

User Manual



DIR-X1530

AX1500 Wi-Fi 6 Gigabit Router

Contents

Chapter 1. Introduction	5
Contents and Audience	5
Conventions	5
Document Structure	5
Chapter 2. Overview	6
- General Information	6
Specifications	8
Product Appearance	
Upper Panel	13
Back Panel	15
Delivery Package	
Chapter 3. Installation and Connection	
Before You Begin	
Connecting to PC	
PC with Ethernet Adapter	
Obtaining IP Address Automatically (OS Windows 7)	
Obtaining IP Address Automatically (OS Windows 10)	
PC with Wi-Fi Adapter	
Obtaining IP Address Automatically and	
to Wireless Network (OS Windows 7)	
Obtaining IP Address Automatically and	Connecting
to Wireless Network (OS Windows 10)	
Connecting to Web-based Interface	
Web-based Interface Structure	
Summary Page	
Home Page	
Menu Sections	
Notifications	
Chapter 4. Configuring via Web-based Interface	43
Initial Configuration Wizard	
Selecting Operation Mode	
Router	
Access Point or Repeater	
Changing LAN IPv4 Address	
Wi-Fi Client	
Configuring WAN Connection	
Static IPv4 Connection	
Static IPv6 Connection	
PPPOE, IPv6 PPPoE, PPPoE Dual	Stack,
PPPoE + Dynamic IP (PPPoE Dual Access) Connections	
PPPoE + Static IP (PPPoE Dual Access) Connection	
PPTP + Dynamic IP or L2TP + Dynamic IP Connection	
PPTP + Static IP or L2TP + Static IP Connection	
Configuring Wireless Network	
Configuring LAN Ports for IPTV/VoIP	
Changing Web-based Interface Password	
Connection of Multimedia Devices	64

Statistics
Network Statistics67
DHCP
Routing
Clients and Sessions71
Port Statistics72
Multicast Groups73
IPsec Statistics74
VPN Statistics75
Connections Setup
WAN
Creating Dynamic IPv4 or Static IPv4 WAN Connection
Creating Dynamic IPv6 or Static IPv6 WAN Connection
Creating PPPoE WAN Connection84
Creating PPTP, L2TP, or L2TP over IPsec WAN Connection
Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection
Creating IPIP6 WAN Connection100
Creating 6in4 WAN Connection103
Creating 6to4 WAN Connection105
Creating 6rd WAN Connection106
LAN
IPv4108
IPv6114
WAN Failover
VPN
IPsec
GRE130
IPIP132
PPTP/L2TP Servers134
VPN Users
EoGRE140
EoIP142
Wi-Fi145
Basic Settings145
Client Management156
WPS157
Using WPS Function via Web-based Interface
Using WPS Function without Web-based Interface
Client161
Additional164
MAC Filter168

Advanced
VLAN172
WAN Remapping
DNS176
DDNS
Ports Settings
Redirect
Routing
TR-069 Client
Port Mirroring
UPnP IGD
UDPXY
IGMP194
ALG/Passthrough
CoovaChilli
Firewall
IP Filter
Virtual Servers
DMZ
MAC Filter
URL Filter
AdBlock
Remote Access
System
Configuration
Firmware Update
Local Update
Remote Update
Schedule
Log
Ping
Traceroute
Telnet/SSH238
System Time
Auto Provision
SkyDNS
Settings
Devices and Rules
Chapter 5. Operation Guidelines
Safety Rules and Conditions249
Wireless Installation Considerations250
Chapter 6. Abbreviations and Acronyms

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DIR-X1530 and explains how to configure and operate it.

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

Conventions

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

Document Structure

Chapter 1 describes the purpose and structure of the document.

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

Chapter 3 explains how to install the router DIR-X1530 and configure a PC in order to access its web-based interface.

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

Chapter 5 includes safety instructions and tips for networking.

Chapter 6 introduces abbreviations and acronyms most commonly used in User Manuals for D-Link customer premises equipment.

CHAPTER 2. OVERVIEW

General Information

The DIR-X1530 device is a wireless dual band gigabit router with a built-in 3-port switch. It provides a fast and simple way to create a wireless and wired network at home or in an office.

You are able to connect the wireless router DIR-X1530 to a cable or DSL modem or to a private Ethernet line and use a high-speed Internet connection to successfully fulfill a wide range of professional tasks. The built-in 3-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network. Any Ethernet port of the device can be used to connect to a private Ethernet line.

Support of Wi-Fi 6 (802.11ax) standard provides faster speeds, greater capacity, and less network congestion for high-performance device-dense environments. It ensures connection of more devices and prevents weakening wireless connectivity by wall obstruction and interference from other appliances.

Using the DIR-X1530 device, you are able to quickly create a high-speed wireless network at home or in your office, which lets computers and mobile devices access the Internet virtually anywhere (within the operational range of your wireless network). Simultaneous activity of 2.4GHz band and 5GHz band allows performing a wide range of tasks. The router can operate as a base station for connecting wireless devices of the standards 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (at the wireless connection rate up to 1500Mbps¹).

The router supports multiple functions for the wireless interface: several security standards (WEP, WPA/WPA2/WPA3), MAC address filtering, WPS, WMM.

In addition, the device is equipped with a button for switching the Wi-Fi network off/on. If needed, for example, when you leave home, you can easily switch the router's WLAN by pressing the button, and devices connected to the LAN ports of the router will stay online.

Multi-user MIMO technology allows to distribute the router's resources to let multiple wireless clients use the Wi-Fi network efficiently, keeping high rates for HD media streaming, lag-free gaming, and fast transfer of large files.

Transmit Beamforming technology allows to flexibly change the antennas' radiation pattern and to redistribute the signal directly to wireless devices connected to the router.

Support of guest Wi-Fi network allows you to create a separate wireless network with individual security settings and maximum rate limitation. Devices connected to the guest network will be able to access the Internet, but will be isolated from the devices and resources of the router's LAN.

The wireless router DIR-X1530 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.

The SSH protocol support provides more secure remote configuration and management of the router due to encryption of all transmitted traffic, including passwords.

¹ Up to 300Mbps for 2.4GHz and up to 1201Mbps for 5GHz.

In addition, the router supports IPsec and allows to create secure VPN tunnels. Support of the IKEv2 protocol allows to provide simplified message exchange and use asymmetric authentication engine upon configuration of an IPsec tunnel.

The router also supports the SkyDNS web content filtering service, which provides more settings and opportunities for safer Internet experience for home users of all ages and for professional activities of corporate users.

Now the schedules are also implemented; they can be applied to the rules and settings of the firewall and used to reboot the router at the specified time or every specified time period and to enable/disable the wireless network and the Wi-Fi filter.

The new ad blocking function effectively blocks advertisements which appear during web surfing.

You can configure the settings of the wireless router DIR-X1530 via the user-friendly web-based interface (the interface is available in two languages – in Russian and in English).

The configuration wizard allows you to quickly switch DIR-X1530 to one of the following modes: router (for connection to a wired or wireless ISP), access point, repeater, or client, and then configure all needed setting for operation in the selected mode in several simple steps.

Also DIR-X1530 supports configuration and management via mobile application for Android and iPhone smartphones.

You can simply update the firmware: the router itself finds approved firmware on D-Link update server and notifies when ready to install it.

Specifications*

Hardware	
Processor	· RTL8198D (900MHz)
RAM	· 256MB, DDR3, built in processor
Flash	· 128MB, SPI NAND
Interfaces	 10/100/1000BASE-T WAN port 3 10/100/1000BASE-T LAN ports
LEDS	 Power Internet WLAN 2.4G WLAN 5G
Buttons	 WPS button to set up wireless connection and enable/disable wireless network RESET button to restore factory default settings
Antenna	· Four external non-detachable antennas (5dBi gain)
МІМО	· 2 x 2, MU-MIMO
Power connector	Power input connector (DC)

Software		
WAN connection types	· PPPoE	
	· IPv6 PPPoE	
	· PPPoE Dual Stack	
	Static IPv4 / Dynamic IPv4	
	Static IPv6 / Dynamic IPv6	
	· PPPoE + Static IP (PPPoE Dual Access)	
	· PPPoE + Dynamic IP (PPPoE Dual Access)	
	· PPTP/L2TP + Static IP	
	· PPTP/L2TP + Dynamic IP	
	· IPIP6 in DSLite mode	
	· 6in4	
	· 6to4	
	· 6rd	

^{*} The device features are subject to change without notice. For the latest versions of the firmware and relevant documentation, visit <u>www.dlink.ru</u>.

User Manual

Software	
Network functions	 DHCP server/relay Advanced configuration of built-in DHCP server Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation Automatic obtainment of LAN IP address (for access point/repeater/client modes) DNS relay Dynamic DNS Static IPv4/IPv6 routing IGMP Proxy RIP Support of UPnP Support of VLAN WAN ping respond Support of SIP ALG Support of RTSP WAN failover LAN/WAN conversion Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port Built-in UDPXY application Port mirroring
Firewall functions	 Network Address Translation (NAT) Stateful Packet Inspection (SPI) IPv4/IPv6 filter MAC filter URL filter URL filter Ad blocking function DMZ Virtual servers Built-in SkyDNS web content filtering service
VPN	 IPsec/PPTP/L2TP/PPPoE pass-through PPTP/L2TP servers PPTP/L2TP tunnels L2TP over IPsec GRE/EoGRE/EoIP/IPIP tunnels IPsec tunnels Transport/Tunnel mode IKEv1/IKEv2 support DES encryption NAT Traversal Support of DPD (Keep-alive for VPN tunnels)
Management and monitoring	 Local and remote access to settings through SSH/TELNET/WEB (HTTP/HTTPS) Bilingual web-based interface for configuration and management (Russian/English) Support of D-Link Assistant application for Android and iPhone smartphones 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 logging to remote host Automatic synchronization of system time with NTP server and manual time/date setup Ping utility Traceroute utility TR-069 client Schedules for rules and settings of firewall, automatic reboot, and enabling/disabling wireless network and Wi-Fi filter Automatic upload of configuration file from ISP's server (Auto Provision)

Wireless Module Parameters

Wireless Module Parameters	
Standards Frequency range The frequency range depends upon the radio frequency regulations applied in your country	 IEEE 802.11ax IEEE 802.11ac Wave 2 IEEE 802.11a/b/g/n IEEE 802.11w 2400 ~ 2483.5MHz 5150 ~ 5350MHz 5650 ~ 5850MHz
Wireless connection security	 WEP WPA/WPA2 (Personal/Enterprise) WPA3 (Personal) MAC filter WPS (PBC/PIN)
Advanced functions	 Support of client mode WMM (Wi-Fi QoS) Information on connected Wi-Fi clients Advanced settings Guest Wi-Fi / support of MBSSID Limitation of wireless network rate Periodic scan of channels, automatic switch to least loaded channel Support of 5GHz TX Beamforming Autonegotiation of channel bandwidth in accordance with environment conditions (20/40 Coexistence) CoovaChilli authentication portal Support of TWT technology
Wireless connection rate	 IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54Mbps IEEE 802.11b: 1, 2, 5.5, and 11Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54Mbps IEEE 802.11n (2.4GHz/5GHz): from 6.5 to 300Mbps (MCS0–MCS15) IEEE 802.11ac (5GHz): from 6.5 to 867Mbps IEEE 802.11ax (5GHz): from 6.5 to 1201Mbps

Wireless Module Parameters		
Transmitter output power	 802.11a (typical at room temperature 25 °C) 15dBm at 6, 9, 12, 18, 24, 36, 48, 54Mbps 	
The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country	 802.11b (typical at room temperature 25 °C) 15dBm at 1, 2, 5.5, 11Mbps 	
	 802.11g (typical at room temperature 25 °C) 15dBm at 6, 9, 12, 18, 24, 36, 48, 54Mbps 	
	 802.11n (typical at room temperature 25 °C) 2.4GHz, HT20 15dBm at MCS0/8~7/15 2.4GHz, HT40 15dBm at MCS0/8~7/15 5GHz, HT20 15dBm at MCS0/8~7/15 5GHz, HT40 	
	15dBm at MCS0/8~7/15	
	 802.11ac (typical at room temperature 25 °C) VHT20 15dBm at MCS0~8 VHT40 15dBm at MCS0~9 VHT80 15dBm at MCS0~9 	
	 802.11ax (typical at room temperature 25 °C) 15dBm at MCS10 15dBm at MCS11 	
Receiver sensitivity	 802.11a (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -94dBm at 6Mbps -76dBm at 54Mbps 	
	 802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C) -96dBm at 1Mbps -89dBm at 11Mbps 	
	 802.11g (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -92dBm at 6Mbps -72dBm at 54Mbps 	
	 802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) 2.4GHz, HT20 -91dBm at MCS0/8 -72dBm at MCS7/15 2.4GHz, HT40 -90dBm at MCS0/8 -71dBm at MCS7/15 5GHz, HT20 -93dBm at MCS0/8 -74dBm at MCS7/15 5GHz, HT40 -90dBm at MCS0/8 -74dBm at MCS7/15 5GHz, HT40 -90dBm at MCS0/8 -74dBm at MCS7/15 5GHz, HT40 -90dBm at MCS0/8 	

Г

Wireless Module Parameters	
	 802.11ac (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) VHT20 93dBm at MCS0 68dBm at MCS8 VHT40 90dBm at MCS0 63dBm at MCS9 VHT80 87dBm at MCS0 60dBm at MCS9 802.11ax (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) HE20 90dBm at MCS0 65dBm at MCS0 65dBm at MCS11 HE40 87dBm at MCS0 62dBm at MCS11 HE80 84dBm at MCS0 59dBm at MCS1

Physical Parameters	
Dimensions (L x W x H)	· 194 x 139 x 55 mm (7.64 x 5.47 x 2.17 in)
Weight	· 300 g (0.66 lb)

Operating Environment	
Power	· Output: 12V DC, 1A
Temperature	 Operating: from 0 to 40 °C Storage: from -20 to 65 °C
Humidity	 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			
	Solid orange	The router is being loaded.			
	Solid white	The router is powered on.			
Power	Blinking (white and orange alternately)	The firmware is being updated.			
	No light	The router is powered off.			

LED	Mode	Description			
	Solid white	The default WAN connection is on.			
Internet	Solid orange	The default WAN connection is off, orthere are no WAN connections created.			
	No light	The WAN cable is not connected.			
	Solid white	The router's WLAN of the relevant band is on.			
WLAN 2.4G WLAN 5G	Blinking white	Attempting to add a wireless device via the WPS function.			
No light		The router's WLAN of the relevant band is off.			

In case the **Power** and **Internet** LEDs are blinking white and orange alternately, the device is in the emergency mode. Power the device off and on. If the device is loaded in the emergency mode again, restore the factory default settings via the hardware **RESET** button.

Back Panel



Figure 2. Back panel view.

Port	Description		
LAN 1-3	3 Ethernet ports to connect computers or network devices.		
INTERNET	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).		
WPS	A button to set up a wireless connection (the WPS function) and enable/disable the wireless network.To use the WPS function: with the device turned on, press the button, hold it for 2 seconds, and release. The WLAN 2.4G and WLAN 5G LEDs should start blinking.		
	To disable the router's wireless network: with the device turned on, press the button, hold for 10 seconds, and release. The WLAN 2.4G and WLAN 5G LEDs should turn off.		

Port	Description
RESET	A button to restore the factory defaults. To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.
DC IN 12V=1A	Power connector.

The device is also equipped with four external non-detachable Wi-Fi antennas.

Delivery Package

The following should be included:

- Router DIR-X1530
- Power adapter DC 12V/1A
- Ethernet cable
- "Quick Installation Guide" (brochure).

The "*User Manual*" and "*Quick Installation Guide*" documents are available on D-Link website (see <u>www.dlink.ru</u>).

<u>Using a power supply with a different voltage rating than the one included will cause</u> <u>damage and void the warranty for this product.</u>

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.

Computer or Mobile Device

Configuration of the wireless dual band gigabit router with a built-in 3-port switch DIR-X1530 (hereinafter referred to as "the router") is performed via the built-in web-based interface. The web-based interface is available from any operating system that supports a web browser.

Also you can use D-Link Assistant application for Android or iPhone mobile devices (smartphones or tablets).

PC 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 or Wireless NIC (Ethernet or Wi-Fi Adapter)

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

Wireless Connection

Wireless workstations from your network should be equipped with a wireless 802.11a, b, g, n, ac, or ax NIC (Wi-Fi adapter). In addition, you should specify the values of SSID, channel number and security settings defined in the web-based interface of the router for all these wireless workstations.

Connecting to PC

PC with Ethernet Adapter

- 1. Connect an Ethernet cable between any of LAN ports located on the back panel of the router and the Ethernet port of your PC.
- 2. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.

Then make sure that your PC is configured to obtain an IP address automatically (as DHCP client).

Obtaining IP Address Automatically (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.)

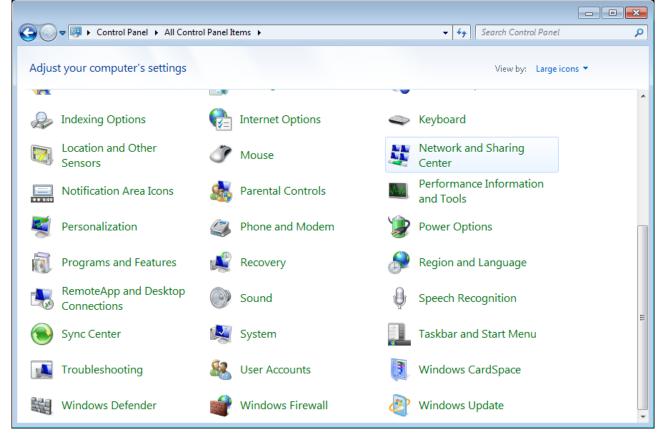


Figure 3. The Control Panel window.

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

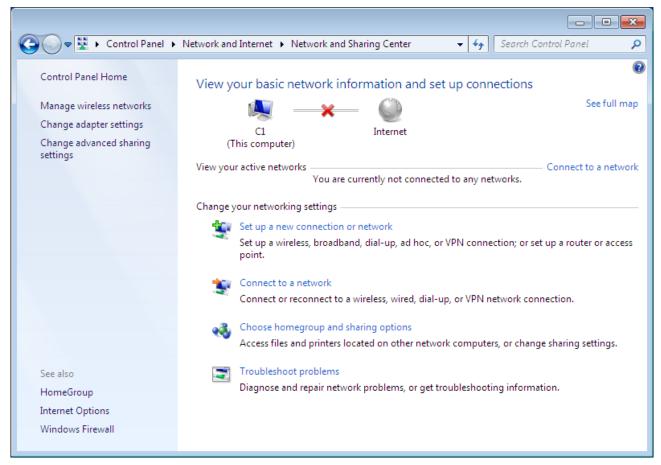


Figure 4. The Network and Sharing Center window.

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

	Control Panel > Network an	d Internet 🔸 Network Connec	tions 🕨	✓ 4 Search Network Co		
Organize 🔻	Disable this network device	Diagnose this connection	Rename this connection	»	== ₩= ▼	(?
LA	AN					
	Disable					
~~	Status					
	Diagnose					
(Bridge Connections					
	Create Shortcut					
0	Delete					
6	Rename					
	Properties					
	-					

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.

🖳 LAN Properties
Networking
Connect using:
2
<u>C</u> onfigure
This connection uses the following items:
 QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Internet Protocol Version 9 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder
Install
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK Cancel

Figure 6. The Local Area Connection Properties window.

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server** address automatically choices of the radio buttons are selected. Click the **OK** button.

Internet Protocol Version 4 (TCP/IPv4)	Properties	? 🔀		
General Alternate Configuration				
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.				
Obtain an IP address automatical	V			
OUse the following IP address:				
IP address:				
S <u>u</u> bnet mask:				
Default gateway:	· · · ·			
Obtain DNS server address auton	natically			
OUSe the following DNS server add	resses:			
Preferred DNS server:				
<u>A</u> lternate DNS server:				
Validate settings upon exit	Ady	anced		
	ОК	Cancel		

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

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

Obtaining IP Address Automatically (OS Windows 10)

- 1. Click the **Start** button and proceed to the **Settings** window.
- 2. Select the Network & Internet section.

Settings				_	\times
	Windows	Settir	igs		
	Find a setting		٩		
	System Display, sound, notifications, power		Devices Bluetooth, printers, mouse		
	Phone Link your Android, iPhone		Network & Internet Wi-Fi, airplane mode, VPN		
<u>ل</u>	Personalization Background, lock screen, colors		Apps Uninstall, defaults, optional features		
8	Accounts Your accounts, email, sync, work, family	色 A字	Time & Language Speech, region, date		

Figure 8. The Windows Settings window.

3. In the **Change your network settings** section, select the **Change adapter options** line.

← Settings	- 🗆 X
යි Home	Status
Find a setting P You're connected to the Internet If you have a limited data plan, you can make this network & Internet Network & Internet	
	Change connection properties
⊕ Status	Show available networks
🕼 Wi-Fi	
史 Ethernet	Change your network settings
ଳ Dial-up	Change adapter options View network adapters and change connection settings.
∞ VPN	Sharing options For the networks you connect to, decide what you want to share.
r∯ Airplane mode	
^(ပု) Mobile hotspot	Metwork troubleshooter Diagnose and fix network problems.
🕒 Data usage	View your network properties
	Windows Firewall
Proxy	Network and Sharing Center

Figure 9. The Network & Internet window.

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

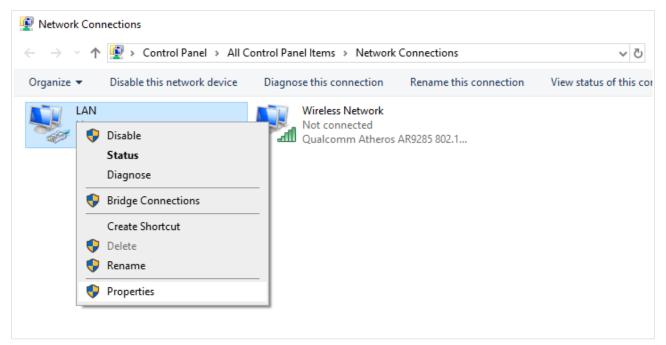


Figure 10. The Network Connections window.

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.

Ethernet Properties	×
Networking Sharing	
Connect using:	
Realtek PCIe FE Family Controller	
<u>C</u> onfigure	
This connection uses the following items:	_
Client for Microsoft Networks	^
File and Printer Sharing for Microsoft Networks	
QoS Packet Scheduler	
Internet Protocol Version 4 (TCP/IPv4)	
Image: Microsoft Network Adapter Multiplexor Protocol Image: Microsoft LLDP Protocol Driver	
Internet Protocol Version 6 (TCP/IPv6)	
< >	Ť
Install Uninstall Properties	
Description	
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
OK Can	cel

Figure 11. The local area connection properties window.

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.

Internet Protocol Version 4 (TCP/IPv4) Properties				×			
General	Alternate Configuration						
this cap	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
() Ob	otain an IP address automatica	lly					
OUs	e the following IP address:						
IP ac	ldress:]	
Subn	et mask:]	
Defa	ult gateway:				1.0]	
() Ot	otain DNS server address auto	matically	y				
OUs	e the following DNS server ad	dresses	-				
Prefe	erred DNS server:]	
Alter	nate DNS server:]	
V	alidate settings upon exit				Advan	ced	
				OK		Cancel	

Figure 12. The Internet Protocol Version 4 (TCP/IPv4) Properties window.

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

PC with Wi-Fi Adapter

- 1. Connect the power cord to the power connector port on the back panel of the router, then plug the power adapter into an electrical outlet or power strip.
- 2. Make sure that your Wi-Fi adapter is on. As a rule, modern notebooks with built-in wireless NICs are equipped with a button or switch that turns on/off the wireless adapter (refer to your PC documents). If your PC is equipped with a pluggable wireless NIC, install the software provided with your Wi-Fi adapter.

Then make sure that your Wi-Fi adapter is configured to obtain an IP address automatically (as DHCP client).

Obtaining IP Address Automatically and Connecting to Wireless Network (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.)

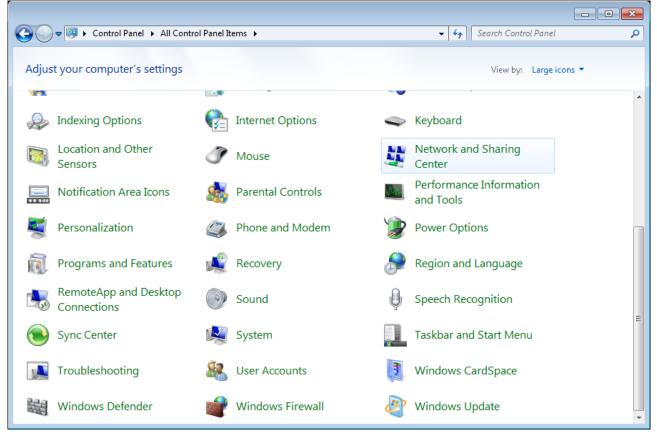


Figure 13. The **Control Panel** window.

- 3. In the menu located on the left part of the window, select the **Change adapter settings** line.
- 4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.
- 5. In the Wireless Network Connection Properties window, on the Networking tab, select the Internet Protocol Version 4 (TCP/IPv4) line. Click the Properties button.

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server** address automatically choices of the radio buttons are selected. Click the **OK** button.

Internet Protocol Version 4 (TCP/IPv4	4) Properties
General Alternate Configuration	
You can get IP settings assigned autory this capability. Otherwise, you need for the appropriate IP settings.	
Obtain an IP address automatic	ally
OUse the following IP address: —	
IP address:	· · · · ·
S <u>u</u> bnet mask:	· · · · · · · · · · · ·
Default gateway:	
Obtain DNS server address auto	omatically
OUSE the following DNS server ac	ldresses:
Preferred DNS server:	
<u>A</u> lternate DNS server:	
Validate settings upon exit	Ad <u>v</u> anced
	OK Cancel

Figure 14. The Internet Protocol Version 4 (TCP/IPv4) Properties window.

- 7. Click the **OK** button in the connection properties window.
- 8. To open the list of available wireless networks, select the icon of the wireless network connection and click the **Connect To** button or left-click the network icon in the notification area located on the right side of the taskbar.



Figure 15. The notification area of the taskbar.

 In the opened Wireless Network Connection window, select the wireless network DIRx1530 (for operating in the 2.4GHz band) or DIR-x1530-5G (for operating in the 5GHz band) and click the Connect button.

Not connected	÷2			
Connections are available				
Wi-Fi	^			
wireless router	lite.			
Connect automatically	<u>C</u> onnect			
Open Network and Sharing Center				

Figure 16. The list of available networks.

- 10. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **OK** button.
- 11. Wait for about 20-30 seconds. After the connection is established, the network icon will be displayed as the signal level scale.

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

Obtaining IP Address Automatically and Connecting to Wireless Network (OS Windows 10)

- 1. Click the **Start** button and proceed to the **Settings** window.
- 2. Select the Network & Internet section.

Settings				_	×
Windows Settings					
	Find a setting		9		
므	System Display, sound, notifications, power		Devices Bluetooth, printers, mouse		
	Phone Link your Android, iPhone		Network & Internet Wi-Fi, airplane mode, VPN		
<u>I</u>	Personalization Background, lock screen, colors		Apps Uninstall, defaults, optional features		
8	Accounts Your accounts, email, sync, work, family	A≠	Time & Language Speech, region, date		

Figure 17. The Windows Settings window.

- 3. In the **Change your network settings** section, select the **Change adapter options** line.
- 4. In the opened window, right-click the relevant **Wireless Network Connection** icon. Make sure that your Wi-Fi adapter is on, then select the **Properties** line in the menu displayed.
- 5. In the Wireless Network Connection Properties window, on the Networking tab, select the Internet Protocol Version 4 (TCP/IPv4) line. Click the Properties button.

6. Make sure that the **Obtain an IP address automatically** and **Obtain DNS server address automatically** choices of the radio buttons are selected. Click the **OK** button.

Internet Protocol Version 4 (TCP/IPv4) Properties X						
General Alternate Configuration						
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
Obtain an IP address automatically						
O Use the following IP address:						
IP address:						
Subnet mask:						
Default gateway:						
Obtain DNS server address automatically						
O Use the following DNS server addresses:						
Preferred DNS server:						
Alternate DNS server:						
Validate settings upon exit	Advanced					
	OK Cancel					

Figure 18. The Internet Protocol Version 4 (TCP/IPv4) Properties window.

- 7. Click the **Close** button in the connection properties window.
- 8. To open the list of available wireless networks, select the icon of the wireless network connection and click the **Connect To** button or left-click the network icon in the notification area located on the right side of the taskbar.



Figure 19. The notification area of the taskbar.

 In the opened Wireless Network Connection window, select the wireless network DIRx1530 (for operating in the 2.4GHz band) or DIR-x1530-5G (for operating in the 5GHz band) and click the Connect button.

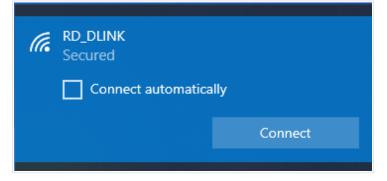


Figure 20. The list of available networks.

- 10. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **Next** button.
- 11. Allow or forbid your PC to be discoverable by other devices on this network (Yes / No).

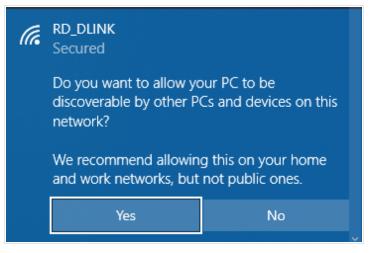


Figure 21. PC discovery settings.

12. Wait for about 20-30 seconds. After the connection is established, the network icon will be displayed as a dot with curved lines indicating the signal level.

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

Connecting to Web-based Interface

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

For security reasons, DIR-X1530 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 18). In the address bar of the web browser, enter the domain name of the router (by default, **dlinkrouter.local**) with a dot at the end and press the **Enter** key. Also you can enter the IP address of the device (by default, **192.168.0.1**).



Figure 22. Connecting to the web-based interface of the DIR-X1530 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 router, make sure that you have properly connected the router 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 Wizard opens (see the *Initial Configuration Wizard* section, page 43).

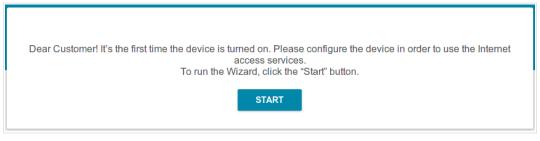


Figure 23. The page for running the Initial Configuration Wizard.

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.

Authori	zation	
Username*		
Password*		
••		Ø
Sta	ay signed in	
Forgot pass	sword?	
	Authorization error	
	Attempts remaining: 4	
LOGIN	CLEAR	

Figure 24. The login page.

In order not to log out, move the **Stay signed in** switch to the right. After closing the web browser or rebooting the device, you need to enter the username and the password again.

If you enter a wrong password several times, the web-based interface will be blocked for a while. Please wait for one minute and reenter the password you specified.

Web-based Interface Structure

Summary Page

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

🗧 🗸 Home	Sum	imary	
Device Information	on	Wi-Fi 5 GHz	
Model:	DIR-X1530	Status:	On
Hardware version:	A1	Broadcasting:	On
Firmware version:	4.0.1	Additional networks:	
Build time:	Thu May 5 2022 3:30:19 PM MSK	Network name (SSID):	DIR-X1530-5G-C93
JI version:	1.33.0.c088670-embedded	Security:	WPA2-PSK
/endor:	D-Link Russia		
Serial number:	DIR000000001		
Support:	support@dlink.ru	WAN IPv4	
Summary:	Root filesystem image for DIR_X1530_RT8198D	Connection type:	Dynamic IP
Jptime:	5 h. 34 min.	Status:	Connected
Device mode:	Router	MAC address	10:62:EB:2D:C9:3
		IP address:	192.168.161.2
Wi-Fi 2.4 GHz			
	On	LAN	
Status:	On • On •	LAN LAN IPv4:	192.168.0
Status: Broadcasting:			192.168.0
Status: Broadcasting: Additional networks:	On •	LAN IPv4:	192.168.0
Status: Broadcasting: Additional networks: Network name (SSID):	On •	LAN IPv4: Wireless connections:	192.168.0
Status: Broadcasting: Additional networks: Network name (SSID):	On • 0 DIR-X1530-C938	LAN IPv4: Wireless connections:	192.168.0
Status: Broadcasting: Additional networks: Network name (SSID):	On • 0 DIR-X1530-C938	LAN IPv4: Wireless connections: Wired connections:	192.168.0
Wi-Fi 2.4 GHz Status: Broadcasting: Additional networks: Network name (SSID): Security:	On • 0 DIR-X1530-C938	LAN IPv4: Wireless connections: Wired connections: LAN Ports	

Figure 25. The summary page.

The **Device Information** section displays the model and hardware version of the router, 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.

To change the operation mode of the device, left-click the name of the mode in the **Device mode** line. In the opened window, click the **Initial Configuration Wizard** link (for the detailed description of the Wizard, see the *Initial Configuration Wizard* section, page 43).

The **Wi-Fi 2.4 GHz** and **Wi-Fi 5 GHz** sections display data on the state of the device's wireless network, its name and the authentication type, and availability of an additional wireless network in the relevant band.

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 router, the LAN MAC address, and the number of wired and wireless clients of the device are displayed.

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

Home Page

The Home page displays links to the most frequently used pages with device's settings.

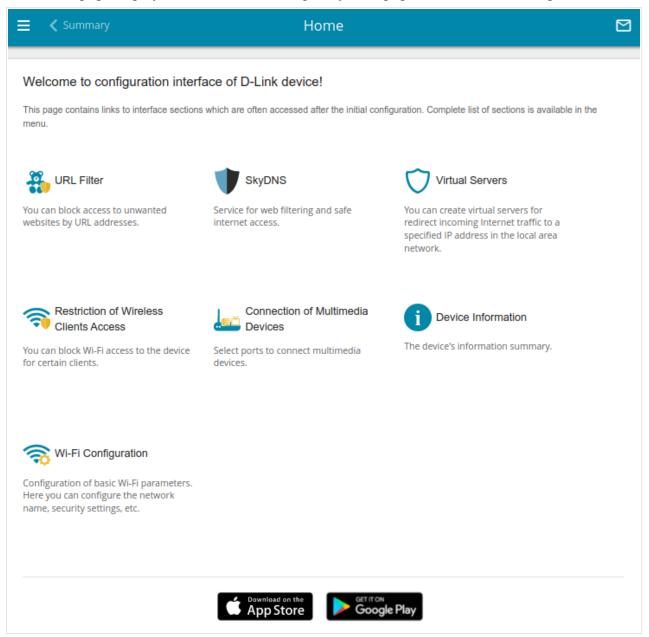


Figure 26. The Home page.

Other settings of the router are available in the menu in the left part of the page.

Menu Sections

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

In the **Initial Configuration** section you can run the Initial Configuration Wizard. The Wizard allows you to configure the router for operation in the needed mode and specify all parameters necessary for getting started (for the description of the Wizard, see the *Initial Configuration Wizard* section, page 43).

The pages of the **Statistics** section display data on the current state of the router (for the description of the pages, see the *Statistics* section, page 67).

The pages of the **Connections Setup** section are designed for configuring basic parameters of the LAN interface of the router and creating a connection to the Internet (for the description of the pages, see the *Connections Setup* section, page 76).

The pages of the **VPN** section are designed for configuring VPN connections based on IPsec/GRE/ EoGRE/EoIP/IPIP protocols and creating a PPTP or L2TP server and accounts for access to it (for the description of the pages, see the *VPN* section, page 121).

The pages of the **Wi-Fi** section are designed for specifying all needed settings of the router's wireless network (for the description of the pages, see the *Wi-Fi* section, page 145).

The pages of the **Advanced** section are designed for configuring additional parameters of the router (for the description of the pages, see the *Advanced* section, page 171).

The pages of the **Firewall** section are designed for configuring the firewall of the router (for the description of the pages, see the *Firewall* section, page 201).

The pages of the **System** section provide functions for managing the internal system of the router (for the description of the pages, see the *System* section, page 221).

The pages of the **SkyDNS** section are designed for configuring the SkyDNS web content filtering service (for the description of the pages, see the *SkyDNS* section, page 244).

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

Notifications

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



Figure 27. The web-based interface notifications.

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

CHAPTER 4. CONFIGURING VIA WEB-BASED INTERFACE

Initial Configuration Wizard

To start the Initial Configuration Wizard, go to the **Initial Configuration** section. On the opened page, click the **OK** button and wait until the factory default settings are restored.

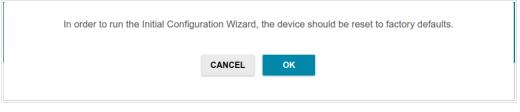


Figure 28. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network **DIR-X1530** (for operating in the 2.4GHz band) or **DIR-X1530-5G** (for operating in the 5GHz band) and click the **NEXT** button.



Figure 29. Checking connection to the wireless network.

Click the **START** button.

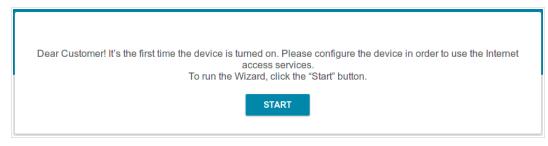


Figure 30. Starting the Wizard.

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.

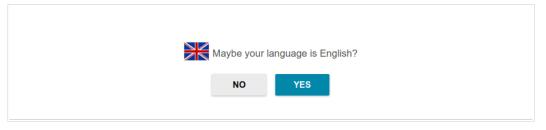


Figure 31. Selecting a language.

You can finish the wizard earlier and go to the menu of the web-based interface. To do this, click the **ADVANCED SETTINGS** button. On the opened page, change the default settings: specify the administrator password in the **User's interface password** and **Password confirmation** and the name of the wireless network in the 2.4GHz and 5GHz bands in the **Network name 2.4 GHz** (SSID) and **Network name 5 GHz** (SSID) fields correspondingly. Then click the **APPLY** button.

Defaults
In order to start up, please change several default settings.
User's interface password*
Password should be between 1 and 31 ASCII character
Password confirmation*
Network name 2.4 GHz (SSID)*
DIR-XXX-2A16
Network name 5 GHz (SSID)*
DIR-XXX-5G-2A16
< васк

Figure 32. Changing the default settings.

To continue the configuration of the router via the Wizard, click the **CONTINUE** button.

Selecting Operation Mode

Select the needed operation mode and click the **NEXT** button.

Router

In order to connect your device to a wired ISP, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Router** value. In this mode you can configure a WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, configure LAN ports to connect an STB or VoIP phone, and set your own password for access to the web-based interface of the device.

Device mode		
Connection method		
Wired connection	•	
Nork mode		ssip
Router	•	. D
	🗲 ВАСК	NEXT >

Figure 33. Selecting an operation mode. The **Router** mode.

In order to connect your device to a wireless ISP (WISP), on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **WISP Repeater** value. In this mode you can connect your device to another access point, configure a WAN connection, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

Device mode		
Connection method		_
Wi-Fi	•	
Work mode		SSID_Ext
WISP Repeater	•	
	🗸 ВАСК	NEXT >

Figure 34. Selecting an operation mode. The WISP Repeater mode.

Access Point or Repeater

In order to connect your device to a wired router for adding a wireless network to the existing local network, on the **Device mode** page, from the **Connection method** list, select the **Wired connection** value. Then from the **Work mode** list select the **Access point** value. In this mode you can change the LAN IP address, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

Connection method			
Wired connection	•		رريط
Work mode			SSID
Access point	•		2
	4 DACK	NEXT &	
	< BACK	NEXT >	

Figure 35. Selecting an operation mode. The Access point mode.

In order to connect your device to a wireless router for extending the range of the existing wireless network, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **Repeater** value. In this mode you can change the LAN IP address, connect your device to another access point, set your own settings for the wireless network in the 2.4GHz and 5GHz bands, and set your own password for access to the web-based interface of the device.

Device mode		
Connection method		
Wi-Fi	•	
		SSID_Ext
Work mode Repeater	-))) ssid (((
	< ВАСК	NEXT >

Figure 36. Selecting an operation mode. The Repeater mode.

In order to let wired PCs connected to your device access the network of a wireless router, on the **Device mode** page, from the **Connection method** list, select the **Wi-Fi** value. Then from the **Work mode** list select the **Client** value. In this mode you can change the LAN IP address, connect your device to another access point, and set your own password for access to the web-based interface of the device.

Connection method		
Wi-Fi	•	
Work mode		
Client	•	
	< ВАСК	NEXT >

Figure 37. Selecting an operation mode. The **Client** mode.

Changing LAN IPv4 Address

This configuration step is available for the Access point, Repeater, and Client modes.

- 1. Select the **Automatic obtainment of IPv4 address** to let DIR-X1530 automatically obtain the LAN IPv4 address.
- 2. In the **Hostname** field, you should specify a domain name of the router using which you can access the web-based interface after finishing the Wizard. Enter a new domain name of the router ending with **.local** or leave the value suggested by the router.
- In order to access the web-based interface using the domain name, in the address bar of the web browser, enter the name of the router with a dot at the end.

If you want to manually assign the LAN IPv4 address for DIR-X1530, do not select the **Automatic** obtainment of IPv4 address checkbox and fill in the IP address, Subnet mask, DNS IP address, Hostname fields and, if needed, the **Gateway IP address** field. Make sure that the assigned address does not coincide with the LAN IPv4 address of the router to which your device connects.

LAN	
Automatic obtainment of IPv4 address	
▲ Automatic obtainment of IPv4 address sufficiently prot avoid IPv4 address conflicts, static IPv4 addresses of LAN assigned by an upper-level router (or a local DHCP server)	ects against use of the same addresses in one LAN. In order to devises should not coincide with addresses from the address range .
IP address*	
192.168.0.1	
Subnet mask*	
255.255.255.0	
Gateway IP address	
DNS IP address*	
8.8.8	
Hostname*	
dlinkap799b.local	
③ Specify a domain name ending with .local. In order to a name with a dot and slash at the end in the address bar of	ccess the web-based interface using the domain name, enter this the web browser (for example, dlinkap12ab.local./)
< васк	NEXT >

Figure 38. The page for changing the LAN IPv4 address.

3. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Wi-Fi Client

This configuration step is available for the WISP Repeater, Repeater, and Client modes.

1. On the Wi-Fi Client page, click the WIRELESS NETWORKS button and select the network to which you want to connect in the opened window. When you select a network, the Network name (SSID) and BSSID fields are filled in automatically.

If you cannot find the needed network in the list, click the **UPDATE LIST** icon (



2. If a password is needed to connect to the selected network, fill in the relevant field. Click the **Show** icon (\bigotimes) to display the entered password.

Frequency band		
2.4 GHz	-	Attention! Upon connection to networks with WEP or TK. encryption, basic settings of Wi-Fi networks will be changed:
Network name (SSID)*		the standards 802.11b and g will be used in the 2.4GHz band and the standard 802.11a will be used in the 5GHz band.
RD_DLINK		Network authentication
BSSID		WPA2-PSK
74:DA:DA:0A:8F:C9		
		Password PSK*
		(i) Password should be between 8 and 63 ASCII character
		Encryption type*
		AES
WIRELESS NETWORKS		

Figure 39. The page for configuring the Wi-Fi client.

If you connect to a hidden network, select the band where the hidden network operates from the Frequency band list and enter the network name in the Network name (SSID) field. Then select a needed value from the Network authentication list and then, if needed, enter the password in the relevant field.

When the **Open** or **WEP** authentication type is selected, the following settings are displayed on the page:

Parameter	Description
	For Open authentication type only.
Enable encryption WEP	The checkbox activating WEP encryption. When the checkbox is selected, the Default key ID drop-down list, the Encryption key WEP as HEX checkbox, and four Encryption key fields are displayed on the page.

Parameter	Description
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Select the checkbox to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the Default key ID drop-down list. It is required to specify all the fields. Click the Show icon (\bigotimes) to display the entered key.

When the **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK mixed**, **WPA3-SAE**, or **WPA2-PSK/WPA3-SAE mixed** authentication type is selected, the following fields are displayed:

Parameter	Description
Password PSK	A password for WPA encryption. Click the Show icon (\bigotimes) to display the entered password.
	An encryption method: TKIP , AES , or TKIP+AES .
Encryption type	TKIP and TKIP+AES encryption types are not available for WPA3-SAE and WPA2-PSK/WPA3-SAE mixed authentication types.

3. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Configuring WAN Connection

This configuration step is available for the **Router** and **WISP Repeater** modes.



You should configure your 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.

- 1. On the **Internet connection type** page, click the **SCAN** button (available for the **Router** mode only) to automatically specify the connection type used by your ISP or manually select the needed value from the **Connection type** list.
- 2. Specify the settings necessary for the connection of the selected type.
- 3. If a particular MAC address was registered by your ISP upon concluding the agreement, from the MAC address assignment method drop-down list (available for the Router mode only), select the Manual value and enter this address in the MAC address field. Choose the Clone MAC address of your device value to place the MAC address of your network interface card in the field, or leave the Default MAC address value to place the router's WAN interface MAC address in the field.
- 4. If the Internet access is provided via a VLAN channel, select the **Use VLAN** checkbox and fill in the **VLAN ID** field (available for the **Router** mode only).
- 5. Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

Static IPv4 Connection

Internet connec	tion type	
Connection type		
Static IPv4	-	
 A connection of t 	his type allows you to use a fixed IP a	
SCAN	Network scan for connection ty	pe and parameters detection
IP address*		_
Subnet mask*		_
Gateway IP addres	:S*	_
DNS IP address*		_
MAC address assignmen Default MAC addre		-
MAC address		
10:62:eb:2c:c8:3a	6	
() In some ISP's ne	tworks, it is required to register a cer	tain MAC address in order to get access to the Internet.
Use VLAN		
 Select the check 	box if the Internet access is provided	via a VLAN channel.
Use IGMP		
(i) Internet Group M	anagement Protocol is designed to n	nanage multicast traffic in IP-based networks.
Ping		
	< BACK	NEXT >

Figure 40. The page for configuring Static IPv4 WAN connection.

Fill in the following fields: IP address, Subnet mask, Gateway IP address, and DNS IP address.

Static IPv6 Connection

Internet conne	ection type
Connection type	
Static IPv6	-
0	
(i) A connection of	this type allows you to use a fixed IP address provided by your ISP.
SCAN	Network scan for connection type and parameters detection
IP address*	
Prefix*	
Gateway IP addre	ess*
DNS IP address*	
MAC address assignme Default MAC add	
MAC address	
10:62:eb:2c:c8:3a	
i In some ISP's n	etworks, it is required to register a certain MAC address in order to get access to the Internet.
Use VLAN	
i Select the check	kbox if the Internet access is provided via a VLAN channel.
Ping	
	< BACK NEXT >

Figure 41. The page for configuring Static IPv6 WAN connection.

Fill in the following fields: IP address, Prefix, Gateway IP address, and DNS IP address.

PPPoE, IPv6 PPPoE, PPPoE Dual Stack, PPPoE + Dynamic IP (PPPoE Dual Access) Connections

PPoE A connection of this type requires a user name and password. SCAN Network scan for connection type and parameters detection Without authorization sername* assword* C address assignment method befault MAC address	onnection type			
A connection of this type requires a user name and password. SCAN Network scan for connection type and parameters detection Without authorization sername* assword* Ac address assignment method befault MAC address	PPPoE	-		
SCAN Network scan for connection type and parameters detection Without authorization sername* assword* ervice name AC address assignment method erefult MAC address				
SCAN Network scan for connection type and parameters detection Without authorization sername* assword* ervice name AC address assignment method erefult MAC address	A connection of this type requ	ires a user name and pass	vord.	
Without authorization sername* assword* ervice name AC address assignment method befault MAC address	-			
sername* assword* ervice name AC address assignment method befault MAC address	SCAN Network	scan for connection type	and parameters detect	ion
assword* ervice name AC address assignment method Default MAC address	Without authorization			
assword* ervice name AC address assignment method Default MAC address				
AC address assignment method	Username*			
AC address assignment method				
AC address assignment method Pefault MAC address	Password*	8		
AC address assignment method Pefault MAC address				
efault MAC address	Service name			
efault MAC address				
	MAC address assignment method			
AC address	Default MAC address	-		
	MAC address			
0:62:eb:2c:c8:3a	10:62:eb:2c:c8:3a	<u>n</u>		
	(i) In some ISP's networks, it is i	required to register a certain	MAC address in order to	get access to the Internet.
) In some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet.	Use VLAN			
	Select the checkbox if the Inte	ernet access is provided via	a VLAN channel.	
Use VLAN	•			
	- Ding			

Figure 42. The page for configuring PPPoE WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (∞) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

PPPoE + Static IP (PPPoE Dual Access) Connection

Internet connection type	
Connection type PPPoE + Static IP (PPPoE Dual Access)	
(i) A connection of this type requires a user name, password, and a fixed IP address provid	led by your ISP.
SCAN Network scan for connection type and parameters detection	
Without authorization	
Username*	
Password* &	
Service name	
IP address*	
Subnet mask*	
Gateway IP address*	
DNS IP address*	

Figure 43. The page for configuring PPPoE + Static IP (PPPoE Dual Access) WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (∞) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

Also fill in the following fields: IP address, Subnet mask, Gateway IP address, and DNS IP address.

PPTP + Dynamic IP or L2TP + Dynamic IP Connection

Internet connect	ion type	
Connection type PPTP + Dynamic IP	· -	
PPTP and L2TP ar	re methods for implementing virtual pr	ivate networks.
SCAN	Network scan for connection type	and parameters detection
Without authorization	n	
Username*		
Password*	Q	
VPN server address	*	
MAC address assignment r Default MAC addres		
MAC address		
10:62:eb:2c:c8:3a	6	
i) In some ISP's netw	vorks, it is required to register a certai	n MAC address in order to get access to the Internet.
Use VLAN		
Select the checkbo	ox if the Internet access is provided via	a a VLAN channel.
Use IGMP		
(i) Internet Group Mai	nagement Protocol is designed to ma	nage multicast traffic in IP-based networks.
Ping		
	🗸 ВАСК	NEXT >

Figure 44. The page for configuring PPTP + Dynamic IP WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (∞) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

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

PPTP + Static IP or L2TP + Static IP Connection

Internet connec	tion type		
Connection type			
PPTP + Static IP	•		
 PPTP and L2TP a 	re methods for implementing virtual p	private networks.	
SCAN	Network scan for connection typ	e and parameters detection	
Without authorizati	on		
Username*			
Password*	ø		
VPN server address	\$*		
IP address*			
Subnet mask*			
Gateway IP address	*		
DNS IP address*			

Figure 45. The page for configuring PPTP + Static IP WAN connection.

In the **Username** field enter the login and in the **Password** field enter the password provided by your ISP. Click the **Show** icon (∞) to display the entered password. If authorization is not required, select the **Without authorization** checkbox.

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

Also fill in the following fields: **IP address**, **Subnet mask**, **Gateway IP address**, and **DNS IP address**.

Configuring Wireless Network

This configuration step is available for the **Router**, **Access point**, **WISP Repeater**, and **Repeater** modes.

- 1. On the **Wireless Network 2.4 GHz** page, in the **Network name** field, specify your own name for the wireless network in the 2.4GHz band or leave the value suggested by the router.
- 2. In the **Password** field, specify your own password for access to the wireless network or leave the value suggested by the router (WPS PIN of the device, see the barcode label).
- 3. If the router is used as a Wi-Fi client, you can specify the same parameters of the wireless network as specified for the network to which you are connecting. To do this, click the **USE** button (available for the **WISP Repeater** and **Repeater** modes only).
- 4. You can restore the parameters of the wireless network specified before resetting to factory defaults. To do this, click the **RESTORE** button.

Wireless Network 2.4 GHz	
Enable	
Broadcast wireless network 2.4 GHz	
(i) Disabling broadcast does not influence the ability to con	nect to another Wi-Fi network as a client.
Network name*	
my wi-fi	
Open network	
Password*	
کې	
③ Password should be between 8 and 63 ASCII character	
Use the same parameters as on the root acc	ess point.
RESTORE You can restore network name and security	that was set before applying factory settings.

Figure 46. The page for configuring the wireless network.

 If you want to create an additional wireless network isolated from your LAN in the 2.4GHz band, select the Enable guest network checkbox (available for the Router and WISP Repeater modes only).

Enable guest network
① Guest Wi-Fi network allows connection to your device and getting access to the Internet. Upon that computers connected to this wireless network will be isolated from the resources of your main local area network. This helps to secure your LAN while you provide access to the Internet for temporary users.
Network name*
my wi-fi_Guest
Open network
Max associated clients*
0
Enable shaping
Shaping (Mbit/s)*
0

Figure 47. The page for configuring the wireless network.

- 6. In the **Network name** field, specify your own name for the guest wireless network or leave the value suggested by the router.
- 7. If you want to create a password for access to the guest wireless network, deselect the **Open network** checkbox and fill in the **Password** field.
- 8. If you want to limit the bandwidth of the guest wireless network, select the **Enable shaping** checkbox and fill in the **Shaping** field.
- 9. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.
- 10. On the **Wireless Network 5 GHz** page, specify needed settings for the wireless network in the 5GHz band and click the **NEXT** button.

Configuring LAN Ports for IPTV/VoIP

This configuration step is available for the **Router** mode.

1. On the **IPTV** page, select the **Is an STB connected to the device** checkbox.

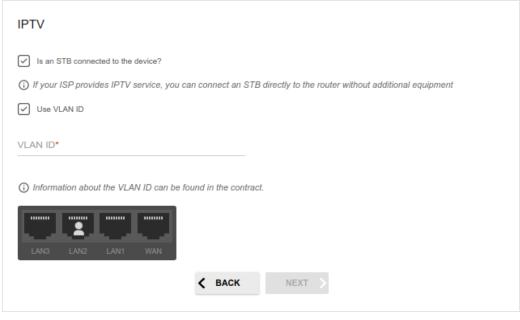


Figure 48. The page for selecting a LAN port to connect an IPTV set-top box.

- 2. Select a free LAN port for connecting your set-top box.
- 3. If the IPTV service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.
- 4. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

5. On the VoIP page, select the Is an IP phone connected to the device checkbox.

VoIP
Is an IP phone connected to the device?
() If your ISP provides VoIP service, you can connect an IP phone directly to the router without additional equipment
Use VLAN ID
VLAN ID*
() Information about the VLAN ID can be found in the contract.
LAN3 LAN2 LAN1 WAN
< BACK NEXT >

Figure 49. The page for selecting a LAN port to connect an VoIP phone.

- 6. Select a free LAN port for connecting your IP phone.
- 7. If the VoIP service is provided via a VLAN channel, select the **Use VLAN ID** checkbox and fill in the **VLAN ID** field.
- 8. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.

Changing Web-based Interface Password

On this page, you should change the default administrator password. To do this, enter a new password in the **User's interface password** and **Password confirmation** fields. You may set any password except **admin**. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.²

Changing web-based interfa	ace password			
For security reasons, please chang	je the password used to	o access the dev	vice's settings.	
User's interface password*	Q			
(i) Password should be between 1 an	d 31 ASCII characters			
Password confirmation*	Q			
	К ВАСК	NEXT		

Figure 50. The page for changing the web-based interface password.

Remember or write down the new password for the administrator account. In case of losing

- the new password, you can access the settings of the router only after restoring the factory
- default settings via the hardware **RESET** button. This procedure wipes out all settings that you have configured for your router.

Click the **NEXT** button to continue or click the **BACK** button to return to the previous page.

On the next page, check all specified settings.

Also you can save a text file with parameters set by the Wizard to your PC. To do this, click the **SAVE CONFIGURATION FILE** button and follow the dialog box appeared.

To finish the Wizard, click the **APPLY** button. The router will apply settings and reboot. Click the **BACK** button to specify other settings.

^{2 0-9,} A-Z, a-z, space, !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~.

If the Wizard has configured a WAN connection, after clicking the **APPLY** button, the page for checking the Internet availability opens.

Connection to the Internet is configured and ready to use Click "Finish" to get started on the Internet
ADVANCED SETTINGS FINISH
An application for smartphones and pads is available Completed on the Completed on the Completed Play

Figure 51. Checking the Internet availability.

If the router has been successfully connected to the Internet, click the **FINISH** button.

If problems appeared when connecting to the Internet, click the **CHECK AGAIN** button to recheck the state of the WAN connection.

If problems of connection have not been solved, contact the technical support of your ISP (as a rule, the technical support phone is provided with the agreement) or the D-Link technical support (the phone number will be displayed on the page after several attempts of checking the connection).

To specify other settings, click the **ADVANCED SETTINGS** button. After clicking the **ADVANCED SETTINGS** button, the **Home** page opens (see the *Home Page* section, page 40).

Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports or available wireless interfaces of the router for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DIR-X1530 in order to use these devices.

To start the Wizard, on the **Home** page, select the **Connection of Multimedia Devices** section.

If you need to select a port or wireless interface in order to use an additional device, left-click the relevant element in the **LAN** section (the selected element will be marked with a frame). Then click the **APPLY** button.

Ξ < Home (Connection of Multi	imedia Devic	es	
You can connect an STB or IP phone di interface and then connect your device In some cases IPTV/VoIP services are p	e to it.			
LAN				
LAN1	LAN2		LAN3	
DIR-XXX-5G	DIR-XXX			
ADVANCED MODE				
	APPLY			

Figure 52. The Multimedia Devices Connection Wizard. The simplified mode.

If you need to configure a connection via VLAN, click the **ADVANCED MODE** button.

LAN			
LAN1 Bridged with No ▼	LAN2	LAN3 Bridged with No	
DIR-XXX-5G Bridged with No	DIR-XXX Bridged with No		
SIMPLIFIED MODE			
WAN	(+)		
	APPLY		

Figure 53. The Multimedia Devices Connection Wizard. The advanced mode.

In the **WAN** section, click the **Add** icon (\bigcirc) .

New Connection	×
Name*	
VLAN ID*	
SAVE	

Figure 54. Adding a connection.

In the opened window, specify a name of the connection for easier identification in the **Name** field (you can specify any name). Specify the VLAN ID provided by your ISP and click the **SAVE** button.

Then in the **LAN** section, from the **Bridged with** drop-down list of the element corresponding to the LAN port or wireless interface to which the additional device is connected, select the created connection. Click the **APPLY** button.

The selected port or wireless interface cannot use the default connection to access the Internet.

To deselect the port or wireless interface in the simplified mode, left-click the selected element (the frame will disappear) and click the **APPLY** button.

To deselect the port or wireless interface in the advanced mode, select the **No** value from the **Bridged with** drop-down list of the element corresponding to the needed LAN port or interface. Then in the **WAN** section, select the connection via VLAN which will not be used any longer and click the **DELETE** button. Then click the **APPLY** button.

Statistics

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

- network statistics
- IP addresses leased by the DHCP server
- the routing rules and routing tables
- data on devices connected to the router's network and its web-based interface, and information on current sessions of these devices
- statistics for traffic passing through ports of the router
- addresses of active multicast groups
- statistics for IPsec tunnels of the router
- the list of clients connected to the PPTP or L2TP server of the router.

Network Statistics

On the **Statistics / Network Statistics** page, you can view statistics for all connections existing in the system (WAN connections, LAN, WLAN). 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, and volume of data received and transmitted (with increase of the volume the units of measurement are changed automatically: byte, Kbyte, Mbyte, Gbyte).

< Connec	tion of Multimedia Devices Netwo	ork Statistics		
etwork St	atistics	the system		
u can view stat	istics for all niterraces (connections) existing it	i the system.		
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 - 192.168.0.1	4.46 Mbyte / 47.58 Mbyte	0/0	-
statip_67	IPv4: 192.168.161.191/24 - 192.168.161.1	54.13 Mbyte / 144.07 Mbyte	0/0	1 d, 17 h., 19 min
WiFi_5GHz_1	-	-/-	0/0	-
WiFi_2GHz_1		94.14 Mbyte / -	0/0	-

Figure 55. The Statistics / Network Statistics page.

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

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.

Network Statistics	DHCP	,		
DHCP You can view the information on devices the	at have got IP addresses from the I	DHCP server.		
Hostname	IP address	MAC	Expires	
android-c2dfe5fa660d5ed1	192.168.0.129	D0:17:C2:00:29:85	1h 1m 4s	

Figure 56. The Statistics / DHCP page.

Routing

Rules							
Table	Туре	IP (Source/Destination)	Interfac	es (Incoming/Outgoing)	Priority	ToS	FWmark (HEX)
group_1	IPv4	all / all		LAN / any	100	0	0x0
group_1	IPv4	all / all		any / any	200	0	0x64
main	IPv4	all / all		any / any	32766	0	0x0
group_1	IPv6	all / all		LAN / any	100	0	0x0
group_1	IPv6	all / all		any / any	200	0	0x64
main	IPv6	all / all		any / any	32766	0	0x0
ables							
ID	Na	me	Description				
254	ma	ain	Main routing ta	able			
257	gro	oup_1	Routing table f	or groups			
256	static_1 Routing table fo		or connections				

The **Statistics / Routing** page displays the routing rules and routing tables.

Figure 57. The Statistics / Routing page.

The **Rules** section displays routing rules, their corresponding routing tables, incoming and outgoing interfaces, priority levels, and other data.

The **Tables** section displays the list of routing tables stored in the device's memory. To view detailed information on routes, left-click the relevant line in the table.

Routing Tal	ble main Information on routes.					
Interface	Destination	Subnet mask	Gateway	Flags	Metric	Table
WAN	0.0.0.0	0.0.0.0	192.168.161.1	UG	410	254
WAN	1.1.1.1		192.168.161.1	UGH	0	254
LAN	192.168.0.0	255.255.255.0		U	0	254
WAN	192.168.161.0	255.255.255.0		U	0	254

Figure 58. The routing table page.

The opened page displays the information on routes in the selected routing table. The table contains destination IP addresses, gateways, subnet masks, and other data.

Clients and Sessions

On the **Statistics / Clients and Sessions** page, you can view the list of devices connected to the local network of the router and information on current sessions of each device.

C Routing	g Clients and Sessions					
Clients				and an af an all days to		
You can view the list of device	es connected to the local he	etwork of the router and informa	ation on current s	essions of each device.		
MAC	IP address	Hostname	Flags	Interface		
MAC > D0:17:C2:00:29:85	IP address 192.168.0.129	Hostname android-c2dfe5fa660	Flags reachable	Interface WLAN		

Figure 59. The Statistics / Clients and Sessions 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.

To view the information on current sessions of a device, select this device in the table. On the opened page, the following data for each session of the selected device will be displayed: the protocol for network packet transmission, the source IP address and port, and the destination IP address and port.

Port Statistics

On the **Statistics / Port Statistics** page, you can view statistics for traffic passing through ports of the router. The information shown on the page can be used for diagnosing connection problems.

	and Sessions	Port Statistics	cs	
Port Statist	ics			
/ou can view stati	stics for traffic passing throu	ugh ports of the device. This informatio	n can be used for diagnosing connection problems.	
Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte	
LAN3	Disconnected	0	0	
LAN2	Connected	8	1	
LAN1	Disconnected	0	0	
WAN	Connected	0	0	

Figure 60. The Statistics / Port Statistics page.

To view the full list of counters for a port, click the line corresponding to this port.

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.

Multicast Groups				
	multicast groups (including IPTV channels a	and groups for transferrin	g service information) to which the device	is
	multicast groups (including IPTV channels a ugh which the device is subscribed.	and groups for transferrin	g service information) to which the device	is
	ugh which the device is subscribed.	and groups for transferrin	g service information) to which the device	is
subscribed, and the interface thro	ugh which the device is subscribed.		g service information) to which the device	is

Figure 61. The Statistics / Multicast Groups page.

IPsec Statistics

On the **Statistics / IPsec Statistics** page, you can view statistics for IPsec tunnels of the router. For each tunnel 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), remote host address or domain name, operation mode and connection type, and number of packets and volume of data received and transmitted.

Psec Stat	istics				
'ou can view st	atistics for IPsec connecti	ions.			
Name	Remote host	Packets received / Packets sent	Traffic received / Traffic sent	Mode	Туре

Figure 62. The Statistics / IPsec Statistics page.

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

VPN Statistics

On the **Statistics / VPN Statistics** page, you can view the list of clients connected to the PPTP or L2TP server of the router.

≡	< IP	sec Statistics	VPN Statis	stics		
-		atistics w statistics for PPTP/L2 ⁻	TP VPN servers connections.			
	Login	Client IP address	Packets sent / Packets received	Traffic sent / Traffic received	Connection type	
	test	10.90.90.2/32	7/7	87.00 byte / 93.00 byte	РРТР	

Figure 63. The Statistics / VPN Statistics page.

For each VPN client the following data are displayed: the unique IP address, username, connection type, and number of packets and volume of data received and transmitted.

To view detailed data on a connected VPN client, click the line corresponding to this client.

Connections Setup

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

WAN

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

By default, a **Dynamic IPv4** connection is configured in the system. It is assigned to the **INTERNET** port of the router.

E 🗸 Multicast Groups	WAN	
WAN		
You can create and edit connections used by the rou	uter.	
Dynamic IPv4		
EDIT RECONNECT		
Connection type:		Dynamic IPv4
Status:		Connected
Interface:		WAN
IP address:		192.168.161.235
Subnet mask:		255.255.255.0
Gateway IP address:		192.168.161.1

Figure 64. The Connections Setup / WAN page. The simplified mode.

To edit an existing connection, click the **EDIT** button. On the opened page, change the needed parameters and click the **APPLY** button.

To disconnect a connection and establish it again, click the **RECONNECT** button.

To remove an existing connection and create a new one, click the **CHANGE CONFIGURATION** button. Upon that the connection creation page opens.

To create several WAN connections, go to the advanced mode. To do this, click the **ADVANCED MODE** button.

When connections of some types are created, the **Connections Setup / WAN** page is automatically displayed in the advanced mode.

		WAN		2
WAN				
You can create and edit conr	nections used by the router.			
Default Gateway IPv	4	Default Gatev	vay IPv6	
The specified connection wil	l be used by default.	No IPv6 connection	created.	
🔘 dynip_95				
IGMP On the IGMP page you can a configure its settings.	llow the router to use IGMP an	d		
Connections List REG	CONNECT 🕂 🗍			
Name	Connection type	Interface	Status	
dynip_95	Dynamic IPv4	WAN	Connected	
SIMPLIFIED MODE				

Figure 65. The Connections Setup / WAN page. The advanced mode.

To create a new connection, click the **ADD** button (+) in the **Connections List** section. Upon that the connection creation page opens.

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

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 (\boxed{III}).

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP** link (for the description of the page, see the *IGMP* section, page 194).

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.

To return to the simplified mode, click the **SIMPLIFIED MODE** button (the button is unavailable if several WAN connections are created).

Creating Dynamic IPv4 or Static IPv4 WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

Gene	ral Settings
Connecti	on type
Static	IPv4 ▼
Interface	
WAN	•
Connecti	on name*
statip_	65
	Enable connection
	NAT
~	network address translation function. It is recommended not to nless your ISP requires it.
	Ping
i WAI external	V Ping Respond allows the device to respond to ping requests from th network.

Figure 66. The page for creating a new Static IPv4 connection. The General Settings section.

Parameter	Description			
General Settings				
Interface	A physical or virtual WAN interface to which the new connection will be assigned.			
Connection name	A name for the connection for easier identification.			
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.			
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.			
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.			
RIP	Move the switch to the right to allow using RIP for this connection.			

Ethernet	t
MAC address BC:0F:9A:	
	one MAC address of your NIC b:2B:34:A5:A8:FB)
	RESTORE DEFAULT MAC ADDRESS
MTU* 1500	

Figure 67. The page for creating a new **Static IPv4** connection. The **Ethernet** section.

Parameter	Description			
	Ethernet			
	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.			
MAC address	To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, 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.			
	To set the router's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).			
MTU	The maximum size of units transmitted by the interface.			

IPv4	
IP address*	
192.168.1	61.224
Subnet mask	*
255.255.2	55.0
Gateway IP a	ddress*
192.168.1	61.1
Primary DNS	*
1.1.1.1	
Secondary DI	45
1.0.0.1	
(i) If the co	nnection is created for the IPTV service only and no data on IP
addressing is	given by your ISP, then you can set the following values: IP
address = 1.0	0.0.1, Netmask = 255.255.255.252, Gateway IP address = 1.0.0.2,

Figure 68. The page for creating a new Static IPv4 connection. The IPv4 section.

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

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

Creating Dynamic IPv6 or Static IPv6 WAN Connection

General Settings
Connection type
Static IPv6
Interface
WAN •
Connection name*
statipv6_67
(i) The number of characters should not exceed 32
Enable connection
Ping
(j) WAN Ping Respond allows the device to respond to ping requests from the external network.

Figure 69. The page for creating a new Static IPv6 connection. The General Settings section.

Parameter	Description	
General Settings		
Interface	A physical or virtual WAN interface to which the new connection will be assigned.	
Connection name	A name for the connection for easier identification.	
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.	
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.	

Etherne	t
MAC address BC:0F:9A	
	one MAC address of your NIC 0:2B:34:A5:A8:FB)
	RESTORE DEFAULT MAC ADDRESS
мти* 1500	

Figure 70. The page for creating a new Static IPv6 connection. The Ethernet section.

Parameter	Description		
	Ethernet		
	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.		
MAC address	To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, 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.		
	To set the router's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).		
МТО	The maximum size of units transmitted by the interface.		
	IPv6		
	IPv6 address*		

Prefix*	
Gateway IPv6 address*	
Primary IPv6 DNS server*	
Secondary IPv6 DNS server	r

Figure 71. The page for creating a new **Static IPv6** connection. The **IPv6** section.

Parameter	Description	
	IPv6	
For Static IPv6 type		
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.	
For Dynamic IPv6 type		
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the Automatically value.	
Enable prefix delegation	Move the switch to the right if it is necessary that the router requests a prefix to configure IPv6 addresses for the local network from a delegating router.	
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.	

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

Creating PPPoE WAN Connection

General S	Settings
Connection typ	e
PPPoE	•
Interface	
WAN	•
Connection nar	ne*
pppoe_21	
Enal	ble connection
0	ork address translation function. It is recommended not to your ISP requires it.
Ping	1
(i) WAN Ping external netwo	Respond allows the device to respond to ping requests from the rk.
RIP	

Figure 72. The page for creating a new **PPPoE** connection. The **General Settings** section.

Parameter	Description	
General Settings		
Interface	A physical or virtual WAN interface to which the new connection will be assigned.	
Connection name	A name for the connection for easier identification.	
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.	
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.	
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.	
RIP	Move the switch to the right to allow using RIP for this connection.	

Ethernet		
MAC address* BC:0F:9A:6D:36:4C		
	ne MAC address of your NIC 2B:34:A5:A8:FB)	
	RESTORE DEFAULT MAC ADDRESS	
MTU*		

Figure 73. The page for creating a new **PPPoE** connection. The **Ethernet** section.

Parameter	Description		
	Ethernet		
	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.		
MAC address	To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, 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.		
	To set the router's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).		
MTU	The maximum size of units transmitted by the interface.		

Without authorization	
Username*	
Password*	Q
Service name	
MTU* 1492	
Encryption protocol No encryption	-
Authentication protocol	
AUTO	•
Keep Alive	
LCP interval*	
-	
LCP interval* 30	
LCP interval* 30 LCP fails*	
LCP interval* 30 LCP fails* 3	
LCP interval* 30 LCP fails*	
LCP interval* 30 LCP fails* 3 Dial on demand	
LCP interval* 30 LCP fails* 3	
LCP interval* 30 LCP fails* 3 Dial on demand	
LCP interval* 30 LCP fails* 3 Dial on demand	

Figure 74. 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.
ΜΤυ	The maximum size of units transmitted by the interface.

Parameter	Description
	Select a method of MPPE encryption.
	• No encryption : MPPE encryption is not applied.
	• MPPE 40 128 bit : MPPE encryption with a 40-bit or 128-bit key is applied.
Encryption protocol	• MPPE 40 bit : MPPE encryption with a 40-bit key is applied.
	• MPPE 128 bit : MPPE encryption with a 128-bit key is applied.
	MPPE encryption can be applied only if the MS-CHAP , MS-CHAPv2 , or AUTO value is selected from the Authentication protocol drop-down list.
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 router 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.
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the Maximum idle time field, specify a period of inactivity (in seconds) after which the connection should be terminated.
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.

IPv4	
Obtain DNS server addresses automatically	
Primary DNS	
Secondary DNS	A

Figure 75. The page for creating a new **PPPoE** connection. The **IPv4** section.

Parameter	Description	
Obtain DNS server addresses automatically	Move the switch to the right to configure automatic assignment of DNS server addresses. Upon that the Primary DNS and Secondary DNS fields are not available for editing.	
Primary DNS / Secondary DNS	Enter addresses of the primary and secondary DNS servers in the relevant fields.	

When all needed settings are configured, click the **APPLY** button. In the simplified mode, 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 CONNECTION** button. On the page displayed, specify the parameters for the connection of the Dynamic IPv4 or Static IPv4 type and click the **APPLY** button.

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, L2TP, or L2TP over IPsec WAN Connection

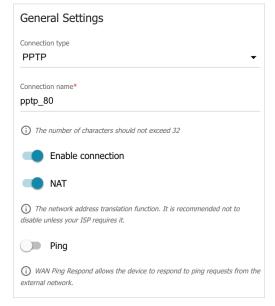


Figure 76. The page for creating a new **PPTP** connection. The **General Settings** section.

Parameter	Description
	General Settings
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
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.
Ping	<i>For the</i> PPTP <i>and</i> L2TP <i>types only.</i> If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

PPP	
Without authorization	
Username*	
Password*	Ø
VPN server address*	
MTU*	
1456	
Encryption protocol	
No encryption	•
Authentication protocol	
AUTO	•
Keep Alive	
LCP interval*	
30	
LCP fails*	
3	
Dial on demand	
Maximum idle time (in seconds)	ß
Static IP address	

Figure 77. 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 (\bigotimes) to display the entered password.
VPN server address	The IP or URL address of the PPTP or L2TP authentication server.
МТО	The maximum size of units transmitted by the interface.

Parameter	Description	
	Select a method of MPPE encryption.	
	• No encryption : MPPE encryption is not applied.	
Encryption protocol	• 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.	
	MPPE encryption can be applied only if the MS-CHAP , MS-CHAPv2 , or AUTO value is selected from the Authentication protocol drop-down list.	
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 router 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.	
Dial on demand	Move the switch to the right if you want the router to establish connection to the Internet on demand. In the Maximum idle time field, specify a period of inactivity (in seconds) after which the connection should be terminated.	
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.	
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.	

IPv4	
Obtain DNS server addresses automatically	
Primary DNS	
Secondary DNS	

Figure 78. The page for creating a new **PPTP** connection. The **IPv4** section.

Parameter	Descriptior	1
Obtain DNS server addresses automatically	Move the switch to the right to configu DNS server addresses. Upon that Secondary DNS fields are not availab	the Primary DNS and
Primary DNS / Secondary DNS	Enter addresses of the primary and sec relevant fields.	condary DNS servers in the
	IPsec	
	Pre-shared key*	
	Enable PFS	
	Specify connection port	

Figure 79. The page for creating a new L2TP over IPsec connection. The IPsec section.

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

Parameter	Description
	IPsec (for the L2TP over IPsec type)
Pre-shared key	A key for mutual authentication of the parties. Click the Show icon (\textcircled{Q}) to display the entered key.
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 upon establishing the IPsec tunnel. This option enhances the security level of data transfer, but increases the load on DIR-X1530.
Specify connection port	Move the switch to the right to change the port used for data exchange with the other party enter the needed value in the Port field displayed. By default, the value 1701 is specified.

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 an existing connection which will be used to access the PPTP/L2TP server and click the **CONTINUE** button; or select the **create a new connection** choice of the radio button and click the **CREATE CONNECTION** 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 and click the **CONTINUE** button.

After creating a connection of the L2TP over IPsec type, on the **VPN / IPsec** page, in the **Status** section, the current state of the IPsec tunnel is displayed.

Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection

General Settings
Connection type
PPPoE IPv6
Interface
WAN -
Connection name*
pppoev6_90
The number of characters should not exceed 32 Enable connection
Ping
() WAN Ping Respond allows the device to respond to ping requests from the external network.

Figure 80. The page for creating a new **PPPoE IPv6** connection. The **General Settings** section.

Parameter	Description
	General Settings
Interface	A physical or virtual WAN interface to which the new connection will be assigned.
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	<i>For the</i> PPPoE Dual Stack <i>type only.</i> If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
RIP	<i>For the</i> PPPoE Dual Stack <i>type only.</i> Move the switch to the right to allow using RIP for this connection.

Ethernet	
MAC address* BC:0F:9A:6	
	ne MAC address of your NIC 2B:34:A5:A8:FB)
	RESTORE DEFAULT MAC ADDRESS

Figure 81. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.

Parameter	Description		
	Ethernet		
	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.		
MAC address	To set the MAC address of the network interface card (of the computer that is being used to configure the router at the moment) as the MAC address of the WAN interface, 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.		
	To set the router's MAC address, click the RESTORE DEFAULT MAC ADDRESS button (the button is available when the switch is moved to the right).		
MTU	The maximum size of units transmitted by the interface.		

PPP	
Without authorization	
Username*	
Password*	<i>S</i>
Service name	
MTU*	
1492	
Encryption protocol	
No encryption	•
Authentication protocol	
AUTO	•
Keep Alive	
LCP interval*	
30	
LCP fails*	
3	
Static IP address	
PPP debug	

Figure 82. 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 (\bigotimes) to display the entered password.
Service name	The name of the PPPoE authentication server.
MTU	The maximum size of units transmitted by the interface.

Parameter	Description	
	Select a method of MPPE encryption.	
	• No encryption : MPPE encryption is not applied.	
	• MPPE 40 128 bit : MPPE encryption with a 40-bit or 128-bit key is applied.	
Encryption protocol	• MPPE 40 bit : MPPE encryption with a 40-bit key is applied.	
	• MPPE 128 bit : MPPE encryption with a 128-bit key is applied.	
	MPPE encryption can be applied only if the MS-CHAP, MS-CHAPv2, or AUTO value is selected from the Authentication protocol drop-down list.	
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 router 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.	
Static IP address	Fill in the field if you want to use a static IP address to access the Internet.	
PPP debug	Move the switch to the right if you want to log all data on PPP connection debugging.	

IPv4	
Obtain DNS server addresses automatically	
Primary DNS	
Secondary DNS	

Figure 83. The page for creating a new **PPPoE Dual Stack** connection. The **IPv4** section.

Parameter	Des	cription
	IPv4 (for the PPPoE Dual Stack type)	
Obtain DNS server addresses automatically	l c	o configure automatic assignment of on that the Primary DNS and t available for editing.
Primary DNS / Secondary DNS	Enter addresses of the primary and secondary DNS servers in the relevant fields.	
	IPv6 Get IPv6 Automatically Enable prefix delegation	• •
	Obtain DNS server addresses automati Primary IPv6 DNS server	icany 🔒
	Secondary IPv6 DNS server	a

Figure 84. The page for creating a new **PPPoE Pv6** connection. The **IPv6** section.

Parameter	Description
	IPv6
Get IPv6	Select a method for IPv6 address assignment from the drop-down list or leave the Automatically value.
Enable prefix delegation	Move the switch to the right if it is necessary that the router requests a prefix to configure IPv6 addresses for the local network from a delegating router.
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.

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

Creating IPIP6 WAN Connection



Figure 85. The page for creating a new **IPIP6** connection. The **General Settings** section.

Parameter	Description
General Settings	
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
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.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

IP		
ob	tain remote host address automatically	
Remote h	ost	A
Mode*		
DSLite		•

Figure 86. The page for creating a new **IPIP6** connection. The **IP** section.

Parameter	Description	
IP		
Obtain remote host address automatically	Move the switch to the right to configure automatic assignment of a remote host IPv6 address.	
	Select an identification method for the remote host from the drop- down list:	
Туре	• Address : The remote host is identified by its IPv6 address.	
Type	• FQDN : The remote host is identified by its domain name.	
	The drop-down list is displayed if the Obtain remote host address automatically switch is moved to the left.	
Remote host	Enter the remote host IPv6 address if the Address value is selected from the Type drop-down list.	
	Enter the remote host domain name if the FQDN value is selected from the Type drop-down list.	
	The field is available for editing, if the Obtain remote host address automatically switch is moved to the left.	
Mode	An operation mode of the connection.	
Mode	From the drop-down list, select the DSLite value.	
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically.	
	Move the switch to the left to specify this parameter manually. Upon that the MTU field is displayed.	
МТО	The maximum size of units transmitted by the interface.	

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 an existing connection which will be used to access the VPN server or select the **create a new connection** choice of the radio button and click the **CONTINUE** 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. Then select an existing connection which will be used to access the VPN server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

Creating 6in4 WAN Connection

Before configuring the connection, please first register on a tunnel broker's web site.

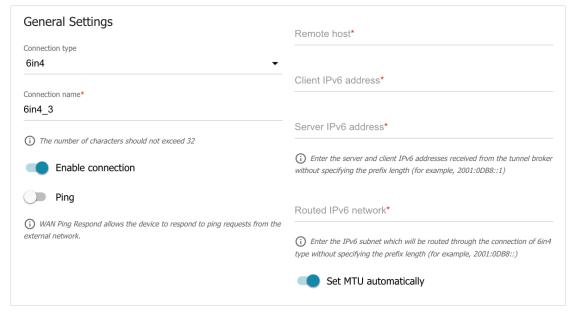


Figure 87. The page for creating a new 6in4 connection.

Parameter	Description	
General Settings		
Connection name	A name for the connection for easier identification.	
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.	
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.	
Remote host	Enter the IPv4 address of the server provided by the tunnel broker.	
Client IPv6 address	Enter the IPv6 address of the router provided by the tunnel broker (without specifying the prefix length).	
Server IPv6 address	Enter the IPv6 address of the server provided by the tunnel broker (without specifying the prefix length).	
Routed IPv6 network	Enter the address of the routed IPv6 subnet (without specifying the prefix length) provided by the tunnel broker.	

Parameter	Description
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically. Move the switch to the left to specify this parameter manually. Upon that the MTU field is displayed.
MTU	The maximum size of units transmitted by the interface.

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

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

To use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select an existing connection which will be used to access the server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

Creating 6to4 WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

General Settings	6to4 Relay Router 192.88.99.1	A
Connection type		
6to4 🗸	Set MTU automatically	
Connection name*		
6to4_77		
(i) The number of characters should not exceed 32		
Enable connection		
Ping		
(i) WAN Ping Respond allows the device to respond to ping requests from the external network.		

Figure 88. The page for creating a new **6to4** connection.

Parameter	Description	
General Settings		
Connection name	A name for the connection for easier identification.	
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.	
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.	
6to4 Relay Router	The IPv4 address of the gateway which is used to transfer IPv6 packets.	
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically.	
	Move the switch to the left to specify this parameter manually. Upon that the MTU field is displayed.	
MTU	The maximum size of units transmitted by the interface.	

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

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

To use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select an existing connection which will be used to access the server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

Creating 6rd WAN Connection

On the connection creation page, in the **General Settings** section, select the relevant value from the **Connection type** drop-down list and specify the needed values.

General Settings	Obtain 6rd settings automatically	
Connection type		
6rd 👻	6rd Border Relay	
Connection name*		
6rd_36	6rd IPv6 prefix	
(i) The number of characters should not exceed 32	6rd IPv6 prefix length	
Enable connection	32	
	IPv4 mask length	
Ping	0	
(i) WAN Ping Respond allows the device to respond to ping requests from the external network.	Hub and spoke	
	Set MTU automatically	

Figure 89. The page for creating a new **6rd** connection.

Parameter	Description
General Settings	
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.
Obtain 6rd settings automatically	Move the switch to the right to let the router obtain 6rd domain settings automatically from the LAN DHCP server or from a delegating router.
	Upon that the 6rd Border Relay, 6rd IPv6 prefix, 6rd IPv6 prefix length, and IPv4 mask length fields are not available for editing.
6rd Border Relay	Enter the IPv4 address of the router provided by your ISP for the 6rd domain.
6rd IPv6 prefix	The IPv6 prefix for the 6rd domain provided by your ISP.
6rd IPv6 prefix length	The IPv6 prefix length for the 6rd domain (in bits) allocated by your ISP. By default, the value 32 is specified.

Parameter	Description
IPv4 mask length	The number of bits in the IPv4 address of the router in the 6rd domain.
Hub and spoke	Move the switch to the right to exchange traffic between clients through the main host of the network in the 6rd domain. Move the switch to the left to exchange traffic between clients without the main host of the network.
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically. Move the switch to the left to specify this parameter manually. Upon that the MTU field is displayed.
MTU	The maximum size of units transmitted by the interface.

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

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

To use this WAN connection to access the Internet, select the **to the Internet** choice of the radio button. Then select an existing connection which will be used to access the server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

LAN

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

IPv4

Go to the **IPv4** tab to change the IPv4 address of the router, configure the built-in DHCP server, specify MAC address and IPv4 address pairs, or add own DNS records.

IP address*	
192.168.0.1	
Mask*	
255.255.255.0	
Hostname	
dlinkrouter.local	
(i) Specify a domain name ending with .local. In order to access the web	
based interface using the domain name, enter this name with a dot and sla	
at the end in the address bar of the web browser (for example,	

Figure 90. Configuring the local interface. The IPv4 tab. The Local IP Address section.

Parameter	Description	
Local IP Address		
Mode of local IP address assignment	Available if the Access point, Repeater, or Client mode was selected in the Initial Configuration Wizard.	
	Select the needed value from the drop-down list.	
	• Static : The IPv4 address, subnet mask, and the gateway IP address are assigned manually.	
	• Dynamic : The router automatically obtains these parameters from the LAN DHCP server or from the router to which it connects.	
IP address	The IPv4 address of the router in the local subnet. By default, the following value is specified: 192.168.0.1 .	
Mask	The mask of the local subnet. By default, the following value is specified: 255.255.0 .	
Gateway IP address	Available if the Access point, Repeater, or Client mode was selected in the Initial Configuration Wizard.	
	The gateway IPv4 address which is used by the router to connect to the Internet (e.g., for synchronizing the system time with an NTP server). <i>Optional</i> .	

Parameter	Description
Hostname	The name of the device assigned to its IPv4 address in the local subnet.
	Dynamic IP Addresses Mode of IPv4 address assignment DHCP
	SELECT ADDRESS RANGE Lease time (in minutes)* 1440 DNS relay Assigns the LAN IP address of the device as the DNS server for connected clients.

Figure 91. Configuring the local interface. The IPv4 tab. The Dynamic IP Addresses section.

Parameter	Description		
	Dynamic IP Addresses		
Mode of IPv4 address assignment	 An operating mode of the router's DHCP server. Disable: The router's DHCP server is disabled, clients' IP addresses are assigned manually. DHCP: The router 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, the SELECT ADDRESS RANGE button, and the DNS relay switch are displayed on the tab. Also when this value is selected, the DHCP Options, Static IP Addresses, and Hosts sections are displayed on the tab. 		
	 Relay: An external DHCP server is used to assign IP addresses to clients. When this value is selected, the External DHCP server IP, Option 82 Circuit ID, Option 82 Remote ID, and Option 82 Subscriber ID fields are displayed on the tab. Available if the Router or WISP Repeater mode was selected in the Initial Configuration Wizard. 		

Parameter	Description
Start IP	The start IP address of the address range used by the DHCP server to distribute IP addresses to clients.
End IP	The end IP address of the address range used by the DHCP server to distribute IP addresses to clients.
SELECT ADDRESS RANGE	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the SAVE button to automatically fill in the Start IP and End IP fields.
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	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the Advanced / DNS page as the DNS server address.
External DHCP server IP	The IP address of the external DHCP server which assigns IP addresses to the router's clients.
Option 82 Circuit ID Option 82 Remote ID Option 82 Subscriber ID	The value of the relevant field of DHCP option 82. Do not fill in the fields unless your ISP or the administrator of the external DHCP server provided these values.

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

In the **DHCP Options** section, you can change default values for some options of DHCP protocol (IP address, subnet mask, DNS servers) or specify additional parameters which the built-in DHCP server should send to clients to configure the local network.

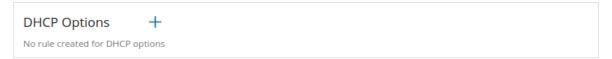


Figure 92. Configuring the local interface. The **IPv4** tab. The section for configuring DHCP options.

To do this, click the **ADD** button (+).

DHCP Options	×
Known DHCP options Select option	•
Options value	ß
Force	
SAVE	

Figure 93. Configuring the local interface. The IPv4 tab. The window for configuring a DHCP option. In the opened window, you can specify the following parameters:

Parameter	Description
Known DHCP options	From the drop-down list, select an option which you want to configure.
Options value	Specify the value for the selected option.
Force	Move the switch to the right to let the DHCP server send the selected option regardless of the client's request. Move the switch to the left to let the DHCP server send the selected option only when the client requests it.

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

To edit the parameters of an option, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove the value of an option, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ($\boxed{10}$). Then click the **APPLY** button.

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

Static IP Addresses	+
In order to assign an IP address to	a MAC address, select a device from the list of connected clients or add a new device

Figure 94. Configuring the local interface. The **IPv4** tab. The section for creating MAC-IPv4 pairs.

To create a MAC-IPv4 pair, click the **ADD** button (+). In the opened window, fill in the **MAC** address field. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant MAC address from the drop-down list (the field will be filled in automatically). Then in the **IP address** field, enter an IPv4 address which will be assigned to the device with the specified MAC address. In the **Hostname** field, specify a network name of the device for easier identification. To limit the time of the specified IPv4 address assignment, specify the required value in the **Lease time** field. Click the **SAVE** button.

To edit the settings for an existing MAC-IPv4 pair, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a MAC-IPv4 pair, select the checkbox located to the left of the relevant line in the table

and click the **DELETE** button ($\boxed{10}$). Then click the **APPLY** button.

If needed, you can add your own address resource records. To do this, click the **ADD** button (+) in the **Hosts** section (available if in the **Dynamic IP Addresses** section the **DHCP** value is selected from the **Mode of IPv4 address assignment** drop-down list).

Add Host	×
Name*	
IP address	Ŧ
ADD	
In order to delete IP address just leave the field empty	
SAVE	

Figure 95. Configuring the local interface. The **IPv4** tab. The window for adding a DNS record.

In the **Name** field, specify the domain or domain name to which the specified IPv4 address will correspond. In the **IP address** field, specify a host from the internal or external network. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv4 address from the drop-down list (the field will be filled in automatically). To specify several IP addresses, click the **ADD** button. Click the **SAVE** button.

To edit an existing record, in the **Hosts** section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a record, in the **Hosts** section, select the checkbox located to the left of the relevant line

in the table and click the **DELETE** button ($\boxed{10}$).

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

IPv6

Go to the **IPv6** tab to change or add the IPv6 address of the router, configure IPv6 addresses assignment settings, specify MAC address and IPv6 address pairs, or add own DNS records.

Local IPv6 Address	
For example: fd00::1/64	Î
i) Enter IPv6 address, slash (/), and a decimal value equal to the size in the prefix.	bits of
ADD	
Hostname	
dlinkrouter.local	

Figure 96. Configuring the local interface. The IPv6 tab. The Local IPv6 Address section.

To add an IPv6 address of the router, click the **ADD** button. In the line displayed, enter an IPv6 address and then a slash followed by a decimal value of the prefix length. In the **Hostname** field, enter the name of the device assigned to its IPv6 address in the local subnet. To change an IPv6 address of the router, edit the corresponding line.

To remove an IPv6 address, click the **DELETE** $(\overline{\square})$ button in the corresponding line of the table. Then click the **APPLY** button. In the Dynamic IP Addresses section, you can configure IPv6 addresses assignment settings.

Dynamic IP Addresses
Mode of IPv6 address assignment
Stateful -
Start IP*
::2
End IP*
::64
SELECT ADDRESS RANGE
Lease time (in minutes)*
1440
() Lease time will be chosen by ISP based on the delegated prefix life time.
The default route for LAN clients
ONS relay
() Assigns the LAN IP address of the device as the DNS server for connected clients.

Figure 97. Configuring the local interface. The **IPv6** tab. The **Dynamic IP Addresses** section.

Parameter	Description	
Dynamic IP Addresses		
Mode of IPv6 address assignment	 Select the needed value from the drop-down list. Disable: Clients' IPv6 addresses are assigned manually. Stateless: Clients themselves configure IPv6 addresses using the prefix. Stateful: The built-in DHCPv6 server of the router allocates addresses from the range specified in the Start IP and End IP fields. Also when this value is selected, the Static IP Addresses and Hosts sections are displayed on the tab. 	
	• Relay : An external DHCP server is used to assign IPv6 addresses to clients. When this value is selected, the External DHCP server IP field is displayed on the tab. <i>Available if the Router or WISP Repeater mode was selected in the Initial Configuration Wizard.</i>	
Start IP / End IP	The start and the end values for the latest hextet (16 bit) of the range of IPv6 addresses which the DHCPv6 server distributes to clients.	

Parameter	Description
SELECT ADDRESS RANGE	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the SAVE button to automatically fill in the Start IP and End IP fields.
Lease time	The lifetime of IPv6 addresses provided to clients.
The default route for LAN clients	Move the switch to the right to let the clients, that received IPv6 addresses or configured them using the prefix, use the router as the default IPv6 route.
	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address.
DNS relay	Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the Advanced / DNS page as the DNS server address.

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

In the **Static IP Addresses** section, you can specify MAC address and IPv6 address pairs (set a fixed IPv6 address in the local area network for a device with a certain MAC address). The router assigns IPv6 addresses in accordance with the specified pairs only when the **Stateful** value is selected from the **Mode of IPv6 address assignment** drop-down list in the **Dynamic IP Addresses** section.

Static IP Addresses + In order to assign an IP address to a MAC address, select a device from the list of connected clients or add a new device

Figure 98. Configuring the local interface. The IPv6 tab. The section for creating MAC-IPv6 pairs.

To create a MAC-IPv6 pair, click the **ADD** button (+). In the opened window, fill in the **MAC** address field. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant MAC address from the drop-down list (the field will be filled in automatically). Then in the **IP address** field, enter an IPv6 address which will be assigned to the device with the specified MAC address. In the **Hostname** field, specify a network name of the device for easier identification. To limit the time of the specified IPv6 address assignment, specify the required value in the **Lease time** field. Click the **SAVE** button.

To edit the settings for an existing MAC-IPv6 pair, left-click the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a MAC-IPv6 pair, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ($\boxed{10}$). Then click the **APPLY** button.

If needed, you can add your own address resource records. To do this, click the **ADD** button (+) in the **Hosts** section (*available if in the* **Dynamic IP Addresses** section the **Stateful** value is selected from the **Mode of IPv6 address assignment** drop-down list).

Add Host	×
Name*	
IP address	•
ADD	
() In order to delete IP address just leave the field empty	ld
SAVE	

Figure 99. Configuring the local interface. The IPv6 tab. The window for adding a DNS record.

In the **IP address** field, specify a host from the internal or external network. You can choose a device connected to the router's LAN at the moment. To do this, select the relevant IPv6 address from the drop-down list (the field will be filled in automatically). In the **Name** field, specify the domain or domain name to which the specified IPv6 address will correspond. Click the **SAVE** button.

To edit an existing record, in the **Hosts** section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a record, in the **Hosts** section, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ($\boxed{10}$).

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

WAN Failover

On the **Connections Setup / WAN Failover** page, you can enable the WAN backup function, which provides you with uninterrupted access to the Internet. When your main connection breaks down, the router activates the backup connection; and when the main channel is recovered, the router switches to it and disconnects the reserve one.

≡ < wan		WAN Failover	
		with uninterrupted access to the Internet. When your main connection breaks he main channel is recovered, the router switches to it and disconnects the	
Connections IPv4 The list of available connect Connection pppoe_28 static_Internet	tions on order of priority. Check with ping On On	Check with ping Interval between checks (in seconds)* 30 Waiting for response (in seconds)* 1 Number of attempts* 3 (1) Number of ping requests to the specified hosts Hosts 8.8.8.8 77.88.55.55 94.100.180.200 ADD HOST	x x x
APPLY			

Figure 100. The Connections Setup / WAN Failover page.

To activate the backup function, create several WAN connections. After that go to the **Connections Setup / WAN Failover** page, move the **Enable** switch to the right.

In the **Connections IPv4** section, the existing IPv4 connections are displayed in order of their priority. The first connection on the list serves as the main connection, the others are backup connections.

To change the priority of a connection, left-click the relevant line in the table.

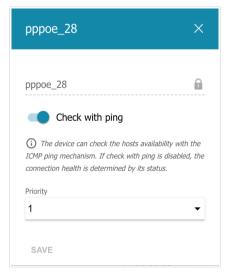


Figure 101. The window for changing the priority of a connection.

In the opened window, specify the needed parameters.

Parameter	Description
Check with ping	Move the switch to the right to let the router use ICMP ping mechanism for checking the connection. Move the switch to the left to let the router check only the status of
	the connection (may be useful for unstable connections).
Priority	The priority level of the connection. Level 1 is for the main connection, the others are backup connections. Select the required value from the drop-down list.

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

In the **Check with ping** section, specify settings of checking the connection using ICMP ping mechanism.

Parameter	Description			
Check with ping				
Interval between checks	A time period (in seconds) between regular checks of the hosts' availability. By default, the value 30 is specified. The value of this field should be higher than product of Waiting for response and Number of attempts fields values.			
	Several ping requests are sent to check the hosts. After a successful attempt the router keeps using the main connection. After several failed attempts the next connection from the list is enabled.			
Waiting for response A time period (in seconds) allocated for a response request.				
Number of attempts	A number of failed attempts to check the health of a connection after which the next connection from the list is enabled.			
	External IP addresses that the router will check for availability via ICMP ping mechanism.			
Hosts	Click the ADD HOST button, and in the line displayed, enter an IP address or leave values suggested by the router.			
	To remove an IP address from the list, click the Delete icon (\times) in the line of the address.			

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

VPN

In this menu you can configure VPN connections based on IPsec/GRE/EoGRE/EoIP/IPIP protocols and create a PPTP or L2TP server and accounts for access to it.

IPsec

On the **VPN / IPsec** page, you can configure VPN tunnels based on IPsec protocol.

IPsec is a protocol suite for securing IP communications.

K WAN Failover		IPsec		
Psec				
ou can configure VPN tunnels based on IPsec protoc	ol.			
DISABLE				
ogging level				
Basic		•		
Funnels reconnect 🕂 🗊				
	Interface	Encryption/hashing algo	prithm	
Remote host Mode Interf	ace	The First Phase	The Second Phase	
tatus				
bialus				
Status Remote host	IKE	CHILD	State	

Figure 102. The VPN / IPsec page.

To allow IPsec tunnels, click the **ENABLE** button. Upon that the **Tunnels** and **Status** sections and the **Logging level** drop-down list are displayed on the page.

In the **Status** section, the current state of an existing tunnel is displayed.

From the **Logging level** drop-down list, select a detail level of messages recorded to the system log or leave the value specified by default. The **Basic** value is recommended to establish an IPsec tunnel faster. To view the log, go to the **System / Log** page (see the *Log* section, page 232).

To create a new tunnel, click the **ADD** button (+) in the **Tunnels** section.

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

(IPsec	IPsec/Ac	lding D
General Settings		
Enable		Enable DPD
Name*		DPD - Dead Peer Detection
ipsec_19	(DPD delay (in seconds)*
The number of characters should not exceed 32	:	30
IP version	1	DPD timeout (in seconds)*
IPv4	•	120
Dynamic IPsec		TCP MSS
Туре		Path MTU discovery -
Address	-	
Remote host*		
Remote identifier		
Remote port		
Pre-shared key*	ø	
Local WAN		
Default gateway	•	
Local identifier		
Local port		
NAT Traversal		
Enabled	•	
Mode		
TUNNEL	•	

Figure 103. The page for adding an IPsec tunnel. The General Settings section.

You can specify the following parameters:

Parameter	Description
	General Settings
Enable	Move the switch to the right to enable the tunnel. Move the switch to the left to disable the tunnel.

Parameter	Description
Name	A name for the tunnel for easier identification. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout. ³
IP version	An IP version.
Dynamic IPsec	Move the switch to the right to allow a remote host with any public IP address to connect to the router via IPsec protocol. Such a setting can be specified for one IPsec tunnel only. Connection requests via this tunnel can be sent by a remote host only.
	Select an identification method for the remote host (router) from the drop-down list:
Туре	• Address : The remote host is identified by its IP address.
1360	• FQDN : The remote host is identified by its domain name.
	The drop-down list is displayed if the Dynamic IPsec switch is moved to the left.
	Enter the remote subnet VPN gateway IP address if the Address value is selected from the Type drop-down list.
Remote host	Enter the remote subnet VPN gateway domain name if the FQDN value is selected from the Type drop-down list.
	The field is available for editing if the Dynamic IPsec switch is moved to the left.
Remote identifier	A remote host identifier to establish connection over IPsec with particular hosts only. To establish connection, DIR-X1530 remote identifier value should correspond to the local identifier value specified in the settings of the remote host. Use an IP address, domain name, or certificate CN. <i>Optional</i> .
Remote port	A port of the remote host, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If the field is left blank and the network address translation (NAT) function is used for the connection, port 4500 is used.
Pre-shared key	A PSK key for mutual authentication of the parties. Click the Show icon (\bigotimes) to display the entered key.

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

Parameter	Description
	A WAN connection through which the tunnel will pass. Select a value from the drop-down list.
Local WAN	• Interface : When this value is selected, the Interface drop- down list is displayed. Select an existing WAN connection from the list.
	• Default gateway : When this value is selected, the router uses the default WAN connection.
Local identifier	A local identifier of the router to establish connection over IPsec with particular hosts only. To establish connection, DIR-X1530 local identifier value should correspond to the remote identifier value specified in the settings of the remote host. Use an IP address, domain name, or certificate CN. <i>Optional</i> .
Local port	A port of the router, that is used for IPsec packets exchange during the First Phase of the connection. If the field is left blank, port 500 is used. If the field is left blank and the network address translation (NAT) function is used for the connection, port 4500 is used.
	The NAT Traversal function allows VPN traffic to pass through the NAT-enabled device. DIR-X1530 allows to forcibly encapsulate VPN traffic in UDP packets for passing through a remote device regardless of whether it supports address translation.
NAT Traversal	If you need to enable forced encapsulation of VPN traffic, select the Enabled value.
	If you need to disable forced encapsulation of VPN traffic, select the Disabled value.
	An operation mode of the IPsec tunnel. Select a value from the drop- down list.
Mode	• TUNNEL : As a rule, it is used to create a secure connection to remote networks. In this mode, the source IP packet is fully encrypted and added to a new IP packet and data transfer is based on the header of the new IP packet.
	• TRANSPORT : As a rule, it is used to encrypt data stream within one network. In this mode, only the content of the source IP packet is encrypted, its header remains unchanged and data transfer is based on the source header.
Allow traffic from IPsec to router	Move the switch to the left to deny access to your router from the remote subnet via IPsec. The switch is displayed when the TUNNEL value is selected from the Mode drop-down list.

Parameter	Description
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 the remote host: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD messages to the remote host. If the switch is moved to to the left, the DPD delay and DPD timeout fields are not available for editing.
DPD delay	A time period (in seconds) between DPD messages. By default, the value 30 is specified.
DPD timeout	A waiting period for the response to a DPD message (in seconds). If the host does not answer in the specified time, the router breaks down the tunnel connection, updates information on it, and tries to reestablish the connection. By default, the value 120 is specified.
	<i>Maximum Segment Size of a TCP packet.</i> This parameter influences the size of a TCP packet which will be sent from the remote host to the router.
TCP MSS	If the Manual value is selected, you can specify the value of this parameter for each subnet of the tunnel in the MTU field. The field is displayed in the window for adding a subnet in the Tunneled Networks section.
	If the Path MTU discovery value is selected, the parameter will be configured automatically for all created subnets.

The First Phase	The Second Phase	
First phase encryption algorithm	Second phase encryption algorithm	
DES	✓ DES	•
Encryption mode	Encryption mode	
CBC	✓ CBC	•
Hashing algorithm	Hashing algorithm	
MD5	✓ MD5	•
Size of hash	Size of hash	
96	▼ 96	•
Hashing mode	Hashing mode	
HMAC	✓ HMAC	•
First phase DHgroup type	Enable PFS	
MODP768	•	
	Second phase DHgroup type	
IKE-SA lifetime*	MODP768	•
10800	IPsec-SA lifetime*	
Aggressive Mode	3600	
IKE version		
1	•	

Figure 104. The page for adding an IPsec tunnel. The First Phase / The Second Phase sections.

Parameter	Description
	The First Phase
First phase encryption algorithm	Select an available encryption algorithm from the drop-down list.
Encryption mode	Select an encryption mode from the drop-down list.
Hashing algorithm	Select a hashing algorithm from the drop-down list.
Size of hash	The length of the hash in bits.
Hashing mode	Select a hashing mode from the drop-down list.
First phase DHgroup type	A Diffie-Hellman key group for the First Phase. 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 be greater than the value specified in the IPsec-SA lifetime field.
Aggressive Mode	Move the switch to the right to enable the aggressive mode for mutual authentication of the parties. Such a setting accelerates the connection establishment, but reduces its security.

Parameter	Description	
IKE version	IKE (<i>Internet Key Exchange</i>) is a protocol of keys exchange between two hosts of VPN connections. Select a version of the protocol from the drop-down list.	
	The Second Phase	
Second phase encryption algorithm	Select an available encryption algorithm from the drop-down list.	
Encryption mode	Select an encryption mode from the drop-down list.	
Hashing algorithm	Select a hashing algorithm from the drop-down list.	
Size of hash	The length of the hash in bits.	
Hashing mode	Select a hashing mode from the drop-down list.	
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 the Second Phase. This option enhances the security level of data transfer, but increases the load on DIR-X1530.	
Second phase DHgroup type	A Diffie-Hellman key group for the Second Phase. Select a value from the drop-down list. The drop-down list is available if the Enable PFS switch is moved to the right.	
IPsec-SA lifetime	The lifetime of the Second Phase keys in seconds. After the specified period it is required to renegotiate the keys. The value specified in this field should be greater than zero.	

To specify IP addresses of local and remote subnets for this tunnel, click the **ADD** button (+) in the **Tunneled Networks** section.

Add Rule	×
Local network	
ADD SUBNET	
Specify the local subnet of router's LAN). Example: 192.16	
Remote subnet	
ADD SUBNET	
Specify the remote subner of the device which acts as a re 192.168.10.0/24	
of the device which acts as a ro	

Figure 105. 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
	A local subnet IP address and mask.
Local network	To add one more subnet, click the ADD SUBNET button and enter the subnet address in the displayed line (available if 2 is selected from the IKE version list in the The First Phase section).
	To remove the subnet, click the Delete icon (\times) in the line of the subnet address.
	A remote subnet IP address and mask.
Remote subnet	To add one more subnet, click the ADD SUBNET button and enter the subnet address in the displayed line (available if 2 is selected from the IKE version list in the The First Phase section).
	To remove the subnet, click the Delete icon (\times) in the line of the subnet address.
MTU	The maximum size (in bytes) of a non-fragmented packet. The field is displayed when the Manual value is selected from the TCP MSS drop-down list in the General Settings section.

Click the **SAVE** button.

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 (1). Also you can remove a subnet in the editing window.

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

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 disconnect an existing tunnel and establish it again, select the checkbox located to the left of the relevant line in the table and click the **RECONNECT** 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 ($\overline{\blacksquare}$). Also you can remove a tunnel on the editing page.

To disable VPN tunnels based on IPsec protocol, click the **DISABLE** button.

GRE

On the **VPN / GRE** page, you can configure VPN tunnels based on GRE protocol.

GRE (*Generic Routing Encapsulation*) is a protocol for tunneling network packets, which enables you to create unprotected VPN tunnels.

≡ < IPsec	GRE	
GRE You can configure VPN tunnel	s based on GRE protocol.	
No tunnel created You can add a tunnel	+	

Figure 106. The VPN / GRE page.

To create a new tunnel, click the **ADD** button (+).

≡ < gre	GRE/Adding
Tunnel settings Enable Name* GRE	Static route settings Remote LAN IP address*
① The number of characters should not exceed 32	Remote LAN mask*
IP address*	Remote GRE interface IP address*
Mask*	
Interface* Not selected	•
Remote IP*	
мт ∪* 1400	
Allow traffic GRE -> LAN	
APPLY	

Figure 107. The page for adding a GRE tunnel.

You can specify the following parameters:

Parameter	Description		
	Tunnel settings		
Enable	Move the switch to the right to enable the GRE tunnel.		
	Move the switch to the left to disable the GRE tunnel.		
Name	A name of the tunnel for easier identification. You can specify any name.		
IP address	The IP address of the GRE tunnel interface.		
Mask	The mask of the subnet.		
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.		
Remote IP	Enter the public IP address of the remote subnet VPN gateway.		
MTU	The maximum size of units transmitted from the remote host to the router.		
Allow traffic GRE → LAN	Move the switch to the right to allow GRE tunnel users access devices in the remote local subnet.		
Static route settings			
Remote LAN IP address	The IP address of the remote local subnet.		
Remote LAN mask	The mask of the remote local subnet.		
Remote GRE interface IP address	The IP address of the GRE tunnel interface in the remote subnet.		

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

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 ($\boxed{10}$).

IPIP

On the **VPN / IPIP** page, you can configure VPN tunnels based on IPIP protocol.

IPIP (*IP Encapsulation within IP*) is a protocol for IP-tunneling network packets, which enables you to create unprotected VPN tunnels, encapsulating IP packets within other IP packets.

😑 🗸 gre	IPIP	
IPIP You can configure VPN tunnels	pased on IPIP protocol.	
No tunnel created You can add a tunnel	+	

Figure 108. The VPN / IPIP page.

To create a new tunnel, click the **ADD** button (+).

≡ < IPIP	IPIP/Adding	
Tunnel settings	Static route settings	
Name* IPIP_62	Remote LAN IP address*	
The number of characters should not exceed 32	Remote LAN mask*	
IP address*	Remote IPIP interface subnet*	
Mask*	Remote IPIP interface mask*	
Interface* Not selected	•	
Remote IP*		
мтu* 1400		
Allow traffic IPIP -> LAN		
APPLY		

Figure 109. The page for adding an IPIP tunnel.

You can specify the following parameters:

Parameter	Description		
Tunnel settings			
Enable	Move the switch to the right to enable the IPIP tunnel.		
LIIdDie	Move the switch to the left to disable the IPIP tunnel.		
Name	A name of the tunnel for easier identification. You can specify any name.		
IP address	The IP address of the IPIP tunnel interface.		
Mask	The mask of the subnet.		
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.		
Remote IP	Enter the public IP address of the remote subnet VPN gateway.		
MTU	The maximum size of units transmitted from the remote host to the router.		
Allow traffic IPIP \rightarrow LAN	Move the switch to the right to allow IPIP tunnel users access devices in the remote local subnet.		
	Static route settings		
Remote LAN IP address	The IP address of the remote local subnet.		
Remote LAN mask	The mask of the remote local subnet.		
Remote IPIP interface subnet	The subnet of the remote IPIP interface.		
Remote IPIP interface mask	The mask of the remote IPIP interface.		

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

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 ($\boxed{10}$).

PPTP/L2TP Servers

On the **VPN / PPTP/L2TP Servers** page, you can enable the PPTP or L2TP VPN server. To configure the PPTP or L2TP server, go to the relevant tab.

PPTP and L2TP help to establish a secure connection creating a tunnel in the standard insecure network.

Before creating the PPTP or L2TP server	; it is required to create user accounts ((see the
VPN Users section, page 139).		

E < GRE PPTP/L	2TP Servers
РРТР	L2TP
PPTP Server	
You can enable PPTP VPN server.	
Enable	
VPN network	Access policies and NAT
Server local IP address*	VPN <> LAN* Unknown
	VPN <> WAN*
Start client IP*	Unknown
End client IP*	VPN → Router* Unknown
Interface*	NAT VPN -> WAN
Not selected -	NAT VPN -> LAN
Authentication	0
Enable authentication	Advanced Settings
	Maximum number of connections*
MPPE	100
Enable MPPE	MTU*
MPPE settings are available upon enabled authentication and require only MSCHAP or MSCHAPv2.	1400
	DNS
	Obtain DNS server addresses automatically
	You can use addresses of the WAN connection selected from the "Interface" I or specify them manually.
	Primary DNS
	1.1.1.1
	Secondary DNS
	1.0.0.1
Users List +	
Users list is empty	

Figure 110. The VPN / PPTP/L2TP Servers page.

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

You can specify the following parameters:

Parameter	Description	
	VPN network	
Server local IP address	The IP address of the VPN server.	
Start client IP	The start IP address of the address range for VPN server's clients.	
End client IP	The end IP address of the address range for VPN server's clients.	
Interface	Select a WAN connection through which this VPN server will be available. If the Default gateway value is selected, the router uses the default WAN connection.	
	Access policies and NAT	
	Select a value from the drop-down list.	
VPN ↔ LAN	• Allow : VPN server's clients can access the router's local network; clients from the router's local network can access the VPN server's network.	
	• Deny : VPN server's clients cannot access the router's local network; clients from the router's local network cannot access the VPN server's network.	
	Select a value from the drop-down list.	
VPN ↔ WAN	• Allow : VPN server's clients can access the external network; clients from the external network can access the VPN server's network.	
	• Deny : VPN server's clients cannot access the external network; clients from the external network cannot access the VPN server's network.	
	Select a value from the drop-down list.	
$\textbf{VPN} \rightarrow \textbf{Router}$	• Allow: VPN server's clients can access the router.	
	• Deny : VPN server's clients cannot access the router.	
NAT VPN \rightarrow WAN	If the switch is moved to the right, the network address translation function between the VPN server's interface and the external network interface is enabled.	
NAT VPN \rightarrow LAN	If the switch is moved to the right, the network address translation function between the VPN server's interface and the local network interface is enabled.	

Parameter	Description	
Authentication		
Enable authentication	Move the switch to the right to enable authentication. Upon that the Multiple sessions , CHAP , MSCHAP , MSCHAPv2 , and PAP lists are displayed on the page.	
	The mode of connection for the users listed in the Users List section. Select a value from the drop-down list.	
Multiple sessions	• Allow : Several users with the same user account are allowed to connect.	
Multiple sessions	• Only new connections : If there are several users with the same user account, only new users are allowed to connect.	
	• Only old connections : If there are several users with the same user account, new users are not allowed to connect.	
	Challenge Handshake Authentication Protocol.	
	Microsoft Challenge Handshake Authentication Protocol.	
СНАР	Password Authentication Protocol.	
	Select the needed action from the drop-down list for the relevant protocol.	
MSCHAPv2 PAP	• Auto : Enable automatic client authentication over this protocol.	
	• Refuse : Disable client authentication over this protocol.	
	• Require : Require client authentication over this protocol.	
	MPPE	
	Move the switch to the right to enable MPPE encryption.	
Enable MPPE	MPPE encryption can be applied only if the Require value is selected from the MSCHAP or MSCHAPv2 drop-down list.	
	MPPE encryption with a 40-bit or 128-bit key is applied. Select the needed action from the drop-down list.	
MPPE40	• Auto : Allow clients to connect to the VPN server automatically with MPPE encryption.	
MPPE128	• Refuse : Restrict clients from connecting to the VPN server with MPPE encryption.	
	• Require : Allow clients to connect to the VPN server only with MPPE encryption.	

Parameter	Description		
	Advanced Settings		
Maximum number of connections Available on the PPTP tab. The maximum number of devices allowed to connect to t server.			
Port	Available on the L2TP tab. The port of L2TP server. By default, the value 1701 is specified.		
MTU	TU The maximum size of units transmitted by the interface.		
Enable debug mode	Move the switch to the right if you want to log all data on this VPN server debugging.		
DNS			
Obtain DNS server addresses automatically	Move the switch to the right to let VPN server's clients obtain DNS server addresses of the WAN connection which is selected from the Interface list. Upon that the Primary DNS and Secondary DNS fields are not available for editing.		
Primary DNS / Secondary DNS	Enter addresses of the primary and secondary DNS servers in the relevant fields.		

If you want to specify the list of accounts to provide access to this server, click the ADD (+) button in the **Users List** section.

User*	
Not selected	•
Set IP address	
Auto	•

Figure 111. A window for adding a user.

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

Parameter	Description	
User	Select a user account to allow access.	
Set IP address	 The mode of IP address assignment. Select a value from the drop-down list. Auto: The IP address is assigned to the user automatically. Single IP: The IP address is assigned to the user manually. When this value is selected, the IP address field is displayed. 	
IP address	Specify an IP address from the range specified in the Start client IP and End client IP fields.	

Click the **SAVE** button.

To edit an existing user, in the **Users List** section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove a user, in the **Users List** section, select the checkbox located to the left of the relevant

line in the table and click the **DELETE** button ($\overline{\square}$).

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

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

VPN Users

PPTP or L2TP server.

PPTP/L2TP Servers	VPN Users	E
VPN Users	uther land accord to a DDTD or LOTD conver	
There are no users +	uthorized access to a PPTP or L2TP server.	
You can add first user		

On the VPN / VPN Users page, you can create user accounts to provide authorized access to a

Figure 112. The VPN / VPN Users page.

To create a new user account, click the **ADD** button (+).

User	×
Username*	
Password*	Ø
SAVE	

Figure 113. The window for adding a user.

In the opened window, in the **Username** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.⁴ Click the **Show** icon (\bigotimes) to display the entered key.

Click the **SAVE** button.

To view passwords of all user accounts, move the **Show password** switch to the right.

To edit the parameters of an account, select the relevant line in the table. In the opened window, enter a new value in the relevant field, and then click the **SAVE** button.

To remove an account, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ($\boxed{10}$).

^{4 0-9,} A-Z, a-z, !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~.

EoGRE

On the VPN / EoGRE page, you can configure VPN tunnels based on EoGRE technology.

EoGRE (*Ethernet over GRE*) technology allows transferring traffic through VPN tunnels in heterogeneous networks, encapsulating Ethernet frames with the help of GRE protocol and transferring them over a network which uses a network protocol of another level.

≡	VPN Users	EoGRE	
	GRE can configure VPN tunnels based on EoGRE technolo	ygy.	
	can add a tunnel		

Figure 114. The VPN / EoGRE page.

To create a new tunnel, click the **ADD** button (+).

	EoGRE/Adding	
Enable		
Name*	Interface*	
EoGRE	Not selected	•
(i) The number of characters should not exceed 32	мт u* 1400	
Remote IP address*		
Tagged traffic		

Figure 115. The page for adding an EoGRE tunnel.

You can specify the following parameters:

Parameter	Description	
Enable	Move the switch to the right to enable the EoGRE tunnel.	
	Move the switch to the left to disable the EoGRE tunnel.	
NameA name of the tunnel for easier identification. You can specify a name.		
Remote IP address	IP address The IP address of the remote local subnet.	
Tagged trafficMove the switch to the right to assign a tag (VLAN ID) to Ed traffic and specify the needed value in the VLAN ID field display		
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.	
MTU	The maximum size of units transmitted by the interface.	

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

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 ($\overline{\blacksquare}$).

VPN tunnels using EoGRE technology will appear in the **EoGRE interfaces** section on the **Advanced / VLAN** page and will be automatically removed from this section after the tunnel is deleted from the current page.

EoIP

On the **VPN / EoIP** page, you can configure VPN tunnels based on EoIP technology.

EoIP (*Ethernet over IP*) technology allows creating an Ethernet tunnel between two routers via connections which can transmit IP packets (e.g., IPIP, PPTP connections).

	EoIP	
EoIP You can configure VPN tunnels	based on EoIP technology.	
No tunnel created You can add a tunnel	+	

Figure 116. The VPN / EoIP page.

To create a new tunnel, click the **ADD** button (+).

EoIP	EoIP/Adding		
Contraction Contra			
Name*	Interface*		
EoIP	Not selected -		
	MTU*		
Remote IP address*	1400		
Tunnel ID*	Keep Alive		
MAC address			
Tagged			
APPLY			

Figure 117. The page for adding an EoIP tunnel.

You can specify the following parameters:

Parameter	Description
Enable	Move the switch to the right to enable the EoIP tunnel.
Enable	Move the switch to the left to disable the EoIP tunnel.
Name	A name of the tunnel for easier identification. You can specify any name.
Remote IP address	Enter the IP address of the remote local subnet.
	Specify a unique identifier of the tunnel.
Tunnel ID	The value for both parties which establish the tunnel should be the same.
MAC address	A MAC address assigned to the EoIP tunnel interface. Optional.
	If the field is blank, the MAC address is assigned automatically.
TaggedMove the switch to the right to assign a tag (VLAN ID) to traffic and specify the needed value in the Tag ID field displayed	
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.
MTU The maximum size of units transmitted by the interface.	
	Move the switch to the right to let the router detect the state of the tunnel on the other end. In the Interval and Attempts fields displayed, specify the required values.
Keep Alive	The router sends several check requests. If after several failed attempts the connection on the other end of the tunnel is inactive, the tunnel will be disabled. Upon that it will be enabled automatically when the other end tries to establish the connection.
Interval	A time period (in seconds) allocated for one request to check the state of the tunnel on the other end. By default, the value 5 is specified.
A number of failed attempts to check the state of the tunnel of other end after which the tunnel is disabled. By default, the val is specified.	

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

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 ($\boxed{10}$).

VPN tunnels using EoIP technology will appear in the **EoIP interfaces** section on the **Advanced / VLAN** page and will be automatically removed from this section after the tunnel is deleted from the current page.

Wi-Fi

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

Basic Settings

In the **Wi-Fi** / **Basic Settings** section, you can change basic parameters for the wireless interface of the router and configure the basic and additional wireless networks. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

≡	K EOIP B	asic Settings
	2.4 GHz	5 GHz
	sic Settings can change basic parameters for the wireless interface o	f the device.
	🔵 Enable Wireless 🕓	Wi-Fi Network
Cour	ntry	Network name (SSID)*
RL	ISSIAN FEDERATION	JIR-XXX
	less mode 2.11 B/G/N mixed	Hide SSID Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect
	Select channel automatically	to manually specify the SSID of the access point
í	The least loaded data transfer channel will be used	BSSID
	Enable additional channels	10:62:eb:2d:c9:3d
		Max associated clients*
avaii	Attention! The device automatically selects a channel from the list able channels depending on your country. Make sure that your wire ces support channels above 12	0
Char		Enable shaping
aut	o (channel 1)	Shaping (Mbit/s)*
() ()	Enable periodic scanning The device will periodically check the channels load and switch to t	0 Broadcast wireless network
least	loaded one	() Allows you to enable/disable broadcast of this SSID without disconnecting
Scan	ning period (in seconds)	the wireless module of the router. Can be used with the mode "Wi-Fi Client"
0		Clients isolation
		(i) Block traffic between devices connected to the access point

Figure 118. Basic settings of the wireless LAN in the 2.4GHz band.

In the **Basic Settings** section, the following parameters are available:

Parameter	Description
	To enable Wi-Fi connection, move the switch to the right.
	To disable Wi-Fi connection, move the switch to the left.
	To enable/disable Wi-Fi connection on a schedule, click the Set schedule icon (). In the opened window, from the Rule drop- down list, select the Create rule value to create a new schedule (see the <i>Schedule</i> section, page 228) or select the Select an existing one value to use the existing one. Existing schedules are displayed in the Rule name drop-down list.
Enable Wireless	To enable Wi-Fi connection at the time specified in the schedule and disable it at the other time, select the Enable wireless connection value from the Action drop-down list and click the SAVE button.
	To disable Wi-Fi connection at the time specified in the schedule and enable it at the other time, select the Disable wireless connection value from the Action drop-down list and click the SAVE button.
	To change or delete the schedule, click the Edit schedule icon
	(\bigcirc). In the opened window, change the parameters and click the SAVE button or click the DELETE FROM SCHEDULE button.
Country	The country you are in. Select a value from the drop-down list.
Wireless mode	Operating mode of the wireless network of the router. This parameter defines standards of the devices that will be able to use your wireless network. Select a value from the drop-down list.
Select channel automatically	Move the switch to the right to let the router itself choose the channel with the least interference.
Enable additional channels	If the switch is moved to the left, the device automatically selects one of available standard channels. To use additional channels (the 12th and 13th – in the 2.4 GHz band, the 100th and higher – in the 5 GHz band), move the switch to the right.
	The wireless channel number.
Channel	To select a channel manually, left-click; in the opened window, select a channel and click the SAVE button. The action is available, when the Select channel automatically switch is moved to the left.

Parameter	Description	
Enable periodic scanning	Move the switch to the right to let the router search for a free channel in certain periods of time. When the switch is moved to the right, the Scanning period field is available for editing.	
Scanning period	Specify a period of time (in seconds) after which the router rescans channels.	

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

To edit the settings of the basic wireless network, in the **Wi-Fi Network** section, change the needed parameters and click the **APPLY** button.

Also you can create an additional wireless network. To do this, click the **ADD WI-FI NETWORK** button. On the opened page, specify the relevant parameters.

	Add Wi-Fi Network	
Wi-Fi Network	Security Settings	
Network name (SSID)*	Network authentication	
DIR-XXX.2	WPA2-PSK	•
Hide SSID	Password PSK*	
() Inde 5515	······	Q
Wireless network name (SSID) will not appear in the list of avail networks with customers. Go to a hidden network, you can connect to specify the SSID of the access point		
Max associated clients*	Encryption type*	
0	AES	•
Enable shaping	Group key update interval (in seconds)* 3600	
Broadcast wireless network	802.11w (Protected Management Frames)	
Allows you to enable/disable broadcast of this SSID without disc wireless module of the router. Can be used with the mode "Wi-Fi Clie	connecting the Disabled	•
Clients isolation		
(i) Block traffic between devices connected to the access point		
Enable guest network		
(i) Enable the guest network in order to isolate Wi-Fi clients from the	he LAN network	
APPLY		

Figure 119. Creating a wireless network.

Parameter	Description	
Wi-Fi Network		
Network name (SSID) A name for the wireless network.		

Description
If the switch is moved to the right, other users cannot see your Wi-Fi network. It is recommended not to hide the network in order to simplify initial configuration of the wireless network.
The unique identifier for this wireless network. You cannot change the value of this parameter, it is determined in the device's internal settings. The field is displayed in the settings of the existing wireless network.
The maximum number of devices connected to the wireless network. When the value 0 is specified, the device does not limit the number of connected clients.
Move the switch to the right to limit the maximum bandwidth of the wireless network. In the Shaping field displayed, specify the maximum value of speed (Mbps). Move the switch to the left not to limit the maximum bandwidth.

Parameter	Description
	If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DIR-X1530 can connect to another access point as a wireless client.
	To enable/disable broadcasting on a schedule, click the Set schedule icon (③). In the opened window, from the Rule drop-
	down list, select the Create rule value to create a new schedule (see the <i>Schedule</i> section, page 228) or select the Select an existing one value to use the existing one. Existing schedules are displayed in the Rule name drop-down list.
Broadcast wireless network	To enable broadcasting at the time specified in the schedule and disable it at the other time, select the Enable wireless network broadcasting value from the Action drop-down list and click the SAVE button. When the wireless connection is disabled, the device will not be able to enable broadcasting of this wireless network on schedule.
	To disable broadcasting at the time specified in the schedule and enable it at the other time, select the Disable wireless network broadcasting value from the Action drop-down list and click the SAVE button.
	To change or delete the schedule, click the Edit schedule icon
	(\bigcirc). In the opened window, change the parameters and click the SAVE button or click the DELETE FROM SCHEDULE button.
	If you created an additional network, you can configure, change or delete a schedule for each network. To do this, click the icon in the line of the network.
Clients isolation	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
Enable guest network	This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.

In the Security Settings section, you can change security settings of the wireless network.

By default, the **WPA2-PSK** network authentication type of both bands of the wireless network is specified. WPS PIN from the barcode label is used as the network key.

letwork authentication	
WPA2-PSK	•
Open	
WEP	
WPA	
WPA-PSK	
WPA2 WPA2-PSK	
WPA2-PSK WPA/WPA2 mixed	
WPA-PSK/WPA2-PSK mixed	
WPA3-SAE	
WPA2-PSK/WPA3-SAE mixed	
iroup key update interval (in seconds)*	
roup key update interval (in seconds)* 600	

Figure 120. Network authentication types supported by the router.

The router supports the following authentication types:

Authentication type	Description
Open	Open authentication (with WEP encryption for wireless network modes not supporting 802.11n or 802.11ac devices).
WEP	Authentication with a shared key with WEP encryption. This authentication type is not available when a mode supporting 802.11n or 802.11ac devices is selected from the Wireless mode drop-down list on the Wi-Fi / Basic Settings page.
WPA	WPA-based authentication using a RADIUS server.
WPA-PSK	WPA-based authentication using a PSK.
WPA2	WPA2-based authentication using a RADIUS server.
WPA2-PSK	WPA2-based authentication using a PSK.
WPA/WPA2 mixed	A mixed type of authentication. When this value is selected, devices using the WPA authentication type and devices using the WPA2 authentication type can connect to the wireless network.
WPA-PSK/WPA2-PSK mixed	A mixed type of authentication. When this value is selected, devices using the WPA-PSK authentication type and devices using the WPA2-PSK authentication type can connect to the wireless network.
WPA3-SAE WPA3-based authentication using a PSK and SAE me	

Authentication type	Description
WPA2-PSK/WPA3-SAE mixed	A mixed type of authentication. When this value is selected, devices using the WPA2-PSK authentication type and devices using the WPA3-SAE authentication type can connect to the wireless network.

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

When the **Open** or **WEP** value is selected, the following settings are displayed on the page (unavailable for the wireless network operating modes which support the standard 802.11n or 802.11ac):

Open	
Enable encryption WEP	
•	
Default key ID 1	
with many devices.	
Length of WEP key should be 5 or 13 characters.	
① Length of WEP key should be 5 or 13 characters.	
Length of WEP key should be 5 or 13 characters. Encryption key 1*	;

Figure 121. The **Open** value is selected from the **Network authentication** drop-down list.

Parameter	Description
	For Open authentication type only.
Enable encryption WEP	To activate WEP encryption, move the switch to the right. Upon that the Default key ID drop-down list, the Encryption key WEP as HEX switch, and four Encryption key fields are displayed on the page.
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the Default key ID drop-down list. It is required to specify all the fields. Click the Show icon () to display the entered key.

When the WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK mixed, WPA3-SAE, or WPA2-PSK/WPA3-SEA mixed value is selected, the following fields are displayed on the page:

Security Settings	
Network authentication	
WPA2-PSK	•
Password PSK*	
	Ø
Password should be between 8 and 63 ASCII characters	
Encryption type*	
AES	•
Group key update interval (in seconds)*	
3600	
3600 802.11w (Protected Management Frames)	

Figure 122. The WPA2-PSK value is selected from the Network authentication drop-down list.

Parameter	Description	
Password PSK	A password for WPA encryption. The password can contain digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout. ⁵ Click the Show icon ((()) to display the entered password.	

^{5 0-9,} A-Z, a-z, space, !"#%&'()*+,-./:;<=>?@[\]^_`{|}~.

Parameter	Description	
Encryption type	An encryption method: TKIP , AES , or TKIP+AES . TKIP and TKIP+AES encryption types are not available for WPA3-SAE and WPA2-PSK/WPA3-SAE mixed authentication types.	
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed.	
802.11w (Protected	 For WPA2-PSK, WPA3-SAE, and WPA2-PSK/WPA3-SAE mixed authentication types only. Protected Management Frames help to improve packet privacy protection for wireless data transmission. Select a value for the wireless network from the drop-down list. Disabled: Protected Management Frames are not used. 	
Management Frames)	 Optional: Protected Management Frames are optional. Required: Protected Management Frames are required. When this value is selected, devices not supporting the 802.11w standard cannot connect to the wireless network. The default value cannot be changed for WPA3-SAE and WPA2- PSK/WPA3-SAE mixed authentication types. 	

When the **WPA**, **WPA2**, or **WPA/WPA2 mixed** value is selected, the following settings are displayed on the page:

Secu	rity Settings
Network	authentication
WPA2	-
	WPA2 Pre-authentication
IP addre	ss RADIUS server*
192.16	88.0.254
RADIUS	server port*
1812	
RADIUS	encryption key*
dlink	
Encryptic	on type*
AES	•
Group ke	ey update interval (in seconds)*
3600	
802.11w	(Protected Management Frames)
Disab	led 🗸

Figure 123. The WPA2 value is selected from the Network authentication drop-down list.

Parameter	Description		
WPA2 Pre- authentication	Move the switch to the right to activate preliminary authentication (displayed only for the WPA2 and WPA/WPA2 mixed authentication types).		
IP address RADIUS server	The IP address of the RADIUS server.		
RADIUS server port	A port of the RADIUS server.		
RADIUS encryption key	The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings).		
Encryption type	An encryption method: TKIP , AES , or TKIP+AES .		
Group key update interval	The time period (in seconds), at the end of which a new key for WPA encryption is generated. When the value 0 is specified for this field, the key is not renewed.		

Parameter	Description	
802.11w (Protected Management Frames)	 For WPA2 authentication type only. Protected Management Frames help to improve packet privacy protection for wireless data transmission. Select a value for the wireless network from the drop-down list. Disabled: Protected Management Frames are not used. Optional: Protected Management Frames are optional. Required: Protected Management Frames are required. When this value is selected, devices not supporting the 802.11w standard cannot connect to the wireless network. 	

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

To edit the basic or additional wireless network, left-click the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

To remove the additional network, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ($\boxed{10}$). Then click the **APPLY** button.

Client Management

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

		Client Man	agement		
Client Manageme You can view the list of wire		he router.			
List of Wi-Fi Clients	REFRESH DISCONNEC	т			
Hostname	MAC address	Band	Network name (SSID)	Signal level	Online
MI6-MiPhone	50:8F:4C:E3:9E:50	2.4 GHz	DIR-XXX	 100%	0 min

Figure 124. The page for managing the wireless clients.

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

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

To view the latest data on a connected device, left-click the line containing the MAC address of this device.

WPS

On the **Wi-Fi / WPS** page, you can enable the function for configuration of the WLAN and select a method for connection to the WLAN.

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

The WPS function allows adding devices only to the basic wireless network of the router.

Before using the function you need to configure one of the following authentication types:
 Open with no encryption, WPA2-PSK or WPA-PSK/WPA2-PSK mixed with the AES encryption method. When other security settings are specified, controls of the WPS page on the tab of the relevant band are not available.

Client Management	WPS	
2.4 GHz	5 GHz	
WPS The WPS function helps to automatically connect to the wireles DISABLE WPS	is network of the router. The connecting devices m	ust support this function.
WPS Control	Information	
	WPS state:	Configured
ESTABLISH CONNECTION	Default PIN code:	12345670
-	Network name (SSID):	DIR-XXX
Enable WPS function with hardware button	Network authentication:	WPA2-PSK
Move the switch to the left in order to forbid enabling the WPS function with the relevant hardware button	ith Encryption:	AES
	Password PSK:	12345670
	UPDATE	

Figure 125. The page for configuring the WPS function.

You can activate the WPS function via the web-based interface or the hardware **WPS** button on the cover of the device.

To activate the WPS function via the hardware button, move the **Enable WPS function with** hardware button switch to the right on the tabs of both bands. Then, with the device turned on, press the WPS the button, hold it for 2 seconds, and release. The WLAN 2.4G and WLAN 5G LEDs should start blinking. In addition, upon pressing the button, the wireless interfaces of the device are enabled if they were disabled before.

If you want to disable activating the WPS function via the hardware button, on the tabs of both bands, move the **Enable WPS function with hardware button** switch to the left and make sure that the WPS function is not activated via the web-based interface.

To activate the WPS function via the web-based interface, on the tab of the relevant band, click the **ENABLE WPS** button.

Parameter	Description	
	The state of the WPS function:	
WPS state	• Configured (all needed settings are specified; these settings will be used upon establishing the wireless connection)	
	• Unconfigured (after activating the WPS function, the SSID and the encryption key will be configured automatically, the network authentication type will be changed to WPA2-PSK).	
Default PIN code	The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function.	
Network name (SSID)	The name of the router's wireless network.	
Network authentication	The network authentication type specified for the wireless network.	
Encryption	The encryption type specified for the wireless network.	
Password PSK	The encryption password specified for the wireless network.	
UPDATE	Click the button to update the data on the page.	

When the WPS function is enabled, the **Information** section is available on the page.

Using WPS Function via Web-based Interface

To connect to the basic wireless network via the PIN method of the WPS function, follow the next steps:

- 1. Click the **ENABLE WPS** button.
- 2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.
- 3. In the opened window, select the **PIN** value from the **WPS method** drop-down list.
- 4. Select the PIN method in the software of the wireless device that you want to connect to the router's WLAN.
- 5. Click the relevant button in the software of the wireless device that you want to connect to the WLAN.
- 6. Right after that, enter the PIN code specified on the cover of the wireless device or in its software in the **PIN code** field.
- 7. Click the **CONNECT** button in the web-based interface of the router.

To connect to the basic wireless network via the PBC method of the WPS function, follow the next steps:

- 1. Click the **ENABLE WPS** button.
- 2. In the **WPS Control** section, click the **ESTABLISH CONNECTION** button.
- 3. In the opened window, select the **PBC** value from the **WPS method** drop-down list.
- 4. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
- 5. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
- 6. Right after that, click the **CONNECT** button in the web-based interface of the router.

Using WPS Function without Web-based Interface

You can use the WPS function without accessing the web-based interface of the router. To do this, you need to configure the following router's settings:

- 1. Specify relevant security settings for the wireless network of the router.
- 2. Make sure that the **Enable WPS function with hardware button** switch is moved to the right on the tabs of both bands.
- 3. Click the **ENABLE WPS** button.
- 4. Close the web-based interface (click the **Logout** line of the menu).

Later you will be able to add wireless devices to the WLAN by pressing the **WPS** button of the router.

- 1. Select the PBC method in the software of the wireless device that you want to connect to the router's WLAN.
- 2. Click the relevant button in the software or press the WPS button on the cover of the wireless device that you want to connect to the WLAN.
- 3. Press the **WPS** the button, hold it for 2 seconds, and release. The **WLAN 2.4G** and **WLAN 5G** LEDs should start blinking.

Client

On the **Wi-Fi** / **Client** page, you can configure the router as a client to connect to a wireless access point or to a WISP. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

< wmm		Client		
2.4	łGHz		5GHz	
Wi-Fi Client	s a client to connect to a wire	less access point or to a WISP.		
Enable				
Broadcast wireless r If the broadcast switch is moved router's WLAN. Upon that the router wireless client.	d to the left, devices cannot conne			
Connecting to network Select network from list		•		
APPLY				
Wireless Networks	UPDATE LIST			
Network name (SSID)		Security Settings	Ch	annel
ᅙ RT-WiFi-799C		[WPA2-PSK/WPA3-SAE mixed] [AES]		10
🗟 [SDK2] DIR-620-209	7	[WPA2-PSK] [AES]		9

Figure 126. The page for configuring the client mode.

To configure the router as a client, move the **Enable** switch to the right. Upon that the following fields are displayed on the page:

Parameter	Description
Broadcast wireless network 2.4 GHz / Broadcast wireless network 5 GHz	If the switch is moved to the left, devices cannot connect to the router's WLAN. Upon that the router can connect to another access point as a wireless client.
Connecting to network	A method for connecting to another access point.

In the **Wireless Networks** section, the list of available wireless networks is displayed. To view the latest data on available wireless networks, click the **UPDATE LIST** button.

To connect to a wireless network from the list, select the needed network. Move the **Network options** switch to the right to view more detailed information on the network to which the router connects. If a password is required, enter it in the relevant field. Click the **CONNECT** button.

To connect to a hidden network, select the **Connect to hidden network** value from the **Connecting to network** drop-down list. Enter the name of the network in the **Network name** (SSID) field. If needed, fill in the **BSSID** field. Then select the needed type of authentication from the **Network authentication** drop-down list.

When the **Open** or **WEP** authentication type is selected, the following settings are displayed on the page:

Parameter	Description	
	For Open authentication type only.	
Enable encryption WEP	To activate WEP encryption, move the switch to the right. Upon that the Default key ID drop-down list, the Encryption key WEP as HEX switch, and four Encryption key fields are displayed on the page.	
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.	
Encryption key WEP as HEX	Move the switch to the right to set a hexadecimal number as a key for encryption.	
Encryption key (1-4)	Keys for WEP encryption. The router uses the key selected from the Default key ID drop-down list. It is required to specify all the fields. Click the Show icon () to display the entered key.	

When the WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK mixed, WPA3-SAE, and WPA2-PSK/WPA3-SAE mixed authentication type is selected, the following fields are displayed:

Parameter	Description
Password PSK	A password for WPA encryption. Click the Show icon (\bigotimes) to display the entered key.
	An encryption method: TKIP , AES , or TKIP+AES .
Encryption type	TKIP and TKIP+AES encryption types are not available for WPA3-SAE and WPA2-PSK/WPA3-SAE mixed authentication types.

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

When connecting to a wireless access point, the wireless channel of DIR-X1530 will switch to the channel of the access point to which you have connected.

In addition, the **Connection Information** section in which you can view the connection status and the network basic parameters is displayed.

If you want to connect to the WISP network, after configuring the device as a client, you need to create a WAN connection with relevant parameters for the **WiFiClient_2GHz** interface in the 2.4GHz band or for the **WiFiClient_5GHz** interface in the 5GHz band.

Additional

On page of the **Wi-Fi** / **Additional** section, you can define additional parameters for the WLAN of the router. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

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

∃ 	itional	P
2.4 GHz	5 GHz	
Wi-Fi Additional Settings		
You can define additional parameters for the WLAN of the router.		
Bandwidth	B/G protection	
Auto -	Auto	•
(i) Using bandwidth of one or several channels of the wireless network	Short GI	
simultaneously	Enable	•
① Current bandwidth: 40 MHz	Beacon period (in milliseconds)*	
Autonegotiation 20/40 (Coexistence)	100	
Automatic change of bandwidth in the loaded environment	RTS threshold (in bytes)*	
TX power (in percent)	2347	
100 -	Frag threshold (in bytes)*	
	2346	
	DTM arrived (in based former)#	
	DTIM period (in beacon frames)* 1	
	Station Keep Alive (in seconds)* 0	
APPLY		

Figure 127. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description	
	The channel bandwidth for 802.11n standard in the 2.4GHz band (the 2.4 GHz tab).	
	• 20 MHz : 802.11n clients operate at 20MHz channels.	
	• 20/40 MHz : 802.11n clients operate at 20MHz or 40MHz channels.	
	• Auto : The router automatically chooses the most suitable channel bandwidth for 802.11n clients.	
Bandwidth	The channel bandwidth for 802.11n and 802.11ac standards in 5GHz band (the 5 GHz tab).	
	• 20 MHz : 802.11n and 802.11ac clients operate at 20MHz channels.	
	• 20/40 MHz : 802.11n and 802.11ac clients operate at 20MHz or 40MHz channels.	
	• 20/40/80 MHz : 802.11ac clients operate at 20MHz, 40MHz, or 80MHz channels.	
	• Auto : The router automatically chooses the most suitable channel bandwidth for 802.11n and 802.11ac clients.	
	Available on the 2.4 GHz tab.	
Autonegotiation 20/40 (Coexistence)	Move the switch to the right to let the router to automatically choose the most suitable channel bandwidth (20MHz or 40MHz) for the connected devices (this setting can substantially lower the data transfer rate of your wireless network). The switch is displayed when the 20/40 MHz or Auto value is selected from the Bandwidth drop-down list.	
TX power	The transmit power (in percentage terms) of the router.	
	Available on the 5 GHz tab.	
Enable DFS	Move the switch to the right to enable the DFS (<i>Dynamic Frequency Selection</i>) mechanism. Upon that the router uses the channels at which radars and other mobile or stationary radio systems can operate, but switches to other channels if these devices require this. In order to use the DFS mechanism, the automatic channel selection should be enabled (on the Wi-Fi / Basic Settings page).	
	Move the switch to the left not to let the router use the channels at which radars and other mobile or stationary radio systems can operate.	

Parameter	Description		
/	<i>Available on the</i> 5 GHz <i>tab.</i> TX Beamforming is the signal processing/directing technique which		
Enable TX Beamforming	helps to support a high enough transfer rate in the areas with difficult conditions for the signal propagation.		
	Move the switch to the right to improve the signal quality.		
	Available on the 5 GHz tab.		
OFDMA ⁶	OFDMA (<i>Orthogonal frequency-division multiple access</i>) is a Wi-Fi 6 standard technology, that improves performance of wireless networks with a large number of clients by establishing subcarriers with independent modulations.		
	Move the switch to the right to improve the network performance.		
	Available on the 5 GHz tab.		
тwт	TWT <i>(Target Wake Time)</i> is a Wi-Fi 6 standard technology, that allows to negotiate wireless devices' wake-up time for data exchange with the router and to conserve their battery life.		
	Move the switch to the right to save the battery power for the connected wireless devices.		
	Available on the 2.4 GHz tab.		
	The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network.		
	Select a value from the drop-down list.		
B/G protection	• Auto : The protection function is enabled and disabled automatically depending on the state of the network (this value is recommended if your wireless local area network consists of both 802.11b and 802.11g devices).		
	• Always On : The protection function is always enabled (this setting can substantially lower the efficiency of your wireless network).		
	• Always Off: The protection function is always disabled.		

⁶ Correct operation of the thechnology will be implemented in the next firmaware version.

Parameter	Description	
	Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices.	
Short GI	• Enable : The router uses the 400 ns short guard interval. Only for the wireless network operating modes which support 802.11n and 802.11ac standards (see the value of the Wireless mode drop-down list on the Wi-Fi / Basic Settings page).	
	• Disable : The router uses the 800 ns standard guard interval.	
Beacon period	The time interval (in milliseconds) between packets sent to synchronize the wireless network.	
RTS threshold	The minimum size (in bytes) of a packet for which an RTS frame is transmitted.	
Frag threshold	The maximum size (in bytes) of a non-fragmented packet. Larger packets are fragmented (divided).	
DTIM period	The number of beacon frames between sending DTIM messages (messages notifying on broadcast or multicast transmission).	
Station Keep Alive	The time interval (in seconds) between keep alive checks of wireless devices from your WLAN. When the value 0 is specified, the checking is disabled.	

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

MAC Filter

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

It is recommended to configure the Wi-Fi MAC filter through a wired connection to DIR-X1530.

≡	✔ Additional	MAC Filter	
	C Filter		
	n will not be allowed to	C addresses of devices which will be allowed to access the WLAN, or define MAC addresses of devices to access the WLAN.	
4	1t is recommend	ded to configure the Wi-Fi MAC filter through a wired connection to the device	
2.4	GHz	5 GHz	
	R-XXX) Off	DIR-XXX-5G (i) Off	
Filte No ru	ers +	filter	

Figure 128. The page for configuring the MAC filter for the wireless network.

By default, the Wi-Fi MAC filter is disabled.

To configure the MAC filter, first you need to create rules (specify MAC addresses of devices for which the specified filtering modes will be applied). To do this, click the **ADD** button (+).

Add Rule	×
Frequency band 2.4 GHz	_
SSID	-
DIR-XXX	•
(i) MAC filters for this network are disabled	
MAC address*	•
Name*	
() The number of characters should not exceed 32	
Enable	
SAVE	

Figure 129. The window for adding a rule for the MAC filter.

You can specify the following parameters:

Parameter	Description
Frequency band	From the drop-down list, select a band of the wireless network.
SSID	A wireless network to which the rule will be applied. Select the needed value from the drop-down list.
MAC address	In the field, enter the MAC address to which the selected filtering mode will be applied.
Hostname	The name of the device for easier identification (<i>optional</i>). You can specify any name.
Enable	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.

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

To edit the parameters of the existing rule, in the **Filters** section, left-click the needed rule. In the opened window, change the settings and click the **SAVE** button.

To remove the rule from the page, in the **Filters** section, select the checkbox located to the left of the relevant rule and click the **DELETE** button ($\boxed{10}$).

After creating the rules you need to configure the filtering modes.

To open the basic or additional wireless network for the devices which MAC addresses are specified on this page and to close the wireless network for all other devices, in the section corresponding to the band (**2.4 GHz** or **5 GHz**), left-click the line of the wireless network. In the opened window, move the **Enable MAC filter** switch to the right. Upon that the **MAC filter restrict mode** drop-down list will be displayed. Select the **Allow** value from the drop-down list and click the **SAVE** button.

To close the wireless network for the devices which MAC addresses are specified on this page, select the **Deny** value from the **MAC filter restrict mode** drop-down list and click the **SAVE** button.

To set a schedule for the MAC filter rule, click the **Set schedule** icon (()) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 228) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the MAC filter rule at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the MAC filter rule at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

To change or delete the schedule for a rule, click the **Edit schedule** icon (\bigcirc) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

Advanced

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

- create or edit VLANs
- use any LAN port of the router as WAN port
- add name servers
- configure a DDNS service
- configure autonegotiation or manually configure speed and duplex mode for each Ethernet port of the router
- configure notifications on the reason of the Internet connection failure
- define static routes
- configure TR-069 client
- enable the function of mirroring the router's ports
- enable the UPnP function
- enable the built-in UDPXY application for the router
- allow the router to use IGMP
- allow the router to use RTSP, enable the SIP ALG, the PPPoE/PPTP/L2TP/IPsec pass through functions for the router
- configure the CoovaChilli service.

VLAN

On the **Advanced / VLAN** page, you can edit existing and create new virtual networks (VLAN), e.g., for distinguishing traffic or specifying additional WAN interfaces.

By default, 2 VLANs are created in the router's system.

- **LAN**: For the LAN interface, it includes LAN ports and Wi-Fi networks. You cannot delete this VLAN.
- **WAN**: For the WAN interface; it includes the **INTERNET** port. You can edit or delete this VLAN.

≡	< MAC Filter	VLAN		
VLA				
	N List +	-	iterfaces and ports of tr	he router, for example, for distinguishing different types of traffic.
	VLAN ID	Name	Tagged Ports	Untagged ports
	-	LAN	-	DIR-XXX, DIR-XXX-5G, LAN1, LAN2, LAN3
	-	WAN	-	WAN

Figure 130. The Advanced / VLAN page.

In order to add untagged LAN ports or available Wi-Fi networks to an existing or new VLAN, first you need to exclude them from the **LAN** network on this page. To do this, select the **LAN** line. On the opened page, from the **Type** drop-down list of the element corresponding to the relevant LAN port or Wi-Fi network, select the **Excluded** value and click the **APPLY** button.r

To create a new VLAN, click the **ADD** button (+).

🗮 < VLAN	VLAN/	Adding			
VLAN Name*			ate Interface n the bridge	e" function is disabled, th e mode and packets pass	
VLAN ID*			reate inter	face	
QoS* O					
Ports	IIIIIIII LAN2			LAN1	
Type Tagged •	Type Excluded		•	Type Excluded	
WAN Type Excluded -					
Wireless interfaces					
DIR-XXX-5G Type Excluded	DIR-XXX Type Excluded	•			
APPLY					

Figure 131. The page for adding a VLAN.

You can specify the following parameters:

Parameter	Description		
Name	A name for the VLAN for easier identification.		
VLAN ID	An identifier of the VLAN.		
QoS	A priority tag for the transmitted traffic.		
Create interface	Move the switch to the right to create an interface that can be used for creating WAN connections.		
oreate interface	Move the switch to the left for the VLAN to work in the bridge mode. This mode is mostly used to connect IPTV set-top boxes.		

Parameter	Description		
	Select a type for each port included in the VLAN.		
	• Untagged : Untagged traffic will be transmitted through the specified port.		
Ports	• Tagged : Tagged traffic will be transmitted through the specified port. If at least one port of this type is included to the VLAN, it is required to fill in the VLAN ID and QoS fields.		
	Leave the Excluded value for the ports not included in the VLAN.		
Wireless interfaces	Select the Untagged value for each Wi-Fi interface included in the VLAN.		
	Leave the Excluded value for the Wi-Fi interfaces not included in the VLAN.		

Click the **APPLY** button.

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

To remove an existing VLAN, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ($\boxed{10}$).

WAN Remapping

On the **Advanced / WAN Remapping** page, you can use any LAN port the router to connect to a private Ethernet line.

😑 < VLAN	WAN Remapping	
WAN Remapp	aina	
	I port of the router to access the Internet via Ethernet technology.	
To use the router's L	AN port as the WAN port, click the icon corresponding to this port and click the Apply button.	
To disconnect the LA	N port from the private Ethernet line, click the port icon and click the Apply button.	
APPLY		

Figure 132. The Advanced / WAN Remapping page.

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

If in the future you need to disconnect the LAN port from the private Ethernet line, click the icon highlighted in teal and click the **APPLY** button.

DNS

	AN	DNS	
DNS			
DNS servers addresses of		e IP address from the name of a server in Intranets of configure the router to obtain DNS servers addresse	
IPv4		IPv6	
Mar	nual	🔵 Manual	
🛑 Defa	ault gateway	Default gateway	
Interface		Interface	
statip_81		6	
Designed to	Prvers be used by the local netw	ork clients.	
Name Se Designed to IPv4 1.1.1.1	be used by the local netw	ork clients.	
Designed to			
Designed to IPv4 1.1.1.1	be used by the local netw		
Designed to IPv4 1.1.1.1 1.0.0.1	be used by the local netw		
Designed to IPv4 1.1.1.1 1.0.0.1 ADD SERVI Reserve S	be used by the local netwood of the local netwo		omatically are unavailable.
Designed to IPv4 1.1.1.1 1.0.0.1 ADD SERVI Reserve S	be used by the local netwood of the local netwo		omatically are unavailable.
Designed to IPv4 1.1.1.1 1.0.0.1 ADD SERVI Reserve S Designed to	be used by the local netwo ER Servers be used by the router who	en the addresses specified manually or obtained auto	omatically are unavailable.
Designed to IPv4 1.1.1.1 1.0.0.1 ADD SERVI Reserve S Designed to IPv4	be used by the local netwo ER Servers be used by the router who	en the addresses specified manually or obtained auto	matically are unavailable.

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

Figure 133. 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 router to obtain DNS servers addresses automatically from your ISP upon installing a connection. Also here you can specify addresses of reserve DNS servers which the router can use if the addresses specified manually or obtained automatically are unavailable.

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

Specify needed settings for IPv4 in the **IPv4** section and for IPv6 in the **IPv6** section.

If you want to configure automatic obtainment of DNS servers addresses, move the **Manual** switch to the left. 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 router to use the default WAN connection to obtain addresses of DNS servers, move the **Default gateway** switch to the right.

To specify a DNS server manually, move the **Manual** switch to the right. In the **Name Servers** section of the relevant IP version, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server.

To specify a reserve DNS server, in the **Reserve Servers** section of the relevant IP version, click the **ADD SERVER** button, and in the line displayed, enter an IP address of the DNS server.

To remove a DNS server from the page, click the **Delete** icon (\times) in the line of the address.

When all needed settings are configured, 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.

≡	🗙 DNS	DDNS	
	DNS the DDNS page, yo	ou can define parameters of the DDNS service, which allows associating a domain name with dynamic IP addresses	j.
	DNS List	+ ated	

Figure 134. The Advanced / DDNS page.

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

< DDNS A	Add DDNS	
Chable	Username [*]	
Hostname		
For example: host.ru	× Password*	Ø
	Interface*	
ADD HOST	Default gateway	•
DDNS service*	Update period (in minutes)*	
changeip.com	•	
SAVE		

Figure 135. The page for adding a DDNS service.

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

Parameter	Description
Enable	Move the switch to the right to enable DDNS.
	Move the switch to the left to disable DDNS.
	Enter the full domain name registered at your DDNS provider.
Hostname	If you want to use another domain name of this DDNS provider, click the ADD HOST button, and in the line displayed, enter the needed value.
	To remove a domain name, click the Delete icon (×) in the line of the name.
DDNS service	Select the DDNS provider from the drop-down list. If your provider is not in the list, select the Custom provider value and fill in the fields displayed on the page. Specify the DDNS provider name in the Name field, the domain name of the provider's server in the Server field, and the location of settings in the Path field.
Username	The username to authorize for your DDNS provider.
Password	The password to authorize for your DDNS provider. Click the Show icon (\bigotimes) to display the entered password.
Interface	From the drop-down list, select a WAN connection which will be used for DDNS, or leave the Default gateway value.
Update period	An interval (in minutes) between sending data on the router'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. On the opened page, 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 ($\boxed{10}$).

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 router.

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.

< DDNS	Ports Settings			
Ports Set	tings			
		of speed and duplex mode or ma able data flow control in the auto		d duplex mode for each Ethernet
Port	Status	Autonegotiation	Speed	Flow control
LAN3	Disconnected	On	-	
LAN2	Connected	On	1000M-Full	Off
LAN1	Disconnected	On	-	-
WAN	Connected	On	100M-Full	Off

Figure 136. 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.

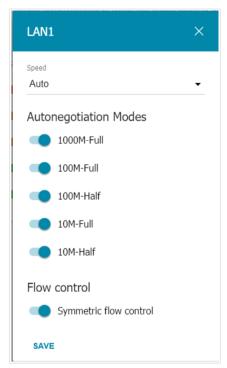


Figure 137. The window for changing the settings of the router's port.

In the opened window, specify the needed parameters:

Parameter	Description	
	Select the Auto value to enable autonegotiation. When this value is selected, the Autonegotiation Modes and Flow control sections are displayed.	
	Select the 10M-Half , 10M-Full , 100M-Half , or 100M-Full value to manually configure speed and duplex mode for the selected port.	
	• 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.	
Speed	• 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.	

Parameter	Description	
Autonegotiation Modes		
To enable the needed data transfer modes, move relevant switches to the right.		
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 router'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.

Ports Settings Redirect	
Redirect	
You can enable notifications on the reason of the Internet connection failure. Notifications will be displayed in the browser we attempting to open a web site on the Internet.	vindow when a user is
DISABLE	
Reasons for Redirect	
Physical connection error	
No connection	
The device is not configured	
APPLY	

Figure 138. The Advanced / Redirect page.

To configure notifications, click the **ENABLE** button. 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).
No connection	Notifications in case of problems of the default WAN connection (authorization error, the IPS's server does not respond, etc.).
The device is not configured	Notifications in case when the device works with default settings.

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

To disable notifications, click the **DISABLE** button.

Routing

On the Advanced / Routing page, you can specify static (fixed) routes.

Redirect	Routing	
Routing		
You can specify static (fixed) routes.		
Routes +		

Figure 139. The Advanced / Routing page.

To specify a new route, click the **ADD** button (+).

Enable	
Protocol*	
IPv4	•
Interface*	
Auto	-
Destination network*	
Destination netmask*	
Gateway*	
Metric	
Table*	
group_1	•

Figure 140. The window for adding a new route.

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

Parameter	Description	
Enable	Move the switch to the right to enable the route.	
	Move the switch to the left to disable the route.	
Protocol	An IP version.	
Interface	From the drop-down list, select an interface (connection) through which the device will communicate with the remote network. If you have selected the Auto value, the router itself sets the interface according to the data on the existing dynamic routes.	
Destination network	A remote network which can be accessed with help of this route. You can specify an IPv4 or IPv6 address.	
	The format of a host IPv6 address is 2001:db8:1234::1 , the format of a subnet IPv6 address is 2001:db8:1234::/64 .	
Destination netmask	For IPv4 protocol only.	
	The remote 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> .	
Table	From the drop-down list, select a routing table for the route.	
	• group_1 table is used to route user traffic.	
	• main table is used to route management traffic from internal system services of the router.	

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 ($\boxed{10}$).

TR-069 Client

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

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

069 Client 🖸	ing TR-06
	69 Client n configure the router for communication with a remote 069 client is used for remote monitoring and managem
Inform Settings	Enable TR-069 client
on	2*
Interval (in seconds) 120	natic -
Connection Request Settings	Configuration Server Settings
Username	Get URL address via DHCP
Password &	ddress
Request port 8999	ame
Ø.	vord &
≷ Request path	PLY

Figure 141. The page for configuring the TR-069 client.

You can specify the following parameters:

Parameter	Description	
	TR-069 Client	
Enable TR-069 client	Enable TR-069 client Move the switch to the right to enable the TR-069 client.	
Interface	The interface which the router 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.	

Parameter	Description	
Inform Settings		
On	Move the switch to the right so the router may send reports (data on the device and network statistics) to the ACS.	
Interval	Specify the time period (in seconds) between sending reports.	
Auto Configuration Server Settings		
Get URL address via DHCP	If the switch is moved to the right, the router obtains the URL address of the ACS upon establishing the Dynamic IP type connection.	
	If you need to specify the URL address manually, move the switch to the left and enter the needed value in the URL address field.	
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. Click the Show icon (\bigotimes) to display the entered password.	
	Connection Request Settings	
Username	The username used by the ACS to transfer a connection request to the router.	
Password	The password used by the ACS. Click the Show icon (\bigotimes) to display the entered password.	
Request port	The port used by the ACS. By default, the port 8999 is specified.	
Request path	The path used by the ACS.	

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

Port Mirroring

On the **Advanced / Port Mirroring** page, you can enable the function of mirroring the router's ports. This function allows to copy traffic from one or several ports to the destination port to monitor network issues with the help of traffic analysis software.

🚍 < TR-069 Client	Port Mirrori	ng	
Port Mirroring You can enable the function of mirrorin destination port to monitor network is: DISABLE		ws to copy traffic from one or several source p ftware.	ports to the
Destination port	-		
Source port			
LAN1 Mode None	LAN2 Mode None -	LAN3 Mode None -	
WAN Mode None -			
APPLY			

Figure 142. The Advanced / Port Mirroring page.

To enable the function, click the **ENABLE** button. Upon that the following settings are available on the page.

Parameter	Description
Destination port	The port of the router to which a copy of traffic from one or several ports will be sent. Select the relevant value from the drop-down list.

Parameter	Description
	Select the mode for each port traffic from which should be copied to the destination port:
	• Both : Copy incoming and outgoing traffic from the source port to the destination port.
Source port	• TX : Copy outgoing traffic from the source port to the destination port.
	• RX : Copy incoming traffic from the source port to the destination port.
	Leave the None value for ports from which it is not required to copy traffic.

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

To disable the function of port mirroring, click the **DISABLE** button.

UPnP IGD

On the **Advanced / UPnP IGD** page, you can enable the UPnP function. The UPnP function allows to automatically create port forwarding rules for applications in the router's LAN requiring a connection from an external network.

≡	Port Mirroring		UPnP IGD		
	PnP IGD	GD protocol. The router u	ises the UPnP IGD protocol for a	utomatic configuration of its parameters	5
for r	network applications re	quiringan incoming conn	ection to the router.		
	'4 IGD				
IP a	ddress	Private port	Public port	Description	
	6 IGD				
IP a	ddress	Private port	Public port	Pinhole ID	

Figure 143. The Advanced / UPnP IGD page.

By default, the UPnP function is enabled. You can also manually add port forwarding rules for network applications on the **Firewall / Virtual Servers** page.

Port forwarding rules will be automatically created only in case the router's default WAN connection uses a public IP address.

When the function is enabled, the following parameters of the router are displayed on the page:

Parameter	Description	
	IPv4 IGD / IPv6 IGD	
Protocol	A protocol for network packet transmission.	
IP address	A port of a client's IP address to which traffic is directed from a	
Private port		
Public port	A public port of the router from which traffic is directed to a client's IP address.	
Description	<i>For IPv4 IGD only.</i> Information transmitted by a client's network application.	

Parameter	Description
Pinhole ID	<i>For IPv6 IGD only.</i> An identifier of the rule created for an incoming connection to the router.

If you want to disable the UPnP function, move the **Enable** switch to the left.

UDPXY

On the **Advanced / UDPXY** page, you can allow the router to use the built-in UDPXY application. The UDPXY application transforms UDP traffic into HTTP traffic. This application allows devices which cannot receive UDP streams to access stream video.

😑 🔇 UPnP IGD	UDPXY 🖸
UDPXY	
	IDPXY application. The UDPXY application transforms UDP traffic into HTTP cannot receive UDP streams to access stream video.
Enable	
Port*	Buffer size for incoming data*
4022	131071
Maximum client number*	Buffer size for data transferred to client*
3	32768
	WAN interface*
	Not selected -
_	
APPLY	

Figure 144. The Advanced / UDPXY page.

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

Upon that the following fields are displayed on the page:

Parameter	Description
Port	The port of the router which the UDPXY application uses.
Maximum client number Maximum number of devices from the router's LAN which served by the application.	
Buffer size for incoming data	Size of intermediate buffer for received data. By default, the minimum acceptable value is specified.
Buffer size for data transferred to client	Size of intermediate buffer for transmitted data. By default, the minimum acceptable value is specified.
WAN interface	From the drop-down list, select a WAN connection which will be used for operation with streaming video.

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

To access the status page of the application, click the **Status** link.

Server Process ID	Accepting clie	ents on	Multicast address	Active clients
1447	192.168.0.1:402	2	192.168.161.235	0
	omplate		Function	
Request 1				
Request 1	•	Relay m	ulticast traffic from mca	st addr:mport
· ·	o/mcast_addr:mport/	,		st_addr:mport

Figure 145. The UDPXY application status page.

IGMP

On the **Advanced / IGMP** page, you can allow the router to use IGMP and specify needed settings.

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.

IGMP	
up Management Protocol is designed to manage multicast traffic in IP-ba	sed networks.
ble	
•	
rnet 👻	
	up Management Protocol is designed to manage multicast traffic in IP-bas ble

Figure 146. The Advanced / IGMP page.

The following elements are available on the page:

Parameter	Description	
	IGMP	
Enable Move the switch to the right to enable IGMP.		
IGMP versionSelect a version of IGMP from the drop-down list.		
Interface	From the drop-down list, select a connection of the Dynamic IPv4 or Static IPv4 type for which you need to allow multicast traffic (e.g. streaming video).	

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

ALG/Passthrough

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

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 router.

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

≡	K IGMP	ALG/Passthrough	
	ALG/Passthrough You can allow the router to use RTSP, enable the S	SIP ALG and PPPoE/PPTP/L2TP/IPsec passthrough functions.	
(SIP	PPPoE passthrough	
(i) Allow traffic over SIP	IPsec passthrough	
(RTSP	L2TP passthrough	
(i) Allow troffic over RTSP	PPTP passthrough	
	APPLY		

Figure 147. The Advanced / ALG/Passthrough page.

The following elements are available on the page:

Parameter	Description
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 router. ⁷
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.

⁷ On the **Connections Setup / WAN** page, create a WAN connection, move the **SIP** switch to the right on the **Advanced / ALG/Passthrough** page, connect an Ethernet cable between a LAN port of the router and the IP phone. Specify SIP parameters on the IP phone and configure it to obtain an IP address automatically (as DHCP client).

Parameter	Description
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.

CoovaChilli

The CoovaChilli service provides authorized Internet access for clients in your corporate or public network. On the **Advanced / CoovaChilli** page, you can add an authorization server.

Configuration	CoovaChilli	
	(+)	
	No server created	
	You can add a server	
	ADD	

Figure 148. The Advanced / CoovaChilli page.

To add an authorization server, click the **ADD** button (+). On the opened page, move the **Enable** switch to the right to enable the CoovaChilli service.

Main S	Settings
Interface*	
Not sele	cted
<u> </u>	want to use a separate LAN port or a Wi-Fi network as the interface r to create another VLAN group for this port or network.
Lease time ((in seconds)
86400	
Logging leve	2
System i	is not efficient
IP addres	55 *
IP addres	SS*
IP addres	5S*

Figure 149. The page for adding an authorization server. The Main Settings section.

In the **Main Settings** section, you can specify the following parameters:

Parameter	Description	
Interface	From the drop-down list, select a physical or virtual interface to be used for the authorization server. In order to specify an additional interface, for example, a separate LAN port or a Wi-Fi network, it is necessary to create another VLAN for this port or network (see the VLAN section, page <i>172</i>).	
Lease time	The interval (in seconds) between sending authorization requests to clients.	
Logging level	Select a type of messages and alerts/notifications to be logged.	
IP address	Specify an IP address of the router to be used for authorized client access.	
Mask	Specify a subnet mask.	
Ping	If the switch is moved to the right, the router responds to ping requests by the IP address specified on this page. For security reasons, it is recommended to disable this function.	
	RADIUS server	
	Primary RADIUS server address*	

RADIUS server
Primary RADIUS server address*
Secondary RADIUS server address
RADIUS encryption key*
RADIUS server port
1813
Authentication port
1812
NASID

Figure 150. The page for adding an authorization server. The **RADIUS server** section.

In the **RADIUS server** section, you can specify the following parameters:

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

Parameter	Description		
RADIUS encryption key	The password which the router uses for communication with the RADIUS server (the value of this parameter is specified in the RADIUS server settings).		
RADIUS server port	A port of the RADIUS server.		
Authentication port	The number of a router port which will be used to connect to the RADIUS server. By default, the value 1812 is specified.		
NASID	A network access server ID (the value of this parameter is specified in the RADIUS server settings).		
	MAC authentication Enable Password		

Suffix

Figure 151. The page for adding an authorization server. The **MAC** authentication section.

In the **MAC authentication**⁸ section, you can specify the following parameters:

Parameter	Description	
Enable	MAC authentication allows the RADIUS server to authorize clients by their MAC addresses. Move the switch to the right to enable MAC authentication.Move the switch to the left to disable MAC authentication.	
Password	If required, specify the password to authenticate clients by their MAC addresses.	
Suffix	Specify a suffix for anonymous MAC authentication.	

⁸ Will be available in future software versions.

Fna	ble CHAP authentication
() If the swit	ch is moved to the left, PAP authentication is used.
Authorization p	ort
3990	
LIANA comio	-*
UAM serve	*
	* ss of the UAM server should start with a protocol. Example:
The addre http://dlink.ru	
The addree http://dlink.ru Access for	ss of the UAM server should start with a protocol. Example:
 The addre http://dlink.ru Access for The list of 	ss of the UAM server should start with a protocol. Example: unauthorized users

Figure 152. The page for adding an authorization server. The **UAM** section.

In the **UAM** section, you can specify the following parameters:

Parameter	Description	
Enable CHAP	Move the switch to the right to enable CHAP authentication.	
authentication	Move the switch to the left to enable PAP authentication (the value of this parameter is specified in the RADIUS server settings).	
Authorization port	The number of a router port which will be used for UAM server authorization. By default, the value 3990 is specified.	
UAM server	Specify the URL of the UAM server which ensures client authorization. The address of the UAM server should start with a protocol. Example: http://dlink.ru	
Access for unauthorized users	Specify the list of resources (separated by a comma) which unauthorized users are allowed to access. Please specify a site address and a port. Example: dlink.ru:80	
UAM encryption key	Specify the UAM authentication encryption key.	

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

After adding an authorization server, on the **Advanced / CoovaChilli** page, in the **Status** section, the current state of the server connection is displayed.

To edit the parameters of a server, left-click 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 in the table and click

the **DELETE** button ($\boxed{10}$).

Firewall

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

- add rules for IP filtering
- create virtual servers
- define a DMZ
- configure the MAC filter
- specify restrictions on access to certain web sites
- enable the function of blocking advertisements
- create rules for remote access to the web-based interface.

IP Filter

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

ALG/Passthrough	IP Filter	
	(+)	
	Filters	
	No rules created for IP filter	
	ADD	

Figure 153. The Firewall / IP Filter page.

```
To create a new rule, click the ADD button (+).
```

🖌 🕻 IP Filter		IP F	ilter/Adding (
General Setting	şs		Source IP address
Enable rule			You can specify a range of IP addresses, a single IP address, or a subnet IP address (for example, 10.10.10.10/24 for IPv4 or 2001:0db8:85a3:08d3:1319:8c2e:0370:7532/64 for IPv6)
Name*			Set as
 The number of charact 	ers should no	t exceed 32	Range or single IP address
Action Allow			Start IPv4 address
Protocol TCP			End IPv4 address
IP version IPv4			•
Direction ^{Source}	Ŧ	Destination WAN	*
Source interface		Destination interface	
Auto		Auto	▼
Destination IP	address		Ports
You can specify a range address (for example, 10.10 2001:0db8:85a3:08d3:1319	0.10.10/24 for		You can specify one port, several ports separated by a comma (for example, 80,90), or a range of ports separated by a colon (for example, 80:90)
Set as Range or single IP a	ddress		■ Destination port
Start IPv4 address			Set source port manually
			_
End IPv4 address			•

Figure 154. 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.	
Name	A name for the rule for easier identification. You can specify any name.	

Parameter	Description	
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.	
Direction	 The direction of network packet transmission to which the rule will be applied. Select the source of the packet direction from the Source drop-down list. WAN: The rule will be applied to the packets transmitted from the external network. LAN: The rule will be applied to the packets transmitted from the local network. GRE: The rule will be applied to the packets transmitted from the GRE tunnel (available if a GRE tunnel has been created on the device). IPIP: The rule will be applied to the packets transmitted from the IPIP tunnel (available if an IPIP tunnel has been created on the device). IPSec: The rule will be applied to the packets transmitted from the IPSec tunnel (available if an IPSec tunnel has been created on the device). PPTP Server: The rule will be applied to the packets transmitted from the PPTP server (available if a PPTP server has been created on the device). L2TP Server: The rule will be applied to the packets transmitted from the L2TP server (available if an L2TP server has been created on the device). Select the destination of the packet direction from the Destination drop-down list. Router: The rule will be applied to the packets transmitted 	
	 to DIR-X1530. WAN: The rule will be applied to the packets transmitted to the external network. 	

Parameter	Description	
	• LAN: The rule will be applied to the packets transmitted to the local network.	
	• GRE : The rule will be applied to the packets transmitted to the GRE tunnel (<i>available if a GRE tunnel has been created on the device</i>).	
	• IPIP : The rule will be applied to the packets transmitted to the IPIP tunnel (<i>available if an IPIP tunnel has been created on the device</i>).	
	• IPsec : The rule will be applied to the packets transmitted to the IPsec tunnel (available if an IPsec tunnel has been created on the device).	
	• PPTP Server : The rule will be applied to the packets transmitted to the PPTP server (<i>available if a PPTP server has been created on the device</i>).	
	• L2TP Server : The rule will be applied to the packets transmitted to the L2TP server (<i>available if an L2TP server has been created on the device</i>).	
	From the Source interface and Destination interface drop- down lists, select source and destination interfaces for which the rule will be applied. Leave the Auto values to apply the rule to all created WAN interfaces.	
	Source IP address	
Set as	Select the needed value from the drop-down list.	
	The source host start IPv4 or IPv6 address.	
Start IPv4 address /	If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank.	
Start IPv6 address	You can choose a device connected to the router'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		
	Destination IP address	

Parameter	Description	
	The destination host start IPv4 or IPv6 address.	
Start IPv4 address /	If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank.	
Start IPv6 address	You can choose a device connected to the router'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 /	The destination host end IPv4 or IPv6 address.	
End IPv6 address	The desunation nost end IPv4 of 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 portA port of the destination IP address. You can specify of several ports separated by a comma, or a range of ports sepa 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 set a schedule for the IP filter rule, click the **Set schedule** icon (()) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 228) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the IP filter rule at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the IP filter rule at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

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

To change or delete the schedule for a rule, click the **Edit schedule** icon (\bigcirc) in the line corresponding to this rule. On the opened page, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click

the **DELETE** button ($\boxed{10}$). 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.

IP Filter	Virtual Servers	
	+	
	Virtual Servers	
	No virtual server exists	
	ADD	

Figure 155. The Firewall / Virtual Servers page.

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

	rvers/Adding
General Settings	Private Network Settings
Name* The number of characters should not exceed 32 Template	Private port* (i) You can specify one port, several ports separated by a comma (for example, 80,90), or a range of ports separated by a colon (for example, 80:90)
Custom Interface <all> Protocol TCP</all>	
 NAT Loopback Public Network Settings Remote IP You can specify a single IP address, or a subnet IP address (for example, 	The following ports are used in remote access settings and other rules for virtual servers: "80" You cannot use them for the current rule.
Remote IP ×	
ADD REMOTE IP Public port* You can specify one port, several ports separated by a comma (for example, 80,90), or a range of ports separated by a colon (for example, 80:90) APPLY	

Figure 156. The page for adding a virtual server.

You can specify the following parameters:

Parameter	Description	
General Settings		
Enable	Move the switch to the right to enable the server.	
	Move the switch to the left to disable the server.	

Parameter	Description	
Name	A name for the virtual server for easier identification. You can specify any name.	
TemplateSelect a virtual server template from the drop-down list, or setCustom to specify all parameters of the new virtual set 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.	
NAT Loopback	NAT LoopbackMove the switch to the right in order to let the users of the router's LAN access the local server using the external IP address of the router or its DDNS name (if a DDNS service is configured). Users from the external network access the router using the same address (or DDNS name).	
	Public Network Settings	
Enter the IP address of the server from the external network.		
Remote IP	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 (\times) in the line of the address.	
Public portA port of the router from which traffic is directed to the IP ad specified in the Private IP field in the Private Network Sett section. You can specify one port or several ports separated comma.		
	Private Network Settings	
Private IP	The IP address of the server from the local area network. To choose a device connected to the router's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).	
Private port	A port of the IP address specified in the Private IP field to which traffic is directed from the Public port . You can specify one port or several ports separated by a comma.	

Click the **APPLY** button.

To set a schedule for a virtual server, click the **Set schedule** icon (\bigcirc) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 228) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the virtual server at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the virtual server at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** 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 change or delete the schedule for a server, click the **Edit schedule** icon (\bigcirc) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

To remove a server, select the checkbox located to the left of the relevant line of the table and click

the **DELETE** button (1). Also you can remove a rule on the editing page.

DMZ

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

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

≡	Virtual Servers	DMZ	
A D cap	MZ MZ is a host or network segment located "between" internal (loca ability to transfer a request coming to a port of the router from t can specify the IP address of the DMZ host.	il) and external (global) networks. In the router, the DMZ implements the he external network to a specified host of the internal network.	
	 Enable () Enable NAT Loopback 		
IP	address*	•	
	APPLY		

Figure 157. 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 router's LAN at the moment, select the relevant value from the drop-down list (the field will be filled in automatically).

Move the **Enable NAT Loopback** switch to the right in order to let the users of the router's LAN access the DMZ host using the external IP address of the router or its DDNS name (if a DDNS service is configured). Users from the external network access the router using the same address (or DDNS name).

Click the **APPLY** button.

Note that when the DMZ is enabled, all traffic coming to a port of the WAN interface of the router is directed to the same port of the specified IP address. Also note that virtual servers have higher priority than the DMZ host. In other words, if there has been created a virtual server that directs traffic from external port 80 to a port of the device from the router's local network, then entering http://router_WAN_IP in the address bar, users of the external network are directed to the specified port and IP address configured for the virtual server, but not to port 80 of the device with the IP address specified on the Firewall / DMZ page. To set a schedule for the DMZ, click the **Set schedule** icon ((). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 228) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the DMZ for the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the DMZ for the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

To change or delete the schedule for the DMZ, click the **Edit schedule** icon (\bigcirc). In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

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 router's LAN.

✔ DMZ	MAC Filter	
MAC Filter		
	s-based filtering for computers of the router's LAN.	
Default mode		
Allow	•	
List of Exceptions No rules created for MAC filter	+	

Figure 158. 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 router's network.

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

Add Rule	×
Enable rule	
Allow	-
MAC address*	•
Name*	
SAVE	

Figure 159. The window for adding a rule for the MAC filter.

In the opened window	you can enacify the following parameters:
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.	
	Select an action for the rule.	
Action	• 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 router'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 router's LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).	
Name	The name of the device for easier identification. You can specify any name.	

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

To set a schedule for the MAC filter rule, click the **Set schedule** icon (\bigcirc) in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 228) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the MAC filter rule at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the MAC filter rule at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and 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 change or delete the schedule for a rule, click the **Edit schedule** icon (\bigcirc) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

To remove a rule, select the checkbox located to the left of the relevant line of the table and click

URL Filter

On the **Firewall / URL Filter** page, you can specify restrictions on access to certain web sites and define devices to which the specified restrictions will be applied.

✓ MAC Filter	L Filter
URL Filter You can specify restrictions on access to certain websites. Rules can be applied to those devices that are added to the list or to all but devices from the list. The Device of the list o	
Address filtering Block listed URLs	Client filtering All but devices from list
Addresses + II URL address Match with template	Clients + II MAC address
APPLY	

Figure 160. The Firewall / URL Filter page.

To enable the URL filter, move the **Enable** switch to the right, then select a mode from the **Address filtering** drop-down list.

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

To specify URL addresses to which the selected filtering mode will be applied, in the **Addresses** section, click the **ADD** button (+). In the opened window, you can specify the following parameters:

Parameter	Description
URL address	A URL address, a part of URL address, or a keyword.
Match with template	 Select a value from the drop-down list. Full: The request address should exactly match the value specified in the field above.
	• End : The request address should end with the value specified in the field above.
	• Partly : The request address should contain the value specified in the field above in any part of it.

Click the **SAVE** button.

To remove a URL address from the list, select the checkbox located to the left of the relevant address in the table and click the **DELETE** button ($\boxed{10}$). Also you can remove an address in the editing window.

To define devices to which the specified restrictions will be applied, select a needed value from the **Client filtering** drop-down list.

- **Devices from list**: when this value is selected, the router applies restrictions only to the devices specified in the **Clients** section;
- All but devices from list: when this value is selected, the router does not apply restrictions to the devices specified in the **Clients** section, but applies restrictions to other devices.

To add a client to the list, in the **Clients** section, click the **ADD** button (+). In the opened window, in the **MAC address** field, enter the MAC address of the device from the LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically) and click the **SAVE** button.

To remove a client from the list, select the checkbox located to the left of the relevant rule of the

table and click the **DELETE** button ($\overline{\square}$). Also you can remove a client in the editing window.

After completing configuration of the URL filter, click the **APPLY** button.

To set a schedule for the URL filter, click the **Set schedule** icon (\bigcirc). In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 228) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the URL filter for the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the URL filter for the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

To change or delete the schedule for URL filter, click the **Edit schedule** icon (\bigcirc) in the **URL Filter** section. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button.

AdBlock

On the **Firewall / AdBlock** page, you can enable the function of blocking advertisements which appear during web surfing.

≡	🕻 URL Filter	AdBl	ock	
	llock ice for blocking ads and malicious websites.			
Com	nmon Settings		URL	
-	Enable		() Here you can add, edit, and remove addresses of files which contain host lists.	
Path				
/tmp		6	ADD	
	Save to the device's memory			
AP	PLY			

Figure 161. The Firewall / AdBlock page.

To enable the advertisements blocking function, in the **Common Settings** section, move the **Enable** switch to the right. Then in the **URL** section, click the **ADD** button and in the line displayed, enter a URL address of a file containing the list of advertising web sites which should be blocked. Click the **APPLY** button and wait while the file is being loaded to the device's memory.

Files saved to the device's memory are updated upon every reboot of the router or its or firmware update. In case the file is not available at that moment, the list of web sites to be blocked will not be received.

If you don't want to use a file for blocking advertisements any longer, click the **Delete** icon (\times) in the line of the URL address of the relevant file. Then click the **APPLY** button.

To disable the advertisements blocking function, move the **Enable** switch to the left and click the **APPLY** button.

Remote Access

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

≡	🗙 AdBlock	Remote Access	
You	emote Access u can configure access to the web-based interface of t ed to allow access to the router from the external net	he router. By default, the access from external networks to the router is closed. If yo vork, create relevant rules.	u
	Iles + rules created for remote access		

Figure 162. The Firewall / Remote Access page.

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

Add I	Rule	×
	Enable	
Name*		
() The	number of characters should not exceed 32	
Interface	1	
Autom	atic	•
IP versio	n	
IPv4		•
	Open access from any external	
IP add	host	
	host	
IP add	host ress*	
IP add	host ress*	
IP add Mask* Public po	host ress*	
IP add Mask* Public po 80	host ress*	•

Figure 163. The window for adding a rule for remote management.

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

Parameter	Description
Enable	Move the switch to the right to enable the rule.
	Move the switch to the left to disable the rule.
Name	A name for the rule for easier identification. You can specify any name.
Interface	From the drop-down list, select an interface (WAN connection) through which remote access to the router will operate. Leave the Automatic value to allow remote access to operate through all created WAN connections.
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 router 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.
Maala	For the IPv4-based network only.
Mask	The mask of the subnet.
Dukkarat	For the IPv4-based network only.
Public port	An external port of the router. You can specify only one port.
Protocol	The protocol available for remote management of the router.

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

To set a schedule for the remote access rule, click the **Set schedule** icon (() in the line corresponding to this rule. In the opened window, from the **Rule** drop-down list, select the **Create rule** value to create a new schedule (see the *Schedule* section, page 228) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

To enable the rule for remote access at the time specified in the schedule and disable it at the other time, select the **Enable rule** value from the **Action** drop-down list and click the **SAVE** button.

To disable the rule for remote access at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and 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 change or delete the schedule for a rule, click the **Edit schedule** icon (\bigcirc) in the line corresponding to this rule. In the opened window, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** 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 ($\boxed{10}$).

System

In this menu you can do the following:

- change the password used to access the router's settings
- restore the factory default settings
- create a backup of the router's configuration
- restore the router's configuration from a previously saved file
- save the current settings to the non-volatile memory
- reboot the router
- change the web-based interface language
- update the firmware of the router
- configure automatic notification on new firmware version
- enable/disable Wi-Fi connection and the Wi-Fi filter, configure automatic reboot of the device on a schedule, and set a schedule for different rules and settings of the firewall
- 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 router
- trace the route to a host
- allow or forbid access to the router via TELNET and SSH
- configure automatic synchronization of the system time or manually configure the date and time for the router
- enable the Auto Provision function.

Configuration

On the **System / Configuration** page, you can change the password for the administrator account used to access the web-based interface of the router and to access the device settings via TELNET and SSH, restore the factory defaults, backup the current configuration, restore the router'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.

🗲 AdBlock	Configuration
User	Factory
	Reset factory default settings
admin	Save current configuration to a file
New password	Load previously saved configuration to the device Save
(i) Password should be between 1 and 31 ASCL characters	Save current settings
Password confirmation	Reboot device
SAVE	Idle time (in minutes)* 5
Language English	() When the function "Stay signed in" is enabled, then users are not redirected to the login page despite the specified idle time.
	SAVE

Figure 164. The System / Configuration page.

In order to change the password for the administrator account, in the **User** section, enter a new password in the **New password** and **Password confirmation** fields. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.⁹ Click the **Show** icon () to display the entered values. Then click the **SAVE** button.

Remember or write down the new password for the administrator account. In case of losing

the new password, you can access the settings of the router only after restoring the factory default settings via the hardware **RESET** button. This procedure wipes out all settings that you have configured for your router.

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

^{9 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 Panel</i> section, page 15).
Backup	Click the button to save the configuration (all settings of the router) 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 router) located on your PC and upload it.
Save	Click the button to save settings to the non-volatile memory. The router 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.

In the **ldle time** field specify a period of inactivity (in minutes) after which the router completes the session of the interface. By default, the value **5** is specified. Then click the **SAVE** button.

Firmware Update

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

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

	Firmware Update	
Local Update (i) Current firmware version: 4.0.1	Remote Update Remote server URL	
Restore factory defaults update	after firmware fwupdate.dlink.ru ADD	
CHOOSE FILE File is not sele	cted Check for updates automatically Interval (in seconds)* 43200	
	At this time, the device works with the latest version of the soft	ware
	CHECK FOR UPDATES APPLY SETTINGS	

Figure 165. The System / Firmware Update page.

The current version of the router's firmware is displayed in the **Current firmware version** field.

By default, the automatic check for the router's firmware updates is enabled. If the Access point, **Repeater**, or **Client** mode was selected in the Initial Configuration Wizard and the **Static** value is selected from the **Mode of local IP address assignment** list on the **Connections Setup** *I* **LAN** page, the **Gateway IP address** field should also be filled in on order to realize automatic check.

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. In the **Interval** field, specify the time period (in seconds) between checks or leave the value specified by default (**43200**).

By default, in the **Remote server URL** field, the D-Link update server address (**fwupdate.dlink.ru**) is specified. To add one more address, click the **ADD** button and enter the address in the displayed line. To remove the address, click the **Delete** icon (\times) in the line of the address.

Click the **APPLY SETTINGS** button.

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

Local Update



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

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

- 1. Download a new version of the firmware from <u>www.dlink.ru</u>.
- 2. Click the CHOOSE FILE button in the Local Update section on the System / Firmware Update page to locate the new firmware file.
- 3. If you want to restore the factory default settings immediately after updating the firmware, move the **Restore factory defaults after firmware update** switch to the right.
- 4. Click the **UPDATE FIRMWARE** button.
- 5. Wait until the router is rebooted (about one and a half or two minutes).
- 6. Log into the web-based interface using the login (admin) and the current password.

If after updating the firmware the router 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 router is rebooted.

Remote Update



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

To update the firmware of the router 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 router 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 router 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 router is rebooted.

Schedule

On the **System / Schedule** page, you can enable/disable Wi-Fi connection and the Wi-Fi filter, configure automatic reboot of the device on a schedule, and set a schedule for different rules and settings of the firewall.

Before creating a schedule you need to configure automatic synchronization of the system time with a time server on the Internet(see the *System Time* section, page 239).

Firmware Update	Schedule	
Auto Reboot		
State	Off	
REBOOT ON SCHEDULE		
All Tasks +		

Figure 166. The System / Schedule page.

To configure automatic reboot of the device on a schedule, click the **REBOOT ON SCHEDULE** button in the **Auto Reboot** section.

	n Time:		8 July 2022, 16:19
Mode			
Simp	lified mode		-
Sche	dule name*		
(i) Th	e number of chan	acters should no	t exceed 32
Interva	l of execution		
	y day		•
	y day		-
	y day Hours (0-23)	Minutes	• ; (0-59)
		Minute: : 0	₹ ; (0-59)

Figure 167. The window for configuring automatic reboot on a schedule.

In the opened window, in the **System Time** field, the system time of the device is displayed. You can select the **Simplified mode** value from the **Mode** drop-down list and specify the following parameters:

Parameter	Description	
	Simplified mode	
Schedule name	Specify a schedule name for easier identification. You can specify any name.	
	Specify the time period for the device's reboot.	
	• Every day : When this value is selected, the Time field is displayed in the section.	
Interval of execution	• Every week : When this value is selected, the names of days of the week and the Time field are displayed in the section.	
	• Every month: When this value is selected, the Day of month and Time fields are displayed in the section.	
Time	Specify the time for the device's reboot.	
Days of week	Select a day or days of the week when the device will be automatically rebooted. To do this, select the checkbox located to the left of the relevant value.	
Day of month	Specify a day of the month. You can specify one value or several values separated by a comma.	

In the advanced mode, you can specify more parameters for the schedule using a cron expression. To do this, select the **Advanced mode** value from the **Mode** drop-down list and specify the needed values in the fields displayed. You can specify one value or several values separated by a comma. You can use the character * (asterisk) to specify the entire range of possible values. Upon that the **Schedule** field will be filled in automatically. In the **Schedule name** field, specify a schedule name for easier identification (you can specify any name).

Click the **SAVE** button.

To edit the automatic reboot schedule, click the **EDIT** button in the **Auto Reboot** section. In the opened window, change the needed parameters and click the **SAVE** button.

To disable automatic reboot of the device on a schedule, click the **EDIT** button in the **Auto Reboot** section. In the opened window, click the **DISABLE** button.

To set a schedule for a task which will be applied to a rule or setting of the firewall or will enable/disable Wi-Fi connection or Wi-Fi filter, click the **ADD** button (+) in the **All Tasks** section.

		ned only if the system time of onized with an NTP server.
System	Time:	8 July 2022, 16:19
	Perform task o	n schedule
Mode Simpl	ified mode	-
Sched	ule name*	
(i) The	number of characters	should not exceed 32
Interval Every	of execution day	-
	Hours (0-23)	Minutes (0-59)
	0 :	0
Time		
(i) Win	en entering several par , "2, 5, 12" or "2-12")	ameters, use the symbol "," or "-" (for
(i) Win	"2, 5, 12" or "2-12")	ameters, use the symbol "," or "-" (for
() Wh example	, "2, 5, 12" or "2-12")	ameters, use the symbol "," or "-" (for Seconds*

Figure 168. The window for adding a schedule for a task.

In the opened window, in the **System Time** field, the system time of the device is displayed. You can select the simplified mode of the schedule. To do this, select the **Simplified mode** value from the **Mode** drop-down list and specify the following parameters:

Parameter	Description
Perform task on	Move the switch to the right to enable the schedule.
schedule	Move the switch to the left to disable the schedule.
	Simplified mode
Schedule name	Specify a schedule name for easier identification. You can specify any name.

Parameter	Description	
	Specify the time period for performing a task.	
Interval of execution	Every minute.	
	• Every hour : When this value is selected, the Time field is displayed in the section.	
	• Every day : When this value is selected, the Time field is displayed in the section.	
	• Every week : When this value is selected, the names of days of the week and the Time field are displayed in the section.	
	• Every month: When this value is selected, the Day of month and Time fields are displayed in the section.	
Duration	Specify the interval during which the task will be performing.	
Time	Specify the time when the task should start running.	
Days of week	Select a day or days of the week when the task will be performing. To do this, select the checkbox located to the left of the relevant value.	
Day of month	Specify a day of the month. You can specify one value or several values separated by a comma.	

In the advanced mode, you can specify more parameters for the schedule using a cron expression. To do this, select the **Advanced mode** value from the **Mode** drop-down list and specify the needed values in the fields displayed. You can specify one value or several values separated by a comma. You can use the character * (asterisk) to specify the entire range of possible values. Upon that the **Schedule** field will be filled in automatically. In the **Schedule name** field, specify a schedule name for easier identification (you can specify any name).

You can also use the calendar mode to configure the schedule. To do this, select the **Calendar mode** value from the **Mode** drop-down list. In the **Schedule name** field, specify a schedule name for easier identification (you can specify any name). In the table, select cells corresponding to needed hours and days of the week. To deselect a cell, left-click it once again. To deselect all cells and select others, click the **RESET** button and select new cells.

Click the **SAVE** button.

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

To remove a schedule, in the All Tasks section, select the checkbox located to the left of the

relevant line in the table and click the **DELETE** button ($\overline{\square}$).

To assign a created schedule to a task which will be applied to a rule or setting of the firewall or will enable/disable Wi-Fi connection or Wi-Fi filter, go to the relevant page of the web-based interface of the device.

Log

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

Log
Settings
Level Debugging messages

Figure 169. The System / Log page. The Settings tab.

To enable logging of the system events, go to the **Settings** tab and move the **Enable** switch to the right. Then specify the needed parameters.

Parameter	Description			
	Logging			
	Select a type of logging from the drop-down list.			
	• Local: The system log is stored in the router's memory. When this value is selected, the Server and Port fields are not displayed.			
Туре	• 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 router's memory and sent to the remote host specified in the Server field.			
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, click the **APPLY** button.

To disable logging of the system events, move the **Enable** switch to the left and click the **APPLY** button.

To view the system log, go to the **Log** tab.

🗸 Schedule	Lo	og 🖸
	Log	Settings
Aug 7 17:46:1 Aug 7 17:40:1 Aug 7 17:43:4 Aug 7 17:43:5 Aug 7 17:44:4 Aug 7 17:44:4 Aug 7 17:44:4 </th <th>EXPORT EDIRECTto-ports 5555] 3 [DBG] unload firewall rule[11185]: Bule #- 3 [DBG] check diff args[72]: dnsmasq@26(rest 3 [TRCE] load[11185]: Generic stream failure! 4 [INF0] CONFIG[11185]: Saving config - OK 4 [DBG] dwatcher[wrkr][11218]: Process actio 9 [TRCE] load[11262]: Generic stream failure! 0 [INF0] CONFIG[11262]: Saving config - OK 0 [DBG] dwatcher[wrkr][11263]: Process actio 9 [INF0] udhcpc[442]: lease of 192.168.161.22 0 [DBG] ugdate_udhcpc[11767]: action=send_re ce.Network.Interface.Ethernet.2.; 0 [DBG] DynPortMap[11775]: could not open le 0 [INF0] dhcp_opt_print[11769]: Option(3): 19 0 [INF0] dhcp_opt_print[11769]: Option(3): 19 0 [INF0] dhcp_opt_print[11769]: Option(6): 1. 0 [INF0] dhcp_opt_print[11769]: Option(51): 6 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: action=renew; ce.Network.Interface.Ethernet.2.; 1 [ERR] d url parse[11856]: Can't parse sche 0 [NOTE] AUTH[72]: Attempt to proceed a RPC w 0 [INF0] durl parse[12029]: Can't parse sche 0 [INF0] durl parse[12029]: Can't parse sche 0 [INF0] AUTH[72]: Attempt to proceed a RPC w</th> <th><pre>10002 UNLOADED art): arguments are equal, nothing to do n: ConfigSaved n: ConfigSaved 8.161.1 8 obtained, lease time 600 new; stop_on_fail=0; 8.161.1 ase file: /tmp/miniupnpd/1.lease 5.255.255.0 2.168.161.1 1.1.1 1.0.0.1 00 92.168.161.1 stop_on_fail=0; me in url=; ith invalid token: f6ce7a0e-5d59-4b62-89a2-a24c49ec5d1b ith invalid token: f6ce7a0e-5d59-4b62-89a2-a24c49ec5d1b </pre></th>	EXPORT EDIRECTto-ports 5555] 3 [DBG] unload firewall rule[11185]: Bule #- 3 [DBG] check diff args[72]: dnsmasq@26(rest 3 [TRCE] load[11185]: Generic stream failure! 4 [INF0] CONFIG[11185]: Saving config - OK 4 [DBG] dwatcher[wrkr][11218]: Process actio 9 [TRCE] load[11262]: Generic stream failure! 0 [INF0] CONFIG[11262]: Saving config - OK 0 [DBG] dwatcher[wrkr][11263]: Process actio 9 [INF0] udhcpc[442]: lease of 192.168.161.22 0 [DBG] ugdate_udhcpc[11767]: action=send_re ce.Network.Interface.Ethernet.2.; 0 [DBG] DynPortMap[11775]: could not open le 0 [INF0] dhcp_opt_print[11769]: Option(3): 19 0 [INF0] dhcp_opt_print[11769]: Option(3): 19 0 [INF0] dhcp_opt_print[11769]: Option(6): 1. 0 [INF0] dhcp_opt_print[11769]: Option(51): 6 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: option(51): 1 0 [INF0] dhcp_opt_print[11769]: action=renew; ce.Network.Interface.Ethernet.2.; 1 [ERR] d url parse[11856]: Can't parse sche 0 [NOTE] AUTH[72]: Attempt to proceed a RPC w 0 [INF0] durl parse[12029]: Can't parse sche 0 [INF0] durl parse[12029]: Can't parse sche 0 [INF0] AUTH[72]: Attempt to proceed a RPC w	<pre>10002 UNLOADED art): arguments are equal, nothing to do n: ConfigSaved n: ConfigSaved 8.161.1 8 obtained, lease time 600 new; stop_on_fail=0; 8.161.1 ase file: /tmp/miniupnpd/1.lease 5.255.255.0 2.168.161.1 1.1.1 1.0.0.1 00 92.168.161.1 stop_on_fail=0; me in url=; ith invalid token: f6ce7a0e-5d59-4b62-89a2-a24c49ec5d1b ith invalid token: f6ce7a0e-5d59-4b62-89a2-a24c49ec5d1b </pre>

Figure 170. The System / Log page. The Log tab.

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

To save the system log to your PC, click the **EXPORT** button. 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.

🗸 Log	g Ping				
Ping					
You can check availability of a	host from the local or global	network via the p	ping utili	ty.	
Host*	Number of attempts*		IPv6		
		0			
	START CL	EAR CAN	ICEL		

Figure 171. The System / Ping page.

To check availability of a host, enter the IP address or name of this host in the **Host** field and specify a number of requests that will be sent in order to check its availability in the **Number of attempts** field. If availability check should be performed with IPv6, move the **IPv6** switch to the right.

To specify additional settings, click the **MORE SETTINGS** button.

	×
Packet size (in byte 56	25) *
 Specifies the n Waiting for response 3 	number of data bytes to be sent. se (in seconds)*
0	ects only timeout in absence of any se ping waits for two RTTs
OK	DEFAULT SETTINGS

Figure 172. The **System / Ping** page. The additional settings window.

In the opened window, in the **Packet size** field, specify the volume of data sent in a request. In the **Waiting for response** field, specify the response waiting period in seconds. To restore the default field values, click the **DEFAULT SETTINGS** button.

After specifying the additional parameters, click the **OK** button.

To run the check, click the **START** button. After a while, the results will be displayed on the page.

If you need to interrupt the check, click the **CANCEL** button (the button is available from the moment the check starts).

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.

V Ping	Traceroute	2	
Traceroute You can determine the route of data transfer to	o a host via the traceroute utility.		
Host* IPv6	MORE SETTINGS		
	START CLEAR	CANCEL	

Figure 173. 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.

To specify additional settings, click the **MORE SETTINGS** button.

			×
Maximum 30	TTL value'		
0	<i>maximum r.</i> f attempts'	umber of hops	
-	<i>number of)</i> (in second	orobe packets to a hop	
(i) Waiti	ing for resp	onse (in seconds)	
OK		DEFAULT SETTIN	GS

Figure 174. The System / Traceroute page. The additional settings window.

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

Parameter	Description
Maximum TTL value	Specify the TTL (<i>Time to live</i>) parameter value. The default value is 30 .
Number of attempts	The number of attempts to hit an intermediate host.
Wait time	A period of waiting for an intermediate host response.

To restore the default field values, click the **DEFAULT SETTINGS** button.

After specifying the additional parameters, click the **OK** button.

To run the check, click the **START** button. After a while, the results will be displayed on the page.

If you need to interrupt the check, click the **CANCEL** button (the button is available from the moment the check starts).

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

Telnet/SSH

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

	Telnet/SSH	
ſelnet/SSH		
/ou can enable or disable access to the device s	ettings via TELNET and SSH from your LAN.	
Enable Telnet	Enable SSH	
Port	Port	
23	A 22	A

Figure 175. The System / Telnet/SSH page.

To enable access via TELNET and/or SSH, move the **Enable Telnet** switch and/or **Enable SSH** switch to the right. In the **Port** field, enter the number of the router's port through which access will be allowed (by default, the port **23** is specified for Telnet and the port **22** is specified for SSH). Then click the **APPLY** button.

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

System Time

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

🗮 < Telnet/SSH	Syster	n Time 🖸
System time You can set up automatic synchronization	of the system time	with a time server on the Internet
Enable NTP	or the system time	Time interval between NTP requests after synchronization with NTP server Auto
 UTC offset settings Configure daylight saving time 	e manually	Time interval between NTP requests for unsynchronized NTP client
Get NTP server addresses usin	-	Time zone* Europe/Moscow
System date:	24.06.2021	
System time: Synchronization:	16:09 Completed	DETERMINE TIMEZONE
NTP Servers		
pool.ntp.org	×	
ADD SERVER		
APPLY		

Figure 176. 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 **Time zone** drop-down list. 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. In case of successful synchronization with the NTP server, the **Completed** value will be displayed in the **Synchronization** field.

If the router failed to get data from the server, the **Failed** value will be displayed in the **Synchronization** field. Upon that the creation date and time of the router's current firmware version is specified.

Parameter	Description	
UTC offset settings	Move the switch to the right to set the UTC (<i>Coordinated Universal Time</i>) offset for the router clock manually. In the UTC offset field displayed, specify the required offset time (in minutes).	
Configure daylight saving time manually	Move the switch to the right to configure settings for daylight saving time for the router clock manually. In the Daylight Saving Time section displayed, specify the required offset time for daylight saving time (in minutes), and specify the needed values in the Beginning of daylight saving time and End of daylight saving time sections.	
Get NTP server addresses using DHCP	Move the switch to the right if NTP servers addresses are provided by your ISP. Contact your ISP to clarify if this setting needs to be enabled.	
	If the switch is moved to the right, the NTP Servers section is not displayed.	
Run as a server for the local network	Move the switch to the right to allow connected devices to use the IP address of the router in the local subnet as a time server.	
Time interval between NTP requests after synchronization with NTP server	From the drop-down list, select a time period (in seconds) after which a request to update the system time will be sent to the NTP server or leave the Auto value.	
Time interval between	A time period (in seconds) after which a request to synchronize the system time will be sent to the NTP server.	
NTP requests for unsynchronized NTP	Select the needed value from the drop-down list.	
client	 Auto: The time period is defined automatically. Manual: The time period is defined in accordance with the 	
	value specified in the Interval value field.	

Additional settings are also available on the page:

Parameter	Description
Interval value	Specify the time period (in seconds). The minimum acceptable value is 3.

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

When the router is powered off or rebooted, the system time is reset to the default value.

If you have set automatic synchronization for the system time, the internal clock of the device will be configured after connecting to the Internet. If you have set the system time manually, you need to set the time and date again (see above).

Auto Provision

On the System / Auto Provision page, you can enable the Auto Provision function.

The Auto Provision function allows your ISP to manage the device's settings remotely: DIR-X1530 connects to the ISP's server, compares the current configuration file with the configuration file stored on this server, and updates its settings if the files are different.

iystem Time	Auto Provision	t
Auto Provision		
Enable Auto Provision	Status:	No check has been run yet
Use BOOTP option	CHECK STATUS	
Autoconfiguration server address		
File name		
File check period (in seconds)		
1800		
Protocol type		
TFTP	•	

Figure 177. The page for configuring the Auto Provision function.

You can specify the following parameters:

Parameter	Description
Enable Auto Provision	Move the switch to the right to enable the Auto Provision function. Move the switch to the left to disable the Auto Provision function.
Use BOOTP option	If the switch is moved to the right, the parameters of your ISP's server (the address, the location of the configuration file, and the protocol) are automatically specified using DHCP options 66 and 67. Upon that a connection of the Dynamic IPv4 type should be configured on the Connections Setup / WAN page.
	If the switch is moved to the left, the parameters of your ISP's server should be specified manually.
Autoconfiguration server address	The IP or URL address of your ISP's server where the configuration file is stored.

Parameter	Description
File name	The location of the configuration file on the ISP's server.
File check period	A time period (in seconds) between attempts to compare the current configuration file with the configuration file on the ISP's server.
Protocol type	A protocol for communication with the ISP's server where the configuration file is stored.

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

If you need to check manually if the current configuration file corresponds to the configuration file on the ISP's server, click the **CHECK STATUS** button. The check result will be displayed in the **Status** field. If the files are different, the device's settings will be updated.

SkyDNS

This menu is designed to configure the SkyDNS service.

SkyDNS is a web content filtering service which provides protection against malicious web sites for devices connected to the router's network, and also allows to configure filtering, block access to adult web sites, and use search engines safely. In order to use the service, first register an account on the SkyDNS service web site.

Settings

On the **SkyDNS / Settings** page, you can enable the SkyDNS service and specify settings for its operation.

Auto Provision	Setti	ngs	
♥ SkyDNS	SkyDNS Service for web content filtering	and safe Internet access.	
Safe Internet at Home		Web Content Filtering Service for Public Wi-Fi Networks	
A convenient instrument for pare provision for home users accessir		Reliable protection for public Wi-Fi hotspots in cafes, restaurants, fitness clubs, movie theaters, etc.	
Protection Against Malwar	e	Convenient Management	
The service also protects against r resources, and botnets.	nalware, phishing	Highly flexible filtering parameters; clear and simple interface.	
Basic Settings		Account	
DISABLE		Mail* test@dlink.ru	
Provider			
SkyDNS		Password*	
Provider is available			Ø
GO TO PERSONAL PROFILE PAG	2E	Tariff	
		Домашний	-
Default profile* Основной	•	Successfully authorized	
Sync period (in seconds)* 3600			
APPLY MANUALLY SYNC			

Figure 178. The SkyDNS / Settings page.

To enable the SkyDNS service, click the **ENABLE** button. Then in the **Mail** and **Password** fields, enter the account data (the e-mail address and the password correspondingly) specified upon registration on the SkyDNS service web site. Click the **APPLY** button. The account data (authorization status, the tariff used), the **Default profile** drop-down list, and the **Sync period** field will be displayed on the page. If needed, from the **Default profile** list, select another filtering profile which will be used for all devices of your LAN and click the **APPLY** button again.

The default filtering profile will be applied to all devices newly connected to the router's network.

To change the parameters of your account on the SkyDNS service web site, click the **GO TO PERSONAL PROFILE PAGE** button.

By default, the account parameters are automatically synchronized with the SkyDNS service web site once an hour (3600 seconds). To change the automatic synchronization period, specify another value in the **Sync period** field and click the **APPLY** button. To start synchronization manually, click the **MANUALLY SYNC** button.

To use another account, specify its data in the **Mail** and **Password** fields and click the **APPLY** button.

To disable the SkyDNS service, click the **DISABLE** button.

Devices and Rules

IP address	MAC address	Name	Profile
192.168.0.3	00:13:46:62:2f:4c	-	Not selected
Rules 🕂 🗍			
	included in the table the default	profile set in the settings will be u	used.

On the **SkyDNS / Devices and Rules** page, you can assign a specific filtering profile to a device connected to the router's network.

Figure 179. The SkyDNS / Devices and Rules page.

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

To assign a specific filtering profile for a device, click the **ADD** button (+) in the **Rules** section or left-click the name of the filtering profile in the line of the device for which a profile should be assigned in the **Known Clients** section.

Adding	×
MAC address*	
Profile* Основной	•
Hostname	
SAVE	

Figure 180. The SkyDNS / Devices and Rules page. The window for adding a rule.

In the opened window, specify the following parameters:

Parameter	Description
MAC address	The MAC address of a device from the router's LAN to which the specified filtering profile will be applied. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Profile	Select the filtering profile which will be used for the device with the specified MAC address from the drop-down list.
Hostname	Enter a name for the rule for easier identification. <i>Optional</i> .

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 ($\boxed{10}$).

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.

Wireless Installation Considerations

The DIR-X1530 device lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF noise in your home or office. To maximize your wireless range, follow the guidelines below.

- Keep the number of walls and ceilings between the DIR-X1530 device and other network devices to a minimum – each wall or ceiling can reduce your wireless network range by 3-90 feet (1-30 meters).
- 2. Be aware of the direct line between network devices. Place your devices so that the signal travels straight through a wall or ceiling (instead of at an angle) for better reception.
- 3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on your wireless range. Try to position your router, access points, and computers so that the signal passes through drywalls or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
- 4. Keep your router away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
- 5. If you are using 2.4 GHz cordless phones or X-10 equipment (wireless devices such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. Note, that the base transmits a signal even if the phone in not in use.

CHAPTER 6. ABBREVIATIONS AND ACRONYMS

3G	Third Generation
AC	Access Category
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BPSK	Binary Phase-shift Keying
BSSID	Basic Service Set Identifier
ССК	Complementary Code Keying
СНАР	Challenge Handshake Authentication Protocol
DBSK	Differential Binary Phase-shift Keying
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DPD	Dead Peer Detection
DQPSK	Differential Quadrature Phase-shift Keying
DSL	Digital Subscriber Line
DSSS	Direct-sequence Spread Spectrum
DTIM	Delivery Traffic Indication Message
EoGRE	Ethernet over Generic Routing Encapsulation
GMT	Greenwich Mean Time
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
НТТР	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

ICMP	Internet Control Message Protocol
ID	Identifier
IGD	Internet Gateway Device
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPTV	Internet Protocol Television
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light-emitting diode
LTE	Long Term Evolution
MAC	Media Access Control
MBSSID	Multiple Basic Service Set Identifier
MIB	Management Information Base
MIMO	Multiple Input Multiple Output
MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Controller
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PAP	Password Authentication Protocol

PBC	Push Button Configuration
PFS	Perfect Forward Secrecy
PIN	Personal Identification Number
ΡοΕ	Power over Ethernet
PPP	Point-to-Point Protocol
pppd	Point-to-Point Protocol Daemon
PPPoE	Point-to-point protocol over Ethernet
РРТР	Point-to-point tunneling protocol
PSK	Pre-shared key
PUK	PIN Unlock Key
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-shift Keying
RADIUS	Remote Authentication in Dial-In User Service
RIP	Routing Information Protocol
RIPng	Next Generation Routing Information Protocol
RTS	Request To Send
RTSP	Real Time Streaming Protocol
SA	Security Association
SAE	Simultaneous Authentication of Equals
SIM	Subscriber Identification Module
SIP	Session Initiation Protocol
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
STBC	Space-time block coding
ТСР	Transmission Control Protocol
•	·

TKIP	Temporal Key Integrity Protocol
UAM	Universal Access Method
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRID	Virtual Router Identifier
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup