



DIR-620

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

Contents

| | |
|--|-----------|
| Chapter 1. Introduction..... | 5 |
| Contents and Audience..... | 5 |
| Conventions..... | 5 |
| Document Structure..... | 5 |
| Chapter 2. Overview..... | 6 |
| General Information..... | 6 |
| Specifications..... | 7 |
| Product Appearance..... | 10 |
| Front Panel and Right Side Panel..... | 10 |
| Back Panel..... | 11 |
| Delivery Package..... | 12 |
| Chapter 3. Installation and Connection..... | 13 |
| Before You Begin..... | 13 |
| Connecting to PC..... | 15 |
| PC with Ethernet Adapter..... | 15 |
| Obtaining IP Address Automatically in OS Windows XP..... | 15 |
| Obtaining IP Address Automatically in OS Windows 7..... | 18 |
| PC with Wi-Fi Adapter..... | 23 |
| Configuring Wi-Fi Adapter in OS Windows XP..... | 24 |
| Configuring Wi-Fi Adapter in OS Windows 7..... | 25 |
| Connecting to Web-based Interface..... | 27 |
| Saving and Restoring Settings..... | 31 |
| Chapter 4. Configuring via Web-based Interface..... | 33 |
| Setup Wizards..... | 33 |
| Internet Setup Wizard..... | 33 |
| PPPoE Connection..... | 35 |
| Static IP Connection..... | 39 |
| Dynamic IP Connection..... | 42 |
| PPTP + Static IP or L2TP + Static IP Connection..... | 44 |
| PPTP + Dynamic IP or L2TP + Dynamic IP Connection..... | 50 |
| 3G Connection..... | 55 |
| Site Setup Wizard..... | 58 |
| Wi-Fi Setup Wizard..... | 59 |
| IPTV Setup Wizard..... | 65 |
| Status..... | 66 |
| Network Statistics..... | 66 |
| DHCP..... | 67 |
| Routing Table..... | 68 |
| LAN Clients..... | 69 |

| | |
|---|------------|
| Net | 70 |
| WAN..... | 70 |
| <i>Creating 3G WAN Connection</i> | 71 |
| <i>Creating PPPoE WAN Connection</i> | 74 |
| <i>Creating Static IP WAN Connection</i> | 78 |
| <i>Creating Dynamic IP WAN Connection</i> | 81 |
| <i>Creating PPTP + Static IP or L2TP + Static IP WAN Connection</i> | 84 |
| <i>Creating PPTP + Dynamic IP or L2TP + Dynamic IP WAN Connection</i> | 89 |
| LAN..... | 93 |
| Wi-Fi | 95 |
| Common settings..... | 95 |
| Basic Settings..... | 96 |
| Security Settings..... | 97 |
| MAC Filter..... | 102 |
| Station List..... | 104 |
| WPS..... | 105 |
| <i>Using WPS Function via Web-based Interface</i> | 107 |
| <i>Using WPS Function without Web-based Interface</i> | 107 |
| Additional Settings..... | 109 |
| WMM..... | 111 |
| Client..... | 113 |
| Advanced | 116 |
| VLAN..... | 116 |
| UPnP..... | 119 |
| DDNS..... | 120 |
| DNS..... | 122 |
| Routing..... | 123 |
| Remote Access..... | 125 |
| IGMP..... | 126 |
| Firewall | 127 |
| IP Filters..... | 127 |
| Virtual Servers..... | 130 |
| DMZ..... | 132 |
| MAC Filter..... | 133 |
| USB Modem | 134 |
| Information..... | 134 |
| PIN..... | 135 |
| WiMAX | 137 |
| Information..... | 137 |
| USB Storage | 139 |
| Information..... | 139 |
| Filebrowser..... | 140 |
| FTP..... | 141 |
| Users..... | 142 |

| | |
|--|------------|
| Torrent | 143 |
| Torrent-client..... | 143 |
| Settings..... | 144 |
| Control | 146 |
| URL Filter..... | 146 |
| System | 148 |
| Administrator Password..... | 148 |
| Configuration..... | 149 |
| System Log..... | 150 |
| Firmware Upgrade..... | 152 |
| NTP Client..... | 153 |
| Ping..... | 154 |
| Telnet..... | 155 |
| Chapter 5. Operation Guidelines | 156 |
| Supported USB Modems..... | 156 |
| Safety Instructions..... | 157 |
| Wireless Installation Considerations..... | 157 |
| Connecting to Cable or DSL Modem..... | 158 |
| Chapter 6. Abbreviations and Acronyms | 159 |


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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the router DIR-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 modem¹, which can be used to establish connection to the Internet. In addition, to the USB port of the router you can connect a USB storage device, which will be used as a network drive.

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 can operate as a base station for connecting wireless devices of the standards 802.11b, 802.11g, and 802.11n (at the rate up to 300Mbps).

The router supports multiple functions for the wireless interface: several security standards (WEP, WPA/WPA2), MAC address filtering, 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 several languages).

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 156.

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 or USB storage.

Network Functions:

- WAN connection types:
 - 3G
 - PPPoE
 - Static IP
 - Dynamic IP
 - PPTP/L2TP + Static IP
 - PPTP/L2TP + Dynamic IP
- DHCP server and client
- DNS relay
- VPN pass-through (PPTP/L2TP)
- Dynamic DNS
- Static IP routing
- Remote management
- Network statistics for each interface
- IGMP Proxy
- RIP
- UPnP
- Support of VLAN.

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

USB Modem²:

- Auto connection to available type of supported network (3G/2G)
- Enabling/disabling PIN code check, changing PIN code.

USB Storage:

- Built-in FTP server
- Access to storage via accounts
- Access control (for ext2/3 file systems).

Wireless Connection:

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

Torrent Client:

- Uploading/downloading files from/to USB storage.

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 GSM USB modems only.

Configuration and Management:

- Multilingual web-based interface for configuration and management
- Access via TELNET
- Firmware update via web-based interface
- Saving/restoring configuration to/from file
- Support of remote logging
- Automatic synchronization of system time with NTP server
- 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 °C (from 32 to 104 °F).

Storage Temperature:

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

Operating Humidity:

- from 10% to 90% non-condensing.

Storage Humidity:

- from 5% to 95% non-condensing.

Product Appearance

Front Panel and Right Side Panel



Figure 1. Front panel view.

| LED | Mode | Description |
|-----------------|-----------------------|--|
| Power | <i>Solid green</i> | The router is powered on. |
| | <i>No light</i> | The router is powered off. |
| | <i>Solid yellow</i> | When powered on: the router is being loaded; when loaded: a malfunction of the router. |
| Internet | <i>Solid green</i> | The Internet connection is on. |
| | <i>Blinking green</i> | The WAN interface is active (upstream or downstream traffic). |
| | <i>Solid yellow</i> | The Internet connection is off. |
| WLAN | <i>Solid green</i> | The router's WLAN is on. |
| | <i>Blinking green</i> | The WLAN interface is active (upstream or downstream traffic). |
| LAN 1-4 | <i>Solid green</i> | A device (computer) is connected to the relevant port, the connection is on. |
| | <i>Blinking green</i> | The LAN port is active (upstream or downstream traffic). |

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 |
|----------------------|--|
| <i>Blinking blue</i> | Attempting to add a wireless device via the WPS function. |
| <i>Solid blue</i> | The wireless device is connected to the router's WLAN (lights for several minutes). |
| <i>Solid yellow</i> | 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 Internet³.

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.

For CDMA USB modems, it is required 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

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 port⁴ 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 in OS Windows XP

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

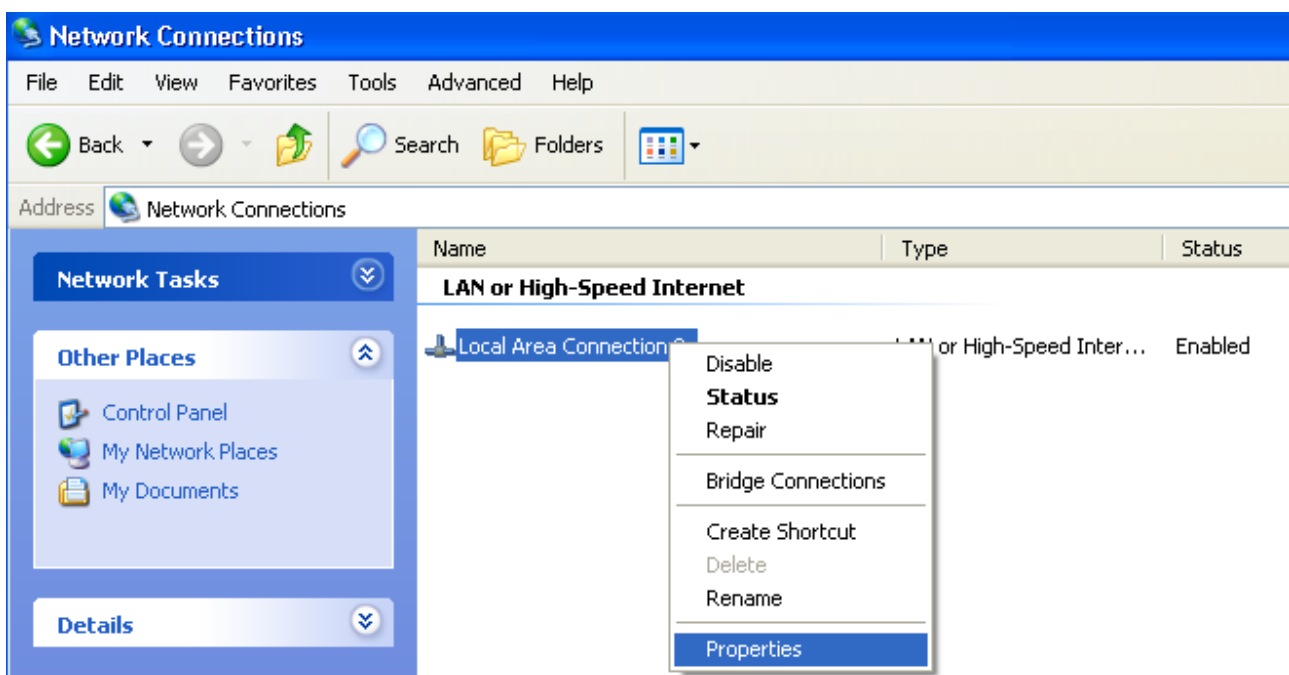


Figure 3. The **Network Connections** window.

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

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

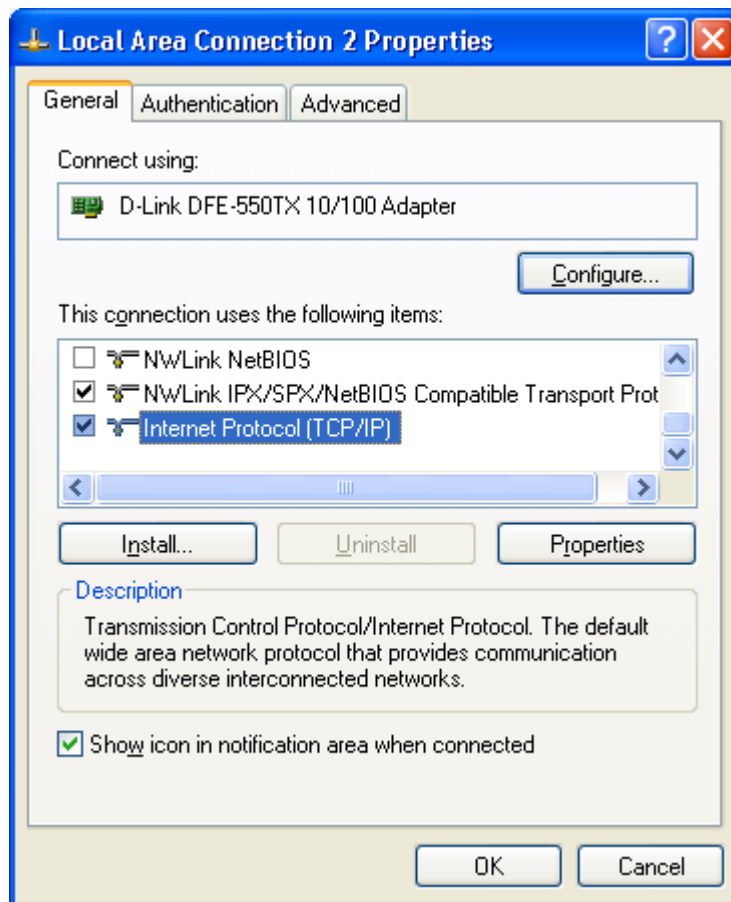


Figure 4. The **Local Area Connection Properties** window.

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

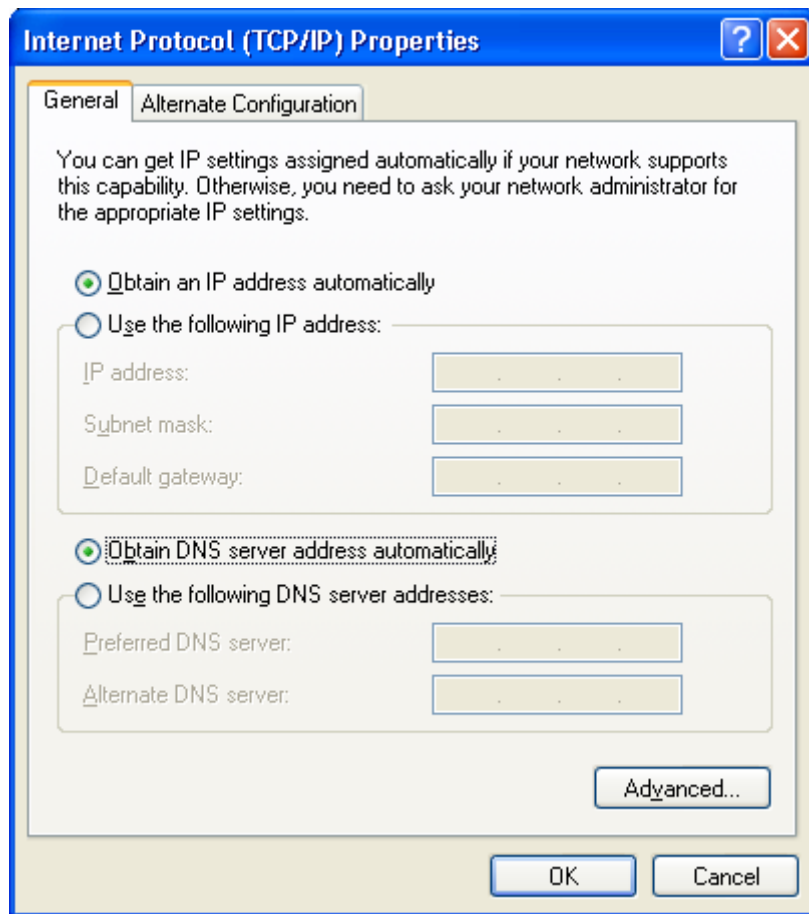


Figure 5. The **Internet Protocol (TCP/IP) Properties** window.

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

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

Obtaining IP Address Automatically in OS Windows 7

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

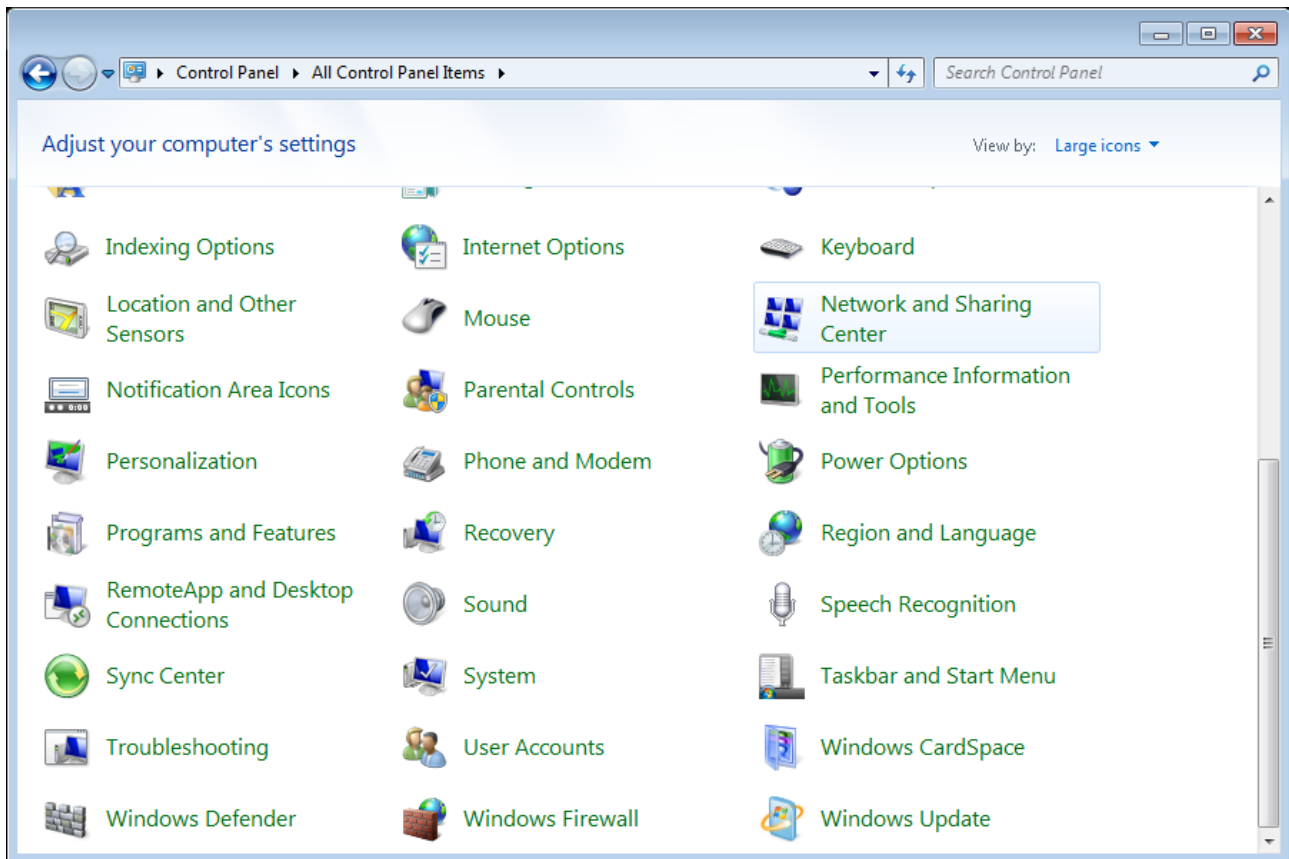


Figure 6. The **Control Panel** window.

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

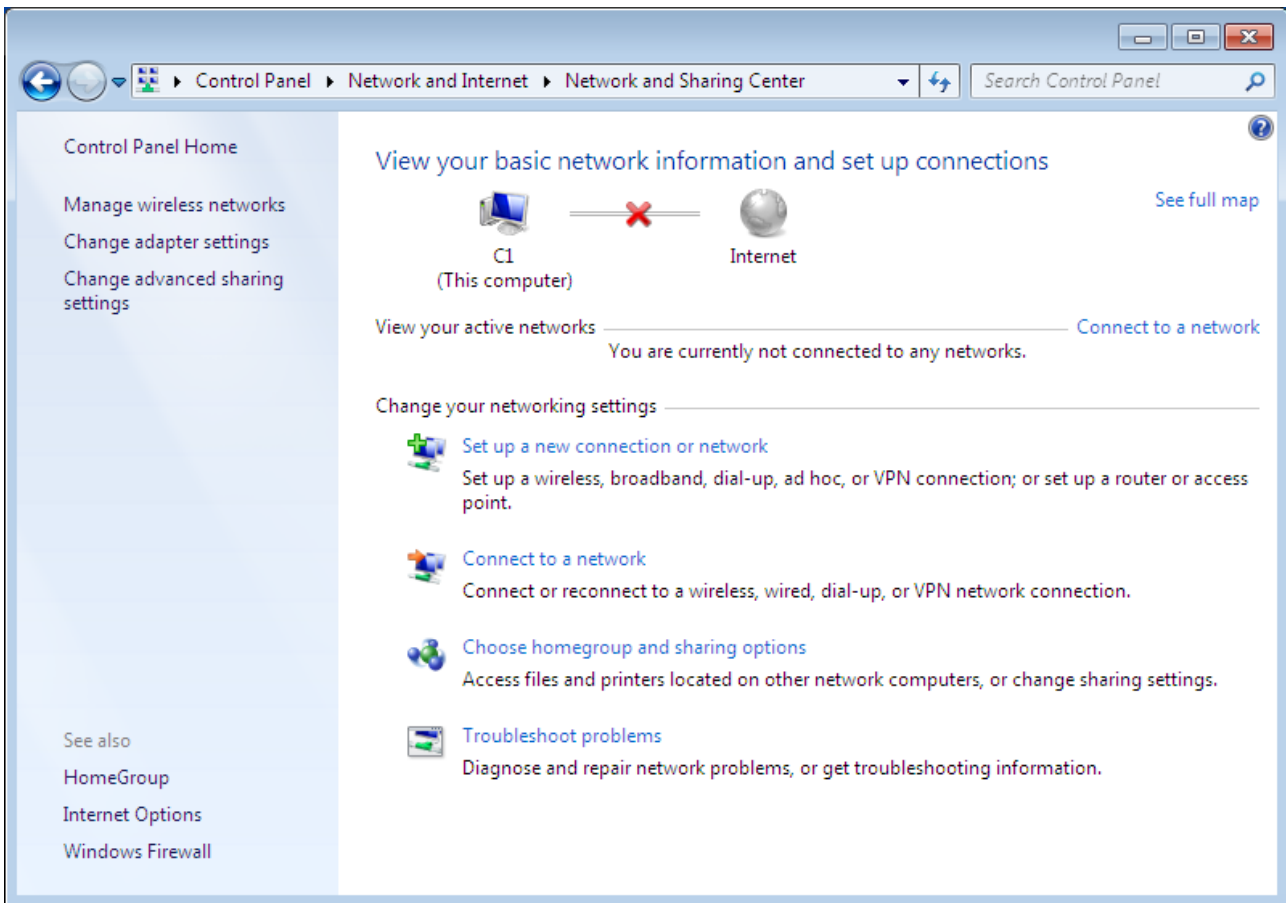


Figure 7. The **Network and Sharing Center** window.

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

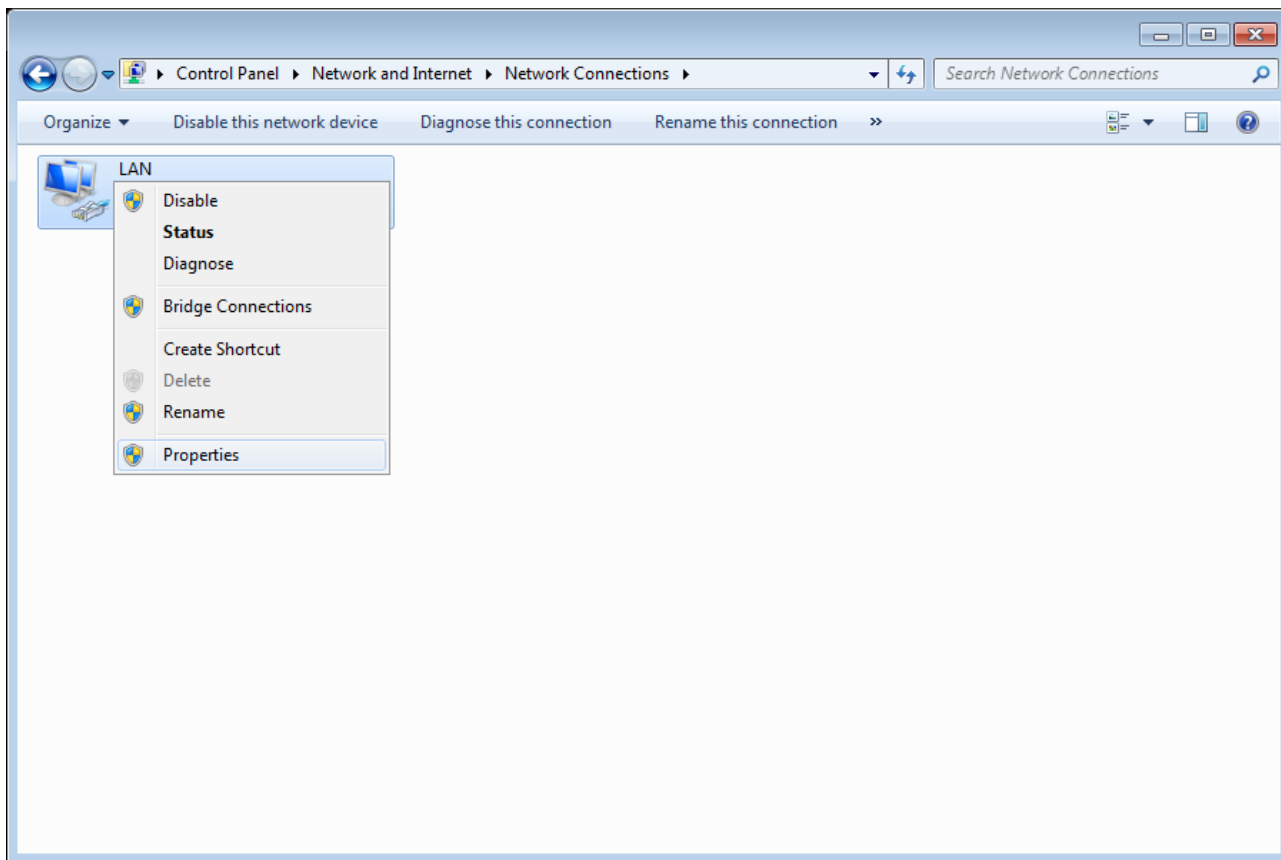


Figure 8. The **Network Connections** window.

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

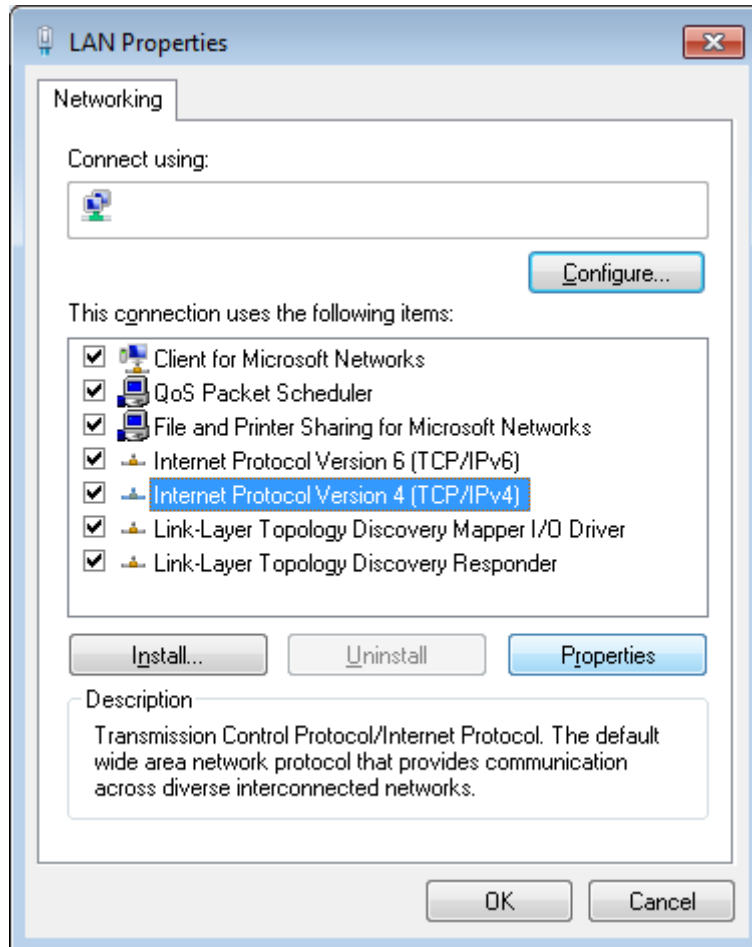


Figure 9. The **Local Area Connection Properties** window.

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

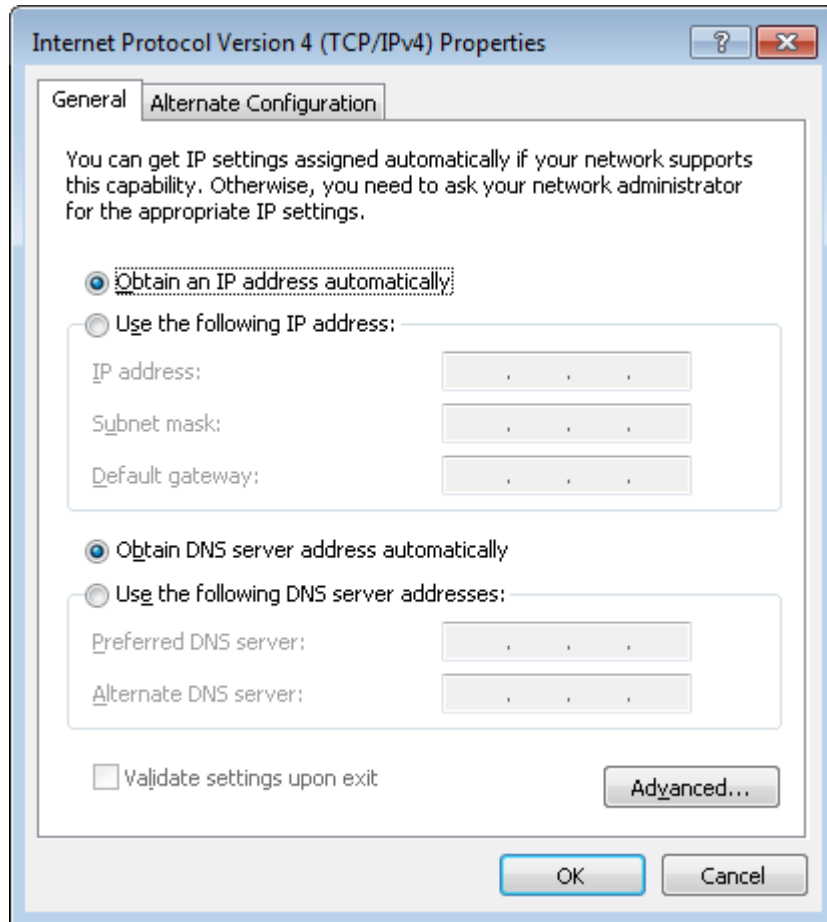


Figure 10. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

Now 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 port⁵ 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.

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

Configuring Wi-Fi Adapter in OS Windows XP

1. Click the **Start** button and proceed to the **Control Panel > Network and Internet Connections > Network Connections** window.
2. Select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.

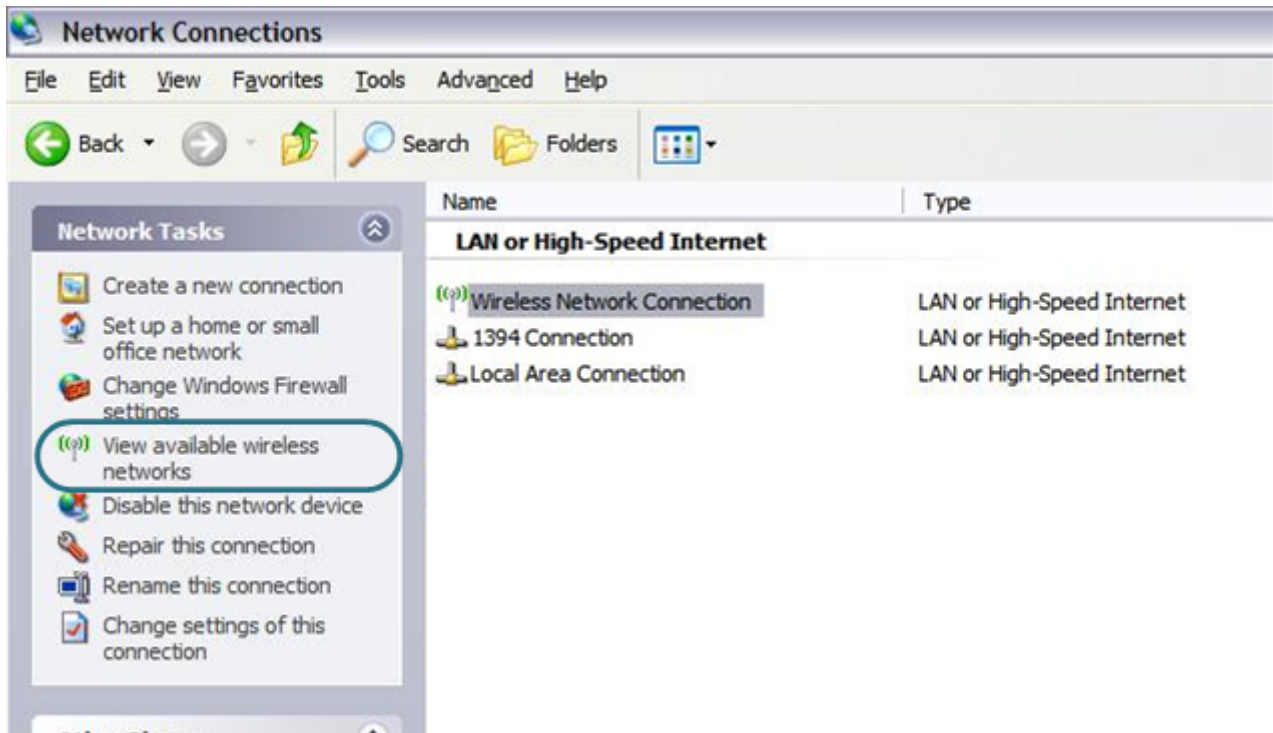


Figure 11. The **Network Connections** window.

3. Search for available wireless networks.
4. In the opened **Wireless Network Connection** window, select the wireless network **DIR-620** and click the **Connect** button.

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

! If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings of the router you will need to reconfigure the wireless connection using the newly specified settings.

Configuring Wi-Fi Adapter in OS Windows 7

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

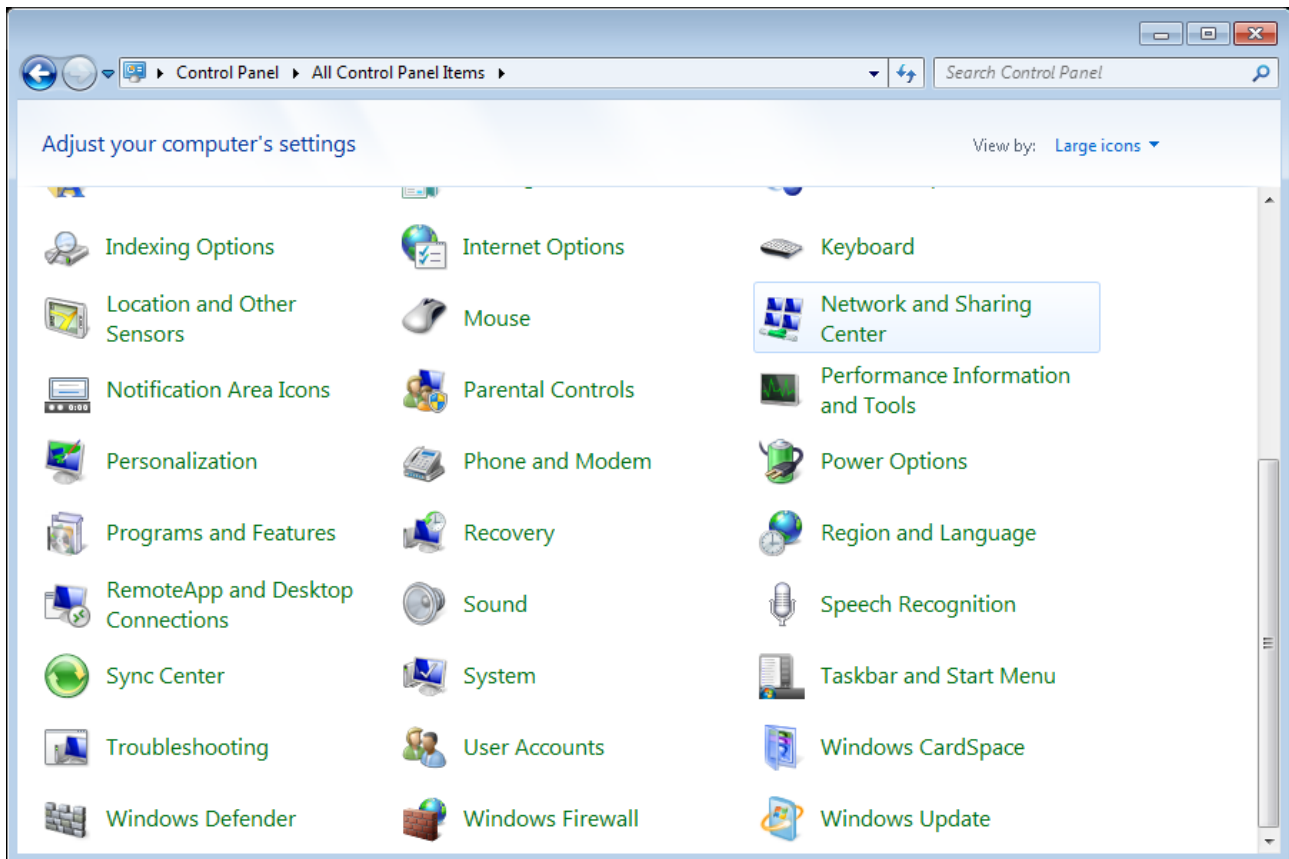


Figure 12. The **Control Panel** window.

3. In the menu located on the left part of the window, select the **Change adapter settings** line.
4. In the opened window, select the icon of the wireless network connection and make sure that your Wi-Fi adapter is on.
5. To open the list of available wireless networks, select the icon of the wireless network connection and click the **Connect To** button or left-click the network icon in the notification area located on the right side of the taskbar.

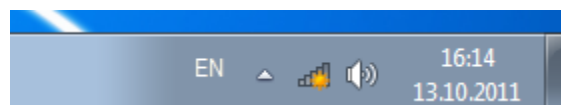


Figure 13. The notification area of the taskbar.

6. In the opened window, in the list of available wireless networks, select the wireless network **DIR-620** and click the **Connect** button.

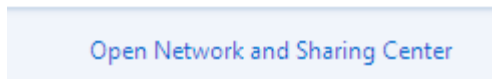
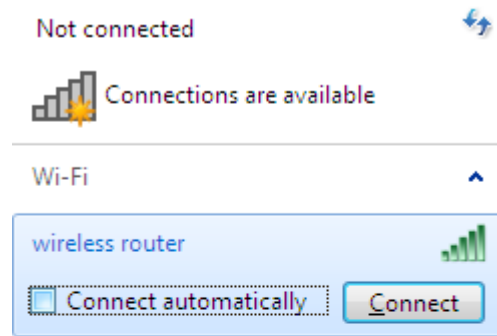


Figure 14. The list of available networks.

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

! If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings of the router 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 13).
2. In the address bar of the web browser, enter the IP address of the router (by default, the following IP address is specified: **192.168.0.1**). Press the **Enter** key.



Figure 15. 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** link.



Figure 16. The login page.



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

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

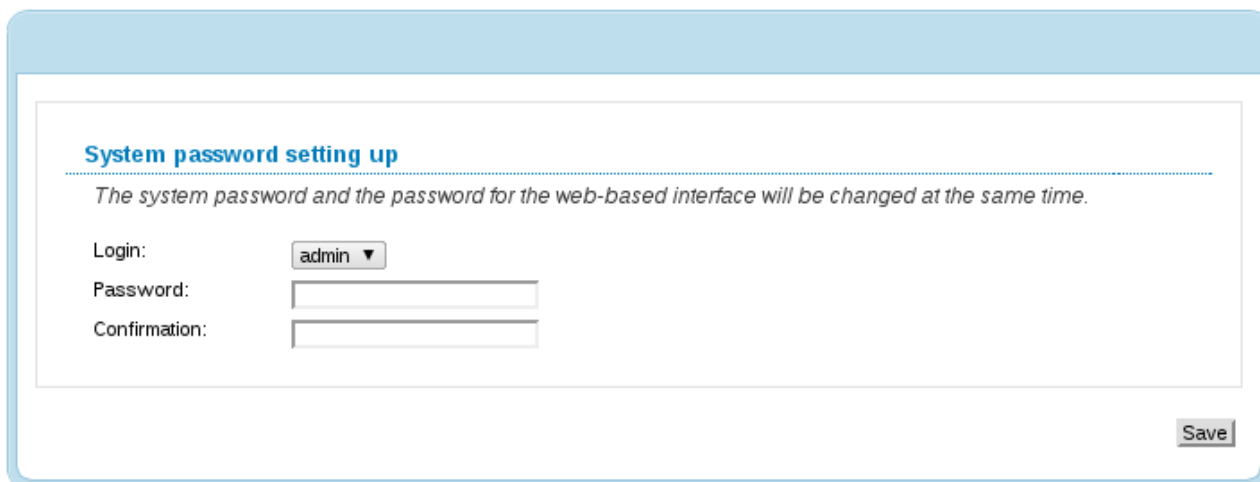


Figure 17. The page for changing the default administrator password.

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

! Remember or write down the new password for the administrator account. In case of losing the new password, you can access the settings of the 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 router's quick settings page opens.

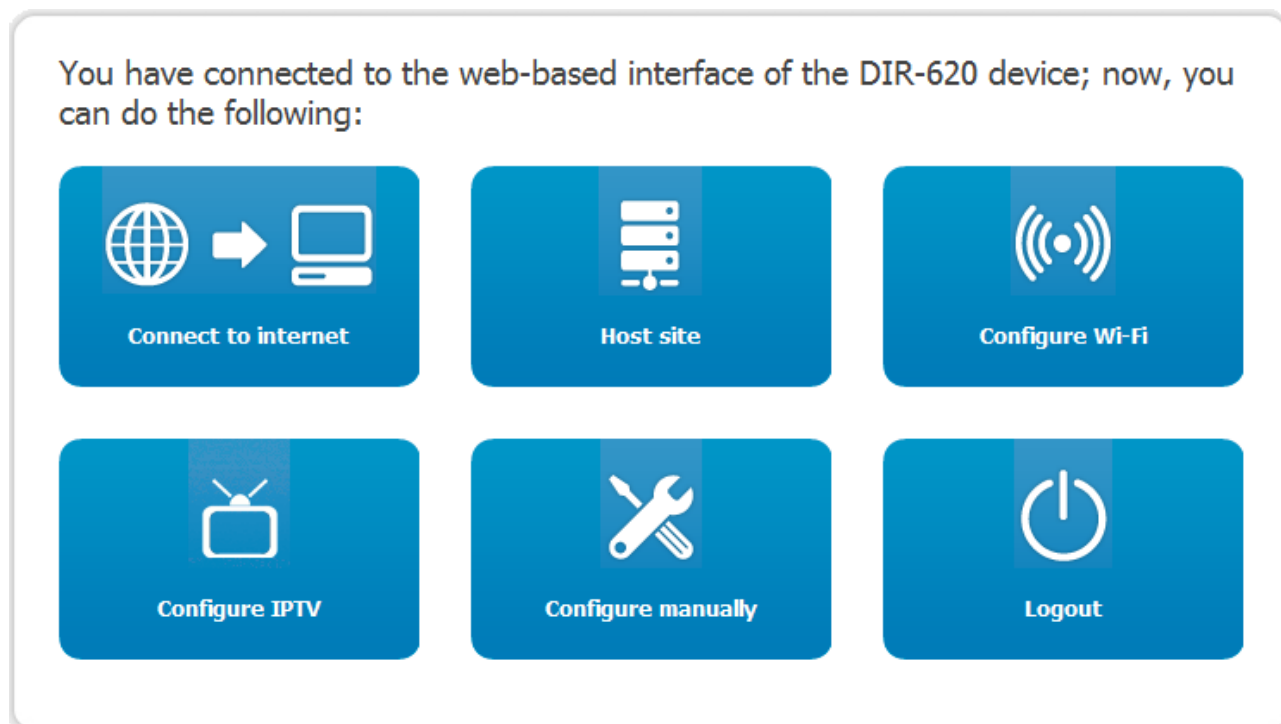


Figure 18. The quick settings page.

To configure connection to the Internet, click the **Connect to internet** button. After clicking the button, the Internet Setup Wizard opens (see the *Internet Setup Wizard* section, page 33).

To configure access from the Internet to a web server located in your LAN, click the **Host site** button. After clicking the button, the Site Setup Wizard opens (see the *Site Setup Wizard* section, page 58).

To configure the router's wireless network, click the **Configure Wi-Fi** button. After clicking the button, the Wi-Fi Setup Wizard opens (see the *Wi-Fi Setup Wizard* section, page 59).

To configure the router to use an IPTV set-top box, click the **Configure IPTV** button. After clicking the button, the IPTV Setup Wizard opens (see the *IPTV Setup Wizard* section, page 65).

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

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

After clicking the button the system statistics page opens. The page displays general information on the router and its software (the version and the date of the firmware, the IP address of the device, the name of the WLAN, etc.).



Figure 19. The system statistics page.

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

To upgrade the firmware of the router, left-click the current firmware version (the right column of the **Firmware version** line). After clicking the line, the **System / Firmware upgrade** page opens (see the *Firmware Upgrade* section, page 152).

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

To edit the router's local interface parameters, left-click the IP or MAC address of the local interface (the right column of the **LAN IP** line or **LAN MAC** line correspondingly). After clicking the line, the page for editing the LAN interface opens (see the *LAN* section, page 93).

To configure the router's WLAN parameters, left-click the SSID of the WLAN (the right column of the **SSID** line). After clicking the line, the **Wi-Fi / Basic settings** page opens (see the *Basic Settings* section, page 96).

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

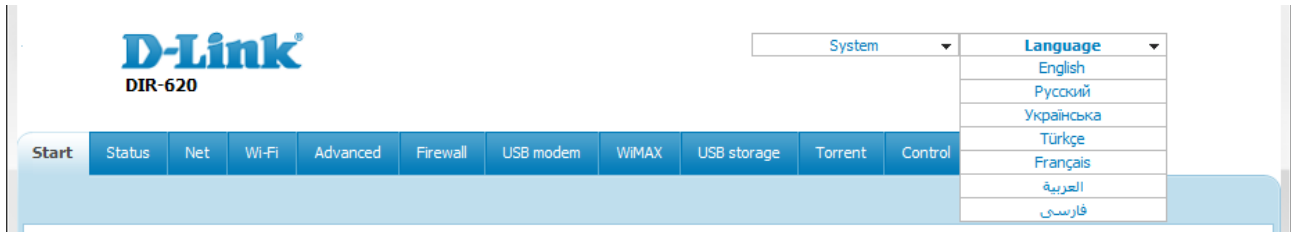


Figure 20. Changing the language of the web-based interface.

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

Saving and Restoring Settings

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

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

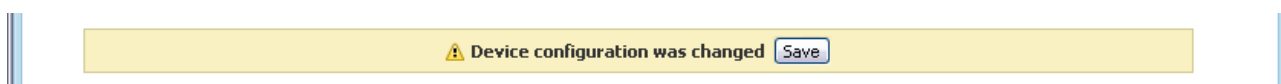


Figure 21. The notification on unsaved changes.

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

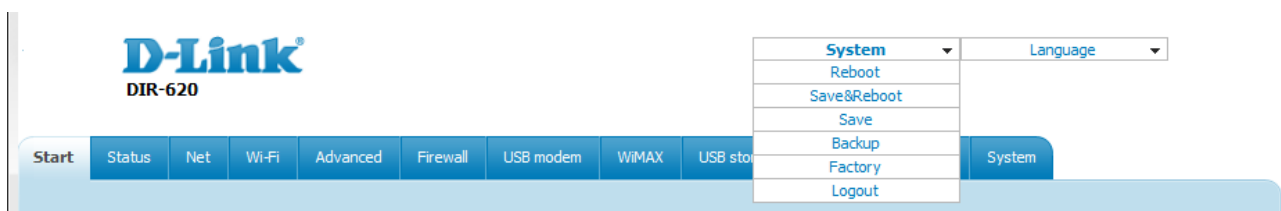


Figure 22. The top-page menu.

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 button is located on the back panel of the router next to the power connector.

To restore the factory default settings, insert a small paperclip into the hole of the button (with the router **powered on**), push, and hold for 10 seconds. Then remove the paperclip. All LEDs of the router should turn off and then turn on again.

Wait for about 30 seconds. Now you can access the web-based interface of the router using the default IP address, username and password.

If you fail to restore the factory defaults via the method described above, use the emergency reset method.

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



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

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

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Setup Wizards

Internet Setup Wizard

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

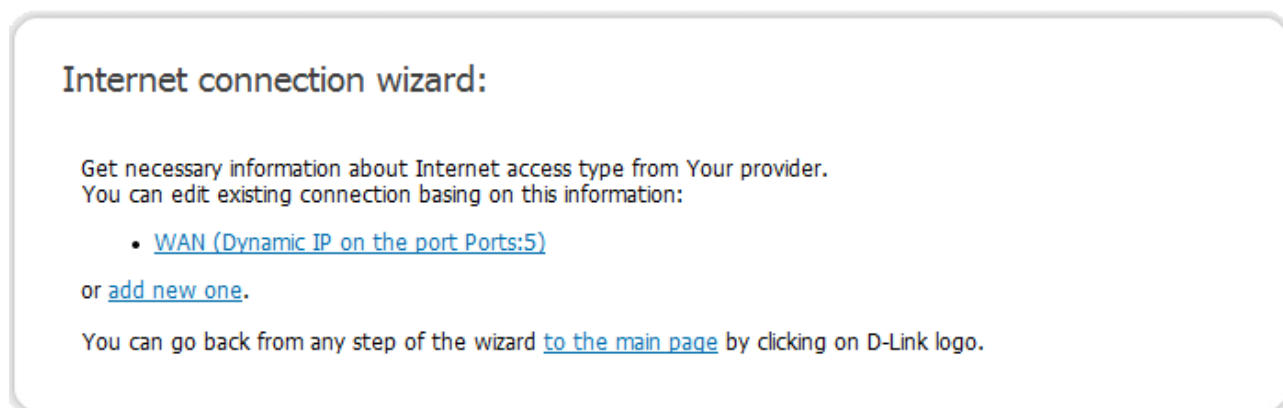


Figure 23. Configuring connection to the Internet.

By default, the **WAN** connection is configured in the system. To edit this connection, click the **WAN** link and change the relevant parameters (see the *Dynamic IP Connection* section, page 42).

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

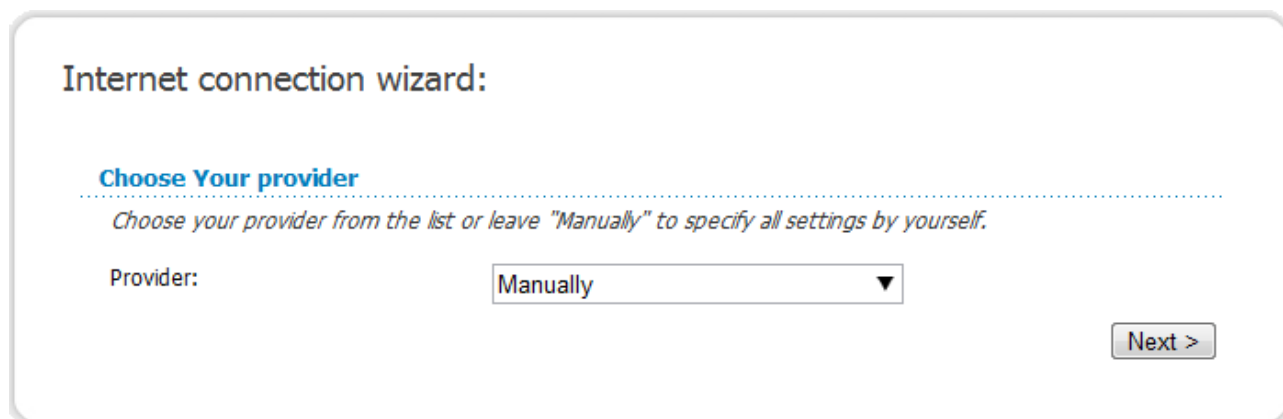


Figure 24. The page for selecting a 3G network operator.

On the opened page, from the **Provider** drop-down list, select your country and operator if you are going to configure a 3G network connection, or leave the **Manually** value, if you are going to configure a wired or WiMAX WAN connection or you want to specify all settings for your 3G WAN connection independently.

Click the **Next** button to continue.

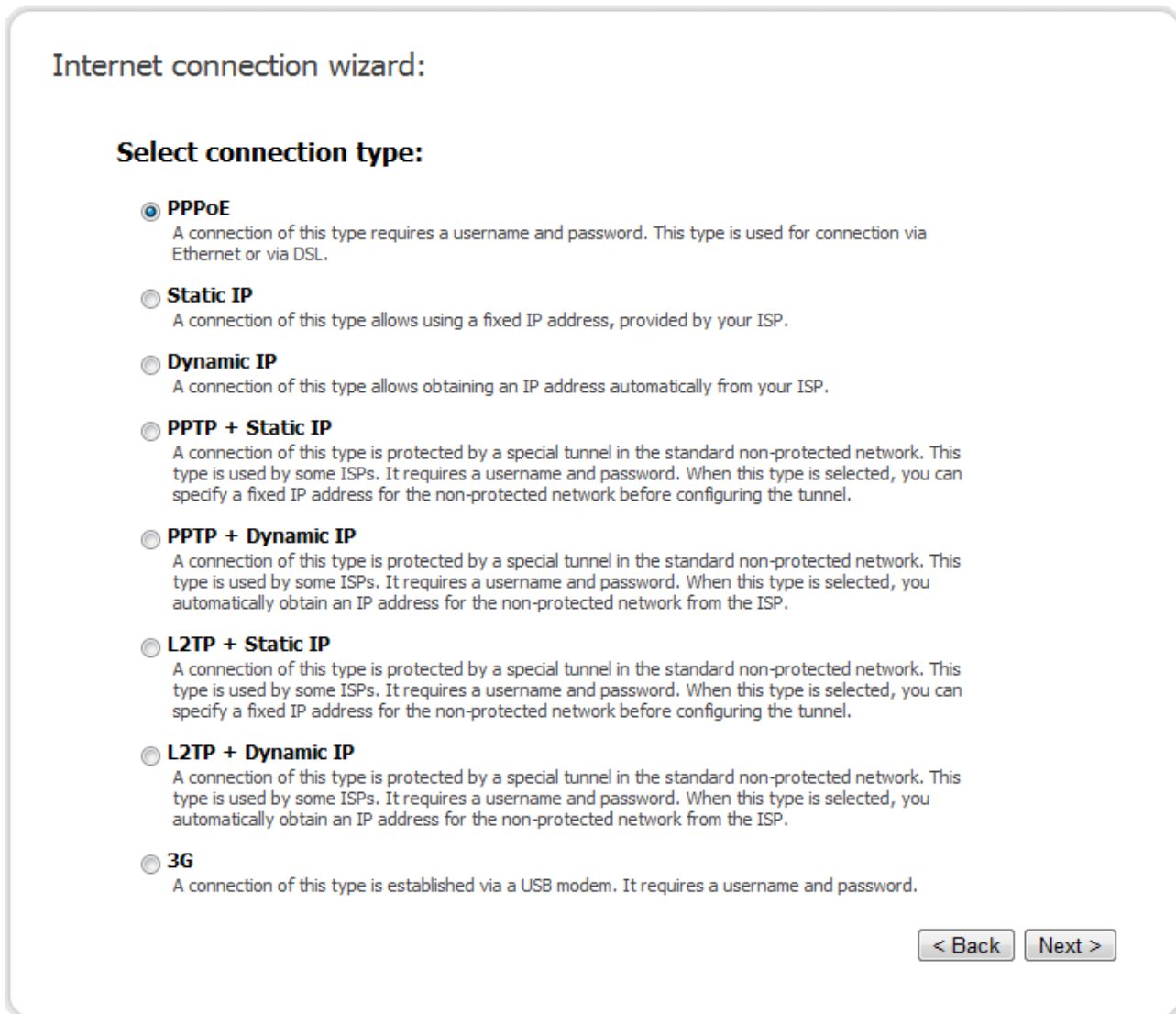



Figure 25. The page for selecting the connection type.

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

To create a WiMAX WAN connection, on the opened page, select the **USB-WiMAX** choice and click the **Next** button (the page is displayed only when a WiMAX USB modem is connected to the router).

PPPoE Connection



Internet connection wizard:

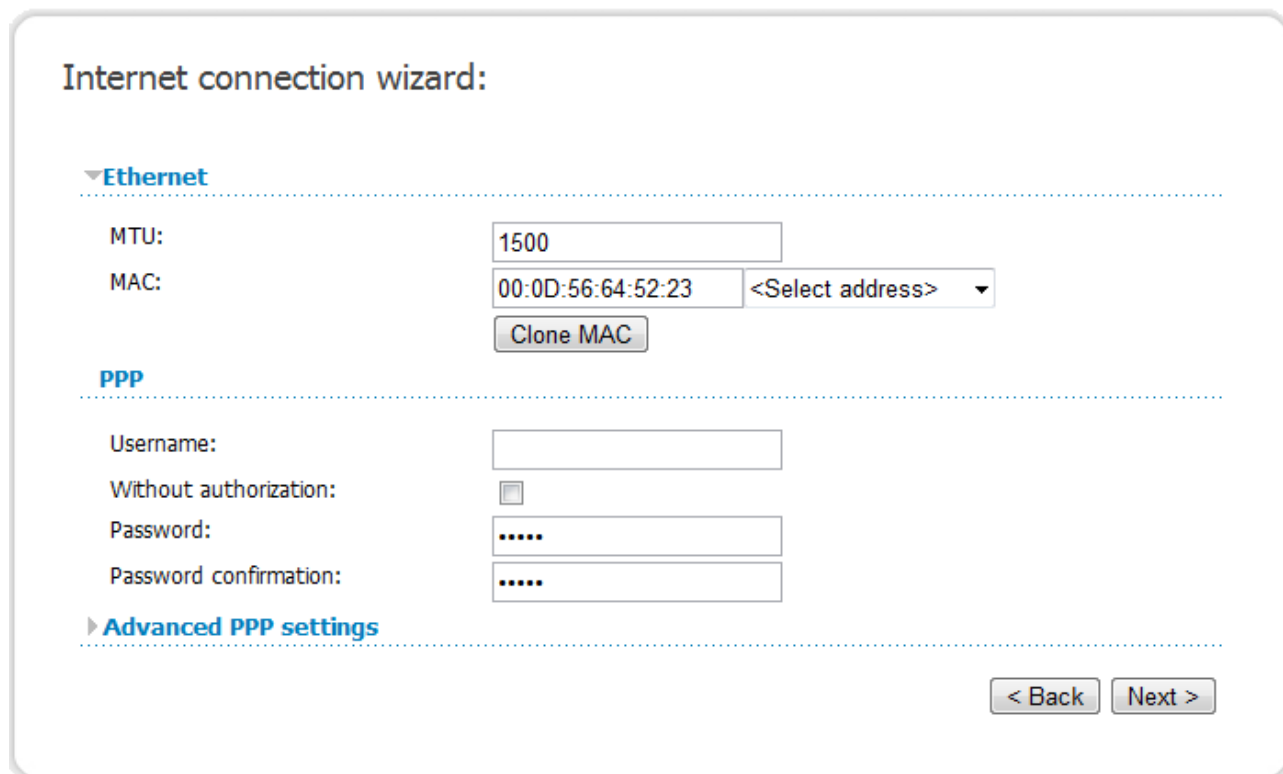
Connection name

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

Name:

Figure 26. Configuring PPPoE WAN connection.

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



Internet connection wizard:

Ethernet

MTU:

MAC:

PPP

Username:

Without authorization:

Password:

Password confirmation:

Advanced PPP settings

Figure 27. Configuring PPPoE WAN connection.

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

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

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

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

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

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

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

Internet connection wizard:

▶ **Ethernet**

PPP

Username:

Without authorization:

Password:

Password confirmation:

▼ **Advanced PPP settings**

Service name:

Authentication algorithm:

MTU:

Keep Alive:

LCP interval (sec):

LCP fails:

Dial on demand:

PPP IP extension:

Use Static IP Address:

PPP debug:

PPPoE pass through:

Figure 28. Configuring PPPoE WAN connection.

| Parameter | Description |
|---------------------------------|---|
| Service name | The name of the PPPoE authentication server. |
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. |

| Parameter | Description |
|------------------------------|--|
| Keep Alive | Select the checkbox if you want the 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. |
| 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. |
| PPP IP extension | This option is used by some ISPs. Contact your ISP to clarify if this checkbox needs to be enabled. |
| Use Static IP Address | Select the checkbox if you want to use a static IP address to access the Internet. In the Static 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. |

Click the **Next** button to continue.

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

Internet connection wizard:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

< Back Next >

Figure 29. Configuring PPPoE WAN connection.

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

Click the **Next** button to continue.

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

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

Static IP Connection

Internet connection wizard:

Connection name

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

Name:

Figure 30. Configuring Static IP WAN connection.

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

Internet connection wizard:

▼ **Ethernet**

MTU:

MAC:

IP

IP Address:

Netmask:

Gateway IP address:

Primary DNS server:

Secondary DNS server:

▶ **Advanced IP settings**

Figure 31. Configuring Static IP WAN connection.

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

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

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

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

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

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

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

Click the **Next** button to continue.

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

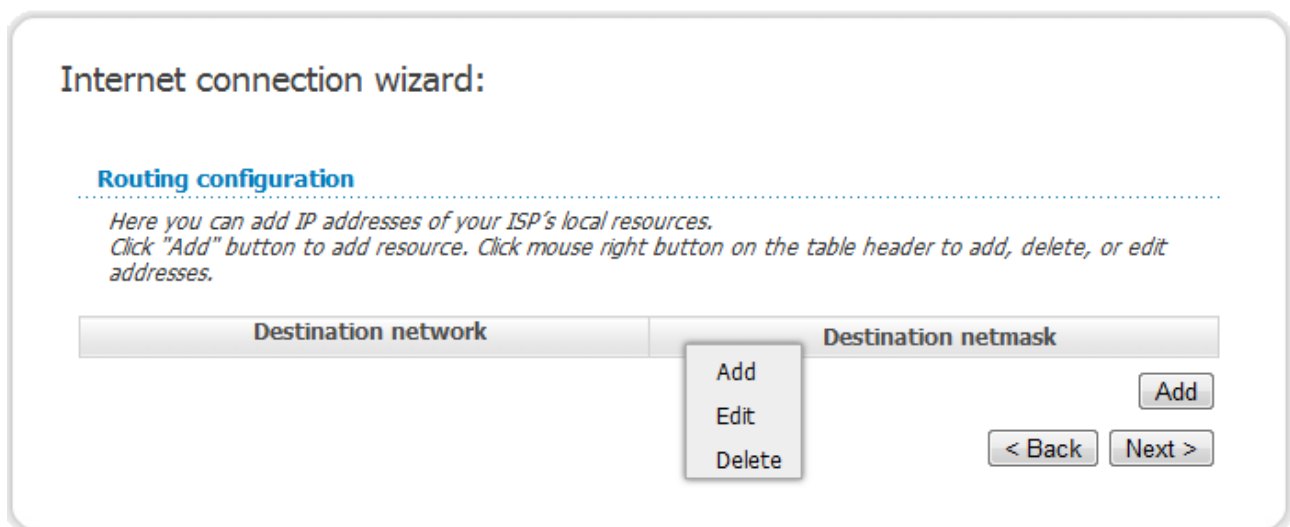


Figure 32. Configuring Static IP WAN connection.

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

Click the **Next** button to continue.

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

Internet connection wizard:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

< Back Next >

Figure 33. Configuring Static IP WAN connection.

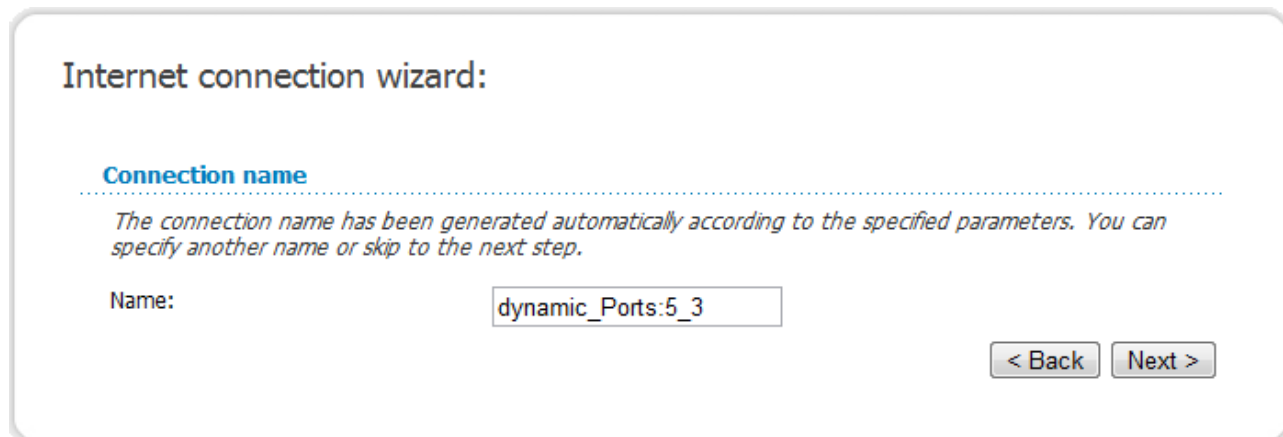
| Parameter | Description |
|------------------------------|---|
| Enable RIP | Select the checkbox to allow using RIP for this connection. |
| Enable IGMP Multicast | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |
| NAT | Select the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

Click the **Next** button to continue.

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

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

Dynamic IP Connection



Internet connection wizard:

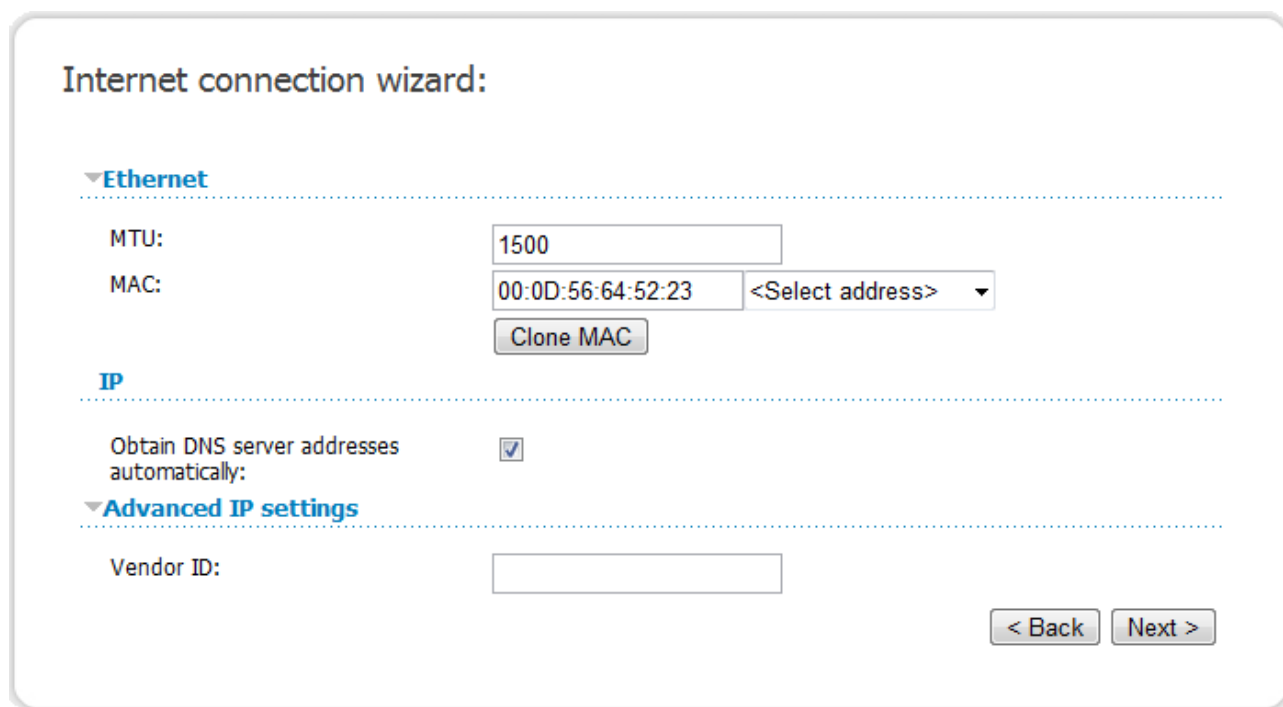
Connection name

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

Name:

Figure 34. Configuring Dynamic IP WAN connection.

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



Internet connection wizard:

Ethernet

MTU:

MAC:

IP

Obtain DNS server addresses automatically:

Advanced IP settings

Vendor ID:

Figure 35. Configuring Dynamic IP WAN connection.

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

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

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

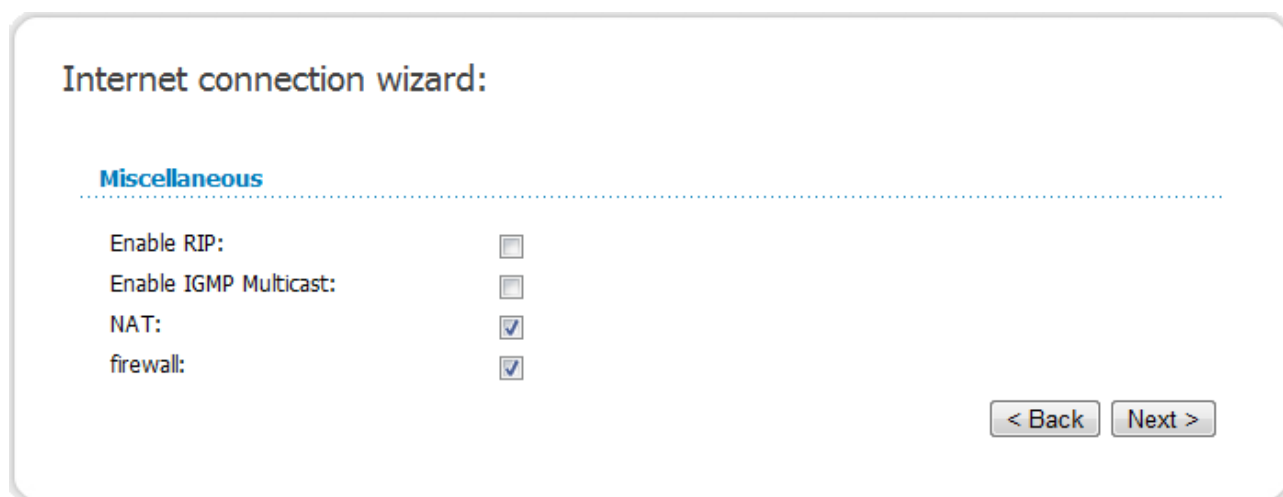
Also you can set the address of a device connected to the router's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).

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

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

Click the **Next** button to continue.

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



The screenshot shows a web interface titled "Internet connection wizard:". Below the title, the "Miscellaneous" section is highlighted with a blue header and a dotted line. It contains four settings, each with a checkbox: "Enable RIP:" (unchecked), "Enable IGMP Multicast:" (unchecked), "NAT:" (checked), and "firewall:" (checked). At the bottom right of the section, there are two buttons: "< Back" and "Next >".

Figure 36. Configuring Dynamic IP WAN connection.

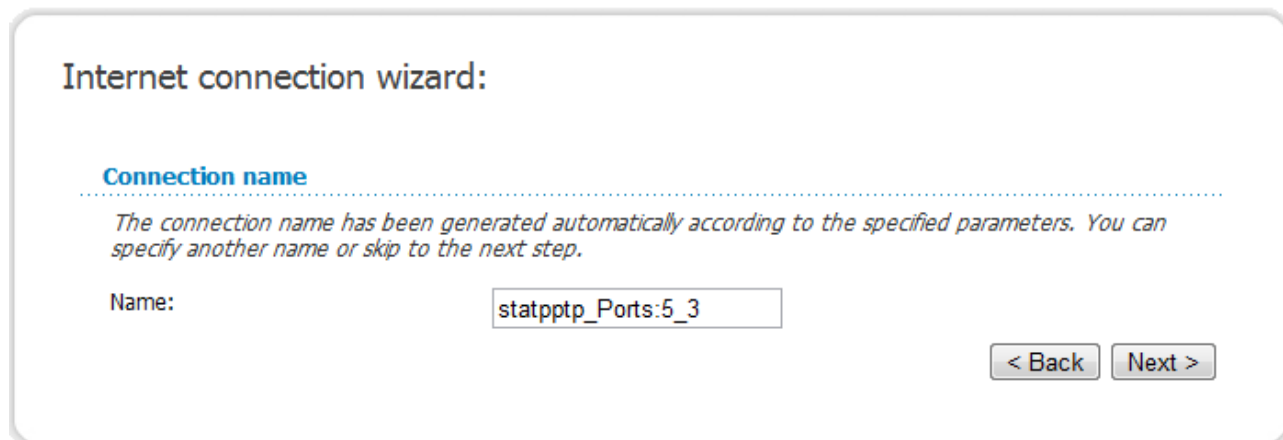
| Parameter | Description |
|------------------------------|---|
| Enable RIP | Select the checkbox to allow using RIP for this connection. |
| Enable IGMP Multicast | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |
| NAT | Select the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

Click the **Next** button to continue.

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

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

PPTP + Static IP or L2TP + Static IP Connection



Internet connection wizard:

Connection name

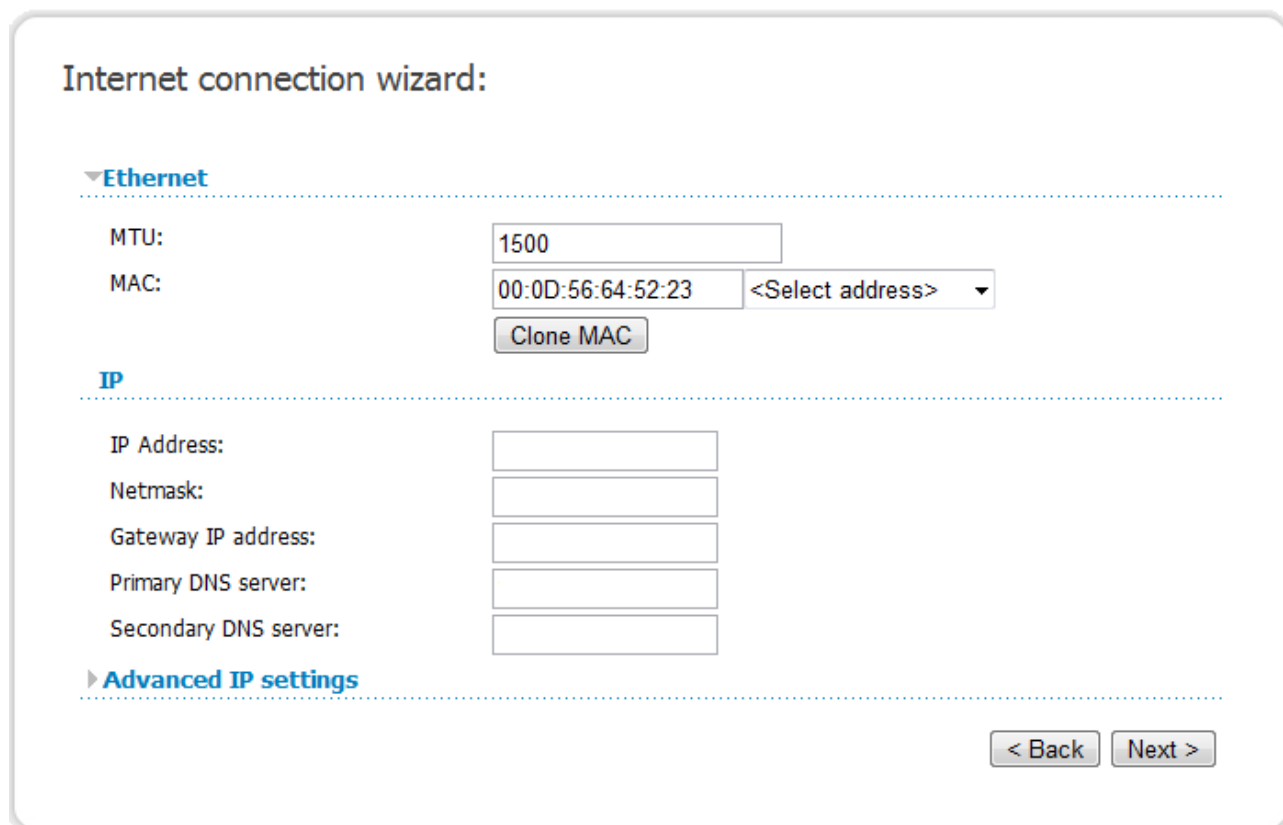
The connection name has been generated automatically according to the specified parameters. You can specify another name or skip to the next step.

Name:

< Back Next >

Figure 37. Configuring PPTP + Static IP WAN connection.

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



Internet connection wizard:

▼ **Ethernet**

MTU:

MAC: <Select address> ▼

IP

IP Address:

Netmask:

Gateway IP address:

Primary DNS server:

Secondary DNS server:

► **Advanced IP settings**

< Back Next >

Figure 38. Configuring PPTP + Static IP WAN connection.

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

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

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

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

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

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

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

Click the **Next** button to continue.

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

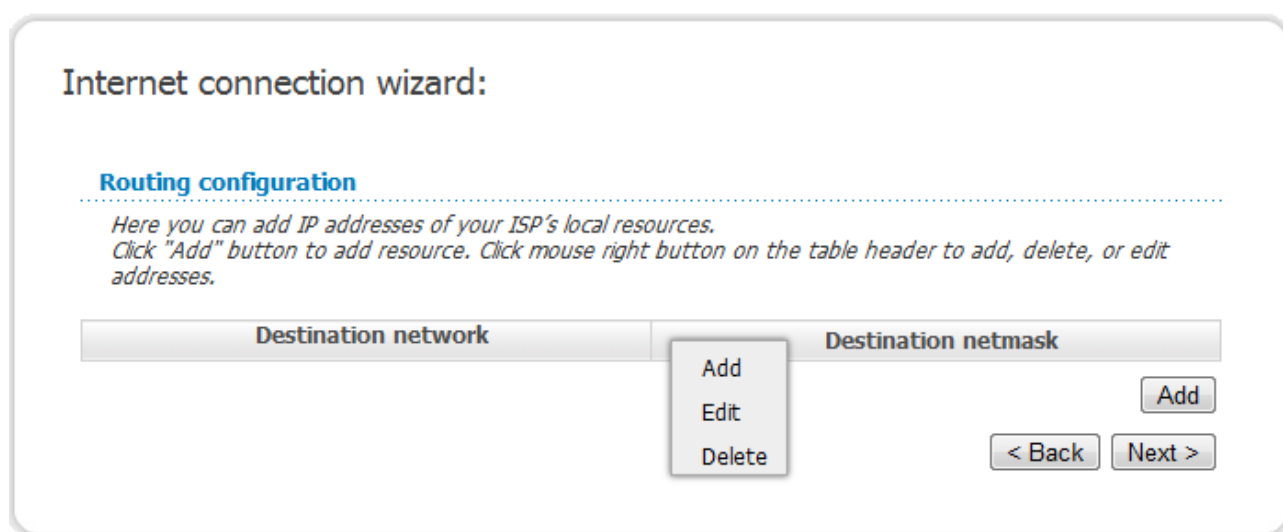
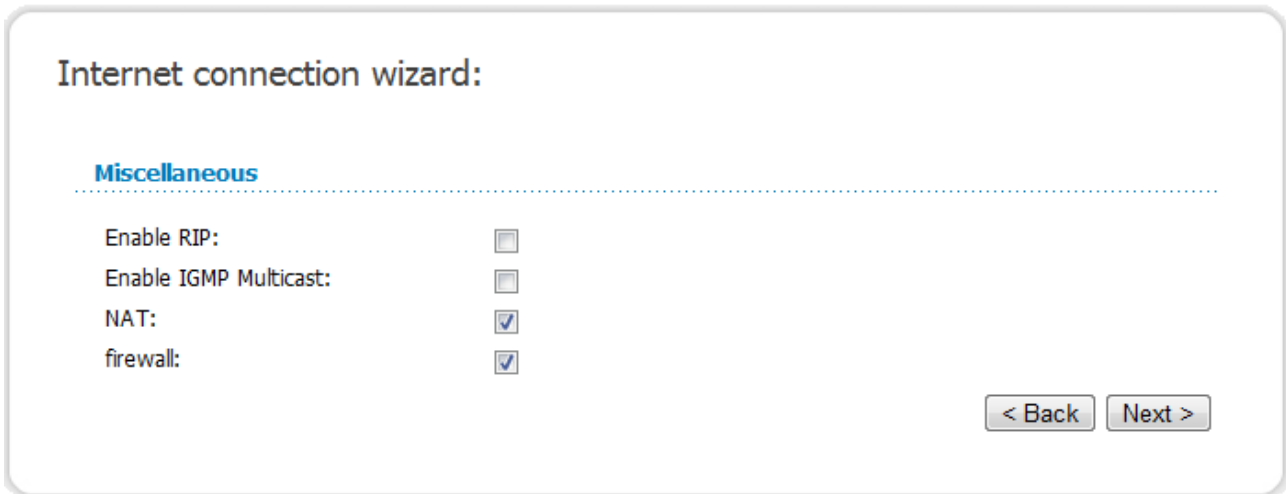


Figure 39. Configuring PPTP + Static IP WAN connection.

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

Click the **Next** button to continue.

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



The screenshot shows a web-based configuration interface for an internet connection wizard. The title is "Internet connection wizard:". Below the title, the section "Miscellaneous" is highlighted with a blue underline. There are four settings listed, each with a checkbox: "Enable RIP:" (unchecked), "Enable IGMP Multicast:" (unchecked), "NAT:" (checked), and "firewall:" (checked). At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 40. Configuring PPTP + Static IP WAN connection.

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

Click the **Next** button to continue.

Internet connection wizard:

VPN

Connect automatically:

Username:

Without authorization:

Password:

Password confirmation:

VPN server address:

Advanced PPP settings

Encryption:

Authentication algorithm:

MTU:

Keep Alive:

Extra options:

Dial on demand:

PPP debug:

IP received:

Figure 41. Configuring PPTP + Static IP WAN connection.

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

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

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

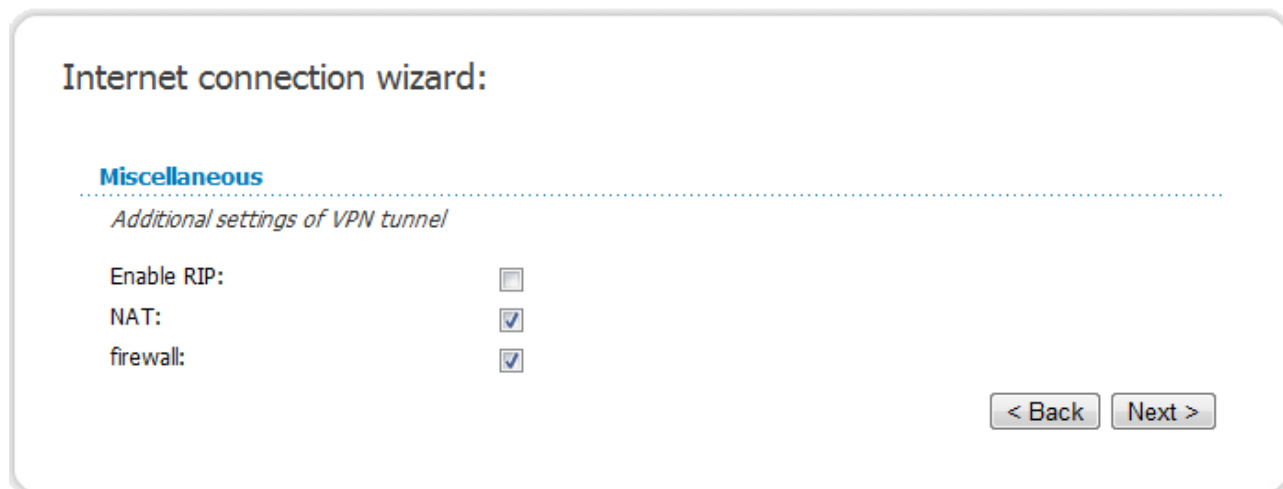
In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

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

| Parameter | Description |
|---------------------------------|--|
| Encryption | <p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encrypt: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP, MS-CHAP-V2, or AUTO value is selected from the Authentication algorithm drop-down list.</p> |
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. |
| Keep Alive | Select the checkbox if you want the 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. <i>Optional.</i> |
| 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. |
| PPP debug | Select the checkbox if you want to log all data on PPP connection debugging. |
| IP received | The IP address assigned by the ISP. |

Click the **Next** button to continue.

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



The screenshot shows a web-based configuration interface titled "Internet connection wizard:". Under the "Miscellaneous" section, there is a sub-section for "Additional settings of VPN tunnel". It contains three settings: "Enable RIP:" with an unchecked checkbox, "NAT:" with a checked checkbox, and "firewall:" with a checked checkbox. At the bottom right, there are two buttons: "< Back" and "Next >".

Figure 42. Configuring PPTP + Static IP WAN connection.

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

Click the **Next** button to continue.

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

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

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

Internet connection wizard:

Connection name

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

Name:

Figure 43. Configuring PPTP + Dynamic IP WAN connection.

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

Internet connection wizard:

Ethernet

MTU:

MAC:

IP

Obtain DNS server addresses automatically:

Advanced IP settings

Vendor ID:

Figure 44. Configuring PPTP + Dynamic IP WAN connection.

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

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

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

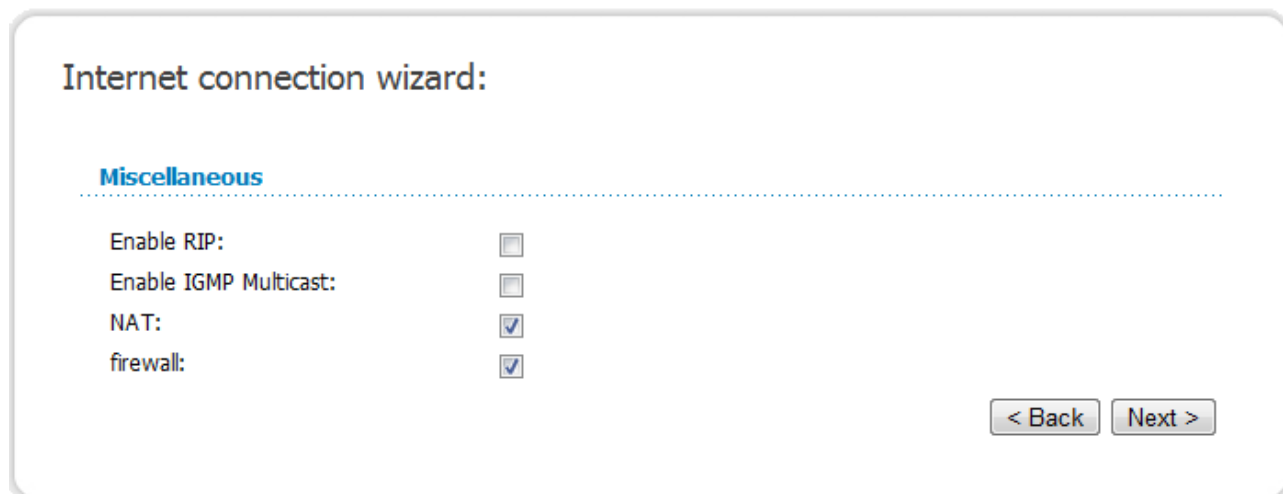
Also you can set the address of a device connected to the router's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).

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

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

Click the **Next** button to continue.

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



The screenshot shows a web-based configuration interface titled "Internet connection wizard:". Under the "Miscellaneous" section, there are four settings: "Enable RIP:" with an unchecked checkbox, "Enable IGMP Multicast:" with an unchecked checkbox, "NAT:" with a checked checkbox, and "firewall:" with a checked checkbox. At the bottom right, there are two buttons: "< Back" and "Next >".

Figure 45. Configuring PPTP + Dynamic IP WAN connection.

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

Click the **Next** button to continue.

Internet connection wizard:

VPN

Connect automatically:

Username:

Without authorization:

Password:

Password confirmation:

VPN server address:

Advanced PPP settings

Encryption:

Authentication algorithm:

MTU:

Keep Alive:

Extra options:

Dial on demand:

PPP debug:

IP received:

Figure 46. Configuring PPTP + Dynamic IP WAN connection.

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

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

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

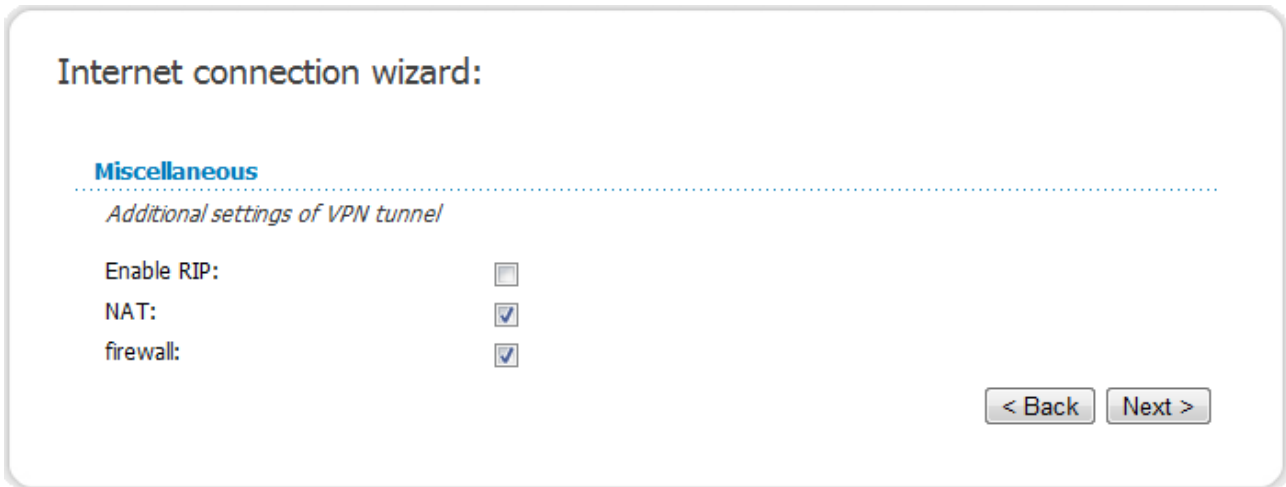
In the **VPN server address** field, enter the IP or URL address of the PPTP or L2TP authentication server.

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

| Parameter | Description |
|---------------------------------|--|
| Encryption | <p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encrypt: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP, MS-CHAP-V2, or AUTO value is selected from the Authentication algorithm drop-down list.</p> |
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. |
| Keep Alive | Select the checkbox if you want the 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. <i>Optional.</i> |
| 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. |
| PPP debug | Select the checkbox if you want to log all data on PPP connection debugging. |
| IP received | The IP address assigned by the ISP. |

Click the **Next** button to continue.

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



The screenshot shows a web-based configuration interface titled "Internet connection wizard:". Under the "Miscellaneous" section, which is underlined with a dotted line, there is a sub-section titled "Additional settings of VPN tunnel". This section contains three settings: "Enable RIP:" with an unchecked checkbox, "NAT:" with a checked checkbox, and "firewall:" with a checked checkbox. At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 47. Configuring PPTP + Dynamic IP WAN connection.

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

Click the **Next** button to continue.

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

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

3G Connection

Internet connection wizard:

Connection name

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

Name:

Figure 48. Configuring 3G connection.

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

Internet connection wizard:

▼ **3G**

Mode:

PPP

Username:

Without authorization:

Password:

Password confirmation:

APN:

Dial number:

▼ **Advanced PPP settings**

Authentication algorithm:

MTU:

Keep Alive:

LCP interval (sec):

LCP fails:

Extra options:

Dial on demand:

PPP debug:

Figure 49. Configuring 3G connection.

In the **Mode** drop-down list, leave the **auto** value in order to let the router connect automatically to an available type of network, or select a needed value from the drop-down list. *For GSM USB modems only.*

In the **Username** field, enter your login, and in the **Password** and **Password confirmation** fields – the password provided by your 3G operator.

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

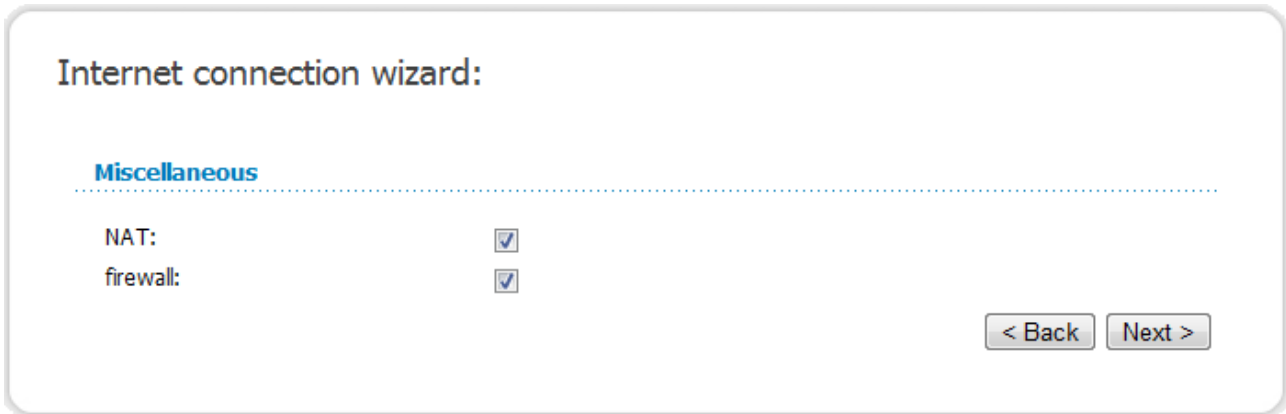
In the **APN** field (for GSM USB modems only), enter the access point name, and in the **Dial number** field, enter the number dialed to connect to the authorization server of the operator.

If needed, specify additional settings for your 3G WAN connection.

| Parameter | Description |
|---------------------------------|--|
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. <i>Optional.</i> |
| 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. |
| Extra options | In the field, you can specify additional data for encryption or authentication. <i>Optional.</i> |
| 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. |
| PPP debug | Select the checkbox if you want to log all data on PPP connection debugging. |

Click the **Next** button to continue.

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



The screenshot shows a web-based configuration interface titled "Internet connection wizard:". Below the title, the "Miscellaneous" section is highlighted with a blue dotted line. Under this section, there are two rows of settings: "NAT:" with a checked checkbox, and "firewall:" with a checked checkbox. At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 50. Configuring 3G connection.

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

Click the **Next** button to continue.

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

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

Site Setup Wizard

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

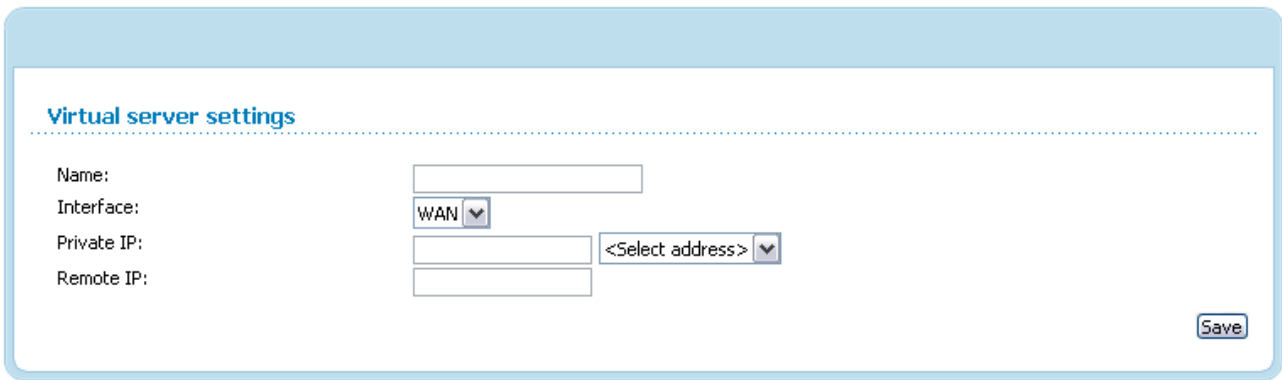


Figure 51. The page for adding a virtual server.

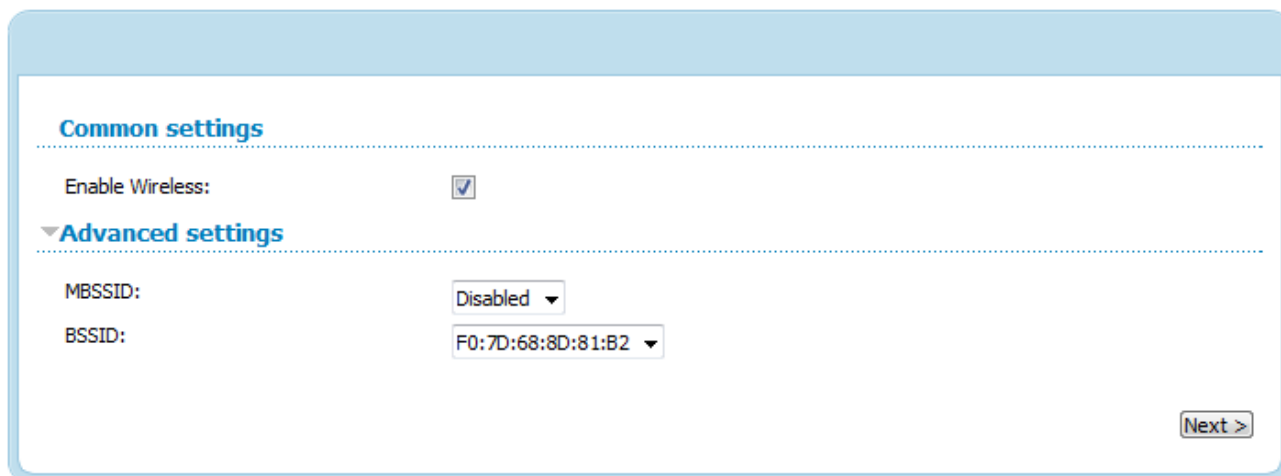
On the opened page, you can specify the following parameters:

| Parameter | Description |
|-------------------|--|
| Name | Enter a name for the virtual server for easier identification. You can specify any name. |
| Interface | Select a WAN connection to which this virtual server will be assigned. |
| Private IP | Enter the IP address of the server from the local area network. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list located to the right of the Private IP field (the field will be filled in automatically). |
| Remote IP | Enter the IP address of the server from the external network. |

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

Wi-Fi Setup Wizard

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



The screenshot shows the 'Common settings' and 'Advanced settings' sections of the Wi-Fi Setup Wizard. In the 'Common settings' section, the 'Enable Wireless' checkbox is checked. In the 'Advanced settings' section, the 'MBSSID' dropdown is set to 'Disabled' and the 'BSSID' dropdown is set to 'F0:7D:68:8D:81:B2'. A 'Next >' button is located at the bottom right of the settings area.

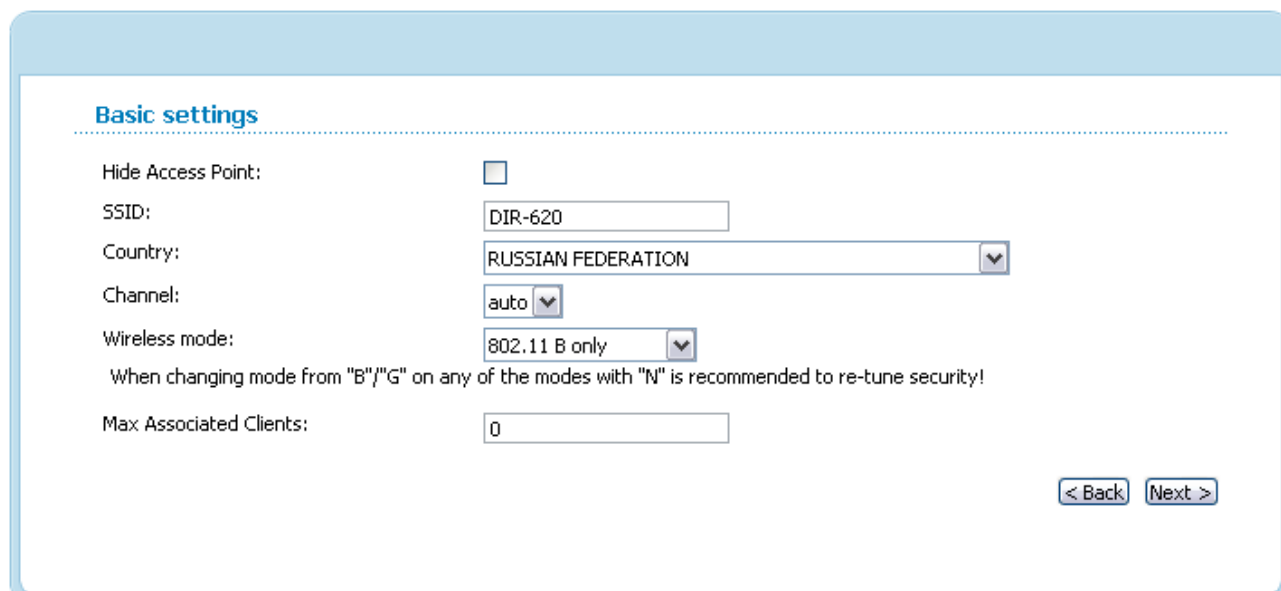
Figure 52. Common and advanced settings of the wireless LAN.

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

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

Click the **Next** button to continue.

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



The screenshot shows the 'Basic settings' section of the Wi-Fi Setup Wizard. The 'Hide Access Point' checkbox is unchecked. The 'SSID' text field contains 'DIR-620'. The 'Country' dropdown is set to 'RUSSIAN FEDERATION'. The 'Channel' dropdown is set to 'auto'. The 'Wireless mode' dropdown is set to '802.11 B only'. Below the 'Wireless mode' dropdown, there is a note: 'When changing mode from "B"/"G" on any of the modes with "N" is recommended to re-tune security!'. The 'Max Associated Clients' text field contains '0'. At the bottom right, there are '< Back' and 'Next >' buttons.

Figure 53. Basic settings of the wireless LAN.

Click the **Next** button to continue.

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

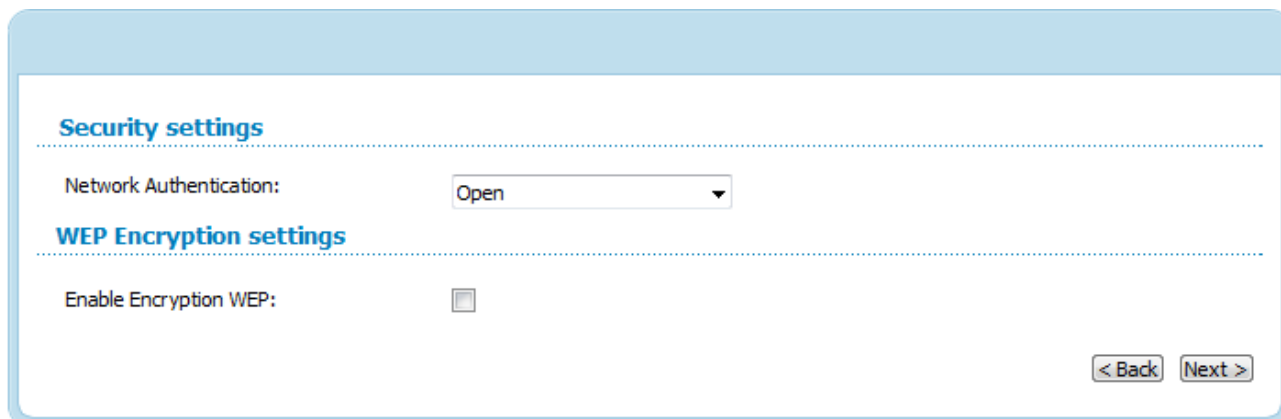


Figure 54. The default security settings.

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

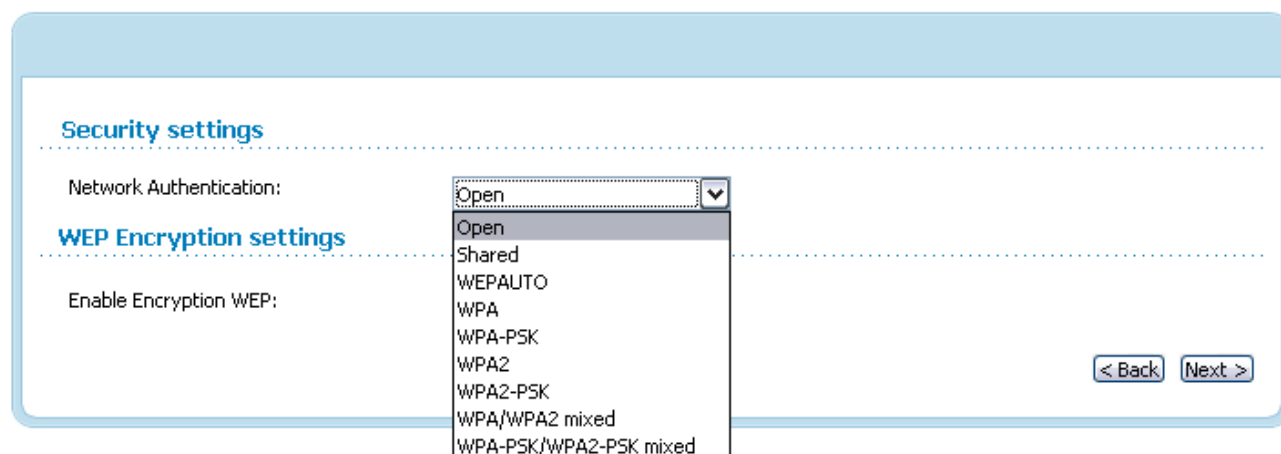


Figure 55. Network authentication types supported by the router.

The router supports the following authentication types:

| Authentication type | Description |
|---------------------|--|
| Open | Open authentication (with WEP encryption for wireless network modes not supporting 802.11n devices). |
| Shared | Shared key authentication with WEP encryption. This authentication type is not available when on the basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected. |

| Authentication type | Description |
|-------------------------------|--|
| WEPAUTO | <p>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.</p> <p>This authentication type is not available when on the basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected.</p> |
| WPA | WPA-based authentication using a RADIUS server. |
| WPA-PSK | WPA-based authentication using a PSK. |
| WPA2 | WPA2-based authentication using a RADIUS server. |
| WPA2-PSK | WPA2-based authentication using a PSK. |
| WPA/WPA2 mixed | A mixed type of authentication. When this value is selected, devices using the WPA authentication type and devices using the WPA2 authentication type can connect to the WLAN of the router. |
| WPA-PSK/WPA2-PSK mixed | A mixed type of authentication. When this value is selected, devices using the WPA-PSK authentication type and devices using the WPA2-PSK authentication type can connect to the WLAN of the router. |



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

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

Figure 56. The **Open** value is selected from the **Network Authentication** drop-down list.

| Parameter | Description |
|----------------------------------|--|
| Enable Encryption WEP | The checkbox activating WEP encryption. When the checkbox is selected, the Default Key ID field, the Encryption Key WEP as HEX checkbox, and four Encryption Key WEP fields are displayed on the page. For the Shared 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 as HEX | Select the checkbox to set a hexadecimal number as a key for encryption. |
| Encryption Key WEP (1-4) | Keys for WEP encryption. The 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). If the Encryption Key WEP as HEX checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F). |

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

The screenshot shows a web-based configuration interface for WPA settings. It is divided into two main sections: "Security settings" and "WPA Encryption settings".

- Security settings:**
 - Network Authentication:** A dropdown menu with "WPA2-PSK" selected.
 - Encryption Key PSK:** A text input field containing "76543210".
 - WPA2 Pre-authentication:** An unchecked checkbox.
- WPA Encryption settings:**
 - WPA Encryption:** A dropdown menu with "TKIP" selected.
 - WPA renewal:** A text input field containing "3600".

At the bottom right of the form, there are two buttons: "< Back" and "Next >".

Figure 57. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.

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

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

The screenshot displays the configuration page for wireless security. It is divided into three sections: Security settings, RADIUS settings, and WPA Encryption settings. In the Security settings, 'Network Authentication' is set to 'WPA2' and 'WPA2 Pre-authentication' is unchecked. The RADIUS settings section includes 'IP address' (192.168.0.254), 'Port' (1812), and 'RADIUS encryption key' (dlink). The WPA Encryption settings section shows 'WPA Encryption' set to 'AES' and 'WPA renewal' set to 3600. Navigation buttons for '< Back' and 'Next >' are located at the bottom right of the form.

Figure 58. The **WPA2** value is selected from the **Network Authentication** drop-down list.

| Parameter | Description |
|--------------------------------|--|
| WPA2 Pre-authentication | The checkbox activating preliminary authentication (displayed only for the WPA2 and WPA/WPA2 mixed authentication types). |
| IP address | The IP address of the RADIUS server. |
| Port | A port of the RADIUS server. |
| RADIUS encryption key | The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings). |
| WPA Encryption | An encryption method: TKIP (available only for the WPA authentication type), AES (available only for the WPA2 and WPA/WPA2 mixed authentication types). |
| WPA renewal | The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed. |

Click the **Next** button to continue.

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

IPTV Setup Wizard

To configure the router to use an IPTV set-top box, click the **Configure IPTV** button.

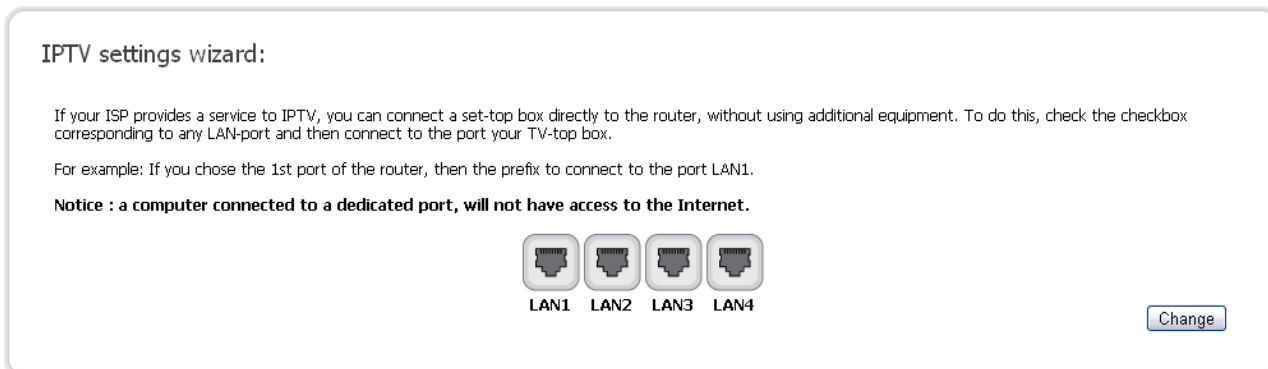


Figure 59. The page for selecting a LAN port to connect an IPTV set-top box.

On the opened page, select the LAN port of the router to which you will connect your IPTV set-top box and click the **Change** button. After that you will get to the quick settings page.

If in the future you need to disconnect your IPTV set-top box from the specified LAN port and connect to it a computer, on the current page deselect the LAN port and click the **Change** button.

If for accessing the Internet and IPTV services your ISP uses virtual local area networks with identifiers (VLAN ID), to configure access to the IPTV service, proceed to the **Advanced / VLAN** page, create a group of ports with the required value of the **VLAN ID** parameter, **Transparent** type, and the port to which the set-top box will be connected (see the *VLAN* section, page 116, for a detailed description of the elements from the page).

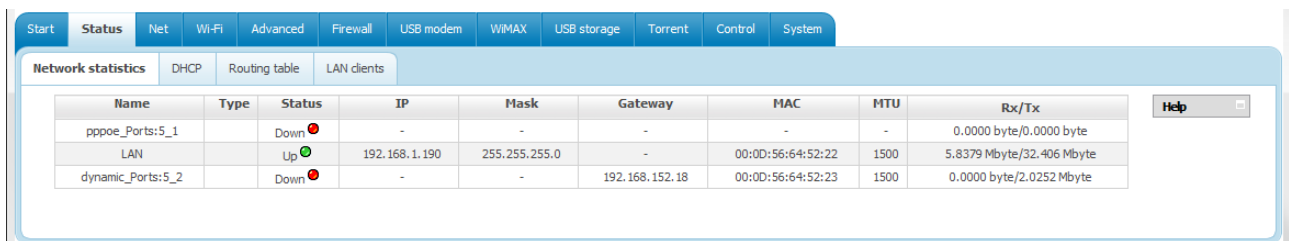
Status

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

- network statistics
- IP addresses leased by the DHCP server
- the routing table
- data on devices connected to the router's network and its web-based interface.

Network Statistics

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



The screenshot shows the 'Status' page with the 'Network statistics' tab selected. The table below displays the status of three network interfaces: pppoe_Ports:5_1 (Down), LAN (Up), and dynamic_Ports:5_2 (Down). The LAN interface is the only one with an IP address (192.168.1.190) and a gateway (192.168.152.18).

| Name | Type | Status | IP | Mask | Gateway | MAC | MTU | Rx/Tx |
|-------------------|------|--------|---------------|---------------|----------------|-------------------|------|---------------------------|
| pppoe_Ports:5_1 | | Down | - | - | - | - | - | 0.0000 byte/0.0000 byte |
| LAN | | Up | 192.168.1.190 | 255.255.255.0 | - | 00:0D:56:64:52:22 | 1500 | 5.8379 Mbyte/32.406 Mbyte |
| dynamic_Ports:5_2 | | Down | - | - | 192.168.152.18 | 00:0D:56:64:52:23 | 1500 | 0.0000 byte/2.0252 Mbyte |

Figure 60. The **Status / Network statistics** page.

DHCP

The **Status / DHCP** page displays the information on computers that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the device, as well as the IP address expiration periods (the lease time).

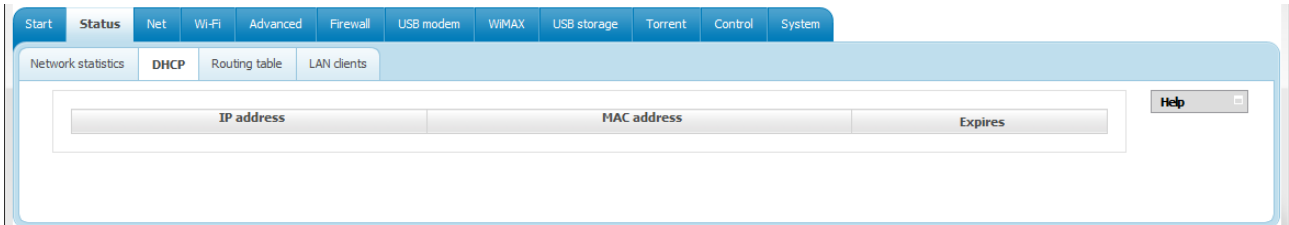
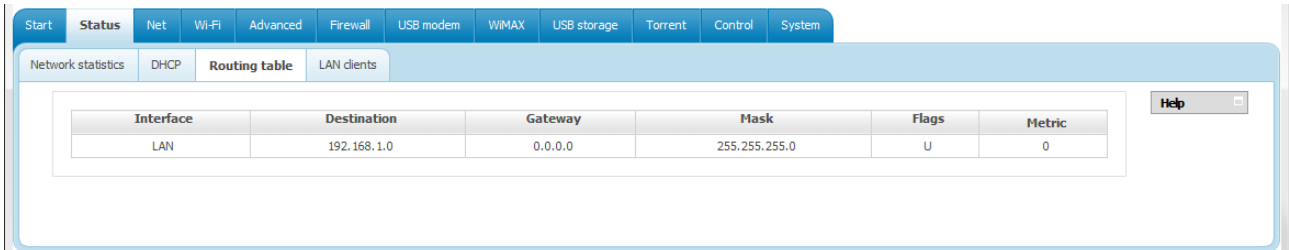


Figure 61. The **Status / DHCP** page.

Routing Table

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

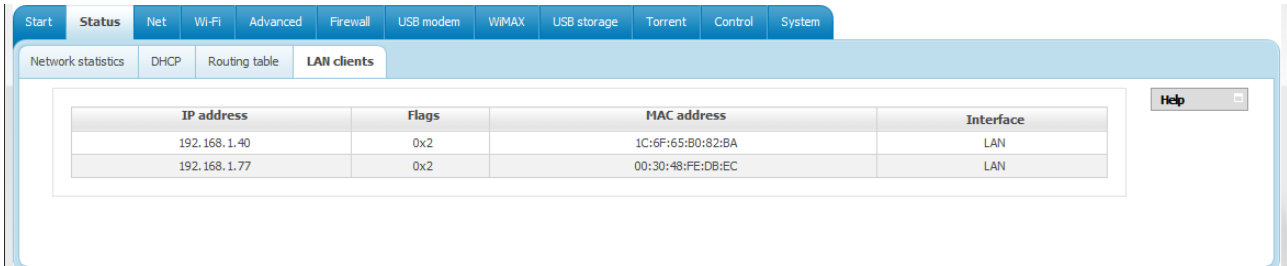


| Interface | Destination | Gateway | Mask | Flags | Metric |
|-----------|-------------|---------|---------------|-------|--------|
| LAN | 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U | 0 |

Figure 62. The **Status / Routing table** page.

LAN Clients

On the **Status / LAN clients** page, you can view the list of devices connected to the router and devices accessing its web-based interface.



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

Figure 63. The **Status / LAN clients** page.

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

Net

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

WAN

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

By default, the **WAN** connection is configured in the system. It is assigned to the INTERNET port of the router. You can edit this connection or delete it.

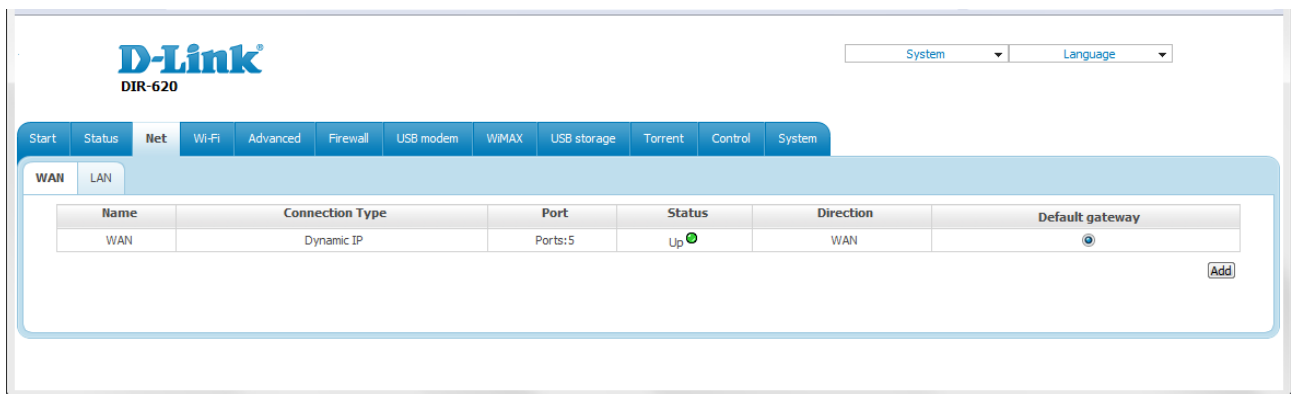


Figure 64. The **Net / WAN** page.

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

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

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

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

Creating 3G WAN Connection

If the PIN code check is enabled for the SIM card inserted into your USB modem, then prior to creating a 3G WAN connection, proceed to the **USB modem** menu and enter the PIN code on the page displayed (see the *USB Modem* section, page 134). Then proceed to the **Net / WAN** page, click the **Add** button, and select the **3G** value from the **Connection Type** drop-down list.

General settings

Provider:

Connection Type:

Port:

Name:

Enable:

Direction: *WAN*

3G

Mode:

Figure 65. The page for creating a new connection. The **General settings** and **3G** sections.

| Parameter | Description |
|-------------------------|---|
| General settings | |
| Provider | To automatically specify all settings required to connect to the Internet, select your country and operator from the drop-down list. To specify all settings independently, leave the Manually value. |
| Port | Select the USB value. |
| Name | A name for connection for easier identification. |
| Enable | Select the checkbox to enable the connection. |
| Direction | The direction of this connection. |
| 3G | |
| Mode | The value of the field specifies the type of the network to which the router connects. Leave the auto value to let the router connect automatically to an available type of network, or select a needed value from the drop-down list. <i>For GSM USB modems only.</i> |

PPP

Username:

Without authorization:

Password:

Password confirmation:

APN:

Dial number:

Authentication algorithm:

MTU:

Keep Alive:

LCP interval (sec):

LCP fails:

Extra options:

Dial on demand:

PPP debug:

Miscellaneous

NAT:

firewall:

Figure 66. The page for creating a new connection. The **PPP** and **Miscellaneous** sections.

| Parameter | Description |
|---------------------------------|--|
| 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. |
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. <i>Optional</i> . |
| 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 |
|-----------------------|---|
| Extra options | In the field, you can specify additional data for encryption or authentication. <i>Optional.</i> |
| 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. |
| PPP debug | Select the checkbox if you want to log all data on PPP connection debugging. |
| 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, click the **Add** button on the **Net / WAN** page. On the opened page, select the **PPPoE** value from the **Connection Type** drop-down list and specify the needed values.

General settings

Provider:

Connection Type:

Port:

Name:

Enable:

Direction: *WAN*

Ethernet

MTU:

MAC:

Figure 67. The page for creating a new connection. The **General settings** and **Ethernet** sections.

| Parameter | Description |
|-------------------------|--|
| General settings | |
| Provider | Leave the Manually value. |
| Port | A physical or virtual interface to which the new connection will be assigned. Select the USB-WIMAX value to assign this connection to the WiMAX USB modem. |
| Name | A name for connection for easier identification. |
| Enable | Select the checkbox to enable the connection. |
| Direction | The direction of this connection. |
| Ethernet | |
| MTU | The maximum size of units transmitted by the interface. |

| Parameter | Description |
|------------|---|
| MAC | <p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>You can click the Clone MAC button to set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface.</p> <p>Also you can set the address of a device connected to the router's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).</p> |

PPP

Username:

Without authorization:

Password:

Password confirmation:

Service name:

Authentication algorithm:

MTU:

Keep Alive:

LCP interval (sec):

LCP fails:

Dial on demand:

PPP IP extension:

Use Static IP Address:

PPP debug:

PPPoE pass through:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Figure 68. The page for creating a new connection. The **PPP** and **Miscellaneous** sections.

| Parameter | Description |
|---------------------------------|--|
| PPP | |
| Username | A username (login) to access the Internet. |
| Without authorization | Select the checkbox if you don't need to enter a username and password to access the Internet. |
| Password | A password to access the Internet. |
| Password confirmation | The confirmation of the entered password (to avoid mistypes). |
| Service name | The name of the PPPoE authentication server. |
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. |
| 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. |
| 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. |
| PPP IP extension | This option is used by some ISPs. Contact your ISP to clarify if this checkbox needs to be enabled. |
| Use Static IP Address | Select the checkbox if you want to use a static IP address to access the Internet. In the Static 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. |
| Enable IGMP Multicast | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |
| Miscellaneous | |
| Enable RIP | Select the checkbox to allow using RIP for this connection. |

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

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

Creating Static IP WAN Connection

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

General settings

Provider:

Connection Type:

Port:

Name:

Enable:

Direction: *WAN*

Ethernet

MTU:

MAC:

Figure 69. The page for creating a new connection. The **General settings** and **Ethernet** sections.

| Parameter | Description |
|-------------------------|--|
| General settings | |
| Provider | Leave the Manually value. |
| Port | A physical or virtual interface to which the new connection will be assigned. Select the USB-WIMAX value to assign this connection to the WiMAX USB modem. |
| Name | A name for connection for easier identification. |
| Enable | Select the checkbox to enable the connection. |
| Direction | The direction of this connection. |
| Ethernet | |
| MTU | The maximum size of units transmitted by the interface. |

| Parameter | Description |
|------------|---|
| MAC | <p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>You can click the Clone MAC button to set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface.</p> <p>Also you can set the address of a device connected to the router's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).</p> |

IP

IP Address:

Netmask:

Gateway IP address:

Primary DNS server:

Secondary DNS server:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Figure 70. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

| Parameter | Description |
|---|--|
| IP | |
| IP Address | Enter an IP address for this WAN connection. |
| Netmask | Enter a subnet mask for this WAN connection. |
| Gateway IP Address | Enter an IP address of the gateway used by this WAN connection. |
| Primary DNS server/ Secondary DNS server | Enter addresses of the primary and secondary DNS servers in the relevant fields. |
| Miscellaneous | |
| Enable RIP | Select the checkbox to allow using RIP for this connection. |

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

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

Creating Dynamic IP WAN Connection

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

General settings

Provider:

Connection Type:

Port:

Name:

Enable:

Direction: *WAN*

Ethernet

MTU:

MAC:

Figure 71. The page for creating a new connection. The **General settings** and **Ethernet** sections.

| Parameter | Description |
|-------------------------|--|
| General settings | |
| Provider | Leave the Manually value. |
| Port | A physical or virtual interface to which the new connection will be assigned. Select the USB-WIMAX value to assign this connection to the WiMAX USB modem. |
| Name | A name for connection for easier identification. |
| Enable | Select the checkbox to enable the connection. |
| Direction | The direction of this connection. |
| Ethernet | |
| MTU | The maximum size of units transmitted by the interface. |

| Parameter | Description |
|------------|---|
| MAC | <p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>You can click the Clone MAC button to set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface.</p> <p>Also you can set the address of a device connected to the router's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).</p> |

IP

Obtain DNS server addresses automatically:

Vendor ID:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Figure 72. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

| Parameter | Description |
|--|---|
| IP | |
| Obtain DNS server addresses automatically | Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the Primary DNS server and Secondary DNS server fields are not displayed. |
| Primary DNS server/ Secondary DNS server | Enter addresses of the primary and secondary DNS servers in the relevant fields. |
| Vendor ID | The identifier of your ISP. <i>Optional.</i> |
| Miscellaneous | |
| Enable RIP | Select the checkbox to allow using RIP for this connection. |
| Enable IGMP Multicast | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |

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

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

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

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

General settings

Provider:

Connection Type:

Port:

Name:

Enable:

Direction: *WAN*

Ethernet

MTU:

MAC:

Figure 73. The page for creating a new connection. The **General settings** and **Ethernet** sections.

| Parameter | Description |
|-------------------------|--|
| General settings | |
| Provider | Leave the Manually value. |
| Port | A physical or virtual interface to which the new connection will be assigned. Select the USB-WIMAX value to assign this connection to the WiMAX USB modem. |
| Name | A name for connection for easier identification. |
| Enable | Select the checkbox to enable the connection. |
| Direction | The direction of this connection. |
| Ethernet | |
| MTU | The maximum size of units transmitted by the interface. |

| Parameter | Description |
|------------|---|
| MAC | <p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>You can click the Clone MAC button to set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface.</p> <p>Also you can set the address of a device connected to the router's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).</p> |

IP

IP Address:

Netmask:

Gateway IP address:

Primary DNS server:

Secondary DNS server:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Figure 74. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

| Parameter | Description |
|---|--|
| IP | |
| IP Address | Enter an IP address for this WAN connection. |
| Netmask | Enter a subnet mask for this WAN connection. |
| Gateway IP Address | Enter an IP address of the gateway used by this WAN connection. |
| Primary DNS server/ Secondary DNS server | Enter addresses of the primary and secondary DNS servers in the relevant fields. |
| Miscellaneous | |
| Enable RIP | Select the checkbox to allow using RIP for this connection. |

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

VPN

Connect automatically:

Username:

Without authorization:

Password:

Password confirmation:

VPN server address:

Encryption:

Authentication algorithm:

MTU:

Keep Alive:

Extra options:

Dial on demand:

PPP debug:

IP received:

Miscellaneous

Enable RIP:

NAT:

firewall:

Figure 75. The page for creating a new connection. The **VPN** and **Miscellaneous** sections.

| Parameter | Description |
|---------------------------------|--|
| VPN | |
| Connect automatically | Select the checkbox to enable auto-start of the connection upon the boot-up of the router. |
| Username | A username (login) to access the Internet. |
| Without authorization | Select the checkbox if you don't need to enter a username and password to access the Internet. |
| Password | A password to access the Internet. |
| Password confirmation | The confirmation of the entered password (to avoid mistypes). |
| VPN server address | The IP or URL address of the PPTP or L2TP authentication server. |
| Encryption | <p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encrypt: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP, MS-CHAP-V2, or AUTO value is selected from the Authentication algorithm drop-down list.</p> |
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. |
| Keep Alive | Select the checkbox if you want the 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. <i>Optional</i> . |
| 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. |

| Parameter | Description |
|----------------------|--|
| PPP debug | Select the checkbox if you want to log all data on PPP connection debugging. |
| IP received | The IP address assigned by the ISP. |
| Miscellaneous | |
| Enable RIP | Select the checkbox to allow using RIP for this connection. |
| NAT | Select the checkbox if you want one WAN IP address to be used for all computers of your LAN. |
| Firewall | Select the checkbox to enable protection against ARP and DDoS attacks. |

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

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

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

General settings

Provider:

Connection Type:

Port:

Name:

Enable:

Direction: *WAN*

Ethernet

MTU:

MAC:

Figure 76. The page for creating a new connection. The **General settings** and **Ethernet** sections.

| Parameter | Description |
|-------------------------|--|
| General settings | |
| Provider | Leave the Manually value. |
| Port | A physical or virtual interface to which the new connection will be assigned. Select the USB-WIMAX value to assign this connection to the WiMAX USB modem. |
| Name | A name for connection for easier identification. |
| Enable | Select the checkbox to enable the connection. |
| Direction | The direction of this connection. |
| Ethernet | |
| MTU | The maximum size of units transmitted by the interface. |

| Parameter | Description |
|------------|---|
| MAC | <p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>You can click the Clone MAC button to set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface.</p> <p>Also you can set the address of a device connected to the router's LAN at the moment. To do this, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically).</p> |

IP

Obtain DNS server addresses automatically:

Vendor ID:

Miscellaneous

Enable RIP:

Enable IGMP Multicast:

NAT:

firewall:

Figure 77. The page for creating a new connection. The **IP** and **Miscellaneous** sections.

| Parameter | Description |
|--|---|
| IP | |
| Obtain DNS server addresses automatically | Select the checkbox to configure automatic assignment of DNS server addresses. If the checkbox is selected, the Primary DNS server and Secondary DNS server fields are not displayed. |
| Primary DNS server/ Secondary DNS server | Enter addresses of the primary and secondary DNS servers in the relevant fields. |
| Vendor ID | The identifier of your ISP. <i>Optional.</i> |
| Miscellaneous | |
| Enable RIP | Select the checkbox to allow using RIP for this connection. |
| Enable IGMP Multicast | Select the checkbox to allow multicast traffic from the external network (e.g. video streaming) to be received. |

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

VPN

Connect automatically:

Username:

Without authorization:

Password:

Password confirmation:

VPN server address:

Encryption:

Authentication algorithm:

MTU:

Keep Alive:

Extra options:

Dial on demand:

PPP debug:

IP received:

Miscellaneous

Enable RIP:

NAT:

firewall:

Figure 78. The page for creating a new connection. The **VPN** and **Miscellaneous** sections.

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

| Parameter | Description |
|---------------------------------|--|
| Encryption | <p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encrypt: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP, MS-CHAP-V2, or AUTO value is selected from the Authentication algorithm drop-down list.</p> |
| Authentication algorithm | Select a required authentication method from the drop-down list or leave the AUTO value. |
| MTU | The maximum size of units transmitted by the interface. |
| Keep Alive | Select the checkbox if you want the 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. <i>Optional.</i> |
| 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. |
| PPP debug | Select the checkbox if you want to log all data on PPP connection debugging. |
| IP received | The IP address assigned by the ISP. |
| Miscellaneous | |
| Enable RIP | Select the checkbox to allow using RIP for this connection. |
| NAT | Select the checkbox if you want one WAN IP address to be used for all computers of your LAN. |
| Firewall | Select the checkbox to enable protection against ARP and DDoS attacks. |

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

LAN

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

The screenshot shows the LAN configuration page with the following sections:

- Basic Settings:** IP Address: 192.168.0.1, Netmask: 255.255.255.0
- Static DHCP:** Fields for IP address, MAC address, and Host name, with a table below them and 'Remove' and 'Add' buttons.
- DHCP server:** Mode: Enable, Start IP: 192.168.0.2, End IP: 192.168.0.254, Lease time (min): 86400. A 'Save' button is at the bottom right.

Figure 79. The page for configuring the local interface.

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

| Parameter | Description |
|-------------------|--|
| IP Address | The IP address of the router in the local subnet. By default, the following value is specified: 192.168.0.1 . |
| Netmask | The mask of the local subnet. By default, the following value is specified: 255.255.255.0 . |

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

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

To create a MAC-IP pair, click the **Add** button and 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. <i>Optional</i> . |

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

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

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

| Parameter | Description |
|--------------------------------|---|
| Mode | An operating mode of the router's DHCP server. Enable: the router assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the Start IP , End IP , and the Lease time fields are displayed on the page. 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 page. |
| Start IP | The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients. |
| End IP | The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients. |
| Lease time | The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address. |
| External DHCP server IP | The IP address of the external DHCP server which assigns IP addresses to the router's clients. |

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

Wi-Fi

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

Common settings

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

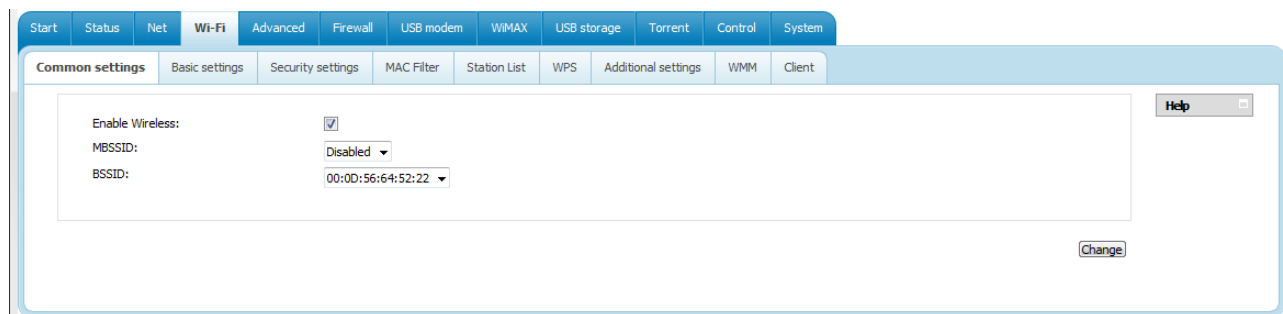


Figure 80. Common settings of the wireless LAN.

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

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

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

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

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

Basic Settings

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

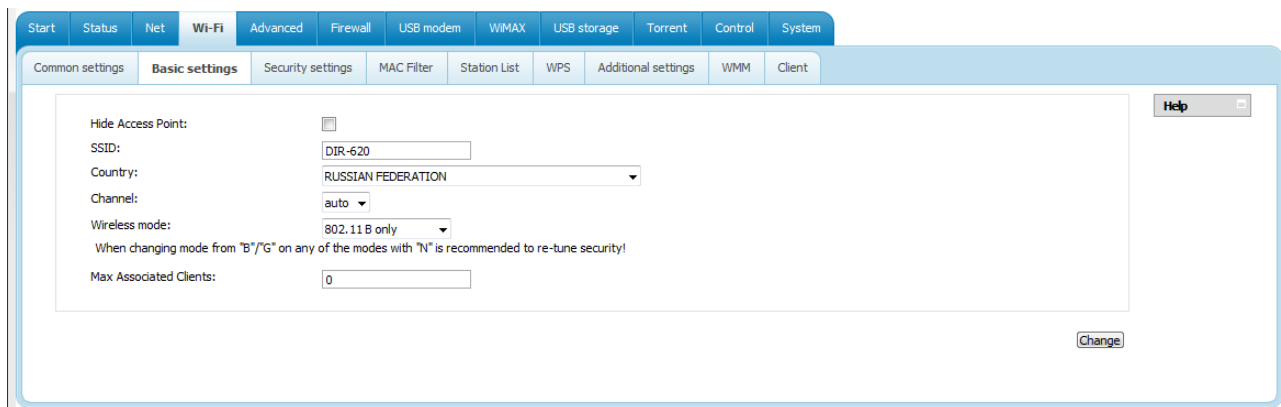


Figure 81. Basic settings of the wireless LAN.

| 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 splitted 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). |
| 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 wireless network of the router. 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 device does not limit the number of connected clients. |

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

Security Settings

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

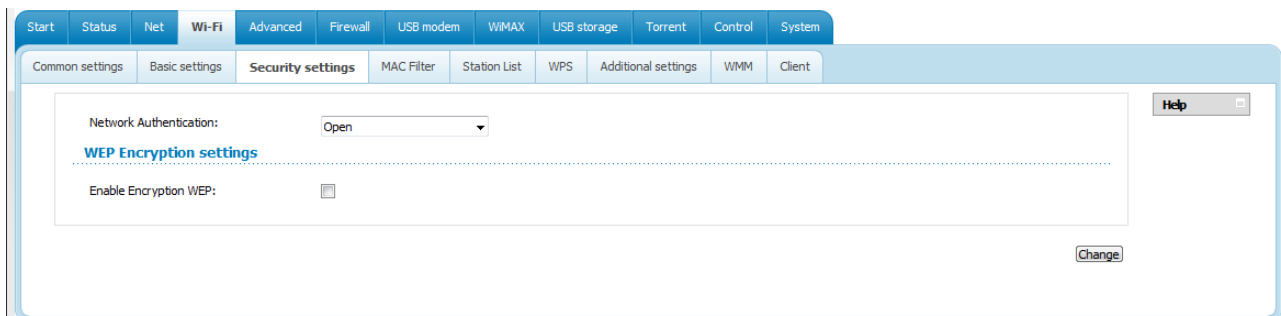


Figure 82. The default security settings.

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



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

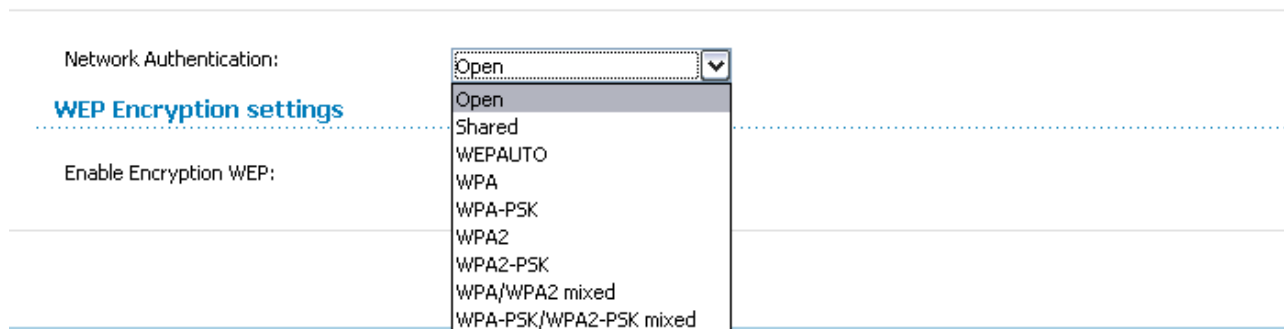


Figure 83. Network authentication types supported by the router.

The router supports the following authentication types:

| Authentication type | Description |
|---------------------|---|
| Open | Open authentication (with WEP encryption for wireless network modes not supporting 802.11n devices). |
| Shared | Shared key authentication with WEP encryption. This authentication type is not available when on the Wi-Fi / Basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected. |

| Authentication type | Description |
|-------------------------------|---|
| WEPAUTO | <p>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.</p> <p>This authentication type is not available when on the Wi-Fi / Basic settings page, in the Wireless mode drop-down list, a mode supporting 802.11n devices is selected.</p> |
| WPA | WPA-based authentication using a RADIUS server. |
| WPA-PSK | WPA-based authentication using a PSK. |
| WPA2 | WPA2-based authentication using a RADIUS server. |
| WPA2-PSK | WPA2-based authentication using a PSK. |
| WPA/WPA2 mixed | A mixed type of authentication. When this value is selected, devices using the WPA authentication type and devices using the WPA2 authentication type can connect to the WLAN of the router. |
| WPA-PSK/WPA2-PSK mixed | A mixed type of authentication. When this value is selected, devices using the WPA-PSK authentication type and devices using the WPA2-PSK authentication type can connect to the WLAN of the router. |



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

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

Network Authentication:

WEP Encryption settings

Enable Encryption WEP:

Default Key ID:

Encryption Key WEP as HEX:

Encryption Key WEP (1):

Encryption Key WEP (2):

Encryption Key WEP (3):

Encryption Key WEP (4):

Figure 84. The **Open** value is selected from the **Network Authentication** drop-down list.

| Parameter | Description |
|----------------------------------|--|
| Enable Encryption WEP | The checkbox activating WEP encryption. When the checkbox is selected, the Default Key ID field, the Encryption Key WEP as HEX checkbox, and four Encryption Key WEP fields are displayed on the page. For the Shared 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 as HEX | Select the checkbox to set a hexadecimal number as a key for encryption. |
| Encryption Key WEP (1-4) | Keys for WEP encryption. The 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). If the Encryption Key WEP as HEX checkbox is selected, you can specify only keys containing 10 symbols (the digits 0-9 and the characters A-F). |

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

Network Authentication:

Encryption Key PSK:

WPA2 Pre-authentication:

WPA Encryption settings

WPA Encryption:

WPA renewal:

Figure 85. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.

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

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

Network Authentication:

WPA2 Pre-authentication:

RADIUS settings

IP address:

Port:

RADIUS encryption key:

WPA Encryption settings

WPA Encryption:

WPA renewal:

Figure 86. The **WPA2** value is selected from the **Network Authentication** drop-down list.

| Parameter | Description |
|--------------------------------|--|
| WPA2 Pre-authentication | The checkbox activating preliminary authentication (displayed only for the WPA2 and WPA/WPA2 mixed authentication types). |
| IP address | The IP address of the RADIUS server. |
| Port | A port of the RADIUS server. |
| RADIUS encryption key | The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings). |
| WPA Encryption | An encryption method: TKIP (available only for the WPA authentication type), AES (available only for the WPA2 and WPA/WPA2 mixed authentication types). |
| WPA renewal | The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed. |

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

MAC Filter

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

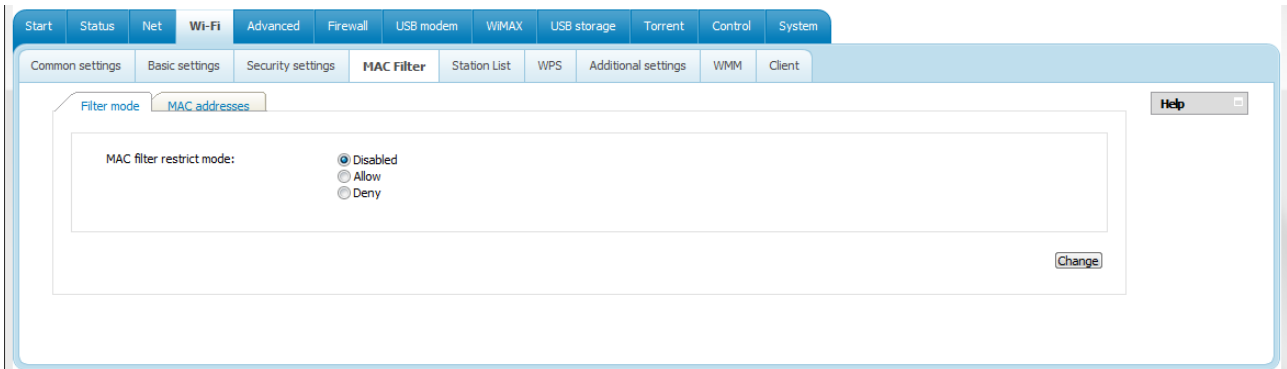


Figure 87. The MAC filter for the wireless network.

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

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

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

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

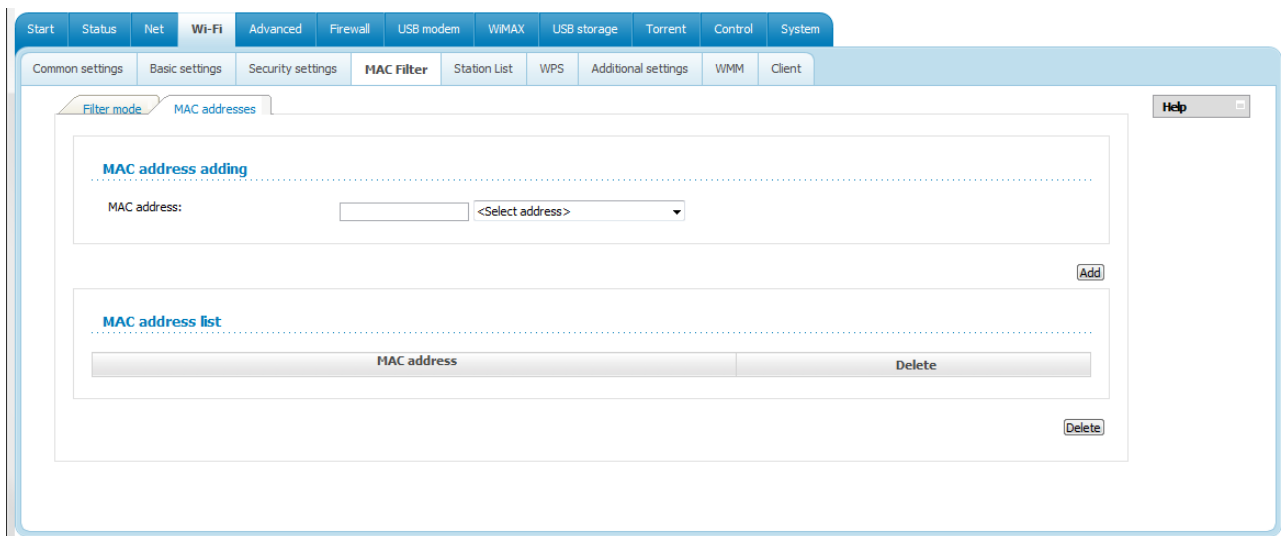


Figure 88. The tab for adding a MAC address.

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

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

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

Station List

On the **Wi-Fi / Station List** page, you can view the list of wireless clients connected to the router.

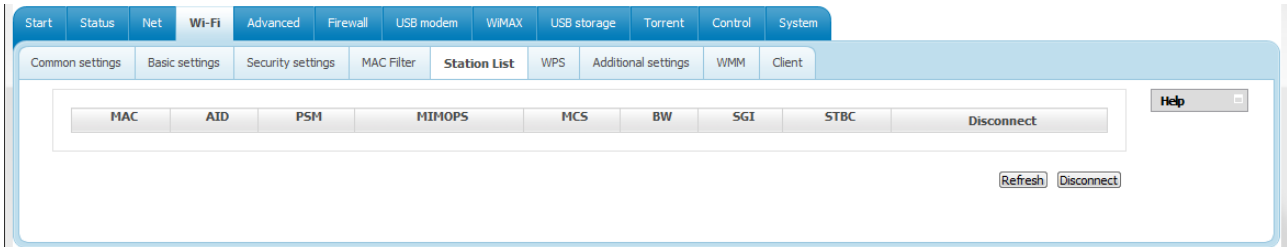


Figure 89. The list of the wireless clients.

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

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

WPS

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

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

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

! Before using the function you need to configure one of the following authentication types: **Open** with no encryption, **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** with the **AES** or **TKIP+AES** encryption method (on the **Wi-Fi / Security settings** page).

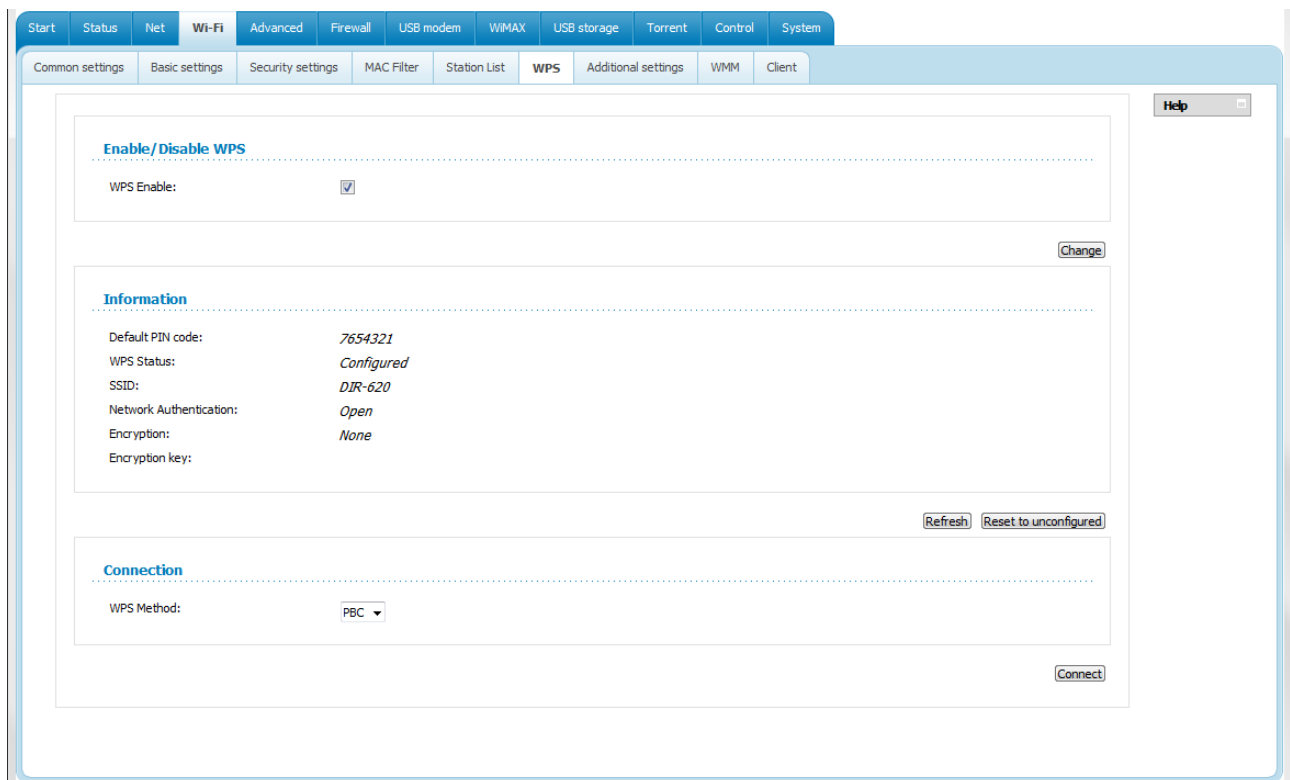


Figure 90. The page for configuring the WPS function.

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

| Parameter | Description |
|-------------------------------|--|
| Default PIN code | The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function. |
| WPS Status | The state of the WPS function: <ul style="list-style-type: none"> • Configured (all needed settings are specified) • Unconfigured (you need to specify the relevant settings). |
| SSID | The name of the 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 the first part of the WLAN). |
| Encryption | The encryption type specified for the WLAN (or the first part of the WLAN). |
| Encryption key | The encryption key specified for the WLAN (or the first part of the WLAN). |
| Refresh | Click the button to refresh the data on the page. |
| Reset to unconfigured | Click the button to reset the parameters of the WPS function. |
| WPS Method | A method of the WPS function. Select a value from the drop-down list. PIN : Connecting the device via the PIN code. PBC : Connecting the device via the push button (actual or virtual). |
| PIN Code | The PIN code of the WPS-enabled device that needs to be connected to the wireless network of the router. The field is displayed only when the PIN value is selected from the WPS Method drop-down list. |
| Connect | Click the button to connect the wireless device to the router's WLAN via the WPS function. |

Using WPS Function via Web-based Interface

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

1. Select the **WPS Enable** checkbox.
2. Click the **Change** button.
3. Select the **PIN** value from the **WPS Method** drop-down list.
4. Select the PIN method in the software of the wireless device that you want to connect to the router's WLAN.
5. Click the relevant button in the software of the wireless device that you want to connect to the WLAN.
6. Right after that, enter the PIN code specified on the cover of the wireless device or in its software in the **PIN Code** field.
7. Click the **Connect** button in the web-based interface of the router.

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

1. Select the **WPS Enable** checkbox.
2. Click the **Change** button.
3. Select the **PBC** value from the **WPS Method** drop-down list.
4. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
5. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
6. Click the **Connect** button in the web-based interface of the 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. Specify corresponding security settings for the wireless network of the router.
2. Select the **WPS Enable** checkbox.
3. Click the **Change** button.
4. Save the settings and close the web-based interface (click the **Save** line in the top-page menu displayed when the mouse pointer is over the **System** caption, then click the **Logout** line).

Later you will be able to add wireless devices to the WLAN by pressing the **WPS** button 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 press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
3. Press the **WPS** button of the 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.

Additional Settings

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

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

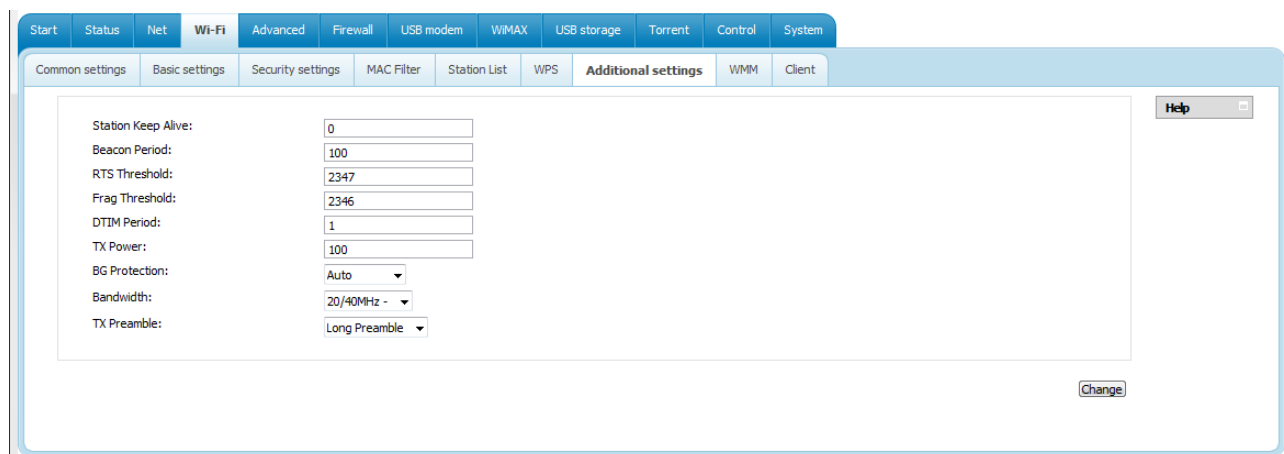


Figure 91. Additional settings of the WLAN.

The following fields are available on the page:

| Parameter | Description |
|---------------------------|--|
| Station Keep Alive | The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value 0 is specified, the checking is disabled. |
| Beacon Period | The time interval (in milliseconds) between packets sent to synchronize the wireless network. |
| RTS Threshold | The minimum size (in bites) of a packet for which an RTS frame is transmitted. |
| Frag Threshold | The maximum size (in bites) of a non-fragmented packet. Larger packets are fragmented (divided). |
| DTIM Period | The time period (in seconds) between sending a DTIM (a message notifying on broadcast or multicast transmission) and data transmission. |
| TX Power | The transmit power (in percentage terms) of the router. |

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

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

WMM

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

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

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

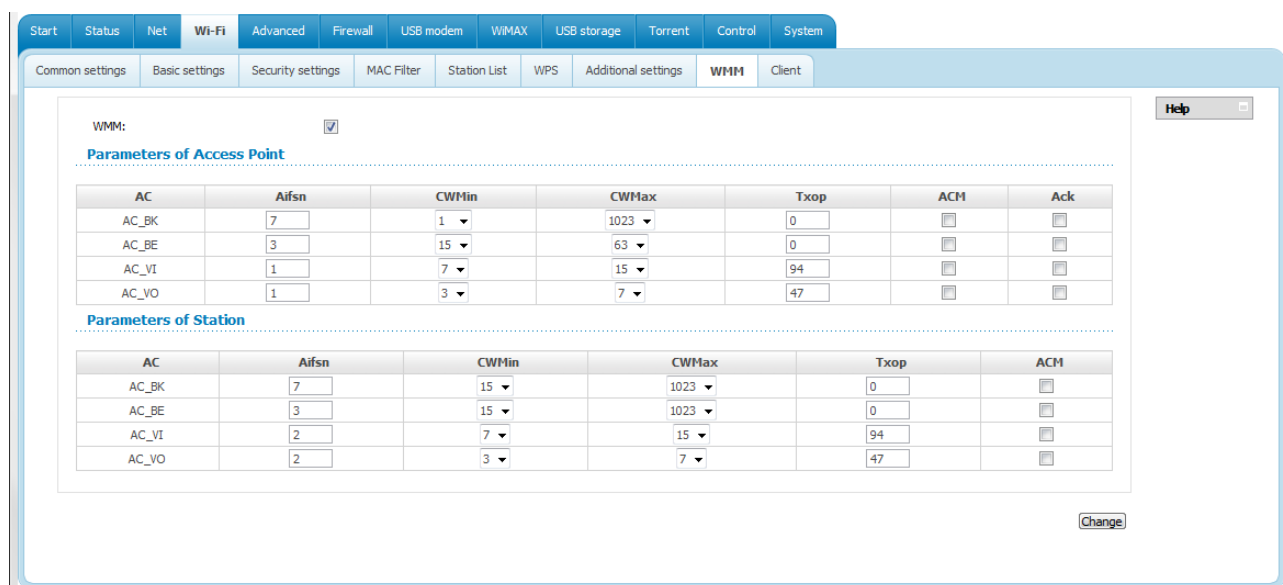


Figure 92. The page for configuring the WMM function.

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

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

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

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

For every Access Category the following fields are available:

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

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

Client

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

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

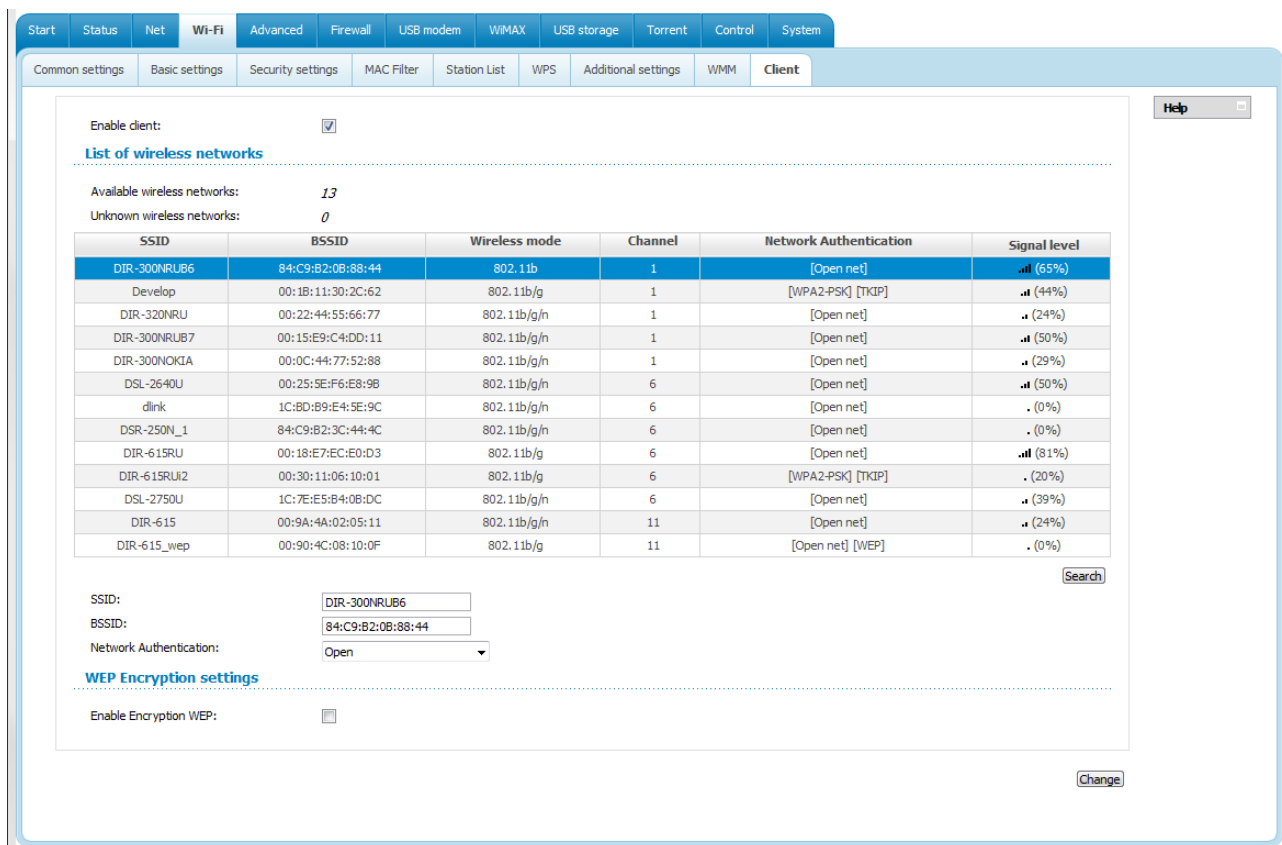


Figure 93. The page for configuring the client mode.

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

| Parameter | Description |
|-------------------------------|--|
| 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 WEP fields are displayed on the page. For the Shared authentication type the checkbox is always selected. |
| Default Key ID | The number of the key (from first to fourth) which will be used for WEP encryption. |
| Encryption Key WEP (1-4) | Keys for WEP encryption. The 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**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK mixed** authentication type is selected, the following fields are available:

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

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

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

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

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

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

For the **Open** authentication type with encryption and the **Shared** authentication type, select a needed value from the **Default Key ID** drop-down list, fill in 4 **Encryption Key WEP** fields, and click the **Change** button.

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

After clicking the **Change** button, the wireless channel of DIR-620 will switch to the channel of the wireless access point to which you have connected.

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

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

Advanced

In this menu you can configure advanced settings of the router:

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

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

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

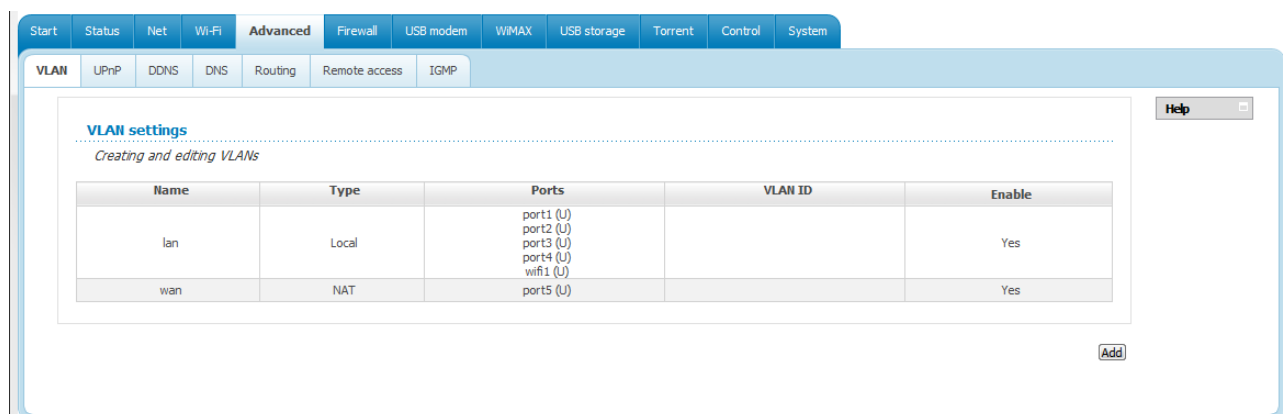


Figure 94. The **Advanced / VLAN** page.

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

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

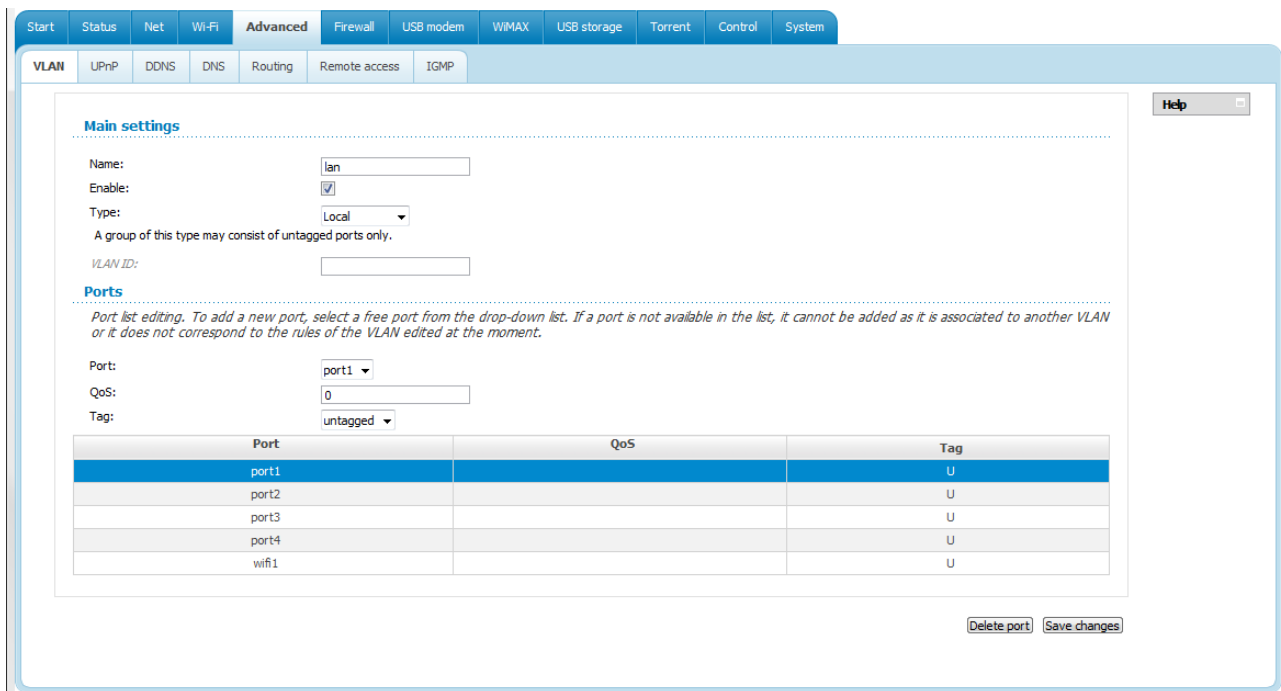


Figure 95. The page for editing a group of ports for VLAN.

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 | <p>The type of the VLAN which identifier is specified in the VLAN ID field.</p> <p>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.</p> <p>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 (on the Net / WAN page).</p> <p>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.</p> |
| VLAN ID | An identifier of the VLAN to which this group of ports will be assigned. |

| Parameter | Description |
|--------------|---|
| Ports | |
| Port | From the list, select an available value (a physical port of the router, the wireless interface, or, if the wireless network is splitted into parts, a part of the wireless network) to assign it to this group. The port will be displayed in the table at the bottom of the page. |
| 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: <ul style="list-style-type: none">• 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.

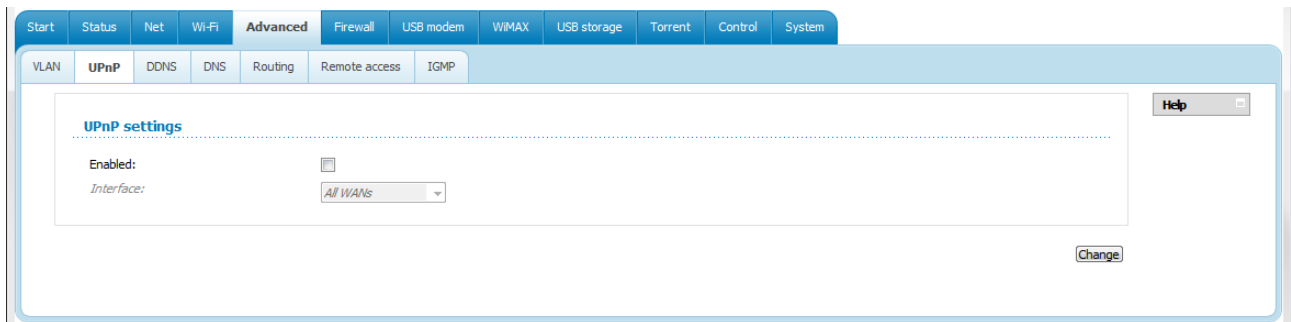


Figure 96. The **Advanced / UPnP** page.

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

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

DDNS

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

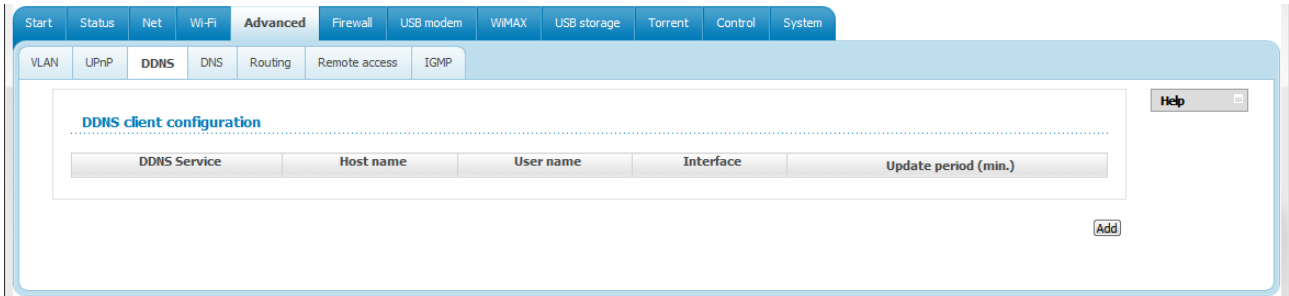


Figure 97. The **Advanced / DDNS** page.

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

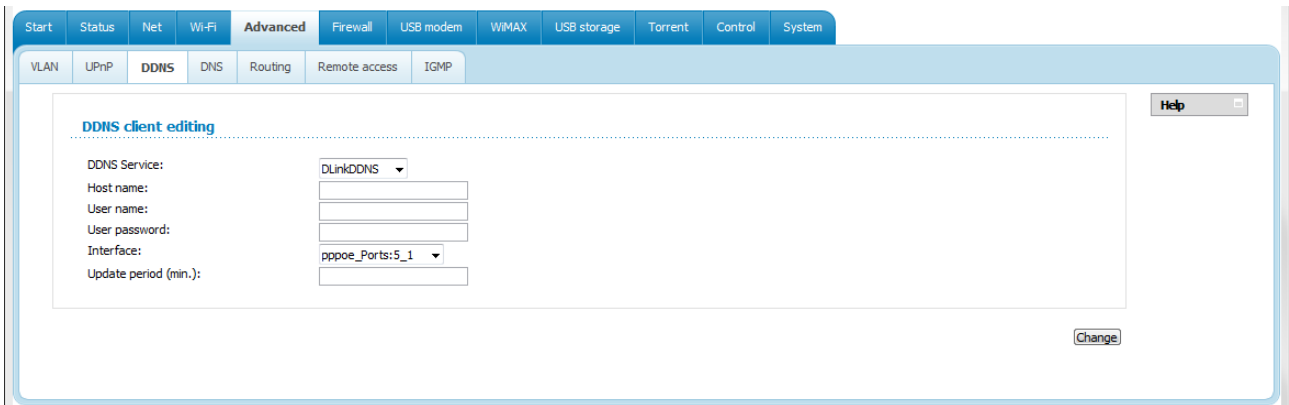


Figure 98. The page for adding a DDNS service.

You can specify the following parameters:

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

Click the **Change** button.

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

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

DNS

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

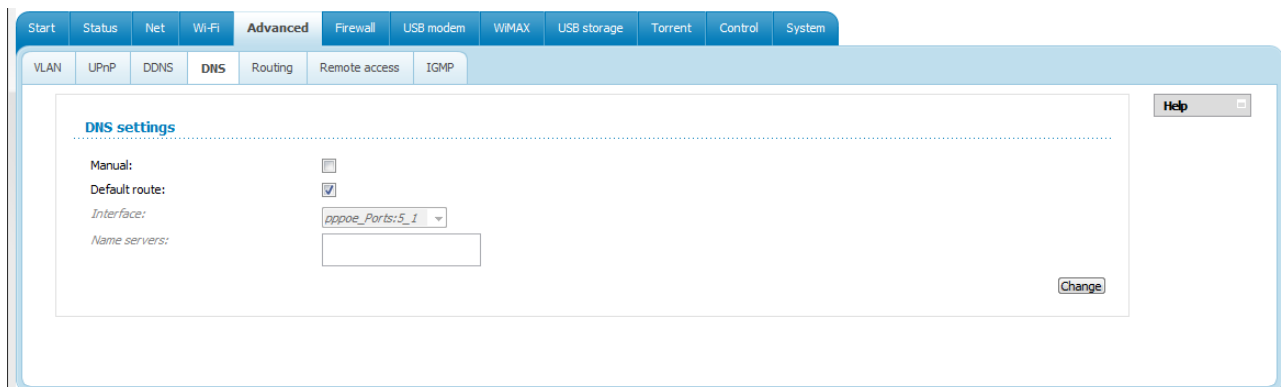


Figure 99. The **Advanced / DNS** page.

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 / WAN** page) to obtain DNS server addresses, and click the **Change** button.

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

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

Routing

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

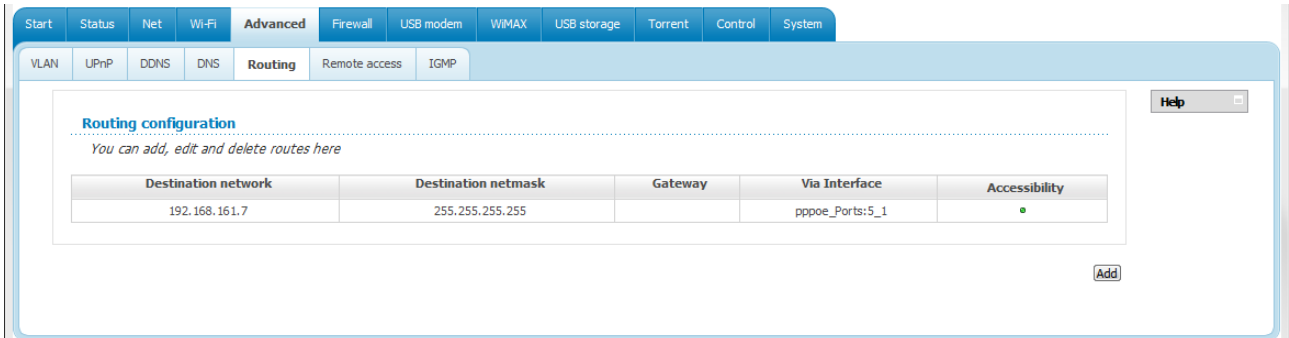


Figure 100. The **Advanced / Routing** page.

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

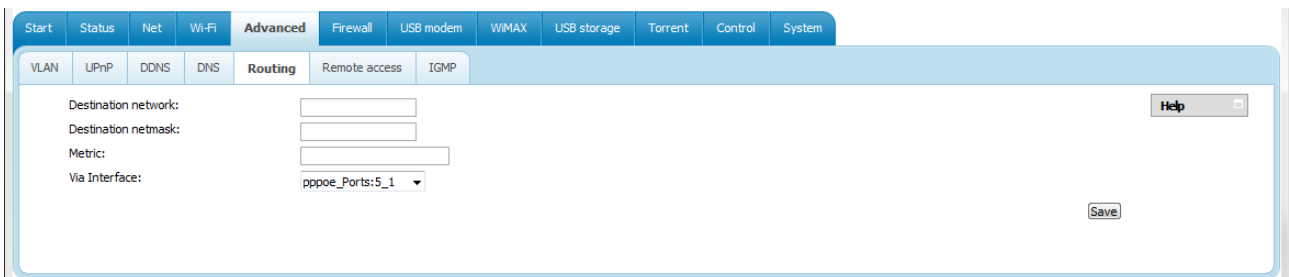


Figure 101. The page for adding a static route.

You can specify the following parameters:

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

Click the **Save** button.

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

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

Remote Access

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

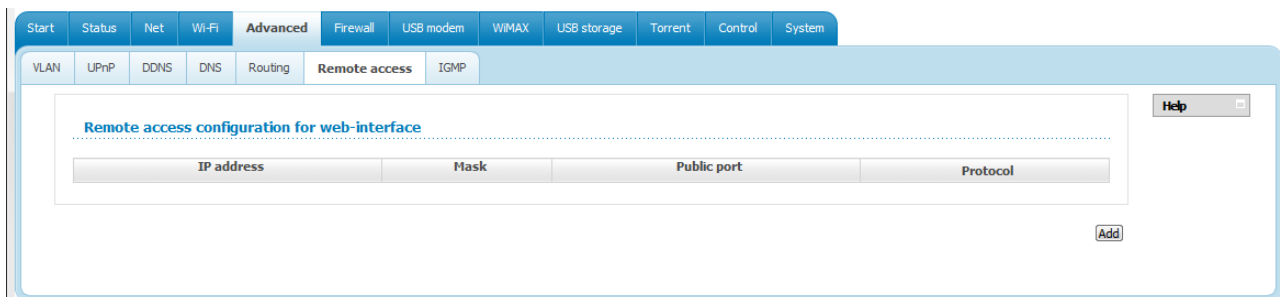


Figure 102. The **Advanced / Remote access** page.

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



Figure 103. The page for adding a rule for remote management.

You can specify the following parameters:

| Parameter | Description |
|--------------------|---|
| IP address | A host or a subnet to which the rule is applied. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically). |
| 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.

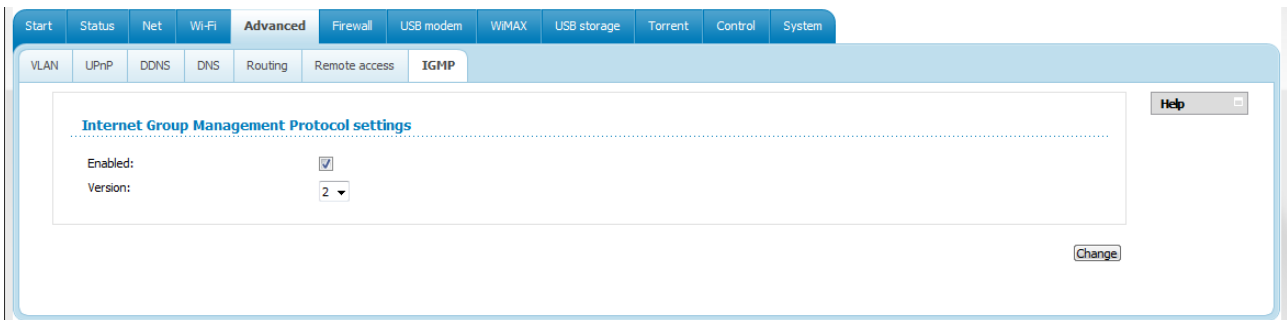


Figure 104. The **Advanced / IGMP** page.

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
- create virtual servers
- define a DMZ
- configure the MAC filter.

IP Filters

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

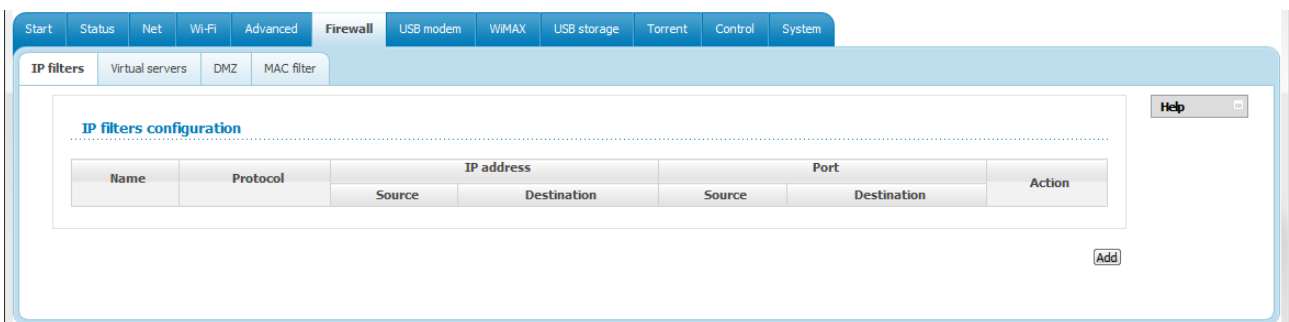


Figure 105. The **Firewall / IP filters** page.

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

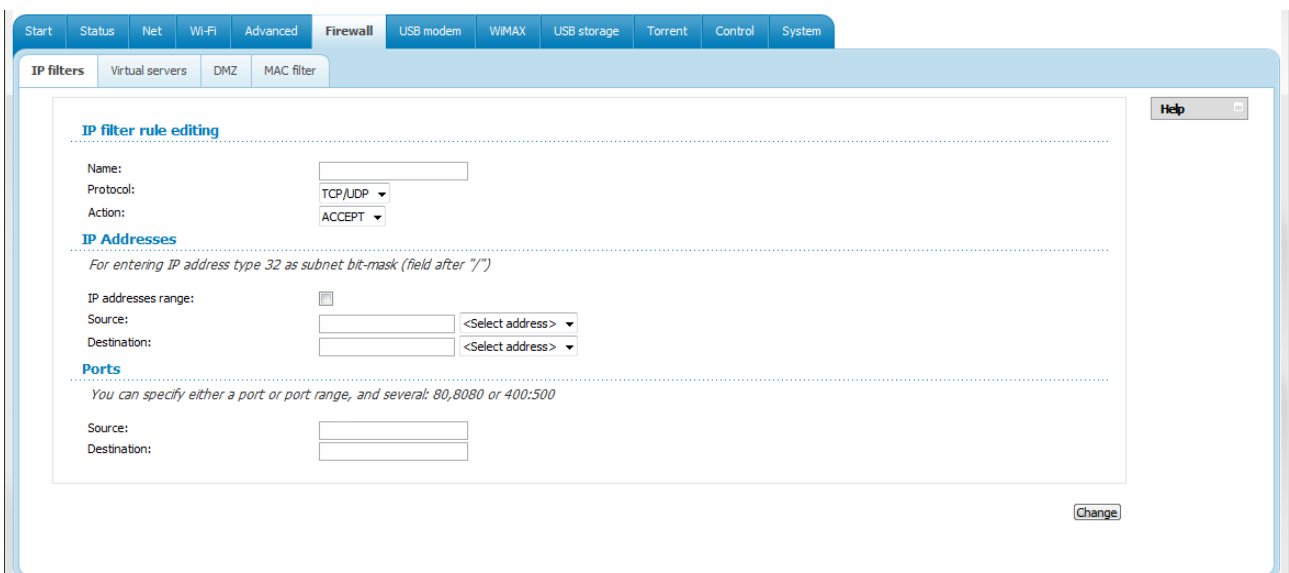


Figure 106. The page for adding a rule for IP filtering.

You can specify the following parameters:

| Parameter | Description |
|-------------------------------|--|
| IP filter rule editing | |
| Name | A name for the rule for easier identification. |
| Protocol | A protocol for network packet transmission. Select a value from the drop-down list. |
| Action | Select an action for the rule. ACCEPT: Allows packet transmission in accordance with the criteria specified by the rule. DROP: Denies packet transmission in accordance with the criteria specified by the rule. |
| IP Addresses | |
| IP address range | Select the checkbox if you want to specify a range of IP addresses as the source or destination IP address. |
| Source | The source host/subnet IP address. If the IP address range checkbox is selected, specify the starting IP address of the range in the Source (first) field and the ending IP address in the Source (last) field. If the IP address range checkbox is not selected, specify the IP address of the host or subnet in the Source field. To specify an IP address add <code>/32</code> . To choose a device connected to the router's LAN at the moment, select the relevant IP address from the drop-down list located to the right of the field (the field will be filled in automatically). |
| Destination | The destination host/subnet IP address. If the IP address range checkbox is selected, specify the starting IP address of the range in the Destination (first) field and the ending IP address in the Destination (last) field. If the IP address range checkbox is not selected, specify the starting IP address of the host or subnet in the Destination field. To specify an IP address add <code>/32</code> . To choose a device connected to the router's LAN at the moment, select the relevant IP address from the drop-down list located to the right of the field (the field will be filled in automatically). |

| 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.



Figure 107. The **Firewall / Virtual servers** page.

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

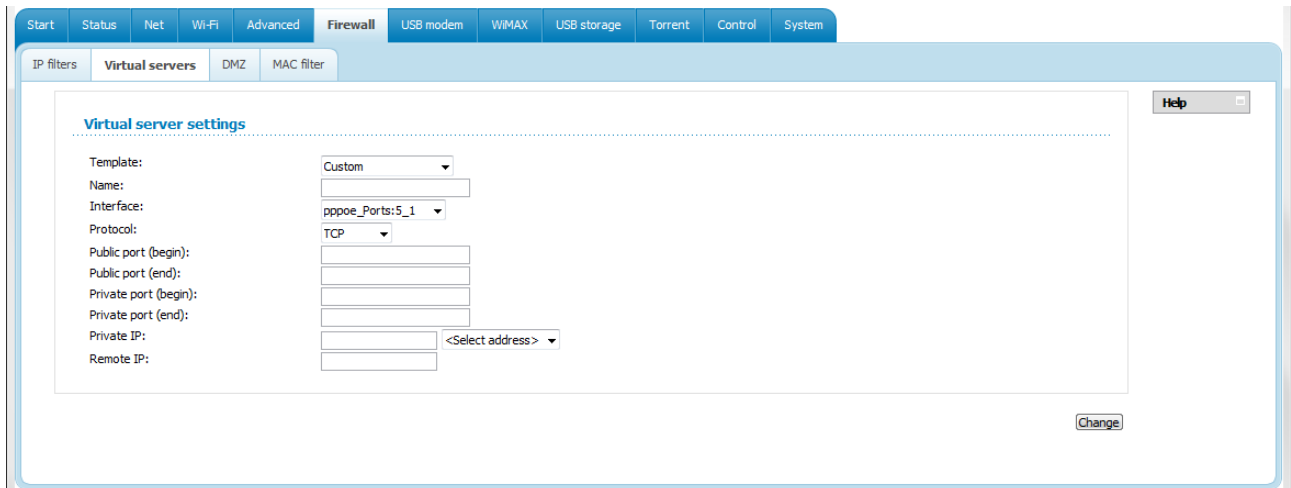


Figure 108. The page for adding a virtual server.

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. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list located to the right of the Private IP field (the field will be filled in automatically). |
| Remote IP | The IP address of the server from the external network. |

Click the **Change** button.

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

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

DMZ

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

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

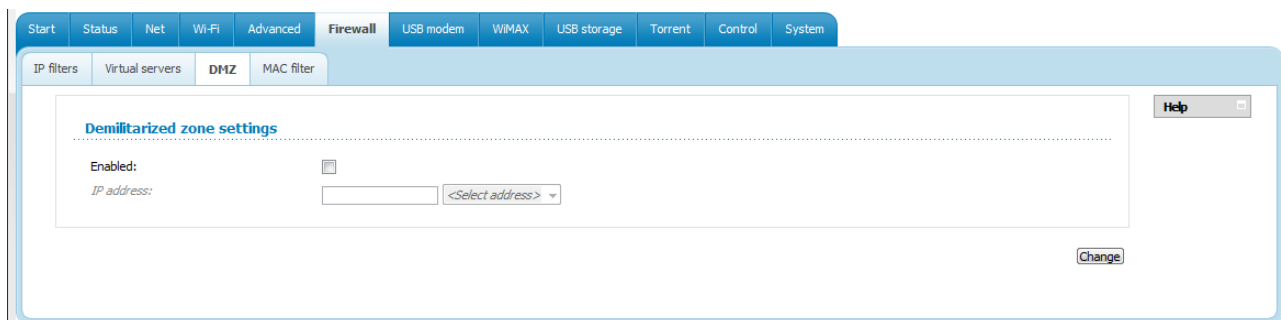


Figure 109. The **Firewall / DMZ** page.

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

Note that when the DMZ is enabled, all traffic coming to a port of the WAN interface of the router is directed to the same port of the specified IP address. Also note that virtual servers have higher priority than the DMZ host. In other words, if there has been created a virtual server that directs traffic from external port 80 to a port of the device from the router's local network, then entering **http://router_WAN_IP** in the address bar, users of the external network are directed to the specified port and IP address configured for the virtual server, but not to port 80 of the device with the IP address specified on the **Firewall / DMZ** page.

To disable the DMZ, deselect the **Enabled** checkbox and click the **Change** button.

MAC Filter

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

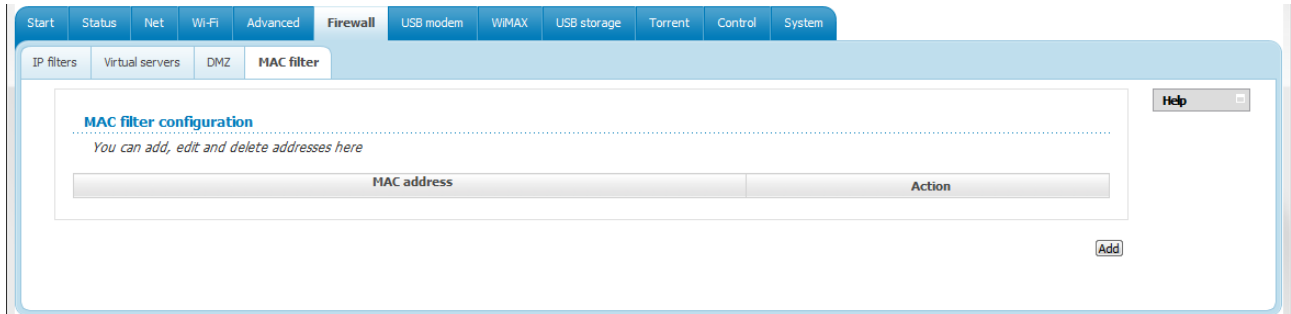


Figure 110. The **Firewall / MAC filter** page.

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

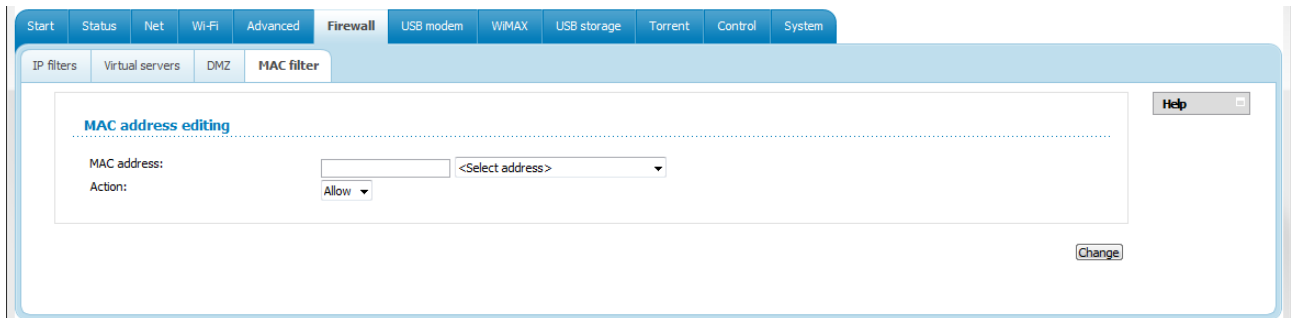


Figure 111. The page for adding an address for the MAC filter.

On the opened page, enter the MAC address of the device from the router's LAN in the **MAC address** field. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list located to the right of the field (the field will be filled in automatically). Then select the **Deny** value from the **Action** drop-down list and click the **Change** button.

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

USB Modem

This menu is designed to operate USB modems.

If the PIN code check for the SIM card inserted into your USB modem is not disabled, then upon the first access to the pages of the **USB modem** menu (under the current web-interface session) the page for checking the PIN code is displayed⁶. Enter the PIN code in the relevant field and click the **Enter** button.

Information

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

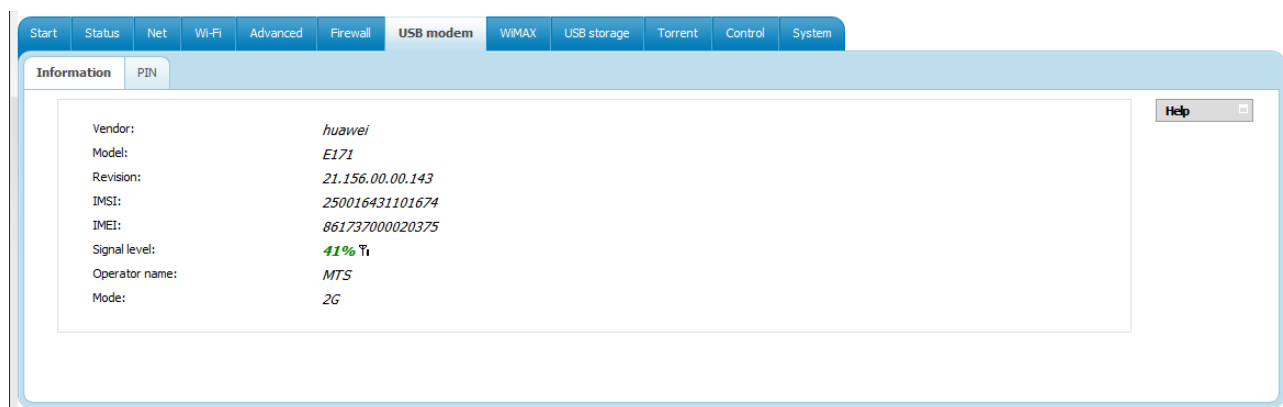


Figure 112. The **USB modem / Information** page.

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

| Parameter | Description |
|----------------------|--|
| Vendor | The manufacturer of your USB modem. |
| Model | The alphanumeric code of the model of your USB modem. |
| Revision | The revision of the firmware of your USB modem. |
| IMSI | The code stored in the SIM card inserted to your USB modem. |
| IMEI | The code stored in the memory of the 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 selected operator's network. |
| Operator name | When the needed network is available, the name of the operator is displayed in this field. |

⁶ For GSM USB modems only. For CDMA USB modems, it is required to disable the PIN code check on the identification card prior to connecting the USB modem to the router.

| Parameter | Description |
|-------------|---|
| Mode | A type of the network to which the USB modem is connected (2G or 3G). |

PIN

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

! The operations presented on this page are not available for CDMA USB modems.

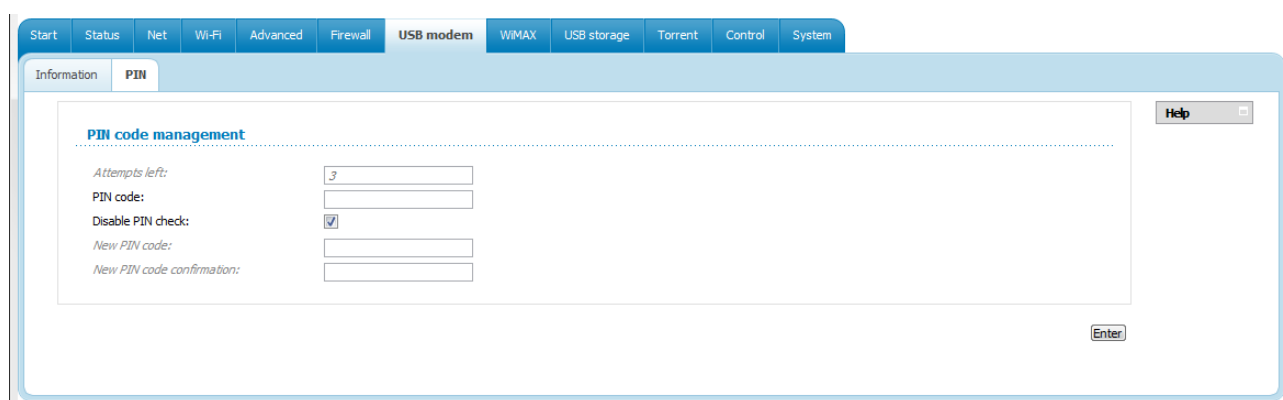


Figure 113. The **USB modem / PIN** page.

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 **Enter** button.

To enable the PIN code check, deselect the **Disable PIN check** checkbox, enter the PIN code, used before disabling the check, in the **PIN code** field and click the **Enter** button.

To change the PIN code, enable the PIN code check, enter the current code in the **PIN code** field, then enter a new code in **New PIN code** and **New PIN code confirmation** fields and click the **Enter** button.

If upon 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 USB modem is blocked.

 **PIN code management**

| | |
|----------------------------|---------------------------------------|
| Attempts left: | <input type="text" value="10"/> |
| PUK code: | <input type="text" value="59685477"/> |
| Disable PIN check: | <input type="checkbox"/> |
| New PIN code: | <input type="text" value="5285"/> |
| New PIN code confirmation: | <input type="text" value="5285"/> |

Figure 114. Entering the PUK code.

For further use of the card, enter the PUK code in the relevant field, and then specify a new PIN code for your SIM card in the **New PIN code** and **New PIN code confirmation** fields. Click the **Enter** 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.

The screenshot shows a web interface for WiMAX configuration. It includes the following fields and values:

- SSID: [Empty text input field]
- Diode on modem:
- Link status: ●
- MAC-address: 00:24:91:3b:71:aX
- RSSI: -78 dB \Uparrow
- CINR: 9.00 dBm
- Base station ID: 00:00:15:0e:26:c9
- Transmit power: -81.92
- Frequency: 2515000

At the bottom right of the form area, there is a button labeled "Disconnect".

Figure 115. 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. |
| 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. |

| Parameter | Description |
|-------------------|---|
| Connect | Click the button to connect to the WiMAX network. Beforehand, you need to create a WAN connection with relevant parameters. <i>The button is displayed when the connection is not established.</i> |
| Disconnect | Click the button to disconnect from the WiMAX network. <i>The button is displayed when the connection is established or is being established.</i> |

To save the values of the **SSID** and **Diode on modem** field, click the **Connect** button.

USB Storage

This menu is designed to operate USB storages. Here you can do the following:

- view data on the connected USB storage
- view content of the connected USB storage and configure access to it
- enable the built-in FTP server of the router
- create accounts for users to allow access to the content of the USB storage.

Information

On the **USB storage / Information** page, you can view data on the USB storage connected to the router.

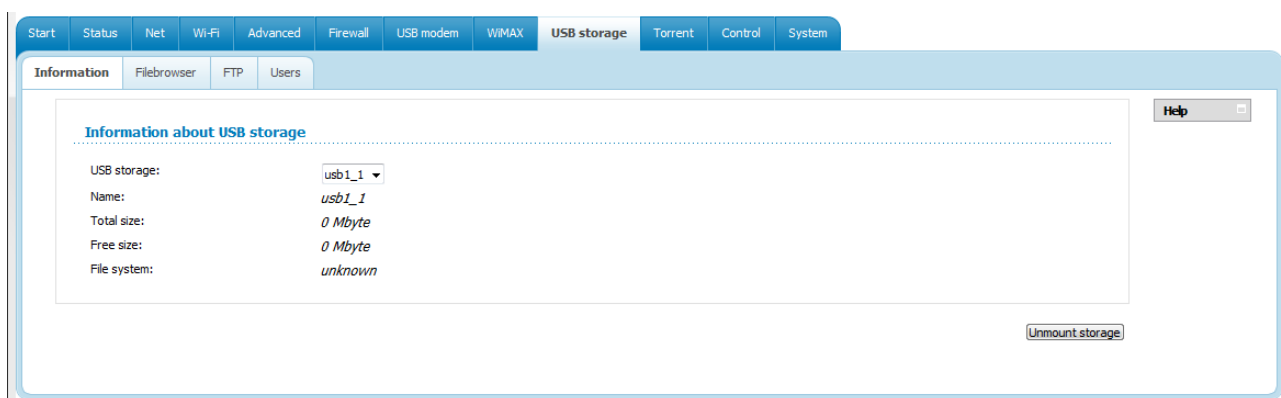


Figure 116. The **USB storage / Information** page.

The following data are presented on the page: the name, total and free space of the storage, and the type of its file system.

If the USB storage is divided into volumes, several values are displayed in the **USB storage** drop-down list. Select the needed value to view data on the volume (partition) of the USB storage.

To safely disconnect the USB storage, click the **Unmount storage** button. When the **No** value is displayed in the **USB storage** drop-down list, remove the storage from the router.

To disconnect one volume of the storage, select the needed value from the **USB storage** drop-down list and click the **Unmount volume** button.

Filebrowser

On the **USB storage / Filebrowser** page, you can view the content of your USB storage connected to the router and remove separate folders and files from the USB storage.

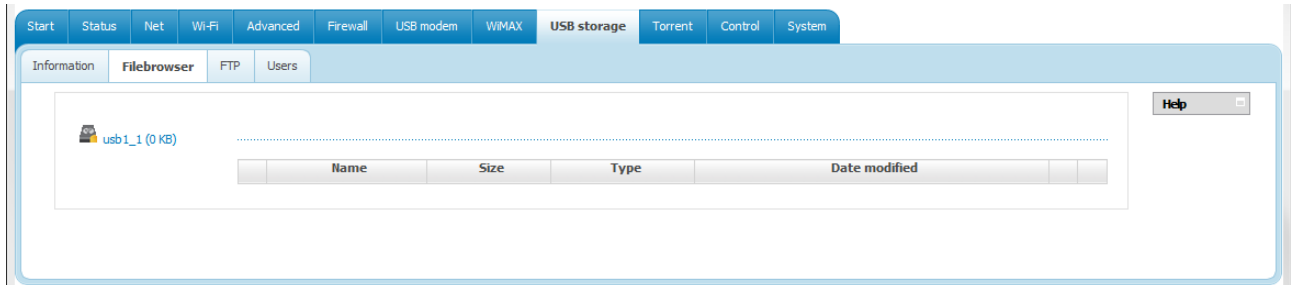


Figure 117. The **USB storage / Filebrowser** page.

To view the content of the USB storage, click the link with the name of the storage or storage partition. The list of folders and files will be displayed on the page.

To proceed to a folder, select it in the directory structure on the left part of the page.

To remove a folder or file, click the **delete** link in the line corresponding to this folder or file.

For content of ext2 or ext3 storages or storage partitions, the **Change rule** link is displayed on the page. Click the link and in the opened window select a user to which you allow access to this folder or file. Then click the **Apply** button.

FTP

On the **USB storage / FTP** page, you can enable the built-in FTP server of the router to provide access to the USB storage for users of your LAN.

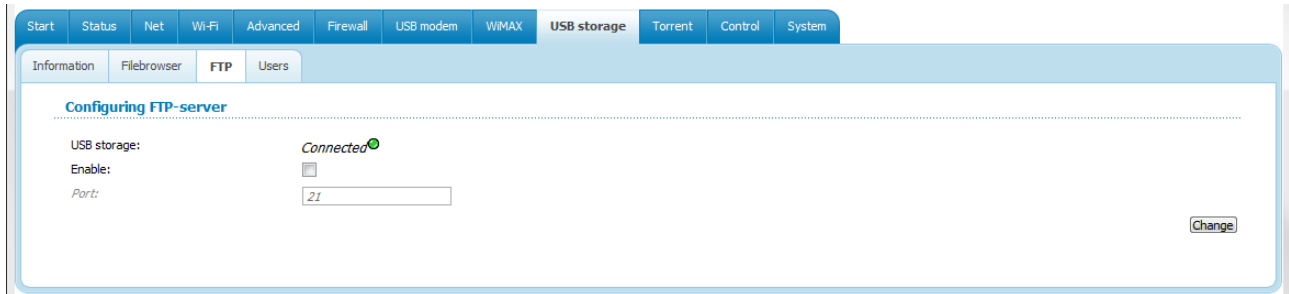


Figure 118. The **USB storage / FTP** page.

You can enable the FTP server only when a USB storage is connected to the router (in this case, the **Connected** value is displayed in the **USB storage** field). Select the **Enable** checkbox; if needed, change the router's port used by the FTP server in the **Port** field (by default, the standard port **21** is specified). Then click the **Change** button.

To allow access to the content of the USB storage for users of your LAN, proceed to the **USB storage / Users** page and create needed accounts.

To disable the built-in FTP server of the router, deselect the **Enable** checkbox and click the **Change** button.

Users

On the **USB storage / Users** page, you can create user accounts to provide access to data on the USB storage connected to the router.

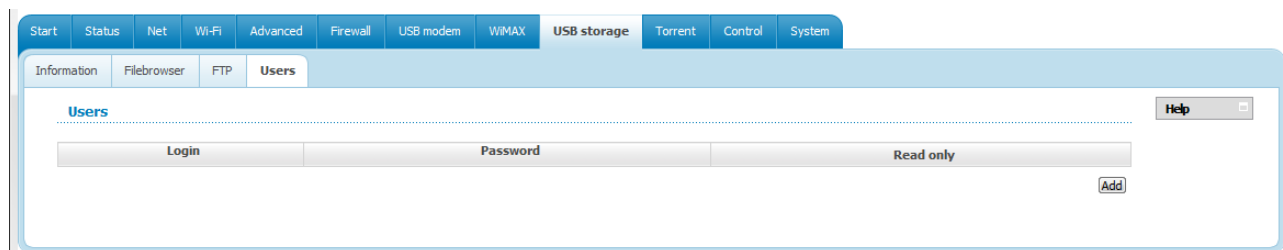


Figure 119. The **USB storage / Users** page.

To create a new user account, click the **Add** button.

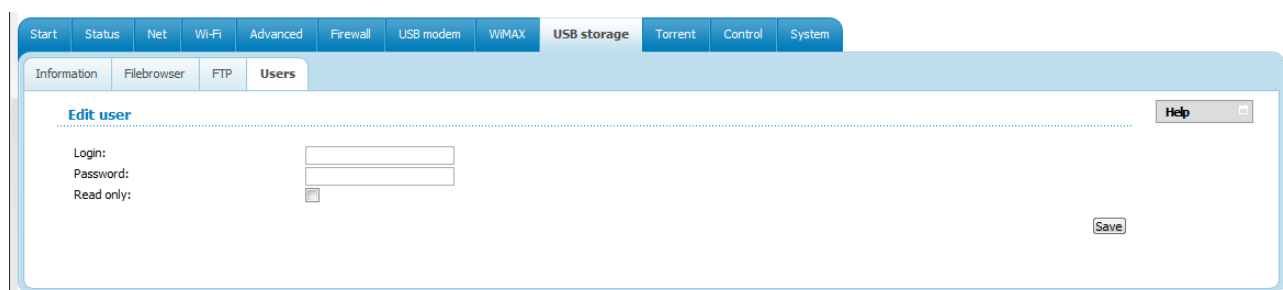


Figure 120. The page for adding a user.

On the opened page, specify a username and password for the account in the relevant fields. You can use letters of the Latin and Russian alphabets (uppercase and/or lowercase) and digits.

! You cannot create accounts with the following usernames: ftp, admin, support, user, nobody.

To change the password of an account, select the relevant line in the table. On the opened page, enter a new value in the **Password** field and click the **Save** button.

To delete an account, select a relevant line in the table. On the opened page, click the **Delete** button.

For ext2 or ext3 storages or storage partitions, it is possible to create users with limited rights. Select the **Read only** checkbox not to let the user create, change, or delete files.

In addition, by default, users with accounts from this page cannot access ext2 or ext3 storages or storage partitions. To configure access, it is necessary to proceed to the **USB storage / Filebrowser** page and assign relevant rights.

Torrent

In this menu you can configure the built-in torrent client and manage distributing and downloading processes.

Torrent-client

On the **Torrent / Torrent-client** page, you can add new torrent files to the system, start and stop downloading files to the USB storage connected to the router, and view data on the files that are being downloaded.

To add a new torrent file, click the **Choose/Browse**⁷ button on the **Add new** tab and select a file stored on your PC. Select the **Run after adding** checkbox to start downloading right after adding the torrent file. Then click the **Add file** button.

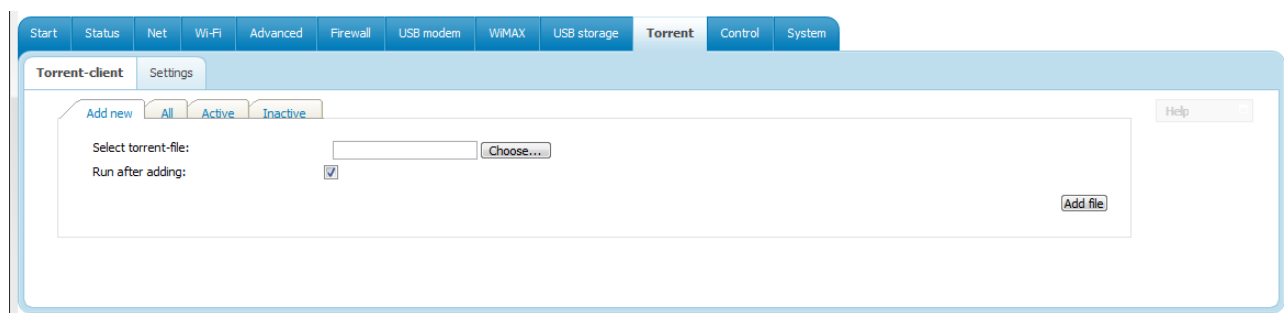


Figure 121. The **Torrent / Torrent-client** page. The **Add new** tab.

The **All**, **Active**, and **Inactive** tabs are designed for managing the files that are being downloaded and view data on them. On the tabs, you can start downloading for all files presented on the tab (click the **Start all** button), stop downloading (click the **Stop all** button), or delete all files presented on the tab (click the **Delete all** button).

To view data on a file, select it in the list on the relevant tab.

To start or stop downloading, click the **Start/Stop** button.

To remove a file (torrent) from the USB storage, click the **Delete** button.

To close the file data and return to the list, click the **Back to list** button.

⁷ The name of the button depends upon the web browser that you use.

Settings

On the **Torrent / Settings** page, you can configure the built-in torrent client.

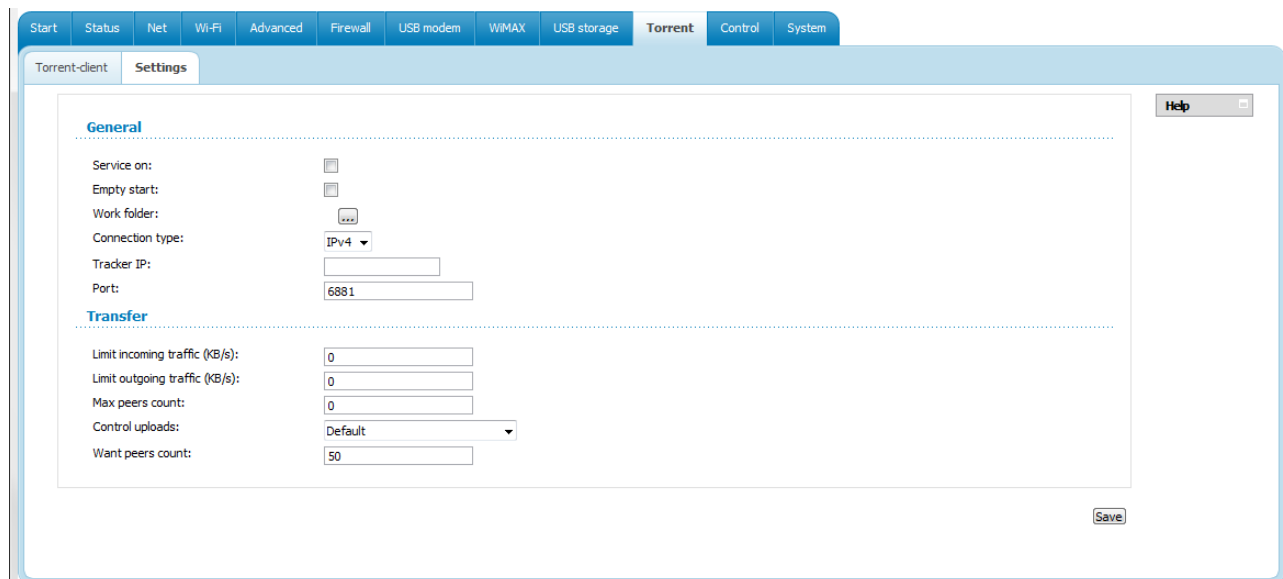


Figure 122. The **Torrent / Settings** page.

You can specify the following parameters:

| Parameter | Description |
|-------------------------------|--|
| General | |
| Service on | Select the checkbox to start the torrent client. If the checkbox is not selected, you cannot download files and view contents of the tabs from the Torrent / Torrent-client page. |
| Empty start | Select the checkbox to forbid the torrent client to renew downloading files upon its start. |
| Work folder | Select the USB storage folder to which the files that are being downloaded will be saved. |
| Connection type | Select a version of the Internet Protocol which will be used for downloading and transmitting files. |
| Tracker IP | In the field, you can specify the IP address of the preferred tracker. |
| Port | Enter the port of the router which will be used by the torrent client. By default, the standard port is specified (6881). |
| Transfer | |
| Limit incoming traffic | Specify the maximum rate for downloading files. |
| Limit outgoing traffic | Specify the maximum rate for uploading files. |

| Parameter | Description |
|-------------------------|--|
| Max peers count | Specify the maximum number of the torrent service users from which you can download files. |
| Control uploads | Select a way for uploading files to other users: Default: uploading is not limited. Upload to every interested peer. Don't upload. Set peers count: when this value is selected, the Max upload peers field is displayed. |
| Want peers count | Specify the desired number of the torrent service users from which you can download files. |

After specifying the needed parameters, click the **Save** button. After that the torrent client will be restarted in accordance with the specified settings.

Control

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

URL Filter

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



Figure 123. The **Control / URL filter** page. The **Configuration** tab.

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

- **Block listed URLs:** when this value is selected, the router blocks access to all addresses specified on the **URL addresses** tab;
- **Block all URLs except listed:** when this value is selected, the router allows access to addresses specified on the **URL addresses** tab and blocks access to all other web sites.

Click the **Change** button.

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

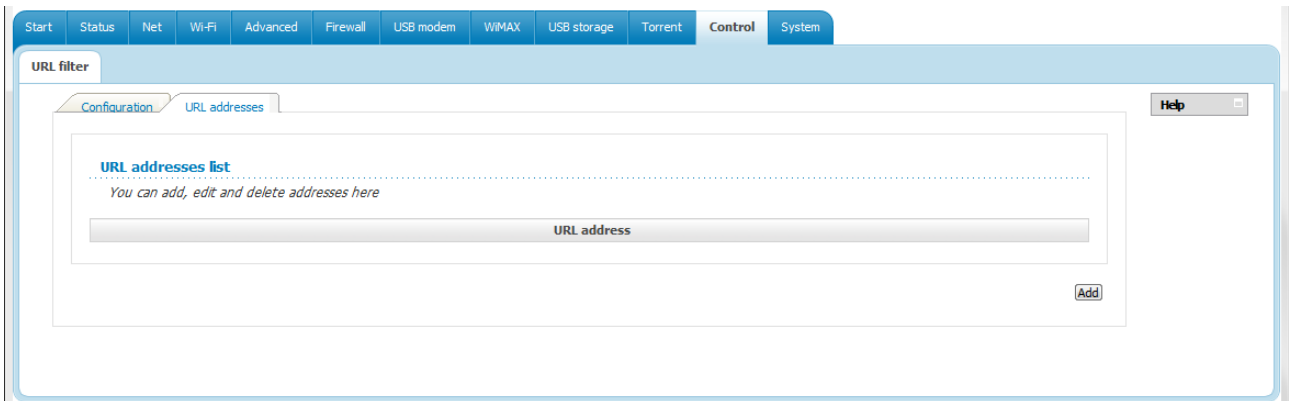


Figure 124. The **Control / URL filter** page. The **URL addresses** tab.

On the opened page, specify the needed parameters.

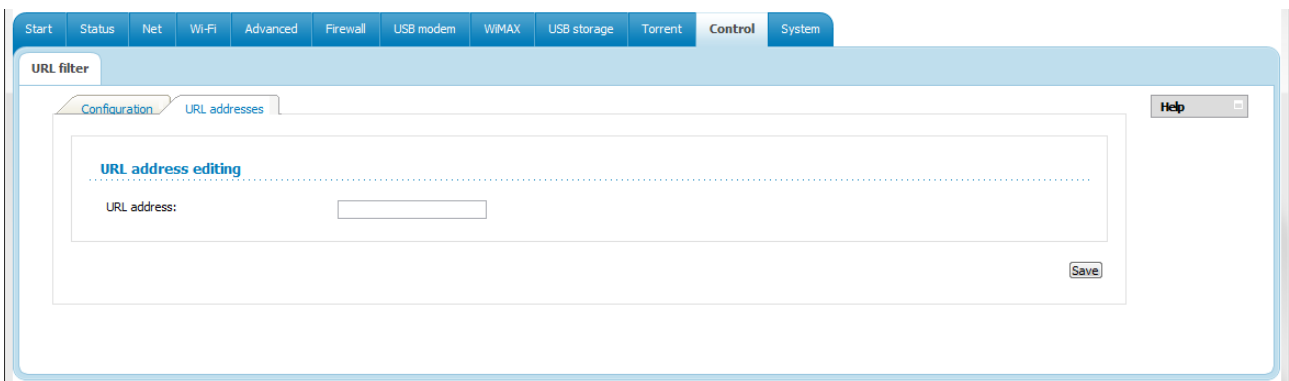


Figure 125. The page for adding an address for the URL filter.

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

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

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

System

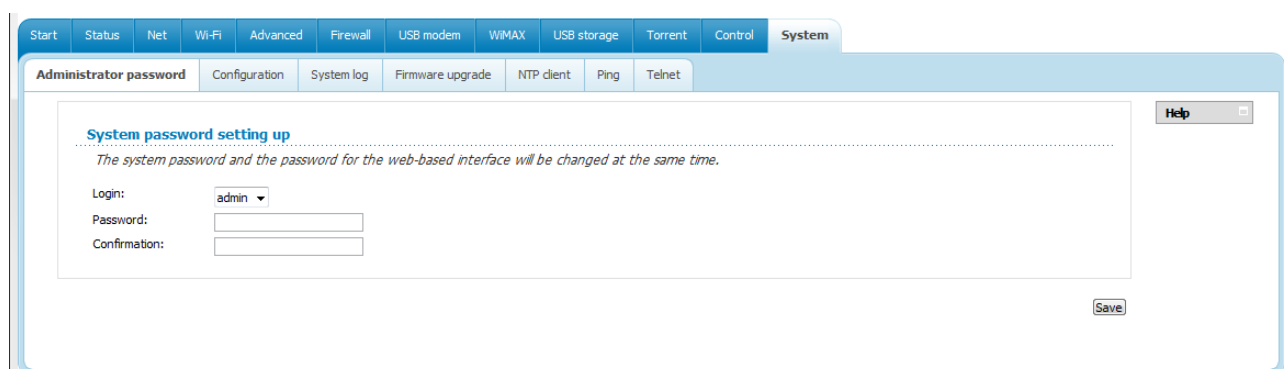
In this menu you can do the following:

- change the password used to access the router's settings
- 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
- update the firmware of the router
- configure automatic synchronization of the system time
- check availability of a host on the Internet through the web-based interface of the router
- allow or forbid access to the router via TELNET.

Administrator Password

On the **System / Administrator password** page, you can change the password for the administrator account used to access the web-based interface of the router and to access the device settings via TELNET.

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



The screenshot shows the 'Administrator password' page in the router's web-based interface. The page has a blue header with navigation tabs: Start, Status, Net, Wi-Fi, Advanced, Firewall, USB modem, WiMAX, USB storage, Torrent, Control, and System. Below the header, there are sub-tabs: Administrator password, Configuration, System log, Firmware upgrade, NTP client, Ping, and Telnet. The main content area is titled 'System password setting up' and contains the following text: 'The system password and the password for the web-based interface will be changed at the same time.' Below this text, there are three input fields: 'Login:' with a dropdown menu showing 'admin', 'Password:', and 'Confirmation:'. A 'Save' button is located at the bottom right of the form area. A 'Help' button is also visible in the top right corner of the main content area.

Figure 126. The page for modifying the administrator password.

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

Configuration

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

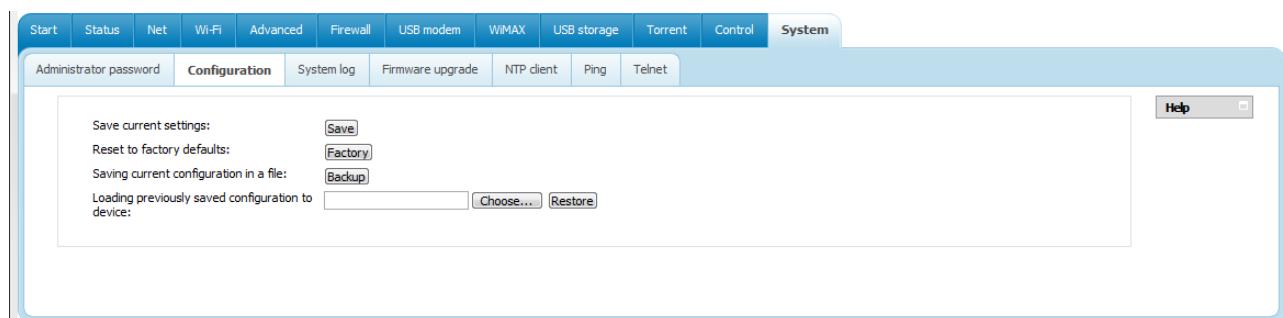


Figure 127. The **System / Configuration** page.

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 <i>Saving and Restoring Settings</i> section, page 31). |
| Backup | Click the button and follow the dialog box appeared to save the configuration (all settings of the router) to your PC. |
| 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 ⁸ button to select a previously saved configuration file located on your PC. |

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

⁸ The name of the button depends upon the web browser that you use.

System Log

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



Figure 128. The **System / System log** page. The **Configuration** tab.

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

| Control | Description |
|----------------------------|---|
| Logging type | <p>Select a type of logging from the drop-down list.</p> <ul style="list-style-type: none"> • Local: the system log is stored in the router's memory (and displayed on the Log tab). When this value is selected, the Server address type, Server, and Port fields are not displayed. • Remote: the system log is sent to the remote host specified in the Server field. • Local and remote: the system log is stored in the router's memory (and displayed on the Log tab) and sent to the remote host specified in the Server field. |
| Logging level | Select a type of messages and alerts/notifications to be logged. |
| Server address type | From the drop-down list, select the IP value to specify an IP address of a host from the local or global network, or the URL value to specify a URL address of a remote server. |
| Server | The IP or URL address of the host from the local or global network, to which the system log will be sent. |
| Port | A port of the host specified in the Server field. By default, the value 514 is specified. |

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

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

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

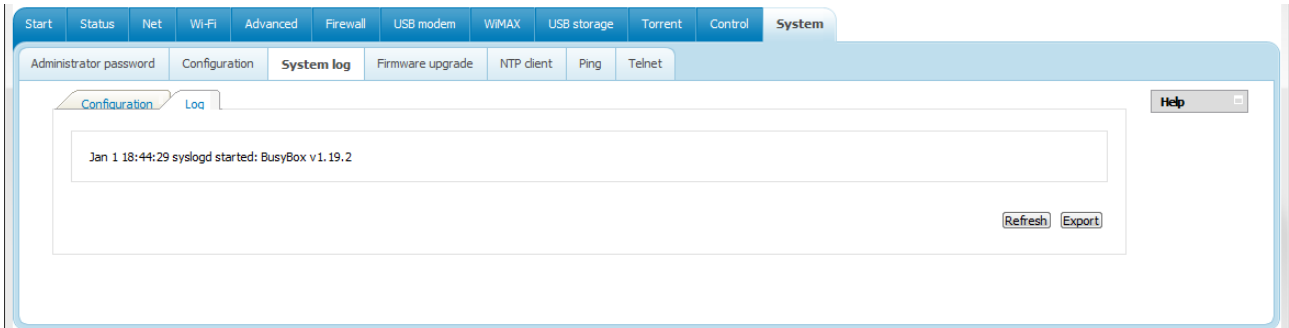


Figure 129. The **System / System log** page. The **Log** tab.

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

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

Firmware Upgrade

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

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

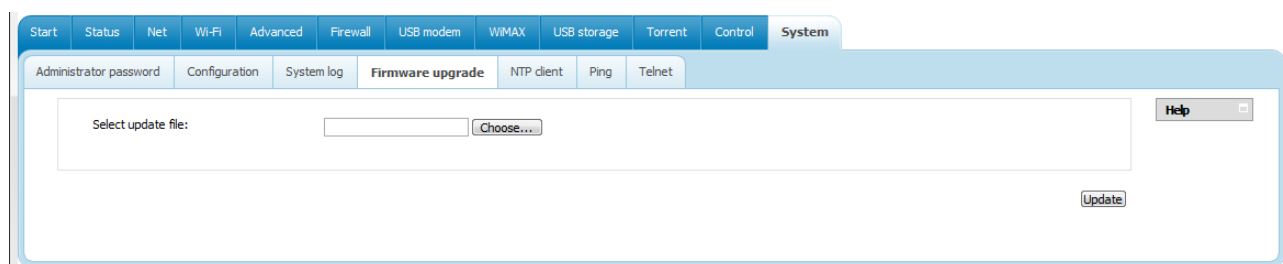


Figure 130. The **System / Firmware upgrade** page.

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

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

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **Choose/Browse**⁹ button on the **System / Firmware upgrade** page to locate the new firmware file.
3. Click the **Update** button to upgrade the firmware of the router.
4. Wait until the router is rebooted (about one and a half or two minutes).
5. Log into the web-based interface using the login (**admin**) and the current password.
6. Select the **Factory** line in the top-page menu displayed when the mouse pointer is over the **System** caption.
7. Wait until the router is rebooted. Log into the web-based interface, using the default IP address, login and password (**192.168.0.1**, **admin**, **admin**).

⁹ The name of the button depends upon the web browser that you use.

NTP Client

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

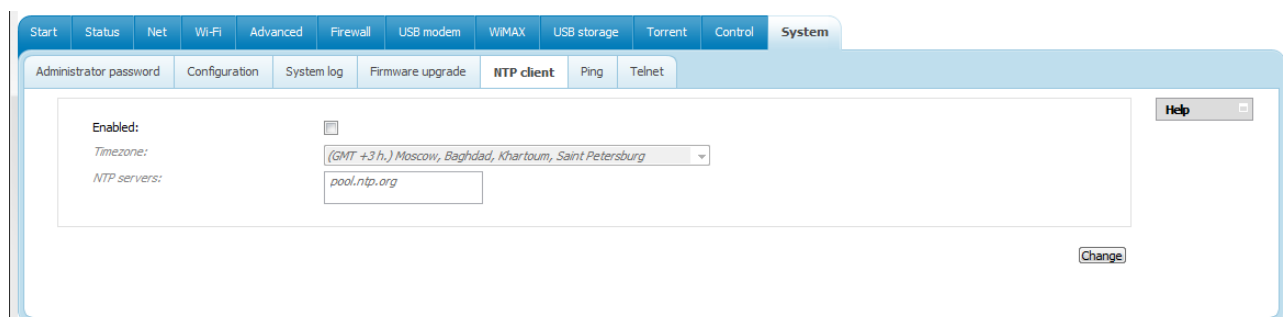


Figure 131. The **System / NTP client** page.

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 a host from the local or global network via the Ping utility.

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

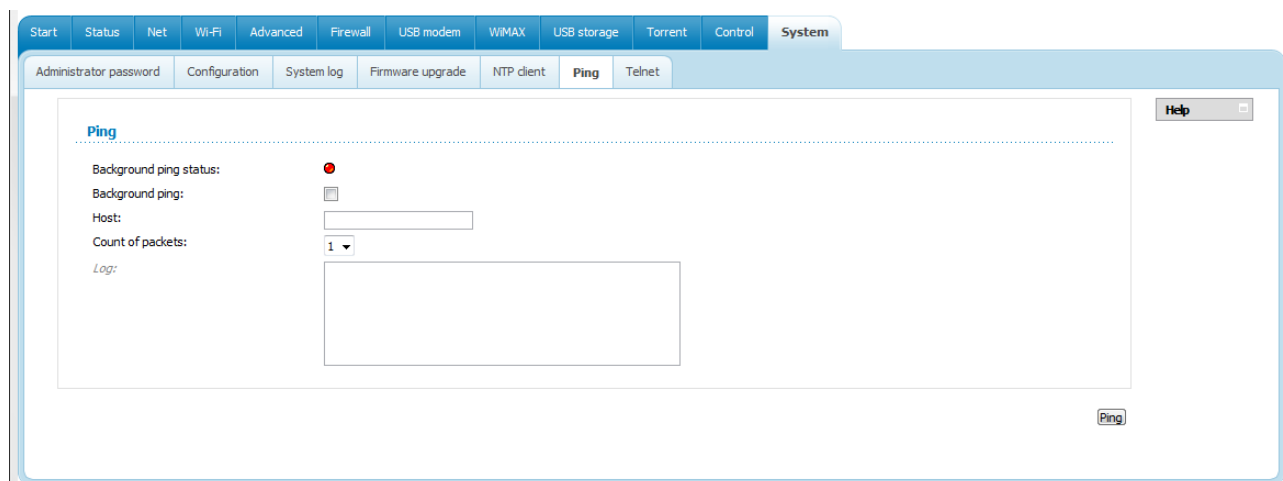


Figure 132. The **System / Ping** page.

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

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

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

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

Telnet

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

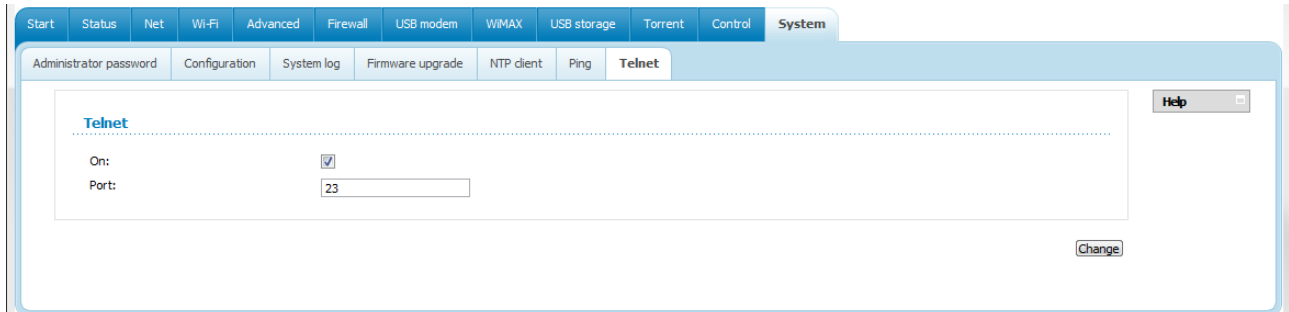


Figure 133. The **System / Telnet** page.

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

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

CHAPTER 5. OPERATION GUIDELINES

Supported USB Modems

GSM modems:

- Huawei E1550
- Huawei E160G
- Huawei E169G
- Huawei E171
- Huawei E173
- Huawei E220
- ZTE MF112
- ZTE MF192
- ZTE MF626
- ZTE MF627
- ZTE MF652
- ZTE MF668
- ZTE MF752.

CDMA modems¹⁰:

- Airplus MCD-650
- Airplus MCD-800
- AnyDATA ADU-300A
- AnyDATA ADU-310A
- Axesstel MV110
- Ubiquam UM-400
- WeTelecom WM-D200.

WiMAX modem:

- Samsung SWC-U200 (firmware version *u200_rev1-2.7.40-C114*).



The manufacturer does not guarantee proper operation of the router with every modification of the firmware of USB modems.

¹⁰ Performance of CDMA USB modems is not tested for the current firmware version.

Safety Instructions

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

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

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

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

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

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

Wireless Installation Considerations

The DIR-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 is not in use.

Connecting to Cable or DSL Modem

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

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

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

| | |
|--------------|--|
| 3G | Third Generation |
| AC | Access Category |
| AES | Advanced Encryption Standard |
| ARP | Address Resolution Protocol |
| BSSID | Basic Service Set Identifier |
| 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 |
| IGMP | Internet Group Management Protocol |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| L2TP | Layer 2 Tunneling Protocol |
| LAN | Local Area Network |
| LCP | Link Control Protocol |
| MAC | Media Access Control |
| MTU | Maximum Transmission Unit |
| NAT | Network Address Translation |
| NTP | Network Time Protocol |
| 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 |
| 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 |