

User Manual



DIR-1260

AC1200 Wave 2 MU-MIMO Wi-Fi Gigabit Router with 3G/LTE Support and USB Port

Contents

Chapter 1. Introduction	6
Contents and Audience	6
Conventions	6
Document Structure	6
Chapter 2. Overview	7
General Information	
Specifications	
Product Appearance	
Upper Panel	
Back Panel	
Delivery Package	
Chapter 3. Installation and Connection	
Before You Begin	
Connecting to Mobile Device with D-Link Assistant Application	
Connecting to PC	
PC with Ethernet Adapter	
Obtaining IP Address Automatically (OS Windows 7)	
Obtaining IP Address Automatically (OS Windows 10)	
PC with Wi-Fi Adapter	
Obtaining IP Address Automatically and Connecting to Wireless Network	•••
(OS Windows 7)	35
Obtaining IP Address Automatically and Connecting to Wireless Network	••55
(OS Windows 10)	38
Connecting to Web-based Interface	
Web-based Interface Structure	
Summary Page	
Home Page	
Menu Sections	
Notifications	
Chapter 4. Configuring via Web-based Interface	
Initial Configuration Wizard	
Selecting Operation Mode	
Router	
Access Point or Repeater	
Creating 3G/LTE WAN Connection	
Changing LAN IPv4 Address	
Wi-Fi Client	
Configuring Wired WAN Connection	
Static IPv4 Connection	
Static IPv6 Connection	
PPPoE, IPv6 PPPoE, PPPoE Dual Stack,	••••
PPPoE + Dynamic IP (PPPoE Dual Access) Connections	62
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 Wileless Network Configuring LAN Ports for IPTV/VoIP	
Changing Web-based Interface Password	
Connection of Multimedia Devices	

Statistics. .75 Network Statistics. .75 DHCP. .76 Routing. .77 Clients and Sessions. .79 Port Statistics. .80 Multicast Groups. .81 IPsec Statistics. .82 VPN Statistics. .82 VPN Statistics. .82 WAN. .84 Creating Dynamic IPV4 or Static IPV4 WAN Connection. .84 Creating Pprox IPFCE WAN Connection. .89 Creating PPECE WAN Connection. .92 Creating PPECE WAN Connection. .92 Creating PPECE WAN Connection. .92 Creating PPECE NAN Connection. .94 Creating PPECE NAN Connection. .97 Creating Mobile Internet WAN Connection. .100 Creating 614 WAN Connection. .121 Creating 614 WAN Connection. .122 LNN. .124 IPV4. .124 IPv6. .30 WAN Failover. .33 Auto Configuration of 3G/LTE. .35 PTF/LITP Servers. .16 <		
DHCP.		
Routing.		
Clients and Sessions.		
Port Statistics. 80 Multicast Groups 81 IPsec Statistics. 82 VPN Statistics. 83 Connections Setup 84 WAN. 84 Creating Dynamic IPv4 or Static IPv4 WAN Connection. 86 Creating Dynamic IPv6 or Static IPv6 WAN Connection. 89 Creating PPTP WAN Connection. 92 Creating PPTP, L2TP, L2TP Dual Stack, or 97 L2TP over IPsec WAN Connection. 97 Creating PPTP, L2TP, L2TP PDeI Jal Stack WAN Connection. 104 Creating PPTP WAN Connection. 104 Creating ford WAN Connection. 119 Creating Gtod WAN Connection. 121 Creating Gtod WAN Connection. 122 IPv6. 130 WAN Pailover. 124 IPv4. 124 IPv6. 130 WAN Pailover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 161 VPN. 162 GRE. 153 PPTP/L2TP Servers. 153 VPN Users. 161		
Multicast Groups. .81 TPsec Statistics. .62 VPN Statistics. .83 Connections Setup. .84 WAN. .84 Creating Dynamic IPv4 or Static IPv4 WAN Connection. .86 Creating PPTP LTP6 or Static IPv6 WAN Connection. .89 Creating PPTP, L2TP, L2TP Dual Stack, or .92 Creating PPTP IPSe WAN Connection. .97 Creating Mobile Internet WAN Connection. .97 Creating Gin4 WAN Connection. .100 Creating Gin4 WAN Connection. .116 Creating Gin4 WAN Connection. .121 Creating Gin4 WAN Connection. .122 LAN. .124 IPv4. .124 IPv4. .124 IPv4. .124 IPv5. .130 WAN Failover. .135 Auto Configuration of 3G/LTE. .138 Treffic Balancing. .140 VPN. .142 IPPr. .151 IPTP. .161 EGRE. .161 EORE. .161 EORE. .161		
IPsec Statistics. 82 VPN Statistics. 83 Connections Setup. 84 WAN. 84 Creating Dynamic IPv4 or Static IPv4 WAN Connection. 86 Creating PPDE WAN Connection. 89 Creating PPDE WAN Connection. 92 Creating PPDE WAN Connection. 92 Creating PPDE WAN Connection. 97 Creating PPDE IPv6 or PPED Dual Stack wan Connection. 100 Creating IPIP6 WAN Connection. 110 Creating Girl WAN Connection. 110 Creating Girl WAN Connection. 110 Creating Girl WAN Connection. 112 Creating Girl WAN Connection. 121 Creating Girl WAN Connection. 122 LAN. 124 IPv4. 124 IPv4. 124 IPv6. 130 WAN Failover. 142 Mat Configuration of 36/LTE. 135 Auto Configuration of 36/LTE. 161 IPv6. 162 EoIP. 163 VPN. 162 EoIP. 163 VPN. <td></td> <td></td>		
VPN Statistics. .83 Connections Setup. .84 WAN. .84 Wan. .84 Creating Dynamic IPv4 or Static IPv4 WAN Connection. .89 Creating PPTS Data .89 Creating PPTP, L2TP, L2TP Dual Stack, or .92 Creating PPTP, L2TP, L2TP Dual Stack, or .97 Creating PPTP (PPOF or PPOE Dual Stack WAN Connection. .97 Creating Mobile Internet WAN Connection. .104 Creating Gin4 WAN Connection. .105 Creating Gin4 WAN Connection. .121 Creating Gin4 WAN Connection. .122 LAN. .124 IPv4. .124 IPv6. .135 Auto Configuration of 3G/LTE. .135 PTP/L2TP Servers. .151 IPTP .162 EoIP. .164 Wi-	Multicast Groups	
Connections Setup. 84 WAN. 84 Creating Dynamic IPv4 or Static IPv4 WAN Connection. 86 Creating Pynamic IPv6 or Static IPv6 WAN Connection. 89 Creating PPDE WAN Connection. 92 Creating PPTP, L2TP, L2TP Dual Stack, or 92 Creating PPTE IPv6 or PPFOE Dual Stack WAN Connection. 97 Creating PPTE IPv6 or PPFOE Dual Stack WAN Connection. 104 Creating TPTE WAN Connection. 116 Creating Gin4 WAN Connection. 116 Creating 6rd WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 GRE. 151 IPIP. 153 VPN Users 164 Wi-Fi. 165 VPN Users 161 EoGRE. 162 EoIP. 164 Wi-Fi. 165 Using WFS Function via Web-based Interface. 179 <td></td> <td></td>		
WAN.	VPN Statistics	83
Creating Dynamic IPv6 or Static IPv6 WAN Connection. .86 Creating Dynamic IPv6 or Static IPv6 WAN Connection. .89 Creating PPPEW WAN Connection. .92 Creating PPTP, L2TP, L2TP Dual Stack, or .97 L2TP over IPsec WAN Connection. .97 Creating PPDE IPv6 or PPPoE Dual Stack WAN Connection. .104 Creating Mobile Internet WAN Connection. .106 Creating Gin4 WAN Connection. .110 Creating Gin4 WAN Connection. .121 Creating Gin4 WAN Connection. .122 LAN. .124 IPv6. .122 LAN. .124 IPv6. .130 WAN Failover. .133 Auto Configuration of 3G/LTE. .138 Traffic Balancing. .142 IPsec. .142 GRE. .161 EOGRE. .162 EoTP. .164 Wi-Fi. .167 Basic Settings. .167 Dasic Settings. .167 Dasic Settings. .177 Using WPS Function via Web-based Interface. .179 Using WPS F	Connections Setup	84
Creating Dynamic IPv6 or Static IPv6 WAN Connection. 89 Creating PPDE WAN Connection. 92 Creating PPTP, L2TP, L2TP Dual Stack, or 97 L2TP over IPsec WAN Connection. 97 Creating PPDE IPv6 or PPDE Dual Stack WAN Connection. 104 Creating Mobile Internet WAN Connection. 110 Creating for WAN Connection. 110 Creating Gin4 WAN Connection. 112 Creating 6in4 WAN Connection. 121 Creating 6in4 WAN Connection. 122 LAN. 124 IPv4. 124 IPv4. 124 IPv6. 130 WAN Failover. 138 Traffic Balancing. 140 VPN. 142 IPsec. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Dasic Settings. 167 Client Management. 177 Using WPS Function via Web-based Interface. 179 Using WPS Funct	WAN	
Creating PPPoE WAN Connection. 92 Creating PPTP, L2TP Dual Stack, or 97 L2TP over IFsec WAN Connection. 97 Creating PPDE IPv6 or PPDE Dual Stack WAN Connection. 104 Creating IPTP6 WAN Connection. 110 Creating Gin4 WAN Connection. 110 Creating Gin4 WAN Connection. 112 Creating Gin4 WAN Connection. 121 Creating Gin4 WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 GRE. 142 GRE. 142 GRE. 151 IPTP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EOGRE. 162 EoIP. 164 Wi Fi. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 <t< td=""><td>Creating Dynamic IPv4 or Static IPv4 WAN Connection</td><td> 86</td></t<>	Creating Dynamic IPv4 or Static IPv4 WAN Connection	86
Creating PPTP, L2TP, L2TP Dual Stack, or 97 L2TP over IBsec WAN Connection. 97 Creating PPF0E IPv6 or PPP0E Dual Stack WAN Connection. 104 Creating Mobile Internet WAN Connection. 110 Creating fin4 WAN Connection. 116 Creating 6to4 WAN Connection. 119 Creating 6to4 WAN Connection. 121 Creating 6to4 WAN Connection. 122 LAN. 124 IPv4. 124 IPv4. 124 IPv4. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPTP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EOGRE. 162 EoIP. 164 Wi-Fi. 167 Using WPS Function via Web-based Interface. 179 Using WPS Function via Web-based Interface. 180 WMM. 181 Client. 184	Creating Dynamic IPv6 or Static IPv6 WAN Connection	
L2TP over IPsec WAN Connection. .97 Creating PPDE IPv6 or PPDE Dual Stack WAN Connection. .104 Creating Mobile Internet WAN Connection. .110 Creating IPIP6 WAN Connection. .116 Creating 6in4 WAN Connection. .119 Creating 6in4 WAN Connection. .121 Creating 6in4 WAN Connection. .121 Creating 6in4 WAN Connection. .121 Creating 6rd WAN Connection. .122 LAN. .124 IPv4. .124 IPv6. .130 WAN Failover. .135 Auto Configuration of 3G/LTE. .138 Traffic Balancing. .140 VPN. .142 IPsec. .142 GRE. .151 IPIP. .153 PPTP/L2TP Servers. .155 VPN Users. .167 Client Management. .176 WPS. .167 Using WPS Function via Web-based Interface. .180 WMM. .181 Client. .184 Additional. .181 Reaming. .	Creating PPPoE WAN Connection	
Creating PPPOE IPv6 or PPPOE Dual Stack WAN Connection. 104 Creating Mobile Internet WAN Connection. 110 Creating IPIP6 WAN Connection. 116 Creating 6ind WAN Connection. 119 Creating 6tod WAN Connection. 121 Creating 6tod WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 130 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 142 IPve. 142 GRE. 151 IPIP. 153 PPTP/LZTP Servers. 155 VPN Users 161 EoGRE. 162 EoIP. 164 Wi-Fi. 176 Wasic Settings. 167 Client Management. 177 Using WPS Function via Web-based Interface. 180 WMM. 181 Client. 184 Additional. 181 Client. 184 Additional. 181 Client. 181	Creating PPTP, L2TP, L2TP Dual Stack, or	
Creating Mobile Internet WAN Connection. 110 Creating FIPP6 WAN Connection. 116 Creating 6in4 WAN Connection. 119 Creating 6to4 WAN Connection. 121 Creating 6rd WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 161 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WFS Function via Web-based Interface. 179 Using WFS Function without Web-based Interface. 179 Using WFS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. <	L2TP over IPsec WAN Connection	
Creating Mobile Internet WAN Connection. 110 Creating FIPP6 WAN Connection. 116 Creating 6in4 WAN Connection. 119 Creating 6to4 WAN Connection. 121 Creating 6rd WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 161 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WFS Function via Web-based Interface. 179 Using WFS Function without Web-based Interface. 179 Using WFS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. <	Creating PPPoE IPv6 or PPPoE Dual Stack WAN Connection	
Creating IPIP6 WAN Connection. 116 Creating 6in4 WAN Connection. 119 Creating 6to4 WAN Connection. 121 Creating 6rd WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 GRE. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Basic Settings. 167 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 191		
Creating 6in4 WAN Connection. 119 Creating 6to4 WAN Connection. 121 Creating 6rd WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Basic Settings. 167 Using WPS Function via Web-based Interface. 179 Using WPS Function via Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 191		
Creating 6to4 WAN Connection. 121 Creating 6rd WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 142 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194	-	
Creating 6rd WAN Connection. 122 LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
LAN. 124 IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 GRE. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function via Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
IPv4. 124 IPv6. 130 WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PVPY/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 MMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194	-	
IPv6		
WAN Failover. 135 Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VFN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function via Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
Auto Configuration of 3G/LTE. 138 Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
Traffic Balancing. 140 VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 MMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
VPN. 142 IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
IPsec. 142 GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
GRE. 151 IPIP. 153 PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
IPIP. .153 PPTP/L2TP Servers. .155 VPN Users. .161 EoGRE. .162 EoIP. .164 Wi-Fi. .167 Basic Settings. .167 Client Management. .176 WPS. .177 Using WPS Function via Web-based Interface. .179 Using WPS Function without Web-based Interface. .180 WMM. .181 Client. .184 Additional. .187 MAC Filter. .191 Roaming. .194		
PPTP/L2TP Servers. 155 VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
VPN Users. 161 EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
EoGRE. 162 EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter 191 Roaming. 194	,	
EoIP. 164 Wi-Fi. 167 Basic Settings. 167 Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional 187 MAC Filter. 191 Roaming. 194		
<pre>Wi-Fi</pre>		
Basic Settings		
Client Management. 176 WPS. 177 Using WPS Function via Web-based Interface. 179 Using WPS Function without Web-based Interface. 180 WMM. 181 Client. 184 Additional. 187 MAC Filter. 191 Roaming. 194		
<pre>WPS</pre>		
Using WPS Function via Web-based Interface		
Using WPS Function without Web-based Interface	WPS	
WMM	Using WPS Function via Web-based Interface	
Client	Using WPS Function without Web-based Interface	
Additional	WMM	
MAC Filter	Client	
Roaming194	Additional	
	MAC Filter	
	Roaming	
	Print Server	

USB Storage
Information
USB Users
Samba199
FTP
Filebrowser
DLNA
Torrent Client
XUPNPD
USB Modem
Basic Settings
SMS215
USSD
Advanced
VLAN
WAN Assignment
Using LAN Ports as WAN Ports222
Using WAN Port as LAN Port223
SNMP
DNS
DDNS
Ports Settings
Redirect
Routing
TR-069 Client
Port Mirroring
UPnP
UDPXY
IGMP/MLD
ALG/Passthrough
CoovaChilli
VRRP
Wake-on-LAN
Firewall
IP Filter
Virtual Servers
DMZ
MAC Filter
URL Filter
AdBlock
Remote Access

System	
Configuration	
Creating Configuration Backup	
Buttons Configuration	
Firmware Update	
Local Update	
Remote Update	
Schedule	
Logging	
Local	
Remote	
Record to File	
Ping	
Traceroute	
Telnet/SSH	
System Time	
Auto Provision	
SkyDNS	
Settings	
Devices and Rules	
Chapter 5. Operation Guidelines	
Terms and Conditions for Installation, Safe Operation,	
Storage, Transportation, and Disposal	
Wireless Installation Considerations	
Chapter 6. Abbreviations and Acronyms	

CHAPTER 1. INTRODUCTION

Contents and Audience

This manual describes the router DIR-1260 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-1260 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-1260 device is a wireless dual band gigabit router with 3G/LTE support. It provides a fast and simple way to create a wireless and wired network at home or in an office.

The router is equipped with a USB port for connecting a USB modem¹, which can be used to establish connection to the Internet. In addition, to the USB port of the router you can connect a USB storage device, which will be used as a network drive, or a printer.

In order to use the multifunction USB port effectively, the router supports simultaneous operation of several USB devices. For example, you can access multimedia content of the connected HDD storage and at the same time share a USB printer.²

You can use any Ethernet port of the router as LAN or WAN port. The new-generation firmware supports assigning several WAN ports, for example, in order to configure the primary and backup WAN connection of different ISPs. In addition, you can configure the WAN failover using a 3G/4G modem.

You are also able to connect the wireless router DIR-1260 to a cable or DSL modem or to a private Ethernet line and use a high-speed Internet connection to successfully fulfill a wide range of professional tasks. The built-in 4-port switch enables you to connect Ethernet-enabled computers, game consoles, and other devices to your network.

Using the DIR-1260 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 1167Mbps³).

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

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

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

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

Smart adjustment of Wi-Fi clients is useful for networks based on several D-Link access points or routers – when the smart adjustment function is configured on each of them, a client always connects to the access point (router) with the highest signal level.

¹ Not included in the delivery package. D-Link does not guarantee compatibility with all USB modems. For the list of supported USB modems, see the *Specifications* section, page 9.

² When using a USB hub with external power supply.

³ Up to 300Mbps for 2.4GHz and up to 867Mbps for 5GHz.

Support of guest Wi-Fi network allows you to create a separate wireless network with individual security settings. 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-1260 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.

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 automatically save the configuration of the router to a connected USB storage, 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-1260 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-1260 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-1260 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	· MT7621DAT (880MHz, dual core)
RAM	· 128MB, DDR3
Flash	· 128MB, NAND
Interfaces	 10/100/1000BASE-T WAN port 4 10/100/1000BASE-T LAN ports USB 2.0 port
LEDs	 Power Internet WLAN 2.4G WLAN 5G
Buttons	 POWER button to power on/power off RESET button to restore factory default settings WPS button to set up wireless connection and enable/disable wireless network
Antenna	· Four external non-detachable antennas (5dBi gain)
МІМО	· 2 x 2, MU-MIMO
Power connector	Power input connector (DC)
Mounting	 Desktop Wall

Software	
WAN connection types	 Mobile Internet (via supported USB modem) 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 + Static IP PPTP/L2TP + Dynamic IP L2TP Dual Stack IPIP6 in DSLite mode 6in4 6to4 6rd

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

Software	
Network functions	 DHCP server/relay Advanced configuration of built-in DHCP server Stateful/Stateless mode for IPv6 address assignment, IPv6 prefix delegation Automatic obtainment of LAN IP address (for access point/repeater/client modes) DNS relay Dynamic DNS Static IPv4/IPv6 routing IGMP/MLD Proxy RIP Support of UPnP Support of VLAN WAN ping respond Support of SIP ALG Support of RTSP WAN failover LAN/WAN conversion Multi-WAN support Autonegotiation of speed, duplex mode, and flow control / Manual speed and duplex mode setup for each Ethernet port Built-in UDPXY application XUPNPD plug-in Equal load distribution while using several WAN connections (traffic balancing) Support of VRRP Port mirroring Wake-on-LAN support
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 servers PPTP/L2TP tunnels L2TP over IPsec client GRE/EoGRE/EoIP/IPIP tunnels IPsec tunnels Transport/Tunnel mode IKEv1/IKEv2 support DES encryption NAT Traversal Support of DPD (Keep-alive for VPN tunnels)
USB interface functions	 USB modem USB modem Auto connection to available type of supported network (4G/3G/2G) Auto configuration of connection upon plugging in USB modem Enabling/disabling PIN code check, changing PIN code⁴ Sending/receiving/reading/removing SMS messages⁴ Support of USSD requests⁴ USB storage File browser Print server Access to storage via accounts Built-in Samba server Built-in FTP server supporting TLS Built-in Transmission torrent client; uploading/downloading files from/to USB storage

⁴ For some models of USB modems.

Software	
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/connected USB storage Automatic synchronization of system time with NTP server and manual time/date setup Ping utility Traceroute utility TR-069 client Schedules for rules and settings of firewall, automatic reboot and saving a configuration backup to a connected USB storage, and enabling/disabling wireless network and Wi-Fi filter Automatic upload of configuration file from ISP's server (Auto Provision) Configuration of action for hardware buttons

Wireless Module Parameters	Wireless Module Parameters	
Standards	 IEEE 802.11ac Wave 2 IEEE 802.11a/b/g/n IEEE 802.11k/v 	
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) 	
Advanced functions	 Support of client mode WMM (Wi-Fi QoS) Information on connected Wi-Fi clients Advanced settings Smart adjustment of Wi-Fi clients Guest Wi-Fi / support of MBSSID 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 CoovaChilli authentication portal 	
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 (from MCS0 to MCS15) IEEE 802.11ac (5GHz): from 6.5 to 867Mbps (from MCS0 to MCS9) 	

· Less than 20dBm (100mW)
 802.11a (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -93dBm at 6Mbps -90dBm at 9Mbps -90dBm at 12Mbps -87dBm at 18Mbps -84dBm at 24Mbps -81dBm at 36Mbps -77dBm at 48Mbps -75dBm at 54Mbps 802.11b (typical at PER = 8% (1000-byte PDUs) at room temperature 25 °C) -96dBm at 1Mbps -93dBm at 2Mbps -92dBm at 5.5Mbps -88dBm at 11Mbps
 802.11g (typical at PER < 10% (1000-byte PDUs) at room temperature 25 °C) -93dBm at 6Mbps -91dBm at 9Mbps -91dBm at 12Mbps -88dBm at 18Mbps -85dBm at 24Mbps -82dBm at 36Mbps -77dBm at 48Mbps -75dBm at 54Mbps
 802.11n (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) 2.4GHz, HT20 92dBm at MCS0/8 89dBm at MCS1/9 87dBm at MCS2/10 84dBm at MCS3/11 80dBm at MCS6/14 77dBm at MCS6/14 77dBm at MCS0/8 86dBm at MCS1/9 84dBm at MCS1/9 84dBm at MCS3/11 77dBm at MCS0/8 77dBm at MCS0/8 86dBm at MCS1/9 84dBm at MCS3/11 77dBm at MCS5/13 77dBm at MCS1/9 84dBm at MCS3/11 77dBm at MCS6/14 77dBm at MCS3/11 77dBm at MCS3/11 77dBm at MCS6/14 70dBm at MCS6/14 70dBm at MCS1/9 86dBm at MCS1/9 86dBm at MCS1/15 5GHz, HT20 91dBm at MCS0/8 88dBm at MCS1/9 86dBm at MCS1/9 86dBm at MCS1/1 77dBm at MCS0/8 70dBm at MCS0/8 78dBm at MCS1/1 79dBm at MCS3/11 79dBm at MCS3/11 79dBm at MCS3/11 79dBm at MCS3/11

Wireless Module Parameters	
	5GHz, HT40 -90dBm at MCS0/8 -85dBm at MCS2/10 -80dBm at MCS2/11 -76dBm at MCS4/12 -73dBm at MCS6/14 -70dBm at MCS7/15 • 802.11ac (typical at PER = 10% (1000-byte PDUs) at room temperature 25 °C) VHT20 -91dBm at MCS0 -89dBm at MCS1 -87dBm at MCS2 -84dBm at MCS3 -81dBm at MCS5 -75dBm at MCS6 -75dBm at MCS5 -76dBm at MCS5 -76dBm at MCS5 -76dBm at MCS6 -73dBm at MCS6 -73dBm at MCS6 -73dBm at MCS5 -76dBm at MCS5 -76dBm at MCS5 -77dBm at MCS6 -73dBm at MCS5 -72dBm at MCS5 -72dBm at MCS6 -70dBm at MCS5 -72dBm at MCS6 -70dBm at MCS8 -66dBm at MCS9 VHT80 -85dBm at MCS1 -82dBm at MCS1 -82dBm at MCS8 -66dBm at MCS9 VHT80 -85dBm at MCS1 -80dBm at MCS1
Modulation schemes	 802.11a: BPSK, QPSK, 16QAM, 64QAM with OFDM 802.11b: DQPSK, DBPSK, DSSS, CCK 802.11g: BPSK, QPSK, 16QAM, 64QAM with OFDM 802.11n: BPSK, QPSK, 16QAM, 64QAM, 256QAM with OFDM 802.11ac: BPSK, QPSK, 16QAM, 64QAM, up to 256QAM with OFDM

Physical Parameters		
Dimensions (L x W x H)	· 238 x 156 x 31 mm (9.37 x 6.14 x 1.2 in)	
Weight	· 328 g (0.72 lb)	

Operating Environment		
Power	Output: 12V DC, 1.5A	
Temperature	 Operating: from 0 to 40 °C Storage: from -20 to 65 °C 	
Humidity	 Operating: from 10% to 90% (non-condensing) Storage: from 5% to 95% (non-condensing) 	

Supported USB modems⁵		
GSM	· Alcatel X500	
	· D-Link DWM-152C1	
	· D-Link DWM-156A6	
	· D-Link DWM-156A7	
	· D-Link DWM 156A8	
	· D-Link DWM-156C1	
	· D-Link DWM-157B1	
	· D-Link DWM-157B1 (Velcom)	
	· D-Link DWM-158D1	
	· D-Link DWR-710	
	· Huawei E150	
	· Huawei E1550	
	· Huawei E156G	
	· Huawei E160G	
	· Huawei E169G	
	· Huawei E171	
	 Huawei E173 (Megafon) 	
	Huawei E220	
	 Huawei E3131 (MTS 420S) 	
	Huawei E352 (Megafon)	
	Huawei E3531	
	Prolink PHS600	
	Prolink PHS901	
	· ZTE MF112	
	· ZTE MF192	
	· ZTE MF626	
	· ZTE MF627	
	· ZTE MF652	
	· ZTE MF667	
	· ZTE MF668	
	· ZTE MF752	

⁵ The manufacturer does not guarantee proper operation of the router with every modification of the firmware of USB modems.

Product Appearance

Upper Panel



Figure 1. Upper panel view.

LED	Mode	Description		
	Solid orange	The router is being loaded.		
Barra	Solid white	The router is powered on.		
Power	Blinking white	The firmware is being updated.		
	No light	The router is powered off.		

LED	Mode	Description		
	Solid white	The default WAN connection is on.		
	Blinking white	The default WAN connection is active.		
Internet	Solid orange	The default WAN connection is off, orthere are no WAN connections created.		
	Blinking orange	Attempting to establish the default WAN connection.		
	No light	 The WAN cable is not connected, or the device is configured as an access point or repeater. 		
Solid white		The router's WLAN of the relevant band is on.		
WLAN 2.4G WLAN 5G	Fast blinking white	Data transfer through the Wi-Fi network of the relevant band.		
	Blinking white	Attempting to add a wireless device via the WPS function.		
	No light	The router's WLAN of the relevant band is off.		

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

Back Panel



Figure 2. Back panel view.

Port	Description
WPS	 A button to set up a wireless connection (the WPS function) and enable/disable the wireless network. To use the WPS function: with the device turned on, press the button, hold it for 2 seconds, and release. The WLAN 2.4G and WLAN 5G LEDs should start blinking. To disable the router's wireless network: with the device turned on, press the button, hold for 10 seconds, and release. The WLAN 2.4G and WLAN 2.4G and WLAN 5G and WLAN 5G LEDs should turn off.
RESET A button to restore the factory defaults. To restore the factory defaults, push the button (with the deturned on), hold it for 10 seconds, and then release the button.	
LAN 1-4	4 Ethernet ports to connect computers or network devices.

Port	Description	
INTERNET	A port to connect to a cable or DSL modem or to a private Ethernet line (it is recommended to use the cable included in the delivery package).	
USB 2.0	A port for connecting a USB device (modem, storage, printer).	
12V/1.5A DC IN	Power connector.	
POWER	A button to turn the router on/off.	

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

Delivery Package

The following should be included:

- Router DIR-1260
- Power adapter DC 12V/1.5A
- 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 3G/LTE support DIR-1260 (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.

USB Modem

To connect to an LTE or 3G network, you should use a USB modem. Connect it to the USB port of the router, then access the web-based interface of the router, and you will be able to configure a connection to the Internet.⁶

Your USB modem should be equipped with an active SIM card of your operator.

Some operators require subscribers to activate their USB modems prior to using them. Please, refer to connection guidelines provided by your operator when concluding the

agreement or placed on its website.

For some models of USB modems, it is required to disable the PIN code check on the SIM card prior to connecting the USB modem to the router.

⁶ Contact your operator to get information on the service coverage and fees.

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 **POWER** 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-1260 (for operating in the 2.4GHz band) or DIR-1260-5G (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-1260.
- 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-1260 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. *To connect via USB modem*: Connect your USB modem to the USB port⁷ located on the back panel of the router.



In some cases you will need to reboot the router after connection of the USB modem.

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

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

⁷ It is recommended to use a USB extension cable to connect a USB modem to the router.

Obtaining IP Address Automatically (OS Windows 7)

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

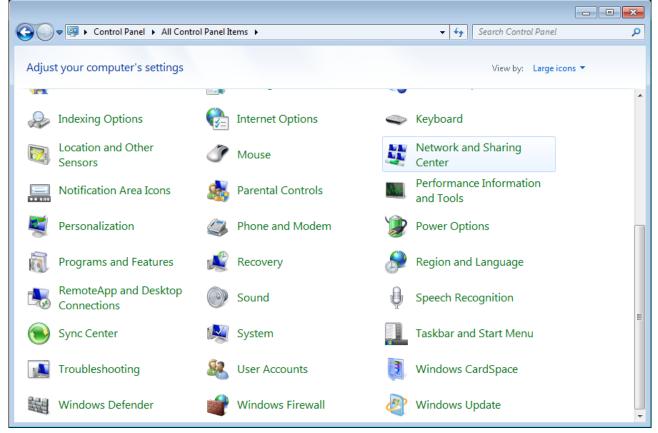


Figure 3. The Control Panel window.

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

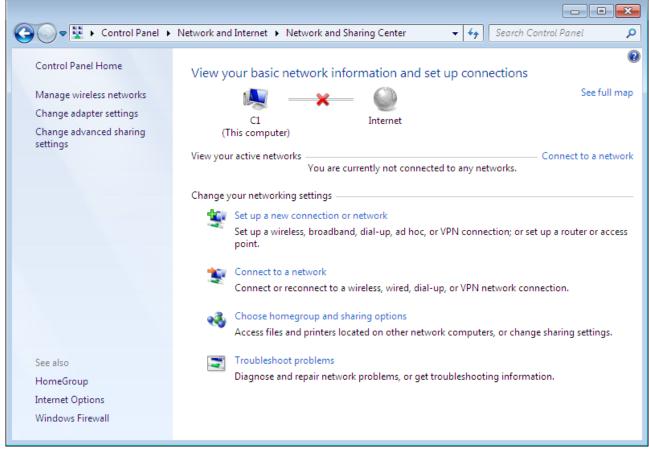


Figure 4. The Network and Sharing Center window.

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

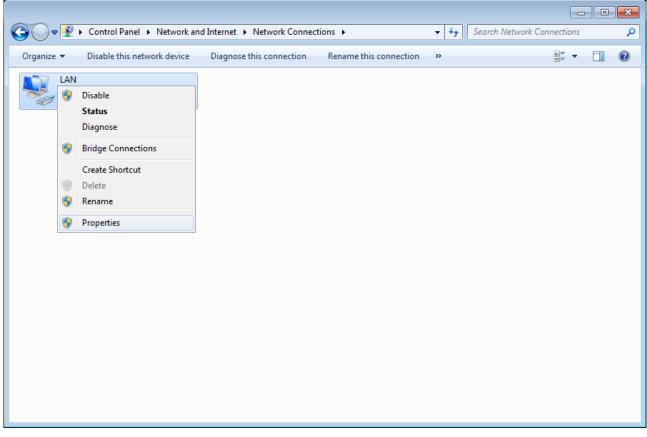


Figure 5. The Network Connections window.

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 		
I <u>n</u> stall <u>U</u> ninstall <u>Properties</u>		
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	X		
OUse the following IP address:			
IP address:	· · · ·		
Sybnet mask:	1 1 1		
Default gateway:			
Obtain DNS server address autor	natically		
OUSE the following DNS server add	resses:		
Preferred DNS server:	· · · ·		
Alternate DNS server:			
Vaļidate 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		٩		
므	System Display, sound, notifications, power		Devices Bluetooth, printers, mouse		
	Phone Link your Android, iPhone		Network & Internet Wi-Fi, airplane mode, VPN		
Ę	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 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	
도 Ethernet	Change your network settings
ଳ Dial-up	Change adapter options View network adapters and change connection settings.
∞ VPN	Sharing options For the networks you connect to, decide what you want to share.
r∯→ Airplane mode	
^(ပု) Mobile hotspot	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.

Vetwork Connections						
$\leftarrow \rightarrow \cdot \cdot \uparrow$	😰 > Control Panel > All Control Panel Items > Network Connections 🗸 🗸					
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					
٩	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	×				
Networking Sharing					
Connect using:					
🚍 Realtek PCIe FE Family Controller					
<u>C</u> onfigure					
This connection uses the following items:					
Client for Microsoft Networks	^				
File and Printer Sharing for Microsoft Networks					
QoS Packet Scheduler					
Internet Protocol Version 4 (TCP/IPv4)					
Microsoft Network Adapter Multiplexor Protocol					
Internet Protocol Version 6 (TCP/IPv6)	~				
Install Uninstall Properties					
Description					
Transmission Control Protocol/Internet Protocol. The default					
wide area network protocol that provides communication across diverse interconnected networks.					
OK Cano	el				
Chi Odine					

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 Advar	nced					
OK	Cancel					

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

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

PC with Wi-Fi Adapter

1. *To connect via USB modem*: Connect your USB modem to the USB port⁸ located on the back panel of the router.

In some cases you will need to reboot the router after connection of the USB modem.

- 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 **POWER** button on its back panel.
- 4. 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).

⁸ It is recommended to use a USB extension cable to connect a USB modem to the router.

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.)

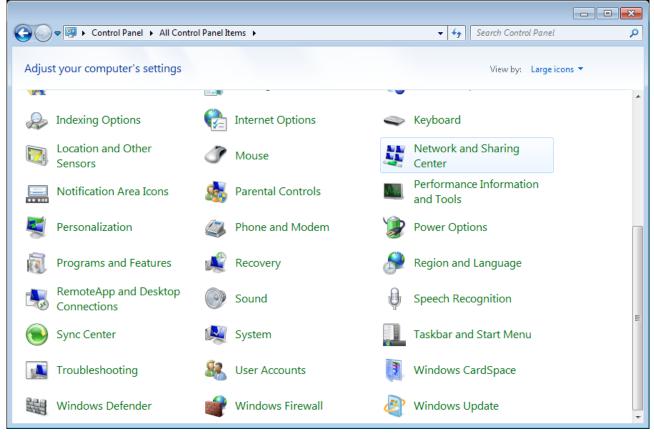


Figure 13. The **Control Panel** window.

- 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 automatically						
O Use the following IP address:						
IP address:	· · · ·					
S <u>u</u> bnet mask:						
Default gateway:						
Obtain DNS server address automatically						
Use the following DNS server addresses:						
Preferred DNS server:	· · · · · ·					
Alternate DNS server:	· · ·					
Vaļidate settings upon exit	Ad <u>v</u> anced					
OK Cancel						

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

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



Figure 15. The notification area of the taskbar.

 In the opened Wireless Network Connection window, select the wireless network DIR-1260 (for operating in the 2.4GHz band) or DIR-1260-5G (for operating in the 5GHz band) and click the Connect button.

Not connected	÷,
Connections are available	
Wi-Fi	^
wireless router	lte.
Connect automatically	onnect
Open Network and Sharing) Center

Figure 16. The list of available networks.

- 10. In the opened window, enter the network key (see WPS PIN on the barcode label on the bottom panel of the device) in the **Security key** field and click the **OK** button.
- 11. Wait for about 20-30 seconds. After the connection is established, the network icon will be displayed as the signal level scale.
- If you perform initial configuration of the router via Wi-Fi connection, note that immediately after changing the wireless default settings of the router you will need to reconfigure the wireless connection using the newly specified settings.

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

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

Settings				_	×
	Windows	Settir	igs		
	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		
⊈	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 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:	- 1
Preferred DNS server:	
Alternate DNS server:	
Validate settings upon exit Advanced	
OK Cance	2

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-1260 (for operating in the 2.4GHz band) or DIR-1260-5G (for operating in the 5GHz band) and click the Connect button.

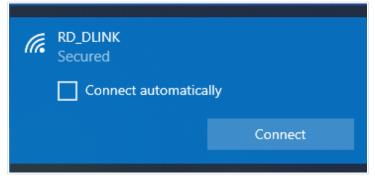


Figure 20. The list of available networks.

- 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 yo discoverable by other Po network?	
	We recommend allowing and work networks, but	
	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 21). 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-1260 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 48).

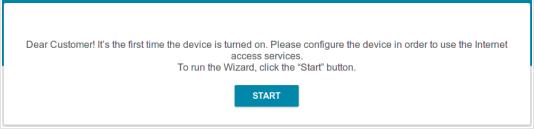


Figure 23. The page for running the Initial Configuration Wizard.

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.

Authoriza	ation	
Username*		
Password*		ŵ
Stay	signed in	
Forgot passw	ord?	
	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	Su	mmary	
Device Information		WAN IPv4	
Model:	DIR-1260	Connection type:	Dynamic IPv4
Hardware version:	R1	Status:	Connected 🔵
Firmware version:	4.0.6	MAC address:	00:0C:43:27:61:61
Build time:	Mon Sep 23 2024 2:03:37 PM MSK	IP address:	192.168.161.234
UI version:	1.50.1.119e975-embedded		
Vendor:	D-Link Russia		
Serial number:	DIR1260000001	LAN	
Support:	support@dlink.ru	LAN IPv4:	192.168.0.1
Summary:	Root filesystem image for DIR_1260_MT7621D	Wireless connections:	
Uptime:	1 h. 17 min.	Wired connections:	1
Device mode:	Router		
Enable LEDs:			
		LAN Ports	
		1	
Wi-Fi 2.4 GHz		LAN4:	Off
Status:	On 🕒		Off
Broadcasting:	On 🕒	LAN2:	1000M-Full 😅 🔵
Additional networks:	0		Off
Network name (SSID):	DIR-1260-6161		
Security:	WPA2-PSK	USB Devices	
		No connected devices	
Wi-Fi 5 GHz			
Status:	On 🌑		
Broadcasting:	On 🛑		
Additional networks:	0		
Network name (SSID):	DIR-1260-5G-6161		
Security:	WPA2-PSK		

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 48).

If needed, you can disable the LEDs of the device. To do this, move the **Enable LEDs** switch⁹ to the left. In order to enable the LEDs, 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 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 and data transfer mode of active ports.

The **USB Devices** section displays the device connected to the USB port of the router.

⁹ Correct operation of the switch will be implemented in the next firmware version.

Home Page

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

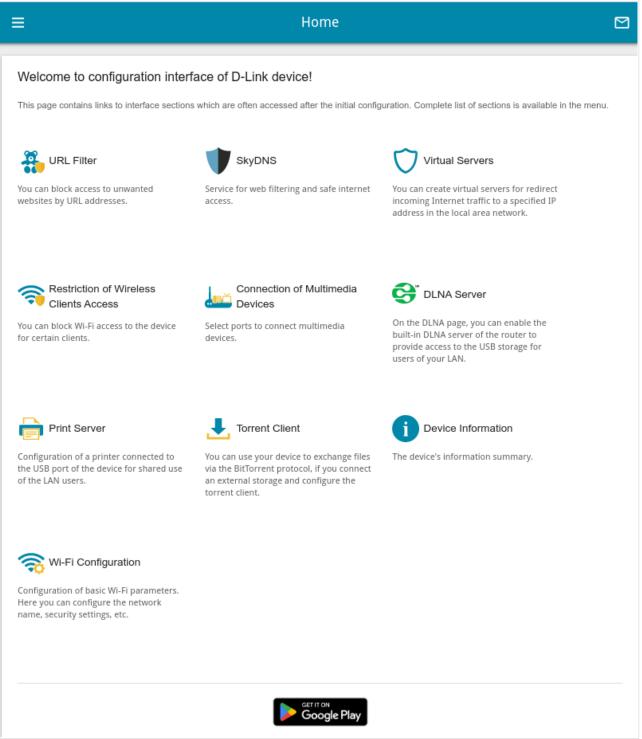


Figure 26. The Home page.

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 48).

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 75).

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 84).

The pages of the **VPN** section are designed for configuring VPN connections based on IPsec/GRE/EoGRE/EoIP/IPIP protocols and creating a PPTP or L2TP server and accounts for access to it (for the description of the pages, see the *VPN* section, page 142).

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 167).

The **Print Server** section is designed for configuring the router as a print server (see the *Print Server* section, page 196).

The pages of the **USB Storage** section are designed for operating the connected USB storage (for the description of the pages, see the *USB Storage* section, page 197).

The pages of the **USB Modem** section are designed for operating the connected 3G or LTE USB modem (for the description of the pages, see the *USB Modem* section, page 211).

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 218).

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 257).

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 278).

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 310).

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.

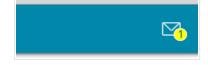


Figure 27. The web-based interface notifications.

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.

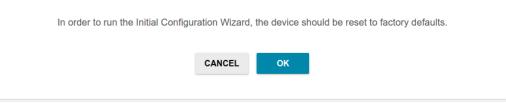


Figure 28. Restoring the default settings in the Wizard.

If you perform initial configuration of the router via Wi-Fi connection, please make sure that you are connected to the wireless network **DIR-1260** (for operating in the 2.4GHz band) or **DIR-1260-5G** (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.

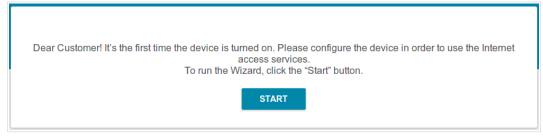


Figure 30. Starting the Wizard.

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.

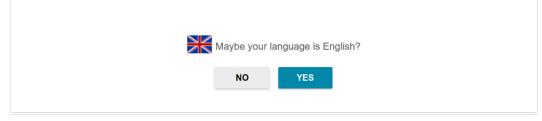


Figure 31. Selecting a language.

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.

In order to start up, please change several default settings. User's interface password* Password should be between 1 and 31 ASCII characters Password confirmation* Network name 2.4 GHz (SSID)* DIR-XXX Network name 5 GHz (SSID)* DIR-XXX-5G	Defaults	
Password should be between 1 and 31 ASCII characters Password confirmation* Network name 2.4 GHz (SSID)* DIR-XXX Network name 5 GHz (SSID)*	In order to start up, please change several o	lefault settings.
Password confirmation* Network name 2.4 GHz (SSID)* DIR-XXX Network name 5 GHz (SSID)*	User's interface password*	Ø
Network name 2.4 GHz (SSID)* DIR-XXX Network name 5 GHz (SSID)*	Password should be between 1 and 31	ASCII characters
DIR-XXX Network name 5 GHz (SSID)*	Password confirmation*	Ø
Network name 5 GHz (SSID)*	Network name 2.4 GHz (SSID)*	
	DIR-XXX	
		🗙 ВАСК

Figure 32. Changing the default settings.

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

Selecting Operation Mode

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

Router

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

Device mode		
Connection method		
Wired connection	•	
Vork mode		ssiD
Router	•	2
	< ВАСК	NEXT >

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

In order to connect your device to the network of a 3G or LTE operator, on the **Device mode** page, from the **Connection method** list, select the **Mobile Internet** value. In this mode you can configure a 3G/LTE 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.



Figure 34. Selecting an operation mode. The Mobile Internet mode.

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

	_
•	
	SSID_Ext
•	
К ВАСК	NEXT >
	•

Figure 35. Selecting an operation mode. The WISP Repeater mode.

Access Point or Repeater

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

Device mode			
Connection method			
Wired connection	•		
Work mode			SSID
Access point	•		2
		••••••••	
		_	
	< BACK	NEXT >	

Figure 36. Selecting an operation mode. The Access point mode.

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

Device mode	
Connection method Wi-Fi	
Work mode Repeater	

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

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

Device mode		
Connection method		
Wi-Fi	•	
))) ssid (((
Vork mode		
Client	•	
	< BACK	NEXT >

Figure 38. Selecting an operation mode. The **Client** mode.

Creating 3G/LTE WAN Connection

This configuration step is available for the **Mobile Internet** mode.

1. If the PIN code check is enabled for the SIM card inserted into your USB modem, enter the PIN code in the **PIN** field and click the **APPLY** button.

Modem S	settings		
Vendor: Model:	E3131		
Modem E3131			
Please ente Modem: E3 Attempts let	r the PIN code of the SIN 131 ft: 3	I card	
PIN*		Ø	
		APPLY	
		< BACK NEXT >	

Figure 39. The page for entering the PIN code.

2. Please wait while the router automatically creates a WAN connection for your mobile operator.

Modem S	ettings
Vendor: Model:	E3131
Modem	
E3131	•
lf you want t	tion has been created automatically. to change the connection settings configured automatically, click the "Configure manually" button. to continue with the configured connection settings, click the "Next" button.

Figure 40. The page for creating 3G/LTE connection.

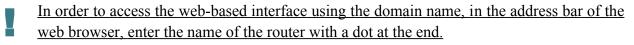
3. Click the **NEXT** button.

If the router failed to create a WAN connection automatically or you want to change the WAN connection settings configured automatically, click the **CONFIGURE MANUALLY** button. On the **Modem Settings** page, configure all needed settings and click the **NEXT** button.

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-1260 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-1260, 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 asigned 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 B.8.8.8 Hostname* dlinkap18c6.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	
dlinkap18c6.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 (



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

requency band			
2.4 GHz	-	 Attention! Upon connection to network encryption, basic settings of Wi-Fi network 	
Network name (SSID)*		the standards 802.11b and g will be used and the standard 802.11a will be used in	d in the 2.4 GHz band
		Network authentication	
ISSID		WPA2-PSK	•
74:da:da:0a:8f:c9			
		Password PSK*	હ
		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.	
Default key ID	The number of the key (from first to fourth) which will be used for WEP encryption.	

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

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

Parameter	Description
Password PSK	A password for WPA encryption. Click the Show icon (\bigotimes) to display the entered password.
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.

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

Configuring Wired 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

SCAN Ne IP address* IP address* Subnet mask* IP address* Gateway IP address* IP address* DNS IP address* IP address* MAC address assignment methon Default MAC address MAC address IP address	e allows you to use a fixe twork scan for connect					
A connection of this type SCAN Ne Subnet mask* Gateway IP address* DNS IP address* MAC address assignment meth Default MAC address MAC address						
IP address* Subnet mask* Gateway IP address* DNS IP address*						
IP address* Subnet mask* Gateway IP address* DNS IP address* MAC address assignment meth Default MAC address MAC address	twork scan for connect	ion type and p	arameters d	etection		
Subnet mask* Gateway IP address* DNS IP address* MAC address assignment meth Default MAC address MAC address						
Subnet mask* Gateway IP address* DNS IP address* MAC address assignment meth Default MAC address MAC address						
Gateway IP address* DNS IP address* MAC address assignment meth Default MAC address MAC address						
DNS IP address* MAC address assignment meth Default MAC address MAC address						
DNS IP address* MAC address assignment meth Default MAC address MAC address						
MAC address assignment meth Default MAC address MAC address						
MAC address assignment meth Default MAC address MAC address						
Default MAC address						
MAC address	bd					
		•				
C0:43:34:19:12:22						
 In some ISP's network 	s, it is required to register	a certain MAC a	address in ord	ler to get acce	ess to the Internet.	
Use VLAN						
 Select the checkbox if 	the Internet access is pro	vided via a VLA	N channel.			
Use IGMP						
(i) Internet Group Manag	ement Protocol is designe	d to manage m	ulticast traffic i	in IP-based ne	etworks.	
Ping						
Enable automatic creati	on of Mobile Internet connec	tion				
	< 1	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 connec	ction type	
Connection type		
Static IPv6	-	
-	his type allows you to use a fixed IP ac	
SCAN	Network scan for connection typ	e and parameters detection
IP address*		
Prefix*		
Gateway IP addres	ss*	
DNS IP address*		
MAC address assignmer Default MAC addr		
MAC address		
C0:43:34:19:12:22	a	
(i) In some ISP's ne	tworks, it is required to register a certa	in MAC address in order to get access to the Internet.
Use VLAN		-
(i) Select the check	box if the Internet access is provided v	a a VLAN channel.
Ping		
Enable automatic	creation of Mobile Internet connection	
	< ВАСК	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

Internet connection type	
Connection type	
PPPoE	•
A connection of this type requires a user name a SCAN Network scan for connect	
Without authorization	ion type and parameters detection
Without authorization	
Username*	
Password*	<i>ق</i>
Service name	
MAC address assignment method Default MAC address	•
MAC address	
C0:43:34:19:12:22	
 In some ISP's networks, it is required to register Use VLAN Select the checkbox if the Internet access is pro Ping Enable automatic creation of Mobile Internet connection 	
< 1	

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)	-
① A connection of this type requires a user name, pa	ssword, and a fixed IP address provided by your ISP.
SCAN Network scan for connection	n type and parameters detection
Without authorization	
Username*	
Osemanie	
Password*	8
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

onnection type		
PPTP + Dynamic IP	-	
PPTP and L2TP are methods for	implementing virtual private networks.	
SCAN Network sca	an for connection type and parameters dete	ction
Without authorization		
Username*		
e ormanite		
Descuverd*	200	
Password*	Ø	
VPN server address*		
VPN server address*		
MAC address assignment method		
MAC address assignment method Default MAC address MAC address		
MAC address assignment method Default MAC address MAC address	-	
MAC address assignment method Default MAC address MAC address	-	
MAC address assignment method Default MAC address MAC address C0:43:34:19:12:22	• irred to register a certain MAC address in order	to get access to the Internet.
MAC address assignment method Default MAC address MAC address C0:43:34:19:12:22		to get access to the Internet.
MAC address assignment method Default MAC address MAC address C0:43:34:19:12:22 ① In some ISP's networks, it is requ Use VLAN		to get access to the Internet.
MAC address assignment method Default MAC address MAC address C0:43:34:19:12:22 ① In some ISP's networks, it is requ Use VLAN	iired to register a certain MAC address in order	to get access to the Internet.
MAC address assignment method Default MAC address MAC address C0:43:34:19:12:22 ① In some ISP's networks, it is requ Use VLAN ③ Select the checkbox if the Internet V Use IGMP	ired to register a certain MAC address in order in a certain MAC address in order in a certain the second state	-
MAC address assignment method Default MAC address MAC address C0:43:34:19:12:22 In some ISP's networks, it is requ Use VLAN Select the checkbox if the Internet Use IGMP Internet Group Management Pro	iired to register a certain MAC address in order	-
MAC address assignment method Default MAC address MAC address C0:43:34:19:12:22 ① In some ISP's networks, it is requ Use VLAN ③ Select the checkbox if the Internet V Use IGMP	ired to register a certain MAC address in order in a certain MAC address in order in a certain the second state	-

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 address or full domain name of the PPTP or L2TP authentication server.

PPTP + Static IP or L2TP + Static IP Connection

Connection type		
PPTP + Static IP	•	
PPTP and L2TP	are methods for implementing virtual p	vrivate networks.
SCAN	Network scan for connection typ	e and parameters detection
Without authoriza	ation	
	4001	
Username*		
Password*	ø	
r assword	<i>u</i> ,	
VPN server addres	SS*	
IP address*		
Subnet mask*		
Gateway IP addres	SS [*]	

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 address or full domain name 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 **Mobile Internet**, **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.

5. 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 **Mobile Internet**, **Router**, and **WISP Repeater** modes only).

Enable guest network	
③ 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	

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. Click the **NEXT** button to continue or click the **BACK** button to specify other settings.
- 9. 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.

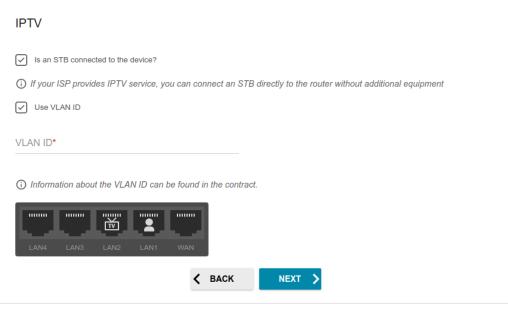


Figure 51. The page for selecting a LAN port to connect an IPTV set-top box.

- 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.
LAN4 LAN3 LAN2 LAN1 WAN
< 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.¹⁰

Changing web-based interface password					
For security reasons, please change	the password used	to access the	device's settir	ngs.	
User's interface password*	Ø				
 Password should be between 1 and 	31 ASCII characters				
Password confirmation*	Ø				
	< 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** 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.

^{10 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.

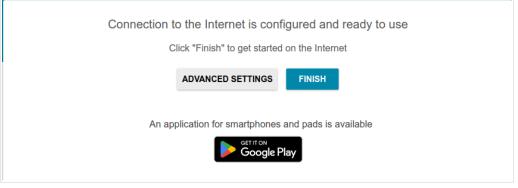


Figure 54. Checking the Internet availability.

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 45).

Connection of Multimedia Devices

The Multimedia Devices Connection Wizard helps to configure LAN ports or available wireless interfaces of the router for connecting additional devices, for example, an IPTV set-top box or IP phone. Contact your ISP to clarify if you need to configure DIR-1260 in order to use these devices.

To start the Wizard, on the **Home** page, select the **Connection of Multimedia Devices** section. If you need to select a port or wireless interface in order to use an additional device, left-click the relevant element in the **LAN** section (the selected element will be marked with a frame). Then click the **APPLY** button.

≡ < Home	Connection of Multi	media Devices	
You can connect an STB or IP phone directly to the router. In order to do this, select a free port of the router or its wireless interface and then connect your device to it. In some cases IPTV/VoIP services are provided through a tagged VLAN. In these cases it is necessary to use "Advanced mode"			
	LAN2	LAN3	
LAN4	TIR-XXX	DIR-XXX-5G	
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	
LAN4 Bridged with No	DIR-XXX Bridged with No	DIR-XXX-5G Bridged with No	
SIMPLIFIED MODE			
WAN	(+)		
	APPLY		

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

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

Add VLAN	×
Name*	
VLAN ID*	
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 or wireless interface to which the additional device is connected, select the created connection. Click the **APPLY** button.

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

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

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

Statistics

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

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

Network Statistics

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

letwork Sta	atistics			
ou can view statis	stics for all interfaces (connections) existing in the syste	em.		
Name	IP - Gateway	Rx/Tx	Rx/Tx errors	Duration
LAN	IPv4: 192.168.0.1/24 - 192.168.0.1	571.79 Kbyte / 7.80 Mbyte	0 / 0	-
WAN	IPv4: 192.168.161.244/24 - 192.168.161.1	151.60 Kbyte / 1.83 Kbyte	0/0	6 min
DIR-XXX		28.92 Kbyte / 11.85 Kbyte	0/0	-
		-/-	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 devices that have been identified by hostnames and MAC addresses and have got IP addresses from the DHCP server of the router.

📄 🔇 Summary		DHCP		
DHCP				
You can view the list	of IP addresses which local clients	obtained from the DHCP server.		
Hostname	IP address	MAC	Expires	
Galaxy-M21	192.168.0.154	66:C5:55:3D:D2:91	23h 55m 52s	

Figure 59. The Statistics / DHCP page.

Routing

Rules							
Table	Туре	IP (Source/Destination)	Interfac	ces (Incoming/Outgoing)	Priority	ToS	FWmark (HEX)
group_1	IPv4	all / all		LAN / any	100	0	0x0
group_1	IPv4	all / all		any / any	200	0	0x64
main	IPv4	all / all		any / any	32766	0	0x0
group_1	IPv6	all / all		LAN / any	100	0	0x0
group_1	IPv6	all / all		any / any	200	0	0x64
main	IPv6	all / all		any / any	32766	0	0x0
Tables							
ID	Na	ame [Description				
254	m	ain I	Main routing t	able			
257	gr	oup_1	Routing table	for groups			
256	sta	atic_1	Routing table	for connections			

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		Routir	ng Table			
Routing Ta	ble main					
'ou can view the	e information on routes.					
Interface	Destination	Subnet mask	Gateway	Flags	Metric	Table
WAN	0.0.0.0	0.0.0.0	192.168.161.1	UG	410	254
WAN	1.0.0.1		192.168.161.1	UGH	0	254
WAN	1.1.1.1		192.168.161.1	UGH	0	254
LAN	192.168.0.0	255.255.255.0		U	0	254
WAN	192.168.161.0	255.255.255.0		U	0	254

Figure 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	Clier	nts and Sessions		
Clients				
You can view the list of dev	vices connected to the local n	etwork of the router and inform	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.

😑 < Summa	ary	Port Statistic	S	
Port Statist		through ports of the device. This inform	nation can be used for diagnosing connection problen	ns.
Port	Status	Traffic sent, Mbyte	Traffic received, Mbyte	
LAN4	-	0	0	
LAN3	Connected	76	3	
LAN2	-	0	0	
LAN1	-	0	0	
WAN	Connected	61	277	

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.

Psec St	atistics				
ou can viev	v statistics for IPsec tunne	els.			
lame	Remote host	Packets received / Packets sent	Traffic received / Traffic sent	Mode	Туре

Figure 65. The Statistics / IPsec Statistics page.

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

VPN Statistics

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

≡ < 1	Psec Statistics	VPN Statis	stics	
	atistics ew statistics for PPTP/L2	TP VPN servers connections.		
Login	Client IP address	Packets sent / Packets received	Traffic sent / Traffic received	Connection type
test	10.90.90.2/32	7/7	87.00 byte / 93.00 byte	РРТР

Figure 66. The Statistics / VPN Statistics page.

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

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

Connections Setup

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

WAN

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

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

WAN		
You can create and edit connections used by the	ne router.	
Dynamic IDv4		
Dynamic IPv4		
EDIT RECONNECT		
Connection type:		Dynamic IPv4
Status:		Connected
Interface:		WAN
IP address:		192.168.161.239
Subnet mask:		255.255.255.0
Gateway IP address:		192.168.161.1

Figure 67. 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.

🗧 < Home		WAN	l
WAN			
You can create and	edit connections used by the router.		
Default Gatew	vay IPv4	Default Gateway IPv6	
The specified conne	ection will be used by default.	No IPv6 connection created.	
WAN			
IGMP/MLD			
On the IGMP/MLD r	page you can allow the router to use their settings.	IGMP and	
MLD and configure			
MLD and configure	List reconnect + 🗊		
MLD and configure	List RECONNECT + 🗊	Interface Status	

Figure 68. 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 (\blacksquare).

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 245).

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.

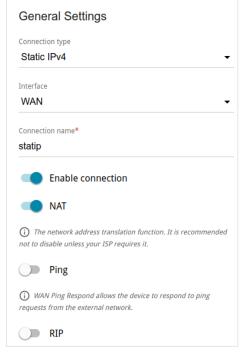


Figure 69. The page for creating a new Static IPv4 connection. The General Settings section.

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 for IPv4 is enabled. Do not disable the function unless your ISP requires this.	
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.	
RIP	Move the switch to the right to allow using RIP for this connection.	

Ethern	
MAC addre	
BC:0F:9A:6D:36:4C	
	Clone MAC address of your NIC 90:2B:34:A5:A8:FB)
	90:2B:34:A5:A8:FB)

Figure 70. 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.	

TV service only and no data on IP can set the following values: IP

Figure 71. 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_35
Enable connection
NATV6
① The network address translation function. It is recommended not to disable unless your ISP requires it.
Ping
WAN Ping Respond allows the device to respond to ping requests from the external network.
RIPng

Figure 72. 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.	
NATv6	If the switch is moved to the right, the network address translation function for IPv6 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.	
RIPng	Move the switch to the right to allow using RIPng for this connection.	

Etherne	-
BC:0F:9A:6D:36:4C	
	one MAC address of your NIC 0:2B:34:A5:A8:FB)
	0:2B:34:A5:A8:FB)

Figure 73. The page for creating a new **Static IPv6** connection. The **Ethernet** section.

Parameter	Descriptior	1
	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 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 MAC ADDRESS button (the button is moved to the right).	
MTU	The maximum size of units transmitted	by the interface.
	IPv6	
	IPv6 address*	
	Prefix*	

Gateway IPv6 address*		
Cateway in vo address		
Primary IPv6 DNS server*		

Figure 74. 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	 From the drop-down list, select the mode of a prefix request from a delegating DHCPv6 server to configure a range of IPv6 addresses for the local network. None: The mode without prefix request. Auto: The mode with the ability to request a prefix. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is not mandatory to establish the connection. Force: The mode with forced prefix request. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is not mandatory to establish the connection. 	
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.

General Settings	
Connect	ion type
PPPo	E
Interfac	9
WAN	
Connect	ion name*
pppoe	
_	
•	Enable connection NAT
~	
~	NAT network address translation function. It is recommended not t
disable	NAT network address translation function. It is recommended not t unless your ISP requires it.

Figure 75. 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 for IPv4 is enabled. Do not disable the function unless your ISP requires this.	
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.	
RIP	Move the switch to the right to allow using RIP for this connection.	

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

Figure 76. 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.

PPP	
Without authorization	
Username*	
Password*	\$
Service name	
мтu* 1492	
Encryption protocol No encryption	•
Authentication protocol	•
Keep Alive	
LCP interval (in seconds)* 30	
LCP failures* 3	
Dial on demand	
Maximum idle time (in seconds) 30	ĥ
Static IP address	
PPP debug	

Figure 77. 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	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the LCP interval and LCP failures fields correspondingly or leave the default 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 this PPP connection debugging. Upon that the Debugging messages value should be selected from the Level drop-down list in the settings of the corresponding event log in the Logging section (see the <i>Logging</i> section, page 294).

IPv4	
Obtain DNS server addresses automatically	
Primary DNS	6
Secondary DNS	A

Figure 78. 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, L2TP Dual Stack, 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.

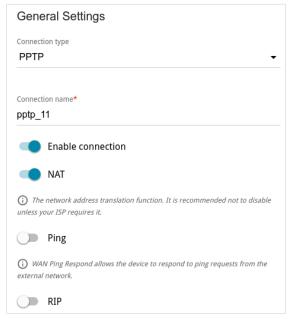


Figure 79. The page for creating a new **PPTP** connection. The **General Settings** section.

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 for IPv4 is enabled. Do not disable the function unless your ISP requires this.
NATv6	<i>For the</i> L2TP Dual Stack <i>type only.</i> If the switch is moved to the right, the network address translation function for IPv6 is enabled. Do not disable the function unless your ISP requires this.
Ping	For the PPTP , L2TP , and L2TP Dual Stack types only. 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> PPTP <i>and</i> L2TP <i>types only.</i> Move the switch to the right to allow using RIP for this connection.

PPP		
	Without authorization	
Usern	ame*	
Passv	ord*	٩
VPN s	erver address*	
MTU* 1456		
	on protocol cryption	
Authent AUTC	ication protocol	
	Keep Alive	
LCP inte 30	rval (in seconds)*	
LCP faile 3	res*	
	Dial on demand	
Maximu 30	m idle time (in seconds)	
Static	P address	

Figure 80. 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 address or full domain name of the PPTP or L2TP authentication server.
ΜΤυ	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	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the LCP interval and LCP failures fields correspondingly or leave the default values.	
Dial on demand	For the PPTP , L2TP , and L2TP over IPsec types only. 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 this PPP connection debugging. Upon that the Debugging messages value should be selected from the Level drop-down list in the settings of the corresponding event log in the Logging section (see the <i>Logging</i> section, page 294).	

IPv4	
Obtain DNS server addresses automatically	
Primary DNS	F
Secondary DNS	A

Figure 81. 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.	
	IPv6 Get IPv6 Automatically Enable prefix delegation Auto	
	Obtain DNS server addresses automatically Primary IPv6 DNS server Secondary IPv6 DNS server	

Figure 82. The page for creating a new L2TP Dual Stack connection. The IPv6 section.

Parameter	Description
IPv6 (for the L2TP Dual Stack type)	
Get IPv6Select a method for IPv6 address assignment from the drop- list or leave the Automatically value.	

Parameter	Description	
	 From the drop-down list, select the mode of a prefix request from a delegating DHCPv6 server to configure a range of IPv6 addresses for the local network. None: The mode without prefix request. 	
Enable prefix delegation	• Auto : The mode with the ability to request a prefix. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is not mandatory to establish the connection.	
	• Force : The mode with forced prefix request. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is mandatory to establish the connection.	
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.	
	IPsec	

IPsec	
Pre-shared key*	Ø
Enable PFS	
DPD action	
Restart	•
DPD - Dead Peer Detection	
DPD delay (in seconds)*	
30	
DPD timeout (in seconds)*	
120	

Figure 83. The page for creating a new L2TP over IPsec connection. The IPsec section.

The value of the **Pre-shared key** field should be the same for both parties of the tunnel.

Parameter	Description	
IPsec (for the L2TP over IPsec type)		
Pre-shared key	A key for mutual authentication of the parties. Click the Show icon ((()) 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-1260.	
DPD action	 Using DPD protocol (<i>Dead Peer Detection</i>) allows to check the status of the remote host in the tunnel: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD requests to the remote host. Select the needed action from the drop-down list. Restart: Restart the tunnel connection immediately. Hold: Reestablish the connection upon request when the traffic matching the tunnel appears. Clear: Close the tunnel connection with no further action. Off: Disable DPD. When this value is selected, 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.	
Specify connection port	Move the switch to the right to change the port used for data exchange with the other party enter the needed value in the Port field displayed. By default, the value 1701 is specified.	

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

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

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

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

After creating a connection of the L2TP over IPsec type, on the VPN / IPsec page, in the Status section, and on the IPsec Statistics page 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.

connecti	on type
PPPoE	E IPv6
nterface	
WAN	
Connecti	on name*
pppoev	6_19
	Enable connection
	ΝΑΤν6
	You can't use prefix delegation and NATv6 simultaneously
-	network address translation function. It is recommended not to disable Ir ISP requires it.
	Ping
	Ping Respond allows the device to respond to ping requests from the
WAN external n	etwork.

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

Parameter	Description	
General Settings		
Interface	A physical or virtual WAN interface to which the new connection will be assigned.	
Connection name	A name for the connection for easier identification.	
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.	
NAT	<i>For the</i> PPPoE Dual Stack <i>type only.</i> If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.	
NATv6	If the switch is moved to the right, the network address translation function for IPv6 is enabled. Do not disable the function unless your ISP requires this.	

Parameter	Description	
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 PPPoE Dual Stack type only.</i> Move the switch to the right to allow using RIP for this connection.	
RIPng	Move the switch to the right to allow using RIPng for this connection.	
	Ethornot	

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

Figure 85. 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.		

PPP	
Without authorization	
Username*	
Password*	Ø
Service name	
MTU*	
Encryption protocol No encryption	•
Authentication protocol AUTO	Ţ
Keep Alive	
LCP interval (in seconds)* 30	
LCP failures* 3	
Static IP address	
PPP debug	

Figure 86. 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 (N) 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	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the LCP interval and LCP failures fields correspondingly or leave the default 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 this PPP connection debugging. Upon that the Debugging messages value should be selected from the Level drop-down list in the settings of the corresponding event log in the Logging section (see the <i>Logging</i> section, page 294).	

IPv4		
Obtain DNS server addresses automatically		
Primary DNS		
Secondary DNS		

Figure 87. The page for creating a new **PPPoE Dual Stack** connection. The **IPv4** section.

Parameter	Descrij	otion
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 Auto	~
	Obtain DNS server addresses automatically Primary IPv6 DNS server	
	Secondary IPv6 DNS server	

Figure 88. The page for creating a new PPPoE Pv6 connection. The IPv6 section.

Parameter	Description	
IPv6		
Get IPv6Select a method for IPv6 address assignment from the drop-de list or leave the Automatically value.		

Parameter	Description	
Enable prefix delegation	 From the drop-down list, select the mode of a prefix request from a delegating DHCPv6 server to configure a range of IPv6 addresses for the local network. None: The mode without prefix request. Auto: The mode with the ability to request a prefix. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is not mandatory to establish the connection. 	
	• Force : The mode with forced prefix request. When this value is selected, the router requests a prefix from a DHCPv6 server. Upon that obtaining a prefix is mandatory to establish the connection.	
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.	

Creating Mobile Internet WAN Connection

If the PIN code check is enabled for the SIM card inserted into your USB modem, for correct operation of the mobile WAN connection click the **ENTER PIN** button in the notification in the top right corner of the page and enter the PIN code in the window displayed. Then 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.

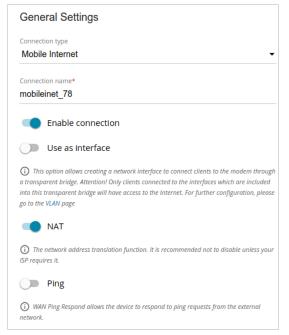


Figure 89. The page for creating a new Mobile Internet connection. The General Settings section.

Parameter	Description	
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.	
Use as interface	Move the switch to the right in order to create a network interface for this connection, for example, to combine several interfaces into a transparent connection.	
NAT	If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.	
	The switch is displayed when the IPv4 or Dual value is selected from the Type drop-down list in the Modem Settings section.	

Parameter	Description	
NATv6	 If the switch is moved to the right, the network address translation function for IPv6 is enabled. Do not disable the function unless your ISP requires this. The switch is displayed when the IPv6 or Dual value is selected from the Type drop-down list in the Modem Settings section. 	
PingIf the switch is moved to the right, the router responds requests from the external network through this connection security reasons, it is recommended to disable this function.		

MODEM/SIM CARD	SELECTION
Mode	
Auto	•
APN	
Dial number	
*99#	
Without authorization	
	ſ
Authentication protocol	
Authentication protocol PAP	
Authentication protocol PAP Username	6

Figure 90. The page for creating a new Mobile Internet connection. The Modem Settings section.

Parameter	Description	
Modem Settings		
MODEM/SIM CARD SELECTIONClick the button in order to assign the connection to one connected USB modems.11		
Mode	The value of the field specifies the type of the network to which the router connects. Leave the Auto value to let the router connect automatically to an available type of network, or select a needed value from the drop-down list.	

¹¹ When several devices are connected to one USB port of the router, it is recommended to use a self-powered USB hub.

Parameter	Description	
APN	An access point name.	
Dial number	A number dialed to connect to the authorization server of the operator.	
Without authorization	Move the switch to the right if your operator does not require authorization.	
Authentication protocol	Select a required authentication method from the drop-down list.	
Username	A username (login) to connect to the network of the operator.	
Password	A password to connect to the network of the operator. Click the Show icon (\bigotimes) to display the entered password.	
Туре	An IP version which will be used by this connection. Select the IPv4 , IPv6 , or Dual value from the drop-down list.	
	PPP MTU* 1370 Keep Alive LCP interval (in seconds)* 30 LCP failures* 3	

мтu* 1370	
Keep Alive	
LCP interval (in seconds)*	
30	
LCP failures*	
3	
Dial on demand	
Maximum idle time (in seconds)	
30	6

Figure 91. The page for creating a new **Mobile Internet** connection. The **PPP** section.

Parameter	Description		
	PPP		
MTU	The maximum size of units transmitted by the interface.		
Keep Alive	If the switch is moved to the right, the router sends echo requests in order to check the connection state. After several consecutive unanswered requests the router restarts the PPP connection. If needed, change the interval (in seconds) between requests and the number of unanswered requests in the LCP interval and LCP failures fields correspondingly or leave the default values.		

Parameter	Description	
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.	
PPP debug	Move the switch to the right if you want to log all data on this PPP connection debugging. Upon that the Debugging messages value should be selected from the Level drop-down list in the settings of the corresponding event log in the Logging section (see the <i>Logging</i> section, page 294).	
1	IPv4	

IPv4	
Obtain DNS server addresses automatically	
Primary DNS	
Secondary DNS	6

Figure 92. The page for creating a new **Mobile Internet** connection. The **IPv4** section.

Parameter	Description	
IPv4 (for the Dual and IPv4 types)		
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 Obtain DNS server addresses automatically	
	Primary IPv6 DNS server	

Figure 93. The page for creating a new Mobile Internet connection. The IPv6 section.

A

Secondary IPv6 DNS server

Parameter	Description	
	IPv6 (for the Dual and IPv6 types)	
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.	
	Health Check	
	Enable	
	Checking connection status using the ping command The maximum number of attempts 10 Connection restart	
	① The connection will be restarted after the number of attempts to check the destination host availability reaches the maximum value	
	Addresses	
	() List is empty (Default 8.8.8) ADD	
	Modem IP address verification	
	When the IP address of the modern is changed, the request to update the IP address is sent to all actual connections	

Figure 94. The page for creating a new Mobile Internet connection. The Health Check section.

Parameter	Description	
Health Check		
Enable	Move the switch to the right to check the connection health using the ICMP ping mechanism.	
The maximum number of attempts	A number of requests to check the health of the connection. By default, the value 10 is specified. Several ping requests are sent to check the hosts. After several failed attempts the connection status is changed until a successful attempt is made.	
Connection restart	Move the switch to the right to reestablish connection if the maximum number of ping requests fails.	

Parameter	Description
	IP addresses from the external network that the router will check for availability via ICMP ping mechanism. By default, the router checks the IP address 8.8.8.8. Click the ADD button, and in the line displayed, enter an IP address
Addresses	or leave value suggested by the router. You can add several addresses.
	To remove an IP address from the list, click the DELETE button
	$(\overline{\Box})$ in the line of the address.
Modem IP address verification	Move the switch to the right to let the router request the actual IP address from the modem in case modem's IP address changes before expiration of the previous one.

Creating IPIP6 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 IPIP6	•
Connection name* ipipv6_33	
Enable connection	
NAT NAT	
() The network address translation function. It is recommended not to disab unless your ISP requires it.	le
Ping	
() WAN Ping Respond allows the device to respond to ping requests from the external network.	3

Figure 95. The page for creating a new **IPIP6** connection. The **General Settings** section.

Parameter	Description
General Settings	
Connection name	A name for the connection for easier identification.
Enable connection	Move the switch to the right to enable the connection. Move the switch to the left to disable the connection.
NAT	If the switch is moved to the right, the network address translation function for IPv4 is enabled. Do not disable the function unless your ISP requires this.
Ping	If the switch is moved to the right, the router responds to ping requests from the external network through this connection. For security reasons, it is recommended to disable this function.

Obtain remote host address automatic	ally
Remote host	Ţ
Mode*	
DSLite	•

Figure 96. The page for creating a new **IPIP6** connection. The **IP** section.

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

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

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

If you have already configured the connection to the Internet and you want to use this WAN connection only to connect to the virtual private network, select the **to the virtual private network** choice of the radio button. Then select an existing connection which will be used to access the VPN server or select the **create a new connection** choice of the radio button and click the **CONTINUE** button.

Creating 6in4 WAN Connection

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

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	Remote host*
Connection type	
6in4 🗸	
	Client IPv6 address*
Connection name*	
6in4_59	
	Server IPv6 address*
Enable connection	
	 Enter the server and client IPv6 addresses received from the tunnel broker without specifying the prefix length (for example, 2001:0DB8::1)
Ping	without specifying the prenx length (for example, 2001.00681)
() WAN Ping Respond allows the device to respond to ping requests from the external network.	Routed IPv6 network*
RIPng	Enter the IPv6 subnet which will be routed through the connection of 6in4 type without specifying the prefix length (for example, 2001:0DB8::)
	Set MTU automatically

Figure 97. The page for creating a new **6in4** connection.

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

Parameter	Description
Routed IPv6 network	Enter the address of the routed IPv6 subnet (without specifying the prefix length) provided by the tunnel broker.
Set MTU automatically	Move the switch to the right to set the maximum size of units transmitted by the interface automatically. Move the switch to the left to specify this parameter manually. Upon that the MTU field is displayed.
мти	The maximum size of units transmitted by the interface.

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

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

Creating 6to4 WAN Connection

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

General Settings	6to4 Relay Router 192.88.99.1	Α
Connection type		
6to4 •	Set MTU automatically	
Connection name*		
6to4_74		
Enable connection		
Ping		
() WAN Ping Respond allows the device to respond to ping requests from the external network.		

Figure 98. The page for creating a new **6to4** connection.

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

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

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

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

Creating 6rd WAN Connection

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

General Settings	Obtain 6rd settings automatically	
Connection type		
6rd -	6rd Border Relay	
Connection name*		
6rd_18	6rd IPv6 prefix	
Enable connection	6rd IPv6 prefix length	
•	32	
Ping Ping		
0	IPv4 mask length	
WAN Ping Respond allows the device to respond to ping requests from the external network.	0	A
	Hub and spoke	
	Set MTU automatically	

Figure 99. The page for creating a new 6rd connection.

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

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

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

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

LAN

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

IPv4

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

IP address*	
192.168.0.1	
Mask*	
255.255.255.0	
Hostname	
dlinkrouter.local	
 Specify a domain n 	ame ending with .local. In order to access the web-
0, ,	e domain name, enter this name with a dot and slash
at the end in the addres dlinkrouter.local./)	s bar of the web browser (for example,

Figure 100. 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. When this value is selected, the controls of the Dynamic IP Addresses section are not available. Also when this value is selected, the Obtain DNS server addresses automatically switch is displayed on the tab. 	
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 .	

Parameter	Description
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). Optional.
Hostname	The name of the device assigned to its IPv4 address in the local subnet.
Obtain DNS server addresses automatically	Available if the Access point, Repeater, or Client mode was selected in the Initial Configuration Wizard. Move the switch to the right to configure automatic assignment of DNS server IPv4 addresses. Upon that the DNS IP address field is not available for editing.
DNS IP address	 Available if the Access point, Repeater, or Client mode was selected in the Initial Configuration Wizard. If needed, specify a DNS server IPv4 address for the selected mode of local IP address assignment. If you want to specify several DNS servers, click the ADD button, and in the line displayed, enter the IPv4 address. To remove the address, click the DELETE button (1) in the line of the address. The DNS servers specified on this page will have higher priority than the servers specified on the Advanced / DNS page.

Dynamic IP Addresses	
Mode of DHCF	IPv4 address assignment
Start IP*	
192.16	68.0.100
End IP*	
192.16	68.0.199
SELEC	T ADDRESS RANGE
Lease tin	ne (in minutes)*
1440	
	DNS relay
\sim	igns the LAN IP address of the device as the DNS server for ed clients.

Figure 101. 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 State IP, Option 82 Circuit ID, Option 82 Remote ID, and Option 82 Subscriber ID fields are displayed on the tab. Available if the Router, WISP Repeater, or Mobile Internet mode was selected in the Initial Configuration Wizard. 		
Start IP	The start IP address of the address range used by the DHCP server to distribute IP addresses to clients.		
End IP	The end IP address of the address range used by the DHCP server to distribute IP addresses to clients.		
SELECT ADDRESS RANGE	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the SAVE button to automatically fill in the Start IP and End IP fields.		
Lease time	The lifetime of IP addresses leased by the DHCP server. At the end of this period the leased IP address is revoked and can be distributed to another device, unless the previous device has confirmed the need to keep the address.		
DNS relay	Move the switch to the right so that the devices connected to the router obtain the address of the router as the DNS server address. Move the switch to the left so that the devices connected to the router obtain the address transmitted by the ISP or specified on the Advanced / DNS page as the DNS server address.		

Parameter	Description
External DHCP server IP	The IPv4 address of the external DHCP server which assigns IPv4 addresses to the router's clients.
	To specify several IPv4 addresses, click the ADD button, and in the line displayed, enter an IPv4 address.
	To remove the IPv4 address, click the DELETE button ($\overline{\square}$) in the line of the address.
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.

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.

```
DHCP Options +
```

Figure 102. Configuring the local interface. The IPv4 tab. The section for configuring DHCP options.

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

DHCP Options	×
Supported DHCP options Select option	•
Options value	
Force	
SAVE	

Figure 103. 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	
Supported 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 ($\overline{\mathbf{II}}$). 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 104. Configuring the local interface. The **IPv4** tab. The section for creating MAC-IPv4 pairs.

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

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

To remove a MAC-IPv4 pair, select the checkbox located to the left of the relevant line in the table and click the **DELETE** button ($\boxed{10}$). Then click the **APPLY** button.

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

Add Host	×
Name*	
IP address*	•
ADD	
SAVE	

Figure 105. Configuring the local interface. The **IPv4** tab. The window for adding a DNS record.

In the **Name** field, specify the hostname or full 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 ($\boxed{\blacksquare}$).

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

IPv6

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

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

Figure 106. 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. To change an IPv6 address of the router, edit the corresponding line.

To remove an IPv6 address, click the **DELETE** $(\overline{\square})$ button in the corresponding line of the table. Then click the **APPLY** button.

Also you can specify the following parameters:

Parameter	Description	
Local IPv6 Address		
	Available if the Access point, Repeater, or Client mode was selected in the Initial Configuration Wizard.	
Gateway IPv6 address	The gateway IPv6 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> .	
Hostname	The name of the device assigned to its IPv6 address in the local subnet.	

Parameter	Description
	Available if the Access point, Repeater, or Client mode was selected in the Initial Configuration Wizard.
	If needed, specify a DNS server IPv6 address.
DNS IP address	If you want to specify several DNS servers, click the ADD button, and in the line displayed, enter the IPv6 address.
	To remove the address, click the DELETE button ($\boxed{10}$) in the line of the address.
	The DNS servers specified on this page will have higher priority than the servers specified on the Advanced / DNS page.

In the Dynamic IP Addresses section, you can configure IPv6 addresses assignment settings.

Dynamic IP Addresses	
	f IPv6 address assignment
Statef	Tul -
Start IP*	٠
::2	
End IP*	
::64	
Lease tir 1440	me (in minutes)*
i Lea time.	se time will be chosen by ISP based on the delegated prefix lif
	The default route for LAN clients
	DNS relay
-	igns the LAN IP address of the device as the DNS server for ed clients

Figure 107. 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, WISP Repeater, or Mobile Internet 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.	
SELECT ADDRESS RANGE	Use the button to set one of the available IP address ranges. In the window displayed, select the needed range and click the SAVE button to automatically fill in the Start IP and End IP fields.	
Lease time	The lifetime of IPv6 addresses provided to clients.	
The default route for LAN clients	Move the switch to the right to let the clients, that received IPv6 addresses or configured them using the prefix, use the router as the default IPv6 route.	
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 IPv6 address of the external DHCP server which assigns IPv6 addresses to the router's clients. To specify several IPv6 addresses, click the ADD button, and in the line displayed, enter an IPv6 address. To remove the IPv6 address, click the DELETE button (1) in the line of the address. 	

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 108. 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	
SAVE	

Figure 109. Configuring the local interface. The IPv6 tab. The window for adding a DNS record.

In the **Name** field, specify the hostname or full domain name to which the specified IPv6 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 IPv6 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.

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.

😑 < Home		WAN Failover	
	WAN backup function, which provides y uter activates the backup connection; a	you with uninterrupted access to the Internet. When your main connection and when the main channel is recovered, the router switches to it and	
Connections	Pv4 connections on order of priority.	Check with ping Interval between checks (in seconds)*	
Connection	Check with ping	30 Waiting for response (in seconds)*	
pppoe_95	On	1	
WAN	On	Number of ping requests* 3	
		Hosts	
		8.8.8	×
		77.88.55.55	×
		94.100.180.200	×
		ADD HOST	
APPLY			

Figure 110. 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.

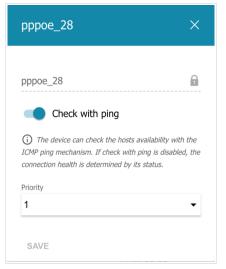


Figure 111. The window for changing the priority of a connection.

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 ping requests fields values.	
	After a successful check the router keeps using the main connection. If the check fails, the router repeats it. After two failed checks the next operational connection from the list will be used as the default connection.	
Waiting for response A time period (in seconds) allocated for a response to one request.		
Number of ping requestsThe number of ping requests sent for each check.A check is considered failed in case none of the sent pine receive a response.		
Hosts	External IP addresses that the router will check for availability via ICMP ping mechanism. Click the ADD HOST button, and in the line displayed, enter an IP address or leave values suggested by the router.	
	To remove an IP address from the list, click the Delete icon (\times) in the line of the address.	

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

Auto Configuration of 3G/LTE

On the **Connections Setup / Auto Configuration of 3G/LTE** page, you can enable the function for automatic creation of a mobile WAN connection upon plugging a USB modem into the router.

≡	🗸 Summary	Auto Configuration of 3G/LTE	
	Itomatic Creation of Mobile	e Internet Connection	
()	 Set as default gateway Create without IMSI Allows to automatically create a Mobile Internet 	connection without ISP-	
	ific settings (APN, username, password).		

Figure 112. The Connections Setup / Auto Configuration of 3G/LTE page.

If you want to enable the function for automatic creation of a mobile WAN connection, click the **ENABLE** button. If needed, change the settings on this page.

Parameter	Description	
Set as default gateway	Move the switch to the right to allow the router to use an automatically created mobile WAN connection as the default connection. Move the switch to the left if you want the router to continue using the existing default connection when automatically creating a	
	mobile WAN connection.	
Create without IMSI	Move the switch to the right to enable automatic creation of a mobile WAN connection without the operator's settings. This setting will be useful if the code stored in the SIM card is unavailable.	
	Move the switch to the left to disable automatic creation of a mobile WAN connection without the operator's settings.	

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

If the PIN code check for the SIM card inserted into your USB modem is disabled, then an active WAN connection with the operator's settings will be automatically created when plugging the USB modem into the router. The connection will be displayed on the **Connections Setup / WAN** page.

If you want to disable the function for automatic creation of a mobile WAN connection, click the **DISABLE** button.

Traffic Balancing

On the **Connections Setup / Traffic Balancing** page, you can enable the traffic balancing function. This function enables equal load balancing on the router and increases maximum bandwidth of your Internet connection while using several WAN connections (for example, if access to the Internet is provided by several ISPs).

Auto configuration of 3G/LTE	Traffic Balancing	
Traffic Balancing		
Connections List +		
APPLY		

Figure 113. The Connections Setup / Traffic Balancing page.

To enable the traffic balancing function, move the **Enable** switch to the right. Then add connections to the page among which traffic will be balanced. To do this, click the **ADD** button

(+) in the **Connections List** section.

Connection	×
Connection* Not selected	•
Traffic adjustment Auto	Ŧ
SAVE	

Figure 114. The window for adding a new connection to the page.

In the opened window, specify the needed parameters.

Parameter	Description	
Connection	From the drop-down list, select a WAN connection to which traffic balancing will be applied.	
Traffic adjustment	 Select a value from the drop-down list. Auto: Traffic is equally divided among connections with the same setting. Manual: Traffic is equally divided among connections in accordance with the value specified in the Weight field. 	
Weight	Specify the percentage of traffic which will pass through the connection.	

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

To edit the setting for an added connection, in the **Connections List** section, select the relevant line in the table. In the opened window, change the value and click the **SAVE** button.

To remove a connection from the page, in the **Connections List** section, select the checkbox

located to the left of the relevant line of the table and click the **DELETE** button ($\overline{10}$).

After specifying the needed parameters, click the **APPLY** button. Upon that the **Status** field is displayed on the page.

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

VPN

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

IPsec

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

IPsec is a protocol suite for securing IP communications.

ALG/Passthrough		IPsec		
IPsec You can configure VPN tunnels b DISABLE	ased on IPsec protocol.			
Logging level Basic		•		
Tunnels reconnect +				
Remote host	Mode Interface	Encryption/hashing a	Igorithm	
		The First Phase	The Second Phase	
Status				
Remote host	IKE	CHILD	State	

Figure 115. The VPN / IPsec page.

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

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

From the **Logging level** drop-down list, select a detail level of messages recorded to the system log or leave the value specified by default. The **Basic** value is recommended to establish an IPsec tunnel faster. To view the log, go to the **System / Logging / Local** page (see the *Local* section, page 294).

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

The values selected from the **IP version**, **Mode**, **IKE version** lists and the values of the **Pre-shared key** field and elements in the **The First Phase** and **The Second Phase** sections should be the same for both parties of the tunnel.

The values of the remote settings for one party of the tunnel should be the same as the values of the local settings for the other party of the tunnel.

🗧 🗶 IPsec	IPsec/Adding		
General Settings			
Caller Enable	DPD action		
Name*	Restart -		
IPsec_72	() DPD - Dead Peer Detection		
IP version	DPD delay (in seconds)*		
IPv4	→ 30		
~	DPD timeout (in seconds)*		
Dynamic IPsec	120		
Туре			
Address	TCP MSS Path MTU discovery		
Remote host*	Aggressive Mode		
	IKE version		
Remote identifier	1		
Remote port	When the IKE version is changed, the first and second phase parameters can be changed.		
Pre-shared key*	Q		
Local WAN			
Default gateway	•		
Local identifier			
Local port			
NAT Traversal			
Enabled	•		
Mode TUNNEL	·		
Allow traffic from IPsec to route			

Figure 116. The page for adding an IPsec tunnel. The General Settings section. In the **General Settings** section, you can specify the following parameters:

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

Parameter	Description	
Name	A name for the tunnel for easier identification.	
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. Use an IP address of a host or subnet, the value %any (all IP addresses), a domain name, or certificate CN. By default, the value specified in the Remote host field is used.	
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 at the same time the network address translation (NAT) function is used for the connection, port 4500 is used.	
Pre-shared key	A PSK key for mutual authentication of the parties. Click the Show icon (\bigotimes) to display the entered key.	
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. 	

Parameter	Description		
Local identifier	A local identifier of the router to establish connection over IPsec with particular hosts only. 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 at the same time 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-1260 allows to forcibly encapsulate VP traffic in UDP packets for passing through a remote device regardle 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. 		
Allow traffic from IPsec to router	Move the switch to the left to deny access to your router from the remote subnet via IPsec. The switch is displayed when the TUNNEL value is selected from the Mode drop-down list.		

Parameter	Description		
DPD action	 Using DPD protocol (<i>Dead Peer Detection</i>) allows to check the status of the remote host in the tunnel: if encrypted packets exchange between the router and the remote host breaks down, the router starts sending DPD requests to the remote host. Select the needed action from the drop-down list. Restart: Restart the tunnel connection immediately. Hold: Reestablish the connection upon request when the traffic matching the tunnel appears. Clear: Close the tunnel connection with no further action. Off: Disable DPD. When this value is selected, 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. 		
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. The switch is displayed when the 1 value is selected from the IKE version drop-down list. 		
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.		

To specify encryption algorithms for the first and second phases of the IPsec tunnel, click the **ADD** button (+) in the **The First Phase** and **The Second Phase** sections correspondingly. You can specify several combinations of encryption algorithms for each phase of the IPsec tunnel. In the opened window, you can specify the following parameters:

The First Phase	X
First phase encryption algorithm	
DES	•
Encryption mode	
CBC	•
Hashing algorithm	
MD5	•
Size of hash	
96	•
Hashing mode	
HMAC	•
First phase DHgroup type	
MODP768	•

Figure 117. The window for configuring the first phase of the IPsec tunnel. The First Phase section.

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.			
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.			

Parameter	Description		
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.		
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.		
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-1260.		

Click the **SAVE** button.

To edit the parameters for each phase of the IPsec tunnel, in the relevant section, select the relevant line in the table. In the opened window, change the needed parameters and click the **SAVE** button.

To remove an encryption algorithm for a phase, in the relevant section, 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 an algorithm in the editing window.

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

Add Rule	\times
ocal network	
ADD SUBNET	
Specify the local subnet of IPsec tunnel (the router's LAN). Example: 192.168.0.0/24	
Remote subnet	
ADD SUBNET	
Specify the remote subnet of IPsec tunnel (the l of the device which acts as a router). Example: 192.168.10.0/24	AN
NTU*	
1300	

Figure 118. 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 General Settings 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 General Settings 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 (1). Also you can remove a subnet in the editing window.

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

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

To disconnect an existing tunnel and establish it again, select the checkbox located to the left of the relevant line in the table and click the **RECONNECT** button.

To remove an existing tunnel, select the checkbox located to the left of the relevant line in the table

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

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

GRE

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

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

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

Figure 119. The VPN / GRE page.

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

≡ < GRE	GRE/Adding
Tunnel settings	Static route settings
Carlo Enable	Remote GRE interface subnet*
Name* GRE_8	Remote LAN IP addresses
IP address*	ADD SUBNET
Interface*	
Not selected	•
Remote IP address*	
мтu+ 1400	
Allow traffic GRE -> LAN	
APPLY	

Figure 120. The page for adding a GRE tunnel.

You can specify the following parameters:

Parameter	Description			
Tunnel settings				
Enable	Move the switch to the right to enable the GRE tunnel. Move the switch to the left to disable the GRE tunnel.			
Name	A name of the tunnel for easier identification. You can specify any name.			
IP address	The IP address of the GRE tunnel interface with the mask of the subnet.			
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.			
Remote IP address	Enter the IP address of the remote subnet VPN gateway.			
MTU	The maximum size of units transmitted from the remote host to the router.			
Allow traffic GRE → LAN	Move the switch to the right to allow GRE tunnel users access devices in the remote local subnet.			
	Static route settings			
Remote GRE interface subnet	The subnet and mask of the remote GRE interface.			
Remote LAN IP addresses				
Remote subnet	To specify the IP address and mask of the remote local subnet, click the ADD SUBNET button, and in the line displayed, enter the needed value.			
	To remove a subnet, click the Delete icon (\times) in the corresponding line.			

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

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

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

IPIP

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

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

😑 < GRE		IPIP	
IPIP You can configure VPN tunnels	based on IPIP protocol.		
No tunnel created You can add a tunnel	+		

Figure 121. The VPN / IPIP page.

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

	IPIP/Adding	
Tunnel settings Enable Name* IPIP_72 IP address* Interface* Not selected	Static route settings Remote IPIP interface subnet* Remote LAN IP addresses ADD SUBNET	
Remote IP address* MTU* 1400 Allow traffic IPIP -> LAN APPLY		

Figure 122. The page for adding an IPIP tunnel.

You can specify the following parameters:

Parameter Description		
Tunnel settings		
EnableMove the switch to the right to enable the IPIP tunnel.Move the switch to the left to disable the IPIP tunnel.		
Name	A name of the tunnel for easier identification. You can specify any name.	
IP address The IP address of the IPIP tunnel interface with the mask of t subnet.		
InterfaceFrom the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.		
Remote IP address Enter the IP address of the remote subnet VPN gateway.		
MTU	The maximum size of units transmitted from the remote host to the router.	
Allow traffic IPIP \rightarrow LAN	Move the switch to the right to allow IPIP tunnel users access devices in the remote local subnet.	
Static route settings		
Remote IPIP interface subnet	The subnet and mask of the remote IPIP interface.	
Remote LAN IP addresses		
Remote subnet	To specify the IP address and mask of the remote local subnet, click the ADD SUBNET button, and in the line displayed, enter the needed value.	
	To remove a subnet, click the Delete icon (x) in the corresponding line.	

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

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

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

PPTP/L2TP Servers

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

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

😑 🔇 Summary		PPTP/L2TP Servers	
	РРТР	L2TP	
No server added You can add a server	+		

Figure 123. The VPN / PPTP/L2TP Servers page.

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

Before creating a PPTP or L2TP server with authentication enabled, it is required to create user accounts (see the *VPN Users* section, page 161).

PPTP/L2TP Servers	PPTP/L2TP Servers/Adding
PPTP Server	
Constant Con	Name* PPTP_Server_VPN_99
VPN network	Access policies and NAT
Server local IP address*	vpn <> LAN* Unknown ✓
	VPN <-> WAN*
Start client IP*	Unknown •
End client IP*	VPN → Router* Unknown
Interface* Not selected	NAT VPN -> WAN
	NAT VPN -> LAN
Authentication Enable authentication	Advanced Settings Maximum number of connections* 100
MPPE	MTU*
Enable MPPE MPPE settings are available upon enabled authentication MSCHAP or MSCHAPv2.	on and require only PPP debug
	DNS
	Obtain DNS server addresses automatically
	You can use addresses of the WAN connection selected from the "Interface" list or specify them manually.
	Primary DNS
	1.1.1.1
	Secondary DNS 1.0.0.1
Users List 🔶 🕂	
Users list is empty	

Figure 124. The page for adding a PPTP server.

You can specify the following parameters:

Parameter	Parameter Description	
PPTP Server / L2TP Server		
Enable	Move the switch to the right to enable the server. Move the switch to the left to disable the server.	
NameA name of the server for easier identification. You can specify name.		

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

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

Parameter	Description		
	Advanced Settings		
Maximum number of connections	Available for a PPTP server. The maximum number of devices allowed to connect to the PPTP server.		
Port	PortAvailable for an L2TP server.The port of L2TP server. By default, the value 1701 is specified.		
MTU	The maximum size of units transmitted by the interface.		
PPP debug Move the switch to the right if you want to log all data on the server debugging. Upon that the Debugging messages should be selected from the Level drop-down list in the set the corresponding event log in the Logging section (s 			
	DNS		
Obtain DNS server addresses automaticallyMove the switch to the right to let VPN server's clients obtain 1 server addresses of the WAN connection which is selected from Interface list. Upon that the Primary DNS and Secondary I fields are not available for editing.			
Primary DNS / Secondary DNS	Enter addresses of the primary and secondary DNS servers in the relevant fields.		

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

User	×
User*	
Not selected	-
Set IP address	
Auto	•

Figure 125. A window for adding a user.

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

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

Click the **SAVE** button.

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

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

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

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

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

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

VPN Users

On the **VPN / VPN Users** page, you can create user accounts to provide authorized access to a PPTP or L2TP server.

≡	PPTP/L2TP Servers	VPN Users	
VP	PN Users		
You	I can create user accounts to p	ovide authorized access to a PPTP or L2TP server.	
	ere are no users	+	

Figure 126. The VPN / VPN Users page.

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

User	×
Username*	
Password*	Ø
SAVE	

Figure 127. The window for adding a user.

In the opened window, in the **Username** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.¹² Click the **Show** icon (\bigotimes) to display the entered key.

Click the **SAVE** button.

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

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

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

^{12 0-9,} A-Z, a-z, !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~.

EoGRE

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

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

😑 🗸 VPN Users	EoGRE	
EoGRE You can configure VPN tunnels	s based on EoGRE technology.	
No tunnel created You can add a tunnel	+	

Figure 128. The VPN / EoGRE page.

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

≡ < Eogre	EoGRE/Adding
Enable	
Enable creation of WAN connection	
Name*	Interface*
EoGRE_6	Not selected
	MTU*
Remote IP address*	1400
Tagged traffic	
APPLY	

Figure 129. The page for adding an EoGRE tunnel.

You can specify the following parameters:

Parameter	Description
Enable	Move the switch to the right to enable the EoGRE tunnel.
LIIADIe	Move the switch to the left to disable the EoGRE tunnel.

Parameter	Description
Enable creation of WAN connection	Move the switch to the right to use the EoGRE tunnel as an interface for creating a WAN connection. For further configuration, you need to create a VLAN which will include the EoGRE interface (see the <i>VLAN</i> section, page 219), and then create a WAN connection which will be assigned to the interface of this VLAN (see the <i>WAN</i> section, page 84). Move the switch to the left if creating a WAN connection is not required.
Name	A name of the tunnel for easier identification. You can specify any name.
Remote IP address	The IP address of the remote local subnet.
Tagged traffic	Move the switch to the right to assign a tag (VLAN ID) to EoGRE traffic and specify the needed value in the VLAN ID field displayed.
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.
МТО	The maximum size of units transmitted by the interface.

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

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

To remove an existing tunnel, select the checkbox located to the left of the relevant line in the table

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

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

EolP

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

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

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

Figure 130. The VPN / EoIP page.

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

≡ < EoIP	EoIP/Adding	
Carle Enable		
Enable creation of WAN connection		
Name*	Interface*	
EoIP_14	Not selected	•
	MTU*	
Remote IP address*	1400	
Tunnel ID*	C Keep Alive	
MAC address		
Tagged traffic		
APPLY		

Figure 131. The page for adding an EoIP tunnel.

You can specify the following parameters:

Parameter	Description
Enable	Move the switch to the right to enable the EoIP tunnel. Move the switch to the left to disable the EoIP tunnel.
Enable creation of WAN connection	Move the switch to the right to use the EoIP tunnel as an interface for creating a WAN connection. For further configuration, you need to create a VLAN which will include the EoIP interface (see the <i>VLAN</i> section, page 219), and then create a WAN connection which will be assigned to the interface of this VLAN (see the <i>WAN</i> section, page 84). Move the switch to the left if creating a WAN connection is not required.
Name	A name of the tunnel for easier identification. You can specify any name.
Remote IP address	Enter the IP address of the remote local subnet.
Tunnel ID	Specify a unique identifier of the tunnel. The value for both parties which establish the tunnel should be the same.
MAC address	A MAC address assigned to the EoIP tunnel interface. <i>Optional</i> . If the field is blank, the MAC address is assigned automatically.
Tagged traffic	Move the switch to the right to assign a tag (VLAN ID) to EoIP traffic and specify the needed value in the Tag ID field displayed.
Interface	From the drop-down list, select a WAN connection through which the tunnel will pass. Select the Default gateway value to use the default WAN connection.
MTU	The maximum size of units transmitted by the interface.
Keep Alive	Move the switch to the right to let the router detect the state of the tunnel on the other end. In the Interval and Attempts fields displayed, specify the required values. The router sends several check requests. If after several failed attempts the connection on the other end of the tunnel is inactive, the tunnel will be disabled. Upon that it will be enabled automatically when the other end tries to establish the connection.
Interval	A time period (in seconds) allocated for one request to check the state of the tunnel on the other end. By default, the value 5 is specified.

Parameter	Description
Attempts	A number of failed attempts to check the state of the tunnel on the other end after which the tunnel is disabled. By default, the value 5 is specified.

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

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

To remove an existing tunnel, select the checkbox located to the left of the relevant line in the table

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

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

Wi-Fi

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

Basic Settings

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

≡ < wan Basic S	Settings 🖸
2.4 GHz	5 GHz
Basic Settings	
You can change basic parameters for the wireless interface of the device	
Enable Wireless	Wi-Fi Network
•	Network name (SSID)*
Country RUSSIAN FEDERATION	DIR-XXX
Wireless mode	Hide SSID
802.11 B/G/N mixed -	() Wireless network name (SSID) will not appear in the list of available wireless
Select channel automatically	networks with customers. Go to a hidden network, you can connect to manually specify the SSID of the access point
(i) The least loaded data transfer channel will be used	BSSID
	00:98:c8:24:ac:a5
Enable additional channels	Max associated clients*
① Attention! The device automatically selects a channel from the list of available channels depending on your country. Make sure that your wireless devices	0
support channels above 12	Broadcast wireless network
Channel	
auto (channel 5) 🔒 🖸	① Allows you to enable/disable broadcast of this SSID without disconnecting the wireless module of the router. Can be used with the mode "Wi-Fi Client"
~	wireless module of the router. Can be used with the mode "Wi-H Client"
Enable periodic scanning	Clients isolation
① The device will periodically check the channels load and switch to the least loaded one	() Block traffic between devices connected to the access point
Scanning period (in seconds)	Security Settings
0	Network authentication
	WPA2-PSK -

Figure 132. 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 289) 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 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
	The wireless channel number.
Channel	To select a channel manually, left-click; in the opened window, select a channel and click the SAVE button. The action is available, when the Select channel automatically switch is moved to the left.
	To make the router select the currently least loaded channel, click
	the Refresh icon (\mathbf{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*	
		4
Wireless network name (SSID) will not appear in the networks with customers. Go to a hidden network, you c specify the SSID of the access point		
	Encryption type*	
Max associated clients* D	AES	
5		
Broadcast wireless network	Group key update interval (in seconds)*	
	3600	
Allows you to enable/disable broadcast of this SSID wireless module of the router. Can be used with the module		
	de <i>merelien</i> e	
Clients isolation		
Block traffic between devices connected to the acce	ess point	
Enable guest network		
	lients from the LAN	
	lients from the LAN	

Figure 133. 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
Broadcast wireless network	If the wireless network broadcasting is disabled, devices cannot connect to the wireless network. Upon that DIR-1260 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 289) 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. 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 or click the DELETE FROM SCHEDULE button. If you created an additional network, you can configure, change or delete a schedule for each network. To do this, click the button in the line of the network.
Clients isolation	Move the switch to the right to forbid wireless clients of this wireless network to communicate to each other.
Enable guest network	This function is available for the additional network. Move the switch to the right if you want the devices connected to the additional network to be isolated from the devices and resources of the router's LAN.

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

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

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 134. 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.	
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	•
(i) It is recommended to use the first key by o with many devices.	lefault to ensure compatibility
Encryption key WEP as HE	Х
Encryption key WEP as HE Length of WEP key should be 5 or 13 chail	
	racters.
() Length of WEP key should be 5 or 13 chai	racters.
() Length of WEP key should be 5 or 13 chai	
Length of WEP key should be 5 or 13 chai Encryption key 1*	racters.
Length of WEP key should be 5 or 13 chai Encryption key 1*	ractors.
① Length of WEP key should be 5 or 13 chail Encryption key 1* Encryption key 2*	racters.

Figure 135. The **Open** value is selected from the **Network authentication** drop-down list.

Parameter	Description
Enable encryption WEP	For Open authentication type only. 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:

Password PSK*	
•••••	Ø
Password should be between 8 and 63 ASCII characters Encryption type*	
AES	•

Figure 136. 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. ¹³ 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.
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.

^{13 0-9,} A-Z, a-z, space, !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~.

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

Network	authentication	
WPA2		-
VVFA2		•
	WPA2 Pre-authentication	
IP addre	ss RADIUS server*	
192.16	8.0.254	
RADIUS	erver port*	
1812		
RADIUS	encryption key*	
dlink		
Encrypti	on type*	
AES		•
Group k	y update interval (in seconds)*	
3600		

Figure 137. 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.		

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 Setting	s	Client Mai	nagement			
Client Managen You can vlew the list of v	nent vireless clients connected to ti	he router.				
List of Wi-Fi Clien	ts REFRESH DISCONNE	СТ				
Hostname	MAC address	Band	Network name (SSID)	Signal level	Online	
Galaxy-M21	66:C5:55:3D:D2:91	2.4 GHz	DIR-XXX	रू 100%	0 min	

Figure 138. 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.

≡ < Summary W	/PS	
2.4 GHz	5 GHz	
WPS The WPS function helps to automatically connect to the wireless netw DISABLE WPS	rork of the router. The connecting devices must si	upport this function.
WPS Control	Information	
	Default PIN code:	12345670
ESTABLISH CONNECTION	Network name (SSID):	DIR-XXX
	Network authentication:	WPA2-PSK
Enable WPS function with hardware button	Encryption:	AES
① Move the switch to the left in order to forbid enabling the WPS function with the relevant hardware button	Password PSK:	12345670
	UPDATE	

Figure 139. The page for configuring the WPS function.

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

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

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

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

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

Parameter	Description
Default PIN code	The PIN code of the router. This parameter is used when connecting the router to a registrar to set the parameters of the WPS function.
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. Make sure that the **Enable WPS function with hardware button** switch is moved to the right on the tabs of both bands.
- 3. Click the **ENABLE WPS** button.
- 4. Close the web-based interface (click the **Logout** line of the menu).

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

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

WMM

On the **Wi-Fi / WMM** page, you can enable the Wi-Fi Multimedia function. To configure the 2.4GHz band or 5GHz band, go to the relevant tab.

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.

WPS						W	'MM					
			2.4 GHz				_			5 GHz		
The me Work m	Vi-Fi Multimedia he mechanism for improving WI-Fi network performance. It is recommended for users not to change the specified values Vork mode Manual											
Acce	ss Point						Statio	on				
AC	AIFSN	CWMin	CWMax	TXOP	ACM	ACK	AC	AIFSN	CWMin	CWMax	ТХОР	ACM
BE	3	15	63	0	off	off	BE	3	15	1023	0	off
ВК	7	31	1023	0	off	off	ВК	7	15	1023	0	off
VI	2	7	15	94	off	off	VI	2	7	15	94	off
VO	2	3	7	47	off	off	VO	2	3	7	47	off

Figure 140. 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 141. 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
АСК	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.

🗮 < Summary	Client		E
2.4GHz		5GHz	
Wi-Fi Client You can configure the router as a client to connect to a	wireless access point or to a WISP		
C Enable			
Broadcast wireless network 2.4 GHz			
If the broadcast switch is moved to the left, devices cannot a router's WLAN. Upon that the router can connect to another accumireless client.			
Connecting to network Select network from list	•		
APPLY Wireless Networks UPDATE LIST			
Network name (SSID)	Security Settings	RSSI	Channel
ົຈີຍ [SDK2] DIR-825-799C-799B	[WPA2-PSK] [AES]	-79dBm	13
ିକ୍ତି [SDK2] DWR-956-0002-0001	[WPA2-PSK] [AES]	-79dBm	6

Figure 142. 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	For Open authentication type only. 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-1260 will switch to the channel of the access point to which you have connected.

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

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

Additional

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

C1 ·	· 1 · 1 ·		. 1	<u> </u>		TTT AR	L T I
I honging noromotore	nragantad on thig	nanamai	i norotivolv	attact v	uour V	A/I /\r	
Changing parameters	DICSCHICCI OH HIS	טמצט ווומע	Inceatively	ancu	vou v	V LAI	N !

≡ < Summary Add	itional	
2.4 GHz	5 GHz	
Wi-Fi Additional Settings You can define additional parameters for the WLAN of the router.		
Bandwidth Auto	B/G protection Auto	•
Using bandwidth of one or several channels of the wireless network simultaneously	Short GI Enable	•
 <i>Current bandwidth: 40 MHz</i> Autonegotiation 20/40 (Coexistence) 	Beacon period (in milliseconds)* 100	
Automatic change of bandwidth in the loaded environment TX power (in percent)	RTS threshold (in bytes)* 2347	
100 Preamble*	Frag threshold (in bytes)* 2346	
Auto -	DTIM period (in beacon frames)* 1	
Disables multicasting (IGMP, SSDP, etc.) for the wireless network. In some cases this helps to improve performance	Station Keep Alive (in seconds)* O	
STBC		
Enable 802.11k		
APPLY		

Figure 143. Additional settings of the WLAN.

The following fields are available on the page:

Parameter	Description
Bandwidth	The channel bandwidth for devices operating on modern standards. When the Auto value is selected, router automatically chooses the most suitable channel bandwidth for these clients.
Autonegotiation 20/40 (Coexistence)	Available on the 2.4 GHz tab. 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.
Preamble	 This parameter defines the length of the CRC block sent by the router when communicating to wireless devices. Select the needed value from the drop-down list. Auto: The length of the block is defined automatically. Long: The long block. Short: The short block (this value is recommended for networks with high-volume traffic).
Enable DFS	Available on the 5 GHz tab. 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.
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.

Parameter	Description
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.
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.
Enable 802.11k	802.11k standard allows faster roaming of clients between access points within the same network. Clients supporting 802.11k standard can request a list of neighbor access points with their signal levels and Wi-Fi channel numbers. The device does not need to probe all of the available channels, but selects an access point to roam to from the list. Move the switch to the right if you need to use 802.11k standard.
Enable 802.11v	802.11v roaming allows improving the wireless client load balancing. If the wireless access point supports 802.11v standard, then with a large number of devices connected to this point, a request may be sent to some clients to switch to a less loaded point with the same network parameters or to transfer from a loaded band to a freer band (in case the SSID and security settings are the same in both frequency bands) to improve operation of each client. The request is advisory, upon that the device does not forcibly disconnect clients. Move the switch to the right if you need to use 802.11v standard. The switch is displayed if the Enable 802.11k switch is moved to the right.

Parameter	Description	
B/G protection	 Available on the 2.4 GHz tab. The 802.11b and 802.11g protection function is used to minimize collisions between devices of your wireless network. Select a value from the drop-down list. 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. 	
Short GI	 Guard interval (in nanoseconds). This parameter defines the interval between symbols transmitted when the router is communicating to wireless devices. 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-1260.

≡	🗙 Additional	MAC Filter 🖂	
You	AC Filter I can define a set of MA	C addresses of devices which will be allowed to access the WLAN, or define MAC addresses of devices which will not be N.	
		ded to configure the WI-FI MAC filter through a wired connection to the device	
2.4	4 GHz	5 GHz	
	DIR-XXX (i) Off	DIR-XXX-5G ① Off	
	ters +	îlter	

Figure 144. The page for configuring the MAC filter for the wireless network.

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

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

Add Rule	×
Frequency band 2.4 GHz	•
SSID DIR-XXX	•
(i) MAC filters for this network are disabled	
MAC address*	•
Name*	
Enable	
SAVE	

Figure 145. 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.	
Name	The name of the device for easier identification. 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 289) 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.

Roaming

On the Wi-Fi / Roaming page, you can enable the function of smart adjustment of Wi-Fi clients.

This function is designed for wireless networks based on several access points or routers. If the function is enabled for all access points (routers) which establish a wireless network, then wireless clients will always connect to the device with the highest signal level.

K MAC Filter	MAC Filter Smart Adjustment E	
enabled for all access points (routers) wh with the highest signal level.	Clients ned for wireless networks based on several access points or routers. If the function is ich establish a wireless network, then wireless clients will always connect to the device recommended to specify the same parameters of the WLAN (SSID, authentication type,	
Port** 7890	 Use multicast for service data exchange <i>Select the checkbox if APs are located in different subnets</i> 	
 2.4 GHz Maximum time of storing data (in seconds)* 60 	5 GHz Maximum time of storing data (in seconds)* 60	
 Maximum time of storing data on adjacent of Minimum level of connection quality (in percent) 60 		
Dead zone (from -50% to 50%)* 15	Dead zone (from -50% to 50%)* 15	
Threshold value of connection quality (in percented of the second	t)* Threshold value of connection quality (in percent)* 40	
APPLY		

Figure 146. The Wi-Fi / Roaming page.

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

Parameter	Description
Port	The number of the port used for data exchange between access points (routers).
Use multicast for service data exchange	Move the switch to the right in order to use multicast traffic for service data exchange between access points (routers). This setting is needed if the devices which support the smart adjustment function are located in different subnets. If the switch is moved to the right, the Multicast TTL and Multicast group address fields are displayed on the page. If the switch is moved to the left, broadcast traffic is used for service data exchange.
Multicast TTL	Specify the TTL (<i>Time to live</i>) parameter value.
Multicast group address	Specify the address of the multicast group (from the subnet 239.255.0.0/16).
	2.4 GHz / 5 GHz
Maximum time of storing data	The maximum time period (in seconds) during which the access point (router) stores data on the signal strength of the client located on its coverage area.
Minimum level of connection quality	The signal strength upon which the access point (router) starts scanning other devices in order to find a device with a higher signal level.
Dead zone	This parameter is used for calculation of the signal strength upon which the smart adjustment function goes off. If the signal strength provided by another device is less than the sum of the Minimum level of connection quality field value and the Dead zone field value, then the client disconnects from the access point (router). You can specify the values from -50% to +50%.
Threshold value of connection quality	The signal strength upon which the access point (router) disconnects the client from its wireless network regardless of the signal levels of other devices. This value should not be greater than the value specified in the field Minimum level of connection quality .

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

To disable the function of smart adjustment of Wi-Fi clients, click the **DISABLE** button.

Print Server

On the **Print Server** page, you can configure the router as a print server. Being configured in this way, the router will allow your LAN users to share the printer connected to the USB port of the router.

To connect a printer to the router, power off both devices. Connect the printer to the USB port of the router, power on the printer, then power on the router.

≡	< USB Modem	Print Server		
Yo	rint Server u can configure the router as a print server. E inter connected to the USB port of the router		the router will allow your LAN users to share the	
	Enable print server nter ot selected	<u>.</u>	In order to operate the print server, you should also configure the client PC. For more information on how to configure the print server please refer to the FAQ section at www.dlink.ru.	
Sta	APPLY	connected •		

Figure 147. The Print Server page.

To configure the router as a print server, move the **Enable print server** switch to the right. Make sure that the printer connected to the router is selected from the **Printer** drop-down list. Click the **APPLY** button. The status of the connected device will be displayed in the **Status of print server** field.

If you don't want to use the router as a print server, move the **Enable print server** switch to the left and click the **APPLY** button.

USB Storage

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

- view data on the connected USB storage
- create accounts for users to allow access to the content of the USB storage
- enable the built-in Samba server of the router
- enable the built-in FTP server of the router
- view content of the connected USB storage
- enable the built-in DLNA server of the router
- configure the built-in Transmission torrent client and manage distributing and downloading processes
- enable the XUPNPD plug-in.

Information

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

Print Server	Inforn	nation	
JetFlash TS2GJFV30		JetFlash TS2GJFV30	
usb1_1 Total size: Free:	1.04 GB	usb1_2 Total size: Free:	882.00 MB
Filesystem:	FAT16/32	Filesystem:	NTFS
UNMOUNT		UNMOUNT	
	UNMOUNT AL	L STORAGES	

Figure 148. The USB Storage / Information page.

The following data are presented on the page: the name, total and free space of the storage, and the type of its file system (supported file systems: FAT16/32, exFAT, NTFS, ext2/3/4).

If the USB storage is divided into volumes, a section for every volume (partition) of the USB storage is displayed on the page.

To safely disconnect the USB storage or a volume of the USB storage, click the **UNMOUNT** button in the relevant section and wait for several seconds.

To disconnect all volumes of the USB storage, click the **UNMOUNT ALL STORAGES** button.

USB Users

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

Information USB Users	
(+)	
There are no users	
You can add first user	
ADD	

Figure 149. The USB Storage / USB Users page.

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

Add User	×
Username*	
Password*	ø
Read only	
SAVE	

Figure 150. The window for adding a user.

In the opened window, in the **Username** field, specify a username, and in the **Password** field – the password for the account. Use digits, Latin letters (uppercase and/or lowercase), and other characters available in the US keyboard layout.¹⁴

Some reserved words (e.g., **root**, **admin**, **nobody**, etc.) cannot be usernames.

Move the **Read only** switch to the right not to let the user create, change, or delete files.

Click the **SAVE** button.

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

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

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

^{14 0-9,} A-Z, a-z, space, !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~.

Samba

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

😑 < USB Users	Samba 🖸
Samba On this page you can enable the built-in Samba server of th The Samba server	e router to provide access to the USB storage for users of your LAN.
Configuring a Samba Server	Directories +
Anonymous login	Name Path
(i) If anonymous login is disabled, to access the USB storage contenneeded to create users	t it will be
Work group	
WORKGROUP	
Short description	
D-LINK SERVER	
NetBIOS	
D-LINK	
APPLY	

Figure 151. The USB Storage / Samba page.

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

The **Anonymous login** switch (by default, the switch is moved to the right) allows anonymous access to the content of the USB storage for users of your LAN.

If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

In the **Work group** field, leave the value specified by default (**WORKGROUP**) or specify a new name of a workgroup which participants will have access to the content of the USB storage.

In the **Short description** field, you can specify an additional description for the USB storage. This value will be displayed in some operating systems. Use digits and/or Latin characters.

In the **NetBIOS** field, specify a name of the USB storage which will be displayed for users of your LAN. Use digits and/or Latin characters.

To allow access only to a certain folder of the USB storage, click the ADD (+) button in the **Directories** section.

Add directory	×
Path*	م
Name*	
SAVE	

Figure 152. Specifying a folder.

In the opened window, locate a folder containing files. To do this, click the **Search** icon (\mathbf{Q}) in the **Path** field. Then go to the needed folder and click the **SELECT** button.

In the **Name** field, specify a name of the selected folder which will be displayed for users of your LAN. Use digits and/or Latin characters.

Click the **SAVE** button.

To remove a folder from the list in the Directories section, select the checkbox located to the left

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

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

To disable the built-in Samba server of the router, move the **Enable Samba server** switch to the left and click the **APPLY** button.

FTP

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

🗮 < Home	FTP	
FTP		
	the router to provide access to the USB storage for users of your L	LAN.
Enable FTP server		
For correct display of containing Cyrillic letter	s file names, please use UTF-8 encoding on the FTP client	
Configuring FTP Server		
Anonymous login		
() If anonymous login is disabled, to access the needed to create users	USB storage content it will be	
 When anonymous access is used, all users con read-only access rights 	nnected via the FTP server have	
Port		
21		
Directory	۹	
TLS		
Enabled	•	
The use of TLS may reduce th	e data transfer rate.	
APPLY		

Figure 153. The USB Storage / FTP page.

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

Move the **Anonymous login** switch to the right to allow anonymous access to the content of the USB storage for users of your LAN. If you want to provide authorized access to the content of the USB storage for users of your LAN, move the switch to the left. After applying the parameters on this page, go to the **USB Storage / USB Users** page and create needed accounts.

If needed, change the router's port used by the FTP server in the **Port** field (by default, the standard port **21** is specified).

To allow access only to a certain folder of the USB storage for users of your LAN, locate a folder containing files. To do this, click the **Search** icon (\mathbf{Q}) in the **Directory** field. Then go to the needed folder and click the **SELECT** button.

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

To allow access to all the content of the USB storage for users of your LAN again, remove the value specified in the **Directory** field and click the **APPLY** button.

By default, the TLS (*Transport Layer Security*) encryption protocol is enabled for the FTP server of the router. To change TLS usage parameters, select the required value from the **TLS** drop-down list:

- **Enabled**: When this value is selected, any type of connection to the server is allowed.
- **Disabled**: When this value is selected, attempts to connect via TLS will be rejected.
- **For control connection**: When this value is selected, TLS is required for the control connection, while data can be transferred without encryption.
- For control connection and data: When this value is selected, TLS is required both for the control connection and for data transfer.

To disable the built-in FTP server of the router, move the **Enable FTP server** switch to the left and click the **APPLY** button.

Filebrowser

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

=		Configuration Filebrowser		
,		ebrowser can view the content of your USB storage connected to the router and remove s age.	separate folders and files from the USB	
	\uparrow	usb1_1 FAT16/32		:
(0	.fseventsd 22.04.2020 13:53		
	0	System Volume Information 18.02.2020 18:17		

Figure 154. The USB Storage / Filebrowser page.

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

To go to a folder, click the line corresponding to this folder.

To refresh the folder contents, click the **Actions** icon (:) in the line corresponding to this folder and select the **Refresh** value.

To remove a folder or file, click the **Actions** icon (:) in the line corresponding to this folder or file and select the **Delete** value.

DLNA

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

The built-in media server allows DLNA certified devices of your LAN to play multimedia content of the USB storage. Multimedia content can be played only when a USB storage is connected to the router.

😑 < Filebrowser	DLNA
DLNA On the DLNA page, you can enable the built-in DLNA server of the r The built-in media server allows DLNA certified devices of your LAN played only when a USB storage is connected to the router. To enable the service, you must specify at least one Media Folder.	outer to provide access to the USB storage for users of your LAN. to play multimedia content of the USB storage. Multimedia content can be
Main Settings Enable Update interval* 900	Media Folders + 🔟 Path Type
DLNA server name* D-Link DLNA Server	
APPLY	

Figure 155. The USB Storage / DLNA page.

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

In the **Update interval** field, specify the time period (in seconds), at the end of which the media server updates the file list of the USB storage, or leave the value specified by default (**900**).

In the **DLNA server name** field, specify a name of the DLNA server which will be displayed for users of your LAN or leave the value specified by default (**D-Link DLNA Server**). Use digits and/or Latin characters.

To allow access to the content of the USB storage for users of your LAN, click the **ADD** (+) button in the **Media Folders** section.

Specify Media Folder	×
Path*	
	۹
Type*	
All	•

Figure 156. Specifying a media folder.

In the opened window, locate a folder containing files. To do this, click the **Search** icon (\mathbf{Q}) in the **Path** field. Then go to the needed folder and click the **SELECT** button.

For each folder you can define the type of files which will be available for users of your LAN. To do this, select the needed type of files from the **Type** drop-down list. To share all files of a folder, select the **All** value from the **Type** drop-down list.

Click the **SAVE** button.

To remove a folder from the list in the Media Folders section, select the checkbox located to the

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

After specifying all needed settings on the USB Storage / DLNA page, click the APPLY button.

To disable the built-in DLNA server of the router, move the **Enable** switch to the left and click the **APPLY** button.

Torrent Client

On the **USB Storage / Torrent Client** page, you can configure all needed settings for the built-in Transmission client.

Ξ < Summary Torre	ent Client E
Transmission Using the web-based interface of the built-in Transmission torrent client connected to the router.	you can manage the process of downloading files to the USB storage
Enable	
Main Settings	Authorization Enable
52666	
Path* Q	
Directory* torrents	
Enable download queue	
Download queue size* 1	
Peer limit* 4	
① The recommended maximum number of peers is 4. A higher value can result in unstable performance.	
Enable download speed limit	
Use uTP	
Web-based interface port* 9091	
Web-based interface page: http://192.168.8.254:9091	
APPLY	

Figure 157. The USB Storage / Torrent Client page.

You can specify the following parameters:

Parameter	Description	
Transmission		
Enable Move the switch to the right to activate the Transmission		
Main Settings		
Port The router's port which will be used by the Transmission client.		

Parameter	Description
Path	Locate data of the Transmission client. To do this, click the Search icon (\mathbf{Q}), select the needed value, and click the SELECT button.
Directory	The folder on the USB storage where data of the Transmission client will be stored.
Enable download queue	Move the switch to the right if you want to limit the number of simultaneous downloads. Upon that the Download queue size field will be displayed. Move the switch to the left not to limit the number of simultaneous downloads.
Download queue size	The maximum number of simultaneous downloads. By default, the value 1 is specified.
Peer limit	The maximum number of the service users from which you can download files.
Enable download speed limit	Move the switch to the right to limit the maximum file download speed. In the Download speed limit field displayed, specify the maximum value of speed (KBps). Move the switch to the left not to limit the maximum download speed.
Use uTP	Move the switch to the right to enable μ TP (<i>Micro Transport Protocol, a transport protocol for file sharing</i>). Such a setting can increase the load on the router. Move the switch to the left to disable μ TP.
Web-based interface port	The port on which the web-based interface of the Transmission client is available.
	Authorization
Enable	Move the switch to the right if you want the Transmission client to request for username and password when accessing its web-based interface. Then fill in the Username and Password fields.
Username	The username to access the web-based interface of the Transmission client.
Password	The password to access the web-based interface of the Transmission client.

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

In the **Web-based interface page** field, the address of the web-based interface of the Transmission client is displayed. To access the web-based interface of the Transmission client, click the link.

Transmission Web In ×	
← → C □ 192.168.0.1:9091/transmission/web/	☆ =
For quick access, place your bookmarks here on the bookmarks bar. Imp	ort bookmarks now
🖆 🥥 🕐 🛄	
Show All All (Filter 0 Transfers	✓ 0 kB/s へ 0 kB/s
Choose Files Or enter a URL: Free space : 5.25 ♥ Start when an	rrent file to upload: No file chosen

Figure 158. The web-based interface of the Transmission torrent client.

Using the web-based interface of the built-in Transmission torrent client you can manage the process of downloading files to the USB storage connected to the router.

The following buttons are available on the page:

Parameter	Description
Dpen Torrent	Click the button to add a new torrent file (a metadata file according to which the Transmission client downloads files) to the download queue. In the dialog box appeared, select a file stored on your PC and click the Upload button.
Remove Selected Torrents	Select the torrent file which you want to remove from the download queue and click the button.
Start Selected Torrents	Select the torrent file corresponding to the download which should be restarted and click the button.

Parameter	Description
Start All Torrents	Click the button to restart all downloads. If you limited the maximum number of simultaneous downloads, the Transmission client starts processing of the specified number of torrent files; after completing download of the first one, the client proceeds to the next file in the queue.
Pause Selected Torrents	Select the torrent file corresponding to the download which should be stopped and click the button.
Pause All Torrents	Click the button to stop all downloads.
Toggle Inspector	Select a torrent file and click the button to view its data.

XUPNPD

On the **USB Storage / XUPNPD** page, you can enable the XUPNPD plug-in. It allows to broadcast media content received from the Internet sources or IPTV service to DLNA-certified devices of your LAN.

≡	✔ Torrent Client	XUPNPD	
XU	PNPD		
<u> </u>	<i>"his program is a light DLNA Me</i> st conversion).	dia Server which provides service for sharing IPTV unicast streams over local area network (with UDPXY for multicast to HTTP	
	Enable		
Direc	ctory*	Q	
Servi	ce: http://192.168.0.1:404	14	
	APPLY		

Figure 159. The USB Storage / XUPNPD page.

To use the XUPNPD plug-in, connect a USB storage to the router and move the **Enable** switch to the right.

To let IPTV services operate using the XUPNPD plug-in, enable the UDPXY application.

In the **Directory** field, locate a folder to which playlists added on the page of the XUPNPD plug-in will be saved. To do this, click the **Search** icon (\mathbf{Q}), then go to the needed folder and click the **SELECT** button.

Click the **APPLY** button.

In the **Service** field, the address of the web-based interface of the XUPNPD plug-in is displayed. To access the page of the XUPNPD plug-in and configure all needed settings, click the link.

Figure 160. The XUPNPD plug-in page.

USB Modem

This menu is designed to operate USB modems.



Some models of USB modems do not allow performing operations available in this menu section through the web-based interface of the router.

If the PIN code check for the SIM card inserted into the USB modem is not disabled, the relevant notification will be displayed in the top right corner of the page.

:::	Notification SIM card is blocked
	→ E3131: ENTER PIN

Figure 161. The notification on the PIN code check.

Click the **ENTER PIN** button and enter the PIN code in the **PIN input** window. Click the **Show** icon (\bigotimes) to display the entered code. Then click the **APPLY** button.

PIN input	×
PIN*	ø
(i) The number of remaining attempts: 3	
APPLY	

Figure 162. The window for entering the PIN code.

Some USB modems in the router mode and Android smartphones in the modem mode have an IP address from the subnet which coincides with the router's local subnet. In this case, the router's web-based interface can be unavailable. For correct operation, disconnect the device from the USB port and reboot the router. Then access the web-based interface, go to the **Connections Setup** *I* **LAN** page, and change the value of the **IP address** field on the **IPv4** tab (for example, specify the value **192.168.2.1**). Wait until the router is rebooted.

Basic Settings

On the **USB Modem / Modem name / Basic Settings** page, you can view data on the USB modem connected to the router, change the PIN code of the SIM card inserted into your USB modem, disable or enable the check of the PIN code.

WAN Basic Settings		(
Information		Network information	
Model	E3131	Mode	30
Vendor		RSSI	-67 dBn
IMEI	862733019089559	Signal level	
Interface		Operator name	"MTS RUS
Revision	21.158.13.03.143	Roaming	Disable
Serial number	-	IMSI	25001560272357
		PIN status	Device is unlocked
		SMS	
		DISABLE PIN CODE REQUEST	
		CHANGING PIN CODE	
		USSD	

Figure 163. The USB Modem / Modem name / Basic Settings page.

If the PIN code check for the SIM card inserted into your USB modem is disabled, then an active WAN connection with default settings (for LTE modems) or the operator's settings (for GSM modems) will be automatically created when plugging the USB modem into the router. The connection will be displayed on the **Connections Setup / WAN** page.

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

Parameter	Description		
Information			
Model	The alphanumeric code of the model of your USB modem.		
Vendor	The manufacturer of your USB modem.		
IMEI The code stored in the memory of the USB modem.			
Interface	The network interface name.		
Revision	The revision of the firmware of your USB modem.		
Serial number	The unique identifier assigned to the device by its manufacturer.		

Parameter	Description			
	Network information			
Mode	A type of the network to which the USB modem is connected.			
RSSI The strength of the signal received by the USB modem.				
Signal level	The signal level at the input of the modem's receiver. The zero signal level shows that you are out of the coverage area of the selected operator's network.			
Operator name The name of the mobile operator proving the service.				
Roaming	Roaming mode status of the SIM card inserted into the USB modem.			
IMSI The code stored in the SIM card inserted into your USE				
PIN status PIN code request status of the SIM card inserted into the modem.				
SMS	The number of text messages stored in the memory of the SIM card inserted into the USB modem. Click the number of text messages in the line to go to USB Modem / Modem name / SMS page.			

If the PIN code check for the SIM card inserted into your USB modem is not disabled, the **PIN INPUT** button is displayed on the page.

To disable the PIN code check, click the **DISABLE PIN CODE REQUEST** button (the button is displayed if the PIN code check is enabled). In the opened window, enter the current PIN code in the **PIN code** field and click the **DISABLE** button.

To enable the PIN code check, click the **ENABLE PIN CODE REQUEST** button (the button is displayed if the PIN code check is disabled). In the opened window, enter the PIN code used before disabling the check in the **PIN code** field and click the **ENABLE** button.

To change the PIN code, click the **CHANGING PIN CODE** button (the button is displayed if the PIN code check is enabled). In the opened window, enter the current code in the **PIN code** field, then enter a new code in the **New PIN code** and **New PIN code confirmation** fields and click the **SAVE** button.

If upon one of the operations described above you have entered an incorrect value in the **PIN code** field three times (the number of remaining attempts is displayed in the PIN input window), the SIM card inserted into your USB modem is blocked.

PUK input	×
PUK*	Ø
New PIN code*	Ø
New PIN code confirmation*	Ø
(i) The number of remaining attempts: 10	
APPLY	

Figure 164. The USB Modem / Modem name / Basic Settings page. The window for PUK code input. For further use of the card, click the **PUK INPUT** button, enter the PUK code in the relevant field, and then specify a new PIN code for your SIM card in the **New PIN code** and **New PIN code** confirmation fields. Click the **Show** icon (**(**) to display the entered values. Click the **APPLY** button.

Click the USSD button to go to the USB Modem / Modem name / USSD page.

SMS

When a new text message is received, the relevant notification will be displayed in the top right corner of the page. Click the **CHECK** button. After clicking the button, the **USB Modem / Modem name / SMS** page opens.

On the **USB Modem / Modem name / SMS** page, you can create and send a text message and also view the history and status of sent and received messages stored in the memory of the SIM card.

😑 < Summary		SMS		
SMS		_	SMS Me	mory
SMS: SIM 1 Message filter Incoming Incoming REFRESH Date and time 11.12.2024 11:20:46	From 79537367706	• Message Test	Status Read	REPLY FORWARD

Figure 165. The USB Modem / Modem name / SMS page. The SMS tab.

To view all outgoing and incoming messages on the **SMS** tab, select the relevant value from the **Message filter** drop-down list.

To view the latest data on sent and received messages, click the **REFRESH** button.

To create and send a text message, click the **New message** button (\geq).

New message	×
Number	
ADD Message*	
Enter your message	
Entered characters: 0	
SEND	

Figure 166. The window for creating a new text message.

In the **Number** field, enter the recipient's phone number. If you need to send the text message to several recipients, click the **ADD** button, and in the line displayed, enter a phone number. Enter the text of the message in the **Message** field and click the **SEND** button.

To remove a message, select the checkbox located to the left of the relevant line in the table and

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

To reply to an incoming message, click the **REPLY** button in the line corresponding to the message.

To forward an incoming message, click the **FORWARD** button in the line corresponding to the message.

On the **SMS Memory** tab, you can view data on the number of messages and the state of the SIM card memory.

✓ Home	SMS
SMS	SMS Memory
SMS Memory: SIM 1	
Incoming:	
Outgoing:	
Total:	-
Used memory:	1/5

Figure 167. The USB Modem / Modem name / SMS page. The SMS Memory tab.

USSD

On the **USB Modem / Modem name / USSD** page, you can send a USSD command.¹⁵

USSD (*Unstructured Supplementary Service Data*) is a technology which provides real-time message exchange between a subscriber and a mobile operator's special application. USSD commands are often used to check the SIM card balance, receive data on the rate plan or service packets, etc.

✓ SMS	USSD	
USSD: SIM 1 You can send a USSD request		
Number*		
Response		
SEND		

Figure 168. The USB Modem / Modem name / USSD page.

In the **Number** field, enter a USSD command and click the **SEND** button. After a while, the results will be displayed in the **Response** field.

¹⁵ Contact your operator to get information on USSD commands and their functions.

Advanced

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

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

VLAN

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

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

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

≡	🔇 Summary			VLAN	
	AN can combine inte	erfaces and po	rts of the router to de	marcate traffic on the data link layer.	
VL	AN List 🕂	ÎI			
	VLAN ID	Name	Tagged Ports	Untagged ports	
	-	LAN	-	DIR-XXX (2.4GHz), DIR-XXX-5G (5GHz), LAN1, LAN2, LAN3, LAN4	
	-	WAN	-	WAN	

Figure 169. 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 (+).

😑 < VLAN	VLAN	I/Adding	7
VLAN Name*		Interface If the "Create Interface" function is disabled, the VLAN operates in the transparent bridge mode. Create interface	
VLAN ID* QoS* O			
Ports LAN4 Type Tagged	LAN3 Type Excluded	LAN2 Type Excluded	
LAN1 Type Excluded •	WAN Type Excluded	•	
Wireless interfaces			
DIR-XXX (2.4GHz) Type Excluded	DIR-XXX-5G (5G Type Excluded	iHz)	
APPLY			

Figure 170. The page for adding a VLAN.

You can specify the following parameters:

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

Parameter	Description	
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 ($\boxed{10}$).

WAN Assignment

On the **Advanced / WAN Assignment** page, you can use LAN ports of the router as additional WAN ports and also use the WAN port as a LAN port.

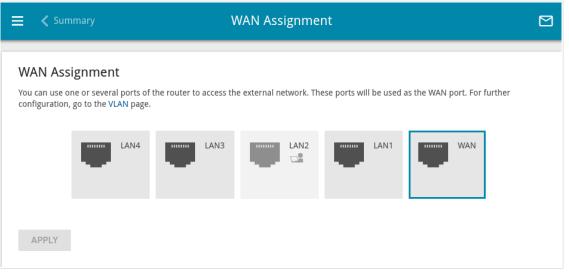


Figure 171. The Advanced / WAN Assignment page.

Using LAN Ports as WAN Ports

To configure one or several LAN ports of the router to be used as WAN ports, follow the next steps:

- 1. On the **Advanced / WAN Assignment** page, select LAN ports and click the **APPLY** button.
- 2. Go to the **Advanced / VLAN** page and create additional VLANs each of which will include one selected LAN port (see the *VLAN* section, page 219).

To create a network interface to which a WAN connection can be assigned upon adding the VLAN, the **Create interface** switch should be moved to the right.

3. Go to the **Connections Setup / WAN** page and create WAN connections which will be assigned to the network interfaces of the corresponding VLANs (see the *WAN* section, page 84).

If you don't want to use a LAN port as a WAN port any longer, follow the next steps:

- 1. On the **Connections Setup / WAN** page, remove the WAN connection assigned to the network interface of the VLAN which includes the corresponding LAN port (see the *WAN* section, page 84).
- 2. Go to the **Advanced / VLAN** page and remove the VLAN (see the *VLAN* section, page 219).
- 3. Go to the **Advanced / WAN Assignment** page, deselect the corresponding LAN port, and click the **APPLY** button.

Using WAN Port as LAN Port

To configure the WAN port of the router to be used as a LAN port, follow the next steps:

- 1. On the **Connections Setup / WAN** page, remove the WAN connection assigned to the network interface of the VLAN which includes the WAN port (see the *WAN* section, page 84).
- 2. Go to the **Advanced / VLAN** page and remove the VLAN (see the *VLAN* section, page 219).
- 3. On the **Advanced / WAN Assignment** page, deselect the WAN port and click the **APPLY** button.

If you don't want to use the WAN port as a LAN port any longer, follow the next steps:

- 1. On the **Advanced / WAN Assignment** page, select the WAN port and click the **APPLY** button.
- 2. Go to the **Advanced / VLAN** page and create a VLAN which will include the WAN port (see the *VLAN* section, page 219).

To create a network interface to which a WAN connection can be assigned upon adding the VLAN, the **Create interface** switch should be moved to the right.

3. Go to the **Connections Setup / WAN** page and create a WAN connection which will be assigned to the network interface of the VLAN (see the *WAN* section, page 84).

SNMP

On the **Advanced / SNMP** page, you can enable and configure the SNMP agent of the router.

The SNMP agent is a service which sends data on the state and settings of the device where is it enabled to the SNMP manager (the network management system of your ISP or system administrator).

≡	K Home S	NMP 🖸
SN	IMP	
	can enable and configure the SNMP agent of the router. The S ice where is it enabled to the SNMP manager (the network mar	NMP agent is a service which sends data on the state and settings of the agement system of your ISP or system administrator).
Co	nfiguration	Remote subnets
\bigcirc	Enable SNMP	ADD
Hos	iname	
Ro	uter	
The	contact information for the administrator	
	nin <root@localhost></root@localhost>	
	_	
	em location	
Tes	t room	-
Us	ers +	
The	re are no users	
Co	mmunities +	
The	re are no communities	
	APPLY	

Figure 172. The Advanced / SNMP page.

In order to enable the SNMP agent, in the **Configuration** section, move the **Enable SNMP** switch to the right. Then specify the needed parameters.

Parameter	arameter Description		
Configuration			
Hostname	A name of the router for identification in the SNMP manager.		
The contact information for the administrator	Additional information used to contact the administrator of the router.		
System location	Additional information used to locate the router.		

If needed, specify an IP address of the remote subnet for which access to the SNMP agent of the router will be allowed. To do this, in the **Remote subnets** section, click the **ADD** button and enter the address of the subnet in the line displayed.

To remove an IP address of the subnet, click the **Delete** icon (\times) in the relevant line.

If the SNMP manager operates over SNMPv3, create a read-only user which will be used by the SNMP manager to get data on the device. To do this, in the **Users** section, click the **ADD** button (+).

Add User	×
Name	
Authentication protocol	
MD5	•
Authentication password*	Ø
Encryption protocol	
AES	•
Encryption key*	Ø
MIB subtree	
SAVE	

Figure 173. The window for adding a user.

In the opened window, specify the needed parameters:

Parameter	Description
Name	Specify a username for access from the SNMP manager.

Parameter	Description	
Authentication protocol	Select a required authentication method from the drop-down list of leave the None value if authentication is not required.	
Authentication password	Specify a password for user authentication from the SNMP manager. The field is displayed if the MD5 or SHA value is selected from the Authentication protocol drop-down list.	
Encryption protocol	Select a required encryption method from the drop-down list leave the None value if encryption is not required. The list displayed if the MD5 or SHA value is selected from Authentication protocol drop-down list.	
Encryption key	Specify an encryption key for data exchange between the SNMP agent and SNMP manager. The field is displayed if the DES or AES value is selected from the Encryption protocol drop-down list.	
MIB subtree	Specify a MIB element which will be available to the SNMP manager.	

Click the **SAVE** button.

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

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

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

If the SNMP manager operates over SNMPv2c, create a read-only community which will be used by the SNMP manager to get data on the device. To do this, in the **Communities** section, click the

ADD button (+) and specify the community name in the **Name** field in the opened window.

To remove a community, select the checkbox located to the left of the relevant line in the table and

click the **DELETE** button ($\overline{\mathbf{10}}$).

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

In order to disable the SNMP agent, in the **Configuration** section, move the **Enable SNMP** switch to the left and click the **APPLY** button.

DNS

C VLAN	DNS	
DNS		
	nine the IP address from the name of a server in Intranets or the Internet. You a ually or configure the router to obtain DNS servers addresses automatically from	
IPv4	IPv6	
Manual	Manual	
Default gateway	Default gateway	
Interface	Interface	
statip_81	<u> </u>	
Name Servers		
Designed to be used by the loca	al network clients.	
IPv4		
1.1.1.1	0	
1.0.0.1		
ADD SERVER		
Reserve Servers		
Designed to be used by the rou	ter when the addresses specified manually or obtained automatically are unav	ailable.
IPv4	IPv6	
IPv4 add server	IPv6 Add server	

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

Figure 174. 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** button ($\boxed{10}$) 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 pag	e, you can define parameters o	f the DDNS service, which allows asso	clating a domain name with dynamic IP addresses.
DDNS List	+ s created		

Figure 175. The Advanced / DDNS page.

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

≡ < ddns	DDNS/Adding	
Calle Enable	Username*	
Hostname		
For example: host.ru	Password*	Ø
ADD HOST	Interface* Default gateway	•
DDNS service* changeip.com	Update period (in minutes)*	
SAVE		

Figure 176. 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 serviceSelect the DDNS provider from the drop-down list. If is not in the list, select the Custom provider value fields displayed on the page. Specify the DDNS prov the Name field, the domain name of the provider's Server field, and the location of settings in the Path for		
Username	The username to authorize for your DDNS provider.	
Password	The password to authorize for your DDNS provider. Click the Show icon (N) 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.

😑 < DDN	IS	Ports Setting	S			
Ports Settings You can configure or disable autonegotiation of speed and duplex mode or manually configure speed and duplex mode for each Ethernet port of the device. Also you can enable or disable data flow control in the autonegotiation mode.						
Port	Status	Autonegotiation	Speed	Flow control		
LAN4	Disconnected	On	-	-		
LAN3	Disconnected	On	-	-		
LAN2	Disconnected	On	-			
LAN1	Connected	On	1000M-Full	Off		
WAN	Connected	On	1000M-Full	Off		

Figure 177. 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 178. 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 the	ransfer modes, move relevant switches to the right.	
Flow control		
Symmetric flow control	Move the switch to the right to enable the flow control function for the port.	
	Move the switch to the left to disable the flow control function for the port.	

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

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

Redirect

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

≡	Summary	Redirect	
Re	edirect		
Υοι		ection failure. Notifications will be displayed in the browser window when a	à
DIS	SABLE		
Re	easons for Redirect		
	Physical connection error		
	 No connection The device is not configured 		
	The device is not configured		
	APPLY		

Figure 179. 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 errorNotifications in case of physical connection problems (the cable is not connected, an additional device needed to acc Internet is not connected).		
No connection	Notifications in case of problems of the default WAN connection (authorization error, the ISP'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 + No route created		

Figure 180. The Advanced / Routing page.

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

Enable Name* Route_3 Protocol IPv4 Interface Auto Destination network* Destination netmask* Gateway* Metric Table group_1	Add Route	×
Route_3 Protocol IPv4 Interface Auto Destination network* Destination netmask* Gateway* Metric Table	Carable	
Protocol IPv4 Interface Auto Destination network* Gateway* Metric Table	Name*	
IPv4 Interface Auto Destination network* Gateway* Metric Table	Route_3	
IPv4 Interface Auto Destination network* Gateway* Metric Table	Protocol	
Auto Destination network* Destination netmask* Gateway* Metric Table		•
Auto Destination network* Destination netmask* Gateway* Metric Table		
Destination network* Destination netmask* Gateway* Metric Table		
Destination netmask* Gateway* Metric Table	Auto	•
Destination netmask* Gateway* Metric Table		
Gateway* Metric Table	Destination network*	
Gateway* Metric Table		
Gateway* Metric Table	Destination netmask*	
Metric		
Metric		
Table	Gateway*	
Table		
	Metric	
group_1		
	group_1	•
	SAVE	
SAVE	Set St Inc.	

Figure 181. The window for adding a new route.

In the opened	window, v	ou can specify	the following	parameters:
p n				P

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

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.

Kouting	TR-069	9 Client	
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	
		Username	
URL address			
		Password	Ø
Username		Request port 8999	
Password	Ø		
APPLY		Request path	

Figure 182. 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 on the device and network statistics) to the ACS.
Interval	Specify the time period (in seconds) between sending reports.
	Auto Configuration Server Settings
Get URL address via DHCP	If the switch is moved to the right, the router obtains the URL address of the ACS upon establishing the Dynamic IP type connection.
	If you need to specify the URL address manually, move the switch to the left and enter the needed value in the URL address field.
URL address	The URL address of the ACS provided by the ISP.
Username	The username to connect to the ACS.
Password	The password to connect to the ACS. Click the Show icon (\bigotimes) to display the entered password.
	Connection Request Settings
Username	The username used by the ACS to transfer a connection request to the router.
Password	The password used by the ACS. Click the Show icon (\bigotimes) to display the entered password.
Request port	The port used by the ACS. By default, the port 8999 is specified.
Request path	The path used by the ACS.

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

Port Mirroring

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

🔳 < St	ımmary	Port Mirrori	ng	
	able the function of mirrorin	g the router's ports. This function allov ues with the help of traffic analysis sof	vs to copy traffic from one or several source ports to th tware.	e
Destination p LAN4 Source J				
	LAN4 Mode None	LAN3 Mode None -	LAN2 Mode None -	
	LAN1 Mode None -	WAN Mode None -		
APPLY				

Figure 183. The Advanced / Port Mirroring page.

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

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

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

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

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

UPnP

On the **Advanced / UPnP** 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.

🗮 < Sumr	mary	UPn	P	
from an extern ^{Type} IPv4		-	g rules for applications in the	router's LAN requiring a connection
IPv4				
Protocol	IP address	Private port	Public port	Description
IPv6				
Protocol	IP address	Private port	Public port	Pinhole ID

Figure 184. The Advanced / UPnP 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. From the **Type** drop-down list, select the WAN connection type through which the function will operate.

- **IPv4**: When this value is selected, port forwarding rules will operate only through the IPv4 connection.
- **Dual**: When this value is selected, port forwarding rules will operate through IPv4 and IPv6 connections.

Move the **Allow creating rules for private subnets** switch to the right if it is necessary that the port forwarding function operates with the WAN interfaces which IPv4 addresses belong to the range for private networks.

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 / IPv6
Protocol	A protocol for network packet transmission.
IP address	The IP address of a client from the local area network.
Private port	A port of a client's IP address to which traffic is directed from a public port of the router.
Public port	A public port of the router from which traffic is directed to a client's IP address.
Description	<i>For IPv4 only.</i> Information transmitted by a client's network application.
Pinhole ID	<i>For IPv6 only.</i> An identifier of the rule created by the client for an incoming connection to the router.

If you want to disable the UPnP function, click the **DISABLE** button.

UDPXY

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

≡	Summary	UDPXY 🖸
U	DPXY	
	i can allow the router to use the built-in UDPXY application. Th ws devices which cannot receive UDP streams to access strea	e UDPXY application transforms UDP traffic into HTTP traffic. This application m video.
	Enable	
Por	(*	Buffer size for incoming data*
40	22	131071
Max	ximum client number*	Buffer size for data transferred to client*
3		32768
		WAN interface*
		Not selected -
	APPLY	

Figure 185. The Advanced / UDPXY page.

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

Upon that the following fields are displayed on the page:

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

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

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

Server Process ID	Accepting clie	ents on	Multicast address	Active client
1447	192.168.0.1:402	2	192.168.161.235	0
		Restart]	
Request	template	HIIP	requests: Function	
				-t - data
http://address:port/ud	p/mcast_addr:mport/	Relay m	ulticast traffic from mca	st_addr:mport
http://address:port/ud http://address:port/st			ulticast traffic from mca udpxy status	st_addr:mport

Figure 186. The UDPXY application status page.

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.

🚍 🗶 Summary	IGMP/MLD
IGMP	MLD
Internet Group Management Protocol is designed to manage multicast traffic in IP-based networks.	Multicast Listener Discovery is designed to manage multicast traffic in IPv6-based networks.
C Enable	Enable
IGMP version	MLD version
IGMPv2	✓ MLDv1v2
Interface*	Interface
statip_39	✓ Not selected ✓

Figure 187. 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 version	Select 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 enable the RTSP, SIP ALG mechanisms, 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.

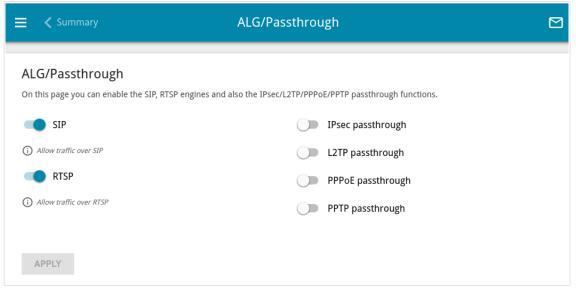


Figure 188. The Advanced / ALG/Passthrough page.

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. ¹⁶
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.
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.
PPPoE pass through	Move the switch to the right to enable the PPPoE 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.

¹⁶ 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).

CoovaChilli

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

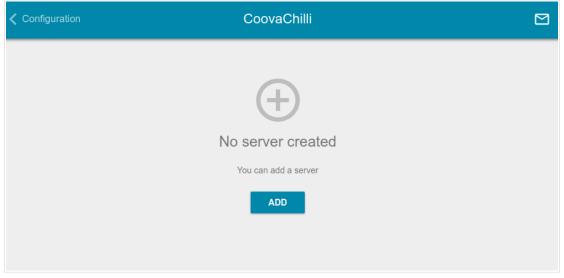


Figure 189. The Advanced / CoovaChilli page.

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

<u> </u>	There are no interfaces available for CoovaChilli
<u> </u>	want to use a separate LAN port or a Wi-Fi network as the interface ary to create another VLAN group for this port or network.
Lease time	(in seconds)
86400	
Logging lev	vel
Error m	essages
IP addre	SS*
Mask*	

Figure 190. The page for adding an authorization server. The Main Settings section.

Parameter	Descriptior	1
Interface	 From the drop-down list, select an in authorization server. A VLAN which includes a separate LA (see the <i>VLAN</i> section, page 219) is a server. 	AN port or a Wi-Fi network
Lease time	The interval (in seconds) between sending authorization requests to clients.	
Logging level	Select a type of messages and alerts/notifications to be logged.	
IP address	Specify an IP address of the router to be used for authorized client access.	
Mask	Specify a subnet mask.	
Ping	If the switch is moved to the right, the router responds to ping requests by the IP address specified on this page. For security reasons, it is recommended to disable this function.	
	RADIUS server Primary RADIUS server address* Secondary RADIUS server address RADIUS encryption key* RADIUS server port 1813 Authentication port 1812	

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

Figure 191. The page for adding an authorization server. The **RADIUS server** section.

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

NASID

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

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

Figure 192. The page for adding an authorization server. The MAC authentication section.

In the **MAC authentication**¹⁷ section, you can specify the following parameters:

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

¹⁷ Will be available in future software versions.

-	
Enable CHAP authentication	
() If the switch is moved to the left, PAP authentication is used	
Authorization port	
3990	
UAM encryption key*	Ø
UAM server*	
UAM server* ① The address of the UAM server should start with a protocol. http://dlink.ru	Example:

Figure 193. The page for adding an authorization server. The **UAM** section.

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

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

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

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

To edit the parameters of a server, left-click the relevant line in the table. On the opened page, change the needed parameters and click the **APPLY** button.

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

the **DELETE** button ($\overline{\blacksquare}$).

VRRP

On the **Advanced / VRRP** page, you can enable VRRP (*Virtual Router Redundancy Protocol*), which is designed to improve availability of routers acting as default gateways. The protocol enables you to configure several devices as the default virtual router with a common IP address, which is used as the default gateway by LAN clients.

🗧 🔇 Summary	VRRP			
VRRP Virtual Router Redundancy Protocol is Enable VRRP	Virtual Router Redundancy Protocol is a network protocol designed to improve availability of the routers which act as default gateways.			
Mode:	Backup	operation of the VRRP, it is necessary to		
Priority:	100 disable Re	irect		
Status:	Disable			
Interface*	Assign virtu	I MAC address		
LAN	~			
VRID*	Preempt m	de		
1	Authorization			
	Without authorizat	n 👻		
Priority* 100	Enable Obje	t Tracking		
IP address*				
Mask*				
Delay (in seconds)*				

Figure 194. The Advanced / VRRP page.

For correct operation of the router while using VRRP, it is required to disable notifications on the reason of the Internet connection failure on the **Advanced / Redirect** page (see the *Redirect* section, page 234).

If you want to enable VRRP, move the **Enable VRRP** switch to the right. When the protocol is enabled, the following elements are displayed on the page:

Parameter	Description	
Mode	 The operation mode of the router. Master: The router ensuring data transfer at present. A device with a higher priority switches to the Master mode. Backup: A reserve router, which switches to the Master mode upon the main router failure in accordance with its priority level. 	
Priority	The current priority level of the device. It can differ from the priority specified by the user if the Enable Object Tracking switch is moved to the right.	
Status	 The status of the service working over VRRP. Disable: The service is not active. Enabled: The service is active. 	
Interface	A network interface used by VRRP.	
VRID	Specify a unique ID of the virtual router. By default, the value 1 is specified.	
Priority	The priority of the router over other devices, which is used to switch it to the Master mode. Specify a value from the range 1~255 . By default, the value 100 is specified. If several devices have the same priority level, the router with the highest IP address will switch to the Master mode.	
IP address	The IP address used by LAN devices to access the router.	
Mask	The subnet mask of the virtual router.	
Delay	An interval (in seconds) between sending service advertisements, containing information on the priority level and connection status of the device working in the Master mode. By default, the value 1 is specified.	
Assign virtual MAC address	Move the switch to the right to enable access to the virtual router by a virtual MAC address. A virtual MAC address is generated automatically.	

Parameter	Description	
Preempt mode	The preempt mode enables a backup router to switch to the Master mode if its priority level is higher than the priority of the current Master . Move the switch to the left to disable the preempt mode. If a device is the owner of the IP address specified on this page, it uses the preempt mode regardless of the position of this switch.	
Authorization	 Select the authorization method for devices working over VRRP. Without authorization: Authorization is not required. PW: Authorization by password (a HEX key). The maximum key length is 8 symbols. The key should begin with the Ox prefix. 	
Enable Object Tracking	Move the switch to the right to track the status of the router connection. When the connection breaks down, the priority of the router is lowered. Select the relevant connection from the Connection for Object Tracking drop-down list displayed. Move the switch to the left to disable connection status tracking.	

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

If you want to disable VRRP, move the **Enable VRRP** switch to the left and click the **APPLY** button.

Wake-on-LAN

On the **Advanced / Wake-on-LAN** page, you can enable the Wake-on-LAN function. This function allows you to remotely power on or wake up devices connected to the router's LAN via a specific packet.

Make sure that the NIC of your device supports the Wake-on-LAN function.

Wake-on-LAN			
Wake-on-LAN is a feature tha	allows you to remotely turn on or wake	up a PC connected to the device's L	AN.
Enable			
Interface			
<all></all>	•		
Public port*			
9			

Figure 195. The Advanced / Wake-on-LAN page.

To enable the function, move the **Enable** switch to the right. Then from the **Interface** drop-down list, select an interface (WAN connection) through which the router will receive the packet to wake up the device or leave the **All** value to receive the packet through all existing WAN connections. If needed, change the port used by the router to receive the packet to wake up the device in the **Public port** field (by default, the standard port **9** is specified). Click the **APPLY** button.

To disable the function, move the **Enable** switch to the left and click the **APPLY** 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/Pas	through IP Filter 🗠
	(+)
	Filters
	No rules created for IP filter
	ADD

Figure 196. The Firewall / IP Filter page.

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

E < IP Filter IP F	Filter/Adding 🗠 🗠
General Settings	Source IP address (i) 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 2001:0db8:85a3:08d3:1319:8c2:e0370:7532/64 for IPv6)
Name* Priority* 0	Set as Set as Start IPv4 address T
Action Allow Protocol TCP	 End IPv4 address ✓
IP version IPv4 Direction Source Destination	•
LAN VAN Source interface Auto Auto	•
Destination IP address (i) 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)	Ports You can specify one port, several ports separated by a comma (for example, 80,90), or a range of ports separated by a colon (for example, 80:90)
Set as Range or single IP address	Destination port Set source port manually
Start IPv4 address End IPv4 address APPLY	▼ ▼

Figure 197. The page for adding a rule for IP filtering.

You can specify the following parameters:

Parameter	Description	
General Settings		
Enable rule	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.	
Name	A name for the rule for easier identification. You can specify any name.	

Parameter	Description	
Priority	The priority level of the rule. In the field, enter the needed value. The lower the value, the higher is the priority of the rule. You can specify a value from 0 to 5000.	
Action	 Select an action for the rule. Allow: Allows packet transmission in accordance with the criteria specified by the rule. Deny: Denies packet transmission in accordance with the criteria specified by the rule. 	
Protocol	A protocol for network packet transmission. Select a value from the drop-down list.	
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.	
Direction	 The direction of network packet transmission to which the rule will be applied. Select the source of the packet direction from the Source drop-down list. WAN: The rule will be applied to the packets transmitted from the external network. LAN: The rule will be applied to the packets transmitted from the local network. GRE: The rule will be applied to the packets transmitted from the GRE tunnel (available if a GRE tunnel has been created on the device). IPIP: The rule will be applied to the packets transmitted from the IPIP tunnel (available if an IPIP tunnel has been created on the device). IPSEC: The rule will be applied to the packets transmitted from the IPSec tunnel (available if an IPSec tunnel has been created on the device). PPTP Server: The rule will be applied to the packets transmitted from the IPSec tunnel (available if an IPSec tunnel has been created on the device). L2TP Server: The rule will be applied to the packets transmitted from the IPTP server (available if an L2TP server has been created on the device). 	

Parameter	Description
	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-1260.
	• WAN : The rule will be applied to the packets transmitted to the external network.
	• LAN: The rule will be applied to the packets transmitted to the local network.
	• GRE : The rule will be applied to the packets transmitted to the GRE tunnel (<i>available if a GRE tunnel has been created on the device</i>).
	• IPIP : The rule will be applied to the packets transmitted to the IPIP tunnel (<i>available if an IPIP tunnel has been created on the device</i>).
	• IPsec : The rule will be applied to the packets transmitted to the IPsec tunnel (<i>available if an IPsec tunnel has been created on the device</i>).
	• PPTP Server : The rule will be applied to the packets transmitted to the PPTP server (<i>available if a PPTP server</i> has been created on the device).
	• L2TP Server : The rule will be applied to the packets transmitted to the L2TP server (<i>available if an L2TP server</i> has been created on the device).
	From the Source interface and Destination interface drop- down lists, select source and destination interfaces for which the rule will be applied. Leave the Auto values to apply the rule to all created WAN interfaces.
	Source IP address
Set as	Select the needed value from the drop-down list.
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.

Parameter	Description	
Subnet IPv4 address / Subnet IPv6 address	The source subnet IPv4 or IPv6 address. The field is displayed when the Subnet value is selected from the Set as drop-down list.	
Destination IP address		
Set as	Select the needed value from the drop-down list.	
Start IPv4 address / Start IPv6 address	The destination host start IPv4 or IPv6 address. If it is necessary to specify a single address, leave the End IPv4 address / End IPv6 address field blank. You can choose a device connected to the 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 (()) 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 289) or select the **Select an existing one** value to use the existing one. Existing schedules are displayed in the **Rule name** drop-down list.

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

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

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

To create a copy of an IP filter rule, select the checkbox located to the left of the relevant line in the table and click the **Clone** (\Box) icon. On the opened page, change the needed parameters and click the **APPLY** button.

To change or delete the schedule for a rule, click the **Edit schedule** icon (\bigcirc) in the line corresponding to this rule. 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 ($\overline{\square}$).

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	
	(\pm)	
	Virtual Servers	
	No virtual server exists	
	ADD	

Figure 198. The Firewall / Virtual Servers page.

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

E 🗸 Virtual Servers	Virtual Servers/Adding C
General Settings	Private Network Settings
Name*	
Template Custom	Private port* Order port, several ports separated by a comma (for example, 80,90), or a range of ports separated by a colon (for example, 80:90)
<all></all>	~
Protocol	•
Public Network Settings Remote IP address	
Vou can specify a single iP address, or a subnet iP oddress (for e 10.10.10.10/24)	xample,
Remote IP address	×
ADD REMOTE IP	
Public port*	
Wou can specify one port, several ports separated by a comma (80,90), or a range of ports separated by a colon (for example, 80:90)	

Figure 199. 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
	The IP address of the host/subnet of the client that will connect to the virtual server.
Remote IP address	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 289) 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 create a copy of a virtual server, select the checkbox located to the left of the relevant line in the table and click the **Clone** (\Box) icon. 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 ($\boxed{10}$).

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.

≡	K Home DMZ	
DN	ΛZ	
A D	MZ is a host or network segment located "between" internal (local) and external (global) networks. In the router, the DMZ implements the ability to transfer a request coming to a port of the router from the external network to a specified host of the internal network.	
	Enable 🕓	
\bigcirc	Enable NAT Loopback	
IP a	address* •	
	APPLY	

Figure 200. 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 289) 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	•	
List of Exceptions No rules created for MAC	filter	

Figure 201. The Firewall / MAC Filter page.

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

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

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

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

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

Figure 202. 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.
Action	 Select an action for the rule. Deny: Blocks access to the Internet for the device with the specified MAC address even if the default mode allows access for all devices. Allow: Allows access to the router's network and to the Internet for the device with the specified MAC address even if the default mode denies access for all devices.
MAC address	The MAC address of a device from the router's LAN. You can enter the MAC address of a device connected to the router's LAN at the moment. To do this, select the relevant device from the drop-down list (the field will be filled in automatically).
Name	The name of the device for easier identification. You can specify any name.

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 289) 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 (10). 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.

😑 < Summary	URL Filter	
	+	
	URL Filter	
	No rules created for URL Filter	
	ADD	

Figure 203. The Firewall / URL Filter page.

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

URL Filter URL	Filter/Adding
URL Filter	can be applied to those devices that are added to the list or to all but
devices from the list.	
Enable	
Address filtering	Client filtering
Block all URLs except listed	✓ All but devices from list
Addresses +	Clients +
URL address Match with template	MAC address
APPLY	

Figure 204. The page for adding a rule for URL filter.

On the opened page, move the **Enable** switch to the right to enable the rule, 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.
	 specified in the field above. Partly: The request address should contain the value specified in the field above in any part of it.

Click the **SAVE** button.

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

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

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

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

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

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

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

To set a schedule for the URL filter 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 289) 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 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 URL filter rule at the time specified in the schedule and enable it at the other time, select the **Disable rule** value from the **Action** drop-down list and click the **SAVE** button.

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

To change or delete the schedule for a rule, click the **Edit schedule** icon (\bigcirc) in the line corresponding to this rule. 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 ($\boxed{\blacksquare}$).

AdBlock

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

< URL Filter	AdB	lock	
AdBlock A service for blocking ads and malicious websites.			
Common Settings		URL	
Enable		G Here you can add, edit, and remove addresses of files which contain host lists.	
Path*	۹	ADD	
Save to the device's memory			
APPLY			

Figure 205. The Firewall / AdBlock page.

To enable the advertisements blocking function, in the **Common Settings** section, move the **Enable** switch to the right.

In the **Path** field, locate a folder to which a file for blocking advertisements will be saved. To do this, click the **Search** icon (\mathbf{Q}), go to the needed folder, and click the **SELECT** button.

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 memory of the USB storage. Also you can save the file with the list of advertising web sites to the device's memory. To do this, move the **Save to the device's memory** switch to the right, and then click the **APPLY** button.

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

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

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

Remote Access

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

≡	< AdBlock	Remote Access	
Re	emote Access		
	I can configure access to the web-based interface of the ed to allow access to the router from the external netwo	e router. By default, the access from external networks to the router is closed. If your ork, create relevant rules.	u
Ru	ıles +		
No	rules created for remote access		

Figure 206. The Firewall / Remote Access page.

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

Add Rule	×
C Enable	
Name*	
Interface Automatic	
Automato	•
IP version	
IPv4	•
Open access from any extern host	nal
Open access from any extern host	nal
host IP address*	nal
host IP address* Mask*	nal
host	nal
host IP address* Mask* Public port* 80	nal
host IP address* Mask* Public port*	nal •
host IP address* Mask* Public port* 80 Protocol	nal T

Figure 207. The window for adding a rule for remote management.

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

Parameter	Description
Enable	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.
Name	A name for the rule for easier identification. You can specify any name.
Interface	From the drop-down list, select an interface (WAN connection) through which remote access to the router will operate. Leave the Automatic value to allow remote access to operate through all created WAN connections.
IP version	An IP version to which the rule will be applied. Select the relevant value from the drop-down list.
Open access from any external host	Move the switch to the right to allow access to the router for any host. Upon that the IP address and Mask fields are not displayed.
IP address	A host or a subnet to which the rule is applied. You can specify an IPv4 or IPv6 address.
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 (() 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 289) 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
- disable automatic save of the settings or save the changed settings manually to the non-volatile memory
- reboot the router
- change the web-based interface language
- edit or add commands for the hardware buttons
- update the firmware of the router
- configure automatic notification on new firmware version
- configure rules to enable/disable Wi-Fi connection and the Wi-Fi filter, automatic reboot of the device and saving a configuration backup to the connected USB storage on a schedule, and set a schedule for different rules and settings of the firewall
- enable event logging and set its basic options
- create rules for sending the event log to a remote server
- create rules for recording the event log to a USB storage connected to the router
- check availability of a host on the Internet through the web-based interface of the router
- trace the route to a host
- enable or disable access to the device settings via TELNET and/or 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 or configure automatic saving of the configuration backup to the connected USB storage on a schedule, restore the router's configuration from a previously created file, disable automatic save of the settings or save the changed settings manually to the non-volatile memory, reboot the device, or change the web-based interface language.

🗮 < Summary	Configuration	
User	Action	
admin		Factory Reset factory default settings
New password		Backup Save current configuration to a file
Password should be between 1 and 31 ASCII characters		Restore Load previously saved configuration to the device
Password confirmation		Save Save current settings
SAVE	()	Reboot Reboot device
Miscellaneous		
Language English	•	
Autosave		
() Automatic save of the current settings after their change.		
Idle time (in minutes)* 10		
When the function "Stay signed in" is enabled, then users are n redirected to the login page despite the specified idle time.	ot	
SAVE		

Figure 208. 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.¹⁸ Click the **Show** icon (\bigotimes) to display the entered values. Then click the **SAVE** button.

^{18 0-9,} A-Z, a-z, space, !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~.

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

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

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

By default the router saves changed settings automatically (the **Autosave** switch in the **Miscellaneous** section is moved to the right). Move the **Autosave** switch to the left if you don't want the changed settings to be saved automatically. In this case, a notification will be displayed in the top right part of the page when the settings are changed.

To change a period of inactivity after which the router completes the session of the interface, in the **Miscellaneous** section, in the **Idle time** field, specify the needed value (in minutes). By default, the value **5** is specified. Then click the **SAVE** button.

Control	Description
Factory	Click the button to restore the factory default settings. Also you can restore the factory defaults via the hardware RESET button (see the <i>Back Panel</i> section, page 18).
Backup	Click the button to save the configuration (all settings of the router) to your PC or a USB storage connected to the router. See the <i>Creating Configuration Backup</i> section, page 282 for details on backup creation.
Restore	Click the button to select and upload a previously saved configuration file (all settings of the router) located on your PC or a USB storage connected to the router. To upload a configuration file from your PC, select the Local storage value from the File location drop-down list. Click the CHOOSE FILE button and follow the dialog box appeared.
	To upload a configuration file from a USB storage connected to the router, select the USB Storage value from the File location drop-down list. Then locate the needed configuration file. To do this, click the Search icon (Q) in the Path field. Then choose the needed file and click the SELECT button. To upload the configuration file, click the APPLY button.

The following buttons are available in the **Action** section:

Control	Description
Save	Click the button to save settings to the non-volatile memory. If the automatic save of the router's settings is disabled, save settings manually after you change the router's parameters. Otherwise the changes will be lost upon reboot of the router.
Reboot	Click the button to reboot the device. All unsaved changes will be lost after the device's reboot.

Creating Configuration Backup

To create a configuration backup, click the **Backup** button in the **Action** section.

Backup	×
File location USB Storage	•
O Backup manually	
 Schedule backup Path to save on schedule* Path is not selected 	م
File name*	.tar.gz
Attention! Unmount storage in 'USB storage/Information' menu before removing	USB storage
SET SCHEDULE	

Figure 209. The window for creating a configuration backup.

To save the configuration backup to your PC, select the **Local storage** value from the **File location** drop-down list and click the **SAVE** button. The configuration backup will be stored in the download location of your web browser.

To save the configuration backup to a USB storage connected to the router, select the **USB Storage** value from the **File location** drop-down list. Then select the **Backup manually** choice of the radio button and click the **SAVE** button. In the opened window, in the **File name** field, specify a name for the configuration file. Then go to the needed folder and click the **SELECT** button to save the file.

To configure automatic creation of a configuration backup on a schedule, select the **Schedule backup** choice of the radio button and locate a folder to save the files (available if the **USB Storage** value was selected in the **File location** drop-down list). To do this, click the **Search**

icon (\mathbf{Q}) in the **Path to save on schedule** field. Then go to the needed folder and click the **SELECT** button.

In the **File name** field, specify a name for the configuration file. Then click the **SET SCHEDULE** button.

In the opened window, specify a schedule name and the interval and time for its execution (see the *Schedule* section, page 289 for detailed description of the fields).

Click the **SAVE** button.

To change or delete the schedule, click the **Edit schedule** icon ((). In the opened window, click the **CHANGE SCHEDULE** button, change the parameters and click the **SAVE** button or click the **DELETE FROM SCHEDULE** button¹⁹.

¹⁹ Correct operation of the button will be implemented in the next firmware version.

Buttons Configuration

On the **System / Buttons Configuration** page, you can edit or add commands for the **RESET** and **WPS** hardware buttons.

🗧 🗸 Summary	Buttons Configurati	on	t
Buttons Configuration			
On this page you can configure actions of the o	levice hardware buttons.		
Reset +			
Command	Action	Button press duration	
Reset config and reboot	Long press	7 - 60	
WPS +			
Command	Action	Button press duration	
Enable WPS	Long press	0 - 7	
Enable/Disable Wi-Fi	Long press	7 - 60	
APPLY			

Figure 210. The System / Buttons Configuration page.

The page displays commands assigned to the buttons by default (for the description of the buttons actions with the commands assigned by default, see the *Product Appearance* section, page 16). You can edit or delete them.

To add a command for a button, click the **ADD** button (+) in the relevant section.

Add command	×
Command Reset config and reboot	·
Action Double click	•
SAVE	

Figure 211. The window for adding a command.

In the opened window, specify the following parameters:

Control	Description	
Reset / WPS		
Command	From the drop-down list, select a command.	
Action	 From the drop-down list, select an action for the command. Single click: One short press of the button lasting less than one second. The action is not available if the Long press action with the duration from 0 seconds has already been specified for the hardware button. Double click: Two short presses of the button. Long press: A prolonged press of the button. When this value is selected, the Button press duration section is displayed. 	
Button press duration	Specify a period of time (in seconds) within which you should hold the button. You can specify values from 0 to 60.	

Click the **SAVE** button.

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

To remove a command, select the checkbox located to the left of the relevant line in the table and

click the **DELETE** button ($\overline{\square}$).

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

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.

≡ < Summary Firmw	are Update (
Local Update () Current firmware version: 4.0.6 () Restore factory defaults after firmware update CHOOSE FILE File is not selected UPDATE FIRMWARE	Remote Update Remote server URL fwupdate.dlink.ru ADD Check for updates automatically Interval (in seconds)* 43200 At this time, the device works with the latest version of the software CHECK FOR UPDATES APPLY SETTINGS	Ĵ

Figure 212. 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

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** button (\blacksquare) in the line of the address.

Click the **APPLY SETTINGS** button.

check.

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

Local Update

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

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

- 1. Download a new version of the firmware from <u>www.dlink.ru</u>.
- 2. Click the CHOOSE FILE button in the Local Update section on the System / Firmware Update page to locate the new firmware file.
- 3. If you want to restore the factory default settings immediately after updating the firmware, move the **Restore factory defaults after firmware update** switch to the right.
- 4. Click the **UPDATE FIRMWARE** button.
- 5. Wait until the router is rebooted (about one and a half or two minutes).
- 6. Log into the web-based interface using the login (admin) and the current password.

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

Remote Update



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

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

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

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

Schedule

On the **System / Schedule** page, you can enable/disable Wi-Fi connection and the Wi-Fi filter, configure automatic reboot of the device on a schedule, and set a schedule for different rules and settings of the firewall.

Before creating a schedule you need to configure automatic synchronization of the system time with a time server on the Internet (see the *System Time* section, page 305).

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

Figure 213. 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.

	device is syn		ed only if the system time of the nized with an NTP server.
Syster	n Time:		19 March 2024, 13:
Mode			
Simp	lified mode		
Interva	dule name* I of execution y day		
	Hours (0-23)		Minutes (0-59)
Time	0	:	0

Figure 214. 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.

Schedul	e	×		
		d only if the system time of the zed with an NTP server.		
System Time: 19 March 2024, 13:33				
D Pe	rform task on	schedule		
Mode				
Simplified	d mode	•		
Interval of ex Every day Hou	y	• Minutes (0-59)		
Time 0	:	0		
<u> </u>	ntering several par , "2, 5, 12" or "2-12	rameters, use the symbol "," or "-" 2")		
Hours*	Minutes*	Seconds*		
0	0	30		
SAVE				

Figure 215. The window for adding a schedule for a task.

In the opened window, in the **System Time** field, the system time of the device is displayed. You can select the simplified mode of the schedule. To do this, select the **Simplified mode** value from the **Mode** drop-down list and specify the following parameters:

Parameter	Description
Perform task on schedule	Move the switch to the right to enable the task. Move the switch to the left to disable the task.

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.

Logging

In this menu you can enable event logging and create rules for sending the log to a remote server and/or a USB storage connected to the router.

Local

On the **System / Logging / Local** page, you can enable event logging and set its basic options.

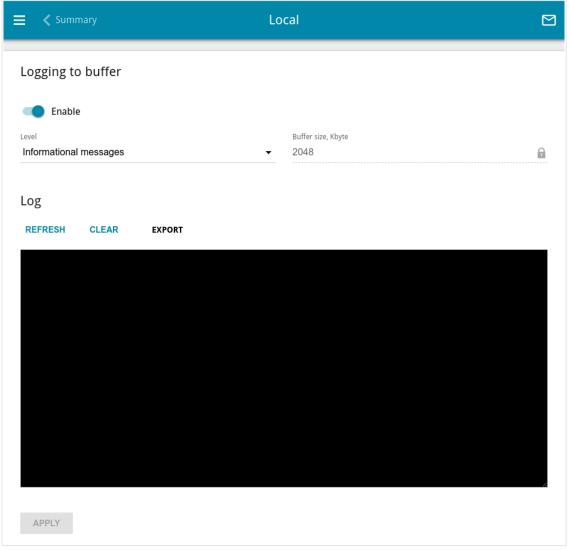


Figure 216. The System / Logging / Local page.

To enable logging of events to the router's RAM, in the **Logging to buffer** section, move the **Enable** switch to the right. Then specify the needed parameters.

Parameter	ter Description		
Logging to buffer			
Level	From the drop-down list, select the severity level of messages which will be logged. Upon that messages which severity level is equal to the selected level or higher than the selected one will be logged.		
Buffer size	The amount of RAM (in kilobytes) allocated for the system event log. You cannot change this value.		

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

To disable logging of events to the router's RAM, move the **Enable** switch to the left and click the **APPLY** button.

You can view the event log in the **Log** section.

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

To remove all log entries from the router's RAM, click the **CLEAR** button.

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

Remote

On the **System / Logging / Remote** page, you can create rules for sending the event log to a remote server.

🗮 🔇 Summary	Remote	
	(+)	
	No remote server added	
	You can add a remote server	
	ADD	

Figure 217. The System / Logging / Remote page.

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

😑 🕻 Remote	Editing	
Enable Level Informational messages	Server* Port* 514	

Figure 218. The page for adding a rule.

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

Parameter	Description	
Enable	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.	
Level	From the drop-down list, select the severity level of messages which will be logged in the event log. Upon that messages which severi level is equal to the selected level or higher than the selected of will be logged.	
Server	The IP address or full domain name of the host from the local or global network, to which the event log will be sent.	

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

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

Record to File

On the **System / Logging / Record to file** page, you can create rules for recording the event log to a USB storage connected to the router.

😑 < Summary	Record to file	2
	(+)	
	No log file added	
	You can add a log file	
	ADD	

Figure 219. The System / Logging / Record to file page.

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

	Ed	iting	
Main Settings			
Level		Path*	٩
Informational messages	•	File name*	
		The maximum size of one file (in kilobytes)* O	
		 0 - no file size limit Number of saved archive files 	
		1	Â
USB Storage	UNMOUNT		
Unmount the USB storage device before removing			
APPLY			

Figure 220. The page for adding a rule.

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

Parameter	Description	
Enable	Move the switch to the right to enable the rule. Move the switch to the left to disable the rule.	

Parameter	Description
Level	From the drop-down list, select the severity level of messages which will be logged in the event log. Upon that messages which severity level is equal to the selected level or higher than the selected one will be logged.
USB Storage	If a USB storage is connected to the router, its name is displayed in the field. To safely disconnect the USB storage, click the UNMOUNT button.
Path	Click the Search icon (\mathbf{Q}) located to the right of the field in order to locate the folder where system log files will be stored.
File name	A name for system log files.
The maximum size of one file	The maximum size (in kilobytes) of one system log file. When the value 0 is specified, the file size of the event log is not limited.
Number of saved archive files	The maximum number of archive files allowed to be recorded on the USB storage. When this number is exceeded, the archive file containing the oldest data will be deleted. The field is available for editing if the value specified in the The maximum size of one file field is greater than zero.

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

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

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

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.

😑 < Summary	Ping	
Ping		
	a host from the local or global network via the ping utility.	
Host*	Number of attempts* 3 IPv6 MORE SETTINGS	
	3 IPv6 MORE SETTINGS	
		4
	START CLEAR CANCEL	

Figure 221. The System / Ping page.

To check availability of a host, enter the IP address or name of this host in the **Host** field and specify a number of requests that will be sent in order to check its availability in the **Number of attempts** field. If availability check should be performed with IPv6, move the **IPv6** switch to the right.

To specify additional settings, click the **MORE SETTINGS** button.

	×
Packet size (in byte	25)*
 <i>Specifies the I</i> Waiting for respon 3 	number of data bytes to be sent. se (in seconds)*
0	fects only timeout in absence of any ise ping waits for two RTTs
ОК	DEFAULT SETTINGS

Figure 222. 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 trace the route of data transfer to a host via the traceroute utility.

😑 < Ping		Traceroute	
Traceroute You can trace the route of d	ata transfer to a host via the trace	eroute utility.	
Host*	IPv6 MORE SETT	INGS	
	START	CLEAR CANCEL	

Figure 223. The System / Traceroute page.

To trace the route, enter the name or IP address of a host in the **Host** field. If the route should be traced using IPv6, move the **IPv6** switch to the right.

To specify additional settings, click the **MORE SETTINGS** button.

		×
Max 30	imum TTL value*	
i	The maximum number of hops	
Num 2	iber of attempts*	
i	The number of probe packets to a hop	
Wait 3	t time (in seconds)*	
(j	Waiting for response (in seconds)	
	OK DEFAULT SETTINGS	

Figure 224. 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.

< Tr	aceroute Telr	net/SSI	ł	
	Celnet/SSH Du can enable or disable access to the device settings via TELNET and S	SH from y	bur LAN.	
	Enable Telnet		Enable SSH	
Р	ort	Port		
2	3	22	ĥ	
	APPLY			

Figure 225. 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.

😑 < Summary	Syster	n Time	
System time You can set up automatic synchronizatio	n of the system time with a ti		
 Enable NTP UTC offset settings Configure daylight saving tin Get NTP server addresses us 	ing DHCP	Time interval between NTP requests After synchronization with NTP server (in seconds) Auto For unsynchronized NTP client (in seconds) Auto	•
System time: Synchronization:	пеtworк 17.02.2023 12:30 Сотрleted	Time zone ^{Time zone*} Europe/Moscow	•
NTP Servers pool.ntp.org ADD SERVER	×	DETERMINE TIMEZONE	

Figure 226. The System / System Time page.

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

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

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

- 1. Move the **Enable NTP** switch to the right.
- 2. Specify the needed NTP server or leave the value specified by default in the **NTP Servers** section. If you need to specify several servers, click the **ADD SERVER** button.
- 3. Select your time zone from the **Time zone** drop-down list. To set the time zone in accordance with the settings of your operating system or portable device, click the **DETERMINE TIMEZONE** button.

4. Click the **APPLY** button. The **System date** and **System time** fields will be filled in automatically. In case of successful synchronization with the NTP server, the **Completed** value will be displayed in the **Synchronization** field.

If the router failed to get data from the server, the **Failed** value will be displayed in the **Synchronization** field. Upon that the creation date and time of the router's current firmware version is specified.

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 manually	Move the switch to the right to configure settings for daylight saving time for the router clock manually. In the Daylight Saving Time section displayed, specify the required offset time for daylight saving time (in minutes), and specify the needed values in the Beginning of daylight saving time and End of daylight saving time sections.
Get NTP server addresses using DHCP	Move the switch to the right if NTP servers addresses are provided by your ISP. Obtained addresses will be displayed in the NTP Servers section. Contact your ISP to clarify if this setting needs to be enabled. If the switch is moved to the right, settings of the NTP Servers section are unavailable.
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.
-	Γime 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.
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-1260 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	٥
Auto Provision		
Enable Auto Provision	Status:	No check has been run yet
Use BOOTP option	CHECK STATUS	
Autoconfiguration server address		
File name		
File check period (in seconds)		
1800		
Protocol type		
TFTP	•	

Figure 227. The page for configuring the Auto Provision function.

You can specify the following parameters:

Parameter	Description	
Enable Auto Provision	Move the switch to the right to enable the Auto Provision function. Move the switch to the left to disable the Auto Provision function.	
Use BOOTP option	If the switch is moved to the right, the parameters of your ISP's server (the address, the location of the configuration file, and the protocol) are automatically specified using DHCP options 66 and 67. Upon that a connection of the Dynamic IPv4 type should be configured on the Connections Setup / WAN page.	
	If the switch is moved to the left, the parameters of your ISP's server should be specified manually.	
Autoconfiguration server address	The IP address or full domain name of your ISP's server where the configuration file is stored.	

Parameter	Description	
File name	The location of the configuration file on the ISP's server.	
File check period	A time period (in seconds) between attempts to compare the current configuration file with the configuration file on the ISP's server.	
Protocol type	A protocol for communication with the ISP's server where the configuration file is stored.	

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

If you need to check manually if the current configuration file corresponds to the configuration file on the ISP's server, click the **CHECK STATUS** button. The check result will be displayed in the **Status** field. If the files are different, the device's settings will be updated.

SkyDNS

This menu is designed to configure the SkyDNS service.

SkyDNS is a web content filtering service which provides protection against malicious web sites for devices connected to the router's network, and also allows to configure filtering, block access to adult web sites, and use search engines safely. In order to use the service, first register an account on the SkyDNS service web site.

Settings

On the **SkyDNS / Settings** page, you can enable the SkyDNS service and specify settings for its operation.

Auto Provision	Settings		
▼ SkyDNS s	kyDNS rvice 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 parenta provision for home users accessing		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 ma resources, and botnets.	ware, phishing	Highly flexible filtering parameters; clear and simple interface.	
Basic Settings		Account	
DISABLE		^{Mail*} test@dlink.ru	
Provider			
SkyDNS	<u> </u>	Password*	
Provider is available			Ø
GO TO PERSONAL PROFILE PAGE		Tariff	
		Домашний	
Default profile* Основной	-	 Successfully authorized 	
Sync period (in seconds)* 3600			
APPLY MANUALLY SYNC			

Figure 228. 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	Devi	ces and Rules		
Known Clients				
IP address	MAC address	Name	Profile	
192.168.0.3	00:13:46:62:2f:4c	-	Not selected	
Rules 🕂 🗊				
 For all devices not 	included in the table the default pro	ofile set in the settings will be u	sed.	
MAC address	;	Profile	Hostname	

Figure 229. 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 230. 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 device, 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: F - 2015, *G* - 2016, *H* - 2017, *I* - 2018, *J* - 2019, *0* - 2020, *I* - 2021, *2* - 2022, *3* - 2023, *4* - 2024.

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-1260 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-1260 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
CoS	Class of Service
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
	Internet Control Message Protocol
ID	Identifier
IGD	Internet Gateway Device
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPTV	Internet Protocol Television
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light-emitting diode
LTE	Long Term Evolution
MAC	Media Access Control
MBSSID	Multiple Basic Service Set Identifier
MIB	Management Information Base
МІМО	Multiple Input Multiple Output
MPPE	Microsoft Point-to-Point Encryption
MPU	Maximum Packet Unit
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Controller

NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
ΡΑΡ	Password Authentication Protocol
РВС	Push Button Configuration
РСР	Port Control Protocol
PFS	Perfect Forward Secrecy
PIN	Personal Identification Number
РМР	Port Mapping Protocol
РоЕ	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
ТКІР	Temporal Key Integrity Protocol
TLS	Transport Layer Security
ToS	Type of Service
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