Open authentication using a RADIUS server (with or without WEP encryption).
<b>Shared</b>	Shared key authentication with WEP encryption.
<b>WPAUTO</b>	A mixed type of authentication. When this value is selected, devices using the <b>Open</b> authentication type with enabled WEP encryption and devices using the <b>Shared</b> authentication type can connect to the router's WLAN.
<b>WPA</b>	WPA-based authentication using a RADIUS server.
<b>WPA-PSK</b>	WPA-based authentication using a PSK.
<b>WPA2</b>	WPA2-based authentication using a RADIUS server.
<b>WPA2-PSK</b>	WPA2-based authentication using a PSK.
<b>WPA/WPA2 mixed</b>	A mixed type of authentication. When this value is selected, devices using the <b>WPA</b> authentication type and devices using the <b>WPA2</b> authentication type can connect to the router's WLAN.
<b>WPA-PSK/WPA2-PSK mixed</b>	A mixed type of authentication. When this value is selected, devices using the <b>WPA-PSK</b> authentication type and devices using the <b>WPA2-PSK</b> authentication type can connect to the router's WLAN.

**!** The **Open-IEEE8021X**, **WPA**, **WPA2**, and **WPA/WPA2 mixed** authentication types require a RADIUS server.

When the **Open**, **Shared**, or **WEPAUTO** values are selected, the **WEP Encryption settings** section is displayed:

## Wi-Fi / Security settings

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):

[Change](#)

Figure 31. The **Open** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
<b>Enable Encryption WEP</b>	The checkbox activating WEP encryption. When the checkbox is selected, the <b>Default Key ID</b> field, the <b>Encryption Key WEP as HEX</b> checkbox, and four <b>Encryption Key WEP</b> fields are displayed on the page. For the <b>Shared</b> and <b>WEPAUTO</b> authentication types the checkbox is always selected.
<b>Default Key ID</b>	The number of the key (from first to fourth) which will be used for WEP encryption.
<b>Encryption Key WEP as HEX</b>	Select the checkbox to set a hexadecimal number as a key for encryption.
<b>Encryption Key WEP (1-4)</b>	Keys for WEP encryption. The router uses the key selected from the <b>Default Key ID</b> drop-down list. It is required to specify all the fields.  You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters). If the <b>Encryption Key WEP as HEX</b> checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F).

When the **Open-IEEE8021X** value is selected, the **WEP Encryption settings** and **RADIUS settings** sections are displayed:

## Wi-Fi / Security settings

Network Authentication:	<input type="text" value="Open-IEEE8021X"/>
<hr/>	
<b>WEP Encryption settings</b>	
Enable Encryption WEP:	<input checked="" type="checkbox"/>
Default Key ID:	<input type="text" value="3"/>
Encryption Key WEP as HEX:	<input type="checkbox"/>
Encryption Key WEP (1):	<input type="text"/>
Encryption Key WEP (2):	<input type="text"/>
Encryption Key WEP (3):	<input type="text"/>
Encryption Key WEP (4):	<input type="text"/>
<hr/>	
<b>RADIUS settings</b>	
IP address:	<input type="text" value="192.168.0.254"/>
Port:	<input type="text" value="1812"/>
RADIUS encryption key:	<input type="text" value="dlink"/>

[Change](#)

Figure 32. The **Open-IEEE8021X** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
<b>Enable Encryption WEP</b>	The checkbox activating WEP encryption. When the checkbox is selected, the <b>Default Key ID</b> field, the <b>Encryption Key WEP as HEX</b> checkbox, and four <b>Encryption Key WEP</b> fields are displayed on the page.
<b>Default Key ID</b>	The number of the key (from first to fourth) which will be used for WEP encryption.
<b>Encryption Key WEP as HEX</b>	Select the checkbox to set a hexadecimal number as a key for encryption.
<b>Encryption Key WEP (1-4)</b>	<p>Keys for WEP encryption. The router uses the key selected from the <b>Default Key ID</b> drop-down list. It is required to specify all the fields.</p> <p>You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters). If the <b>Encryption Key WEP as HEX</b> checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F).</p>
<b>IP address</b>	The IP address of the RADIUS server.
<b>Port</b>	A port of the RADIUS server.
<b>RADIUS encryption key</b>	A password to access the RADIUS server.



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


## Wi-Fi / Security settings

Network Authentication:

Encryption Key PSK:

WPA2 Pre-authentication:

---

 **WPA Encryption settings**

---

WPA Encryption:

WPA renewal:

[Change](#)

Figure 33. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
<b>Encryption Key PSK</b>	A key for WPA encryption. The key can contain digits and/or Latin characters.
<b>WPA2 Pre-authentication</b>	The checkbox activating preliminary authentication (displayed only for the <b>WPA2-PSK</b> and <b>WPA-PSK/WPA2-PSK mixed</b> authentication types).
<b>WPA Encryption</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> .
<b>WPA renewal</b>	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value <b>0</b> is specified for this field, the key is not renewed.


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

## Wi-Fi / Security settings

Network Authentication:

WPA2 Pre-authentication:

---

 **RADIUS settings**


---

IP address:

Port:

RADIUS encryption key:

---

 **WPA Encryption settings**

---

WPA Encryption:

WPA renewal:

[Change](#)

Figure 34. The **WPA2** value is selected from the **Network Authentication** drop-down list.

Parameter	Description
<b>WPA2 Pre-authentication</b>	The checkbox activating preliminary authentication (displayed only for the <b>WPA2-PSK</b> and <b>WPA-PSK/WPA2-PSK mixed</b> authentication types).
<b>IP address</b>	The IP address of the RADIUS server.
<b>Port</b>	A port of the RADIUS server.
<b>RADIUS encryption key</b>	A password to access the RADIUS server.
<b>WPA Encryption</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> .
<b>WPA renewal</b>	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value <b>0</b> is specified for this field, the key is not renewed.

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

## MAC Filter

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

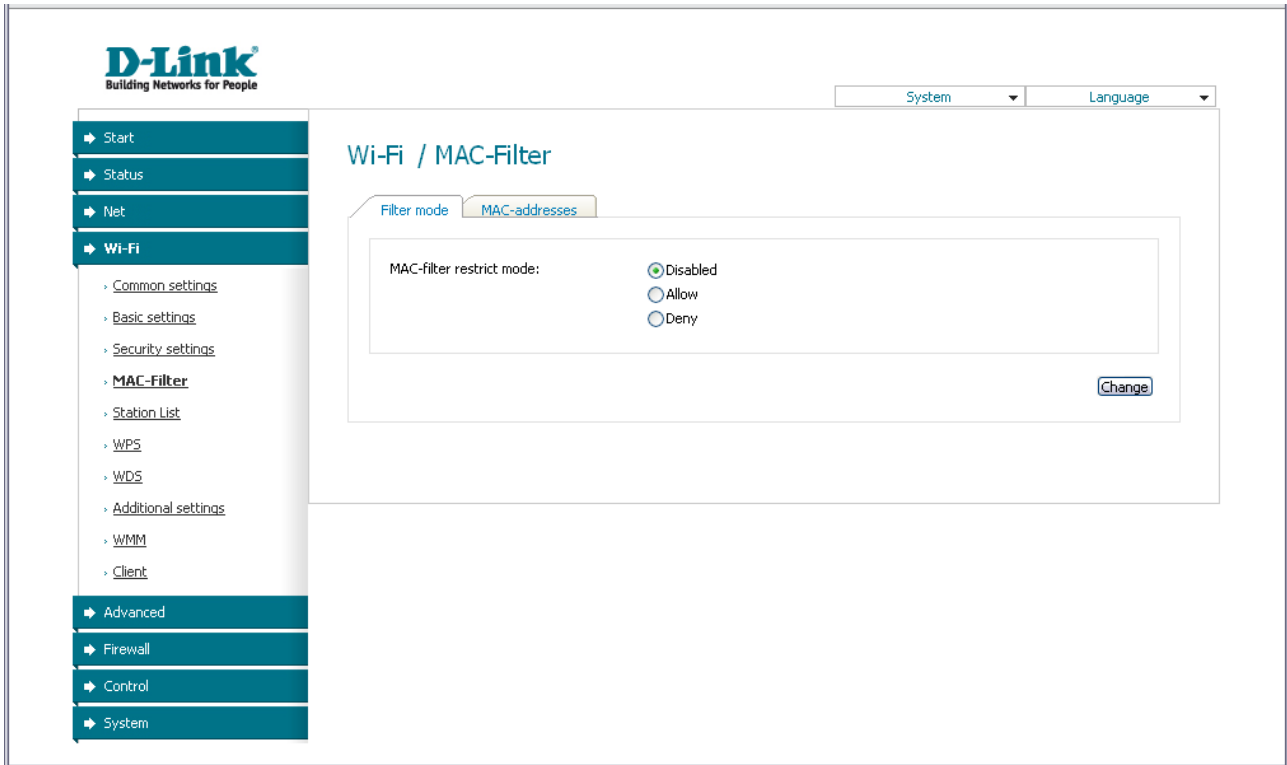


Figure 35. The MAC filter for the wireless network.

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, enter this address in the **MAC-address** field of the **MAC-address adding** section, and click the **Add** button. After that, the entered address will be displayed in the **MAC-address list** section.

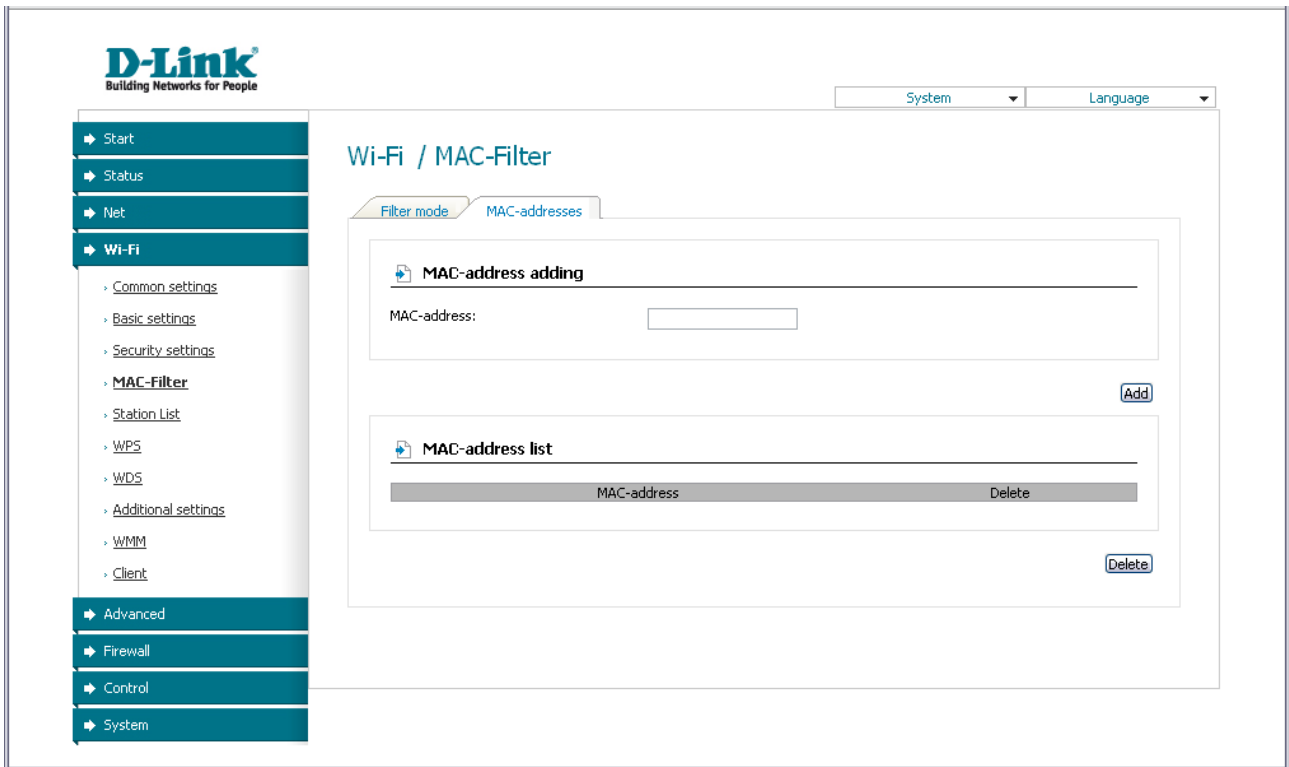


Figure 36. The tab for adding a MAC address.

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 router. Devices connected to the router via the WDS function are not displayed in the list.

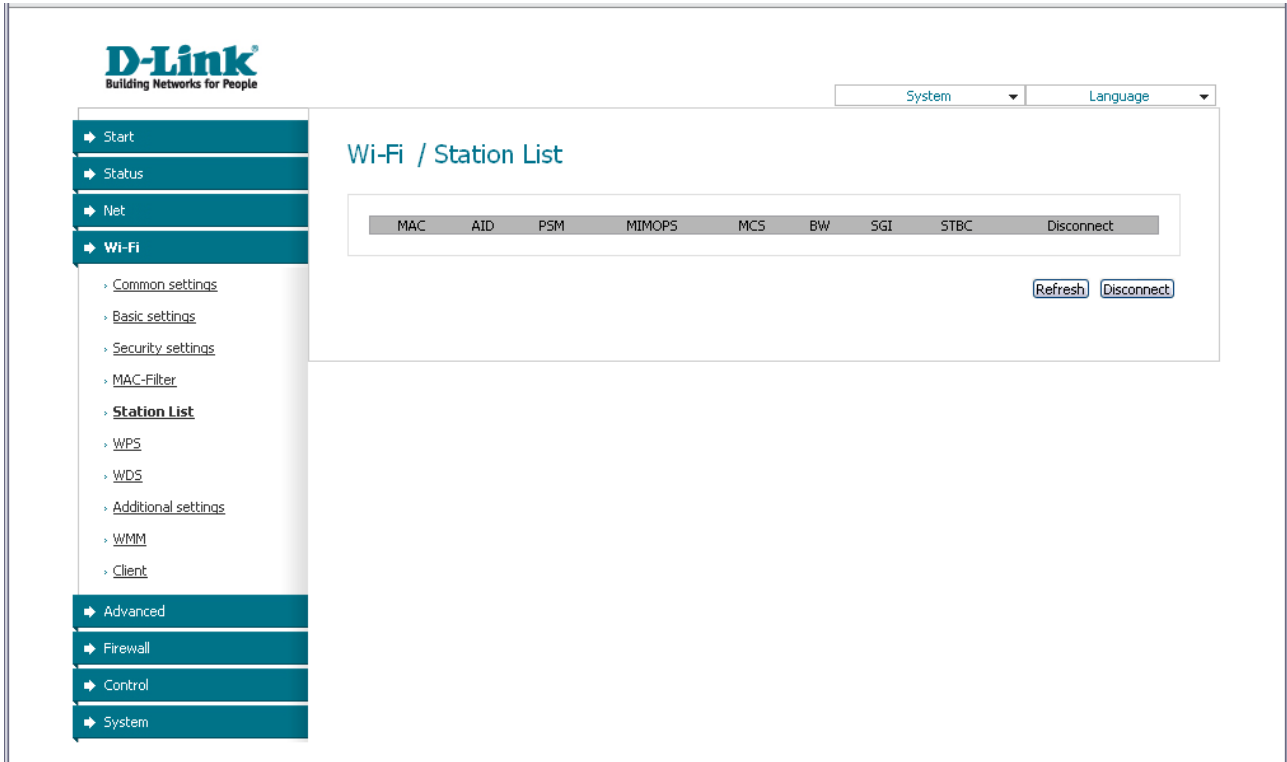


Figure 37. The list of the router's wireless clients.

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 router'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.

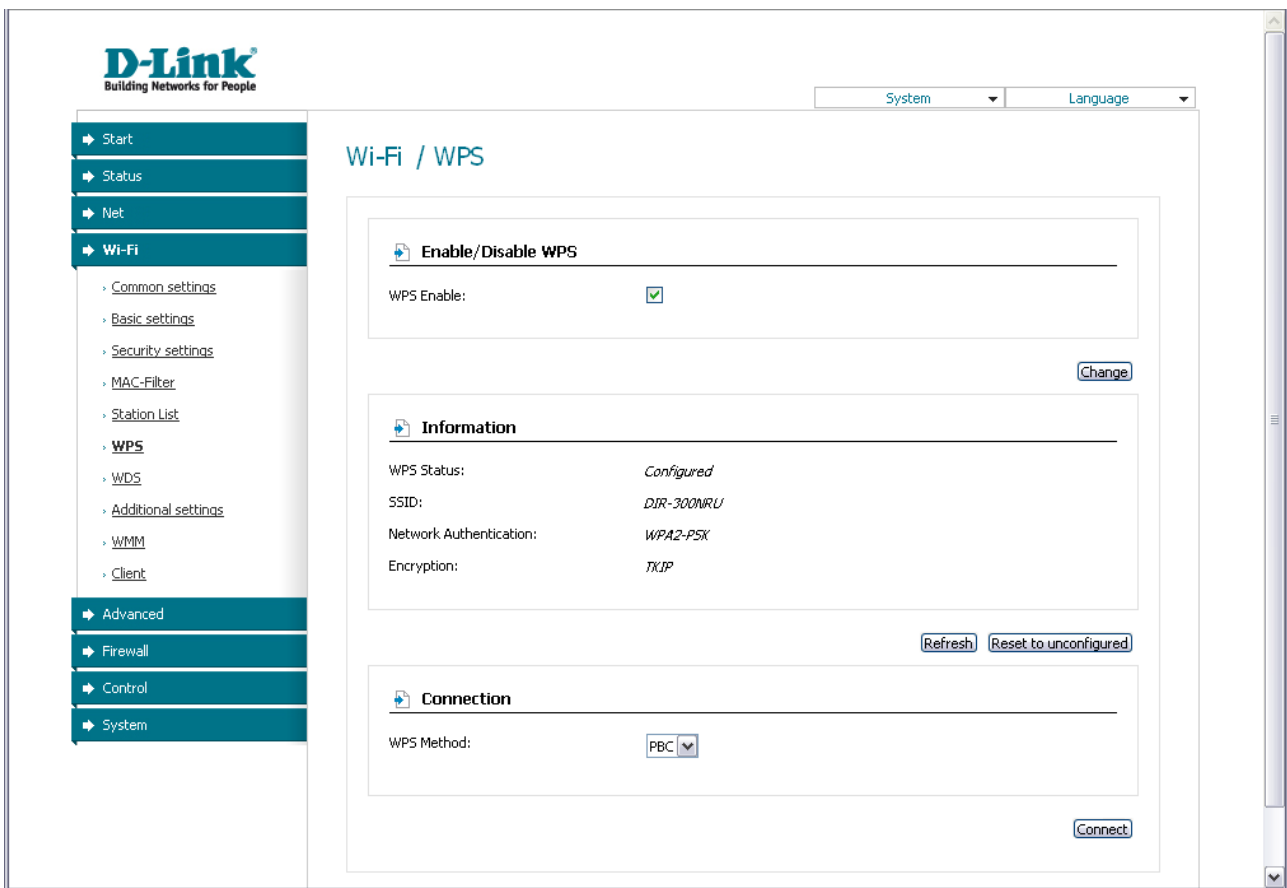


Figure 38. The page for configuring the WPS function.

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
<b>WPS Status</b>	The state of connecting the wireless device via the WPS function.
<b>SSID</b>	The name of the router's WLAN (or the first part of the WLAN if the network is splitted into parts).
<b>Network Authentication</b>	The network authentication type specified for the WLAN (or first part of the WLAN).
<b>Encryption</b>	The encryption type specified for the WLAN (or the first part of the WLAN).
<b>Refresh</b>	Click the button to view the latest data on the state of connecting the wireless device via the WPS function.
<b>Reset to unconfigured</b>	Click the button to reset the parameters of the WPS function in order to connect the next device.
<b>WPS Method</b>	A method of the WPS function. Select a value from the drop-down list. <b>PIN</b> : Connecting the device via the PIN code. <b>PBC</b> : Connecting the device via the push button (actual or virtual).
<b>PIN Code</b>	The PIN code of the WPS-enabled device that needs to be connected to the wireless network of the router. The field is displayed only when the <b>PIN</b> value is selected from the <b>WPS Method</b> drop-down list.
<b>Connect</b>	Click the button to connect the wireless device to the router's WLAN via the WPS function.

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

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

1. Select the **WPS Enable** checkbox.
2. Click the **Change** button.
3. Select the **PIN** value from the **WPS Method** drop-down list.
4. Select the PIN method in the software of the wireless device that you want to connect to the router's WLAN.
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 router.

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 router's WLAN.
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 router.

## ***Using WPS Function without Web-based Interface***

You can add a wireless device to the router's WLAN without accessing the web-based interface of the router. To do this, you need to configure the following router's settings:

1. Configure a type of WPA encryption for the WLAN (or the first part of the WLAN).
2. Select the **WPS Enable** checkbox.
3. Click the **Change** button.
4. Save the settings and close the web-based interface (click the **Save** line in the top-page menu displayed when the mouse pointer is over the **System** caption, then click the **Logout** line).

Later you will be able to add wireless devices to the WLAN by clicking the hardware WPS button located on the right side panel of the router.



1. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
2. Click the relevant button in the software or on the cover of the wireless device that you want to connect to the WLAN.
3. Click the WPS button on the right side panel of the router.

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

## WDS

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

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

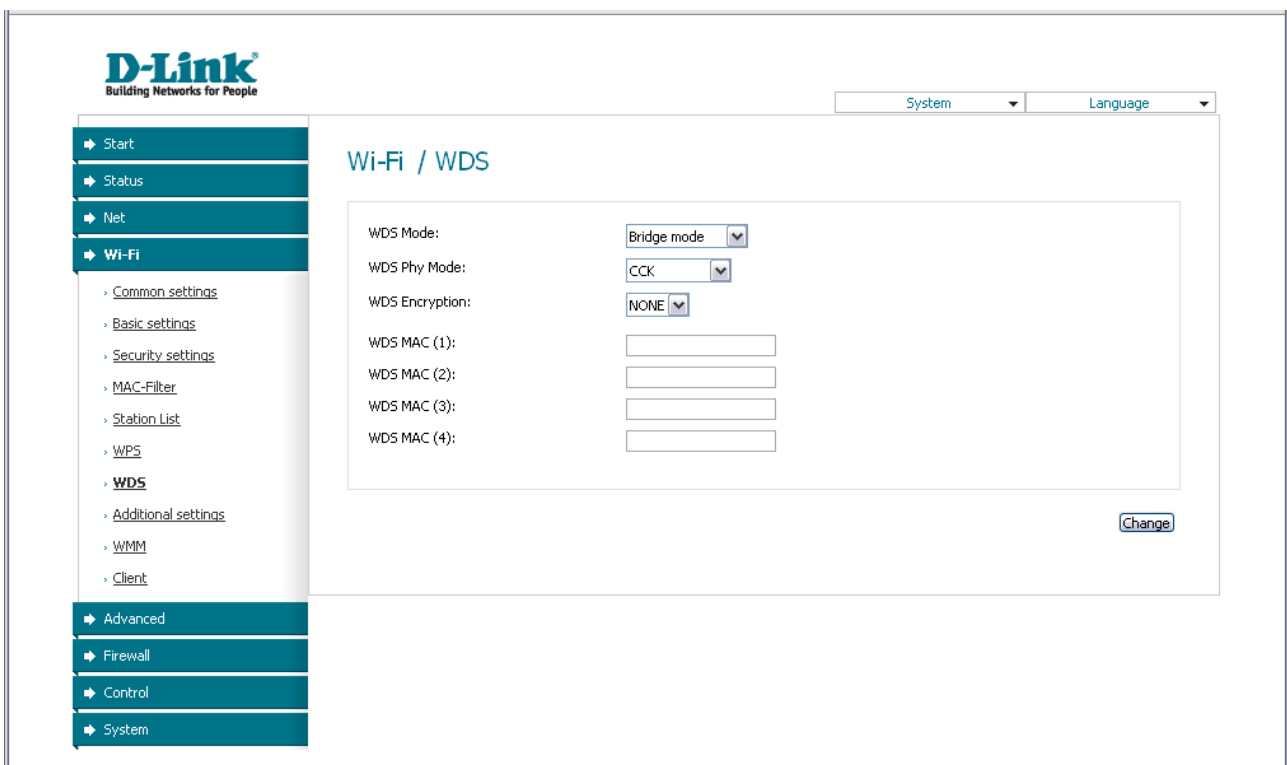


Figure 39. The page for configuring the WDS function.

The following fields are available on the page:

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



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

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

## Additional Settings

On the **Wi-Fi / Additional settings** page, you can define additional parameters for the router's WLAN.

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

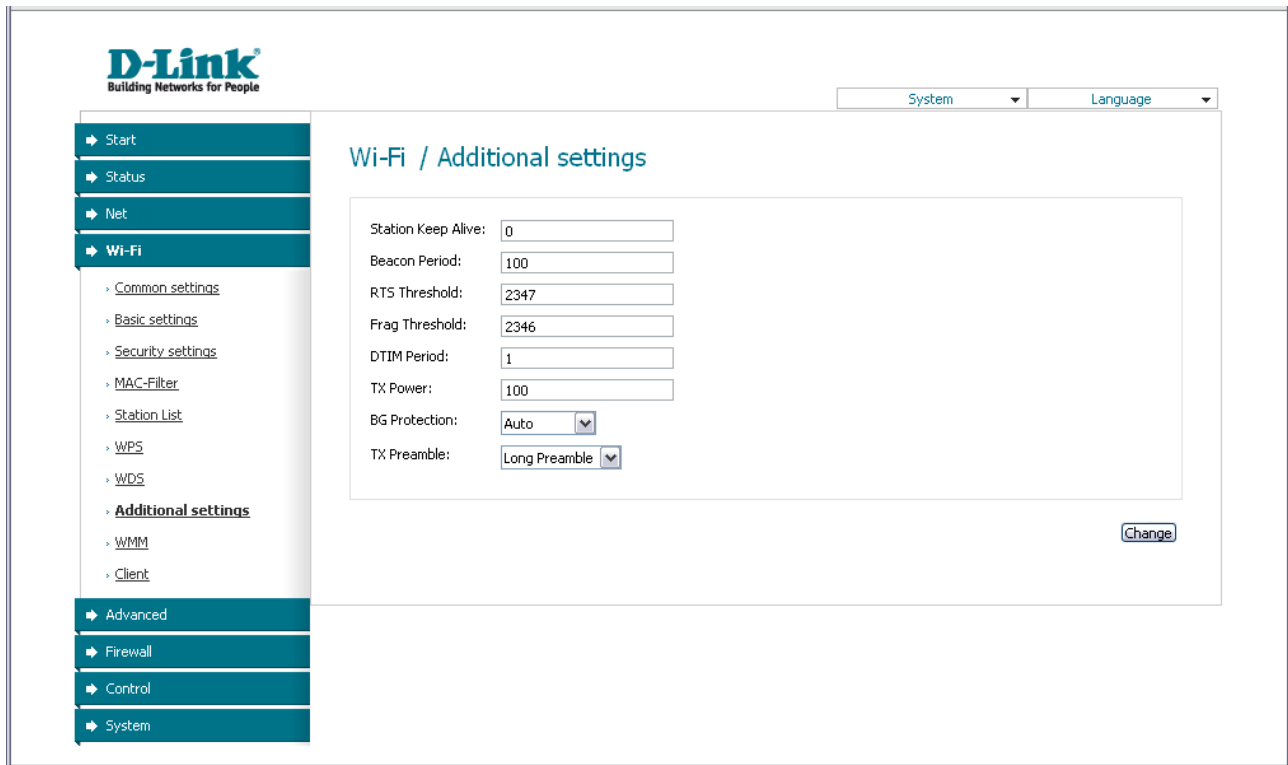


Figure 40. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
<b>Station Keep Alive</b>	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value <b>0</b> is specified, the checking is disabled.
<b>Beacon Period</b>	The time interval (in milliseconds) between packets sent to synchronize the wireless network.
<b>RTS Threshold</b>	The minimum size (in bites) of a packet for which an RTS frame is transmitted.
<b>Frag Threshold</b>	The maximum size (in bites) of a non-fragmented packet. Larger packets are fragmented (divided).
<b>DTIM Period</b>	The time period (in seconds) between sending a DTIM (a message notifying on broadcast or multicast transmission) and data transmission.
<b>TX Power</b>	The router's transmit power (in percentage terms).
<b>BG Protection</b>	<p>The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.</p> <p>Select a value from the drop-down list.</p> <p><b>Auto:</b> The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices).</p> <p><b>Always On:</b> The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).</p> <p><b>Always Off:</b> The protection function is always disabled.</p>
<b>TX Preamble</b>	<p>This parameter defines the length of the CRC block sent by the router when communicating to wireless devices.</p> <p>Select a value from the drop-down list.</p> <p><b>Long Preamble.</b></p> <p><b>Short Preamble</b> (this value is recommended for networks with high-volume traffic).</p>

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

## WMM

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

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

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

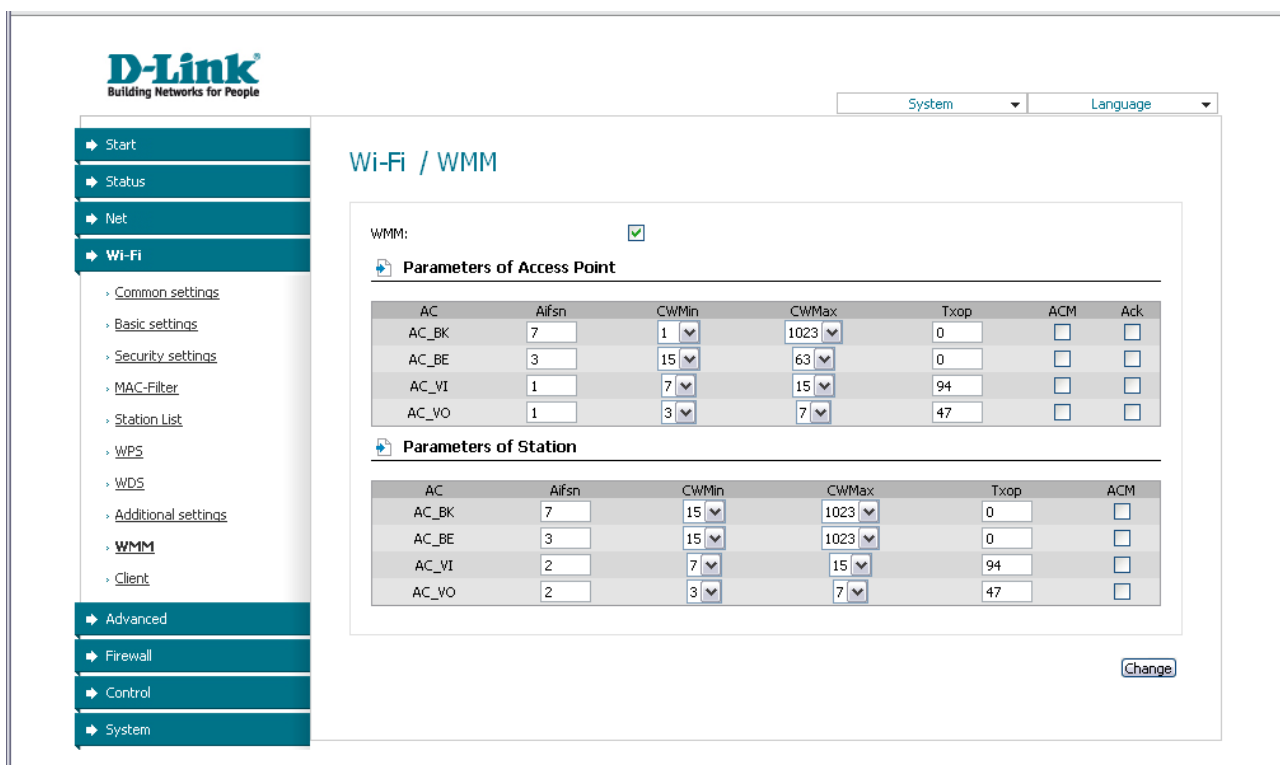


Figure 41. The page for configuring the WMM function.

**!** All needed settings for the WMM function are specified in the router'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 router 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
<b>Aifsn</b>	<i>Arbitrary Inter-Frame Space Number.</i> This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
<b>CWMin/CWMax</b>	<i>Contention Window Minimum/Contention Window Maximum.</i> Both fields influence time delays for the relevant Access Category. The <b>CWMax</b> field value should not be lower, than the <b>CWMin</b> field value. The lower the difference between the <b>CWMax</b> field value and the <b>CWMin</b> field value, the higher is the Access Category priority.
<b>Txop</b>	<i>Transmission Opportunity.</i> The higher the value, the higher is the Access Category priority.
<b>ACM</b>	<i>Admission Control Mandatory.</i> If selected, prevents from using the relevant Access Category.
<b>Ack</b>	<i>Acknowledgment.</i> Answering response requests while transmitting. Displayed only in the <b>Parameters of Access Point</b> section. If not selected, the router answers requests. If selected, the router does not answer requests.

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

## Client

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

As a rule, the client mode is used to connect to a WISP network. All parameters specified on this page should be provided by your WISP.

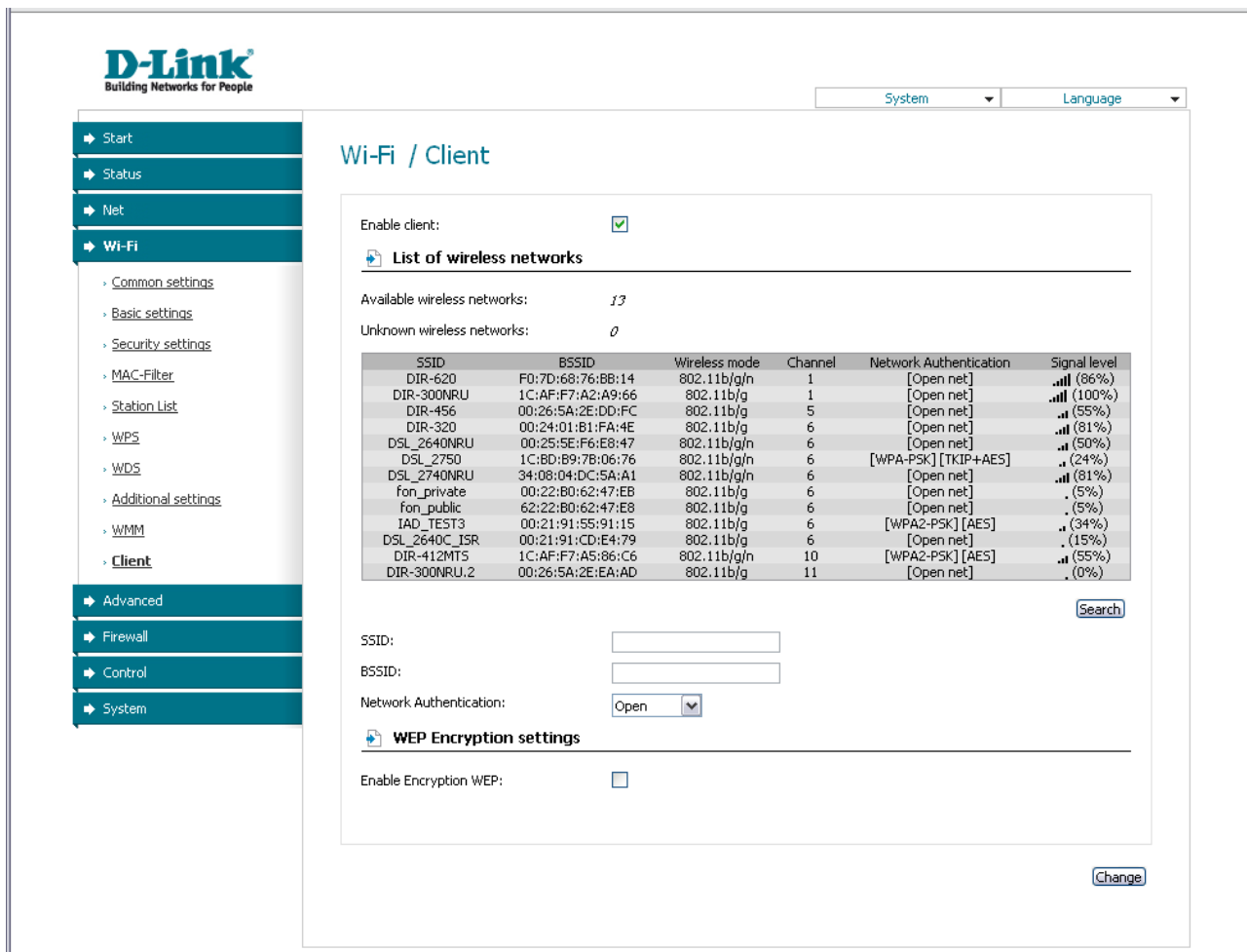


Figure 42. The page for configuring the client mode.

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

Parameter	Description
<b>SSID</b>	The name of the network to which the router connects.
<b>BSSID</b>	The unique identifier of the network to which the router connects.
<b>Network Authentication</b>	The authentication type of the network to which the router connects.

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

Parameter	Description
<b>Enable Encryption WEP</b>	The checkbox activating WEP encryption. When the checkbox is selected, the <b>Default Key ID</b> field and four <b>Encryption Key WEP</b> fields are displayed on the page. For the <b>Shared</b> authentication type the checkbox is always selected.
<b>Default Key ID</b>	The number of the key (from first to fourth) which will be used for WEP encryption.
<b>Encryption Key WEP (1-4)</b>	Keys for WEP encryption. The router uses the key selected from the <b>Default Key ID</b> 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** or **WPA2-PSK** authentication type is selected, the following fields are available:

Parameter	Description
<b>WPA Encryption</b>	An encryption method: <b>TKIP</b> , <b>AES</b> , or <b>TKIP+AES</b> .
<b>Encryption Key PSK</b>	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** or **WPA2-PSK** authentication types, fill in the **Encryption Key PSK** field and click the **Change** button.

If the router 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 router: define static routes and rules for remote access to the web-based interface, add name servers, enable the UPnP function, configure a DDNS service, allow the router to use IGMP, and create groups of ports for virtual networks.

### VLAN

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

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

- **lan**: for the LAN interface; it includes ports 1-4 and the wireless interface (if the wireless network is splitted into parts, the first part);
- **wan**: for the WAN interface; it includes port 5.

The **VLAN ID** parameter is not specified for both groups. Such a setting means that these groups of ports are not assigned to any VLAN.

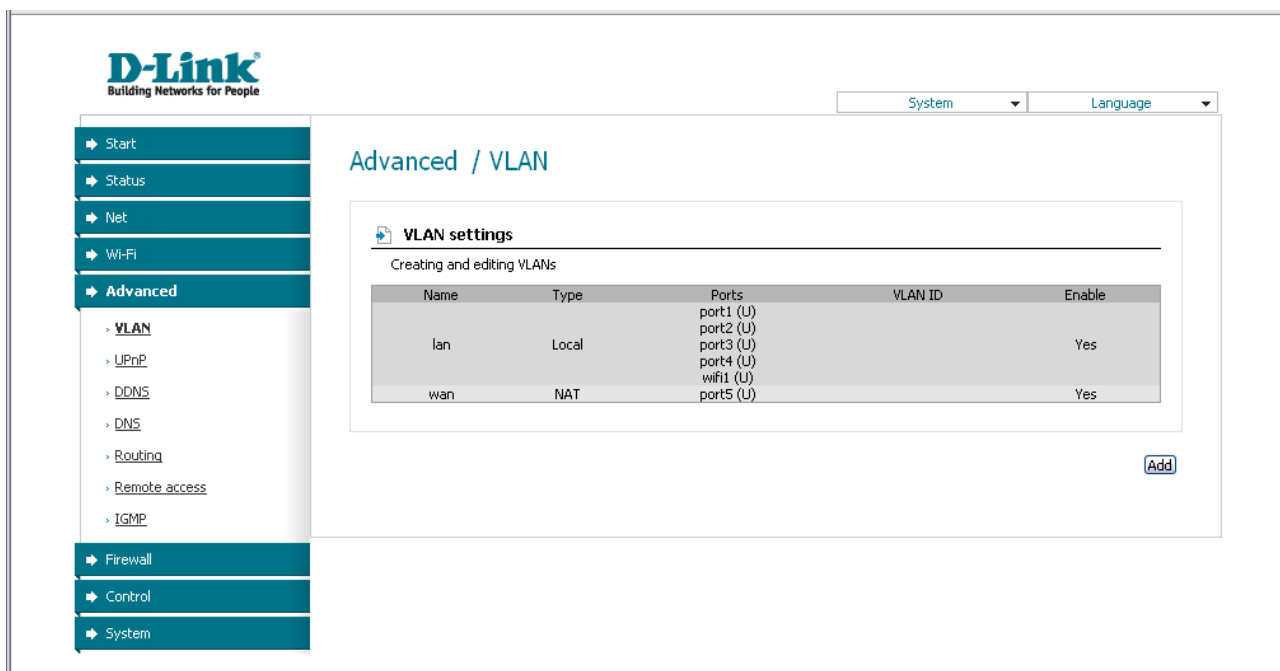


Figure 43. The **Advanced / VLAN** page.

To create a new group for VLAN, click the **Add** button.

- ! If you want to create a group including LAN ports or the wireless network of the router, first delete relevant records from the **lan** group on this page.

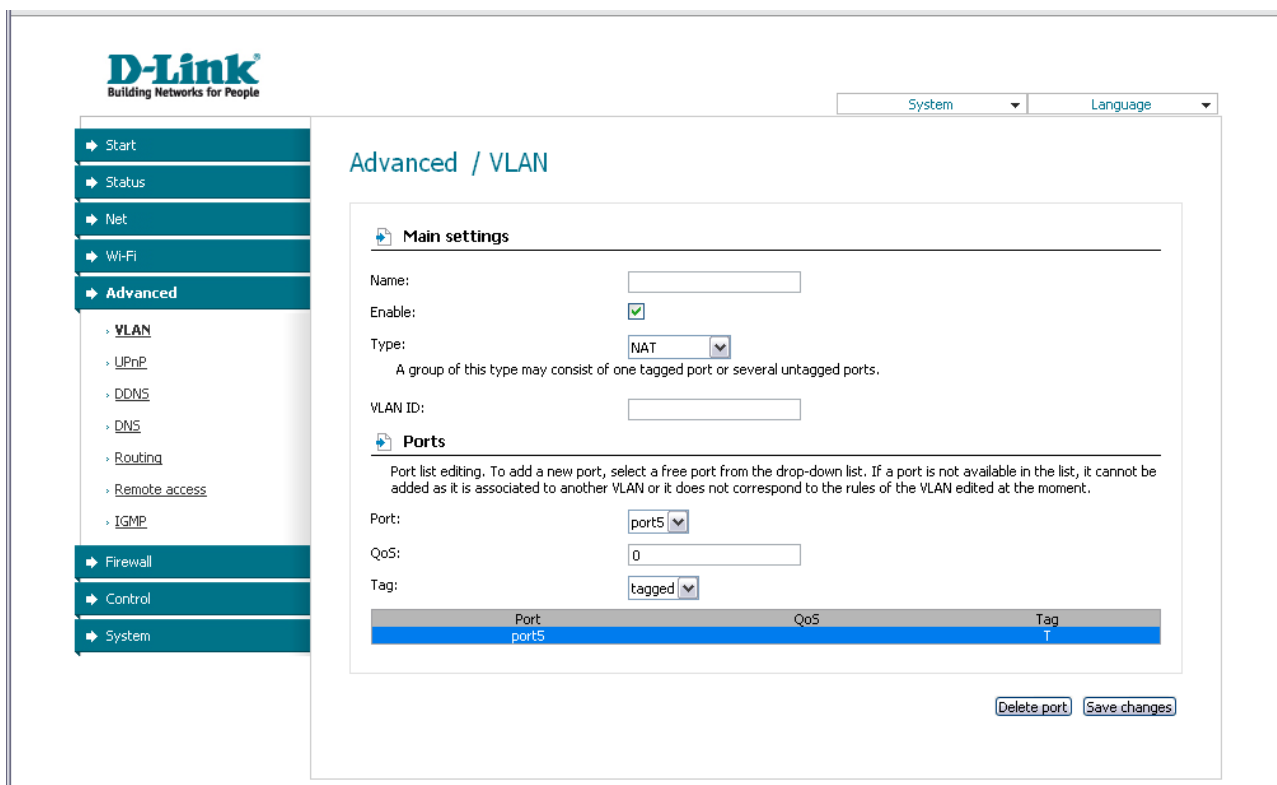


Figure 44. The page for adding a group of ports for VLAN.

You can specify the following parameters:

Parameter	Description
<b>Main settings</b>	
<b>Name</b>	A name for the port for easier identification.
<b>Enable</b>	Select the checkbox to allow using this group of ports.
<b>Type</b>	<p>The type of the VLAN which identifier is specified in the <b>VLAN ID</b> field.</p> <p><b>Local.</b> The group of this type is a channel used to connect local clients to the router. It is mostly used to connect different types of clients, which require separate connection settings.</p> <p><b>NAT.</b> The group of this type is an external connection with address translation. It is mostly used to connect to the Internet. Later the VLAN which identifier is specified in the <b>VLAN ID</b> field is used to create a WAN connection of the IPoE or PPPoE type (on the <b>Net / Connections</b> page).</p> <p><b>Transparent.</b> The group of this type is a transparent connection between an internal port and an external connection. It is mostly used to connect IPTV set-top boxes.</p>

<b>VLAN ID</b>	An identifier of the VLAN to which this group of ports will be assigned.
<b>Ports</b>	
<b>Port</b>	From the list, select an available value (a physical port of the router, the wireless interface, or, if the wireless network is splitted into parts, a part of the wireless network) to assign it to this group. The port will be displayed in the table at the bottom of the page.
<b>QoS</b>	A priority tag for the traffic transmitted through the port highlighted in the table at the bottom of the page.
<b>Tag</b>	Select a value for the port highlighted in the table at the bottom of the page: <ul style="list-style-type: none"><li>• <b>tagged,</b></li><li>• <b>untagged.</b></li></ul>

Click the **Save changes** button.

Click the **Delete port** button to delete the port highlighted in the table at the bottom of the page.

Click the **Delete VLAN** button to delete this group of ports form the system.



For further use of groups of ports for VLAN it is required to save the changed settings to the non-volatile memory of the router and reboot it (click the **Save&Reboot** line in the top-page menu displayed when the mouse pointer is over the **System** caption).

## 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 router.

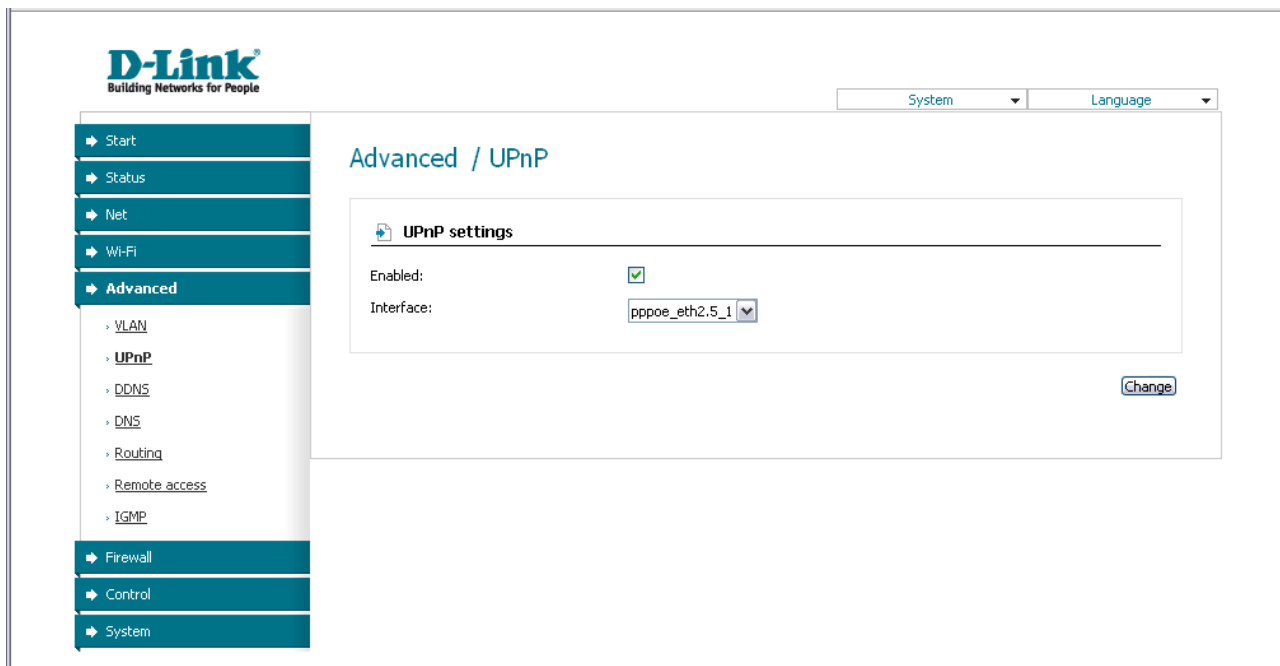


Figure 45. The **Advanced / UPnP** page.

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 router, select the **Enabled** checkbox, select an interface for which the router'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.

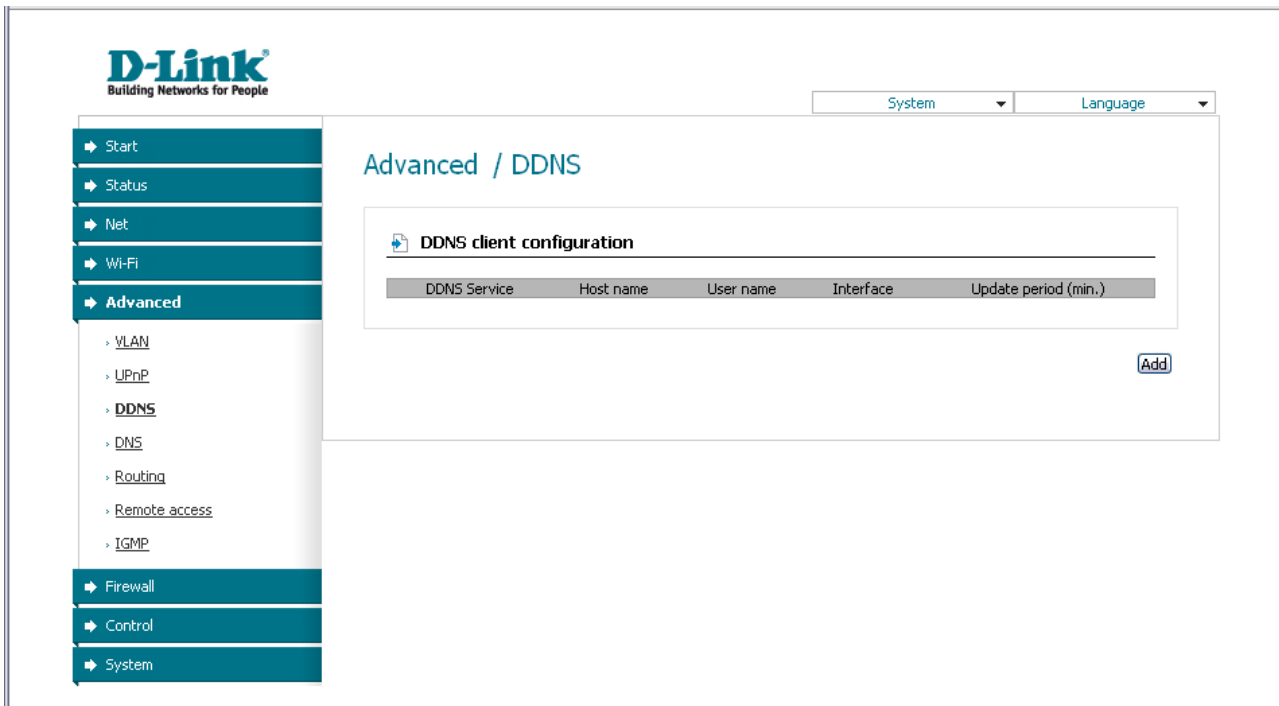


Figure 46. The **Advanced / DDNS** page.

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

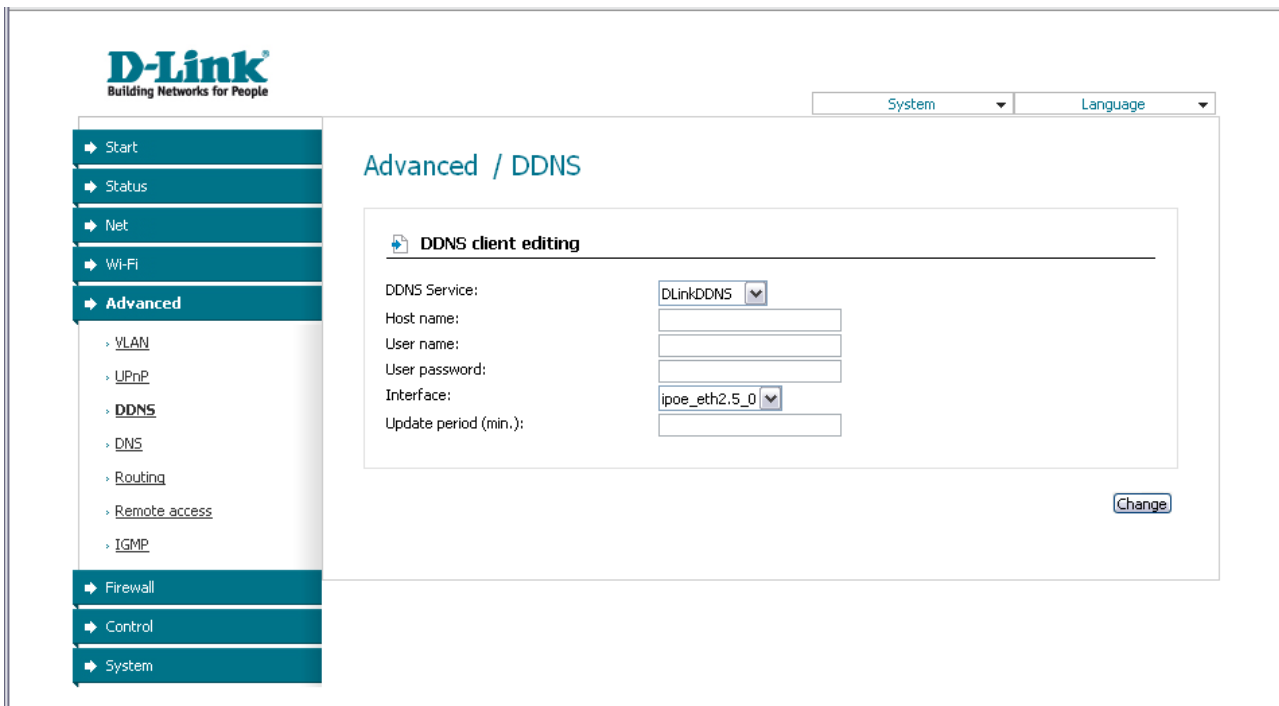


Figure 47. The page for adding a DDNS service.

You can specify the following parameters:

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

Click the **Change** button.

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

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

## DNS

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

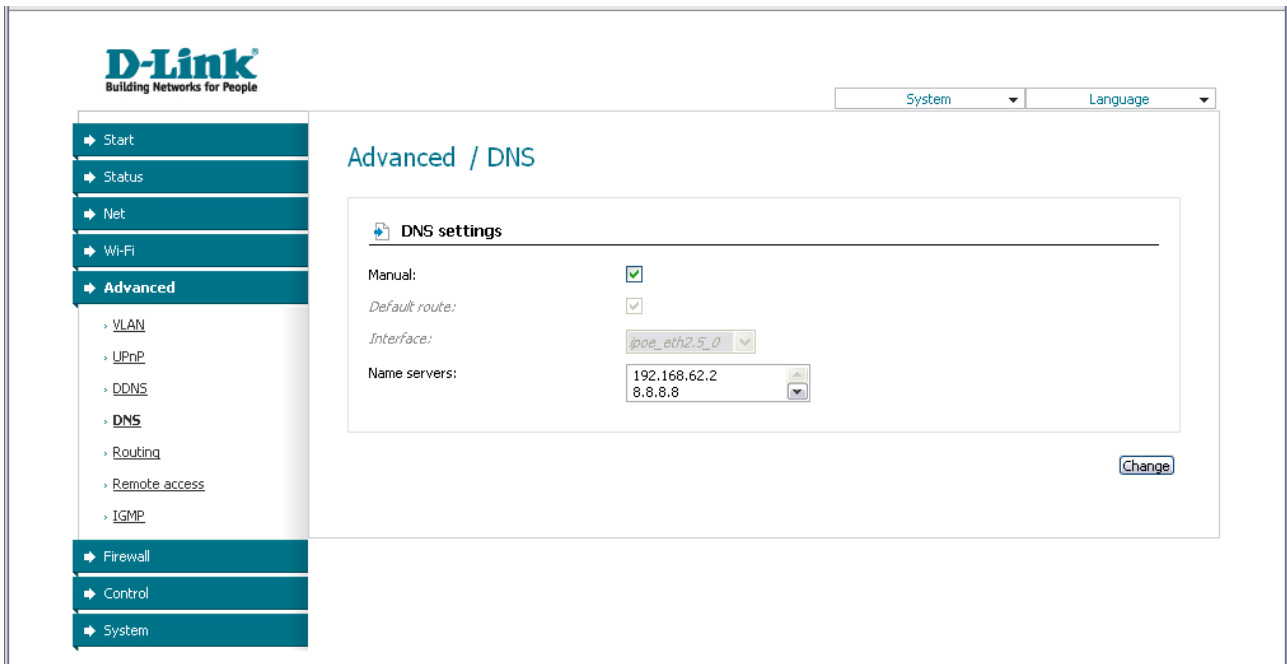


Figure 48. The **Advanced / DNS** page.

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 router 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 router could use the connection set as the default gateway (on the **Net / Connections** page) to obtain DNS server addresses, and click the **Change** button.

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

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

## Routing

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

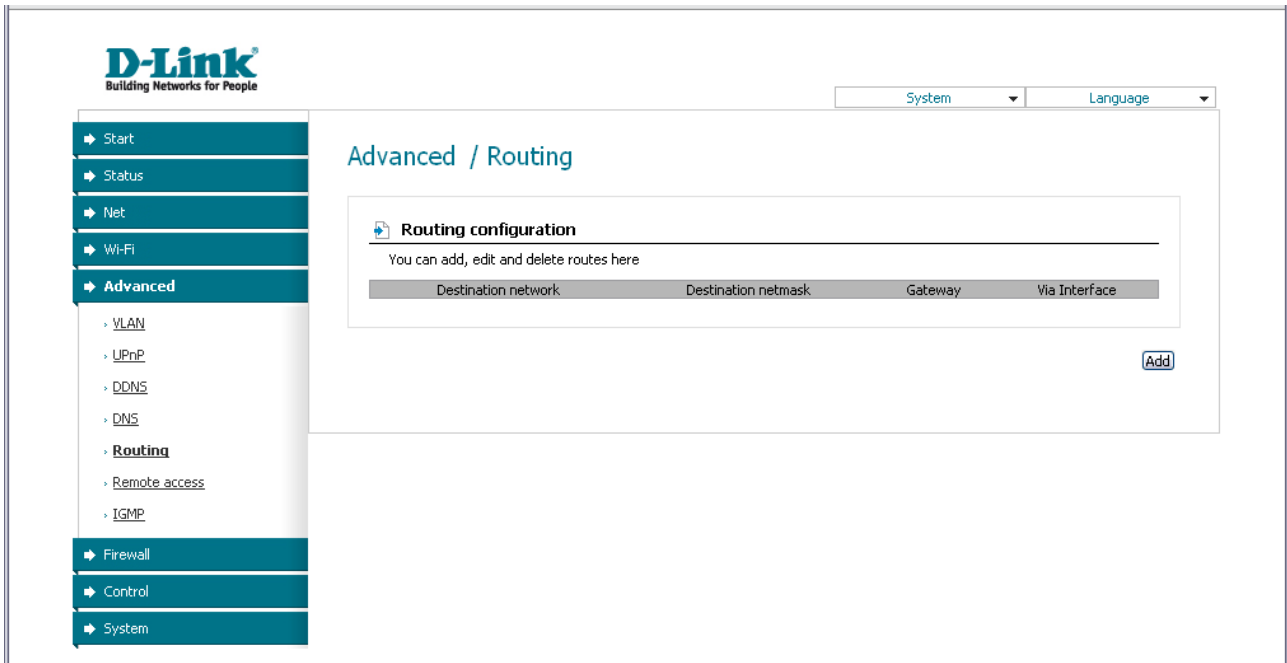


Figure 49. The **Advanced / Routing** page.

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



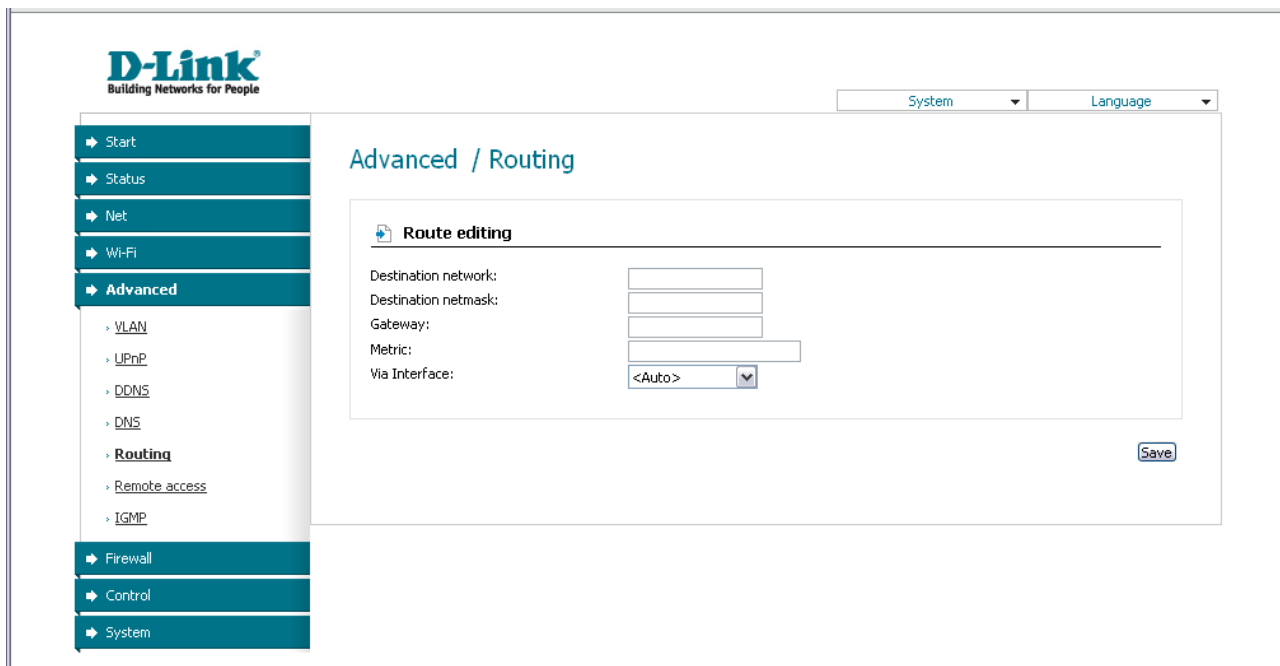


Figure 50. The page for adding a static route.

You can specify the following parameters:

Parameter	Description
<b>Destination network</b>	A destination network to which this route is assigned.
<b>Destination netmask</b>	The destination network mask.
<b>Gateway</b>	An IP address through which the destination network can be accessed.
<b>Metric</b>	A metric for the route. The lower the value, the higher is the route priority. <i>Optional.</i>
<b>Via Interface</b>	Select an interface through which the destination network can be accessed from the drop-down list. If you have selected the <b>&lt;Auto&gt;</b> value of this drop-down list, the router itself sets the interface on the basis of data on connected networks.

Click the **Save** button.

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

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

## Remote Access

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

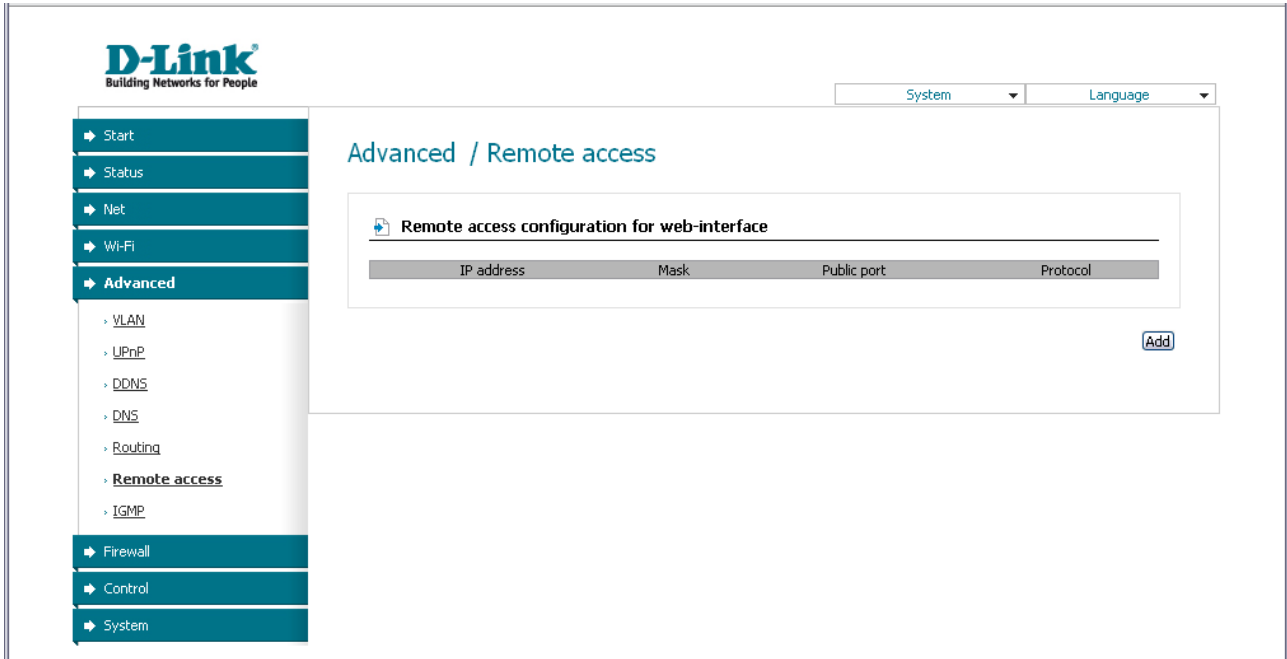


Figure 51. The **Advanced / Remote access** page.

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

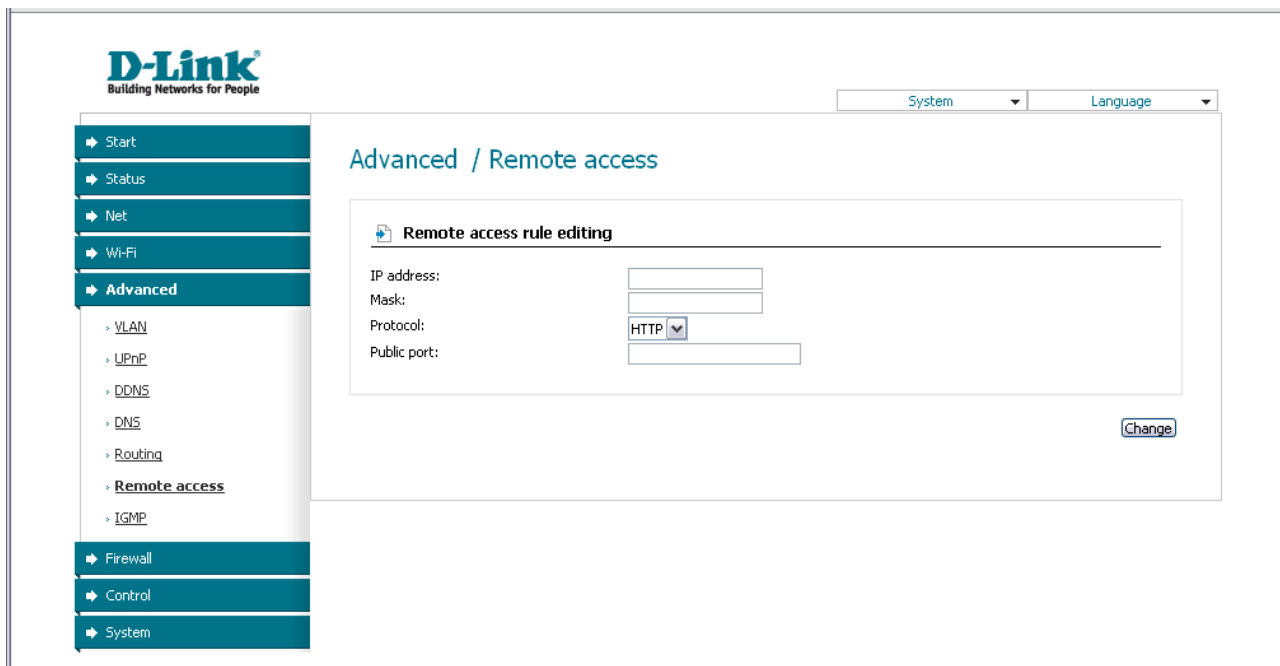


Figure 52. The page for adding a rule for remote management.

You can specify the following parameters:

Parameter	Description
<b>IP address</b>	A host or a subnet to which the rule is applied.
<b>Mask</b>	The mask of the subnet.
<b>Protocol</b>	The protocol available for remote management of the router.
<b>Public port</b>	An external port of the router. 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 router.

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

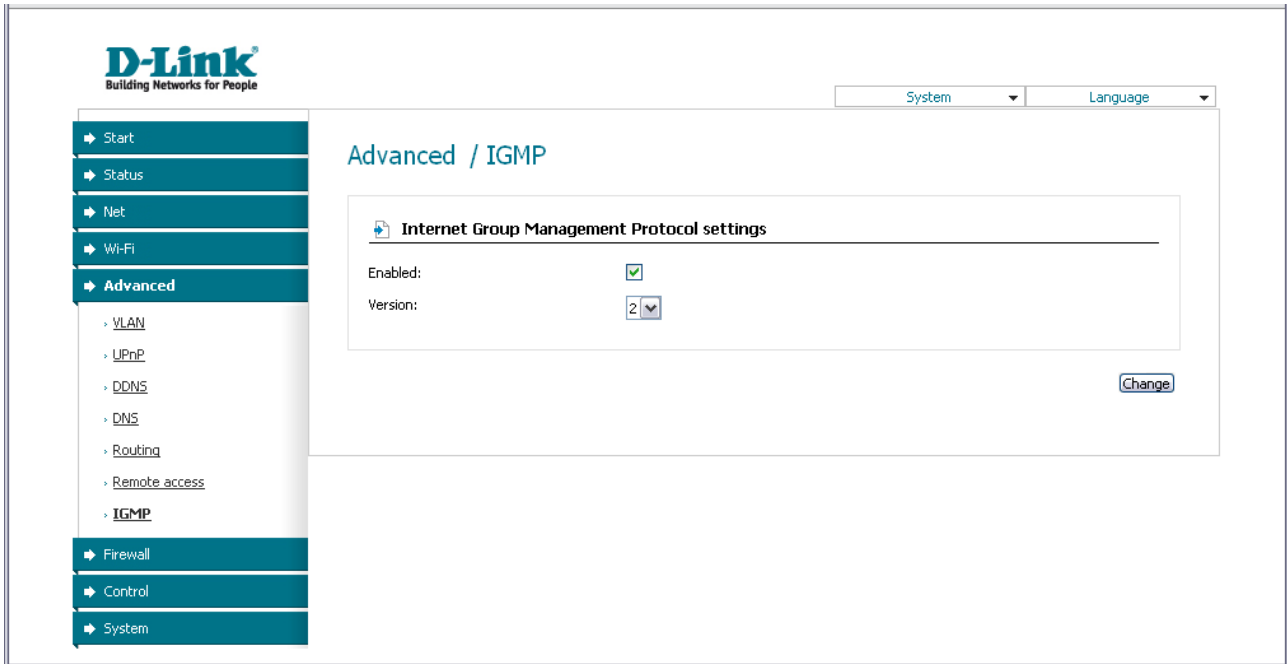


Figure 53. The **Advanced / IGMP** page.

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 router: add rules for IP filtering, define a DMZ-zone, create virtual servers, and configure MAC filters.

### IP Filters

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

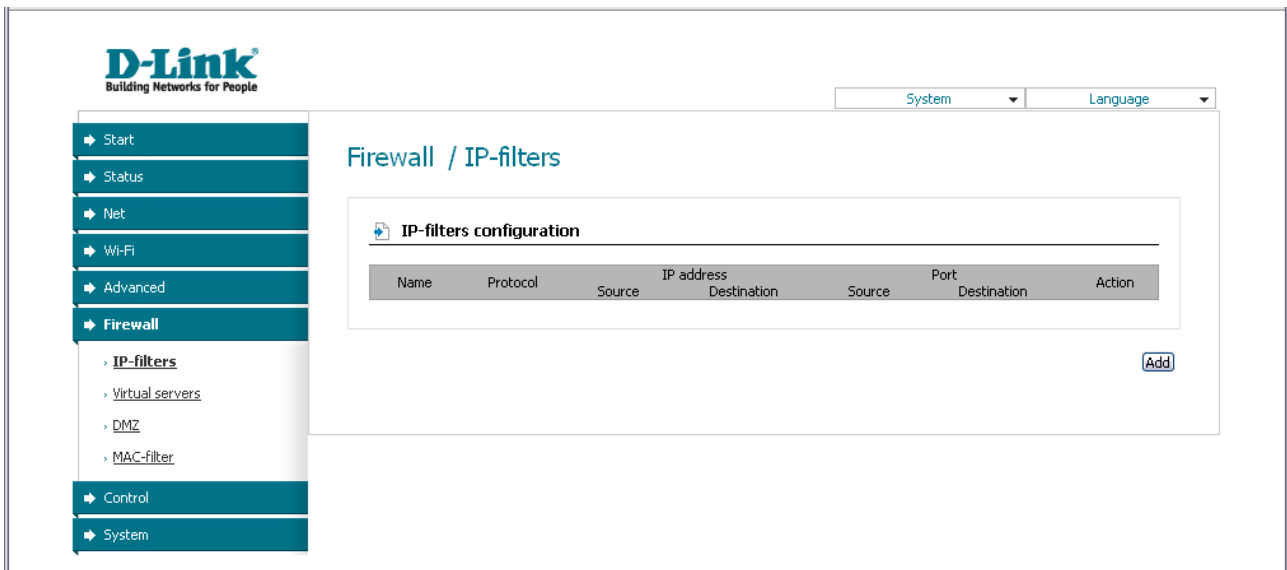


Figure 54. The **Firewall / IP filters** page.

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

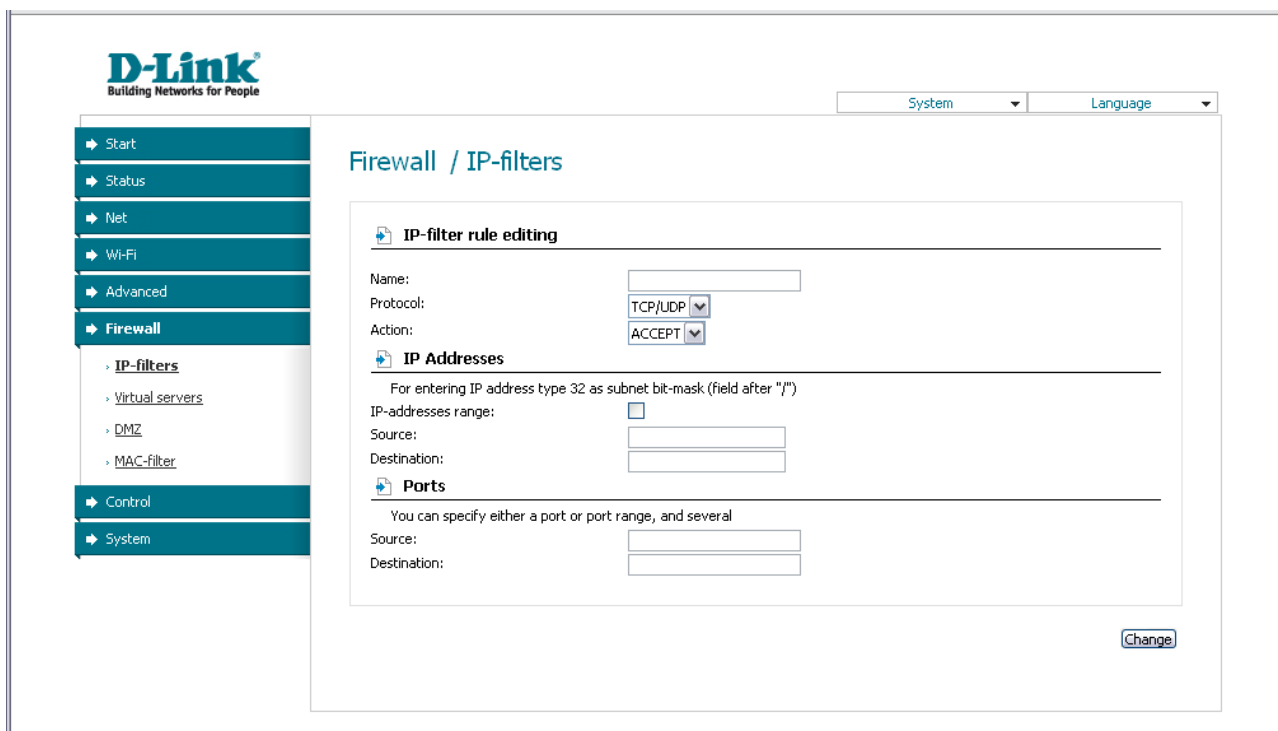


Figure 55. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
<b>IP-filter rule editing</b>	
<b>Name</b>	A name for the rule for easier identification.
<b>Protocol</b>	A protocol for network packet transmission. Select a value from the drop-down list.
<b>Action</b>	Select an action for the rule. <b>ACCEPT:</b> Allows packet transmission in accordance with the criteria specified by the rule. <b>DROP:</b> Denies packet transmission in accordance with the criteria specified by the rule.
<b>IP Addresses</b>	
<b>IP address range</b>	Select the checkbox if you want to specify a range of IP addresses as the source or destination IP address.
<b>Source</b>	The source host/subnet IP address. To specify an IP address add <b>/32</b> .
<b>Destination</b>	The destination host/subnet IP address. To specify an IP address add <b>/32</b> .

Parameter	Description
<b>Ports</b>	
<b>Source</b>	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.
<b>Destination</b>	A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

Click the **Change** button.

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

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

## Virtual Servers

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

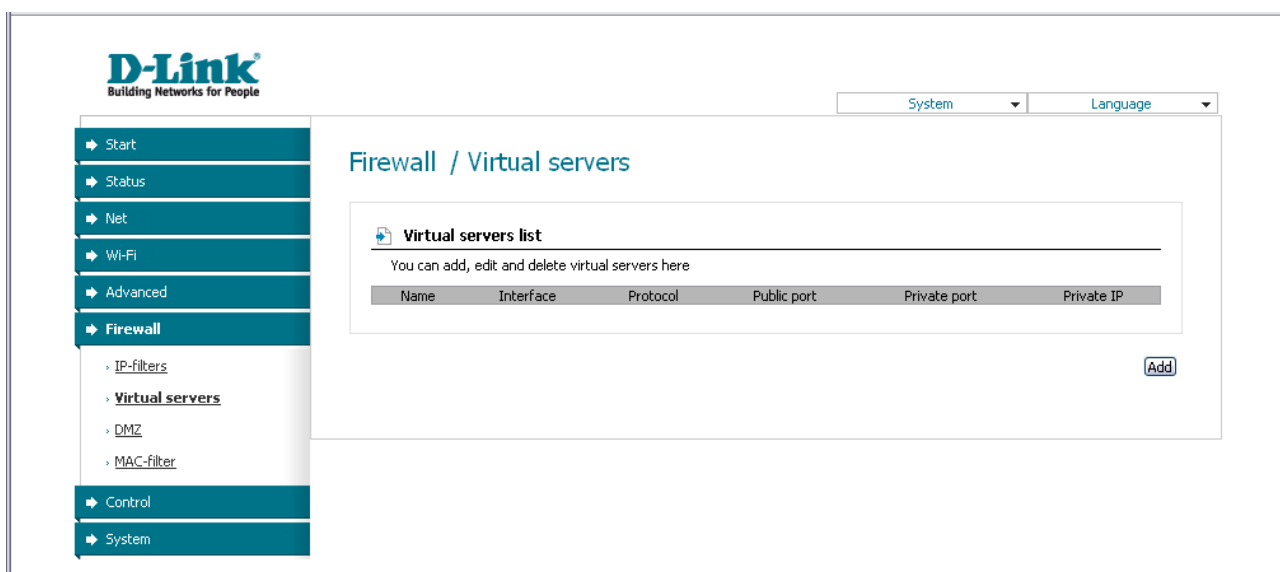


Figure 56. The **Firewall / Virtual servers** page.

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

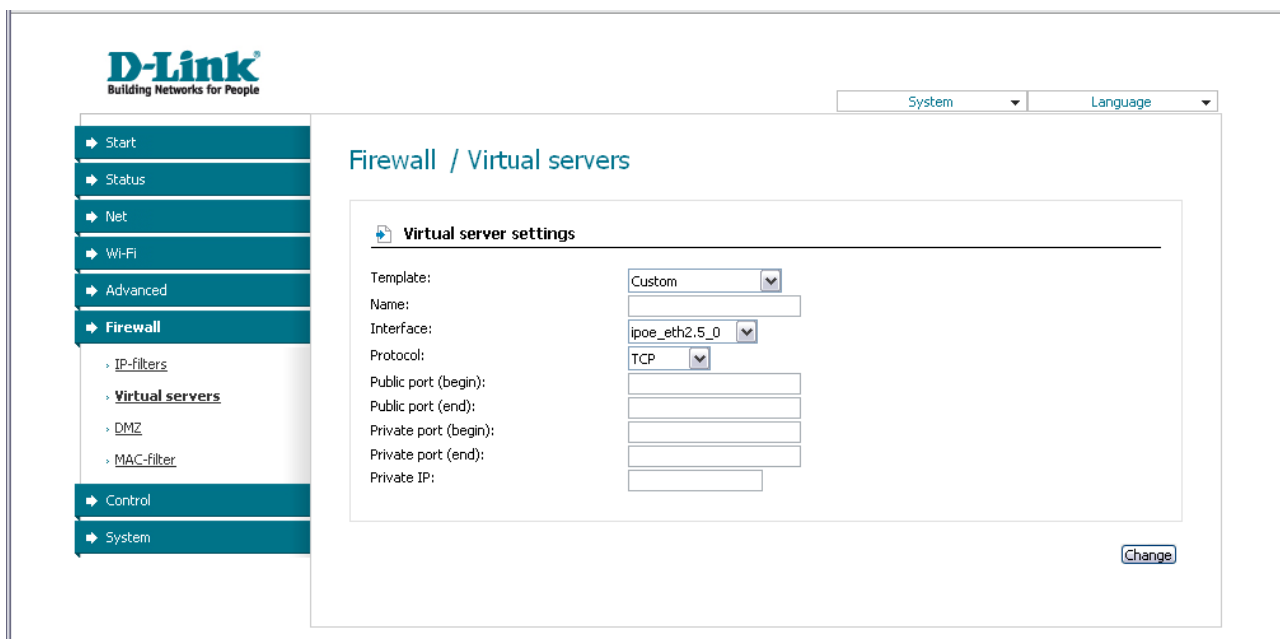


Figure 57. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
<b>Template</b>	Select a virtual server template from the drop-down list, or select <b>Custom</b> to specify all parameters of the new virtual server manually.
<b>Name</b>	A name for the virtual server for easier identification. You can specify any name.
<b>Interface</b>	A WAN connection to which this virtual server will be assigned.
<b>Protocol</b>	A protocol that will be used by the new virtual server. Select a value from the drop-down list.
<b>Public port (begin)/ Public port (end)</b>	A port of the router from which traffic is directed to the IP address specified in the <b>Private IP</b> 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 <b>Public port (begin)</b> field and leave the <b>Public port (end)</b> field blank.
<b>Private port (begin)/ Private port (end)</b>	A port of the IP address specified in the <b>Private IP</b> field to which traffic is directed from the <b>Public port</b> . Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the <b>Private port (begin)</b> field and leave the <b>Private port (end)</b> field blank.
<b>Private IP</b>	The IP address of the server from the local area 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 router, the DMZ implements the capability to transfer a request coming to a port of the router from the external network to a specified host of the internal network.

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

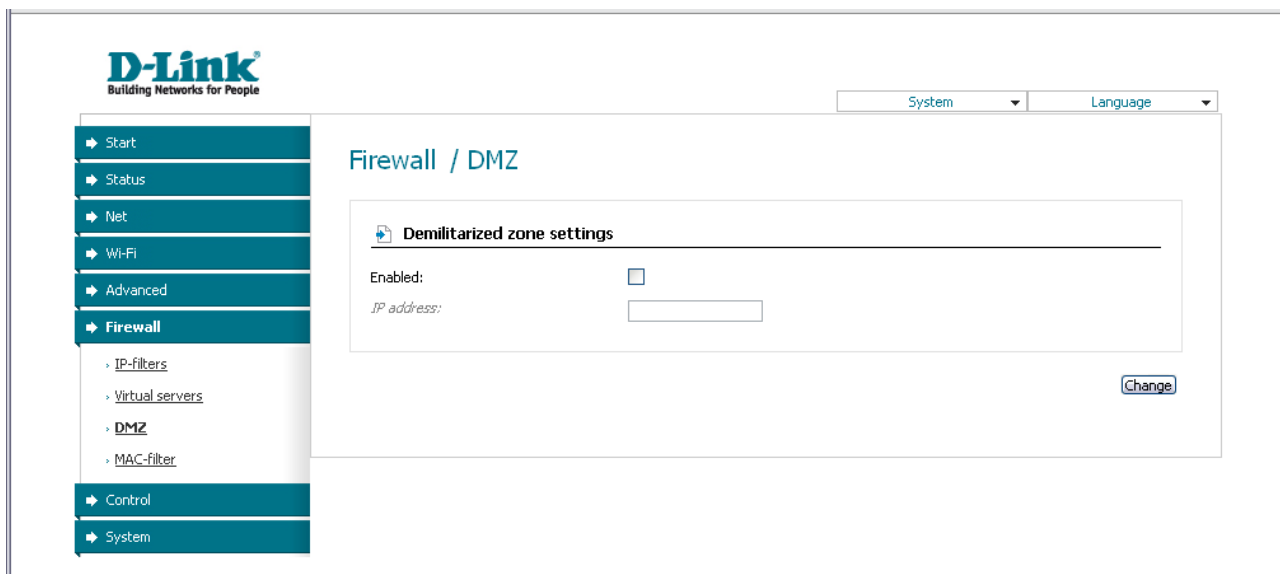


Figure 58. The **Firewall / DMZ** page.

To enable the DMZ, select the **Enabled** checkbox, enter the IP address of a host from your network in the **IP address** field, and click the **Change** button.

Note that when the DMZ is enabled, all traffic coming to a port of the WAN interface of the router 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 router's local network, then entering **http://router\_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 router's LAN.

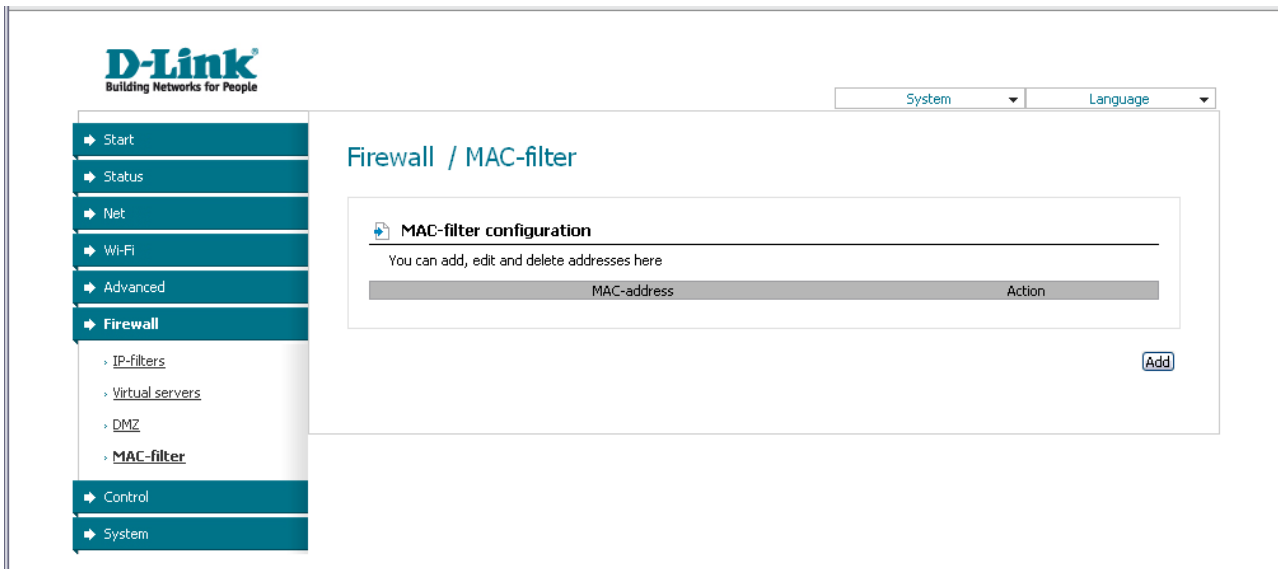


Figure 59. The **Firewall / MAC-filter** page.

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

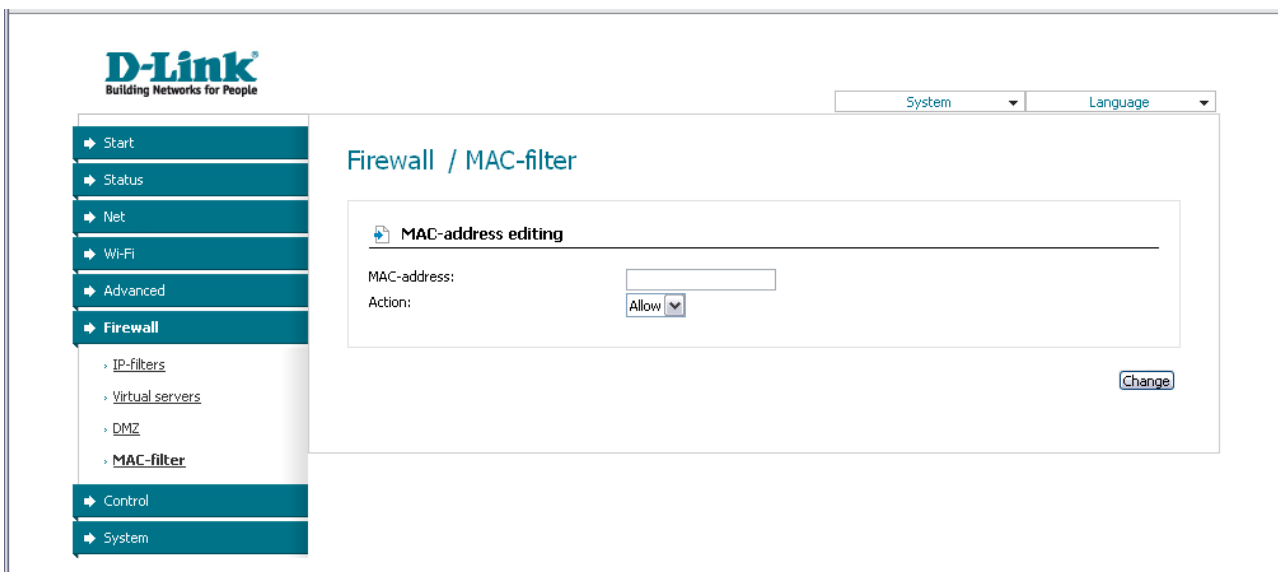


Figure 60. The page for adding an address for the MAC filter.

On the opened page, enter the MAC address of the device from the router's LAN in the **MAC-address** field and select the **Deny** value from the **Action** drop-down list. Then 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 URL addresses which will be unavailable for users of the LAN.

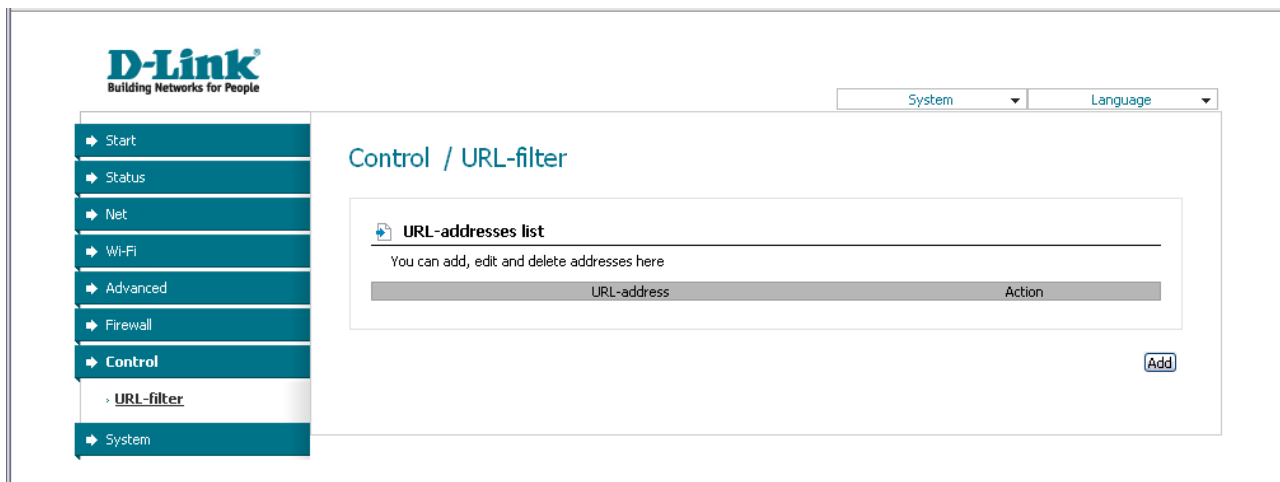


Figure 61. The **Control / URL-filter** page.

In order to forbid access to a URL address, click the **Add** button.

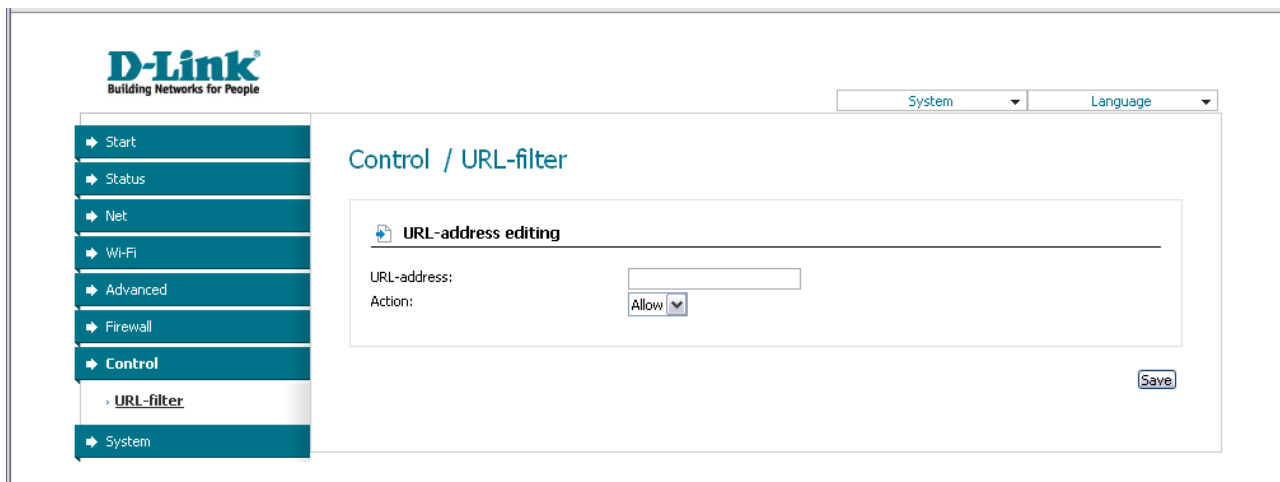


Figure 62. A page for adding a forbidden URL.

On the opened page, enter a URL address which should be forbidden for your LAN users in the **URL-address** field, select the **Deny** value from the **Action** drop-down list, then click the **Save** button.

To remove a URL address from the list of forbidden addresses, click the relevant link. On the opened page, click the **Delete** button.

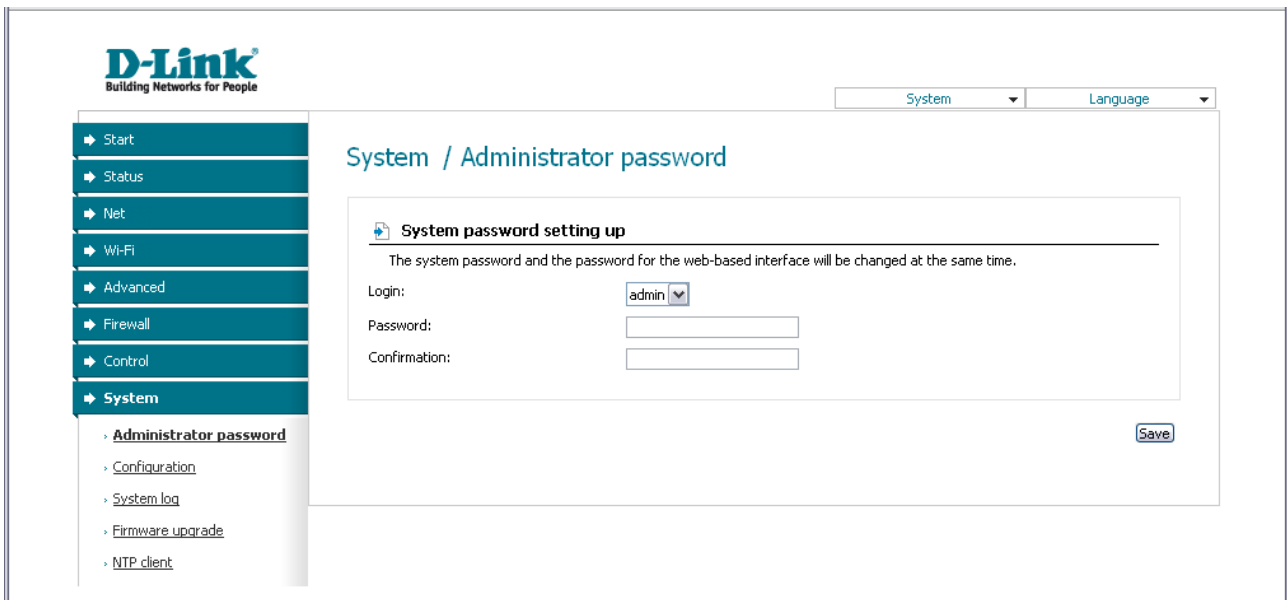
## System

In this menu you can save the current settings to the non-volatile memory, create a backup of the router's configuration, restore the router's configuration from a previously saved file, restore the factory default settings, view the system log, configure automatic synchronization of the system time, update the firmware of the router, and change the password used to access its settings.

### 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 router 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 router.



The screenshot shows the D-Link web interface. On the left is a navigation menu with options: Start, Status, Net, Wi-Fi, Advanced, Firewall, Control, and System. Under the System menu, 'Administrator password' is selected. The main content area is titled 'System / Administrator password' and contains a section for 'System password setting up'. A note states: 'The system password and the password for the web-based interface will be changed at the same time.' Below this note are three input fields: 'Login:' with a dropdown menu showing 'admin', 'Password:', and 'Confirmation:'. A 'Save' button is located at the bottom right of the form.

Figure 63. 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 router's configuration from a previously created file.

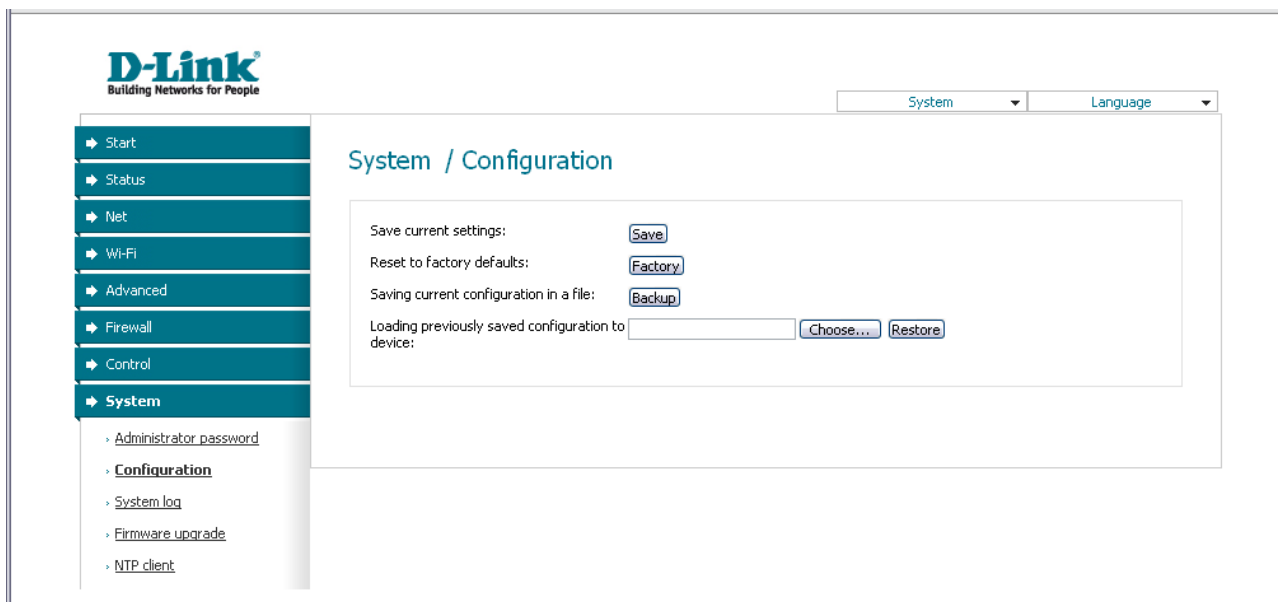


Figure 64. The **System / Configuration** page.

The following buttons are available on the page:

Control	Description
<b>Save</b>	Click the button to save settings to the non-volatile memory. Please, save settings every time you change the router's parameters. Otherwise the changes will be lost upon hardware reboot of the router.
<b>Factory</b>	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware Reset button (see the <i>Saving and Restoring Settings</i> section, page 21).
<b>Backup</b>	Click the button and follow the dialog box appeared to save the configuration (all settings of the router) to your PC.
<b>Restore</b>	Click the button to upload a previously saved configuration (all settings of the router) from a file on your PC. Click the <b>Choose/Browse</b> <sup>1</sup> 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.

<sup>1</sup> The name of the button depends upon the web browser that you use.

## System Log

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

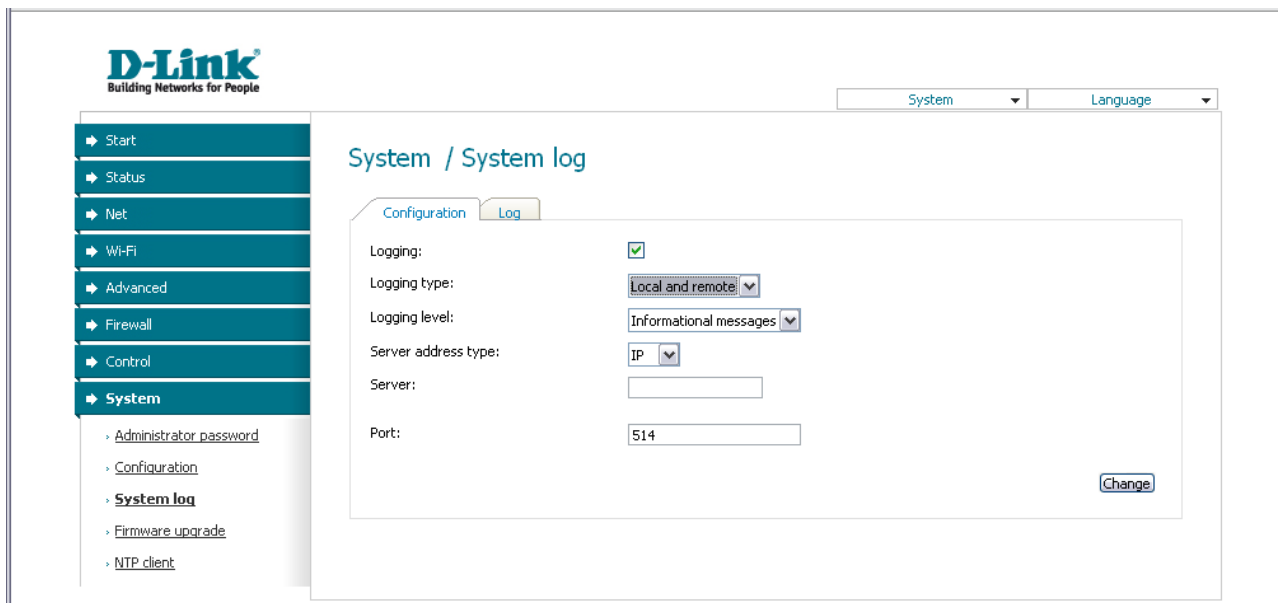


Figure 65. The **System / System log** page. The **Configuration** tab.

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

Control	Description
<b>Logging type</b>	<p>Select a type of logging from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Local</b>: the system log is stored in the router's memory (and displayed on the <b>Log</b> tab). When this value is selected, the <b>Server address type</b>, <b>Server</b>, and <b>Port</b> fields are not displayed.</li> <li>• <b>Remote</b>: the system log is sent to the remote host specified in the <b>Server</b> field.</li> <li>• <b>Local and remote</b>: the system log is stored in the router's memory (and displayed on the <b>Log</b> tab) and sent to the remote host specified in the <b>Server</b> field.</li> </ul>
<b>Logging level</b>	Select a type of messages and alerts/notifications to be logged.
<b>Server address type</b>	From the drop-down list, select the <b>IP</b> value to specify an IP address of a host from the local or global network, or the <b>URL</b> value to specify a URL address of a remote server.
<b>Server</b>	The IP or URL address of the host from the local or global network, to which the system log will be sent.

Control	Description
<b>Port</b>	A port of the host specified in the <b>Server</b> field. By default, the value <b>514</b> is specified.

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

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

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

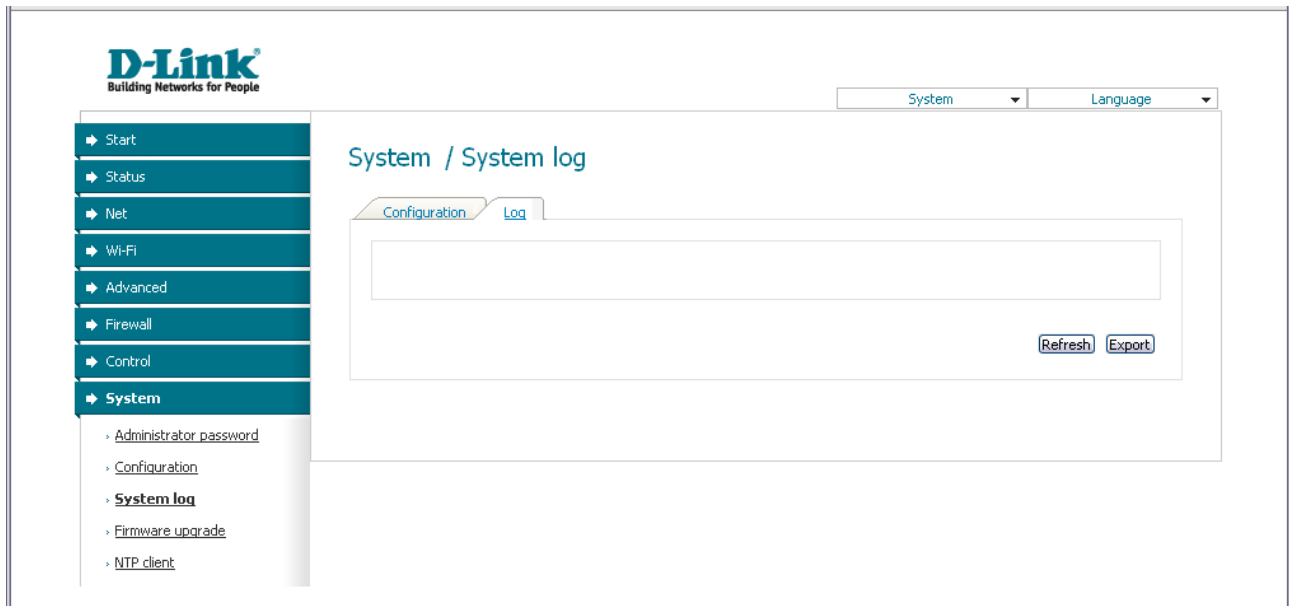


Figure 66. The **System / System log** page. The **Log** tab.

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 router.

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

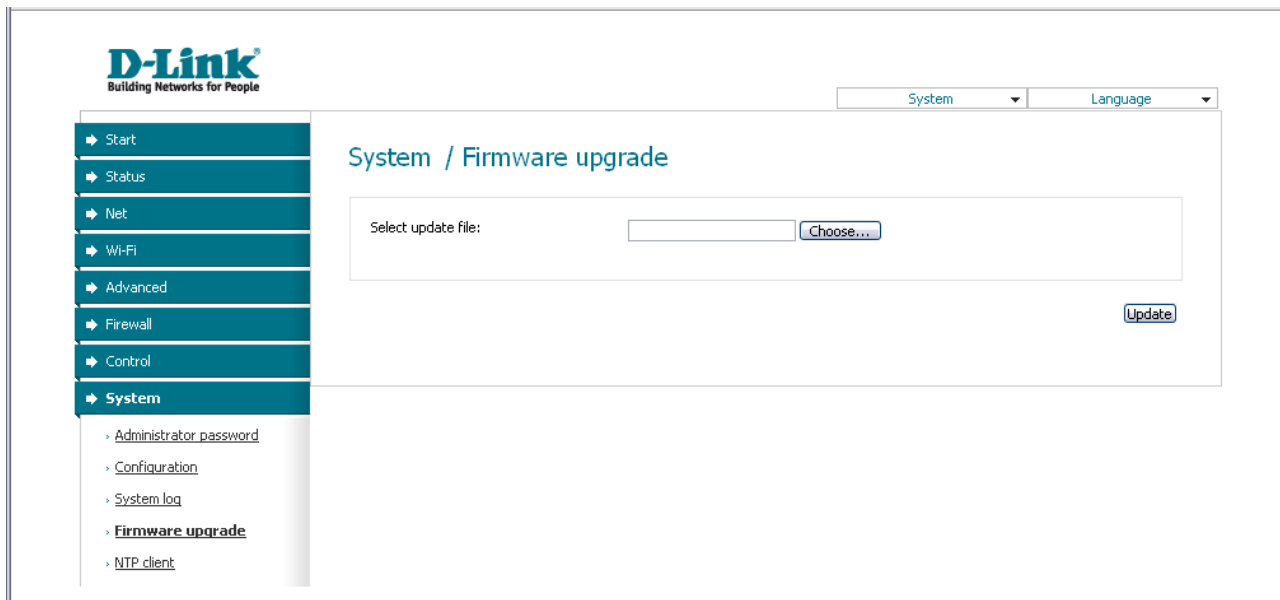


Figure 67. The **System / Firmware upgrade** page.

The current version of the router'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 router before the firmware upgrade is completed. This may cause the device breakdown.

1. Download a new version of the firmware from [www.dlink.ru](http://www.dlink.ru).
2. Click the **Choose/Browse**<sup>2</sup> button on the **System / Firmware upgrade** page to locate the new firmware file.
3. Click the **Update** button to upgrade the firmware of the router.
4. Wait until the router 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 router is rebooted. Log into the web-based interface, using the default IP address, login and password (**192.168.0.1**, **admin**, **admin**).

<sup>2</sup> 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.

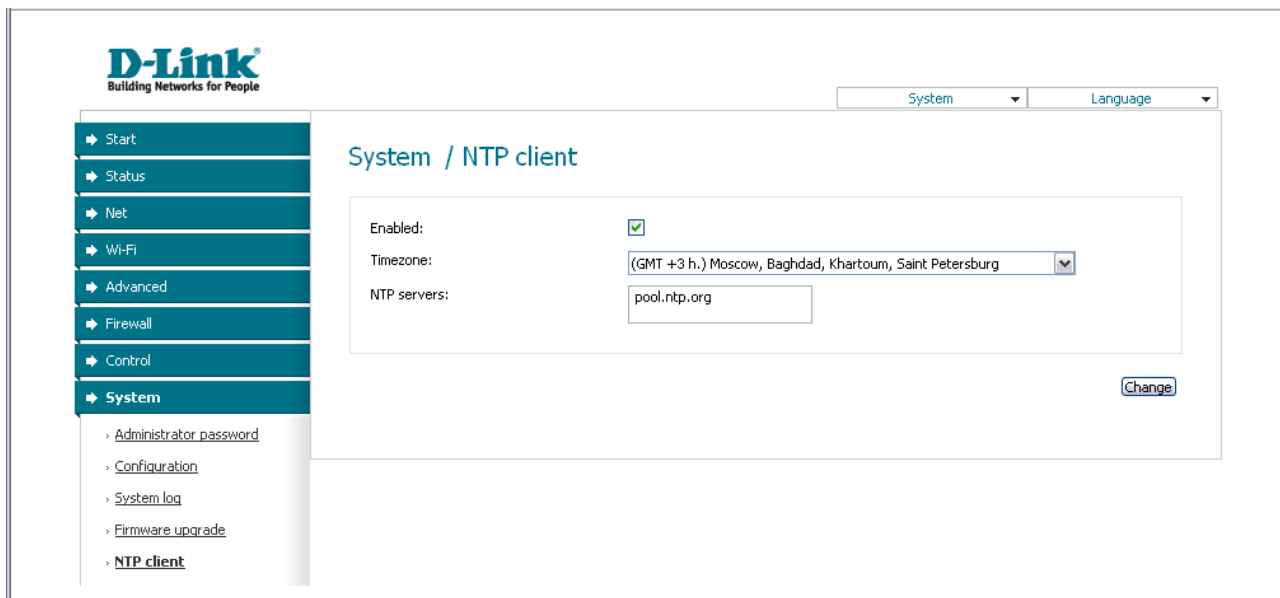


Figure 68. The **System / NTP client** page.

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 router 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.

## CHAPTER 5. OPERATION GUIDELINES

### ***Safety Instructions***

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

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

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

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

Do not open the cover of the router. 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 DIR-300NRU 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 DIR-300NRU 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 router, access points, and computers 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 router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone is not in use.

## ***Connecting to Cable or DSL Modem***

If you need to connect the router to a cable or DSL modem, do the following.

1. Place the router in an open location in the supposed center of your wireless network. Do not plug the power adapter into the router.
2. Turn off your PC.
3. Unplug the Ethernet cable (that connects your PC to your modem) from your computer and place it into the INTERNET port of your router.
4. Plug another Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port of your PC.
5. Turn on your modem. Wait until the modem is booted (about 30 seconds).
6. Plug the power adapter to the router and connect to an electrical outlet or power strip. Wait until the router is booted (about 30 seconds).
7. Turn on your PC.
8. Verify the LEDs of the router. The following LEDs should be on: **Power**, **LAN** (of the relevant Ethernet port), and **Internet**. If not, make sure that your computer, modem, and router are powered on and the relevant cables are connected correctly.

## CHAPTER 6. ABBREVIATIONS AND ACRONYMS

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

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