

DPN-1021G

**GPON ONT VoIP Gateway with 1 GPON Port,
1 10/100/1000Base-T Port, 1 10/100Base TX Port,
and 1 FXS Port**

Contents

Chapter 1. Introduction	4
Contents and Audience	4
Conventions	4
Document Structure	4
Chapter 2. Overview	5
General Information	5
Specifications*	6
Product Appearance	9
Upper Panel	9
Back and Bottom Panels	11
Delivery Package	12
Chapter 3. Installation and Connection	13
Before You Begin	13
Connecting to PC	14
Obtaining IP Address Automatically in OS Windows 7	15
Connecting to Web-based Interface	20
Web-based Interface Structure	22
Summary Page	22
Menu Sections	24
Notifications	25
Chapter 4. Configuring via Web-based Interface	26
Initial Configuration	26
Statistics	28
Network Statistics	28
PON Statistics	29
DHCP	30
Routing Table	31
Clients	32
Multicast Groups	33
Clients and Session	34
Connections Setup	35
WAN	35
<i>Creating Dynamic IPv4 or Static IPv4 WAN Connection</i>	37
<i>Creating Dynamic IPv6 or Static IPv6 WAN Connection</i>	41
<i>Creating PPPoE WAN Connection</i>	45
<i>Creating PPTP or L2TP WAN Connection</i>	50
<i>Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection</i>	54
LAN	60
IPv4	60
IPv6	63

Advanced	65
VLAN.....	66
MVR.....	68
PON.....	69
EtherWAN.....	70
DNS.....	71
Ports Settings.....	72
Redirect.....	75
DDNS.....	76
Routing.....	78
TR-069 Client.....	80
Remote Access.....	82
UPnP IGD.....	84
IGMP/ALG/Passthrough.....	85
IPsec.....	87
VoIP	94
Basic Settings.....	94
Advanced.....	97
SIP Lines.....	100
Fax Settings.....	103
Audio Settings.....	105
Routing call.....	108
Call Feature Codes.....	110
Call Logging.....	112
Security.....	113
Alarm Clock.....	114
Firewall	115
IP Filter.....	115
Virtual Servers.....	119
DMZ.....	122
MAC Filter.....	123
URL Filter.....	125
System	126
Configuration.....	127
Firmware Update.....	129
<i>Local Update</i>	130
<i>Remote Update</i>	131
Log.....	132
Ping.....	134
Traceroute.....	135
Telnet.....	136
System Time.....	137
Yandex.DNS	139
Settings.....	139
Devices and Rules.....	141
Chapter 5. Operation Guidelines	143
Safety Rules and Conditions	143
Abbreviations and Acronyms	144


CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the GPON ONT VoIP gateway DPN-1021G and explains how to configure and operate it.

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

Conventions

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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the gateway DPN-1021G 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.

Chapter 6 introduces abbreviations and acronyms used in this manual.

CHAPTER 2. OVERVIEW

General Information

The DPN-1021G device is a GPON ONT VoIP gateway with one GPON port, one 10/100/1000Base-T port, one 10/100Base-TX port, and one FXS port.

The gateway DPN-1021G provides an optical line connection to a GPON OLT device. The key advantage of GPON technology is extraordinary bandwidth of the channel. This helps to deliver the next generation of high-speed Internet services to home and office users. DPN-1021G helps to provide a reliable, long-reaching last-mile connection by extending the high-bandwidth public network to people living and working in remote multi-unit buildings.

High-speed broadband access with the rate up to 2.4Gbps allows to provide customers with all high-demand services (such as HD IPTV, VoIP, Internet connection) simultaneously.

Also the device is equipped with an FXS port which allows connection of an analog phone for calls via Internet.

Any Ethernet port of the device can be configured to connect to a private Ethernet line.

The VoIP gateway DPN-1021G includes a built-in firewall. The advanced security functions minimize threats of hacker attacks, prevent unwanted intrusions to your network, and block access to unwanted websites for users of your LAN.

In addition, the gateway supports IPsec and allows to create secure VPN tunnels.

Built-in Yandex.DNS service protects against malicious and fraudulent web sites and helps to block access to adult content on children's devices.

You can configure the settings of the gateway DPN-1021G via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

DPN-1021G itself checks the D-Link update server. If a new approved firmware is available, a notification will appear in the web-based interface of the device.

The built-in TR-069 client allows to perform remote configuration and diagnostics of the device independently from the customer.

Specifications*

Hardware	
Processor	<ul style="list-style-type: none"> RTL9602
RAM	<ul style="list-style-type: none"> 128MB, DDR3
Flash	<ul style="list-style-type: none"> 128MB, NAND
Interfaces	<ul style="list-style-type: none"> GPON port (SC/APC connector) 10/100/1000BASE-T LAN port 10/100BASE-TX LAN port RJ-11 FXS port
LEDs	<ul style="list-style-type: none"> POWER GPON Internet VoIP 2 LAN LEDs
Buttons	<ul style="list-style-type: none"> ON/OFF button to power on/power off RESET button to restore factory default settings
Power connector	<ul style="list-style-type: none"> Power input connector (DC)

PON	
GPON features	<ul style="list-style-type: none"> Class B+ GPON optical transceiver Upstream (transmitter): 1310nm ± 50nm, 1.244Gbps upstream burst data rate Downstream (digital receiver): 1490nm ± 10nm, 2.488Gbit/s downstream continuous data rate Single mode fiber cable AES encryption Support of IGMP v1/v2 Snooping, 16 entries, enable/disable, Fast leaving MAC learning UNI port configuration (rate, duplex mode, flow control, disable/enable, auto mode) Maximum frame length to 1522 bytes Compliance to ONT dying gasp ONT authentication

Phone	
General SIP features	<ul style="list-style-type: none"> Invite with Challenge Register by IP address or domain name of SIP server Backup proxy support Support of DHCP option 120 RFC3986 SIP URI format support Outbound proxy support STUN client NAT keep-alive Call types: voice/modem/fax User programmable Dial Plan Manual peer table (P2P) E.164 Numbering, ENUM support

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

Phone	
Call features	<ul style="list-style-type: none"> · Direct IP-to-IP call without SIP proxy · Call hold/retrieve · Call awaiting · Forwarding (unconditional, busy, no answer) · Do Not Disturb · Blocking hidden number calls · Speed dialing · Phone book · Hotline · Vertical service codes · Filtering by IP address (white/black list) · Alarm clock
Voice features	<ul style="list-style-type: none"> · Codecs: G.711 a/μ-law, G.729A, G.726, G.722, G.723.1 · DTMF detection and generation · In-band DTMF, out-of-band DTMF (RFC2833, SIP-INFO) · Comfort Noise Generation (CNG) · Voice Activity Detection (VAD) · Dynamic Jitter Buffer · Call progress tone generation (FXS) · DTMF/PULSE dial support · Caller ID detection and generation · T.30 FAX bypass to G.711, T.38 Real Time FAX Relay · Adjustable Flash Time · Volume control (speaker/microphone)

Software	
WAN connection types	<ul style="list-style-type: none"> · Static IPv4 / Dynamic IPv4 · Static IPv6 / Dynamic IPv6 · PPPoE · PPTP/L2TP · PPPoE IPv6 · PPPoE Dual Stack
Network functions	<ul style="list-style-type: none"> · DHCP server/relay · Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation · DNS relay · Dynamic DNS · Static IP routing · Static IPv6 routing · IGMP Proxy · RIP · Support of UPnP IGD · Support of VLAN · Support of MVR · WAN ping respond · Support of SIP ALG · Support of RTSP · Autonegotiation of speed, duplex mode, and flow control/Manual speed and duplex mode setup for each Ethernet port

Software	
Firewall functions	<ul style="list-style-type: none"> · Network Address Translation (NAT) · Stateful Packet Inspection (SPI) · IP filter · IPv6 filter · MAC filter · URL filter · DMZ · Prevention of ARP and DDoS attacks · Virtual servers · Built-in Yandex.DNS web content filtering service
VPN	<ul style="list-style-type: none"> · IPsec/PPTP/L2TP/PPPoE pass-through · IPsec tunnels
Management	<ul style="list-style-type: none"> · Local and remote access to settings through TELNET/WEB (HTTP/HTTPS) · Bilingual web-based interface for configuration and management (Russian/English) · Notification on connection problems and auto redirect to settings · Firmware update via web-based interface · Automatic notification on new firmware version · Saving/restoring configuration to/from file · Support of remote logging · Automatic synchronization of system time with NTP server and manual time/date setup · Ping utility · Traceroute utility · TR-069 client

Physical Parameters	
Dimensions (L x W x H)	<ul style="list-style-type: none"> · 160 x 115 x 43 mm (6.3 x 4.5 x 1.7 in)
Weight	<ul style="list-style-type: none"> · 200 g (0.44 lb)

Operating Environment	
Power	<ul style="list-style-type: none"> · Output: 12V DC, 1A
Temperature	<ul style="list-style-type: none"> · Operating: from 0 to 40 °C · Storage: from -40 to 70 °C
Humidity	<ul style="list-style-type: none"> · Operating: from 10% to 90% (non-condensing) · Storage: from 5% to 95% (non-condensing)

Product Appearance

Upper Panel



Figure 1. Upper panel view.

LED	Mode	Description
POWER	<i>Solid green</i>	The gateway is powered on.
	<i>No light</i>	The gateway is powered off.
GPON	<i>Solid green</i>	The gateway is synchronized with the OLT device.
	<i>Blinking green</i>	Synchronization with the OLT device is in progress.
	<i>No light</i>	The fiber optic cable is not connected.
Internet	<i>Solid green</i>	The connection is on.
	<i>No light</i>	The connection is off.
VoIP	<i>Solid green</i>	The phone is registered on the SIP server.
	<i>Blinking green</i>	Dialing a number, making or accepting a call.
	<i>No light</i>	The phone is not registered on the SIP server.

LED	Mode	Description
LAN1	<i>Solid green</i>	A device (computer) is connected to the port, the connection is on (at the rate of up to 1000Mbps).
	<i>Blinking green</i>	Data transfer through the LAN port at the rate of up to 1000Mbps.
	<i>Solid orange</i>	A device (computer) is connected to the port, the connection is on (at the rate of up to 100Mbps).
	<i>Blinking orange</i>	Data transfer through the LAN port at the rate of up to 100Mbps.
	<i>No light</i>	The cable is not connected to the port.
LAN2	<i>Solid green</i>	A device (computer) is connected to the port, the connection is on (at the rate of up to 100Mbps).
	<i>Blinking green</i>	Data transfer through the LAN port at the rate of up to 100Mbps.
	<i>No light</i>	The cable is not connected to the port.

Back and Bottom Panels

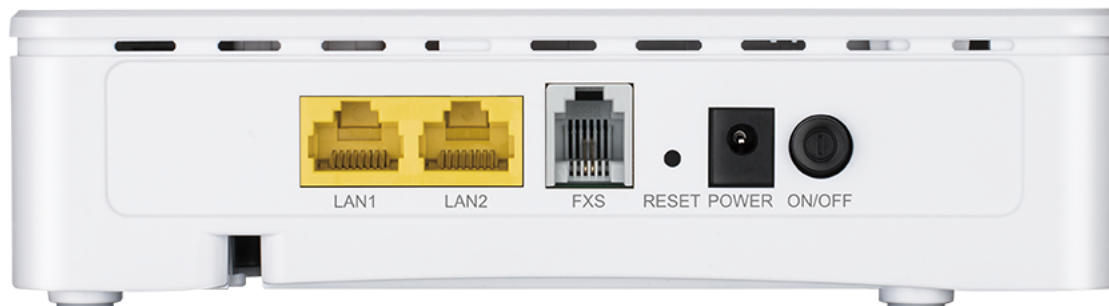


Figure 2. Back panel view.

Name	Description
LAN1/LAN2	2 Ethernet ports to connect computers or network devices. One port can be used to connect to a private Ethernet line.
FXS	A port to connect an analog phone.
RESET	A button to restore the factory default settings. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.
POWER	Power connector.
ON/OFF	A button to turn the gateway on/off.

The PON port located on the bottom panel of the gateway is designed to connect to a fiber optic line.

Delivery Package

The following should be included:

- GPON ONT VoIP gateway DPN-1021G
- Power adapter DC 12V/1A
- “***Quick Installation Guide***” (brochure).

The “***User Manual***” and “***Quick Installation Guide***” documents are available on D-Link website (see www.dlink.ru).



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 GPON ONT VoIP gateway with fiber GPON port DPN-1021G (hereinafter referred to as “the gateway”) 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:

- Apple Safari 8 and later
- Google Chrome 48 and later
- Microsoft Internet Explorer 10 and later
- Microsoft Edge 20.10240 and later
- Mozilla Firefox 44 and later
- Opera 35 and later.

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 NIC (Ethernet Adapter)

Any computer that uses the gateway should be equipped with an Ethernet adapter (NIC). If your computer is not equipped with such a device, install an Ethernet adapter prior to using the gateway.

VoIP

In order to use VoIP over SIP, you need to connect an analog phone to the FXS port of the gateway. Then access the web-based interface of the gateway, and you will be able to configure all needed settings.

Connecting to PC

- ! Invisible laser radiation may be emitted from the end of the fiber and/or from DPN-1021G. Take all necessary precautions to avoid unnecessary exposure to this radiation.

1. Connect an Ethernet cable between the Ethernet port of your PC and the 10/100/1000Base-T port (**LAN1**) or 10/100Base-TX port (**LAN2**).
2. **To connect the device to a fiber optic line:** connect the fiber optic cable to the PON port in the bottom panel of the gateway. Make sure that center conductor of the cable is inserted directly into the center of the PON connector. Secure the cable by carefully pushing the fiber connector onto the PON connector until tight. Be careful not to over-tighten the connector or you may damage either the cable or the device.
3. **To connect the device to an Ethernet line:** in the web-based interface of the gateway, select the gateway's LAN port that will be used as the WAN port and create an Ethernet WAN connection. Then connect an Ethernet cable between an available Ethernet port of the gateway and the Ethernet line.

- ! Please connect the gateway to the ISP's Ethernet line only after setting the WAN port and creating the Internet connection.

4. Connect a phone cable between the FXS port of the gateway and the phone.
5. Connect the power cord to the power connector port on the back panel of the gateway, then plug the power adapter into an electrical outlet or power strip.
6. Turn on the gateway by pressing the **ON/OFF** button on its back panel.
7. Wait for several minutes. When the device receives all needed settings, the **GPON** LED will stop blinking and will light solid green. When the Internet connection is established, the **Internet** LED will light solid green.

Obtaining IP Address Automatically in OS Windows 7

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

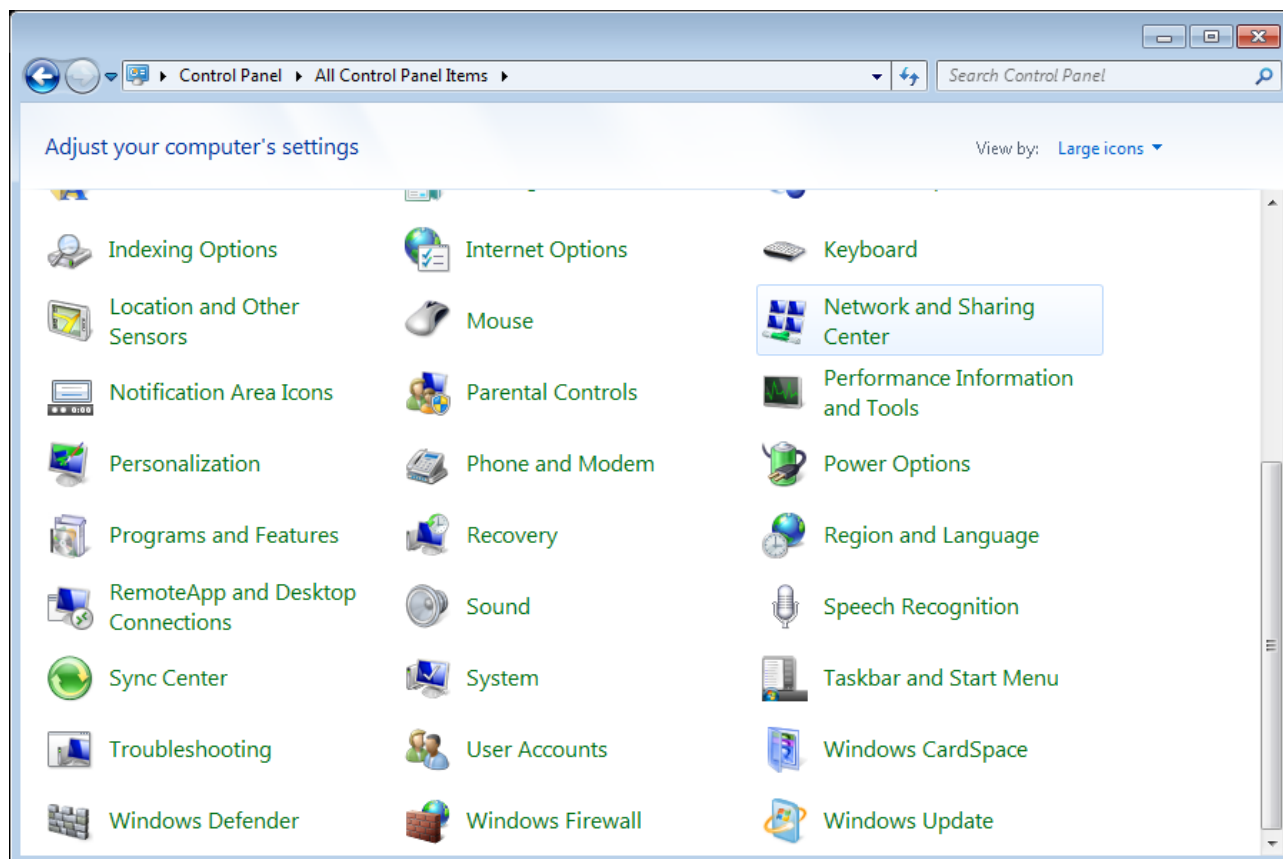


Figure 3. The **Control Panel** window.

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

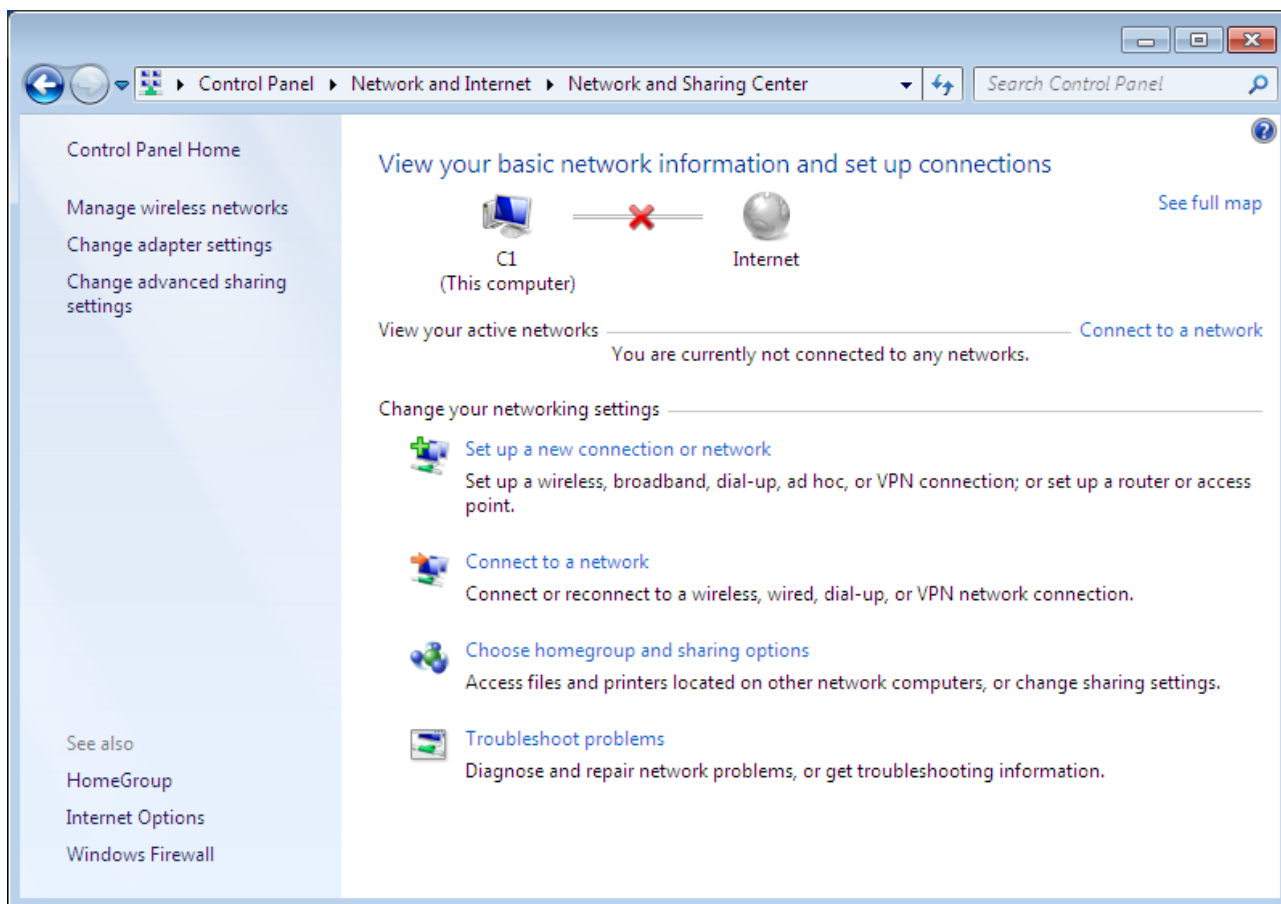


Figure 4. The **Network and Sharing Center** window.

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

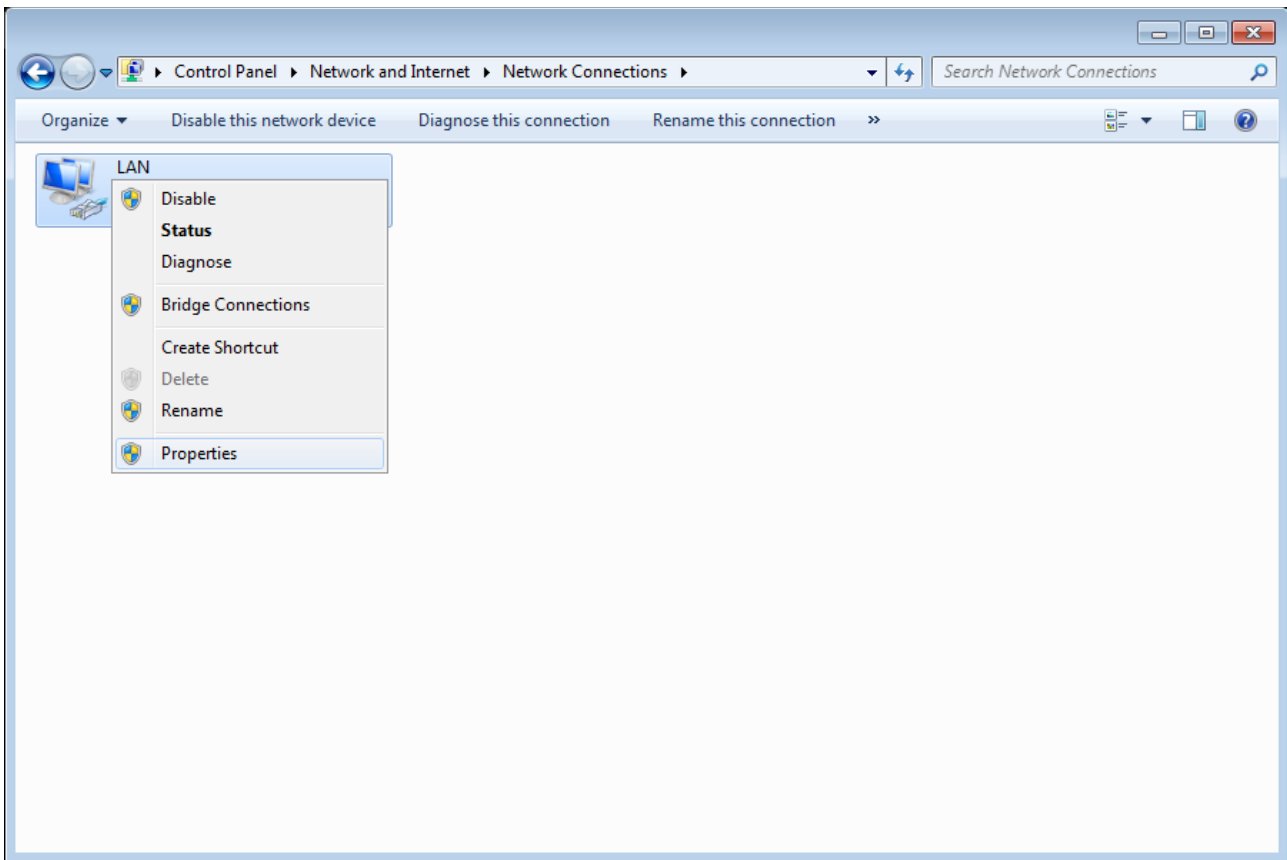


Figure 5. The **Network Connections** window.

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

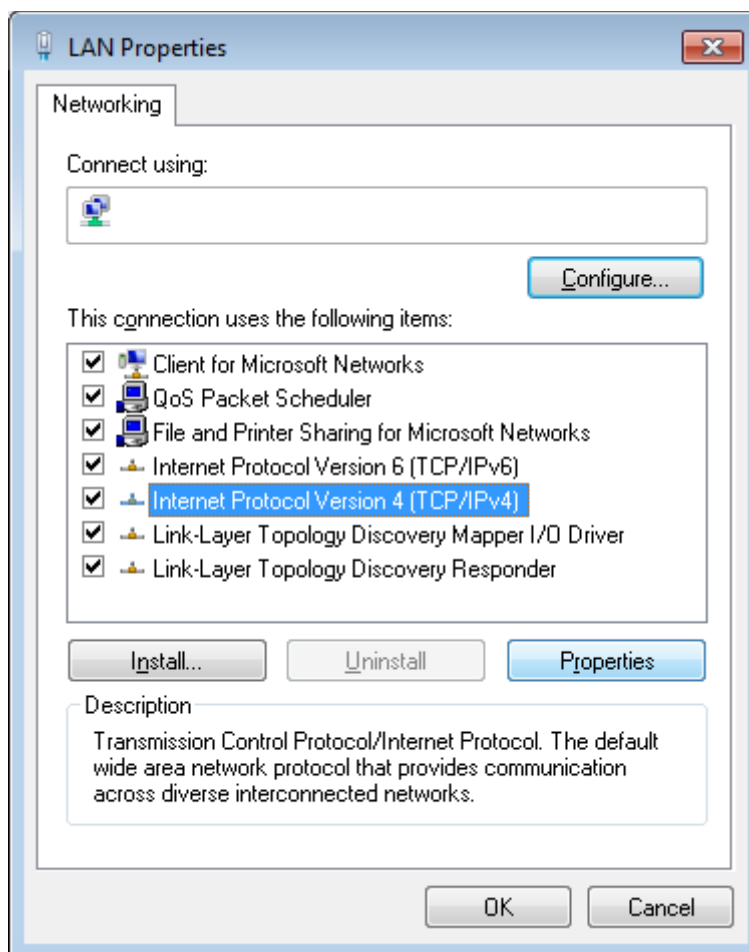


Figure 6. The **Local Area Connection Properties** window.

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

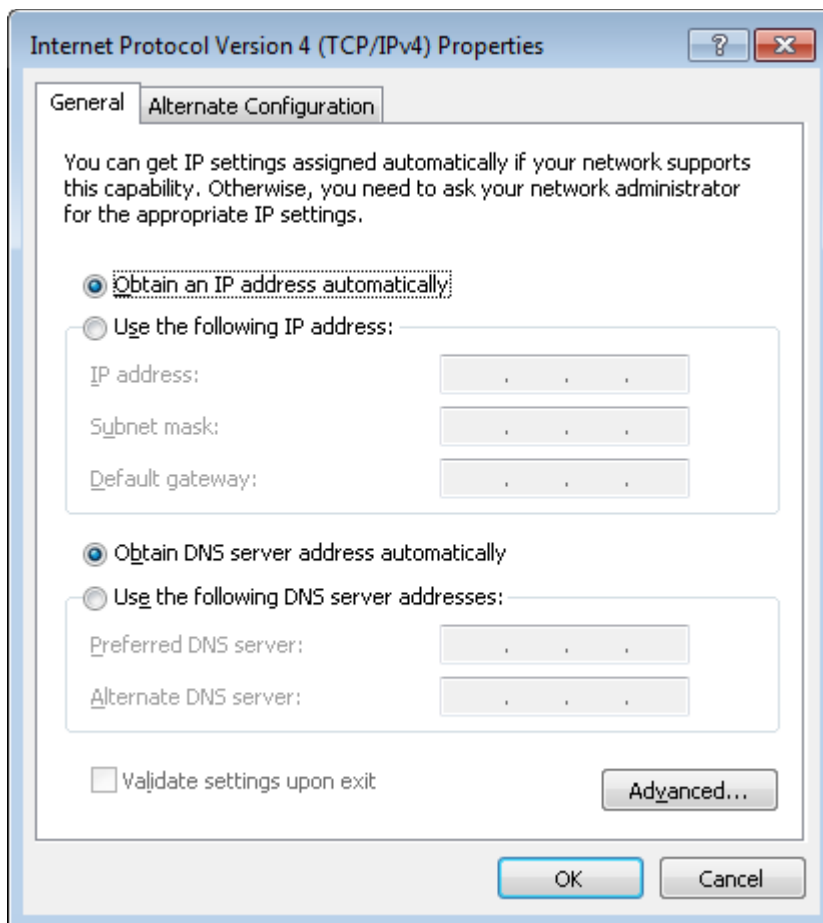


Figure 7. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

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

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

Connecting to Web-based Interface

When you have configured your computer, you can access the web-based interface and configure needed parameters (create a WAN connection, configure VoIP, specify the settings of the firewall, etc.).

! For security reasons, DPN-1021G with default settings cannot connect to the Internet. To get started, please set your own password used to access the web-based interface and, if needed, configure other settings recommended by your ISP.

Start a web browser (see the **Before You Begin** section, page 13). In the address bar of the web browser, enter the IP address of the gateway (by default, **192.168.0.1**). Press the **Enter** key.



Figure 8. Connecting to the web-based interface of the DPN-1021G device.

! 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 gateway, make sure that you have properly connected the gateway to your computer.

If the device has not been configured previously or the default settings have been restored, after access to the web-based interface the Initial Configuration page opens (see the **Initial Configuration** section, page 26).

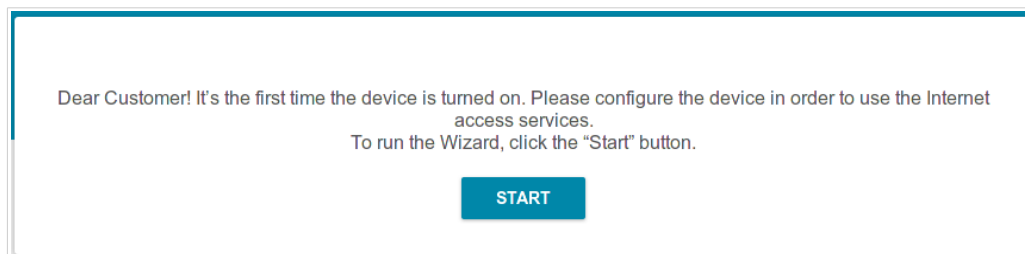


Figure 9. The Initial Configuration page.

If you configured the device previously, after access to the web-based interface the login page opens. Enter the username (**admin**) in the **Username** field and the password you specified in the **Password** field, then click the **LOGIN** button.

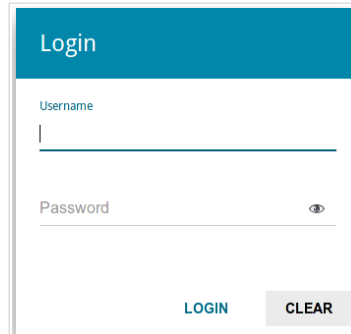
The image shows a web-based login interface. At the top, there is a blue header with the word "Login" in white. Below the header, there are two input fields: "Username" and "Password". The "Username" field has a vertical cursor at the beginning. The "Password" field has a small eye icon to its right, indicating a toggle for visibility. At the bottom of the form, there are two buttons: a blue "LOGIN" button and a grey "CLEAR" button.

Figure 10. The login page.

Web-based Interface Structure

Summary Page

On the **Summary** page, detailed information on the device state is displayed.

The screenshot shows the 'Summary' page of the web-based interface. The page is divided into several sections:

- Device Information:** Model: DPN-1021G, Hardware revision, Firmware version: [3.0.8](#), Build time: Tue Jan 17 17:13:13 MSK 2017, Vendor: D-Link Russia, Support: support@dlink.ru, Summary: Root filesystem image for DPN-1021G, Uptime: 0d 00:11:13.
- VoIP Line 1:** Line status: Registration off (red dot), Phone status: Handset is put down (green handset icon).
- Yandex DNS:** Yandex logo, Yandex.DNS toggle switch (off), Enable button. Below it, Safe: 1 device, Child: 0 devices, Protection off: 0 devices.
- WAN IPv4:** Connection type: Dynamic IPv4, Status: Connected (green dot), IP address: 192.168.161.243.
- LAN:** LAN IPv4: [192.168.0.1](#), LAN IPv6: [fd01::1/64](#), Wired connections: 1.
- LAN Ports:** LAN1 (green dot), LAN2 (green dot).
- CPU:** CPU load: 24% (with progress bar).
- Memory:** Used: 33% (30.15 Mbyte) (with progress bar), Free: 62.52 Mbyte, Buffered: 4.51 Mbyte, Total: 92.68 Mbyte.
- GPON Status:** Sync status: EtherWAN.

Figure 11. The summary page.

The **Device Information** section displays the model and hardware version of the gateway, the firmware version, and other data.

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

In the **WAN** section, data on the type and status of the existing WAN connection are displayed.

In the **LAN** section, the IPv4 and IPv6 address of the and the number of wired clients of the device are displayed.

The **LAN Ports** section displays the state of the device's LAN ports.

In the **VoIP Line 1** section, data on the status of registration on the SIP proxy server and the phone status are displayed.

The **Yandex.DNS** section displays the Yandex.DNS service state and operation mode. To enable the Yandex.DNS service, move the **Enable** switch to the right. If needed, change the operation mode of the service.

The **GPON Status** section displays the state of synchronization with the OLT.

Menu Sections

To configure the gateway use the menu in the left part of the page.

The pages of the **Statistics** section display data on the current state of the gateway (for the description of the pages, see the *Statistics* section, page 28).

The pages of the **Connections Setup** section are designed for configuring basic parameters of the LAN interface of the gateway and creating a connection to the Internet (for the description of the pages, see the *Connections Setup* section, page 35).

The pages of the **Advanced** section are designed for configuring additional parameters of the gateway (for the description of the pages, see the *Advanced* section, page 65).

The pages of the **VoIP** section are designed for specifying all settings needed for VoIP (for the description of the pages, see the *VoIP* section, page 94).

The pages of the **Firewall** section are designed for configuring the firewall of the gateway (for the description of the pages, see the *Firewall* section, page 115).

The pages of the **System** section provide functions for managing the internal system of the gateway (for the description of the pages, see the *System* section, page 126).

The pages of the **Yandex.DNS** section are designed for configuring the Yandex.DNS web content filtering service (for the description of the pages, see the *Yandex.DNS* section, page 139).

To exit the web-based interface, click the **Logout** line of the menu.

Notifications

The gateway's web-based interface displays notifications in the top right part of the page.

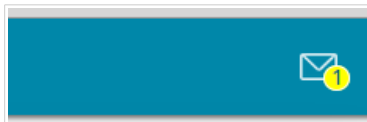


Figure 12. The web-based interface notifications.

Click the icon displaying the number of notifications to view the complete list and click the relevant button.



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

To save the settings of the gateway, click the **SAVE** button.

You can also save the gateway's settings on the **System / Configuration** page (see the *Configuration* section, page 127).

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration

If the device has not been configured previously or the default settings have been restored, the Initial Configuration page opens automatically upon access to the web-based interface or upon opening a web site on the Internet.

Click the **START** button.

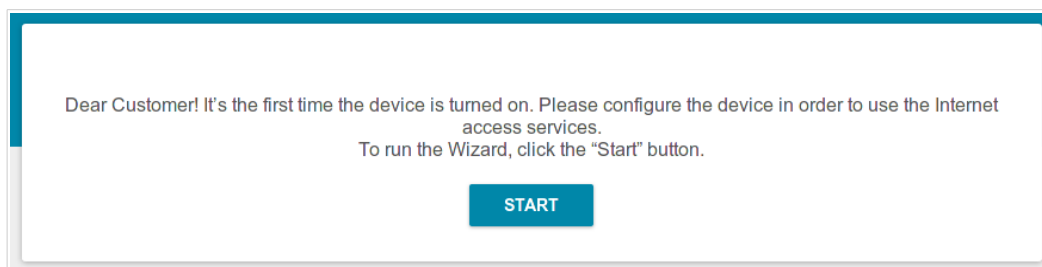


Figure 13. The initial configuration page.

On the opened page, click **YES** in order to leave the current language of the web-based interface or click **NO** to select the other language.

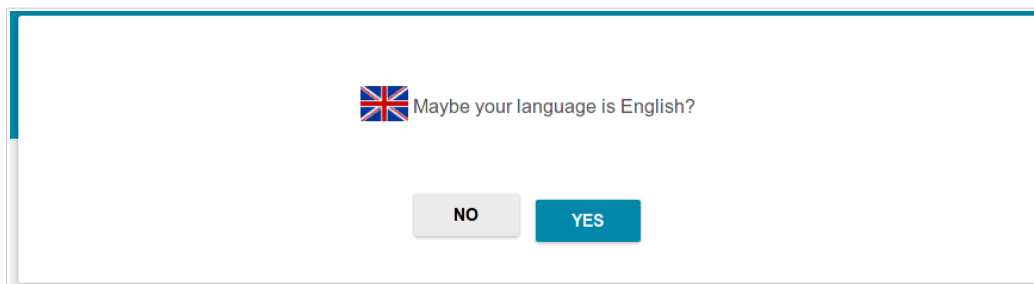


Figure 14. Selecting a language.

On the next page, change the default settings: specify the administrator password in the **Admin password** field. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.¹

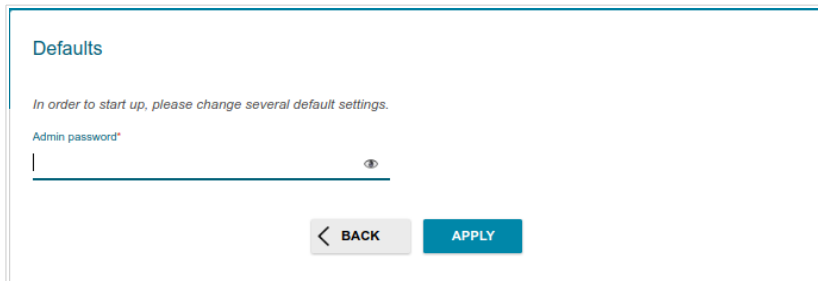


Figure 15. Changing the default settings

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

Click the **APPLY** button to continue or click the **BACK** button to return to the previous page. After clicking the **APPLY** button, the **Summary** page opens (see the *Summary Page* section, page 22).

¹ 0-9, A-Z, a-z, space, !"#%&'()*+,-./:;<=>?@[]^_`{|}~.

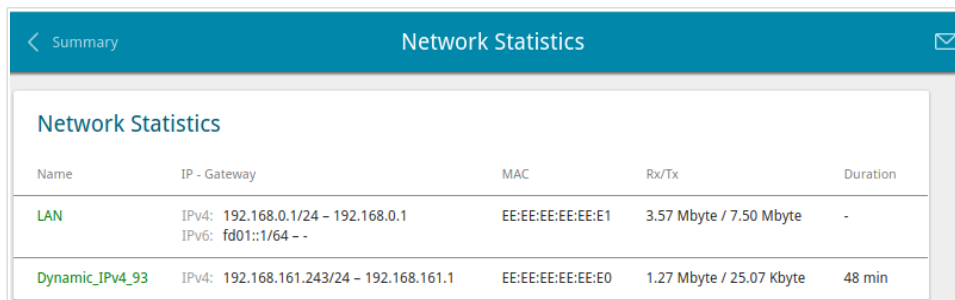
Statistics

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

- network statistics
- statistics for the PON interface
- IP addresses leased by the DHCP server
- the routing table
- data on devices connected to the gateway's network and its web-based interface
- addresses of active multicast groups
- active sessions.

Network Statistics

On the **Statistics / Network Statistics** page, you can view statistics for all connections existing in the system (WAN connections, LAN). For each connection the following data are displayed: name and state (when the connection is on, its name is highlighted in green, when the connection is off, its name is highlighted in red), IP address and subnet mask, gateway (if the connection is established), MAC address, and volume of data received and transmitted (with increase of the volume the units of measurement are changed automatically: byte, Kbyte, Mbyte, Gbyte).



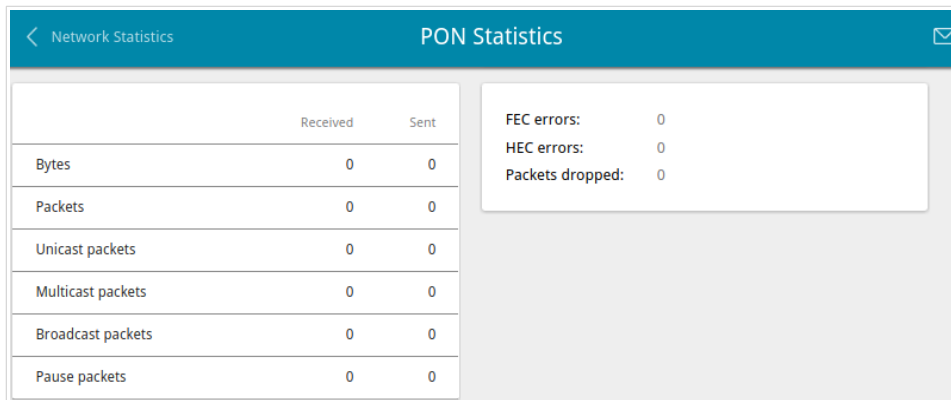
Name	IP - Gateway	MAC	Rx/Tx	Duration
LAN	IPv4: 192.168.0.1/24 - 192.168.0.1 IPv6: fd01::1/64 - -	EE:EE:EE:EE:EE:E1	3.57 Mbyte / 7.50 Mbyte	-
Dynamic_IPv4_93	IPv4: 192.168.161.243/24 - 192.168.161.1	EE:EE:EE:EE:EE:E0	1.27 Mbyte / 25.07 Kbyte	48 min

Figure 16. The **Statistics / Network Statistics** page.

To view detailed data on a connection, click the line corresponding to this connection.

PON Statistics

On the **Statistics / PON Statistics** page, you can view statistics for the PON interface (volume of data transmitted/received, number of packets of different types, and number of errors).



The screenshot shows the 'PON Statistics' page with a teal header. On the left, a table displays data for 'Received' and 'Sent' across various categories. On the right, a box lists error statistics: FEC errors, HEC errors, and Packets dropped, all with a value of 0.

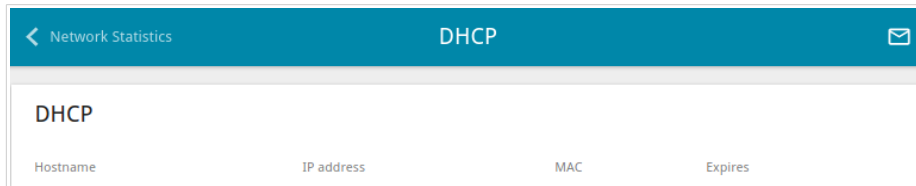
	Received	Sent
Bytes	0	0
Packets	0	0
Unicast packets	0	0
Multicast packets	0	0
Broadcast packets	0	0
Pause packets	0	0

FEC errors:	0
HEC errors:	0
Packets dropped:	0

Figure 17. The **Statistics / PON Statistics** page.

DHCP

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

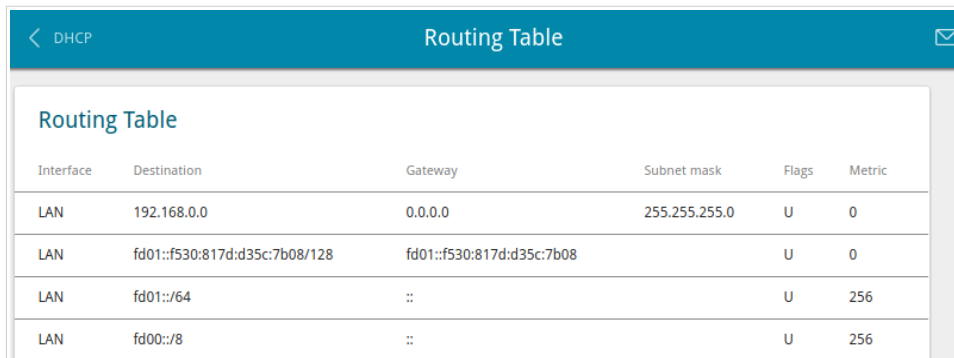


Network Statistics		DHCP	
DHCP			
Hostname	IP address	MAC	Expires

Figure 18. The **Statistics / DHCP** page.

Routing Table

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

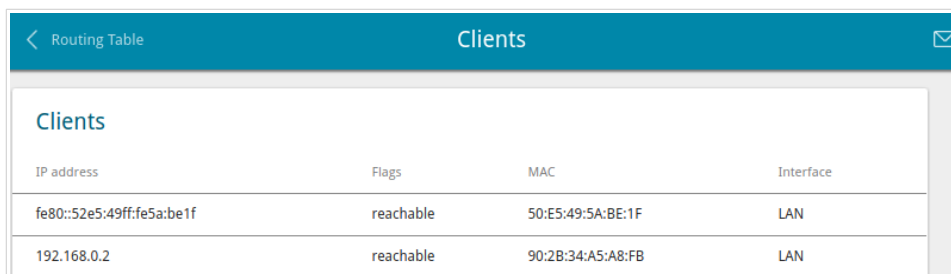


Interface	Destination	Gateway	Subnet mask	Flags	Metric
LAN	192.168.0.0	0.0.0.0	255.255.255.0	U	0
LAN	fd01::f530:817d:d35c:7b08/128	fd01::f530:817d:d35c:7b08		U	0
LAN	fd01::/64	::		U	256
LAN	fd00::/8	::		U	256

Figure 19. The **Statistics / Routing Table** page.

Clients

On the **Statistics / Clients** page, you can view the list of devices connected to the local network of the gateway.



IP address	Flags	MAC	Interface
fe80::52e5:49ff:fe5a:be1f	reachable	50:E5:49:5A:BE:1F	LAN
192.168.0.2	reachable	90:2B:34:A5:A8:FB	LAN

Figure 20. The **Statistics / Clients** page.

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

Multicast Groups

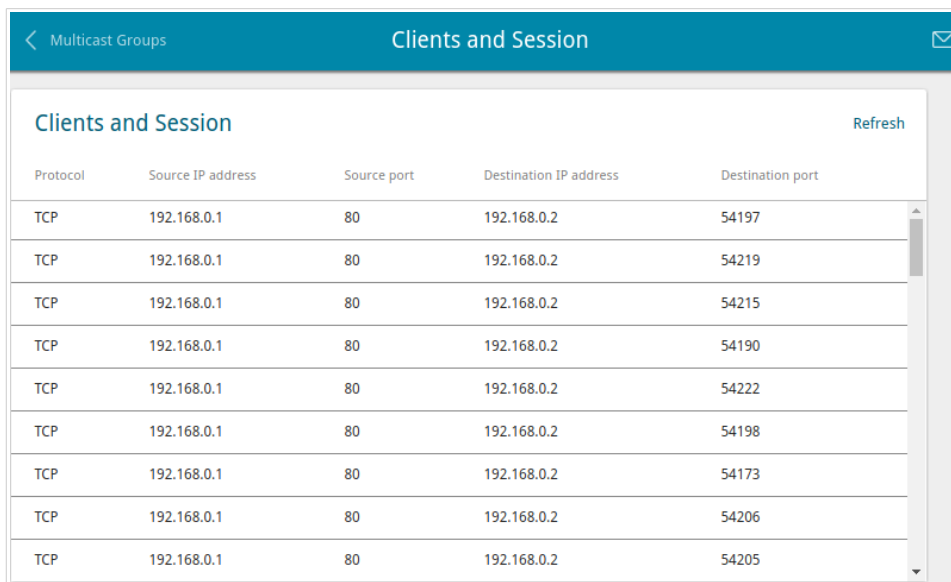
The **Statistics / Multicast Groups** page displays addresses of active multicast groups (including IPTV channels and groups for transferring service information) to which the device is subscribed, and the interface through which the device is subscribed.

IPv4		IPv6	
IP address	Interface	IP address	Interface
228.8.8.8	LAN		
239.255.255.250			

Figure 21. The **Statistics / Multicast Groups** page.

Clients and Session

On the **Statistics / Clients and Session** page, you can view information on current sessions in the gateway's network. For each session the following data are displayed: the protocol for network packet transmission, the source IP address and port, and the destination IP address and port.



Protocol	Source IP address	Source port	Destination IP address	Destination port
TCP	192.168.0.1	80	192.168.0.2	54197
TCP	192.168.0.1	80	192.168.0.2	54219
TCP	192.168.0.1	80	192.168.0.2	54215
TCP	192.168.0.1	80	192.168.0.2	54190
TCP	192.168.0.1	80	192.168.0.2	54222
TCP	192.168.0.1	80	192.168.0.2	54198
TCP	192.168.0.1	80	192.168.0.2	54173
TCP	192.168.0.1	80	192.168.0.2	54206
TCP	192.168.0.1	80	192.168.0.2	54205

Figure 22. The **Statistics / Clients and Session** page.

To view the latest data on current sessions in the gateway's network, click the **Refresh** button.

Connections Setup

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

WAN

When the gateway connects to a fiber optic line, a WAN connection is created and configured automatically.

! When the gateway connects to an Ethernet line, you should configure your Ethernet WAN connection in accordance with data provided by your Internet service provider (ISP). Make sure that you have obtained all necessary information prior to configuring your connection. Otherwise contact your ISP.

On the **Connections Setup / WAN** page, you can create and edit connections used by the gateway.

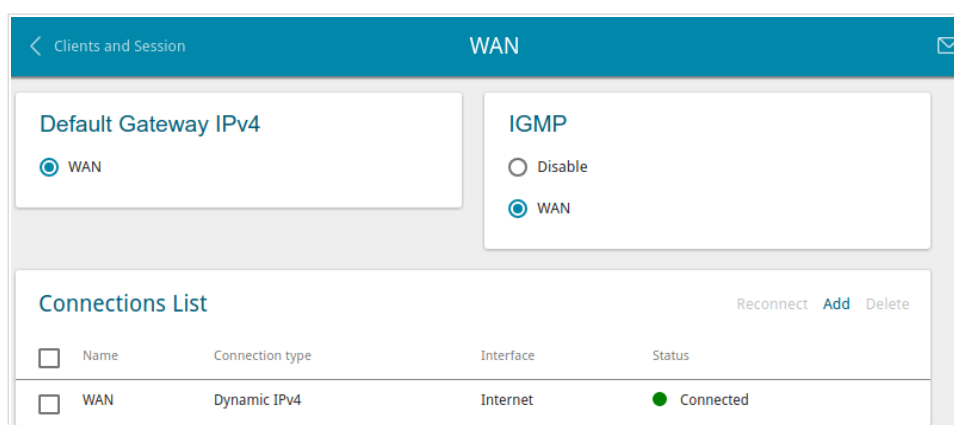


Figure 23. The **Connections Setup / WAN** page.

To create a new connection, click the **Add** button in the **Connections List** section. On the opened page, specify relevant parameters.

To edit an existing connection, in the **Connections List** section, left-click the relevant line in the table. On the opened page, change the parameters and click the **APPLY** button.

To disconnect a connection and establish it again, select the checkbox located to the left of the relevant line in the table and click the **Reconnect** button.

On the **Basic** tab, mandatory settings of a WAN connection are displayed. To view all available settings of the needed WAN connection, go to the **All Settings** tab.

To remove a connection, in the **Connections List** section, select the checkbox located to the left of the relevant line in the table and click the **Delete** button. Also you can remove a connection on the editing page.

To allow multicast traffic (e.g. streaming video) for a connection, in the **IGMP** section, select the choice of the radio button which corresponds to this connection (only for connections of the Dynamic IPv4 or Static IPv4 type).

To forbid multicast traffic for all WAN connections, select the **Disable** choice of the radio button.

To use one of existing WAN connections as the default IPv4 or IPv6 connection, in the **Default gateway** section, select the choice of the radio button which corresponds to this connection.

Creating Dynamic IPv4 or Static IPv4 WAN Connection

To create a connection of the Dynamic IPv4 or Static IPv4 type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.

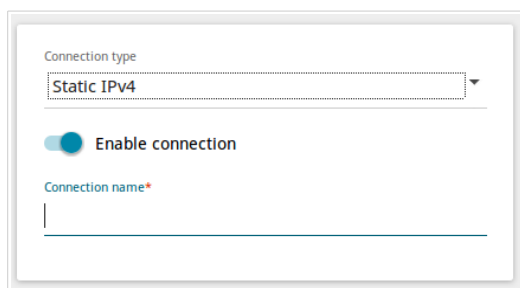


Figure 24. The page for creating a new **Static IPv4** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

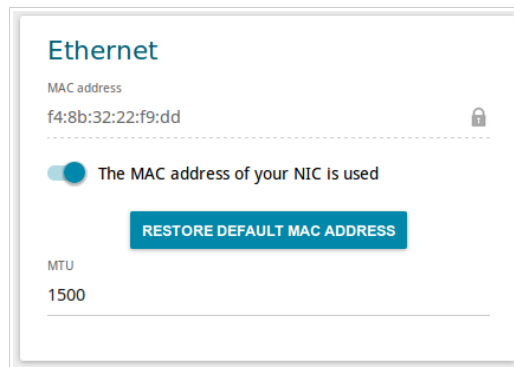


Figure 25. The page for creating a new **Static IPv4** connection. The **Ethernet** section.

Parameter	Description
Ethernet	
MAC address	<p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>To set the MAC address of the network interface card (of the computer that is being used to configure the gateway at the moment) as the MAC address of the WAN interface, move the Clone MAC address of your NIC switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the gateway's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).</p>
MTU	The maximum size of units transmitted by the interface.

Figure 26. The page for creating a new **Static IPv4** connection. The **IPv4** section.

Parameter	Description
IPv4	
<i>For Static IPv4 type</i>	
IP address	Enter an IP address for this WAN connection.
Netmask	Enter a subnet mask for this WAN connection.
Gateway IP address	Enter an IP address of the gateway used by this WAN connection.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
<i>For Dynamic IPv4 type</i>	
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the Primary DNS server and Secondary DNS server fields are not available for editing.
Primary DNS server/ Secondary DNS server	Enter addresses of the primary and secondary DNS servers in the relevant fields.
Vendor ID	The identifier of your ISP. <i>Optional.</i>
Host name	A name of the gateway specified by your ISP. <i>Optional.</i>

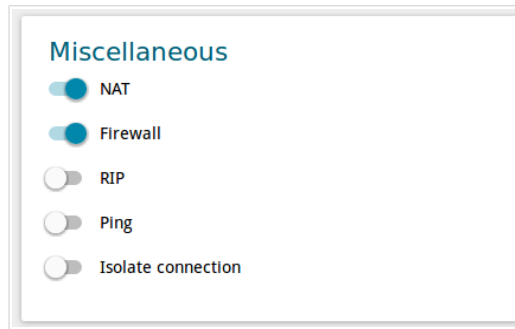


Figure 27. The page for creating a new **Static IPv4** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the gateway responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the gateway uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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

Creating Dynamic IPv6 or Static IPv6 WAN Connection

To create a connection of the Dynamic IPv6 or Static IPv6 type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.

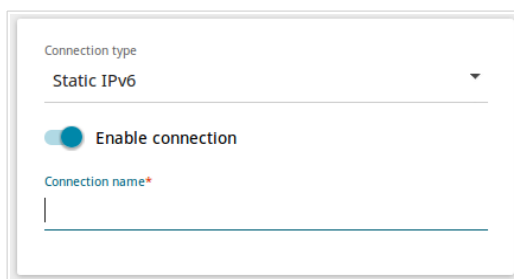


Figure 28. The page for creating a new **Static IPv6** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

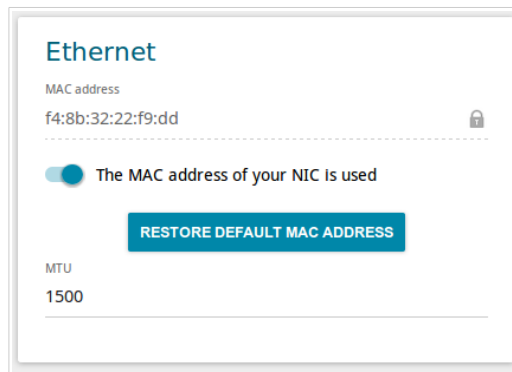


Figure 29. The page for creating a new **Static IPv6** connection. The **Ethernet** section.

Parameter	Description
Ethernet	
MAC address	<p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>To set the MAC address of the network interface card (of the computer that is being used to configure the gateway at the moment) as the MAC address of the WAN interface, move the Clone MAC address of your NIC switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the gateway's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).</p>
MTU	The maximum size of units transmitted by the interface.

Figure 30. The page for creating a new **Static IPv6** connection. The **IPv6** section.

Parameter	Description
IPv6	
<i>For Static IPv6 type</i>	
IPv6 Address	Enter an IPv6 address for this WAN connection.
Prefix	The length of the subnet prefix. The value 64 is used usually.
Gateway IPv6 address	Enter an IPv6 address of the gateway used by this WAN connection.
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.
<i>For Dynamic IPv6 type</i>	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the Automatically value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (<i>Stateless Address Autoconfiguration</i>).
Gateway IPv6 address	The address of the IPv6 gateway. The field is available for editing if the Gateway by SLAAC switch is moved to the left.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the Primary IPv6 DNS server and Secondary IPv6 DNS server fields are not available for editing.

Parameter	Description
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.

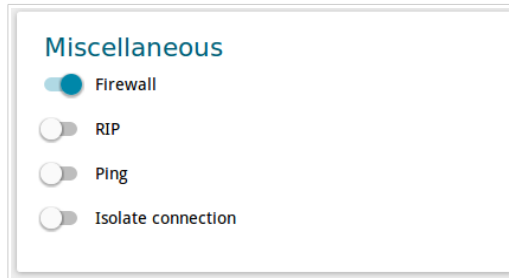


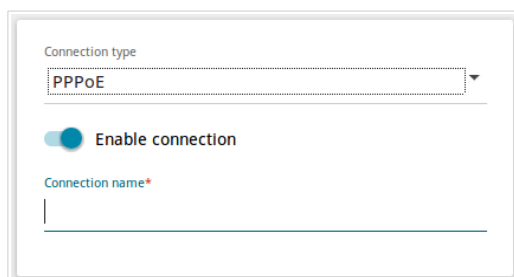
Figure 31. The page for creating a new **Static IPv6** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the gateway responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the gateway uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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

Creating PPPoE WAN Connection

To create a connection of the PPPoE type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection Type** drop-down list and specify the needed values.



The screenshot shows a configuration form for a new connection. At the top, there is a label 'Connection type' above a dropdown menu that currently displays 'PPPoE'. Below the dropdown is a toggle switch labeled 'Enable connection', which is currently turned on (indicated by a blue circle). Underneath the toggle is a text input field labeled 'Connection name*' which is currently empty.

Figure 32. The page for creating a new **PPPoE** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

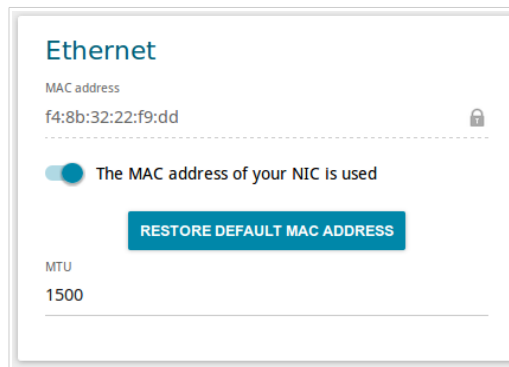


Figure 33. The page for creating a new **PPPoE** connection. The **Ethernet** section.

Parameter	Description
Ethernet	
MAC address	<p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>To set the MAC address of the network interface card (of the computer that is being used to configure the gateway at the moment) as the MAC address of the WAN interface, move the Clone MAC address of your NIC switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the gateway's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).</p>
MTU	The maximum size of units transmitted by the interface.

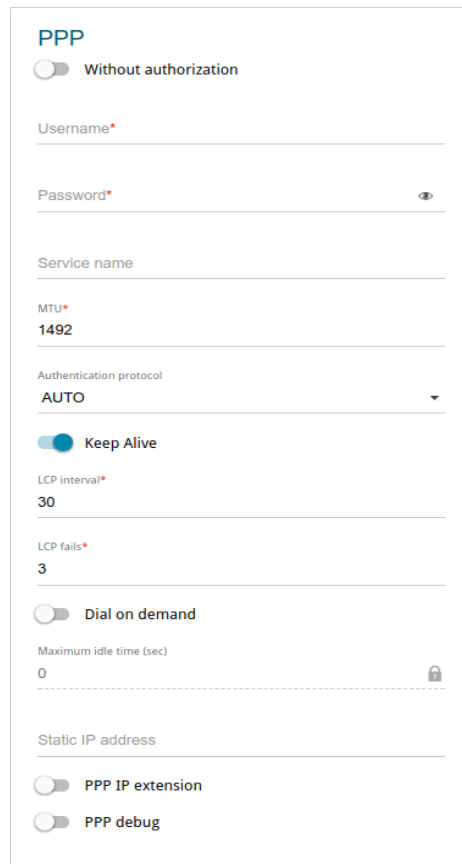



Figure 34. The page for creating a new **PPPoE** connection. The **PPP** section.

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the Show icon () to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the AUTO value.
Keep Alive	Move the switch to the right if you want the gateway to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the LCP interval and LCP fails fields are available. Specify the required values.

Parameter	Description
Dial on demand	Move the switch to the right if you want the gateway to establish connection to the Internet on demand. In the Maximum idle time field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

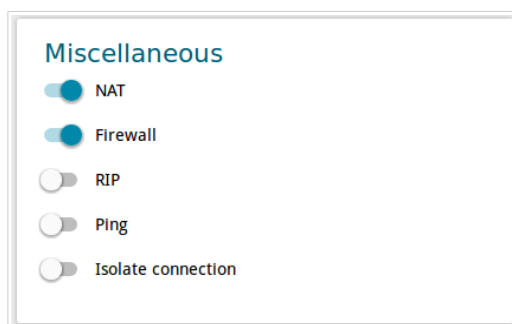


Figure 35. The page for creating a new **PPPoE** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the gateway responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the gateway uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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

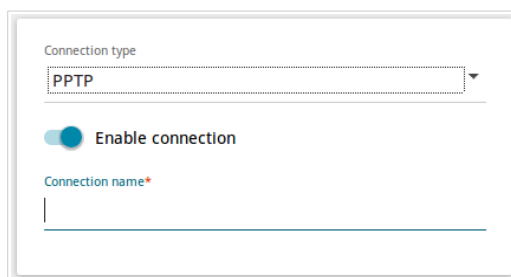
After clicking the button, the window for creating an additional connection opens.

If your ISP offers access to local services (e.g. audio and video resources), click the **CREATE** button. On the page displayed, specify the parameters for the connection of the Dynamic IPv4 or Static IPv4 type and click the **APPLY** button. Click the **BACK** button to specify other settings for the connection of the PPPoE type.

If you do not need to create an additional connection, click the **SKIP** button. In this case, the **Connections Setup / WAN** page opens.

Creating PPTP or L2TP WAN Connection

To create a connection of the PPTP or L2TP type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.



The screenshot shows a configuration form for a new connection. At the top, there is a label 'Connection type' above a dropdown menu that currently displays 'PPTP'. Below this is a toggle switch labeled 'Enable connection', which is currently turned on (indicated by a blue circle). At the bottom, there is a text input field labeled 'Connection name*' which is currently empty.

Figure 36. The page for creating a new **PPTP** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

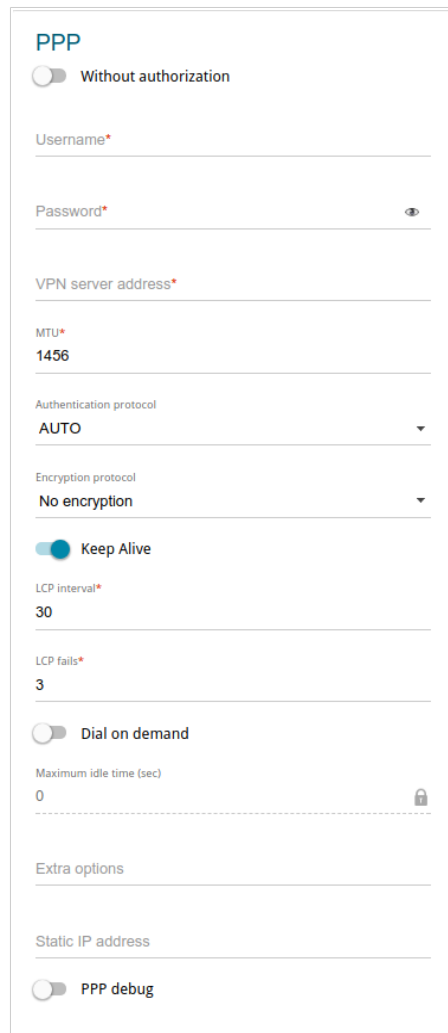



Figure 37. The page for creating a new PPTP connection. The PPP section.

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the Show icon () to display the entered password.
VPN server address	The IP or URL address of the PPTP or L2TP authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the AUTO value.

Parameter	Description
<p>Encryption protocol</p>	<p>Select a method of MPPE encryption.</p> <ul style="list-style-type: none"> • No encryption: MPPE encryption is not applied. • MPPE 40/128 bit: MPPE encryption with a 40-bit or 128-bit key is applied. • MPPE 40 bit: MPPE encryption with a 40-bit key is applied. • MPPE 128 bit: MPPE encryption with a 128-bit key is applied. <p>MPPE encryption can be applied only if the MS-CHAP, MS-CHAPV2, or AUTO value is selected from the Authentication protocol drop-down list.</p>
<p>Keep Alive</p>	<p>Move the switch to the right if you want the gateway to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the LCP interval and LCP fails fields are available. Specify the required values.</p>
<p>Dial on demand</p>	<p>Move the switch to the right if you want the gateway to establish connection to the Internet on demand. In the Maximum idle time field, specify a period of inactivity (in seconds) after which the connection should be terminated.</p>
<p>Extra options</p>	<p>Advanced options of the pppd daemon which need to be specified for this connection. <i>Optional.</i></p>
<p>Static IP address</p>	<p>Fill in the field if you want to use a static IP address to access the Internet.</p>
<p>PPP debug</p>	<p>Move the switch to the right if you want to log all data on PPP connection debugging.</p>

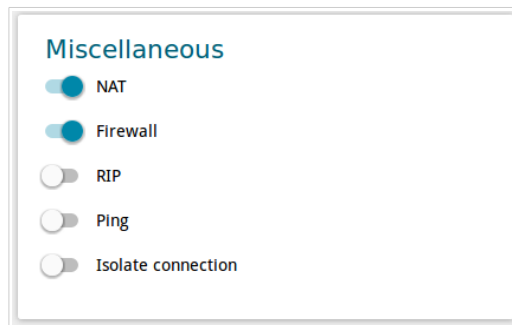


Figure 38. The page for creating a new PPTP connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
NAT	If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.
Firewall	If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.
RIP	Move the switch to the right to allow using RIP for this connection.
Ping	If the switch is moved to the right, the gateway responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Isolate connection	If the switch is moved to the right, the gateway uses an alternate routing table for this connection. Enable this function only when your ISP requires this.

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

After clicking the button, the window for additional configuration of the connection opens.

If you want to use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select the existing connection which will be used to access the PPTP/L2TP server or select the **create a new connection** choice of the radio button.

If you have already configured the connection to the Internet and you want to use this WAN connection only to connect to the virtual private network, select the **to the virtual private network** choice of the radio button.

Click the **OK** button.

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

To create a connection of the PPPoE IPv6 or PPPoE Dual Stack type, click the **Add** button on the **Connections Setup / WAN** page in the **Connections List** section. On the opened page, go to the **All Settings** tab. Then select the relevant value from the **Connection type** drop-down list and specify the needed values.

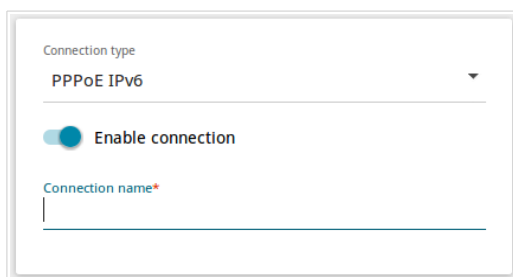


Figure 39. The page for creating a new **PPPoE IPv6** connection. Selecting a connection type.

Parameter	Description
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Connection name	A name for the connection for easier identification.

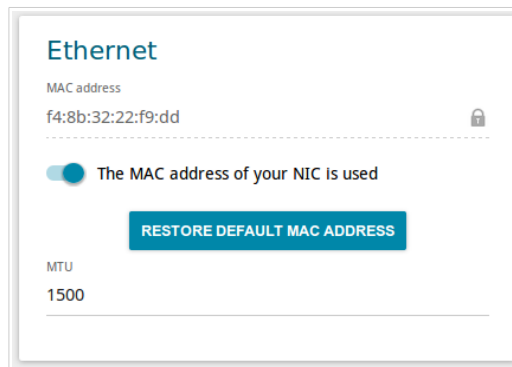


Figure 40. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.

Parameter	Description
Ethernet	
MAC address	<p>A MAC address assigned to the interface. This parameter is mandatory if your ISP uses MAC address binding. In the field, enter the MAC address registered by your ISP upon concluding the agreement.</p> <p>To set the MAC address of the network interface card (of the computer that is being used to configure the gateway at the moment) as the MAC address of the WAN interface, move the Clone MAC address of your NIC switch to the right. When the switch is moved to the right, the field is unavailable for editing.</p> <p>To set the gateway's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).</p>
MTU	The maximum size of units transmitted by the interface.

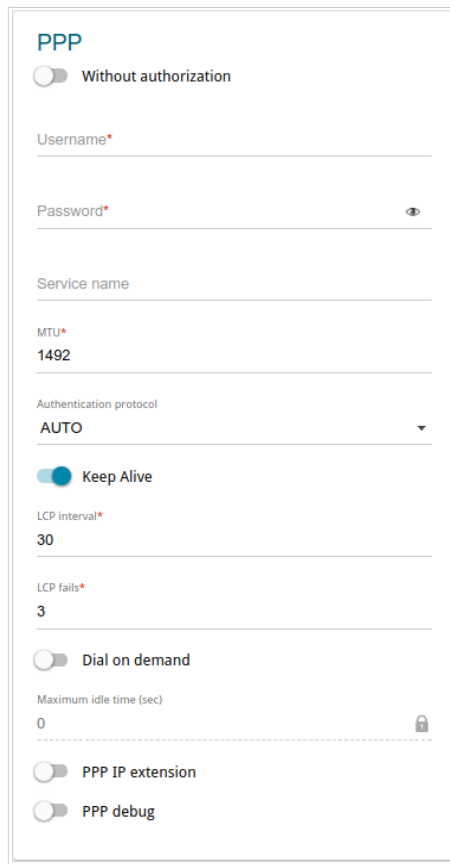



Figure 41. The page for creating a new **PPPoE IPv6** connection. The **PPP** section.

Parameter	Description
PPP	
Without authorization	Move the switch to the right if you don't need to enter a username and password to access the Internet.
Username	A username (login) to access the Internet.
Password	A password to access the Internet. Click the Show icon () to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.
Authentication protocol	Select a required authentication method from the drop-down list or leave the AUTO value.
Keep Alive	Move the switch to the right if you want the gateway to keep you connected to your ISP even when the connection has been inactive for a specified period of time. If the switch is moved to the right, the LCP interval and LCP fails fields are available. Specify the required values.

Parameter	Description
Dial on demand	Move the switch to the right if you want the gateway to establish connection to the Internet on demand. In the Maximum idle time field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	<i>For the PPPoE Dual Stack type only.</i> Fill in the field if you want to use a static IP address to access the Internet.
PPP IP extension	This option is used by some ISPs. Contact your ISP to clarify if this option needs to be enabled. If it is required, move the switch to the right.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

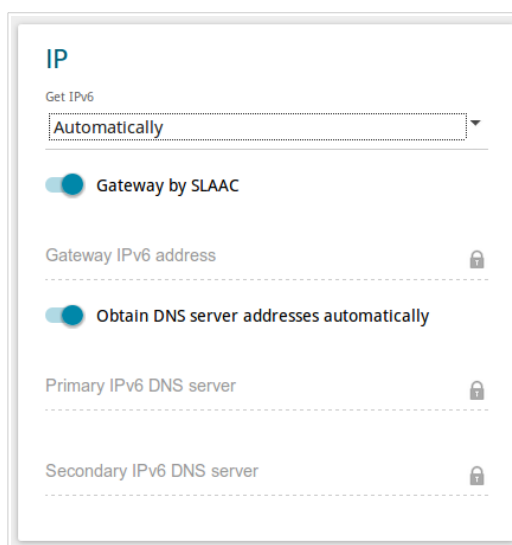


Figure 42. The page for creating a new PPPoE IPv6 connection. The IP section.

Parameter	Description
IP	
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the Automatically value.
Gateway by SLAAC	Move the switch to the right to automatically assign the IPv6 gateway address with help of SLAAC (<i>Stateless Address Autoconfiguration</i>).
Gateway IPv6 address	The address of the IPv6 gateway. The field is available for editing if the Gateway by SLAAC switch is moved to the left.
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of IPv6 DNS server addresses. Upon that the Primary IPv6 DNS server and Secondary IPv6 DNS server fields are not available for editing.
Primary IPv6 DNS server/Secondary IPv6 DNS server	Enter addresses of the primary and secondary IPv6 DNS servers in the relevant fields.



Figure 43. The page for creating a new **PPPoE IPv6** connection. The **Miscellaneous** section.

Parameter	Description
Miscellaneous	
NAT	<p><i>For the PPPoE Dual Stack type only.</i></p> <p>If the switch is moved to the right, the network address translation function is enabled. Do not disable the function unless your ISP requires this.</p>
Firewall	<p>If the switch is moved to the right, protection against external connections for the LAN devices is enabled (for example, against attempts to get information about the LAN devices or to hack a device from the LAN). For security reasons, it is recommended not to disable this function.</p>
RIP	<p>Move the switch to the right to allow using RIP for this connection.</p>
Ping	<p>If the switch is moved to the right, the gateway responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.</p>
Isolate connection	<p>If the switch is moved to the right, the gateway uses an alternate routing table for this connection. Enable this function only when your ISP requires this.</p>

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

LAN

To configure the gateway's local interface, go to the **Connections Setup / LAN** page.

IPv4

Go to the **IPv4** tab to change IPv4 address, configure the built-in DHCP server, or specify MAC address and IP address pairs.

Figure 44. Configuring the local interface. The **IPv4** tab. The **IP** section.

Parameter	Description
IP	
IP address	The IP address of the gateway in the local subnet. By default, the following value is specified: 192.168.0.1 .
Subnet mask	The mask of the local subnet. By default, the following value is specified: 255.255.255.0 .
Device domain name	The name of the device assigned to its IP address in the local subnet.

Figure 45. Configuring the local interface. The **IPv4** tab. The **DHCP** section.

Parameter	Description
DHCP	
Mode	<p>An operating mode of the gateway's DHCP server.</p> <p>Server: the gateway assigns IP addresses to clients automatically in accordance with the specified parameters. When this value is selected, the Start IP, End IP, Lease time fields and the DNS relay switch are displayed on the tab.</p> <p>Disable: the gateway's DHCP server is disabled, clients' IP addresses are assigned manually.</p> <p>Relay: an external DHCP server is used to assign IP addresses to clients. When this value is selected, the External DHCP server IP field is displayed on the tab.</p>
Start IP	The start IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address pool used by the DHCP server to distribute IP addresses to clients.
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.
DNS relay	<p>Move the switch to the right so that the devices connected to the gateway obtain the address of the gateway as the DNS server address.</p> <p>Move the switch to the left so that the devices connected to the gateway obtain the address transmitted by the ISP or specified on the Advanced / DNS page as the DNS server address.</p>
External DHCP server IP	The IP address of the external DHCP server which assigns IP addresses to the gateway's clients.

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

In the **Static DHCP** section, you can specify MAC address and IP address pairs (set a fixed IPv4 address in the local area network for a device with a certain MAC address). The gateway assigns IP addresses in accordance with the specified pairs only when the DHCP server is enabled (in the **DHCP** section, the **Server** value is selected from the **Mode** drop-down list).

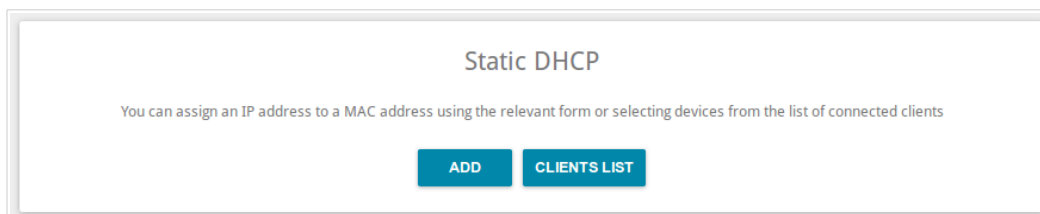


Figure 46. The section for creating MAC-IP pairs.

To create a MAC-IP pair, click the **ADD** button. In the opened window, in the **IP address** field, enter an IPv4 address which will be assigned to the device from the LAN, then in the **MAC address** field, enter the MAC address of this device. In the **Host** field, specify a network name of the device for easier identification (*optional*). Click the **APPLY** button.

Also you can create a MAC-IP pair for a device connected to the gateway's LAN at the moment. To do this, click the **CLIENTS LIST** button. In the opened window, select the relevant device and click the **OK** button. To view the latest list of the connected devices, click the **REFRESH** button.

To edit the settings for the existing MAC-IP pair, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **APPLY** button.

To remove a MAC-IP pair, select the checkbox located to the left of the relevant line in the table and click the **Delete** button. Then click the **APPLY** button. Also you can remove a MAC-IP pair in the editing window.

IPv6

Go to the **IPv6** tab to change IPv6 address of the gateway and configure IPv6 addresses assignment settings.

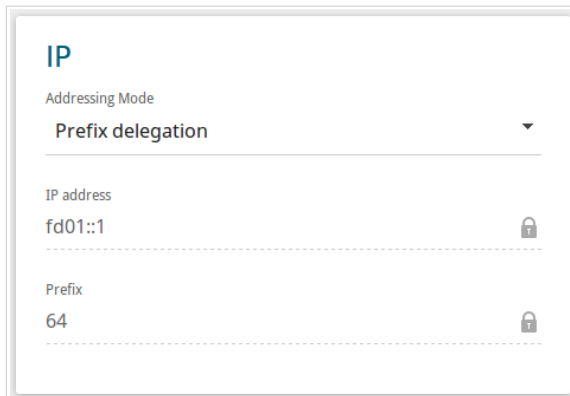


Figure 47. Configuring the local interface. The **IPv6** tab. The **IP** section.

Parameter	Description
IP	
Addressing Mode	Select the needed value from the drop-down list. Static : an IPv6 address and a prefix are specified manually. Prefix delegation : the gateway requests a prefix to configure an IPv6 address from a delegating router.
IP address	The IPv6 address of the gateway in the local subnet. By default, the following value is specified: fd01::1 . The field is available for editing if the Static value is selected from the Addressing Mode drop-down list.
Prefix	The length of the prefix subnet. By default, the value 64 is specified. The field is available for editing if the Static value is selected from the Addressing Mode drop-down list.

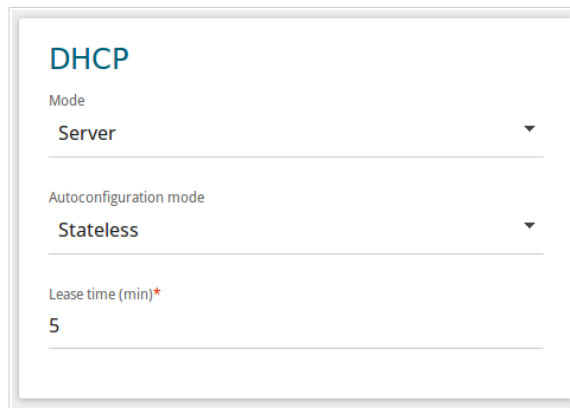


Figure 48. Configuring the local interface. The IPv6 tab. The DHCP section.

Parameter	Description
DHCP	
Mode	Select a mode of IPv6 address assignment from the drop-down list. Server: the gateway assigns IPv6 addresses to clients automatically in accordance with the specified parameters. When this value is selected, the Autoconfiguration mode drop-down list and the Lease time field are displayed on the tab. Disable: clients' IPv6 addresses are assigned manually.
Autoconfiguration mode	Select a mode from the drop-down list. Stateless: clients themselves configure IPv6 addresses using the prefix. Stateful: the built-in DHCPv6 server of the gateway allocates addresses from the range specified in the Start IP and End IP fields.
Start IP	The start IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
End IP	The end IPv6 address of the address pool used by the DHCPv6 server to distribute addresses to clients.
Lease time	The lifetime of IPv6 addresses provided to clients. The field is available for editing if the Static value is selected from the Addressing Mode list in the IP section.

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

Advanced

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

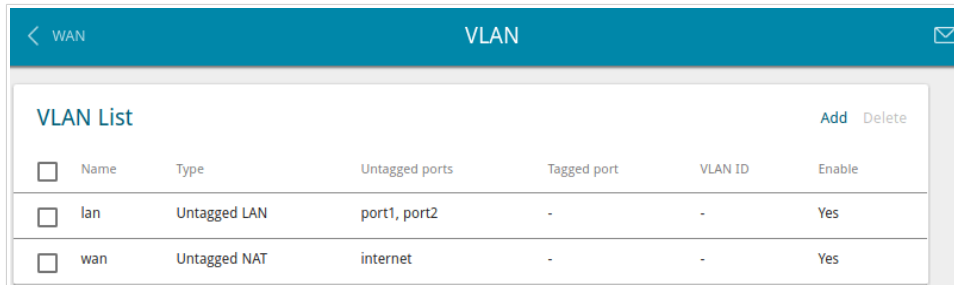
- create groups of ports for VLANs
- allow using MVR technology
- view physical parameters of the gateway transmitter and the status of synchronization with the OLT device and specify data for authorization
- allow the gateway to connect to a private Ethernet line
- add name servers
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the gateway
- configure notifications on the reason of the Internet connection failure
- configure a DDNS service
- define static routes
- configure TR-069 client
- create rules for remote access to the web-based interface
- enable the UPnP IGD protocol
- allow the gateway to use IGMP, RTSP, enable the SIP ALG, and the PPPoE/PPTP/L2TP/IPsec pass through functions
- configure VPN tunnels based on IPsec protocol.

VLAN

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

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

- **lan**: it includes ports 1-2. You cannot delete this group.
- **wan**: for the WAN interface; it includes the PON port. You can edit or delete this group.

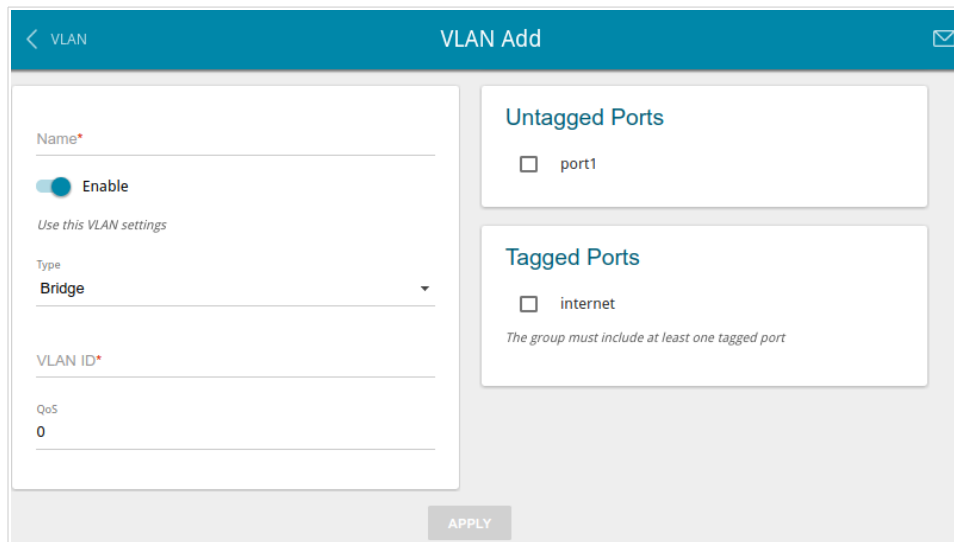


VLAN List		Add	Delete			
<input type="checkbox"/>	Name	Type	Untagged ports	Tagged port	VLAN ID	Enable
<input type="checkbox"/>	lan	Untagged LAN	port1, port2	-	-	Yes
<input type="checkbox"/>	wan	Untagged NAT	internet	-	-	Yes

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

If you want to create a group including LAN ports of the gateway, first delete relevant records from the **lan** group on this page. To do this, select the **lan** group. On the opened page, in the **Untagged Ports** section, deselect the checkbox located to the left of the relevant port, and click the **APPLY** button.

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



VLAN Add

Name* _____

Enable

Use this VLAN settings

Type
Bridge

VLAN ID* _____

QoS
0

Untagged Ports

port1

Tagged Ports

internet

The group must include at least one tagged port

APPLY

Figure 50. The page for adding a group of ports for VLAN.

You can specify the following parameters:

Parameter	Description
Name	A name for the port for easier identification.
Enable	Move the switch to the right to allow using this group of ports.

Parameter	Description
Type	<p>The type of the VLAN.</p> <p>Untagged NAT. The group of this type is an external connection with address translation. It is mostly used to transmit untagged traffic. When this value is selected, the VLAN ID and QoS fields and the Tagged Ports section are not displayed. Only one group of this type can exist in the system.</p> <p>Tagged NAT. The group of this type is an external connection with address translation. It is mostly used to connect to the Internet. Later the VLAN which identifier is specified in the VLAN ID field is used to create a WAN connection (on the Connections Setup / WAN page). When this value is selected, the Untagged Ports section is not displayed.</p> <p>Bridge. The group of this type is a transparent connection between an internal port and an external connection. It is mostly used to connect IPTV set-top boxes.</p>
VLAN ID	An identifier of the VLAN to which this group of ports will be assigned.
QoS	A priority tag for the transmitted traffic.
Untagged Ports	<p>The section includes the ports that can be added to the group.</p> <p>To add a port to the group, select the checkbox located to the left of the relevant port.</p> <p>To remove a port from the group, deselect the checkbox located to the left of the relevant port.</p>
Tagged Ports	Select an available value to assign it to this group. To do this, select the checkbox located to the left of the relevant port.

Click the **APPLY** button.

To edit an existing group, select the relevant group in the table. On the page displayed, change the parameters and click the **APPLY** button.

To remove an existing group, select the checkbox located to the left of the relevant line in the table and click the **Delete** button.

MVR

On the **Advanced / MVR** page, you can allow using MVR technology.

MVR technology (*Multicast VLAN Registration*) allows a server located in one VLAN to transmit multicast stream to clients located in other VLANs.

The screenshot shows the 'MVR' configuration page. It has a blue header with a back arrow and 'VLAN' on the left, and 'MVR' and a mail icon on the right. Below the header are two panels: 'IPv4' and 'IPv6'. Each panel contains an 'Enable MVR' toggle switch, a 'VLAN ID' input field, a 'Priority' input field, and 'LAN ports' with checkboxes for 'port2' and 'port1'. The IPv4 panel shows 'VLAN ID' as 12 and 'Priority' as 0. The IPv6 panel shows 'VLAN ID' as 0 and 'Priority' as 0. An 'APPLY' button is located at the bottom center of the page.

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

You can specify the following parameters:

Parameter	Description
IPv4/IPv6	
Enable MVR	Move the switch to the right to allow using MVR technology for the relevant protocol.
VLAN ID	An identifier of the VLAN which transmits multicast traffic.
Priority	A priority tag for multicast traffic.
LAN ports	Select the checkboxes corresponding to the ports to which multicast traffic will be transmitted.

Click the **APPLY** button.

PON

On the **Advanced / PON** page, physical parameters of the gateway transmitter and the status of synchronization with the OLT device are displayed. In addition, you can specify data for authorization on this page.

Section	Parameter	Value
Settings	user	user
	password	password
	PLOAM password	1234567890
	OMCI mode	Hybrid
PON Status	Temperature	255.996094 C
	Voltage	6.553500 V
	TX power	8.164733 dBm
	RX power	8.164733 dBm
	Bias current	131.070000 mA
GPON Status	Sync status	EtherWAN
	Serial number	DLNK1DFF6556

Figure 52. The **Advanced / PON** page.

If authorization is needed for synchronization with the OLT, enter the authorization data provided by your ISP in the fields of the **Settings** section and select the needed value from the **OMCI mode** drop-down list (*ONT Management and Control Interface*). Then click the **APPLY** button.

In the **PON Status** section, the current state of the transmitter is displayed.

In the **GPON Status** section, the state of synchronization with the OLT and the serial number of the gateway used for identification by the OLT are displayed.

EtherWAN

On the **Advanced / EtherWAN** page, you can configure the gateway to connect to a private Ethernet line.



The Ethernet WAN function allows using any LAN port of the gateway to access the Internet via Ethernet technology. When the function is enabled, the optical port of the gateway is inactive.

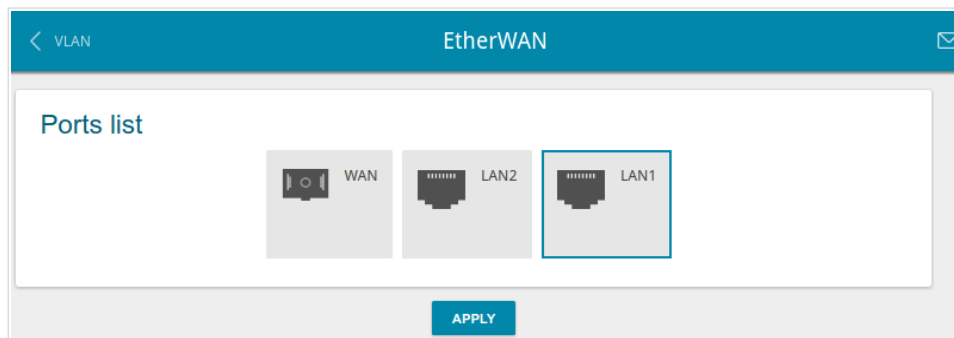


Figure 53. The **Advanced / EtherWAN** page.

To use one of the gateway's LAN port as the WAN port, click the icon corresponding to this port and click the **APPLY** button. Port configured as the WAN port is highlighted in blue.

If in the future you need to connect the gateway to a fiber optic line, click the **WAN** icon and then click the **APPLY** button.

DNS

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

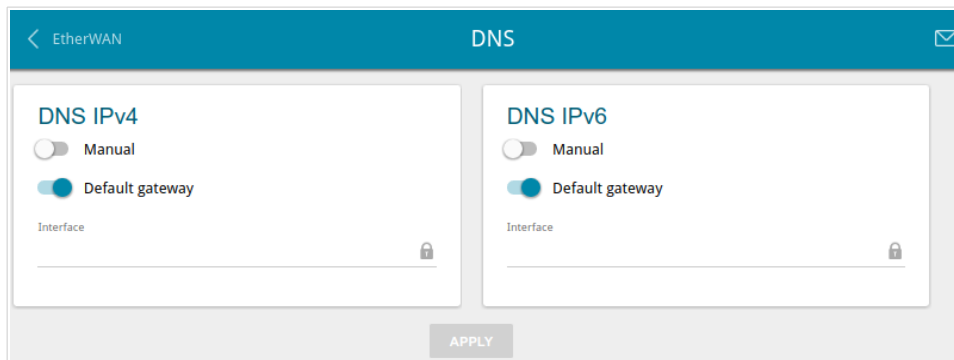


Figure 54. The **Advanced / DNS** page.

DNS servers are used to determine the IP address from the name of a server in Intranets or the Internet (as a rule, they are specified by an ISP or assigned by a network administrator).

You can specify the addresses of DNS servers manually on this page or configure the gateway to obtain DNS servers addresses automatically from your ISP upon installing a connection.

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

If you want to configure automatic obtainment of DNS servers addresses, move the **Manual** switch to the left (use the **DNS IPv4** section for IPv4 and the **DNS IPv6** section for IPv6). Then move the **Default gateway** switch to the left and from the **Interface** drop-down list select a WAN connection which will be used to obtain addresses of DNS servers automatically. If you want the gateway to use the default WAN connection to obtain addresses of DNS servers, move the **Default gateway** switch to the right. Then click the **APPLY** button.

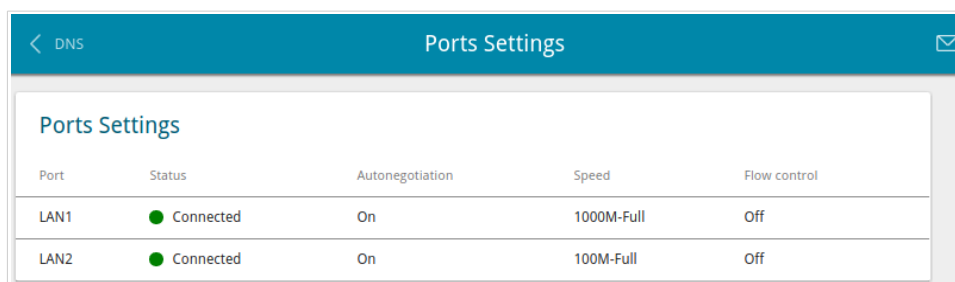
To specify a DNS server manually, move the **Manual** switch to the right (use the **DNS IPv4** section for IPv4 and the **DNS IPv6** section for IPv6). In the **Name Servers IPv4** or **Name Servers IPv6** section, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server. Then click the **APPLY** button.

To remove a DNS server from the page, click the **Delete** icon (✕) in the line of the address and then click the **APPLY** button.

Ports Settings

On the **Advanced / Ports Settings** page, you can configure or disable autonegotiation of speed and duplex mode or manually configure speed and duplex mode for each Ethernet port of the gateway.

Also you can enable or disable data flow control in the autonegotiation mode. This function is used for equal load balancing in ISPs' networks. Contact your ISP to clarify if this function needs to be enabled.



Port	Status	Autonegotiation	Speed	Flow control
LAN1	● Connected	On	1000M-Full	Off
LAN2	● Connected	On	100M-Full	Off

Figure 55. The **Advanced / Ports Settings** page.

In order to configure autonegotiation or configure speed and duplex mode manually for an Ethernet port, select it in the table.



Autonegotiation should be enabled for both devices connected to each other.



When autonegotiation is disabled, speed and duplex mode settings for both devices connected to each other should be the same.

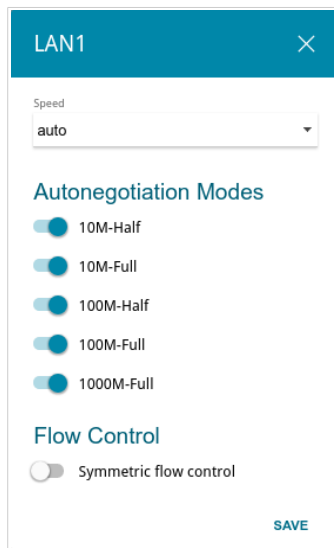


Figure 56. The window for changing the settings of the gateway's port.

In the opened window, specify the needed parameters:

Parameter	Description
<p>Speed</p>	<p>Data transfer mode.</p> <p>Select the auto value to enable autonegotiation. When this value is selected, the Autonegotiation Modes and Flow Control sections are displayed.</p> <p>Select the 10M-Half, 10M-Full, 100M-Half, or 100M-Full value to manually configure speed and duplex mode for the selected port:</p> <ul style="list-style-type: none"> • 10M-Half: Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 10Mbps. • 10M-Full: Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 10Mbps. • 100M-Half: Data transfer in just one direction at a time (data can be either sent or received) at the maximum possible rate of up to 100Mbps. • 100M-Full: Data transfer in two directions simultaneously (data can be sent and received at the same time) at the maximum possible rate of up to 100Mbps.
<p>Autonegotiation Modes</p>	
<p>To enable the needed data transfer modes, move relevant switches to the right.</p>	

Parameter	Description
Flow Control	
Symmetric flow control	Move the switch to the right to enable the flow control function for the port. Move the switch to the left to disable the flow control function for the port.

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

If in the future you need to edit the parameters of the gateway's port, select the port in the table. In the opened window, change the needed parameters and click the **SAVE** button.

Redirect

On the **Advanced / Redirect** page, you can enable notifications on the reason of the Internet connection failure. Notifications will be displayed in the browser window when a user is attempting to open a web site on the Internet.

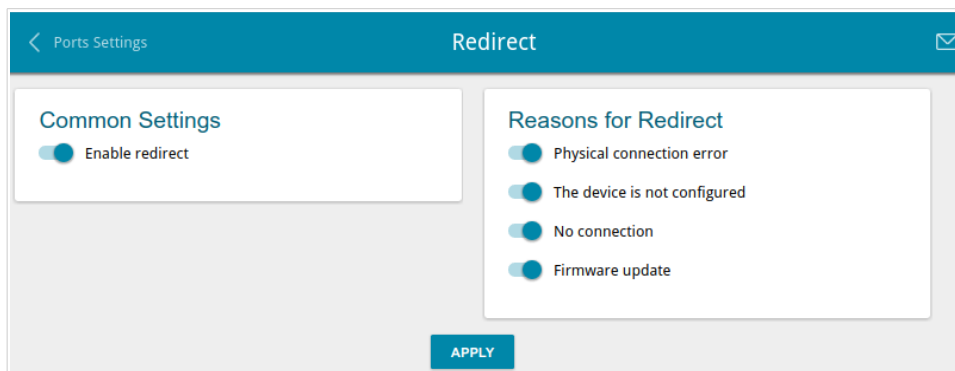


Figure 57. The **Advanced / Redirect** page.

To configure notifications, in the **Common Settings** section, move the **Enable redirect** switch to the right. Then, in the **Reasons for Redirect** section, move the needed switches to the right.

Parameter	Description
Reasons for Redirect	
Physical connection error	Notifications in case of physical connection problems (the ISP's cable is not connected, an additional device needed to access the Internet is not connected).
The device is not configured	Notifications in case when the device works with default settings.
No connection	Notifications in case of problems of the default WAN connection (authorization error, the IPS's server does not respond, etc.).
Firmware update	Notifications in case of update of the device's firmware.

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

To disable notifications, move the **Enable redirect** switch to the left and click the **APPLY** button.

DDNS

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

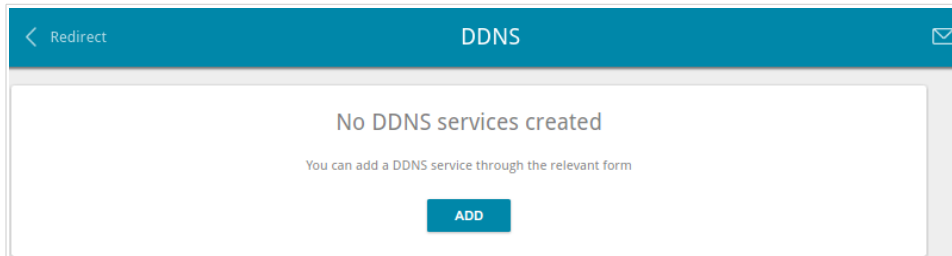


Figure 58. The **Advanced / DDNS** page.

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

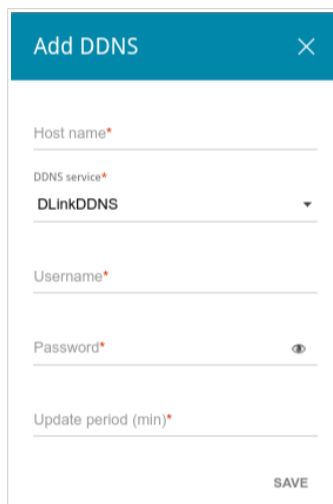

The image shows a modal window titled 'Add DDNS' with a close button (X) in the top right corner. The form contains five fields: 'Host name*' (text input), 'DDNS service*' (dropdown menu with 'DLInkDDNS' selected), 'Username*' (text input), 'Password*' (password input with a show/hide icon), and 'Update period (min)*' (text input). A 'SAVE' button is located at the bottom right of the form.

Figure 59. The window for adding a DDNS service.

In the opened window, you can specify the following parameters:

Parameter	Description
Host name	The full domain name registered at your DDNS provider.
DDNS service	Select a DDNS provider from the drop-down list.
Username	The username to authorize for your DDNS provider.
Password	The password to authorize for your DDNS provider. Click the Show icon () to display the entered password.
Update period	An interval (in minutes) between sending data on the gateway's external IP address to the relevant DDNS service.

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

To edit parameters of the existing DDNS service, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove an existing DDNS service, select the checkbox located to the left of the relevant line in the table and click the **Delete** button.

Routing

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

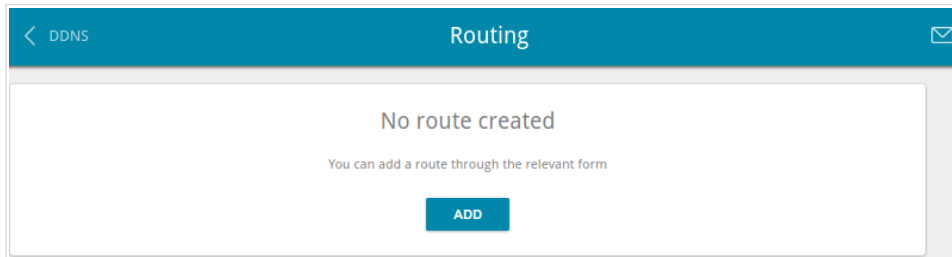


Figure 60. The **Advanced / Routing** page.

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

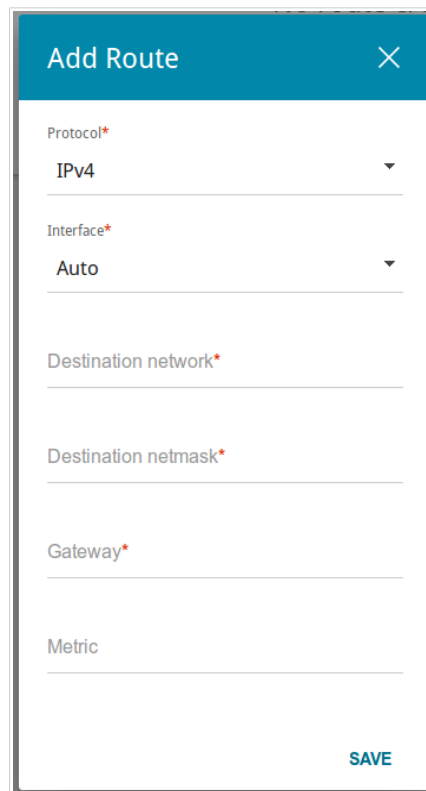
The 'Add Route' dialog box has a teal header with a close 'X' icon. It contains several input fields: 'Protocol*' with a dropdown menu showing 'IPv4'; 'Interface*' with a dropdown menu showing 'Auto'; 'Destination network*'; 'Destination netmask*'; 'Gateway*'; and 'Metric'. A teal 'SAVE' button is located at the bottom right of the dialog.

Figure 61. The window for adding a new route.

In the opened window, you can specify the following parameters:

Parameter	Description
Protocol	A protocol that the route will use.
Interface	From the drop-down list, select an interface through which the destination network can be accessed. If you have selected the Auto value, the gateway itself sets the interface on the basis of data on connected networks.
Destination network	A destination network to which this route is assigned. You can specify an IPv4 or IPv6 address. You can specify an IPv6 address (2001:db8:1234::1) or an IPv6 address with a prefix (2001:db8:1234::/64).
Destination netmask	<i>For IPv4 protocol only.</i> The destination network mask.
Gateway	An IP address through which the destination network can be accessed.
Metric	A metric for the route. The lower the value, the higher is the route priority. <i>Optional.</i>

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

To edit an existing route, select a relevant line of the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove an existing route, select the checkbox located to the left of the relevant line in the table and click the **Delete** button.

TR-069 Client

On the **Advanced / TR-069 Client** page, you can configure the gateway for communication with a remote Auto Configuration Server (ACS).

The TR-069 client is used for remote monitoring and management of the device.

Figure 62. The page for configuring the TR-069 client.

You can specify the following parameters:

Parameter	Description
TR-069 Client	
Interface	The interface which the gateway uses for communication with the ACS. Leave the Automatic value to let the device select the interface basing on the routing table or select another value if required by your ISP.
Enable TR-069 client	Move the switch to the right to enable the TR-069 client.
Inform Settings	
Enable	Move the switch to the right so the gateway may send reports (data on the device and network statistics) to the ACS.
Interval	Specify the time period (in seconds) between sending reports.

Parameter	Description
Auto Configuration Server Settings	
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS.
Connection Request Settings	
Username	The username used by the ACS to transfer a connection request to the gateway.
Password	The password used by the ACS.
Request port	The port used by the ACS. By default, the port 8999 is specified.
Request path	The path used by the ACS.
Network settings	
DSCP	<i>Differentiated Services Codepoint.</i> From the drop-down list, select a priority tag for the transmitted traffic.

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

Remote Access

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

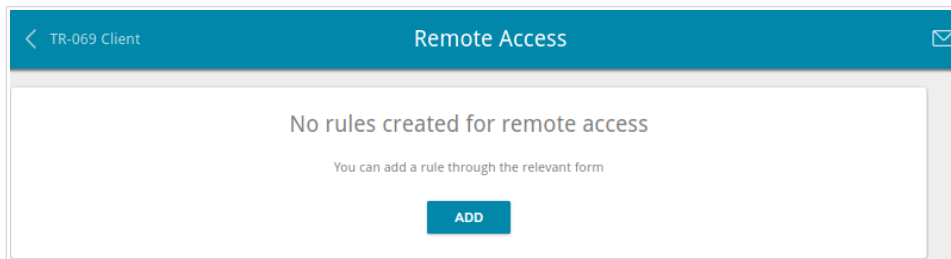


Figure 63. The **Advanced / Remote Access** page.

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

Figure 64. The window for adding a rule for remote management.

In the opened window, you can specify the following parameters:

Parameter	Description
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Open access from any external host	Move the switch to the right to allow access to the gateway for any host. Upon that the IP address and Mask fields are not displayed.
IP address	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.

Parameter	Description
Mask	<i>For the IPv4-based network only.</i> The mask of the subnet.
Public port	<i>For the IPv4-based network only.</i> An external port of the gateway. You can specify only one port.
Protocol	The protocol available for remote management of the gateway.

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

To edit a rule for remote access, left-click the relevant rule. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule for remote access, select the checkbox located to the left of the relevant line in the table and click the **Delete** button.

UPnP IGD

On the **Advanced / UPnP IGD** page, you can enable the UPnP IGD protocol. The gateway uses the UPnP IGD protocol for automatic configuration of its parameters for network applications requiring an incoming connection to the gateway.

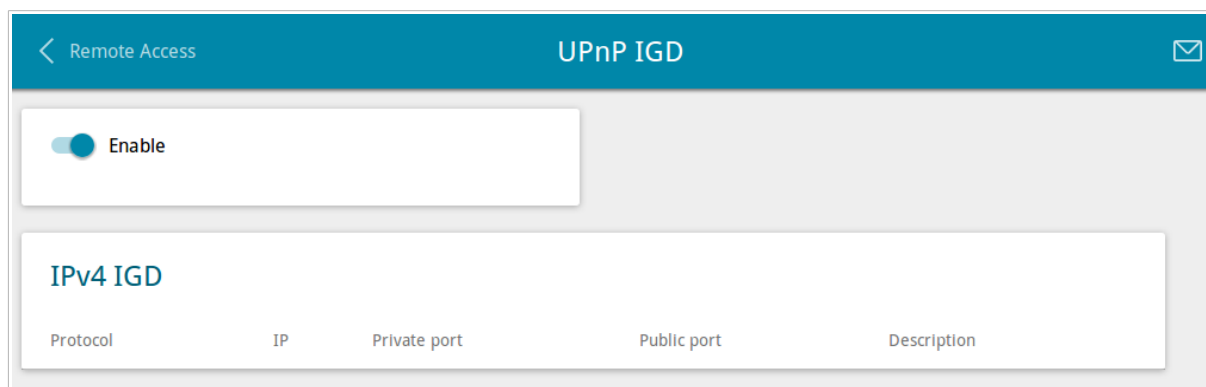


Figure 65. The **Advanced / UPnP IGD** page.

If you want to manually specify all parameters needed for network applications, move the **Enable** switch to the left. Then go to the **Firewall / Virtual Servers** page and specify needed settings.

If you want to enable the UPnP IGD protocol in the gateway, move the **Enable** switch to the right.

When the protocol is enabled, the gateway's parameters configured automatically are displayed on the page:

Parameter	Description
Protocol	A protocol for network packet transmission.
IP	The IP address of a client from the local area network.
Private port	A port of a client's IP address to which traffic is directed from a public port of the gateway.
Public port	A public port of the gateway from which traffic is directed to a client's IP address.
Description	Information transmitted by a client's network application.

IGMP/ALG/Passthrough

On the **Advanced / IGMP/ALG/Passthrough** page, you can allow the gateway to use IGMP and RTSP, enable the SIP ALG and PPPoE/PPTP/L2TP/IPsec pass through functions.

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.

SIP is used for creating, modifying, and terminating communication sessions. This protocol allows telephone calls via the Internet.

RTSP is used for real-time streaming multimedia data delivery. This protocol allows some applications to receive streaming audio/video from the Internet.

The PPPoE pass through function allows PPPoE clients of computers from your LAN to connect to the Internet through connections of the gateway.

The PPTP pass through, L2TP pass through and IPsec pass through functions allow VPN PPTP, L2TP and IPsec traffic to pass through the gateway so that clients from your LAN can establish relevant connections with remote networks.

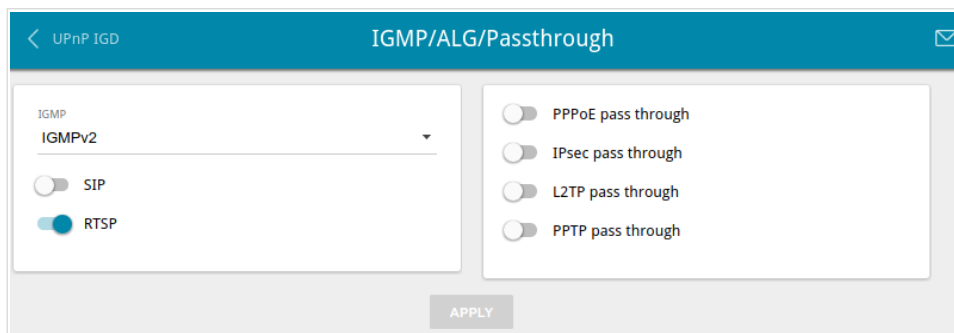


Figure 66. The **Advanced / IGMP/ALG/Passthrough** page.

The following elements are available on the page:

Parameter	Description
IGMP	Select a version of IGMP from the drop-down list. Such a setting allows to enable multicasting from the WAN connection selected in the IGMP section on the Connections Setup / WAN page.
SIP	Move the switch to the right to enable SIP. Such a setting allows using the SIP ALG function. This function allows VoIP traffic to pass through the NAT-enabled gateway. ²
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.

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

² On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / IGMP/ALG/Passthrough** page, connect an Ethernet cable between a LAN port of the gateway and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

IPsec

On the **Advanced / IPsec** page, you can configure VPN tunnels based on IPsec protocol. IPsec is a protocol suite for securing IP communications.

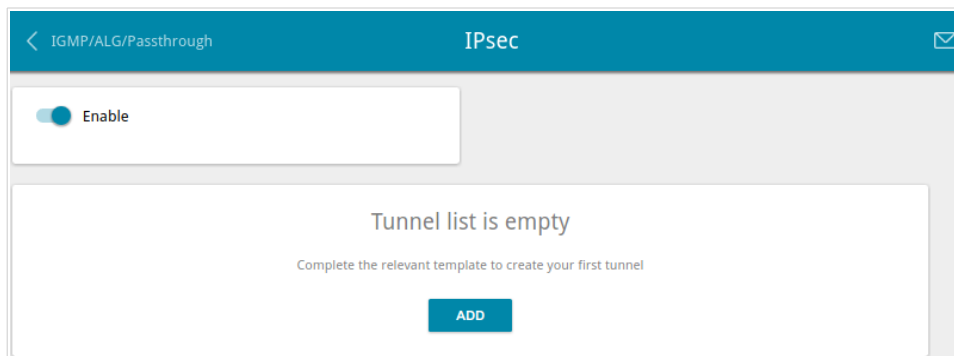
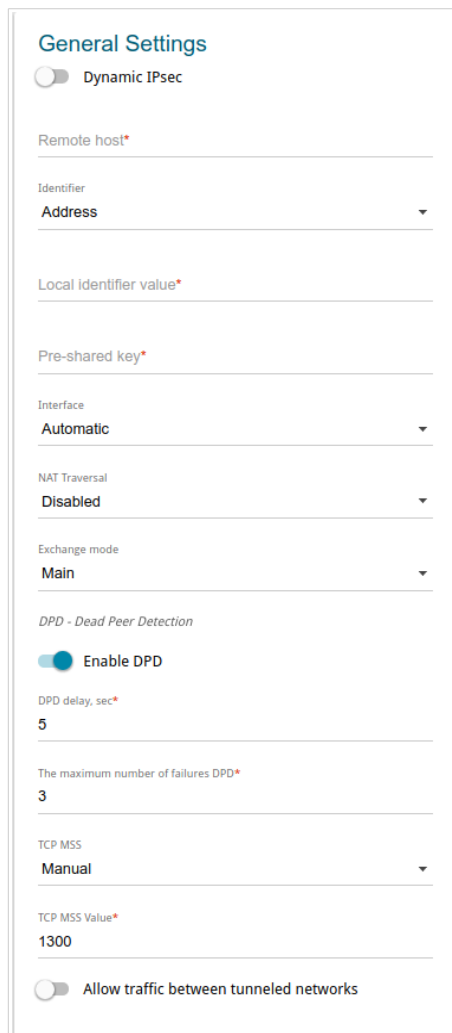


Figure 67. The **Advanced / IPsec** page.

To allow IPsec tunnels, move the **Enable** switch to the right. Then click the **ADD** button to create a new tunnel.



Setting for both devices which establish the tunnel should be the same.



General Settings

Dynamic IPsec

Remote host*

Identifier
Address

Local identifier value*

Pre-shared key*

Interface
Automatic

NAT Traversal
Disabled

Exchange mode
Main

DPD - Dead Peer Detection

Enable DPD

DPD delay, sec*
5

The maximum number of failures DPD*
3

TCP MSS
Manual

TCP MSS Value*
1300

Allow traffic between tunneled networks

Figure 68. The page for adding an IPsec tunnel. The **General Settings** section.

You can specify the following parameters:

Parameter	Description
General Settings	
Dynamic IPsec	Move the switch to the right to allow a remote host with any public IP address to connect to the gateway via IPsec protocol. Such a setting can be specified for one tunnel only. Connection requests via this tunnel can be sent by a remote host only.
Remote host	A remote subnet VPN gateway IP address. The field is available if the Dynamic IPsec switch is moved to the left.

Parameter	Description
Identifier	<p>Select an identification method for the local host (gateway) from the drop-down list:</p> <p>Address: The local host is identified by its IP address.</p> <p>FQDN: The local host is identified by its domain name. The value is unavailable if the Main value is selected from the Exchange mode list.</p>
Local identifier value	Specify the local host identifier.
Pre-shared key	A key for mutual authentication of the parties.
Interface	Select a WAN connection through which the tunnel will pass. When the Automatic value is selected, the gateway uses the default WAN connection.
NAT Traversal	<p>The NAT Traversal function allows VPN traffic to pass through the NAT-enabled gateway.</p> <p>Select the Disabled value to disable the function.</p> <p>Select the Enabled value to enable the function if it is supported by a remote host.</p> <p>Select the Force value to make the function be always on, even if it is not supported by a remote host.</p>
Exchange mode	<p>Select the mode of negotiation from the drop-down list:</p> <p>Main: The mode provides the most secure communication between the parties in the course of negotiation of the authentication procedures.</p> <p>Base: The draft negotiation mode with preliminary authentication of a host.</p> <p>Aggressive: The mode provides faster operation as it skips several stages of negotiation of the authentication procedures.</p>
Enable DPD	Move the switch to the right to enable using DPD protocol for this tunnel. Such a setting allows to check the status of a remote host: if encrypted packets exchange between the gateway and the remote host breaks down, the gateway starts sending DPD messages to the remote host. If the switch is moved to to the left, the DPD delay and The maximum number of failures DPD fields are not available for editing.
DPD delay	A time period (in seconds) between attempts to check the status of a remote host. By default, the value 5 is specified.

Parameter	Description
The maximum number of failures DPD	A number of DPD messages that were sent to check the status of a remote host and left unanswered. By default, the value 3 is specified. If a remote host does not answer the specified number of messages, the gateway breaks down the tunnel connection, removes the encryption keys, and tries to activate the connection.
TCP MSS	<i>Maximum Segment Size of a TCP packet.</i> This parameter influences the size of a TCP packet which will be sent from a remote host to the gateway. If the Manual value is selected, you can specify the parameter in the TCP MSS Value field. If the Path MTU discovery value is selected, the parameter will be configured automatically.
TCP MSS Value	The maximum size (in bytes) of a non-fragmented packet. The field is available for editing when the Manual value is selected from the TCP MSS drop-down list.
Allow traffic between tunneled networks	Move the switch to the right to allow data exchange between subnets with which IPsec tunnels have been created.

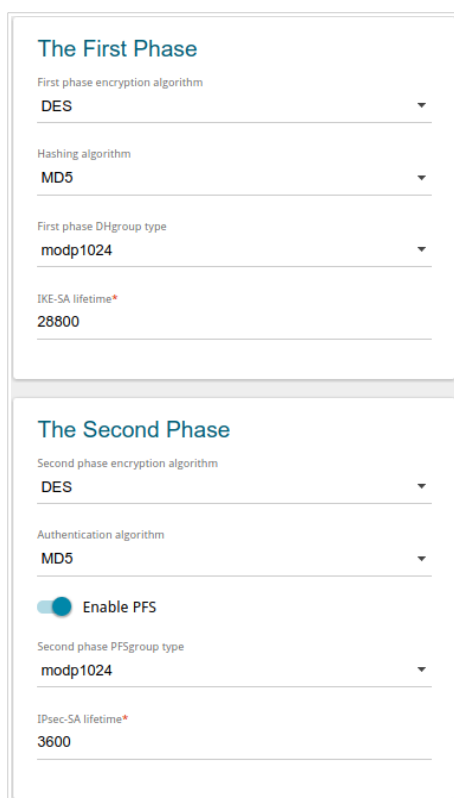


Figure 69. The page for adding an IPsec tunnel. **The First Phase / The Second Phase** sections.

Parameter	Description
The First Phase	
First phase encryption algorithm	Select encryption algorithm from the drop-down list.
Hashing algorithm	Select hashing algorithm from the drop-down list.
First phase DHgroup type	A Diffie-Hellman key group for Phase 1. Select a value from the drop-down list.
IKE-SA lifetime	The lifetime of IKE-SA keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should exceed the value specified in the IPsec-SA lifetime field. Specify 0 if you don't want to limit the lifetime of the keys.
The Second Phase	
Second phase encryption algorithm	Select encryption algorithm from the drop-down list.
Authentication algorithm	Select authentication algorithm from the drop-down list.

Parameter	Description
Enable PFS	Move the switch to the right to enable the PFS option (<i>Perfect Forward Secrecy</i>). If the switch is moved to the right, a new encryption key exchange will be used for Phase 2. This option increases the security level of data transfer.
Second phase PFSgroup type	A Diffie-Hellman key group for Phase 2. Select a value from the drop-down list. The field is available if the Enable PFS switch is moved to the right.
IPsec-SA lifetime	The lifetime of IPsec-SA keys in seconds. After the specified period it is required to renegotiate the keys. Specify 0 if you don't want to limit the lifetime of the keys.

If you need to specify IP addresses of local and remote subnets for creating a tunnel, click the **ADD** button in the **Tunneled Networks** section.

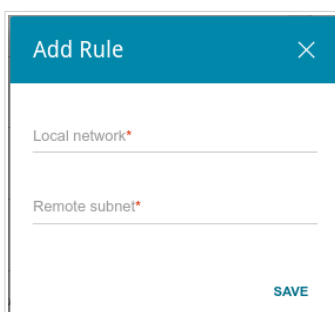


Figure 70. The page for adding an IPsec tunnel. The window for adding a tunneled network.

In the opened window, you can specify the following parameters:

Parameter	Description
Local network	A local subnet IP address and mask.
Remote subnet	A remote subnet IP address and mask.

To edit fields in the **Tunneled Networks** section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a subnet, select the checkbox located to the left of the relevant line in the table and click the **Delete** button. Also you can remove a subnet in the editing window.

After configuring all needed settings for the IPsec tunnel, click the **APPLY** button.

After clicking the **APPLY** button, the page with the **Tunnels** and **Status** sections opens. In the **Status** section, the current state of an existing tunnel is displayed.

To edit the parameters of an existing tunnel, in the **Tunnels** section, select the relevant tunnel in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove an existing tunnel, select the checkbox located to the left of the relevant line in the table and click the **Delete** button. Also you can remove a tunnel on the editing page.

To disable VPN tunnels based on IPsec protocol, move the **Enable** switch to the left.

VoIP

In this menu you can configure all parameters essential for VoIP via SIP and specify all needed settings for the phone connected to the gateway.

Basic Settings

On the **VoIP / Basic Settings** page, you can configure all needed settings for VoIP via SIP.

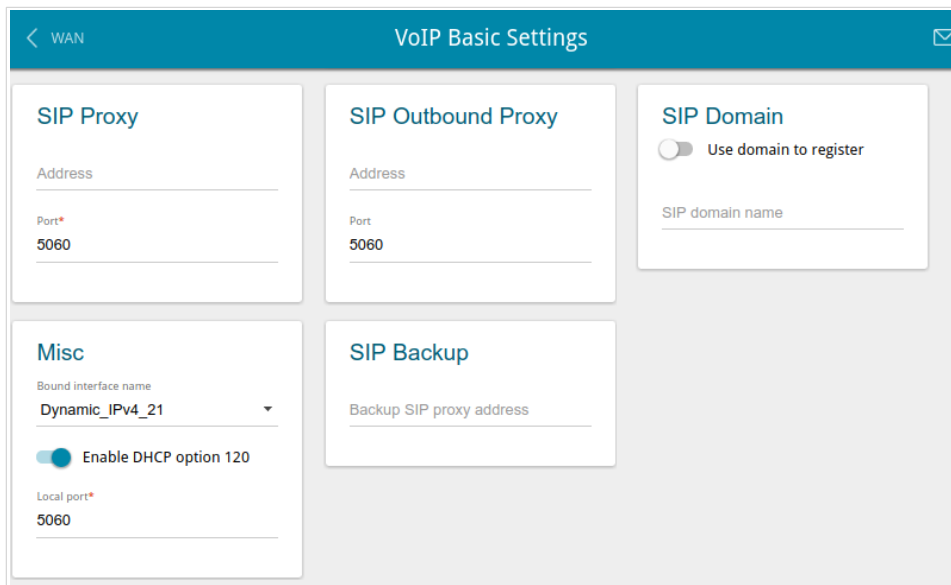


Figure 71. The **VoIP / Basic Settings** page.

Parameter	Description
SIP Proxy	
Address	An IP or URL address of the SIP proxy server.
Port	A port of the SIP proxy server. Unless another setting is given by your ISP, it is recommended to leave the default value (5060).
SIP Outbound Proxy	
Address	An IP or URL address of the SIP outbound proxy server.
Port	A port of the SIP outbound proxy server. Unless another setting is given by your ISP, it is recommended to leave the default value (5060).
SIP Domain	
Use domain to register	Move the switch to the right if your ISP requires to specify a domain name upon registration on the SIP proxy server. Then fill in the SIP domain name field.

Parameter	Description
SIP domain name	When this field is filled in, the gateway registers on the SIP proxy server using the specified domain name. When the field is blank, the gateway uses the IP address assigned to it.
Misc	
Bound interface name	From the drop-down list, select an interface (the local interface or an IPv4 WAN connection) which will be used for VoIP.
Enable DHCP option 120	Move the switch to the right to allow using DHCP option 120. When the option is enabled, the Address field in the SIP Proxy section and the Backup SIP proxy address field in the SIP Backup section are filled in automatically.
Local port	The gateway's port used for exchanging data with the SIP server. Unless another setting is given by your ISP, it is recommended to leave the default value (5060).
SIP Backup	
Backup SIP proxy address	An IP address of the backup SIP proxy server. The gateway uses the backup SIP proxy server in case of no response from the main SIP proxy server.

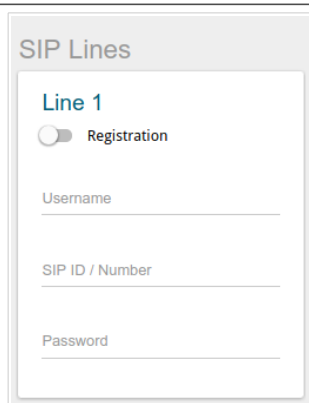


Figure 72. The **VoIP / Basic Settings** page. The **SIP Lines** section.

Parameter	Description
SIP Lines	
Line 1	
Registration	Move the switch to the right to register the line on the SIP proxy server.
Username	A username for this line. For most SIP proxy servers the username coincides with the phone number.

Parameter	Description
SIP ID / Number	A number for this line. The called party sees the specified value as the caller number.
Password	A user password for this line.

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

Advanced

On the **VoIP / Advanced settings** page, you can specify additional settings for VoIP via SIP.

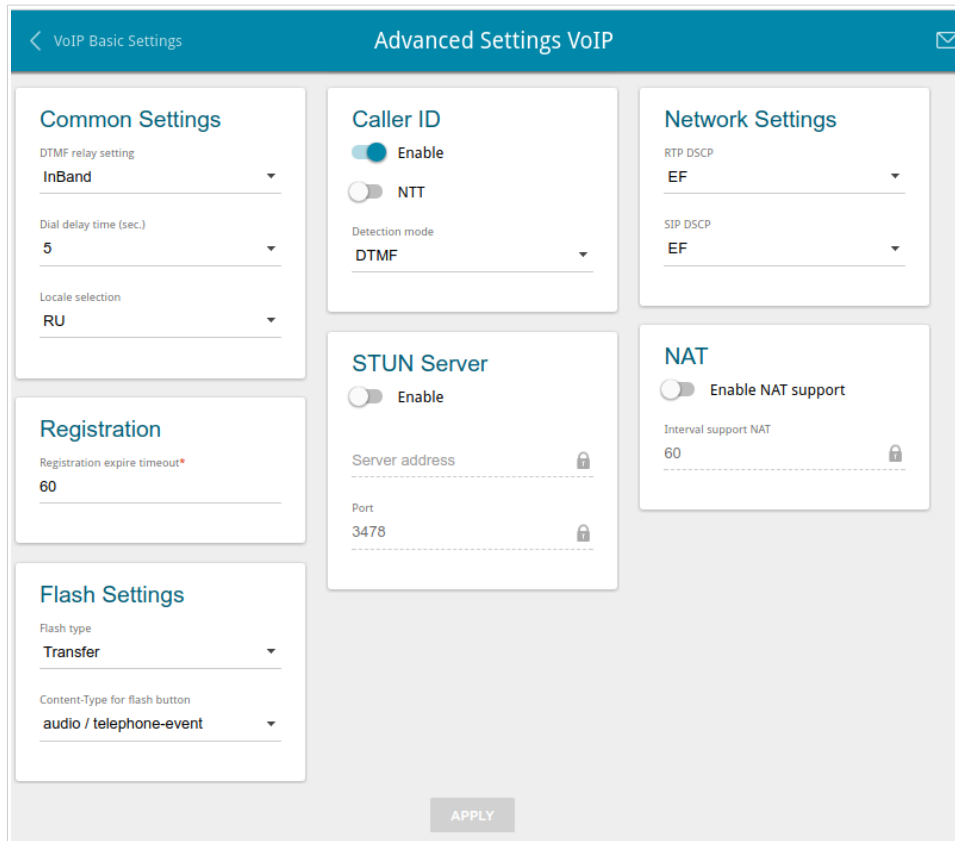


Figure 73. The **VoIP / Advanced** page.

Parameter	Description
Common Settings	
DTMF relay setting	From the drop-down list, select a mode for DTMF signal transmission. <ul style="list-style-type: none"> • InBand: transmission with voice data. • RFC2833: transmission in accordance with RFC2833. • SIPInfo: transmission in the relevant SIP messages.
Payload type	Select a data type from the drop-down list. The list is displayed if the RFC2833 value is selected from the DTMF relay setting drop-down list.
Dial delay time	The delay time before the next digit is dialed (from 3 to 9 seconds). When this time expires, the gateway regards that the dialing is completed and sends the request to the server. Select a needed value from the drop-down list.

Parameter	Description
Locale selection	Select your country from the drop-down list. By default, the value RU (Russia) is specified. This setting defines the parameters of the phone signals traditional for the specific country.
Caller ID	
Enable	Move the switch to the right to activate the automatic caller identification function for the phone connected to the FXS port of the gateway.
NTT	Move the switch to the right to enable support of the NTT standard.
Detection mode	Select the Caller ID mode for the phone connected to the FXS port of the gateway.
Network Settings	
RTP DSCP / SIP DSCP	<i>Differentiated Services Codepoint.</i> From the relevant drop-down list, select tags for voice and signaling traffic.
Registration	
Registration expire timeout	A time period (in seconds) after which the gateway changes the registration status in case of no response from the SIP proxy server.
STUN Server	
Enable	Move the switch to the right to enable the STUN client (<i>Session Traversal Utilities for NAT</i>). The STUN client sends requests to a STUN server. On the basis of the received replies, the client allows VoIP traffic to pass through the NAT-enabled gateway. If the switch is moved to the right, the Server address and Port fields are available for editing.
Server address	An IP or URL address of a STUN server to which a connection is established.
Port	A port of a STUN server to which a connection is established. By default, the port 3478 is specified.
NAT	
Enable NAT support	Move the switch to the right to allow the gateway to support the state of automatically forwarded ports by periodic exchange of service messages. If the switch is moved to the right, the Interval NAT support field is available for editing.

Parameter	Description
Interval support NAT	The time interval between service messages. Specify a needed value.
Flash Settings	
Flash type	The FLASH action type. <ul style="list-style-type: none">• Transfer: switching between calls.• SIPInfo: sending a service message to the SIP server. The value is available if the SIPInfo value is selected from the DTMF relay setting drop-down list.
Content-Type for flash button	If the SIPInfo value is selected from the Flash type drop-down list, you can select the type of data transferred in SIP INFO messages upon pressing the FLASH key.

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

SIP Lines

On the **VoIP / SIP Lines** page, you can specify incoming/outgoing call settings for the SIP line.

Figure 74. The **VoIP / SIP Lines** page.

Parameter	Description
General	
Registration	Move the switch to the right to register the line on the SIP proxy server.
Username	A username for this line. For most SIP proxy servers the username coincides with the phone number.
SIP ID / Number	A number for this line. The called party sees the specified value as the caller number.
Password	A user password for this line.
PIN code to dial	Fill in the field to allow the user of the phone to make calls only after dialing the PIN code.
Advanced	
Call waiting	Move the switch to the right to accept incoming calls when the line is busy. To switch between calls, press the FLASH key on the phone.

Parameter	Description
Anonymous call blocking	Move the switch to the right to reject calls when the calling party conceals its number.
Anonymous calling	Move the switch to the right to conceal your number from the called party.
DND	<i>Do Not Disturb</i> . Move the switch to the right to reject all incoming calls (the busy tone will be heard).
Enable pound key	Move the switch to the right to speed up dialing with pressing # (the pound key) immediately after dialing numbers.
Advanced Transfer	<p>Move the switch to the right to use combination of the FLASH key and number keys of the phone in order to organize three-party calls.</p> <p><u>Use of FLASH key</u></p> <ul style="list-style-type: none"> • The Advanced Transfer function is enabled. The phone connected to this line has an incoming call in the standby mode and an outgoing call in the talk mode. It's needed to press the FLASH key, hear the dial tone, and then press: <ul style="list-style-type: none"> ◦ the number key 0 in order to end the first call and continue the second call, ◦ the number key 1 in order to end the second call and continue the first call, ◦ the number key 2 in order to put the second call on hold and continue the first call, ◦ the number key 3 to have a three-party call with the first and second speakers. • The Advanced Transfer function is not enabled. The phone connected to this line has an incoming call in the standby mode and an outgoing call in the talk mode. It's needed: <ul style="list-style-type: none"> ◦ to press the FLASH key in order to put the second call on hold and continue the first call, ◦ to hang up the receiver in order to end both calls and connect the first and second speakers to each other.
Flash Settings	
Flash time / Flash time minimum	The maximum and minimum value for flash time (the user hangs up the receiver and lifts it again) which the gateway will regard as pressing the FLASH key.

Parameter	Description
Forwarding	
Forwarding	From the drop-down list, select a forwarding mode for the current line. Leave the Off value if forwarding is not needed.
Call forwarding number	A number to which the gateway redirects calls in accordance with the mode selected from the Forwarding list.
Forwarding delay	A time period (in seconds) after which the gateway redirects calls to the number specified in the Call forwarding number field. The field is available for editing if the If no answer value is selected from the Forwarding list.
Hotline	
Enable hotline	Move the switch to the right to make the phone connected to this line dial the number specified in the Number field after the receiver is lifted.
Number	A number dialed by the phone connected to this line after the receiver is lifted. Also you can specify a number in the format phone_number@IP_address for direct IP calls by passing the SIP proxy server. The field is available for editing if the Enable hotline switch is moved to the right.
Connect after	A time period (in seconds) between lifting up the receiver and dialing the hotline number. The field is available for editing if the Enable hotline switch is moved to the right.

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

Fax Settings

On the **VoIP / Fax Settings** page, you can specify settings of data receipt/transfer for the fax machine connected to the FXS port of the gateway.

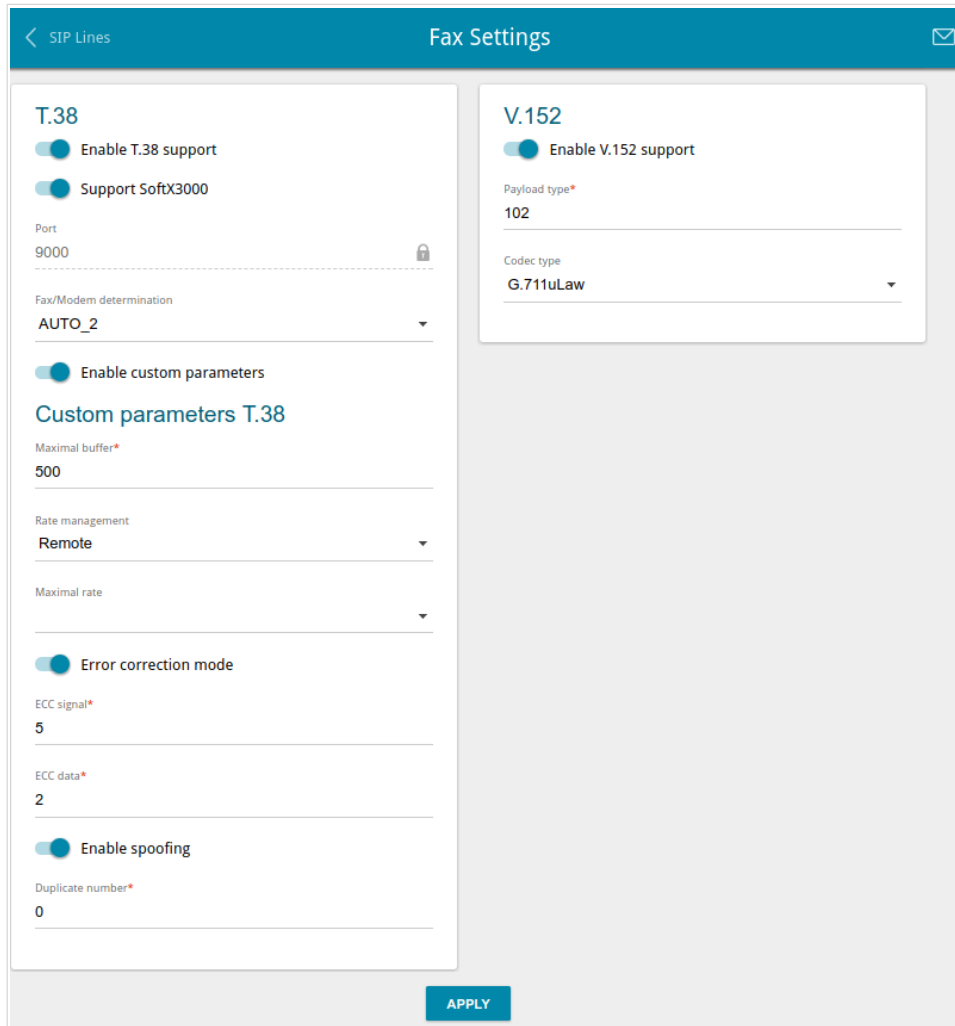


Figure 75. The **VoIP / Fax Settings** page.

Parameter	Description
T.38	
Enable T.38 support	Move the switch to the right to allow support of the T.38 protocol. If the switch is moved to the right, the Support SoftX3000 switch, the Port field, the Fax/Modem determination drop-down list, and the Enable custom parameters switch are displayed on the page.
Support SoftX3000	Move the switch to the right to let the gateway support operation with SoftX3000. If the switch is moved to the right, the Port field is unavailable for editing.

Parameter	Description
Port	The gateway's port for data transfer via T.38.
Fax/Modem determination	From the drop-down list, select a mode of fax/modem signal detection.
Enable custom parameters	Move the switch to the right to specify additional parameters for T.38. Upon that the Custom parameters T.38 section is displayed on the page.
Custom parameters T.38	
Maximal buffer	The maximum buffer size for data received by the gateway.
Rate management	From the drop-down list, select a method for facsimile data transfer rate management: Local or Remote .
Maximal rate	From the drop-down list, select the maximum rate for facsimile data receipt/transfer.
Error correction mode	Move the switch to the right to enable the error correction mode. When the switch is moved to the right, the ECC signal and ECC data fields are available for editing.
Enable spoofing	Move the switch to the right to let the gateway simulate facsimile data receipt/transfer in case of delays.
Duplicate number	Specify number of packet duplications.
V.152	
Enable V.152 support	Move the switch to the right to allow support of the V.152 recommendation. Upon that the Payload type field and the Codec type drop-down list are displayed on the page.
Payload type	Payload data type in accordance with RFC2833.
Codec type	From the drop-down list, select a codec for data transfer in accordance with V.152.

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

Audio Settings

On the **VoIP / Audio settings** page, you can configure audio parameters, volume and voice codecs.

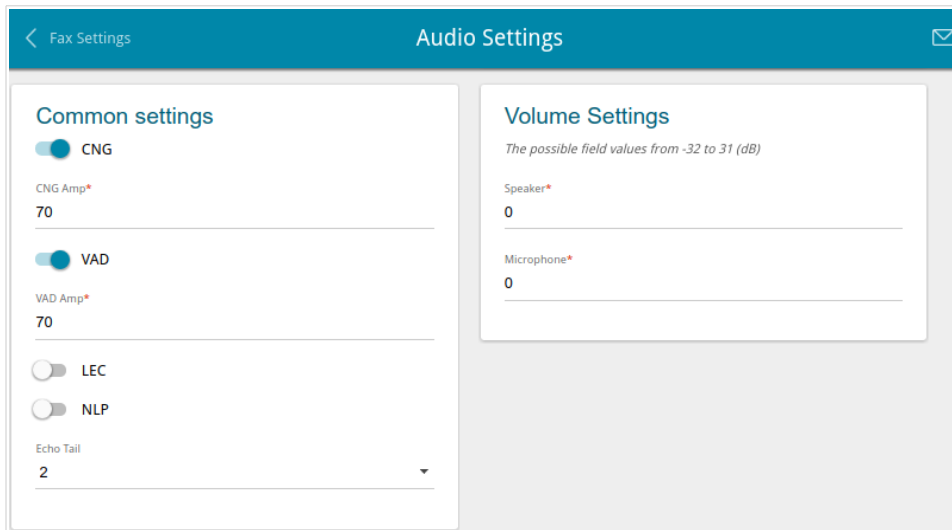


Figure 76. The **VoIP / Audio Settings** page. The **Common settings** and **Volume Settings** sections.

Parameter	Description
Common settings	
CNG	<i>Comfort Noise Generation.</i> Move the switch to the right to enable the function.
CNG Amp	Signal amplitude threshold to start comfort noise generation. Specify a value from 0 to 200 . If 0 is specified, the threshold is not set.
VAD	<i>Voice Activity Detection.</i> Move the switch to the right to enable the function.
VAD Amp	Signal amplitude threshold to start silence compression. Specify a value from 0 to 200 .
LEC	<i>Line Echo Cancellation.</i> Move the switch to the right to enable the function.
NLP	<i>Nonlinear Processing.</i> Move the switch to the right to enable the function.
Echo Tail	Maximum echo tail length (in milliseconds). Select the needed value from the drop-down list.

Parameter	Description
Volume Settings	
Speaker	Specify the earphone volume for the phone connected to the FXS port of the gateway.
Microphone	Specify the microphone sensitivity for the phone connected to the FXS port of the gateway.

In the **Codecs Settings** section, you can configure work of voice codecs in use.

Codec	State	Priority	Period of packetization
G.711uLaw	On	1	20
G.711ALaw	On	2	20
G.729a	On	3	20
G.723.1	On	4	30
G.726-16	On	5	20
G.726-24	On	6	20
G.726-32	On	7	20
G.726-40	On	8	20
G.722	On	9	20

Figure 77. The **VoIP / Audio Settings** page. The **Codecs Settings** section.

To change parameters of a codec, left-click the relevant line in the table.

Figure 78. The window for changing the codec parameters.

In the opened window, you can specify the following parameters:

Parameter	Description
Enable codec	To enable the codec, move the switch to the right. To disable the codec, move the switch to the left.
Priority	Priority of the codec upon setting a voice session. Select the needed value from the drop-down list.
Period of packetization	Quantity of milliseconds transmitted in one packet. Select the needed value from the drop-down list.

Click the **SAVE** button.

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

Routing call

On the **VoIP / Routing call** page, you can fill in the phone book for a device connected to the FXS port of the gateway.

Key	Number
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	

<input type="checkbox"/>	Source number	Destination number

Abbreviated Dial Add Delete

Dialplan Settings

Use dialplan

Misc

PIN code to dial

APPLY

Figure 79. The VoIP / Routing call page.

In the **Speed Dial** section, you can assign phone numbers to the digital keys of the phone set connected to this line. To do this, left-click the line corresponding to the key of the phone set. In the opened window, enter the needed number in the **Number** field and click the **SAVE** button. Also you can specify a number in the format **phone_number@IP_address** for direct IP calls by passing the SIP proxy server.

To change or delete the number assigned to the digital key, left-click the line corresponding to the key of the phone set, in the opened window, edit or remove the value of the **Number** field and click the **SAVE** button.

To use a number specified in the **Speed Dial** section, press # (the pound key) on the phone set, then press the relevant digital key.

In the **Abbreviated Dial** section, you can assign short numbers (as a rule, such numbers consist of two or three digits) to frequently used phone numbers. To do this, click the **Add** button. In the opened window, enter a short number in the **Source number** field, then enter the actual phone number in the **Destination number** field. Click the **SAVE** button. Also in the **Destination number** field you can specify a number in the format **phone_number@IP_address** for direct IP calls by passing the SIP proxy server.

To change a short or actual phone number, select of the relevant line in the table. In the opened window, change needed parameters and click the **SAVE** button.

To remove a phone number, select the checkbox located to the left of the relevant line in the table and click the **Delete** button.

To use a number specified in the **Abbreviated Dial** section, dial the needed short number on the phone set.

In the **Dialplan Settings** section, you can configure the dial plan for VoIP. To do this, move the **Use dialplan** switch to the right and in the **Dialplan** field displayed, specify the needed rule. You can specify several rules separated by the character | (vertical bar). You can use digits (0-9), the characters * (asterisk) and # (pound), and the following characters:

Parameter	Description
[]	Digits and/or the characters * and # within square brackets specify a range of values for a certain position in the number.
X	Any digit, the character * or #.
.	Any number of repetitions (including none) of the previous digit or character.
<>	Angle brackets containing digits separated by : (colon) allow to substitute the digit after the colon for the digit before the colon.

In the **Misc** section, fill in the **PIN code to dial** field to allow the user of the phone to make calls only after dialing the PIN code.

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

Call Feature Codes

On the **VoIP / Call Feature Codes** page, you can allow changing some parameters of the gateway directly from the phone set connected to the FXS port of the gateway.

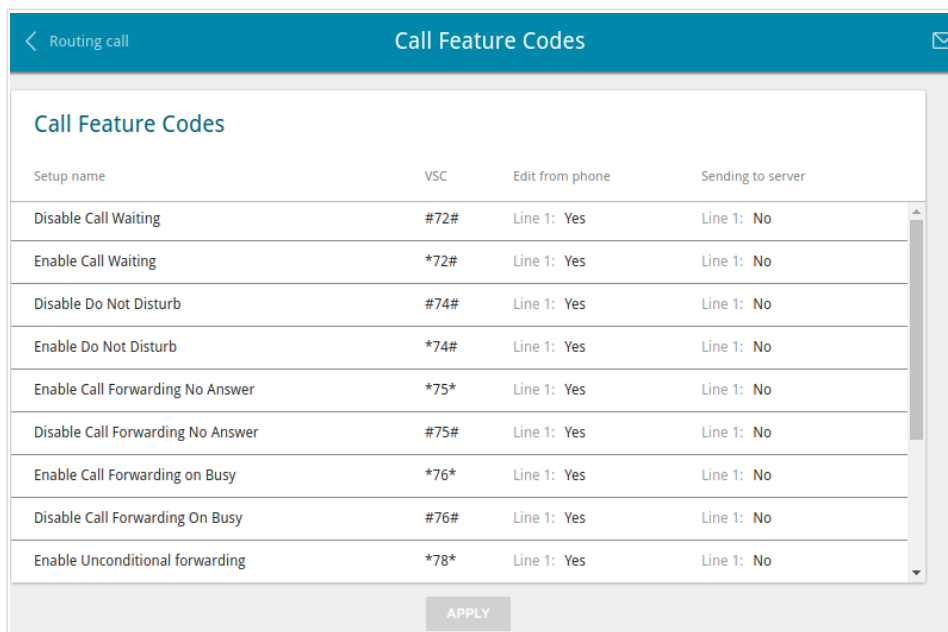


Figure 80. The **VoIP / Call Feature Codes** page.

The following call feature codes are available:

Parameter	Description
Disable Call Waiting	Disables the call waiting function.
Enable Call Waiting	Enables the call waiting function.
Disable Do Not Disturb	Disables rejection of incoming calls.
Enable Do Not Disturb	Enables rejection of all incoming calls (the busy tone will be heard).
Enable Call Forwarding No Answer	Enables call forwarding when this line gives no reply.
Disable Call Forwarding No Answer	Disables call forwarding when this line gives no reply.
Enable Call Forwarding On Busy	Enables call forwarding when this line is busy.
Disable Call Forwarding On Busy	Disables call forwarding when this line is busy.
Enable Unconditional forwarding	Enables forwarding for all calls.
Disable Unconditional forwarding	Disables forwarding for all calls.

Parameter	Description
Disable Hot Line	Disables the hotline.
Enable Hot Line	Enables the hotline.
Enable alarm clock	Enables the alarm clock for the time specified for this line.
Disable alarm clock	Disables the alarm clock.

To change parameters of a code, select the relevant line in the table.

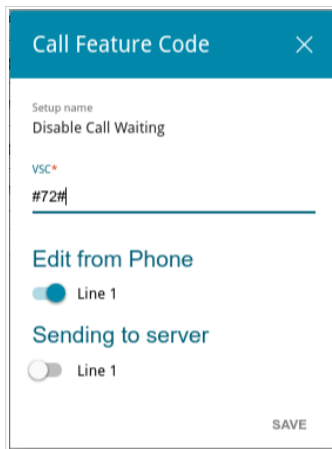


Figure 81. The **VoIP / Call Feature Codes** page. The window for editing the code parameters.

In the opened window, specify the needed parameters:

Parameter	Description
VSC	The value of the code. If the code ends with * (the asterisk key), further you can enter a value for the function in use (a number for call forwarding or time for the alarm clock). For example, the code for enabling the alarm clock: *55*HHMM#, where HHMM is time in 24-hour format.
Edit from Phone	
Line 1	Move the switch to the right to enable the code for the phone connected to the FXS port of the gateway. Move the switch to the left to disable the code for this phone.
Sending to server	
Line 1	Move the switch to the right to inform the SIP server when a user dials the code on the phone. Move the switch to the left if the server should not be informed.

Click the **SAVE** button.

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

Call Logging

On the **VoIP / Call Logging** page, you can configure the call log parameters and view information on all calls.

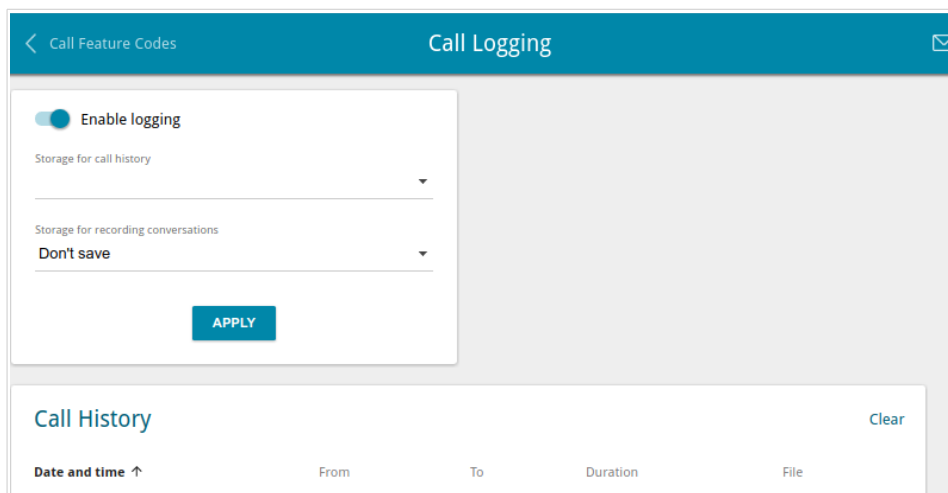


Figure 82. The **VoIP / Call Logging** page.

To enable logging of calls, move the **Enable logging** switch to the right and click the **APPLY** button.

In the **Call History** section, the detailed information on all calls are displayed: date and time, call duration, and a caller or called party number.

To sort the log records, in the **Call History** section, left-click the name of a column and click the **Sort** icon (↑ (ascending), ↓ (descending)) displayed.

To remove the call log, click the **Clear** button. The call log is also removed when the device is rebooted or powered off.

Security

On the **VoIP / Security** page, you can configure filtering rules for incoming calls of the phone connected to the FXS port of the gateway.

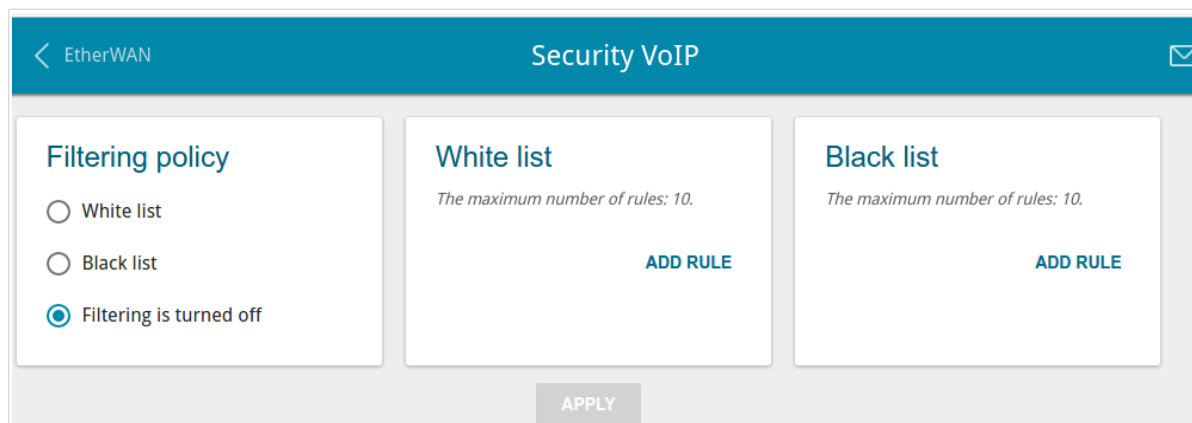


Figure 83. The **VoIP / Security** page.

In the **Filtering policy** section, select the needed choice of the radio button.

- **White list:** the gateway accepts incoming calls (INVITE packets) only from IP addresses or domains specified in the **White list** section;
- **Black list:** the gateway accepts incoming calls (INVITE packets) from any IP addresses or domains except for those specified in the **Black list** section;
- **Filtering is turned off:** filtering by IP addresses or domain names is not performed.

To add an IP address or domain name, click the **ADD RULE** button in the **White list** or **Black list** section correspondingly. In the line displayed, specify the needed value.

To remove an IP address or domain name from the white or black list, click the **Delete** icon (✕) in the relevant line.

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

Alarm Clock

On the **VoIP / Alarm clock** page, you can configure the phone connected to the FXS port of the gateway as an alarm clock.

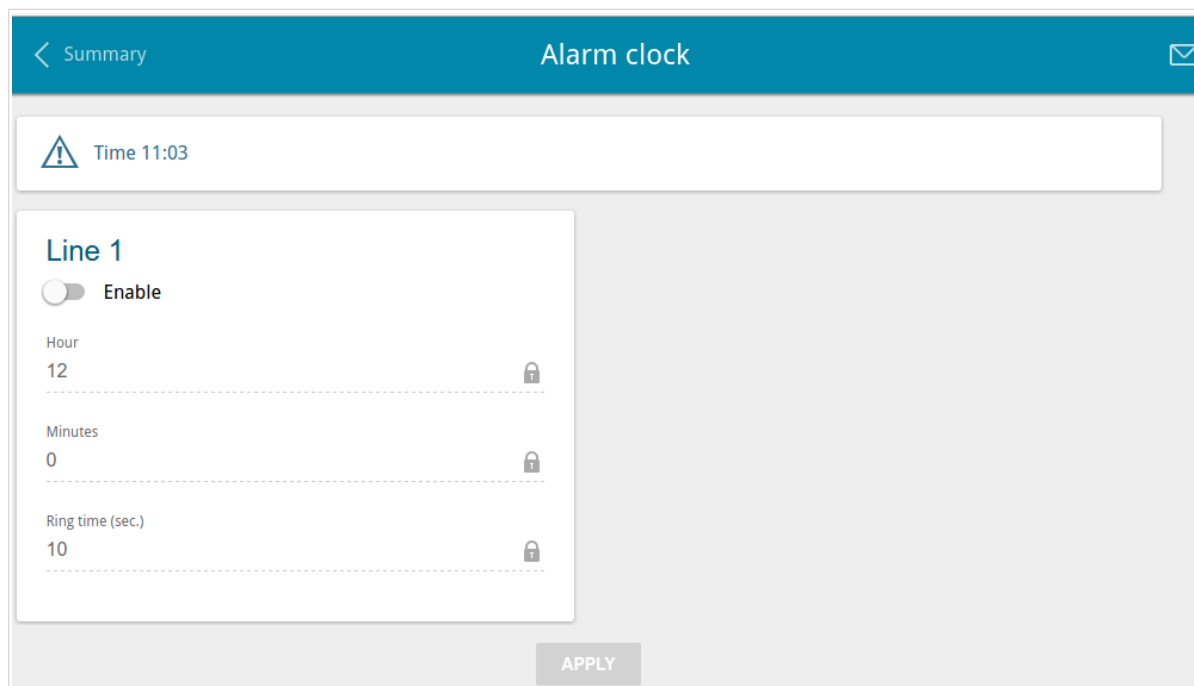


Figure 84. The **VoIP / Alarm clock** page.

Move the **Enable** switch to the right. Then specify the time at which the phone should ring in the **Hour** and **Minutes** fields. In the **Ring time** field, specify the signal duration. Then click the **APPLY** button.



When the gateway 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.

Firewall

In this menu you can configure the firewall of the gateway:

- add rules for IP filtering
- create virtual servers
- define a DMZ
- configure the MAC filter
- specify restrictions on access to certain web sites.

IP Filter

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

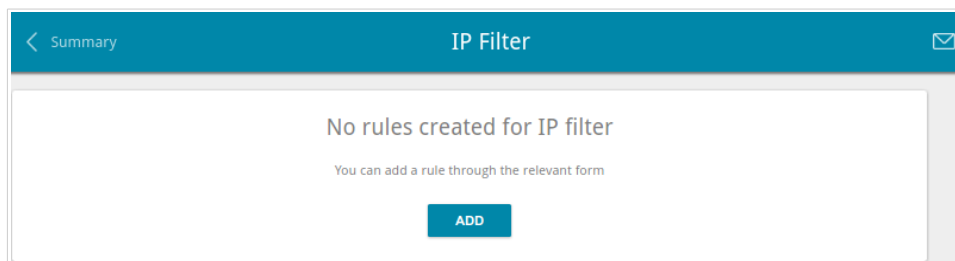


Figure 85. The **Firewall / IP Filter** page.

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

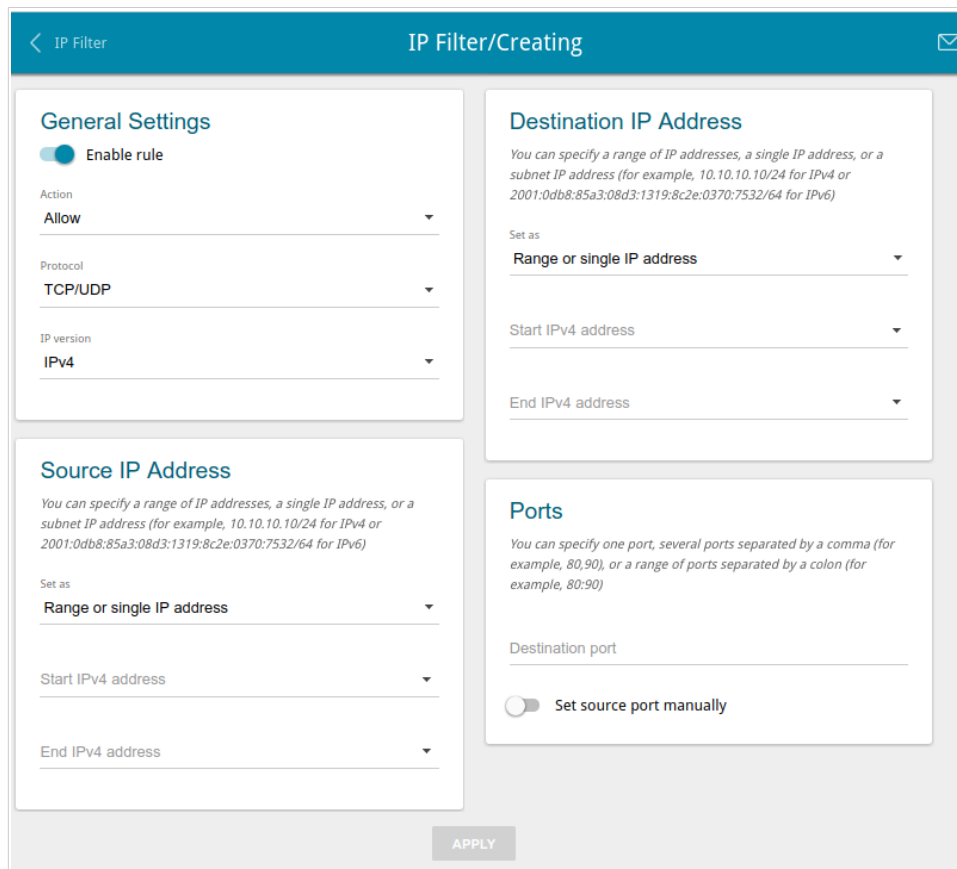


Figure 86. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description
General Settings	
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. Allow: Allows packet transmission in accordance with the criteria specified by the rule. Deny: Denies packet transmission in accordance with the criteria specified by the rule.
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Source IP Address	
Set as	Select the needed value from the drop-down list.

Parameter	Description
Start IPv4 address / Start IPv6 address	The source host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank. You can choose a device connected to the gateway's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The source host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The source subnet IPv4 or IPv6 address. The field is displayed when the Subnet value is selected from the Set as drop-down list.
Destination IP Address	
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank. You can choose a device connected to the gateway's LAN at the moment. To do this, select the relevant IPv4 or IPv6 address from the drop-down list (the field will be filled in automatically).
End IPv4 address / End IPv6 address	The destination host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The destination subnet IPv4 or IPv6 address. The field is displayed when the Subnet value is selected from the Set as drop-down list.
Ports	
Destination port	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.
Set source port manually	Move the switch to the right to specify a port of the source IP address manually. Upon that the Source port field is displayed.
Source port	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.

Click the **APPLY** button.

To edit a rule for IP filtering, select the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **Delete** button. Also you can remove a rule on the editing page.

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.

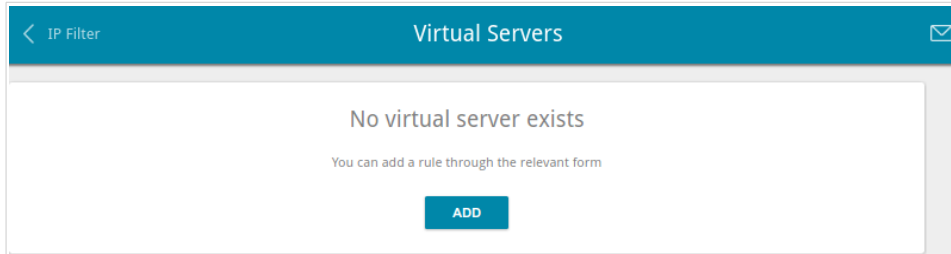


Figure 87. The **Firewall / Virtual Servers** page.

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

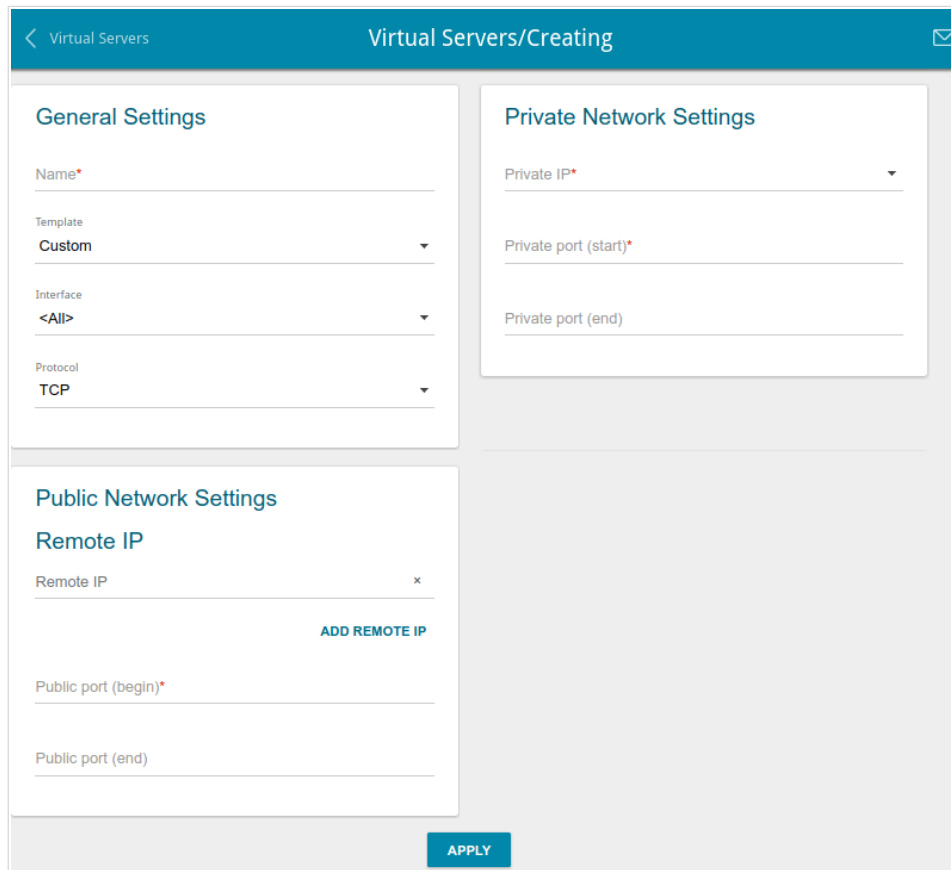


Figure 88. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description
General Settings	
Name	A name for the virtual server for easier identification. You can specify any name.
Template	Select a virtual server template from the drop-down list, or select Custom to specify all parameters of the new virtual server manually.
Interface	A WAN connection to which this virtual server will be assigned.
Protocol	A protocol that will be used by the new virtual server. Select a value from the drop-down list.
Public Network Settings	
Remote IP	Enter the IP address of the server from the external network. To add one more IP address, click the ADD REMOTE IP button and enter the address in the displayed line. To remove the IP address, click the Delete icon (✕) in the line of the address.
Public port (begin)/ Public port (end)	A port of the gateway from which traffic is directed to the IP address specified in the Private IP field in the Private Network Settings section. Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the Public port (begin) field and leave the Public port (end) field blank.
Private Network Settings	
Private IP	The IP address of the server from the local area network. To choose a device connected to the gateway's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).
Private port (start)/ Private port (end)	A port of the IP address specified in the Private IP field to which traffic is directed from the Public port . Specify the start and the end value for the port range. If you need to specify one port, enter the needed value in the Private port (start) field and leave the Private port (end) field blank.

Click the **APPLY** button.

To edit the parameters of an existing server, select the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove a server, select the checkbox located to the left of the relevant line of the table and click the **Delete** button. Also you can remove a server on the editing page.

DMZ

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

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

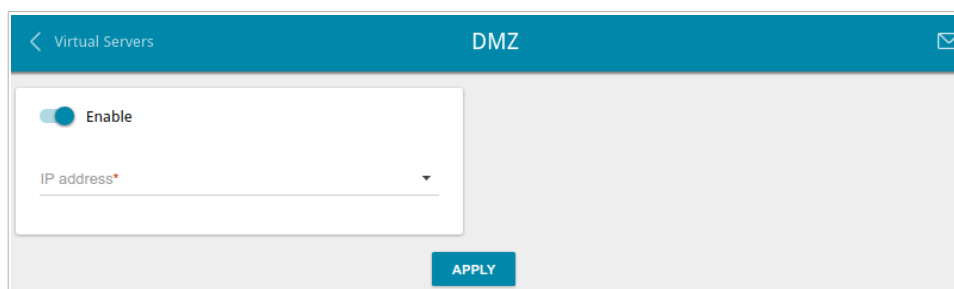


Figure 89. The **Firewall / DMZ** page.

To enable the DMZ, move the **Enable** switch to the right.

Enter the IP address of a host from your network in the **IP address** field. To choose a device connected to the gateway's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).

Click the **APPLY** button.

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

To disable the DMZ, move the **Enable** switch to the left and click the **APPLY** button.

MAC Filter

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

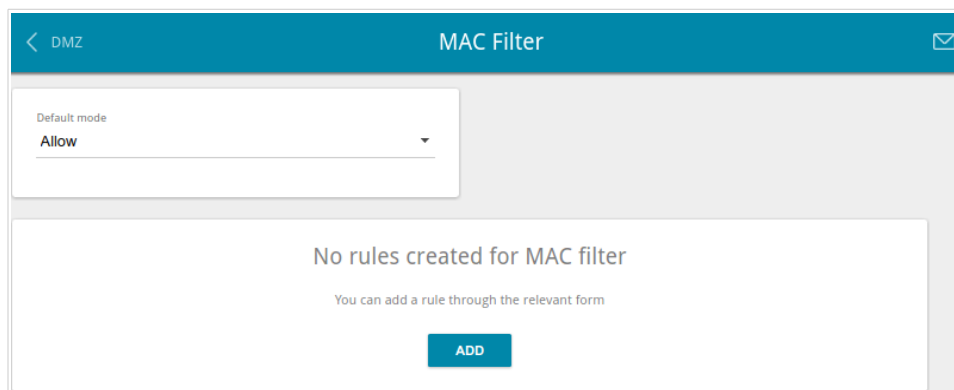


Figure 90. The **Firewall / MAC Filter** page.

Select the needed action from the drop-down list in the **Default mode** section to configure filtering for all devices of the gateway's network:

- **Allow**: Allows access to the gateway's network and to the Internet for devices (the value is specified by default);
- **Deny**: Blocks access to the gateway's network for devices.

! You can use the **Deny** mode only if an active rule which allows access to the device's network is created on the page.

To create a rule (specify a MAC address of a device for which the specified filtering mode will be applied), click the **ADD** button.

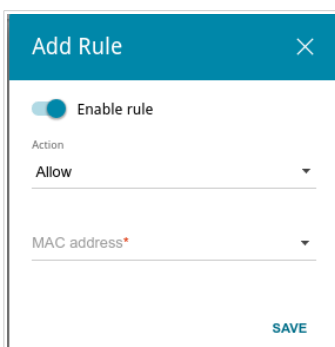


Figure 91. The window for adding a rule for the MAC filter.

In the opened window, you can specify the following parameters:

Parameter	Description
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Action	Select an action for the rule. Deny: Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices. Allow: Allows access to the gateway's network and to the Internet for the device with the specified MAC address even if the default mode denies access for all devices.
MAC address	The MAC address of a device from the gateway's LAN. You can enter the MAC address of a device connected to the gateway's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).

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

To edit a rule, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click the **Delete** button. Also you can remove a rule in the editing window.

URL Filter

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

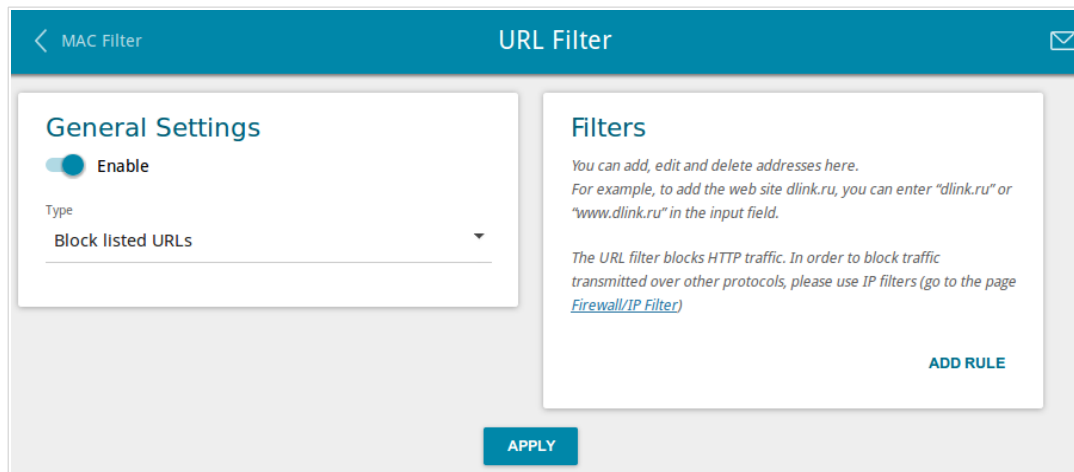


Figure 92. The **Firewall / URL Filter** page.

To enable the URL filter, in the **General Settings** section, move the **Enable** switch to the right, then select the needed mode from the **Type** drop-down list:

- **Block listed URLs:** when this value is selected, the gateway blocks access to all addresses specified in the **Filters** section;
- **Block all URLs except listed:** when this value is selected, the gateway allows access to addresses specified in the **Filters** section and blocks access to all other web sites.

Click the **APPLY** button.

To specify URL addresses to which the selected filtering mode will be applied, in the **Filters** section, click the **ADD RULE** button and enter a relevant address in the displayed line. Then click the **APPLY** button.

To remove an address from the list of URL addresses, click the **Delete** icon (✕) in the line of the relevant URL address. Then click the **APPLY** button.

System

In this menu you can do the following:

- change the password used to access the gateway's settings
- restore the factory default settings
- create a backup of the gateway's configuration
- restore the gateway's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the gateway
- change the web-based interface language
- update the firmware of the gateway
- configure automatic notification on new firmware version
- view the system log; configure sending the system log to a remote host
- check availability of a host on the Internet through the web-based interface of the gateway
- trace the route to a host
- allow or forbid access to the gateway via TELNET
- configure automatic synchronization of the system time or manually configure the date and time for the gateway.

Configuration

On the **System / Configuration** page, you can change the password for the administrator account used to access the web-based interface of the gateway and to access the device settings via TELNET, restore the factory defaults, backup the current configuration, restore the gateway's configuration from a previously created file, save the changed settings to the non-volatile memory, reboot the device, or change the web-based interface language.

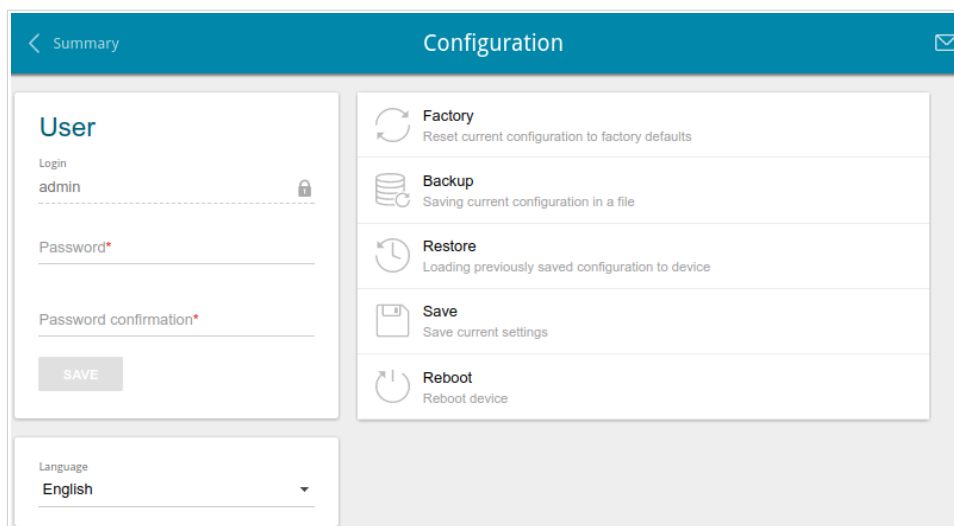


Figure 93. The **System / Configuration** page.

In order to change the password for the administrator account, in the **User** section, enter a new password in the **Password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.³ Then click the **SAVE** button.



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

To change the web-based interface language, select the needed value from the **Language** drop-down list.

³ 0-9, A-Z, a-z, space, !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~.

The following buttons are also available on the page:

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button (see the <i>Back and Bottom Panels</i> section, page 11).
Backup	Click the button to save the configuration (all settings of the gateway) to your PC. The configuration backup will be stored in the download location of your web browser.
Restore	Click the button and follow the dialog box appeared to select a previously saved configuration file (all settings of the gateway) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The gateway saves changed settings automatically. If changed settings have not been saved automatically, a notification is displayed in the top right part of the page.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

Firmware Update

On the **System / Firmware Update** page, you can update the firmware of the gateway and configure the automatic check for updates of the gateway's firmware.

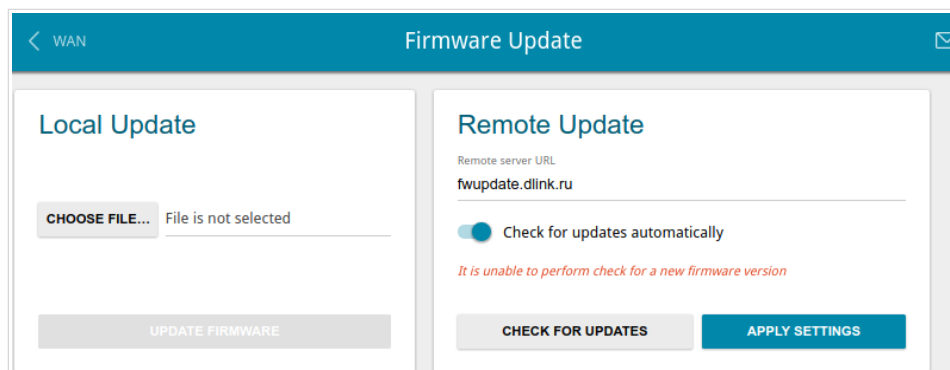


Figure 94. The **System / Firmware Update** page.

You can view the current version of the gateway's firmware on the **Summary** page.

By default, the automatic check for the gateway's firmware updates is enabled. If a firmware update is available, a notification will be displayed in the top right corner of the page.

To disable the automatic check for firmware updates, in the **Remote Update** section, move the **Check for updates automatically** switch to the left and click the **APPLY SETTINGS** button.

To enable the automatic check for firmware updates, in the **Remote Update** section, move the **Check for updates automatically** switch to the right and click the **APPLY SETTINGS** button.

By default, in the **Remote server URL** field, the D-Link update server address (**fwupdate.dlink.ru**) is specified.

You can update the firmware of the gateway locally (from the hard drive of your PC) or remotely (from the update server).

Local Update



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

To update the firmware of the gateway locally, follow the next steps:

1. Download a new version of the firmware from www.dlink.ru.
2. Click the **CHOOSE FILE** button in the **Local Update** section on the **System / Firmware Update** page to locate the new firmware file.
3. Click the **UPDATE FIRMWARE** button.
4. Wait until the gateway is rebooted (about one and a half or two minutes).
5. Log into the web-based interface using the login (**admin**) and the current password.

If after updating the firmware the gateway doesn't work correctly, please restore the factory default settings. To do this, click the **Factory** button on the **System / Configuration** page. Wait until the gateway is rebooted.

Remote Update



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

To update the firmware of the gateway remotely, follow the next steps:

1. On the **System / Firmware Update** page, in the **Remote Update** section, click the **CHECK FOR UPDATES** button to check if a newer firmware version exists.
2. Click the **UPDATE FIRMWARE** button (the button is displayed if a newer version of the firmware is available).
3. Wait until the gateway is rebooted (about one and a half or two minutes).
4. Log into the web-based interface using the login (**admin**) and the current password.

If after updating the firmware the gateway doesn't work correctly, please restore the factory default settings. To do this, click the **Factory** button on the **System / Configuration** page. Wait until the gateway is rebooted.

Log

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

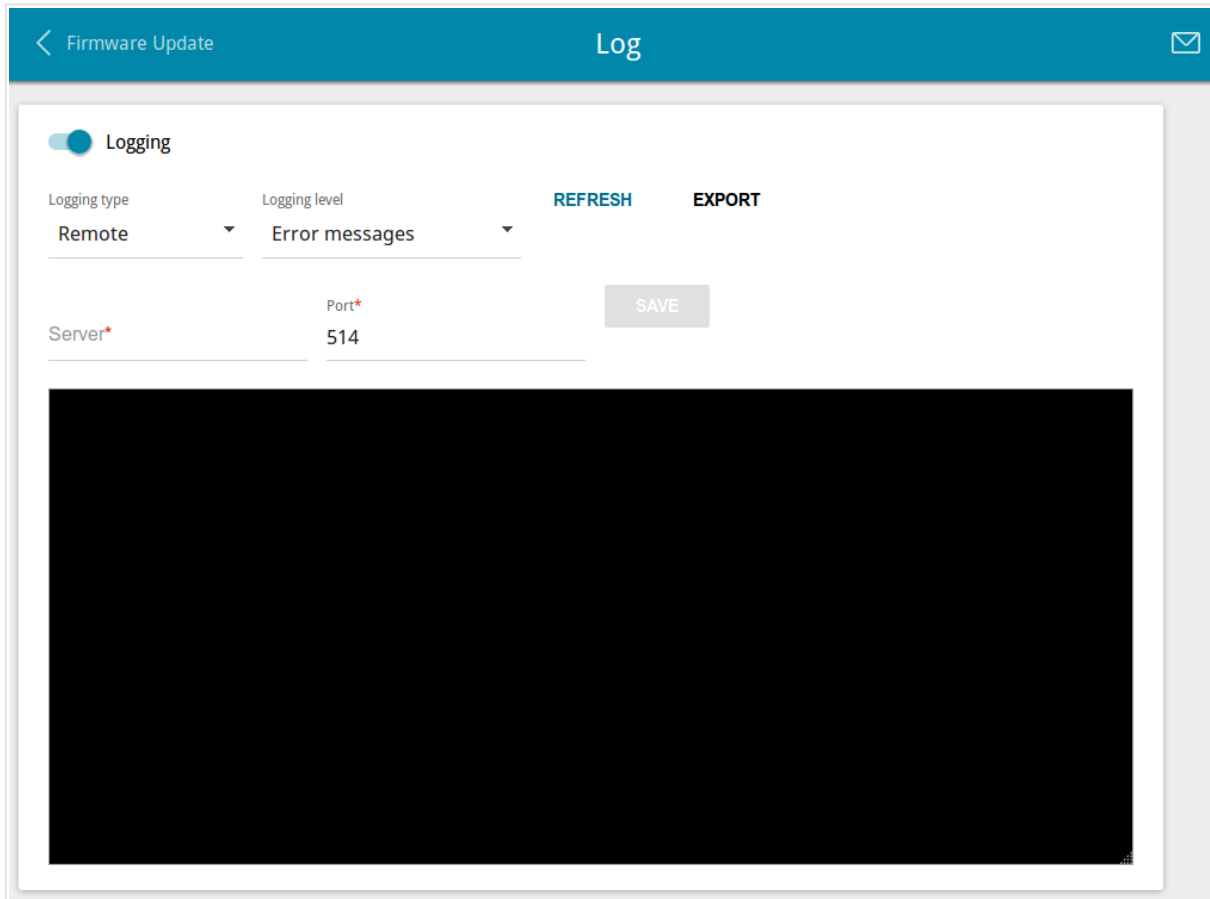


Figure 95. The **System / Log** page.

To enable logging of the system events, move the **Logging** switch to the right. Then specify the needed parameters.

Parameter	Description
Logging type	Select a type of logging from the drop-down list. <ul style="list-style-type: none">• Local: the system log is stored in the gateway's memory. When this value is selected, the Server and Port fields are not displayed.• Remote: the system log is sent to the remote host specified in the Server field.• Remote and local: the system log is stored in the gateway's memory and sent to the remote host specified in the Server field.
Logging level	Select a type of messages and alerts/notifications to be logged.

Parameter	Description
Server	The IP or URL address of the host from the local or global network, to which the system log will be sent.
Port	A port of the host specified in the Server field. By default, the value 514 is specified.

After specifying the needed parameters in the **Server** and **Port** fields, click the **SAVE** button.

To disable logging of the system events, move the **Logging** switch to the left.

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

To save the system log to your PC, click the **EXPORT** button. The file will be stored in the download location of your web browser.

Ping

On the **System / Ping** page, you can check availability of a host from the local or global network via the Ping utility.

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

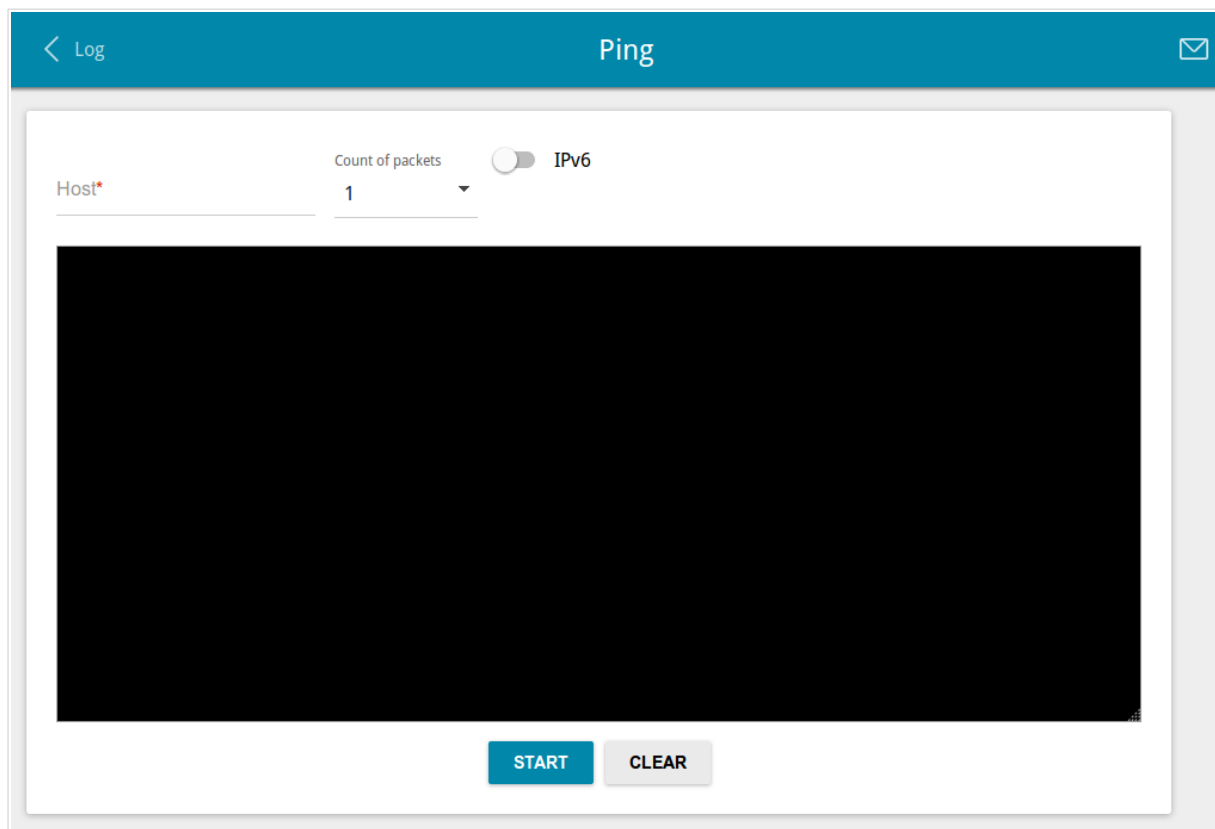


Figure 96. The **System / Ping** page.

To check availability of a host, enter the IP address or name of this host in the **Host** field and select a number of requests that will be sent in order to check its availability from the **Count of packets** drop-down list. If availability check should be performed with IPv6, move the **IPv6** switch to the right. Click the **START** button. After a while, the results will be displayed on the page.

To remove the check result from the page, click the **CLEAR** button.

Traceroute

On the **System / Traceroute** page, you can determine the route of data transfer to a host via the traceroute utility.

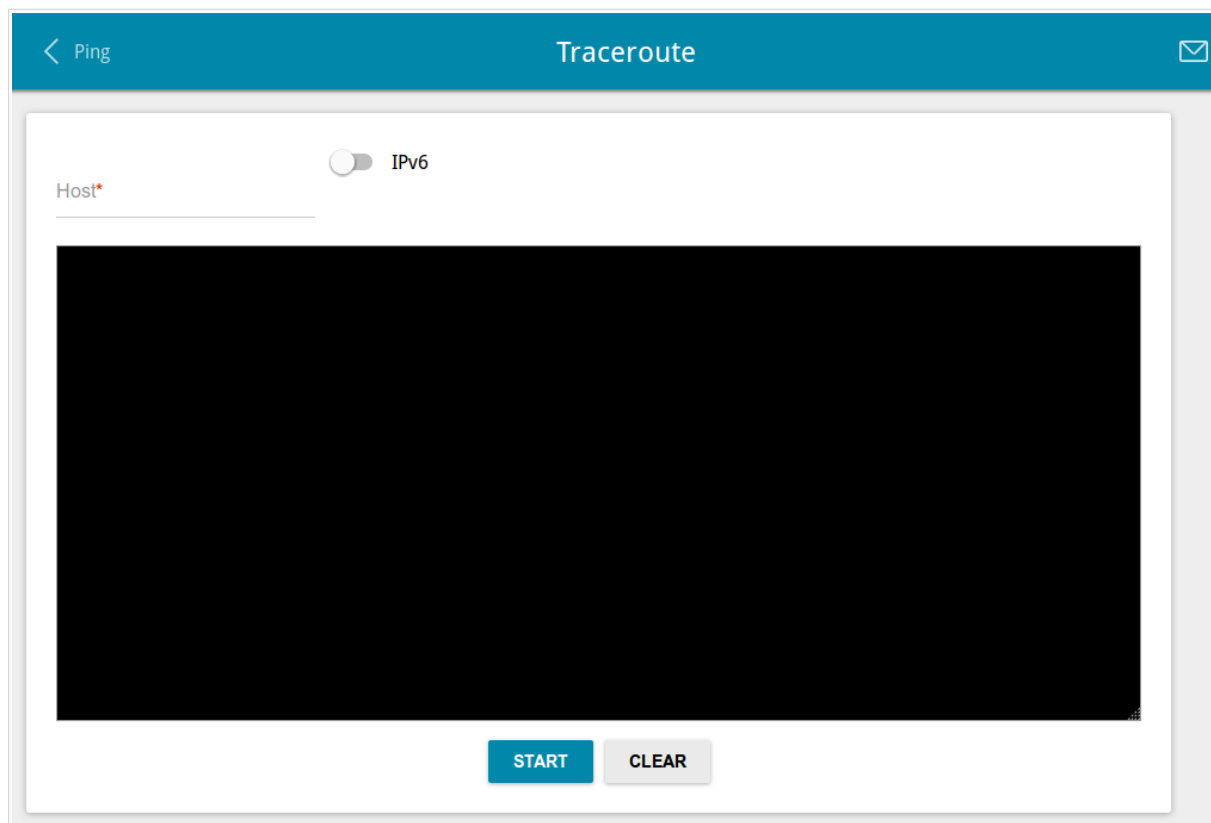


Figure 97. The **System / Traceroute** page.

To determine the route, enter the name or IP address of a host in the **Host** field. If the route should be determined using IPv6, move the **IPv6** switch to the right. Click the **START** button. After a while, the results will be displayed on the page.

To remove the check result from the page, click the **CLEAR** button.

Telnet

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

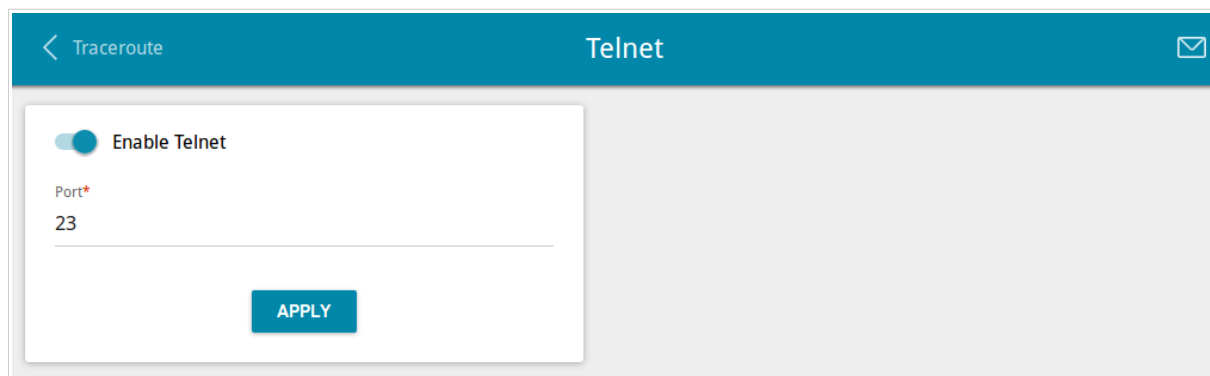


Figure 98. The **System / Telnet** page.

To disable access via TELNET, move the **Enable Telnet** switch to the left and click the **APPLY** button.

To enable access via TELNET again, move the **Enable Telnet** switch to the right. In the **Port** field, enter the number of the gateway's port through which access will be allowed (by default, the port **23** is specified). Then click the **APPLY** button.

System Time

On the **System / System Time** page, you can manually set the time and date of the gateway or configure automatic synchronization of the system time with a time server on the Internet.

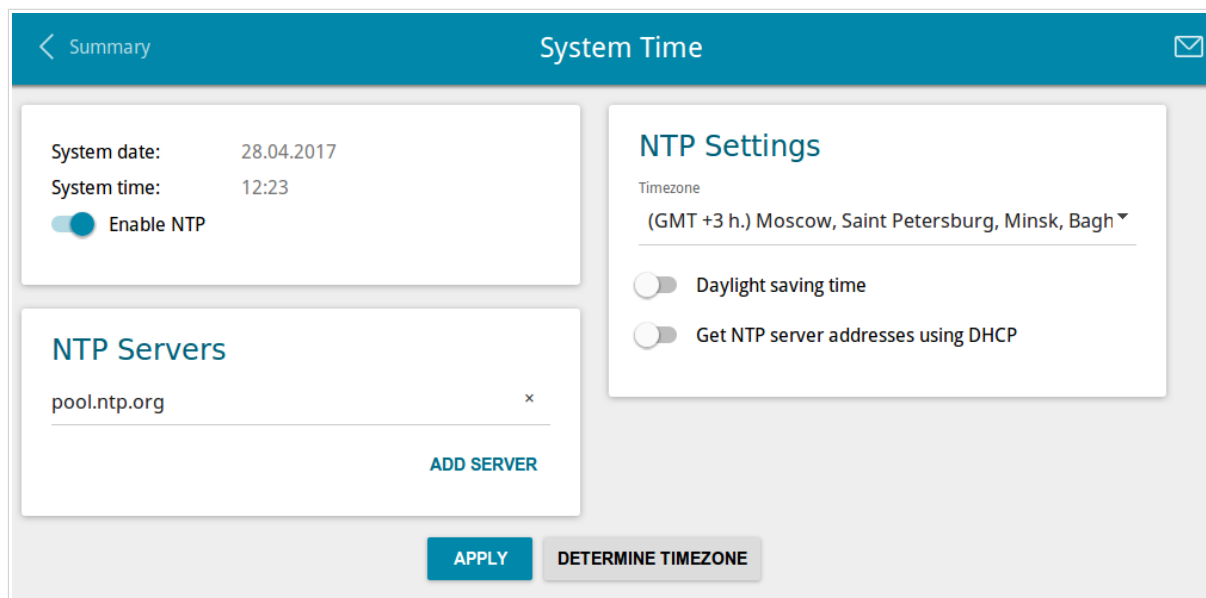


Figure 99. The **System / System Time** page.

To set the system time manually, follow the next steps:

1. Move the **Enable NTP** switch to the left.
2. In the **Time Settings** section, specify needed values. To specify the time set up your PC or portable device, click the **SET LOCAL TIME** button.
3. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

To enable automatic synchronization with a time server, follow the next steps:

1. Move the **Enable NTP** switch to the right.
2. Specify the needed NTP server or leave the value specified by default in the **NTP Servers** section. If you need to specify several servers, click the **ADD SERVER** button.
3. Select your time zone from the **Timezone** drop-down list in the **NTP Settings** section. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.
4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically.

To enable automatic adjustment for daylight saving time of the gateway, move the **Daylight saving time** switch to the right in the **NTP Settings** section and click the **APPLY** button.

In some cases NTP servers addresses are provided by your ISP. In this case, you need to move the **Get NTP server addresses using DHCP** switch in the **NTP Settings** section to the right and click the **APPLY** button. Contact your ISP to clarify if this setting needs to be enabled. If the **Get NTP server addresses using DHCP** switch is moved to the right, the **NTP Servers** section is not displayed.



When the gateway 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).

Yandex.DNS

This menu is designed to configure the Yandex.DNS service.

Yandex.DNS is a web content filtering service which provides the DNS server, protects a computer against malicious web sites, and blocks access to adult web sites.

Settings

On the **Yandex.DNS / Settings** page, you can enable the Yandex.DNS service and configure its operating mode.

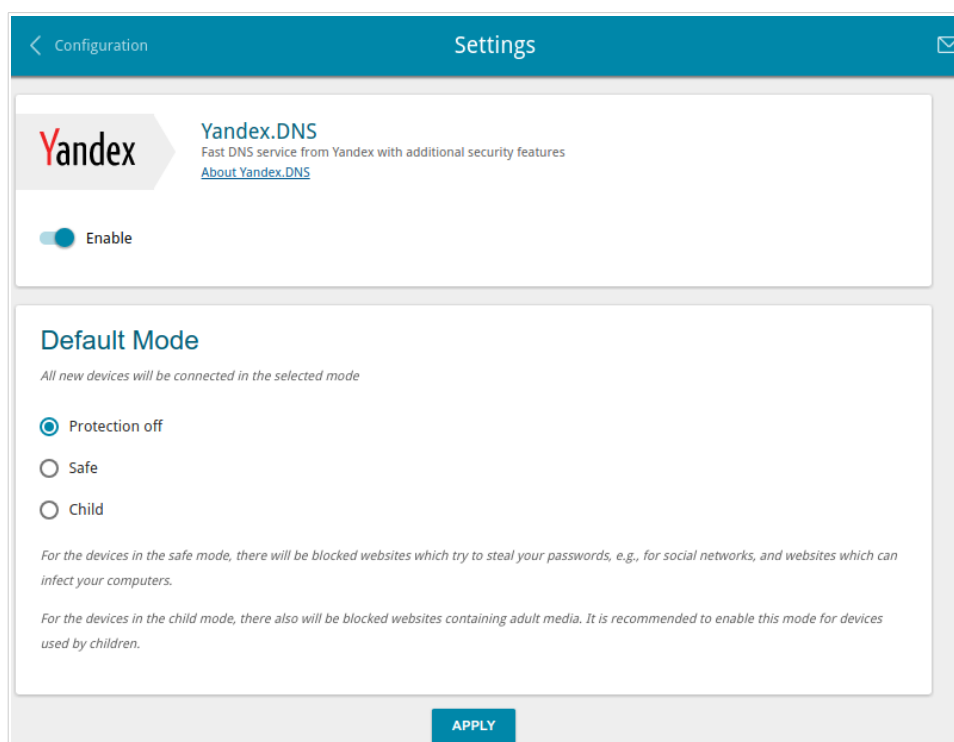


Figure 100. The **Yandex.DNS / Settings** page.

To get detailed information on the service, click the **About Yandex.DNS** link.

To enable the Yandex.DNS service, move the **Enable** switch to the right.

When the service is enabled, the **Default Mode** section is displayed on the page. Select the needed choice of the radio button to configure filtering for all devices of the gateway's network:

- **Protection off**: when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites;
- **Safe**: when this value is selected, the service blocks access to malicious and fraudulent web sites;
- **Child**: when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

Also the selected filtering mode will be applied to all devices newly connected to the gateway's network.

After specifying all needed parameters, click the **APPLY** button.

To disable the Yandex.DNS service, move the **Enable** switch to the left and click the **APPLY** button.

Devices and Rules

On the **Yandex.DNS / Devices and Rules** page, you can specify a filtering mode for each device separately.

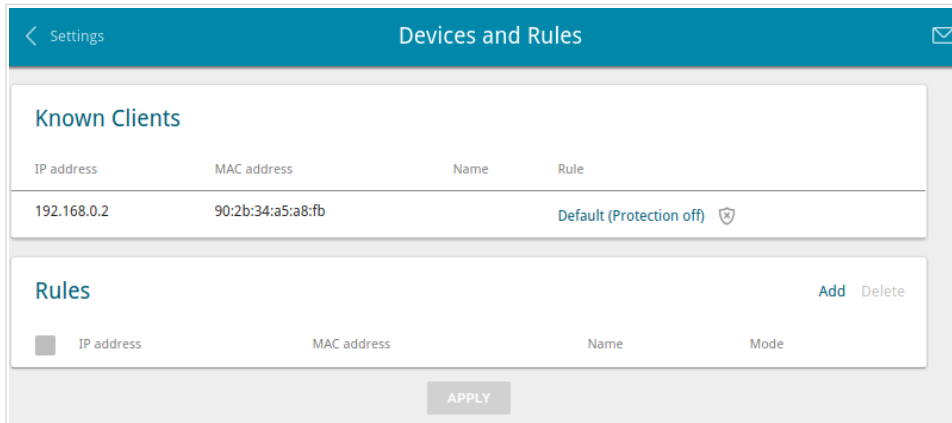


Figure 101. The **Yandex.DNS / Devices and Rules** page.

In the **Known Clients** section, the devices connected to the local network of the gateway at the moment and their relevant filtering mode are displayed.

To create⁴ a new filtering rule for a device, click the **Add** button in the **Rules** section, or left-click the name of the filtering mode in the line of the device for which a rule should be created in the **Known Clients** section.

Figure 102. Adding a new rule for the **Yandex.DNS** service.

⁴ When a new rule for filtering is created, a MAC address and IP address pair is displayed on the **Connections Setup / LAN** page. The created pair will be deleted with the relevant rule.

In the opened window, you can specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the gateway's LAN.
IP address	The IP address of a device from the gateway's LAN.
Name	Enter a name for the rule for easier identification. <i>Optional.</i>
Mode	Select an operating mode of the Yandex.DNS service for this rule. Protection off: when this value is selected, the service provides the DNS server with no restrictions on access to unsafe web sites. Safe: when this value is selected, the service blocks access to malicious and fraudulent web sites. Child: when this value is selected, the service blocks access to malicious and fraudulent web sites and blocks access to adult content.

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

To edit a rule for filtering, select a relevant line of the table, in the opened window, change the needed values and click the **SAVE** button.

To remove a rule for filtering, select the checkbox located to the left of the relevant rule and click the **Delete** button. Also you can remove a rule in the editing window.

After completing the work with rules, click the **APPLY** button.

CHAPTER 5. OPERATION GUIDELINES

Safety Rules and Conditions

Please carefully read this section before installation and connection of the device. Make sure that the power adapter and cables are not damaged. The device should be used only as intended in accordance with the documents.

The device is intended for use in dry, clean, dust-free, and well ventilated areas with normal humidity away from strong heat sources. Do not use the device outdoors or in the areas with high humidity. Do not place foreign objects on the device. Do not obstruct the ventilation openings of the device. The environmental temperature near the device and the temperature inside the device's cover should be within the range from 0 °C to +40 °C.

Only use the power adapter supplied with the device. Do not plug in the adapter, if its case or cable are damaged. Plug the adapter only into working electrical outlets with parameters indicated on the adapter.

Do not open the cover of the device! Unplug the device before dusting and cleaning. Use a damp cloth to clean the device. Do not use liquid/aerosol cleaners or magnetic/static cleaning devices. Prevent moisture getting into the device or the power adapter.

The service life of the device is 2 years.

Abbreviations and Acronyms

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GMT	Greenwich Mean Time
IGD	Internet Gateway Device
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
PPPoE	Point-to-point protocol over Ethernet
PPTP	Point-to-point tunneling protocol
QoS	Quality of Service
RIP	Routing Information Protocol
RTSP	Real Time Streaming Protocol
SIP	Session Initiation Protocol
UDP	User Datagram Protocol

UPnP	Universal Plug and Play
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network