



DIR-830M AC1200 Wave 2 MU-MIMO Wi-Fi EasyMesh Gigabit Router

Contents

Chapter 1. Introduction	. 5
Contents and Audience	5
Conventions	5
Document Structure	5
Chapter 2. Overview	. 6
General Information	6
Specifications	
Product Appearance	
Upper Panel	
Back Panel	.14
Delivery Package	.16
Chapter 3. Installation and Connection	17
- Before You Begin	.17
Connecting to Mobile Device with D-Link Assistant Application	
Connecting to PC	.19
PC with Ethernet Adapter	.19
Obtaining IP Address Automatically (OS Windows 7)	.20
Obtaining IP Address Automatically (OS Windows 10)	.25
PC with Wi-Fi Adapter	.29
Obtaining IP Address Automatically and Connecting to Wireless Network	(OS
Windows 7)	.30
Obtaining IP Address Automatically and Connecting to Wireless Network	(OS
Windows 10)	
Connecting to Web-based Interface	.36
Web-based Interface Structure	.38
Summary Page	.38
Home Page	.40
Menu Sections	.41
Notifications	
Chapter 4. Configuring via Web-based Interface	43
Initial Configuration Wizard	. 43
Selecting Operation Mode	.45
Router	.45
Access Point or Repeater	.46
Mesh Network Main Device (Controller)	
Mesh Network Subordinate Device (Agent)	
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 Du	
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	. 0/

Statistics	70
Network Statistics	
DHCP.	
Routing	
Clients and Sessions	
Port Statistics	
Multicast Groups	
IPsec Statistics	
Connections Setup	
WAN	
Creating Dynamic IPv4 or Static IPv4 WAN Connection	
Creating Dynamic IPv6 or Static IPv6 WAN Connection	
Creating PPPoE WAN Connection	
Creating PPTP, L2TP, or L2TP over IPsec WAN Connection	
Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection	
LAN	102
IPv4	
IPv6	
WAN Failover	112
Wi-Fi	115
Basic Settings	115
Client Management	126
WPS	127
Using WPS Function via Web-based Interface	129
Using WPS Function without Web-based Interface	130
WMM	131
Client	134
Client Shaping	137
Additional	140
MAC Filter	
EasyMesh	147
Connecting Subordinate Devices with Ethernet Cable	148
Connecting Subordinate Devices with Hardware Button	
Connecting Subordinate Devices via Web-based Interface	
Advanced	150
VLAN	151
DNS	
DDNS	
Ports Settings	
Redirect	
Routing	
TR-069 Client	
UPnP IGD	
IGMP/MLD	
ALG/Passthrough	
IPsec	
Firewall	
IP Filter	
Virtual Servers	
DMZ	
MAC Filter	
URL Filter	
AdBlock	
Remote Access	

System	202
Configuration	
Firmware Update	
Local Update	
Remote Update	
Schedule	
Log	
Ping	216
Traceroute	
Telnet/SSH	220
System Time	221
Auto Provision	224
SkyDNS	226
- Settings	227
Devices and Rules	229
Chapter 5. Operation Guidelines	231
Terms and Conditions for Installation, Safe Operation,	Storage,
Transportation, and Disposal	231
Wireless Installation Considerations	232
Chapter 6. Abbreviations and Acronyms	233

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DIR-830M 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-830M 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.

General Information

The DIR-830M 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-830M 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.

Using the DIR-830M 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, and 802.11ac (at the wireless connection rate up to 1167Mbps¹).

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

The EasyMesh function is D-Link implementation of mesh networks designed to quickly connect several² devices into one transport network, for example, when it's required to provide high-quality Wi-Fi coverage without dead zones in living units of complicated planning or it's needed to create a large temporary Wi-Fi network for an outdoor event.

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-830M 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.

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.

¹ Up to 300Mbps for 2.4GHz and up to 867Mbps for 5GHz.

² Up to 6 devices.

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, to set rules for limitation of wireless client maximum bandwidth, 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-830M 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-830M 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-830M supports configuration and management via mobile application for Android 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	· RTL8197FH-VG (1GHz)
RAM	· 128MB, DDR2
Flash	· 16 MB, SPI
Interfaces	 10/100/1000BASE-T WAN port 3 10/100/1000BASE-T LAN ports
LEDs	· Status
Buttons	 PWR button to power on/power off RESET/WPS button to restore factory default settings, connect mesh network devices, and set up wireless connection
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
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/MLD Proxy RIP Support of UPnP Support of VLAN WAN ping respond Support of SIP ALG Support of RTSP WAN failover Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port

^{*} 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>.

Software	
Firewall functions	 Network Address Translation (NAT) Stateful Packet Inspection (SPI) IPv4/IPv6 filter MAC 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 tunnels L2TP over IPsec 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 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, limitation of wireless client maximum bandwidth, and enabling/disabling wireless network and Wi-Fi filter Automatic upload of configuration file from ISP's server (Auto Provision)

Wireless Module Parameters	
Standards	 IEEE 802.11ac Wave 2 IEEE 802.11a/b/g/n IEEE 802.11k/v IEEE 802.11w
Frequency range The frequency range depends upon the radio frequency regulations applied in your country	 2400 ~ 2483.5MHz 5150 ~ 5350MHz 5650 ~ 5850MHz
Wireless connection security	 WEP WPA/WPA2 (Personal/Enterprise) WPA3 (Personal) MAC filter WPS (PBC/PIN)

Wireless Module Parameters	
Advanced functions	 EasyMesh function Support of client mode WMM (Wi-Fi QoS) Information on connected Wi-Fi clients Advanced settings Guest Wi-Fi / support of MBSSID Rate limitation for wireless network/separate MAC addresses 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) Support of STBC
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 (from MCS0 to MCS9)
Transmitter output power	 802.11n (typical at room temperature 25 °C) 2.4GHz/5GHz 15dBm
The maximum value of the transmitter output power depends upon the radio frequency regulations applied in your country	 802.11ac (typical at room temperature 25 °C) 15dBm
Receiver sensitivity	 802.11a (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -94dBm at 6Mbps -92dBm at 9Mbps -91dBm at 12Mbps -89dBm at 18Mbps -86dBm at 24Mbps -82dBm at 36Mbps -78dBm at 48Mbps -77dBm at 54Mbps -802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C)
	-97dBm at 1Mbps -93dBm at 2Mbps -93dBm at 5.5Mbps -89dBm at 11Mbps
	 802.11g (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -95dBm at 6Mbps -92dBm at 9Mbps -92dBm at 12Mbps -89dBm at 18Mbps -86dBm at 24Mbps -83dBm at 36Mbps -78dBm at 54Mbps
	 802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) 2.4GHz, HT20 -94dBm at MCS0/8 -91dBm at MCS1/9 -88dBm at MCS2/10 -86dBm at MCS3/11 -82dBm at MCS4/12 -78dBm at MCS5/13 -76dBm at MCS6/14 -75dBm at MCS7/15

eceiver sensitivity	2.4GHz, HT40
eceiver sensitivity	-90dBm at MCS0/8
	-88dBm at MCS1/9
	-86dBm at MCS2/10
	-82dBm at MCS3/11
	-79dBm at MCS4/12
	-75dBm at MCS5/13
	-73dBm at MCS6/14
	-72dBm at MCS7/15
	5GHz, HT20
	-93dBm at MCS0/8
	-91dBm at MCS1/9
	-88dBm at MCS2/10
	-85dBm at MCS3/11
	-82dBm at MCS4/12
	-77dBm at MCS5/13
	-75dBm at MCS6/14
	-74dBm at MCS7/15
	5GHz, HT40
	-91dBm at MCS0/8
	-87dBm at MCS1/9
	-85dBm at MCS2/10
	-82dBm at MCS3/11
	-79dBm at MCS4/12
	-75dBm at MCS5/13
	-74dBm at MCS6/14
	-71dBm at MCS7/15
	 802.11ac (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °
	VHT20
	-94dBm at MCS0
	-90dBm at MCS1
	-88dBm at MCS2
	-85dBm at MCS3
	-82dBm at MCS4
	-78dBm at MCS5
	-76dBm at MCS6
	-74dBm at MCS7
	-70dBm at MCS8
	VHT40
	-91dBm at MCS0
	-88dBm at MCS1
	-86dBm at MCS2
	-83dBm at MCS3
	-79dBm at MCS4
	-74dBm at MCS5
	-73dBm at MCS6
	-71dBm at MCS0
	-67dBm at MCS8
	-64dBm at MCS9
	VHT80
	-87dBm at MCS0
	-84dBm at MCS1
	-81dBm at MCS2
	-79dBm at MCS3
	-75dBm at MCS4
	-71dBm at MCS5
	-69dBm at MCS6
	-67dBm at MCS7
	-64dBm at MCS8
	-62dBm at MCS9

Physical Parameters	
Dimensions (L x W x H)	· 188 x 120 x 30 mm (7.4 x 4.72 x 1.18 in)
Weight	· 226 g (0.49 lb)

Operating Environment	
Power	Output: 12V DC, 1A
Temperature	 Operating: from 0 to 40 °C Storage: from -10 to 70 °C
Humidity	 Operating: from 10% to 90% (non-condensing) Storage: from 10% to 90% (non-condensing)

Product Appearance

Upper Panel



Figure 1. Upper panel view.

LED	Mode	Description
	Solid red	 The default WAN connection is off, or there are no WAN connections created, or the device is in the Access Point mode.
	Solid green	The default WAN connection is on.
Status	Fast blinking red	The router is being loaded.
	Slow blinking red	The firmware is being updated.
	Blinking green	Attempting to connect mesh network devices or add a wireless device via the WPS function.
	No light	The router is powered off.

In case the **Status** LED is very fast blinking red, 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/WPS** button.

Back Panel



Figure 2. Back panel view.

Port	Description
LAN 1-3	3 Ethernet ports to connect computers or network devices.
WAN	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).
	A button to restore the factory default settings, to connect mesh network devices, or set up wireless connection (the WPS function). To restore the factory defaults, push the button (with the device turned on), hold it for 10 seconds, and then release the button.
RESET/WPS	To connect mesh network devices: with the device turned on and factory default settings or with the EasyMesh function enabled in the router settings, push the button, hold it for 2 seconds, and release. To use the WPS function: with the device turned on, push the button, hold it for 2 seconds, and release. The Status LED should start blinking green.
PWR	A button to turn the router on/off.

Port	Description
DC IN	Power connector

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

Delivery Package

The following should be included:

- Router DIR-830M
- 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>).

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

CHAPTER 3. INSTALLATION AND CONNECTION

Before You Begin

Please, read this manual prior to installing the device. Make sure that you have all the necessary information and equipment.

Computer or Mobile Device

Configuration of the wireless dual band gigabit router with a built-in 3-port switch DIR-830M (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 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, or ac 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 Mobile Device with D-Link Assistant Application

- 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. Turn on the router by pressing the **PWR** button on its back panel.
- 3. Make sure that the Wi-Fi connection on your mobile device is on. To switch it on, go to the mobile device settings.
- In the list of available wireless networks on your mobile device, select the wireless network DIR-830M (for operating in the 2.4GHz band) or DIR-830M-5G (for operating in the 5GHz band).
- 5. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) as the password and connect to the wireless network of DIR-830M.
- 6. Launch D-Link Assistant application on your mobile device. The application is available for Android smartphones in Google Play.



D-Link Assistant for Android

- 7. Make sure that the application correctly identified the router to which you connect.
- 8. In the application interface, select the **Advanced Settings** menu option to go through the Initial Configuration Wizard or finish the Wizard earlier and go the configuration menu (for the description of the configuration pages, see the relevant section of the *Configuring via Web-based Interface* chapter).

As 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.

If you changed the administrator password via the web-based interface, when DIR-830M is accessed with the application the next time, click the **ENTER LOGIN/PASSWORD** button. Enter the username (**admin**) and the password you specified.

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.
- 3. Turn on the router by pressing the **PWR** button on its back panel.

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

1

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.)

😋 🔵 🗢 📴 🕨 Control Panel 🕨	All Control Panel Items 🕨	- E - Search Control Panel
Adjust your computer's sett	ings	View by: Large icons 🔻
		· · · · · · · · · · · · · · · · · · ·
lndexing Options	Internet Options	Keyboard
Location and Other Sensors	J Mouse	Network and Sharing Center
Notification Area Icon	ns 🤹 Parental Controls	Performance Information and Tools
Personalization	Phone and Modem	Power Options
Programs and Featur	res 🙀 Recovery	Region and Language
RemoteApp and Desl	ktop 🕥 Sound	Speech Recognition
Sync Center	🙀 System	Taskbar and Start Menu
Troubleshooting	User Accounts	Vindows CardSpace
Windows Defender	Windows Firewall	🦉 Windows Update

Figure 3. The Control Panel window.

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

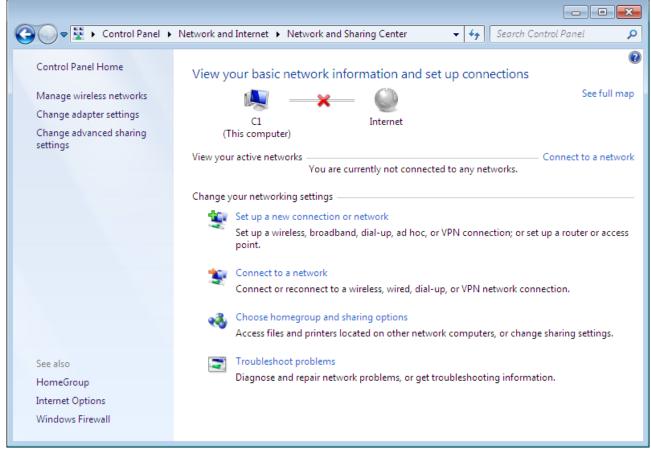


Figure 4. The Network and Sharing Center window.

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

Organize Disable this network device Diagnose this connection Rename this connection > Image: Connection Single Connections Image: Create Shortcut Image: Create Shortcut <) • •	Control Panel Network a	nd Internet Network Connec	tions 🕨	▼ 4 7	Search Network Connections	
Image: Status Diagnose Image: Status Image: Stat	Organize 🔻	Disable this network device	Diagnose this connection	Rename this connection	»		
Status Diagnose Bridge Connections Create Shortcut Delete Rename		N					
Diagnose Bridge Connections Create Shortcut Delete Rename							
Bridge Connections Create Shortcut Delete Rename							
Create Shortcut Delete Rename		Diagnose					
Image: Select end of the select	6	Bridge Connections					
 Delete Rename 		Create Shortcut					
Rename	6						
Properties							
		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:
<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 4 (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	M					
OUse the following IP address:						
IP address:	· · · · ·					
Sybnet mask:	· · · ·					
Default gateway:						
Obtain DNS server address auton	natically					
OUSE the following DNS server add	resses:					
Preferred DNS server:	· · · ·					
Alternate DNS server:						
Validate settings upon exit	Ad <u>v</u> anced					
	OK 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				_	×
	Windows	Settir	ngs		
	Find a setting		Q		
旦	System Display, sound, notifications, power		Devices Bluetooth, printers, mouse		
	Phone Link your Android, iPhone		Network & Internet Wi-Fi, airplane mode, VPN		
⊈ 1	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
டு Home	Status
Find a setting	You're connected to the Internet If you have a limited data plan, you can make this network a metered connection or change other properties.
	Change connection properties
⊕ Status	Show available networks
🦟 Wi-Fi	
記 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 <mark>≫</mark> Airplane mode	
^{((၂))} Mobile hotspot	Network troubleshooter Diagnose and fix network problems.
🕒 Data usage	View your network properties Windows Firewall
Proxy	Windows Firewall 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.

👰 Network Con	nections			
$\leftarrow \rightarrow - \uparrow$	😰 > Control Panel > All C	ontrol Panel Items > Network	Connections	ٽ ~
Organize 🔻	Disable this network device	Diagnose this connection	Rename this connection	View status of this cor
LAN		Wireless Network		
	Disable	Qualcomm Atheros	AR9285 802.1	
	Status			
	Diagnose			
•	Bridge Connections			
	Create Shortcut			
•	Delete			
	Rename			
•	Properties			

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	\times				
Networking Sharing					
Connect using:					
🚍 Realtek PCIe FE Family Controller					
<u>C</u> onfigure					
This connection uses the following items:					
Elient for Microsoft Networks	^				
File and Printer Sharing for Microsoft Networks					
QoS Packet Scheduler					
✓ Internet Protocol Version 4 (TCP/IPv4)					
Microsoft Network Adapter Multiplexor Protocol					
Microsoft LLDP Protocol Driver					
	۲III				
< >>					
Install Uninstall Properties					
Description					
Transmission Control Protocol/Internet Protocol. The default					
wide area network protocol that provides communication across diverse interconnected networks.					
across diverse interconnected networks.					
OK Cance	el				

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						
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 Canc	el					

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. Turn on the router by pressing the **PWR** button on its back panel.
- 3. 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.)

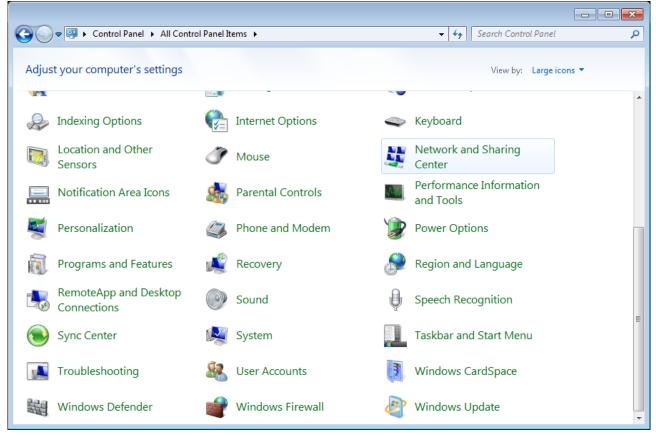


Figure 13. The Control Panel window.

- 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) 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 automatica	Ŋ				
OUse the following IP address: —					
IP address:					
Subnet mask:					
Default gateway:					
Obtain DNS server address autor	natically				
O Use the following DNS server add	resses:				
Preferred DNS server:					
Alternate DNS server:	i i				
Validate settings upon exit		Advance	:d		
	ОК		ancel		

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 DIR-830M (for operating in the 2.4GHz band) or DIR-830M-5G (for operating in the 5GHz band) and click the Connect button.

Not connected	47
Connections are available	
Wi-Fi	^
wireless router Connect automatically Connect	ect
Open Network and Sharing Cer	nter

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		Q		
므	System Display, sound, notifications, power		Devices Bluetooth, printers, mouse		
	Phone Link your Android, iPhone		Network & Internet Wi-Fi, airplane mode, VPN		
⊈ 1	Personalization Background, lock screen, colors		Apps Uninstall, defaults, optional features		
8	Accounts Your accounts, email, sync, work, family	。 A字	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					
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 Advance	ed				
ОК	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 DIR-830M (for operating in the 2.4GHz band) or DIR-830M-5G (for operating in the 5GHz band) and click the Connect button.

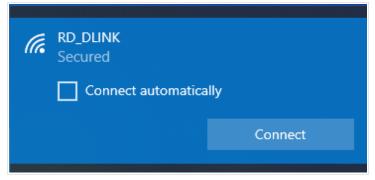


Figure 20. The list of available networks.

- 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).

(i.	RD_DLINK Secured		
	Do you want to allow your PC to be discoverable by other PCs and devices on this network?		
	We recommend allowing this on your home and work networks, but not public ones.		
	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.).

Clients connected to the router with default settings do not have access 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 17). 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-830M 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).

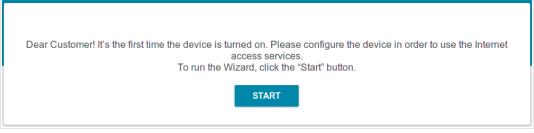


Figure 23. The page for running the Initial Configuration Wizard.

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.

Authorization	
Username*	
Password*	ø
Stay signed in	
Forgot password?	
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	mary	۵
Device Informa	tion	Wi-Fi 5 GHz	
Model:	DIR-830M	Status:	On 🤇
Hardware version:	A1	Broadcasting:	On 🤇
Firmware version:	4.0.1	Additional networks:	
Build time:	Wed Apr 27 2022 5:00:17 PM MSK	Network name (SSID):	DIR-830M-5G-6E9
JI version:	1.32.0.8c10843-embedded	Security:	WPA2-PSK
/endor:	D-Link Russia		
erial number:	1234567890123		
Support:	support@dlink.ru	WAN IPv4	
iummary:	Root filesystem image for DIR_830M_RT8197G	Connection type:	Dynamic IPv
Jptime:	14 min.	Status:	Connected
evice mode:	Router	MAC address	00:0E:1F:A6:6E:9
nable LEDs:	•	IP address:	192.168.161.24
Wi-Fi 2.4 GHz		LAN	
Status:	On 🕒	LAN IPv4:	192.168.0.
Broadcasting:	On 🕒	Wireless connections:	
		Wired connections:	
Additional networks:	1	Wired connections.	
	1 DIR-830M-6E95	miled connections.	
Network name (SSID):			
Network name (SSID):	DIR-830M-6E95	LAN Ports	
Network name (SSID):	DIR-830M-6E95		
Additional networks: Network name (SSID): Security:	DIR-830M-6E95	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).

If needed, you can disable the LED of the device. To do this, move the **Enable LEDs** switch to the left. In order to enable the LED, move the switch to the right and reboot the device.

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.

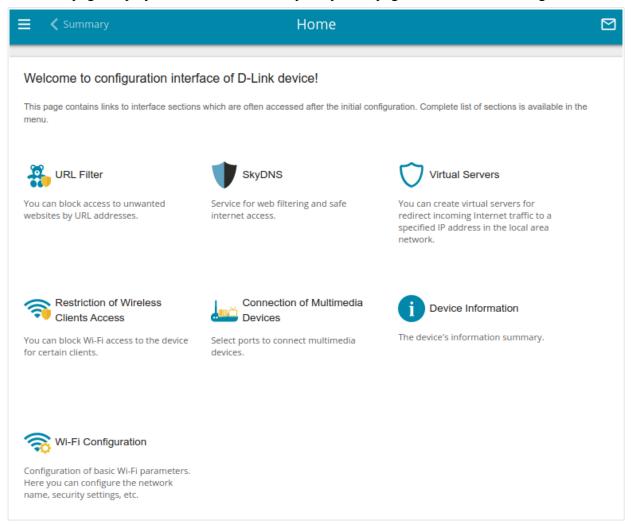


Figure 26. The Home page.

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 70).

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 78).

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 115).

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 150).

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 181).

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 202).

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 226).

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.

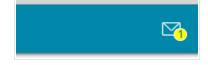


Figure 27. The web-based interface notifications.

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.

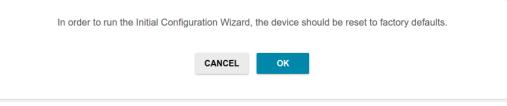


Figure 28. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network **DIR-830M** (for operating in the 2.4GHz band) or **DIR-830M-5G** (for operating in the 5GHz band) and click the **NEXT** button.

Factory defaults are restored
See your wireless network name and password on the barcode label on the device.
If you are connected via Wi-Fi, please make sure that you have not switched automatically to another wireless network.
NEXT

Figure 29. Checking connection to the wireless network.

Click the **START** button.

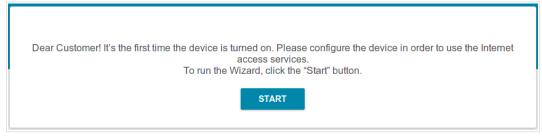


Figure 30. Starting the Wizard.

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.

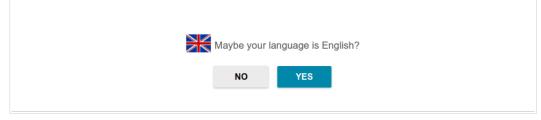


Figure 31. Selecting a language.

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*	ø
Password should be between 1 and 31 ASCII	characters
Password confirmation*	ø
Network name 2.4 GHz (SSID)*	
DIR-XXX	
Network name 5 GHz (SSID)* DIR-XXX-5G	
<	BACK

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 **Autonomous** 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.

Connection method			
Autonomous	•		
Vork mode			
Router	•		ssid
		Internet	

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 **Autonomous** 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.

Connection method		
Autonomous	•	
Vork mode		
WISP Repeater	•	SSID_Ext
	< BACK	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 **Autonomous** 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.

Device mode			
Connection method			
Autonomous	•		
Access point	•		SSID
	< 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 **Autonomous** 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		
Autonomous	▼	
Vork mode		ريد 🛋
Repeater	•	SSID_Ext
))) ssid (((
	< BACK	NEXT >
	La briott	

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 **Autonomous** 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.

Device mode		
Connection method Autonomous	-	
Work mode Client	•	
	🗲 ВАСК	NEXT >

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

Mesh Network Main Device (Controller)

In order to configure DIR-830M as a main device of your mesh network, from the **Connection method** list, select the **EasyMesh** value. Then from the **Device role** list, select the **Controller** value. From the **Backhaul band** list, select the band where your mesh network operates.

The EasyMesh function cannot operate in both bands simultaneously. Select one of the bands (2.4GHz or 5GHz) for all devices of the configured network.

You can connect Agent devices with factory defaults to the main mesh network device via the hardware **RESET/WPS** button. To do this, on the main device, in the **Backhaul band** drop-down list, select the **5 GHz** option and complete the configuration of the main device via the Wizard. Then press the hardware WPS button on both devices, hold it for 2 seconds, and release. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.

In order to connect your main device to a wired ISP, 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.

Connection method	
EasyMesh 🗸	
Device role	
Controller -	
Work mode	
Router -	
Backhaul band	
5 GHz 👻	ssip
① The backhaul band should be the same for the Controller device and all Agent devices	
The EasyMesh function is designed to connect devices in one network. The connection can be wired or wireless.	
The Controller device in the mesh network is equivalent to a router in a usual network. One network can contain only one Controller device. If you already have such a device in your network, configure the present device to act as Agent.	
▲ When Agent devices with factory defaults connect to the mesh network via the hardware button, they obtain the wireless settings and the administrator's password of the	

Figure 38. Configuring the EasyMesh function for the main device. The **Router** mode.

In order to connect your main device to a wireless ISP (WISP), 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.

Connection method EasyMesh ▼		
Device role		
Controller •		
Nork mode		
WISP Repeater		
Backhaul band		
5 GHz 🗸		ssid_Ext
 The backhaul band should be the same for the Controller device and all Agent devices 	(Internet))) SSID	(((III)))) Mesh SSID (((Mesh Controller LAN
The EasyMesh function is designed to connect devices in one network. The connection can be wired or wireless.		
The Controller device in the mesh network is equivalent to a router in a usual network. One network can contain only one Controller device. If you already have such a device in your network, configure the present device to act as Agent.		
When Agent devices with factory defaults connect to the mesh network via the hardware button, they obtain the wireless settings and the administrator's password of the Controller.		

Figure 39. Configuring the EasyMesh function for a main device. The **WISP Repeater** mode.

Mesh Network Subordinate Device (Agent)

In order to configure DIR-830M as a subordinate device of your mesh network, from the **Connection method** list, select the **EasyMesh** value. Then from the **Device role** list, select the **Agent** value. From the **Backhaul band** list, select the band where your main device (in the Controller role) operates.

Then a subordinate device is configured in the access point mode. In this mode you can change the LAN IP address and set your own password for access to the web-based interface of the device.

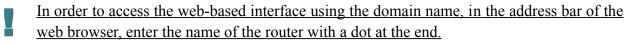
Connection method	
EasyMesh •	
Device role	
Agent -	(1)
Backhaul band 5 GHz	
① The backhaul band should be the same for the Controller device and all Agent devices	
The EasyMesh function is designed to connect devices in one network. The connection can be wired or wireless.	2
When the settings are applied, simultaneously click the "Connect" button in the EasyMesh section (or the hardware WPS button) on the Agent device and on the Controller device (or on two Agent devices) in order to transfer data from one device to another.	((())) Mesh SSID ((())) SSID (Mesh) LAN (Agent) LAN
If needed, disconnect the Agent device from the Controller device (or another Agent device) and move it to its permanent worksite.	

Figure 40. Configuring the EasyMesh function for a subordinate device.

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-830M 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.



If you want to manually assign the LAN IPv4 address for DIR-830M, 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.

Automatic obtainment of IPv4 address Automatic obtainment of IPv4 address sufficiently protects against use of the same addresses in one LAN. In order to avoid IPv4 address conflicts, static IPv4 addresses of LAN devises should not coincide with addresses from the address range assigned by an upper-level router (or a local DHCP server). P address* 192.168.0.1 Subnet mask* 255.255.255.0 Gateway IP address NNS IP address* 8.8.8.8 Hostname* dinkan1866 local	LAN	
avoid IPv4 address conflicts, static IPv4 addresses of LAN devises should not coincide with addresses from the address range assigned by an upper-level router (or a local DHCP server). IP address* 192.168.0.1 Subnet mask* 255.255.255.0 Gateway IP address DNS IP address* 8.8.8.8 Hostname*	Automatic obtainment of IPv4 address	
192.168.0.1 Subnet mask* 255.255.255.0 Gateway IP address DNS IP address* 8.8.8.8 Hostname*	avoid IPv4 address conflicts, static IPv4 addresses of LAN	devises should not coincide with addresses from the address range
Subnet mask* 255.255.255.0 Gateway IP address DNS IP address* 8.8.8.8 Hostname*	IP address*	
255.255.255.0 Gateway IP address DNS IP address* 8.8.8.8 Hostname*	192.168.0.1	
Gateway IP address DNS IP address* 8.8.8.8 Hostname*	Subnet mask*	
DNS IP address* 8.8.8.8 Hostname*	255.255.255.0	
DNS IP address* 8.8.8.8 Hostname*		
8.8.8.8 Hostname*	Gateway IP address	
Hostname*	DNS IP address*	
	8.8.8.8	
dinkan18c6 local	Hostname*	
	dlinkap18c6.local	
	÷ · · ·	-
③ 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 slash at the end in the address bar of the web browser (for example, dlinkap12ab.local./)	< ВАСК	NEXT >

Figure 41. 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 (\bigcirc).

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

requency band			
2.4 GHz	-	▲ Attention! Upon connection to networks with WEI _ encryption, basic settings of Wi-Fi networks will be ch	
vetwork name (SSID)*		the standards 802.11b and g will be used in the 2.4GF and the standard 802.11a will be used in the 5GHz ba	Iz band
RD_DLINK		Network authentication	
SSID		WPA2-PSK	
74:DA:DA:0A:8F:C9			
		Password PSK*	è
		Password should be between 8 and 63 ASCII ch	aracters
		Encryption type*	
		AES	
WIRELESS NETWORKS			

Figure 42. 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
Enable encryption WEP	For Open authentication type only. 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 () 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.
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.

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 SCAN	his type allows you to use					
	J					
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		Â				
() In some ISP's ne	tworks, it is required to re	egister a certain N	IAC address in	order to get acce	ss to the Internet.	
Use VLAN						
(i) Select the check	box if the Internet access	is provided via a	VLAN channel.			
Use IGMP						
(i) Internet Group M	anagement Protocol is d	esigned to manag	ge multicast trafi	fic in IP-based ne	tworks.	
Ping						
		🕻 ВАСК	NEXT	>		

Figure 43. 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	-
(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	/SS [*]
DNS IP address*	
/IAC address assignme	int method
Default MAC add	ress -
MAC address 10:62:eb:2c:c8:3a	
 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	
 Select the check 	kbox if the Internet access is provided via a VLAN channel.
Ping	
	C BACK NEXT >

Figure 44. 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

Connection type		
PPPoE	•	
A connection of ti	his type requires a user name and pa	sword.
SCAN	Network scan for connection type	e and parameters detection
Without authoriza	tion	
Username*		
Password*	8	
Service name		
MAC address assignmen	t method	
Default MAC addre	ess 🔹	
MAC address		
10:62:eb:2c:c8:3a	6	
i In some ISP's ne	tworks, it is required to register a cert	in MAC address in order to get access to the Internet.
Use VLAN		
 Select the checkl 	box if the Internet access is provided	ia a VLAN channel.

Figure 45. 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)	
 A connection of this type requires a user name, passwo 	ord, and a fixed IP address provided by your ISP.
SCAN Network scan for connection typ	e and parameters detection
Without authorization	
Username*	
Password*	
Service name	
IP address*	
Subnet mask*	
Gateway IP address*	
DNS IP address*	

Figure 46. 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 connection type
Connection type
PPTP + Dynamic IP
() PPTP and L2TP are methods for implementing virtual private networks.
SCAN Network scan for connection type and parameters detection
Without authorization
Username*
Password* &
VPN server address* MAC address assignment method Default MAC address
MAC address
10:62:eb:2c:c8:3a
 in some ISP's networks, it is required to register a certain MAC address in order to get access to the Internet. Use VLAN is Select the checkbox if the Internet access is provided via a VLAN channel. is Use IGMP internet Group Management Protocol is designed to manage multicast traffic in IP-based networks.
Ping
SACK NEXT >

Figure 47. 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

nternet conne	ection type		
Connection type PPTP + Static IF	· · ·		
PPTP and L2T	P are methods for implementing virtual p	ivate networks.	
SCAN	Network scan for connection type	e and parameters detection	
Without authori	zation		
Password*	Ø		
VPN server addr	ess*		
P address*			
Subnet mask*			
Gateway IP addr	'ess*		

Figure 48. 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	
 Disabling broadcast does not influence the ab 	ility to connect to another Wi-Fi network as a client.
Network name*	
my <u>wi-fi</u>	
Open network	
Password*	
••••••	Q.
Password should be between 8 and 63 ASCII Use the same parameters as on the same parame	
RESTORE You can restore network name and	d security that was set before applying factory settings.

Figure 49. 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
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 50. 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.

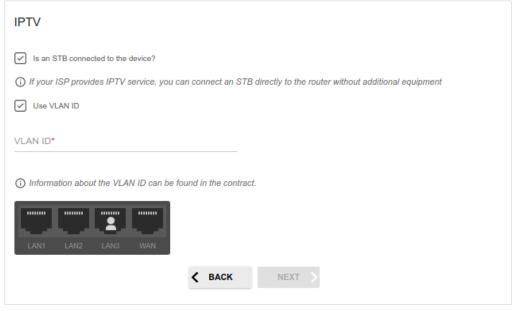


Figure 51. The page for selecting a LAN port to connect an IPTV set-top box.

- 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. LAN1 LAN2 LAN3 WAN
C BACK NEXT >

Figure 52. The page for selecting a LAN port to connect a 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.³

Changing web-based interfac	ce password				
For security reasons, please change	the password used t	to access the de	evice's setting	S.	
User's interface password*	ø				
 Password should be between 1 and 	31 ASCII characters				
Password confirmation*	Q				
	< ВАСК	NEXT >			

Figure 53. 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/WPS** 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.

^{3 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

Figure 54. 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 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-830M 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 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.

😑 < Home	Connection of Multimed	lia Devices	
You can connect an STB or IP phone d your device to it. In some cases IPTV/VoIP services are p			
LAN			
LAN1	LAN2	LAN3	
ADVANCED MODE			
	APPLY		

Figure 55. 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 Bridged with No	LAN3 Bridged with No	
SIMPLIFIED MODE			
WAN			
WAN	Ð		
	APPLY		

Figure 56. The Multimedia Devices Connection Wizard. The advanced mode.

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

New Connection	×
Name*	
VLAN ID*	
Allowed	
SAVE	

Figure 57. 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 to which the additional device is connected, select the created connection. Click the **APPLY** button.



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

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

To deselect the port in the advanced mode, select the **No** value from the **Bridged with** drop-down list of the element corresponding to the needed LAN port. 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.

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).

🖌 Home	Networ	k Statistics		
Network Stati	istics is for all interfaces (connections) existing in t	he system.		
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 - 192.168.0.1	92.05 Mbyte / 99.08 Mbyte	0/0	-
dynamic_Internet		-	-	-
DIR-XXX	-	64.31 Mbyte / 203.23 Kbyte	0/0	-
DIR-XXX-5G	-	19.14 Mbyte / 49.16 Kbyte	0/0	-

Figure 58. 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.

K Network Statistics	DHCP		l	Y
DHCP You can view the information on devices that	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 59. The Statistics / DHCP page.

Routing

Rules						
Table	Туре	IP (Source/Destination)	Interfaces (Incoming/C	Dutgoing) 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
Tables						
ID	Na	ame [Description			
254	m	ain 1	1ain routing table			
257	group_1 Routing table for groups					
256	static_1 Routing table for connections		s			

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

Figure 60. 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 Table \square Routing Table main You can view the information on routes. Interface Destination Subnet mask Gateway Table Flags Metric 0.0.0.0 WAN 0.0.0.0 192.168.161.1 UG 410 254 WAN 1.0.0.1 192.168.161.1 UGH 0 254 WAN 1.1.1.1 192.168.161.1 UGH 254 0 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 61. 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.

Kouting	Clien	ts and Sessions		
Clients				
You can view the list of device	tes connected to the local ne	etwork of the router and informa	ation on current s	essions of each device.
MAC	IP address	Hostname	Flags	Interface
> D0:17:C2:00:29:85	192.168.0.129	android-c2dfe5fa660	reachable	WLAN
90:2B:34:A5:A8:FB	192.168.0.2	-	reachable	LAN

Figure 62. 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.

= < 0	lients and Sessions	Port Statistics	E
Port St	atistics		
You can vie problems.	ew statistics for traffic passin	g through ports of the device. This in	formation can be used for diagnosing connection
Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte
LAN1	Disconnected	0	0
LAN2	Disconnected	0	0
LAN3	Connected	6	0
WAN	Connected	0	0

Figure 63. 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.

Port Statistics	Multicast Gro	ups		
Multicast Groups				
		C . C .		
subscribed, and the interface thro	multicast groups (including IPTV channels and g ough which the device is subscribed.		service information) to which the devi	ce is
	bugh which the device is subscribed.		service information) to which the devia Interface	ce is

Figure 64. 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.

🔇 IPsec		IPsec Statis			
Psec Stat u can view st	istics atistics for IPsec connecti	ions.			
Name	Remote host	Packets received / Packets sent	Traffic received / Traffic sent	Mode	Туре
ipsec_64	192.168.161.189	-/-	-/-	TUNNEL	IPv4

Figure 65. The Statistics / IPsec Statistics page.

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

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 **WAN** port of the router.

≡	IPsec Statistics	WAN	
WA	N		
You o	an create and edit connections used by the router.		
Dyn	namic IPv4		
EDIT	RECONNECT		
Conn	ection type:		Dynamic IPv4
Statu	IS:		Connected
Inter	face:		WAN
IP ad	dress:		192.168.0.142
Subn	et mask:		255.255.255.0
Gate	way IP address:		192.168.0.1
СНА	ANGE CONFIGURATION ADVANCED MODE		

Figure 66. 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.

E < IPsec Statistics	W	AN		
WAN You can create and edit connections used	d by the router.			
Default Gateway IPv4 Default Gateway IPv6 The specified connection will be used by default. No IPv6 connection created. Image: Internet in				
IGMP/MLD On the IGMP/MLD page you can allow the and MLD and configure their settings.				
Name	Connection type	Interface	Status	
dynamic_Internet	Dynamic IPv4	WAN	Connected	
SIMPLIFIED MODE				

Figure 67. 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 ($\overline{\square}$).

To allow multicast traffic (e.g. streaming video) for a connection, click the **IGMP/MLD** link (for the description of the page, see the *IGMP/MLD* section, page 168).

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	eral Settings
Connect	ion type
Static	IPv4 -
Interface	2
WAN	-
Connect	ion name*
statip	
	Enable connection
	NAT
	NAT
<u> </u>	NAT network address translation function. It is recommended not to riless your ISP requires it.
<u> </u>	network address translation function. It is recommended not to
disable u	network address translation function. It is recommended not to nless your ISP requires it.

Figure 68. 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.

Etherne	
DC.0F:9/	A:6D:36:4C
	long MAC address of your NIC
	lone MAC address of your NIC 0:2B:34:A5:A8:FB)
	00:2B:34:A5:A8:FB)

Figure 69. The page for creating a new Static IPv4 connection. The Ethernet section.

Parameter	Description
	Ethernet
MAC address	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. 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.

ΙΡv	4
IP ad	dress*
192.	168.161.224
Subn	et mask*
255.	255.255.0
Gatev	vay IP address*
192.	168.161.1
Prima	ary DNS*
1.1.	1.1
Secor	ndary DNS
1.0.0	D.1
addre addre	If the connection is created for the IPTV service only and no data on IP essing is given by your ISP, then you can set the following values: IP ess = 1.0.0.1, Netmask = 255.255.255.252, Gateway IP address = 1.0.0.2, ny DNS server = 1.0.0.2

Figure 70. 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. Optional.	

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

Creating Dynamic IPv6 or Static IPv6 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
Connection type
Static IPv6
Interface
WAN -
Connection name* statipv6_6
(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.
RIPng

Figure 71. 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.
RIPng	Move the switch to the right to allow using RIPng for this connection.

Ethern	
	A:6D:36:4C
	Clone MAC address of your NIC 90:2B:34:A5:A8:FB)
	90:2B:34:A5:A8:FB)

Figure 72. The page for creating a new **Static IPv6** connection. The **Ethernet** section.

Parameter	Descriptior	۱
	Ethernet	
	A MAC address assigned to the in mandatory if your ISP uses MAC addre the MAC address registered by your agreement.	ss binding. In the field, enter
MAC address	To set the MAC address of the network computer that is being used to configure as the MAC address of the WAN interface address of your NIC switch to the moved to the right, the field is unavailable	re the router at the moment) Face, move the Clone MAC e right. When the switch is
	To set the router's MAC address, click MAC ADDRESS button (the button is moved to the right).	the RESTORE DEFAULT
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	

Figure 73. 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

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.

Genera	al Settings
Connection PPPoE	n type
Interface WAN	•
Connection	
(i) The nu	umber of characters should not exceed 32
() E	nable connection
•	JAT
-	twork address translation function. It is recommended not to ess your ISP requires it.
F	Ping
<u> </u>	Ving Respond allows the device to respond to ping requests tternal network.
J F	RIP

Figure 74. 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.

Ether		
MAC add		
BC:0F:	9A:6D:36:4C	
	Clone MAC address of your NIC	
	Clone MAC address of your NIC (90:2B:34:A5:A8:FB)	
MTU*	(90:2B:34:A5:A8:FB)	

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

Parameter	Description
	Ethernet
MAC address	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. 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	
Without authorization	
Username*	
Password*	Ø
Service name	
MTU*	
1492	
Encryption protocol	
No encryption	•
Authentication protocol	
AUTO	-
_	
Keep Alive	
LCP interval*	
30	
30 LCP fails* 3	
LCP fails*	
LCP fails*	
LCP fails* 3	
LCP fails* 3	6
LCP fails* 3 Dial on demand	ĥ
LCP fails* 3 Dial on demand	

Figure 76. 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 (\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
Encryption protocol	 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. 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	A
Secondary DNS	

Figure 77. 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

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.

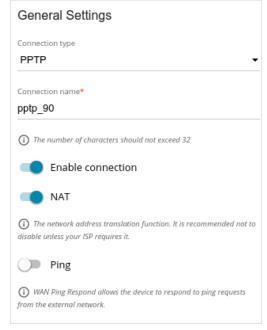


Figure 78. The page for creating a new **PPTP** connection. The **General Settings** section.

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 79. 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.	
MTU	The maximum size of units transmitted by the interface.	

Parameter	Description
Encryption protocol	 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. 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 80. The page for creating a new **PPTP** 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.
	IPsec
	Pre-shared key*
	Enable PFS
	Specify connection port

Figure 81. 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 (\bigotimes) 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-830M.
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 **Advanced / IPsec** page, in the **Status** section, the current state of the IPsec tunnel is displayed.

Creating PPPoE IPv6 or PPPoE Dual Stack 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
Connection type
PPPoE IPv6
Interface
WAN •
Connection name*
pppoev6 19
(i) 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.
RIPng

Figure 82. 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 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.	

Parameter	Description
RIPng	Move the switch to the right to allow using RIPng for this connection.
	Ethernet MAC address* BC:0F:9A:6D:36:4C Clone MAC address of your NIC (90:2B:34:A5:A8:FB) RESTORE DEFAULT MAC ADDRESS
	MTU* 1500

Figure 83. The page for creating a new **PPPoE IPv6** connection. The **Ethernet** section.

Parameter	Description
	Ethernet
MAC address	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. 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*	ĕ
Service name	
MTU* 1492	
Encryption protocol	
No encryption	
Authentication protocol	
Keep Alive	
LCP interval* 30	
LCP fails*	
3	

Figure 84. 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.	
МТО	The maximum size of units transmitted by the interface.	

Parameter	Description
Encryption protocol	 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. 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 85. The page for creating a new **PPPoE Dual Stack** connection. The **IPv4** section.

Parameter	Description
	IPv4 (for the PPPoE Dual Stack 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.
	IPv6 Get IPv6 Automatically Enable prefix delegation Obtain DNS server addresses automatically Primary IPv6 DNS server

Figure 86. The page for creating a new **PPPoE Pv6** connection. The **IPv6** section.

A

Secondary IPv6 DNS server

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.

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	
Specify a domain na	me ending with .local. In order to access the web-
<u> </u>	domain name, enter this name with a dot and slash
at the end in the address	bar of the web browser (for example,

Figure 87. 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
	Start IP* 192.168.0.100
	End IP* 192.168.0.199
	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 88. 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 SELECT 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 89. 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	
Force	
SAVE	

Figure 90. 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 91. 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 ($\overline{10}$). 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 92. 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.

For example: fd00::1/64	Į.
Enter IPv6 address, slash (/), and a decimal value equal to the since prefix.	ze in bits of
ADD	
Hostname	
dlinkrouter.local	

Figure 93. 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** $(\overline{10})$ 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
① 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 94. 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. Available if the Router or WISP Repeater mode was selected in the Initial Configuration Wizard.
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 SELECT 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 95. 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	
(i) In order to delete IP address just leave the file empty	eld
SAVE	

Figure 96. 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 ($\boxed{\blacksquare}$).

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.

📕 < LAN/Edit	ing WAN	l Failover 🗠
WAN Failove	er	
main connection b		s you with uninterrupted access to the Internet. When your ackup connection; and when the main channel is recovered, the
Enable		
Connections	IPv4	Check with ping
The list of available	connections on order of priority.	Interval between checks (in seconds)*
Connection	Check with ping	30
		Waiting for response (in seconds)*
pppoe_100	On	1
statip_22	On	Number of attempts*
statip_22	0.1	3
		Oumber of ping requests to the specified hosts
		Hosts
		8.8.8.8
		77.88.55.55 ×
		94.100.180.200 ×
		ADD HOST
_		
APPLY		

Figure 97. 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.

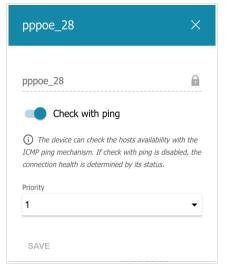


Figure 98. The window for changing the priority of a connection.

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 to one ping 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 (*) in the line of the address.		

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

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.

≡	≮ <u>WAN Failover</u>	Basi	c Settings	
	2	.4 GHz	5 GHz	
	a sic Settings I can change basic parame	eters for the wireless interface of the	device.	
	🔵 Enable Wireless 🔇	0	Wi-Fi Network	
Cour	ntrv		Network name (SSID)*	
	JSSIAN FEDERATION		DIR-XXX	
	eless mode 2.11 B/G/N mixed	•	Hide SSID Wireless network name (SSID) will not appear in the list of available wireles networks with customers. Go to a hidden network, you can connect to manually	
	Select channel auto	omatically	specify the SSID of the access point	
i	The least loaded data transfer c	hannel will be used	BSSID	
			5c:c7:aa:0f:c4:cf	
	Enable additional of the second se	nanneis	Max associated clients*	
chan		ally selects a channel from the list of available . Make sure that your wireless devices support	0	
Char	nnel		Enable shaping	
	to (channel 13)			
0	Enable periodic sca	anning	0 Broadcast wireless network (S	
~	The device will periodically chec led one	k the channels load and switch to the least	Allows you to enable/disable broadcast of this SSID without disconnecting t wireless module of the router. Can be used with the mode "Wi-Fi Client"	:he
Scan	nning period (in seconds)			
0		6	Clients isolation	
			() Block traffic between devices connected to the access point	

Figure 99. Basic settings of the wireless LAN in the 2.4GHz band.

Parameter	Description
Enable Wireless	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 208) 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 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 (). 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.

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

Parameter	Description
Channel	The wireless channel number. 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. To make the router select the currently least loaded channel, click the Refresh icon (C). The icon is displayed, when the Select channel automatically switch is moved to the right.
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.

Wi-Fi Network	Security Settings	
Network name (SSID)*	Network authentication	
DIR-XXX.2	WPA2-PSK	
Hide SSID	Password PSK*	
	•••••	۶
Wireless network name (SSID) will not appear in the list of available wireless networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point	Password should be between 8 and 63 ASCII characters	
Max associated clients*	Encryption type*	
	AES	
-	Group key update interval (in seconds)*	
Enable shaping	3600	
Broadcast wireless network		
Biolacust Wireless network	802.11w (Protected Management Frames)	
Allows you to enable/disable broadcast of this SSID without disconnecting the	Disabled	
vireless module of the router. Can be used with the mode "Wi-Fi Client"		
Clients isolation		
Black traffic between devices connected to the access point		
Enable guest network		

Figure 100. Creating a wireless network.

Parameter	Description	
Wi-Fi Network		
Network name (SSID)	A name for the wireless network.	
Hide SSID	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.	
BSSID	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.	
Max associated clients	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.	

Parameter	Description
Enable shaping	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.
Broadcast wireless network	If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DIR-830M can connect to another access point as a wireless client. To enable/disable broadcasting 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 208) 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 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 (()). In the opened window, change the parameters and click the SAVE button. To change or click the DELETE FROM SCHEDULE button. If you created an additional network, you can configure, change or delete a schedule for each 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.

Security Settings	
Network authentication	
WPA2-PSK	•
Open	
WPA	
WPA-PSK	
WPA2	
WPA2-PSK	
WPA/WPA2 mixed	
WPA-PSK/WPA2-PSK mixed	
WPA3-SAE	
WPA2-PSK/WPA3-SAE mixed	

Figure 101. 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 method.

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):

Network authentication	
Open	
Enable encryption WEP	
Default key ID	
1	
It is recommended to use the first key by d with many devices.	efault to ensure compatibility
Encryption key WEP as HEX	X
Encryption Key WEP as HEA Length of WEP key should be 5 or 13 char	
	acters.
Length of WEP key should be 5 or 13 char	acters.
Length of WEP key should be 5 or 13 char Encryption key 1*	
Length of WEP key should be 5 or 13 char Encryption key 1*	acters.
① Length of WEP key should be 5 or 13 char Encryption key 1* Encryption key 2*	acters.

Figure 102. The Open value is selected from the Network authentication drop-down list.

Parameter	Description
Enable encryption WEP	<i>For Open authentication type only.</i> 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-SAE 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	
802.11w (Protected Management Frames)	
Disabled	-

Figure 103. 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. ⁴ Click the Show icon (()) to display the entered password.
Encryption type	An encryption method: TKIP , AES , or TKIP+AES . <i>TKIP</i> and <i>TKIP+AES</i> encryption types are not available for <i>WPA3-SAE</i> and <i>WPA2-PSK/WPA3-SAE</i> mixed authentication types.

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

Parameter	Description
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 Management Frames)	 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. 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	ess RADIUS server*
192.10	68.0.254
RADIUS	s server port*
1812	
RADIUS	s encryption key*
dlink	
Encrypti	on type*
AES	-
Group k	ey update interval (in seconds)*
3600	
802.11w	r (Protected Management Frames)
Disab	led 🗸

Figure 104. 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.

=	🕻 Basic Settings		Client Man	agement			
	nt Manageme	ent eless clients connected to the	router.				
List o	of Wi-Fi Clients	REFRESH DISCONNECT					
	Hostname	MAC address	Band	Network name (SSID)	Signal level	Online	
	Galaxy-M21	66:C5:55:3D:D2:91	2.4 GHz	DIR-XXX	रि 100%	0 min	

Figure 105. 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 win this function. DISABLE WPS	reless network of the router. The connecting de	evices must support
WPS Control	Information	
	WPS state:	Configured
ESTABLISH CONNECTION	Default PIN code:	12345670
	Network name (SSID):	DIR-XXX
	Network authentication:	WPA2-PSK
	Encryption:	AES
	Password PSK:	12345670
	UPDATE	

Figure 106. The page for configuring the WPS function.

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

To activate the WPS function via the hardware button, with the device turned on, push the button, hold it for 2 seconds, and release. The **Status** LED should start blinking green. In addition, upon pressing the button, the wireless interfaces of the device are enabled if they were disabled before.

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

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

Parameter	Description		
WPS state	 The state of the WPS function: 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.		

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. Click the **ENABLE WPS** button.
- 3. 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 **RESET/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 **RESET/WPS** button of the router, hold it for 2 seconds, and release. The **Status** LED should start blinking green.

WMM

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

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

Select the needed action from the drop-down list in the **Work mode** section to configure the WMM function.

- **Auto**: the settings of the WMM function are configured automatically (the value is specified by default).
- **Manual**: the settings of the WMM function are configured manually. When this value is selected, the **Access Point** and **Station** sections are displayed on the page.

vps WMM												
			2.4 GHz				_			5 GHz		
	node		WI-FI network	performa	nce. It is re	commende	ed for users	not to chan	ge the specifie	d values		
Acce	ss Point						Static	'n				
Acce:	AIFSN	CWMin	CWMax	ТХОР	ACM	ACK	Static AC	n AIFSN	CWMin	CWMax	ТХОР	ACM
			CWMax	TXOP 0	ACM off	ACK off			CWMin 15	CWMax 1023	TXOP 0	ACM off
AC	AIFSN	CWMin					AC	AIFSN				
AC BE	AIFSN 3	CWMin 15	63	0	off	off	AC BE	AIFSN 3	15	1023	0	off

Figure 107. The page for configuring the WMM function.

All needed settings for the WMM function are specified in the device's system. Changing parameters manually may negatively affect your WLAN!

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

- **BK** (*Background*), low priority traffic (print jobs, file downloads, etc.).
- **BE** (*Best Effort*), traffic from legacy devices or devices/applications that do not support QoS.
- **VI** (*Video*).
- **VO** (*Voice*).

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

To edit the parameters of an Access Category, left-click the relevant line. In the opened window, change the needed parameters.

Edit Access Point: Background	×
AIFSN*	
7	•
CWMin	
31	•
CWMax	
1023	•
TXOP*	
0	
ACM	
АСК	
SAVE CLOSE	

Figure 108. The window for changing parameters of the WMM function.

Parameter	Description
AIFSN	<i>Arbitrary Inter-Frame Space Number</i> . This parameter influences time delays for the relevant Access Category. The lower the value, the higher is the Access Category priority.
CWMin / CWMax	<i>Contention Window Minimum/Contention Window Maximum.</i> Both fields influence time delays for the relevant Access Category. The CWMax field value should not be lower, than the CWMin field value. The lower the difference between the CWMax field value and the CWMin field value, the higher is the Access Category priority.
ТХОР	<i>Transmission Opportunity</i> . The higher the value, the higher is the Access Category priority.
ACM	<i>Admission Control Mandatory.</i> If the switch is moved to the right, the device cannot use the relevant Access Category.

Parameter	Description
ACK	Acknowledgment. Answering response requests while transmitting. Displayed only in the Access Point section.If the switch is moved to the left, the router answers requests.If the switch is moved to the right, the router does not answer requests.

Click the **SAVE** button.

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.

< wмм		Client		
2.4	GHz		5GHz	
Wi-Fi Client You can configure the router as	a client to connect to a wirele	ess access point or to a WISP.		
Enable Broadcast wireless n If the broadcast switch is moved router's WLAN. Upon that the router wireless client	to the left, devices cannot connec			
wireless client. Connecting to network Select network from list		•		
APPLY Wireless Networks	UPDATE LIST			
Network name (SSID)		Security Settings	Ch	annel
RT-WiFi-799C		[WPA2-PSK/WPA3-SAE mixed] [AES]		10
🗟 [SDK2] DIR-620-2097	,	[WPA2-PSK] [AES]		9

Figure 109. 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
Enable encryption WEP	<i>For Open authentication type only.</i> 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 (\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 key.
Encryption type	An encryption method: TKIP , AES , or TKIP+AES . <i>TKIP</i> and <i>TKIP+AES</i> encryption types are not available for <i>WPA3-SAE</i> and <i>WPA2-PSK/WPA3-SAE</i> 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-830M 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.

Client Shaping

On the **Wi-Fi / Client Shaping** page, you can limit the maximum bandwidth of upstream and downstream traffic for each wireless client of the router by its MAC address.

🕻 Client	Client Shaping	
Client Shap You can limit the	Ding e maximum bandwidth of upstream and downstream traffic for each wireless client of the router by its MAC address.	
Rules No rule created	+	

Figure 110. The Wi-Fi / Client Shaping page.

If you want to limit the maximum bandwidth of traffic for the router's wireless client, create a relevant rule. To do this, click the **ADD** button (+).

Add Rule	×
Frequency band 2.4 GHz	•
ssid DIR-XXX	•
C Enabled	
MAC address*	•
Upload	
Not limited	
Maximum rate (Mbit/s)*	
Download	
Not limited	
Maximum rate (Mbit/s)*	
SAVE	

Figure 111. The window for setting up rate limit.

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.		
Enabled	If the switch is moved to the right, the rule is active. Move the switch to the left to disable the rule.		
MAC address	In the field, enter the MAC address to which the rule 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).		
	Upload		
Maximum rate	Specify the maximum value of the upstream traffic rate (Mbps) or move the Not limited switch to the right not to limit the maximum bandwidth of upstream traffic.		
Download			
Maximum rate	Specify the maximum value of the downstream traffic rate (Mbps) or move the Not limited switch to the right not to limit the maximum bandwidth of downstream traffic.		

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

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

To edit a rule, left-click the relevant rule. 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 in the table and click the **DELETE** button $(\overline{\mathbf{n}})$

the **DELETE** button (III).

To set a schedule for the bandwidth limitation 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 208) 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 bandwidth limitation 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 bandwidth limitation 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.

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	vour WLAN!

😑 🕻 Client Shaping	Addit	tional	
2.4 GHz		5 GHz	
Wi-Fi Additional Settings You can define additional parameters for the Bandwidth Auto ③ Using bandwidth of one or several channels of the simultaneously ③ Current bandwidth: 40 MHz ④ Autonegotiation 20/40 (Coexists) ③ Automatic change of bandwidth in the loaded end TX power (in percent) 100 ● Drop multicast ④ Disables multicasting (IGMP, SSDP, etc.) for the withis helps to improve performance ● Adaptivity mode ④ Reduces influence on operation of other wireless environment. This can lower performance of your wire	wireless network tence) vironment ireless network. In some cases devices in the loaded	B/G protection Auto Short GI Enable Beacon period (in milliseconds)* 100 RTS threshold (in bytes)* 2347 Frag threshold (in bytes)* 2346 DTIM period (in beacon frames)* 1 Station Keep Alive (in seconds)* 0	· ·
APPLY			

Figure 112. 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		
Drop multicast	Move the switch to the right to disable multicasting for the router's WLAN. Move the switch to the left to enable multicasting from the WAN connection selected on the Advanced / IGMP/MLD page. If the switch is moved to the right, the device will not be available by the domain name for Wi-Fi clients.		
Enable TX Beamforming	 Available on the 5 GHz tab. TX Beamforming is the signal processing/directing technique which 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. 		
Adaptivity mode	Move the switch to the right to let the router switch from the channels at which radars and other mobile or stationary radio systems operate in case it interferes with these devices. Such a setting can slow down the router's WLAN. In order to use the adaptivity mode, the automatic channel selection		
	should be enabled (on the Wi-Fi / Basic Settings page).		
Reduce power on OFDM modulation	 Available on the 5 GHz tab. Move the switch to the right to lower service signals strength for improving the quality of their transmission. Use the setting in case of problems with connecting wireless clients to the router. 		
STBC	The STBC (<i>Space-time block coding</i>) technique allows increasing data transfer reliability even for portable devices equipped with poor antennas (smartphones, pads, etc.) due to using several data streams and processing several versions or received data.		
	Move the switch to the right if you need to use the STBC technique. <i>Available on the</i> 2.4 GHz <i>tab.</i>		
B/G protection	 Available on the 2.4 GH2 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. 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. 		

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-830M.

≡	🕻 Additional	MAC Filter	
You	AC Filter a can define a set of MAC address wwed to access the WLAN.	es of devices which will be allowed to access the WLAN, or define MAC addresses of devi	ces which will not be
	It is recommended to cor	nfigure the WI-FI MAC filter through a wired connection to the device	
2.4	4 GHz	5 GHz	
	DIR-XXX ① Off	DIR-XXX-5G ① Off	
	ters + rules created for MAC filter		

Figure 113. 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	•
() MAC filters for this network are disabled	
MAC address*	•
Name*	
() The number of characters should not exceed 32	
Calle Enable	
SAVE	

Figure 114. 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 (\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 208) 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.

EasyMesh

On the **Wi-Fi / EasyMesh** page, you can enable the EasyMesh function. This function is designed to quickly connect several devices into one transport network for providing high-quality Wi-Fi coverage in living units of complicated planning or for creating a large temporary Wi-Fi network for an outdoor event.

A mesh network consists of a main device (the Controller role) and subordinate devices (the Agent role).⁵ Devices connect to each other via wireless or wired connection. The Controller device enables connection and configuration of other devices of the mesh network, controls the data flow and the roaming of clients between devices in this network. Agents execute commands from the Controller device and serve as Wi-Fi access points for subordinate devices.

≡	🗸 Home	Easy	Mesh	
The The clier	Controller dev		The connection can be wired or wireless. vices of the mesh network, controls the data flow and the roaming of n the Controller device and serves as a Wi-Fi access point for client	
Se	ttings		Management	
Dev	Enable	Controller	Simultaneously click the "Establish Connection" button (or the hardware WPS button) on the Agent device and on the Controller device (or on two Agent devices) in order to connect devices and transfer data from one device to another.	
Stat	tus:	Enabled	ESTABLISH CONNECTION	
	ice name* ntroller			
5 0		•	When Agent devices with factory defaults connect to the mesh network via the hardware button, they obtain the wireless settings and the administrator's password of the Controller.	
	APPLY			
Ne	twork topo	logy		
Ĵ	Controller			
	طَّ Agent-e	2b20		

Figure 115. The **Wi-Fi** / **EasyMesh** page.

To activate the EasyMesh function, in the **Settings** section, move the **Enable** switch to the right.

⁵ At present, you can connect up to 6 D-Link devices with EasyMesh support: 1 in the Controller role and 5 in the Agent role.

The following fields are available on the page:

Parameter	Description	
Device role	The current role of the device in the mesh network.	
Status	 The current status of the mesh network. Enabled: The mesh network is enabled and configured. Waiting: Establishing connection and exchanging parameters between the main and subordinate devices. Disabled: The mesh network is disabled. 	
Device name	The name of the device for easier identification. You can specify any name.	
Backhaul band	The band in which the mesh network operates. Select one of the bands (2.4GHz or 5GHz) for all devices of the configured network.	

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

To configure DIR-830M as the main or subordinate device of the mesh network, go to the **Initial Configuration** section (see the *Initial Configuration Wizard* section, page 43), from the **Connection method** list, select the **EasyMesh** value. Then from the **Device Role** list, select the required value.

To complete your mesh network configuration, connect subordinate devices to the main device.

Connecting Subordinate Devices with Ethernet Cable

To connect a subordinate device with an Ethernet cable, follow the next steps:

- 1. Connect an Ethernet cable between any of the LAN ports of the main and subordinate device.
- 2. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.
- 3. Make sure that the connection is established. To do this, in the web-based interface of the main device, on the **Wi-Fi / EasyMesh** page, in the **Network topology** section, check the information on the connected devices.

Connecting Subordinate Devices with Hardware Button

To connect a subordinate device with the hardware **RESET/WPS** button, follow the next steps:

1. Simultaneously press the hardware **RESET/WPS** button on the cover of the main and the subordinate device (or two subordinate devices, if one of them has previously been connected to the mesh network), hold it for 2 seconds, and release.

Do not press the button on more than two devices simultaneously. When Agent devices with factory defaults connect to the mesh network via the hardware button, the 5 GHz backhaul band should be selected on the main device.

- 2. The **Status** LED of DIR-830M should start blinking green. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.
- 3. Make sure the connection is successful. To do this, in the web-based interface of the main device, on the **Wi-Fi** / **EasyMesh** page, in the **Network topology** section, check the information on the connected devices.

Connecting Subordinate Devices via Web-based Interface

To connect a subordinate device with the **ESTABLISH CONNECTION** button in the web-based interface, follow the next steps:

1. Simultaneously press the **ESTABLISH CONNECTION** button in the web-based interface the main and the subordinate device (or two subordinate devices, if one of them has previously been connected to the mesh network).



Do not press the button on more than two devices simultaneously.

- 2. The **Status** LED of DIR-830M should start blinking green. Wait for about 4 minutes for the subordinate device to receive all mesh network settings and web-based interface password from the main device.
- 3. Make sure the connection is successful. To do this, in the web-based interface of the main device, on the **Wi-Fi** / **EasyMesh** page, in the **Network topology** section, check the information on the connected devices.

To view detailed data on a mesh network device, click the line corresponding to this device in the **Network topology** section.

😑 < EasyMesh		EasyMesh			
Device Informat	ion				
Name					Controller
IP address					192.168.0.1
MAC address					00:10:20:30:40:51
Neighbours					
Name	MAC address	Interface	Band	Signal level	RSSI
Agent-eb20	50:2B:73:F6:EB:20	WLAN	5 GHz	47%	28

Figure 116. The device information page.

Advanced

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

- create or edit VLANs
- 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 UPnP IGD protocol
- allow the router to use IGMP and MLD
- allow the router to use RTSP, enable the SIP ALG, the PPPoE/PPTP/L2TP/IPsec pass through functions for the router
- configure VPN tunnels based on IPsec protocol.

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 WAN port. You can edit or delete this VLAN.

≡	🗲 EasyMesh		VL	AN	
VLA You c		onsisting of inte	erfaces and ports of the	router, for example, for distinguishing different types of trafi	fic.
VLA	N List 🕂 🔋				
	VLAN ID	Name	Tagged Ports	Untagged ports	
	-	LAN		DIR-XXX, DIR-XXX-5G, LAN1, LAN2, LAN3	
	-	WAN		WAN	

Figure 117. 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.

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

E 🗸 VLAN	VLAN/	Adding				٤
VLAN Name*			ate Interface n the bridge	" function is disab mode and packet		
(i) The number of characters should	ld not exceed 32		reate interf	ace		
VLAN ID*						
QoS* 0						
Ports						
LAN1 Type Tagged	▼ LAN2 Type Excluded	•		LAN3 🔜 Type Excluded	Ð	
WAN Type Excluded	•					
Wireless interfaces						
DIR-XXX Type Excluded	DIR-XXX-5G Type Excluded	•				
APPLY						

Figure 118. 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.

Parameter	Description
Create interface	Move the switch to the right to create an interface that can be used for creating WAN connections. Upon that the VLAN should include the WAN port. 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.
Ports	 Select a type for each port included in the VLAN. Untagged: Untagged traffic will be transmitted through the specified port. 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 ($\boxed{10}$).

DNS

	DNS	
DNS		
DNS servers are used to determine the I	IP address from the name of a server in Intranets or the Internet. Yo onfigure the router to obtain DNS servers addresses automatically fi	u can specify rom your ISP
IPv4	IPv6	
Manual	Manual	
Default gateway	Default gateway	
Interface	Interface	
statip_81		
Designed to be used by the local networ	rk clients.	
IPv4	rk clients.	
IPv4 1.1.1.1		
IPv4 1.1.1.1 1.0.0.1		
IPv4 1.1.1.1 1.0.0.1 ADD SERVER Reserve Servers		available.
IPv4 1.1.1.1 1.0.0.1 ADD SERVER Reserve Servers		available.
IPv4 1.1.1.1 1.0.0.1 ADD SERVER Reserve Servers Designed to be used by the router when	the addresses specified manually or obtained automatically are un	available.
IPv4 1.1.1.1 1.0.0.1 ADD SERVER Reserve Servers Designed to be used by the router when IPv4	n the addresses specified manually or obtained automatically are un	available.

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

Figure 119. 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	
_	DDNS On the DDNS page, you can define parameters of the DDNS set	rvice, which allows associating a domain name with dynamic IP addresses.	
_	DDNS List +		

Figure 120. The Advanced / DDNS page.

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

< ddns	Add DDNS	
Cnable	Username*	
Hostname		
For example: host.ru	× Password*	Q
ADD HOST	Interface* Default gateway	•
DDNS service* changeip.com	Update period (in minutes)*	
SAVE		

Figure 121. The page for adding a DDNS service.

Parameter	Description
Enable	Move the switch to the right to enable DDNS. Move the switch to the left to disable DDNS.
Hostname	Enter the full domain name registered at your DDNS provider. 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.

Ports S	Settings			
		tion of speed and duplex mod u can enable or disable data fle		
Port	Status	Autonegotiation	Speed	Flow control
LAN1	Disconnected	On	-	
LAN2	Disconnected	On	-	-
LAN3	Connected	On	1000M-Full	802.3x(tx+rx)
	Connected	On	1000M-Full	Off

Figure 122. 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.

LAN1	×
Speed Auto	•
Autonegotiation Modes	
1000M-Full	
100M-Full	
100M-Half	
10M-Full	
10M-Half	
Flow control	
Symmetric flow control	
SAVE	

Figure 123. 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 tr	ansfer 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.	
Symmetric now control	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 Set	tings Redirect	
Dedin		
Redire	ect	
	enable notifications on the reason of the Internet connection failure. Notifications will be displayed in the browser window when a user is ng to open a web site on the Internet.	
DISABL	E	
Reaso	ns for Redirect	
	Physical connection error	
•	No connection	
	The device is not configured	
APPI	Y	

Figure 124. 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 125. The Advanced / Routing page.

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

Add Route	×
Chable	
Protocol*	
IPv4	•
Interface*	
Auto	-
Destination netmask*	
Gateway*	
Gutoway	
Metric	
Table*	

Figure 126. The window for adding a new route.

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	<i>For IPv4 protocol only.</i> 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.

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

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.

Routing	TR-069 Client	2
TR-069 Client		
You can configure the router for communication with The TR-069 client is used for remote monitoring and		
Enable TR-069 client	Inform Settings	
Interface*	On	
Automatic	 Interval (in seconds) 120 	
Auto Configuration Server Settings	Connection Request Settings	
Auto Configuration Server Settings Get URL address via DHCP	Connection Request Settings Username	
	Username	
Get URL address via DHCP		Ø
Get URL address via DHCP	Username	Ø

Figure 127. The page for configuring the TR-069 client.

You can specify the following parameters:

Parameter	Description		
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 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.				
PasswordThe password to connect to the ACS. Click the Show 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 $\ensuremath{\mathsf{APPLY}}$ 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.

≡ < TR-06	9 Client	UPnP IG	5D		
	the UPnP IGD protocol ations requiringan incor	. The router uses the UPnP IGI ming connection to the router.		configuration of its parameters fo	or
IPv4 IGD					
Protocol	IP address	Private port	Public port	Description	
IPv6 IGD					
Protocol	IP address	Private port	Public port	Pinhole ID	

Figure 128. 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	The IP address of a client from the local area network.A port of a client's IP address to which traffic is directed from a public port of the router.			
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.

IGMP/MLD

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

IGMP and MLD are used for managing multicast traffic (transferring data to a group of destinations) in IPv4 and IPv6 networks correspondingly. These protocols allow using network resources for some applications, e.g., for streaming video, more efficiently.

✓ UPnP IGD IGN	1P/MLD
IGMP	MLD
Internet Group Management Protocol is designed to manage multicast traffic in IP-based networks.	
Enable	Carlos Enable
IGMP version	MLD version
IGMPv2	MLDv1v2
Interface*	Interface
statip_61 -	Not selected

Figure 129. The Advanced / IGMP/MLD page.

The following elements are available on the page:

Parameter	Description		
IGMP			
Enable	Move the switch to the right to enable IGMP.		
IGMP version	Select 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).		

Parameter	Description	
	MLD	
Enable	Move the switch to the right to enable MLD.	
MLD versionSelect a version of MLD from the drop-down list.		
Interface	From the drop-down list, select a connection of the Dynamic IPv6 or Static IPv6 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.

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

Figure 130. 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. ⁶		
RTSP	Move the switch to the right to enable RTSP. Such a setting allows managing media stream: fast forward streaming audio/video, pause and start it.		
PPPoE pass through	Move the switch to the right to enable the PPPoE pass through function.		
IPsec pass through	Move the switch to the right to enable the IPsec pass through function.		
L2TP pass through	Move the switch to the right to enable the L2TP pass through function.		
PPTP pass through	Move the switch to the right to enable the PPTP pass through function.		

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

⁶ 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).

IPsec

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

≡	ALG/Passthrough		IPsec		
You	SEC can configure VPN tunnels based on IPsec p ABLE	protocol.			
Ba	;ing level SiC		•		
Tu	nnels reconnect 🕂 🗍				
			Encryption/hashing alg	orithm	
	Remote host Mode	Interface	The First Phase	The Second Phase	
	itus note host	IKE	CHILD	State	

Figure 131. The Advanced / 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 213).

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< th=""><th>IPsec/Adding</th><th></th></ipsec<>	IPsec/Adding	
General Settings		
Calle Enable	Enable DPD	
Name*	() DPD - Dead Peer Detection	
ipsec_12	DPD delay (in seconds)*	
(i) The number of characters should not exceed 32	30	
IP version	DPD timeout (in seconds)*	
IPv4	▼ 120	
Dynamic IPsec	TCP MSS	
	Path MTU discovery	•
Type Address	•	
Remote host*		
Remote identifier		
Remote port		
Pre-shared key*	<u>م</u>	
Local WAN Default gateway	-	
Local identifier		
Local port		
NAT Traversal Enabled	-	
Mode	•	
Allow traffic from IPsec to router		

Figure 132. 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.	
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. ⁷	
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.	
Туре	 Select an identification method for the remote host (router) from the drop-down list: Address: The remote host is identified by its IP address. 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. 	
Remote host	Enter the remote subnet VPN gateway IP address if the Address value is selected from the Type drop-down list. 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-830M 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.	

^{7 0-9,} A-Z, a-z, space, !"#%&'()*+,-./:;<=>?@[\]^_`{|}~.

Parameter	Description
Pre-shared key	A PSK key for mutual authentication of the parties. Click the Show icon (\bigotimes) to display the entered key.
Local WAN	 A WAN connection through which the tunnel will pass. Select a value from the drop-down list. 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-830M 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.
NAT Traversal	 The NAT Traversal function allows VPN traffic to pass through the NAT-enabled device. DIR-830M allows to forcibly encapsulate VPN traffic in UDP packets for passing through a remote device regardless of whether it supports address translation. 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.
Mode	 An operation mode of the IPsec tunnel. Select a value from the drop-down list. 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.

Parameter	Description
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.
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.
TCP MSS	 Maximum Segment Size of a TCP packet. This parameter influences the size of a TCP packet which will be sent from the remote host to the router. 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	C Enable PFS	
MODP768	Second phase DHgroup type	
IKE-SA lifetime*	MODP768	
10800	IPsec-SA lifetime*	
Aggressive Mode	1Psec-3A lifetime* 3600	
IKE version		
1	•	

Figure 133. 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.	

Parameter	Description	
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.	
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-830M.	
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	×
.ocal network	
ADD SUBNET	
Specify the local subnet of IPsec tunnel (the outer's LAN). Example: 192,168.0.0/24	
Remote subnet	
ADD SUBNET	
Specify the remote subnet of IPsec tunnel (the lof the device which acts as a router). Example: 192.168.10.0/24	LAN
NTU*	
1300	

Figure 134. The page for adding an IPsec tunnel. The window for adding a tunneled network.

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

Parameter	Description
Local network	A local subnet IP address and mask. 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 (*) in the line of the subnet address.
Remote subnet	A remote subnet IP address and mask. 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 (×) in the line of the subnet address.
МТО	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 ($\overline{10}$). 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 ($\overline{10}$). Also you can remove a tunnel on the editing page.

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

Firewall

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

- add rules for IP filtering
- create virtual servers
- define a DMZ
- configure the MAC filter
- 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 135. The Firewall / IP Filter page.

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

🗮 < IP Filte		IP Filte	er/Adding 🛛
General Se	ettings		Source IP address
Cnable	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
(i) The number of a	characters should no	at exceed 32	Range or single IP address
Action			
Allow		•	Start IPv4 address -
Protocol			
TCP		-	End IPv4 address -
IP version			
IPv4		•	_
Direction Source		Destination	
LAN	•	WAN -	
Source interface		Destination interface	
Auto		Auto -	
Destinatio	n IP addre	SS	Ports
-		ses, a single IP address, or a subnet IP	You can specify one port, several ports separated by a comma (for example,
address (for example 2001:0db8:85a3:08d			80,90), or a range of ports separated by a colon (for example, 80:90)
Set as			Destination port
Range or single	e IP address	-	
			Set source port manually
Start IPv4 addr	ess	•	-
End IPv4 addre	ess	-	
			-
APPLY			
APPLI			

Figure 136. 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.
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.

Parameter	Description
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. 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). 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-830M. WAN: The rule will be applied to the packets transmitted to the local network. LAN: The rule will be applied to the packets transmitted to the local network. From the Source interface and Destination interface drop-down list, 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.
Start IPv4 address / Start IPv6 address	The source host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank. You can choose a device connected to the 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.

Parameter	Description
	Destination IP address
Set as	Select the needed value from the drop-down list.
Start IPv4 address / Start IPv6 address	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank. You can choose a device connected to the 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 destination host end IPv4 or IPv6 address.
Subnet IPv4 address / Subnet IPv6 address	The destination subnet IPv4 or IPv6 address. The field is displayed when the Subnet value is selected from the Set as drop-down list.
	Ports
Destination port	A port of the destination IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.
Set source port manually	Move the switch to the right to specify a port of the source IP address manually. Upon that the Source port field is displayed.
Source port	A port of the source IP address. You can specify one port, several ports separated by a comma, or a range of ports separated by a colon.

Click the **APPLY** button.

To set a schedule for the IP 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 208) 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. In the opened window, 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. 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 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 137. The Firewall / Virtual Servers page.

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

E 🗸 Virtual Servers Vir	tual Servers/Adding
General Settings	Private Network Settings
Name*	Private IP*
 The number of characters should not exceed 32 Template 	Private port* ① 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></all>	• •
Protocol TCP	•
NAT Loopback	
Public Network Settings Remote IP	
You can specify a single IP address, or a subnet IP address (for exam 10.10.10.10/24)	iple,
Remote IP	×
ADD REMOTE IP	
Public port*	
You can specify one port, several ports separated by a comma (for el. 80,90), or a range of ports separated by a colon (for example, 80:90)	xample,
APPLY	

Figure 138. 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.
Name	A name for the virtual server for easier identification. You can specify any name.

Parameter	Description
Template	Select a virtual server template from the drop-down list, or select Custom to specify all parameters of the new virtual server manually.
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	Move 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
Remote IP	 Enter the IP address of the server from the external network. To add one more IP address, click the ADD REMOTE IP button and enter the address in the displayed line. To remove the IP address, click the Delete icon (×) in the line of the address.
Public port	A port of the router from which traffic is directed to the IP address specified in the Private IP field in the Private Network Settings section. You can specify one port or several ports separated by a 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 server. 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 208) 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 server. 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 ($\boxed{10}$). Also you can remove a server on the editing page.

DMZ

A DMZ is a host or network segment located "between" internal (local) and external (global) networks. In the 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	
DMZ		
A DMZ is a host or network segment located "betwee	n" internal (local) and external (global) networks. In the router, the DN g to a port of the router from the external network to a specified host	
Chable 🕓		
Enable NAT Loopback		
IP address*		
APPLY		

Figure 139. 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 208) 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		
	ddress-based filtering for computers of the router's LAN.	
Default mode Allow	•	
List of Exceptions No rules created for MAC		

Figure 140. 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 F	Rule	×
	Enable rule	
Allow		·
MAC a	ddress*	*
Name*		
(i) The I	number of characters should not exceed 32	
SAVE		

Figure 141. The window for adding a rule for the MAC filter.

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. 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. 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). The name of the device for easier identification. You can specify any name. 	
Action		
MAC address		
Name		

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

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 208) 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

the **DELETE** button (1). Also you can remove a rule in the editing window.

URL Filter

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

K MAC Filter U	RL Filter
URL Filter You can specify restrictions on access to certain websites. Rules ca from the list.	an be applied to those devices that are added to the list or to all but devices
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 142. 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. Begin: The request address should begin with 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 ($\overline{10}$). 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 (()). 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 208) 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.

AdBlock	
URL	
() Here you can add, edit, and remove addresses of files which contain host lists.	
ADD	
	URL (1) Here you can add, edit, and remove addresses of files which contain host lists.

Figure 143. 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 **Advanced / Remote Access** page, you can configure access to the web-based interface of the router. By default, the access from external networks to the router is closed. If you need to allow access to the router from the external network, create relevant rules.

TR-069 Client	Remote Access	
Remote Access You can configure access to the web-based interfa closed. If you need to allow access to the router fi	ace of the router. By default, the access from external networks to the rout rom the external network, create relevant rules.	er is
Rules + No rules created for remote access		

Figure 144. The Advanced / Remote Access page.

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

Add Rule $ imes$
Cable Enable
Name*
(i) The number of characters should not exceed 32
Interface
Automatic -
IP version
IPv4
ID address*
IP address*
IP address*
Mask*
Mask* Public port*
Mask* Public port* 80
Mask* Public port* 80 Protocol

Figure 145. The window for adding a rule for remote management.

In the opened window	you can specify the	following parameters:
in the opened whiled w	jou oun speen june	rono ning 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.
Mask	<i>For the IPv4-based network only.</i> The mask of the subnet.
Public port	<i>For the IPv4-based network only.</i> An external port of the 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 (\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 208) 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		Reset factory default settings	
admin	6	Backup Save current configuration to a file	
New password	Q	Restore Load previously saved configuration to the device	
Password should be between 1 and 31 AS characters	CII	Save Save current settings	
Password confirmation	ø	Reboot device	
SAVE		Idle time (in minutes)* 5	
Language English	•	(j) When the function "Stay signed in" is enabled, then users are not redirected to the login page despite the specified idle time.	
		SAVE	

Figure 146. 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.⁸ Click the **Show** icon (\bigotimes) 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/WPS** 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.

^{8 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/WPS button (see the <i>Back Panel</i> section, page 14).
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 **Idle 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.

😑 < Configuration	Firmw	are Update 🖸
Local Update (a) Current firmware version: 4.0.1 (b) Restore factory defaults after field is not selected UPDATE FIRMWARE	firmware update	Remote Update Remote server URL fwupdate.dlink.ru ADD Check for updates automatically Interval (in seconds)* 43200 It is unable to perform check for a new firmware version

Figure 147. 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 / 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, set rules for limitation of wireless client maximum bandwidth, 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 221).

<	Firmware Update	Schedule	
ľ	Auto Reboot		1
	State	Off	
	REBOOT ON SCHEDULE		
	All Tasks +		

Figure 148. 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.

		ormed only if the system time of chronized with an NTP server.
Syster	n Time:	4 April 2022, 12:4
Mode		
Simp	lified mode	•
() In	e number of charac	ters should not exceed 32
Interva	e number of charac I of execution y day	ters should not exceed 32
Interva	l of execution	ters should not exceed 32 • Minutes (0-59)
Interva	l of execution y day	-

Figure 149. 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.

Schedu		×
		ed only if the system time of nized with an NTP server.
System Tin	ie:	4 April 2022, 12:55
D Pe	rform task or	n schedule
Mode		
Simplified	mode	•
Schedule	name*	
The num Interval of ex Every day	ecution	should not exceed 32
Hou Time 0	rs (0-23)	Minutes (0-59) O
<u> </u>	5, 12" or "2-12")	imeters, use the symbol "," or "-" (for
Hours*	Minutes*	Seconds*
0	0	30
SAVE		

Figure 150. 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		
Simplified mode			
Schedule name	Specify a schedule name for easier identification. You can specify any name.		
Interval of execution	 Specify the time period for performing a task. 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 ($\boxed{10}$).

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.

😑 🗶 Schedule	Log 🖸
Log	Settings
Logging You can set the system log options.	
Type Remote and local	Level Informational messages ✓
The system log is stored in the router's memory and sent to the remote host specified in the "Server" field	
Server*	_
Port* 514	_
APPLY	

Figure 151. 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			
Туре	 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. 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.		
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	L	og 🖸
	Log	Settings
Aug 7 17:40: Aug 7 17:43: Aug 7 17:44: Aug 7 17:44: Aug 7	EXPORT REDIRECTto-ports 5555] 13 [DBG] unload firewall rule[11185]: Rule # 13 [DBG] check diff args[72]: dnsmasq@26(res: 13 [TRCE] load[11185]: Generic stream failure 14 [INFO] CONFIG[11185]: Saving config - OK 14 [DBG] dwatcher[wrkr][11218]: Process acti: 19 [TRCE] load[11262]: Saving config - OK 20 [INFO] CONFIG[11262]: Saving config - OK 20 [INFO] dwatcher[wrkr][11263]: Process acti: 49 [INFO] udhcpc[442]: sending renew to 192.14 49 [INFO] udhcpc[442]: sending renew to 192.14 49 [INFO] udhcpc[442]: sending renew to 192.15 50 [DBG] update udhcpc[11767]: action=send_r ice. Network.Interface.Ethernet.2.; 50 [DBG] pynPortMap[11775]: could not open l 50 [INFO] dhcp_opt_print[11769]: Option(1): 2 50 [INFO] dhcp_opt_print[11769]: Option(3): 1 50 [INFO] dhcp_opt_print[11769]: option(5): 1 50 [INFO] dhcp_opt_print[11769]: option(5): 1 50 [INFO] dhcp_opt_print[11769]: option(5): 2 50 [INFO] dhcp_opt_print[11769]: option(5): 1 50 [INFO] dhcp_opt_print[11769]: option(5): 2 50 [INFO] dhcp_opt_print[11769]: option[5]: 2 50 [INFO] dhcp_opt_print[11769]: option[5]: 2 50 [INFO] dhcp_opt_print[11769]: option[5]: 2 50 [INFO] dhcp_opt_print[11769]: option[5]: 2 50 [INF	<pre>10002 UNLOADED 10002 UNLOADED tart): arguments are equal, nothing to do pon: ConfigSaved self.1 self.1 self.1 self.1 self.1 stop_on_fail=0; 58.161.1 1.1.1 1.0.0.1 500 192.168.161.1 stop_on_fail=0; eme in url=; with invalid token: f6ce7a0e-5d59-4b62-89a2-a24c49ec5d1b with invalid token: f6ce7a0e-5d59-4b62-89a2-a24c49ec5d1b .</pre>

Figure 152. 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	Pi	ng	
Ping			
You can check availability of	a host from the local or global r	etwork via the ping utility.	
Host*	Number of attempts*	IPv6 MOR	E SETTINGS
			1.
	START CLE	AR CANCEL	

Figure 153. 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 by 56	tes)*	
 Specifies the Waiting for respo 3 	<i>number of data b</i> nse (in seconds)*	ytes to be sent.
0	ffects only timeou vise ping waits for	t in absence of any two RTTs
ОК	DEFAULT	TSETTINGS

Figure 154. 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.

Ping Traceroute	
Traceroute You can determine the route of data transfer to a host via the traceroute utility.	
Host* IPv6 MORE SETTINGS	
START CLEAR CANCEL	

Figure 155. 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.

		×
Max 30	imum TTL value*	
-	The maximum number of hops	
-	The number of probe packets to a hop time (in seconds)*	
i	Waiting for response (in seconds)	
	OK DEFAULT SETTINGS	

Figure 156. 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.

<	Traceroute Teli	Telnet/SSH		
	Telnet/SSH You can enable or disable access to the device settings via TELNET and S	SH from y	our LAN.	
	D Enable Telnet		Enable SSH	
	Port	Port		
	23	22	6	
	APPLY			

Figure 157. 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.

	Systen	n Time 🖸
System time You can set up automatic synchro	nization of the system time	with a time server on the Internet.
 Enable NTP UTC offset settings 		Time interval between NTP requests after synchronization with NTP server Auto
 Configure daylight sav Get NTP server addres 	-	Time interval between NTP requests for unsynchronized NTP client Auto
Run as a server for the	-	Time zone* Europe/Moscow
System date: System time:	24.06.2021	DETERMINE TIMEZONE
Synchronization:	Completed	
NTP Servers		
pool.ntp.org	×	
ADD SERVER		
APPLY		

Figure 158. 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 on 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.

- Select your time zone from the Time zone drop-down list. To set the time zone in accordance with the settings of your PC 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.

Additional settings are also available on the page:

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 manuallyMove the switch to the right to configure settings for daylight time for the router clock manually. In the Daylight Savin section displayed, specify the required offset time for saving time (in minutes), and specify the needed value Beginning of daylight saving time and End of constraints.		
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 NTP requests for unsynchronized NTP client	 A time period (in seconds) after which a request to synchronize the system time will be sent to the NTP server. Select the needed value from the drop-down list. Auto: The time period is defined automatically. Manual: The time period is defined in accordance with the value specified in the Interval value field. 	
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-830M 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.

System Time	Auto Provision	E
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		
APPLY		

Figure 159. The page for configuring the Auto Provision function.

You can specify the following parameters:

Parameter	Description	
Enable Auto ProvisionMove the switch to the right to enable the Auto Provision functionMove 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 curren 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	Settings		
SkyDNS Sky	(yDNS vice for web content filtering	g and safe Internet access.	
Safe Internet at Home		Web Content Filtering Service for Public Wi-Fi Networks	
A convenient instrument for parental provision for home users accessing the		Reliable protection for public Wi-Fi hotspots in cafes, restaurants, fitness clubs, movie theaters, etc.	
Protection Against Malware		Convenient Management	
The service also protects against main resources, and botnets.	vare, phishing	Highly flexible filtering parameters; clear and simple interface.	
Basic Settings		Account	
DISABLE		Mail* test@dlink.ru	
Provider SkyDNS	A	Password*	
Provider is available		Passwoi u -	Ø
GO TO PERSONAL PROFILE PAGE		Tariff	-
Default profile*		Домашний	
Основной	•	 Successfully authorized 	
Sync period (in seconds)* 3600			
APPLY MANUALLY SYNC			

Figure 160. 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

On the **SkyDNS / Devices and Rules** page, you can assign a specific filtering profile to a device connected to the router's network.

✓ Settings	Devices and Rules			
Known Clients				
IP address	MAC address	Name	Profile	
192.168.0.129	d0:17:c2:00:29:85	android-c2dfe5fa660d5ed1	Основной	
Rules +	Î			
(i) For all devices not in	ncluded in the table the default	profile set in the settings will be used	<i>d.</i>	
MAC address		Profile Ho:	stname	

Figure 161. 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 162. 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

Terms and Conditions for Installation, Safe Operation, Storage, Transportation, and Disposal

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 (reception/transmission of data in computer networks); installation should be performed in accordance with the documents available on the official website.

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. The electrical outlet must be installed near the equipment and must be easily accessible.

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 device may be stored and transported only in the original packaging at the temperature and humidity indicated in the specifications. No restrictions apply to sales. Please contact an authorized distributor to dispose of the equipment upon the end of its operation.

The service life of the device is 2 years.

The warranty period starts on the date of purchase from an authorized distributor within Russia or the CIS countries and extends for one year.

Irrespective of the date of purchase, the warranty period cannot exceed 2 years from the date of manufacture, which is determined by 6^{th} (year) and 7^{th} (month) digit in the serial number printed on the device label.

Year: E - 2014, *F* - 2015, *G* - 2016, *H* - 2017, *I* - 2018, *J* - 2019, *0* - 2020, *I* - 2021, *2* - 2022, *3* - 2023.

Month: 1 – January, 2 – February, ..., 9 – September, A – October, B – November, C – December. If a fault is detected, please contact D-Link service center or technical support group.

Wireless Installation Considerations

The DIR-830M device lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF noise in your home or office. To maximize your wireless range, follow the guidelines below.

- 1. Keep the number of walls and ceilings between the DIR-830M 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
МІВ	Management Information Base
ΜΙΜΟ	Multiple Input Multiple Output
MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
МТU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Controller
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing

PAP	Password Authentication Protocol
РВС	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
ΤΚΙΡ	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