User Manual

DIR-620

Multifunction Wireless Router Supporting WiMAX, 3G GSM/CDMA with Built-in Switch

Version 1.2.16. February 2011

Contents

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DIR-620 and explains how to configure and operate it.

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

Conventions

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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the router DIR-620 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-620 device is a multifunction wireless router supporting WiMAX, 3G GSM and CDMA with a built-in switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

The router is equipped with a USB port for connecting a USB modem[1], which can be used to establish connection to the Internet.

Also you are able to connect the multifunction wireless router DIR-620 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-620 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 802.11b/g/n 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 multifunction wireless router DIR-620 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 multifunction wireless router DIR-620 via the user-friendly web-based interface (the interface is available in two languages – in English and in Russian).

[1] Not included in the delivery package. D-Link does not guarantee compatibility with all USB modems. Please, refer to the ***Supported USB Modems*** section, page 102.

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 802.11b/g/n.

USB Interface:

- USB 2.0 type A port for USB modem.

Network Functions:

- WAN connection types:
  - 3G
  - 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.

USB Modem[2]:

- Enabling/disabling PIN code check
- Changing PIN code.

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.

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.

[2] The listed functions are available for some models of 3G USB modems.

Configuration and Management:

- Bilingual (Russian/English) web-based interface for configuration and management
- Firmware update via web-based interface
- Saving/restoring configuration to/from file
- Support of remote logging
- Automatic synchronization of system time with NTP server
- Ping function.

LEDs:

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

Power:

- External power adapter DC 5V/2.5A
- Reset to Factory Defaults button.

Operating Temperature:

- from 0 to 40 ^{0}C (from 32 to 104 ^{0}F).

Storage Temperature:

- from -20 to 65 ^{0}C (from -4 to 149 ^{0}F).

Operating Humidity:

- from 10% to 90% non-condensing.

Storage Humidity:

- from 5% to 95% non-condensing.

Product Appearance

Front Panel and Right Side Panel

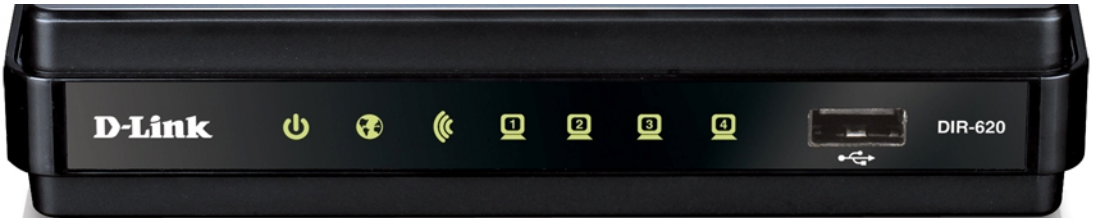


Figure 1. Front panel view.

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

In addition, a port for connecting a USB modem is located on the front panel of the router (the **USB** port).

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
Blinking blue	Attempting to add a wireless device via the WPS function
Solid blue	The wireless device is connected to the router's WLAN (lights for several minutes)
Solid yellow	Failed to add the wireless device via the WPS function or the WPS function is not used and a USB modem is connected to the router

Back Panel

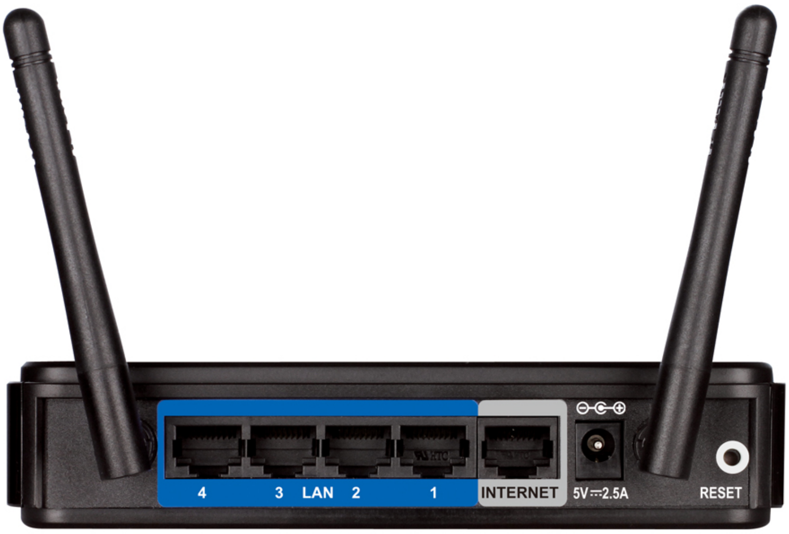


Figure 2. Back panel view.

Port	Description
LAN 1-4	4 Ethernet ports to connect computers or network devices.
INTERNET	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).
5V-2.5A	Power connector.
RESET	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.

Delivery Package

The following should be included:

- wireless router DIR-620
- power adapter 5V/2.5A
- 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 multifunction wireless router DIR-620 supporting WiMAX, 3G GSM and CDMA with a built-in 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.

USB Modem

To connect to a WiMAX, 3G GSM or CDMA network, you should use a USB modem. Connect it to the USB port of the router, then access the web-based interface of the router, and you will be able to configure a connection to the Internet[3].

WiMAX USB modem

Some WiMAX operators require subscribers to activate their WiMAX USB modems prior to using them. Please, refer to connection guidelines provided by your operator when concluding the agreement or placed on its website.

! **3G USB modem**

Your USB modem should be equipped with an active identification card (SIM or R-UIM) of your operator.

It is recommended to disable the PIN code check on the identification card prior to connecting the USB modem to the router.

[3] Contact your operator to get information on the service coverage and fees.

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. To connect via a WiMAX, 3G GSM or CDMA network: connect your USB modem to the USB port[4] located on the front panel of the router.

! If you need to connect or change a USB modem to another one when the router is powered on, power off the router, connect the modem to the USB port, and power on the router.

4. 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.
5. 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.

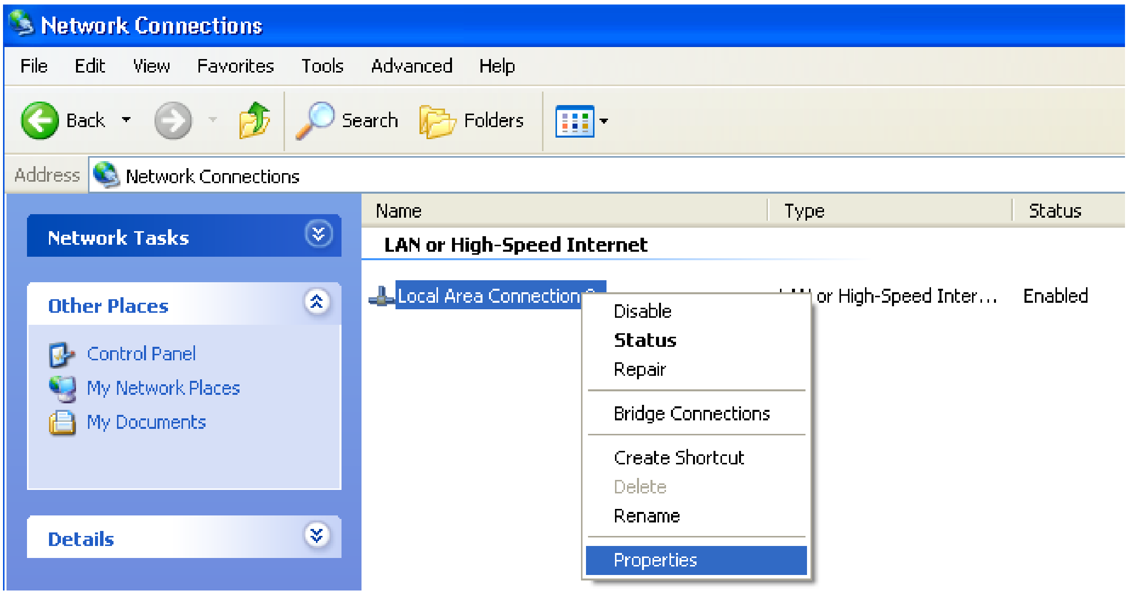
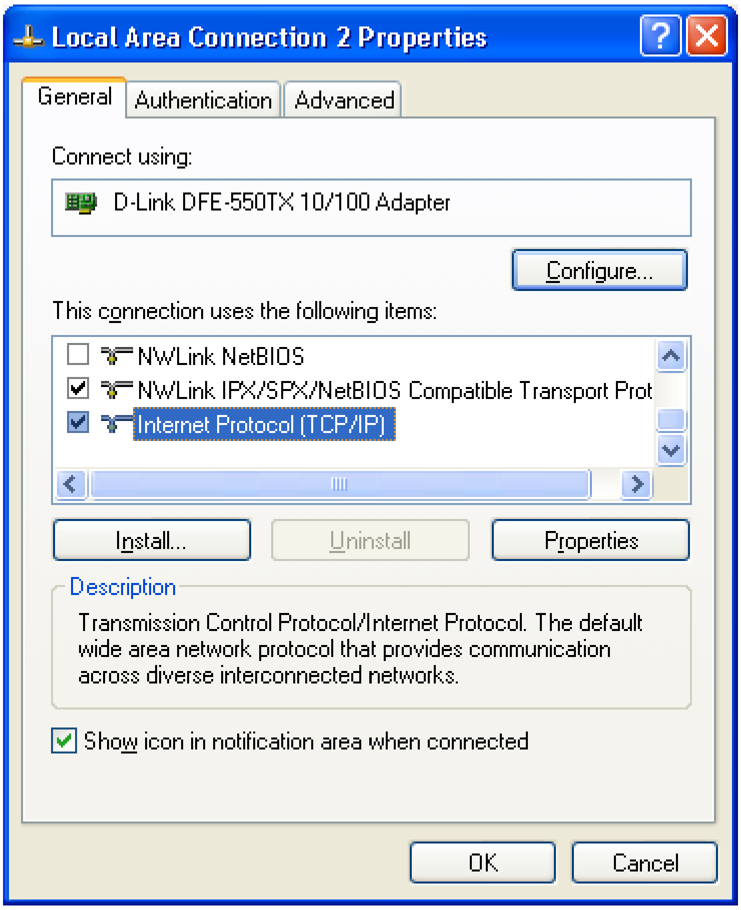


*Figure 3. The **Network Connections** window.*

[4] It is recommended to a USB extension cable to connect a USB modem to the router.

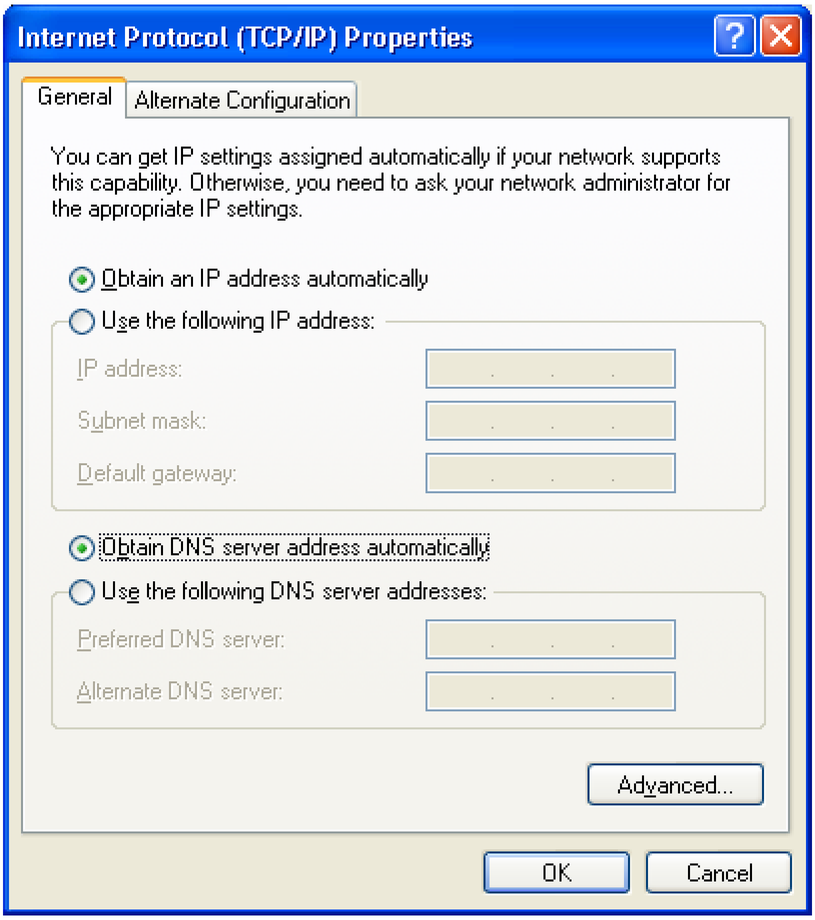
3. In the **Local Area Connection Properties** window, on the **General** tab, in the **This connection uses the following items** section, select the **Internet Protocol (TCP/IP)** line. Click the **Properties** button.



Local Area Connection 2 Properties
General
Authentication
Advanced
Connect using:
D-Link DFE-550TX 10/100 Adapter
Configure...
This connection uses the following items:
☐ NWLink NetBIOS
☑ NWLink IPX/SPX/NetBIOS Compatible Transport Prot
☑ Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
☑ Show icon in notification area when connected
OK
Cancel

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

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



Internet Protocol (TCP/IP) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

Click the **OK** button. Now your computer is configured to obtain an IP address automatically.

PC with Wi-Fi Adapter

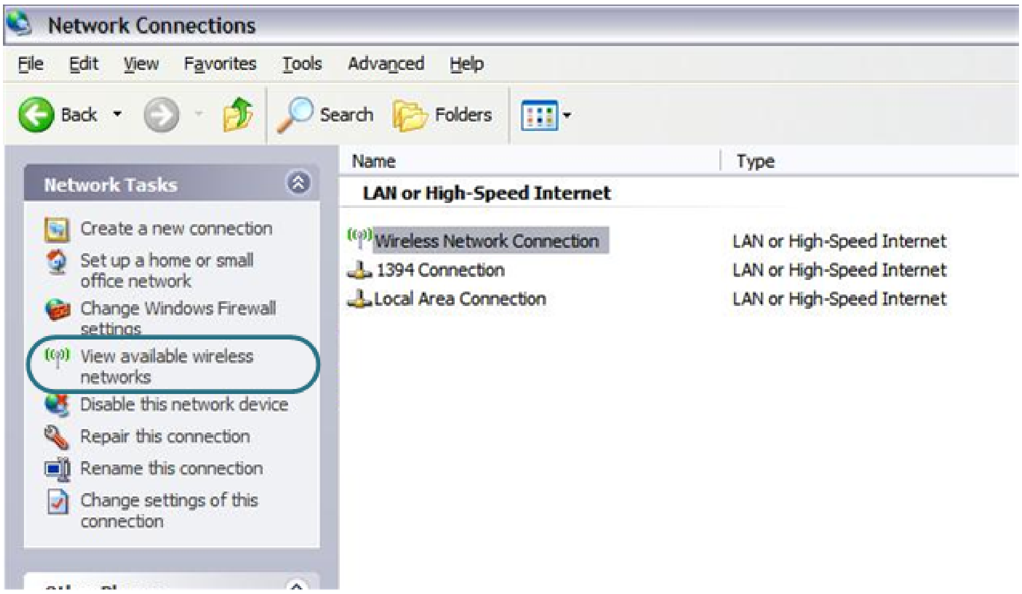
1. To connect via a WiMAX, 3G GSM or CDMA network: connect your USB modem to the USB port[5] located on the front panel of the router.

! If you need to connect or change a USB modem to another one when the router is powered on, power off the device, connect the modem to the USB port, and power on the router.

2. 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.
3. Turn on your PC and wait until your operating system is completely loaded.
4. 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.


Network Connections
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Search
Folders
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
View available wireless networks
Disable this network device
Repair this connection
Rename this connection
Change settings of this connection

Name	Type
LAN or High-Speed Internet	
Wireless Network Connection	LAN or High-Speed Internet
1394 Connection	LAN or High-Speed Internet
Local Area Connection	LAN or High-Speed Internet

*Figure 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-620`) and click the **Connect** button.

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

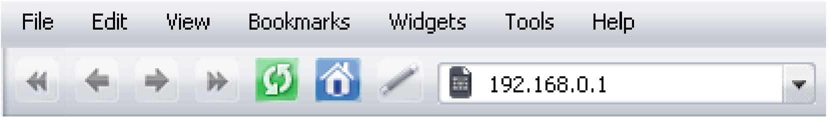
[5] It is recommended to a USB extension cable to connect a USB modem to the router.

! 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.).

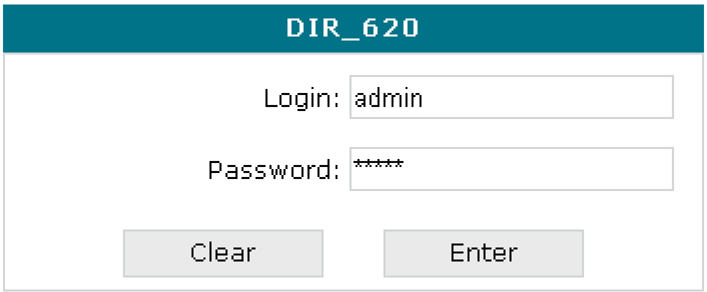
1. Start a web browser (see the ***Before You Begin*** section, page 12).
2. In the address bar of the web browser, enter the IP address of the router (by default, the following IP address is specified: **`192.168.0.1`**). Press the **Enter** key.



192.168.0.1

Figure 7. Connecting to the web-based interface of the DIR-620 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.


DIR_620

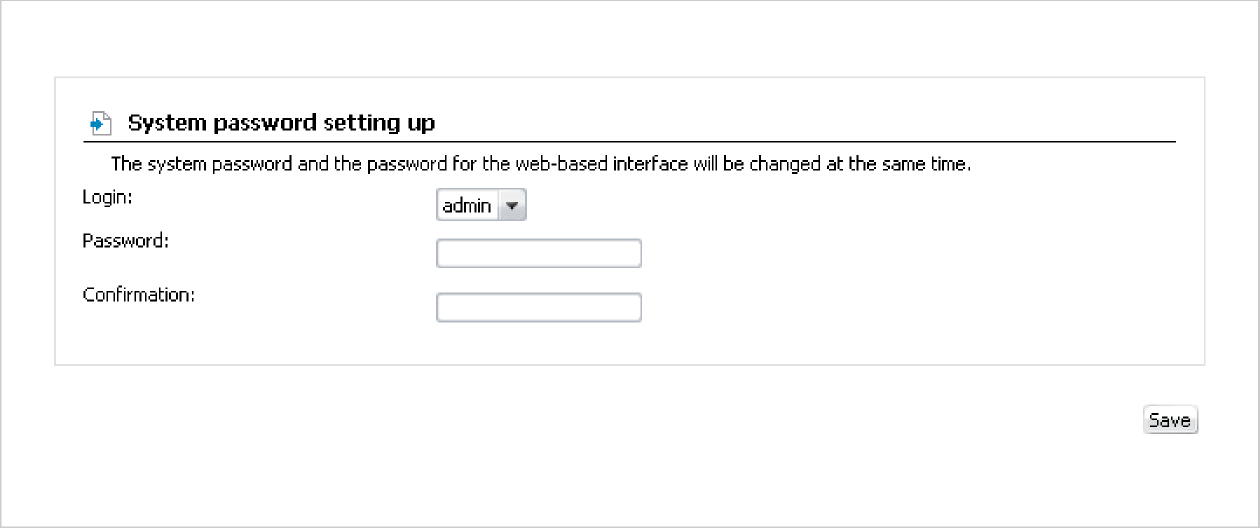
Login: admin

Password: *****

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.



System password setting up

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

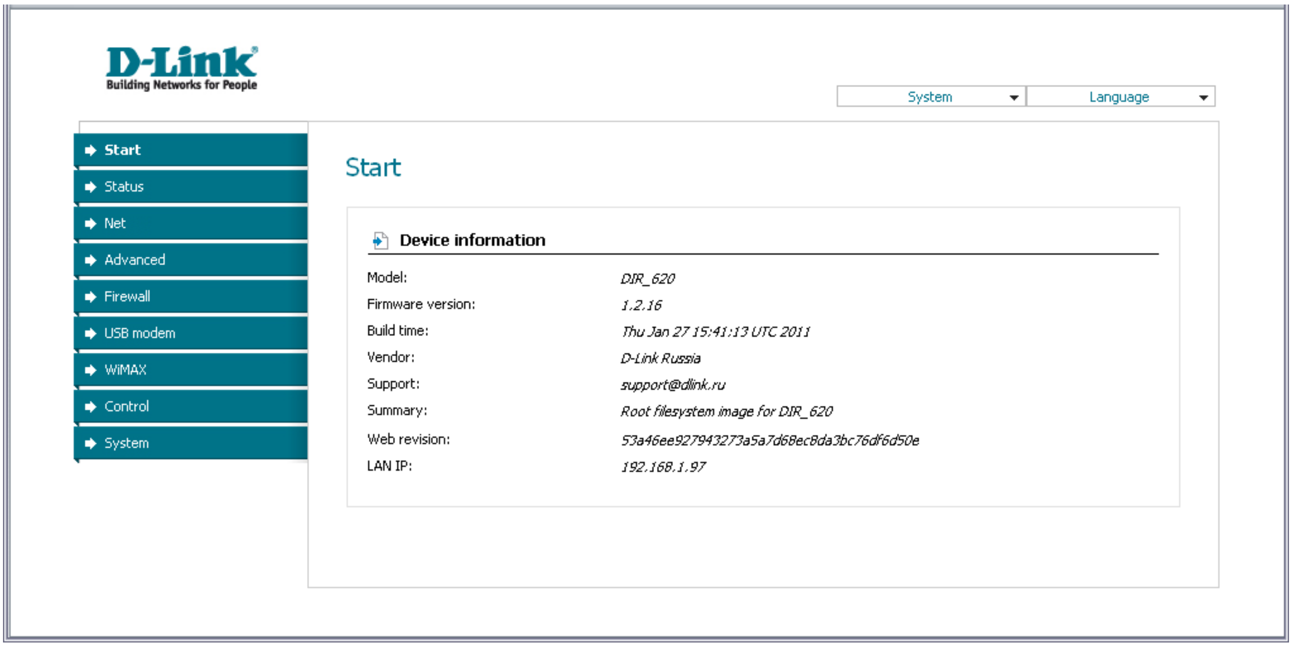
Login:	admin
Password:	
Confirmation:	

Figure 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 web-based interface 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.



Start

Device information

Model:	DIR_620
Firmware version:	1.2.16
Build time:	Thu Jan 27 15:41:13 UTC 2011
Vendor:	D-Link Russia
Support:	support@dlink.ru
Summary:	Root filesystem image for DIR_620
Web revision:	53a46ee927943273a5a7d68ec8da3bc76df6d50e
LAN IP:	192.168.1.97

Figure 10. The system statistics page.

The web-based interface of the router is bilingual (English/Russian). 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.

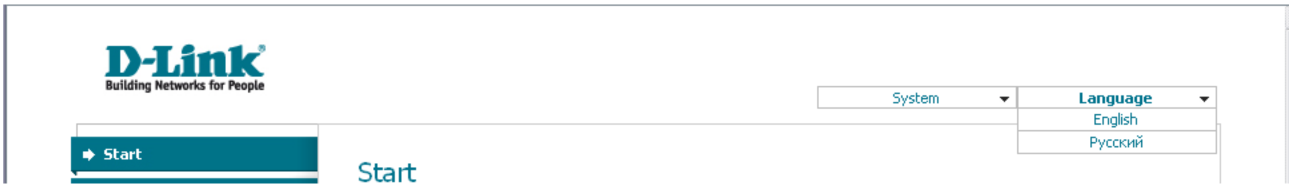


Figure 11. Changing the language of the web-based interface.

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.

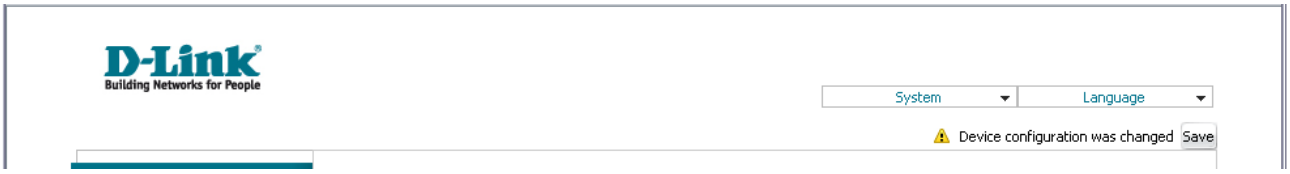

D-Link
Building Networks for People
System
Language
Device configuration was changed
Save

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.

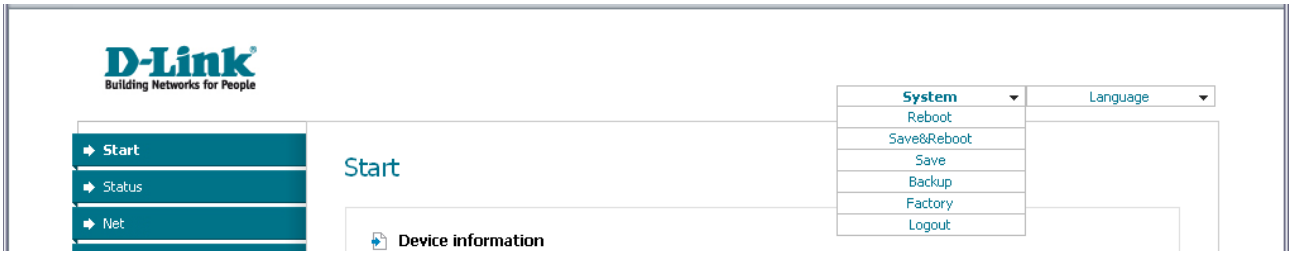


Figure 13. The top-page menu.

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.

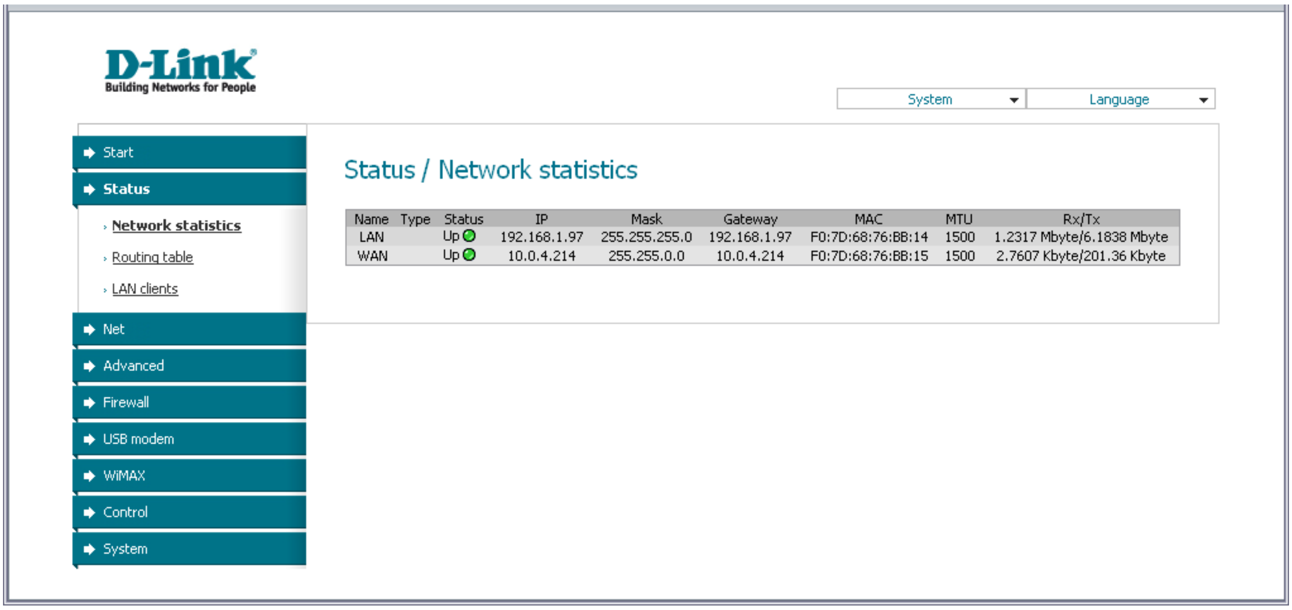
CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

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 active at the moment.



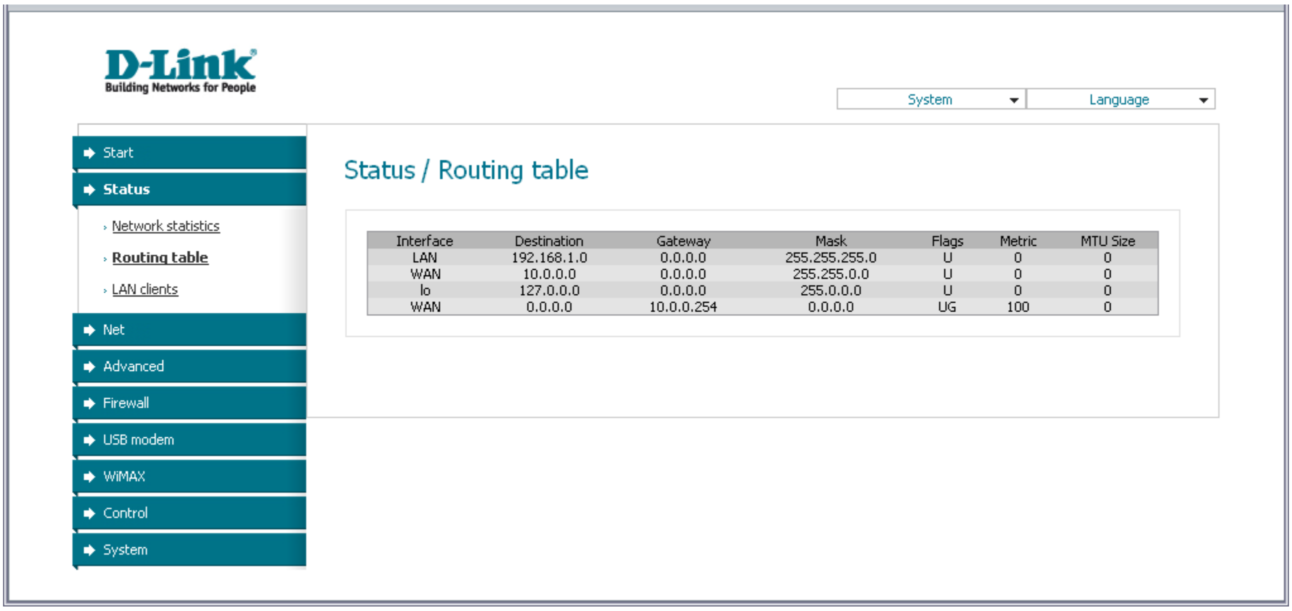
Status / Network statistics

Name	Type	Status	IP	Mask	Gateway	MAC	MTU	Rx/Tx
LAN		Up ●	192.168.1.97	255.255.255.0	192.168.1.97	F0:7D:68:76:BB:14	1500	1.2317 Mbyte/6.1838 Mbyte
WAN		Up ●	10.0.4.214	255.255.0.0	10.0.4.214	F0:7D:68:76:BB:15	1500	2.7607 Kbyte/201.36 Kbyte

*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.



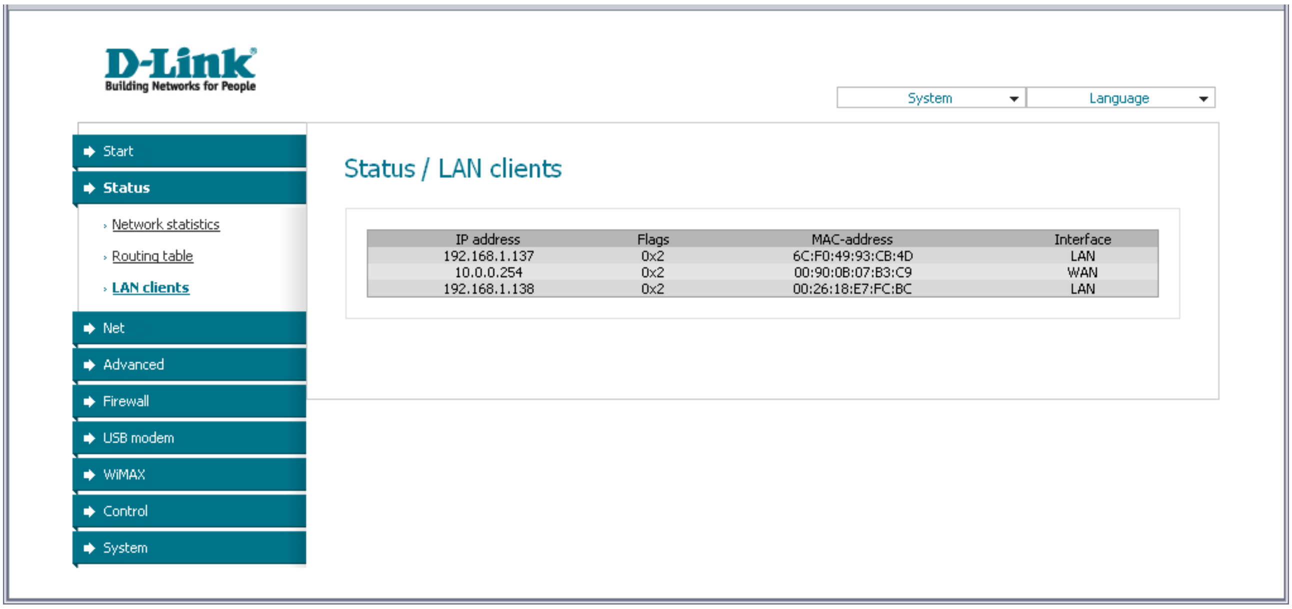
Status / Routing table

Interface	Destination	Gateway	Mask	Flags	Metric	MTU Size
LAN	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0
WAN	10.0.0.0	0.0.0.0	255.255.0.0	U	0	0
lo	127.0.0.0	0.0.0.0	255.0.0.0	U	0	0
WAN	0.0.0.0	10.0.0.254	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.



Status / LAN clients

IP address	Flags	MAC-address	Interface
192.168.1.137	0x2	6C:F0:49:93:CB:4D	LAN
10.0.0.254	0x2	00:90:0B:07:B3:C9	WAN
192.168.1.138	0x2	00:26:18:E7:FC:BC	LAN

*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

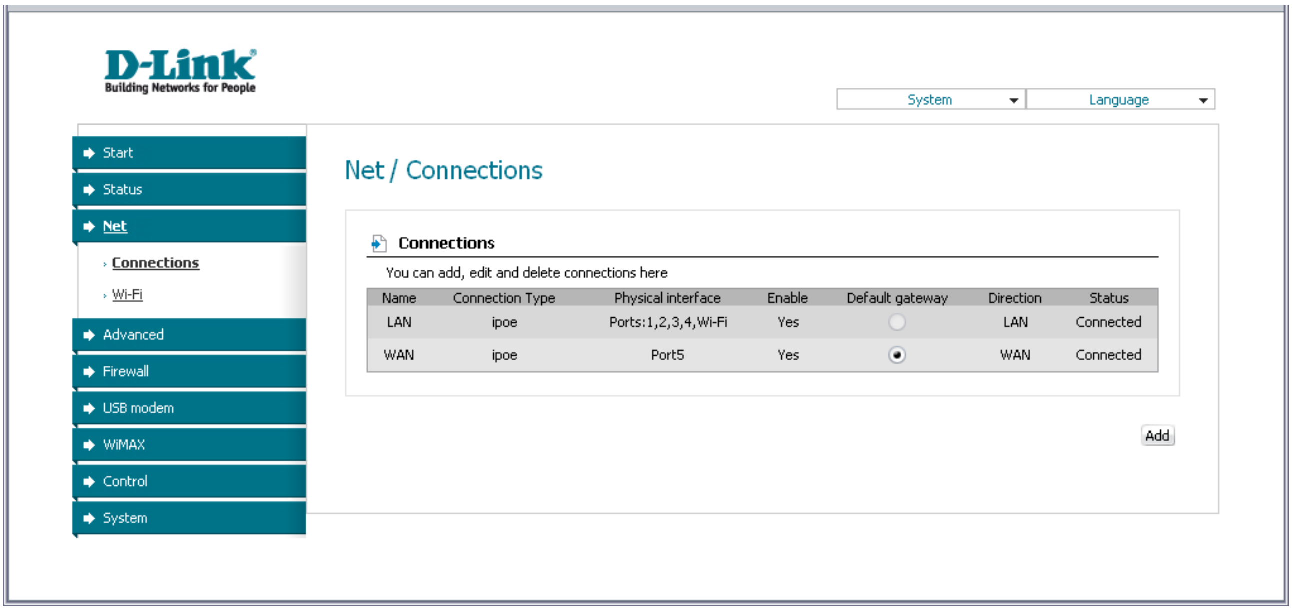
In this menu you can configure basic parameters of the router's local area network, configure connection to the Internet (a WAN connection), and specify all needed settings for your wireless network.

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 (**br0**). 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.



Net / Connections

Connections

You can add, edit and delete connections here

Name	Connection Type	Physical interface	Enable	Default gateway	Direction	Status
LAN	ipoe	Ports:1,2,3,4,Wi-Fi	Yes	○	LAN	Connected
WAN	ipoe	Port5	Yes	●	WAN	Connected

Add

*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.

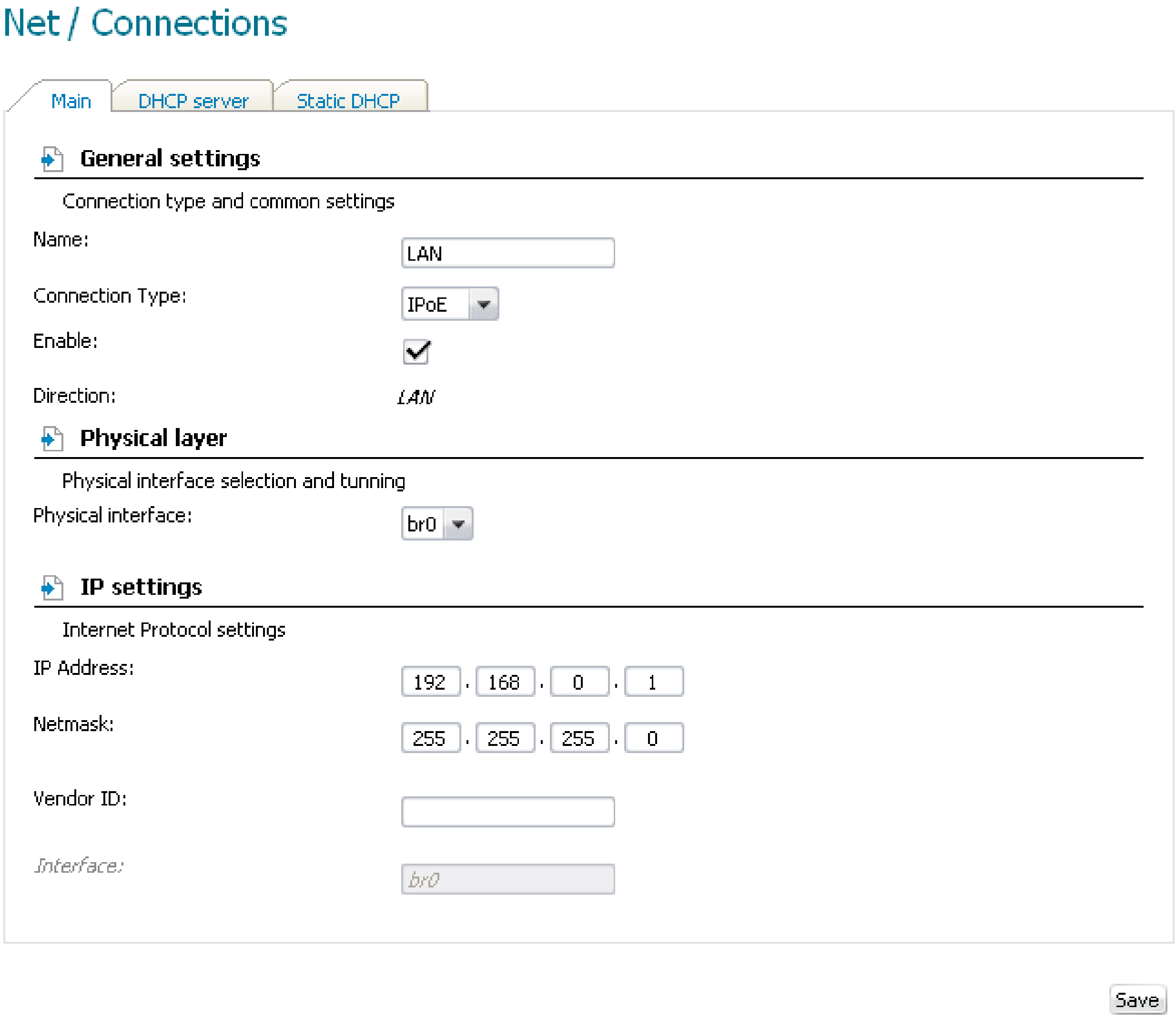
To delete an existing connection, left-click the relevant line in the table. On the page displayed, click the **Delete** button.

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.



Connection type and common settings

Name: LAN

Connection Type: IPoE

Enable: ☑

Direction: LAN

Physical interface selection and tunning

Physical interface: br0

Internet Protocol settings

IP Address: 192 . 168 . 0 . 1

Netmask: 255 . 255 . 255 . 0

Vendor ID:

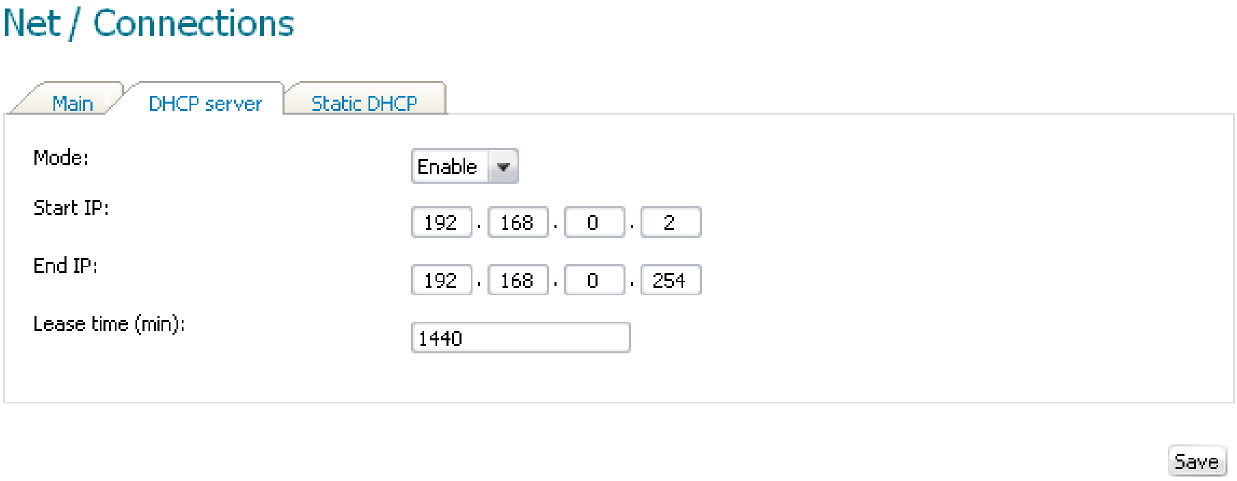
Interface: br0

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

Parameter	Description
General settings	
Name	A name for this connection.
Connection Type	The type of network protocol used by this connection – **IPoE**.
Enable	The checkbox enabling this connection.
Direction	The direction of this connection.
Physical layer	
Physical interface	The physical interface to which this connection is assigned – **br0**.
IP settings	
IP Address	The router's IP address. By default, the following value is specified: `192.168.0.1`.
Netmask	The subnet mask. By default, the following value is specified: `255.255.255.0`.
Interface	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

Mode: Enable

Start IP: 192 . 168 . 0 . 2

End IP: 192 . 168 . 0 . 254

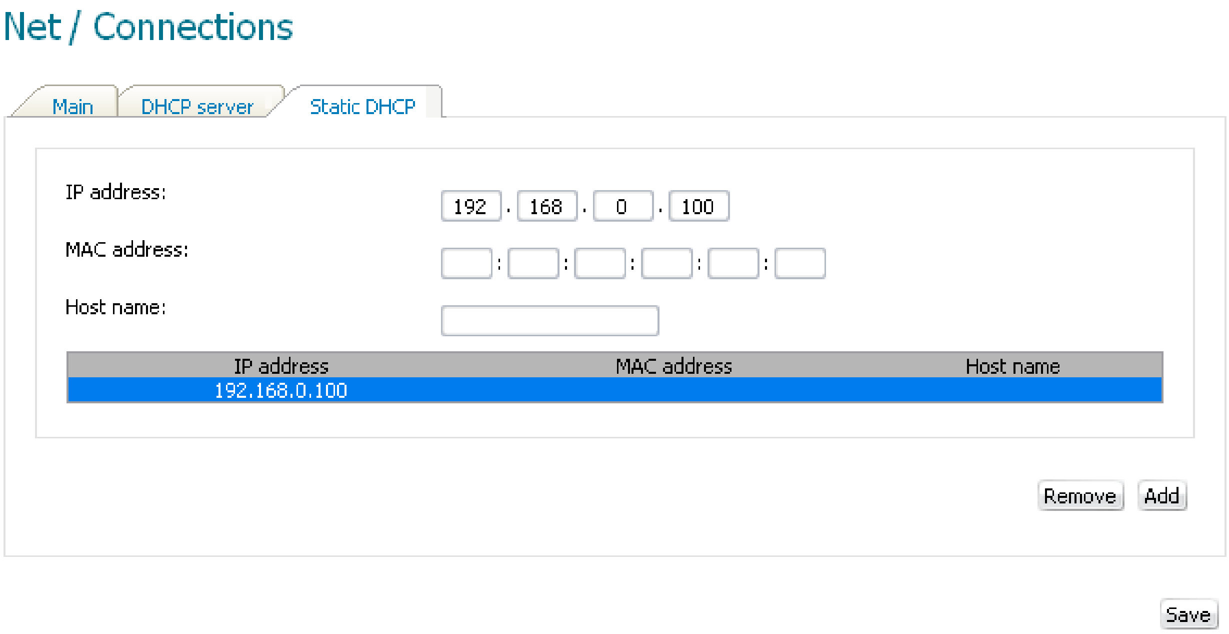
Lease time (min): 1440

Figure 19. The tab for configuring the DHCP server.

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



IP address: 192 . 168 . 0 . 100

MAC address: : : : : :

Host name:

IP address	MAC address	Host name
192.168.0.100		

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:

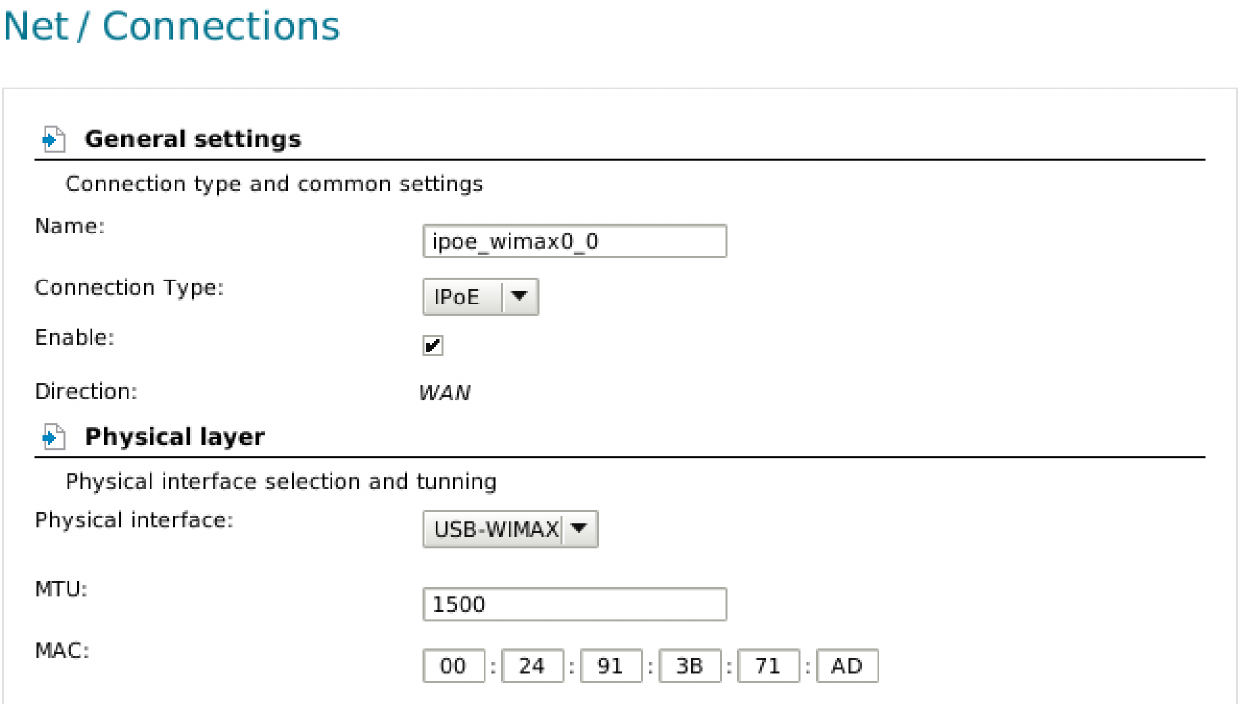
Parameter	Description
IP address	An IP address which will be assigned to the device with the specified MAC address.
MAC address	The MAC address of the device from the LAN.
Host name	A network name of the device for easier identification. *Optional*.

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 WiMAX WAN Connection

You can create a connection of this type only when a WiMAX USB modem is connected to the router. Select the **WAN** connection on the **Net / Connections** page. On the opened page, select the **USB-WIMAX** value from the **Physical interface** drop-down list and specify the needed values.



Net / Connections

General settings

Connection type and common settings

Name: ipoe_wimax0_0

Connection Type: IPoE

Enable: ☑

Direction: *WAN*

Physical layer

Physical interface selection and tunning

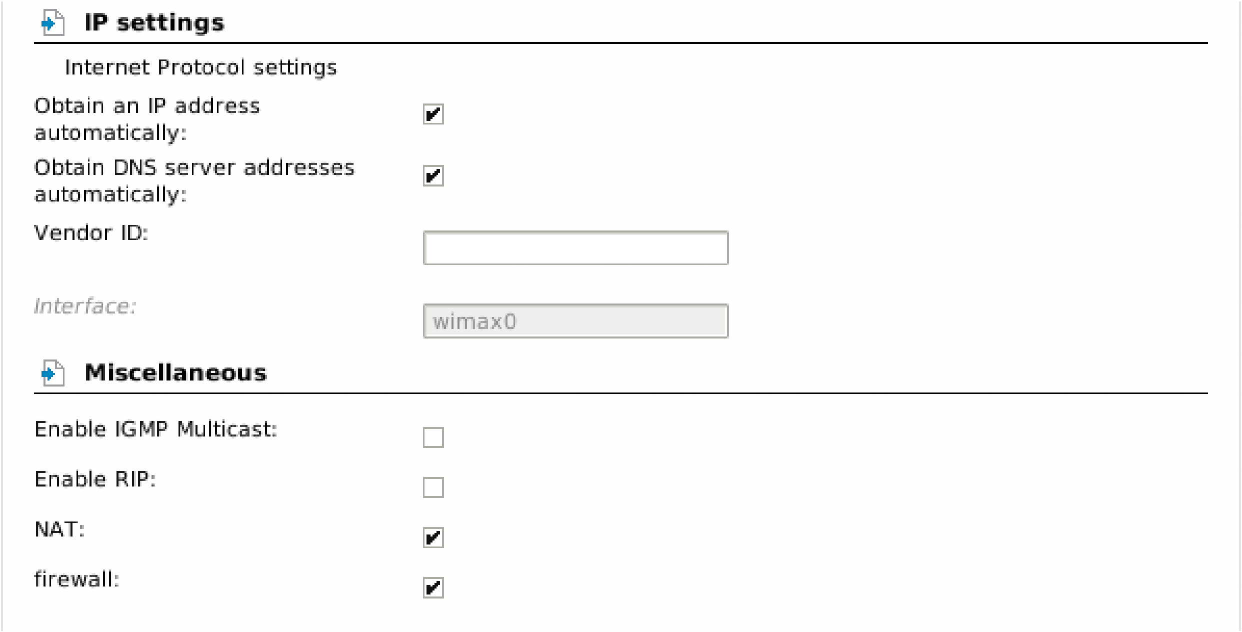
Physical interface: USB-WIMAX

MTU: 1500

MAC: 00 : 24 : 91 : 3B : 71 : AD

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

Parameter	Description
General settings	
Name	A name for connection for easier identification.
Connection Type	Select the **IPoE** value.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.
Physical layer	
MTU	The maximum size of units transmitted by the interface.
MAC	A . By default, the MAC address of your WiMAX USB modem is specified in the field.



IP settings

Internet Protocol settings

Obtain an IP address automatically: ☑

Obtain DNS server addresses automatically: ☑

Vendor ID:

Interface: wimax0

Miscellaneous

Enable IGMP Multicast: □

Enable RIP: □

NAT: ☑

firewall: ☑

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

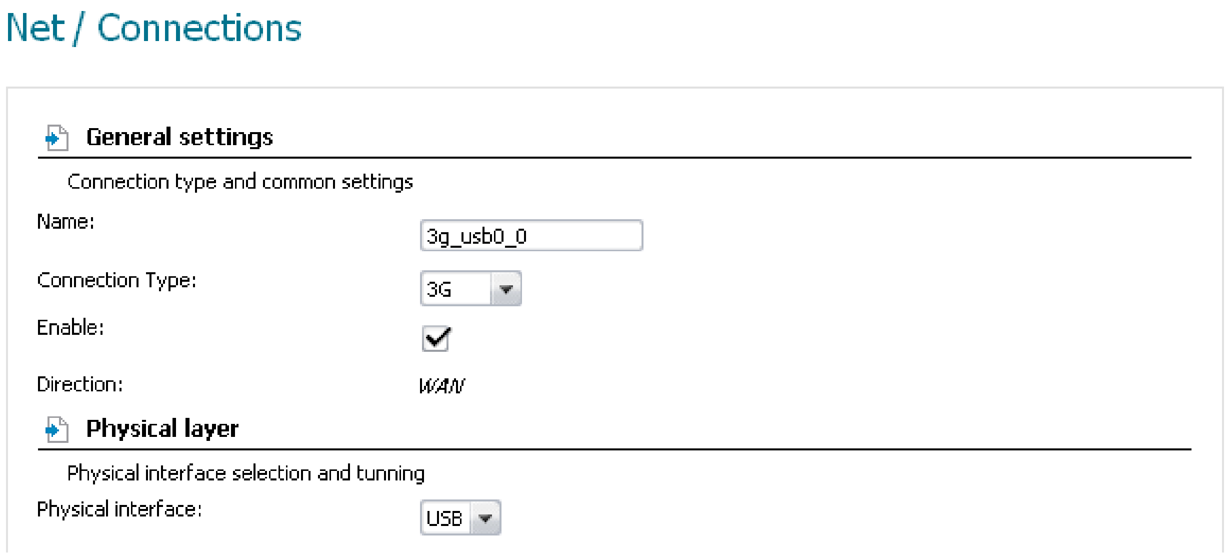
Parameter	Description
IP settings	
Obtain an IP address automatically	Select the checkbox to configure automatic IP address assignment for this connection. When the checkbox is selected, the **IP Address**, **Netmask**, and **Gateway IP Address** fields are not displayed.
IP Address	Enter an IP address for this WAN connection.
Netmask	Enter a subnet mask for this WAN connection.
Gateway IP Address	Enter an IP address of the gateway used by this WAN connection.
Obtain DNS server addresses automatically	Displayed when the **Obtain an IP address automatically** checkbox is selected. Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the **Primary DNS server** and **Secondary DNS server** fields are not displayed.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. This field is specified when the ISP assigns an IP address automatically (the **Obtain an IP address automatically** checkbox is selected). *Optional*.
Interface	The name assigned to the connection by the system.

Parameter	Description
Miscellaneous	
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
Enable RIP	Select the checkbox to allow using RIP for this connection.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.

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

Creating 3G WAN Connection

You can create a connection of this type only when a 3G USB modem is connected to the router. Select the **WAN** connection on the **Net / Connections** page. On the opened page, select the **3G** value from the **Connection type** drop-down list and specify the needed values.



Net / Connections

General settings

Connection type and common settings

Name: 3g_usb0_0

Connection Type: 3G

Enable: ☑

Direction: WAN

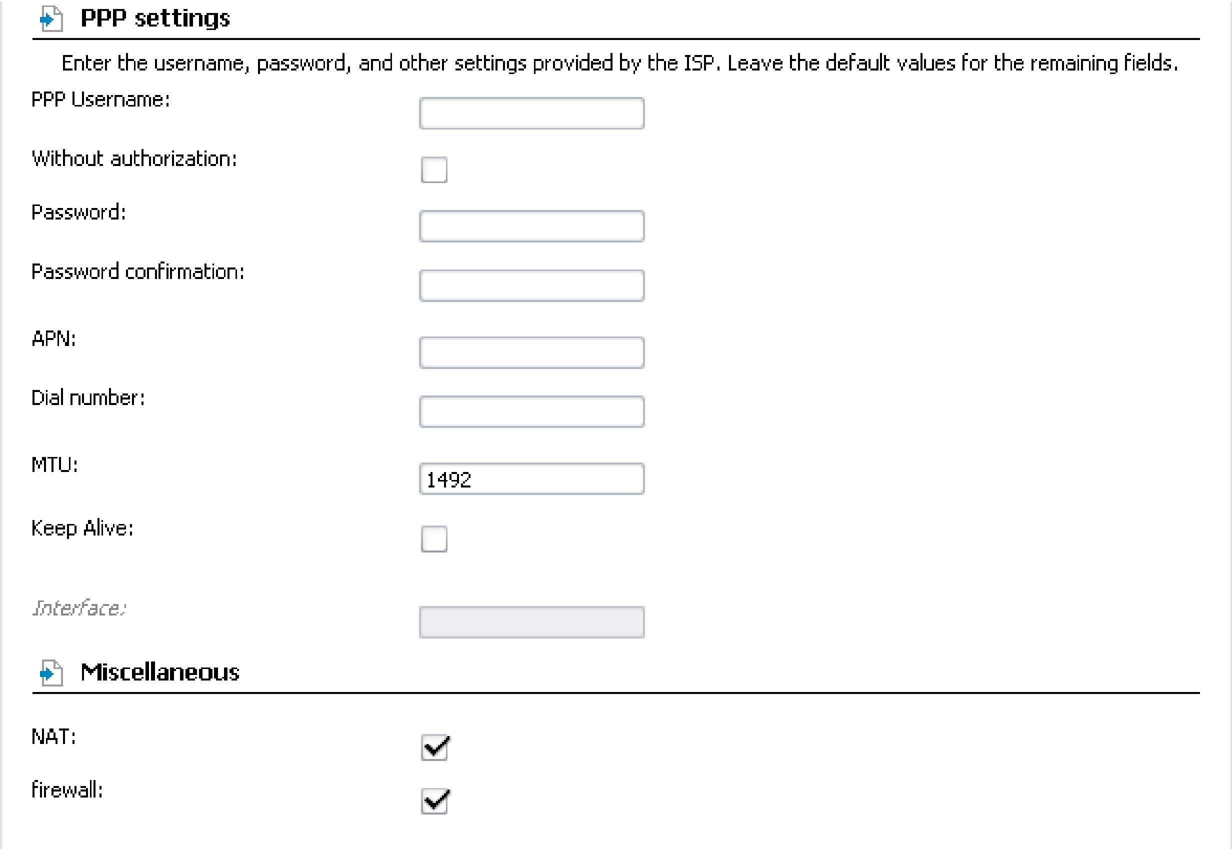
Physical layer

Physical interface selection and tunning

Physical interface: USB

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

Parameter	Description
General settings	
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.
Physical layer	
Physical interface	Select the **USB** value.



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:	
APN:	
Dial number:	
MTU:	1492
Keep Alive:	□
Interface:	

Miscellaneous

NAT:	☑
firewall:	☑

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

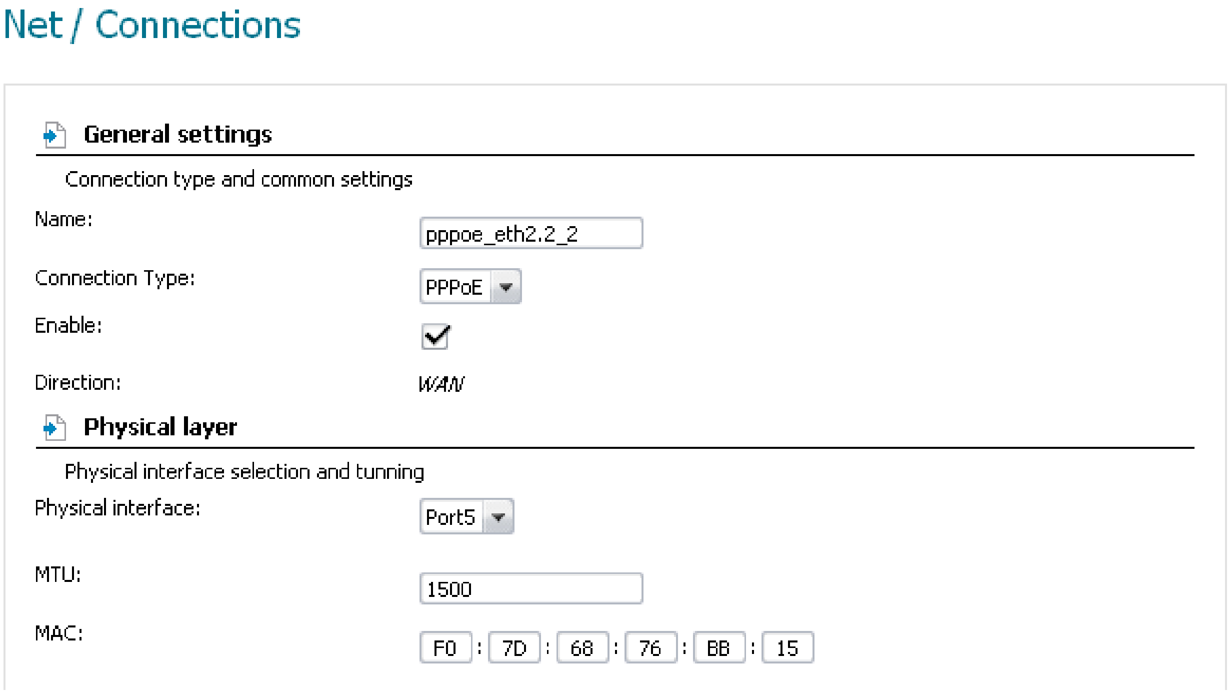
Parameter	Description
PPP settings	
PPP Username	A username (login) to connect to the network of the operator.
Without authorization	Select the checkbox if your operator does not require authorization.
Password	A password to connect to the network of the operator.
Password confirmation	The confirmation of the entered password (to avoid mistypes).
APN	An access point name.
Dial number	A number dialed to connect to the authorization server of the operator.
MTU	The maximum size of units transmitted by the interface. *Optional*.
Keep Alive	Select the checkbox if you want the router to keep you connected to the network of your operator even when the connection has been inactive for a specified period of time. When the checkbox is selected, the **LCP interval** and **LCP fails** fields are available. Specify the required values.

Parameter	Description
Interface	The name assigned to the connection by the system.
Miscellaneous	
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.

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

Creating 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

General settings

Connection type and common settings

Name:	pppoe_eth2.2_2
Connection Type:	PPPoE
Enable:	☑
Direction:	WAN

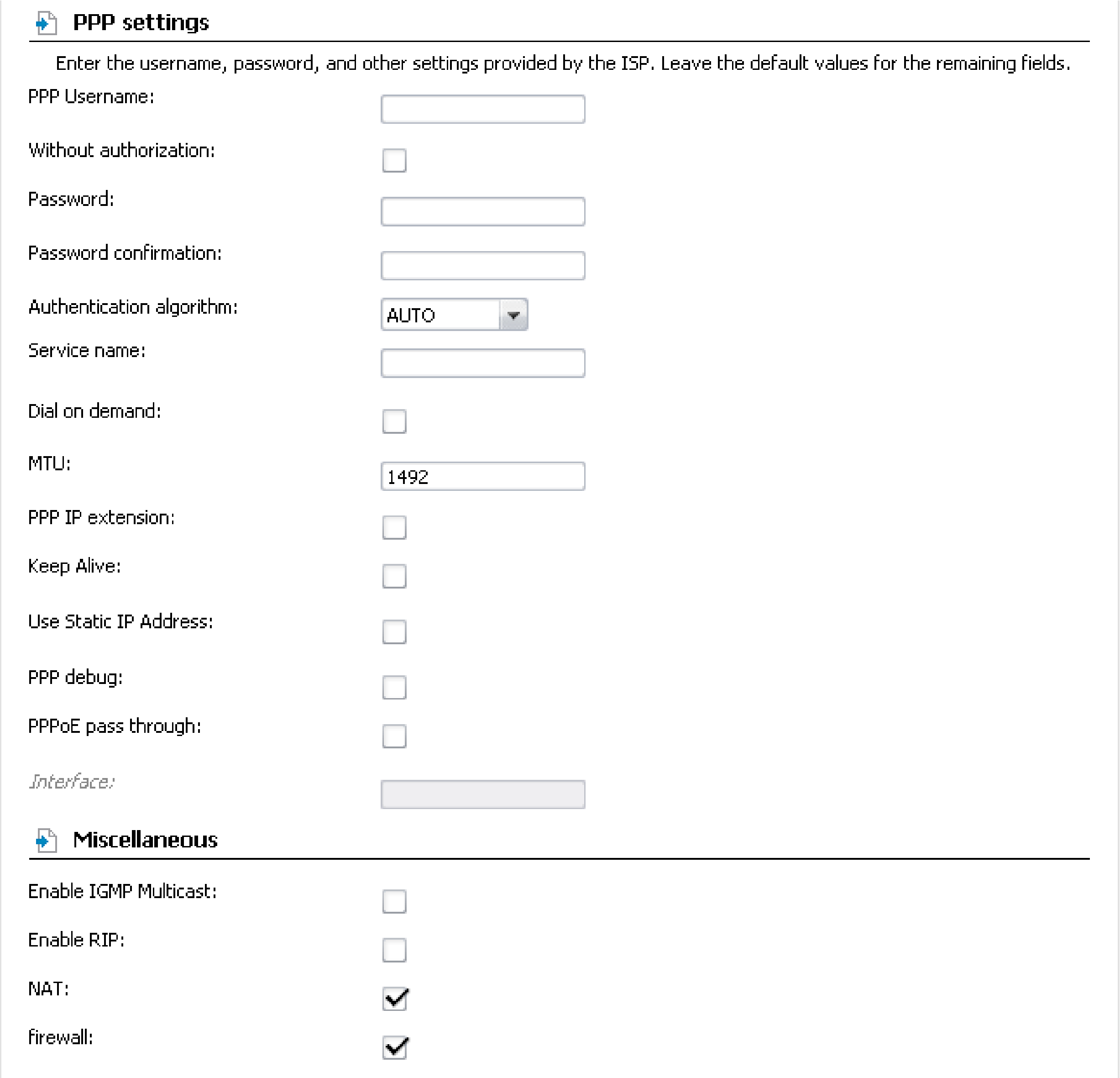
Physical layer

Physical interface selection and tunning

Physical interface:	Port5
MTU:	1500
MAC:	F0 : 7D : 68 : 76 : BB : 15

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

Parameter	Description
General settings	
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.
Physical layer	
Physical interface	A physical or virtual interface to which the new connection will be assigned.
MTU	The maximum size of units transmitted by the interface.
MAC	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. 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:	1492
PPP IP extension:	□
Keep Alive:	□
Use Static IP Address:	□
PPP debug:	□
PPPoE pass through:	□
Interface:	

Miscellaneous

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

*Figure 26. The page for creating a new connection. The **PPP settings** and **Miscellaneous** sections.*

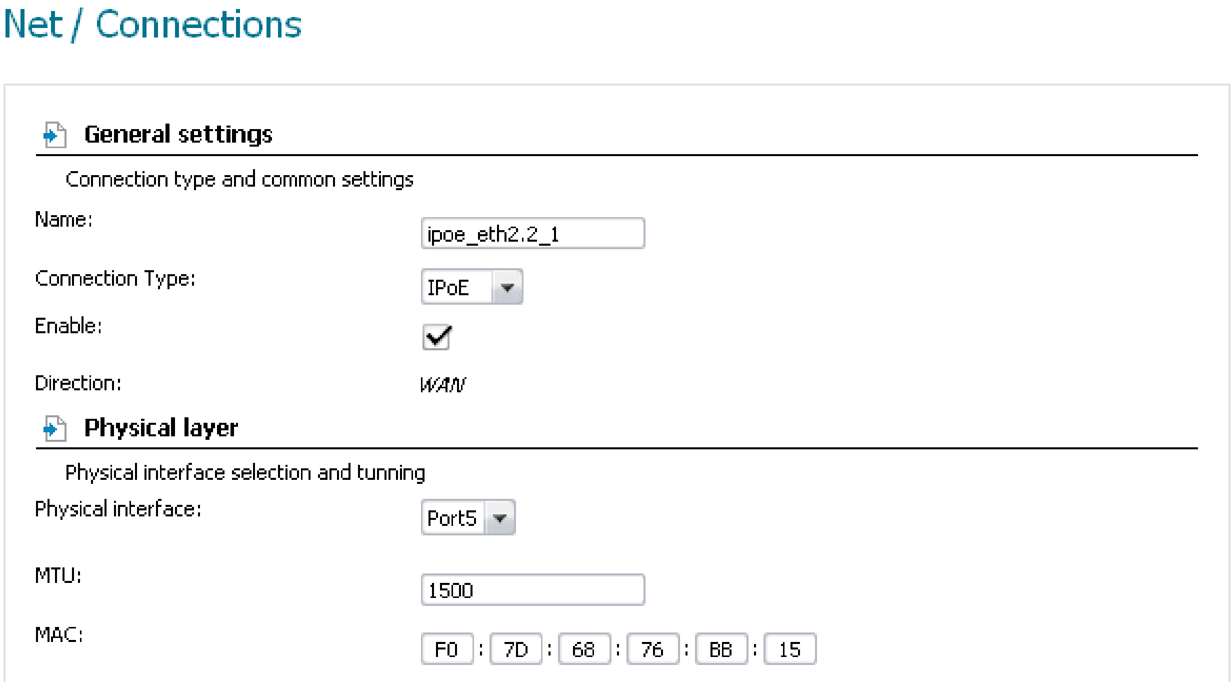
Parameter	Description
PPP settings	
PPP Username	A username (login) to access the Internet.
Without authorization	Select the checkbox if you don't need to enter a username and password to access the Internet.
Password	A password to access the Internet.
Password confirmation	The confirmation of the entered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

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

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

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

General settings

Connection type and common settings

Name:	ipoe_eth2.2_1
Connection Type:	IPoE
Enable:	☑
Direction:	WAN

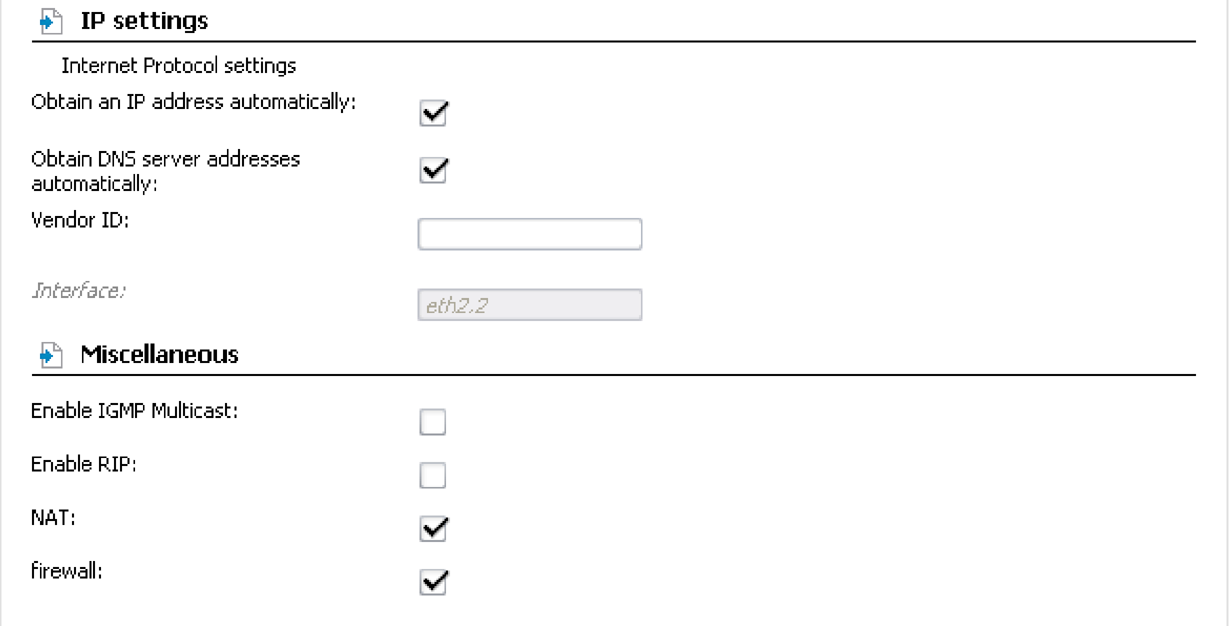
Physical layer

Physical interface selection and tunning

Physical interface:	Port5
MTU:	1500
MAC:	F0 : 7D : 68 : 76 : BB : 15

*Figure 27. The page for creating a new connection. The **General settings** and **Physical layer** sections.*

Parameter	Description
General settings	
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.
Physical layer	
Physical interface	A physical or virtual interface to which the new connection will be assigned.
MTU	The maximum size of units transmitted by the interface.
MAC	A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement. 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: *eth2.2*

Miscellaneous

Enable IGMP Multicast: □

Enable RIP: □

NAT: ☑

Firewall: ☑

*Figure 28. The page for creating a new connection. The **IP settings** and **Miscellaneous** sections.*

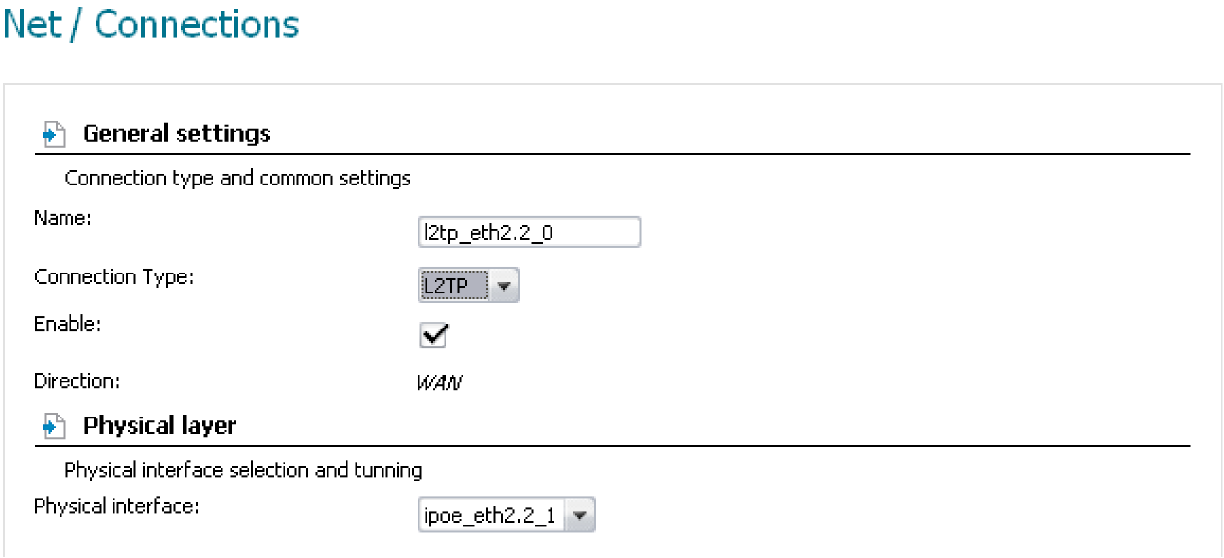
Parameter	Description
IP settings	
Obtain an IP address automatically	Select the checkbox to configure automatic IP address assignment for this connection. When the checkbox is selected, the **IP Address**, **Netmask**, and **Gateway IP Address** fields are not displayed.

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

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

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

General settings

Connection type and common settings

Name: l2tp_eth2.2_0

Connection Type: L2TP

Enable: ☑

Direction: WAN

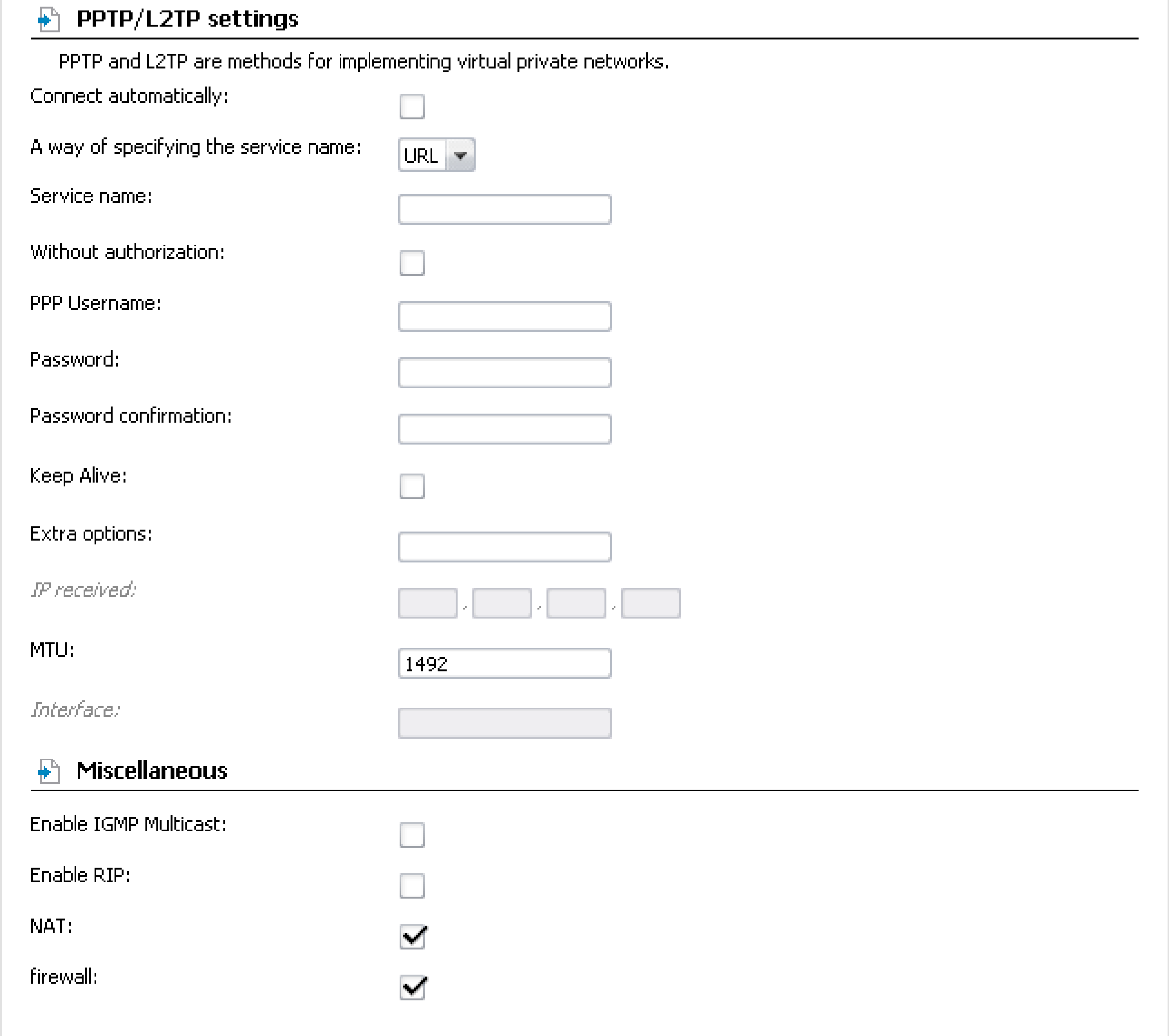
Physical layer

Physical interface selection and tunning

Physical interface: ipoe_eth2.2_1

*Figure 29. The page for creating a new connection. The **General settings** and **Physical layer** sections.*

Parameter	Description
General settings	
Name	A name for connection for easier identification.
Enable	Select the checkbox to enable the connection.
Direction	The direction of this connection.
Physical layer	
Physical interface	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:	
Keep Alive:	□
Extra options:	
IP received:	. . .
MTU:	1492
Interface:	

Miscellaneous

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

*Figure 30. The page for creating a new connection. The **PPTP/L2TP settings** and **Miscellaneous** sections.*

Parameter	Description
PPTP/L2TP settings	
Connect automatically	Select the checkbox to enable auto-start of the connection upon the boot-up of the router.
A way of specifying the service name	Select a way of specifying the address of the PPTP or L2TP server.
Service name	The IP or URL address of the PPTP or L2TP server.
Without authorization	Select the checkbox if you don't need to enter a username and password to access the Internet.
PPP Username	A username (login) to access the Internet.
Password	A password to access the Internet.
Password confirmation	The confirmation of the entered password (to avoid mistypes).
Keep Alive	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 **LCP interval** and **LCP fails** fields are available. Specify the required values.
Extra options	Advanced options of the pppd daemon which need to be specified for this connection. *Optional*.
IP received	The IP address assigned by the ISP.
MTU	The maximum size of units transmitted by the interface.
Interface	The name assigned to the connection by the system.
Miscellaneous	
Enable IGMP Multicast	Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received.
Enable RIP	Select the checkbox to allow using RIP for this connection.
NAT	Select the checkbox if you want one WAN IP address to be used for all computers of your LAN.
Firewall	Select the checkbox to enable protection against ARP and DDoS attacks.

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

Wi-Fi

On the **Net / Wi-Fi** page, you can configure all settings of your wireless local area network (WLAN).

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 spitted (the **Disabled** value is selected from the list).

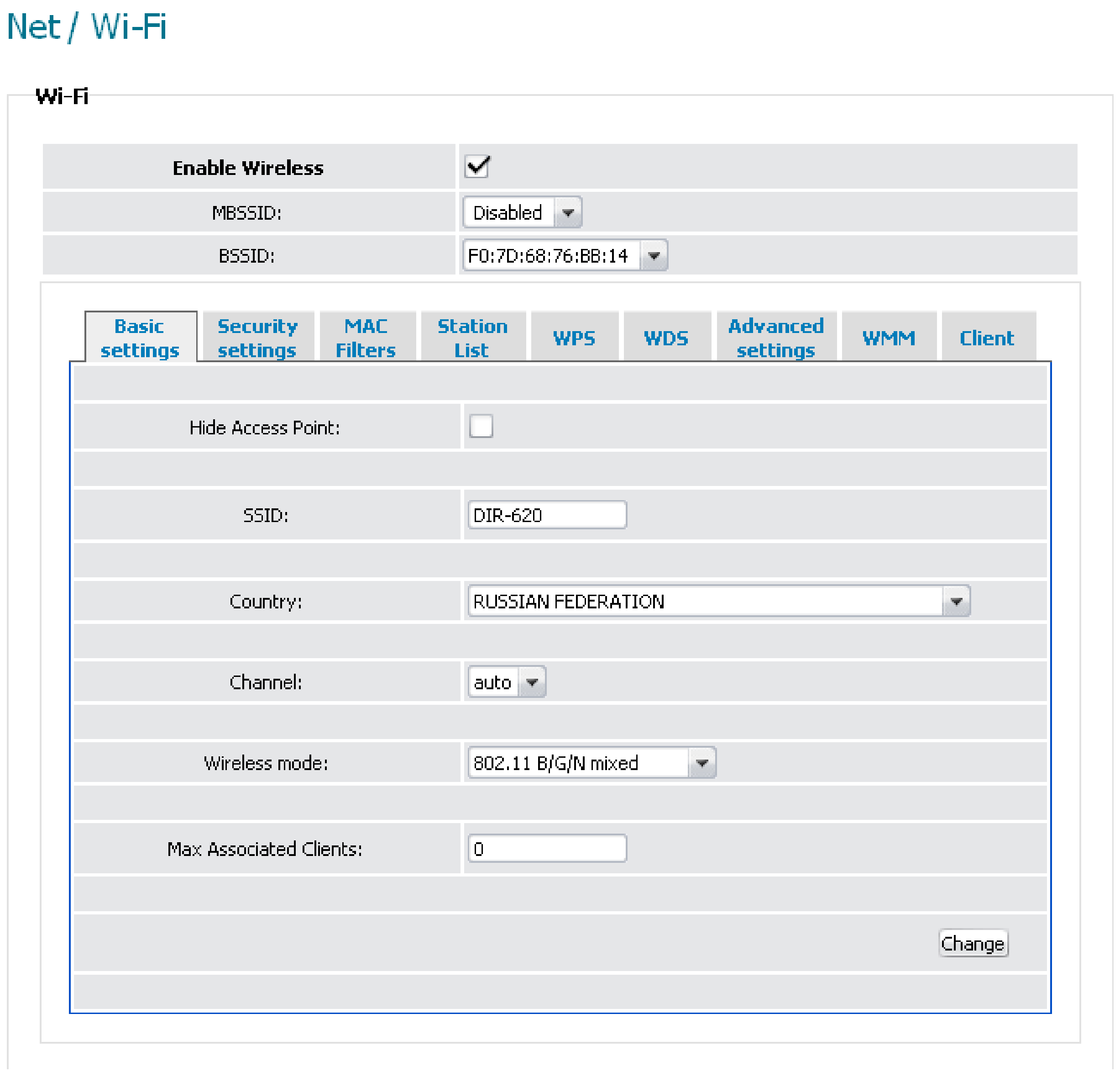
The value from the **BSSID** drop-down list is the unique identifier for your Wi-Fi network. You cannot change the value of this parameter, it is determined in the router's internal settings.

If you have spitted your WLAN into parts, the **BSSID** drop-down list contains several values. Each identifier corresponds to a single part of the WLAN. Select every value to specify a name (SSID), security settings, rules for MAC filtering, and enable the WMM function (if needed).

If the **Enable Wireless** checkbox is selected, tabs for configuring the WLAN settings are displayed on the page.

Basic Settings

On the **Basic settings** tab, you can configure basic parameters of the router's WLAN.



Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14
Hide Access Point:	□
SSID:	DIR-620
Country:	RUSSIAN FEDERATION
Channel:	auto
Wireless mode:	802.11 B/G/N mixed
Max Associated Clients:	0

Figure 31. Basic settings of the wireless LAN.

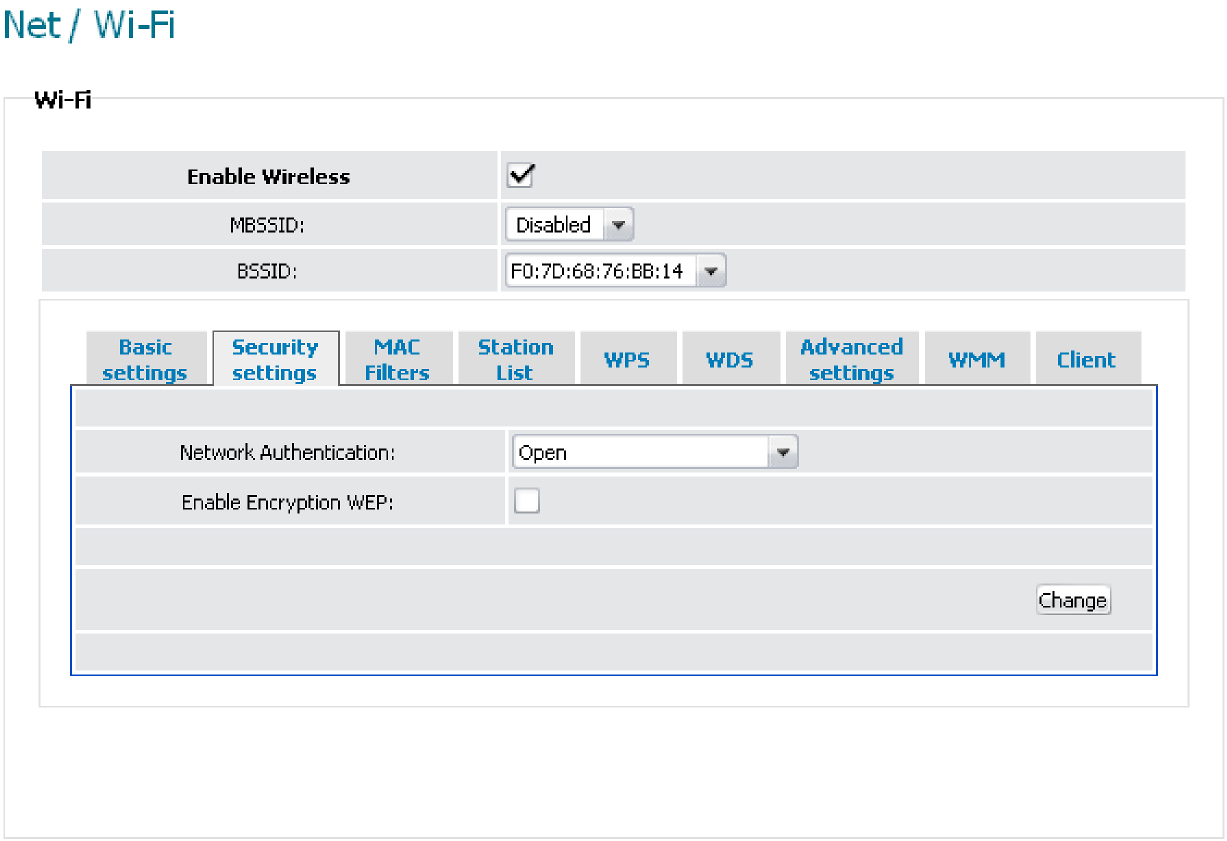
Parameter	Description
Hide Access Point	If the checkbox is selected, other users cannot see your Wi-Fi network. (It is recommended not to select this checkbox in order to simplify initial configuration of your WLAN.)
SSID	A name for the WLAN. By default, the value `DIR-620` is specified. If your network is spitted into parts, each part has the default name (`DIR-620.2`, `DIR-620.3`, and `DIR-620.4`). It is recommended to specify another name for the network upon initial configuration (use digits and Latin characters).

Parameter	Description
Country	The country you are in. Select a value from the drop-down list.
Channel	The wireless channel number. When the **auto** value is selected, the router itself chooses the channel with the least interference.
Wireless mode	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.
Max Associated Clients	The maximum number of devices connected to the wireless network of the router. When the value 0 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 **Security settings** tab, you can modify security settings of the WLAN.


Net / Wi-Fi

Wi-Fi

Enable Wireless: ✓

MBSSID: Disabled

BSSID: F0:7D:68:76:BB:14

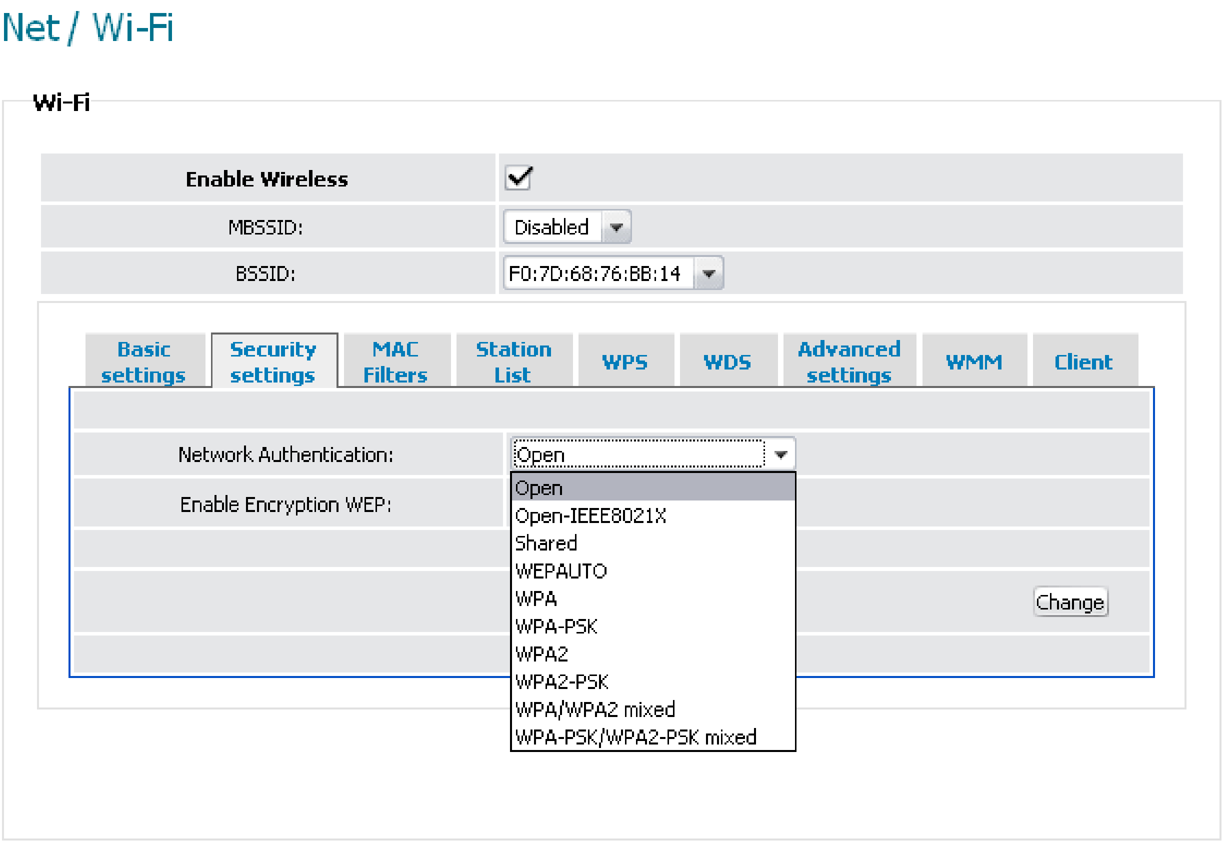
Network Authentication: Open

Enable Encryption WEP: □

Figure 32. 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).



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

Network Authentication: Open

Enable Encryption WEP:

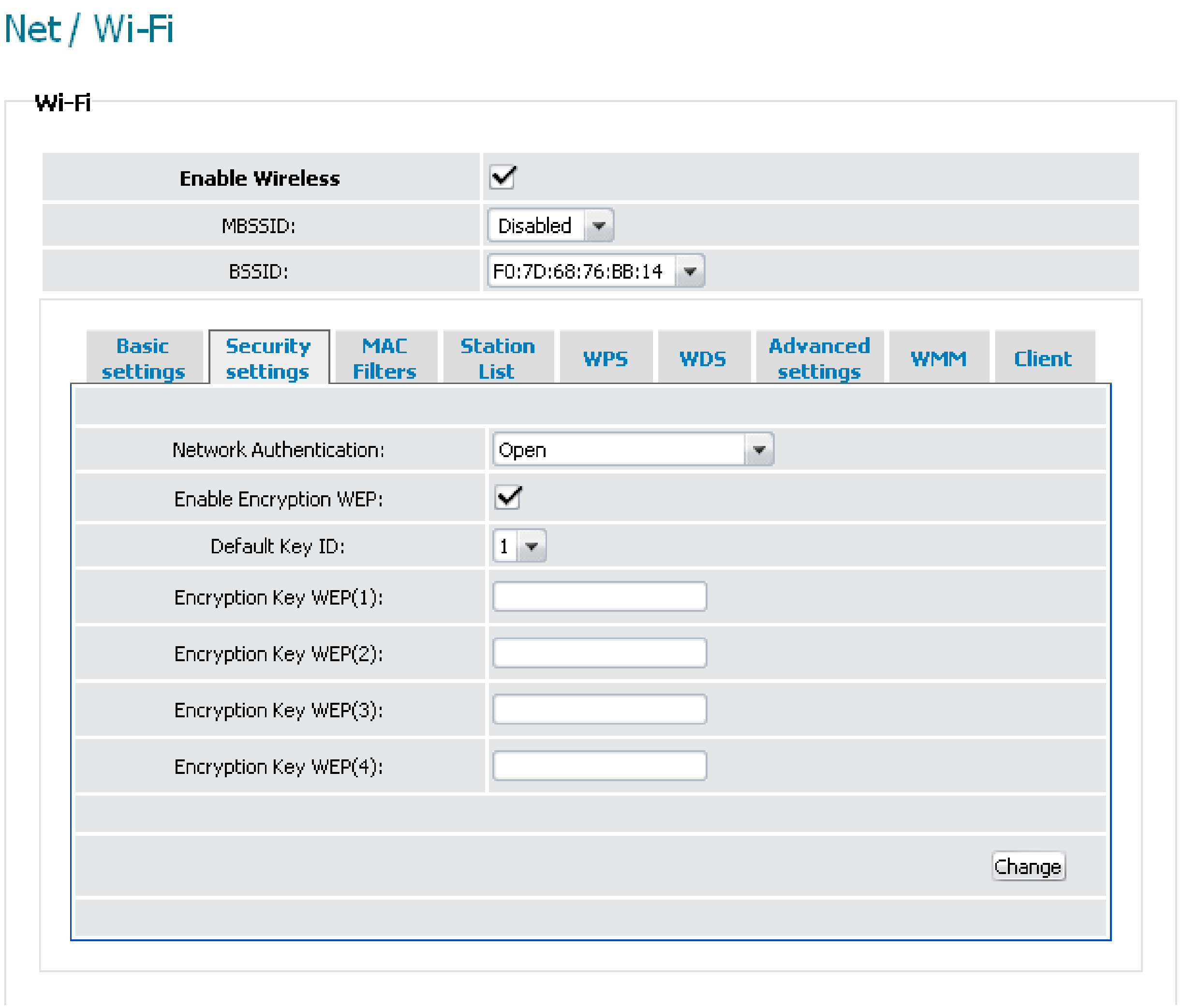
Figure 33. Network authentication types supported by the router.

The router supports the following authentication types:

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

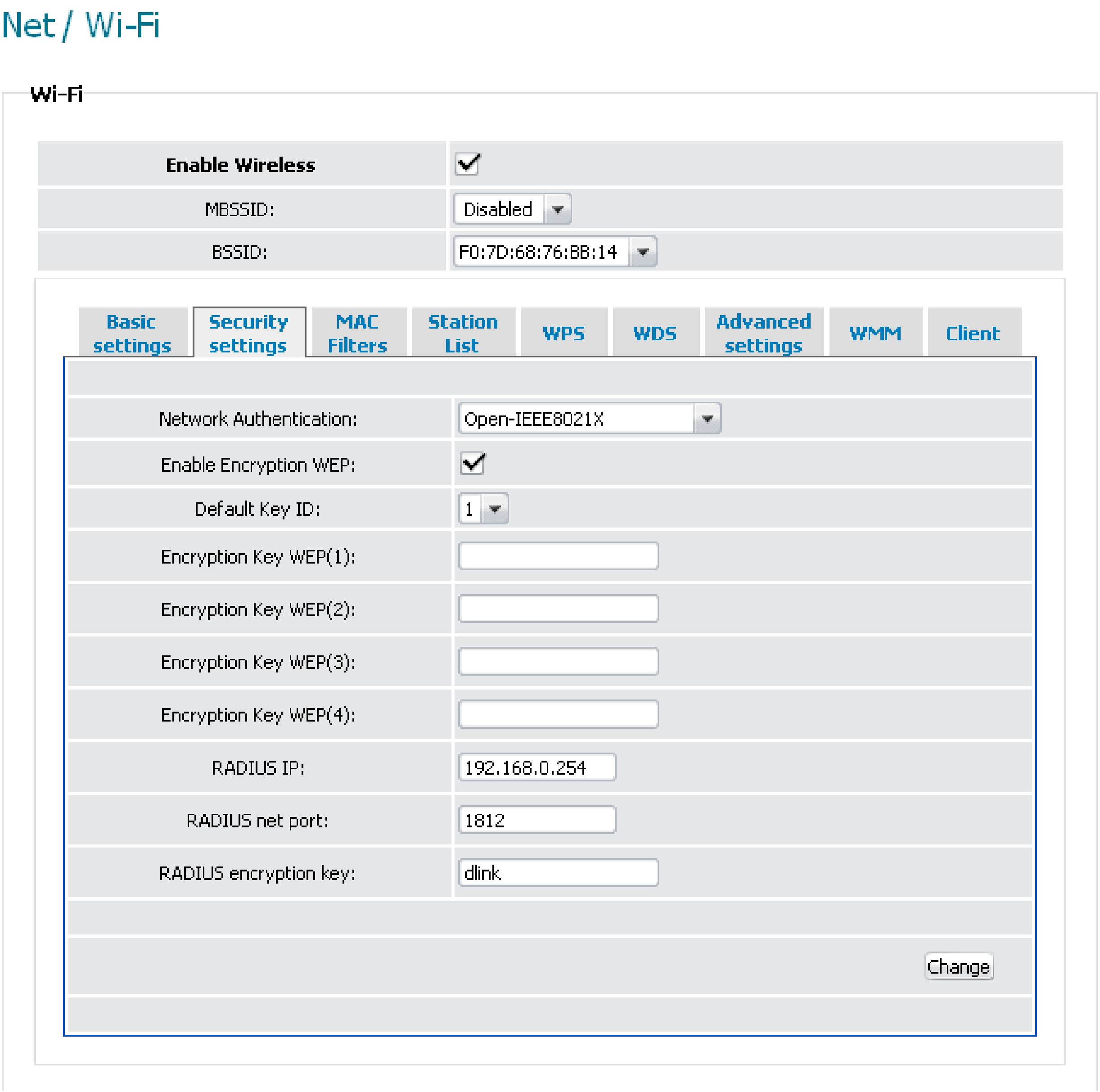


Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14
Network Authentication:	Open
Enable Encryption WEP:	☑
Default Key ID:	1
Encryption Key WEP(1):	
Encryption Key WEP(2):	
Encryption Key WEP(3):	
Encryption Key WEP(4):	

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

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

When the **Open-IEEE8021X** value is selected, the following fields are available:

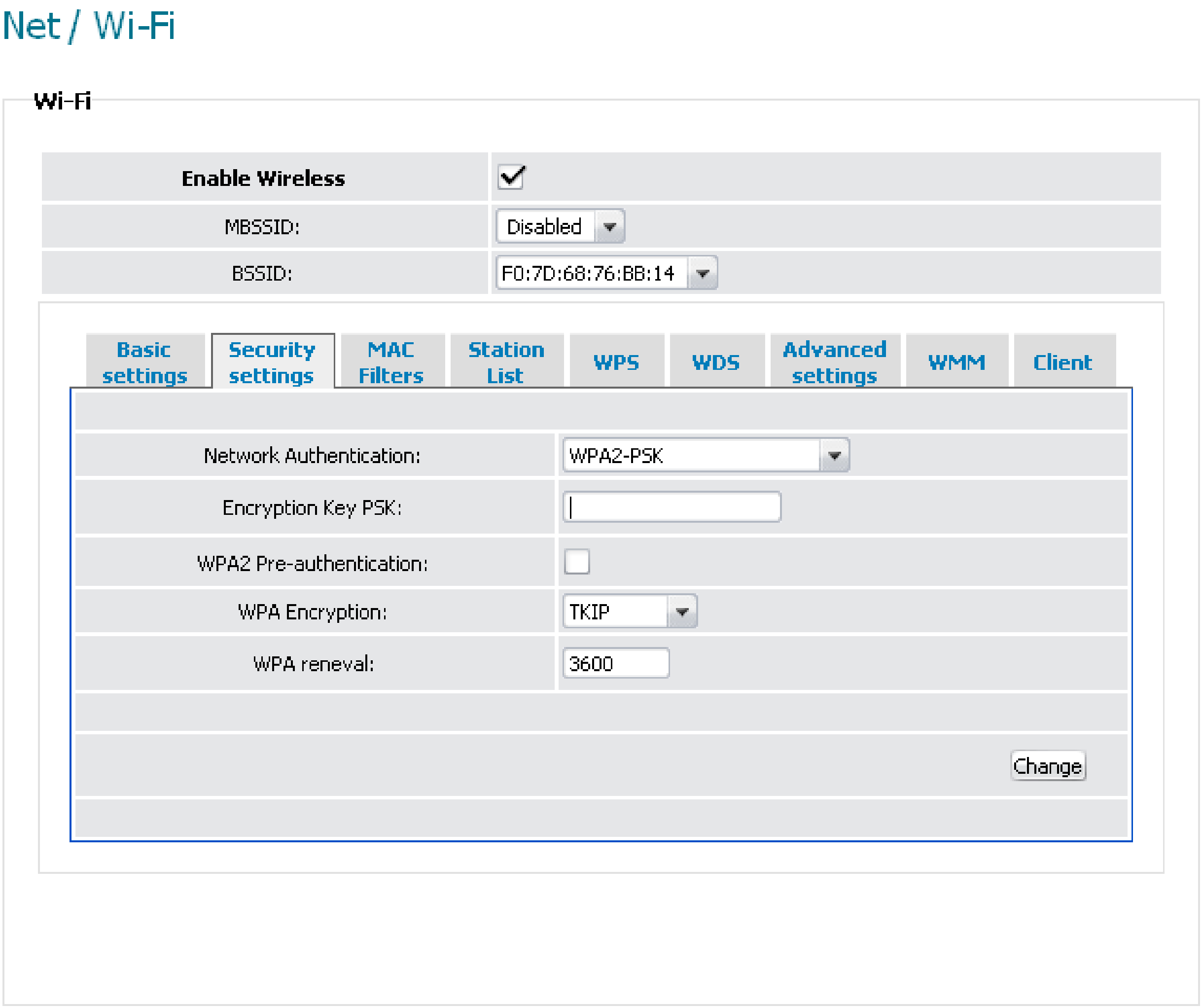


Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14
Network Authentication:	Open-IEEE8021X
Enable Encryption WEP:	☑
Default Key ID:	1
Encryption Key WEP(1):	
Encryption Key WEP(2):	
Encryption Key WEP(3):	
Encryption Key WEP(4):	
RADIUS IP:	192.168.0.254
RADIUS net port:	1812
RADIUS encryption key:	dlink

*Figure 35. The **Open-IEEE8021X** value is selected from the **Network Authentication** drop-down list.*

Parameter	Description
Enable Encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the **Default Key ID** field and four **Encryption Key WEP** fields are displayed on the page.
Default Key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption Key WEP (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default Key ID** drop-down list. It is required to specify all the fields. You can specify keys containing 5 or 13 symbols (use digits and/or Latin characters).
RADIUS IP	The IP address of the RADIUS server.
RADIUS net port	A port of the RADIUS server.
RADIUS encryption key	A password to access the RADIUS server.

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


Net / Wi-Fi

Wi-Fi

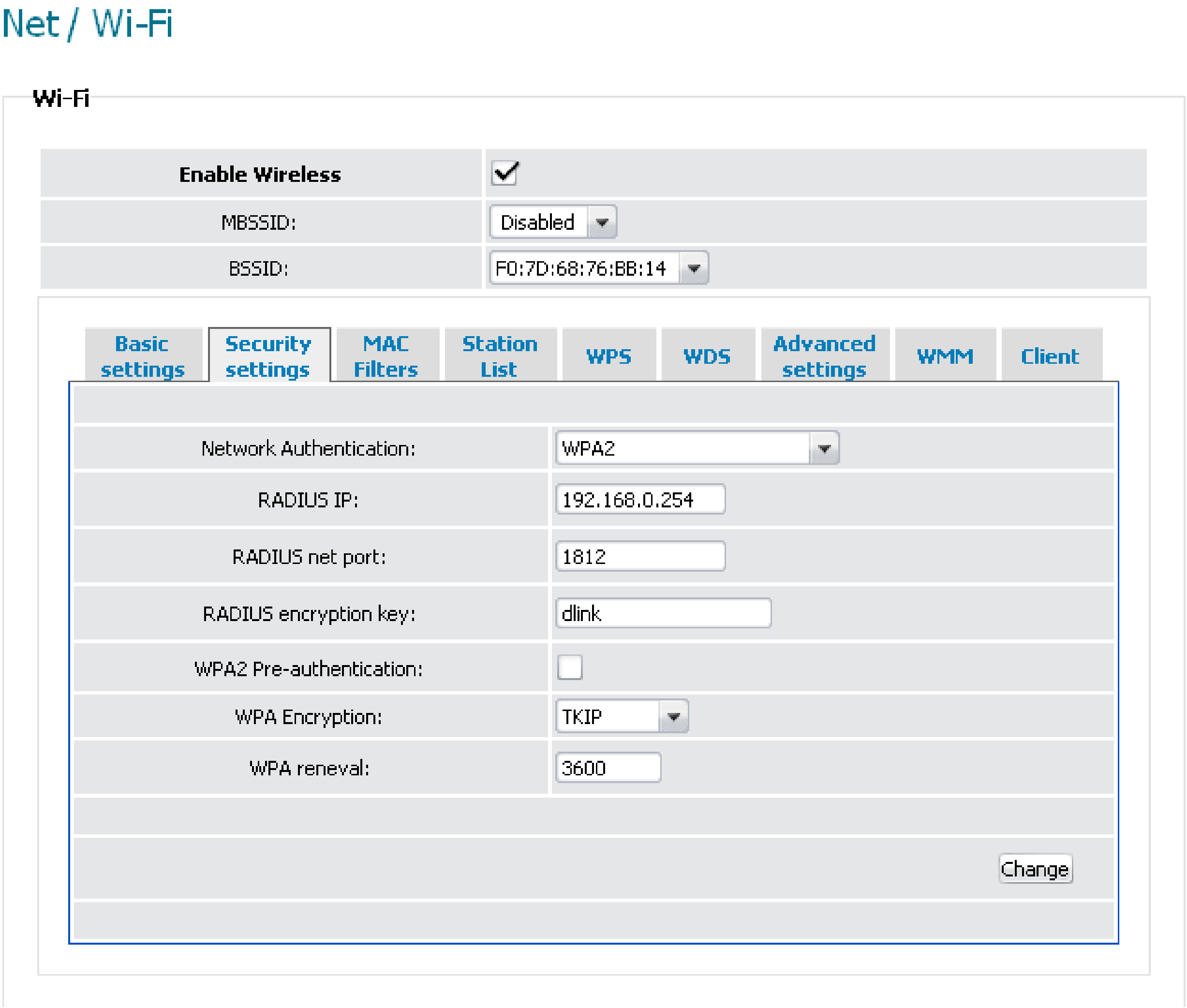
Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

Network Authentication:	WPA2-PSK
Encryption Key PSK:	
WPA2 Pre-authentication:	□
WPA Encryption:	TKIP
WPA reneval:	3600

*Figure 36. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.*

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

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** values are selected, the following fields are available:



Enable Wireless: ☑
MBSSID: Disabled
BSSID: F0:7D:68:76:BB:14
Network Authentication: WPA2
RADIUS IP: 192.168.0.254
RADIUS net port: 1812
RADIUS encryption key: dlink
WPA2 Pre-authentication: □
WPA Encryption: TKIP
WPA reneval: 3600

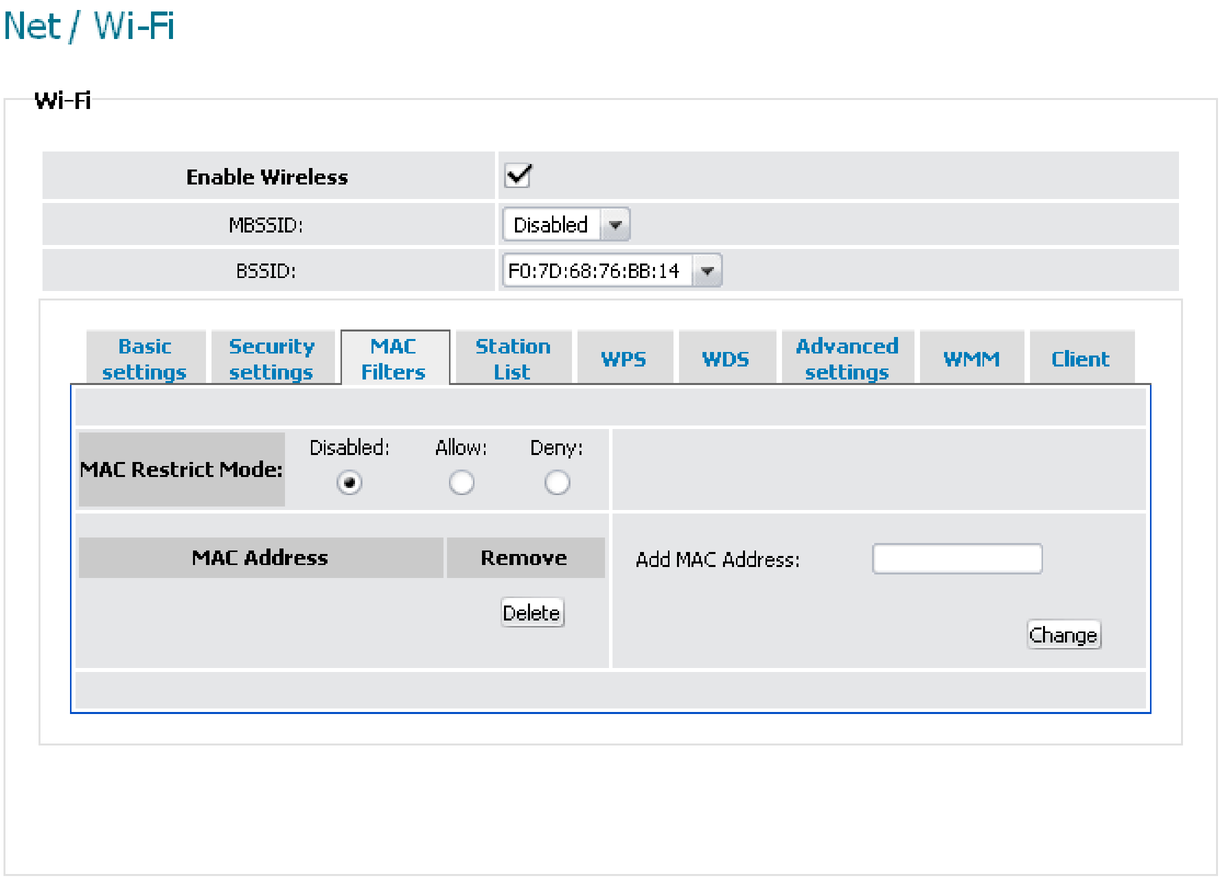
*Figure 37. The **WPA2** value is selected from the **Network Authentication** drop-down list.*

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

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

MAC Filters

On the **MAC Filters** tab, 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.



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

MAC Restrict Mode: Disabled: ● Allow: ○ Deny: ○

MAC Address	Remove

Add MAC Address:

Figure 38. MAC filters for the wireless network.

By default, MAC filtering is not active (the **Disabled** choice of the **MAC Restrict Mode** radio button is selected).

To add a MAC addresses to which the selected filtering mode will be applied, enter this address in the **Add MAC Address** field and click the **Change** button. After that, the entered address will be displayed in the MAC address table on the left part of the tab.

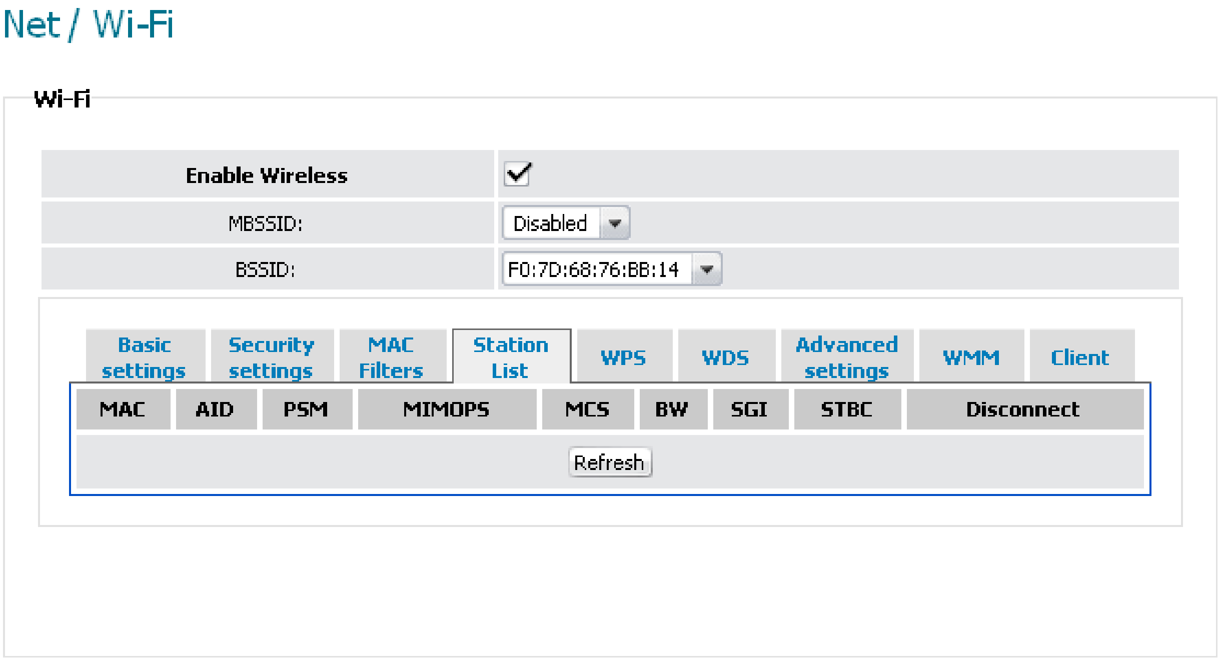
To remove a MAC address from the MAC address table, select the checkbox located to the left of the relevant MAC address in the table and click the **Delete** button.

To open your wireless network for the devices which MAC addresses are displayed in the table and to close the wireless network for all other devices, select the **Allow** choice of the **MAC Restrict Mode** radio button.

To close your wireless network for the devices which MAC addresses are displayed in the table, select the **Deny** choice of the **MAC Restrict Mode** radio button.

Station List

On the **Station List** tab, you can view the list of wireless devices connected to the router.



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

MAC	AID	PSM	MIMOPS	MCS	BW	SGI	STBC	Disconnect

Figure 39. The list of the router's wireless clients.

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

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

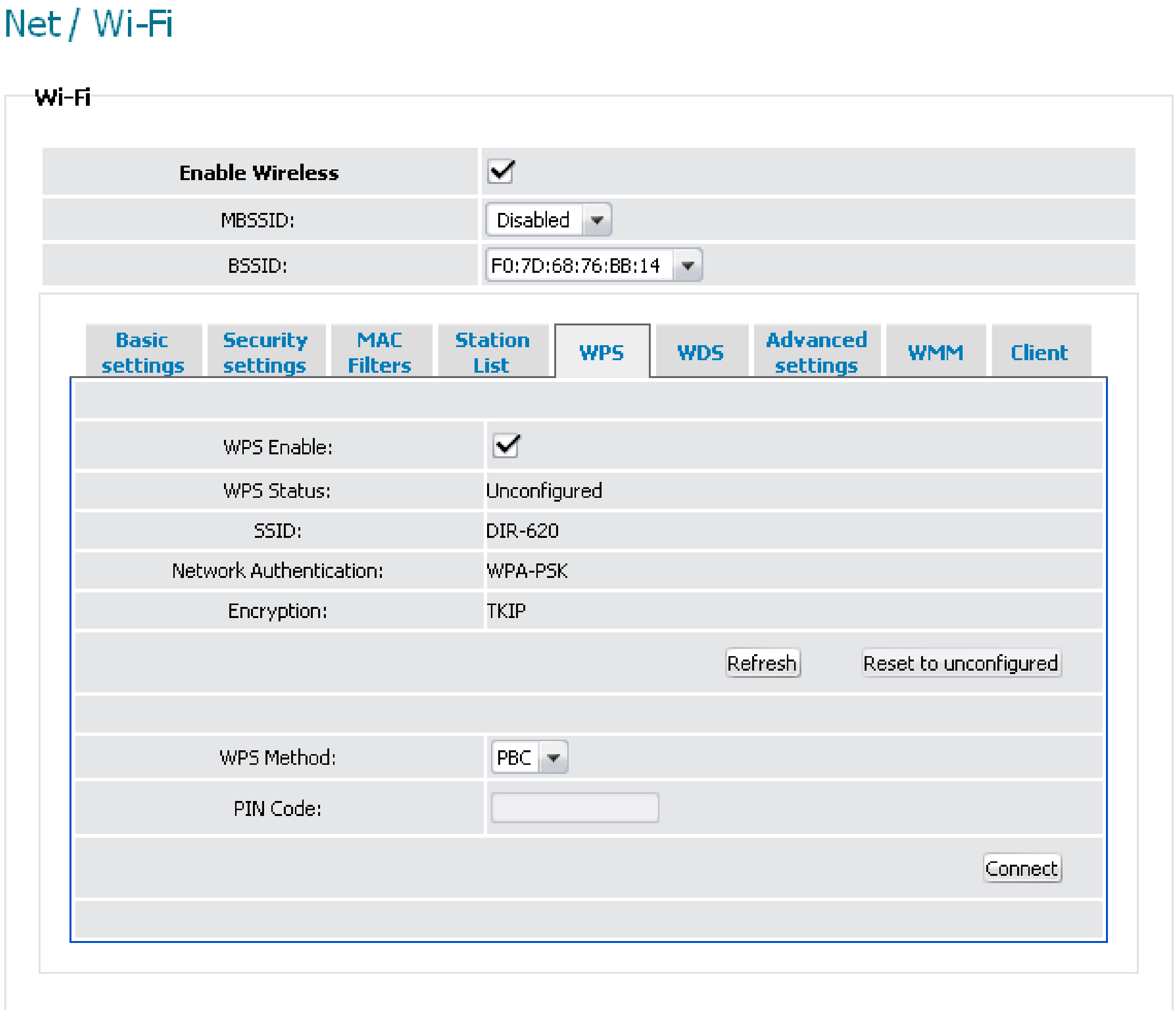
WPS

On the **WPS** tab, 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), 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.



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled ▾
BSSID:	F0:7D:68:76:BB:14 ▾

WPS Enable:	☑
WPS Status:	Unconfigured
SSID:	DIR-620
Network Authentication:	WPA-PSK
Encryption:	TKIP

WPS Method:	PBC ▾
PIN Code:	

Figure 40. The tab for configuring the WPS function.

The following fields are available on the tab:

Parameter	Description
WPS Enable	The checkbox that enables/disables the WPS function. When the checkbox is not selected, the other fields are not displayed on the tab.
WPS Status	The state of connecting the wireless device via the WPS function.
SSID	The name of the router's WLAN (or the first part of the WLAN if the network is splitted into parts).
Network Authentication	The network authentication type specified for the WLAN (or first part of the WLAN).
Encryption	The encryption type specified for the WLAN (or the first part of the WLAN).
Refresh	Click the button to view the latest data on the state of connecting the wireless device via the WPS function.
Reset to unconfigured	Click the button to reset the parameters of the WPS function in order to connect the next device.
WPS Method	A method of the WPS function. Select a value from the drop-down list. **PIN**: Connecting the device via the PIN code. **PBC**: Connecting the device via the push button (actual or virtual).
PIN Code	The PIN code of the WPS-enabled device that needs to be connected to the wireless network of the router. The field is available only when the **PIN** value is selected from the **WPS Method** drop-down list.
Connect	Click the button to connect the wireless device to the 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** checkbox.
2. Select the **PIN** value from the **WPS Method** drop-down list.
3. Select the PIN method in the software of the wireless device that you want to connect to the router's WLAN.
4. Click the relevant button in the software or on the cover of the wireless device that you want to connect to the WLAN.
5. Right after that, enter the PIN code specified on the cover of the wireless device or in its software in the **PIN Code** field.
6. 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** checkbox.
2. Select the **PBC** value from the **WPS Method** drop-down list.
3. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
4. Click the relevant button in the software or on the cover of the wireless device that you want to connect to the WLAN.
5. 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** checkbox.
3. Make sure that the **PBC** value is selected from the **WPS Method** drop-down list.
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.

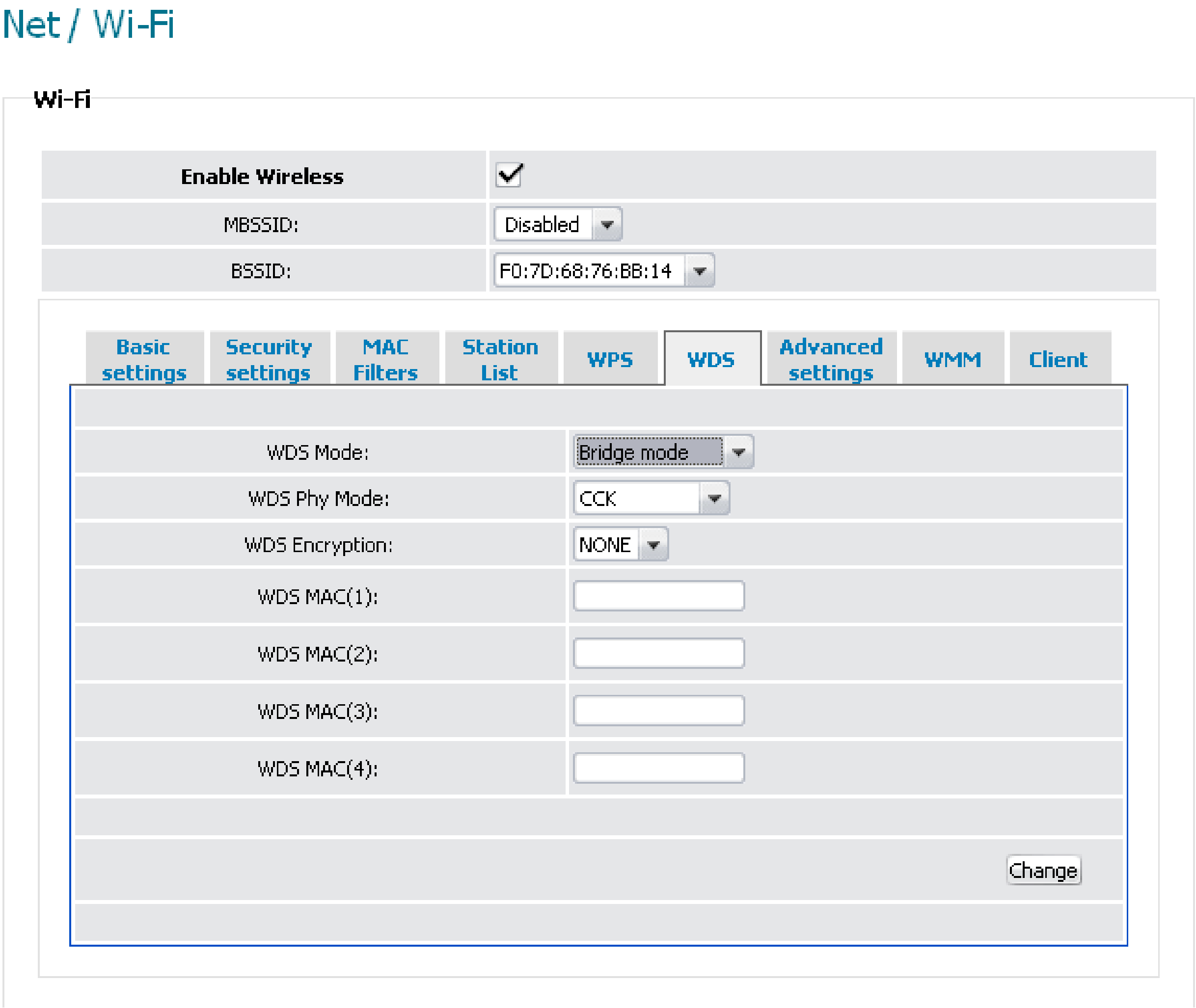
1. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
2. Click the relevant button in the software or on the cover of the wireless device that you want to connect to the WLAN.
3. Click the WPS button on the right side panel of the router.

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 **WDS** tab, you can enable the WDS function and select a mode of this function.

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



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

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

Figure 41. The tab for configuring the WDS function.

The following fields are available on the tab:

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

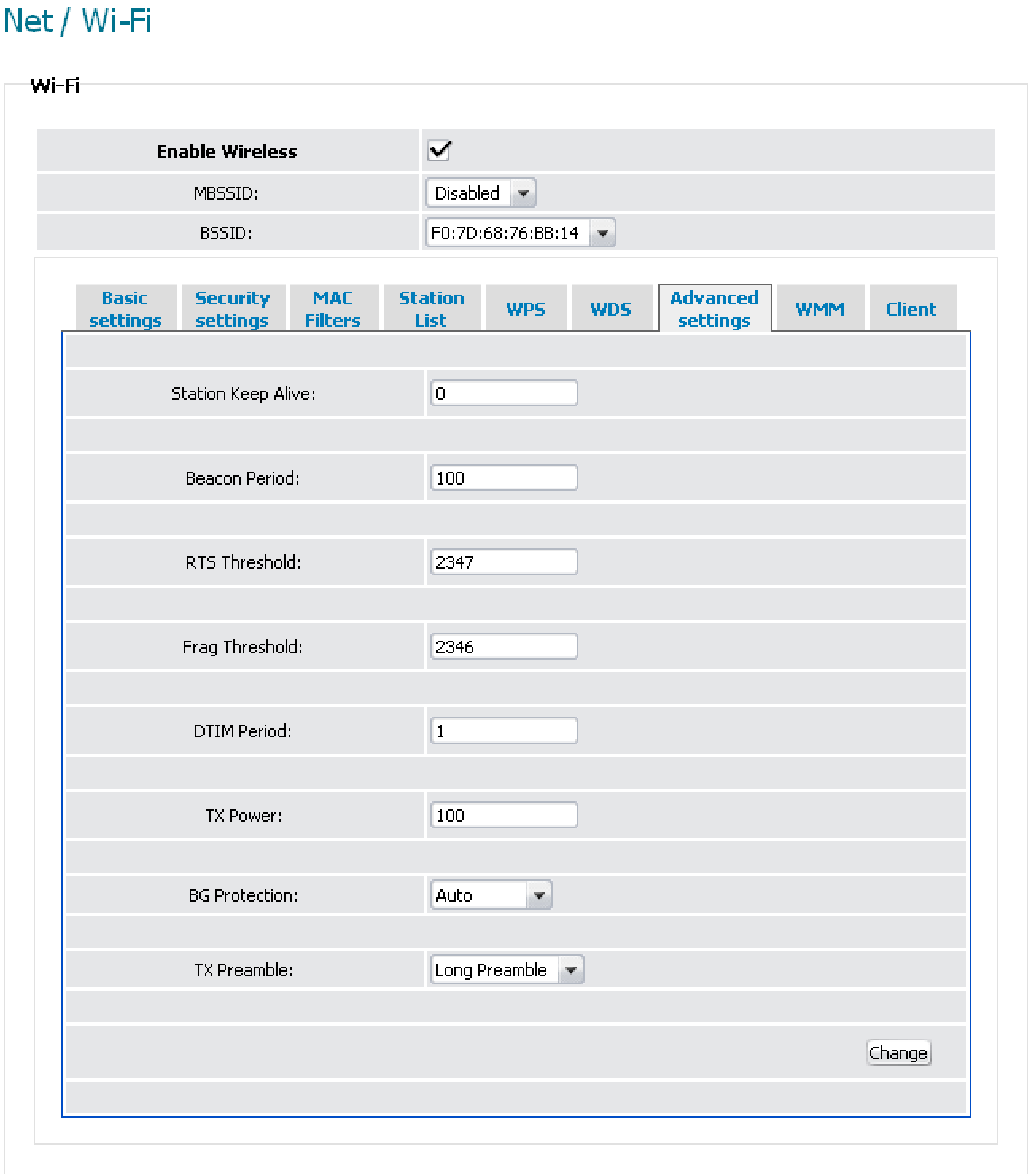
! The WDS function parameters specified on the tab must be the same for all interconnected devices. In addition, it is required to set the same channel (on the **Basic settings** tab).

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

Advanced Settings

On the **Advanced settings** tab, you can define additional parameters for the router's WLAN.

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



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

Station Keep Alive:	0
Beacon Period:	100
RTS Threshold:	2347
Frag Threshold:	2346
DTIM Period:	1
TX Power:	100
BG Protection:	Auto
TX Preamble:	Long Preamble

Figure 42. Advanced settings of the WLAN.

The following fields are available on the tab:

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

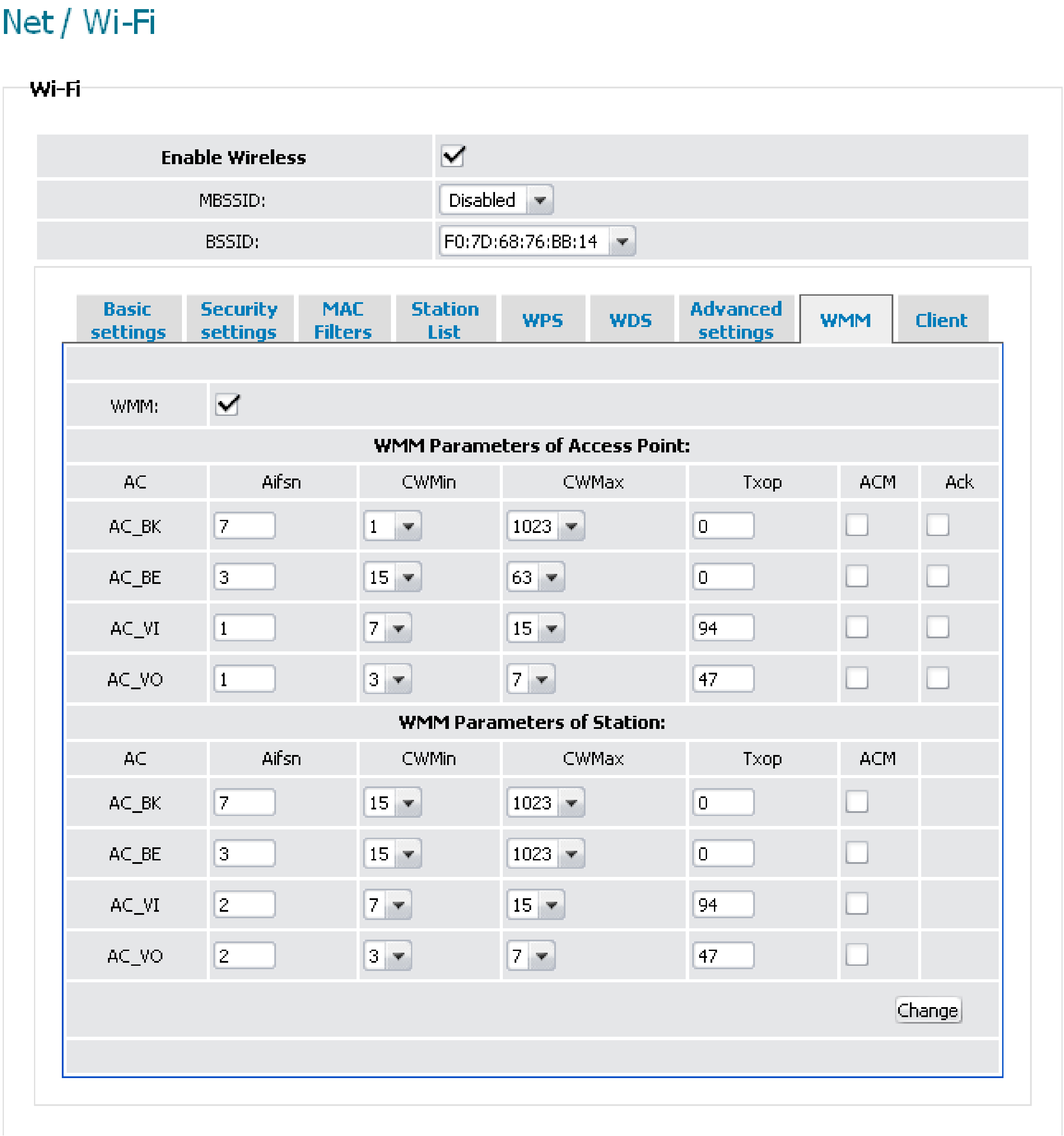
When you have configured the parameters, click the **Change** button.

WMM

On the **WMM** tab, 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.



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

WMM: ☑

WMM Parameters of Access Point:

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

WMM Parameters of Station:

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

Figure 43. The tab 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 **WMM Parameters of Access Point** section) and wireless devices connected to it (in the **WMM Parameters of Station** section).

For every Access Category the following fields are available:

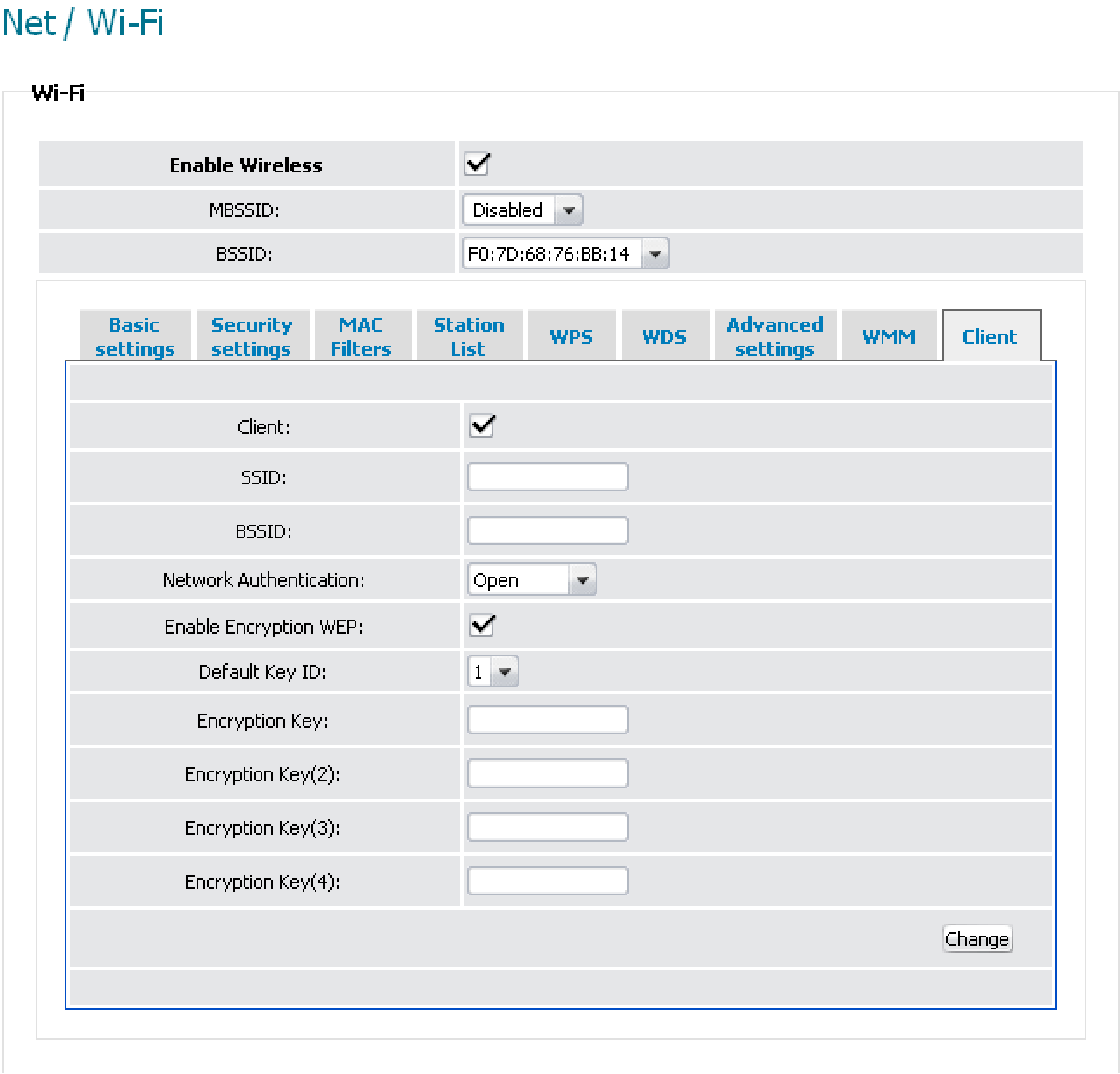
Parameter	Description
Aifsn	*Arbitrary Inter-Frame Space Number*. This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
CWMin/CWMax	*Contention Window Minimum/Contention Window Maximum*. Both fields influence time delays for the relevant Access Category. The **CWMax** field value should not be lower, than the **CWMin** field value. The lower the difference between the **CWMax** field value and the **CWMin** field value, the higher is the Access Category priority.
Txop	*Transmission Opportunity*. The higher the value, the higher is the Access Category priority.
ACM	*Admission Control Mandatory*. If selected, prevents from using the relevant Access Category.
Ack	*Acknowledgment*. Answering response requests while transmitting. Displayed only in the **WMM Parameters of Access Point** 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 **Client** tab, you can configure the router as a client to connect to a wireless access point.

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



Net / Wi-Fi

Wi-Fi

Enable Wireless	☑
MBSSID:	Disabled
BSSID:	F0:7D:68:76:BB:14

Client:	☑
SSID:	
BSSID:	
Network Authentication:	Open
Enable Encryption WEP:	☑
Default Key ID:	1
Encryption Key:	
Encryption Key(2):	
Encryption Key(3):	
Encryption Key(4):	

Figure 44. The tab for configuring the client mode.

The following fields are available on the tab:

Parameter	Description
Client	Select the checkbox to configure the router as a client.
SSID	The name of the network to which the router connects.
BSSID	The unique identifier of the network to which the router connects.
Network Authentication	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
Enable Encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the **Default Key ID** field and four **Encryption Key** fields are displayed on the page. For the **Shared** authentication type the checkbox is always selected.
Default Key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption Key (1-4)	Keys for WEP encryption. The router uses the key selected from the **Default Key ID** drop-down list. It is required to specify all the fields. 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
WPA Encryption	An encryption method: **TKIP** or **AES**.
Encryption Key	A key for WPA encryption.

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

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.

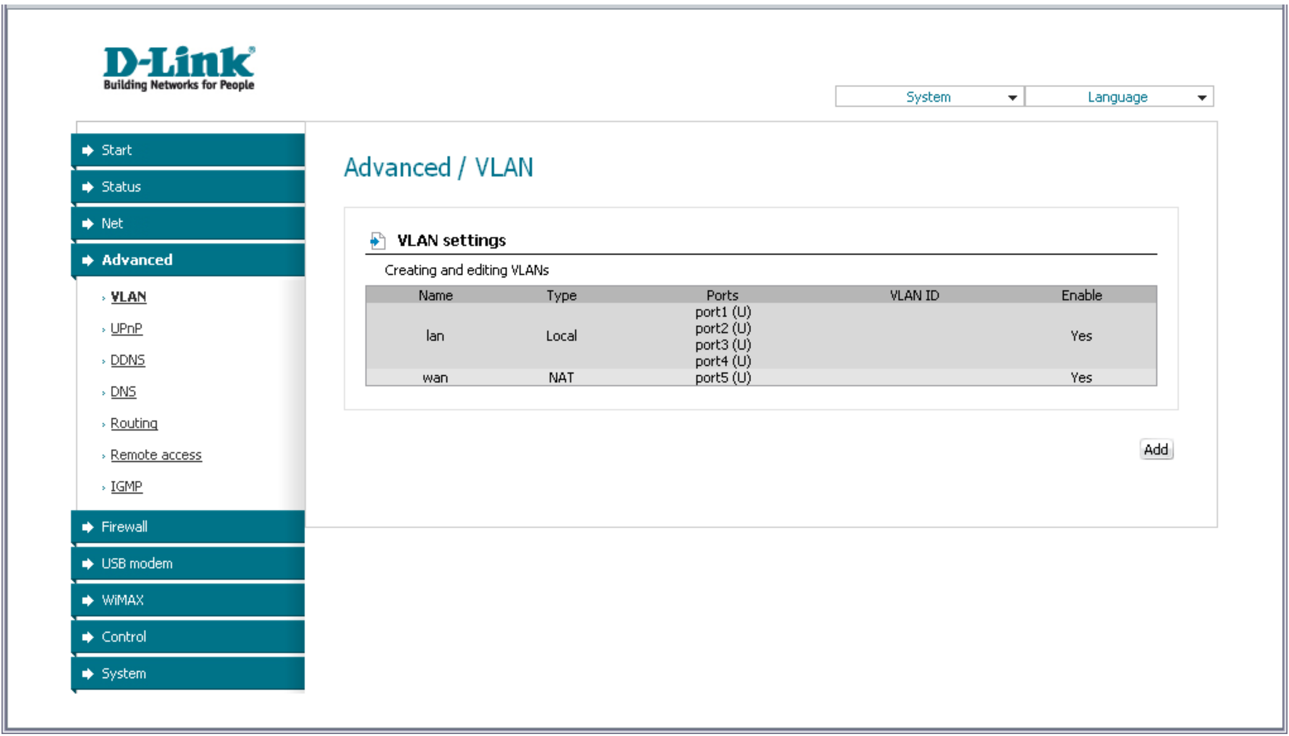
VLAN

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;
- **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.



Advanced / VLAN

VLAN settings

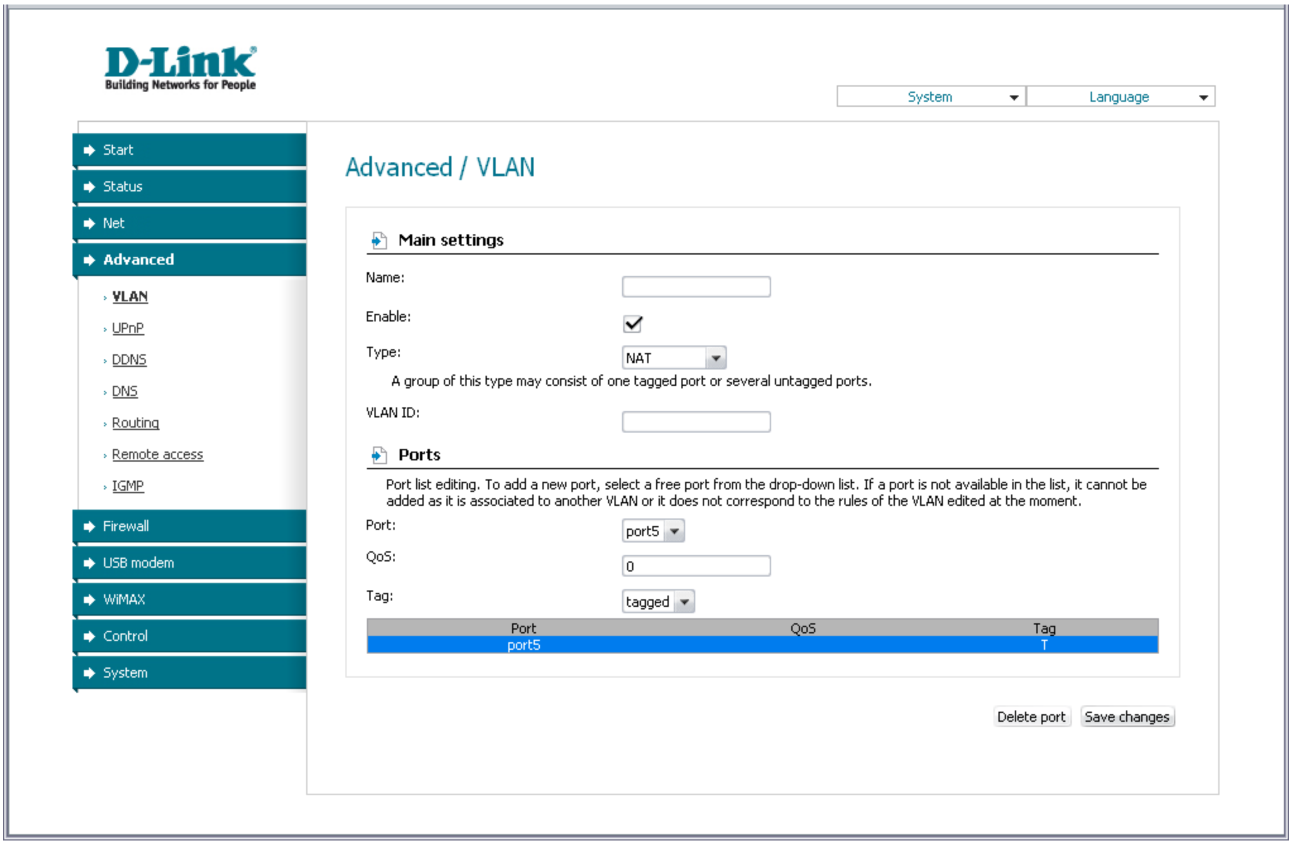
Creating and editing VLANs

Name	Type	Ports	VLAN ID	Enable
lan	Local	port1 (U) port2 (U) port3 (U) port4 (U)		Yes
wan	NAT	port5 (U)		Yes

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

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

! If you want to create a group including ports of the LAN interface, first delete these ports from the **lan** group on this page.



Advanced / VLAN

Main settings

Name:

Enable: ☑

Type: NAT

A group of this type may consist of one tagged port or several untagged ports.

VLAN ID:

Ports

Port list editing. To add a new port, select a free port from the drop-down list. If a port is not available in the list, it cannot be added as it is associated to another VLAN or it does not correspond to the rules of the VLAN edited at the moment.

Port: port5

QoS: 0

Tag: tagged

Port	QoS	Tag
port5		T

Figure 46. The page for adding a group of ports for VLAN.

You can specify the following parameters:

Parameter	Description
Main settings	
Name	A name for the port for easier identification.
Enable	Select the checkbox to allow using this group of ports.
Type	The type of the VLAN which identifier is specified in the **VLAN ID** field. **Local**. 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. **NAT**. The group of this type is an external connection with address translation. It is mostly used to connect to the Internet. Later the VLAN which identifier is specified in the **VLAN ID** field is used to create a WAN connection of the IPoE or PPPoE type (on the **Net / Connections** page). **Transparent**. 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.

VLAN ID	An identifier of the VLAN to which this group of ports will be assigned.
Ports	
Port	From the list, select a free port to assign it to this group. The port will be displayed in the table at the bottom of the page.
QoS	A priority tag for the traffic transmitted through the port highlighted in the table at the bottom of the page.
Tag	Select a value for the port highlighted in the table at the bottom of the page: • **tagged**, • **untagged**.

Click the **Save changes** button.

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

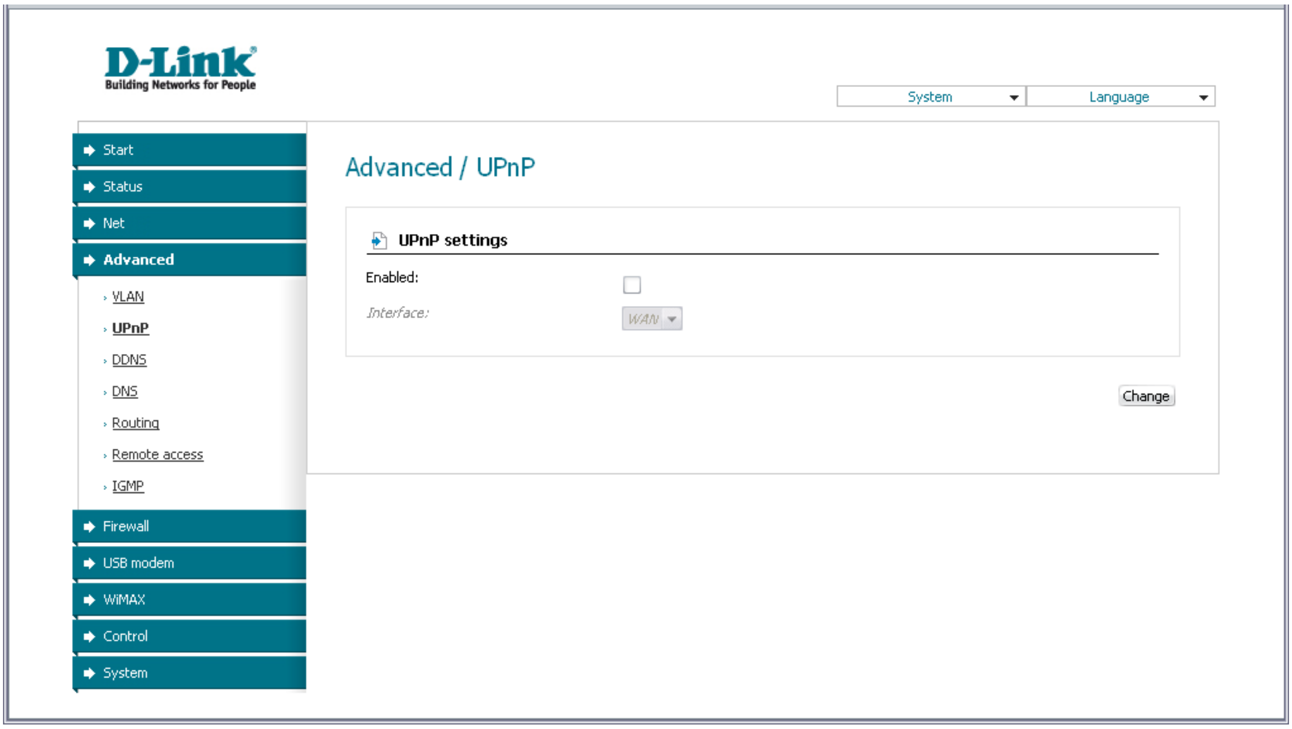
Click the **Delete VLAN** button to delete this group of ports form the system.

! 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.



Advanced / UPnP

UPnP settings

Enabled: □

Interface: WAN

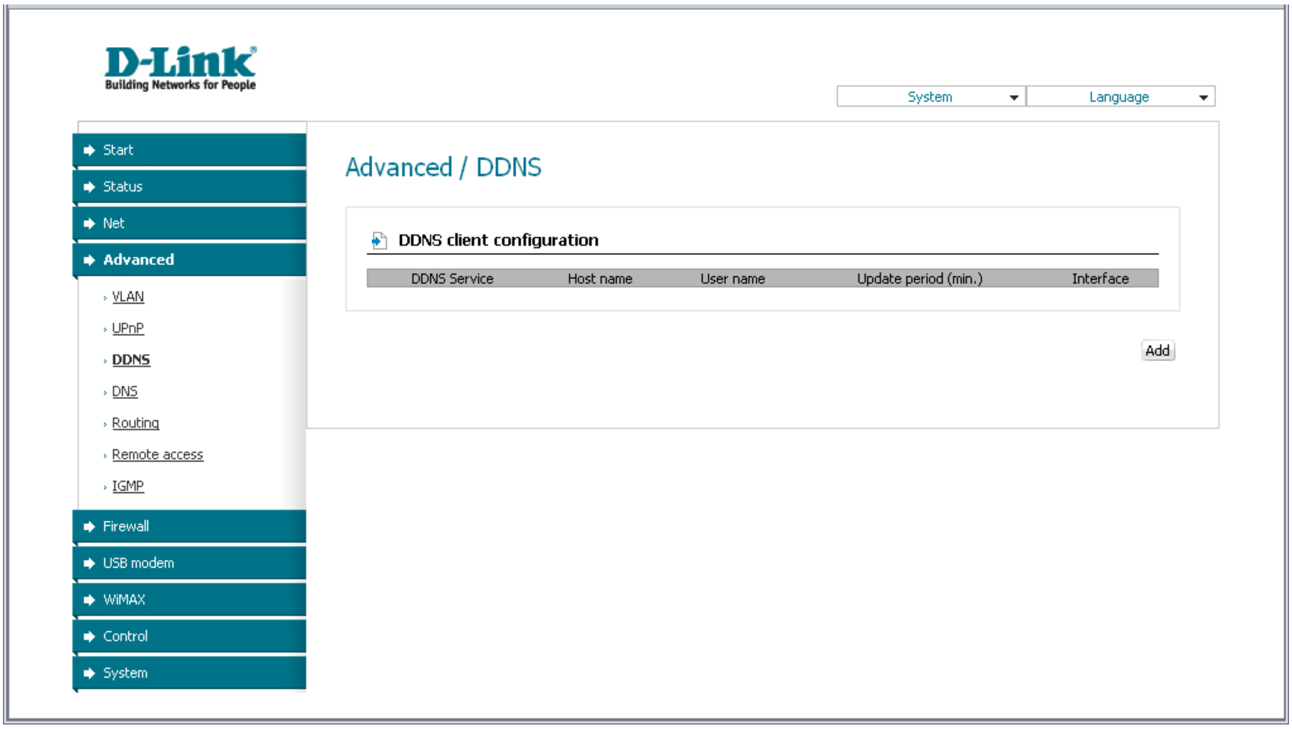
*Figure 47. The **Advanced / UPnP** page.*

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.



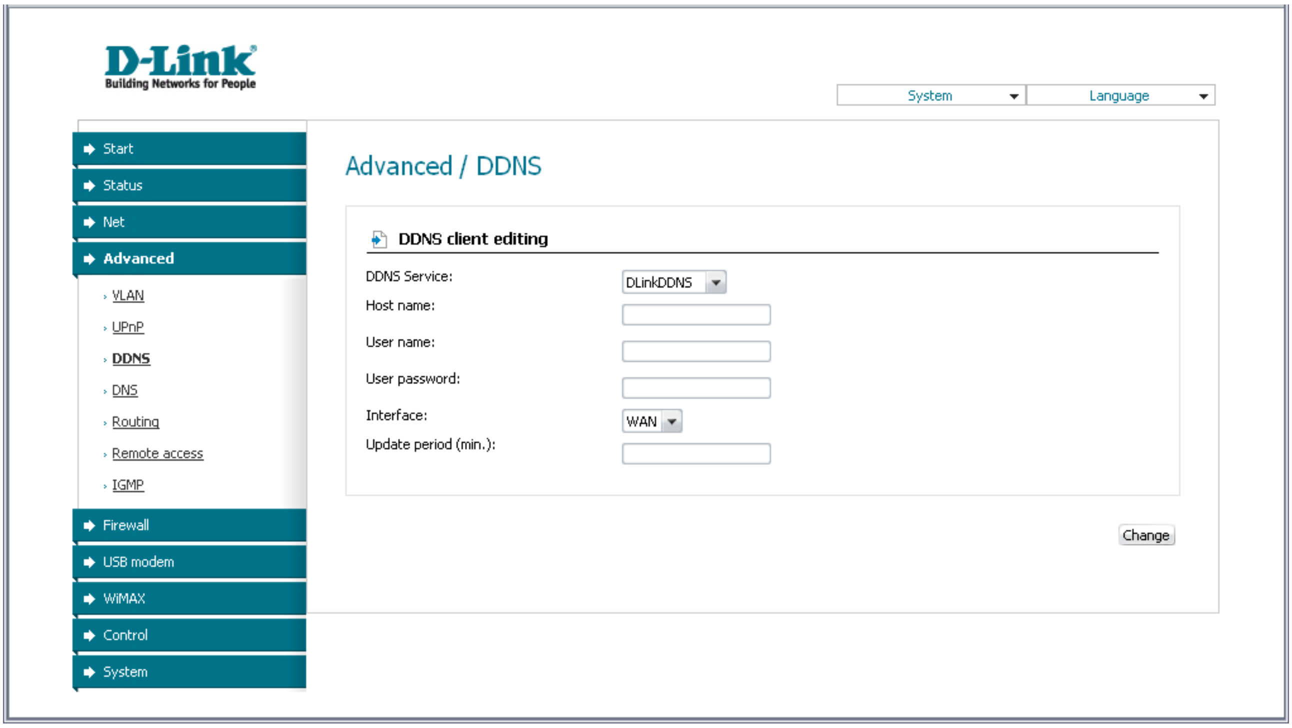
Advanced / DDNS

DDNS client configuration

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

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

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



Advanced / DDNS

DDNS client editing

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

Figure 49. The page for adding a DDNS service.

You can specify the following parameters:

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

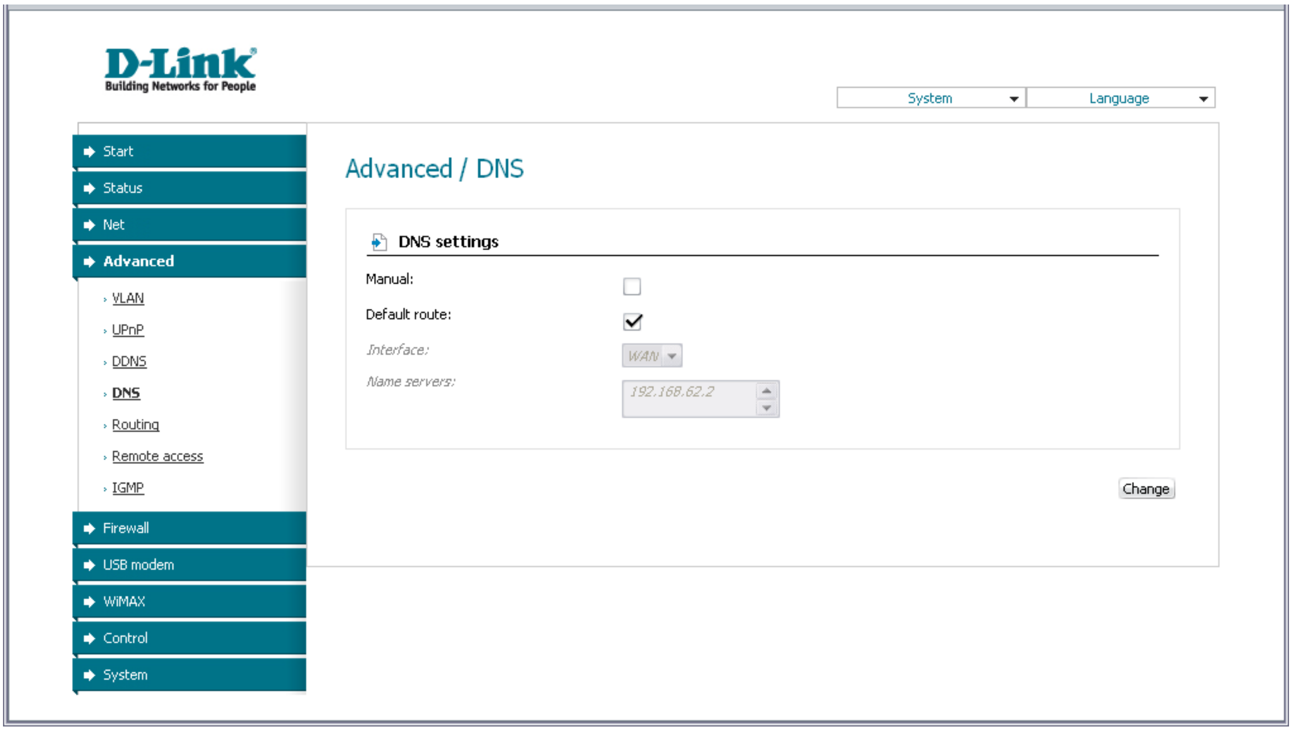
Click the **Change** button.

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

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

DNS

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



Advanced / DNS

DNS settings

Manual: □

Default route: ☑

Interface: WAN

Name servers: 192.168.62.2

*Figure 50. 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.

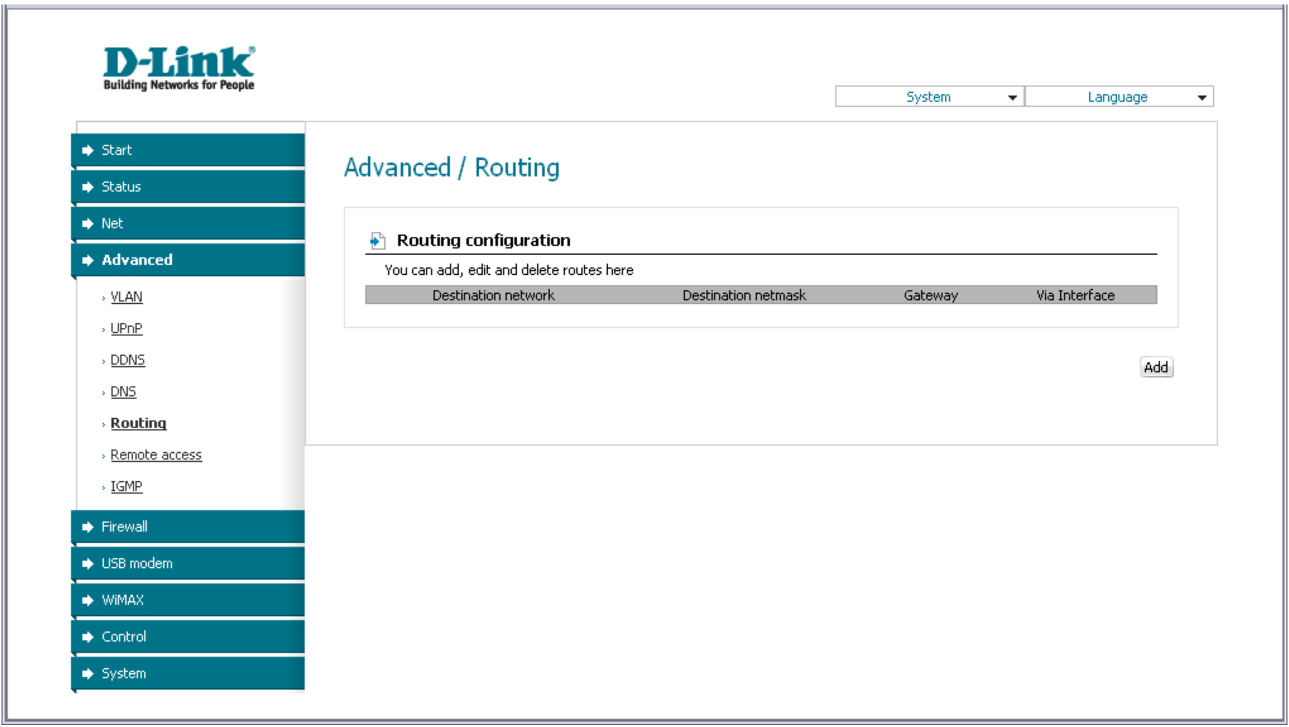
If you want to configure automatic obtainment of DNS servers addresses, deselect the **Manual** checkbox, select a WAN connection which will be used to obtain addresses of DNS servers automatically from the **Interface** drop-down list or select the **Default route** checkbox, so that the router could 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 set addresses of DNS servers manually, select the **Manual** checkbox, enter a DNS server address in the **Name servers** list, and 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.



Advanced / Routing

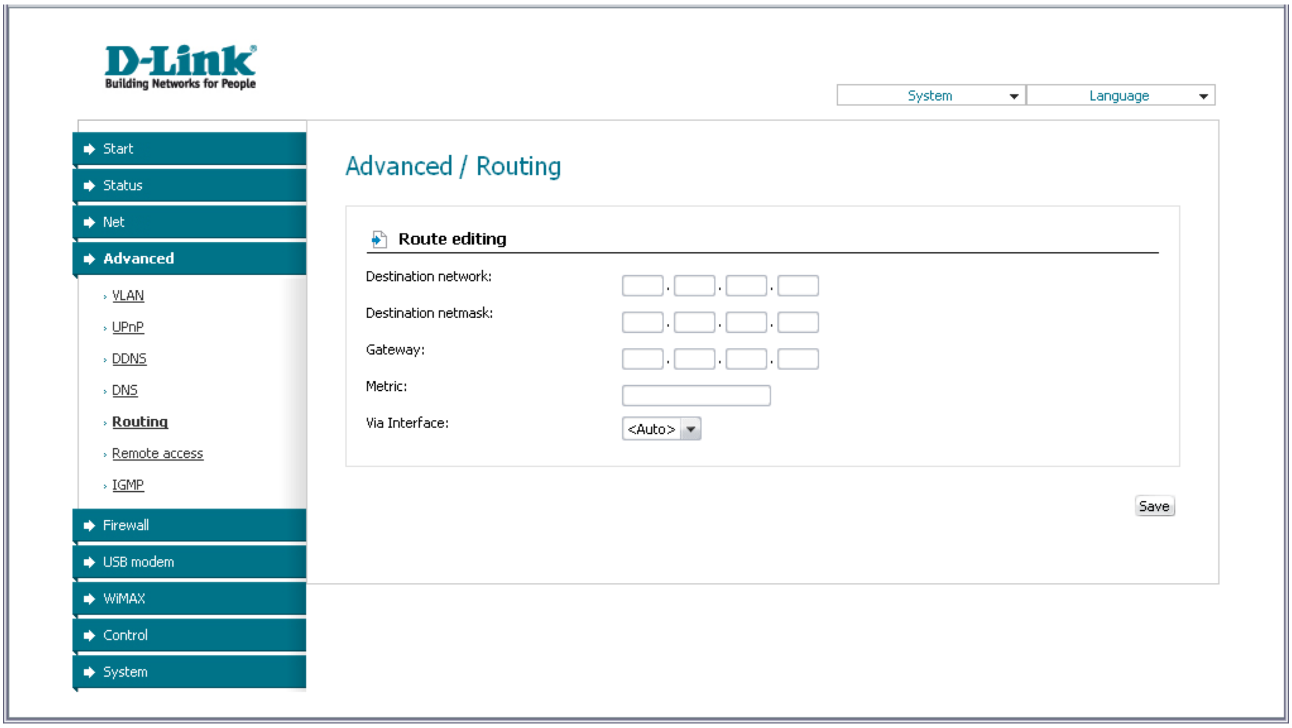
Routing configuration

You can add, edit and delete routes here

Destination network	Destination netmask	Gateway	Via Interface

*Figure 51. The **Advanced / Routing** page.*

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



Advanced / Routing

Route editing

Destination network: . . .

Destination netmask: . . .

Gateway: . . .

Metric:

Via Interface: <Auto>

Figure 52. The page for adding a static route.

You can specify the following parameters:

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

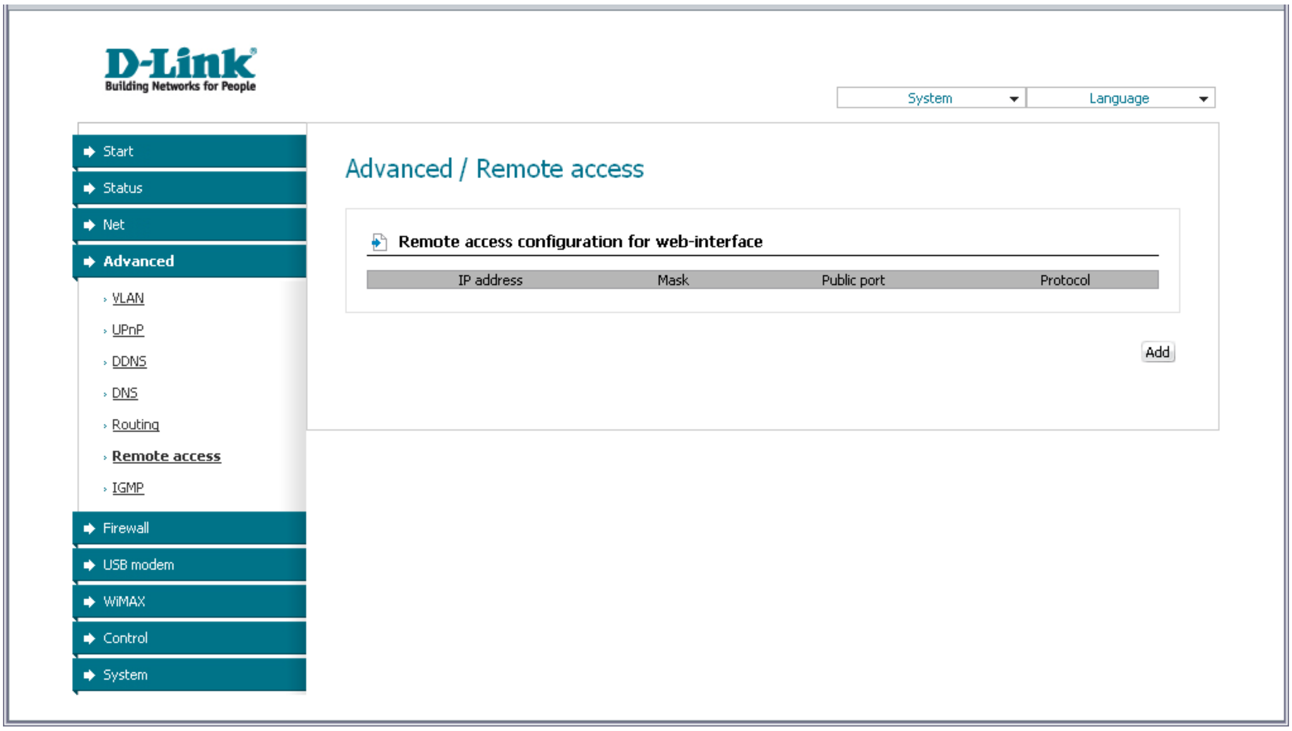
Click the **Change** button.

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



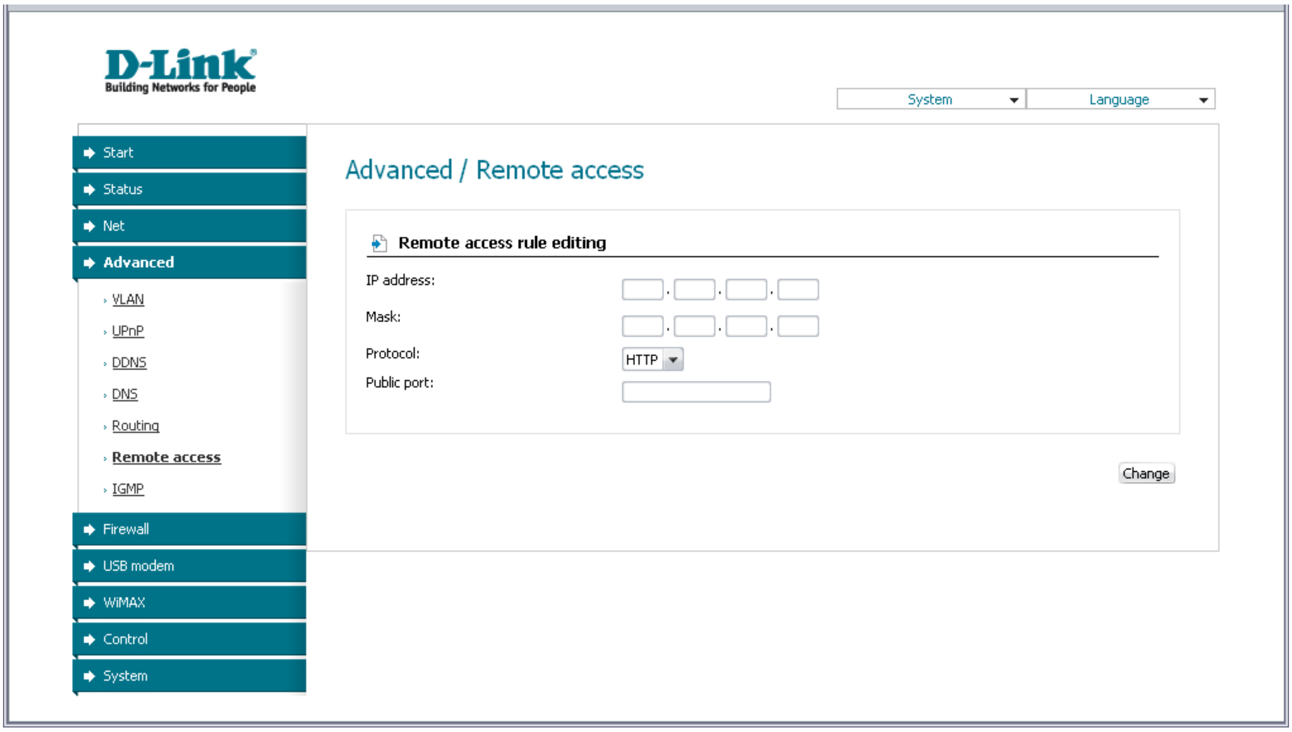
Advanced / Remote access

Remote access configuration for web-interface

IP address	Mask	Public port	Protocol

*Figure 53. The **Advanced / Remote access** page.*

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



Advanced / Remote access

Remote access rule editing

IP address: . . .

Mask: . . .

Protocol: HTTP

Public port:

Figure 54. The page for adding a rule for remote management.

You can specify the following parameters:

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

Click the **Change** button.

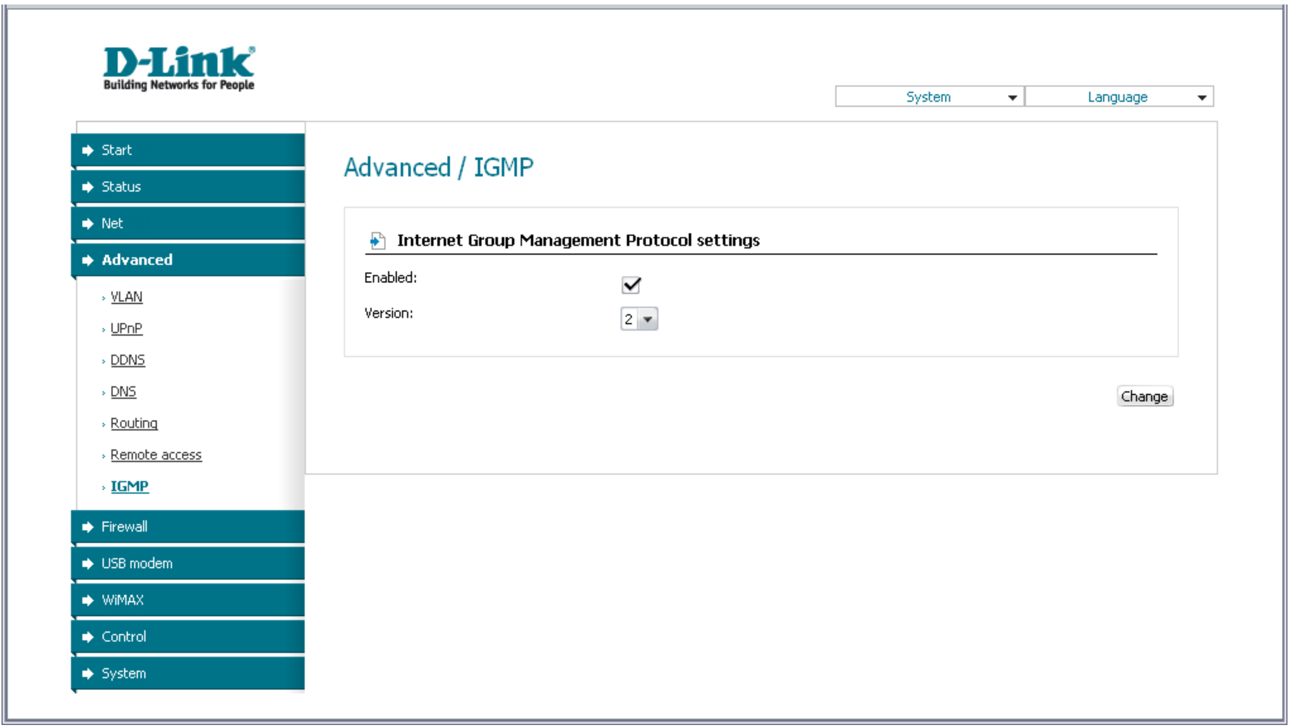
To edit a rule for remote access, click the relevant link. On the opened page, change the needed parameters and click the **Change** button.

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.



Internet Group Management Protocol settings

Enabled: ☑

Version: 2

*Figure 55. 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.

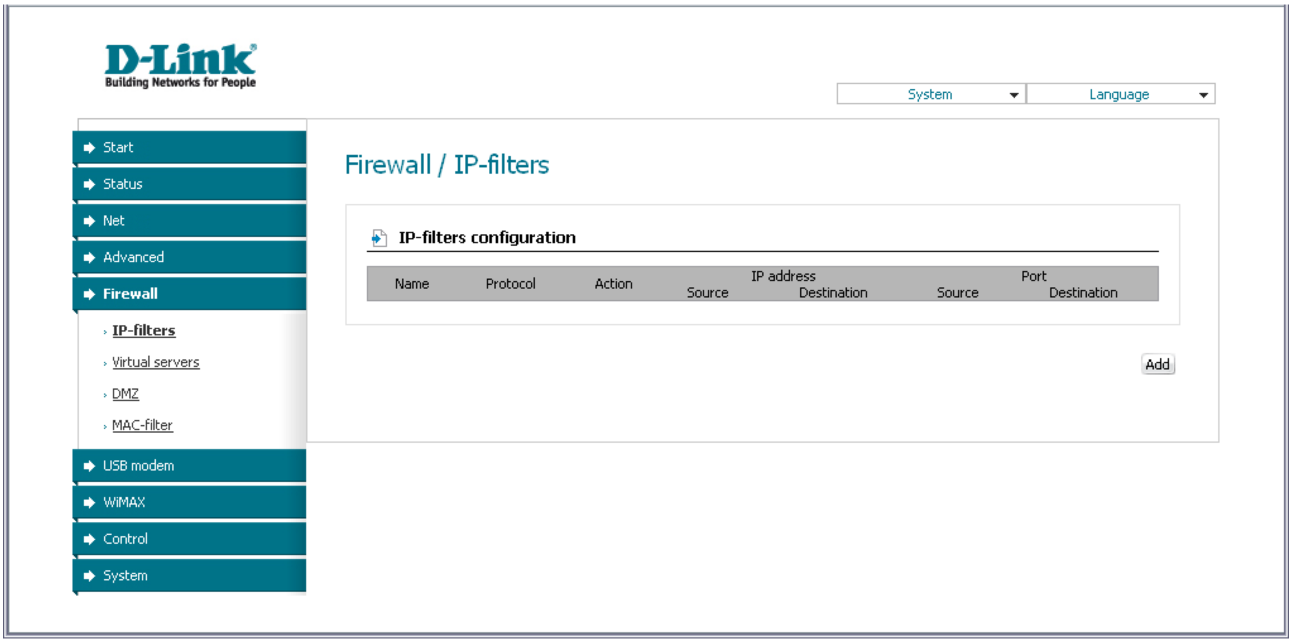


*Figure 56. The **Firewall / IP filters** page.*

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

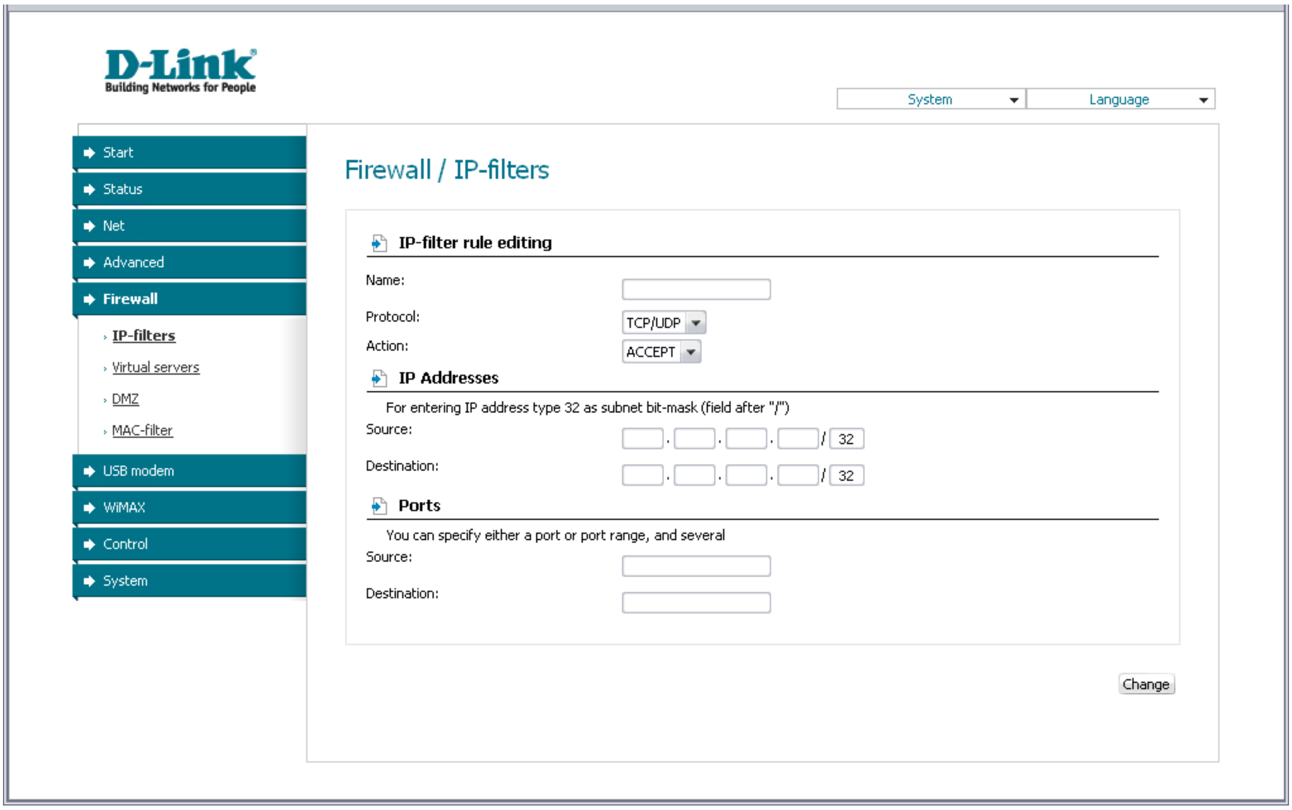


Figure 57. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
IP-filter rule editing	
Name	A name for the rule for easier identification.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.
Action	Select an action for the rule. **ACCEPT**: Allows packet transmission in accordance with the criteria specified by the rule. **DROP**: Denies packet transmission in accordance with the criteria specified by the rule.
IP Addresses	
Source	The source host/subnet IP address. To specify an IP address leave **32** in the field following the slash character (/).
Destination	The destination host/subnet IP address. To specify an IP address leave **32** in the field following the slash character (/).

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

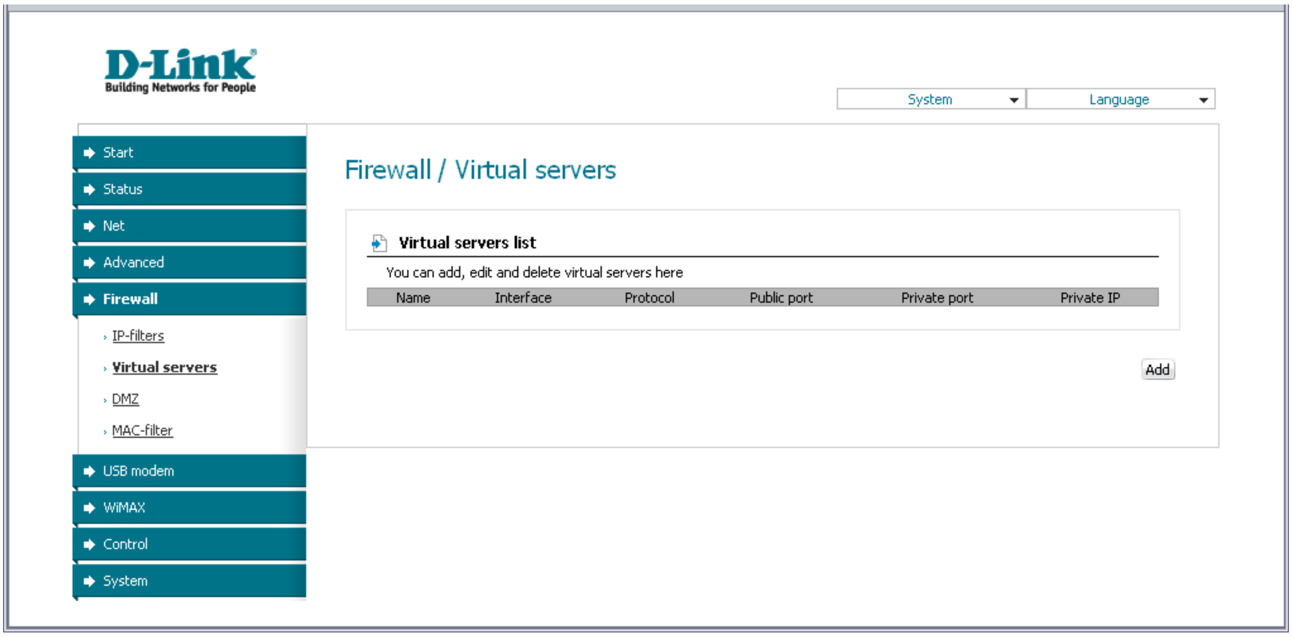
Click the **Change** button.

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

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

Virtual Servers

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



Firewall / Virtual servers

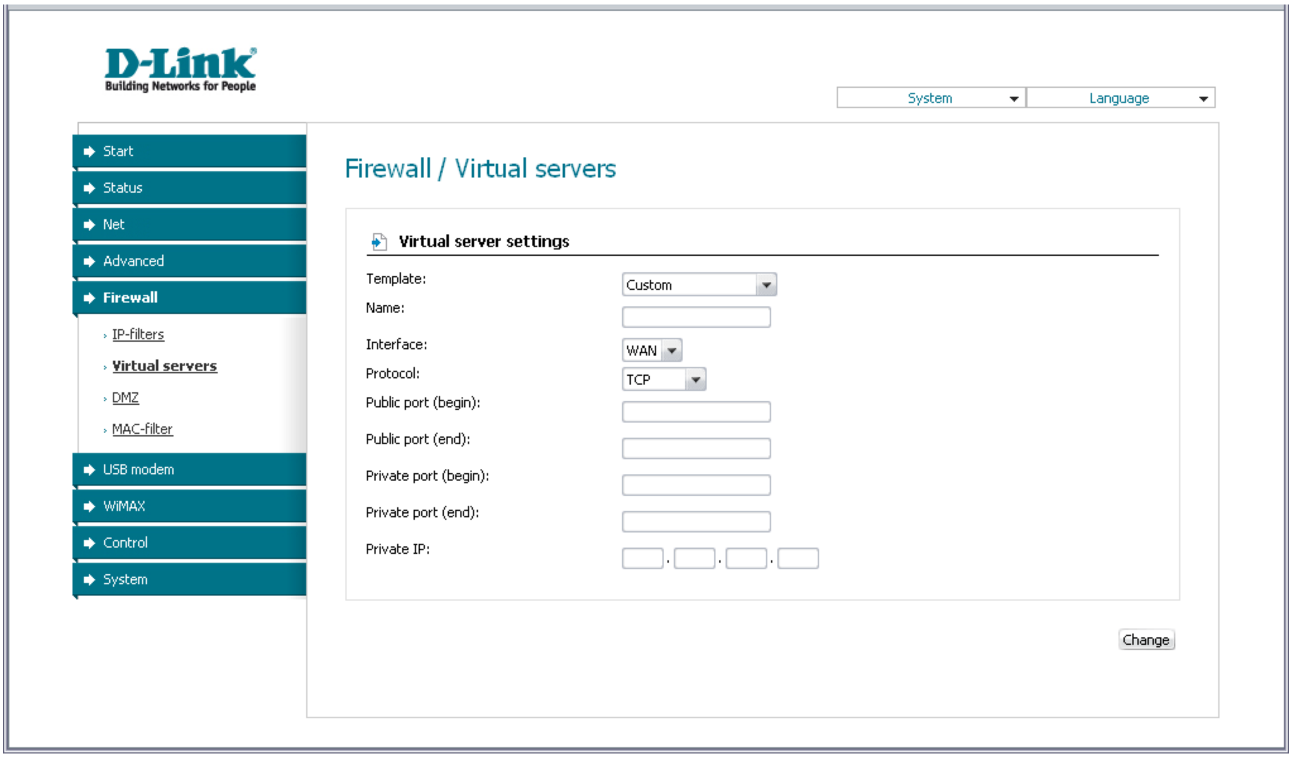
Virtual servers list

You can add, edit and delete virtual servers here

Name	Interface	Protocol	Public port	Private port	Private IP

*Figure 58. The **Firewall / Virtual servers** page.*

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



Firewall / Virtual servers

Virtual server settings

Template: Custom
Name:
Interface: WAN
Protocol: TCP
Public port (begin):
Public port (end):
Private port (begin):
Private port (end):
Private IP: . . .

Figure 59. The page for adding a virtual server.

You can specify the following parameters:

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

Click the **Change** button.

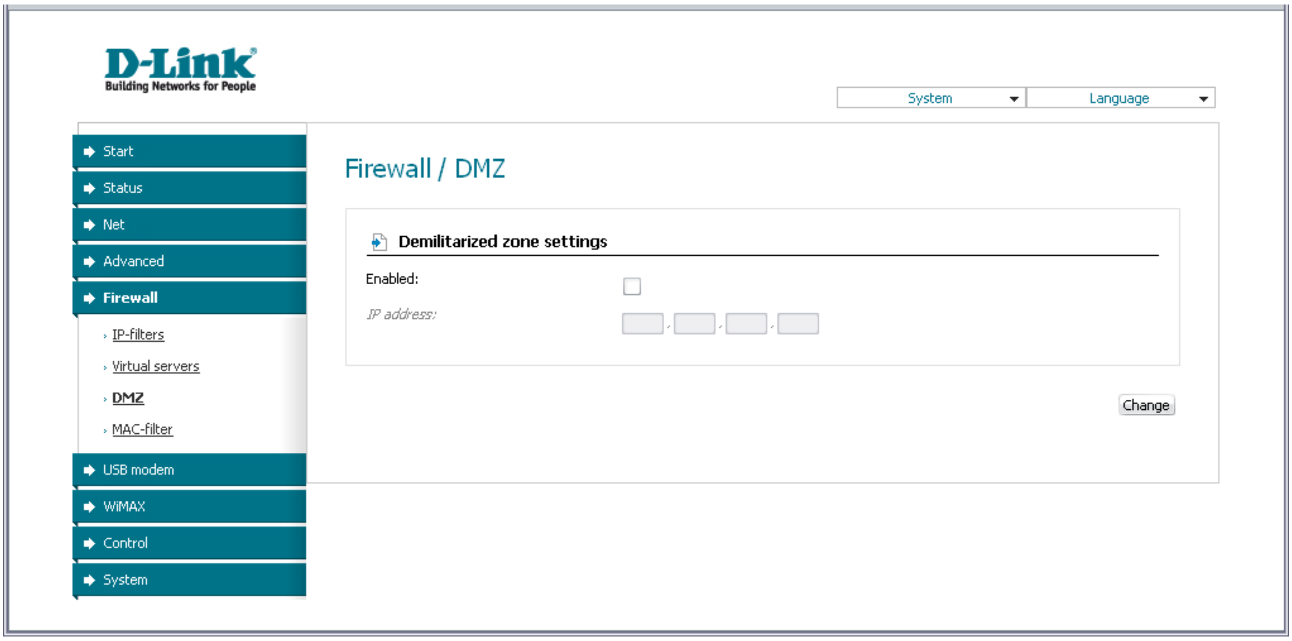
To edit the parameters of an existing server, follow the link with the name of the server. On the opened page, change the needed parameters and click the **Change** button.

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.



Firewall / DMZ

Demilitarized zone settings

Enabled: □

IP address: . . .

*Figure 60. The **Firewall / DMZ** page.*

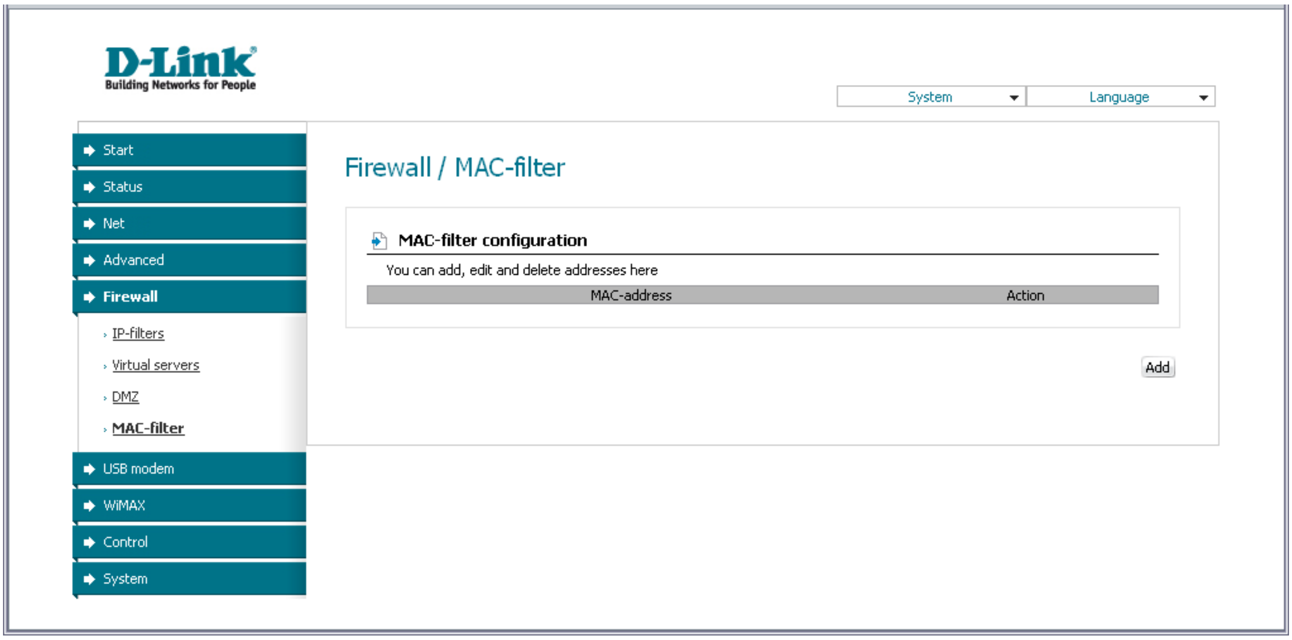
To enable the DMZ, select the **Enabled** checkbox, enter the IP address of a host from your network in the **IP address** field, and click the **Change** button.

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.



Firewall / MAC-filter

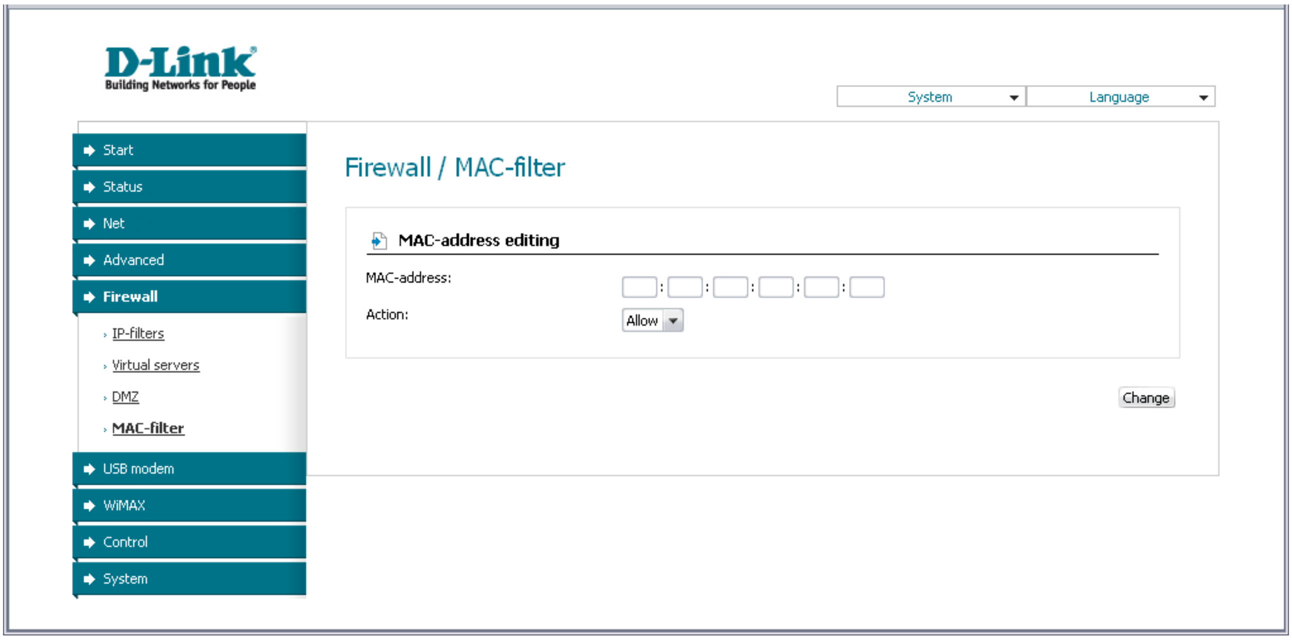
MAC-filter configuration

You can add, edit and delete addresses here

MAC-address	Action

*Figure 61. The **Firewall / MAC-filter** page.*

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



MAC-address: __ : __ : __ : __ : __ : __
Action: Allow

Figure 62. 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.

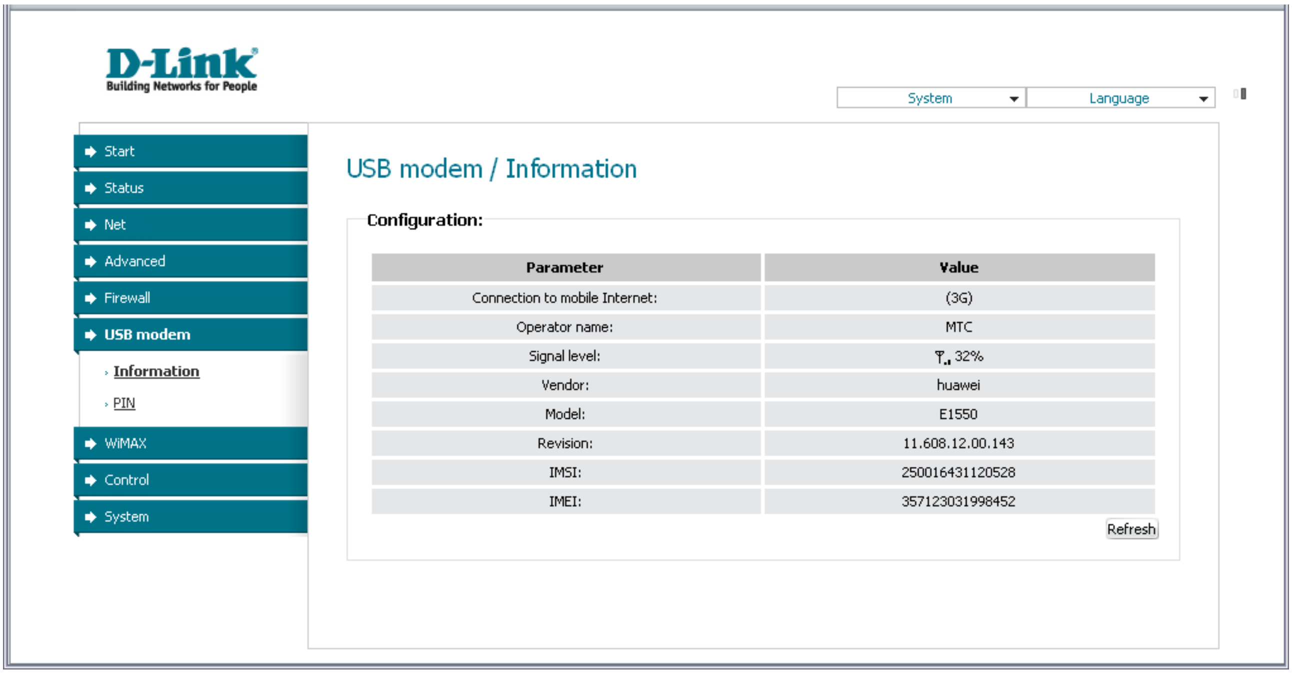
To remove an address from the list of MAC addresses for filtering, select the line with the relevant MAC address. On the opened page, click the **Delete** button.

USB Modem

This menu is designed to operate 3G USB modems.

Information

On the **USB modem / Information** page, you can view data on the connected 3G USB modem.



USB modem / Information

Configuration:

Parameter	Value
Connection to mobile Internet:	(3G)
Operator name:	MTC
Signal level:	32%
Vendor:	huawei
Model:	E1550
Revision:	11.608.12.00.143
IMSI:	250016431120528
IMEI:	357123031998452

*Figure 63. The **USB modem / Information** page.*

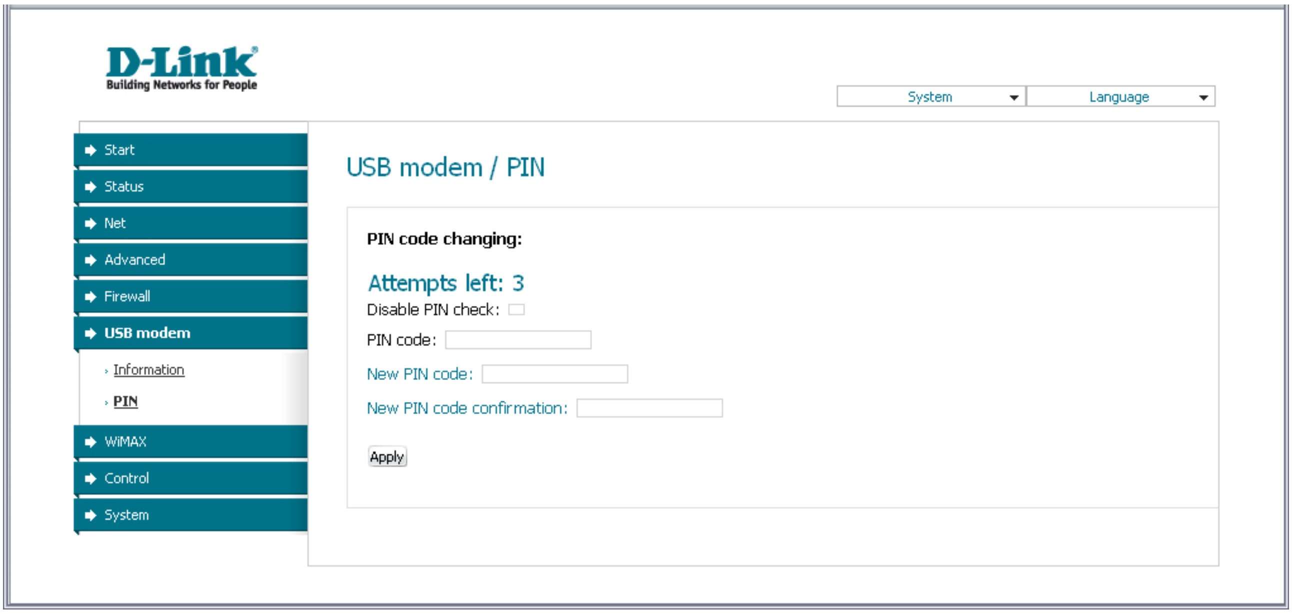
When a 3G USB modem is connected to the router, the following data are available on the page:

Parameter	Description
Connection to mobile Internet	The type of the operator's network. *This field is not displayed for a CDMA USB modem.*
Operator name	When the network is available, the name of the operator is displayed in this field. *This field is not displayed for a CDMA USB modem.*
Signal level	The signal level at the input of the modem's receiver. The zero signal level shows that you are out of the coverage area of the operator's network.
Vendor	The manufacturer of your 3G USB modem.
Model	The alphanumeric code of the model of your USB modem.
Revision	The revision of the firmware of your 3G USB modem.
IMSI	The code stored in the SIM card inserted to your 3G USB modem. *This field is not displayed for a CDMA USB modem.*
IMEI	The code stored in the memory of the 3G USB modem.
Refresh	Click the button to refresh the data on the 3G USB modem connected to the router.

PIN

! Operations presented in the page are available not for all models of 3G USB modems.

On the **USB modem / PIN** page, you can change the PIN code of the identification card inserted to your 3G USB modem, and disable or enable the check of the PIN code.



PIN code changing:

Attempts left: 3

Disable PIN check: □

PIN code:

New PIN code:

New PIN code confirmation:

Apply

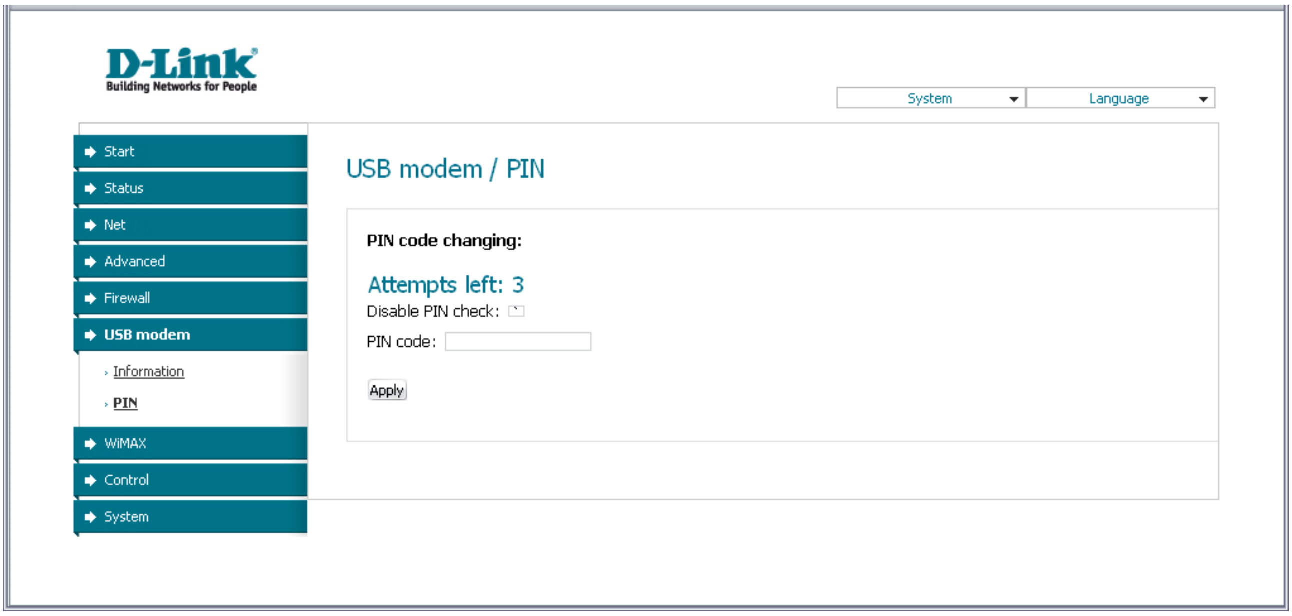
*Figure 64. The **USB modem / PIN** page. The PIN code check is enabled.*

If the PIN code check is enabled (the **Disable PIN check** checkbox is deselected), the following fields are displayed on the page:

Parameter	Description
PIN code	Enter the current PIN code of the identification card in this field.
New PIN code	Enter a new PIN code in this field.
New PIN code confirmation	Enter the new PIN code again to avoid mistypes.

When you have specified the new PIN code, click the **Apply** button.

To disable the PIN code check, select the **Disable PIN check** checkbox, enter the current PIN code in the **PIN code** field, and click the **Apply** button.



PIN code changing:

Attempts left: 3

Disable PIN check: ☑

PIN code:

Apply

*Figure 65. The **USB modem / PIN** page. The PIN code check is disabled.*

If you want to enable the PIN code check, deselect the **Disable PIN check** checkbox and enter the PIN code, used before disabling the check, in the **PIN code** field. Then click the **Apply** button.

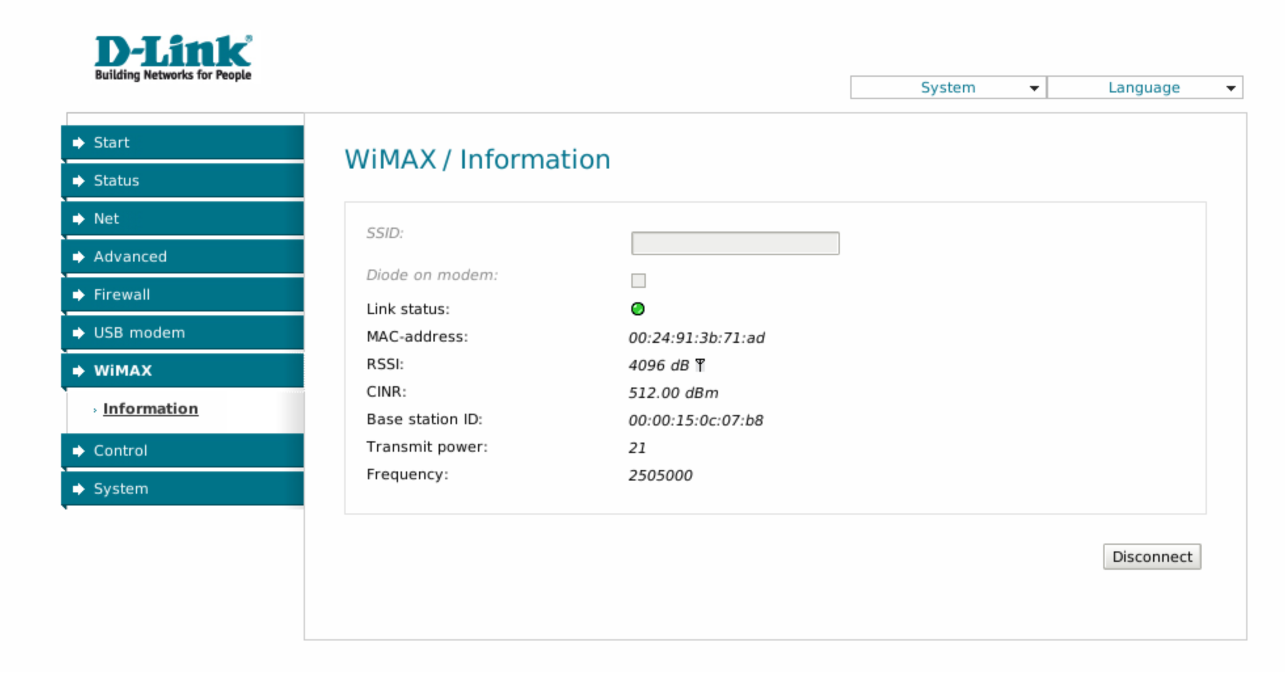
If during one of the operations described above you have entered an incorrect value in the **PIN code** field three times (the number of remaining attempts is displayed in the **Attempts left** field), the identification card inserted into your 3G USB modem is blocked. For further use of the card, enter the PUK code in the relevant field, and then specify a new PIN code in the **New PIN code** and **New PIN code confirmation** fields. Click the **Apply** button.

WiMAX

This menu is designed to operate WiMAX USB modems.

Information

On the **WiMAX / Information** page, you can connect to the network of your WiMAX ISP to establish a high-speed wireless connection to the Internet.



WiMAX / Information

SSID:
Diode on modem: □
Link status: ●
MAC-address: 00:24:91:3b:71:ad
RSSI: 4096 dB
CINR: 512.00 dBm
Base station ID: 00:00:15:0c:07:b8
Transmit power: 21
Frequency: 2505000

*Figure 66. The **WiMAX / Information** page.*

The following fields and controls are available on the page:

Parameter	Description
SSID	An identifier for the WiMAX network. Specify the parameter if your WiMAX ISP requires this.
Diode on modem	Select the checkbox to enable the modem's LED indicator.
Link status	The state of connection to the WiMAX network. **Red light**: The connection is not established. **Yellow light**: The USB modem is connecting to the network. **Green light**: The connection is established.
MAC-address	The MAC address of the WiMAX USB modem.
RSSI	The signal level at the input of the modem's receiver.

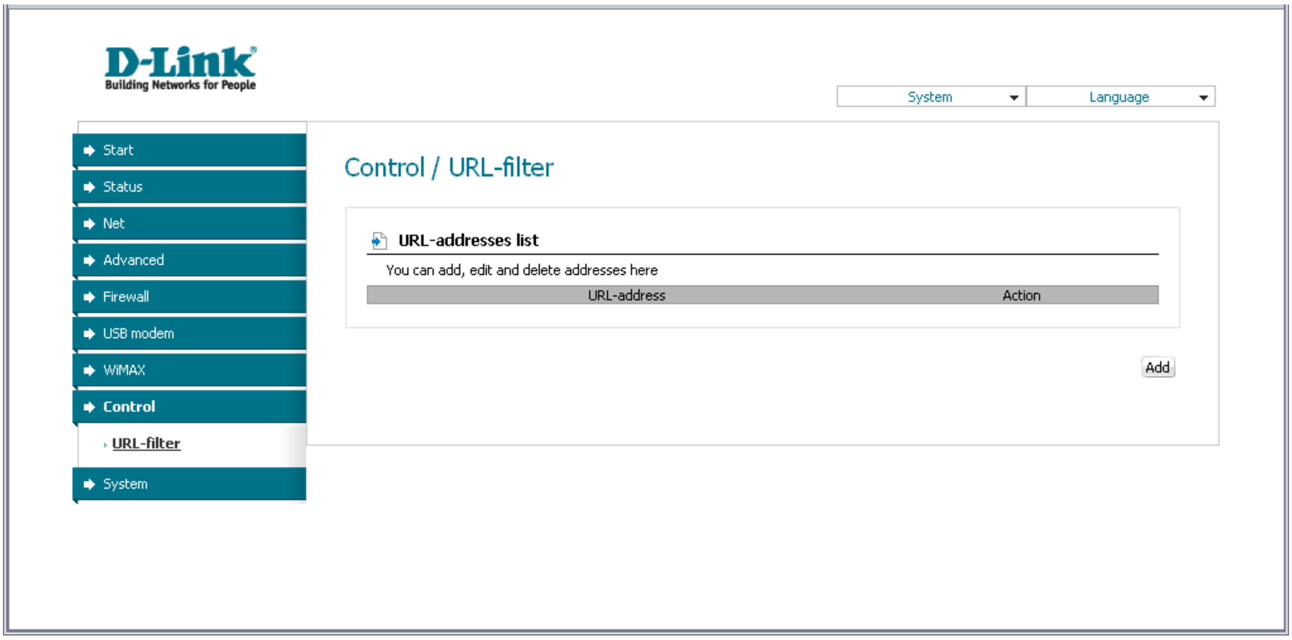
Parameter	Description
CINR	The relation of the signal level to the noise level. This parameter is used to measure the quality of the signal.
Base station ID	The identifier of the base station.
Transmit power	The signal level at the output of the modem's receiver.
Frequency	The frequency of the signal transmitted by the modem's receiver.
Connect	Click the button to connect to the WiMAX network. The button is displayed when the connection is not established.
Disconnect	Click the button to disconnect from the WiMAX network. The button is displayed when the connection is established or is being established.

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.



Control / URL-filter

URL-addresses list

You can add, edit and delete addresses here

URL-address	Action

*Figure 67. The **Control / URL-filter** page.*

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

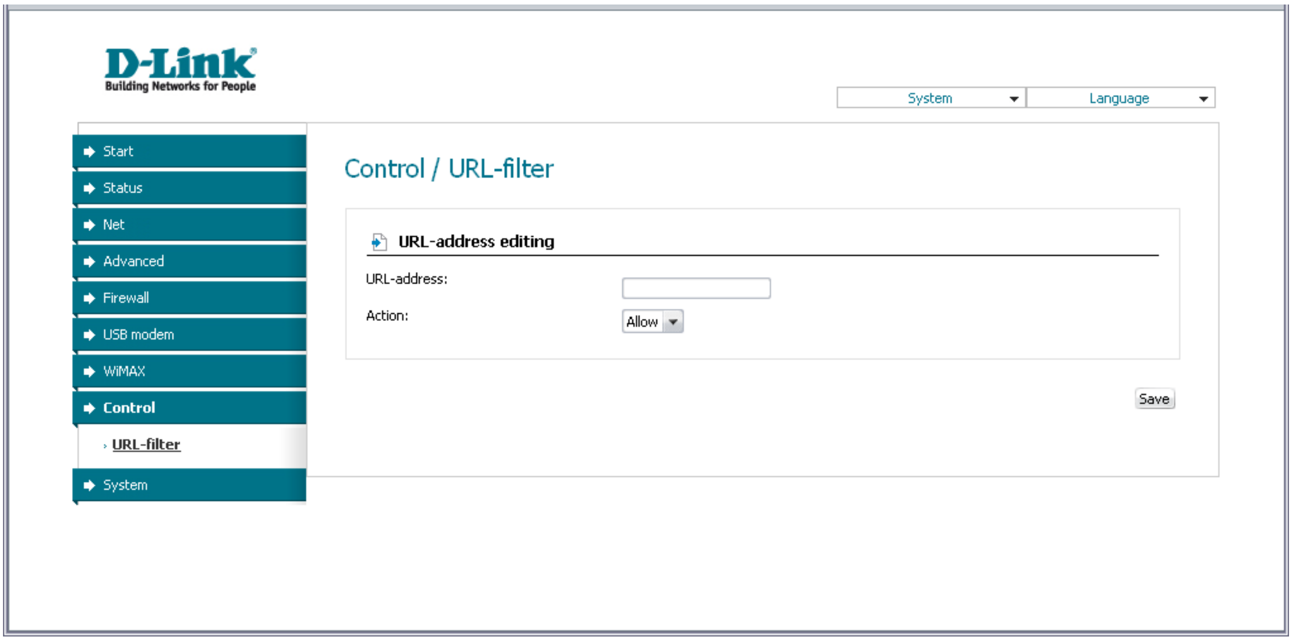


Figure 68. A page for adding a forbidden URL.

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.

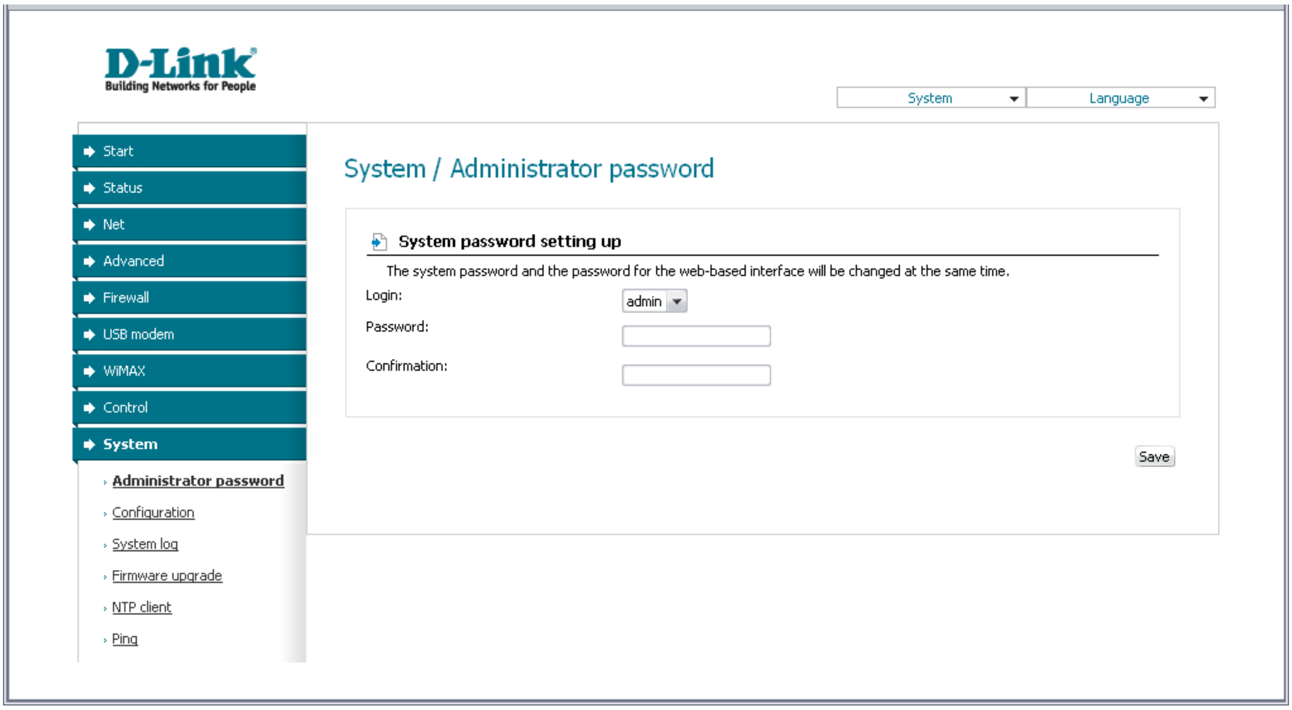
System

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 check availability of a host on the Internet through the web-based interface of the router.

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.

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



System / Administrator password

System password setting up

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

Login: admin

Password:

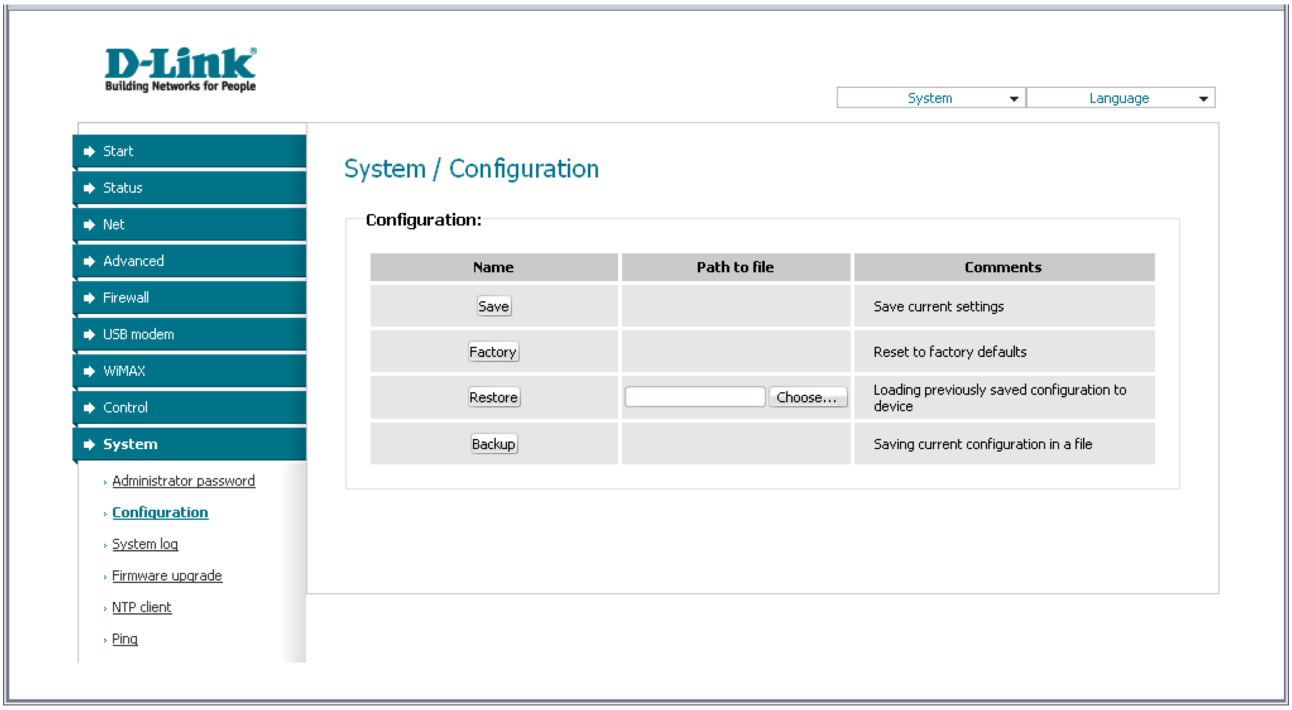
Confirmation:

Figure 69. The page for modifying the administrator password.

Enter the new password for access to the web-based interface of the router 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.



System / Configuration

Configuration:

Name	Path to file	Comments
Save		Save current settings
Factory		Reset to factory defaults
Restore		Loading previously saved configuration to device
Backup		Saving current configuration in a file

Figure 70. The ***System / Configuration*** *page.*

The following buttons are available on the page:

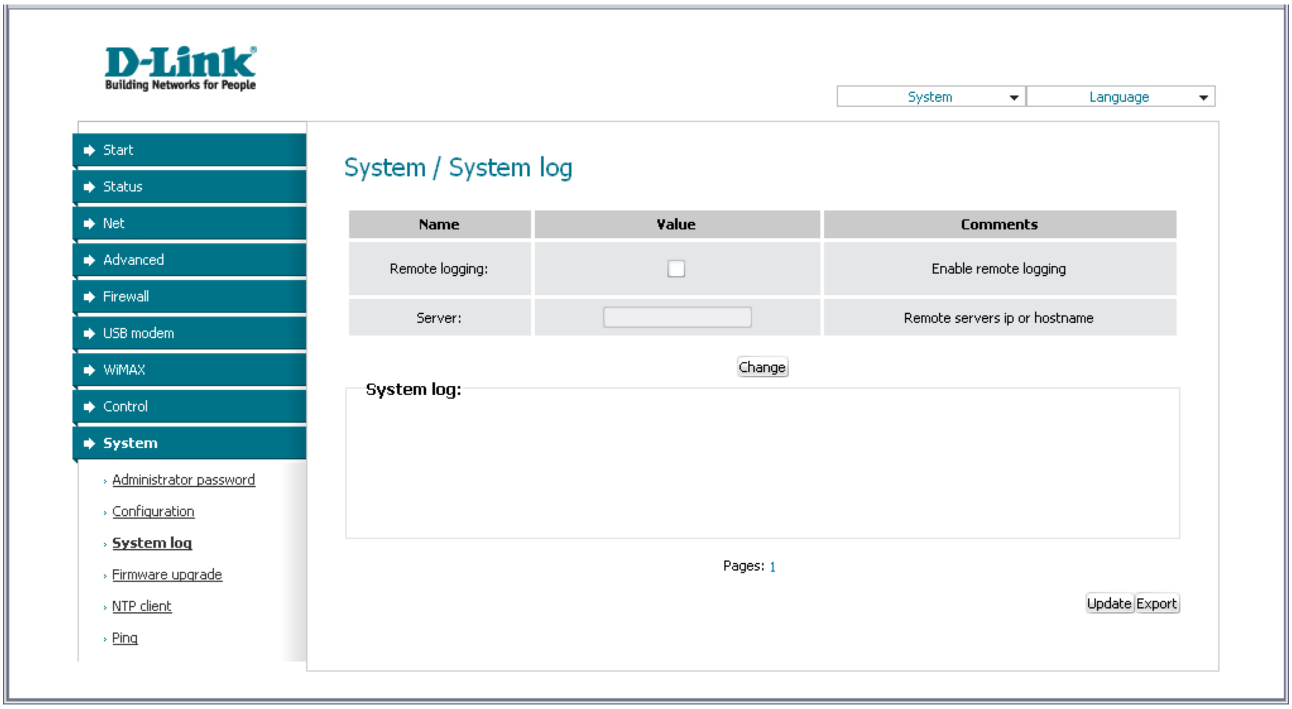
Control	Description
Save	Click the button to save settings to the non-volatile memory. Please, save settings every time you change the router's parameters. Otherwise the changes will be lost upon hardware reboot of the router.
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware Reset button (see the ***Saving and Restoring Settings*** section, page 20).
Restore	Click the button to upload a previously saved configuration (all settings of the router) from a file on your PC. Click the **Choose/Browse**[6] button to select a previously saved configuration file located on your PC.
Backup	Click the button and follow the dialog box appeared to save the configuration (all settings of the router) to your PC.

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

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.

System Log

On the **System / System log** page, you can view the list of system events and configure sending the system log to a remote host.



System / System log

Name	Value	Comments
Remote logging:	□	Enable remote logging
Server:		Remote servers ip or hostname

System log:

*Figure 71. The **System / System log** page.*

The **System log** section displays the results of the router load and operation and the time of the system events.

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

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

To send the system log to a remote host, follow the next steps:

1. Select the **Remote logging** checkbox.
2. In the **Server** field, enter the IP address or name of the remote server to which the router will send the system log.
3. Click the **Change** button.

The system log will be sent to UDP port 514 of the specified remote server via the syslog protocol.

Firmware Upgrade

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

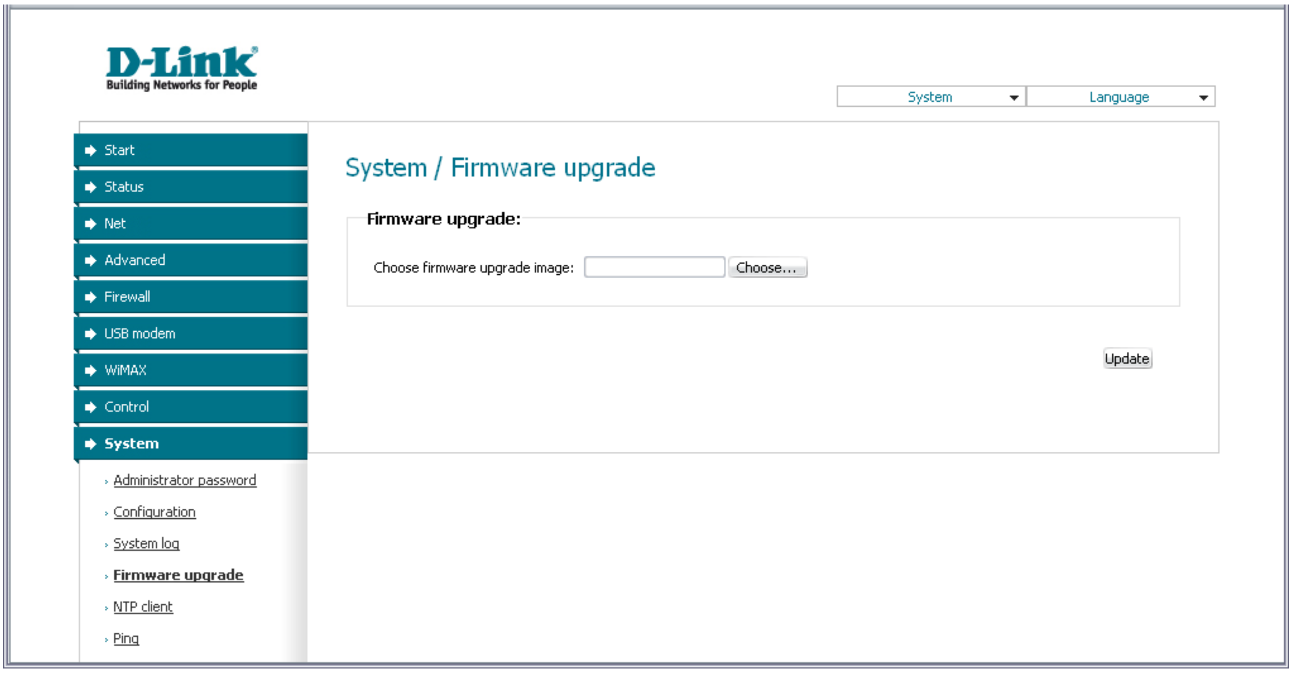


*Figure 72. The **System / Firmware upgrade** page.*

Follow the next steps to upgrade the firmware of your router:

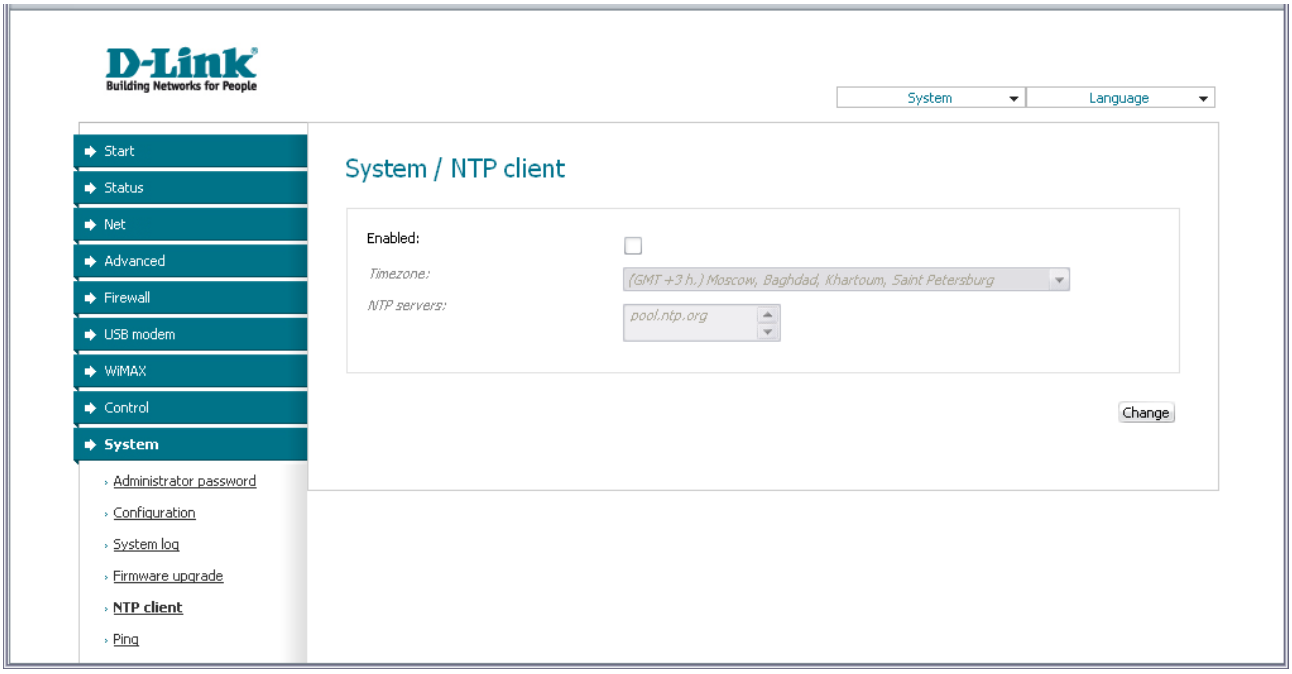
1. Download a new version of the firmware from www.dlink.ru.
2. Click the **Choose/Browse**[7] button on the **System / Firmware upgrade** page to locate the new firmware file.
3. Click the **Update** button to upgrade the firmware of the router.

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

[7] 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.



System / NTP client

Enabled: □

Timezone: (GMT +3 h.) Moscow, Baghdad, Khartoum, Saint Petersburg

NTP servers: pool.ntp.org

*Figure 73. The **System / NTP client** page.*

To enable automatic synchronization with a time server:

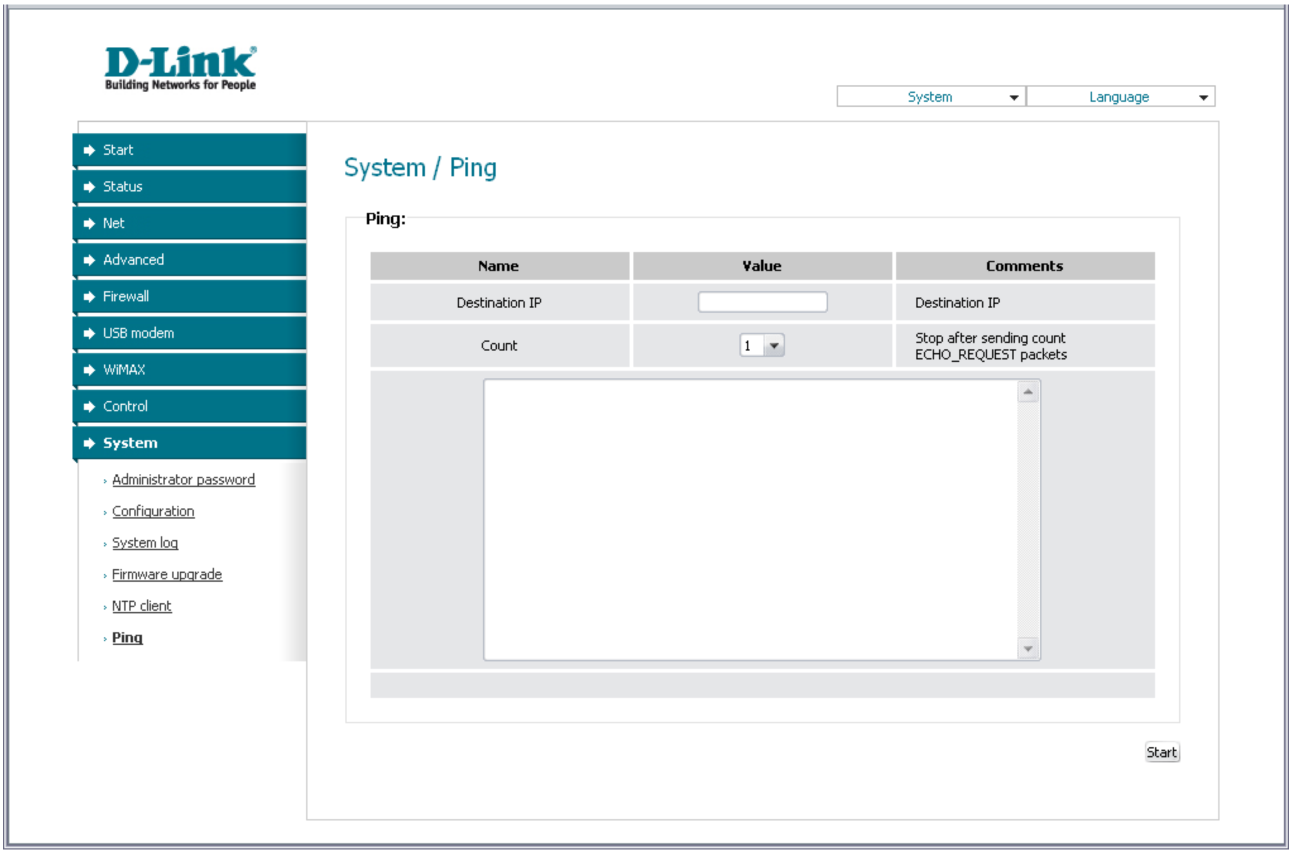
1. select the **Enabled** checkbox
2. select your time zone
3. specify the needed NTP server in the **Ntp servers** field or leave the server specified by default
4. click the **Change** button.

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.

Ping

On the **System / Ping** page, you can check availability of an IP address on the Internet via the Ping utility.

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



System / Ping

Ping:

Name	Value	Comments
Destination IP		Destination IP
Count	1	Stop after sending count ECHO_REQUEST packets

*Figure 74. The **System / Ping** page.*

To check availability of a host on the Internet, enter the IP address of this host in the **Destination IP** field, then select a number of echo requests that will be sent in order to check its availability from the **Count** drop-down list. Click the **Start** button. The check results will be displayed in the field located in the middle of the page.

CHAPTER 5. OPERATION GUIDELINES

Supported USB Modems

GSM modems:

- Huawei E150
- Huawei E1550
- Huawei E160G
- Huawei E169G
- Huawei E220
- ZTE MF626
- ZTE MF627.

CDMA modems:

- Anydata ADU-500A
- Celot CT-650.

WiMAX modem:

- Samsung SWC-U200.

Safety Instructions

Place your router on a flat horizontal surface in a location with sufficient ventilation. Do not mount the router on a wall.

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-620 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-620 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 in 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

3G	Third Generation
AC	Access Category
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BSSID	Basic Service Set Identifier
CCK	Complementary Code Keying
CDMA	Code Division Multiple Access
CINR	Carrier to Interference + Noise Ratio
CRC	Cyclic Redundancy Check
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DTIM	Delivery Traffic Indication Message
GMT	Greenwich Mean Time
GSM	Global System for Mobile Communications
HTMIX	High Throughput Mixed
IGMP	Internet Group Management Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPoE	Internet Protocol over Ethernet
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network

LCP	Link Control Protocol
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PBC	Push Button Configuration
PIN	Personal Identification Number
PPPoE	Point-to-point protocol over Ethernet
PPTP	Point-to-point tunneling protocol
PSK	Pre-shared key
PUK	PIN Unlock Key
QoS	Quality of Service
R-UIM	Removable User Identity Module
RADIUS	Remote Authentication in Dial-In User Service
RIP	Routing Information Protocol
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SIM	Subscriber Identification Module
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WDS	Wireless Distribution System

WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup