



## DIR-620

**Multifunction Wireless Router  
Supporting GSM, CDMA, WiMAX  
with Built-in 4-port 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.....                               | 11 |
| Chapter 3. Installation and Connection.....         | 12 |
| Before You Begin.....                               | 12 |
| Connecting to PC (in OS Windows XP).....            | 13 |
| PC with Ethernet Adapter.....                       | 13 |
| Obtaining IP Address Automatically.....             | 13 |
| PC with Wi-Fi Adapter.....                          | 16 |
| Configuring Wi-Fi Adapter.....                      | 16 |
| Connecting to Web-based Interface.....              | 17 |
| Saving and Restoring Settings.....                  | 20 |
| Chapter 4. Configuring via Web-based Interface..... | 21 |
| Internet Setup.....                                 | 21 |
| Connection Settings.....                            | 21 |
| Status.....   | 24 |
| Routing Table.....                                  | 24 |
| Network Statistics.....                             | 25 |
| LAN Clients.....                                    | 26 |

|   |    |
|---|----|
| Net.....                                      | 27 |
| Network Interfaces.....                       | 27 |
| Configuring Static Interface.....             | 28 |
| Configuring DHCP Interface.....               | 30 |
| Configuring PPPoE Interface.....              | 31 |
| P-t-p Interfaces.....                         | 32 |
| Adding or Editing PPTP or L2TP Interface..... | 33 |
| Adding or Editing PPPoE Interface.....        | 34 |
| Remote Access.....                            | 36 |
| Routing.....                                  | 38 |
| Name Servers.....                             | 40 |
| DDNS.....                                     | 41 |
| DHCP.....                                     | 43 |
| Wireless.....                                 | 46 |
| Basic Settings.....                           | 46 |
| Security Settings.....                        | 47 |
| MAC Filters.....                              | 53 |
| Clients List.....                             | 54 |
| WPS.....                                      | 55 |
| WDS.....                                      | 58 |
| Advanced Settings.....                        | 60 |
| WMM.....                                      | 62 |
| Client.....                                   | 64 |
| Reservation.....                              | 66 |
| IGMP.....                                     | 68 |
| UPnP.....                                     | 69 |
| Firewall.....                                 | 70 |
| IP Filters.....                               | 70 |
| Dynamic NAT.....                              | 72 |
| Virtual Servers.....                          | 74 |
| URL Filter.....                               | 76 |
| ARP and DDOS Protection.....                  | 77 |
| Application Rules.....                        | 78 |
| USB Modem.....                                | 80 |
| Information.....                              | 80 |
| PIN.....                                      | 83 |
| WiMAX.....                                    | 85 |
| Information.....                              | 85 |

|  |    |
|--|----|
| System.....                                | 87 |
| Administrator Password.....                | 88 |
| Configuration.....                         | 89 |
| System Log.....                            | 91 |
| Firmware Upgrade.....                      | 92 |
| System Time.....                           | 93 |
| Ping.....                                  | 94 |
| Chapter 5. Operation Guidelines.....       | 95 |
| Supported USB Modems.....                  | 95 |
| Safety Instructions.....                   | 95 |
| Wireless Installation Considerations.....  | 96 |
| Connecting to Cable or DSL Modem.....      | 97 |
| Chapter 6. Abbreviations and Acronyms..... | 98 |

# CHAPTER 1. INTRODUCTION

## Contents and Audience

This manual describes the multifunction wireless router DIR-620 supporting GSM, CDMA, and WiMAX and explains how to configure and operate it.

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

## Conventions

| Example  | Description   |
|--|---|
| text   | The body text of the manual.  |
| <i>Before You Begin</i>  | A reference to a chapter or section of this manual.                                   |
| <i>“Quick Installation Guide”</i>  | A reference to a document.  |
| <b>Change</b>  | A name of a menu, menu item, control (field, checkbox, drop-down list, button, etc.). |
| <b>192.168.0.1</b>   | 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 features, describes its appearance and the package contents.

*Chapter 3* explains how to install the multifunction 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 GSM, CDMA, and WiMAX with a built-in 4-port switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

The router is equipped with a USB port for connecting a GSM, CDMA, or WiMAX USB modem<sup>1,2</sup>, which can be used to establish connection to the Internet<sup>3</sup>.

Using the DIR-620 device, you are able to quickly create a wireless network at home or in your office, which lets your relatives or employees connect to your wireless network virtually anywhere (within the operational range of your wireless network). The router is designed to work with 802.11b/g/n wireless devices.

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

Also you are able to connect 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.

The multifunction wireless router DIR-620 includes a built-in firewall. The advanced security functions – IP and URL filtering, dynamic network address translation (NAT), virtual servers, protection against ARP and DDoS attack, and the Port Triggering function – minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

The multifunction wireless router DIR-620 supports reservation of an additional channel. The reservation function keeps the router connected to the Internet even when the main connection is not available.

You can configure and manage the settings of the multifunction wireless router DIR-620 via the user-friendly web-based interface (the interface is available in two languages – in English and in Russian).

---

1 Not included in the delivery package.

2 D-Link does not guarantee compatibility with all USB modems. Please, refer to the **Supported USB Modems** section, page 95.

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

## Specifications

### WAN Interface:

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

### LAN Interface:

- 4 10/100BASE-TX Ethernet ports.

### WLAN Interface:

- IEEE 802.11b/g/n.

### USB Interface:

- USB 2.0 type A port for USB modem.

### Network Functions:

- WAN connection types:
  - Static IP
  - Dynamic IP
  - PPPoE
  - PPTP
  - L2TP
- DHCP server and client
- DNS relay
- Dynamic DNS
- Static IP routing
- Remote management
- Network statistics for each interface
- Support of channel reservation
- IGMP
- UPnP.

### USB Modem<sup>4</sup>:

- Always on, Connect on Demand, and Manual modes for Internet connection
- Auto connection to available type of supported network
- Enabling/disabling PIN code check
- Changing PIN code.

---

<sup>4</sup> The listed functions are available for GSM and CDMA USB modems.

---

## Wireless Connection:

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

## Firewall Functions:

- NAT
- IP filters
- URL filters
- Prevention of ARP and DDoS attacks
- Port Triggering
- Virtual servers.

## Configuration and Management:

- Bilingual (Russian/English) web-based interface for configuration and management
- Firmware update via web-based interface
- Saving/restoring configuration to/from file
- Support of remote logging
- Manual setup/automatic synchronization of system time
- 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   |
|---|-----------------------|---|
| <br><b>Power</b>     | <i>Solid green</i>    | Device is powered on  |
|   | <i>No light</i>       | Device is powered off   |
|   | <i>Solid yellow</i>   | Device malfunction  |
| <br><b>Internet</b> | <i>Solid green</i>    | Connection is on  |
|   | <i>Blinking green</i> | WAN interface is active (upstream or downstream traffic)          |
|   | <i>Solid yellow</i>   | Connection is off   |
| <br><b>WLAN</b>    | <i>Solid green</i>    | Wireless connection is on   |
|   | <i>Blinking green</i> | WLAN interface is active (upstream or downstream traffic)         |
| <br><b>LAN 1-4</b> | <i>Solid green</i>    | Device (computer) is connected to relevant port, connection is on |
|   | <i>Blinking green</i> | Relevant LAN port is active (upstream or downstream traffic)      |

In addition, a port for connecting a GSM, CDMA, or WiMAX USB modem<sup>5</sup> 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>    | A wireless device is connected to the router's WLAN (lights for several minutes)  |
| <i>Solid yellow</i>  | Failed to add a wireless device via the WPS function or the WPS function is not used and a USB modem is connected to the router |

<sup>5</sup> It is recommended to a USB extension cable to connect a USB modem 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  |

### Delivery Package

The following should be included:

- multifunction 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 GSM, CDMA, and WiMAX (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, Google Chrome, 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 GSM, CDMA or WiMAX 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 connect to the Internet via the relevant network manually or configure automatic connection.

#### **WiMAX USB modem (4G modem)**

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

#### **CDMA or GSM USB modem (3G/2G modem)**

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

## Connecting to PC (in OS Windows XP)

### PC with Ethernet Adapter

1. Make sure that your PC is powered off.
2. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
3. To connect via a WiMAX, CDMA or GSM network: connect your USB modem to the USB port located on the front panel of the router.
4. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
5. Turn on your PC and wait until your operating system is completely loaded.

### Obtaining IP Address Automatically

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

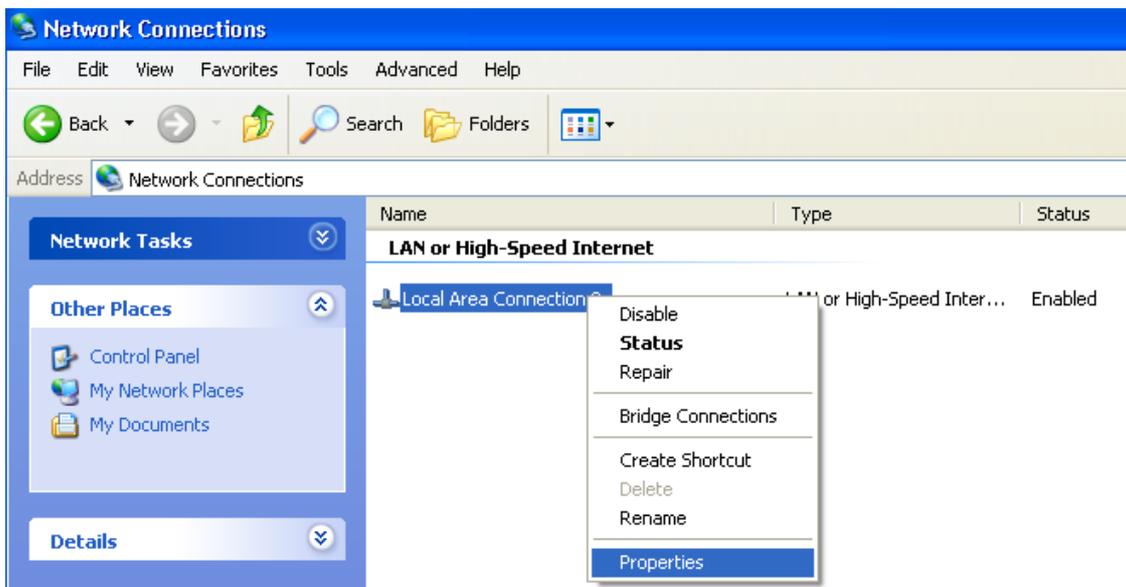


Figure 3. The **Network Connections** window.

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

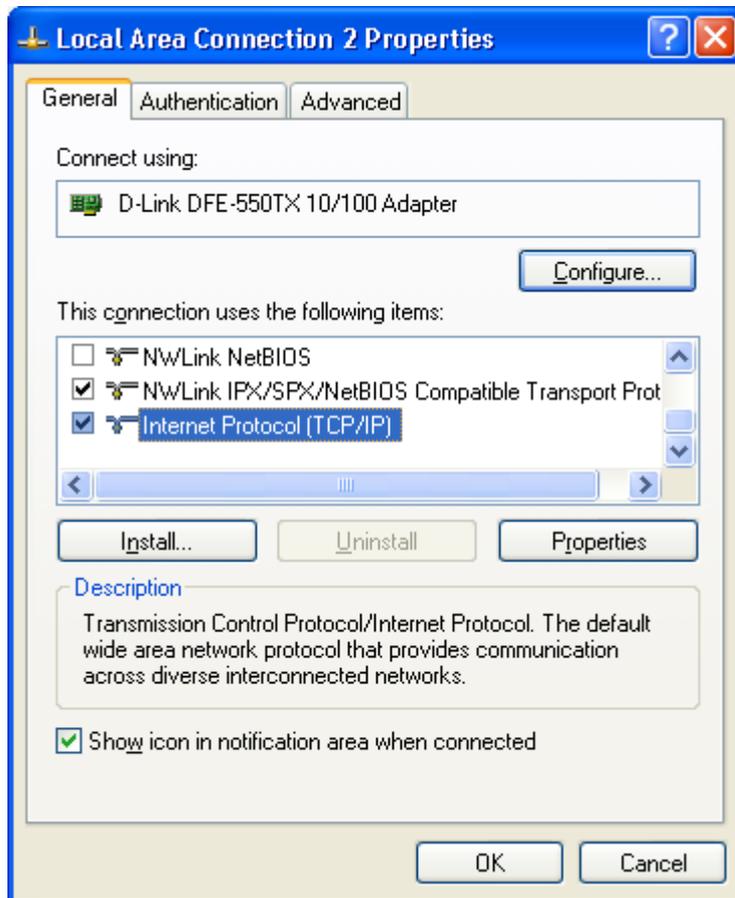


Figure 4. The **Local Area Connection Properties** window.

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

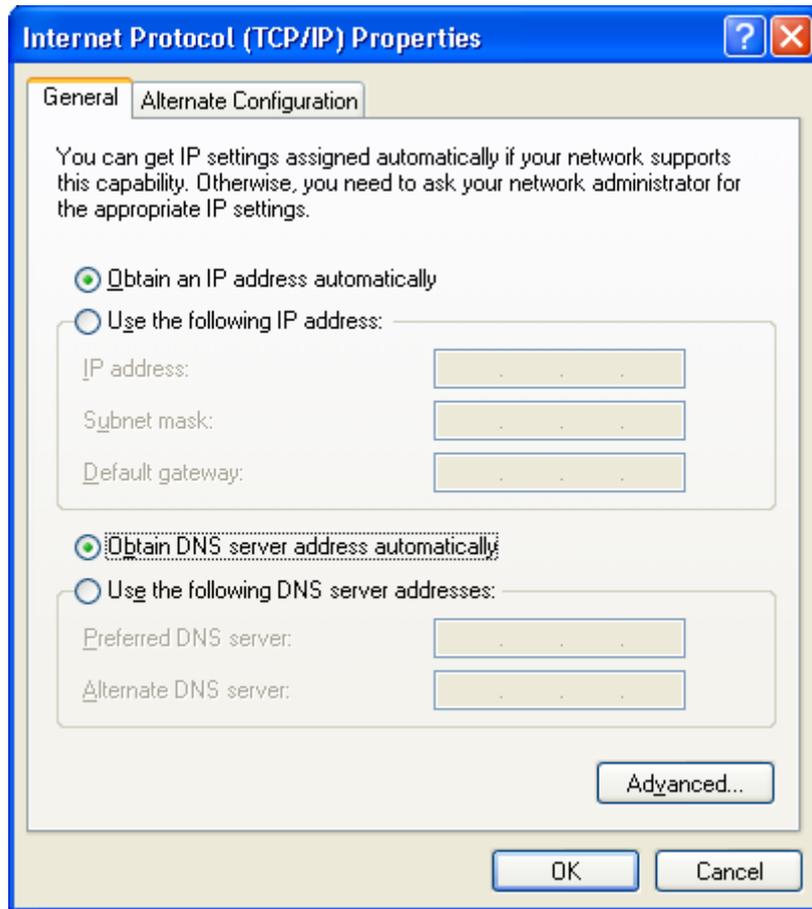


Figure 5. The **Internet Protocol (TCP/IP) Properties** window.

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

## PC with Wi-Fi Adapter

1. To connect via a WiMAX, CDMA or GSM network: connect your USB modem to the USB port located on the front panel of the router.
2. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
3. Turn on your PC and wait until your operating system is completely loaded.
4. Turn on your Wi-Fi adapter. As a rule, modern notebooks with built-in wireless NICs are equipped with a button or switch that turns on/off the wireless adapter (refer to your PC documents). If your PC is equipped with a pluggable wireless NIC, install the software provided with your Wi-Fi adapter.

## Configuring Wi-Fi Adapter

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

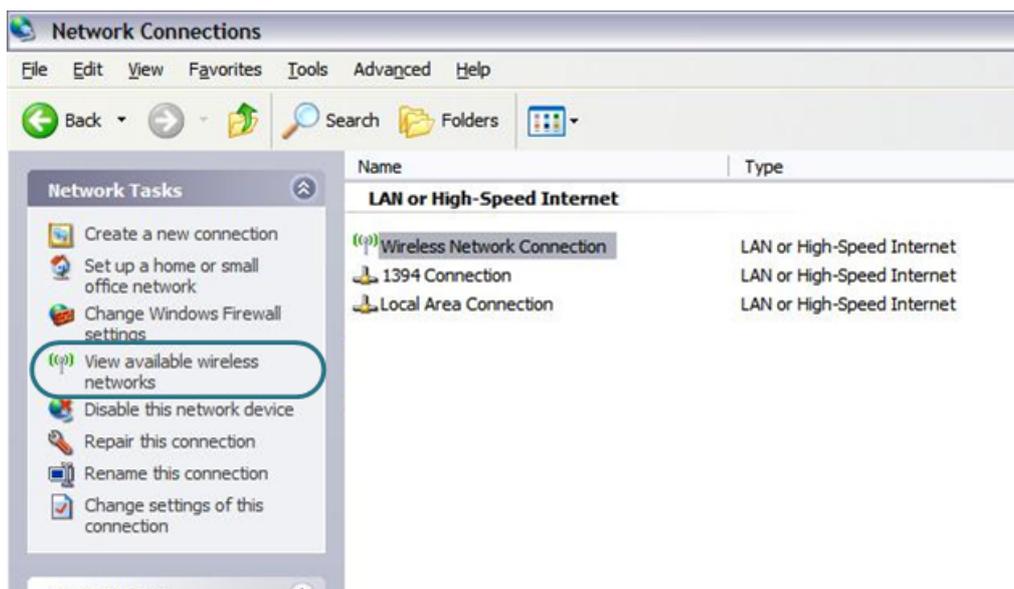


Figure 6. The **Network Connections** window.

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

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

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

## Connecting to Web-based Interface

When you have configured your computer, you can access the web-based interface and configure needed parameters (for example, change the parameters of the wireless network, specify the settings of the firewall, edit the password for the administrator account, or connect to the GSM, CDMA, or WiMAX network via your USB modem, etc.).

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



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

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

A screenshot of a login page. It features two input fields: "Login:" with the text "admin" and "Password:" with "\*\*\*\*\*". Below the fields are two buttons: "Clear" and "Enter".

Figure 8. The login page.

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

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

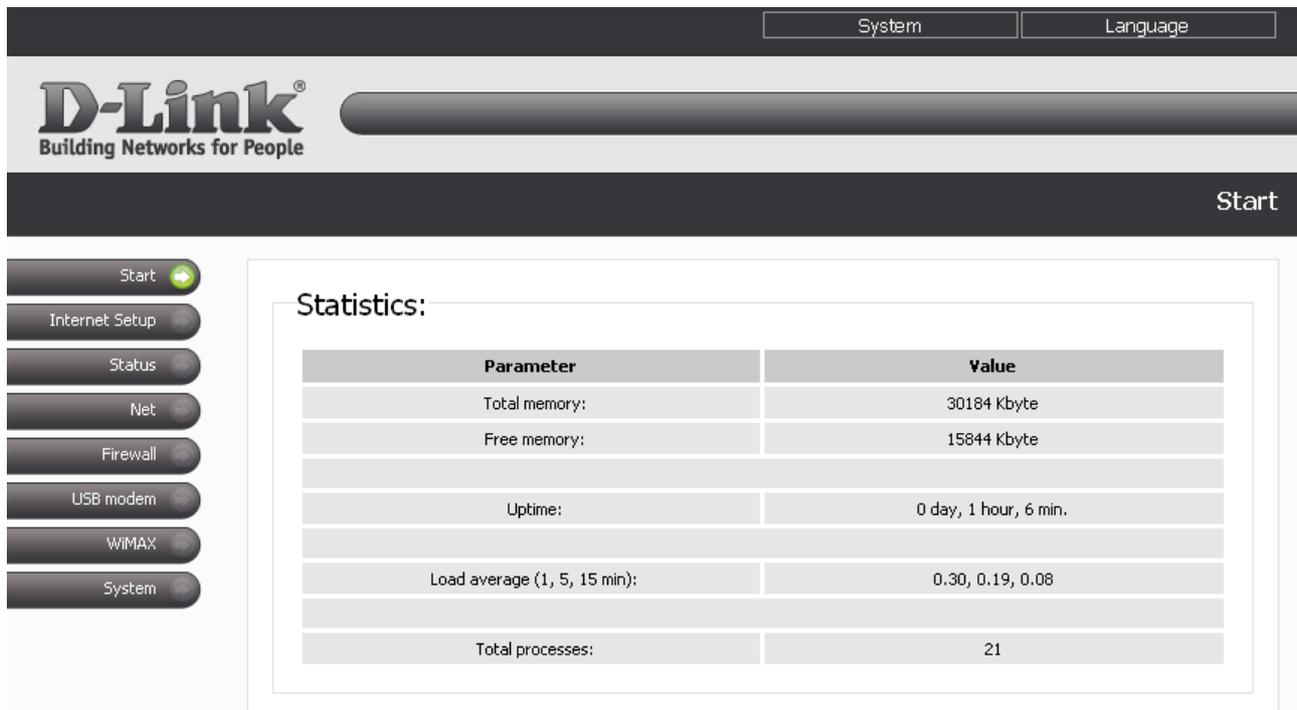


Figure 9. The system statistics page.

**!** For security reasons, it is strongly recommended to change the administrator password upon initial configuration of the router. To do so, proceed to the **System > Administrator password** page.

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

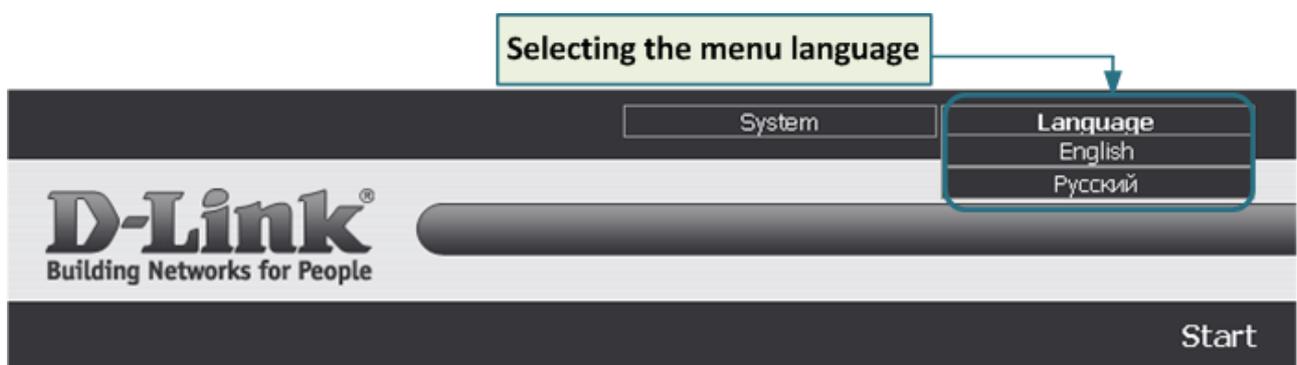


Figure 10. Changing the language of the web-based interface.

If the PIN code check is enabled for the identification card of your CDMA or GSM USB modem, the page for checking the PIN code is displayed after logging in to the web-based interface of the router.

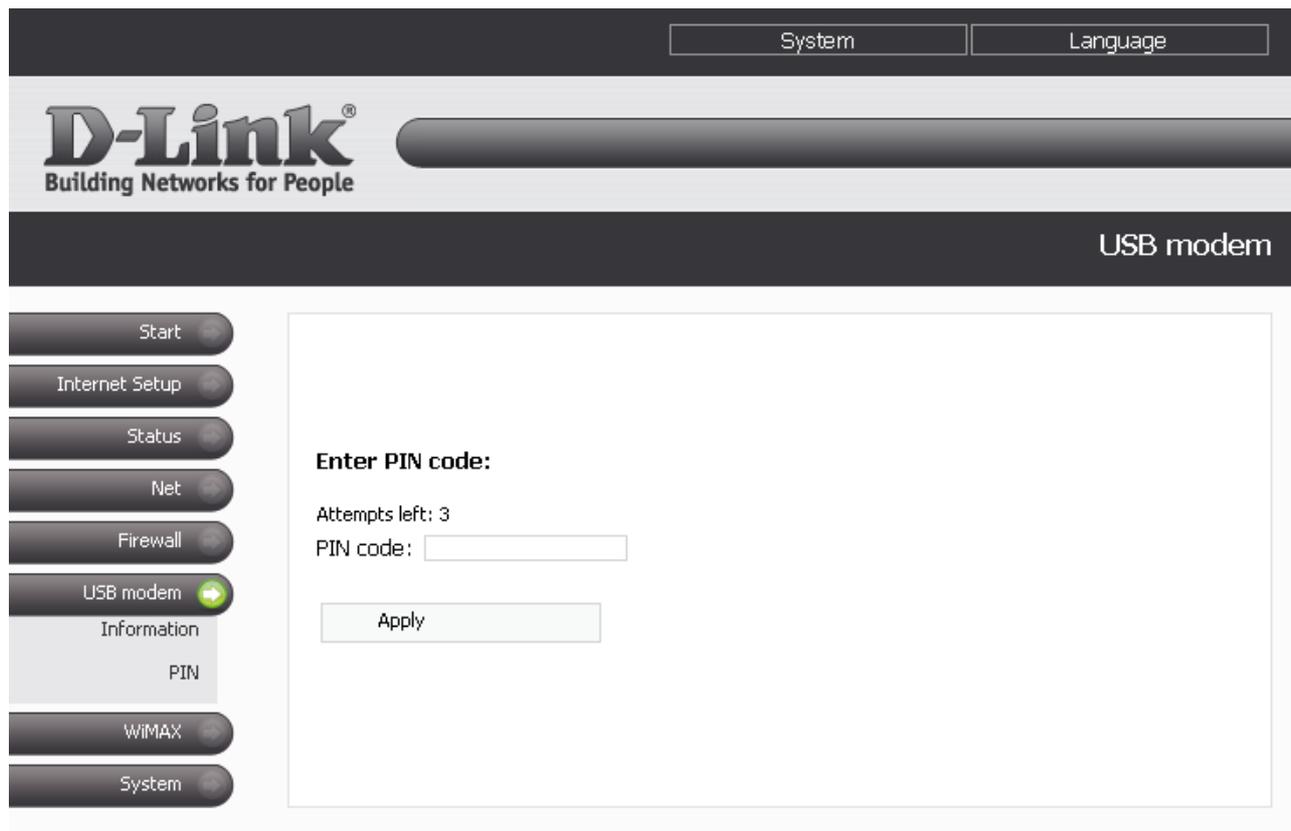


Figure 11. Checking the PIN code.

Enter the PIN code of the identification card in the relevant field and click the **Apply** button.

## Saving and Restoring Settings

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

Some settings of the router are applied immediately after clicking the **Change** button on the relevant page. To apply the other settings, it is required to reboot the device (in this case the router's web-based interface displays the notification on unsaved changes at the top of the page).

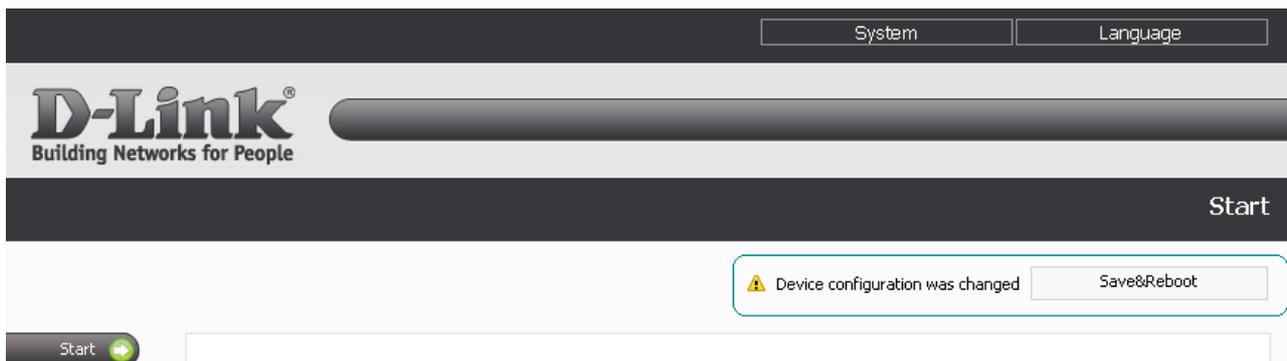


Figure 12. The notification on unsaved changes.

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

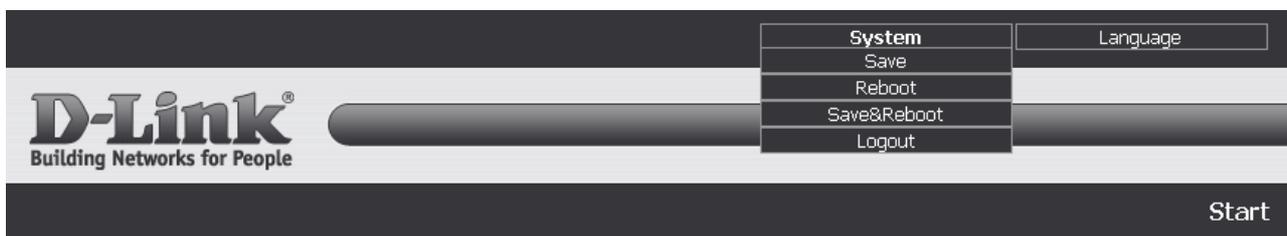


Figure 13. The top-page menu.

Click the **Save** line to save new settings to the non-volatile memory and continue configuring the device.

Click the **Reboot** line if you have already saved the router's settings. Also you can reboot the router via the **Reboot** button on the **System** page.

Click the **Save&Reboot** line to save new settings and immediately reboot the router. Also you can save the device's parameters and reboot it on the **System > Configuration** page via the **Save** button.

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

You can restore the factory default settings via the web-based interface (the **System > Configuration** page, the **Factory** button) or via the hardware Reset button. The hole of the button is located on the back panel of the router next to the power connector. Use a small paperclip to activate the button; insert it into the hole (with the router turned on), push, and hold for 10 seconds. Then remove the paperclip. Wait for about 30 seconds. Now you can access the web-based interface of the router using the default IP address, username and password.

## CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

### Internet Setup

In this menu you can specify settings for the Internet connection via your CDMA or GSM USB modem. To configure connection via your WiMAX USB modem, see the *WiMAX* section, page 85. To configure a wired connection to the Internet, see the *Net* section, page 27.

### Connection Settings

On the **Internet Setup > Connection Settings** page, you can configure your connection to the Internet. You can edit the fields displayed on this page only if a CDMA or GSM USB modem is connected to the router and enabled (on the **USB modem > Information** page).

| Name                           | Value              | Sample      |
|--------------------------------|--------------------|-------------|
| Internet connection interface: | USB Adapter        | USB Adapter |
| Operator:                      | <custom><br>Delete | provider    |
| Operator name:                 | custom             | my_provider |
| User name:                     | login              | my_login    |
| Password:                      | *****              | my_password |
| Dial number:                   |                    |             |
| APN:                           |                    |             |
| Reconnect mode:                | Always On          | Always On   |
| Maximum idle time (min):       | 2                  | 2           |
| MTU:                           | 1300               | 1300        |

Figure 14. The **Internet Setup > Connection Settings** page.

You can specify the following settings:

| Parameter                            | Description   |
|--------------------------------------|---|
| <b>Internet connection interface</b> | An interface that is used to connect to the Internet. <ul style="list-style-type: none"><li>• <b>USB Adapter.</b></li><li>• <b>Ethernet.</b> If this value is selected, the other fields and lists on this page are not displayed.</li></ul>  |
| <b>Operator</b>                      | Select an operator profile from the drop-down list (an identification card (SIM or R-UIM) of the relevant operator needs to be inserted into your USB modem). You can create your own profile containing all needed setting. To do so, select the <b>&lt;custom&gt;</b> value from the drop-down list. After configuring the profile settings and clicking the <b>Change</b> button, the new profile with the name from the <b>Operator name</b> field appears in the list. |
| <b>Operator name</b>                 | A name for the operator profile for easier identification.  |
| <b>User name</b>                     | A username (login) to connect to the network of the operator. Obtain the value from the operator whose network is used to access the Internet.  |
| <b>Password</b>                      | A password to connect to the network of the operator. Obtain the value from the operator whose network is used to access the Internet.  |
| <b>Dial number</b>                   | A number dialed to connect to the authorization server of the operator. Obtain the value from the operator whose network is used to access the Internet.  |
| <b>APN</b>                           | An access point name. Obtain the value from the operator whose network is used to access the Internet.  |

| Parameter                | Description   |
|--------------------------|---|
| <b>Reconnect mode</b>    | <p>A method used to connect to the network of the operator. Select a value from the drop-down list.</p> <p><b>Always On:</b> The router connects to the Internet via the network of the operator when loaded and keeps the connection active (you don't need to access the web-based interface to establish connection to the Internet). This value is set by default.</p> <p><b>Connect On Demand:</b> The router automatically connects to the Internet via the network of the operator when it receives a request from an application installed on a computer from your LAN (you don't need to access the web-based interface to establish connection to the Internet).</p> <p><b>Manual:</b> The Internet connection is established manually via the web-based interface of the router.</p> |
| <b>Maximum idle time</b> | <p>The maximum inactivity period of the Internet connection in minutes. After the specified period the router breaks the Internet connection and reestablishes the connection after the request to connect to the Internet. You can specify this parameter when the <b>Connect On Demand</b> value is selected from the <b>Reconnect mode</b> drop-down list.</p>   |
| <b>MTU</b>               | <p>The maximum transmission unit in the interface. <i>Optional.</i></p>   |

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

## Status

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

### Routing Table

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

The screenshot shows the D-Link web interface. At the top right, there are buttons for 'System' and 'Language'. The D-Link logo and tagline 'Building Networks for People' are on the left. A breadcrumb trail 'Status >> Routing table' is visible. On the left side, there is a vertical navigation menu with buttons for 'Start', 'Internet Setup', 'Status' (highlighted with a green arrow), 'Routing table', 'Network statistics', 'LAN clients', 'Net', 'Firewall', 'USB modem', 'WiMAX', and 'System'. The main content area is titled 'Configuration:' and contains a table with the following data:

| Iface | Destination  | Gateway        | Mask            | Flags | RefCnt | Use | Metric | MTU | Window | IRTT |
|-------|--------------|----------------|-----------------|-------|--------|-----|--------|-----|--------|------|
| vlan2 | 192.168.62.1 | 0.0.0.0        | 255.255.255.255 | UH    | 0      | 0   | 0      | 40  | 0      | 0    |
| vlan2 | 192.168.22.0 | 192.168.62.131 | 255.255.255.255 | UGH   | 0      | 0   | 0      | 40  | 0      | 0    |
| br0   | 192.168.1.0  | 0.0.0.0        | 255.255.255.0   | U     | 0      | 0   | 0      | 40  | 0      | 0    |
| vlan2 | 192.168.62.0 | 0.0.0.0        | 255.255.255.0   | U     | 0      | 0   | 0      | 40  | 0      | 0    |
| vlan2 | 192.168.11.0 | 192.168.62.131 | 255.255.255.0   | UG    | 0      | 0   | 0      | 40  | 0      | 0    |
| vlan2 | 0.0.0.0      | 192.168.62.1   | 0.0.0.0         | UG    | 0      | 0   | 0      | 40  | 0      | 0    |

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

## Network Statistics

On the **Status > Network statistics** page, you can view statistics (the number of received/transmitted packets, errors, etc.) for all interfaces active at the moment.

The screenshot shows the D-Link web interface for the DIR-620 router. The top navigation bar includes 'System' and 'Language' buttons. The D-Link logo and tagline 'Building Networks for People' are visible. The breadcrumb trail indicates the current page is 'Status >> Network statistics'. A left-hand menu contains buttons for 'Start', 'Internet Setup', 'Status' (highlighted with a green arrow), 'Routing table', 'Network statistics', 'LAN clients', 'Net', 'Firewall', 'USB modem', 'WiMAX', and 'System'. The main content area displays statistics for four interfaces:

- eth0:**

| IP address:0.0.0.0<br>Mask:0.0.0.0<br>MTU:1500<br>Metric:1 | Statistics<br>RX/TX: 10.6 Mbyte/ 6.0 Mbyte<br>Received: 70553 Packets, 0 Errors, 0 Dropped<br>Transmitted: 20363 Packets, 0 Errors, 0 Dropped |
|--|---|
|--|---|
- WLAN(air):**

| IP address:0.0.0.0<br>Mask:0.0.0.0<br>MTU:1500<br>Metric:1 | Statistics<br>RX/TX: 0.5 Mbyte/ 7.2 Mbyte<br>Received: 6268 Packets, 0 Errors, 0 Dropped<br>Transmitted: 20666 Packets, 2 Errors, 0 Dropped |
|--|---|
|--|---|
- vlan0:**

| IP address:0.0.0.0<br>Mask:0.0.0.0<br>MTU:1500<br>Metric:1 | Statistics<br>RX/TX: 0/ 5.6 Mbyte<br>Received: 0 Packets, 0 Errors, 0 Dropped<br>Transmitted: 16695 Packets, 0 Errors, 0 Dropped |
|--|--|
|--|--|
- WAN(internet):**

| IP address:192.168.62.251<br>Mask:255.255.255.0<br>MTU:1500 | Statistics<br>RX/TX: 9.4 Mbyte/ 0.4 Mbyte<br>Received: 70553 Packets, 0 Errors, 0 Dropped |
|---|---|
|---|---|

Figure 16. The **Status > Network statistics** page.

## LAN Clients

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



The screenshot shows the D-Link web interface. At the top right, there are buttons for 'System' and 'Language'. The D-Link logo is on the left, and 'Status >> LAN clients' is on the right. A sidebar on the left contains navigation buttons: Start, Internet Setup, Status (highlighted with a green arrow), Routing table, Network statistics, LAN clients, Net, Firewall, USB modem, WIMAX, and System. The main content area is titled 'LAN clients:' and contains a table with the following data:

| IP address     | MAC-address       | Interface     |
|----------------|-------------------|---------------|
| 192.168.62.141 | 00:22:15:74:FD:6D | WAN(internet) |
| 192.168.62.1   | 00:21:91:1A:10:3B | WAN(internet) |

Figure 17. 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 specify basic network settings for the router: modify parameters of the physical interfaces, add p-t-p interfaces, and define static routes and rules for remote access to the web-based interface. In addition, you can add DNS servers, add domains to the search list, edit parameters of the DHCP server, change settings of your wireless network and the reservation function, configure a DDNS service, and enable IGMP and the UPnP function.

### Network Interfaces

On the **Net > Network interfaces** page, you can edit settings of the router's physical interfaces.

| Interface Connection | Parameters   | Status  | Actions  |
|----------------------|--|---------|--|
| LAN                  | Interface type: static<br>IP address: 192.168.1.18<br>Mask: 255.255.255.0<br>Start: Auto | Running | <input type="button" value="Stop"/><br><input type="button" value="Disable"/>  |
| WAN                  | Interface type: dhcp<br>IP address: 55.55.55.7<br>Mask: 255.255.255.0<br>Start: Auto     | Running | <input type="button" value="Stop"/><br><input type="button" value="Disable"/>  |
| WIMAX                | Interface type: dhcp<br>IP address: 0.0.0.0<br>Mask: 0.0.0.0<br>Start: Auto              | Stopped | <input type="button" value="Start"/><br><input type="button" value="Disable"/> |

Figure 18. The **Net > Network interfaces** page.

The LAN interface represents the ports of the built-in switch (ports 1-4) coupled with the wireless interface (the predefined name is **br0**).

The WAN interface represents the Internet port of the router (the predefined name is **vlan2**).

The WIMAX interface represents the router's USB port and a WiMAX USB modem connected to it (the predefined name is **wimax0**).

You can enable, disable, start, or stop either interface. To perform the needed action, click the relevant button in the **Actions** column.

To edit settings of one of these interfaces, follow the relevant link. On the opened page, select a type for the interface from the **Interface type** drop-down list (available for the WAN and WIMAX interfaces).

### Configuring Static Interface

The static type is the only available type for the LAN interface and one of three types available for the WAN and WIMAX interfaces.

**Configuration:**

| Value            |   | Sample            |
|------------------|---|-------------------|
| Interface type   | Static ▾  |                   |
| Interface:       | br0   |                   |
| IP address:      | 192.168.0.1   | 192.168.0.12      |
| Mask:            | 255.255.255.0   | 255.255.255.128   |
| MTU:             |   | 1500              |
| MAC-address:     |   | 00:F1:1C:12:21:00 |
| Metric:          |   | 12                |
| Default gateway: |   | 192.168.0.100     |
| Start:           | <input checked="" type="radio"/> Auto<br><input type="radio"/> Manual | Auto              |

Figure 19. Configuring the LAN interface.

On this page, you can change the following parameters:

| Parameter              | Description  |
|------------------------|--|
| <b>IP address</b>      | The IP address assigned to the interface (the following IP address is set for the LAN interface by default – <b>192.168.0.1</b> ).   |
| <b>Mask</b>            | The subnet mask (the following mask is set for the LAN interface by default – <b>255.255.255.0</b> ).  |
| <b>MTU</b>             | The maximum transmission unit in the interface. <i>Optional</i> .  |
| <b>MAC-address</b>     | <p>A MAC address assigned to the interface. <i>Optional for the LAN and WIMAX interfaces.</i></p> <p>For the WAN 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. You can click the <b>Client MAC-address</b> button (displayed for the WAN interface only) 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> |
| <b>Metric</b>          | The metric for the interface. Allows assigning a priority for the interface. The lower the value, the higher is the interface priority. <i>Optional</i> .  |
| <b>Default gateway</b> | The IP address of the default gateway. Sets the address for routing packets to external networks (applicable for the WAN interface only). <i>Optional</i> .  |
| <b>Start</b>           | Select a radio button to enable or disable the interface auto-start upon the boot-up of the router.  |

Click the **Save&Reboot** button (on the page for configuring the LAN interface) or the **Change** button (on the page for configuring the WAN and WIMAX interfaces).

## Configuring DHCP Interface

This interface type is available for the WAN and WIMAX interfaces. By default, the DHCP type is specified for both interfaces.

**Configuration:**

| Parameter      | Value   | Sample            |
|----------------|---|-------------------|
| Interface type | DHCP  |                   |
| Interface:     | vlan2   |                   |
| MAC-address:   | <input type="text"/><br>Client MAC-address                            | 00:F1:1C:12:21:00 |
| Start:         | <input checked="" type="radio"/> Auto<br><input type="radio"/> Manual | Auto              |

Figure 20. Configuring the WAN interface.

| Parameter             | Description  |
|-----------------------|--|
| <b>Interface type</b> | The type of configuration for this interface ( <b>DHCP</b> ).  |
| <b>MAC-address</b>    | <i>Displayed for the WAN interface only.</i><br>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. You can click the <b>Client MAC-address</b> 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. |
| <b>Start</b>          | Select a radio button to enable or disable the interface auto-start upon the boot-up of the router.  |

Click the **Change** button.

## Configuring PPPoE Interface

This interface type is available for the WAN and WIMAX interfaces.

**Configuration:**

| Parameter      | Value   | Sample            |
|----------------|---|-------------------|
| Interface type | PPPOE ▾   |                   |
| Interface:     | vlan2   |                   |
| MAC-address:   | <input type="text"/><br>Client MAC-address                            | 00:F1:1C:12:21:00 |
| Start:         | <input checked="" type="radio"/> Auto<br><input type="radio"/> Manual | Auto              |

Figure 21. Configuring the WAN interface.

| Parameter             | Description  |
|-----------------------|--|
| <b>Interface type</b> | The type of configuration for this interface ( <b>PPPoE</b> ).   |
| <b>MAC-address</b>    | <i>Displayed for the WAN interface only.</i><br>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. You can click the <b>Client MAC-address</b> 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. |
| <b>Start</b>          | Select a radio button to enable or disable the interface auto-start upon the boot-up of the router.  |

Click the **Change** button.

When you select this type for the WAN or WIMAX interface, it gets IP address 0.0.0.0. Then, if needed, proceed to the **Net > P-t-p interfaces** page and create a PPPoE interface with parameters provided by your ISP.

## P-t-p Interfaces

On the **Net > P-t-p interfaces** page, you can create, edit, or delete PPTP, L2TP, and PPPoE interfaces of the router.

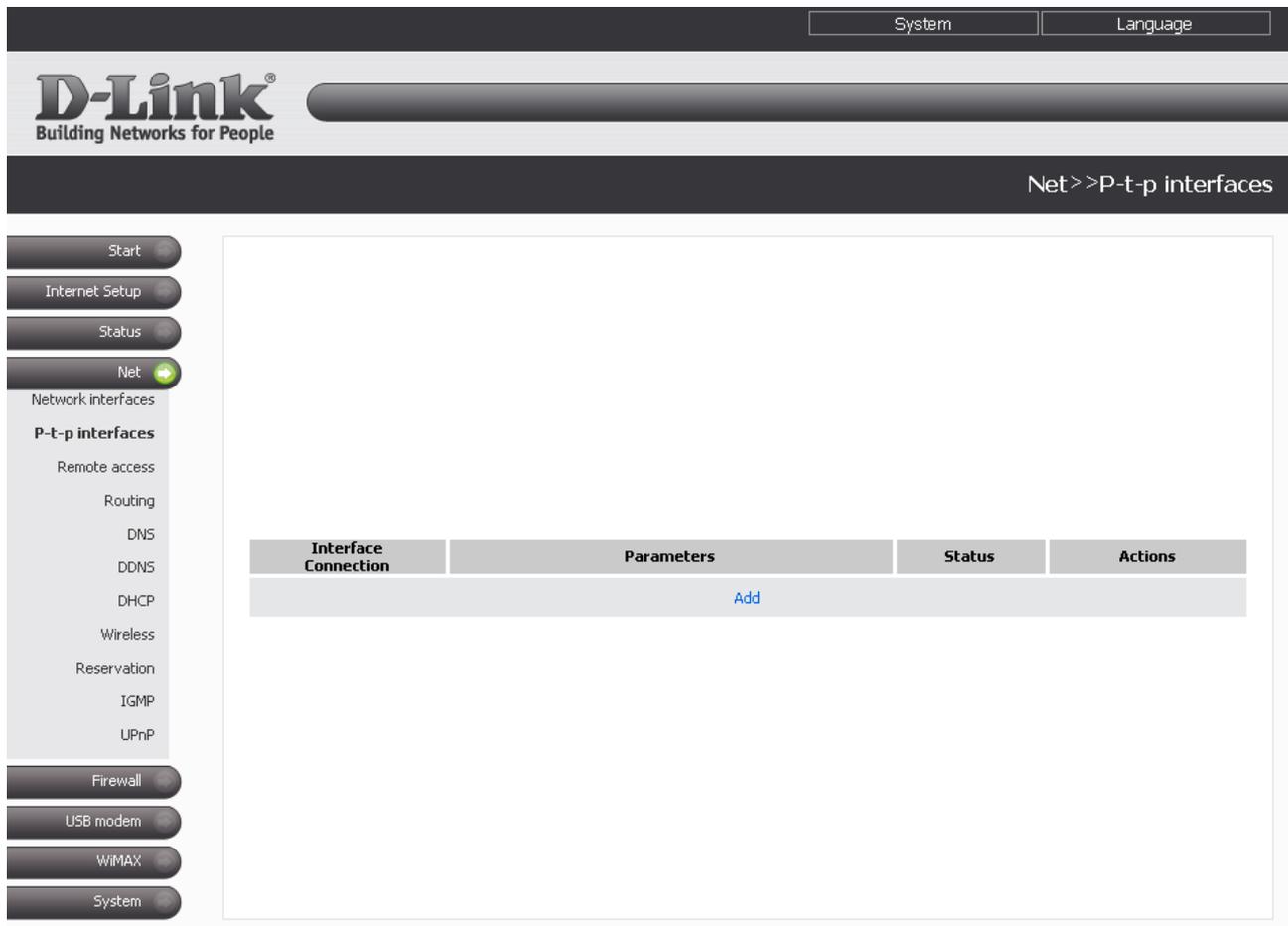


Figure 22. The **Net > P-t-p interfaces** page.

You can enable, disable, start, or stop either interface. To perform the needed action, click the relevant button in the **Actions** column.

To create a new interface, click the **Add** link. On the opened page, select a type for the interface from the **Interface type** drop-down list and specify the needed parameters. Then click the **Change** button.

To change settings of a p-t-p interface, click the relevant interface link. On the opened page, edit the needed parameters and click the **Change** button.

To remove a p-t-p interface, click the relevant interface link, then click the **Delete** button on the opened page.

## Adding or Editing PPTP or L2TP Interface

Configuration

| Parameter       | Value   | Sample          |
|-----------------|---|-----------------|
| Interface type: | PPTP  |                 |
| Connection:     | <input type="text"/>  | Sample_provider |
| Username:       | <input type="text"/>  | Net_Server      |
| Password:       | <input type="text"/> Show password <input type="checkbox"/>           | PasSworD        |
| Server address: | <input type="text"/>  | 192.168.0.1     |
| Default route:  | <input checked="" type="checkbox"/>                                   |                 |
| Metric:         | <input type="text" value="1"/>  | 12              |
| Start:          | <input type="radio"/> Auto<br><input checked="" type="radio"/> Manual | Auto            |

Figure 23. The page for adding a PPTP interface.

You can specify or change the following parameters:

| Parameter             | Description   |
|-----------------------|---|
| <b>Interface type</b> | The type of configuration for this interface ( <b>PPTP</b> or <b>L2TP</b> ).  |
| <b>Connection</b>     | A name for this connection for easier identification (you can specify any name).  |
| <b>Username</b>       | The login to register on the PPTP or L2TP server correspondingly.   |
| <b>Password</b>       | The password to register on the PPTP or L2TP server correspondingly. By default, a value entered in this field is hidden with asterisks (*). To display it, select the <b>Show password</b> checkbox. |
| <b>Server address</b> | The IP address of the PPTP or L2TP server correspondingly.  |
| <b>Default route</b>  | Select this checkbox if you want to use the IP address of the server as the default route (the destination address for all packets, which routes have not been found).                                |
| <b>Metric</b>         | This parameter is used to assign a priority for this interface. The lower the value, the higher is the priority.  |

| Parameter    | Description   |
|--------------|---|
| <b>Start</b> | Select a radio button to enable or disable the interface auto-start upon the boot-up of the router. |

Click the **Change** button.

### Adding or Editing PPPoE Interface

Configuration

| Parameter                 | Value   | Sample          |
|---------------------------|---|-----------------|
| Interface type:           | PPPOE ▾   |                 |
| Connection:               | <input type="text"/>  | Sample_provider |
| Interface:                | LAN1(ports 1-4) ▾   |                 |
| Username:                 | <input type="text"/>  | Net_Server      |
| Password:                 | <input type="text"/> Show password <input type="checkbox"/>           | PasSwoRd        |
| Access concentrator name: | <input type="text"/>  | DSA3110_Conc    |
| Service name:             | <input type="text"/>  | Internet        |
| Default route:            | <input checked="" type="checkbox"/>                                   |                 |
| Metric:                   | <input type="text" value="1"/>  | 12              |
| Start:                    | <input type="radio"/> Auto<br><input checked="" type="radio"/> Manual | Auto            |

Figure 24. The page for adding a PPPoE interface.

You can specify or change the following parameters:

| Parameter                       | Description  |
|---------------------------------|--|
| <b>Interface type</b>           | The type of configuration for this interface ( <b>PPPoE</b> ).   |
| <b>Connection</b>               | A name for this connection for easier identification (you can specify any name).   |
| <b>Interface</b>                | A physical interface to which the configured PPPoE interface will be assigned.   |
| <b>Username</b>                 | The login to register on the PPPoE server.   |
| <b>Password</b>                 | The password to register on the PPPoE server. By default, a value entered in this field is hidden with asterisks (*). To display it, select the <b>Show password</b> checkbox. |
| <b>Access concentrator name</b> | The name of the provider's PPPoE server.   |
| <b>Service name</b>             | The name of the service on the provider's PPPoE server.  |
| <b>Default route</b>            | Select this checkbox if you want to use the IP address of the server as the default route (the destination address for all packets, which routes have not been found).         |
| <b>Metric</b>                   | This parameter is used to assign a priority for this interface. The lower the value, the higher is the priority.   |
| <b>Start</b>                    | Select a radio button to enable or disable the interface auto-start upon the boot-up of the router.  |

Click the **Change** button.

## Remote Access

On the **Net > Remote access** page, you can configure access to the web-based interface of the router from the local (LAN) and global (WAN) interfaces with filtering by IP address.

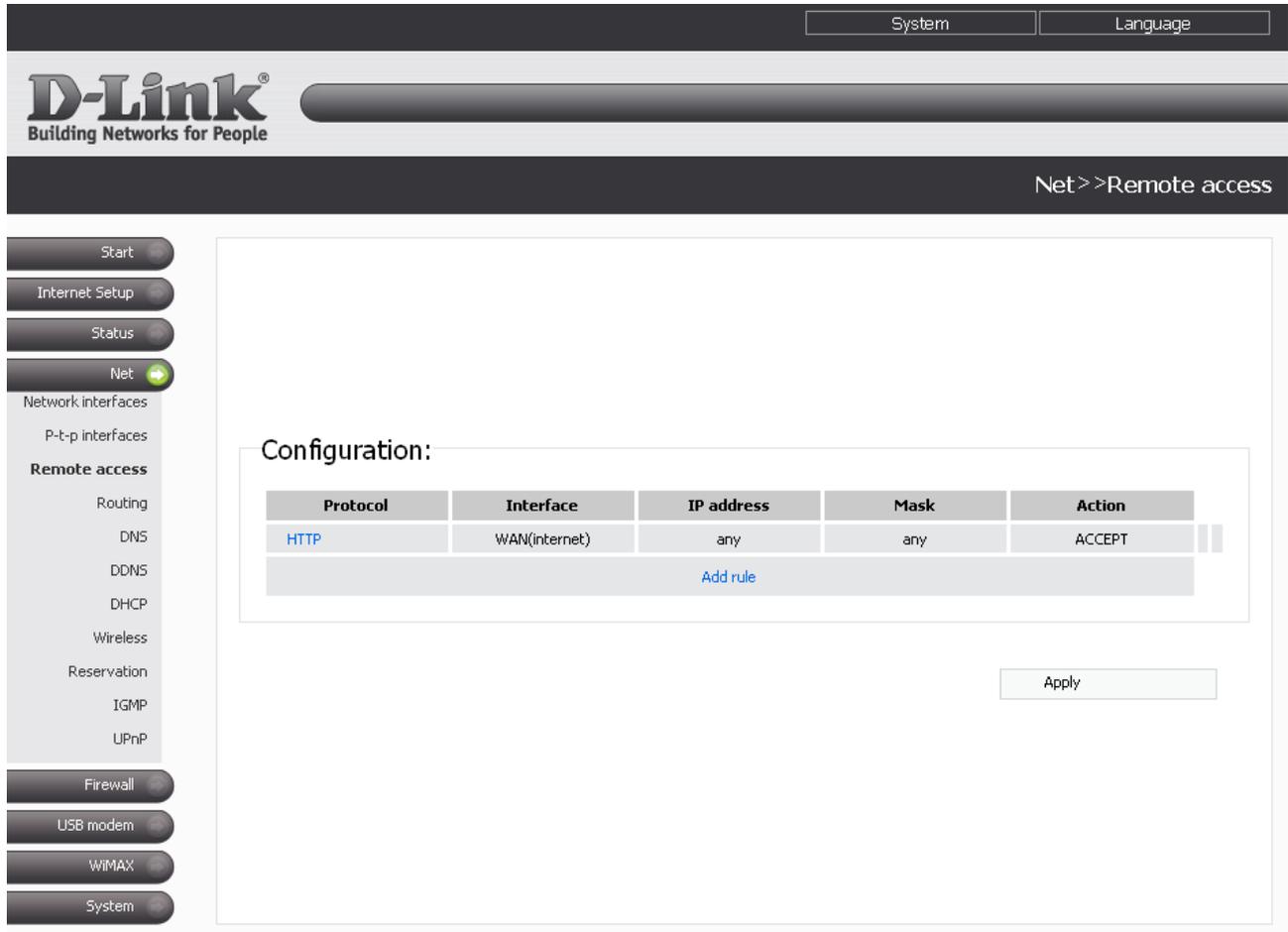


Figure 25. The **Net > Remote access** page.

Rules regulating access to the web-based interface are presented as a table. The rules are processed in the listed order (downwards). The arrow buttons located to the right of the rule table are used to change the order of rules (to move a rule up or down). After changing the order of rules, click the **Apply** button.

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

**Configuration:**

| Parameter  | Value                | Sample        |
|------------|----------------------|---------------|
| Protocol   | HTTP ▾               |               |
| Interface  | <Any> ▾              |               |
| IP address | <input type="text"/> | 192.168.1.100 |
| Mask       | <input type="text"/> | 255.255.255.0 |
| Action     | ACCEPT ▾             |               |

Figure 26. The page for adding a rule for remote management.

You can specify the following parameters:

| Parameter         | Description  |
|-------------------|--|
| <b>Protocol</b>   | The protocol available for remote management of the router.  |
| <b>Interface</b>  | A physical interface through which the web-based interface of the router is accessed.  |
| <b>IP address</b> | A subnet to which the rule is applied.   |
| <b>Mask</b>       | The mask of the subnet (along with the <b>IP address</b> field specifies the subnet to which the rule is applied).   |
| <b>Action</b>     | An action of the rule. The following actions are available:<br><b>ACCEPT:</b> Access to the web-based interface is granted.<br><b>DROP:</b> Access to the web-based interface if denied. |

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.

## Routing

On the **Net > 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.

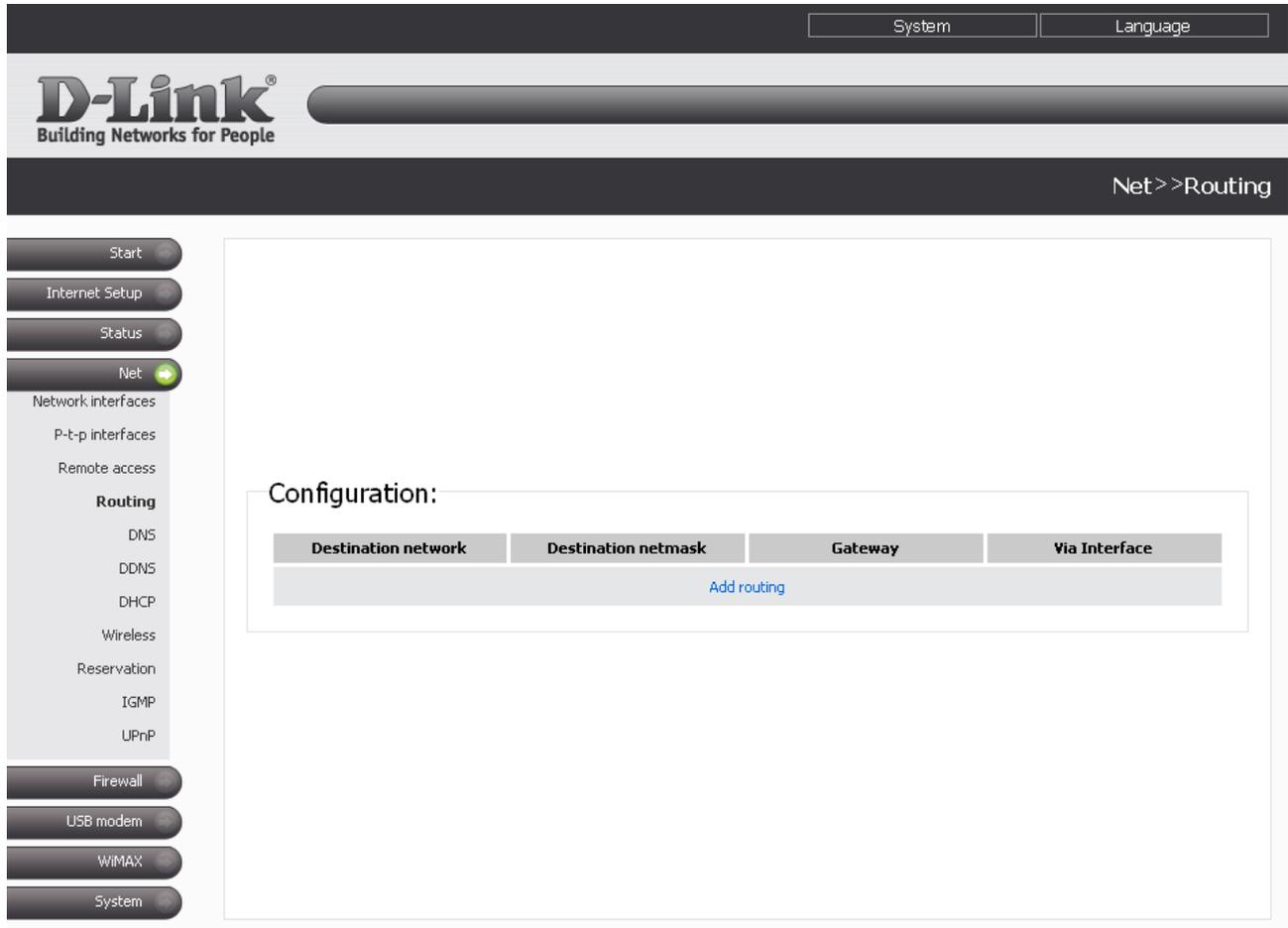


Figure 27. The **Net > Routing** page.

To create a new route, click the **Add routing** link.

**Configuration:**

| Parameter           | Value  | Sample        |
|---------------------|--|---------------|
| Destination network | <input type="text"/>                           | 192.168.0.0   |
| Destination netmask | <input type="text"/>                           | 255.255.255.0 |
| Gateway             | <input type="text"/>                           | 192.168.1.100 |
| Metric              | <input type="text"/>                           | 1             |
| Via Interface       | Automatically <input type="button" value="v"/> |               |

Figure 28. The page for adding a static route.

You can specify the following parameters:

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

Click the **Change** button.

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

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

## Name Servers

On the **Net > DNS** page, you can add DNS servers to the system. Also you can add domains to the search list.

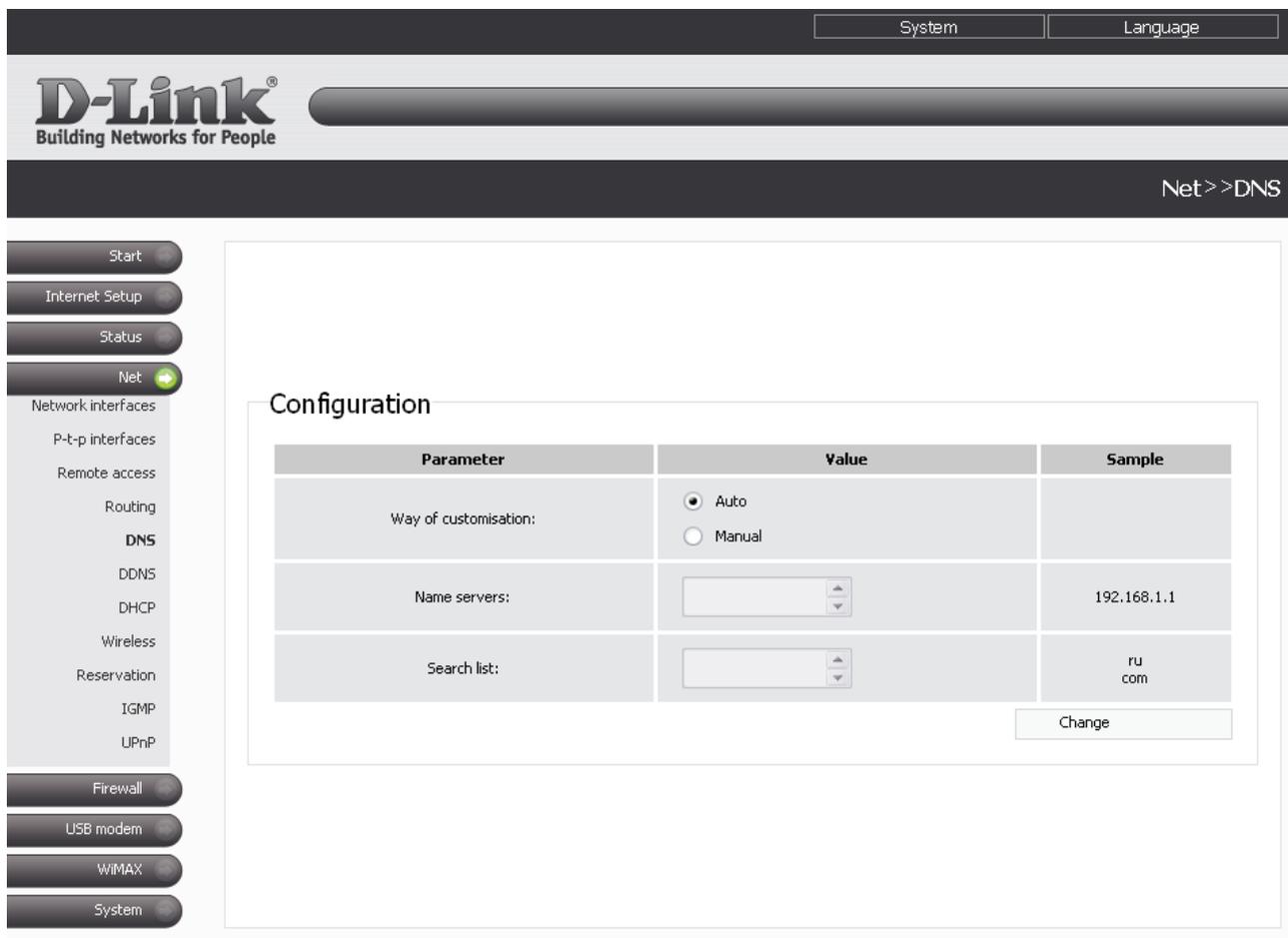


Figure 29. The **Net > DNS** page.

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 search list is used to automatically add top-level and second-level domains when a user enters an incomplete URL (e.g., if the field value is **.com**, and a user enters **google** in the address bar, then it is automatically substituted by **google.com**).

When you use the built-in DHCP server, the network parameters (including DNS servers) are distributed to clients automatically.



External DNS servers are automatically specified in the system when the router connects to a provider.

If you want to configure automatic obtainment of DNS servers addresses, select the **Auto** choice of the **Way of customisation** radio button and click the **Change** button.

If you want to set addresses of DNS servers and search list domains manually, select the **Manual** choice of the **Way of customisation** radio button, enter a DNS server address in the **Name servers** list, enter domains in the **Search list** fields, and click the **Change** button.

To remove a DNS server from the system or a domain from the search list, remove the relevant line from the **Name servers** field or the **Search list** field, and then click the **Change** button.

## DDNS

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

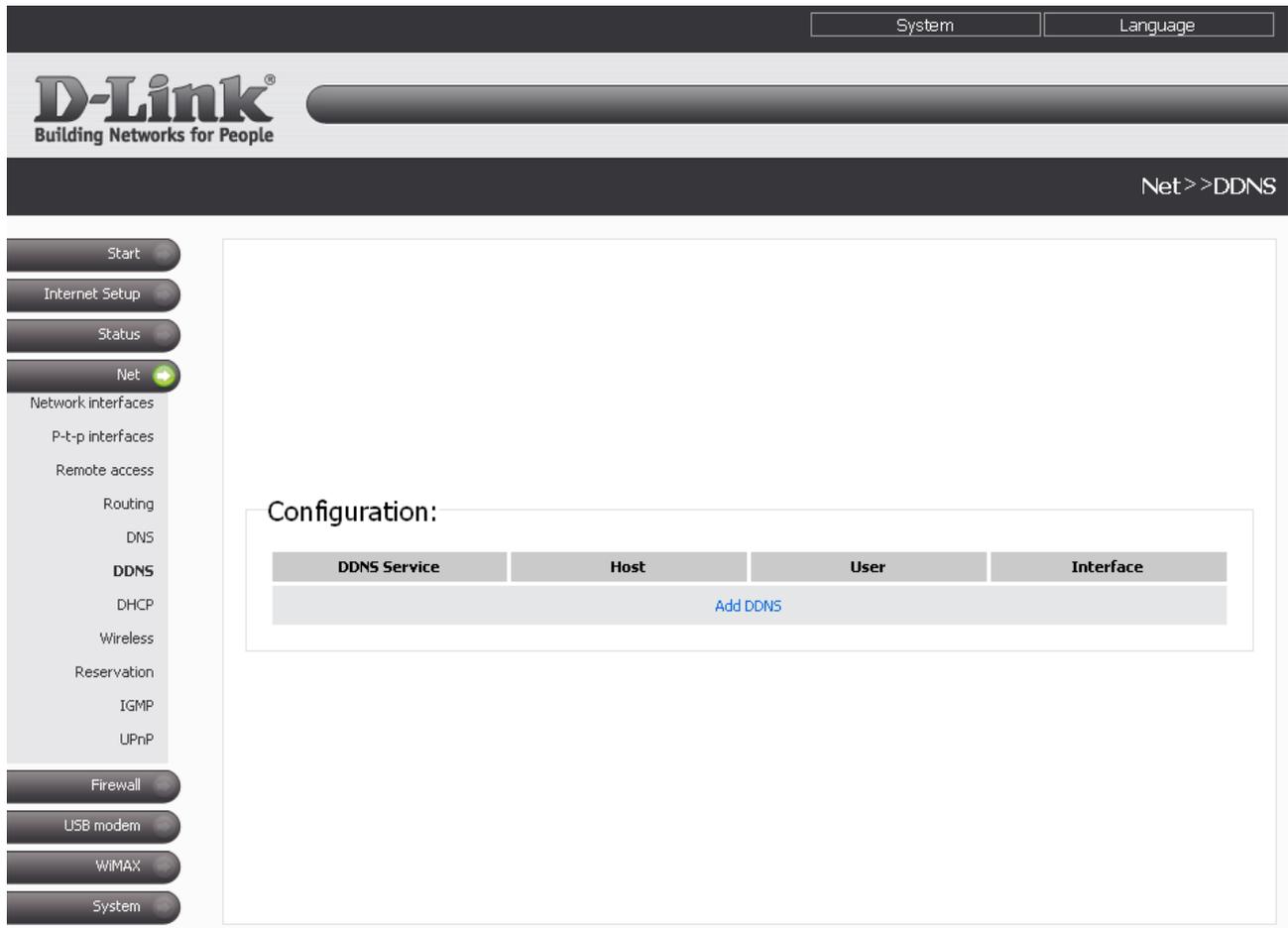


Figure 30. The **Net > DDNS** page.

To add a new DDNS service, follow the **Add DDNS** link.

**Configuration:**

| Parameter     | Value                |
|---------------|----------------------|
| DDNS Service: | DynDNS.org ▼         |
| Host:         | <input type="text"/> |
| User:         | <input type="text"/> |
| Password:     | <input type="text"/> |
| Interface:    | LAN1(ports 1-4) ▼    |

Figure 31. The page for adding a DDNS service.

You can specify the following parameters:

| Parameter           | Description   |
|---------------------|---|
| <b>DDNS Service</b> | Select a DDNS provider from the drop-down list.                               |
| <b>Host</b>         | The domain name registered at your DDNS provider.                             |
| <b>User</b>         | The username to authorize for your DDNS provider.                             |
| <b>Password</b>     | The password to authorize for your DDNS provider.                             |
| <b>Interface</b>    | Select an interface which IP address will be used to access the 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.

## DHCP

On the **Net > DHCP** page, you can modify parameters of the built-in DHCP server and set or edit MAC address and IP address pairs.

Static DHCP:

| MAC address                       | IP address    |
|-----------------------------------|---------------|
| <a href="#">00:01:29:ff:ac:44</a> | 192.168.0.101 |
| <a href="#">00:1d:92:c6:35:82</a> | 192.168.0.122 |

[Add](#)

DHCP server:

| Name                              | Interface | Start address | End address   |
|-----------------------------------|-----------|---------------|---------------|
| <a href="#">auto dhcpd on br0</a> | br0       | 192.168.1.100 | 192.168.1.199 |

Figure 32. The **Net > DHCP** page.

To create a MAC-IP pair (set a fixed IP address in the local area network for a device with a certain MAC address), click the **Add** link in the **Static DHCP** section. On the opened page, enter the relevant values in the **MAC address** and **IP address** fields. Then click the **Change** button.

Configuration:

| Parameter    | Value                |
|--------------|----------------------|
| MAC address: | <input type="text"/> |
| IP address:  | <input type="text"/> |

Figure 33. The page for adding a MAC-IP pair.

The existing MAC-IP pairs are displayed in the **Static DHCP** section on the **Net > DHCP** page. To remove an existing MAC-IP pair, follow the relevant MAC address link and click the **Delete** button.

**!** By default, the DHCP server for the LAN interface is configured in the system.

To edit the parameters of the existing DHCP server, follow the link with the name of the server.

**DHCP server:**

|                |                   |
|----------------|-------------------|
| Name:          | auto dhcpd on br0 |
| Interface:     | br0               |
| Start address: | 192.168.0.100     |
| End address:   | 192.168.0.199     |
| Lease time:    | 10800 min.        |
| Subnet:        | 255.255.255.0     |
| Broadcast:     | 192.168.0.1       |
| Router:        | 192.168.0.1       |
| DNS:           | 192.168.62.209    |
| Max leases:    | 100               |

Figure 34. The page for editing the DHCP server.

You can specify the following parameters:

| Parameter            |  | Description  |
|----------------------|--|--|
| <b>Name</b>          |  | A name for the DHCP server for easier identification.  |
| <b>Interface</b>     |  | A physical interface of the router to which this DHCP server is assigned. The field is available upon creation of a new DHCP server.   |
| <b>Start address</b> |  | The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.  |
| <b>End address</b>   |  | The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.  |
| <b>Lease time</b>    |  | The lifetime of IP addresses leased by the DHCP server, in minutes. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address). |
| <b>Subnet</b>        |  | A mask for the address pool.   |
| <b>Broadcast</b>     |  | An IP address for broadcast packets.   |
| <b>Gateway</b>       |  | The IP address of the default gateway for the DHCP server.   |
| <b>DNS</b>           |  | The name server IP address distributed by the DHCP server.   |
| <b>Max leases</b>    |  | The number of IP addresses in the address pool of the DHCP server.   |

Click the **Change** button.

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

To create a DHCP server, click the **Add DHCP** link. On the opened page, specify the needed parameters and click the **Change** button.

## Wireless

On the **Net > Wireless** page, you can configure all settings of your wireless local area network (WLAN).

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

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

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

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

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

### Basic Settings

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

Wireless

|                 |                                     |
|-----------------|-------------------------------------|
| Enable Wireless | <input checked="" type="checkbox"/> |
| MBSSID:         | Disabled                            |
| BSSID:          | 00:17:9A:12:12:14                   |

Basic settings | Security settings | MAC Filters | Clients List | WPS | WDS | Advanced settings | WMM | Client

|                         |                          |
|-------------------------|--------------------------|
| Hide Access Point:      | <input type="checkbox"/> |
| SSID:                   | DIR-620                  |
| Country:                | RUSSIAN FEDERATION       |
| Channel:                | 6                        |
| Wireless mode:          | 802.11 B/G/N mixed       |
| Max Associated Clients: | 0                        |

Change

Figure 35. Basic settings of the wireless LAN.

| Parameter                     | Description   |
|-------------------------------|---|
| <b>Hide Access Point</b>      | If the checkbox is selected, other users cannot see your Wi-Fi network. (It is recommended not to select this checkbox in order to simplify initial configuration of your WLAN.)  |
| <b>SSID</b>                   | A name for the WLAN. By default, the value <b>DIR-620</b> is specified. If your network is spitted into parts, each part has the default name ( <b>DIR-620.2</b> , <b>DIR-620.3</b> , and <b>DIR-620.4</b> ). It is recommended to specify another name for the network upon initial configuration (use digits and Latin characters). |
| <b>Country</b>                | The country you are in. Select a value from the drop-down list.   |
| <b>Channel</b>                | The wireless channel number. By default, channel 6 is specified. If you want to use another channel, select a value from the drop-down list. When the <b>auto</b> value is selected, the router itself chooses the channel with the least interference.   |
| <b>Wireless mode</b>          | Operating mode of the router's wireless network. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.  |
| <b>Max Associated Clients</b> | The maximum number of devices connected to the wireless network of the router. When the value <b>0</b> is specified, the router does not limit the number of connected clients.   |

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

### Security Settings

On the **Security settings** tab, you can modify security settings of the WLAN.

Wireless

|                 |                                     |
|-----------------|-------------------------------------|
| Enable Wireless | <input checked="" type="checkbox"/> |
| MBSSID:         | Disabled                            |
| BSSID:          | 00:17:9A:12:12:14                   |

|                |                   |             |              |     |     |                   |     |        |
|----------------|-------------------|-------------|--------------|-----|-----|-------------------|-----|--------|
| Basic settings | Security settings | MAC Filters | Clients List | WPS | WDS | Advanced settings | WMM | Client |
|----------------|-------------------|-------------|--------------|-----|-----|-------------------|-----|--------|

|                         |                          |
|-------------------------|--------------------------|
| Network Authentication: | Open                     |
| Enable Encryption WEP:  | <input type="checkbox"/> |

Change

Figure 36. The default security settings.

By default, the **Open** network authentication type with no encryption is specified for the WLAN (or every part of 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).

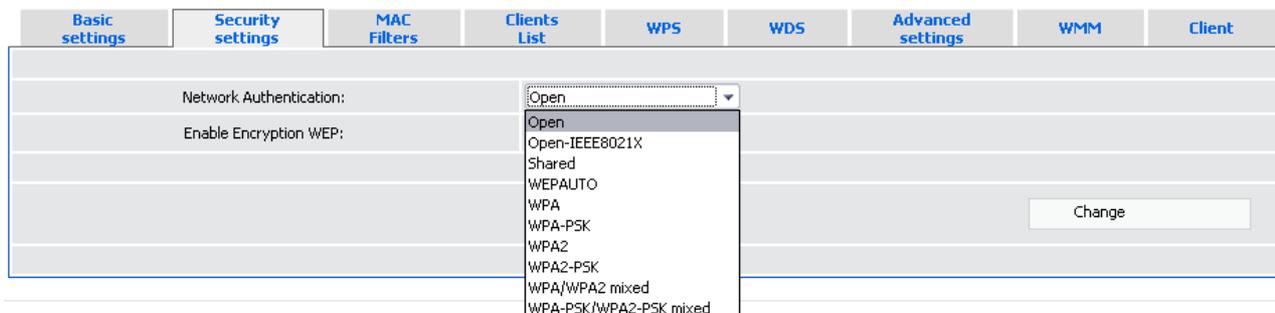


Figure 37. Network authentication types supported by the router.

The router supports the following authentication types:

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

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

When the **Open**, **Shared**, or **WEPAUTO** values are selected, the following fields are available:

| Basic settings          | Security settings | MAC Filters                         | Clients List | WPS | WDS | Advanced settings | WMM | Client |
|-------------------------|-------------------|-------------------------------------|--------------|-----|-----|-------------------|-----|--------|
| Network Authentication: |                   | Open                                |              |     |     |                   |     |        |
| Enable Encryption WEP:  |                   | <input checked="" type="checkbox"/> |              |     |     |                   |     |        |
| Default Key ID:         |                   | 1                                   |              |     |     |                   |     |        |
| Encryption Key WEP(1):  |                   | 12345                               |              |     |     |                   |     |        |
| Encryption Key WEP(2):  |                   | 23456                               |              |     |     |                   |     |        |
| Encryption Key WEP(3):  |                   | 34567                               |              |     |     |                   |     |        |
| Encryption Key WEP(4):  |                   | 45678                               |              |     |     |                   |     |        |
|                         |                   |                                     |              |     |     |                   |     | Change |

Figure 38. The **Open** value is selected from the **Network Authentication** drop-down list.

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

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

| Basic settings          | Security settings | MAC Filters                         | Clients List | WPS | WDS | Advanced settings | WMM | Client |
|-------------------------|-------------------|-------------------------------------|--------------|-----|-----|-------------------|-----|--------|
| Network Authentication: |                   | Open-IEEE8021X                      |              |     |     |                   |     |        |
| Enable Encryption WEP:  |                   | <input checked="" type="checkbox"/> |              |     |     |                   |     |        |
| Default Key ID:         |                   | 1                                   |              |     |     |                   |     |        |
| Encryption Key WEP(1):  |                   | 12345                               |              |     |     |                   |     |        |
| Encryption Key WEP(2):  |                   | 23456                               |              |     |     |                   |     |        |
| Encryption Key WEP(3):  |                   | 34567                               |              |     |     |                   |     |        |
| Encryption Key WEP(4):  |                   | 45678                               |              |     |     |                   |     |        |
| RADIUS IP:              |                   | 192.168.0.254                       |              |     |     |                   |     |        |
| RADIUS net port:        |                   | 1812                                |              |     |     |                   |     |        |
| RADIUS encryption key:  |                   | nokey                               |              |     |     |                   |     |        |
|                         |                   |                                     |              |     |     |                   |     | Change |

Figure 39. The **Open-IEEE8021X** value is selected from the **Network Authentication** drop-down list.

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

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

| Basic settings           | Security settings | MAC Filters                         | Clients List | WPS | WDS | Advanced settings | WMM | Client |
|--------------------------|-------------------|-------------------------------------|--------------|-----|-----|-------------------|-----|--------|
| Network Authentication:  |                   | WPA2-PSK                            |              |     |     |                   |     |        |
| Encryption Key PSK:      |                   | 12345678                            |              |     |     |                   |     |        |
| WPA2 Pre-authentication: |                   | <input checked="" type="checkbox"/> |              |     |     |                   |     |        |
| WPA Encryption:          |                   | TKIP                                |              |     |     |                   |     |        |
| WPA renewal:             |                   | 3600                                |              |     |     |                   |     |        |
|                          |                   |                                     |              |     |     |                   |     | Change |

Figure 40. The **WPA2-PSK** value is selected from the **Network Authentication** drop-down list.

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

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

| Basic settings           | Security settings | MAC Filters | Clients List | WPS                                 | WDS | Advanced settings | WMM | Client |
|--------------------------|-------------------|-------------|--------------|-------------------------------------|-----|-------------------|-----|--------|
| Network Authentication:  |                   |             |              | WPA2                                |     |                   |     |        |
| RADIUS IP:               |                   |             |              | 192.168.0.254                       |     |                   |     |        |
| RADIUS net port:         |                   |             |              | 1812                                |     |                   |     |        |
| RADIUS encryption key:   |                   |             |              | nokey                               |     |                   |     |        |
| WPA2 Pre-authentication: |                   |             |              | <input checked="" type="checkbox"/> |     |                   |     |        |
| WPA Encryption:          |                   |             |              | TKIP                                |     |                   |     |        |
| WPA renewal:             |                   |             |              | 3600                                |     |                   |     |        |
|                          |                   |             |              |                                     |     | Change            |     |        |

Figure 41. The **WPA2** value is selected from the **Network Authentication** drop-down list.

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

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

## MAC Filters

On the **MAC Filters** tab, you can define a set of MAC addresses of devices which will be allowed to access the WLAN, or define MAC addresses of devices which will not be allowed to access the WLAN.

Wireless

Enable Wireless

MBSSID: Disabled

BSSID: 00:0C:43:30:52:88

Basic settings Security settings **MAC Filters** Clients List WPS WDS Advanced settings WMM Client

MAC Restrict Mode: Disabled:  Allow:  Deny:

| MAC Address | Remove                   |
|-------------|--------------------------|
|             | <input type="checkbox"/> |

Add MAC Address:

Figure 42. MAC filters for the wireless network.

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

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

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

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

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

## Clients List

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

Wireless

|                 |                                     |
|-----------------|-------------------------------------|
| Enable Wireless | <input checked="" type="checkbox"/> |
| MBSSID:         | Disabled                            |
| BSSID:          | 00:0C:43:30:52:88                   |

|                |                   |             |                     |     |     |                   |      |            |
|----------------|-------------------|-------------|---------------------|-----|-----|-------------------|------|------------|
| Basic settings | Security settings | MAC Filters | <b>Clients List</b> | WPS | WDS | Advanced settings | WMM  | Client     |
| MAC            | AID               | PSM         | MIMOPS              | MCS | BW  | SGI               | STBC | Disconnect |
| Refresh        |                   |             |                     |     |     |                   |      |            |

Figure 43. The list of the router's wireless clients.

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

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

## WPS

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

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

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

**!** Before using the WPS function it is required to configure a type of WPA encryption.

### Wireless

|                        |                     |                                     |
|------------------------|---------------------|-------------------------------------|
| <b>Enable Wireless</b> |                     | <input checked="" type="checkbox"/> |
| MBSSID:                | Disabled ▾          |                                     |
| BSSID:                 | 00:17:9A:12:12:14 ▾ |                                     |

|                                |                                   |                             |                              |            |                     |                                   |                     |                        |
|--------------------------------|-----------------------------------|-----------------------------|------------------------------|------------|---------------------|-----------------------------------|---------------------|------------------------|
| <a href="#">Basic settings</a> | <a href="#">Security settings</a> | <a href="#">MAC Filters</a> | <a href="#">Clients List</a> | <b>WPS</b> | <a href="#">WDS</a> | <a href="#">Advanced settings</a> | <a href="#">WMM</a> | <a href="#">Client</a> |
|--------------------------------|-----------------------------------|-----------------------------|------------------------------|------------|---------------------|-----------------------------------|---------------------|------------------------|

|   |                                     |
|---|-------------------------------------|
| WPS Enable:   | <input checked="" type="checkbox"/> |
| WPS Status:   | Unconfigured                        |
| SSID:   | DIR-620                             |
| Network Authentication:   | Open                                |
| Encryption:   | None                                |
| <input type="button" value="Refresh"/> <input type="button" value="Reset to unconfigured"/> |                                     |
| WPS Method:   | PBC ▾                               |
| PIN Code:   | <input type="text"/>                |
| <input type="button" value="Connect"/>  |                                     |

Figure 44. The tab for configuring the WPS function.

The following fields are available on the tab:

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

### Using WPS Function via Web-based Interface

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

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

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

1. Select the **WPS** checkbox.
2. Select the **PBC** value from the **WPS Method** drop-down list.
3. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
4. Click the relevant button in the software or on the cover of the wireless device that you want to connect to the WLAN.
5. Click the **Connect** button in the web-based interface of the router.

### Using WPS Function without Web-based Interface

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

1. Configure a type of WPA encryption for the WLAN (or the first part of the WLAN).
2. Select the **WPS** checkbox.
3. Make sure that the **PBC** value is selected from the **WPS Method** drop-down list.
4. Save the settings and close the web-based interface (click the **Save** line in the top-page menu displayed when the mouse pointer is over the **System** caption, then click the **Logout** line).

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

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

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

## WDS

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

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

Wireless

|                        |                                     |
|------------------------|-------------------------------------|
| <b>Enable Wireless</b> | <input checked="" type="checkbox"/> |
| MBSSID:                | Disabled                            |
| BSSID:                 | 00:0C:43:30:52:88                   |

| Basic settings  | Security settings | MAC Filters          | Clients List | WPS | WDS | Advanced settings | WMM | Client |
|-----------------|-------------------|----------------------|--------------|-----|-----|-------------------|-----|--------|
| WDS Mode:       |                   | Bridge mode          |              |     |     |                   |     |        |
| WDS Phy Mode:   |                   | GREENFIELD           |              |     |     |                   |     |        |
| WDS Encryption: |                   | NONE                 |              |     |     |                   |     |        |
| WDS MAC(1):     |                   | 00:0C:43:30:52:E     |              |     |     |                   |     |        |
| WDS MAC(2):     |                   | <input type="text"/> |              |     |     |                   |     |        |
| WDS MAC(3):     |                   | <input type="text"/> |              |     |     |                   |     |        |
| WDS MAC(4):     |                   | <input type="text"/> |              |     |     |                   |     |        |
|                 |                   |                      |              |     |     |                   |     | Change |

Figure 45. The tab for configuring the WDS function.

The following fields are available on the tab:

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

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

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

## Advanced Settings

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

**!** Changing parameters presented on this tab may negatively effect your WLAN!

Wireless

|                 |                                     |
|-----------------|-------------------------------------|
| Enable Wireless | <input checked="" type="checkbox"/> |
| MBSSID:         | Disabled                            |
| BSSID:          | 00:0C:43:30:52:88                   |

| Basic settings      | Security settings | MAC Filters | Clients List | WPS | WDS | Advanced settings    | WMM                                   | Client |  |
|---------------------|-------------------|-------------|--------------|-----|-----|----------------------|---------------------------------------|--------|--|
| Station Keep Alive: |                   |             |              |     |     | <input type="text"/> |                                       |        |  |
| Beacon Period:      |                   |             |              |     |     | 100                  |                                       |        |  |
| RTS Threshold:      |                   |             |              |     |     | 2347                 |                                       |        |  |
| Frag Threshold:     |                   |             |              |     |     | 2346                 |                                       |        |  |
| DTIM Period:        |                   |             |              |     |     | 1                    |                                       |        |  |
| TX Power:           |                   |             |              |     |     | 100                  |                                       |        |  |
| BG Protection:      |                   |             |              |     |     | Auto                 |                                       |        |  |
| TX Preamble:        |                   |             |              |     |     | Long Preamble        |                                       |        |  |
|                     |                   |             |              |     |     |                      | <input type="button" value="Change"/> |        |  |

Figure 46. Advanced settings of the WLAN.

The following fields are available on the tab:

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

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

## WMM

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

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

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

Wireless

|                 |                   |                                     |  |
|-----------------|-------------------|-------------------------------------|--|
| Enable Wireless |                   | <input checked="" type="checkbox"/> |  |
| MBSSID:         | Disabled          |                                     |  |
| BSSID:          | 00:0C:43:30:52:88 |                                     |  |

|                |                   |             |              |     |     |                   |            |        |
|----------------|-------------------|-------------|--------------|-----|-----|-------------------|------------|--------|
| Basic settings | Security settings | MAC Filters | Clients List | WPS | WDS | Advanced settings | <b>WMM</b> | Client |
|----------------|-------------------|-------------|--------------|-----|-----|-------------------|------------|--------|

WMM:

**WMM Parameters of Access Point:**

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

**WMM Parameters of Station:**

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

Change

Figure 47. The tab for configuring the WMM function.

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

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

- **AC\_BK** (*Background*), low priority traffic (print jobs, file downloads, etc.).
- **AC\_BE** (*Best Effort*), traffic from legacy devices or devices/applications that do not support QoS.
- **AC\_VI** (*Video*).
- **AC\_VO** (*Voice*).

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

For every Access Category the following fields are available:

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

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

## Client

On the **Client** tab, you can configure the router as a client to connect to a wireless access point.

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

Wireless

|                 |                                     |
|-----------------|-------------------------------------|
| Enable Wireless | <input checked="" type="checkbox"/> |
| MBSSID:         | Disabled                            |
| BSSID:          | 00:17:9A:12:12:14                   |

|                |                                     |             |                      |        |                      |                         |      |                        |                          |
|----------------|-------------------------------------|-------------|----------------------|--------|----------------------|-------------------------|------|------------------------|--------------------------|
| Basic settings | Security settings                   | MAC Filters | Client List          | WPS    | WDS                  | Advanced settings       | WMM  | Client                 |                          |
| Client:        | <input checked="" type="checkbox"/> | SSID:       | <input type="text"/> | BSSID: | <input type="text"/> | Network Authentication: | Open | Enable Encryption WEP: | <input type="checkbox"/> |
| Change         |                                     |             |                      |        |                      |                         |      |                        |                          |

Figure 48. The tab for configuring the client mode.

The following fields are available on the tab:

| Parameter                     | Description  |
|-------------------------------|--|
| <b>Client</b>                 | Select the checkbox to configure the router as a client.             |
| <b>SSID</b>                   | The name of the network to which the router connects.                |
| <b>BSSID</b>                  | The unique identifier of the network to which the router connects.   |
| <b>Network Authentication</b> | The authentication type of the network to which the router connects. |

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

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

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

| Parameter             | Description                                       |
|-----------------------|---|
| <b>WPA Encryption</b> | An encryption method: <b>TKIP</b> or <b>AES</b> . |
| <b>Encryption Key</b> | A key for WPA encryption.                         |

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

## Reservation

On the **Net > Reservation** page, you can enable reservation of a channel to access the Internet. Due to this function, you can constantly access the Internet, even when your main connection is not available.

The screenshot shows the D-Link web interface for the 'Reservation' configuration page. The page title is 'Net > Reservation'. The left sidebar contains a navigation menu with the following items: Start, Internet Setup, Status, Net (highlighted with a green arrow), Network interfaces, P-t-p interfaces, Remote access, Routing, DNS, DDNS, DHCP, Wireless, **Reservation**, IGMP, UPnP, Firewall, USB modem, WiMAX, and System. The main content area is titled 'Configuration:' and contains a table with the following data:

| Name                 | Value                                      | Comments   |
|----------------------|--|--|
| Reservation:         | <input type="checkbox"/>                   | Enable/disable reservation                           |
| IP for checks (1):   | <input type="text" value="217.69.128.43"/> | IP-address for checks                                |
| IP for checks (2):   | <input type="text" value="217.69.128.44"/> | IP-address for checks                                |
| Time (sec.):         | <input type="text" value="15"/>            | Time between checks in seconds                       |
| Watch route:         | <input type="text" value="default"/>       | Watch route ("default" or like this: 192.168.1.0/24) |
| Connection type (1): | <input type="text" value="ether"/>         | Connection type                                      |
| Connection type (2): | <input type="text" value="3g"/>            | Connection type                                      |

A 'Change' button is located at the bottom right of the configuration table.

Figure 49. The **Net > Reservation** page.

To enable reservation of an additional channel, select the **Reservation** checkbox and set the parameters defining the reserve channel and the order of switching to it.

You can specify the following parameters:

| Parameter                     | Description  |
|-------------------------------|--|
| <b>IP for checks (1), (2)</b> | In these fields specify IP addresses from external network, which will be checked for availability. The system uses the results of these checks to define whether the main connection is active.   |
| <b>Time</b>                   | A time interval (in seconds) between availability checks of the IP addresses specified in the <b>IP for checks (1)</b> and <b>IP for checks (2)</b> fields.  |
| <b>Watch route</b>            | The route corresponding to the reserve channel. The <b>default</b> value represents the external network (the Internet). You can also define a specific network in the format <b>192.168.62.0/24</b> .   |
| <b>Connection type (1)</b>    | The main channel. Select a value from the drop-down list:<br><b>ether</b> : The WAN interface.<br><b>pptp</b> : A PPTP interface created on the <b>Net &gt; P-t-p interfaces</b> page.<br><b>pppoe</b> : A PPPoE interface created on the <b>Net &gt; P-t-p interfaces</b> page.<br><b>wimax</b> : The connection established via your WiMAX USB modem.<br><b>3g</b> : The connection established via your GSM or CDMA USB modem.    |
| <b>Connection type (2)</b>    | The reserve channel. Select a value from the drop-down list:<br><b>ether</b> : The WAN interface.<br><b>pptp</b> : A PPTP interface created on the <b>Net &gt; P-t-p interfaces</b> page.<br><b>pppoe</b> : A PPPoE interface created on the <b>Net &gt; P-t-p interfaces</b> page.<br><b>wimax</b> : The connection established via your WiMAX USB modem.<br><b>3g</b> : The connection established via your GSM or CDMA USB modem. |

Selecting a value from the **Connection type (1)** and **Connection type (2)** drop-down lists, make sure that the relevant interfaces are enabled and configured as needed.

Click the **Change** button.

To disable reservation of an additional channel, deselect the **Reservation** checkbox and click the **Change** button.

## IGMP

On the **Net > 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.

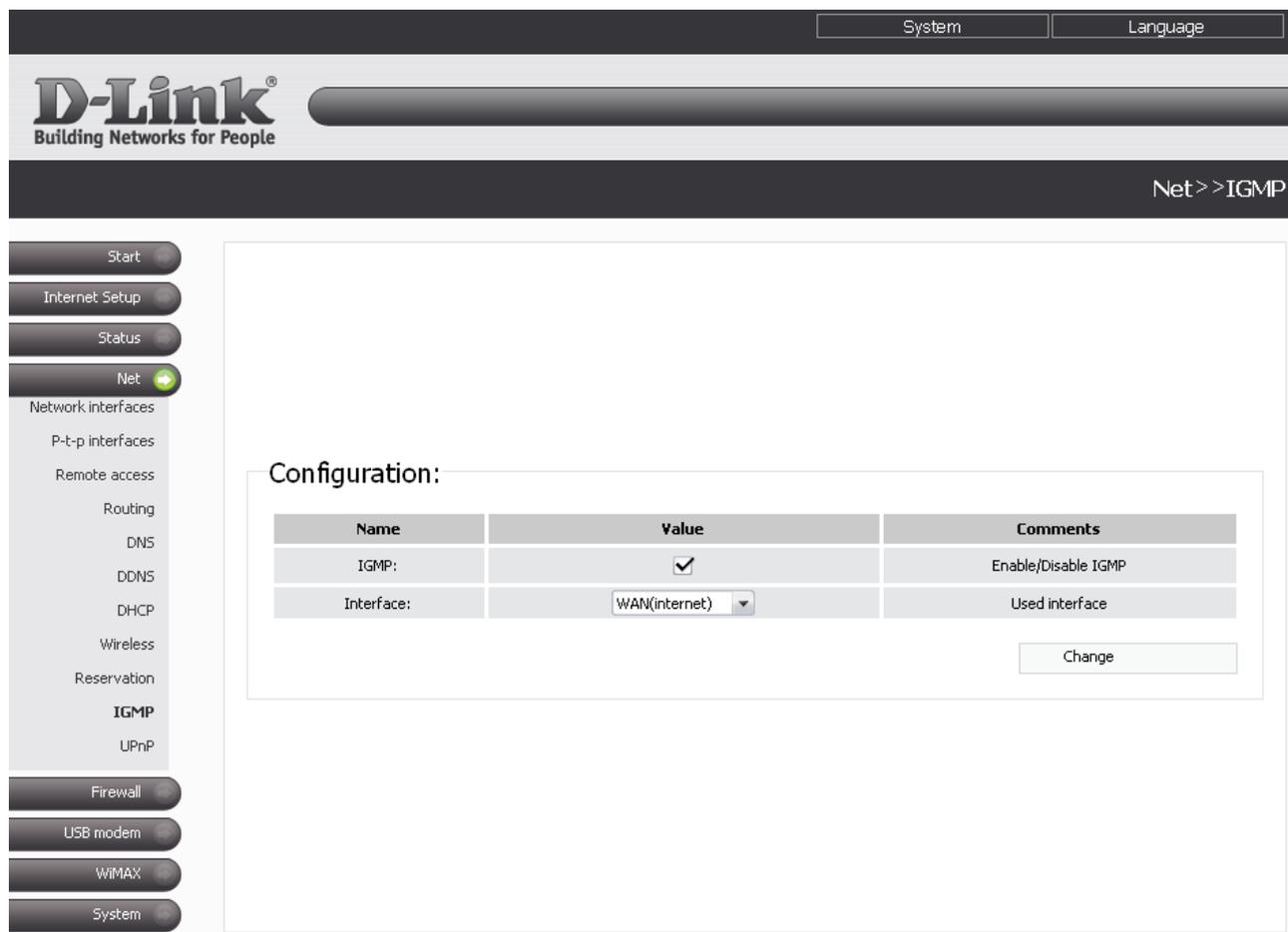


Figure 50. The **Net > IGMP** page.

To enable IGMP, select the **IGMP** checkbox. From the **Interface** drop-down list, select an interface from which the router will accept multicast traffic. Then click the **Change** button.

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

## UPnP

On the **Net > 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.

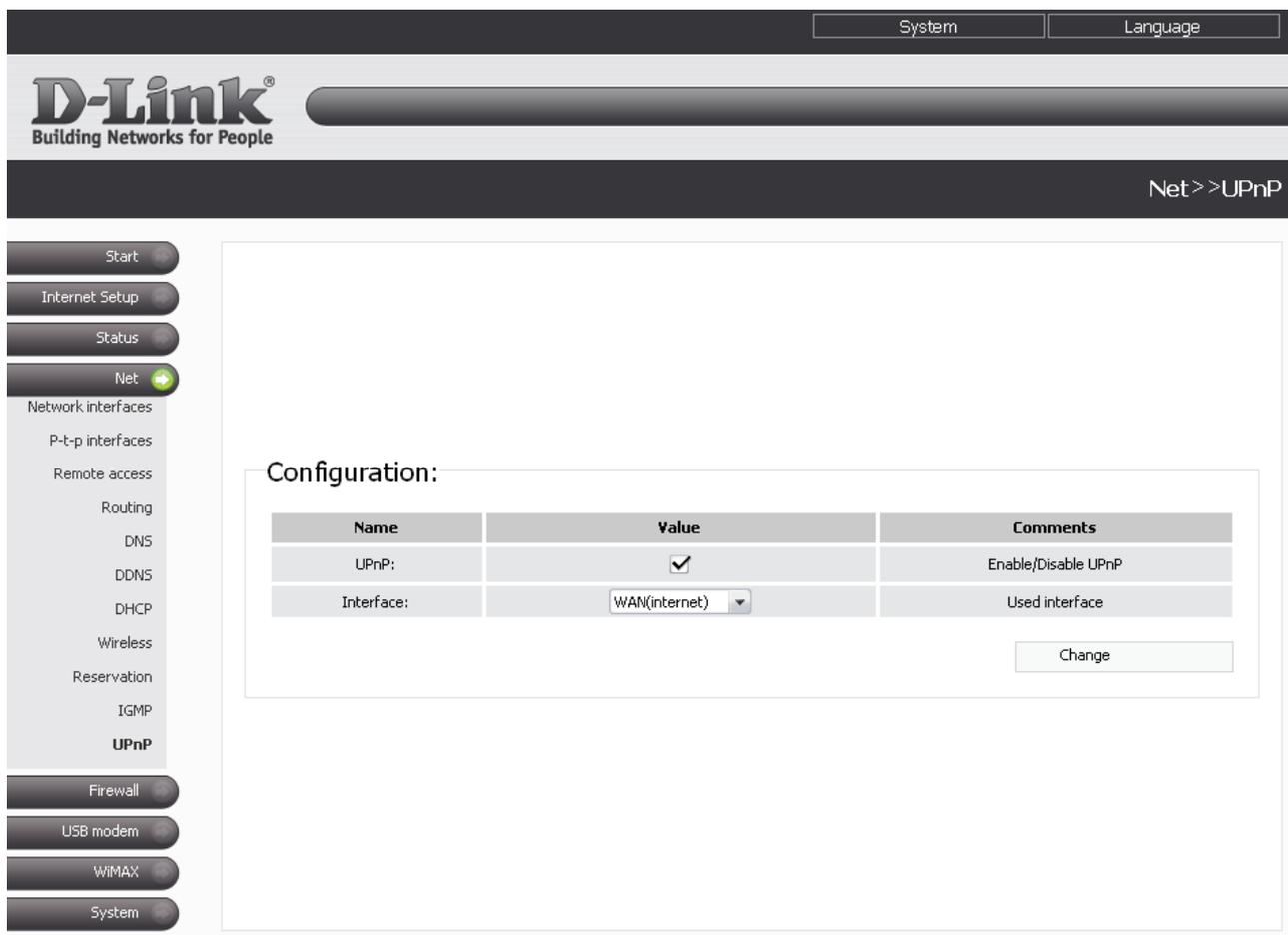


Figure 51. The **Net > UPnP** page.

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

If you want to enable the UPnP function in the router, select the **UPnP** 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.

## Firewall

In this menu you can configure the firewall of the router: add rules for IP filtering, define Dynamic NAT rules, and create virtual servers. In addition, you can add URL filters to the system, enable protection against ARP and DDoS attacks, and configure the Port Triggering function.

### IP Filters

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

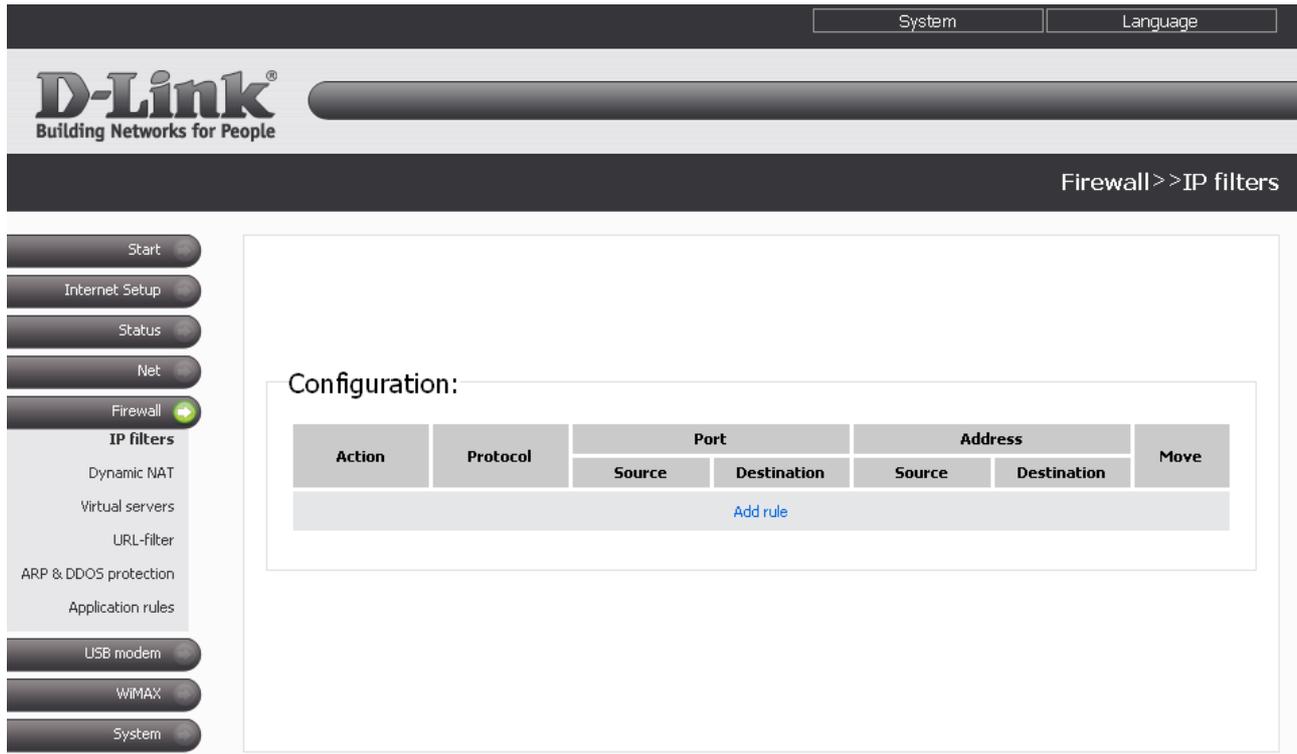


Figure 52. The **Firewall > IP filters** page.

Rules for IP filtering are presented as a table. The rules are processed in the listed order (downwards). The arrow buttons located to the right of the rule table are used to change the order of rules (to move a rule up or down).

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

**Configuration:**

| Parameter                                | Value   | Sample                        |
|--|---|-------------------------------|
| Action:                                  | ACCEPT ▾  |                               |
| Source IP address:                       | <input type="text"/>  | 192.168.1.0/24<br>192.168.1.1 |
| Destination IP:                          | <input type="text"/>  | 192.168.1.0/24<br>192.168.1.1 |
| Protocol:                                | <input checked="" type="radio"/> Main: tcp ▾<br><input type="radio"/> Other: <input type="text"/> | udp                           |
| Port "Source" (port or port range):      | <input type="text"/>  | 3400:3420                     |
| Port "Destination" (port or port range): | <input type="text"/>  | 3500:3520                     |

Figure 53. The page for adding a rule for IP filtering.

You can specify the following parameters:

| Parameter                | Description  |
|--------------------------|--|
| <b>Action</b>            | Select an action for the rule.<br><b>ACCEPT:</b> Allows packet transmission in accordance with the criteria specified by the rule.<br><b>DROP:</b> Denies packet transmission in accordance with the criteria specified by the rule.   |
| <b>Source IP address</b> | The source host/subnet IP address.   |
| <b>Destination IP</b>    | The destination host/subnet IP address.  |
| <b>Protocol</b>          | A protocol for network packet transmission. Select a value from the drop-down list available when the <b>Main</b> radio button is selected, or specify another protocol for network packet transmission (select the <b>Other</b> radio button and enter the name of the protocol in the field to the right of the radio button). |
| <b>Port "Source"</b>     | A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.   |

| Parameter                           | Description   |
|-------------------------------------|---|
| <b>Port</b><br><b>“Destination”</b> | A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon. |

Click the **Change** button.

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

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

## Dynamic NAT

On the **Firewall > Dynamic NAT** page, you can create rules for dynamic network address translation.

Dynamic NAT is a form of network address translation where the source address is set dynamically on the basis of the address specified for the interface.

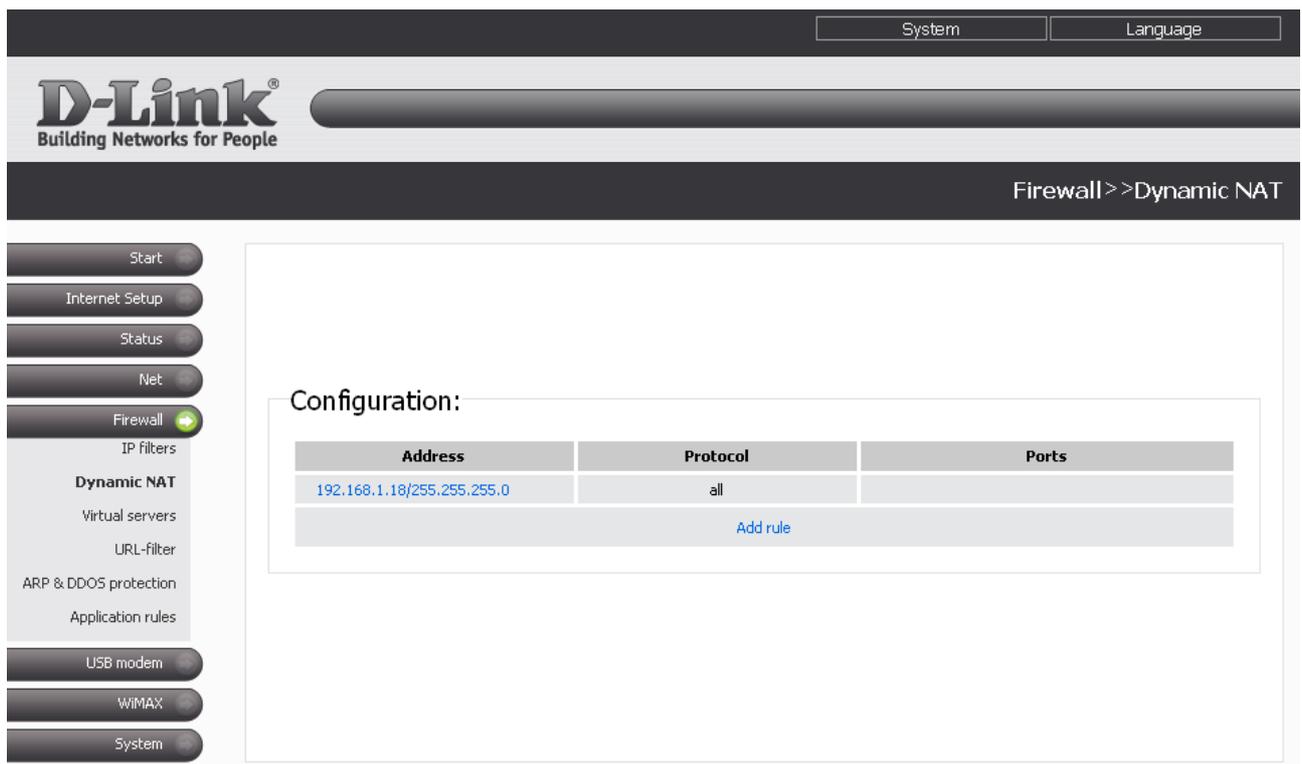


Figure 54. The **Firewall > Dynamic NAT** page.

To create a new rule for dynamic network address translation, click the **Add rule** link.

**Configuration:**

| Parameter | Value   | Sample                        |
|-----------|---|-------------------------------|
| Address:  | <input type="text"/>  | 192.168.0.0<br>192.168.0.0/24 |
| Protocol: | tcp <input type="button" value="v"/>                        | tcp                           |
|           | <input type="text"/> Main: <input checked="" type="radio"/> |                               |
|           | <input type="text"/> Other: <input type="radio"/>           |                               |
| Ports:    | <input type="text"/>  | 80<br>1024:2048               |

Figure 55. The page for adding a rule for dynamic network address translation.

You can specify the following parameters:

| Parameter       | Description  |
|-----------------|--|
| <b>Address</b>  | The IP subnet to which this rule will be applied.  |
| <b>Protocol</b> | A protocol for network address translation. Select a value from the drop-down list available when the <b>Main</b> radio button is selected, or specify another protocol for network address translation (select the <b>Other</b> radio button and enter the name of the protocol in the field to the right of the radio button). |
| <b>Ports</b>    | The ports for which the rule will be applied. 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 dynamic NAT, 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 dynamic NAT, click the link to the relevant rule. On the opened page, click the **Delete** button.

## Virtual Servers

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

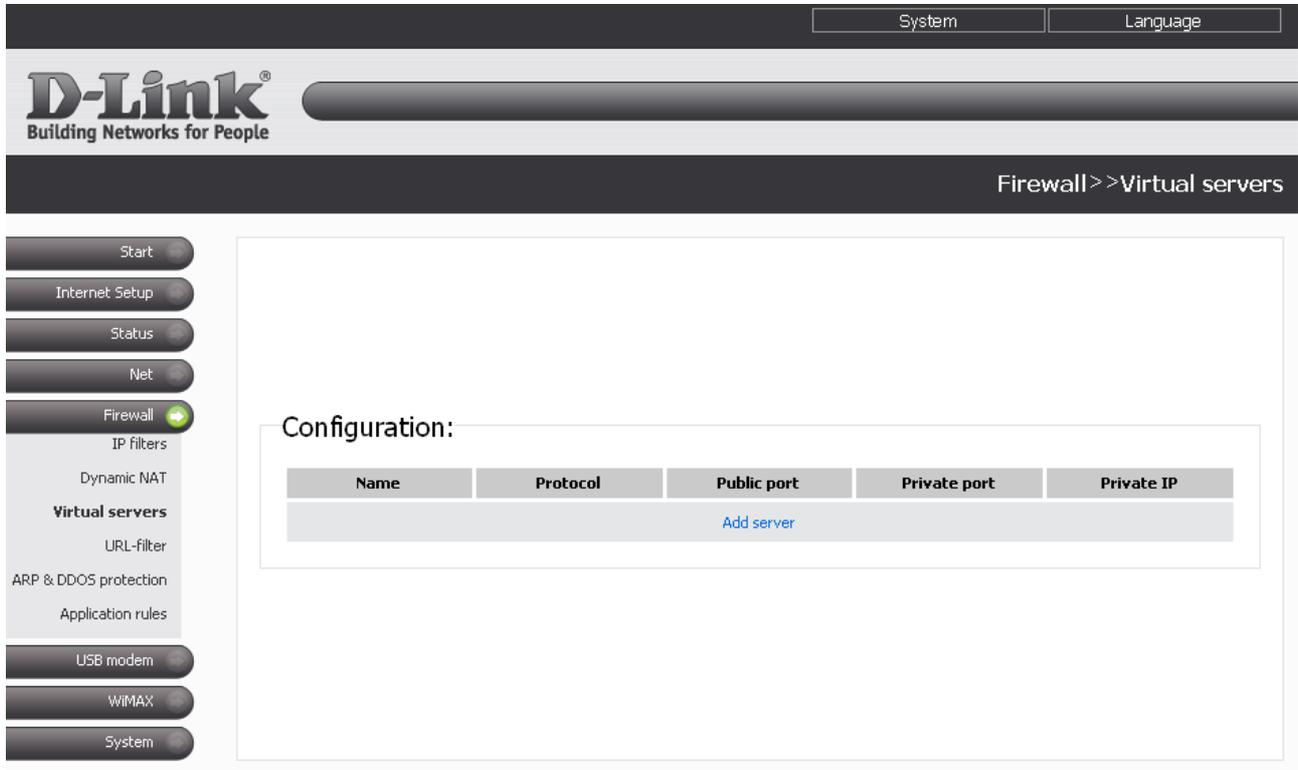


Figure 56. The **Firewall > Virtual servers** page.

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

**Configuration:**

| Name          | Value                | Sample      |
|---------------|----------------------|-------------|
| Template:     | <Custom>             |             |
| Name:         | <input type="text"/> | my_server   |
| Protocol:     | tcp                  |             |
| Public port:  | <input type="text"/> | 80          |
| Private port: | <input type="text"/> | 8080        |
| Private IP:   | <input type="text"/> | 192.168.1.2 |

Figure 57. The page for adding a virtual server.

You can specify the following parameters:

| Parameter           | Description   |
|---------------------|---|
| <b>Template</b>     | Select a virtual server template from the drop-down list, or select <b>&lt;Custom&gt;</b> to specify all parameters of the new virtual server manually. |
| <b>Name</b>         | A name for the virtual server for easier identification. You can specify any name.  |
| <b>Protocol</b>     | A protocol that will be used by the new virtual server. Select a value from the drop-down list.   |
| <b>Public port</b>  | A port of the router from which traffic is directed to the IP address specified in the <b>Private IP</b> field.   |
| <b>Private port</b> | A port of the IP address specified in the <b>Private IP</b> field to which traffic is directed from the <b>Private port</b> .                           |
| <b>Private IP</b>   | The IP address of the server from the local area network.   |

Click the **Change** button.

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

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

## URL Filter

On the **Firewall > URL-filter** page, you can define URL addresses, which will not be available for your LAN users.

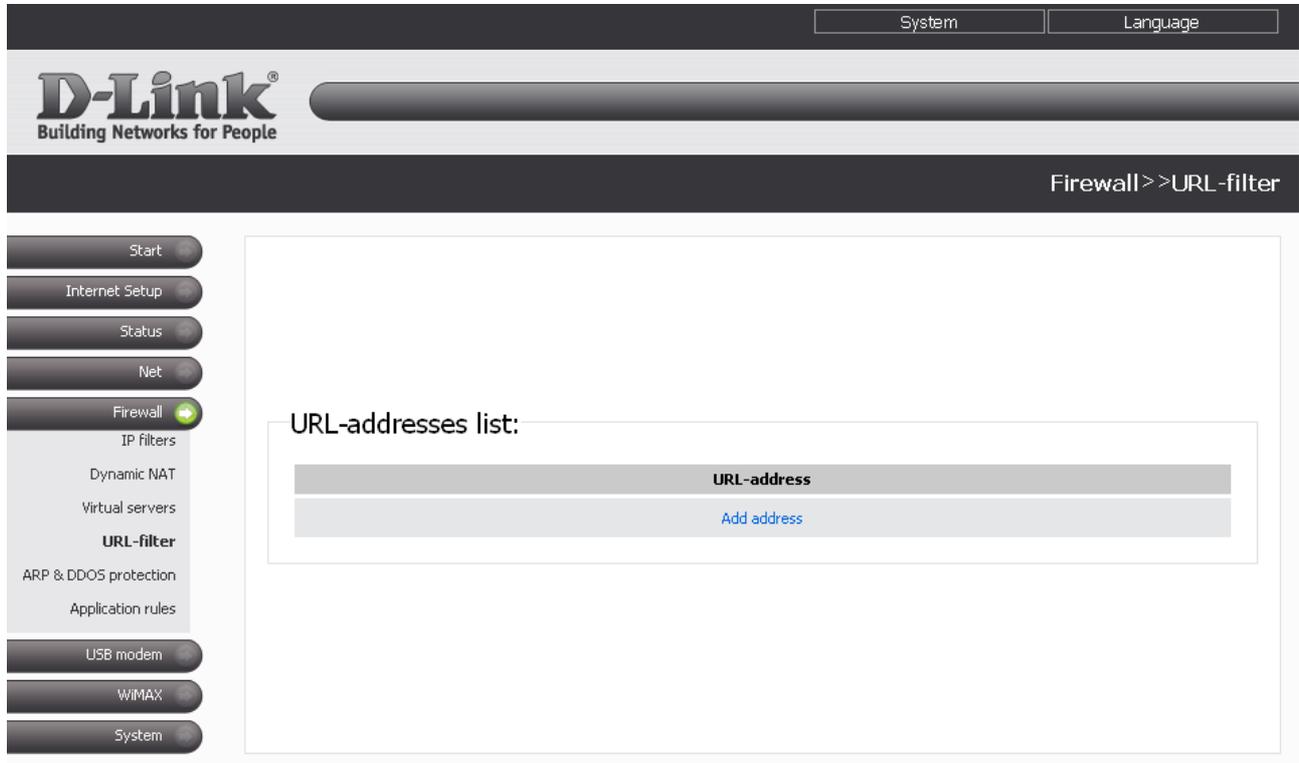


Figure 58. The **Firewall > URL-filter** page.

In order to forbid access to an URL address, click the **Add address** link.

Configuration:

| Name         | Value                | Sample   |
|--------------|----------------------|----------|
| URL-address: | <input type="text"/> | site.com |

Figure 59. A page for adding a forbidden URL.

On the opened page, enter an URL address which should be forbidden for your LAN users in the **URL address** field, then click the **Change** button.

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

## ARP and DDOS Protection

On the **Firewall > ARP & DDOS protection** page, you can enable an additional feature of the firewall, which helps you to protect your network from ARP and DDoS attacks.

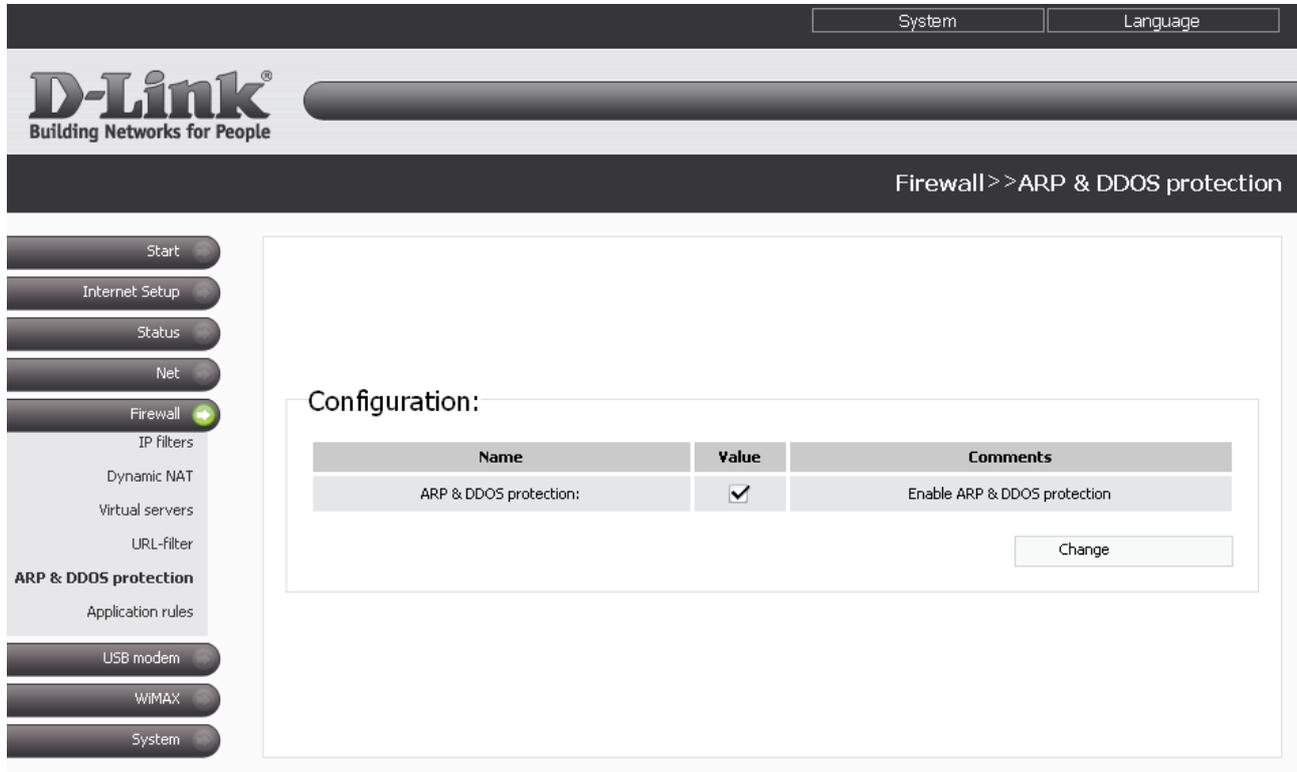


Figure 60. The **Firewall > ARP & DDOS protection** page.

To enable this function, select the **ARP & DDOS protection** checkbox and click the **Change** button.

To disable this function, deselect the **ARP & DDOS protection** checkbox and click the **Change** button.

## Application Rules

On the **Firewall > Application rules** page, you can define rules for the Port Triggering function.

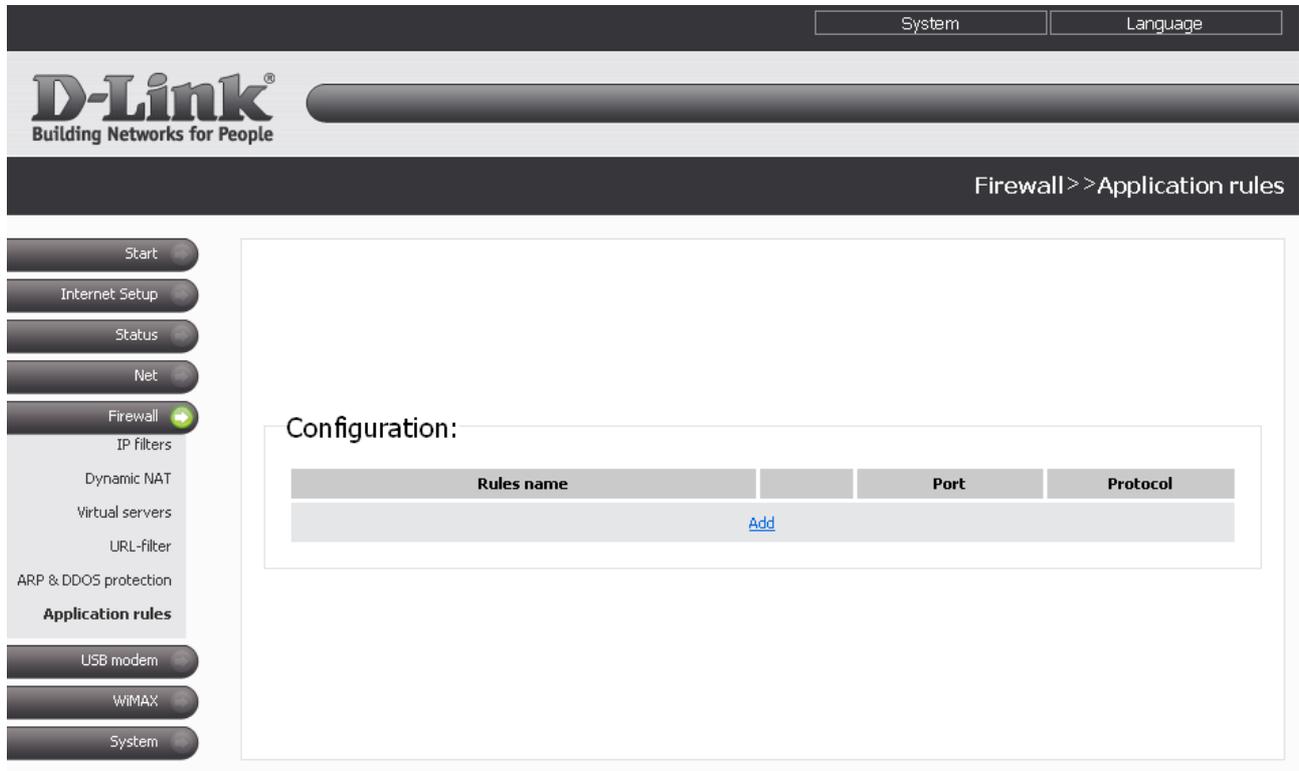


Figure 61. The **Firewall > Application rules** page.

To add a new rule for the Port Triggering function, click the **Add** link.

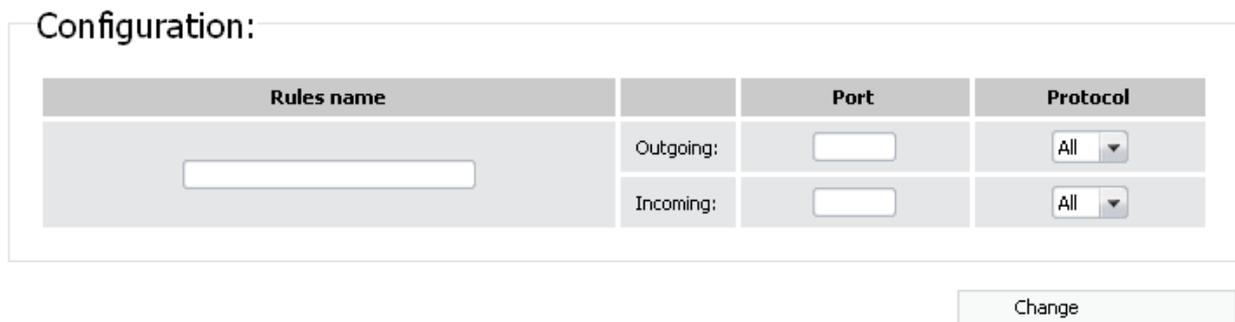


Figure 62. The page for adding a rule for the Port Triggering function.

You can specify the following parameters:

| Parameter         | Description  |
|-------------------|--|
| <b>Rules name</b> | A name for the rule for easier identification.   |
| <b>Outgoing</b>   | A port of the computer from your LAN, from which data are transferred to the external network (outgoing traffic). From the <b>Protocol</b> drop-down list located in this line, you can select a protocol to which this rule will be applied upon transferring data from the specified port. |
| <b>Incoming</b>   | A port of the router, which will be open to receive data from the external network (incoming traffic). From the <b>Protocol</b> drop-down list located in this line, you can select a protocol to which this rule will be applied upon receiving data to the specified port.                 |

Click the **Change** button.

To edit an existing rule for the Port Triggering function, click the relevant rule link. On the opened page, change the needed parameters and click the **Change** button.

To remove an existing rule for the Port Triggering function, click the relevant rule link. On the opened page, click the **Delete** button.

## USB Modem

In this menu you can operate your CDMA or GSM USB modem: select the network type to connect to, establish and break the Internet connection, and handle the PIN code of the identification card inserted into your USB modem.

### Information

On the **USB modem > Information** page, you can connect to the network of your operator to establish connection to the Internet, and select a type of the network to connect to.

The screenshot shows the D-Link web interface for configuring a USB modem. The page title is "USB modem >> Information". On the left, there is a navigation menu with buttons for Start, Internet Setup, Status, Net, Firewall, USB modem (highlighted with a green arrow), Information, PIN, WiMAX, and System. The main content area is titled "Configuration:" and contains a table with the following data:

| Parameter                      | Value                                 |
|--------------------------------|---------------------------------------|
| Enable USB modem:              | 3G 2G                                 |
| Connection to mobile Internet: | <input checked="" type="radio"/> (2G) |
| Operator name:                 | MTC                                   |
| Signal level:                  | 54%                                   |
| Vendor:                        | huawei                                |
| Model:                         | E160G                                 |
| Revision:                      | 11.604.09.00.143                      |
| IMSI:                          | 250015064036427                       |
| IMEI:                          | 359390025357379                       |

At the bottom of the table, there are two buttons: "Refresh" and "Connect".

Figure 63. The **USB modem > Information** page for a GSM USB modem.

When a USB modem is connected to the router, the following fields and controls are available on the page:

| Parameter                                   | Description  |
|---|--|
| <p><b>Enable USB modem</b></p>              | <p>Select a value from the drop-down list to specify the mode for connection to the network of your operator or to disable the USB modem.</p> <p><b>Modes for GSM USB modem:</b></p> <p><b>3G 2G:</b> The USB modem connects to the 3G (UMTS) network. If unavailable, connects to the 2G (GSM/EDGE/GPRS) network.</p> <p><b>2G 3G:</b> The USB modem connects to the 2G (GSM/EDGE/GPRS) network. If unavailable, connects to the 3G (UMTS) network.</p> <p><b>3G:</b> The USB modem connects to the 3G (UMTS) network only.</p> <p><b>2G:</b> The USB modem connects to the 2G (GSM/EDGE/GPRS) network only.</p> <p><b>Off:</b> The USB modem is disabled.</p> <p><b>Modes for CDMA USB modem:</b></p> <p><b>EVDO+1X:</b> The USB modem connects to the EVDO network. If unavailable, connects to the 1X network.</p> <p><b>EVDO only:</b> The USB modem connects to the EVDO network only.</p> <p><b>1X only:</b> The USB modem connects to the 1X network only.</p> <p><b>Off:</b> The USB modem is disabled.</p> |
| <p><b>Connection to mobile Internet</b></p> | <p>The state of the connection to the network of the operator. The type of network to which the USB modem is connected or connecting at the moment is displayed to the right of the light.</p> <p><b>Red light:</b> The connection is not established.</p> <p><b>Yellow light:</b> The USB modem is connecting to the network.</p> <p><b>Green light:</b> The connection is established.</p>   |

| Parameter                              | Description  |
|--|--|
| <b>Operator name</b>                   | <p>When the needed network is available, the name of the operator is displayed in this field.</p> <p>The <b>No service</b> value means that your USB modem has failed to connect to the network type specified in the <b>Enable USB modem</b> field.</p> <p>When the <b>3G 2G</b>, <b>2G 3G</b>, or <b>2G</b> value is selected from the drop-down list, the <b>No service</b> value shows that neither conventional (2G) nor 3G network of the operator is available.</p> <p>When the <b>3G</b> value is selected from the drop-down list, the <b>No service</b> value shows that the operator's 3G network is not available. In this case, the <b>Signal level</b> field displays the signal strength of the operator's conventional (2G) network.</p> <p><i>This field is not displayed for a CDMA USB modem.</i></p> |
| <b>Signal level</b>                    | 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.   |
| <b>Vendor</b>                          | The manufacturer of your USB modem.  |
| <b>Model</b>                           | The alphanumeric code of the model of your USB modem.  |
| <b>Revision</b>                        | The version of the model of your USB modem.  |
| <b>IMSI</b>                            | The code stored in the SIM card inserted to your USB modem.<br><i>This field is displayed for GSM USB modems only.</i>   |
| <b>IMEI</b>                            | The code stored in the memory of the USB modem.  |
| <b>Refresh</b>                         | Click the button to refresh the data on the USB modem connected to the router.   |
| <b>Connect/<br/>Change&amp;Connect</b> | Click the button to connect to the network of the operator. The button is displayed when the connection is not established.  |
| <b>Disconnect</b>                      | Click the button to disconnect from the network of the operator. The button is displayed when the connection to the operator's network is established or is being established.   |

## PIN

On the **USB modem > PIN** page, you can change the PIN code of the identification card inserted to your CDMA or GSM modem, disable or enable the check of the PIN code.

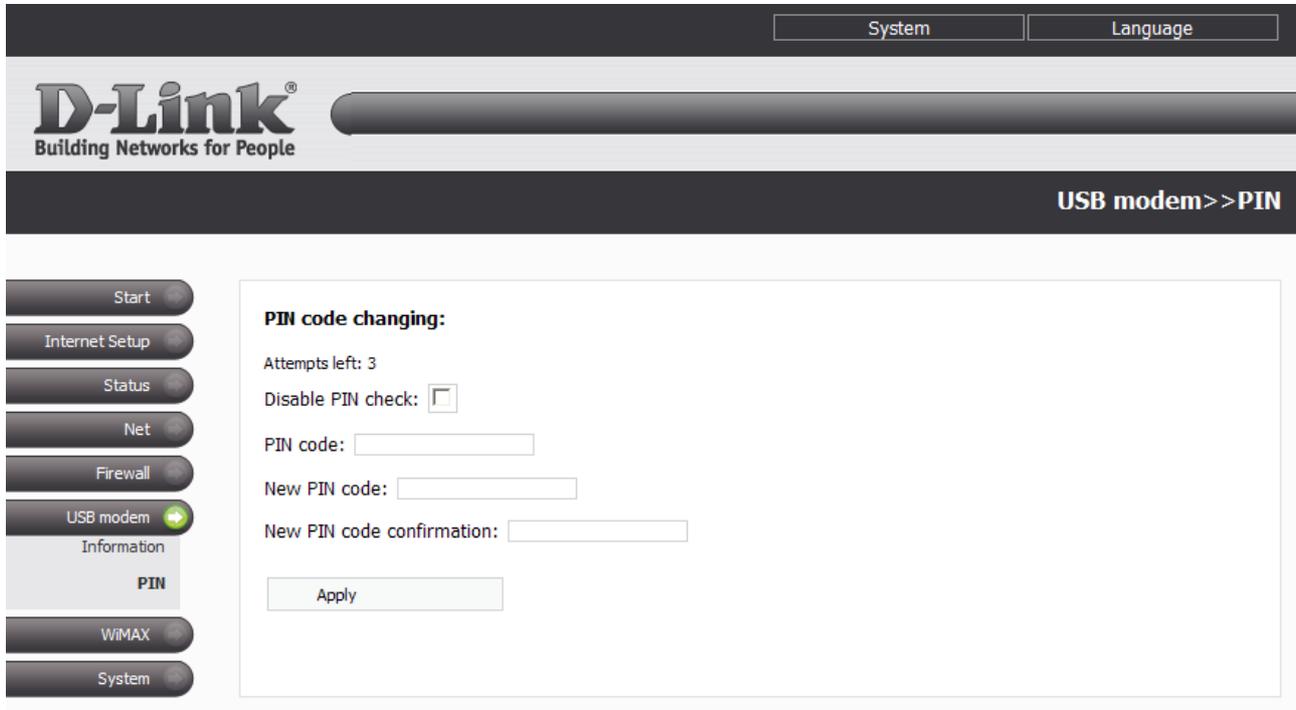


Figure 64. The **USB modem > PIN** page. The PIN code check is enabled.

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

| Parameter                        | Description  |
|----------------------------------|--|
| <b>PIN code</b>                  | Enter the current PIN code of the identification card in this field. |
| <b>New PIN code</b>              | Enter a new PIN code in this field.                                  |
| <b>New PIN code confirmation</b> | Enter the new PIN code again to avoid mistypes.                      |

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

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

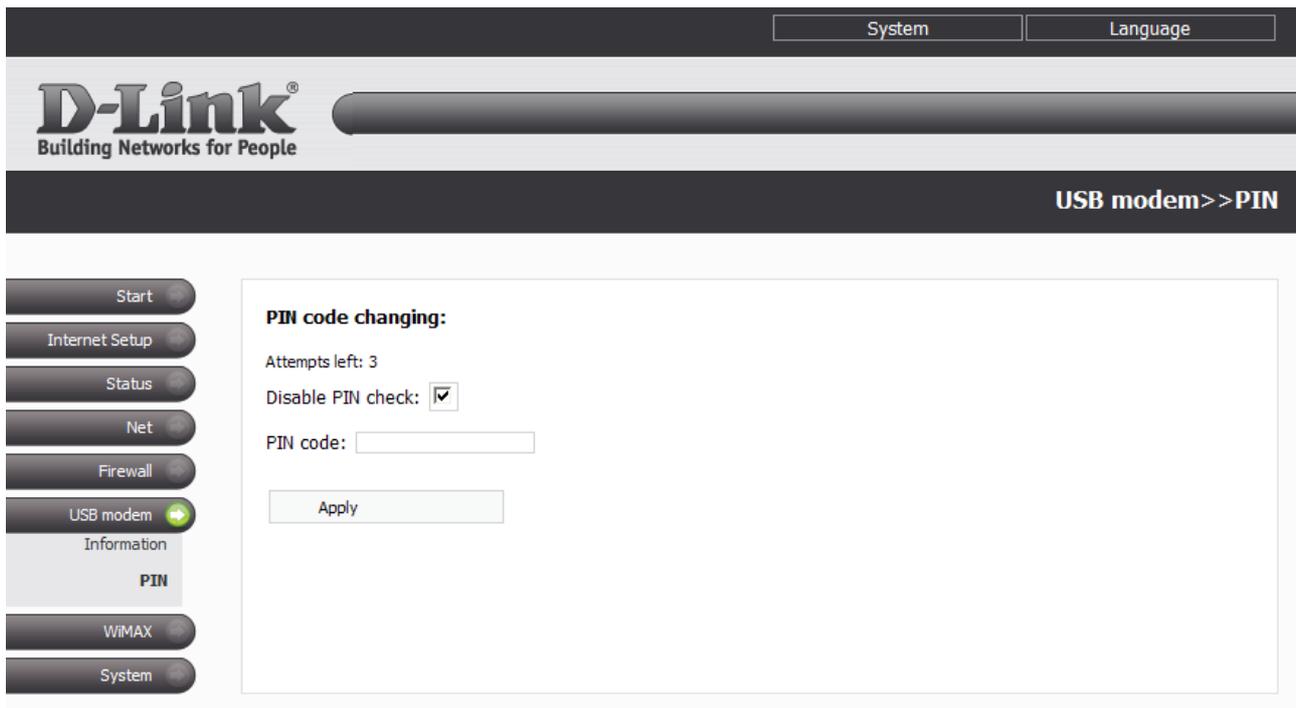


Figure 65. The **USB modem > PIN** page. The PIN code check is disabled.

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

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

## WiMAX

In this menu you can operate your WiMAX USB modem: enable or disable your WiMAX modem, and manually connect to the WiMAX ISP's network and disconnect from it.

### 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.

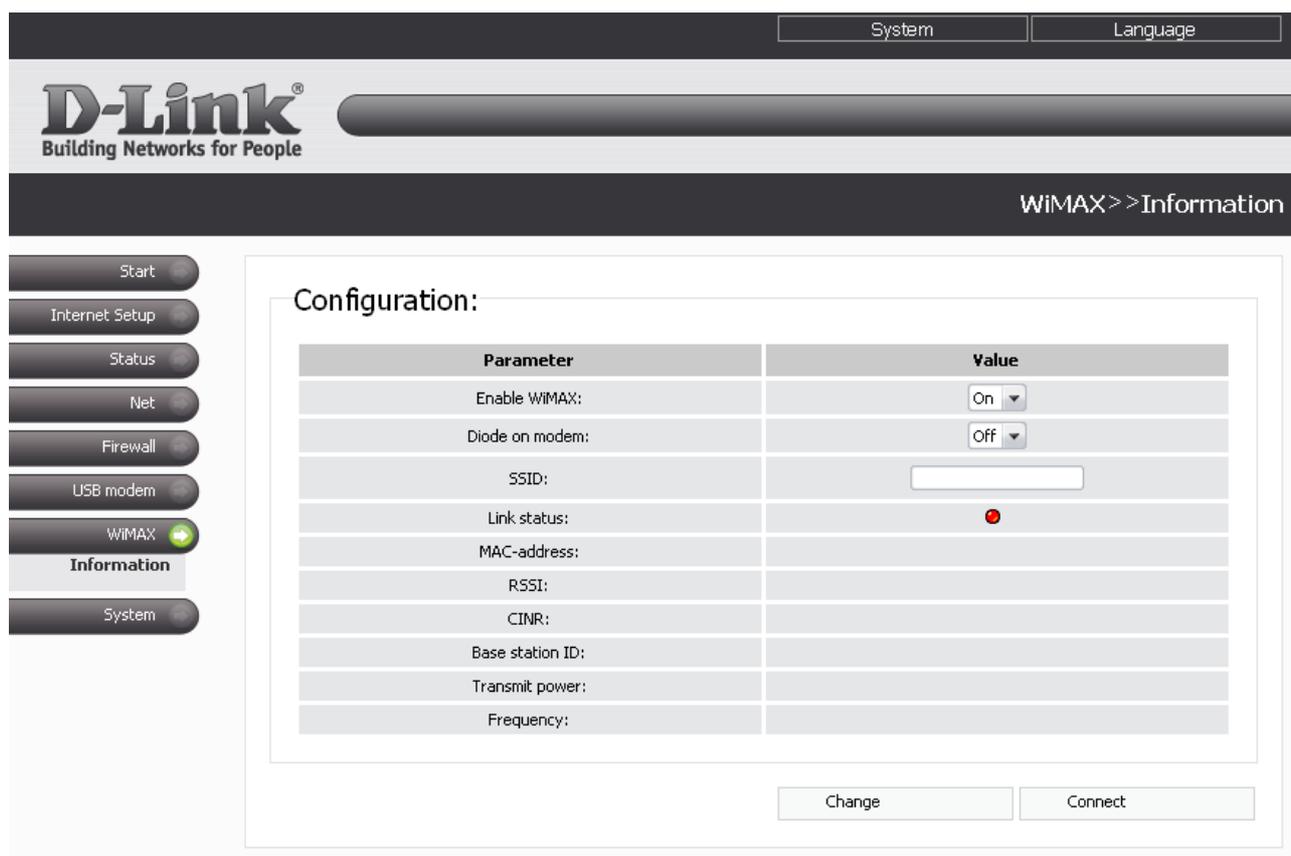


Figure 66. The **WiMAX > Information** page.

The following fields and controls are available on the page:

| Parameter             | Description   |
|-----------------------|---|
| <b>Enable WiMAX</b>   | Select a value from the drop-down list:<br><b>On:</b> The WiMAX USB modem is enabled.<br><b>Off:</b> The WiMAX USB modem is disabled.   |
| <b>Diode on modem</b> | Select a value from the drop-down list:<br><b>On:</b> The modem's LED indicator is on.<br><b>Off:</b> The modem's LED indicator is off. |
| <b>SSID</b>           | An identifier for the WiMAX network. Specify the parameter if your WiMAX ISP requires this.   |

| Parameter              | Description   |
|------------------------|---|
| <b>Link status</b>     | The state of connection to the WiMAX network.<br><b>Red light:</b> The connection is not established.<br><b>Yellow light:</b> The USB modem is connecting to the network.<br><b>Green light:</b> The connection is established. |
| <b>MAC-address</b>     | The MAC address of the WiMAX USB modem.   |
| <b>RSSI</b>            | The signal level at the input of the modem's receiver.  |
| <b>CINR</b>            | The relation of the signal level to the noise level. This parameter is used to measure the quality of the signal.   |
| <b>Base station ID</b> | The identifier of the base station.   |
| <b>Transmit power</b>  | The signal level at the output of the modem's receiver.   |
| <b>Frequency</b>       | The frequency of the signal transmitted by the modem's receiver.  |
| <b>Change</b>          | Click the button to change the parameters. You can change the parameters of this page even when your WiMAX USB modem is not connected to the router.  |
| <b>Connect</b>         | Click the button to connect to the WiMAX network. The button is displayed when the connection is not established.   |
| <b>Disconnect</b>      | Click the button to disconnect from the WiMAX network. The button is displayed when the connection is established or is being established.  |

## System

In this menu you can reboot the router (the **Reboot** button) or proceed to a page of the menu in order to save the changed 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, set the system time, update the firmware of the router, and check availability of a host on the Internet through the web-based interface of the router.

The screenshot shows the D-Link web-based interface for the System menu. At the top, there are buttons for 'System' and 'Language'. The D-Link logo is visible on the left. The main content area has a 'System' header and a 'Save&Reboot' button. Below this, there are two tables: 'Actions' and 'Subpoints'. The 'Actions' table has one row with 'Reboot' and 'Reboot system'. The 'Subpoints' table has six rows with links and descriptions.

| Name   | Comments      |
|--------|---------------|
| Reboot | Reboot system |

| Name                                   | Comments                         |
|--|----------------------------------|
| <a href="#">Administrator password</a> | WEB-interface access password    |
| <a href="#">Configuration</a>          | Load and restore configuration   |
| <a href="#">System log</a>             | System log                       |
| <a href="#">Firmware upgrade</a>       | Firmware upgrade                 |
| <a href="#">System time</a>            | Setup system time                |
| <a href="#">Ping</a>                   | Connections test by ping utility |

Figure 67. The System menu.

## Administrator Password

On the **System > Administrator password** page, you can change the password for the administrator account used to access the web-based interface of the router.

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

| Parameter              | Value  | Sample    |
|------------------------|--|-----------|
| Username:              | admin <input type="checkbox"/> Change system password: <input checked="" type="checkbox"/> | admin     |
| Password:              | *****  | 4EJ10Bek. |
| Password confirmation: | *****  |           |

Figure 68. The page for modifying the administrator password.

The following controls are available on the page:

| Control                       | Description   |
|-------------------------------|---|
| <b>Change system password</b> | Select the checkbox if you need to change the administrator password for both the web-based interface and the CLI mode. It is recommended to keep this checkbox selected. |
| <b>Password</b>               | Enter a new password for the administrator account.   |
| <b>Password confirmation</b>  | Reenter the new password to avoid mistypes.   |

Click the **Change** 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.

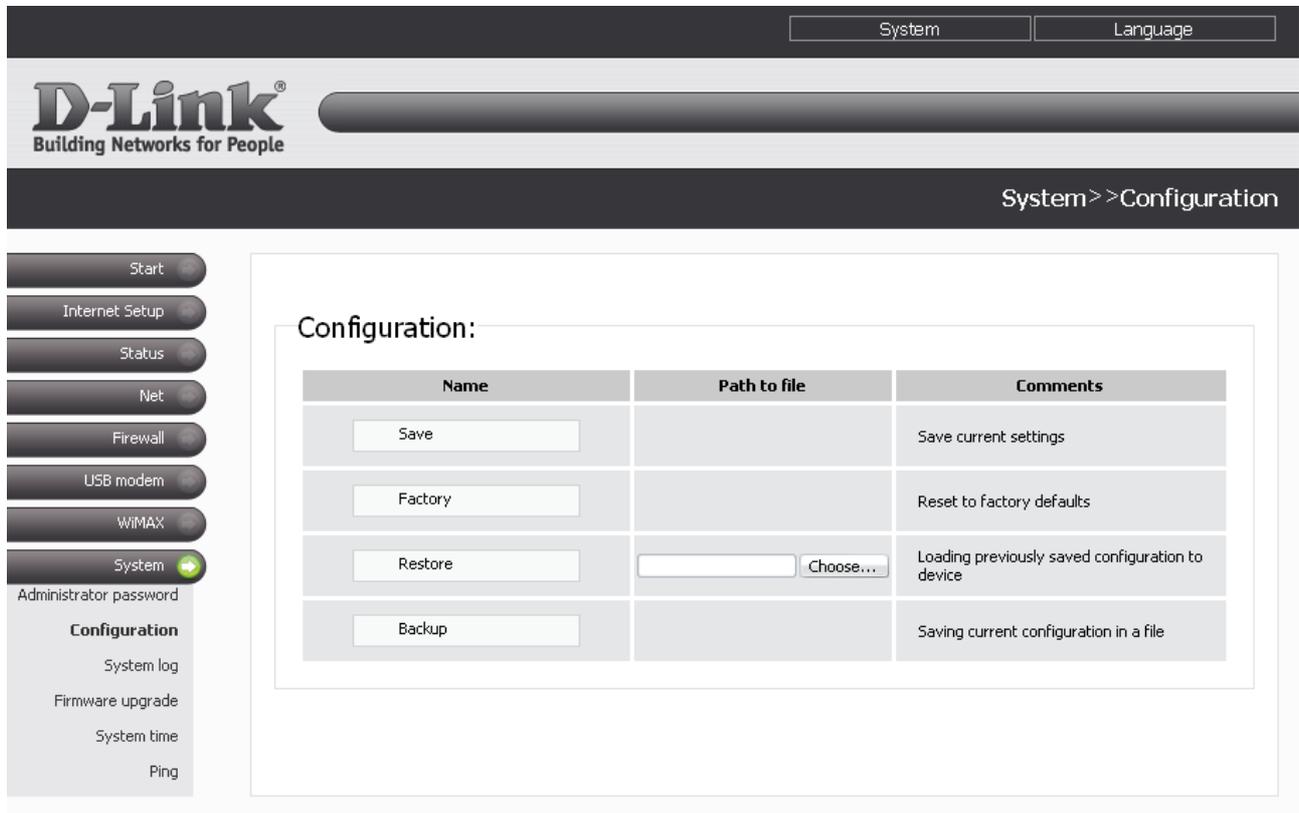


Figure 69. The **System > Configuration** page.

The following buttons are available on the page:

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

<sup>6</sup> The name of the button depends upon the web browser that you use.

## System Log

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

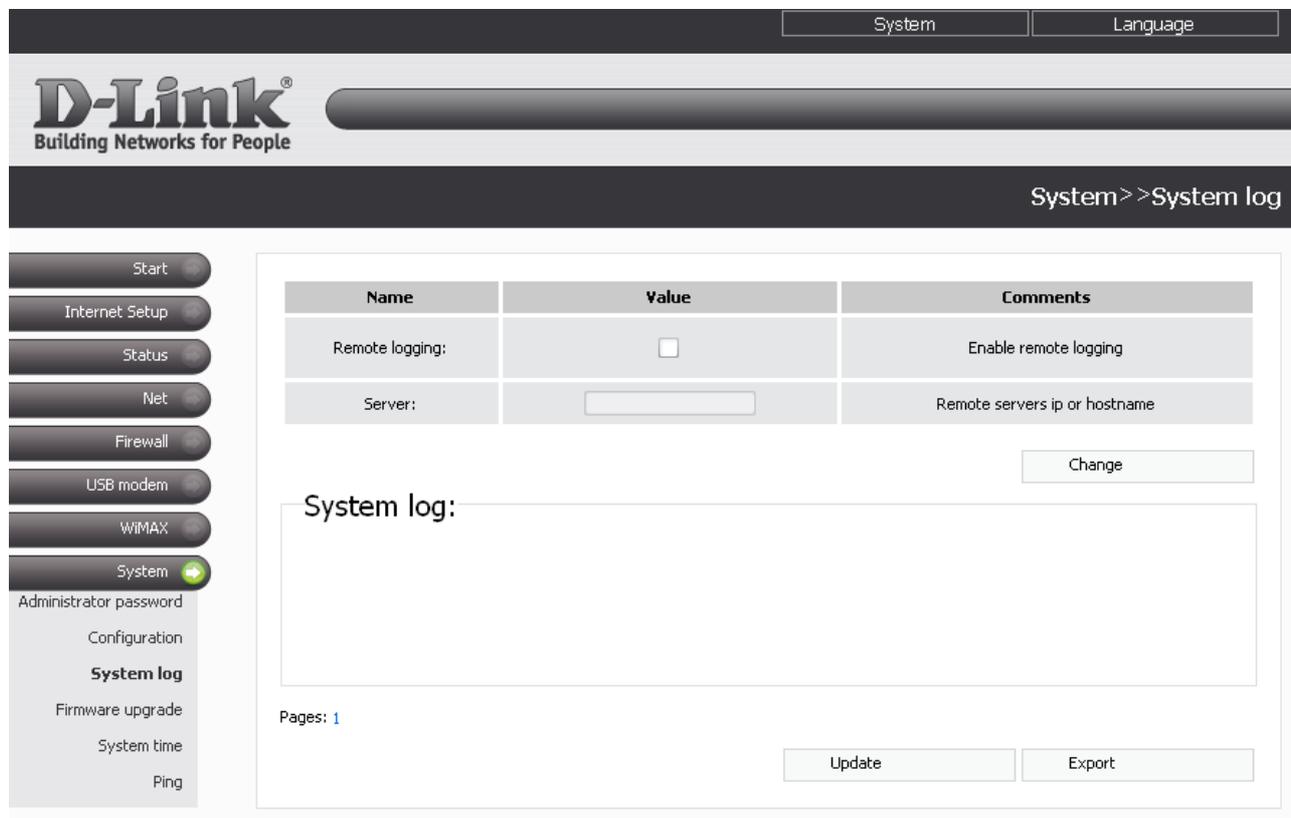


Figure 70. The **System > System log** page.

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

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

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

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

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

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

## Firmware Upgrade

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

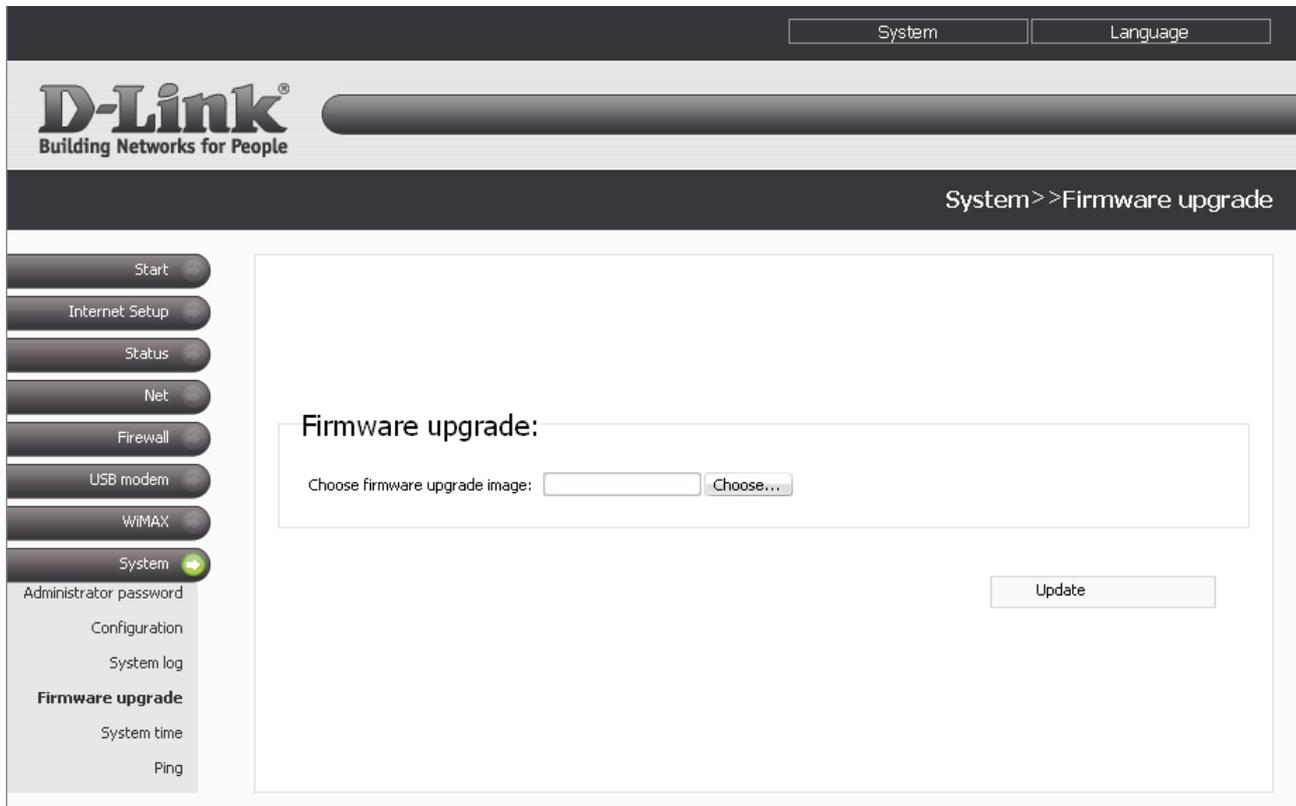


Figure 71. The **System > Firmware upgrade** page.

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

1. Get an updated firmware file (open the website [www.dlink.ru](http://www.dlink.ru), proceed to the [Поддержка \(Support\)](#) section, and then proceed to the [FTP.DLINK.RU](#) section).
2. Click the **Choose/Browse**<sup>7</sup> button on the **System > Firmware upgrade** page to locate the new firmware file.
3. Click the **Update** button to upgrade the firmware of the router.

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

<sup>7</sup> The name of the button depends upon the web browser that you use.

## System Time

On the **System > System time** page, you can manually set the date and time of the router or configure automatic synchronization of the system time.

The screenshot shows the D-Link web interface for configuring system time. The page title is "System >> System time". The left sidebar contains navigation options: Start, Internet Setup, Status, Net, Firewall, USB modem, WIMAX, System (highlighted), Administrator password, Configuration, System log, Firmware upgrade, System time, and Ping. The main content area is titled "System time:" and contains a table with the following fields:

| Name                      | Value   |
|---------------------------|---|
| Time:                     | 11 : 58   |
| Date:                     | 04 / 08 / 2010  |
| Timezone:                 | (GMT +3 h.) Moscow, Baghdad, Khartoum, Saint Petersburg |
| Use daylight saving time: | <input checked="" type="checkbox"/>                     |
| Enable NTP:               | <input type="checkbox"/>                                |
| Ntp servers:              | pool.ntp.org  |

A "Change" button is located at the bottom right of the configuration area.

Figure 72. The **System > System time** page.

To enable automatic synchronization with an NTP server:

- select the **Enable NTP** checkbox
- specify the needed NTP server in the **Ntp servers** field or leave the server specified by default
- select your time zone
- click the **Change** button.

To set the system time manually:

- deselect the **Enable NTP** checkbox (if selected)
- enter the current time and date to the fields **Time** and **Date** correspondingly
- select your time zone
- 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. If you have set the system time manually, you need to set the time and date again (see above).

To configure automatic transition to daylight saving time and back, select the **Use daylight saving time** checkbox. Click the **Change** button.

## Ping

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

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

The screenshot shows the D-Link web interface. At the top right, there are buttons for 'System' and 'Language'. The D-Link logo is on the left. The breadcrumb 'System >> Ping' is at the top right. A left sidebar contains a menu with 'System' highlighted. The main area is titled 'Ping:' and contains a table with three columns: 'Name', 'Value', and 'Comments'. Below the table is a large text area for results and a 'Start' button.

| Name           | Value                | Comments                                      |
|----------------|----------------------|---|
| Destination IP | <input type="text"/> | Destination IP                                |
| Count          | 1                    | Stop after sending count ECHO_REQUEST packets |

Start

Figure 73. The **System > Ping** page.

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

## CHAPTER 5. OPERATION GUIDELINES

### *Supported USB Modems*

#### **GSM modems:**

- Alcatel X200X
- Alcatel X220X
- Huawei E1550
- Huawei E156G
- Huawei E160G
- Huawei E169G
- Huawei E220
- ZTE MF626
- ZTE MF627

#### **CDMA modem:**

- AnyDATA ADU-500A.

#### **WiMAX modem:**

- Samsung SWC-U200.

### *Safety Instructions*

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

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

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

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

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

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

## ***Wireless Installation Considerations***

The DIR-620 device lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF noise in your home or office. To maximize your wireless range, follow the guidelines below.

1. Keep the number of walls and ceilings between the DIR-620 device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).
2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone is not in use.

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

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

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

## CHAPTER 6. ABBREVIATIONS AND ACRONYMS

|              |  |
|--------------|--|
| <b>2G</b>    | Second Generation                        |
| <b>3G</b>    | Third Generation                         |
| <b>AC</b>    | Access Category                          |
| <b>AES</b>   | Advanced Encryption Standard             |
| <b>ARP</b>   | Address Resolution Protocol              |
| <b>BSSID</b> | Basic Service Set Identifier             |
| <b>CCK</b>   | Complementary Code Keying                |
| <b>CDMA</b>  | Code Division Multiple Access            |
| <b>CINR</b>  | Carrier to Interference + Noise Ratio    |
| <b>CRC</b>   | Cyclic Redundancy Check                  |
| <b>DDNS</b>  | Dynamic Domain Name System               |
| <b>DDoS</b>  | Distributed Denial of Service            |
| <b>DHCP</b>  | Dynamic Host Configuration Protocol      |
| <b>DNS</b>   | Domain Name System                       |
| <b>DTIM</b>  | Delivery Traffic Indication Message      |
| <b>EDGE</b>  | Enhanced Data rates for GSM Evolution    |
| <b>EVDO</b>  | Evolution-Data Optimized                 |
| <b>GMT</b>   | Greenwich Mean Time                      |
| <b>GPRS</b>  | General Packet Radio Service             |
| <b>GSM</b>   | Global System for Mobile Communications  |
| <b>HTMIX</b> | High Throughput Mixed                    |
| <b>IGMP</b>  | Internet Group Management Protocol       |
| <b>IMEI</b>  | International Mobile Equipment Identity  |
| <b>IMSI</b>  | International Mobile Subscriber Identity |
| <b>IP</b>    | Internet Protocol                        |
| <b>ISP</b>   | Internet Service Provider                |

|               |   |
|---------------|---|
| <b>L2TP</b>   | Layer 2 Tunneling Protocol                    |
| <b>LAN</b>    | Local Area Network                            |
| <b>MAC</b>    | Media Access Control                          |
| <b>MTU</b>    | Maximum Transmission Unit                     |
| <b>NAT</b>    | Network Address Translation                   |
| <b>NTP</b>    | Network Time Protocol                         |
| <b>OFDM</b>   | Orthogonal Frequency Division Multiplexing    |
| <b>P-t-p</b>  | Point-to-point                                |
| <b>PBC</b>    | Push Button Configuration                     |
| <b>PIN</b>    | Personal Identification Number                |
| <b>PPPoE</b>  | Point-to-point protocol over Ethernet         |
| <b>PPTP</b>   | Point-to-point tunneling protocol             |
| <b>PSK</b>    | Pre-shared key                                |
| <b>PUK</b>    | PIN Unlock Key                                |
| <b>QoS</b>    | Quality of Service                            |
| <b>R-UIM</b>  | Removable User Identity Module                |
| <b>RADIUS</b> | Remote Authentication in Dial-In User Service |
| <b>RSSI</b>   | Received Signal Strength Indicator            |
| <b>RTS</b>    | Request To Send                               |
| <b>SIM</b>    | Subscriber Identification Module              |
| <b>SSID</b>   | Service Set Identifier                        |
| <b>TKIP</b>   | Temporal Key Integrity Protocol               |
| <b>UDP</b>    | User Datagram Protocol                        |
| <b>UMTS</b>   | Universal Mobile Telecommunications System    |
| <b>UPnP</b>   | Universal Plug and Play                       |
| <b>URL</b>    | Uniform Resource Locator                      |
| <b>USB</b>    | Universal Serial Bus                          |
| <b>WAN</b>    | Wide Area Network                             |

---

|              |   |
|--------------|---|
| <b>WDS</b>   | Wireless Distribution System                    |
| <b>WEP</b>   | Wired Equivalent Privacy                        |
| <b>Wi-Fi</b> | Wireless Fidelity                               |
| <b>WiMAX</b> | Worldwide Interoperability for Microwave Access |
| <b>WISP</b>  | Wireless Internet Service Provider              |
| <b>WLAN</b>  | Wireless Local Area Network                     |
| <b>WMM</b>   | Wi-Fi Multimedia                                |
| <b>WPA</b>   | Wi-Fi Protected Access                          |
| <b>WPS</b>   | Wi-Fi Protected Setup                           |