RG-5400

RG-5421G-Wac

User manual, firmware version 2.4.1

Subscriber router

IP address: http://192.168.1.1

login: admin

password: password

Document version	Issue data	Contents of changes
Version 1.3	17.01.2017	Synchronization with firmware version 2.4.1 Added: 3.7.6 'USB services' menu Corrected: 2.3 Device characteristics 2.5 Key specification 3.5 Wizard 3.7.2.1 'Internet' submenu 3.7.2.2 'IPv6' submenu 3.7.2.4 'Shaping traffic' submenu 3.7.2.7 'NAT and port forwarding' submenu 3.7.2.9 'Wi-Fi' submenu 3.7.2.11 'WPS' submenu 3.7.2.12 'Routing' submenu 3.7.2.15 'ALG' submenu 3.7.3.3 'Profile' submenu 3.7.3.4 'QoS' submenu 3.7.7.2 'Access' submenu
Version 1.2	20.09.2016	Synchronization with firmware version 2.4.0 Added: 3.5 Wizard 3.7.2.15 'ALG' submenu 3.7.6.1 'FTP' submenu 3.7.6.2 'SAMBA' submenu 3.7.6.3 'DLNA' submenu Corrected: 2.3 Device characteristics 2.5 Key specification 3.3 WEB interface operation mode 3.7.2.1 'Internet' submenu 3.7.2.2 'IPv6' submenu 3.7.2.3 'QoS' submenu 3.7.2.4 'Shaping traffic' submenu 3.7.2.7 'NAT and port forwarding' submenu 3.7.2.8 'Firewall' submenu 3.7.2.9 'Wi-Fi' submenu 3.7.2.11 'WPS' submenu 3.7.2.12 'Routing' submenu 3.7.3.1 'Network settings' submenu 3.7.3.3 'Profile' submenu 3.7.3.4 'QoS' submenu 3.7.7.2 'Access' submenu
Version 1.1	16.02.2016	Synchronization with firmware version 2.2.0 Corrected: 2.3 Device characteristics 3.6.2.1 'Internet' submenu 3.6.2.4 'Traffic shaping' submenu 3.6.2.5 'MAC address settings' submenu 3.6.2.11 'MAC filter' submenu 3.6.3.2 'Line setting' submenu 3.6.3.3 'Profile' submenu
Version 1.0	09.12.2015	First issue
Firmware version	Firmware version: 2.4.1 Web interface version: 2.4.25	

Symbols

Symbol	Description
Semibold font	Notes, warnings, chapter titles, headers and table titles are written in semibold font.
Calibri Italic	Important information is written by Calibri Italic.
	Analogue phone
	SIP-server
	RG-5400 device family
	Computer
	Digital set-top box STB
	Network connection
	Wireless network

Notes and warnings

✓ **Notes contain important information, tips or recommendations on device operation and setup**

! **Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.**

CONTENTS

1 Introduction ... 6
2 Device description ... 7
2.1 Purpose ... 7
2.2 Design ... 7
2.3 Device characteristics ... 8
2.4 Architecture and the device operation principle ... 10
2.5 Key specification ... 12
2.6 Design ... 14
2.6.1 The device front panel ... 14
2.6.2 Rear panel of the device ... 14
2.6.3 Side panel of the device ... 15
2.7 Light indication ... 16
2.8 Reset to the default settings ... 17
2.9 Delivery package ... 17
3 device control via web configurator ... 18
3.1 Getting started ... 18
3.2 User change ... 18
3.3 WEB interface operation modes ... 19
3.4 Applying configuration and discarding changes ... 20
3.5 Quick Setup Wizard ... 21
3.6 Quick configuration menu ... 23
3.6.1 Internet ... 25
3.6.2 VoIP ... 28
3.6.3 Wi-Fi ... 28
3.6.4 IPTV ... 29
3.6.5 System ... 29
3.7 Advanced settings ... 29
3.7.1 Web interface basic elements ... 29
3.7.2 ‘Network’ menu ... 31
3.7.2.1 ‘Internet’ submenu ... 31
3.7.2.2 ‘IPv6’ submenu ... 41
3.7.2.3 ‘QoS’ submenu ... 43
3.7.2.4 ‘Traffic shaping’ submenu ... 45
3.7.2.5 ‘MAC address setting’ submenu ... 47
3.7.2.6 ‘DHCP server’ submenu ... 48
3.7.2.7 ‘Local DNS’ submenu ... 49
3.7.2.8 Host configuration ... 49
3.7.2.9 ‘NAT and port forwarding' submenu ... 51
3.7.2.10 ‘Firewall’ submenu ... 53
3.7.2.11 ‘Wi-Fi’ submenu ... 55
3.7.2.12 ‘MAC filter’ submenu ... 59
3.7.2.13 ‘WPS’ submenu ... 60
3.7.2.14 ‘Static Routes’ submenu ... 61
3.7.2.15 ‘Dynamic DNS’ submenu ... 62
3.7.2.16 ‘SNMP settings’ submenu ... 63
3.7.2.17 ‘ALG’ submenu ... 64
3.7.2.18 ‘User VLAN’ submenu ... 66
3.7.3 ‘VoIP’ menu ... 67
3.7.3.1 ‘Network configuration’ submenu ... 67
3.7.3.2 ‘Line settings’ submenu ... 68
3.7.3.3 ‘Profile’ submenu ... 73
3.7.3.4 ‘QoS’ submenu ... 86

3.7.3.5 'VAS management prefixes' submenu 87
3.7.3.6 ‘Call signal’ submenu 88
3.7.3.7 ‘Call history’ submenu 89
3.7.4 ‘IPTV’ menu 91
3.7.4.1 ‘IPTV’ submenu 91
3.7.4.2 ‘STB’ submenu 92
3.7.5 ‘Local interfaces’ menu 94
3.7.5.1 ‘Functional assignment’ submenu 94
3.7.6 ‘USB services’ menu 94
3.7.6.1 ‘FTP’ submenu 94
3.7.6.2 ‘Samba’ submenu 96
3.7.6.3 ‘DLNA’ submenu 97
3.7.7 ‘System’ menu 99
3.7.7.1 ‘Time’ submenu 99
3.7.7.2 ‘Access’ submenu 99
3.7.7.3 ‘Log’ submenu 103
3.7.7.4 ‘Password’ submenu 106
3.7.7.5 ‘Configuration managment’ submenu 107
3.7.7.6 ‘Firmware upgrade’ submenu 107
3.7.7.7 ‘Reboot’ submenu 108
3.7.7.8 ‘Autoprovosioning’ submenu 109
3.7.7.9 ‘VLAN management’ submenu 111
3.7.7.10 ‘Additional settings’ submenu 113
3.8 System monitoring 114
3.8.1 ‘Internet’ submenu 114
3.8.2 ‘VoIP’ submenu 115
3.8.3 ‘Ethernet ports’ submenu 118
3.8.4 ‘Wi-Fi’ submenu 119
3.8.5 ‘DHCP’ submenu 121
3.8.6 ‘ARP’ submenu 121
3.8.7 ‘Device’ submenu 122
3.8.8 ‘Conntrack’ submenu 123
3.8.9 ‘Routing’ submenu 124
3.8.10 ‘Call history’ submenu 125
3.9 Configuration example 127
4 VALUE ADDED SERVICES USAGE 131
4.1 Call transfer 131
4.2 Call Waiting 134
4.3 Three-way conference call 135
4.3.1 Local conference 135
4.3.2 Remote conference 136
5 Connection establishment algorithm 138
5.1 Algorithm of a Successful Call via SIP 138
5.2 Call Algorithm Involving SIP Proxy Server 139
5.3 Call Algorithm Involving Forwarding Server 140
6 device automatic update algorithm based on DHCP 141
7 System recovery After firmware update failure 144
Appendix A. calculation of phone line length 145
Appendix B. Running User-defined script upon system startup 146

1 INTRODUCTION

RG-5421G-Wac subscriber router (hereinafter the device) is designed for home users and corresponds to unified access point to all interactive services trough wired and wireless commection channels. RG-5421G-Wac is a development of RG-4402G-W subscriber router and has 4 Gigabit Ethernet ports, FXS port, WPS button and button to enable/disable Wi-Fi. The device supports simultaneous operation in two Wi-Fi frequency ranges: IEEE 802.11b/g/n 2.4 GHz and 802.11a/n/ac 5 GHz.

RG-5421G-Wac has extended functionality for stable delivery of IPTV via wireless network. Smothness and steadiness of video playback are provided by special program functionality. The device allows you to operate at 2.4 and 5 GHz frequencies and provides simultaneous broadcasting the video streams and data transmission.

This operation manual describes intended use, main specification, rules of configuring, monitoring and firmware update for RG-5400 subscriber routers.

2 DEVICE DESCRIPTION

2.1 Purpose

RG-5400 is high-performance VoIP consumer router with the full set of options which allow consumers to use TriplePlay advantages.

RG-5421G-Wac is a versatile wireless solution for home use. The device allows you to create LAN and flexible to configure the home devices via Wi-Fi. WPS support allows you to simplify connection of large numbers of devices (notebook computer, NV-501-Wac, will box, network printer) to RG-5421G-Wac. USB connector is used to connect external drives or 3G/4G USB modem.

2.2 Design

The device is available in the following modification.

Table 1 – Models

Model name	WAN interface	Number of LAN interface's ports	Number of FXS	Presence of Wi-Fi
RG-5421G-Wac	RJ-45	4 Gigabit Ethernet	1	+

RG-5421G-Wac device has built-in Wi-Fi adapter with two indoor antennae. Built-in Wi-Fi adapter supports 802.11ac technology, it allows you to provide data transmission service of the wireless network with superior QoS in contrast with the device supported 802.11n. In addition, the device stays backward compatible with the 802.11n, 802.11g and 802.11b devices. Besides of that, the device supports operation in two frequency bands: 2.4 and 5 GHz.

2.3 Device characteristics

Interfaces:

FXS:	1 port RJ-11;
LAN:	4 Ethernet port RJ-45 10/100/1000BASE-T;
WAN:	1 Ethernet port (RJ-45 10/100/1000BASE-T) or SFP 1000 BASE-X;
WLAN:	IEEE 802.11 a/b/g/n/ac;
USB:	2 port USB2.0.

The device is powered via external 12V adaptor from 220 V power supply network.

Functions:

- *Network functions:*
  - ‘Bridge’ or ‘router’ operation mode;
  - PPPoE support (PAP, SPAP and CHAP authorization, PPPoE compression);
  - PPTP support;
  - L2TP support;
  - Static address and DHCP support (DHCP client on WAN, DHCP server on LAN);
  - DNS support;
  - NAT support;
  - Firewall;
  - NTP support;
  - QoS support (QoS via DSCP and 802.1P);
  - IPv6.
- Supporting IPTV functions;
- Access to media files via DLNA protocol;
- Possability of creating several SSID in a single range;
- VoIP protocols: SIP;
- Echo cancellation (G.168 guidelines);
- Silence detector (VAD);
- Comfortable noise generator;
- DTMF signals detection and generation;
- DTMF transmission (INBAND, rfc2833, SIP INFO);
- Fax transmission:
  - G.711A/G.711U;
  - T.38;
- Work with SIP server and without it;
- *Value added services:*
  - Call Hold;
  - Call Transfer;
  - Call Waiting;
  - Call Forward at Busy;
  - Call Forward at No Response;
  - Call Forward Unconditional;

- DND;
- Caller ID: FSK, DTMF;
- Hotline;
- Call Pickup;
- Flexible dialplan;

- Firmware update via web-interface;
- Backup version of firmware;
- Supporting DHCP-based autoprovisioning;
- TR-069;
- Remote monitoring, configuring and settings: Web interface, Telnet, SNMP.

Fig. 1 shows application diagram of the *RG-5421G-Wac* equipment.

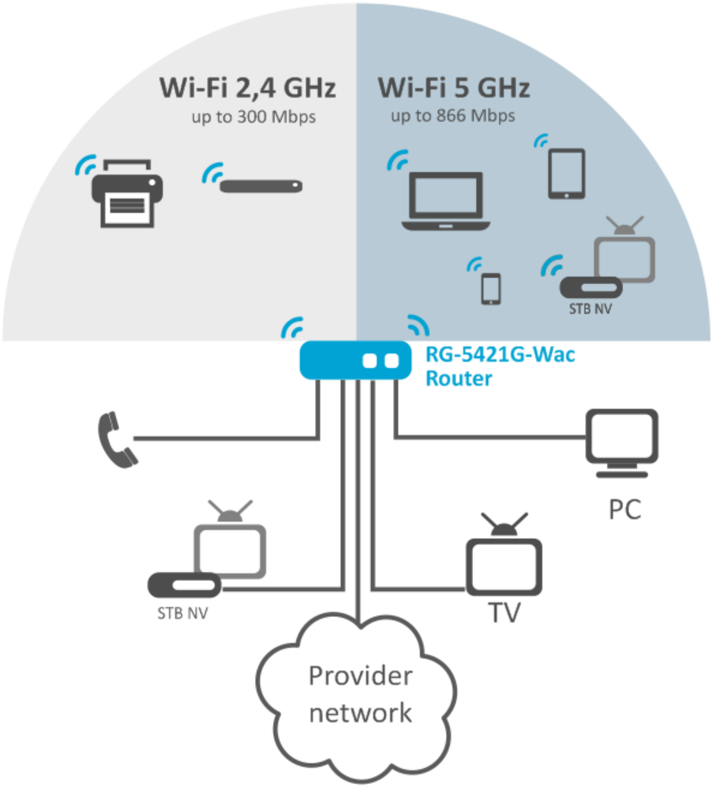


Fig. 1 –RG-5421G - Wac functional diagram

2.4 Architecture and the device operation principle

RG-5421G-Wac subscriber terminal consists of the following subsystem:

- Controller includes:
  - Realtek RTL8954ES System-on-a-Chip – SoC, including processor, gogabyte switch with a built PHY, hardware L2/L3/L4 traffic acceleration, USB 2.0 ports, PCI-E controllers, 12 PCM channels for operation of VoIP applications;
  - Flash memory – 32MB;
  - Operative memory – 128MB (DDR3);
- SLIC Subscriber complex (1×FXS);
- Ethernet switch 10/100/1000BASE-T– LAN (4 ports);
- Ethernet-module WAN: 10/100/1000BASE-T;
- 802.11ac dual-band Wi-Fi adapter;
- x2 USB Host ports.

Fig. 2 shows the device function chart.

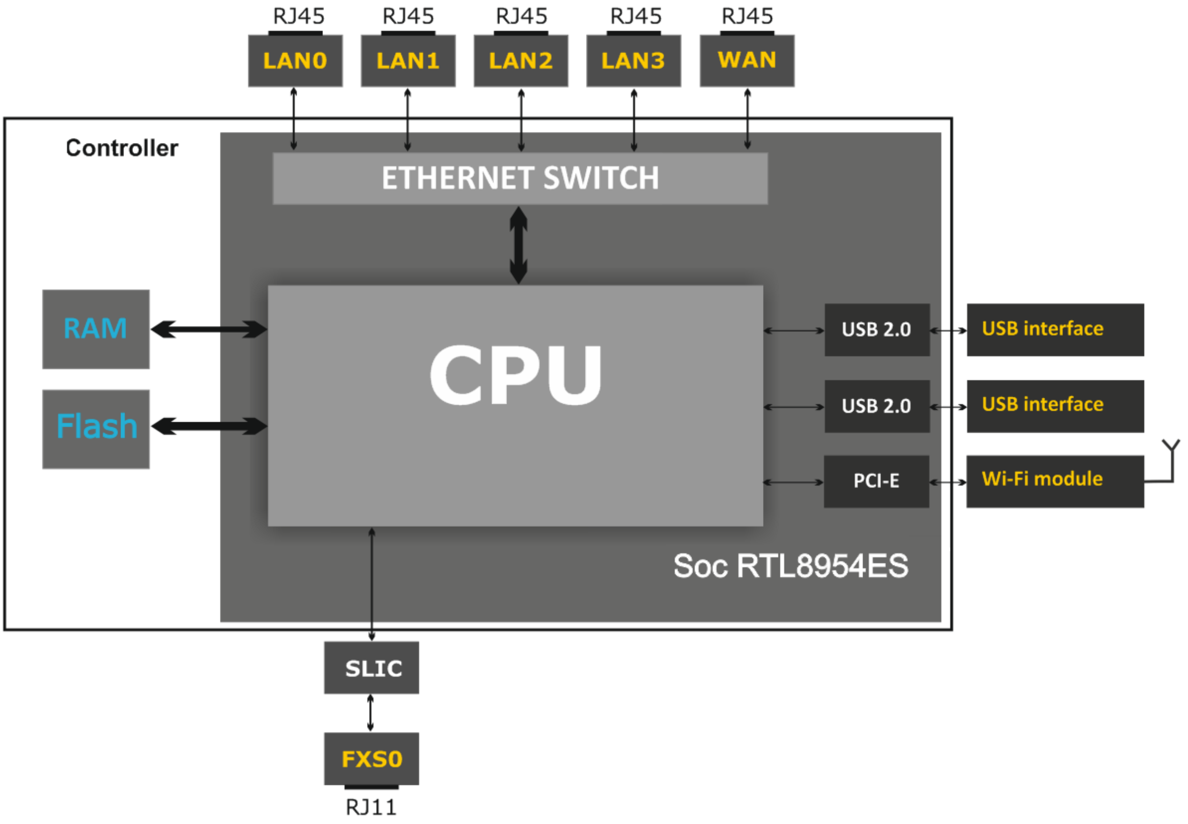


Fig. 2 –RG-5421G-Wac schematic diagram

Linux operating system controls the device operation. Basic control functions are performed by Realtek processor, which enables IP-packets routing, IP-telephony operation, group traffic proxying and etc.

The device can be divided into 4 blocks by functionality:

- Support block of network device functions;
- VoIP block;
- Processing block of multicast traffic;
- Control block (Linux operation system).

Device network features block provides passing and switching IP-packets in accordance with the device routing table and can process both untagged and tagged packets depending on network interface settings. The block supports Static, DHCP, PPPoE, PPTP and L2TP.

VoIP block provides the device operation via SIP protocol to transmit voice signal through packet-switched network. Subscriber's voice signal is transmitted to the SLIC subscriber line module to be digitized. Sampled signal is directed to VoIP block to be encoded in accordance with selected standards and is transmitted further in the form of digital packets to the controller via the intrasystem backbone. In addition to voice signals, digital packets contain control and interaction signals.

Multicast traffic processing block is designed to process IGMP messages and multicast traffic with the aim of IPTV function support.

Control block based on Linux operating system monitors operation of blocks listed above and device subsystems and manages their interaction.

Fig. 3 shows *RG-5421G-Wac* function diagram.

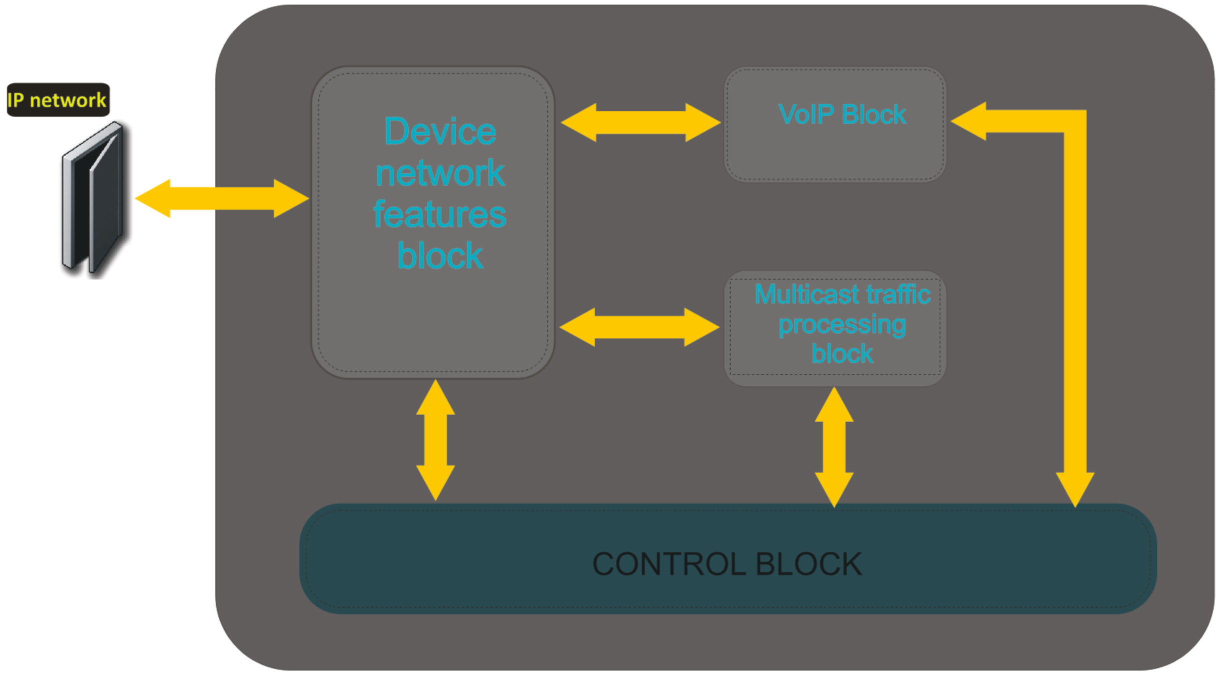

IP network
Device network features block
VoIP Block
Multicast traffic processing block
CONTROL BLOCK

Fig. 3 –*RG-5421G-Wac* function diagram

2.5 Key specification

Table 2 lists key specification of the device:

Table 2 – Key specifications

VoIP Protocols

Supported protocols	SIP

Audio codecs

Codecs	G.729, annex A, annex B, G.711a, G.711u, G.723.1, G.726-24, G.726-32 Modem transmission: G.711a, G.711u Fax transmission: G.711a, G.711u, T.38

Ethernet WAN interface parameters

Port number	1
Electrical connector	RJ-45
Data rate, Mbps	10/100/1000, autodetection
Standard	BASE-T

Ethernet LAN interface parameters

Interface number	4
Electrical connector	RJ-45
Data rate, Mbps	10/100/1000, autodetection
Standard	BASE-T

Parameters of analogue subscriber ports

Port number	1
Line loop resistance	Up to 2 kOhm
Dial reception	pulse/frequency (DTMF)
Protection of customer termination	over-voltage and overcurrent
Getting Caller ID	FSK BELL202/FSK V.23/DTMF

Wireless interface parameters

Standards	802.11 a/b/g/n/ac
Frequency range, MHz	2.4 ~ 2.4835 GHz, 5.15 ~ 5.35 GHz
Modulation	BPSK, QPSK, 16 QAM, 64 QAM, 256 QAM, DBPSK, DQPSK, CCK
Data bit rate, Mbps	**802.11b(CCK):** 1, 2, 5.5 ,11 **802.11g(OFDM):** 6, 9, 12 , 18, 24, 36, 48, 54 **802.11n (HT20, 800ns GI, MCS0-7):** 6.5, 13, 19.5, 26, 39, 52, 58.5, 65 **802.11n (HT20, 800ns GI, MCS8-15):** 13, 26, 39, 78, 104, 117, 130 **802.11n (HT20, 400ns GI, MCS0-7):** 7.2, 14.4, 21,7, 28.9, 43.3, 57.8, 65, 72.2 **802.11n (HT20, 400ns GI, MCS8-15):** 14.4, 28.9, 43.3, 57.8, 86.7, 115.6, 130.3, 144.4 **802.11n (HT40, 800ns GI, MCS0-7):** 13.5, 27, 40.5, 54, 81, 108, 121.5, 135 **802.11n (HT40, 800ns GI, MCS8-15):** 27, 54, 81, 108, 162, 216, 243, 270 **802.11n (HT40, 400ns GI, MCS0-7**): 15, 30, 45, 60, 90, 120, 135, 150 **802.11n (HT40, 400ns GI, MCS8-15):** 30, 60, 90, 120, 180, 240, 270, 300 **802.11ac (VHT20, 800ns GI, 1SS):** 6.5, 13, 19.5, 26, 39, 52, 58, 65, 78

	802.11ac (VHT20, 400ns GI, 1SS): 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 **802.11ac (VHT40, 800ns GI, 1SS):** 13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180 **802.11ac (VHT40, 400ns GI, 1SS):** 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 **802.11ac (VHT80, 800ns GI, 1SS):** 29.3, 58.5, 87.8, 117, 175.5, 234, 263.3, 292.5, 351, 390 **802.11ac (VHT80, 400ns GI, 1SS):** 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 **802.11ac (VHT20, 800ns GI, 2SS):** 13, 26, 39, 52, 78, 104, 117, 130, 156 **802.11ac (VHT20, 400ns GI, 2SS):** 14.4, 28.9, 43.3, 57.8, 86.7, 115.6, 130, 144.4, 173.3 **802.11ac (VHT40, 800ns GI, 2SS):** 27, 54, 81, 108, 162, 216, 243, 270, 324, 360 **802.11ac (VHT40, 400ns GI, 2SS):** 30, 60, 90, 120, 180, 240, 270, 300, 360, 400 **802.11ac (VHT80, 800ns GI, 2SS):** 58.5, 117, 175.5, 234, 351, 468, 526.5, 585, 702, 780 **802.11ac (VHT80, 400ns GI, 2SS):** 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7
Maximum transmitter output power	2,4 GHz **(802.11 b/g/n)**: up to 15 dBm 5 GHz **(802.11 a/n/ac)**: up to 17 dBm
Receiver sensibility	2,4 GHz: **802.11n(MCS0):** -90 dBm **802.11n(MCS4):** -79 dBm **802.11n(MCS7):** -72 dBm 5 GHz: **802.11ac (MCS0):** -92 dBm **802.11ac (MCS4):** -82 dBm **802.11ac (MCS7):** -76 dBm
Safety	64/128/152- bit WEP encryption of the data; WEP, TKIP and AES

Control

Remote control	Web interface, SSH, Telnet, SNMP, TR-069
Access restriction	Via password

General parameters

Power	power adaptor 12V DC, 2 A.
Power consumption	up to 10,2W
Range of working temperatures	from +5 to +40°C
Relative humidity at 25°C	up to 80%
Dimensions	187x124x32 mm
Weight	up to 0,3 kg.

2.6 Design

RG-5421G-Wac subscriber router enclosed into 187x124x32 mm plastic housing.

2.6.1 The device front panel

Fig. 4 shows front panel layout of RG-5421G-Wac device.

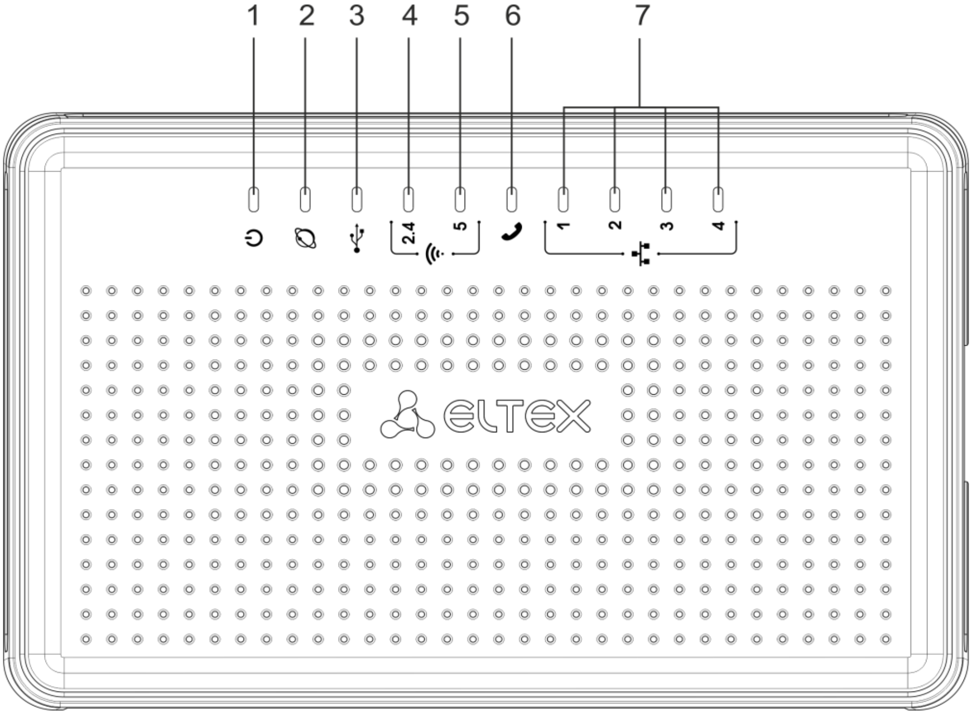


Fig. 4 –RG-5421G-Wac front panel layout

Light indicators are located on the front panel of RG-5421G-Wac, Table 3.

Table 3 – Description of indicators on the front panel

Front panel element		Description
1	Power	Indicator of power supply and the device operation status
2	WAN	WAN interface indicator
3	USB	Operation indicator of external USB devices (USB flash, external hard drive, 3G/4G USB modem)
4	WiFi 2.4	Operation indicator for wireless network (frequency range is 2.4 GHz)
5	WiFi 5	Operation indicator for wireless network (frequency range is 5 GHz)
6	Phone	Analogue phone operation indicator
7	LAN	LAN interface port indicator

2.6.2 Rear panel of the device

The rear panel layout of RG-5421G-Wac device is depicted in Fig. 5.

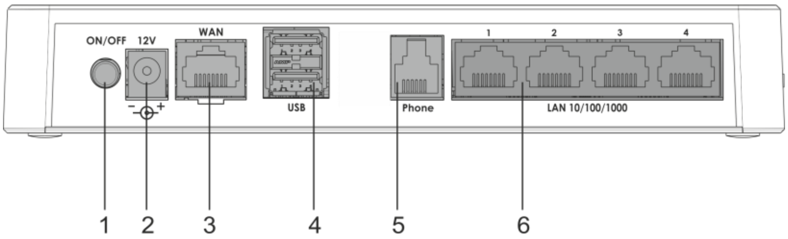


Fig. 5 –RG-5421G-Wac rear panel layout

The following connectors are located on the rear panel of RG-5421G-Wac, Table 4.

Table 4 – Description of the connectors on *RG5421G-Wac* rear panel

Rear panel element		Description
1	On/Off	On/Off main switch
2	12 V	Connector to connect power adaptor
3	WAN	10/100/1000BASE-T port (RJ-45 connector) for connection to external network
4	USB	2×USB connectors to connect external USB devices (USB flash, hard drive, 3G/4G USB modem)
5	Phone	RJ-11 connector for analogue phone connection
6	LAN	4×10/100/1000BASE-T Ethernet ports (RJ-45 connector) to connect network devices

2.6.3 Side panel of the device

Appearance of RG-5421G-Wac side penal is depicted on Fig. 6.

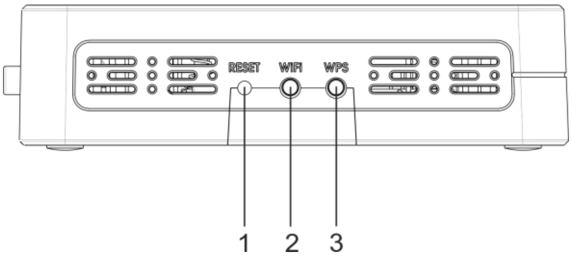


Fig. 6 –RG-5421G-Wac side panel layout

The following controls are located on the side panel of RG-5421G-Wac, Table 5.

Table 5 – Description of *RG5421G-Wac* side panel

Side panel element		Description
1	RESET	Optional button to reboot the device and reset it to default settings
2	Wi-Fi	Optional button to switch on/off Wi-Fi
3	WPS	Optional button for semi-automatic Wi-Fi design

2.7 Light indication

The current device status is displayed by indicators which are located on the front panel. The status list of indicator is shown in Table 6.

Table 6 – Light indication of RG-5400 device status

Indicator	Indicator status	Device status
2.4 GHz	Green, solid on	Wi-Fi network is active (2,4 GHz)
	Green, flashes	Data transmission via wireless network is in progress (2.4 GHz)
5 GHz	Green, solid on	Wi-Fi network is active (5 GHz)
	Green, flashes	Process of data transmission via wireless network (5GHz)
WAN	Green (10, 100Mbps)/ orange (1000 Mbps)	Established connection between station terminal and subscriber device (data rate is 10/100 or 1000 Mbps correspondingly)
	Flashes	Packet data transmission via WAN interface
LAN	Green (10, 100 Mbps)/ orange (1000 Mbps)	Established connection with connected network device (data rate is 10/100 or 1000 Mbps correspondingly)
	flashes	Packet data transmission via LAN interface
Phone	Green, solid on	The phone is off-hook (line is active)
	Off	The phone is on-hook, normal operation
	Flashes during with 20 Hz frequency for 1 second, then 4 seconds pause	Incoming call is on the phone port
	Green , flashes slowly in periods	Subscriber port registration is absent at SIP-proxy server
	Short double flashes after each 3 seconds	Process of line probing
USB	Green, solid on	USB device is connected
	off	USB device is disabled
Power	Green, solid on	Device power is enabled, normal operation
	Orange, solid on	Internet is unavailable
	Red, solid on	The device loading, reset to the default settings
	3 pulses/pauses for 50 ms, 1 s pause	WPS mode is enabled

2.8 Reset to the default settings

In order to start device with the default settings, press and hold ‘Reset’ button (it should be done when the device is loaded) until ‘Power’ indicator begins to flash red. After that, the device will be rebooted automatically. In the default configuration, DHCP client is launched on WAN interface. Interface address – *192.168.1.1*, subnet mask – *255.255.255.0*, username/password for access via web interface – admin/password.

2.9 Delivery package

The standard delivery package of *RG-5400* includes:

- subscriber router;
- power adaptor 220 /12V 2 A ;
- operation manual.

3 DEVICE CONTROL VIA WEB CONFIGURATOR

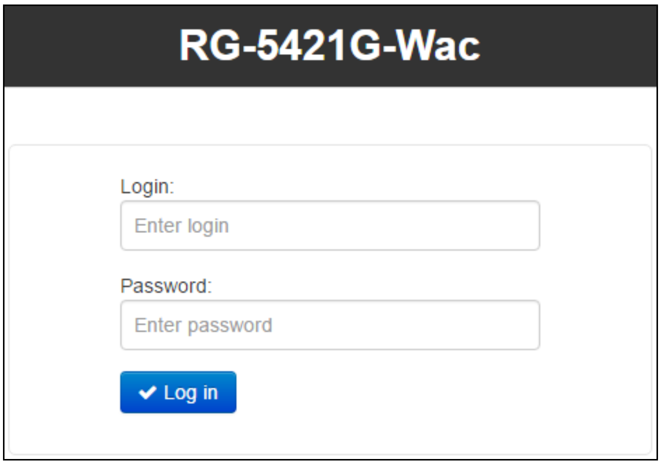
3.1 Getting started

Connect to the device via LAN interface by using Web-browser:

1. Open Web browser (explorer for hypertext document) such as Firefox, Opera and Chrome.
2. Enter IP address of the device into browser string.

The default IP address of the device: 192.168.1.1, subnet mask: 255.255.255.0

If the device is successfully discovered, a page with username and password request will be displayed in a browser window.

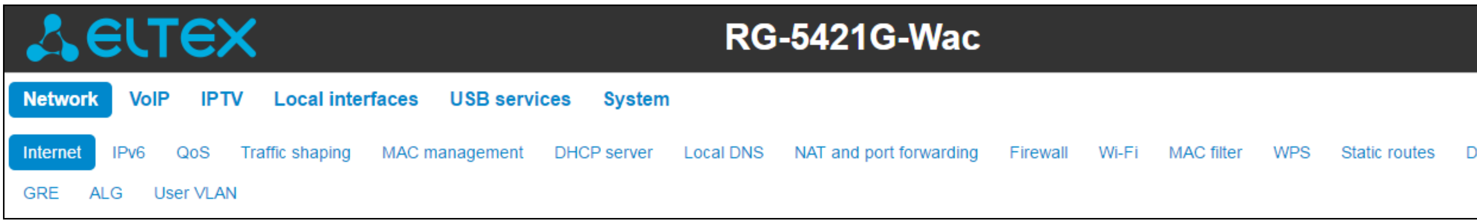


3. Fill in the string 'Login' by username and the string 'Password' by password.

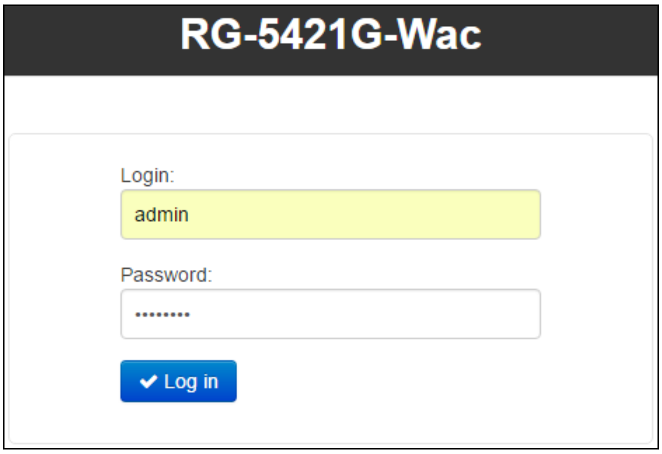
The default settings: login-*admin*, password-*password*.

3.2 User change

There are three user types for the device: **admin**, **user,** and **viewer**. **Admin** (**administrator**, default password: **password**) has the full access to the device: read/write any settings, full device status monitoring. **User** (**user**, default password: **user**) may configure PPPoE in order to connect to the Internet and configure Wi-Fi, may not access the device status monitoring. **Viewer** may only view full device configuration without editing privileges; may access full device status monitoring.



When you click *'Exit'* button, the current user session will be terminated; login window will be displayed:


RG-5421G-Wac

Login: admin

Password: ••••••••

✓ Log in

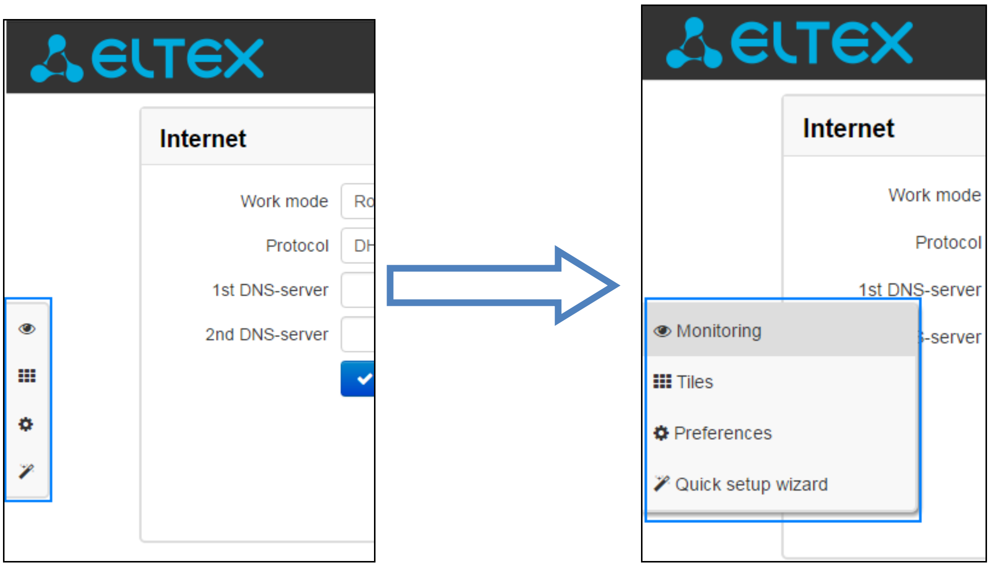
To change the access, you should specify the corresponding username and password and click *'Sign In'* button.

3.3 WEB interface operation modes

RG-5400 WEB interface may operate in three modes:

- **Monitoring** – system monitoring mode – allows you to view various device operation information: Internet connection activity, phone port status, amount of data received/transmitted via interface, etc.;
- **Tiles** – quick system configuration mode – each tiles contents settings grouped by their functions: Internet, VoIP, IPTV and etc. A title only displays basic parameters that allow you to configure a specific device function as a quick as possible;
- **Preferences** – advanced system configuration mode (full configuration mode) – enables full device configuration.
- **Quick setup wizard** – configuration mode for the key device parameters.

To switch between WEB interface modes, use the panel located on the left hand side in WEB interface. The panel will open, when you hover mouse cursor over it:



To proceed from 'Tiles' mode into 'Settings', you may also click 'Details' link in the tile name.

3.4 Applying configuration and discarding changes

1. Applying configuration

✓ **Click 'Apply' button to save the configuration into the device flash memory and apply new settings. All settings will take effect without device restart.**

'Apply' button in the quick configuration and in the advanced settings menu will appear as follow: ✓; ✓ Apply.

WEB interface features visual indication of the current status of the settings application process, see Table Table 7.

Table 7 – Visual indication of the current status of the settings application process

Appearance	Status description
Network settings ⁘	When you click the 'Accept' button, settings will be applied and stored into the device memory. This is indicated by the ⁘ icon in the tab name and on the 'Apply' button.
Network settings ✓	Successful settings saving and application are indicated by ✓ icon in the tab name.
Network settings ⊖	If the parameter value being specified contains an error, you will see a message with the reason description and the ⊖ icon will appear in the tab name, when you click 'Apply' button.

2. Discarding changes

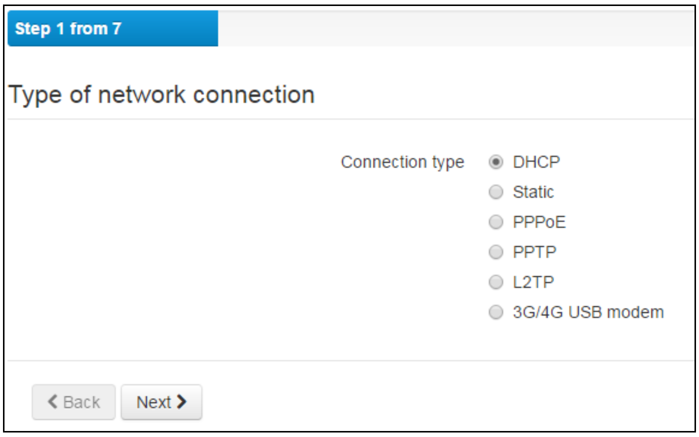
✓ **You may discard changes only until 'Apply' button is clicked. In this case, edited parameters on the page will be updated with the values currently stored in the device memory. After you click 'Apply', you will not be able to restore previous settings.**

Discard changes button in the quick configuration menu and the advanced settings menu will appear as follows: ✖; ✖ Cancel.

3.5 Quick Setup Wizard

Quick setup wizard allows you to provide quick changes of the key device parameters. The settings are divided thematically into 7 steps:

- *Type of network connection* – select protocol for connection to an external network.

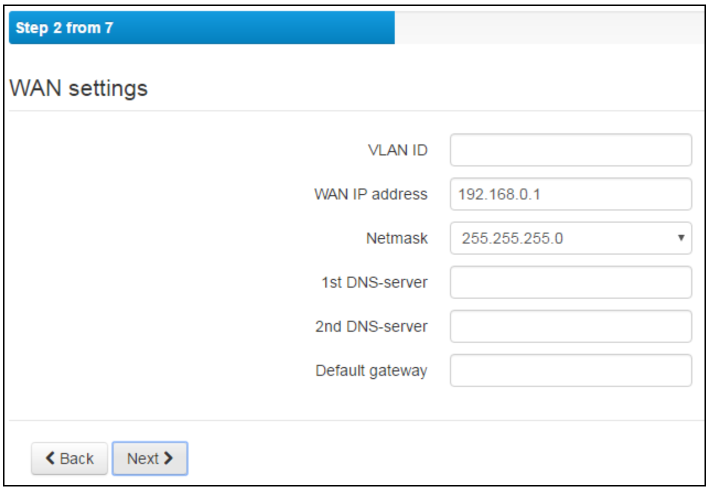


Step 1 from 7

Type of network connection

Connection type
● DHCP
○ Static
○ PPPoE
○ PPTP
○ L2TP
○ 3G/4G USB modem

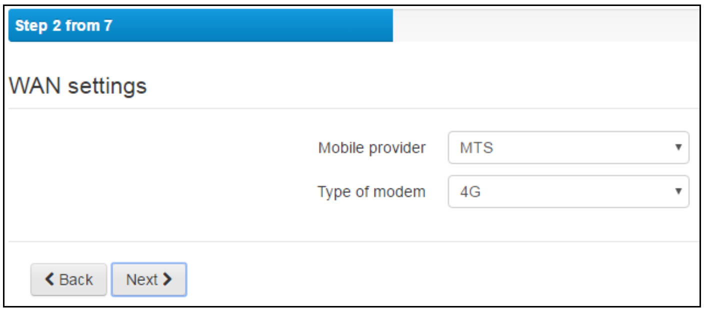
- *WAN settings.* Enter the specific settings of the connection type selected to connect to the external network. If you select connection via 3G/4G modem in the previous step it will be enough to select provider and mobile communication type.



Step 2 from 7

WAN settings

VLAN ID
WAN IP address: 192.168.0.1
Netmask: 255.255.255.0
1st DNS-server
2nd DNS-server
Default gateway

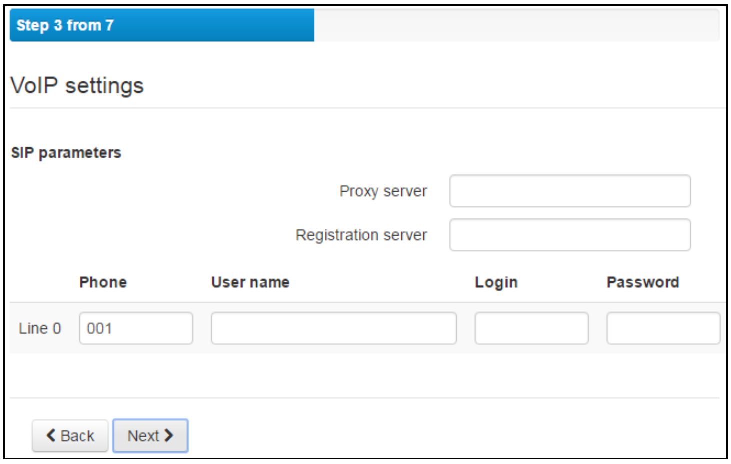


Step 2 from 7

WAN settings

Mobile provider: MTS
Type of modem: 4G

- *VoIP settings.* On this step, basic VoIP configuration is performed. You should enter address of a SIP proxy server, registration server and phone numbers, user names, logins and passwords for phone lines.



Step 3 from 7

VoIP settings

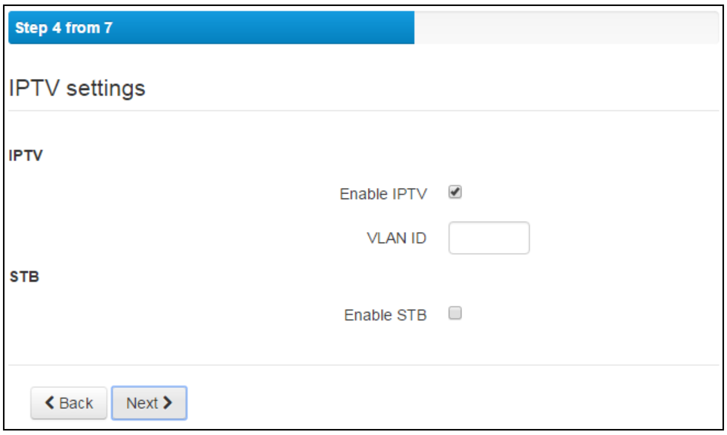
SIP parameters

Proxy server

Registration server

	Phone	User name	Login	Password
Line 0	001			

- *IPTV settings*. It allows you to enable or disable IPTV (if required), enter used VLAN ID and enable and select ports for STB.



Step 4 from 7

IPTV settings

IPTV

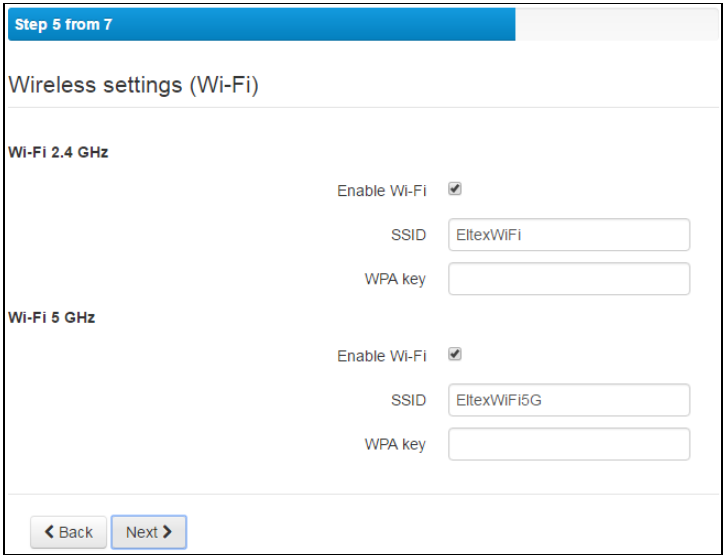
Enable IPTV ☑

VLAN ID

STB

Enable STB ☐

- *Wireless settings (Wi-Fi).* On this step, you may enable or disable Wi-Fi for 2.4 and 5 GHz respectively and configure identifiers for networks and passwords.



Step 5 from 7

Wireless settings (Wi-Fi)

Wi-Fi 2.4 GHz

Enable Wi-Fi ☑

SSID EltexWiFi

WPA key

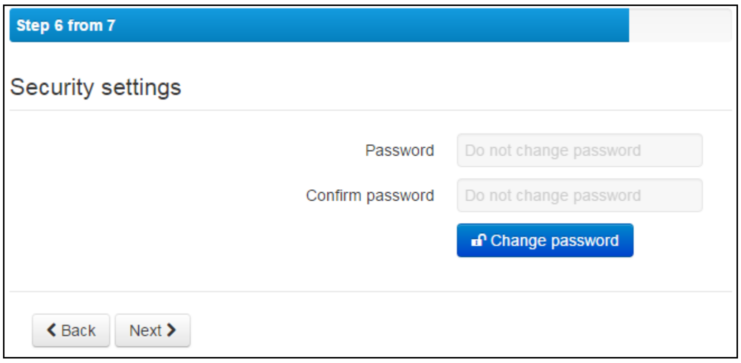
Wi-Fi 5 GHz

Enable Wi-Fi ☑

SSID EltexWiFi5G

WPA key

- *Security settings.* You *are* invited to change a password of the device administrator.



Step 6 from 7

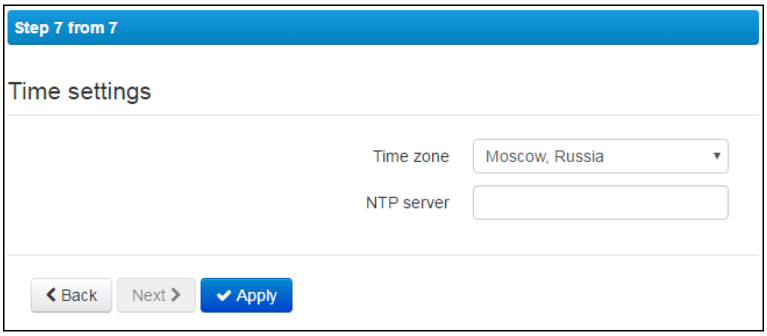
Security settings

Password: Do not change password

Confirm password: Do not change password

A move to the next setting step will be blocked until a new password will not be set (the modified password can be the same with the current password).

- *Time settings.* On this step, you should select time zone and enter address of a time synchronization server or select server from the dropdown list.



Step 7 from 7

Time settings

Time zone: Moscow, Russia

NTP server:

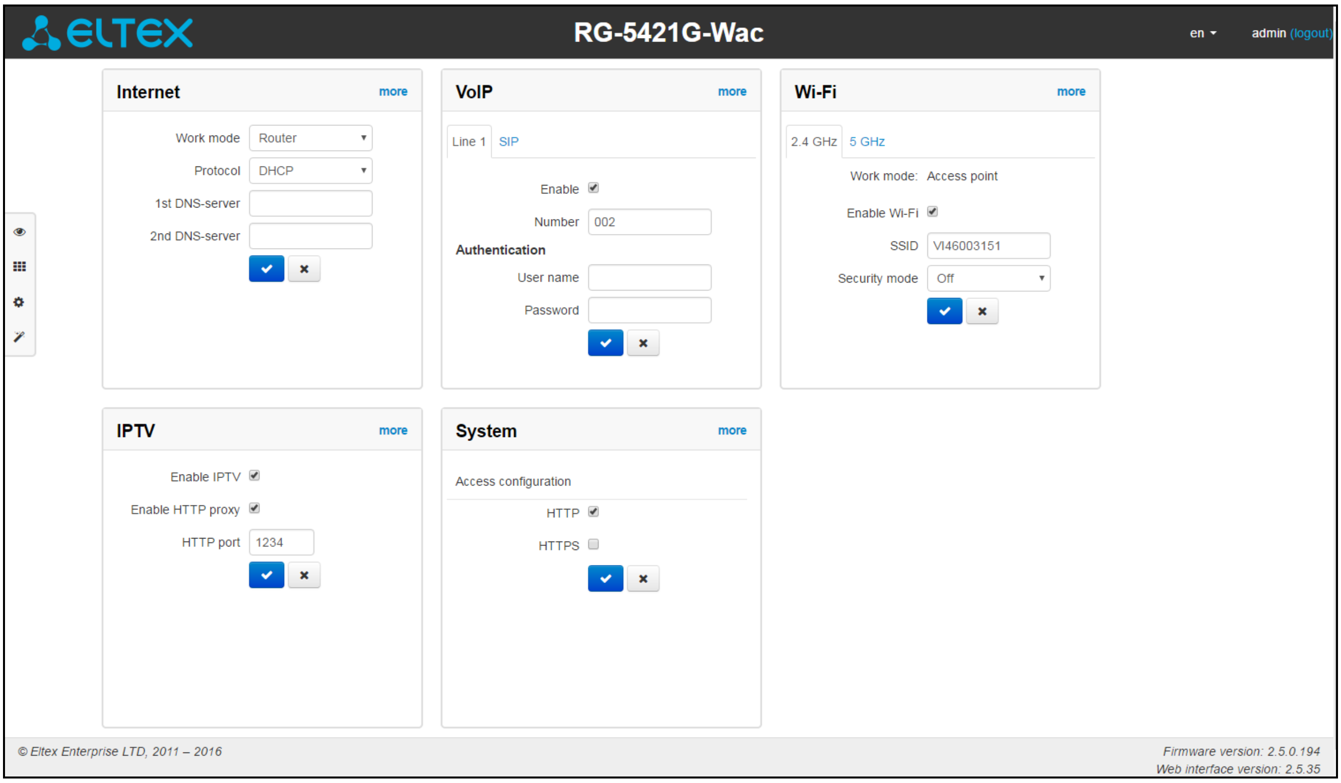
Click 'Apply' button after you complete all the steps to continue working with the device.

After applying configuration, an automatic redirect to http://192.168.1.1/ page will be performed.

At any time, you may exit wizard by selecting *Monitoring*, *Tile* and *Settings* in the side menu.

3.6 Quick configuration menu

In the quick configuration menu, you will find basic device settings, see Fig. 7.



Internet

Work mode: Router
Protocol: DHCP
1st DNS-server:
2nd DNS-server:

VoIP

Line 1 | SIP

Enable ☑
Number: 002

Authentication

User name:
Password:

Wi-Fi

2.4 GHz | 5 GHz

Work mode: Access point
Enable Wi-Fi ☑
SSID: VI46003151
Security mode: Off

IPTV

Enable IPTV ☑
Enable HTTP proxy ☑
HTTP port: 1234

System

Access configuration

HTTP ☑
HTTPS □

© Eltex Enterprise LTD, 2011 – 2016

Firmware version: 2.5.0.194
Web interface version: 2.5.35

Fig. 7 – Quick configuration menu

Settings are divided into the following categories:

- *Internet* – quick Internet access configuration;
- *VoIP* – quick VoIP configuration;
- *Wi-Fi* – wireless access point configuration;
- *IPTV* – configure device to support IPTV features;
- *System* – system parameter settings (access to the device, time synchronization and etc.).

3.6.1 Internet

In order to access the Internet, you should specify basic settings in the ‘Internet’ section. To specify additional parameters, go to advanced settings mode by clicking the 'Details' link.

- *Operation mode* – operation mode of the device:
  - *Router* – router mode is established between LAN- and WAN interfaces (LAN is isolated from WAN);
  - *Bridge* – bridge mode is established between WAN and LAN interfaces: data is transferred transparently from LAN to WAN and back – in fact, the device operates in the switch mode.

- *Protocol* – select the protocol that will be used for device WAN interface connection to provider network:

  - *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. When 'Static' type is selected, the following parameters will be available for editing:
    - *Devices external IP address* – specify device WAN interface IP address in the provider network;
    - *Subnet mask* – external subnet mask;
    - *Default gateway* – address that the packet will be sent to, when its route is not found in the routing table;
    - *Primary DNS, Secondary DNS* – domain name server addresses (allows you to identify the IP address of the device by its domain name). You may leave these fields empty, if they are not required.

  - *DHCP* –operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server.

  Supported options:
    - 1 – netmask;
    - 3 – default network gateway address;
    - 6 – DNS server address;
    - 12 – network device name;
    - 28 – network broadcast address;
    - 33 – static routers;
    - 42 – NTP server address;
    - 43 – specific vendor information;
    - 66 – TFTP server address;
    - 67 – firmware file name (for download via TFTP from the server specified in Option 66);
    - 120 - outbound SIP;
    - 121 – classless static routs.

  In Option 60 DHCP request, the device will send vendor information in the following format:

  - **[VENDOR:**vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:**serial number**][WAN:** WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**firmware version**]**

  Example:
  [VENDOR:Eltex][DEVICE:RG-5421G-Wac][HW:1.3][SN:VI46XXXXXX][WAN:A8:F9:4B:XX:XX:XX]

[LAN:02:20:80:a8:f9:4b][VERSION:#2.2.0.217]

- *PPPoE* –operation mode when PPP session is established on WAN interface. When 'PPPoE' is selected, the following parameters will be available for editing:
  - *Username* – username for authorization on PPP server;
  - *Password* – password for authorization on PPP server;
  - *Service-Name* – 'Service-Name' tag value in PADI message for PPPoE connection initialization (this parameter is optional, and configured only on the provider's request);
  - *Second access* – type of access to local area network resources.
    You may select two options:
    - *DHCP* – dynamic access when IP address and other required parameters are obtained via DHCP;
    - *Static* – in this case, you should specify access settings manually: *IP address, Subnet mask, DNS.*

- *PPTP* – operation mode when the Internet access is established via a special channel—a tunnel—using PPTP. When *'PPTP'* is selected, the following parameters will be available for editing:
  - *PPTP-Server* – PPTP server address (domain name or IP address in IPv4 format);
  - *Username* – username for authorization on PPTP-server;
  - *Password* – password for authorization on PPTP server;
  - *Second access* – access type to local area network resources and PPTP server. You may select two options:
    DHCP – dynamic access when IP address and other required parameters are obtained via DHCP;
    Static – in this case, you should specify PPTP server access settings manually:
    - *IP address* – when the static access is used, PPTP server will be accessed from this address;
    - *Subnet mask* – subnet mask for static access;
    - *DNS* – local area network DNS for static access;
    - *Gateway* – gateway for PPTP server access when the static access is used (if necessary).

- *L2TP* – operation mode when the Internet access is established via a special channel—a tunnel—using L2TP. When *'L2TP'* is selected, the following parameters will be available for editing:
  - *L2TP server* – L2TP server address (domain name or IP address in IPv4 format);
  - *Username* – username for authorization on L2TP server;
  - *Password* – password for authorization on L2TP server;
  - *Second access* – type of access to local area network resources and L2TP server. You may select two options:
    DHCP – dynamic access when IP address and other required parameters are obtained via DHCP;
    Static – in this case, you should specify L2TP server access settings manually:
    - *IP-address* – when the static access is used, PPTP server will be accessed from this address;
    - *Subnet mask* – subnet mask for static access;
    - *DNS* – local area network DNS for static access;
    - *Gateway* – gateway for L2TP server access (if necessary) in case of static access.

PPTP and L2TP allow you to establish secure communication link over the Internet between the remote user's computer and organization's private network. PPTP and L2TP are based on Point-to-Point Protocol (PPP) and act as its extension. First, the OSI model higher level data is encapsulated into PPP, and then into PPTP or L2TP for tunnel transmission via public data networks. PPTP and L2TP functionality differs. L2TP may be used not only in IP networks, service messages for tunnel creation and data transfer use the same format and protocols. PPTP may be used only in IP networks, it requires a dedicated TCP connection for tunnel creation and usage. L2TP over IPSec[1] allows for the higher security level compared to PPTP and provides the higher level of protection for business-critical data.

Due to its characteristics, L2TP is an attractive protocol for building virtual networks.

- *Bridge* – device operates in the bridge mode (switch with 5 ports). Set the following parameters to get access:
  - *IP address* – bridge IP address;
  - *Subnet mask* – subnet mask of bridge.

To apply a new configuration and store settings into the non-volatile memory, click ✓ button. To discard changes, click ✖ button.

To connect the device to the provider network, you should request the network settings from the provider. If you use the static settings, select 'Static' value in the 'Protocol' field and fill the 'External IP address', 'Subnet mask', 'Default gateway', 'Primary DNS', and 'Secondary DNS' fields with the corresponding values obtained from the provider. If devices in the provider network obtain network settings via DHCP, PPPoE, PPTP, or L2TP—select the corresponding protocol in the 'Protocol' field and refer to provider's instructions to achieve complete and correct device configuration.

[1] Disable transmitting the sender addresses for proper IPSec operation.

3.6.2 VoIP

For VoIP operation, you should specify settings in the 'VoIP' section. To specify additional parameters, go to advanced settings mode by clicking the 'Details' link.

In the 'Line 1' tab, you may configure device phone port ('Phone') basic settings:

- *Enable* – when checked, the current line is active;
- *Number* – subscriber number, assigned for this phone line;
- *Username* – username for authentication on SIP server;
- *Password* – password for authentication on SIP server.

In SIP tab, you may configure basic settings for SIP proxy server:

- *SIP proxy server* – SIP server network address – device that manages access to provider's phone network for all subscribers. You may specify IP address as well as the domain name (specify an alternative SIP server UDP port after the colon, default value is 5060);
- *Registration* – when checked, subscriber port registration will be enabled on the registration server;
- *Registration server* – network address of a device that is used for registration of all phone network subscribers in order to provide them with the communication services (specify an alternative registration server port after the colon, default value is 5060). You may specify IP address as well as the domain name. As a rule, registration server is physically co-located with SIP proxy server (they have the same address);
- *SIP domain* – domain where the device is located (fill in, if required).

To apply a new configuration and store settings into the non-volatile memory, click ✓ button. To discard changes, click ✖ button.

3.6.3 Wi-Fi

For Wi-Fi operation, you should specify settings in the 'Wi-Fi' section. To specify additional parameters, go to advanced settings mode by clicking the 'Details' link.

In the ‘2.4 GHz’ tab, you may configure Wi-Fi settings on a frequency of 2.4 GHz. In the ‘5 GHz’ tab, you may configure Wi-Fi settings on a frequency of 5 GHz:

- *Enable Wi-Fi* – when checked, wireless access point is activated in accordance with frequency range (2.4 GHz or 5GHz) otherwise access point is off;
- *SSID* – wireless network name used for connection to a device. Maximum name length is 32 characters that is case-sensitive. The parameter may consist of digits, Latin letters and "-", "_", ".", "!", ";", "#" symbols but "!", ";", "#" symbols can’t be placed first;
- *Secure mode* – selection of secure mode for wireless network:
  - *Off* – wireless network encryption is disabled, low security level;
  - *WEP* – WEP authentication. WEP key should consist of hexadecimal digits with length of 10 or 32 characters or should be string (a-z, A-Z, 0-9, ~!@#$%^&*()_-+= symbols) with length of 5 or 13 characters.
  - *WPA, WPA2* – WPA and WPA2 authentication. The length of key is from 8 to 63 characters. You may use only following symbols: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"`' or space character.

To apply a new configuration and store settings into the non-volatile memory, click ✓ button. To discard changes, click ✖ button.

3.6.4 IPTV

For IPTV operation, you should specify settings in 'IPTV' section. To specify additional parameters, go to advanced settings mode by clicking the 'Details' link.

- *Enable IPTV* – when checked, enable IPTV packet transmission from *TAU-1M.IP* WAN interface (from the provider network) to the devices connected to LAN interface;
- *Enable HTTP proxy* – when checked, use HTTP proxy. HTTP proxy transforms UDP stream into HTTP stream in order to improve stream image quality, when the quality of the communication link in local area network is low. Function is useful for watching IPTV via Wi-Fi channel;
- *HTTP port* – HTTP proxy port number that will be used for video streaming. Use this port to connect to IPTV streams being broadcast by the device.

HFor example, if the device address on LAN interface is 192.168.0.1, proxy server port is 2354, and the desired channel 227.50.50.100 is being broadcast to UDP port 1234, you should specify the following stream address for VLC application: http://@192.168.0.1:2345/udp/227.50.50.100:1234.

To apply a new configuration and store settings into the non-volatile memory, click ✓ button. To discard changes, click ✖ button.

3.6.5 System

In the 'System' section, you may configure access to the device web configurator. To specify additional parameters, go to advanced settings mode by clicking the 'Details' link.

Access to Web via WAN:

- *HTTP* – when checked, WAN port connection to the device web configurator is enabled via HTTP (insecure connection);
- *HTTPS* – when checked, WAN port connection to the device web configurator is enabled via HTTPS (secure connection).

By default, access to the device Web interface is enabled only for LAN interface.

To apply a new configuration and store settings into the non-volatile memory, click ✓ button. To discard changes, click ✖ button.

3.7 Advanced settings

To proceed to the advanced settings mode, click 'Details' link or select 'Settings' item on the left panel.

3.7.1 Web interface basic elements

Fig. 8 shows WEB configurator basic navigation elements in the advanced settings mode.

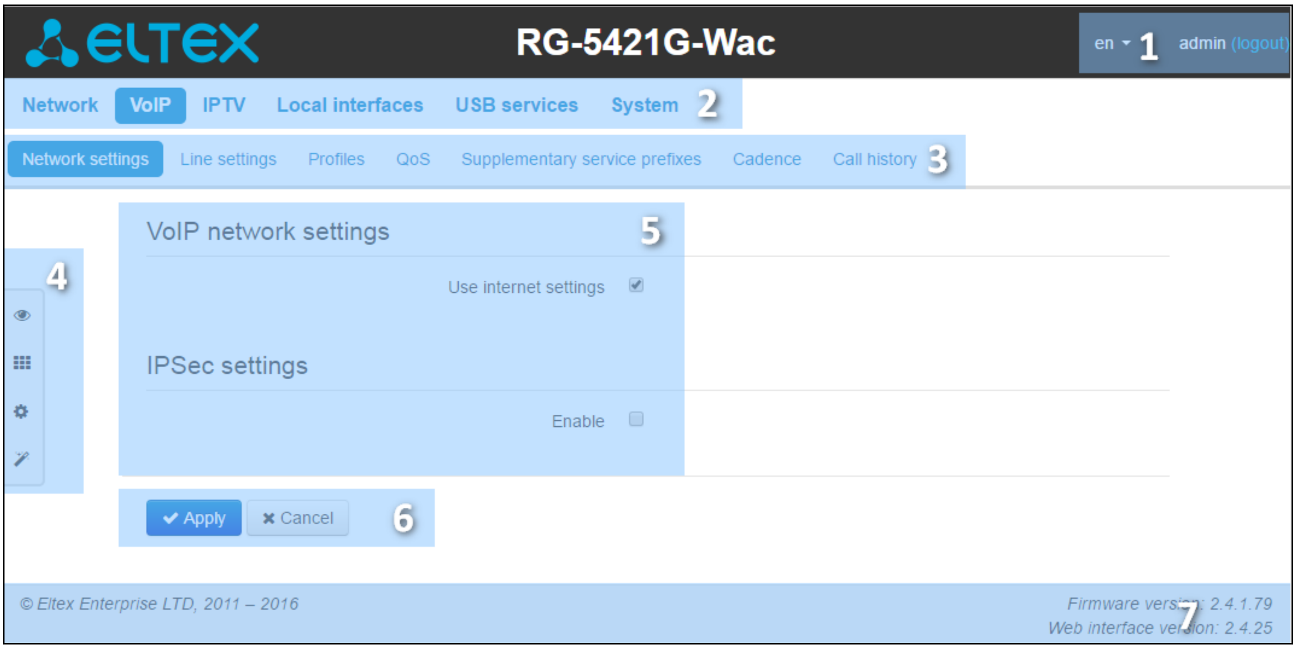


Fig. 8 – Web configurator navigation elements

User interface window is divided into 7 areas:

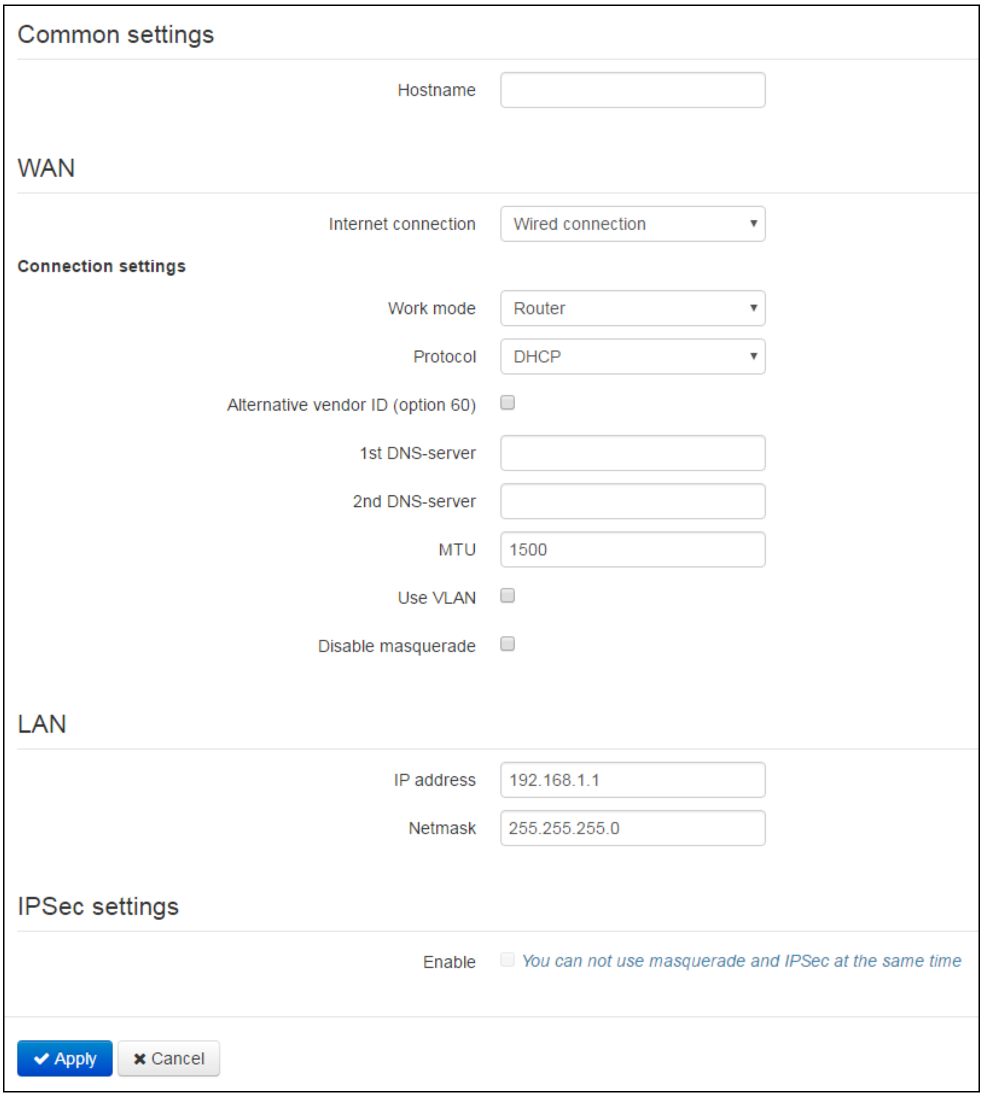
1. Logged in user name and session termination button in the WEB interface ('Sign Out') for the current user.
2. Menu tabs include submenu tabs grouped by a category: Network, VoIP, IPTV, Local interfaces, System.
3. Submenu tabs allow for settings field management.
4. WEB configurator mode changing panel (for description, see section 3.3)
5. Device settings field based on the user selection; allows you to view device settings and enter configuration data.
6. Configuration management buttons; for detailed description, see section 3.4:
7. Informational field showing firmware version and WEB interface version.

3.7.2 ‘Network’ menu

In ‘Network’ menu, you may configure key device network settings.

3.7.2.1 ‘Internet’ submenu

In the 'Internet' submenu, you may configure an external network (via PPPoE, DHCP, PPTP, L2TP, statically, in the router or bridge mode) and LAN.



Common settings

Hostname:

WAN

Internet connection: Wired connection ▾

Connection settings

Work mode: Router ▾

Protocol: DHCP ▾

Alternative vendor ID (option 60): □

1st DNS-server:

2nd DNS-server:

MTU: 1500

Use VLAN: □

Disable masquerade: □

LAN

IP address: 192.168.1.1

Netmask: 255.255.255.0

IPSec settings

Enable: □ *You can not use masquerade and IPSec at the same time*

<u>*Common settings*</u>

– *Host name – network device name.*

<u>*WAN*</u>

– *Internet connection* – external network connection method for the device:

▪ *Wired connection* – connection to the Internet is established using Ethernet cable via WAN port only;

- *3G/4G USB modem* – connection to Internet is established by 3G/4G USB modem (via cellular data network) connected to a USB port of the device;
- *Wi-Fi connection* – connection to Internet is established via Wi-Fi.

Connection settings

1. When you choose **'Wired connection'** method, the following connection settings will become available:

- *Operation mode* – the device operation mode:
  - *Router* – router mode is established between LAN and WAN interfaces (LAN is isolated from WAN);
  - *Bridge* – bridge mode is established between LAN and WAN interfaces: data is transferred transparently from LAN to WAN and back—in fact, the device operates in router mode.

The following settings will be available when you select '*Router'* mode:

- *Protocol* – select the protocol that will be used for device WAN interface connection to provider network:
  - Static – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. When 'Static' type is selected, the following parameters will be available for editing:
    - *External IP address of the device* – specify device WAN interface IP address in the provider network;
    - *Subnet mask – external subnet mask*;
    - *Default gateway* – address that the packet will be sent to, when its route is not found in the routing table;
    - *Primary DNS, Secondary DNS* – domain name server addresses (allows you to identify the IP address of the device by its domain name). You may leave these fields empty, if they are not required.
  - *DHCP* – operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server.

  Supported options:
    - 1 – network mask;
    - 3 – default gateway network address;
    - 6 – DNS server address;
    - 12 – network device name;
    - 28 – network broadcast address;
    - 33 – static routes;
    - 42 – NTP server address;
    - 43 – specific vendor information;
    - 66 – TFTP server address;
    - 67 – firmware file name (for download via TFTP from the server specified in Option 66);
    - 120 - outbound of SIP server;
    - 121 – classless static routs.

For DHCP, you may specify the required value for Option 60.

- *Alternative Vendor ID (Option 60)* – when checked, the device transmits *Vendor ID (Option 60)* field value by Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted in DHCP messages.
  If the *Alternative Vendor ID (Option 60)* checkbox is not selected, the default value will be transmitted in Option 60 in the following format:
  [VENDOR:vendor**][DEVICE:**the device type**][HW:**hardware version**] [SN:**serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**firmware version**]**

  Example:
  [VENDOR:Eltex][DEVICE:RG-5421G-Wac][HW:1.2][SN:VI23000118]
  [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.1.0]

- *Primary DNS, Secondary DNS* – IP address of DNS server – if DNS addresses are not obtained automatically via DHCP, you should define them manually. Manually defined addresses will have a priority over DNS addresses obtained via DHCP.

- *PPPoE* – operation mode when PPP session is established on WAN interface. When 'PPoE' is selected, the following parameters will be available for editing:
  - *Username* – username for authorization on PPP server;
  - *Password* – password for authorization;
  - *Connection type* – in accordance with a selected value of a PPP-session: AlwaysOn; OnDemand (session is initialized when traffic transmission is required); Manual (manual session activation);
  - *Inactivity Timeout, sec* – time interval after which PPP-session will be broken when the PPP-session becomes inactive in the OnDemand mode;
  - *LCP-echo amount* – amount of the unreplied LCP-requests after which PPP session will be broken;
  - *Period of LCP-echo transmission, sec* – period for LCP-echo transmission;
  - *MTU* – maximum block size for data transmitted via the network (1492 is recommended);
  - *Service-Name* – 'Service-Name' tag value in PADI message (this field is optional);
  - *Second access* – type of access to local area network resources.
    You may select two options:
    DHCP – dynamic access when IP address and other required parameters are obtained via DHCP;
    Static – in this case, you should specify access settings manually
    IP address, *Subnet mask, DNS server;*
  - *Hardware traffic acceleration* – increase device bandwidth for PPP traffic (if *PPP* is selected) or IPoE traffic (if *Ethernet* is selected) transmission depending on the selected value.

- *PPTP* – operation mode when the Internet access is established via a special channel—a tunnel—using PPTP. When *'PPTP'* is selected, the following parameters will be available for editing:
  - *PPTP server* – IP address of PPTP server;
  - *User name* – username for authorization on PPTP server;
  - *Password* – password for authorization on PPTP server;
  - *Connection type* – in accordance with a selected value of a PPP-session: AlwaysOn; OnDemand (session is initialized when traffic transmission is required); Manual (manual session activation);

  - *Inactivity Timeout, sec* – time interval after which PPP-session will be broken when the PPP-session becomes inactive in the OnDemand mode;
  - *LCP-echo amount* – amount of the unreplied LCP-requests after which PPP session will be broken;
  - *Period of LCP-echo transmission, sec* – period for LCP-echo transmission;
  - *MTU* – maximum block size for data transmitted via network (1462 is recommended);
  - *Secondary access* – access type to local area network resources and PPTP server. You may select 2 options:
    DHCP – dynamic access when IP address and other required parameters are obtained via DHCP;
    Static – in this case, you should specify PPTP server access settings manually:
  - *IP address* – when the static access is used, PPTP server will be accessed from this address;
  - *Subnet mask* – subnet mask for static access;
  - *DNS server* – local area network DNS for static access;
  - *Gateway* – subnet mask for static access (if necessary).

Hardware traffic acceleration works only for secondary access interface (IPoE).

- *L2TP* – operation mode when the Internet access is established via a special channel—a tunnel—using L2TP. When *'L2TP'* is selected, the following parameters will be available for editing:
  - *L2TP Server* – IP address of L2TP server;
  - *Username* – username for authorization on L2TP server;
  - *Password* – password for authorization on L2TP server;
  - *Connection type* – in accordance with a selected value of a PPP-session: AlwaysOn; OnDemand (session is initialized when traffic transmission is required); Manual (manual session activation);
  - *Inactivity Timeout, sec – time i*nterval after which PPP-session will be broken when the PPP-session becomes inactive in the OnDemand mode;
  - *LCP-echo amount* – amount of the unreplied LCP-requests after which PPP session will be broken;
  - *Period of LCP-echo transmission, sec* – period for LCP-echo transmission;*MTU* – maximum block size for data transmitted via the network (1462 is recommended);
  - *Secondary access* – type of access to local area network resources and L2TP server.
    You may select 2 options:
    DHCP – dynamic access when IP address and other required parameters are obtained via DHCP;
    Static – in this case, you should specify L2TP server access settings manually:
  - *IP address* – when the static access is used, PPTP server will be accessed from this address;
  - *Subnet mask* – subnet mask for static access;
  - *DNS server* – local area network DNS when the static access is used;
  - *Gateway* – gateway for L2TP server access (if necessary) when the static access is used.

Hardware traffic acceleration works only for secondary access interface (IPoE).

PPTP and L2TP allow you to establish secure communication link over the Internet between the remote user's computer and organization's private network. PPTP and L2TP are based on Point-to-Point Protocol (PPP) and act as its extension. First, the OSI model higher level data is encapsulated into PPP, and then into PPRP or L2TP for tunnel transmission via public data networks. PPTP and L2TP functionality differs. L2TP may be used not only in IP networks, service messages for tunnel creation and data transfer use the same format and protocols. PPTP may be used only in IP networks, it requires a dedicated TCP connection for tunnel creation and usage. L2TP over IPSec[1] allows for the higher security level compared to PPTP and guarantees the higher level of protection for business-critical data.

Due to its characteristics, L2TP is an attractive protocol for building virtual networks.

– *Use VLAN in external network* – when checked, use VLAN identifier specified in 'VLAN ID' field for the Internet access.

  ▪ *VLAN ID* – VLAN identifier used for the service;
  ▪ *802.1P* – 802.1P marker (another name: *CoS – Class of Service*), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority).

  VLAN – virtual local area network. VLAN consist of a group of hosts combined into a single network regardless of their location. Devices grouped into a single VLAN will have the same VLAN-ID.

– *Disable source address transmission* – when checked, source address substitution of LAN packets is disabled (disables 'masquerading').

When you choose 'Bridge' operation mode, the following connection settings will become available:

– *Protocol* – select the protocol that will be used for device WAN interface connection to provider network:

  ▪ *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. When 'Static' type is selected, the following parameters will be available for editing:

    – *IP address* – specify device WAN interface IP address in the provider network;
    – *Subnet mask* – external subnet mask;
    – *Default gateway* – address that the packet will be sent to, when its route is not found in the routing table;
    – *Primary DNS, Secondary DNS* – domain name server addresses (allows identifying the IP address of the device by its domain name). You may leave these fields empty, if they are not required.

  ▪ *DHCP* – operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from

    – *Alternative Vendor ID (Option 60)* – when checked, the device transmits *Vendor ID (Option 60)* field value in Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted by DHCP messages.

      If the *Alternative Vendor ID (Option 60)* checkbox is not selected, the default value will be transmitted by Option 60 in the following format:

      [VENDOR:vendor**][DEVICE:**device type**][HW:**hard ware**] [SN:**serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**firmware version**]**

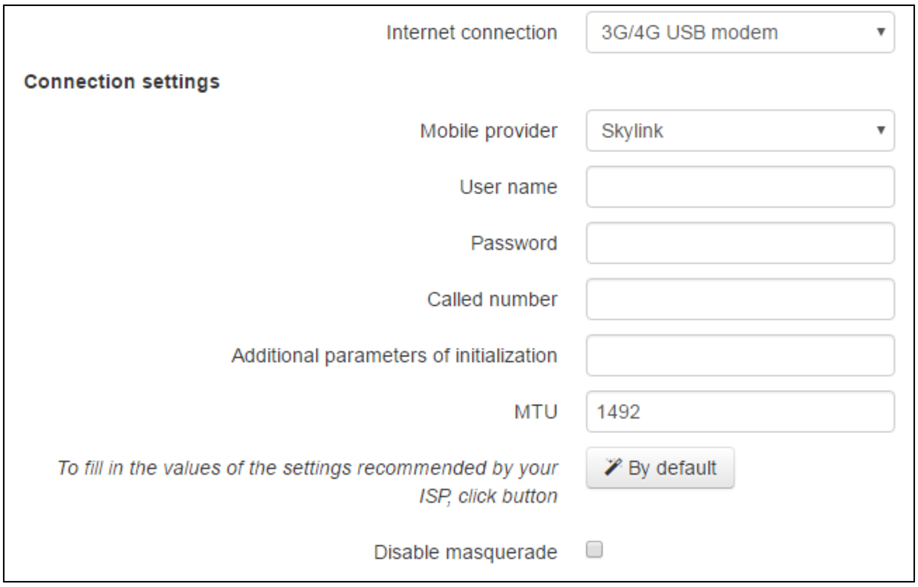
      Example:

[1] Disable transmitting the sender addresses for proper IPSec operation.

[VENDOR:Eltex][DEVICE:RG-5421G-Wac][HW:1.2][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.1.0]

- *Primary DNS, Secondary DNS* – DNS IP-addresses– if DNS addresses are not obtained automatically via DHCP, you should define them manually. Manually defined addresses will have a priority over DNS addresses obtained via DHCP.

2. When **'3G/4G USB modem'** connection method is selected, the following field will become available for configuration:



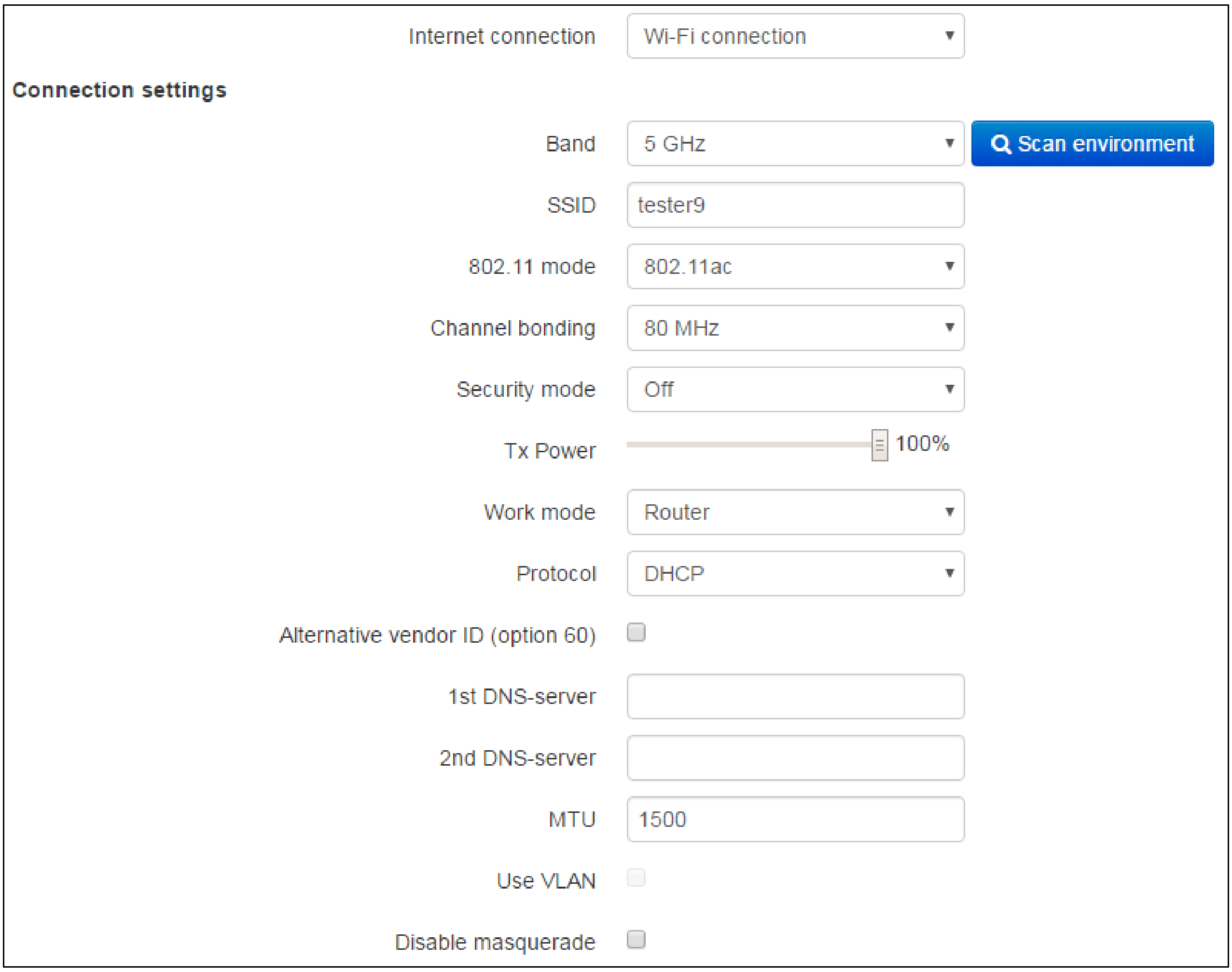
Internet connection	3G/4G USB modem ▾
Connection settings	
Mobile provider	Skylink ▾
User name	
Password	
Called number	
Additional parameters of initialization	
MTU	1492
To fill in the values of the settings recommended by your ISP, click button	By default
Disable masquerade	□

- *Mobile provider* – 3G/4G service provider name. You may select one of the six mobile service providers operating in Russian Federation (their settings are stored in the device memory): Megafon, Beeline, MTS, Skylink, Tele2, Yota. Click 'Default' button to fill in the connection settings with the selected service provider parameters. If the service provider settings in your region differ from the proposed ones, edit them accordingly..

  If your provider is missing from the list, select 'Other' and enter your service provider settings into fields;
- *Protocol* – this field is available only when 'Other' is selected in the mobile service providers list. For most cases, mobile service providers establish network access using PPPoE, however some modems may require DHCP for proper operation;
- *Username* – username used for authentication in the wireless network;
- *Password* – password used for authentication in the wireless network;
- *Called number* – dial-up number for wireless network connection (e.g. *99***1#);
- *Additional parameters* – parameters for wireless network connection (e.g. AT+CGDCONT=1,IP,internet—for Megafon); do not use quotation marks in this string;
- *MTU* – maximum block size for data transmitted via the network (1492 is recommended);
- *Disable source address transmission* – when selected, disable source address substitution for packets sent from LAN (disables 'masquerading').

'Default' button allows you to fill in the service provider settings with preconfigured values from the device memory, to free the user from searching for them in the Internet.

3. When **'Wi-Fi connection'** metod is selected, the following settings will be available:



Internet connection	Wi-Fi connection ▾
Connection settings	
Band	5 GHz ▾
SSID	tester9
802.11 mode	802.11ac ▾
Channel bonding	80 MHz ▾
Security mode	Off ▾
Tx Power	100%
Work mode	Router ▾
Protocol	DHCP ▾
Alternative vendor ID (option 60)	□
1st DNS-server	
2nd DNS-server	
MTU	1500
Use VLAN	□
Disable masquerade	□

– *Range* – selecting operation range: 2.4 GHz or 5 GHz;

✓ **When you use ‘Wi-Fi connection’ mode, a Wi-Fi access point will be not available in the selected range of connection.**

– *Network identifier (SSID)* – wireless network name used for connection to a device. Maximum name length is 32 characters with case-sensitive entering. This parameter may consist of digits, Latin letters, "-", "_", ".", "!", ";", "#" symbols and space, but "!", ";", "#" and space can’t be initial;
– *802.11 mode* – operation mode selection of wireless interface.

For 2.4 GHz:

- *802.11b* – if all wireless client support standard 802.11b (max data rate is 11 Mbps);
- *802.11bg* – if network has wireless clients with 802.11b and 802.11g support. Maximal data rate is 54 Mbps in accordance with 802.11g standard;
- *802.11bgn* – if wireless clients with support 802.11b, 802.11g and 802.11n are presence in network;
- *802.11n* – standard provides maximal data rate of 300 Mbps. 802.11n uses MIMO technology (several outputs and inputs), signal processing and intelligent antenna to transmit several data streams via several antennae. It provides fivefold increasing of performance and twofold increasing of range in contrast with previous 802.11g standard.

For 5 GHz:

- *802.11a* – maximal data rate is 54 Mbps;

  - *802.11n* – standard provides maximal data rate up to 300 Mbps. 802.11n uses MIMO technology (several outputs and inputs), signal processing and intelligent antenna to transmit several data streams via several antennae;
  - *802*.11ac – standard provides maximal data rate up to 866 Mbps. 802.11ac uses MIMO technology (several outputs and inputs), signal processing and intelligent antenna to transmit several data streams via several antennae;

- *Channel width* – width of channel frequency range, where Wi-Fi client works, possesses value of 20, 40 MHz and Wi-Fi client can work on 80 MHz frequency at 5GHz;
- *Security mode* – security mode selection of wireless network:
  - *Off* – wireless network encryption is disabled, low security level;
  - *WEP* – WEP encryption. WEP key consist of hexadecimal digits with length of 10 or 26 characters or should be string (a-z, A-Z, 0-9, ~!@#$%^&*()_-+= symbols) with length of 5 and 13 characters.
  - *WPA, WPA2* – WPA and WPA2 encryption. Key length is from 8 to 63 characters. You may use only symbols: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"`' or space. WPA and WPA2 encryption modes are recommended to use as the most secure at this time.
- *Signal power* – power control of Wi-Fi transmitter/receiver in % of max level;
- *Operation mode* – the device operation mode:
  - *Router* – router mode is established between LAN- and WAN interfaces ((Wi-Fi interface becomes WAN interface) LAN is isolated from WAN);
  - *Bridge* – wireless bridge mode is established for connected Wi-Fi network.
- *Protocol*– protocol selection for connection to provider service delivery network via Wi-Fi interface:
  - *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. When 'Static' type is selected, the following parameters will be available for editing:
    - *External device IP address* – specify device WAN interface IP address in the provider network;
    - *Subnet mask* – external subnet mask;
    - *Default gateway* – address that the packet will be sent to, when its route is not found in the routing table;
    - *Primary DNS, Secondary DNS* – domain name server addresses (allows you to identify the IP address of the device). You may leave these fields empty, if they are not required.
  - *DHCP* – operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from
    - *Alternative Vendor ID (Option 60)* – when checked, the device transmits *Vendor ID (Option 60)* field value by DHCP messages (in Option 60) (Vendor class ID). If the field is empty, Option 60 will not be transmitted by DHCP messages .

      If the *Alternative Vendor ID (Option 60)* checkbox is not selected, the default value will be transmitted by Option 60 in the following format:

      [VENDOR:vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:**serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**firmware version**]**

      Example:

      [VENDOR:Eltex][DEVICE:RG-5421G-W][HW:1.2][SN:VI23000118]
      [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.1.0]

  - *Primary DNS, Secondary DNS* – DNS server IP address – If DNS addresses are not assigned automatically via DHCP, you may difine it manually. Manually defined addresseses will have a priority over DNS addresses obtained via DHCP.

- *MTU size* – max size of frame transmitted via the network, 1492 is recommended value*;*
- *Disable source address transmission* – when selected, disable source address substitution for packets sent from LAN (disables 'masquerading')*.*

LAN:

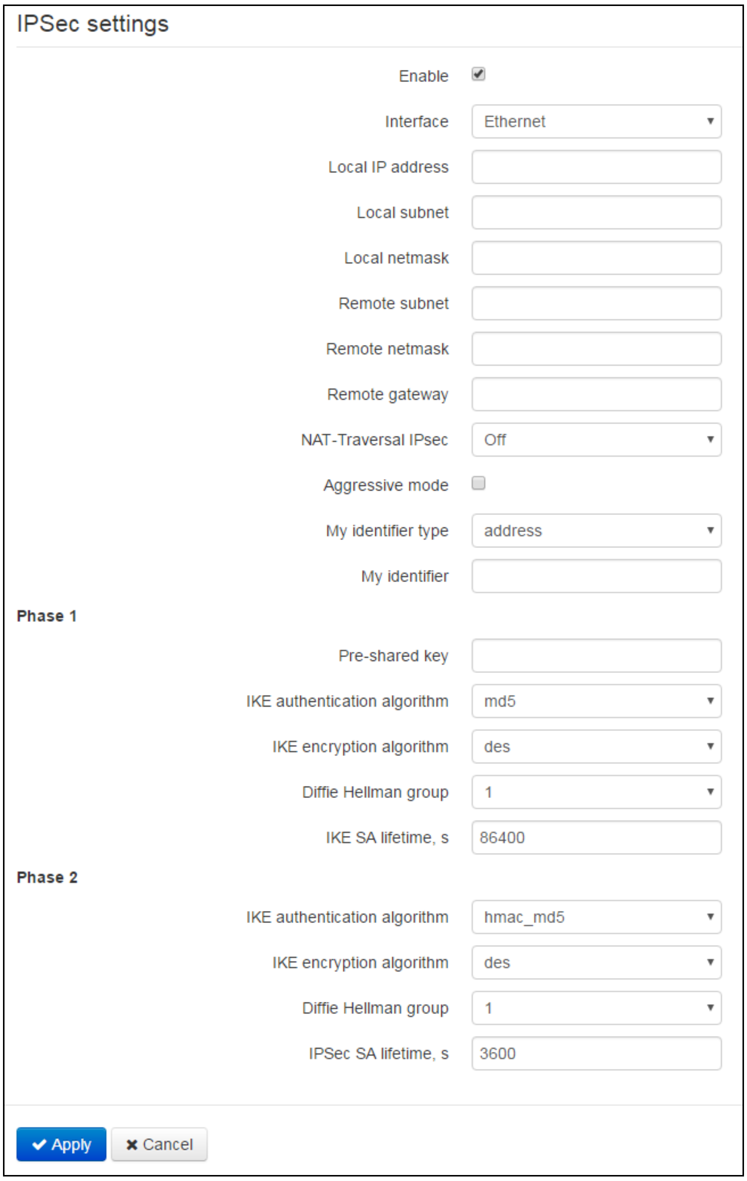
- *IP address of the device*– device IP address in LAN;
- *Subnet mask* – subnet mask in LAN.

✓ **If the local subnet address is changed, the local DHCP server address pool (Network—DHCP Server) will be changed automatically.**

IPSec configuration:

In this section, you may configure IPSec encryption (IP Security).

IPSec is a set of protocols used for protection of data transmitted via Internet Protocol that enables authentication, integrity check and/or encryption of IP packets. IPsec also includes secure Internet Key Exchange protocols.



IPSec settings

Enable	☑
Interface	Ethernet
Local IP address	
Local subnet	
Local netmask	
Remote subnet	
Remote netmask	
Remote gateway	
NAT-Traversal IPsec	Off
Aggressive mode	□
My identifier type	address
My identifier	
Phase 1	
Pre-shared key	
IKE authentication algorithm	md5
IKE encryption algorithm	des
Diffie Hellman group	1
IKE SA lifetime, s	86400
Phase 2	
IKE authentication algorithm	hmac_md5
IKE encryption algorithm	des
Diffie Hellman group	1
IPSec SA lifetime, s	3600

- *Enable* – enable IPSec protocol utilization for data encryption;
- *Interface* – this setting takes effect only when PPPoE, PPTP or L2TP are selected for the Internet, and defines the interface that will be accessed with IPSec: Ethernet (secondary access interface) or PPP (primary access interface). When DHCP or Static protocol is selected, there is only a single interface (Ethernet) active for the service that may be accessed with IPSec only.
- *Local IP address* – device address for operation via IPSec;
- *Local subnet address* in cooperation with *Local subnet mask* determine local subnet to create network-to-network or network-to-point topology;
- *Remote subnet address* in cooperation with *Remote subnet mask* define a remote subnet address used for IPSec-encrypted communication. If the mask value is 255.255.255.255, communication is performed with a single host. Mask that differs from 255.255.255.255 allows you to define a whole subnet. Thus, device features allow you to establish 4 network topologies that utilize IPSec traffic encryption: Point-to-Point, Network-to-Point, Point-to-Network, Network-to-Network;
- *Remote gateway* – gateway for access to remote subnet;
- *NAT-T mode* – NAT-T mode selection. NAT-T (NAT Traversal) encapsulates IPSec traffic and simultaneously creates UDP packets to be sent correctly by a NAT device. For this purpose, NAT-T adds an additional UDP header before IPSec packet so it would be processed as an ordinary UDP packet and the recipient host would not perform any integrity checks. When the packet

arrives to the destination, UDP header is removed and the packet goes further as an encapsulated IPSec packet. With NAT-T technique, you may establish communication between IPSec clients in secured networks and public IPSec hosts via firewalls. NAT-T operation modes::

- *on* – NAT-T mode is activated only when NAT is detected on the way to the destination host;
- *force* – use NAT-T in any case;
- *off* – disable NAT-T on connection establishment.

The following NAT settings are available:

- *NAT-T UDP port* – UDP port for packets for IPSec message encapsulation. Default value is 4500.
- *NAT-T keepalive packet transmission interval, sec* – treansmission interval of periodical messages to support active status of UDP connection on the device forming NAT functions.

- *Aggressive mode* – phase 1 operation mode when all the necessary information is exchanged using three unencrypted packets. In the main mode, the exchange process involves six unencrypted packets;
- *Identifier type* – identifier type of the device: address, fqdn, keyed, user_fqdn, asn1dn;
- *Identifier* – device identifier used for identification during phase 1 (fill in, if required). Identifier format depends on the type.

Phase 1. During the first step (phase), two hosts negotiate on the identification method, encryption algorithm, hash algorithm and Diffie Hellman group. Also, they identify each other. For phase 1, there are the following settings:

- *Pre-shared key* – a secret key used by authentication algorithm in phase 1. A string from 8 to 63 characters long;
- *Authantication algorithm* – selectan authentication algorithm from the list: MD5, SHA1;
- *Encryption algorithm* – select an encryption algorithm from the list: DES, 3DES, Blowfish;
- *Diffie-Hellman group* – Diffie-Hellman group selection;
- *Phase 1 lifetime, sec* – time that should pass for hosts' mutual re-identification and policy comparison (other name 'IKE SA lifetime'). Default value is 24 hours (86400 seconds).

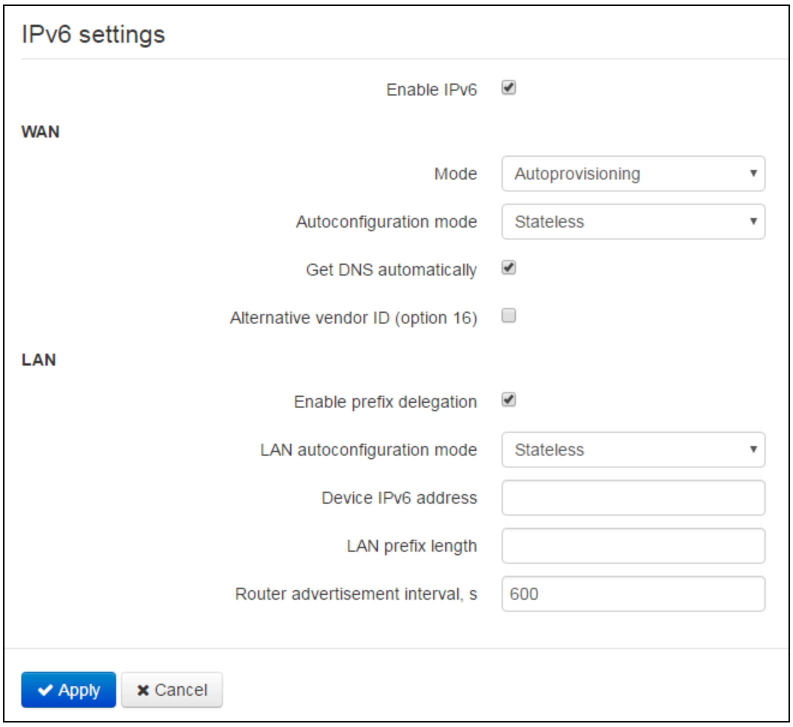
Phase 2. During the second step, key data is generated, hosts negotiate on the utilized policy. This mode—also called as 'quick mode'—differs from the phase 1 in that it may be established after the first step only, when all the phase 2 packets are encrypted.

- *Authantication algorithm* – select an authentication algorithm from the list: HMAC - MD5, HMAC-SHA1, DES, 3DES;
- *Encryption algorithm* – select an encryption algorithm from the list: DES, 3DES, Blowfish;
- *Diffie-Hellman group* –select Diffie-Hellman group;
- *Phase 2 life time, sec* – time that should pass for data encryption key changeover (other name 'IPSec SA lifetime'). Default value is 60 minutes (3600 seconds).

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.2.2 'IPv6' submenu

In the 'IPv6' submenu, you may configure the connection to the external nerwork and local network via IPv6 protocol.



IPv6 settings

Enable IPv6 ☑

WAN

Mode: Autoprovisioning

Autoconfiguration mode: Stateless

Get DNS automatically ☑

Alternative vendor ID (option 16) □

LAN

Enable prefix delegation ☑

LAN autoconfiguration mode: Stateless

Device IPv6 address:

LAN prefix length:

Router advertisement interval, s: 600

IPv6 settings

– *Enable IPv6* – allows you to enable or disable IPv6 protocol usage.

External network

– *Mode* – connection way of the device to external network:

  - *Static* – connection to Internet network via IPv6 protocol is perfomed by settings specified by user;
  - *Autoconfiguring* – Internet connection via IPv6 protocol is performed by settings received trough one of the autoconfiguration modes: SLAAC, Stateless, and Stateful.
  - *PPPoE* – Internet connection through IPv6 is established via PPP-session. To activate this mode, select PPPoE as connection protocol in the Internet settings.

Configuring connection to external network

1. When yoy select **'Static'** mode the following settings will be available:

– *External IPv6 device address* – static IPv6 device address providing access to Internet;
– *Prefix length* – analogue subnet mask in IPv4. It defines what kind of address part determines subnet and what determines host. The max length of prefix is 128. At present, 64 prefix is most in use 64;
– *IPv6 default gateway* – gateway IPv6 address used by default;
– *IPv6* primary DNS – IPv6 address of primary DNS;
– *IPv6* Secondary DNS – IPv6 address of secondary DNS.

2. When you select **'Autoconfiguration'** mode, the following settings will be available:

– *Autoconfiguration mode* – metod for receiving of the settings to connect the device to external network:

  - *SLAAC* – receiving of the IPv6 settings via 'Router Advertisement' messages of ICMPv6;

- *Stateless* – receiving of the IPv6 settings via 'Router Advertisement (RA)' message of ICMPv6 protocol, querying absent parameters via DHCPv6;
- *Stateful* – receiving the IPv6 settings via DHCPv6 protocol.

– *Get DNS addresses automatically* – method of getting the DNS addresses: automatically or manually (like 'Static' mode);

– *Alternative Vendor ID (Option 16)* – setting is equal to IPv4 setting (see section 3.6.2.1)/ It is available when 'Stateless' or 'Stateful' autoconfiguration modes are selected or when 'Permit prefix delegation' setting is available.

3. When you select **'PPPoE'** mode, the settings will be identical with **'Autoconfiguration'** mode.

Local network

– *Permit prefix delegation* – permit transmittion of subnet IPv6 addresses to local network hosts;

– *LAN autoconfiguration mode* – select method for receiving the settings to connect hosts to local network:

- *SLAAC* – receiving the IPv6 settings via 'Router Advertisement' messages of ICMPv6 protocol;
- *Stateless* – receiving the IPv6 settings via 'Router Advertisment (RA)' message of ICMPv6, querying of required parameters via DHCpv6;
- *Stateful* – receiving the IPv6 settings via DHCP protocol;
- *Off* – autoconfiguration is disabled, IPv6 network settings should be assigned on hosts manually.

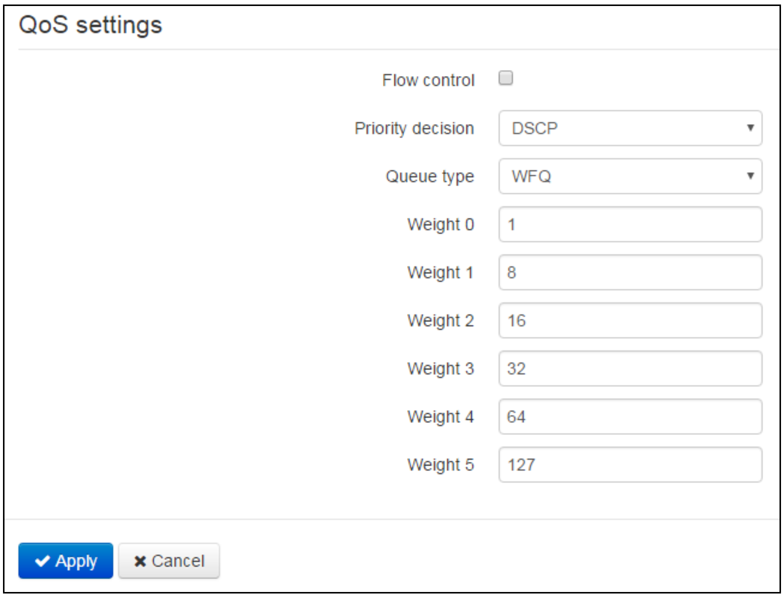
– *IPv6 device address* – IPv6 address of RG-5400 device in local network;

– *LAN prefix length* – define prefix length of local network;

– *Send interval of Router Advertisement, sec* – time interval when the device sends RA messages of ICMPv6 protocol with network settings for hosts.

3.7.2.3 'QoS' submenu

In the 'QoS' subnet, you may configure priority of traffic processing and queue type.



QoS settings

Flow control	□
Priority decision	DSCP
Queue type	WFQ
Weight 0	1
Weight 1	8
Weight 2	16
Weight 3	32
Weight 4	64
Weight 5	127

QoS configuration

- *Priority selection* – select method of traffic prioritization:
  - *DSCP* – classification mechanism of traffic control and providing quality of service by priorities ;
  - *802.1p* – attribute (*CoS – Class of Service*), established on outbound IP packets of the interface. Atribute takes value from 0 (low priority) to 7 (highest priority).
- *Stream control* – on/off control of speed with that determinate types of traffic streams are transmitted into a external network;
- *Queue type* – select service procedure of queues:

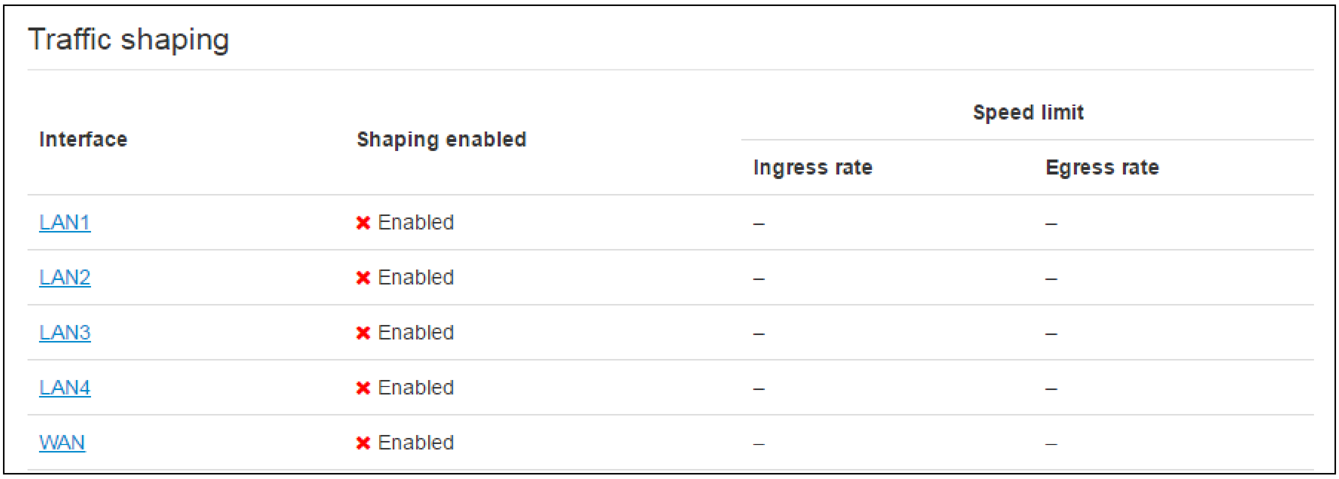
✓ **Settings of the priorities are not available when flow control is enabled.**

  - *Strict* – service procedure of queues when traffic with lowest priority is transmitted only after transmitting queues with higher priority;
  - *WRQ* – service procedure of queues, when accessible bandpass is devided among queues in propotion with priority.
- *0..5 priorities* – define priority weight in range from 1 to 127. Then weight is higher then traffic is more priority.

3.7.2.4 'Traffic shaping' submenu

In the 'Traffic shaping' submenu you may limit income and outcome traffic rate on which single wire and wireless interface and ctreate the restriction rules for traffic rate by membership characters of IP address, MAC address, VLAN, TCP/UDP port.

✓ **Speed limitation for data transmission via VLAN is currently not available for Wi-Fi.**

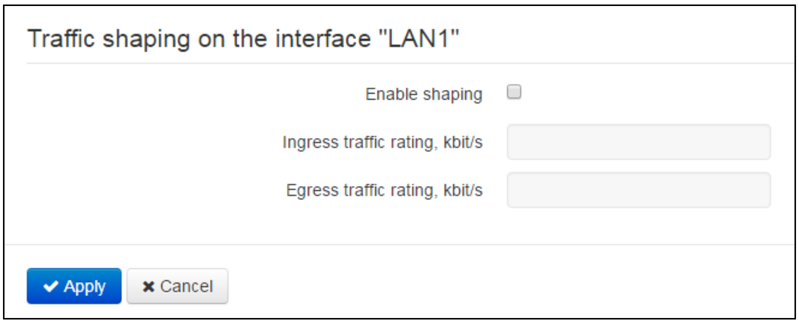


Traffic shaping

Interface	Shaping enabled	Speed limit	
		Ingress rate	Egress rate
LAN1	✗ Enabled	–	–
LAN2	✗ Enabled	–	–
LAN3	✗ Enabled	–	–
LAN4	✗ Enabled	–	–
WAN	✗ Enabled	–	–

Traffic shaping

The 'Traffic shaping' submenu is presented by table where status of shaping and values of maximum permissible data rates of inbound and outbound traffic are specified opposite to each interface.Click the interface name to proceed to settings of a desiered interface.



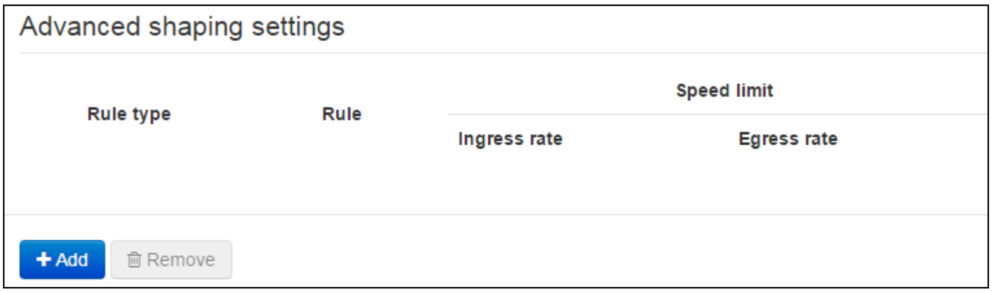
Traffic shaping on the interface "LAN1"

Enable shaping	□
Ingress traffic rating, kbit/s	
Egress traffic rating, kbit/s	

Traffic shaping on interface

– *Enable shaping* – when checked, rate limit of inbound and outbound traffic is enabled;
– *Inbound and outbound traffic limit, Kbps* – max rate of inbound/outbound traffic in the range of 0 to 1048576 kbps, speed variation of inbound traffic is 16 kbps, outbound – 64 kbps.

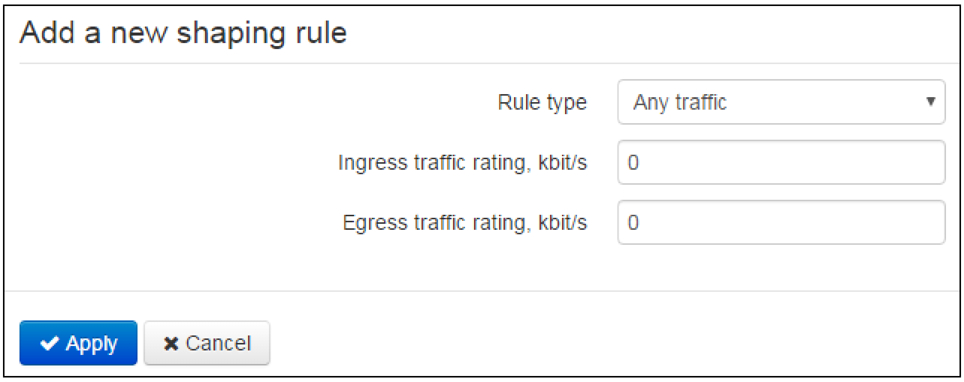
Advanced settings of shaping



Advanced shaping settings

Rule type	Rule	Speed limit	
		Ingress rate	Egress rate

To add a new rule for traffic shaping, click ‘Add’ button and fill in the following fields in the ‘Create new rule’ opened window:



Add a new shaping rule

Rule type: Any traffic

Ingress traffic rating, kbit/s: 0

Egress traffic rating, kbit/s: 0

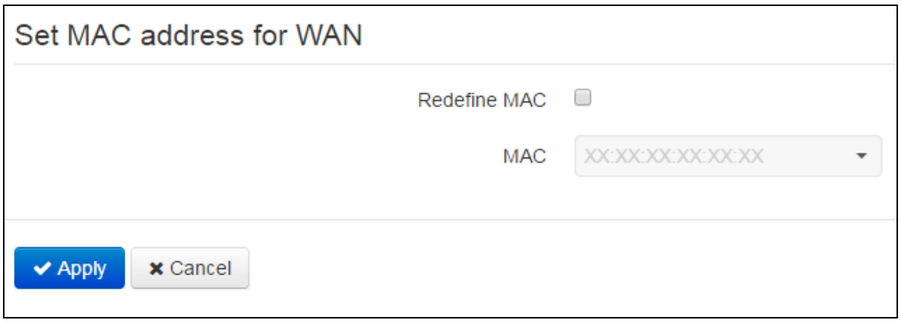
- *Rule type* – attribute for limitation of a data transmission rate:
  - By IP address – limitation of a traffic speed will be performed when source/destination address coincides with a specified IP address or address range;
  - By MAC address – limitation of a traffic speed will be performed when a client MAC-address coincides with the MAC-address specified in the rule;
  - By VLAN – limitation of traffic speed will be performed for traffic tagged by VLAN ID;
  - By port - traffic speed will be provided for specified ranges of the TCP/UDP ports of the traffic transmitter or receiver.
  - Any traffic – speed limitation for any traffic (always transmitted or received traffic) without additional attributes. This type of the rules has the lowest priority during creating the several rules;
- *Ingress traffic rating, kbps* – maximal required speed for ingress traffic corresponding to the rule;
- *Egress traffic rating, kbps* – maximal required speed for egress traffic corresponding to the rule;

Click ‘Apply’ button to add a new rule. To discard changes, click ‘Cancel’ button.

To delete rule from the list you should set flag opposite to corresponding record and click ‘Delete’ button.

3.7.2.5 'MAC address setting' submenu

In 'MAC address setting' submenu, you may change MAC address of the device WAN interface, MAC address of VoIP interfaces and VLAN control if their settings is different from Internet settings.



Set MAC address for WAN

Redefine MAC □

MAC XX:XX:XX:XX:XX:XX

- *Redefine MAC* – when checked, MAC address from MAC address field is used on Internet interface.

In the 'MAC' field, you may write the MAC address of the computer from which you are connected to the WEB configurator by clicking on the button of the drop-down menu. The function will be useful if your Internet-provider uses MAC address binding. In this case if you need to use the RG-5400 device as router you should assign MAC address of your computer to the device WAN interface. To do this, simply connect to the device WEB configurator via LAN interface and click 'Clone' button.

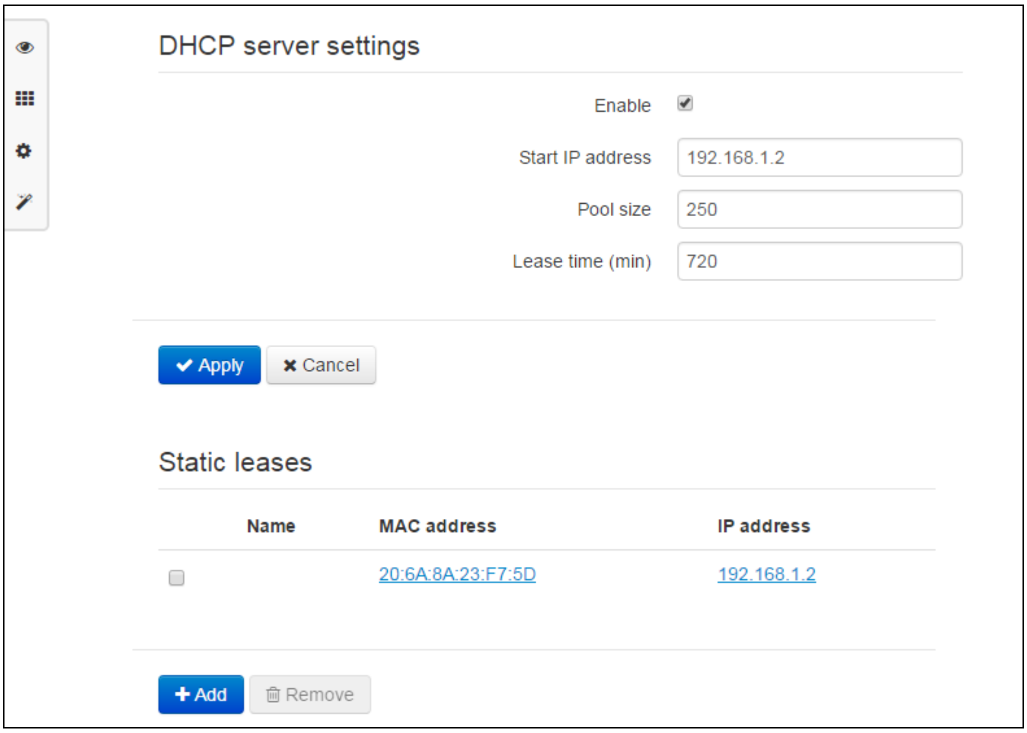
To redefine MAC on *'VoIP'* or *'VLAN control'* interfaces, use section of 'Configuring a MAC address on 'VoIP' interface' or 'Configuring a MAC address on *'VLAN control' interface'*.

To apply new configuration and store settings into non-vilatile memory click 'Apply' button. To discard changes, click 'Concele' button.

3.7.2.6 'DHCP server' submenu

In the DHCP server submenu, you may configure a local DHCP server and install static address bounds.

RG-5400 device – you may assign IP addresses and required parameters for Internet connection of computers connected to the LAN interface and wireless Wi-Fi access point (DHCP – Dynamic Host Configuration Protocol). Its usage allows you to avoid limitations of the TCP/IP manual settings.



DHCP server settings

Enable	☑
Start IP address	192.168.1.2
Pool size	250
Lease time (min)	720

Static leases

	Name	MAC address	IP address
□		20:6A:8A:23:F7:5D	192.168.1.2

<u>*DHCP server configuration*</u>

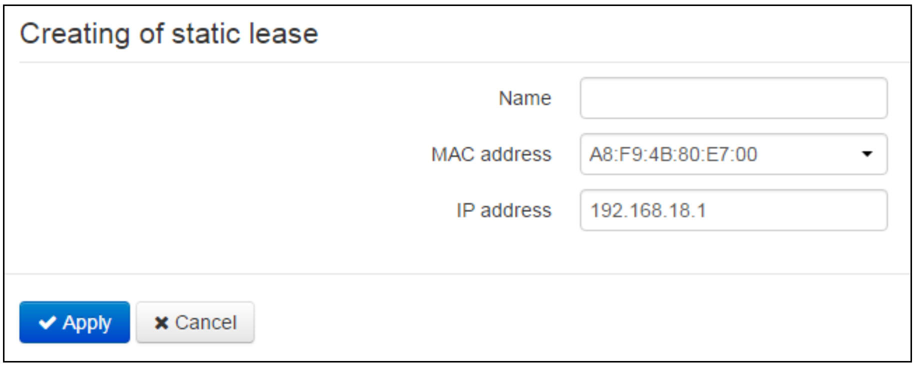
- *Enable* – when checked, enable local DHCP server;
- *Start IP address* – start address of IP address pool;
- *Address number* – address number in pool;
- *Lease time* – set max IP address usage time of connected device. Usage time is specified by server, in minutes.

To apply new configuration and store settings into non-vilatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

When you attempt to modify start value by value of another subnet (in relation to LAN interface) subnet pool will be set under current address value of local subnet automatically.

<u>*Static address bindings*</u>

To add new static binding click 'Add' button and fill in the following fields:



Creating of static lease

Name	
MAC address	A8:F9:4B:80:E7:00
IP address	192.168.18.1

- *Name* – set name of the static binding to separate bindings more simple;
- *MAC address* – set static MAC address. MAC address is assigned in the XX:XX:XX:XX:XX:XX format, also you can select MAC address of host now-connected to the device from dropdown menu;
- *IP address* – set static IP address for assigned MAC address.

Configuring the static bindings is effective if you need to assign determined IP address to desired computer connected to the device LAN interface.

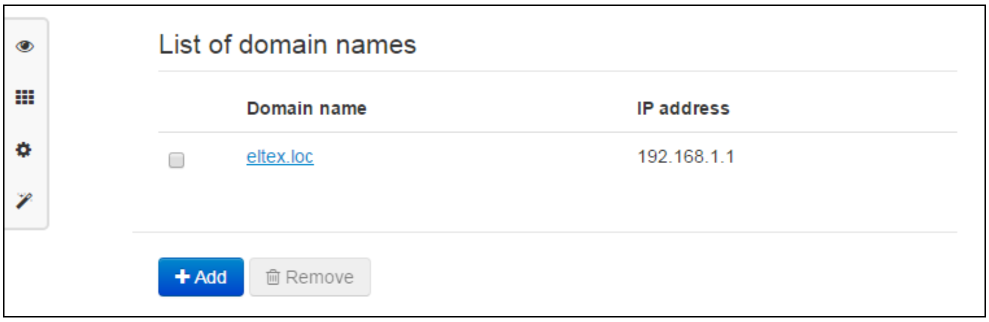
Click 'Apply' button to add IP address to the list of static IP addresses for DHCP server. To concel changes click 'Cancel' button.

To delete address from the list you should set flag opposite to corresponding record and click 'Delete' button.

3.7.2.7 'Local DNS' submenu

In 'Local DNS' submenu, you may configure local DNS server of the device by adding IP address couples (domain name) to the base.

Local DNS allows gateway to get IP address of cooperating device via its network name (host). You may use local DNS in cases when DNS server is missing from the network segment that the gateway belongs to, and you need to establish routing using network names, or when you have to use SIP server network name as its address. Although, you have to know matches between hostnames (hosts) and their IP addresses.

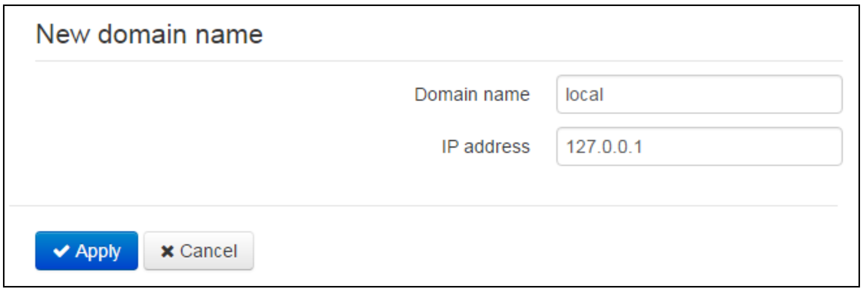


List of domain names

	Domain name	IP address
□	eltex.loc	192.168.1.1

3.7.2.8 Host configuration

To add the address into the list, click *'Add'* button in the 'Create match' window and fill in the following fields:


New domain name

Domain name: local

IP address: 127.0.0.1

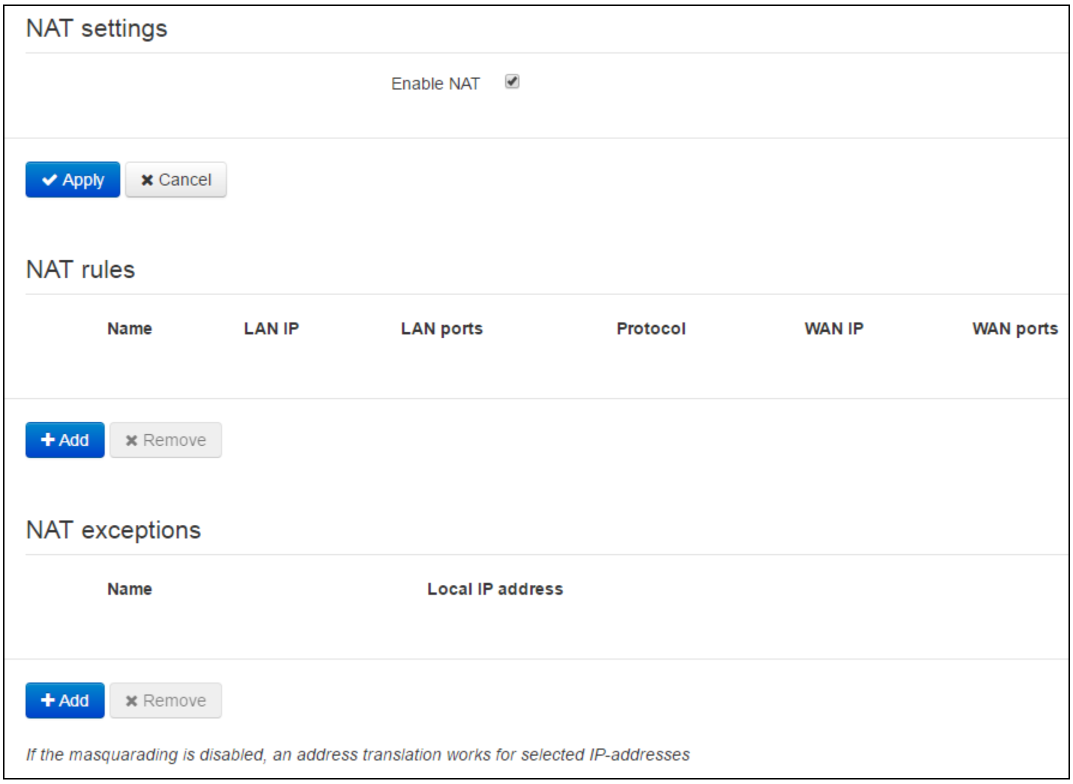
- *Domain name* – host name;
- *IP address* – host IP address.

Click ‘Apply’ button to create ‘IP address - domain name’ pair. To discard changes, click ‘Cancel’ To remove the record from the list, select the checkbox next to the respective record and click *'Delete'*.

3.7.2.9 'NAT and port forwarding' submenu

In the 'NAT and port forwarding' submenu, you may configure port forwarding from WAN interface to LAN interface. This submenu is available only when the Internet service is configured in the router mode.

NAT (Network Address Translation) allows for IP packet address and network port translation. Port forwarding is required when TCP/UDP connection to a local computer (connected to LAN interface) is established from the external network. In this settings menu, you may define the rules allowing packets to pass from the external network to the specified address in the local network and thus enabling connection. In general, port forwarding is necessary for torrent and P2P service operation. For this purpose, you should identify TCP/UDP ports used by a torrent or P2P client in their settings and assign the respective forwarding rules for your computer IP address.



NAT settings

Enable NAT ☑

NAT rules

Name	LAN IP	LAN ports	Protocol	WAN IP	WAN ports

NAT exceptions

Name	Local IP address

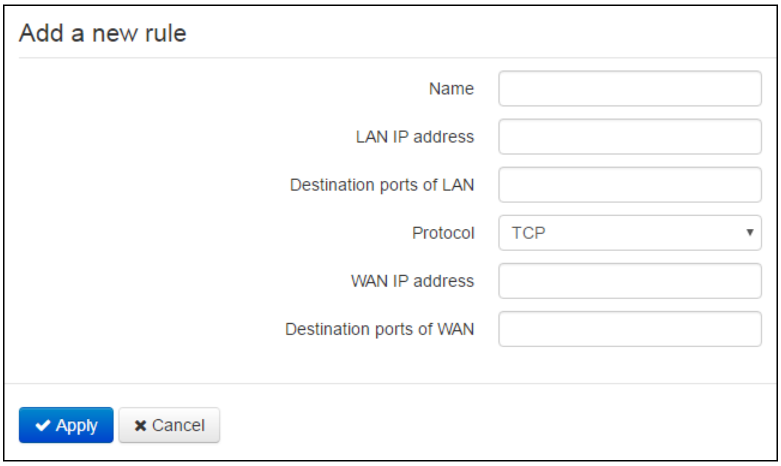
If the masquarading is disabled, an address translation works for selected IP-addresses

NAT configuration

– *Enable NAT* – setting permit/forbid usage of network address translation.

NAT rules

To add new NAT rule click *'Add'* button and fill in the following fields in the opening *'Add a new rule'* window:



Add a new rule

Name	
LAN IP address	
Destination ports of LAN	
Protocol	TCP
WAN IP address	
Destination ports of WAN	

- *Name* – rule name (this field is mandatory);
- *LAN packet destination IP address* – IP address of the host in LAN used for packet translation falling under this rule;
- *LAN destination ports* – recipient TCP/UDP port values that will be used for packet translation into LAN (a single port or port range delimited by '-' is permitted);
- *Protocol* – select packet protocol falling under this rule: TCP, UDP, TCP/UDP;
- *IP address of WAN packet source* – source IP address that sends packets into external networks falling under this rule;
- *WAN desrtinatioin ports* – recipient TCP/UDP port values in the external network that cause the packet to fall under this rule (a single port or port range delimited by '-' is permitted).

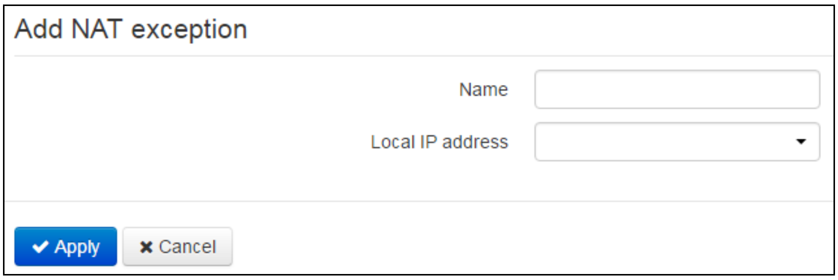
Port forwarding rule will work as follows: For the packet that comes to device WAN interface address via *'Protocol'* to the port from *'WAN ports'* range and has a '*WAN IP address'* source address (if this parameter is empty, source address will not be analyzed), its destination address and port are substituted with values from *'LAN IP address'* and *'LAN ports'* fields.

Click 'Apply' button to add a new rule. To discard changes, click *'Cancel'* button .

To delete the rule from the list, select the checkbox next to the respective record and click 'Delete'

NAT exceptions

To add a new NAT exception click 'Add' button and fill in the following fields in the 'Create NAT exception' opened window:



Add NAT exception

Name	
Local IP address	

- *Name* – exception name;
- Local IP-address – client IP-address for that NAT is not available.

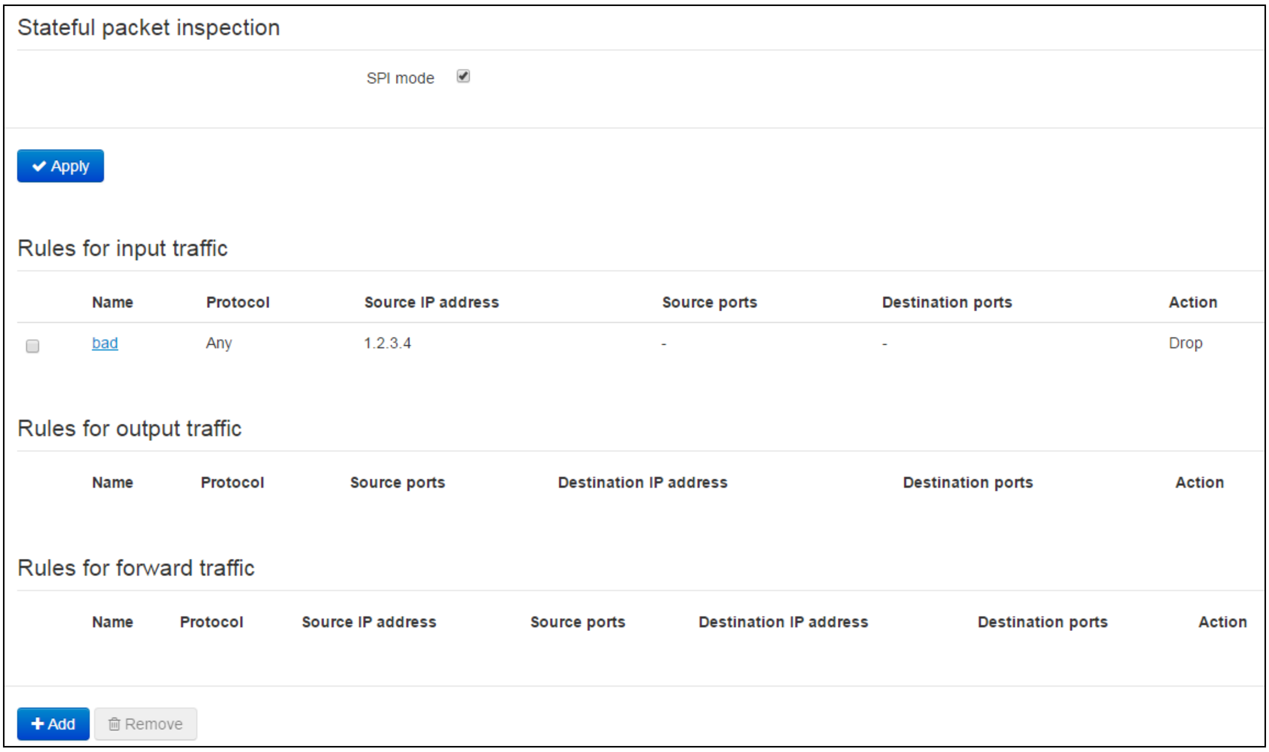
Click 'Apply' button to add a new rule. To cancel changes click 'Cancel' button.

To delete rule from the list you should set the flag opposite to corresponding record and click 'Delete' button.

✓ **If masquerading is disabled on the device this exception enables NAT for the specified client.**

3.7.2.10 'Firewall' submenu

In the 'Firewall' submenu, you may set the rules for the incoming, outgoing, and transit traffic transmission. You may restrict transmission of various traffic types (incoming, outgoing, transit) depending on the protocol, source and destination IP addresses, source and destination TCP/UDP ports (for TCP or UDP messages), ICMP message type (for ICMP messages).



Stateful packet inspection

SPI mode ☑

Rules for input traffic

	Name	Protocol	Source IP address	Source ports	Destination ports	Action
□	bad	Any	1.2.3.4	-	-	Drop

Rules for output traffic

Name	Protocol	Source ports	Destination IP address	Destination ports	Action

Rules for forward traffic

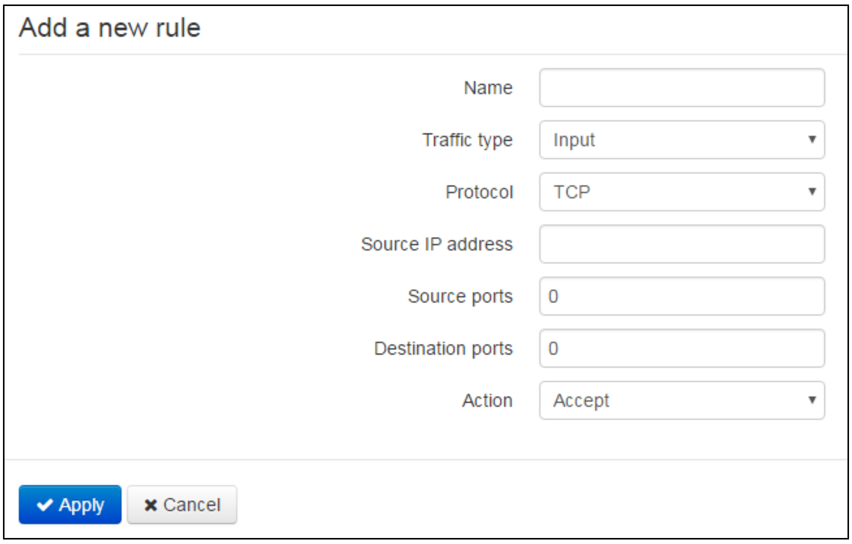
Name	Protocol	Source IP address	Source ports	Destination IP address	Destination ports	Action

Inspection of the packets with status saving

Use the section to enable/disable inspection of the packets with status saving (SPI).

Configuration of firewall rules

To add a new rule, click *'Add'* button and fill in the following fields in the 'Add a new rule' window:



Add a new rule

Name	
Traffic type	Input
Protocol	TCP
Source IP address	
Source ports	0
Destination ports	0
Action	Accept

- *Name* – rule name;
- *Traffic type* – select the traffic type that will fall under this rule:
  - *Input* – incoming device traffic (recipient is one of the device network interfaces). When this traffic type is chosen, the following fields will become available:

    Source address – specify start IP address of source. Use '/' symbol to define a mask in 'xxx.xxx.xxx.xxx' or 'xx' format, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0, when you need to highlight an address range (/24 mask record corresponds to /255.255.255.0);
  - *Outgoing* – outgoing device traffic (traffic generated locally by the device from one of the network interfaces). When this traffic type is chosen, the following fields will become available:
    - *Destination address* – define destination IP address. Use '/' symbol to define a mask in 'xxx.xxx.xxx.xxx' or 'xx' format, e.g. 192.168.18.0/24 or 192.168.18.0/255.255.255.0, when you need to highlight an address range;
  - *Transit* – transit traffic (traffic being transferred between two network interfaces when the source and destination are external devices). When this traffic type is chosen, the following fields will become available:
    - *Source address* – define source IP address. Use '/' symbol to define a mask in 'xxx.xxx.xxx.xxx' or 'xx' format, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0, when you need to highlight an address range;
    - *Destination address* – define destination IP address. Use '/' symbol to define a mask in 'xxx.xxx.xxx.xxx' or 'xx' format, e.g. 192.168.18.0/24 or 192.168.18.0/255.255.255.0, when you need to highlight an address range;
- *Prortocol* – packet protocol that will fall under this rule: TCP, UDP, TCP/UDP, ICMP, any.
- *Action* – action to be performed on packets (reject/skip).

When TCP, UDP, TCP/UDP are selected, the following settings will become available for editing:

- *Source ports* – list of source ports tat will fall under the rule (a single port or port range delimited by '-' is permitted); to specify all ports enter ‘0-65535’ rang;
- *Destination ports* – list of destination ports that will fall under the rule (a single port or port range delimited by '-' is permitted) to specify all ports enter ‘0-65535’ rang.

When ICMP protocol is selected, the following settings will become available for editing:

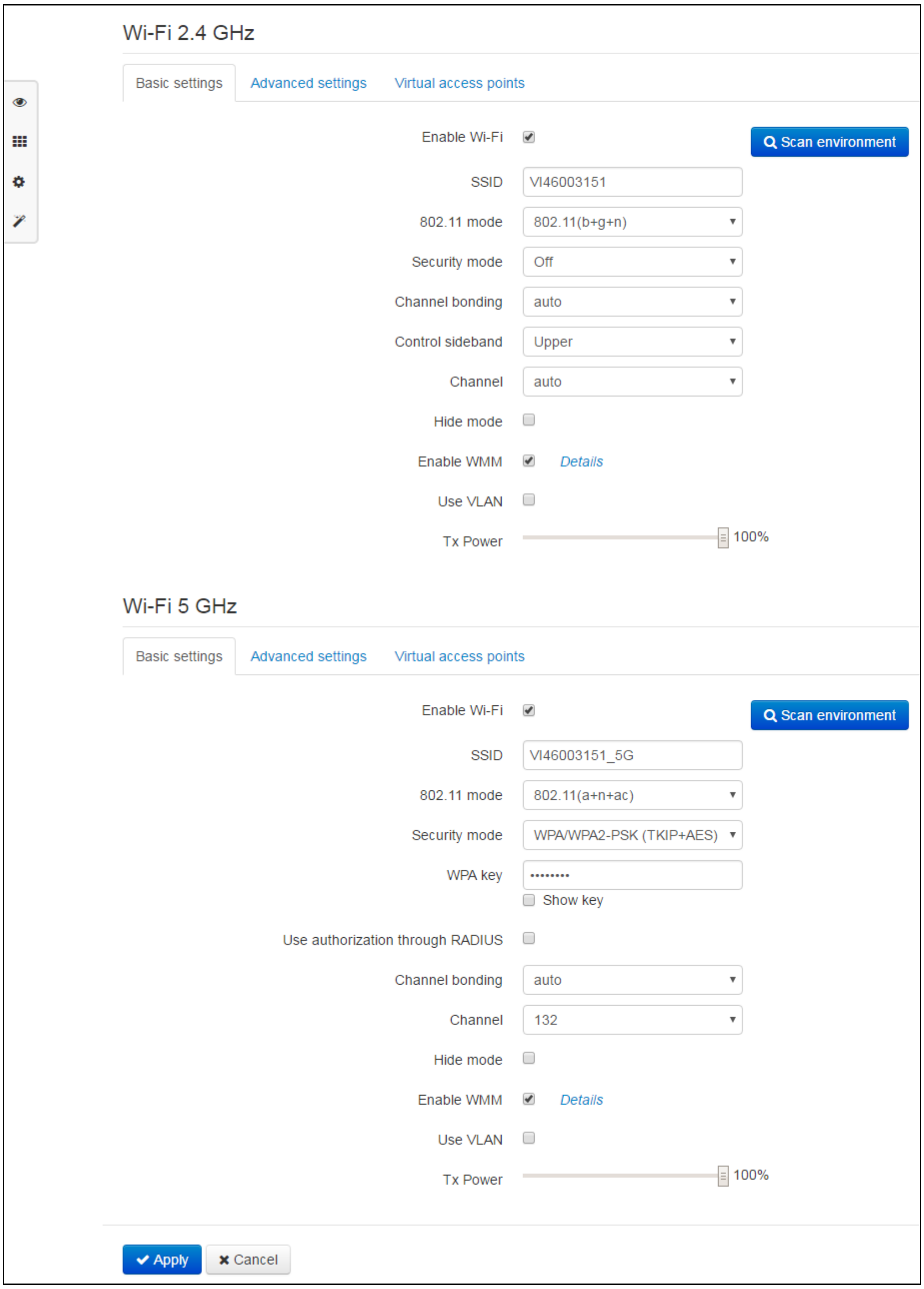
– *Message type* – you may create a rule for the specific ICMP message type only or for all ICMP message types.

Click 'Apply' button to add a new rule. To discard changes, click *'Cancel'* button. To remove the record from the list, select the checkbox next to the respective record and click 'Delete'.

3.7.2.11 'Wi-Fi' submenu

In 'Wi-Fi' submenu, you may configure Wi-Fi network. Wi-Fi configuration is performed on 2.4 GHz and 5 GHz. The device supports simultaneous operation in two frequency ranges.

All settings are devided into the basic settings, extra settings and virtual access points.



Wi-Fi 2.4 GHz

Enable Wi-Fi ☑

SSID: VI46003151

802.11 mode: 802.11(b+g+n)

Security mode: Off

Channel bonding: auto

Control sideband: Upper

Channel: auto

Hide mode □

Enable WMM ☑

Use VLAN □

Tx Power: 100%

Wi-Fi 5 GHz

Enable Wi-Fi ☑

SSID: VI46003151_5G

802.11 mode: 802.11(a+n+ac)

Security mode: WPA/WPA2-PSK (TKIP+AES)

WPA key: ••••••••

□ Show key

Use authorization through RADIUS □

Channel bonding: auto

Channel: 132

Hide mode □

Enable WMM ☑

Use VLAN □

Tx Power: 100%

Key settings

- *Enable Wi-Fi* – when checked, wireless access point is enabled in corresponding frequency range;
- *Network identifier (SSID)* – wireless network name used to connect to the device. Max name of length is 32 characters. The parameter may consist of digits, Latin letters and "-", "_", ".", "!", ";", "#" symbols but "!", ";", "#" symbols can't be placed first;
- *802.11* mode – operation mode of a wireless interface .

  For 2.4 GHz:
  - *802.11b* – if all wireless client support standard 802.11b (max data rate is 11 Mbps);
  - *802.11bg* – if network has wireless clients with 802.11b and 802.11g support. Maximal data rate is 54 Mbps in accordance with 802.11g standard;
  - *802.11bgn* – if wireless clients with support 802.11b, 802.11g and 802.11n are presence in network;
  - *802.11n* – standard provides maximal data rate of 300 Mbps. 802.11n uses MIMO technology (several outputs and inputs), signal processing and intelligent antenna to transmit several data streams via several antennae. It provides fivefold increasing of performance and twofold increasing of range in contrast with previous 802.11g standard.

  For 5 GHz
  - *802.11a* – maximal data rate is 54 Mbps;
  - *802.11n* – standard provides maximal data rate up to 300 Mbps. 802.11n uses MIMO technology (several outputs and inputs), signal processing and intelligent antenna to transmit several data streams via several antennae;
  - *802.11ac* – standard provides maximal data rate up to 866 Mbps. 802.11ac uses MIMO technology (several outputs and inputs), signal processing and intelligent antenna to transmit several data streams via several antennae.
  - *802.11(a+n)* – if network has wireless clients with suppor of 802.11a and 802.11n;
  - *802.11(n+ac)* – if network has wireless clients with suppor of 802.11n and 802.11ac;
  - *802.11(a+n+ac)* – if network has wireless clients with suppor of 802.11a, 802.11n and 802.11ac.
- *Security mode* – security mode selection of wireless network:
  - *Off* – wireless network encryption is disabled, low security level;
  - *WEP* – WEP encryption. WEP key consist of hexadecimal digits with length of 10 or 26 characters or should be string (a-z, A-Z, 0-9, ~!@#$%^&*()_-+= symbols) with length of 5 or 13 characters.
  - *WPA, WPA2* – WPA and WPA2 encryption. Key length is from 8 to 63 characters. You may use only symbols: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"`' or space. WPA and WPA2 encryption modes are recommended to use as the most secure at this time.

✓ **WPA and WPA2 with AES encryption are recommended as the more secure.**

- *Use authorization via RADIUS* – enable authorization on the RADIUS-server and accounting trough RADIUS;
- *Channel width* – frequency bandwidth, where wireless access point works, takes values auto, 20, 40 and 80 MHz (only for 5 GHz);
- *Main channel* – main channel of access point. Setting is available when channel width is 40 MHz. In this case total channel is formed from two 20 MHz adjacent channels. Selecting a main channel is defined regarding location of additional channel:
  - Upper – frequency of main channel is higher then frequency of additional channel;
  - Lower – frequency of main channel is lower then frequency of additional channel.

- *Channel* – number of channel for wireless network operation. When you select 'auto' value, channel with the lower noise level will be determined automatically;
- *Stealth mode* – when checked, access point will be concealed in the air. You are able to connect to the access point only if you know its SSID;
- *Enable WMM* – when checked, WiFi Multimedia function is enabled. This function allows you to optimize transmission of multimedia traffic via wireless environment;
- *Use VLAN* – when checked, access point starts to operate in the bridge mode and to tag traffic in accordance with a specified VLAN ID;
- *Signal power* – signal power adjustment of access point in percent of max level.

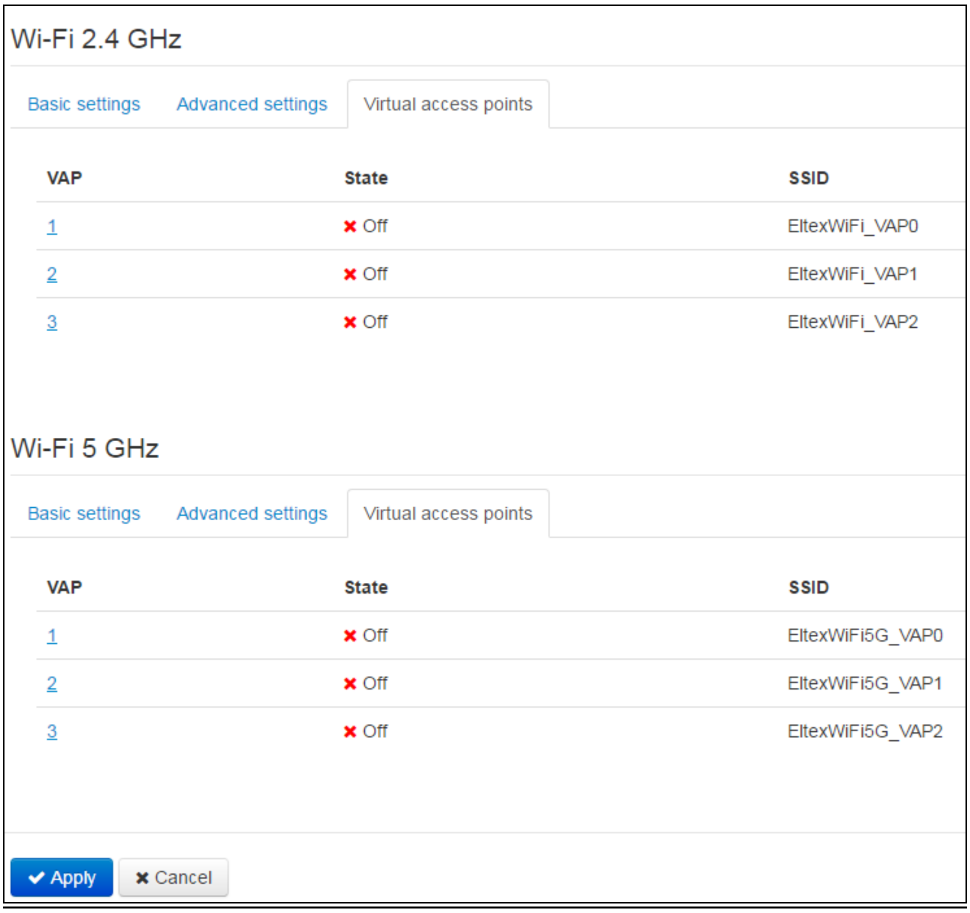
Additional settings

- *Fragmentation Threshold* – maximal size of continuous data block for its transmission via wireless network. The data of larger size will divided into parts — fragmented; takes values from 256 to 2346;
- *RTS Threshold* – maximal requested size of data for transmission. In CSMA/CA technology RTS packets (request to send) are sent to the base station before transmission of real data. If a free window is available, the base responds with CTS packet (clear to send) and the client sends the packet of requested size. The less RTS size is, the more is the probability to receive permission from base station, the quicker is the network recovery after collisions, but the less is the performance of the network as a whole. Takes values from 0 to 2347;
- *Beacon Interval, ms* – time interval between service messages (beaconing) in wireless network. Service messages transmit parameters of frequencies, protocols, safety, transmitted powers, delays etc. Takes values from 20 to 1024;
- *Preample Length* – preamble size shows the length of command box in each packet. Long preamble consists of 128 bits, Short preamble consists of 56 bits. Short preamble increases general system performance, is used for multimedia applications;
- *Enable IAPP* – IAPP protocol (Inter-Access Point Protocol) allows you to use roaming of clients between multiple access points within one network segment;
- *Wi-Fi Protection* – is a special mechanism for 802.11 b/g networks. Activation of the mechanism secures the performance of slow devices of b standard in the media with multiple high-speed devices of g standard. It is reached by increase of service time of old clients, assigning lower RTS window for them, decreasing general network performance;
- *Aggregation* – includes possibility of unifying some little packets for transmission in one big packet;
- *Short GI* – mean of decrease errors by interaction of radio devices — empty interval between transmitted sixteen-digit symbols (0,1,...E,F). Standard long guard interval (Long GI) lasts 800ns. It is considered that a signal approaches the receiver during the time considering all delays and reflections. Upon expiration of this interval, the next symbol is transmitted. Short GI lasts 400ns. Use of short GI increases general wireless network performance by approximately 11%, but leads sometimes to increase of transmission/receiving errors;
- *WLAN Partition* – activation of restriction to interact for wireless clients with each other;
- *Enable STBC* – activation of Space Time Block Coding (STBC) mechanism, is used in wireless networks for transmission of data flow copies via multiple aerials and for securing receipt of different versions of data block for increase of data exchange durability. It is known that radio signal is spread in the media according to complex traces and exposed to reflection, refraction, dissemination, as well as aberration through heat noise of the receiver, which finally leads to the situation when one copies of transmitted signal may occur as sufficiently better (less distorted) than the others. This redundancy increases probability to decode the signal correctly from some of its copies at receiving side. STBC technology unites all copies of received data block optimally for retrieval maximal information from each of them.
- *20/40MHz Coexist* – activated option leads to the situation when if other points at analogous frequency channels are detected in the range of our point of access or all channels are heavily loaded – our point of access deactivates use of 40MHz frequency range, to avoid disturbance;

– *Beamforming* – a technology, providing formation of electromagnetic fields of basic station aerial in far-filed region as narrow-band remote lobe, directed to subscriber device with possibility of change of directed features by change in position of this equipment.

Virtual access points

In one frequency range, you can create up to 3 virtual access points with all the specific settings. To enable and edit VAP parameters, click VAP numerical order in the required range.



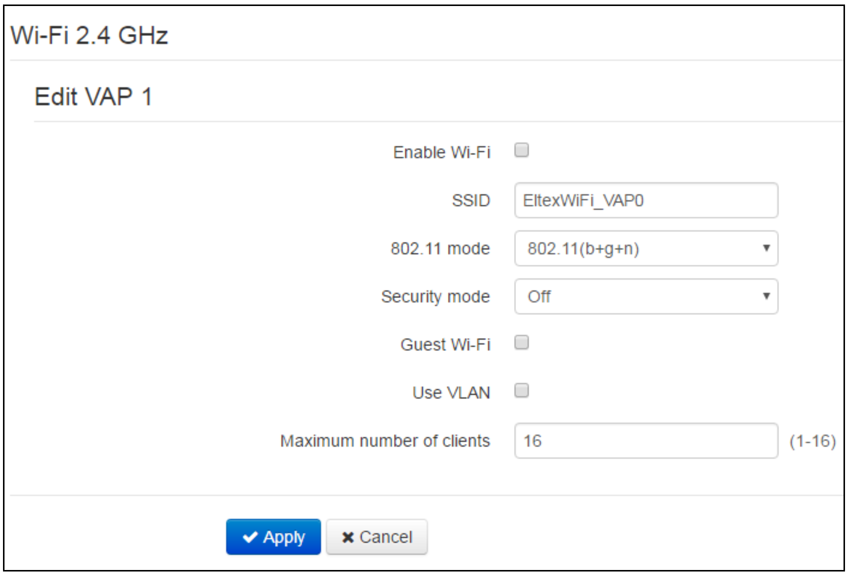
Wi-Fi 2.4 GHz

VAP	State	SSID
1	✖ Off	EltexWiFi_VAP0
2	✖ Off	EltexWiFi_VAP1
3	✖ Off	EltexWiFi_VAP2

Wi-Fi 5 GHz

VAP	State	SSID
1	✖ Off	EltexWiFi5G_VAP0
2	✖ Off	EltexWiFi5G_VAP1
3	✖ Off	EltexWiFi5G_VAP2

Enabling and editing VAP parameters.



Wi-Fi 2.4 GHz

Edit VAP 1

Enable Wi-Fi	□
SSID	EltexWiFi_VAP0
802.11 mode	802.11(b+g+n)
Security mode	Off
Guest Wi-Fi	□
Use VLAN	□
Maximum number of clients	16 (1-16)

- *Enable Wi-Fi* – activate this VAP;
- *SSID parameters, mode, security mode, guest Wi-Fi, use VLAN and maximum number of clients are similar to parameters of the key access point.*

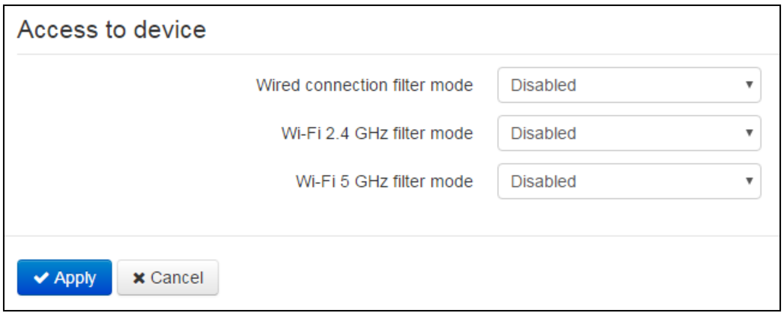
To apply new configuration and store settings into non-voletile memory, click *'Apply'* button. To discard changes, click 'Cancel' button.

If the device operates in two frequency ranges ('Wi-Fi 2.4 GHz' and 'Wi-Fi 5 GHz' are enabled simuilteniously) – max data transmission rate for each frequency range will be reduced as a result of MIMO technology disabling.

To apply new configuration and store settings into non-voletile memory, click *'Apply'* button. To discard changes, click 'Cancel' button.

3.7.2.12 'MAC filter' submenu

In the 'MAC filter' submenu, you may configure access filtering and Internet access by MAC address.



Access to device

Wired connection filter mode: Disabled

Wi-Fi 2.4 GHz filter mode: Disabled

Wi-Fi 5 GHz filter mode: Disabled

Access restriction settings

- *Mode of wired network filter* — defines policy of access to the device via WAN and LAN interfaces;
- *Wi-Fi 2.4/5 GHz filter mode* – determines one from three filter operation algorithm in dependence on client's MAC address:
  - *Disable* – filtration by MAC addresses is disabled – all clients may connect to access point;
  - *Black list* – in this filter operation mode, clients with MAC addresses from the 'MAC address list' are denied to connect to the access point (AP). Subscribers with unlisted MAC addresses are allowed to connect to the AP;
  - *White list* – in this filter operation mode, clients with MAC addresses from the 'MAC address list' are allowed to connect to the access point. Subscribers with unlisted MAC addresses are denied to connect to the AP.

MAC Address List

MAC address list is assigned to wired interface and eash frequency range independently. You may enter up to 30 client MAC addresses which may access the device in accordance to the specified filtering mode.

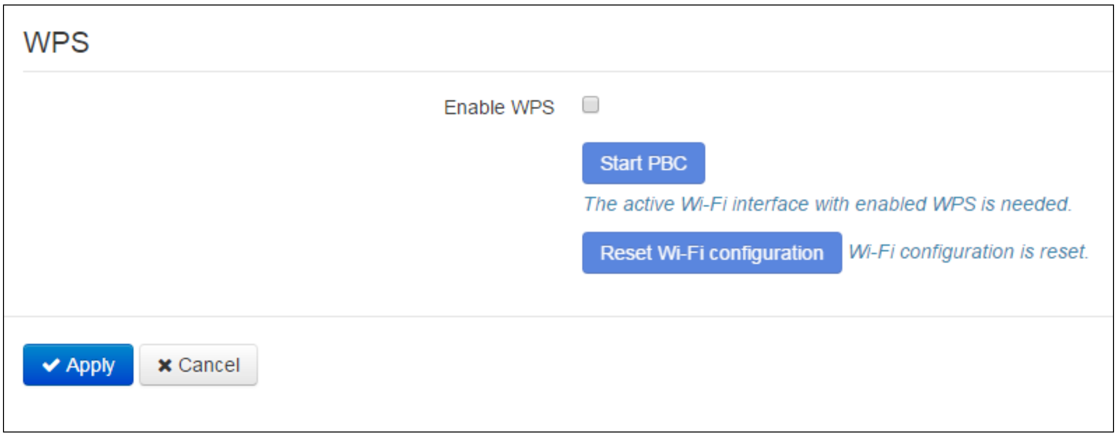
To add a new client to the list, click *'Add'* button and enter its MAC address or select MAC address of host connected to a wireless network.

To apply a new configuration and store settings into the flash memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

3.7.2.13 'WPS' submenu

WPS protocol (Wi-Fi Protected Setup) is set in «WPS» submenu.

WPS – standard of semi-automated generation of Wi-Fi wireless network. The purpose of WPS protocol is simplification of wireless network setting. WPS assigns the name of the network automatically and assigns encryption for protection from unsanctioned access to the network there is no need to assign all parameters manually.



The active Wi-Fi interface with enabled WPS is needed.

Wi-Fi configuration is reset.

WPS function may be deactivated for each frequency range separately.

Using WPS terms, the device can have two statuses:

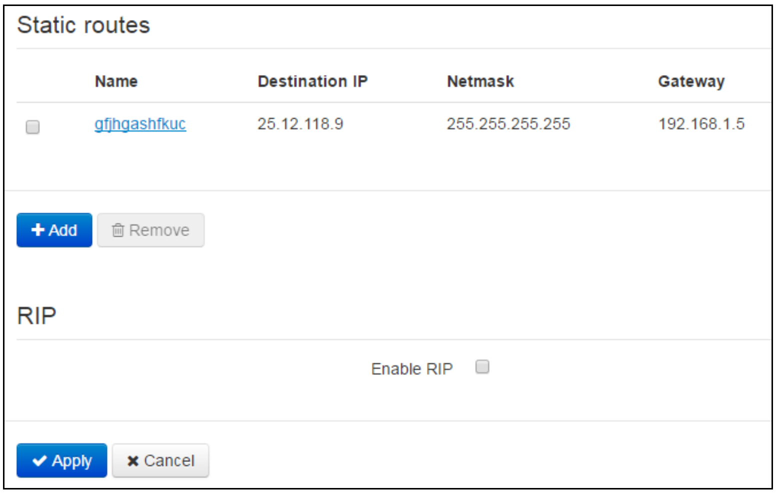
- *Configured* – access point (at least for one frequency range) is configured – it means that network name encryption parameters and other parameters are set;
- *Unconfigured* – access point in both frequency ranges is not configured – it means that all Wi-Fi parameters have default settings.

Depending on access point status some WPS functions may be blocked.

- *Deactivate WPS* – when checked, WPS can be used to autoconfigure wireless network. WPS function will be activated at both selected ranges immediately. WPS function cannot be enabled if WEP or WPA encryption mode is configured at least one frequency range.
- *Start PBC* – plays the role of WPS on casing of the device. Connection of the client is automatically after pushing the button. Connection of the client via PBC button is possible both from «Unconfigured» status (access point is not configured), and from «Configured» status (access point is configured). When connecting from «Configured» status the client receives the network name and encryption parameters set on the device. When connecting from «Unconfigured» status, the device generates and assigns network name and encryption parameters for the client automatically. After pushing PBC button, WPS function is active within two minutes.
- *Reset configuration* – for forced translating the access point from 'Configured' status to 'Unconfigured' status click 'Reset configuration' button (Wi-Fi settings will be established by default).To apply a new configuration and store settings into the flash memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

3.7.2.14 'Static Routes' submenu

In the 'Routing' submenu, you may configure device static routes.


Static routes

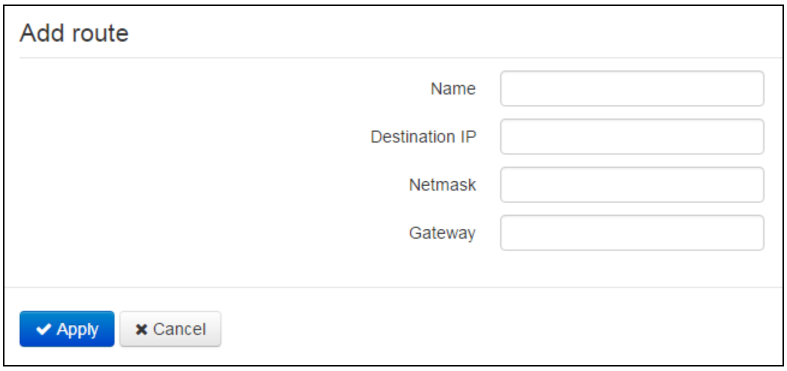
	Name	Destination IP	Netmask	Gateway
□	gfjhgashfkuc	25.12.118.9	255.255.255.255	192.168.1.5

RIP

Enable RIP □

Routing

To add a new route, click *'Add'* button and fill in the following fields:

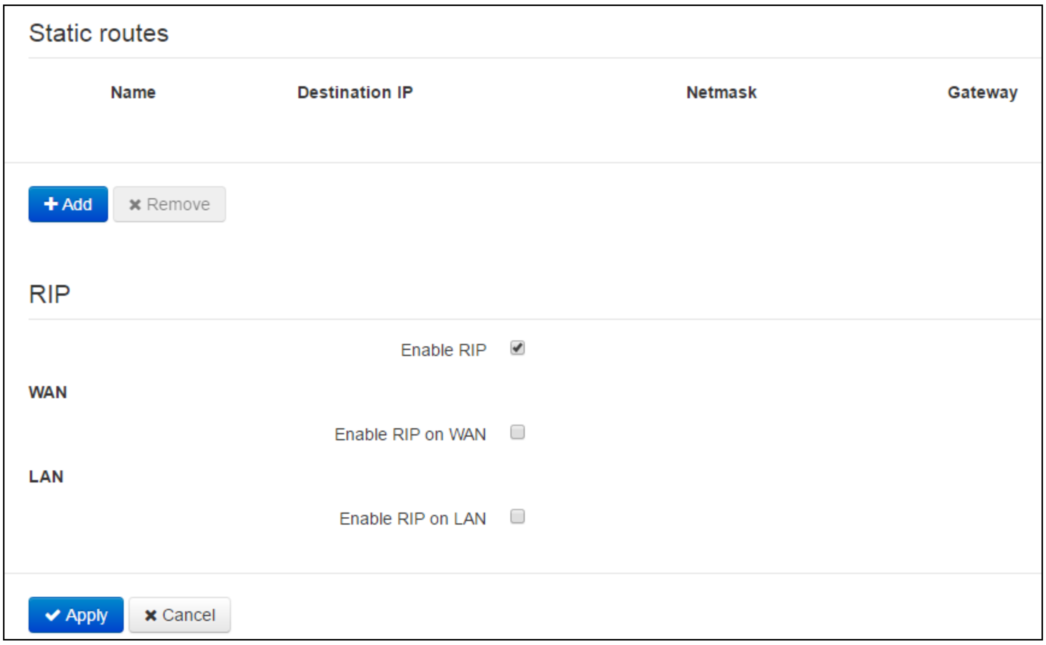

Add route

Name	
Destination IP	
Netmask	
Gateway	

- *Name* – route name, used for human perception convenience;
- *Destination address* – IP address of host or subnet that the router sould be established to;
- *Netmask* – subnet mask. Subnet mask for host should be 255.255.255.255, for subnet—depending on its size;
- *Gateway* – gateway IP address that allows for the access to the *'Destination IP'*.

RIP

To enable RIP, you should activate 'Enable RIP' parameter. The following parameters will be available for each active interface:



Static routes

Name	Destination IP	Netmask	Gateway

RIP

Enable RIP ☑

WAN

Enable RIP on WAN □

LAN

Enable RIP on LAN □

- *Enable RIP on WAN/LAN* – activate subnet announcement of the selected interface;
- *Authentication technique* – select an authentication technique before exchange of routs with neighboring routers: off/Text/MD5X;
- *Password for authentication* – password used for authentication with neighboring router;
- *Protocol version* – the current RIP version: RIPv1, RIPv2, RIPv1+RIPv2.

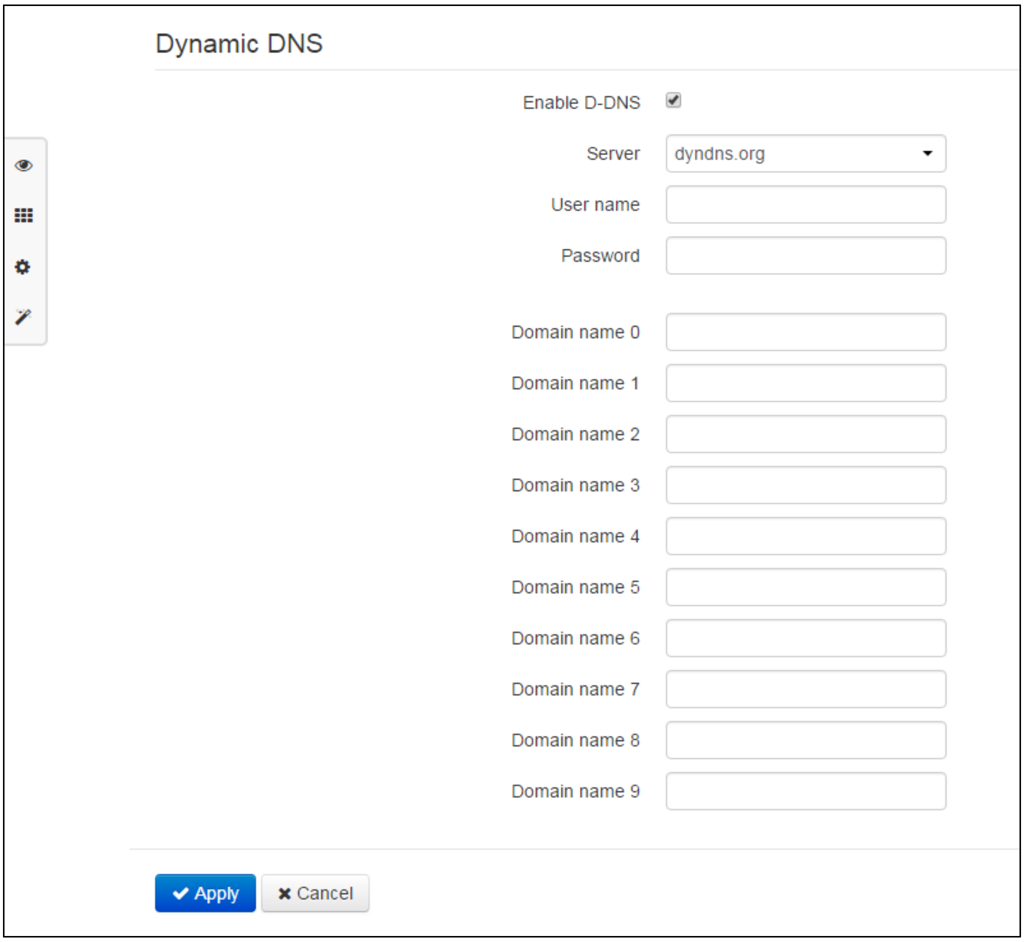
To apply a new configuration and store settings into the flash memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

3.7.2.15 'Dynamic DNS' submenu

In the 'Dynamic DNS' submenu, you may configure the respective service.

Dynamic DNS (D-DNS) allows DNS server information to be updated in real time and (optionally) in automatic mode. It's used for assigning a fixed domain name to a device (to a computer or router) with a dynamic IP address.

Dynamic DNS is frequently used in local networks, where clients are obtaining IP addresses through DHCP and then registering their names on local DNS-server.



Dynamic DNS

Enable D-DNS ☑

Server: dyndns.org

User name

Password

Domain name 0

Domain name 1

Domain name 2

Domain name 3

Domain name 4

Domain name 5

Domain name 6

Domain name 7

Domain name 8

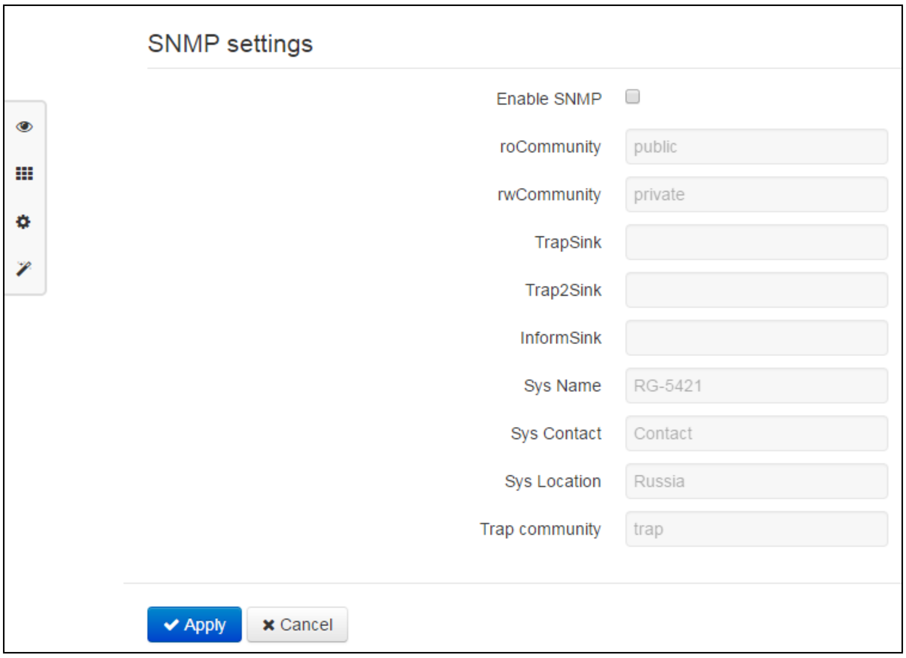
Domain name 9

- *Enable D-DNS* – when seleced, D-DNS service is enabled; the following settings will become available for editing:
- *Server* – provider name, select a provider from the list of available providers;
- *User name* – user name used to access D-DNS service account;
- *Password* – password used to access D-DNS service account;
- *Domain name (0..9)* – you may register up to 10 device domain names (in general, only one name is required). Device IP address information is updated on the provider server periodically in 60 seconds.

To apply a new configuration and store settings into the flash memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

3.7.2.16 'SNMP settings' submenu

RG-5400 firmware allows you to monitor status of the device and configure it via SNMP protocol. In SNMP submenu, you can configure settings of SNMP agent. Device supports SNMPv1, SNMPv2c and SNMPv3 protocol versions.



SNMP settings

Enable SNMP □

roCommunity: public

rwCommunity: private

TrapSink:

Trap2Sink:

InformSink:

Sys Name: RG-5421

Sys Contact: Contact

Sys Location: Russia

Trap community: trap

- *Enable SNMP* – when checked, SNMP will be enabled for utilization;
- *roCommunity* – password for parameter reading (common: '*public*');
- *rwCommunity* – password for parameter writing (common: '*private*');
- *TrapSink* – IP address or domain name of SNMPv1-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *Trap2Sink* – IP address or domain name of SNMPv2-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *InformSink* – IP address or domain name of Inform message recipient in HOST [COMMUNITY [PORT]] format;
- *Sys Name* – device name;
- *Sys Contact* – vendor contact information;
- *Sys Location* – device location information;
- *Trap community* – password enclosed in traps (default value: trap).

In the current firmware version, you may configure specific device parameters via SNMP: SIP basic settings, SIP profile settings, FXS port settings, call group settings, VAS management codes dialled from the phone unit, SNMP settings, system log settings.

Given below is the list of objects that may be read an configured via SNMP:

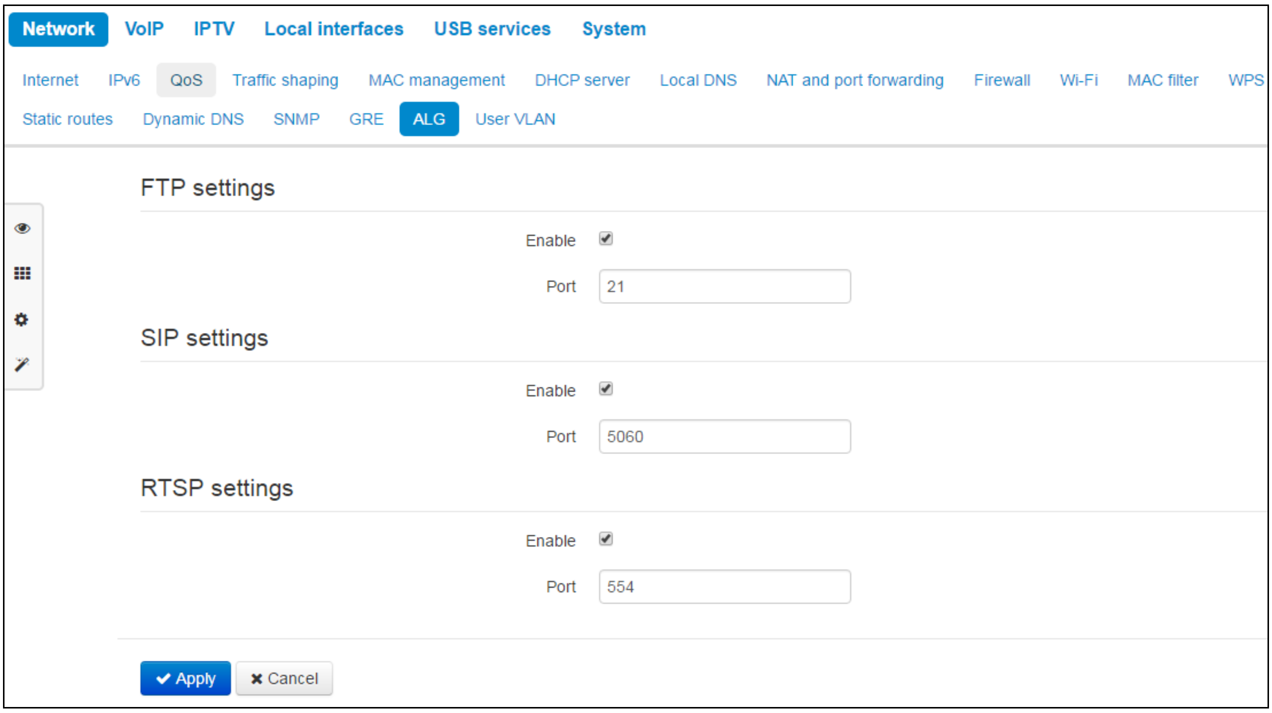
- Enterprise.1.3.1 – SIP profile basic settings
- Enterprise.1.3.2.1 – SIP profile settings
- Enterprise.1.1.2.1 – FXS port settings
- Enterprise.1.4.1.1 – call group settings
- Enterprise.1.5 – VAS activation codes for the phone unit
- Enterprise.2.1 – SNMP settings
- Enterprise.3.1 – system log settings

where Enterprise – 1.3.6.1.4.1.35265.1.56 is the device identifier of Eltex Enterprise.

To save changes into the device operative memory click *'Save Changes'* button. To record settings into non-voletile memory click *'Apply'* button.

3.7.2.17 'ALG' submenu

‘ALG’ submenu allows you to activate ALG for FTP, SIP, and RTSP with the indication of ports used by these protocols.



FTP settings

Enable ☑

Port 21

SIP settings

Enable ☑

Port 5060

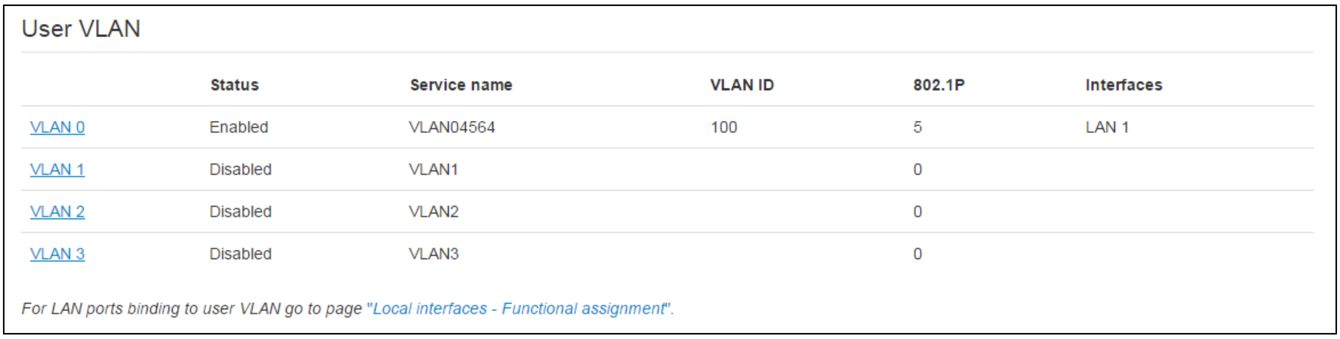
RTSP settings

Enable ☑

Port 554

3.7.2.18 ‘User VLAN’ submenu

User VLAN is described by VLAN identifier which network traffic is transferred transparently from the device WAN interface to LAN with the consequent tag removal in LAN. I.e. when the user VLAN is enabled, the device initializes a network bridge between WAN port and specific LAN ports; at that, on the WAN side the traffic is sent/received with the specified VLAN identifier which is removed on the LAN side.



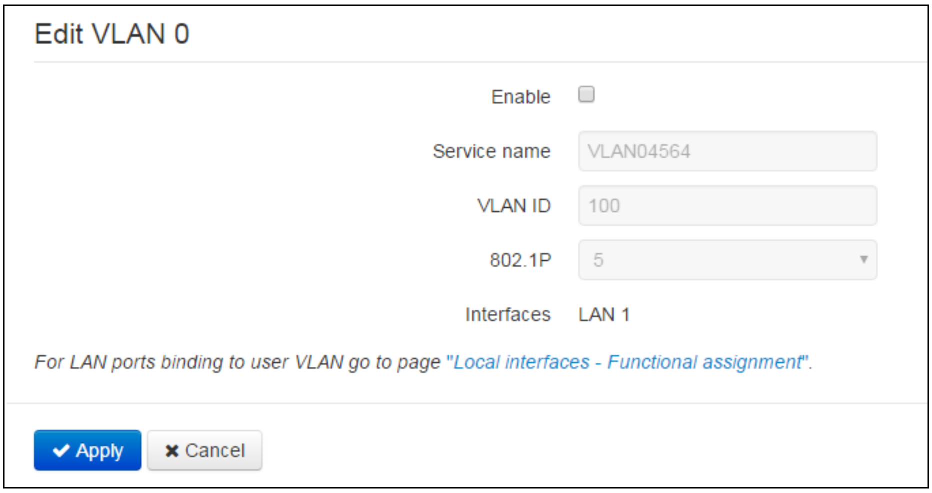
User VLAN

	Status	Service name	VLAN ID	802.1P	Interfaces
VLAN 0	Enabled	VLAN04564	100	5	LAN 1
VLAN 1	Disabled	VLAN1		0	
VLAN 2	Disabled	VLAN2		0	
VLAN 3	Disabled	VLAN3		0	

For LAN ports binding to user VLAN go to page "Local interfaces - Functional assignment".

- *Status*—shows the current VLAN status (enabled/disabled);
- *Service name* – user VLAN name;
- *VLAN ID* – VLAN identifier;
- *Interfaces* – list of LAN ports mapped to the current user VLAN.

The device allows you to configure up to 4 uses VLANs. To open VLAN settings for editing, click one of the links *VLAN0…VLAN3*:



Edit VLAN 0

Enable □

Service name: VLAN04564

VLAN ID: 100

802.1P: 5

Interfaces: LAN 1

For LAN ports binding to user VLAN go to page "Local interfaces - Functional assignment".

- *Enable* – when selected, user VLAN is enabled. If you try to disable a user VLAN with one or multiple LAN ports mapped to it, these LAN ports will be mapped to the Internet service;
- *Service name* – arbitrary name, associated with the current user VLAN;
- *VLAN ID* – VLAN identification number, may take values from 1 to 4095; should not match VLAN identifiers for other services;
- *802.1P* – 802.1P marker (another name: CoS – Class of Service), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority). Utilized by QoS algorithms;

- *Interfaces* – list of interfaces mapped to the current user VLAN. Non-editable field. To map the device LAN ports to user VLAN, go to the 'Local interfaces' tile.

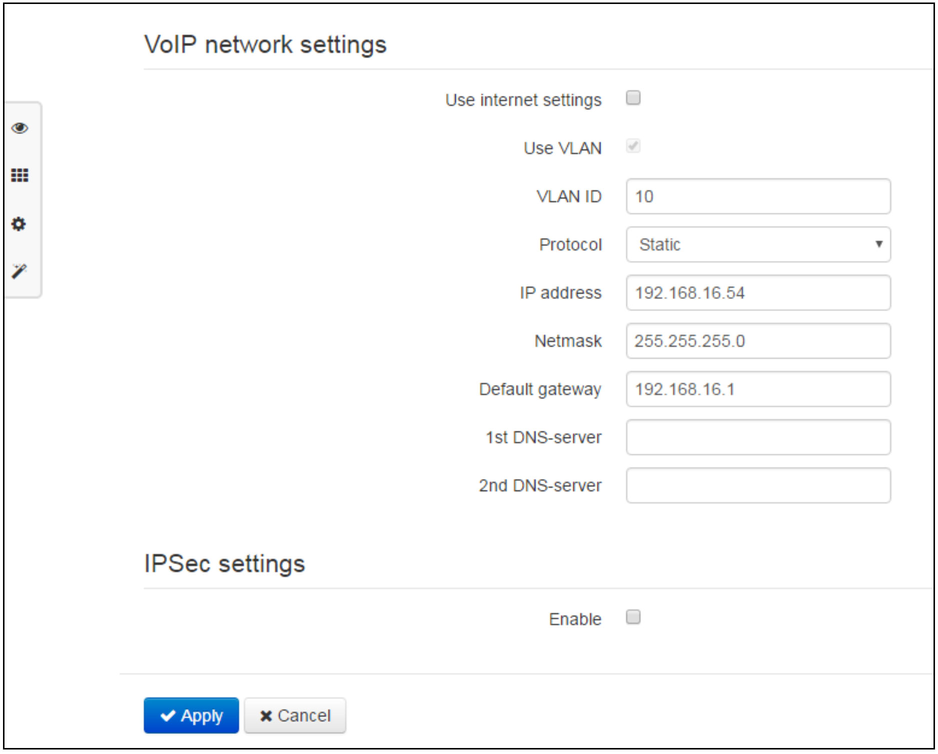
To store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.3 'VoIP' menu

In the 'VoIP' menu, you may configure VoIP (Voice over IP): SIP protocol configuration, FXS interface configuration, installation of codecs, numbering schedule, fax and modem data transfer mode.

3.7.3.1 'Network configuration' submenu

In the 'Network configuration' submenu, you may specify custom network settings for VoIP service.



VoIP network settings

Use internet settings □

Use VLAN ☑

VLAN ID: 10

Protocol: Static

IP address: 192.168.16.54

Netmask: 255.255.255.0

Default gateway: 192.168.16.1

1st DNS-server:

2nd DNS-server:

IPSec settings

Enable □

- *Use Internet settings* – when selected, use network settings specified in the *'Network'* -> *'Internet'* menu, otherwise use settings specified in this menu;
- *Use VLAN*[1] – when selected, VoIP service will use a dedicated interface in a separate VLAN for its operation, with VLAN number specified in *'VLAN ID'* field.
- *Protocol* – select address assigning protocol for the VoIP service interface:
  - *Static* – operation mode, where IP address and all the necessary settings for WAN interface are assigned manually. When 'Static' type is selected, the following parameters will be available for editing:
    - *IP address* – specify the IP address for VoIP service interface;
    - *Subnet mask* – subnet mask for VoIP service interface;
    - *Default gateway* – IP address for VoIP service interface default gateway;

[1] You can set specific network settings of VoIP service only for dedicated VLAN.

- *1st DNS, 2nd DNS*—DNS server IP addresses required for VoIP service operations.

- *DHCP* – operation mode where IP address, subnet mask, DNS address and other necessary settings for service operation (e.g. SIP and registration server static routes) are automatically obtained from DHCP server. If you are unable to obtain DNS server addresses from the provider, you may specify them manually using *'Primary DNS'* and *'Secondary DNS'* fields. Manually defined addresses will have a priority over DNS addresses obtained via DHCP.

  For DHCP, you may specify the required value for Option 60.

  - *Alternative Vendor ID (option 60)* – when selected, the device transmits *Vendor ID (Option 60)* field value in Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted in DHCP messages.
    If the *Alternative Vendor ID (Option 60)* checkbox is not selected, the default value will be transmitted in Option 60 in the following format:
    [VENDOR:device vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:**serial number**][WAN:**Wan interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**firmware version**]**

    Example:

  [VENDOR:Eltex][DEVICE:RG-5421G-Wac][HW:1.2][SN:VI23000118]
  [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.1.0]

IPSec settings:

In this section, you may configure IPSec encryption (IP Security).

IPSec is a set of protocols used for protection of data transmitted via Internet Protocol that enables authentication, integrity check and/or encryption of IP packets. IPsec also includes secure Internet Key Exchange protocols.

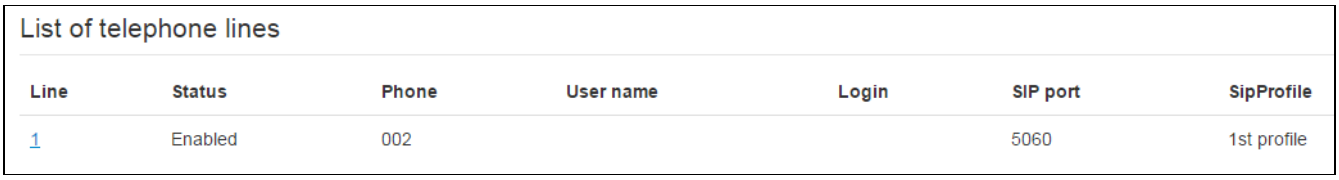
In the current firmware version, you may only access the device management interfaces (Web, Telnet, SSH) using IPSec.

For detailed *IPSec* settings, see Section 3.7.2.1.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.3.2 'Line settings' submenu

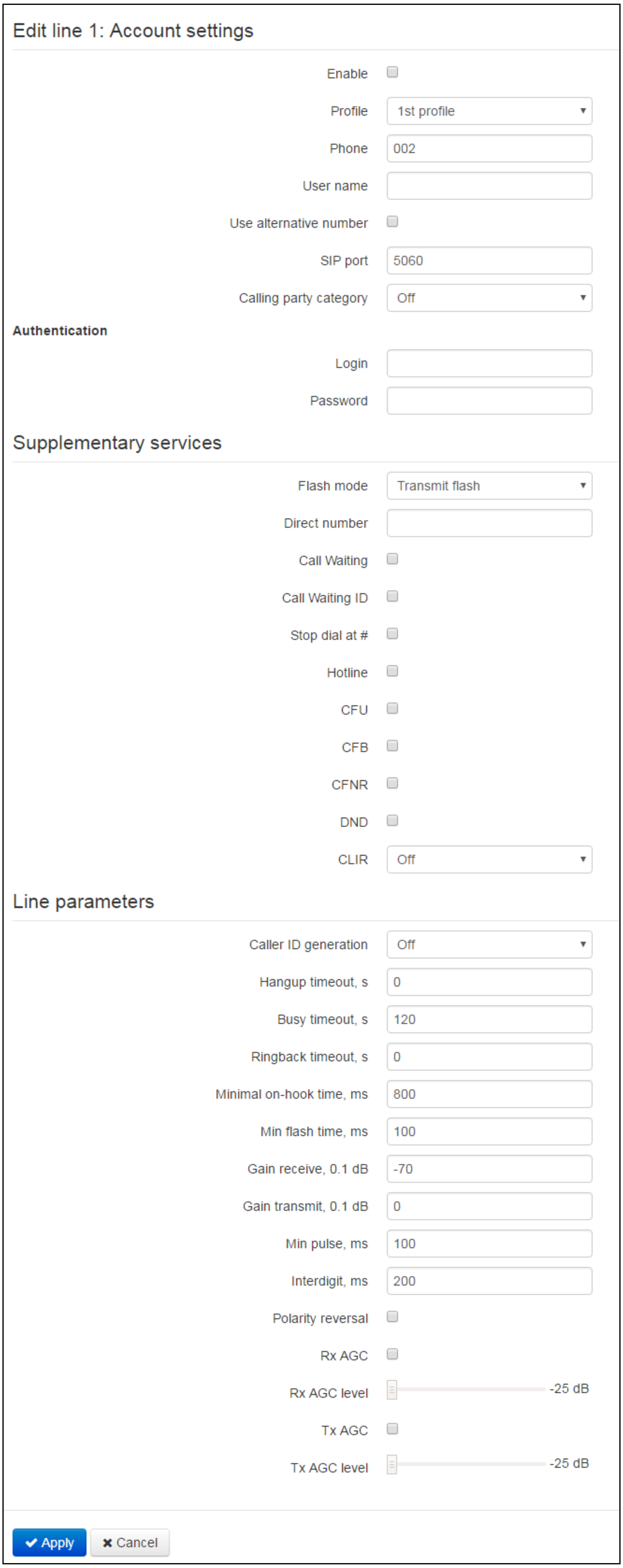
In the *'Line configuration'* submenu, you may configure the phone port.



List of telephone lines

Line	Status	Phone	User name	Login	SIP port	SipProfile
1	Enabled	002			5060	1st profile

To edit settings, press and hold the left mouse button on the link with the line number (1) to configure and fill in the following fields in the 'Edit line' window:



Edit line 1: Account settings

Enable □

Profile: 1st profile ▾

Phone: 002

User name:

Use alternative number □

SIP port: 5060

Calling party category: Off ▾

Authentication

Login:

Password:

Supplementary services

Flash mode: Transmit flash ▾

Direct number:

Call Waiting □

Call Waiting ID □

Stop dial at # □

Hotline □

CFU □

CFB □

CFNR □

DND □

CLIR: Off ▾

Line parameters

Caller ID generation: Off ▾

Hangup timeout, s: 0

Busy timeout, s: 120

Ringback timeout, s: 0

Minimal on-hook time, ms: 800

Min flash time, ms: 100

Gain receive, 0.1 dB: -70

Gain transmit, 0.1 dB: 0

Min pulse, ms: 100

Interdigit, ms: 200

Polarity reversal □

Rx AGC □

Rx AGC level: -25 dB

Tx AGC □

Tx AGC level: -25 dB

Account settings

- *Enable* – when selected, the port is active;
- *Profile* – select SIP profile from the list of available profiles. To configure profiles, use *'VoIP' -> 'Profiles'* menu.
- *Phone number* – subscriber number assigned to phone port;
- *User name* – username associated with the port (shown in 'Display-Name' field of the 'From' header in the outgoing SIP messages);
- *Use alternative number*—when selected, an alternative number will be inserted into the 'From' header of SIP messages sent from this port (particularly, in order to hide the real number from the Caller ID system of the callee);
- *Alternative number* – number assigned to the phone port will be changed to specified number in 'From' header of SIP message;
- *Substitute header into Contact* – number assigned to the phone port will be substituted by a number specified in 'Contact' header of SIP message;
- *SIP port* — UDP port for incoming SIP message receptionfor this account, and for outgoing SIP message transmission from this account. It may take values from 1 to 65535 (default value: 5060);
- *Calling party category* — Subscriber category—enables transmission of outgoing messages in the 'From' header; the latter is transmitted in Tel-URI format (see RFC3966);
- *Authentication login and password*—username and password used for subscriber authentication on SIP server (and on registration server).

Supplementary service

- *flash mode* – flash function operation mode (short clearback):
  - *Transmit flash* – transmit flash into the channel (using one of the methods described in 'Profiles' tab, *'Flash transmission'* parameter);
  - *Attended calltransfer* – flash dialling will be processed locally by the device (call transfer will be performed when the connection with the third party is established). For the 'Attended calltransfer' detailed operation algorithm, see Section 4.1 'Call transfer';
- *Unattended calltransfer* – flash dialling will be processed locally by the device (call transfer will be performed when the subscriber finishes dialling a third party number). For the 'Unattended calltransfer' detailed operation algorithm, see Section *4.1 'Call Transfer'*;*Direct number – when t*he phone goes offhook, dial the defined number immediately;
- *Call waiting* – when selected, 'Call waiting' service will be enabled (this service is available in 'flash—call transfer' function operation mode);
- *Call waiting ID* – when the second call is transmitted to a port and 'Call waiting' service is enabled, callee will receive the calling part number of second line ;
- *Stop dial at # – when se*lected, use '#' button on the phone unit to end the dialling, otherwise '#' will be recognized as a part of the number;
- *Hotline*—when selected, 'Hotline/warmline' service is enabled. This service allows to establish an outgoing connection automatically without dialling the number after the phone handset is picked up with the defined delay (in seconds). When checked, fill in the following fields:
  - *Hotline/warmline number*—phone number that will be used for connection establishment upon 'Delay timeout' expiration after the phone handset is picked up (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule);
  - *Delay timeout, seconds*—time interval that will be used for connection establishment with the opposite subscriber, in seconds;

- *CFU—Call forward unconditional*—when selected, CFU (Call Forward Unconditional) service is enabled—all incoming calls will be forwarded to the specified call forward unconditional number.When checked, fill in the following fields:
  - *Call forward unconditional number*—number that all incoming calls will be forwarded to when *Call forward unconditional* service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule.);
- *CFB—Call forward on busy*—when selected, CFB (Call Forward on Busy) service is enabled—forward the call to the specified number, when the subscriber is busy. When checked, fill in the following fields:
  - *Call forward on busy number*—number that incoming calls will be forwarded to when the subscriber is busy and *Call forward on busy* service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule.);
- *CFNR—Call forward on no answer*—when selected, CFNA (Call Forward at No Answer) service is enabled—forward the call, when there is no answer from the subscriber. When selected, fill in the following fields:
  - *Call forward on no answer number*—number that incoming calls will be forwarded to when there is no answer from the subscriber and *Call forward on no answer* service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule);
  - *No answer timeout, seconds*—time interval that will be used for call forwarding when there is no answer from the subscriber, in seconds;
- *DND—Do not disturb*—when selected, temporary restriction is placed for incoming calls (DND service).

  When multiple services are enabled simultaneously, the priority will be as follows (in the descending order):
  - CFU;
  - DND;
  - CFB, CFNA.

- *CLIR* – caller ID service restriction. When flag is set *Anonymous* sip:anonymous@unknown.host will be transmitted by the *'From'* header of messages via SIP.

Line parameters (Configuration of physical parameters)

- Deliver calling party phone number—select the Caller ID mode. For Caller ID operation, subscriber's phone unit must support the selected method:
  - *Off* – Caller ID is disabled;
  - *FSK Bell 202, FSK V.23* – FSK Caller ID method (using bell202 standard, or ITU-T V.23). The number is served between the first and second ringing tones by a stream of data with a frequency modulation;
  - *DTMF* – DTMF Caller ID method. The number is served between the first and second calls on the line by dual-frequency DTMF;
- *Hangup timeout, seconds* – dialing timeout for the first digit of the number. When there is no dialing during the specified time, 'busy' tone will be sent to the subscriber, and the dialing will be ended;
- *Busy timeout, seconds*—'busy' tone timeout for the subscriber. If the subscriber doesn't put the phone onhook until the timeout expires, an error tone will be sent into the line;
- *Ringback timeout, seconds*—launches when an incoming call is received and defines the maximum call response time. When the defined timeout expires, 'busy' tone will be sent to the remote subscriber.

- *Min onhook time, ms*—minimal clearback detection time, in milliseconds. At that, this parameter represents the maximum flash detection time;
- *Min flash* time—minimal flash detection time, (80–1000) ms;
- *Gain receive, 0.1dB*—received signal gain (transmitted into the phone handset), measurement unit—0.1dB;
- *Gain transmit, 0.1dB*—transmitted signal gain (received by the phone handset microphone), measurement unit—0.1dB;
- *Digit duration, ms* – configuration is required for pulse dialling mode, (10-150) ms;
- *Interdigit, ms*—configuration is required for pulse dialling mode, (150-20000) ms;
- *Polarity reversal*—when this option is enabled, line voltage polarity reversal occurs right after the callee responses to the outgoing call. After the clearback, the voltage polarity returns to its original state. This option is essential for payphone operation (polarity reversal indicates the start of the paid time interval);
- *Automatic gain at the reception (Rx AGC)* – when the flag is set, signal received from RTP is automatically amplified up to assigned level;
- *Gain level at the reception* – desirable level of signal received from RTP.

✓ **Assigned value doesn't show the resultant signal level that is received by handset. The resultant level consists of gain level and gain coefficient at the reception. The default value of gain coefficient at the reception is -7 dB.**

Example:

The signal with -10 dB level was restored from the RTP stream. The required gain level at the reception is -4 dB. Gain coefficient at the reception is -7 dB. As the result, resultant signal on the handset will have level of -11 dB because of initial signal will be amplified up to -4 dB and will be transmitted with the -7 dB gain coefficient at the input of calling equipment.

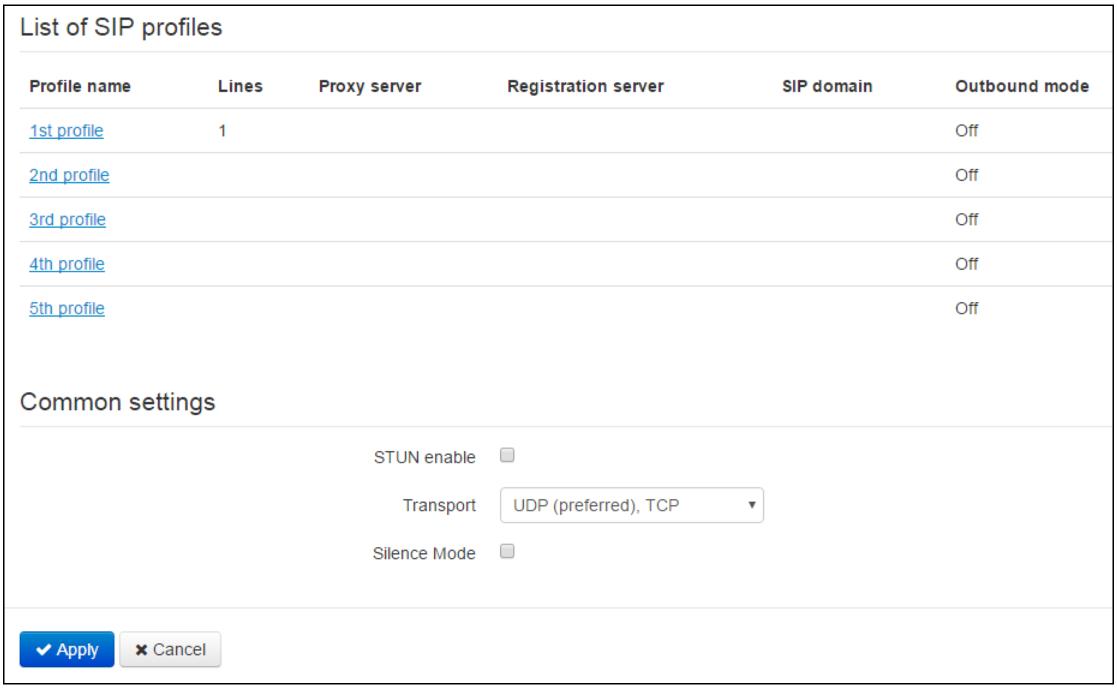
- *Automatic gain on the reception* – when checked, gain of signal transmitted in RTP is performed automatically;
- *Transmission gain level* – desiablre level of signal transmitted in RTP.

✓ **In contrast to reception gain level, specified value shows the resultant level of signal transmitted to RTP.**

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.3.3 'Profile' submenu

In the 'Profiles' submenu, you may configure device SIP profiles. For each SIP profile, you may assign custom SIP and registration server addresses, voice and fax/modem codecs, custom numbering schedule and other parameters. Different SIP profiles are needed when different subscriber ports operate via different communication directions (different SIP servers). At that, for each subscriber port, you may assign only one SIP profile (*'VoIP'* -> *'Profiles'* menu).



List of SIP profiles

Profile name	Lines	Proxy server	Registration server	SIP domain	Outbound mode
1st profile	1				Off
2nd profile					Off
3rd profile					Off
4th profile					Off
5th profile					Off

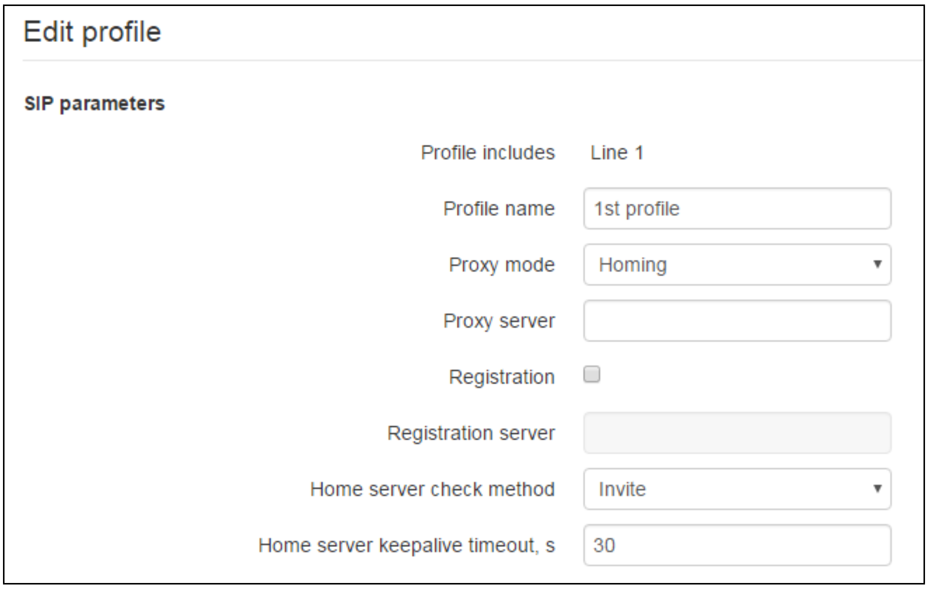
Common settings

STUN enable □

Transport UDP (preferred), TCP

Silence Mode □

To edit profile settings, left-click the link of the profile to be configured. In the 'Edit profile:' window, fill in the following fields:



Edit profile

SIP parameters

Profile includes Line 1

Profile name 1st profile

Proxy mode Homing

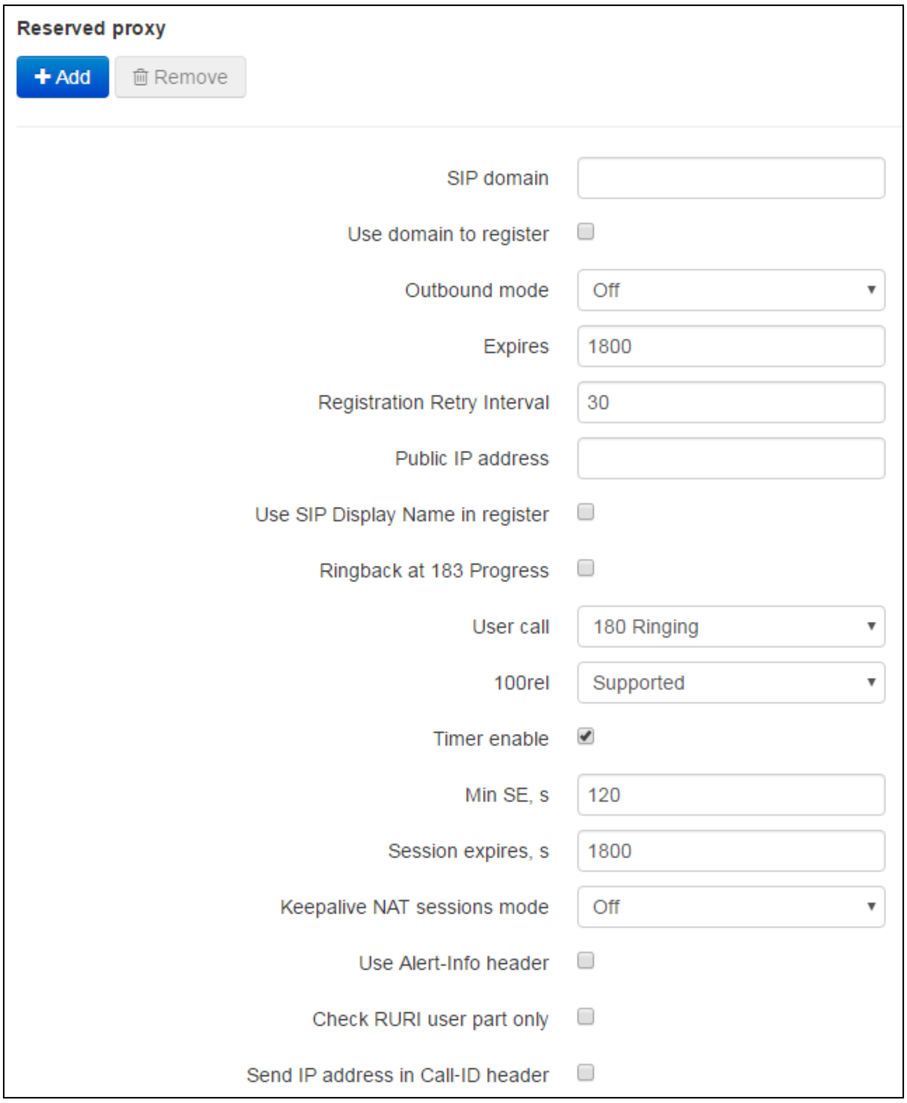
Proxy server

Registration □

Registration server

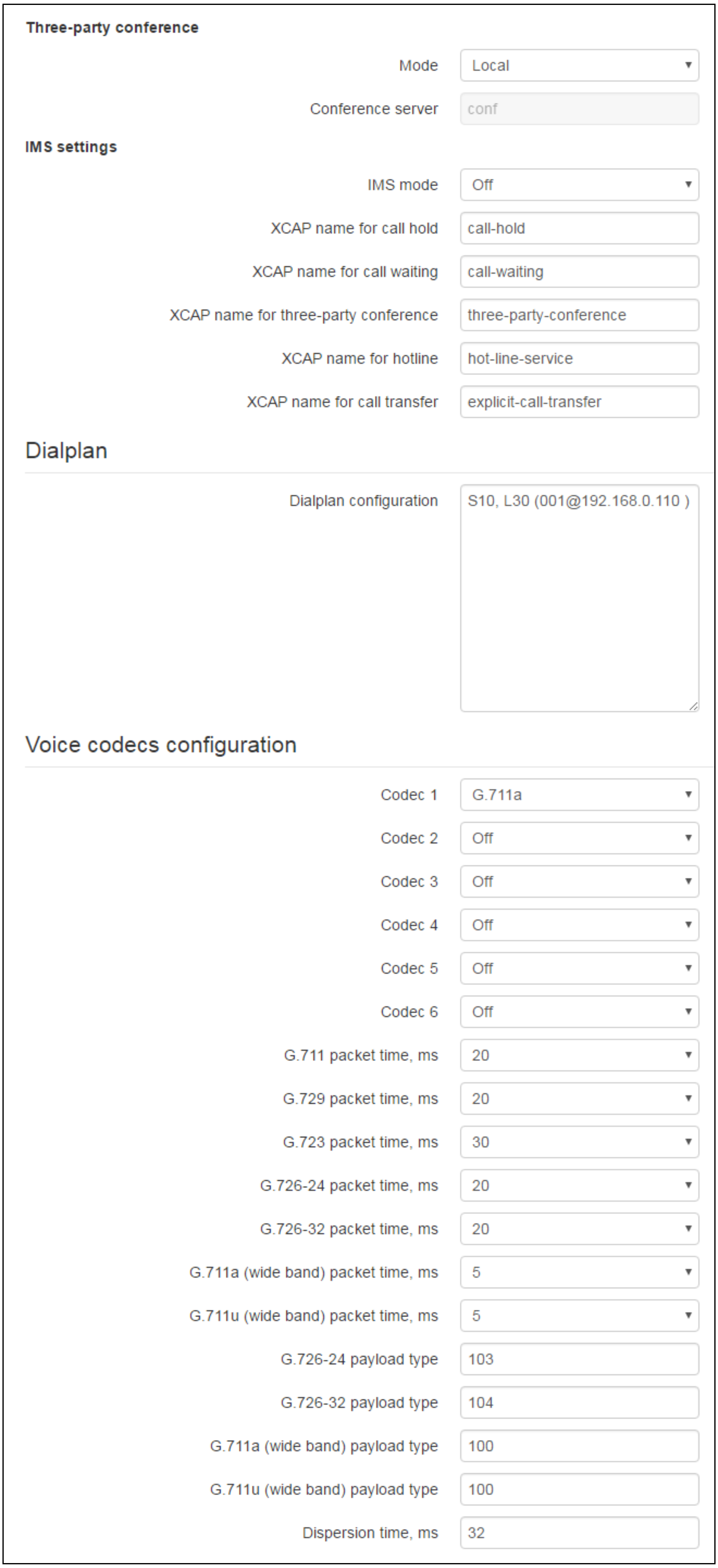
Home server check method Invite

Home server keepalive timeout, s 30



Reserved proxy

SIP domain	
Use domain to register	☐
Outbound mode	Off ▾
Expires	1800
Registration Retry Interval	30
Public IP address	
Use SIP Display Name in register	☐
Ringback at 183 Progress	☐
User call	180 Ringing ▾
100rel	Supported ▾
Timer enable	☑
Min SE, s	120
Session expires, s	1800
Keepalive NAT sessions mode	Off ▾
Use Alert-Info header	☐
Check RURI user part only	☐
Send IP address in Call-ID header	☐



Three-party conference

Mode	Local ▾
Conference server	conf

IMS settings

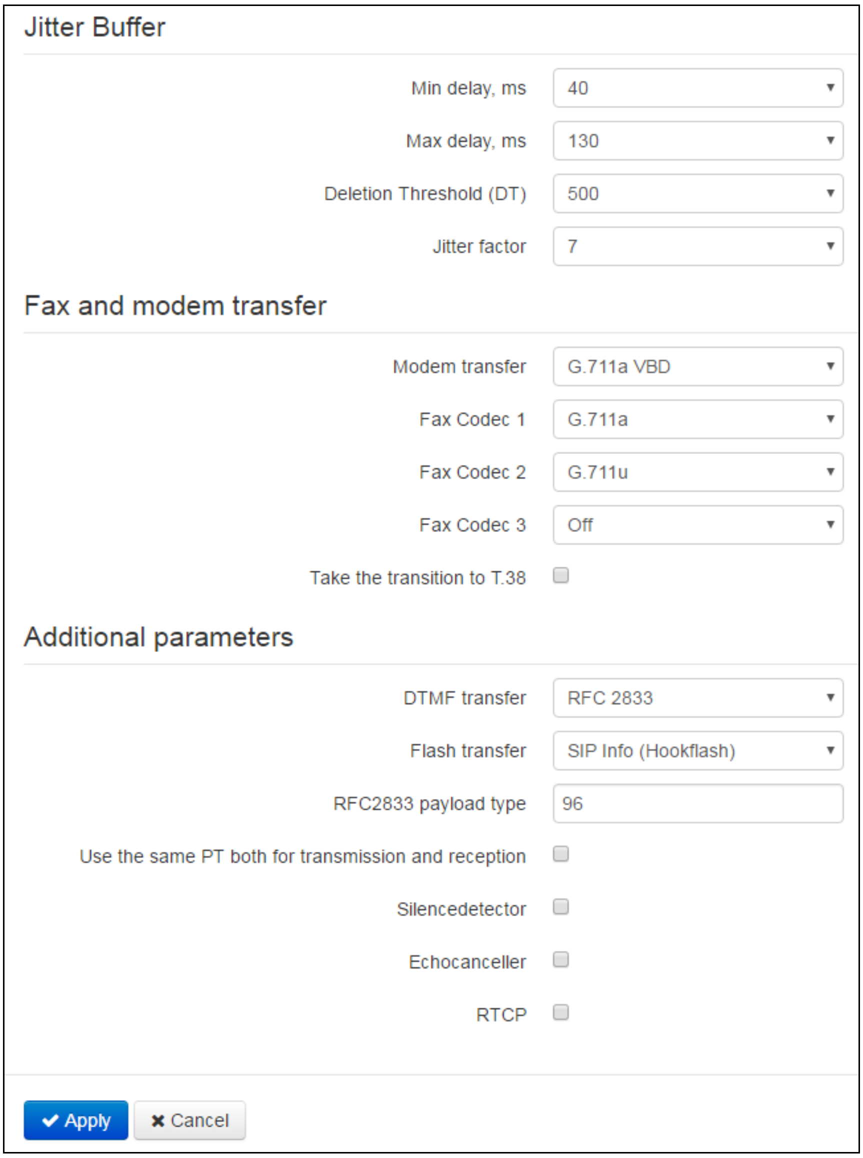
IMS mode	Off ▾
XCAP name for call hold	call-hold
XCAP name for call waiting	call-waiting
XCAP name for three-party conference	three-party-conference
XCAP name for hotline	hot-line-service
XCAP name for call transfer	explicit-call-transfer

Dialplan

Dialplan configuration	S10, L30 (001@192.168.0.110)

Voice codecs configuration

Codec 1	G.711a ▾
Codec 2	Off ▾
Codec 3	Off ▾
Codec 4	Off ▾
Codec 5	Off ▾
Codec 6	Off ▾
G.711 packet time, ms	20 ▾
G.729 packet time, ms	20 ▾
G.723 packet time, ms	30 ▾
G.726-24 packet time, ms	20 ▾
G.726-32 packet time, ms	20 ▾
G.711a (wide band) packet time, ms	5 ▾
G.711u (wide band) packet time, ms	5 ▾
G.726-24 payload type	103
G.726-32 payload type	104
G.711a (wide band) payload type	100
G.711u (wide band) payload type	100
Dispersion time, ms	32



Jitter Buffer

Min delay, ms	40
Max delay, ms	130
Deletion Threshold (DT)	500
Jitter factor	7

Fax and modem transfer

Modem transfer	G.711a VBD
Fax Codec 1	G.711a
Fax Codec 2	G.711u
Fax Codec 3	Off
Take the transition to T.38	□

Additional parameters

DTMF transfer	RFC 2833
Flash transfer	SIP Info (Hookflash)
RFC2833 payload type	96
Use the same PT both for transmission and reception	□
Silencedetector	□
Echocanceller	□
RTCP	□

SIP parameters

- *Profile contents* – list of subscriber ports that the profile is assigned to; this field cannot be changed;
- *Profile name* – custom name of the configured profile;
- *SIP proxy operation mode* – select SIP server operation mode form the drop-down list:
  - Disable;
  - Parking—SIP-proxy redundancy mode without main SIP-proxy management;
  - Homing—SIP-proxy redundancy mode with main SIP-proxy management.

  Gateway may operate with a single main SIP-proxy and up to four redundant SIP-proxies. For exclusive operations with the main SIP-proxy, 'Parking' and 'Homing' modes are identical. In this case, if the main SIP-proxy fails, it will take time to restore its operational status.

  For operations with redundant SIP-proxies, 'Parking' and 'Homing' modes will work as follows. The gateway sends INVITE message to the main SIP-proxy address when performing outgoing call, and REGISTER message when performing registration attempt. If on expiration of *'Invite total timeout'* there is no response from the main SIP-proxy or response 408 or 503 is received, the gateway sends INVITE (or REGISTER) message to the first redundant SIP-proxy address. If it is not available, the request is forwarded to the next redundant SIP-proxy and so forth. When available redundant SIP-proxy if found, registration will be renewed on that SIP-proxy.

Next, the following actions will be available depending on the selected redundancy mode:

1 In the 'parking' mode, the main SIP-proxy management is absent, and the gateway will continue operation with the redundant SIP-proxy even when the main proxy operation is restored. If the connection to the current SIP-proxy is lost, querying of the subsequent SIP-proxies will be continued using the algorithm described above. If the last redundant SIP-proxy is not available, the querying will continue in a cycle, beginning from the main SIP-proxy.

2 In the 'homing' mode, three types of the main SIP-proxy management are available: periodic transmission of OPTIONS messages to its address, periodic transmission of REGISTER messages to its address, or transmission of INVITE request when performing outgoing call. First of all, INVITE request is sent to the main SIP-proxy, and if it is unavailable, then to the next redundant one, etc. Regardless of the management type, when the main SIP-proxy operation is restored, gateway will use it to renew its registration. The gateway will begin operation with the main SIP-proxy.

- *SIP proxy server*—network address of a SIP server—device that manages access to provider's phone network for all subscribers. You may specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060);
- *Registration*—when selected, register ports that utilize this profile on registration server;
- *Registration server*—network address of a device that is used for registration of all phone network subscribers in order to provide them with the communication services (specify registration server UDP port after the colon, default value is 5060). You may specify IP address as well as the domain name. As a rule, registration server is physically co-located with SIP proxy server (they have the same address);
- *Primary server control method*—select availability control method for the primary SIP server in 'Homing' mode:

  - *Invite*—transmission of INVITE request to its address when performing an outgoing call;
  - *Register*—periodic transmission of REGISTER messages to its address;
  - *Options*—periodic transmission of OPTIONS messages to its address.

- *Primary server control period, sec*—periodic message transmission interval in seconds; used for primary SIP server availability check.

Redundant SIP proxies

To add a redundant SIP proxy, click 'Add' button and enter the following settings:

- *SIP proxy server*—network address of redundant SIP server. You may specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060);
- *Registration server*—network address of redundant registration server (specify UDP port after the colon, default value is 5060). You may specify IP address as well as the domain name. If the *'Registration server'* checkbox is selected, the redundant server registration is enabled.

To remove the redundant SIP proxy, select the checkbox next to the specified address and click 'Delete' button.

- *SIP domain*—domain where the device is located (fill in, if required);
- *Apply SIP Domain for registration*—when selected, apply SIP Domain for registration (SIP domain will be inserted into the 'Request-Line' of 'Register' requests);
- *Outbound mode*—'Outbound' mode:

  - *Disabled* — calls will be routed according to the numbering schedule;
  - *Outbound* — numbering schedule is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, PBX response will be sent to the subscriber in order to enable subscriber service management (VAS management);
  - *Outbound with 'Busy' tone* — numbering schedule is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, VoIP will be unavailable: error tone will be transmitted to the phone headset.

- *Registration renewal time period*—time for subscriber port registration on SIP server. At the average, port registration renewal will be performed after 2/3 of the specified period;
- *Registration retry interval*—when the registration is unsuccessful, time period between SIP server registration attempts;
- *Public address*—this parameter is used as an external address of the device when it operates behind the NAT (gateway). As a public address, you may specify an external address (WAN) of a gateway (NAT) that *TAU-1M.IP* operates through. At that, on the gateway (NAT), you should forward the corresponding SIP and RTP ports used by the device;
- *Use SIP Display Name during registration*—when selected, use username in 'SIP Display Info' field of the 'Register' message;
- *Ringback on 183 Progress*—when selected, 'ringback' tone will be sent upon receiving '183 Progress' message (w/o enclosed SDP).

- *Calling subscriber*—provisional response sent by the device to the caller equipment during the incoming call:
  - *180 Ringing*—caller equipment will receive response 180; upon receiving this message, caller equipment should send a local ringback tone into the line;
  - *183 Progress with SDP*—caller equipment will receive response 183+SDP—used for voice frequency path forwarding before the answer of the callee. In this case, *RG-5400* will send a ringback tone remotely to the caller.
- *100rel*—use reliable provisional responses (RFC3262):
  - *supported*—reliable provisional responses are supported;
  - *required*—reliable provisional responses are mandatory;
  - *off*—reliable provisional responses are disabled.

SIP protocol defines two types of responses for connection initiating request (INVITE)—provisional and final. 2xx, 3xx, 4xx, 5xx и 6xx-class responses are final and their transfer is reliable, with ACK message confirmation. 1xx-class responses, except for '100 Trying' response, are provisional, without confirmation (rfc3261). These responses contain information on the current INVITE request processing step, therefore loss of these responses is unacceptable. Utilization of reliable provisional responses is also stated in SIP (rfc3262) protocol and defined by *'100rel'* tag presence in the initiating request. In this case, provisional responses are confirmed with PRACK message.

Setting operation for outgoing communications:

- *Supported*—send the following tag in 'INVITE' request—supported: 100rel. In this case, communicating gateway may transfer provisional responses reliably or unreliably—as it deems fit;
- *Required*—send the following tags in 'INVITE' request—supported: 100rel and required: 100rel. In this case, communicating gateway should perform reliable transfer of provisional replies. If communicating gateway does not support reliable provisional responses, it should reject the request with message 420 and provide the following tag—unsupported: 100rel. In this case, the second INVITE request will be sent without the following tag—required: 100rel;
- *Disabled*—do not send any of the following tags in INVITE request—supported: 100rel and required: 100rel. In this case, communicating gateway will perform unreliable transfer of provisional replies.

Setting operation for incoming communications:

- *Supported, required*—when the following tag is received in 'INVITE' request—supported: 100rel, or required: 100rel—perform reliable transfer of provisional replies. If there is no supported: 100rel tag in INVITE request, the gateway will perform unreliable transfer of provisional replies;
- *Disabled*—when the following tag is received in 'INVITE' request—required: 100rel, reject the request with message 420 and provide the following tag—unsupported: 100rel. Otherwise, perform unreliable transfer of provisional replies.

- *Enable timer*—when selected, the 'timer' (RFC 4028) extension support is enabled. When connection is established, and both sides support 'timer' extension, one of them periodically sends re-INVITE requests for connection monitoring purposes (if both sides support UPDATE method, wherefore it should be specified in the 'Allow' header, the session update is performed by periodic transmission of UPDATE messages);
- *Minimal session time, sec*—minimal time interval for connection health checks (90 to 1800s, 120s by default);
- *Session time, seconds*—period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 80000s, recommended value—1800s, 0—unlimited session);
- *Periodic SIP server polling*—select SIP server polling method:
  - *Disabled*—SIP server will not be polled;
  - *Options*—SIP server polling with OPTIONS messages;
  - *Notify*—SIP server polling with NOTIFY messages;
  - *CLRF*—SIP server polling with an empty UDP packet.
- *Polling interval*—SIP server polling time period, in seconds;
- *Process Alert-Info header*—process INVITE request 'Alert-Info' header to send a non-standard ringing to the subscriber port;
- *Check username only in RURI*—when selected, only subscriber number (user) will be analysed, and if the number matches, the call will be assigned to the subscriber port. When unselected, all

URI elements (user, host and port—subscriber number, IP address and UDP/TCP port) will be analysed upon receiving an incoming call. If all URI elements match, the call will be assigned to the subscriber port;
- *Send IP address in Call-ID header*—when selected, during outgoing communications, device custom IP address will be used in 'Call-ID' header in 'localid@host' format.

Three-way conference call

- *Mode*—three-way conference call operation mode. Two modes are possible:
  - *Local*—conference assembly is performed locally by the device after pressing 'flash+3';
  - *Remote (RFC4579)*—conference assembly is performed at the remote server; after pressing 'flash+3', 'Invite' message will be sent to the server using number specified in the 'Conference server' field. In this case, conference operation complies with the algorithm described in RFC4579. For detailed algorithm description, see Paragraph 4.3.2.
- *Conference server*—in general, address of the server that establishes conference using algorithm described in RFC4579. Address is specified in the following format SIP-URI: user@address:port. You may specify the 'user' URI part only—in this case, 'Invite' message will be sent to the SIP proxy address;

IMS configuration

- *Enable VAS management using IMS*—you may manage some service types using IMS (IP Multimedia Subsystem) server. In this case, 'Three-way conference call' (complies with RFC4579 algorithm), 'Call hold', 'Call waiting', 'Hotline' services (regardless of whether they were enabled in the configuration or not) will be enabled remotely by IMS server that sends 'Notify' messages containing enable/disable commands in XCAP format (in fact, XML, RFC4825);
- *Disabled* – IMS is not used;
- *Without subscription*—you may manage some service types using IMS (IP Multimedia Subsystem) server. In this case, 'Three-way conference call' (complies with RFC4579 algorithm), 'Call hold', 'Call waiting', 'Hotline' services (regardless of whether they were enabled in the configuration or not) will be enabled remotely by IMS server that sends 'Notify' messages containing enable/disable commands in XCAP format (in fact, XML, RFC4825). In this case, when the gateway finishes subscriber registration, SUBSCRIBE requests will not be sent, only NOTIFY requests received from IMS and used for service management will be processed;
- *With subscription*—you may manage some service types using IMS (IP Multimedia Subsystem) server. In this case, 'Three-way conference call' (complies with RFC4579 algorithm), 'Call hold', 'Call waiting', 'Hotline' services (regardless of whether they were enabled in the configuration or not) will be enabled remotely by IMS server that sends 'Notify' messages containing enable/disable commands in XCAP format (in fact, XML, RFC4825). In this case, when the gateway finishes subscriber registration, it sends SUBSCRIBE requests, and if the subscription is successfully completed, it will process NOTIFY requests received from IMS and used for service management
- *'Call hold' service name*—name of the XML element located in the 'Notify' message body that is used for transmission of 'Call hold' enabling/disabling commands. For example, if the service name value is 'call-hold', enabling command will be as follows:
  <call-hold active="true"/>
  and deactivation command:
  <call-hold active="false"/>
- *'Call waiting' service name*—name of the XML element located in the 'Notify' message body that is used for transmission of 'Call waiting' enabling/disabling commands. For example, if the service name value is 'call-waiting', enabling command will be as follows:

```
<call-waiting active="true"/>
```

Disabling command:

```
<call-waiting active="false"/>
```

- *'Three-way conference call' service name*—name of the XML element located in the 'Notify' message body that is used for transmission of 'Three-way conference call' enabling/disabling commands. For example, if the service name value is 'three-party-conference', enabling command will be as follows:

  ```
  < three-party-conference active="true"/>
  ```

  Disabling command:

  ```
  < three-party-conference active="false"/>
  ```

- *'Hotline' service name*—name of the XML element located in the 'Notify' message body that is used for transmission of 'Hotline' enabling command. In the enabling command, you should pass the hotline number and the call timeout. For example, if the service name value is 'hot-line-service' and you should call the number 30001 in 6 seconds after the phone handset is picked up, the enabling command will be as follows:

  ```
  <hot-line-service>
      <addr>30001</addr>
      <timeout>6</timeout>
  </hot-line-service>
  ```

  If the enabling command is not received, the 'Hotline' service will be disabled.

By default, if the enabling command is not received, all the services mentioned above are disabled.

Dial plan

To define the numbering schedule, use regular expressions in the 'Dial plan configuration' field.

The structure and format of regular expressions that enable different dialling features are listed below.

Structure of regular expressions:

Sxx, Lxx ( ),
where
xx – arbitrary values of S and L timers;
() – numbering schedule margins.

- Basis is the designations used for the dialled digit sequence recording. Digit sequence is recorded using several designations—digits dialled from the phone keypad: 0, 1, 2, 3, …, 9, #, and *. **If you use # in the dialplan, you may block the dialling completion using this key!**
- Digit sequence enclosed in square brackets corresponds to any character enclosed in these brackets.
  - Example: ([1239])—corresponds to any digit—1, 2, 3, or 9.
- Use a hyphen to define a range of characters. Mostly used inside square brackets.
  - Example 1: (1–5)—any digit from 1 to 5;
  - Example 2: ([1-39])—example listed above in the different entry format.
- 'X' character corresponds to any digit from 0 to 9.
  - Example: (1XX)—any 3-digit number that begins with 1.
- '.' —repeat previous character from 0 ad infinitum;
- «+»—repeat previous character from 1 ad infinitum;
- {a,b}—repeat previous character from 'a' to 'b' times;

- {a,}—repeat previous character more than 'a' times;
- {,b}—repeat previous character less than 'b' times.
  - Example: (810X.) —international number with any quantity of digits.

Settings affecting dialplan configuration:

- *Interdigit Long Timer ('L' character in numbering schedule record)*—entry timeout for the next digit, if there are no templates that correspond to the dialled combination;
- *Interdigit Short Timer ('S')*—entry timeout for the next digit, if the dialled combination fully matches at least one template and if there is at least one template that requires an extension dialling for the full match.

Additional features:

1. Dialled sequence replacement

Syntax: *<arg1:arg2>*

This feature allows you to replace the dialled sequence with any dialled character sequence. At that, the second argument should be defined with the specific value, both arguments may be empty.

- Example: (<83812:> XXXXXX) - this record will correspond to dialled digits 83812, but this sequence will be skipped and will not be sent to the SIP server.

2. Tone insertion to dialling

For long-distance access (for city access in case of office PBX), it is common to hear a PBX response, that may be implemented by inserting comma in a sequence of digits.

- Example: (8, 770)—when number 8770 is dialled, the continuous tone will be played after the digit '8'.

3. Dialling restriction.

When you specify an exclamation mark '!' at the end of the number template, dialling of numbers corresponding to the template will be blocked.

- Example: (8 10X xxxxxxx! | 8 xxx xxxxxxx) – expression allows long-distance dialling only and denies outgoing international calls.

4. Replacement of dialling timer values

Timer values may be specified for the entire dialplan, as well as for the specific template only. 'S' character deals with the *'Interdigit Short Timer'*, and 'L'— with the *'Interdigit Long Timer'* setting. Timer values may be specified for all templates in the dialplan, when values are listed before the opening parenthesis.

- Example: S4 (8XXX.) or S4,L8 (XXX)

If these values are listed in one sequence only, they are effective only for this sequence. At that, you are not required to delimit the key and timeout value with the colon, value may be specified anywhere within the template.

- Example: (S4 8XXX. | XXX) or ([1-5] XX S0) – record will trigger an instant call transfer, when the 3-digit number beginning with 1, 2, … , 5 is dialled.

5. Direct address dialling (IP Dialing)

'@' placed after the number defines that the dialled call will be sent to the subsequent server address. We recommend using 'IP Dialing', as well as call reception and transmission without registration *('Call Without Reg', 'Answer Without Reg')*. This may help when the server fails.
Also, IP Dialling address format may be used for numbers intended for the call forwarding.

- Example 1: (8 xxx xxxxxxx) - 11-digit number beginning with 8.
- Example 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) - 11-digit number beginning with 8; if 7-digit number is dialled, add 8495 to the number being sent.
- Example 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) - dialling of emergency call numbers and unusual sets of long-distance numbers .
- Example 4: (S0 <:82125551234>) - quickly dial the specified number, similar to 'Hotline' mode on other gateways.
- Example 5: (S5 <:1000> | xxxx) - this dialplan allows you to dial any number that contains digits, and if there was no entry in 5 seconds, dial number '1000' (for example, it belongs to a secretary).
- Example 6: (*5x*xxxx*x#|*2x*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8, [2-9]xxxxxxxxx|8, 10x.|1xx<:@10.110.60.51:5060>).
- Example 7: (1xx|0[1-9]|00[1-8]|*5x*xxxx*x#|*2x*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8, [2-9]xxxxxxxxx|8, 10x.).
- Sometimes you have to make calls locally inside of the device. In this case, if IP address of a device is not known or periodically changed, you may use the reserved "{local}" word as the server address. It means sending an appropriate sequence of digits to the own device address.
- Example: (123@{local}) – 123 dialing number will be processed inside of the device locally.

Interception code configuration

You may establish interception code for specified group by using this command.

- Syntax: ABC@{pickup:X}
- where ABC – inteception code (for example*8);
- *X* – pickup group number (numbering pickup groups begins from 0).
- Example: 112@{pickup:0} – subscribers A and B are located in the same pickup group with 0 index. If a subscriber receives incoming call B subscriber can pick up a call and dial 112 digital combination.

Voice codec configuration

The signal processor of *RG-5400* encodes analogue voice traffic and fax/modem data into digital signal and performs its reverse decoding. Gateway supports the following voice codecs: G.711A, G.711U, G.729, G723.1, G.726-24, G.726-32.

G.711 is a PCM codec that does not employ a compression of voice data. This codec must be supported by all VoIP equipment manufacturers. G.711A and G.711U codecs differ from each other in encoding law (A-law is a linear encoding and U-law is non-linear). The U-law encoding is used in North America, and the A-law encoding—in Europe.

G.723.1 is a voice data compression codec, allows for two operation modes: 6.3kbps and 5.3kbps. G.723.1 codec has a voice activity detector and performs comfort noise generation at the remote end during period of silence.

G.729 is also a voice data compression codec with the rate of 8kbps. As with G.723.1, G.729 codec supports voice activity detector and performs comfort noise generation.

- *Codec 1..6*—you may select a codec and the .and an order of their usage. The highest priority codec should be specified in the 'Codec 1' field. For operation, you should specify at least one codec:
    - *Disabled*—codec will not be used;
    - G.711a—use G.711A codec;
    - G.711u—use G.711U codec;
    - G.723—use G.723.1 codec;
    - G.729—use G.729 codec.
    - G.726-24 – use G.726-24 codec;
    - G.726-32 – use G.726-32 codec;
    - G.711a (wide band) – use G.711a (wide band) codec;
    - G.711u (wide band) – use G.711u (wide band) codec.
- *Packetization time* – amount of milliseconds (ms) transmitted in a single RTP packet.
- *Dispersion time, ms* – parameter that cancels an echo caused by the voice signal dispersion. Parameter values may be specified in the interval from 2ms to 128ms.

You may specify alternative voice codecs for the selected direction. For each direction, you may specify the preferred codec for voice communication in the numbering schedule. Configuration is performed in the numbering schedule. For each direction, an additional codec configuration may be specified in parentheses after the 'codecs:' word. If you have to use multiple codecs, you may separate them with a comma ','. Multiple parameters may be specified for a single direction. In this case, separate them with a semicolon ';' - (param1:subparam1,subparam2; param2:subparam1,subparam2). SubparamX permitted values: g711a, g711u, g729, g723. param1 and param2 permitted values — 'codecs' and 'rfc2833_PT' respectivly.

Example: ([23]xxx(codecs:g729; rfc2833_PT:96)|8x.(codecs:g711a;g711u)).

Jitter buffer

Jitter is a deviation of time periods dedicated to packet delivery. Packet delivery delay and jitter are measured in milliseconds. Jitter value is higher for real time data transfers (e.g. voice or video data).

In RTP, also known as 'media stream protocol', there is a field for precision transmission time tag related to the whole RTP stream. Receiving device uses these time tags to learn when to expect the packet and whether the packet order has been observed. On the basis of this information, the receiving side will learn how to configure its settings in order to evade potential network problems such as delays and jitter. If the expected time for packet delivery from the source to the destination for the whole call period corresponds to the defined value, e.g. 50ms, it is fair to say that there is no jitter in such a network. But packets are delayed in the network frequently, and the delivery time period may fluctuate significantly (in the context of time-critical traffic). If the audio or video recipient application will play packets in the order of their reception time, voice (or video) quality will deteriorate significantly. For example, if the voice data is being transferred, there will be interruptions and interference in the voice.

The device features the following jitter buffer settings:

- *Minimum delay, ms* – minimum expected IP package network propagation delay;
- *Maximum delay, ms* – maximum expected IP package network propagation delay;
- *Threshold for immediate packet deletion, ms* – maximum amount of time for voice package removal from the buffer. The parameter value should be greater or equal to maximum delay;

- *Buffer optimization factor* – parameter used for jitter buffer size optimization. Recommended value is 0.

Fax and modem transmission

Fax may be transmitted using 711 voice codec or T.38 specialized codec for sending facsimile messages.

T.38 is a standard for sending facsimile messages in real time over IP networks. Signals and data sent by the fax unit are copied to T.38 protocol packets. Generated packets may feature redundancy data from previous packets that allows you to perform reliable fax transmissions through unstable channels.

- *Modem transmission*—select a codec to be used for data transmission when the gateway detects modem signals:
  - Disabled—modem signals will not be detected;
  - G.711a VBD – use G.711A codec in VBD mode;
  - G.711u VBD – use G.711U codec in VBD mode.

In VBD (Voice band data) mode, the gateway disables voice activity detection (VAD), comfort noise generator (CNG), and echo cancellers; this is necessary for establishing a modem connection.

✓ **Selected codec should also be enabled in voice codec list.**

- *Fax codec 1..3* – you may select a codec and an order of their usage. The highest priority codec should be specified in the 'Fax codec 1' field. For operation, you should specify at least one codec:
  - *Disabled*—codec will not be used.
  - G.711a – use G.711A codec;
  - G.711u – use G.711A codec;
  - T.38 – use T.38 protocol.

✓ **All fax codecs should be different! Also, when G.711a or G.711u codec is selected, the respective codec should be enabled in the device voice codec list.**

- *Accept transition to T.38* – when selected, incoming *re-invite* to T.38 from the opposite gateway will be enabled;
- *T.38 Redundancy* – add redundancy to T.38 packets; the value corresponds to the number of previous packets which is duplicated in each new T.38 packet. Such redundancy method is intended for packet loss during transmission.

Additional parameters

- *DTMF transmission* – DTMF tone transmission method:
  - *Inband* – inband transmission;
  - *RFC2833* – according to RFC2833 recommendation, as a dedicated payload in RTP voice packets;
  - *SIP info* – transfer messages via SIP in INFO requests.

- *Flash transmission*–Flash transmission method:
  - *SIP info* (Hookflash) – send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/Hook Flash* extansion as *signal=hf*;

  - *SIP info (DTMF Relay)* – send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/dtmf-relay* extansion as *signal=hf;*
  - *SIP info (Broadsoft)* – send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/Broadsoft* extansion as *event flashhook*;
  - SIP info (SSCC) – send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/sscc* extansion as *event flashhook*.

- *Payload type for RFC2833 packets* – payload type for packet transmission via RFC2833 (permitted values: from 96 to 127);
- *Same payload type for transmission and reception* – option is used in outgoing calls for payload type negotiation of events sent via RFC2833 (DTMF and Flash). When selected, event transmission and reception via RFC2833 is performed using the payload from 200Ok message sent by the opposite side. When unselected, event transmission is performed via RFC2833 using the payload from 200Ok being received, and reception—using the payload type from its own configuration (specified in the outgoing Invite);
- *Use voice activity detector* – when selected, enable voice activity detector;
- *Use echo cancellation* – when selected, use echo cancellation;
- *Use RTCP* – when selected, use RTCP for voice link monitoring:

  - *Transmission period* – RTCP packet transmission period, in seconds;
  - *Reception period* – RTCP message reception period measured in transmission period units; if there is not a single RTCP packet received until the reception period expires, RG 5400 will terminate the connection.

SIP profile basic settings

- *Use STUN* – when selected, use STUN (Session Traversal Utilities for NAT) protocol in order to define device public address (external NAT address). We recommend using this protocol for device operation through NAT;
- *STUN server address* – STUN server IP address or domain name; specify an alternative server port after the colon (default value is 3478);
- *STUN server polling period, seconds* – time period that defines transmission of a request to STUN server. The less the polling period, the faster the response to the public address changes.
- *Transport*— used protocol of a transport level:

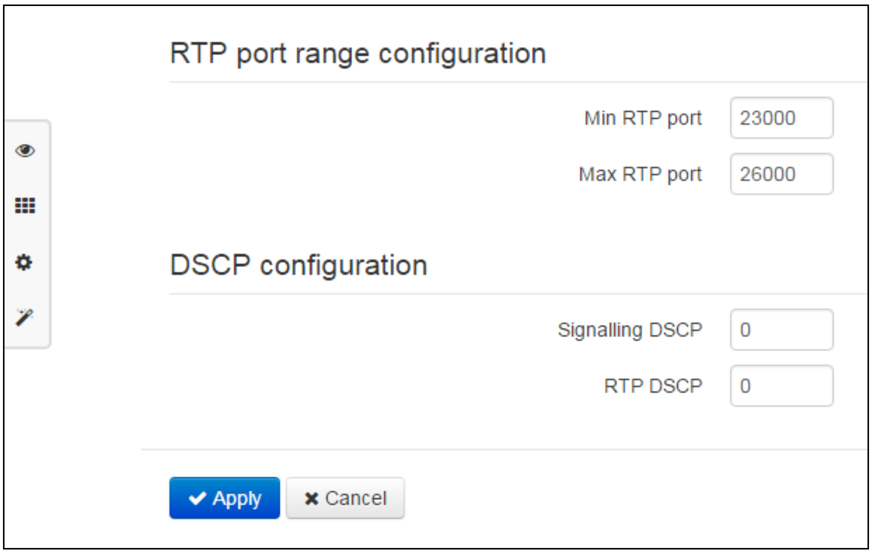
  - *UDP (preferred), TCP* – you may use UDP and TCP but UDP is recommended;
  - *TCP (preferred), UDP* – you may use UDP and TCP but TCP is recommended;
  - *Only UDP* – UDP is used only;
  - *Only TCP* –TCP is used only.

- *Silence mode* – mode of ignoring SIP requests to subscribers that don’t have user accounts on the device.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button*.*

3.7.3.4 ‘QoS’ submenu

In the 'QoS' submenu, you may configure Quality of Service functions.



RTP port range configuration

Min RTP port: 23000

Max RTP port: 26000

DSCP configuration

Signalling DSCP: 0

RTP DSCP: 0

RTP port range configuration

- *Min RTP port* – the lower limit of the RTP port range used for voice traffic transmission;
- *Max RTP port* – the upper limit of the RTP port range used for voice traffic transmission;

DSCP configuration

- *Signalling DSCP* – DSCP field value of IP packet header for signalling traffic (should be specified decimally, may take values from 0 to 63);
- *RTP DSCP* – DSCP field value of IP packet header for voice traffic (should be specified decimally, may take values from 0 to 63).

Setting 802.1P

- *802.1P for SIP* – priority value of the tagged Ethernet frame for traffic SIP messages (varies from 0 to 7);
- *802.1P for RTP* – priority value of the tagged Ethernet frame for RTP traffic (varies from 0 to 7).

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.3.5 'VAS management prefixes' submenu

In the 'VAS management prefixes' submenu, you may configure codes dialled from the phone unit in order to enable or disable VAS.

Subscribers may manage state of services from their phone units. The following functions are available:

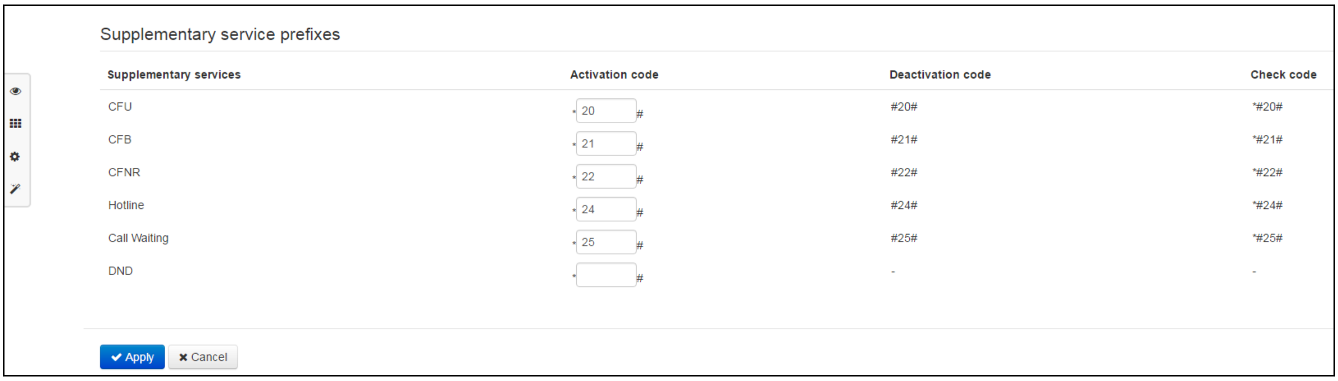
- Service activation – * service_code #;
- Service activity check – *# service_code #;
- Service cancellation - # service_code #;

In order to activate 'Call forward unconditional', 'Call forward on busy', 'Call forward on no answer', or 'Hotline/warmline' service, you should specify a phone number:

* service_code * phone_number #

When the activation code is entered or the service is cancelled, subscriber may hear a 'confirmation' tone (3 short tones) which means that the service has been activated or cancelled successfully.

After service confirmation code entry, the subscriber may hear either 'PBX response' tone (continuous) or a 'busy' tone (intermittent). 'PBX response' tone means that the service has been enabled and activated, 'busy' tone—that this service is disabled.



Supplementary service prefixes

Supplementary services	Activation code	Deactivation code	Check code
CFU	* 20 #	#20#	*#20#
CFB	* 21 #	#21#	*#21#
CFNR	* 22 #	#22#	*#22#
Hotline	* 24 #	#24#	*#24#
Call Waiting	* 25 #	#25#	*#25#
DND	* #	-	-

Subscriber service management

- VAS—VAS list:
  - *CFU (Call forward unconditional)*—when active, all incoming calls will be forwarded to the specified number;
  - *CFB (Call forward on busy)*—when active, all incoming calls will be forwarded to the specified number, if the subscriber is busy;
  - *CFNR (Call forward on no answer)*—when active, all incoming calls will be forwarded to the specified number, if there is no answer from the subscriber;
  - Hotline/warmline—when active, the defined phone number will be dialled upon expiration of the specific time period after the phone handset will have been picked up;
  - *Call waiting*—when active, the subscriber will receive notifications on incoming calls while being in a call state. Subscriber may accept, reject or ignore waiting call;
  - *DND (Do not disturb)*—this service allows the subscriber to put temporary restriction on all incoming calls.
- *Activation code*—service activation code;
- *Deactivation code*—service deactivation code;
- *Service status check code*—service activity check code.

Deactivation code and service status check code are generated automatically based on the activation code.

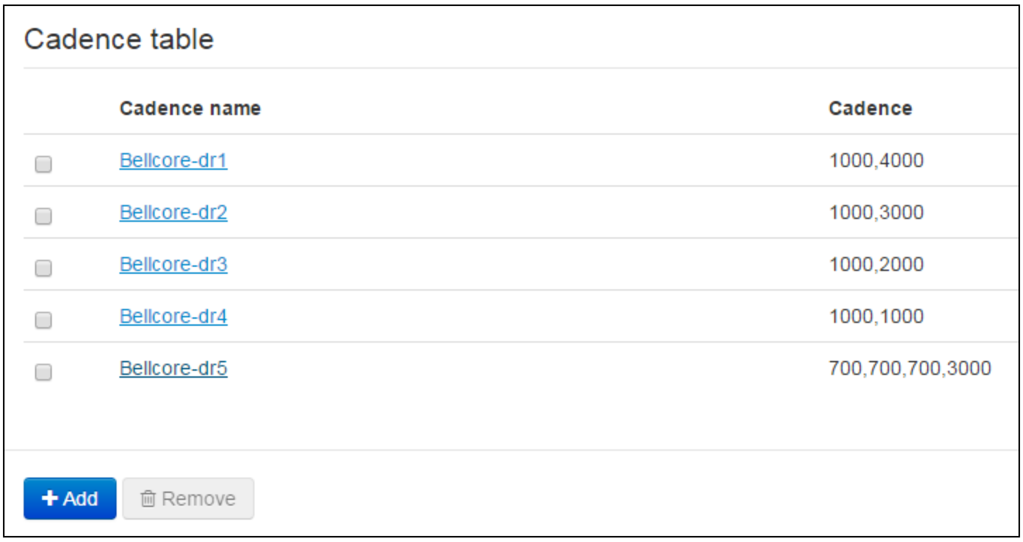
To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button .

3.7.3.6 ‘Call signal’ submenu

In the 'Call signal' submenu, you may configure an alternative call control signal (cadence) depending on the caller number or 'Alert-Info' header value in the incoming 'Invite'. Cadence value for each call signal is represented by the sequence of alternating pulses and pauses delimited by ',' or ';'. Pulse/pause duration should be defined in milliseconds and divisible by 100. Minimum pulse/pause duration is 200ms, maximum is 8,000ms.

To map a specific cadence to 'Alert-Info' header value in the incoming 'Invite', you should select the *'Process Alert-Info header'* checkbox in the respective SIP profile, and define the signal name in 'Signal name' field in cadence settings (e.g. Example-cadence). When 'Alert-Info' header value in the incoming 'Invite' is <http://127.0.0.1/Example-cadence>, cadence will be output into the line.

If the cadence is not found by the 'Alert-Info' header, attempt to find the cadence by the caller number will be taken. If the latter is absent, the standard call signal with the cadence '1000,4000' will be output.

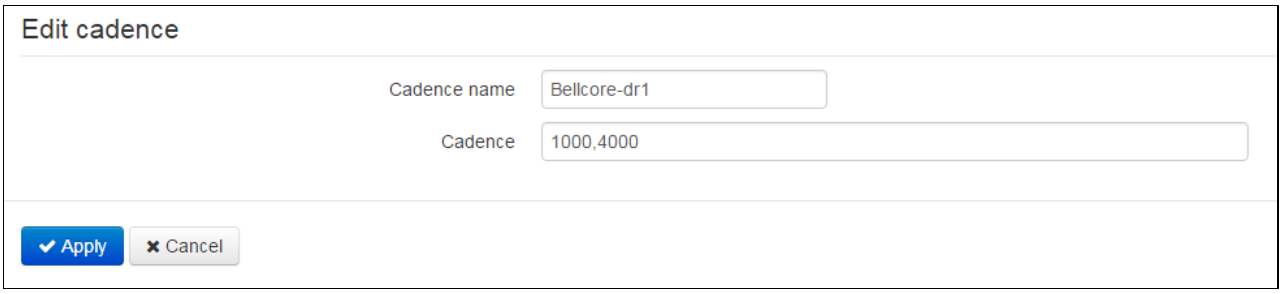


Cadence table

	Cadence name	Cadence
□	Bellcore-dr1	1000,4000
□	Bellcore-dr2	1000,3000
□	Bellcore-dr3	1000,2000
□	Bellcore-dr4	1000,1000
□	Bellcore-dr5	700,700,700,3000

To edit the specific signal, click the respective link in the *'Cadence name'* column.

To add a signal, click 'Add' button and enter the following settings:



Edit cadence

Cadence name: Bellcore-dr1

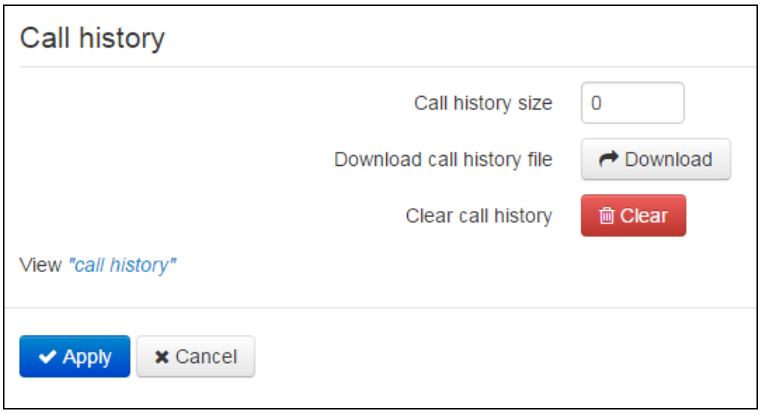
Cadence: 1000,4000

- *Cadence name*—name of the signal;
- *Cadence*—duration of the call voltage application to the phone unit, both values should be divisible by 100ms, minimum value is 200ms, maximum is 8,000ms;

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.3.7 'Call history' submenu

In the call history submenu, you may configure call history logging.



Call history

Call history size	0
Download call history file	Download
Clear call history	Clear

View *"call history"*

- *Call history size* – maximum number of log records, may take values from 0 to 10,000 strings. Enter '0' value to disable call history logging. When the defined log limit is reached, each consequent record will delete the oldest record in the beginning of the log;
- *Download call history file* – to save 'voip_history' file on a local PC, click 'Download' button;
- *Clear call history* **–** to clear call history, click 'Clear' button.

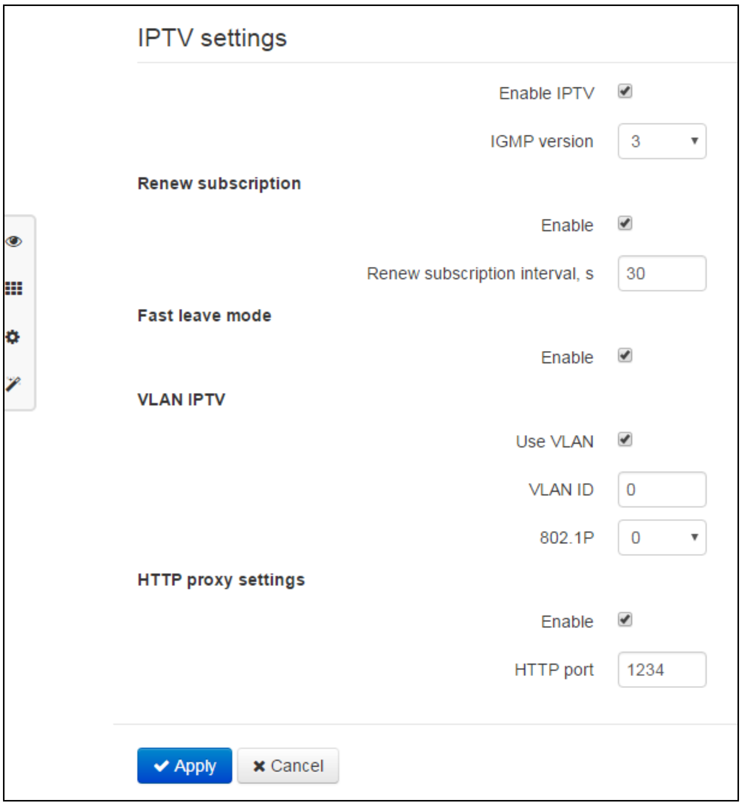
To view the call history, follow the *'View call history'* link. For parameter monitoring description, see Section *3.8.10 'Call history' submenu.*

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

3.7.4 'IPTV' menu

3.7.4.1 'IPTV' submenu

In the 'IPTV' submenu, you may configure IPTV service.



IPTV settings

Enable IPTV ☑

IGMP version 3

Renew subscription

Enable ☑

Renew subscription interval, s 30

Fast leave mode

Enable ☑

VLAN IPTV

Use VLAN ☑

VLAN ID 0

802.1P 0

HTTP proxy settings

Enable ☑

HTTP port 1234

- *Enable IPTV* – when checked, enable IPTV signal transmission from WAN interface of RG-5400 (from the provider network) to the devices connected to LAN interface (via Ethernet or Wi-Fi);
- *IGMP version* – version used for IGMP message transmission from the WAN interface (IPTV channel subscription activation or deactivation messages). Versions 2 and 3 are supported.

Renew subscription

- *Enable* – when checked, periodic transmission of messages containing a list of active IPTV channels is performed from WAN interface to the upstream server broadcasting IPTV signals. Disabling the periodic subscription update function is required if the upstream server disables IPTV channel broadcasting after the definite time period;
- *Renew subscription interval, seconds*—transmission interval for messages containing a list of active IPTV channels, in seconds. Define the update rate value less than the uplink server signal broadcasting timeout.

VLAN IPTV settings

- *Use VLAN* – when checked, use dedicated VLAN for IPTV service (VLAN number may be the same as for the Internet service or STB), otherwise IPTV will use the Internet service interface. This setting allows you to configure the interface for group traffic reception;
- *VLAN ID* – VLAN identifier for IPTV signal reception;

- *802.1P* – 802.1P marker (another name: *CoS – Class of Service*), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority). Utilized by QoS algorithms.

HTTP proxy settings

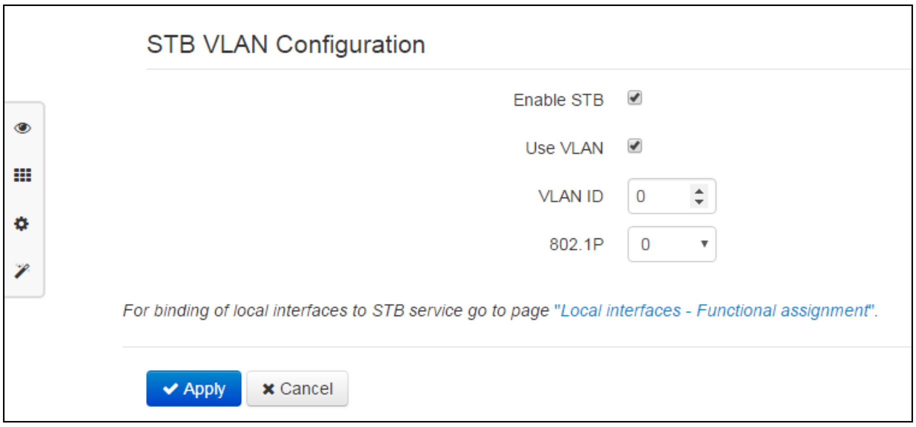
- *Enable*—when selected, enable HTTP proxy feature. HTTP proxy transforms UDP stream into HTTP stream utilizing TCP (reliable packet delivery protocol) in order to improve stream image quality, when the quality of the communication link in local area network is low. Function is usefull to watch IPTV via Wi-Fi;
- *HTTP port*—HTTP proxy port number that will be used for video streaming. Use this port to connect to IPTV streams being broadcast by *RG-5400*.

  For example, if *RG-5400* address on LAN interface is 192.168.0.1, proxy server port is 2354, and the desired channel 227.50.50.100 is being broadcast to UDP port 1234, you should specify the following stream address for VLC application: http://@192.168.0.1:2345/udp/227.50.50.100:1234.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.4.2 'STB' submenu

In the 'STB' submenu, you may configure dedicated VLAN for STB (Set Top Box) operation.



STB VLAN Configuration

Enable STB ☑

Use VLAN ☑

VLAN ID 0

802.1P 0

For binding of local interfaces to STB service go to page "Local interfaces - Functional assignment".

- *Enable STB*—when selected, STB mode will be enabled for the respective ports specified in 'Local interfaces' section;
- *Use VLAN*—when selected, use dedicated VLAN for STB (VLAN number may be the same as for the Internet or IPTV service), otherwise STB will operate without VLAN tag in the external network;
- *VLAN ID*—VLAN number to be used for STB service traffic transmission from the device WAN interface;
- *802.1P*—802.1P marker (another name: *CoS – Class of Service*), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority). Utilized by QoS algorithms.

To add LAN ports to STB service, use *'Local interface'* tile from the quick device configuration mode. Also, you may add 2.4 GHz or 5 GHz access point (or both). Thus, bridge is created between WAN and LAN (WLAN) interfaces of STB for transparent transmitting packets from STB via device and back. It should be noted, that when *'Use VLAN'* option is enabled, traffic will be transferred from WAN interface and received with configured VLAN tag, but on LAN interface (WLAN) the traffic will be untagged (the tag will be removed).

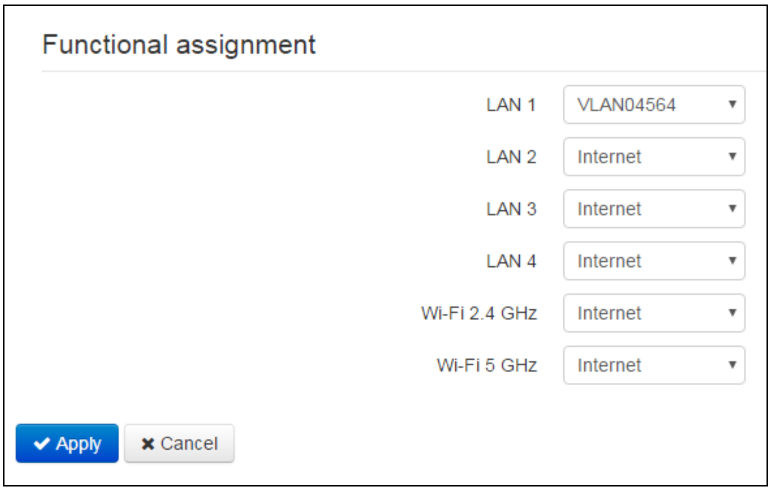
To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button*.*

3.7.5 ‘Local interfaces’ menu

In the 'Local interfaces' menu, you may establish functions for each interface.

3.7.5.1 ‘Functional assignment’ submenu

In the 'Functional assignment' submenu, you may establish service types for each port and Wi-Fi interface.



Functional assignment

LAN 1	VLAN04564
LAN 2	Internet
LAN 3	Internet
LAN 4	Internet
Wi-Fi 2.4 GHz	Internet
Wi-Fi 5 GHz	Internet

In the current firmware version, you may select the Internet, STB and user VLAN service types for local interfaces. At that, IPTV signal broadcasting is enabled for each local interface with active IPTV function.

Internet service type means that the current LAN port will be used for Internet access; STB service type means that it will be used for STB (Set-Top-Box) connection. At that, the Internet port is connected to WAN interface of the respective service by routing, and STB port is connected to STB service WAN interface by bridge (traffic is transferred transparently from LAN to WAN and back).

For STB service WAN interface configuration see 3.7.4.2.

Service type for 2.4 GHz and 5GHz Wi-Fi interfaces is assigned separately. Internet service type means that the current Wi-Fi interface performs Internet access via routing; STB service type means that the Wi-Fi interface is included into the STB bridge and connected transparently with WAN interface of this service.

Thus, RG-5400 device provides Internet access and TV STB connection via both wire channel and Wi-Fi in any frequency range.

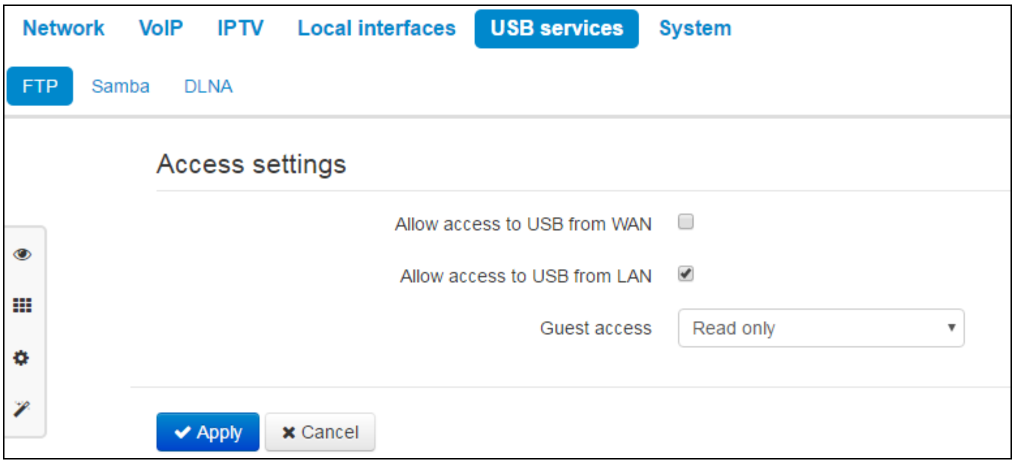
To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click *'Cancel'* button.

3.7.6 ‘USB services’ menu

Use the ‘USB services’ menu to configure protocols providing access to information and playback of media-files which are located on USB-drives connected to the device.

3.7.6.1 ‘FTP’ submenu

Use the submenu to configure access to a USB-drive via FTP.



Access settings

Allow access to USB from WAN □

Allow access to USB from LAN ☑

Guest access: Read only

To permit access to the connected USB device via FTP from external (via WAN-port) or internal network (via LAN port or Wi-Fi access point), set corresponding flags.

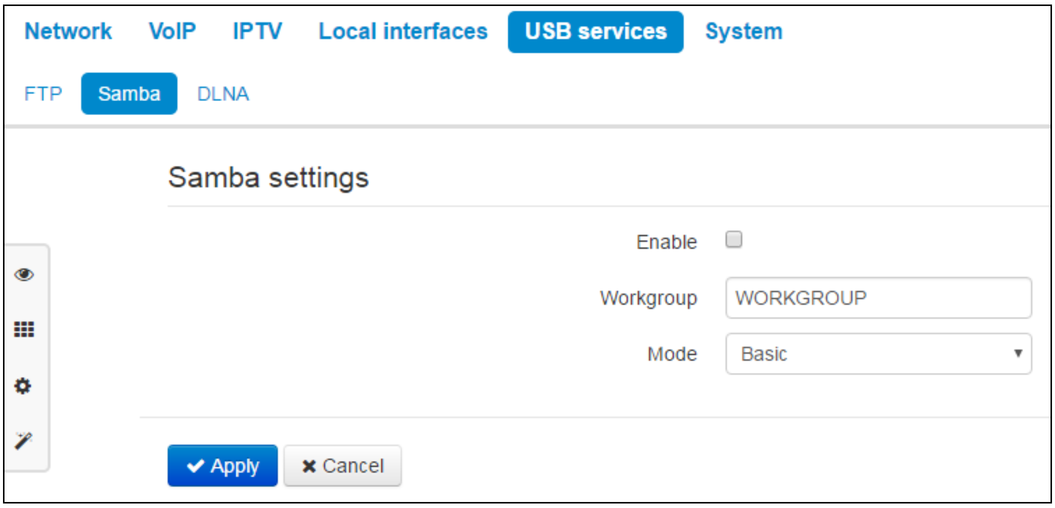
To permit access of anonymous user to the connected USB device, set the ‘Permit access for anonymous user’ flag.

To permit data recording on an USB device of an anonymous user, set the ‘Permit data recording for anonymous user’ flag.

To apply a new configuration and store settings into the non-volatile memory, click 'Apply' button. To discard changes, click 'Cancel' button.

3.7.6.2 'Samba' submenu

Use the submenu to configure access to an USB-drive via SAMBA protocol.



Samba settings

Enable □

Workgroup WORKGROUP

Mode Basic

Two types of protocol configuration are available: basic and extended.

Basic

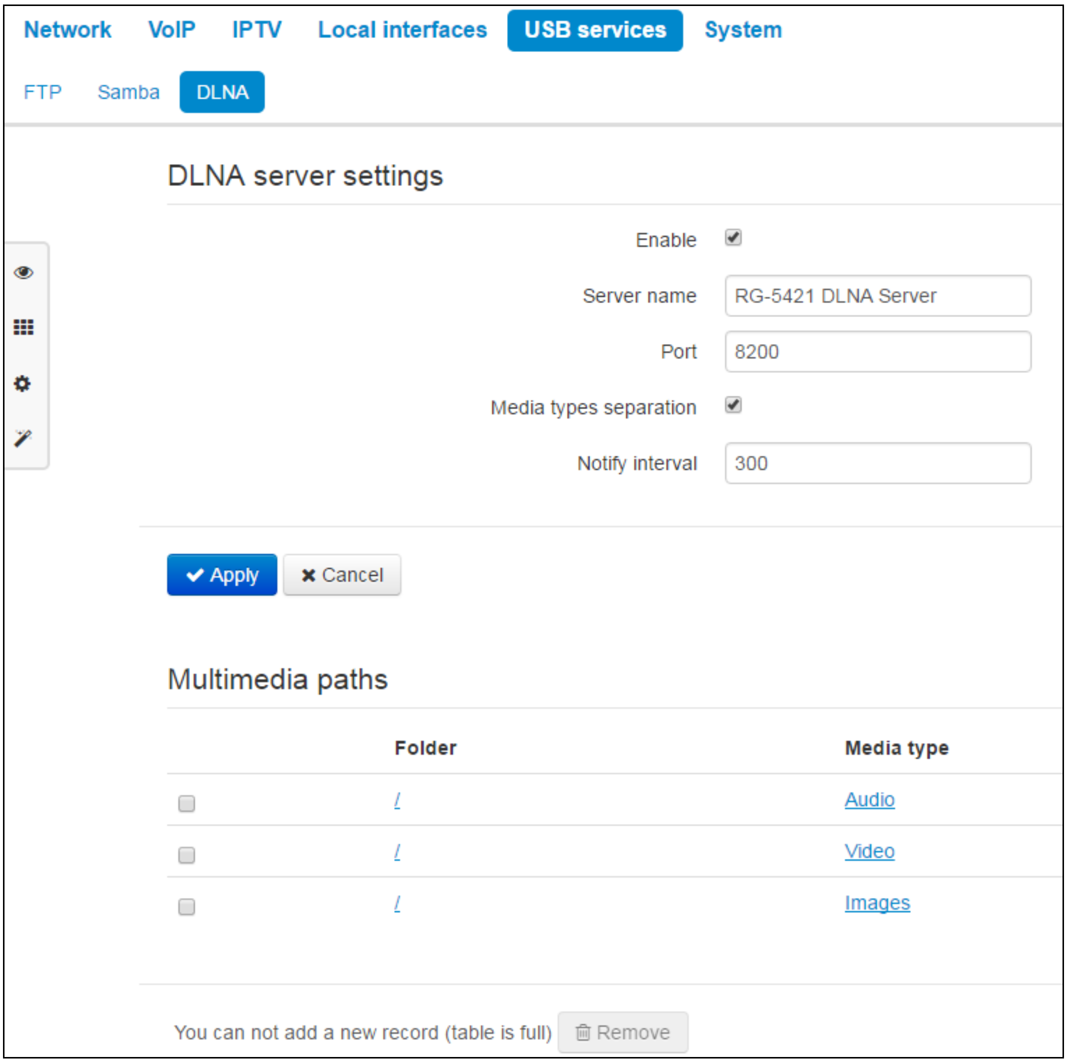
- *Enable* – parameter controls enabling/disabling of protocol operation;
- *Working group* – working group name for access.

Extended

- *Enable* – parameter controls enabling/disabling the protocol operation;
- *Working group* – name of a working group for access;
- *Users* – to configure click 'Add' button and enter the following data:
  - Samba's user name – user name used for authorization;
  - Password – password used for authorization.
- *Folders* – click 'Add' to configure the list of the directories accessible via protocol:
  - Folders – select a folder for granting access;
  - Name – enter folder name for displaying to users;
  - Description – for folder description;
  - Access – user list for accesss to the specified folder.

3.7.6.3 'DLNA' submenu

Use the submenu to configure access to media-files on the USB-drive for remote playback by DLNA technology.



DLNA server settings

Enable ☑

Server name: RG-5421 DLNA Server

Port: 8200

Media types separation ☑

Notify interval: 300

Multimedia paths

	Folder	Media type
□	/	Audio
□	/	Video
□	/	Images

You can not add a new record (table is full)

DLNA server configuration

- *Enable* – parameter controls enabling/disabling the server operation;
- *Server name* – parameter determines announced name of the DLNA server;
- *Port* – transport port used by server;
- *Separation of media types* – different media types are announced separately;
- *Send interval of SSDP-notification, sec* – parameter determines a time interval between SSDP-notification (the default value is 300 sec).

Paths to a multimedia

Use the section to assign folders for specific multimedia type.

✓ **You may specify several folders for multimedia files of the same type.**

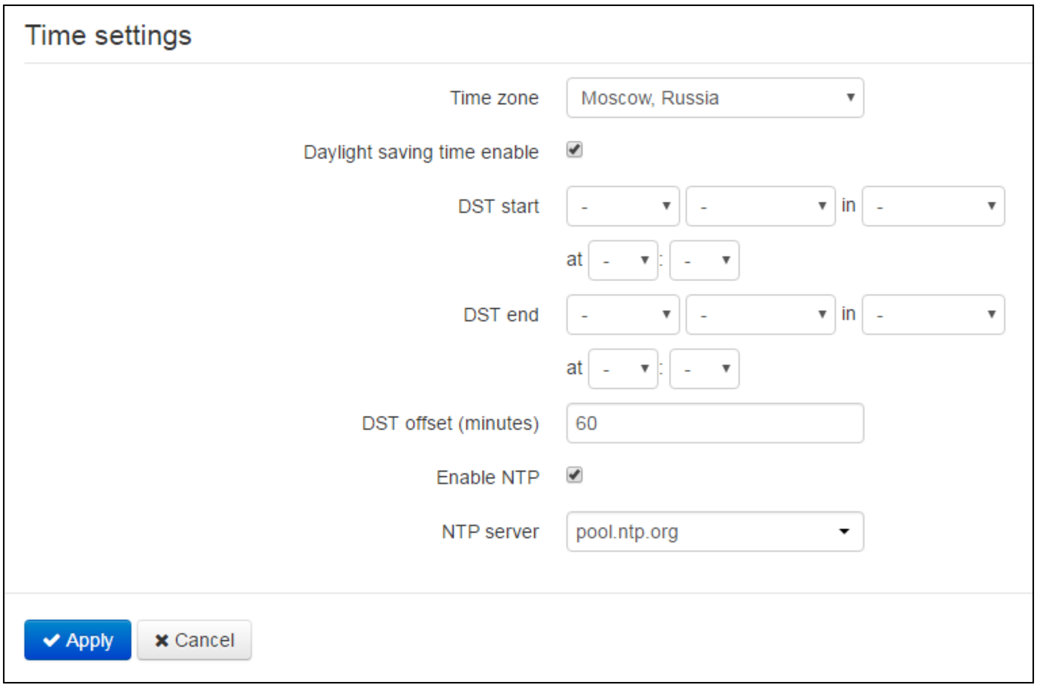
✓ **It is enough to specify a root of a USB-drive when separation of multimedia is disabled.**

3.7.7 ‘System’ menu

In the 'System' menu, you may configure settings for system, time and access to the device via various protocols, change the device password and update the device firmware.

3.7.7.1 ‘Time’ submenu

In the 'Time' submenu, you may configure time synchronization protocol (NTP).



Time settings

Time zone	Moscow, Russia
Daylight saving time enable	☑
DST start	- - in - at - : -
DST end	- - in - at - : -
DST offset (minutes)	60
Enable NTP	☑
NTP server	pool.ntp.org

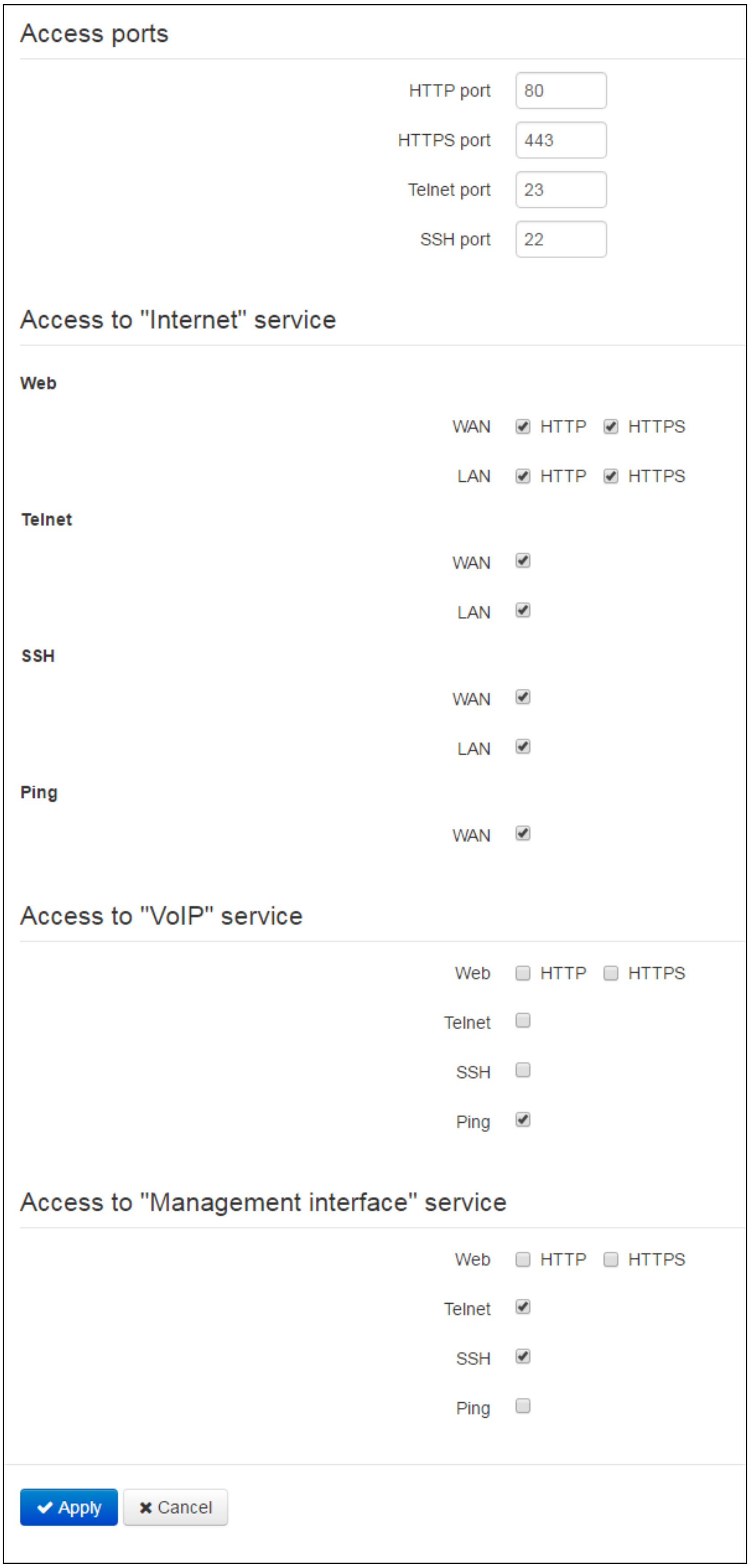
Time settings

- *Time zone* – allows you to set a timezone from the list according to the nearest city in your region;
- *Daylight saving time enable* – when checked, automatic daylight saving change will be performed automatically within the defined time period:
  - *DST start*—daylight saving change starting day.
  - *DST end*—daylight saving change ending day.
  - *DST offset (minutes)*—time shift period in minutes
- *Enable NTP* – select this checkbox to enable device system time synchronization with the particular NTP server;
- *Synchronization server* – time synchronization server IP address/domain name.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.7.2 ‘Access’ submenu

In the 'Access' submenu, you may configure the device access via WEB interface, Telnet and SSH.



Access ports

HTTP port 80

HTTPS port 443

Telnet port 23

SSH port 22

Access to "Internet" service

Web

WAN ☑ HTTP ☑ HTTPS

LAN ☑ HTTP ☑ HTTPS

Telnet

WAN ☑

LAN ☑

SSH

WAN ☑

LAN ☑

Ping

WAN ☑

Access to "VoIP" service

Web □ HTTP □ HTTPS

Telnet □

SSH □

Ping ☑

Access to "Management interface" service

Web □ HTTP □ HTTPS

Telnet ☑

SSH ☑

Ping □

Access ports

In this section, you may configure TCP ports for HTTP, HTTPS, Telnet and SSH services.

- *HTTP port*—number of the port that allows for the device WEB interface access via *HTTP*, default value is 80;
- *HTTPS port*—number of the port that allows for the device WEB interface access via *HTTPS* (secure connection), default value is 443;
- *Telnet port*—number of the port that allows for the device WEB interface access via *Telnet*, default value is 23;
- *SSH port*—number of the port that allows for the device WEB interface access via *SSH*, default value is 22.

You may use *Telnet* and *SSH* protocols in order to access the command line (Linux console).

Access to Internet service

To get a device access from the Internet service interfaces, set the following permissions:

Web, external network:

- *HTTP* – when selected, WAN port connection to the device WEB configurator is enabled via HTTP (insecure connection);
- *HTTPS* – when selected, WAN port connection to the device WEB configurator is enabled via HTTPS (secure connection).

Web, local network:

- *HTTP* – when selected, LAN port (or Wi-Fi wireless access point) connection to the device WEB configurator is enabled via HTTP (insecure connection);
- *HTTPS* – when selected, LAN port connection (or connection via Wi-Fi access point) to the device WEB configurator is enabled via HTTPS (secure connection).

Telnet:

Telnet is a protocol that allows you to establish mechanisms of control over the network. Allows you to remotely connect to the gateway from a computer for configuration and management purposes.

To enable the device access via Telnet protocol from the external (via WAN port) or internal (via LAN port or Wi-Fi wireless access point) network, select the appropriate checkboxes.

SSH:

SSH is a secure device remote control protocol. However, as opposed to Telnet, SSH encrypts all traffic, including passwords being transferred.

To enable the device access via SSH protocol from the external (via WAN port) or internal (via LAN port or Wi-Fi access point) network, select the appropriate checkboxes.

Ping:

ICMP-ping – mechanism realized in ICMPv4 and v6 protocols for control of the network device availability.

To permit response to the incoming ICMP-echo messages, set the corresponding flag.

Access to VoIP service:

In this section, you may configure access to VoIP service interface (to configure VoIP service interface, use IP—VoIP—Network configuration) through the WEB (HTTP or HTTPS), and also via Telnet, SSH and ICMP protocols. To enable access to any protocols listed above, select the appropriate checkboxes.

Access to VLAN servicre management:

Use this section to configure access to the management VLAN interface that allows for device management via HTTP, HTTPS, Telnet, SSH, ICMP protocols. To configure the interface, use **System—Management VLAN** page.To enable access to any protocols listed above, select the appropriate checkboxes.

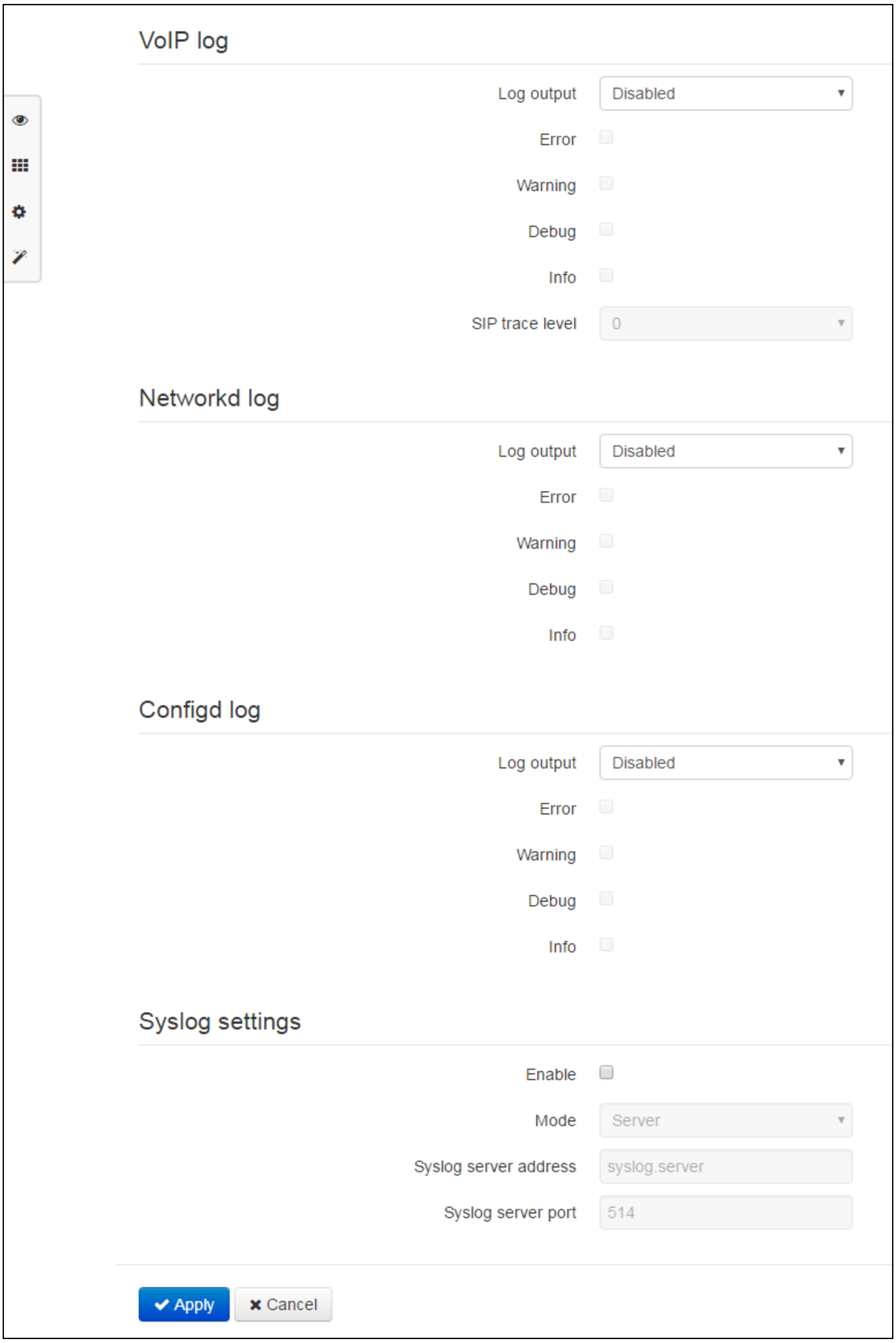
✓ **For Telnet and SSH protocol authorization, you may use default username *admin* and password *password*. After authorization, Linux console will become available that supports basic commands of the 'shell' command interpreter.**

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.7.3 ‘Log’ submenu

In the 'Log' submenu, you may configure output for various debug messages intended for device troubleshooting. Debug information is provided by the following device software modules:

- VoIP manager—deals with VoIP functions operations.
- System manager—deals with the device configuration according to the configuration file.
- Configuration manager—deals with the configuration file operations (config file reads and writes from various sources) and the device monitoring information collection.



VoIP log

Log output: Disabled
Error □
Warning □
Debug □
Info □
SIP trace level: 0

Networkd log

Log output: Disabled
Error □
Warning □
Debug □
Info □

Configd log

Log output: Disabled
Error □
Warning □
Debug □
Info □

Syslog settings

Enable □
Mode: Server
Syslog server address: syslog.server
Syslog server port: 514

VoIP log

- *Log output*—log message output direction:
  - *Disabled*—log is disabled;
  - *Syslog*—messages are output to remote server or local file via syslog protocol (for protocol configuration, see below);
  - *Console*—messages are output to the device console (requires connection via COM port adapter);
  - *Telnet*—messages are output to the telnet session; create *telnet* protocol connection first.

Given below is the configuration of VoIP log message types:

- *Errors*—select this checkbox, if you want to collect 'Error' type messages;
- *Warnings*—select this checkbox, if you want to collect 'Warning' type messages;
- *Debug*—select this checkbox, if you want to collect debug messages;
- *Info*—select this checkbox, if you want to collect information messages;
- *SIP trace level* – specify messages output level of VoIP SIP manager stack.

Configd log (Configuration manager log)

- *Log output*—log message output direction:
  - *Disabled*—log is disabled;
  - *Syslog*—messages are output to remote server or local file via syslog protocol (for protocol configuration, see below);
  - *Console*—messages are output to the device console (requires connection via COM port adapter);
  - *Telnet*—messages are output to the telnet session; create telnet protocol connection first.

Given below is the configuration of configuration manager log message types:

- *Errors*—select this checkbox, if you want to collect 'Error' type messages;
- *Warnings*—select this checkbox, if you want to collect 'Warning' type messages;
- *Debug*—select this checkbox, if you want to collect debug messages;
- *Info*—select this checkbox, if you want to collect information messages;

Configuration manager log

- *Log output*—log message output direction:
  - *Disabled*—log is disabled;
  - *Syslog*—messages are output to remote server or local file via syslog protocol (for protocol configuration, see below);
  - *Console*—messages are output to the device console (requires connection via COM port adapter);
  - *Telnet*—messages are output to the telnet session; create telnet protocol connection first.

Given below is the configuration of configuration manager log message types:

- *Errors*—select this checkbox, if you want to collect 'Error' type messages;
- *Warnings*—select this checkbox, if you want to collect 'Warning' type messages;
- *Debug*—select this checkbox, if you want to collect debug messages;

- *Info*—select this checkbox, if you want to collect information messages.

Syslog settings

If there is at least a single log (VoIP manager, system manager or configuration manager) is configured for Syslog output, you should enable Syslog agent that will intercept debug messages from the respective manager and send them to remote server or save them to a local file in Syslog format.

- *Enable*—when checked, user Syslog agent is launched;
- *Mode*—Syslog agent operation mode:
  - *Server*—log information will be sent to the remote Syslog server (this is the 'remote log' mode);
  - *Local file*—log information will be saved to the local file*;*
  - *Server and file*—log information will be sent to the remote Syslog server and saved to the local file.

Next, the following settings will be available depending on the selected Syslog agent mode:

- *Syslog server address*—Syslog server IP address or domain name (required for 'Server' mode);
- *Syslog server port*—port for Syslog server incoming messages (default value is 514; required for 'Server' mode);
- *File name*—name of the file to store log in Syslog format (required for 'File' mode);
- *File size, KB*—maximum log file size (required for 'File' mode).

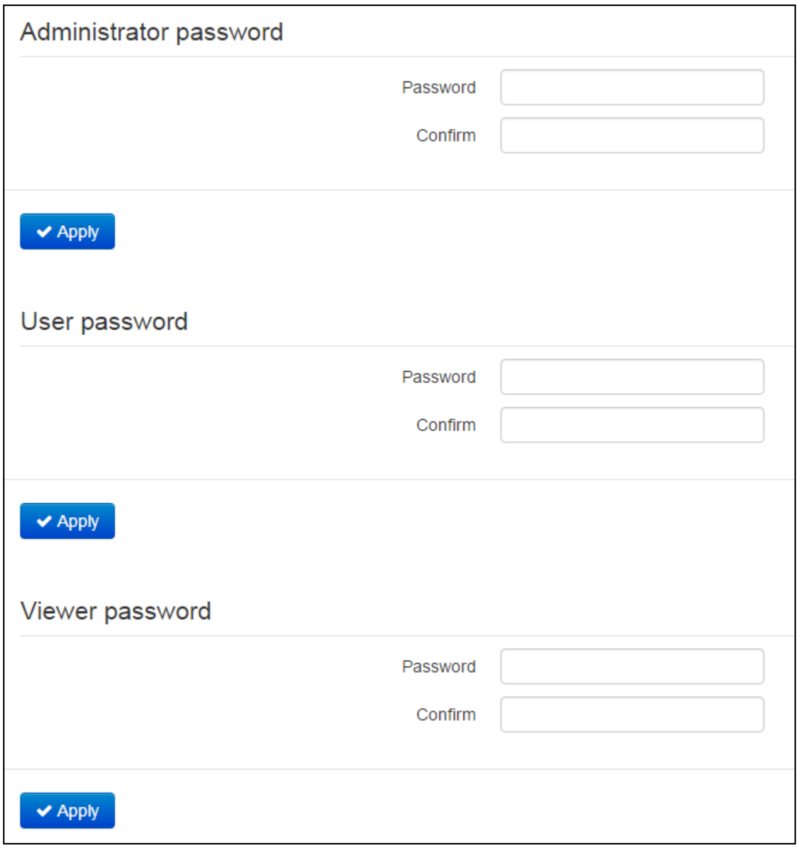
3.7.7.4 'Password' submenu

In the 'Passwords' submenu, you may define passwords for administrator, non-privileged user, and viewer access.

Defined passwords allow for the device access via WEB interface and also via Telnet and SSH protocols.

When signing into WEB interface, administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring. Non-privileged user (default password: **user**) may configure network settings (except for the Internet connection settings), may access the device status monitoring. Viewer (default password: **viewer**) may view the configuration and the device monitoring data only, without any editing permissions.

✓ **Administrator login: admin**
Non-privileged user login: user
Viewer login: viewer


Administrator password

Password:

Confirm:

User password

Password:

Confirm:

Viewer password

Password:

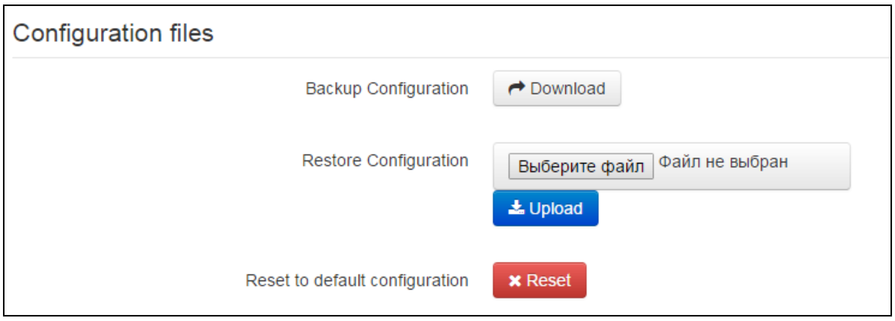
Confirm:

- *Administrator password*—enter administrator password in the respective fields and confirm it;
- *Password comfirmation* – enter password of non-privileged user in the respective fields and confirm it.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.7.5 'Configuration managment' submenu

In the 'Configuration management' submenu, you may save and update the current configuration.



Configuration files

Backup Configuration: Download

Restore Configuration: Выберите файл Файл не выбран

Upload

Reset to default configuration: ✖ Reset

Buckup configuration

To save the current device configuration to a local PC, click 'Download' button.

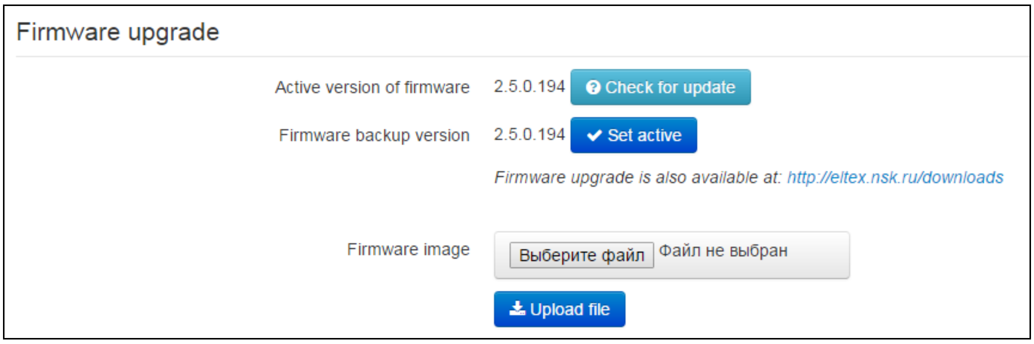
Restore configuration

- *Upload configuration archive to device*—select configuration file stored on a local PC. To update the device configuration, click *'Select file'* button, specify a file (in .tar.gz format) and click *'Upload'* button. Uploaded configuration will be applied automatically and does not require device reboot.

Reset to default configuration—to reset the device to default factory settings, click *'Reset'* button.

3.7.7.6 'Firmware upgrade' submenu

In 'Firmware upgrade' submenu, you may update the firmware of the device.



Firmware upgrade

Active version of firmware: 2.5.0.194 Check for update

Firmware backup version: 2.5.0.194 ✓ Set active

Firmware upgrade is also available at: http://eltex.nsk.ru/downloads

Firmware image: Выберите файл Файл не выбран

Upload file

- *Active firmware version*— current installed firmware version;
- *Check for updates*—click this button to check the availability of the latest firmware version. With this function, you may quickly check the latest firmware version and update the firmware, if necessary.
- *Backup firmware version* – installed firmware version which can be used in case of problems with the current active firmware virsion;
- *Activate* – buttom allowing you to make a backup of the active firmware version. In order to get that done reboot the device.

Firmware update check function requires Internet access.

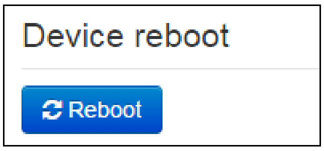
You may update the device firmware manually by downloading the firmware file from the web site http://eltex.nsk.ru/downloads and saving it on the computer. To do this, click the 'Select file' button in the *'Firmware image'* field, and specify path to firmware .tar.gz format file.

To launch the update process, click 'Upload file' button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed.

Do not switch off or reboot the device during the firmware update. If it can not be avoided and uploading firmware image was recorded partly gateway will try to launch backup firmware image (if it is available).

3.7.7.7 'Reboot' submenu

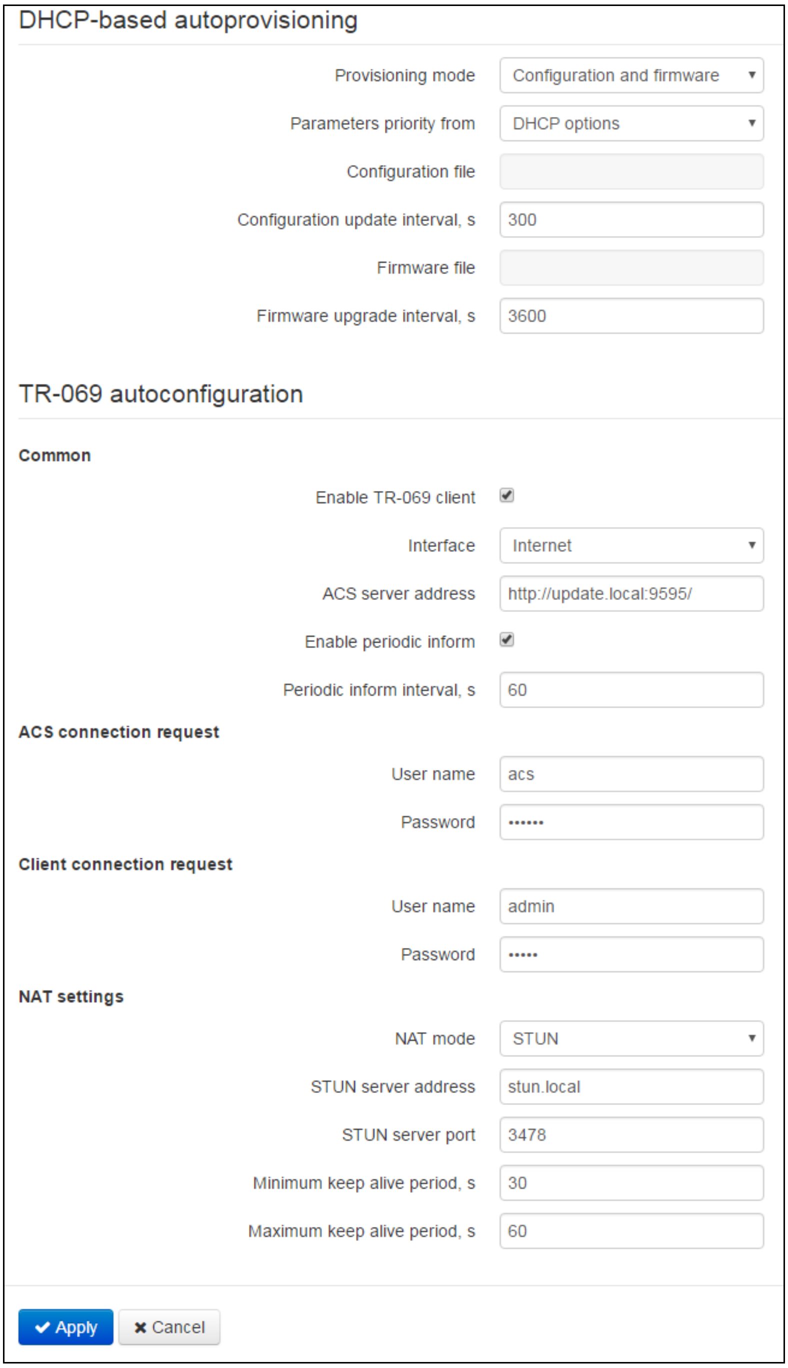
In the 'Reboot' submenu, you may reboot the device.



Click the 'Reboot' button to reboot the device. Device reboot process takes approximately 1 minute to complete.

3.7.7.8 'Autoprovosioning' submenu

In the 'Autoconfiguration' submenu, you may configure DHCP-based autoprovisioning algorithm and TR-069 subscriber device automatic configuration protocol.



DHCP-based autoprovisioning

Provisioning mode	Configuration and firmware ▾
Parameters priority from	DHCP options ▾
Configuration file	
Configuration update interval, s	300
Firmware file	
Firmware upgrade interval, s	3600

TR-069 autoconfiguration

Common

Enable TR-069 client	☑
Interface	Internet ▾
ACS server address	http://update.local:9595/
Enable periodic inform	☑
Periodic inform interval, s	60

ACS connection request

User name	acs
Password	••••••

Client connection request

User name	admin
Password	•••••

NAT settings

NAT mode	STUN ▾
STUN server address	stun.local
STUN server port	3478
Minimum keep alive period, s	30
Maximum keep alive period, s	60

DHCP-based autoprovisioning:

– *Automatic update* – select the device update mode; there are several options available:

- *Disabled*—automatic updates of the device configuration and firmware are disabled;
- *Configuration and firmware*—periodic updates of the device configuration and firmware are enabled;
- *Configuration only*—only periodic updates of the device configuration are enabled;
- *Firmware only*—only periodic updates of the device firmware are enabled.

- *Parameter priority from*—this parameter manages names and locations of configuration and firmware files:
  - *Static settings* – paths to configuration and firmware files are defined by the *'Configuration file'* and *'Firmware file'* settings accordingly; for detailed algorithm operation, see Section 6;
  - *DHCP options* – paths to configuration and firmware files are defined by the DHCP Option 43 and 66 (to do this, you should select DHCP for the Internet service); for detailed algorithm operation, see Section 6;
- *Configuration file*– full path to configuration file—defined in URL format (at this time, you may upload configuration files via TFTP and HTTP protocols):

  tftp://<server address>/<full path to cfg file>
  http://<server address>/<full path to cfg file>
  where < server address > – address of HTTP or TFTP server (domain name or IPv4),
  < full path to cfg file > – full path to firmware file on server;

- *Configuration update interval, seconds*—time period in seconds that will be used for periodic device configuration update; if 0 is selected, device will be updated only once—immediately after the device startup;
- *Firmware file*—full path to firmware file defined in URL format (at this time, you may upload firmware files via TFTP and HTTP protocols):

  tftp://<server address>/<full path to firmware file>
  http://<server address>/<full path to firmware file>
  where < server address > – address of HTTP or TFTP server (domain name or IPv4),
  < full path to firmware file > – full path to firmware file on server;

- *Firmware update interval, seconds*—time period in seconds that will be used for periodic device firmware update; if 0 is selected, device will be updated only once—immediately after the device startup.

For detailed DHCP-based automatic update algorithm, see Section 6.

TR-069 autoconfiguration:

Common:

- *Enable TR-069 client*—when selected, integrated TR-069 protocol client will be enabled;
- *Interface*—select the interface to work via TR-069 protocol. If *'Management VLAN'* interface is enabled on the gateway, this VLAN will be used for TR-069 protocol operation automatically. Interface selection setting will be disabled;
- *ACS address*– autoconfiguration server address. Enter address in the following format http://<address>:<port> or https://<address>:<port> (<address> – ACS server IP address or domain name, <port> – ACS server port, default value is 10301). In the second case , the client will use secure HTTPS protocol for information exchange with ACS;
- *Enable periodic inform*—when selected, integrated TR-069 client performs periodic ACS server polling at intervals equal to 'Periodic inform interval' value, in seconds. Goal of the polling is to identify possible changes in the device configuration.

ACS connection request:

- *Username, password*—username and password used by client to ACS access.

Client connection access:

- *Username, password*— username and password used by ACS server to access TR-069 client .

NAT settings:

If there is a NAT (network address translation) between the client and ACS server, ACS server may not be able to establish the connection to client without specific technologies intended to prevent such situations. These technologies allow the client to identify its so called public address (NAT address or in other words external address of a gateway, that covers the client). When public address is identified, the client reports it to the server that uses this public address for establishing connection to the client in the future.

- *NAT mode*—identifies the method, that will be used by client for obtaining its public address information. The following modes are possible:

  - *STUN*—use STUN protocol for public NAT address discovery;
  - *Manual*—manual mode, when public address is explicit in configuration; in this mode, you should add a forwarding rule on a device that acts as a NAT for TCP port used by TR-069 client;
  - *Off—NAT will not be used*—this mode is recommended only when the device is directly connected to ACS server without network address translation. In this case public address will match local client address.

When choosing STUN mode, you should define the following settings:

- *STUN server address*—STUN server IP address or domain name;
- *STUN server port*—STUN server UDP port (default value is 3478);
- *Minimum keep alive period and maximum keep alive period, in seconds* – define the time interval for periodic transmission of messages to STUN server in order to identify public address changes.

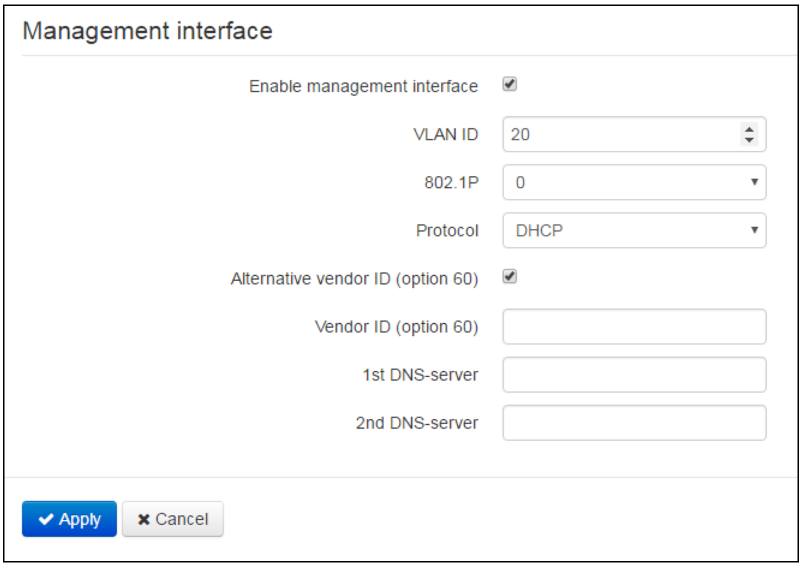
When *Manual* mode is selected the client public address should be entered manually via 'NAT address' parameter (address should be entered in IPv4 format).

TR-069 protocol allows for comprehensive device configuration, software updates, reading device information (software version, model, serial number, etc.), complete configuration file downloading/uploading, remote device restart (TR-069, TR-098, TR-104 specifications are supported).

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.7.9 'VLAN management' submenu

Use the 'VLAN management' submenu to configure the network interface and establish the device network management via HTTP, HTTPS, Telnet or SSH protocols.



Management interface

Enable management interface	☑
VLAN ID	20
802.1P	0
Protocol	DHCP
Alternative vendor ID (option 60)	☑
Vendor ID (option 60)	
1st DNS-server	
2nd DNS-server	

- *Enable management interface* – when checked, the device management can be performed in dedicated VLAN numer of which is specified in 'VLAN ID' field*;*
- *802.1P*—802.1P marker (another name: *CoS – Class of Service*), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority);
- *Protocol*—select address assigning protocol for the interface:

▪ *Static*—operation mode where IP address and all the necessary settings for WAN interface are assigned manually. When 'Static' type is selected, the following parameters will be available for editing:

  - *IP address*—specify the IP address for the management interface;
  - *Netmask*—subnet mask for the management interface;
  - *Default gateway*—default gateway IP address for the management interface;
  - *1st DNS-server, 2nd DNS-server*—DNS server IP addresses required for the gateway autoconfiguration protocols' operation; to configure protocols, use **System**—**Autoconfiguration** page.

▪ DHCP—operation mode where IP address, subnet mask, DNS address and other necessary settings for the interface operation (e.g. static routes) are automatically obtained from DHCP server. If you are unable to obtain DNS server addresses from the provider, you may specify them manually using 'Primary DNS' and 'Secondary DNS' fields. Manually defined addresses will have a priority over DNS addresses obtained via DHCP.

▪ For DHCP, you may specify the required value for Option 60.

  - *Alternative Vendor ID (Option 60)*—when selected, the device transmits *Vendor ID (Option 60)* field value in Option 60 DHCP messages (Vendor class ID). If the field is empty, Option 60 will not be transmitted in DHCP messages.
    If the *Alternative Vendor ID (Option 60)* checkbox is not selected, the default value will be transmitted in Option 60 in the following format:
    [VENDOR: device vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:** serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**firmware version**]**

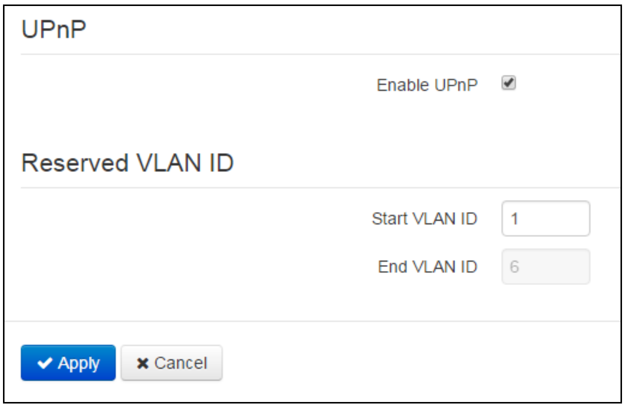
    Example:

▪ [VENDOR:Eltex][DEVICE:RG-5421G-Wac][HW:1.2][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.1.0]

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

3.7.7.10 'Additional settings' submenu

In 'Additional settings' submenu, you may enable UPnP.



UPnP

Enable UPnP ☑

Reserved VLAN ID

Start VLAN ID 1

End VLAN ID 6

— *Enable UPnP*—when selected, UPnP will be active. UPnP is used by some applications (for example, DC clients, such as FlylinkDC++) for automatic creation of forwarding rules for TCP/UDP ports used by these applications on the uplink router. We recommend turning UPnP on in order to enable file sharing services within the network.

Reserved VLAN ID

Reserved VLAN IDs are required for solving intrasystem tasks of the gateway and may be changed depending on the VLAN ID being used for the system:

— *Start VLAN ID*—starting VLAN ID value in the reserved range, may take values in range [1-4090];

— *End VLAN ID*—ending VLAN ID value in the reserved range. This setting is unavailable for editing and calculated automatically.

To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button.To discard changes, click *'Cancel'* button.

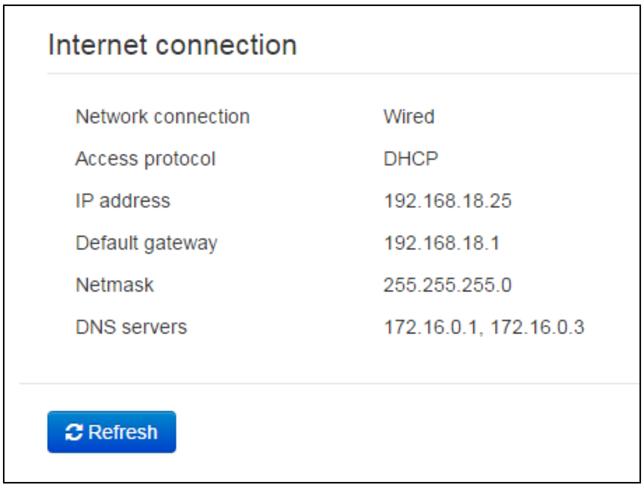
3.8 System monitoring

To switch to the 'System monitoring' mode, select 'Monitoring' from the left-hand side panel.

Some pages do not feature automatic update of the device monitoring data. To obtain the current information from the device, click ⟳ Refresh **button.**

3.8.1 'Internet' submenu

In the 'Internet' submenu, you may view basic network settings of the device.



Internet connection

Network connection	Wired
Access protocol	DHCP
IP address	192.168.18.25
Default gateway	192.168.18.1
Netmask	255.255.255.0
DNS servers	172.16.0.1, 172.16.0.3

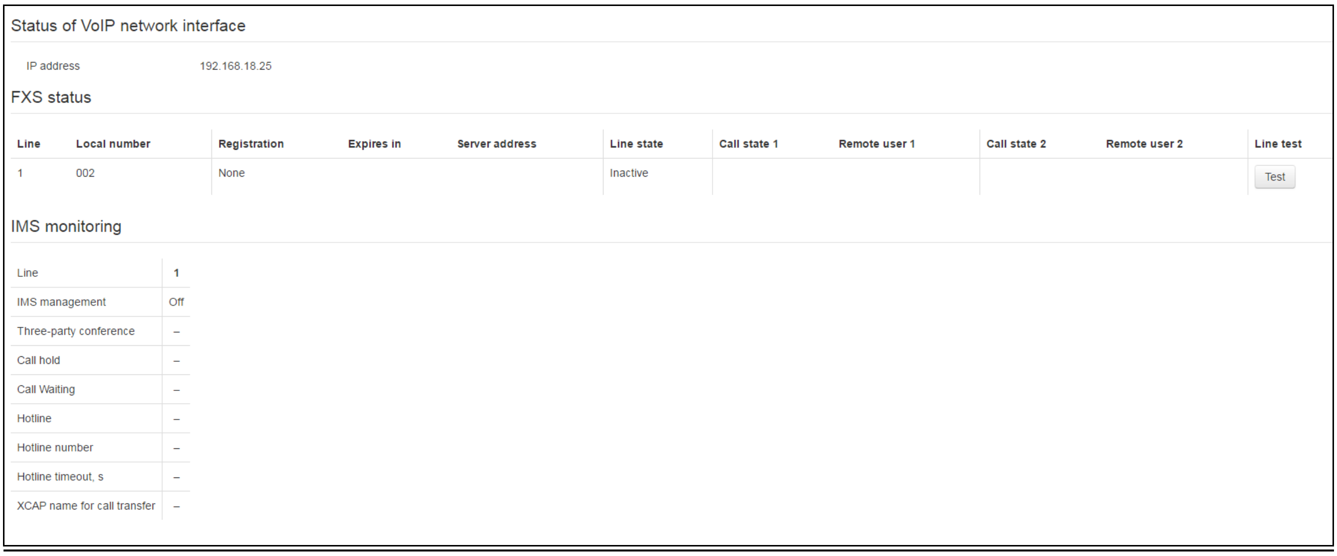
Internet Access

- Network connection—method of connection to data network. To configure the connection, use **Network—Internet** section:
  - *Wired*—connection to the provider network is established through the WAN port using copper-wire or optical patch cord;
  - *3G/4G USB modem*—connection to the provider network is established using 3G/4G USB modem connected to USB port on the device rear panel;
  - *Wi-Fi-client* – connection to the provider network is established using active Wi-Fi access point. In this case, RG5400 acts as Wi-Fi client.

- *Access protocol*—protocol used for the Internet access;
- *IP address*—device IP address in the external network;
- *IP address in the internal provider network*—IP address used within the internal provider network for access to local network resources of the provider.

3.8.2 'VoIP' submenu

In 'VoIP' submenu, you may view VoIP network interface status, monitor subscriber units and status of registration call groups, test lines, and monitor IMS.



Status of VoIP network interface

IP address	192.168.18.25

FXS status

Line	Local number	Registration	Expires in	Server address	Line state	Call state 1	Remote user 1	Call state 2	Remote user 2	Line test
1	002	None			Inactive					Test

IMS monitoring

Line	1
IMS management	Off
Three-party conference	–
Call hold	–
Call Waiting	–
Hotline	–
Hotline number	–
Hotline timeout, s	–
XCAP name for call transfer	–

VoIP network interface status

- *IP address*—IP address for VoIP service network interface.

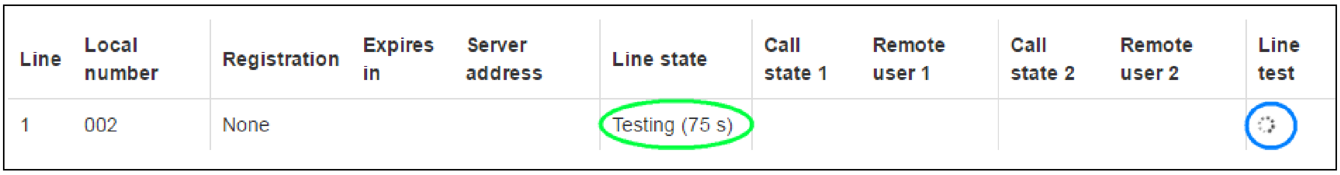
Monitoring of subscriber units

- *Line*—device subscriber unit number;
- *Local number*—subscriber phone number assigned to this subscriber port;
- *Registration*—state of registration on proxy server for the group phone number:
  - *Disabled*—SIP server registration function is disabled in SIP profile settings;
  - *Error*—registration was unsuccessful;
  - *Completed*—registration on SIP server successfully completed.
- *Expires in*—expiration time of subscriber port registration on SIP server;
- *Server address*—address of the server that the subscriber line has been registered at for the last time;
- *Line state*—physical line status. The line may have one of the following states:
  - *Inactive*—the phone handset is on-hook (or subscriber port is disabled), normal operation;
  - *Active*—the phone handset is off-hook; 'PBX response' tone, ringback tone, or error tone is transmitted into the line, or the line is in the call state;
  - *Ringing tone*—ringing tone is supplied to the phone headset (during the incoming call);
  - *Test*—line testing started.

- *Call state 1, 2*—each subscriber port may support up to 2 communication sessions simultaneously. In this field you may see the state of the call with the respective remote subscriber. The call may have one of the following states:

  - *Dialling number*—call is being dialled from the phone unit;
  - *Busy*—call has cleared back for some reason, busy tone is transmitted into the line;
  - *Outgoing call*—remote subscriber is being dialled, ringback tone is transmitted into the line;
  - *Incoming call*—incoming call is being received at the phone port, ringing tone is transmitted into the line;
  - *Conversation*—voice connection is established with the remote subscriber;
  - *Opposite on hold*—remote subscriber is on hold;
  - *Local on hold*—local subscriber has been put on hold by the remote subscriber;
  - *Error, put phone onhook*—error tone is transmitted into the line. As a rule, error tone is played on the busy signal timeout expiration (configured separately for each line), when the subscriber doesn't put the phone onhook.

- *Remote user 1, 2*—remote subscriber phone number for each communication session.
- *Line test*—click the 'Test' button to launch the subscriber line testing. Process status is represented by a countdown timer (in the 'Line state' column) indicating the remaining test time. You cannot run the test for multiple lines simultaneously. Test duration—80 seconds. Subscriber unit is blocked for the time of the test—it will not be able to make or receive calls.

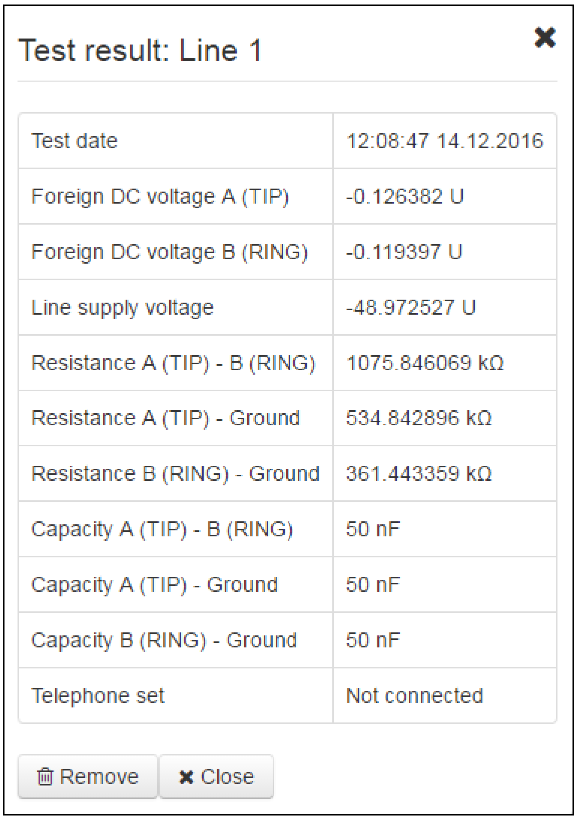


Line	Local number	Registration	Expires in	Server address	Line state	Call state 1	Remote user 1	Call state 2	Remote user 2	Line test
1	002	None			Testing (75 s)					

To see the results when the test finishes, click 🔍 button in the 'Line test' column. Results are represented in the table mode and contain the following data:

- Test date
- TIP wire constant extraneous voltage
- RING wire constant extraneous voltage
- Line power voltage
- Voltage between TIP and RING wires
- Voltage between TIP wire and ground
- Voltage between RING wire and ground
- Capacity between TIP and RING wires
- Capacity between TIP wire and ground
- Capacity between RING wire and ground

Line 1 test result example:



Test result: Line 1

Test date	12:08:47 14.12.2016
Foreign DC voltage A (TIP)	-0.126382 U
Foreign DC voltage B (RING)	-0.119397 U
Line supply voltage	-48.972527 U
Resistance A (TIP) - B (RING)	1075.846069 kΩ
Resistance A (TIP) - Ground	534.842896 kΩ
Resistance B (RING) - Ground	361.443359 kΩ
Capacity A (TIP) - B (RING)	50 nF
Capacity A (TIP) - Ground	50 nF
Capacity B (RING) - Ground	50 nF
Telephone set	Not connected

IMS monitoring

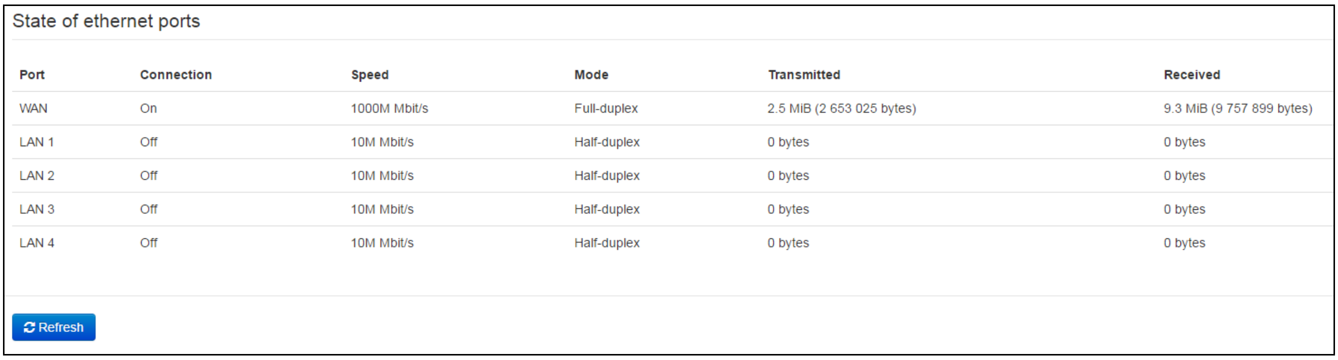
IMS monitoring shows the state (active or inactive) for some services on the subscriber line provided that the remote control from IMS server is enabled for this line (IP Multimedia Subsystem).

- *Management from IMS*—shows whether the subscriber line service remote control from IMS server is enabled (configured in SIP profile, see *'Profiles'* submenu);
- *Three-way conference*—shows whether the 'Three-way conference' service activation command is received from IMS server;
- *Call hold*—shows whether the 'Call hold' service activation command is received from IMS server;
- *Call waiting*—shows whether the 'Call waiting' service activation command is received from IMS server;
- *Hot/warm line*—shows whether the 'Hotline' service activation command is received from IMS server;
- *Hotline number*—shows the 'Hotline' service phone number in the activation command from IMS server;
- *Hotline timeout, seconds*—show the dialling timeout for the 'Hotline' service in the activation command from IMS server;
- *Name of the 'Call transmittion' service* - shows the name used for service.

✓ – service is active;
✗ – service is inactive.

3.8.3 ‘Ethernet ports’ submenu

In the 'Ethernet ports' submenu, you may view the device Ethernet port state.



State of ethernet ports

Port	Connection	Speed	Mode	Transmitted	Received
WAN	On	1000M Mbit/s	Full-duplex	2.5 MiB (2 653 025 bytes)	9.3 MiB (9 757 899 bytes)
LAN 1	Off	10M Mbit/s	Half-duplex	0 bytes	0 bytes
LAN 2	Off	10M Mbit/s	Half-duplex	0 bytes	0 bytes
LAN 3	Off	10M Mbit/s	Half-duplex	0 bytes	0 bytes
LAN 4	Off	10M Mbit/s	Half-duplex	0 bytes	0 bytes

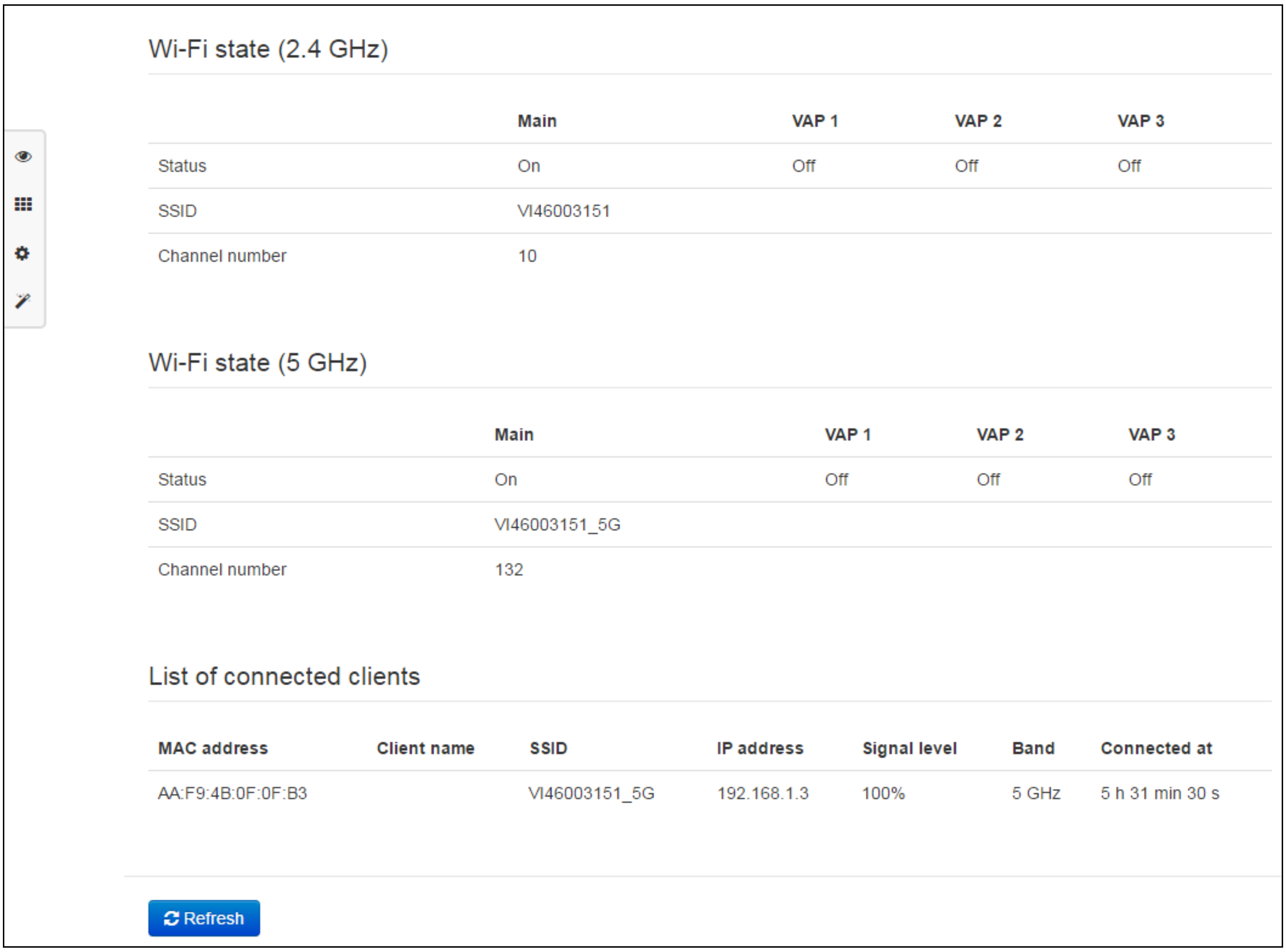
Ethernet port status

- *Port* – port name:
  - *WAN* – external network port;
  - *LAN 1..4* – local area network port.
- *Connection*—status of the connection to this port:
  - *Enabled*—network device is connected to the port (link is active);
  - *Disabled*—network device is not connected to the port (link is inactive).
- *Speed*—data rate of the external network device connected to the port (10/100/1000Mbps);
- *Mode*—data transfer mode:
  - *Full-duplex* – full duplex;
  - *Half-duplex* – half-duplex;
- *Transmitted* —quantity of bytes sent from the port;
- *Received* – quantity of bytes received by the port.

To obtain actual information on the Ethernet port state, click 'Update' button.

3.8.4 'Wi-Fi' submenu

In the 'Wi-Fi' submenu, you may view information about clients connected to a Wi-Fi access point.



Wi-Fi state (2.4 GHz)

	Main	VAP 1	VAP 2	VAP 3
Status	On	Off	Off	Off
SSID	VI46003151			
Channel number	10			

Wi-Fi state (5 GHz)

	Main	VAP 1	VAP 2	VAP 3
Status	On	Off	Off	Off
SSID	VI46003151_5G			
Channel number	132			

List of connected clients

MAC address	Client name	SSID	IP address	Signal level	Band	Connected at
AA:F9:4B:0F:0F:B3		VI46003151_5G	192.168.1.3	100%	5 GHz	5 h 31 min 30 s

Wi-Fi status

- *Status* –status of a Wi-Fi network:
  - *Disabled* – Wi-Fi network is disabled;
  - *Enabled* – Wi-Fi network is enabled.
- *Network ID (SSID)* – Wi-Fi access point name according to frequency range;
- *Channel number* – current channel number used by access point according to frequency range.

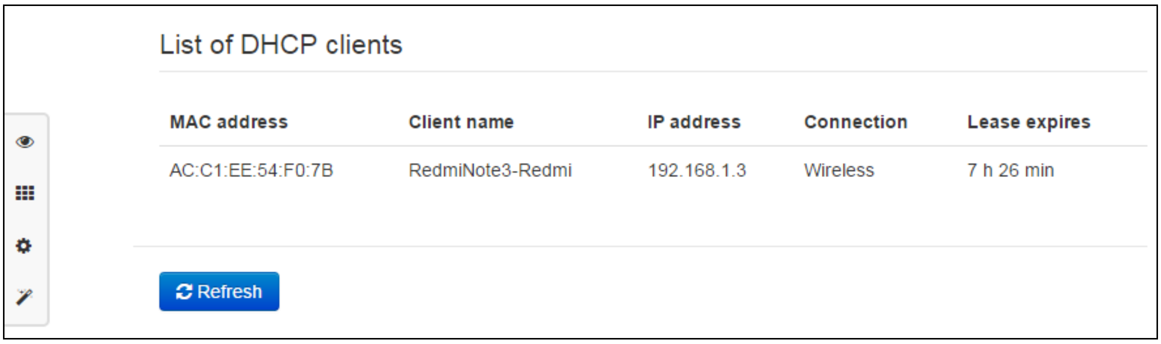
List of the connected clients

- *MAC address* – MAC address of client that is connected to the device via Wi-Fi*;*
- *Client name* – network name for device connection;
- *SSID* – name of access point to which client is connected;
- *IP address* – IP address assigned to a client;
- *Signal level* – level of signal received from client;
- *Range* – frequency range in which a client is connected (2.4 or 5 GHz);
- *Connection time* – client connection time to the access point.

To obtain actual information about connected Wi-Fi clients click 'Update' button.

3.8.5 'DHCP' submenu

In the 'DHCP' submenu, you may view the list of network devices connected to the LAN (WLAN) interface, that were assigned IP addresses by a local DHCP server, and also the IP address lease expiration time.



List of DHCP clients

MAC address	Client name	IP address	Connection	Lease expires
AC:C1:EE:54:F0:7B	RedmiNote3-Redmi	192.168.1.3	Wireless	7 h 26 min

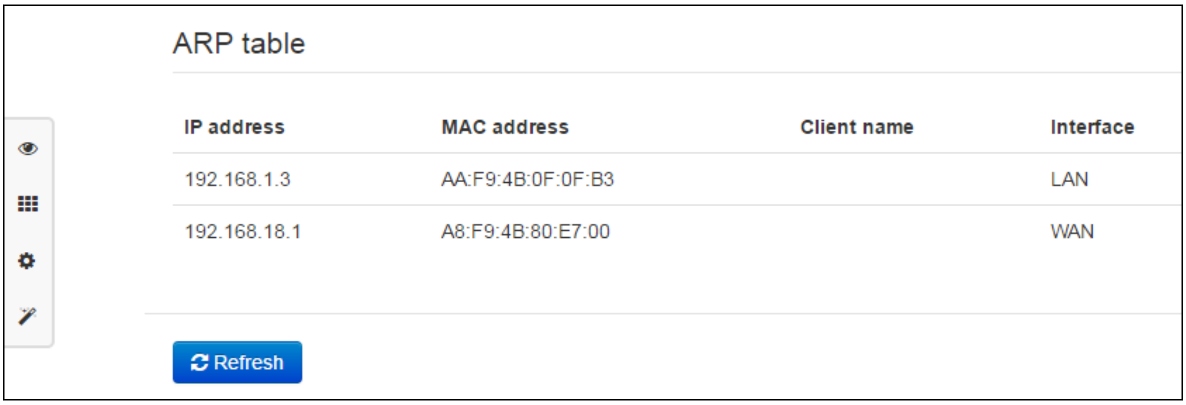
Active DHCP leases

- *MAC* address—connected device MAC address;
- *Client name*—connected device network name;
- *IP address*—IP address assigned to the client from the address pool;
- *Lease expires*—remaining time of the assigned address lease.

To obtain actual information on DHCP clients, click 'Update' button.

3.8.6 'ARP' submenu

In the 'ARP' submenu, you may view an ARP table. In ARP table, you may find information on IP and MAC address correspondence for neighbouring network devices.



ARP table

IP address	MAC address	Client name	Interface
192.168.1.3	AA:F9:4B:0F:0F:B3		LAN
192.168.18.1	A8:F9:4B:80:E7:00		WAN

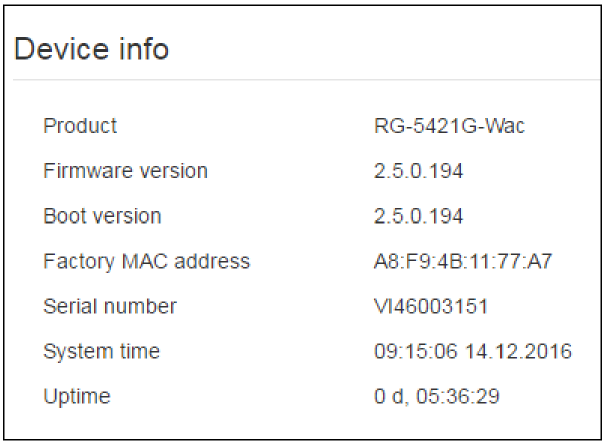
ARP table

- *IP address* – device IP address;
- *MAC address* – device MAC address;
- *Interface* – interface of the device active side: WAN, LAN, Bridge.

To obtain actual information, click 'Update' button.

3.8.7 ‘Device’ submenu

In the 'Device' submenu, you may find general device information.



Device info

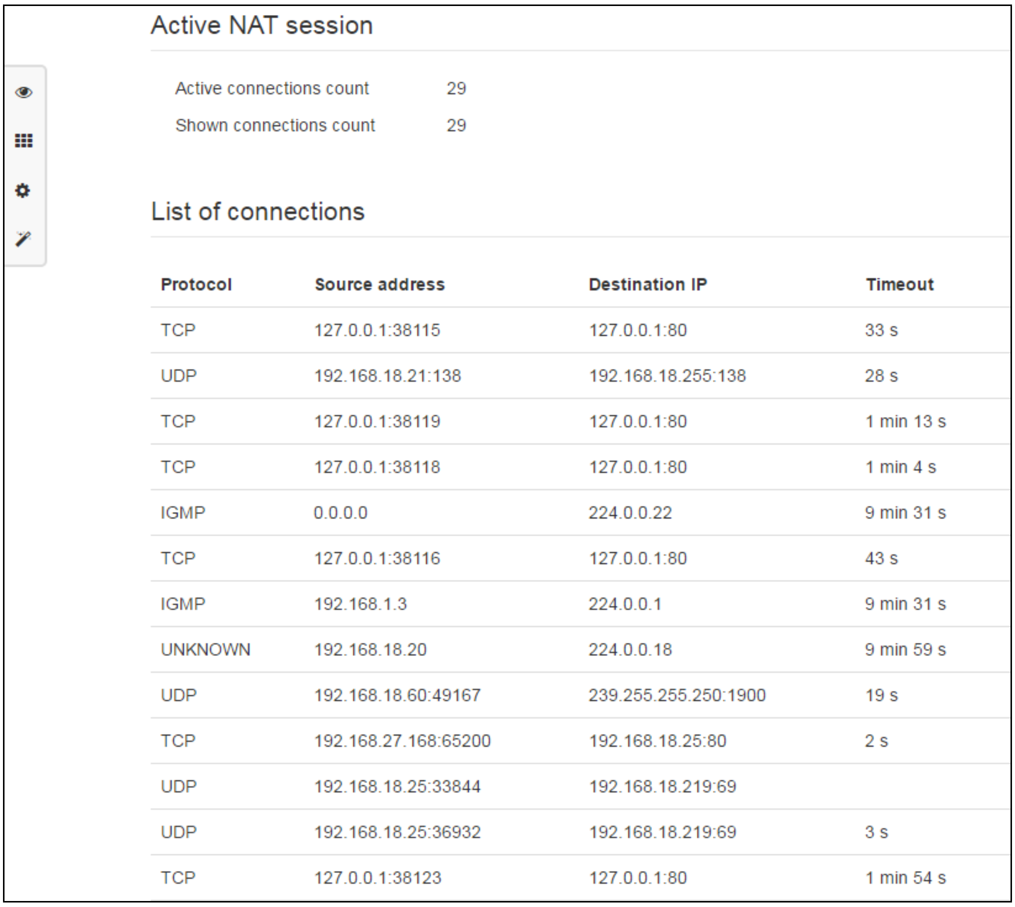
Product	RG-5421G-Wac
Firmware version	2.5.0.194
Boot version	2.5.0.194
Factory MAC address	A8:F9:4B:11:77:A7
Serial number	VI46003151
System time	09:15:06 14.12.2016
Uptime	0 d, 05:36:29

Device information

- *Product* – device model name;
- *Firmware version*—device firmware version;
- *Bootstrap version* — firmware version of the device bootstrap program;
- *Factory MAC address* —device WAN interface MAC address defined by the manufacturer;
- *Serial number*—device serial number defined by the manufacturer.
- *System time*—current date and time defined in the system;
- *Uptime*—time of operation since the last startup or reboot of the device.

3.8.8 ‘Conntrack’ submenu

In the 'Conntrack' submenu, you may find the current active network connections of the device.



Active NAT session

Active connections count	29
Shown connections count	29

List of connections

Protocol	Source address	Destination IP	Timeout
TCP	127.0.0.1:38115	127.0.0.1:80	33 s
UDP	192.168.18.21:138	192.168.18.255:138	28 s
TCP	127.0.0.1:38119	127.0.0.1:80	1 min 13 s
TCP	127.0.0.1:38118	127.0.0.1:80	1 min 4 s
IGMP	0.0.0.0	224.0.0.22	9 min 31 s
TCP	127.0.0.1:38116	127.0.0.1:80	43 s
IGMP	192.168.1.3	224.0.0.1	9 min 31 s
UNKNOWN	192.168.18.20	224.0.0.18	9 min 59 s
UDP	192.168.18.60:49167	239.255.255.250:1900	19 s
TCP	192.168.27.168:65200	192.168.18.25:80	2 s
UDP	192.168.18.25:33844	192.168.18.219:69	
UDP	192.168.18.25:36932	192.168.18.219:69	3 s
TCP	127.0.0.1:38123	127.0.0.1:80	1 min 54 s

Active NAT session

- *Count of active connections*—total number of active network connections;
- *Count of shown connections*—number of connections shown in the WEB interface. In order to maintain high performance of the WEB interface, maximum number of connections shown is limited to 1024. You may view other connections with the device command console (*cat /proc/net/nf_conntrack*).

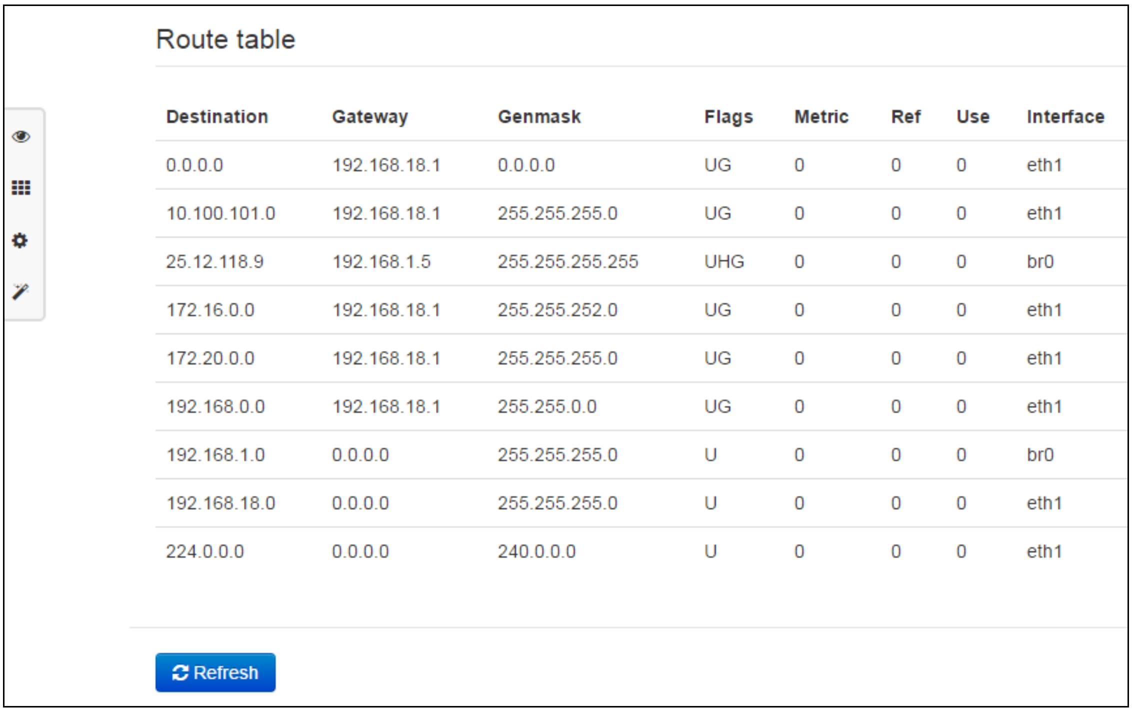
List of connections

- *Protocol*—protocol that the connection is being established through;
- *Source address*—connection initiator IP address and port number;
- *Destination IP*—connection destination IP address and port number;
- *Timeout*—time period until the connection termination.

To obtain actual information, click 'Update' button.

3.8.9 'Routing' submenu

In the 'Routing' submenu, you may view the device routing table.



Route table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	192.168.18.1	0.0.0.0	UG	0	0	0	eth1
10.100.101.0	192.168.18.1	255.255.255.0	UG	0	0	0	eth1
25.12.118.9	192.168.1.5	255.255.255.255	UHG	0	0	0	br0
172.16.0.0	192.168.18.1	255.255.252.0	UG	0	0	0	eth1
172.20.0.0	192.168.18.1	255.255.255.0	UG	0	0	0	eth1
192.168.0.0	192.168.18.1	255.255.0.0	UG	0	0	0	eth1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
192.168.18.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
224.0.0.0	0.0.0.0	240.0.0.0	U	0	0	0	eth1

- *Destination*—IP address of destination host or subnet that the route is established to;
- *Gateway*—gateway IP address that allows for the access to the 'Destination';
- *Genmask* – subnet mask;
- *Flags*—specific route attributes. The following flag values exist:

  - **U -** means that the route is created and passable;
  - **H -** identifies the route to the specific host;
  - **G -** means that the route lies through the external gateway. System network interface provides routes in the network with direct connection. All other routes lie through the external gateways. 'G' flag is marker for all routes except for the routes in the direct connection networks;
  - **R -** means that the route most likely was created by a dynamic routing protocol running on a local system with the 'reinstate' parameter;
  - **D -** means that the route was added on reception of the ICMP Redirect Message. When the system learns the route from the ICMP Redirect message, the route will be added into the routing table in order to exclude redirection of the following packets intended for the same destination. Such routes are marked with the 'D' flag;
  - **M -** means that the route was modified—likely by a dynamic routing protocol running on a local system with the 'mod' parameter applied;
  - **A -** means buffered route with corresponding record in the ARP table.
  - **C -** means that the route source in the core routing buffer;
  - **L -** means that the route destination is an address of this PC. Such 'local routes' exist in the routing buffer only;
  - **B -** means that the route destination is a broadcasting address. Such 'broadcast routes' exist in the routing buffer only;
  - **I -** means that the route is related to the loopback interface with a goal that differs from the access to the ring network. Such 'internal routes' exist in the routing buffer only;
  - **! -** means that datagrams sent to this address will be rejected by the system;

- *Metric*—defines route cost. Metrics allows you to sort the duplicate routes, if they are exist in the table;
- *Ref*—identified number of references to the route for connection establishment (not used by the system);
- *Detection* – number of route detections performed by IP protocol;
- *Interface*—name of the network interface that the route lies through.

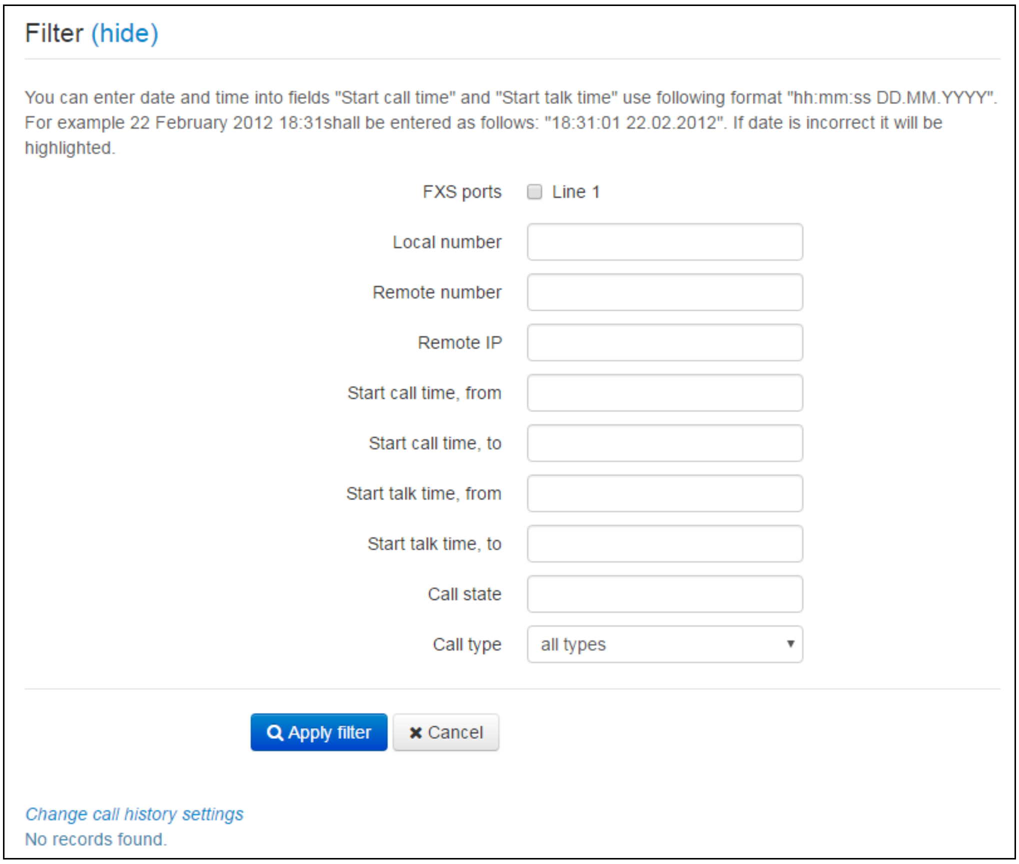
To obtain actual information, click 'Update' button.

3.8.10 'Call history' submenu

In the 'Call history' submenu you may view the list of performed phone calls and the summary for each call.

The device RAM may store up to 10,000 records for performed calls. If the record number exceeds 10,000, the oldest records (at the top of the table) will be removed, and new ones will be added at the end of the file.

Log statistics will not be collected, when the history size is zero.



Filter (hide)

You can enter date and time into fields "Start call time" and "Start talk time" use following format "hh:mm:ss DD.MM.YYYY". For example 22 February 2012 18:31shall be entered as follows: "18:31:01 22.02.2012". If date is incorrect it will be highlighted.

FXS ports	□ Line 1
Local number	
Remote number	
Remote IP	
Start call time, from	
Start call time, to	
Start talk time, from	
Start talk time, to	
Call state	
Call type	all types

Change call history settings

No records found.

'Call history' table field description:

- *#* – sequence number of the record in the table;
- *Line*—device subscriber port number;
- *Local number*—subscriber number assigned to this subscriber port;
- *Remote number*—remote subscriber number that the phone connection has been established with;

- *IP address of the opposite site* – remote subscriber IP address that the phone connection has been established with;
- *Start call time*—call received/performed time and date;
- *Start talk time*—call start time and date;
- *Talk duration*—call duration in seconds;
- *Call status*—transient state or reason for call clearing; description becomes available, when you hover the cursor over the call state record;
- *Call type*—call type: outgoing or incoming;
- *TxPack*—number of RTP packets sent during the call;
- *TxBytes*—number of bytes sent during the call;
- *RxPack*—number of RTP packets received during the call;
- *RxBytes*—number of bytes received during the call.

In the call history table, you may search records by different parameters; to do this, click the 'Filter (Show)' link. Filtering may performed by the subscriber line address, local or remote number, opposite side IP address, call received time, call start time, call state and call type. For filtering parameter description, see call history table field description above.

Call received time from/to or *Call start time from/to*—call received/performed time period or call start time period in the 'hh:mm:ss dd.mm.yyyy' format.

To hide the table record filtration parameter settings, click the *'Hide filter'* link.

To configure call history parameters, click 'Configure call history parameters' link. For more detailed description of parameters, see section *3.7.3.7 'Call history' submenu.*

Click ⏪ button to proceed to the table showing the first record.

Click ❮ button to proceed to the previous page with the call history table.

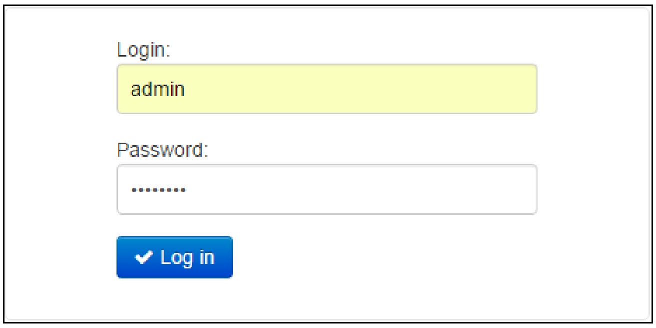
Click ❯ button to proceed to the next page with the call history table.

Click ⏩ button to proceed to the table showing the last record.

Use 'Records on page' selector to configure the number of table records displayed on a single page.

3.9 Configuration example

1. Connect a PC to one of the device LAN ports, connect provider network cable to the WAN port;
2. Enter the gateway IP address in the browser address bar (default value is 192.168.1.1);
3. When the device connection is successfully established, you will see the login and password request window. Fill in the fields and click 'Sign in' button (default login: admin, default password: password).

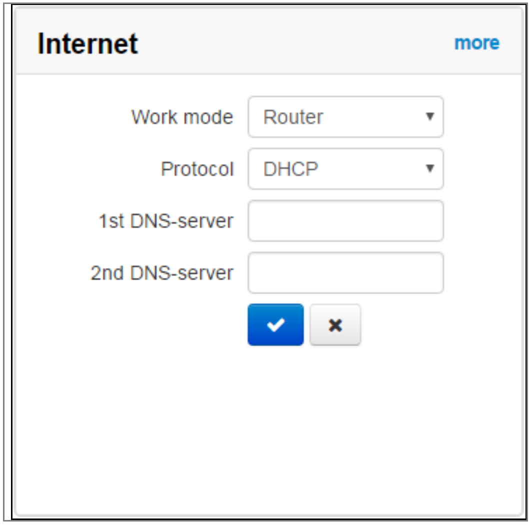


Login: admin

Password: ••••••••

If this field is not visible, make sure that the automatic IP address obtaining feature is enabled in the network connection settings on your PC.

4. In the 'Internet' tile, you may configure an external connection. In 'Protocol' field, select the protocol used by your ISP and enter all the necessary data according to the provider's instructions. If you are required to use static settings in order to connect to the provider network, select 'Static' value in the 'Protocol' field and fill the 'Device external IP address', 'Subnet mask', 'Default gateway', 'Primary DNS', and 'Secondary DNS' fields—parameter values should be obtained from the provider. To save and apply settings, click. ✓ button.



Internet

Work mode: Router

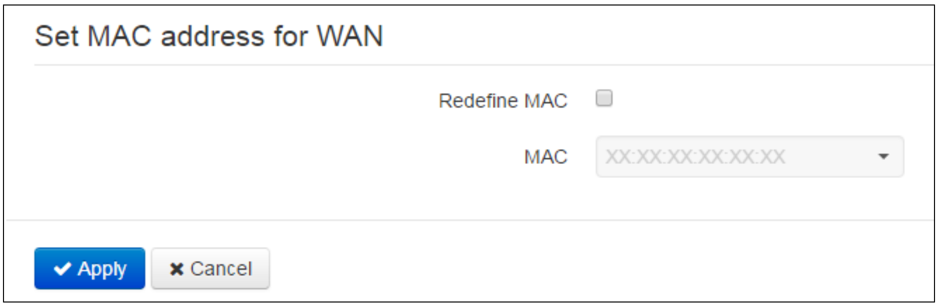
Protocol: DHCP

1st DNS-server

2nd DNS-server

To specify additional parameters, go to advanced settings mode by clicking the 'Details' link (see Section *3.7.2.1*).

5. When your ISP network employs MAC address tethering, click 'Details' button in the 'Internet' tile and open the 'MAC address configuration' submenu. In the 'WAN MAC address configuration' section, select the 'Redefine MAC' checkbox and enter MAC address of the device previously connected to the Internet into the 'MAC' field. To save and apply settings, click 'Apply'. If you have connected a PC that is used for device configuration at the moment, just click context menu button and select MAC address from the drop-down menu.

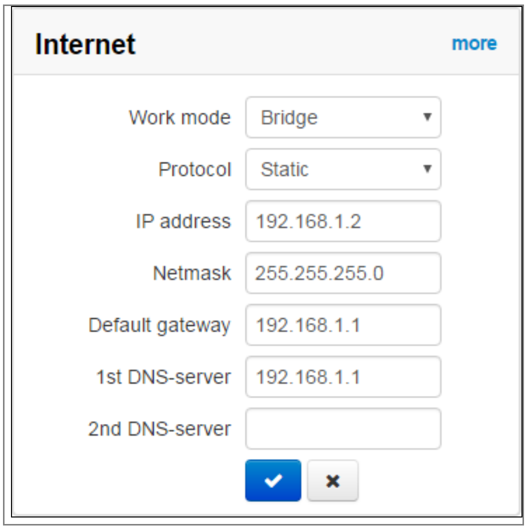


Set MAC address for WAN

Redefine MAC □

MAC: XX:XX:XX:XX:XX:XX

If *5400* is intended to be used as a 5-port switch—select the 'Bridge' value in the 'Operation mode' field of the 'Internet' tile. In *'IP address'* field, specify an address that will be used for the device access. Define subnet mask (default: 255.255.255.0) and default gateway with DNS address if it is required. To save and apply settings, click ✓ button.

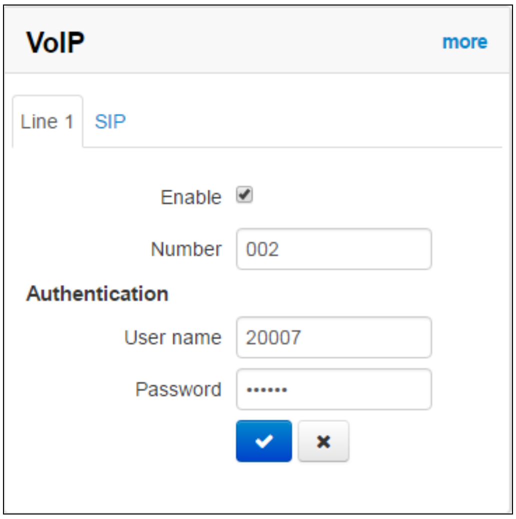


Internet

Work mode	Bridge
Protocol	Static
IP address	192.168.1.2
Netmask	255.255.255.0
Default gateway	192.168.1.1
1st DNS-server	192.168.1.1
2nd DNS-server	

In the *'Bridge'* mode, the gateway will not assign IP addresses automatically using DHCP to devices connected to the LAN interface.

6. In the 'VoIP' tile, you may perform quick configuration of the subscriber line for operation via SIP. To do this, select 'Line' tab with the number of line that should be configured. Select 'Enable' checkbox, enter the phone number for this line, and login and password for SIP server authorization. To save and apply settings, click ✓ button.



VoIP

Line 1 | SIP

Enable ☑

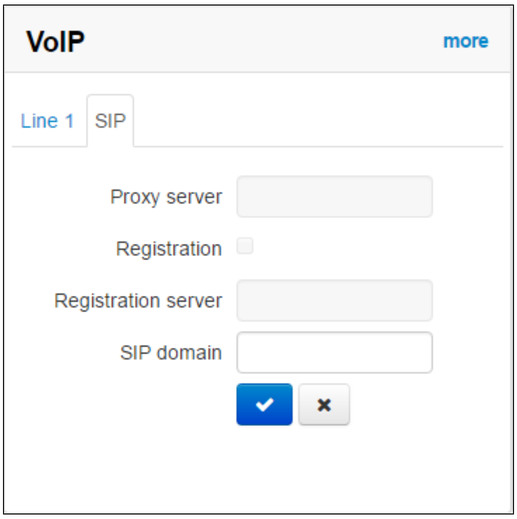
Number: 002

Authentication

User name: 20007

Password: ••••••

7. Select 'SIP' tab in the 'VoIP' tile to configure SIP parameters. Specify IP address or domain name of the SIP server and registration server (if necessary) in the corresponding fields. If ports used by servers differ from 5060, specify alternative ports after the colon. Specify SIP domain, if necessary. Select 'Registration' checkbox, if the subscriber is required to register on SIP server for VoIP operation (as a rule, registration is required). To save and apply settings, click ✓ button.



VoIP

Proxy server

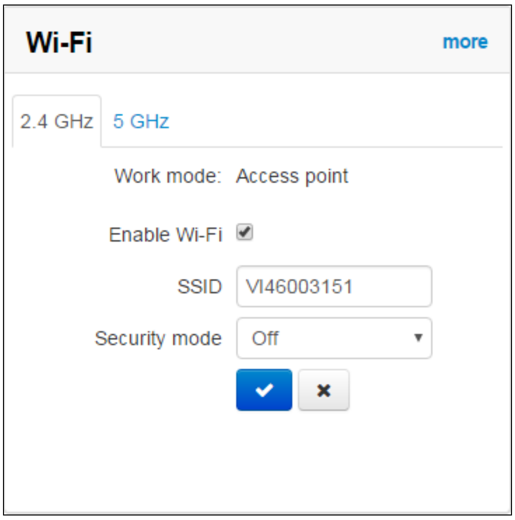
Registration □

Registration server

SIP domain

To specify additional parameters, go to advanced settings mode by clicking the 'Details' link (see Section *3.7.3 'VoIP' menu*).

8. In the 'Wi-Fi' tile you may configure Wi-Fi network parameters. Select required frequency rang: 2.4 GHz or 5GHz. Select 'Enable Wi-Fi' checkbox to enable Wi-Fi network. In the 'SSID' field specify the access point name. Access key is not required to connect to Wi-Fi network when 'off' security mode is selected. To restrict access to Wi-Fi, select 'WEP', 'WPA' or 'WPA2' in the 'Security mode' field and specify a key for network connection. Key length for WEP should be 5 or 13 characters, for WPA and WPA2-from 8 to 64 characters. Use WPA or WPA2 mode to secure Wi-Fi network. To save and apply settings, click ✓ button.



Wi-Fi

Work mode: Access point

Enable Wi-Fi ☑

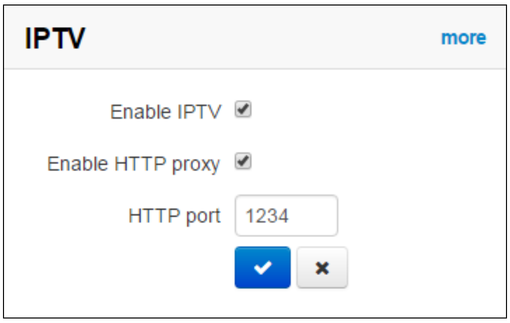
SSID VI46003151

Security mode Off

There is opportunity to use two frequency ranges simultaneously. To do this, configure access point in another tab by the similar way.

To specify additional parameters, go to advanced settings mode by clicking the 'Details' link (see Section *3.7.2.11 'Wi-Fi' submenu*).

9. If you are planning to use IPTV, select 'Enable IPTV' in the 'IPTV' tile. To enable transmission of IPTV streams via HTTP, select 'Enable HTTP proxy' checkbox. In the 'HTTP port' field, specify the port that will be used for connection of external devices to a local HTTP proxy. It is recommended to use HTTP proxy for watching IPTV via Wi-Fi (with the aim of improving a quality of broadcasted image). To save and apply settings, click ✓ button.



Enable IPTV ☑

Enable HTTP proxy ☑

HTTP port 1234

If IPTV service requires a dedicated VLAN, go to advanced settings mode by clicking the 'Details' link and specify VLAN ID in the respective field (see Section 3.7.4 IPTV).

4 VALUE ADDED SERVICES USAGE

4.1 Call transfer

Call transfer service may be performed locally using gateway resources, or remotely using resources of a communicating device. If the service is performed using resources of a communicating device, the access to 'Call transfer' service is established via subscriber port settings menu—*'VoIP' -> 'Line configuration'*—by selecting *'Transmit Flash'* value in *'Flash operation mode'* field. Service process logics in this case will be defined by the communicating device.

When *'Call transfer'* service is performed locally using gateway resources, the access to this service is established via subscriber port settings menu—*'VoIP' -> 'Line configuration'*—by selecting *'Attended calltransfer'* or *'Unattended calltransfer'* in *'Flash operation mode'* field.

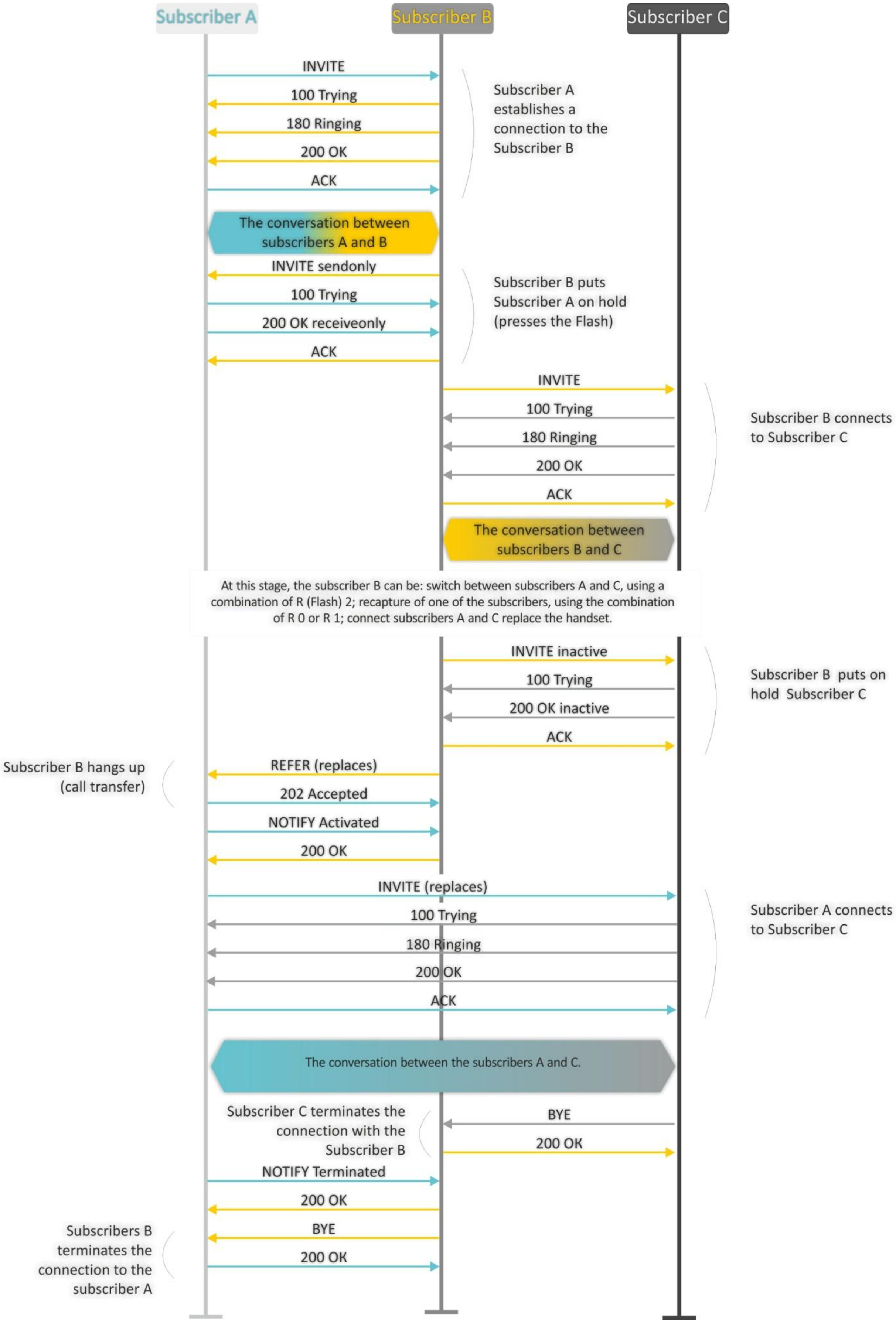
'Attended calltransfer' service allows you to temporarily disconnect an online subscriber (Subscriber A), establish connection with another subscriber (Subscriber C) and return to the previous connection without dialling or transfer the call while disconnecting Subscriber B.

'Attended calltransfer' service usage:

While being in a call state with the subscriber A, put him on hold with short clearback flash (R), wait for station response signal and dial subscriber C number. When Subscriber C answers, the following operations will be possible:

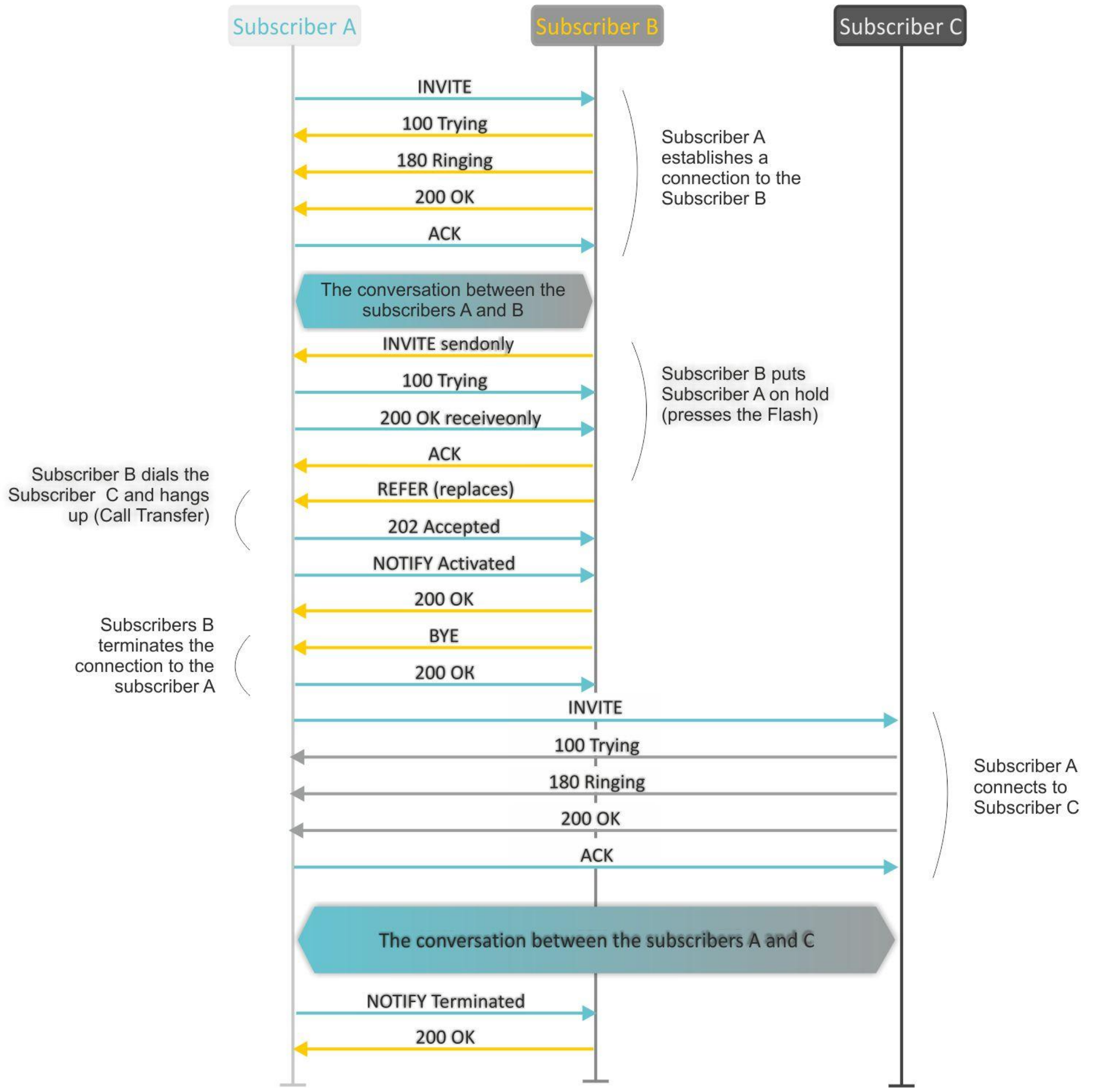
- R 0 – disconnect a subscriber on hold, connect to online subscriber;
- R 1 – disconnect an online subscriber, connect to subscriber on hold;
- R 2 – switch to another subscriber (change a subscriber);
- R 3 – conference;
- R clearback—call transfer; voice connection will be established between Subscribers A and C.

Figure below shows *'Attended calltransfer'* service operation algorithm.


Subscriber A
Subscriber B
Subscriber C
INVITE
100 Trying
180 Ringing
200 OK
ACK
Subscriber A establishes a connection to the Subscriber B
The conversation between subscribers A and B
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Subscriber B puts Subscriber A on hold (presses the Flash)
INVITE
100 Trying
180 Ringing
200 OK
ACK
Subscriber B connects to Subscriber C
The conversation between subscribers B and C
At this stage, the subscriber B can be: switch between subscribers A and C, using a combination of R (Flash) 2; recapture of one of the subscribers, using the combination of R 0 or R 1; connect subscribers A and C replace the handset.
INVITE inactive
100 Trying
200 OK inactive
ACK
Subscriber B puts on hold Subscriber C
Subscriber B hangs up (call transfer)
REFER (replaces)
202 Accepted
NOTIFY Activated
200 OK
INVITE (replaces)
100 Trying
180 Ringing
200 OK
ACK
Subscriber A connects to Subscriber C
The conversation between the subscribers A and C.
Subscriber C terminates the connection with the Subscriber B
BYE
200 OK
NOTIFY Terminated
200 OK
BYE
200 OK
Subscribers B terminates the connection to the subscriber A

'Unattended calltransfer' service allows to put an online subscriber (Subscriber A) on hold with a short clearback flash and dial another subscriber's number (Subscriber C). Call will be transferred automatically when Subscriber B finishes dialling the number.

Figure below shows *'Unattended calltransfer'* service operation algorithm:


Subscriber A
Subscriber B
Subscriber C
INVITE
100 Trying
180 Ringing
200 OK
ACK
Subscriber A establishes a connection to the Subscriber B
The conversation between the subscribers A and B
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Subscriber B puts Subscriber A on hold (presses the Flash)
Subscriber B dials the Subscriber C and hangs up (Call Transfer)
REFER (replaces)
202 Accepted
NOTIFY Activated
200 OK
Subscribers B terminates the connection to the subscriber A
BYE
200 OK
INVITE
100 Trying
180 Ringing
200 OK
ACK
Subscriber A connects to Subscriber C
The conversation between the subscribers A and C
NOTIFY Terminated
200 OK

‘Local calltransfer’ service allows you to transfer call through the gateway without sending the external REFER message if C subscriber is a local *RG 5400* client and its call was directly perfomed with ignoring of the proxy server. If C subscriber is external or local client which was called via proxy server, ‘*Local calltransfer*’ service operates like ‘*Attended calltransfer*’ and call transfer is performed by sending REFER message to the B subscriber

4.2 Call Waiting

This service allows you to inform "busy" subscribers about new incoming calls with a special signal.

Upon receiving this notification, user can answer or reject waiting call.

Access to this service is established via subscriber line settings menu by selecting *'Attended calltransfer'*, *or 'Unattended calltransfer'* in the *'flash operation mode'* field and selecting *'Call waiting'* checkbox.

Service usage:

If you receive a new call while being in a call state, you may do the following operations:

- R 0 – reject a new call;
- R 1 – answer the waiting call;
- R 2 – switch to a new call (change a subscriber);
- R – short clearback (flash).

4.3 Three-way conference call

The three-way conference is a service that enables simultaneous phone communication for 3 subscribers. Press R 3 keys to enter the conference mode (see Section **4.1 Call transfer**).

Subscriber that started the conference is deemed to be it's initiator, two other subscribers are the participants.

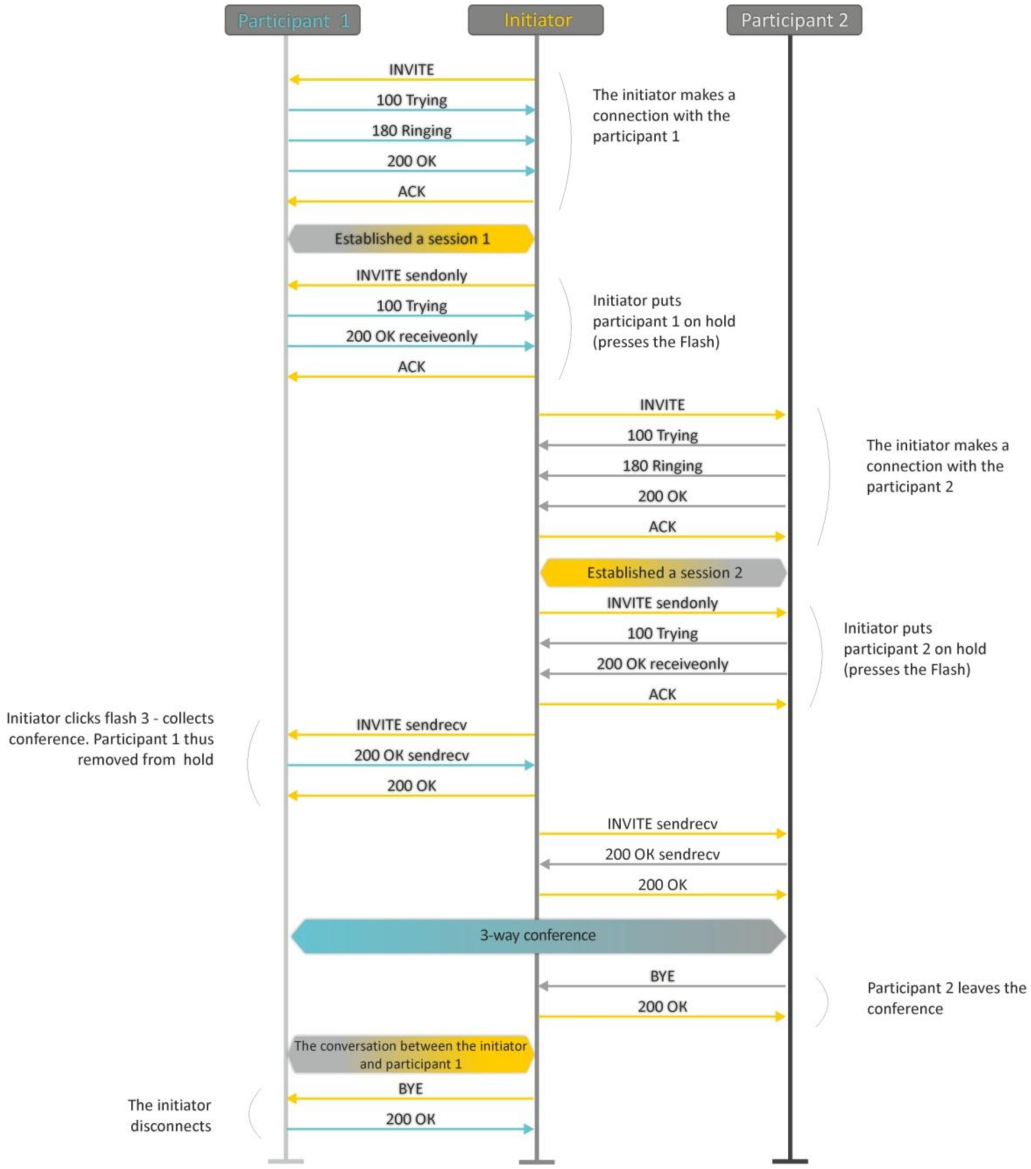
There are two operation modes for a three-way conference: local mode and remote mode. In the first mode, the conference is assembled locally by the initiating subscriber; in the second mode, the conference is established remotely by a remote server, also known as the conference server.

4.3.1 Local conference

In the conference mode, short clearback 'flash' pressed by the initiator is ignored. Signalling protocol messages, received from the participants and intended to put the initiator side into hold mode, force this participant to leave the conference. At that, the initiator and the second participant will switch into the ordinary two-party call mode.

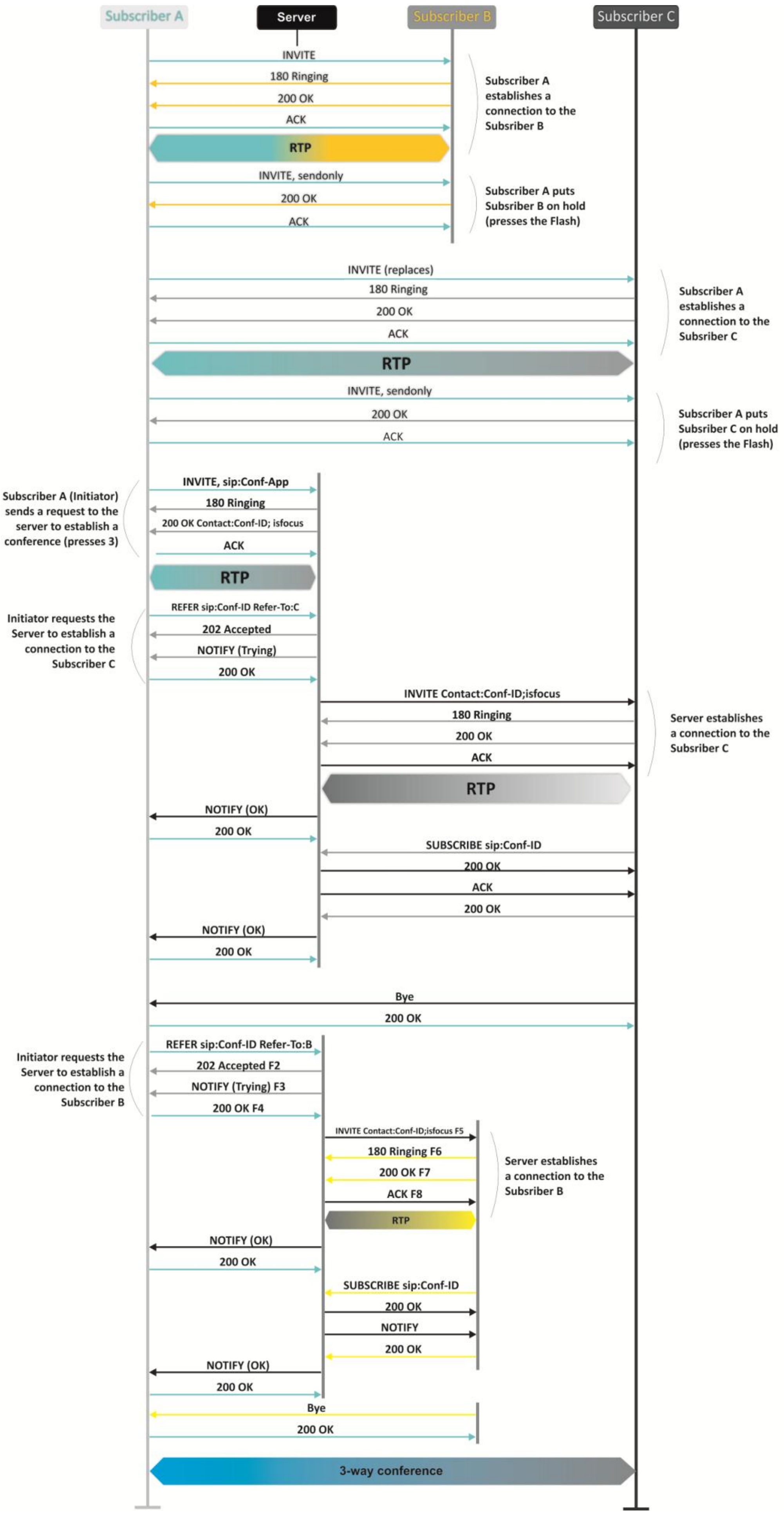
The conference terminates, when initiator leaves; in this case, both participants will receive clearback message. If one of the participants leaves the conference, the initiator and the second participant will switch into a standard two party call. Short flash clearback is processed as described in Sections **4.1 Call transfer** and **4.2 Call Waiting**.

Figure below shows an algorithm of '3-way conference' service performed locally by the Subscriber B via SIP protocol.


Participant 1
Initiator
Participant 2
INVITE
100 Trying
180 Ringing
200 OK
ACK
The initiator makes a connection with the participant 1
Established a session 1
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Initiator puts participant 1 on hold (presses the Flash)
INVITE
100 Trying
180 Ringing
200 OK
ACK
The initiator makes a connection with the participant 2
Established a session 2
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Initiator puts participant 2 on hold (presses the Flash)
Initiator clicks flash 3 - collects conference. Participant 1 thus removed from hold
INVITE sendrecv
200 OK sendrecv
200 OK
INVITE sendrecv
200 OK sendrecv
200 OK
3-way conference
BYE
200 OK
Participant 2 leaves the conference
The conversation between the initiator and participant 1
BYE
200 OK
The initiator disconnects

4.3.2 Remote conference

Conference operation complies with the algorithm described in RFC4579. The special aspect of the algorithm is that the initiating subscriber should press flash+3 in order to establish connection with the conference server (also called 'focus'), and request the focus to connect to remaining conference participants. The figure below shows detailed operation algorithm.

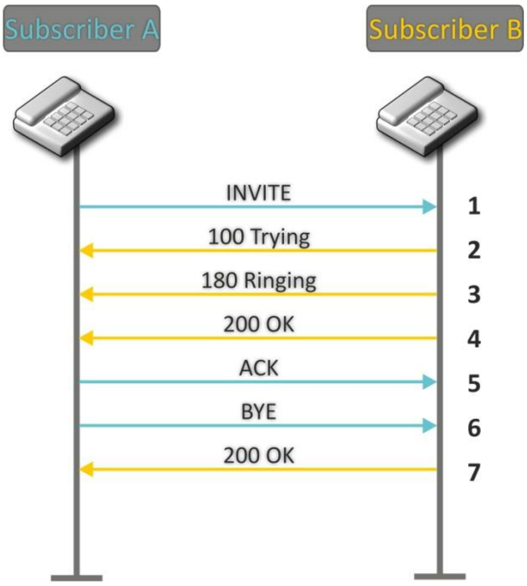

Subscriber A
Server
Subscriber B
Subscriber C
INVITE
180 Ringing
200 OK
ACK
RTP
Subscriber A establishes a connection to the Subsriber B
INVITE, sendonly
200 OK
ACK
Subscriber A puts Subsriber B on hold (presses the Flash)
INVITE (replaces)
180 Ringing
200 OK
ACK
RTP
Subscriber A establishes a connection to the Subsriber C
INVITE, sendonly
200 OK
ACK
Subscriber A puts Subsriber C on hold (presses the Flash)
Subscriber A (Initiator) sends a request to the server to establish a conference (presses 3)
INVITE, sip:Conf-App
180 Ringing
200 OK Contact:Conf-ID; isfocus
ACK
RTP
Initiator requests the Server to establish a connection to the Subscriber C
REFER sip:Conf-ID Refer-To:C
202 Accepted
NOTIFY (Trying)
200 OK
INVITE Contact:Conf-ID;isfocus
180 Ringing
200 OK
ACK
Server establishes a connection to the Subsriber C
RTP
NOTIFY (OK)
200 OK
SUBSCRIBE sip:Conf-ID
200 OK
ACK
200 OK
NOTIFY (OK)
200 OK
Bye
200 OK
Initiator requests the Server to establish a connection to the Subscriber B
REFER sip:Conf-ID Refer-To:B
202 Accepted F2
NOTIFY (Trying) F3
200 OK F4
INVITE Contact:Conf-ID;isfocus F5
180 Ringing F6
200 OK F7
ACK F8
Server establishes a connection to the Subsriber B
RTP
NOTIFY (OK)
200 OK
SUBSCRIBE sip:Conf-ID
200 OK
NOTIFY
200 OK
NOTIFY (OK)
200 OK
Bye
200 OK
3-way conference

5 CONNECTION ESTABLISHMENT ALGORITHM

5.1 Algorithm of a Successful Call via SIP

SIP (Session Initiation Protocol) is a session initiation protocol, that performs basic call management tasks such as starting and finishing session.

SIP defines 3 basic connection initiation scenarios: between users, involving proxy server, involving forwarding server. Basic connection initiation algorithms are described in IETF RFC 3665. This section describes an example of a connection initiation scenario via SIP between two gateways, that know each other IP addresses in advance.

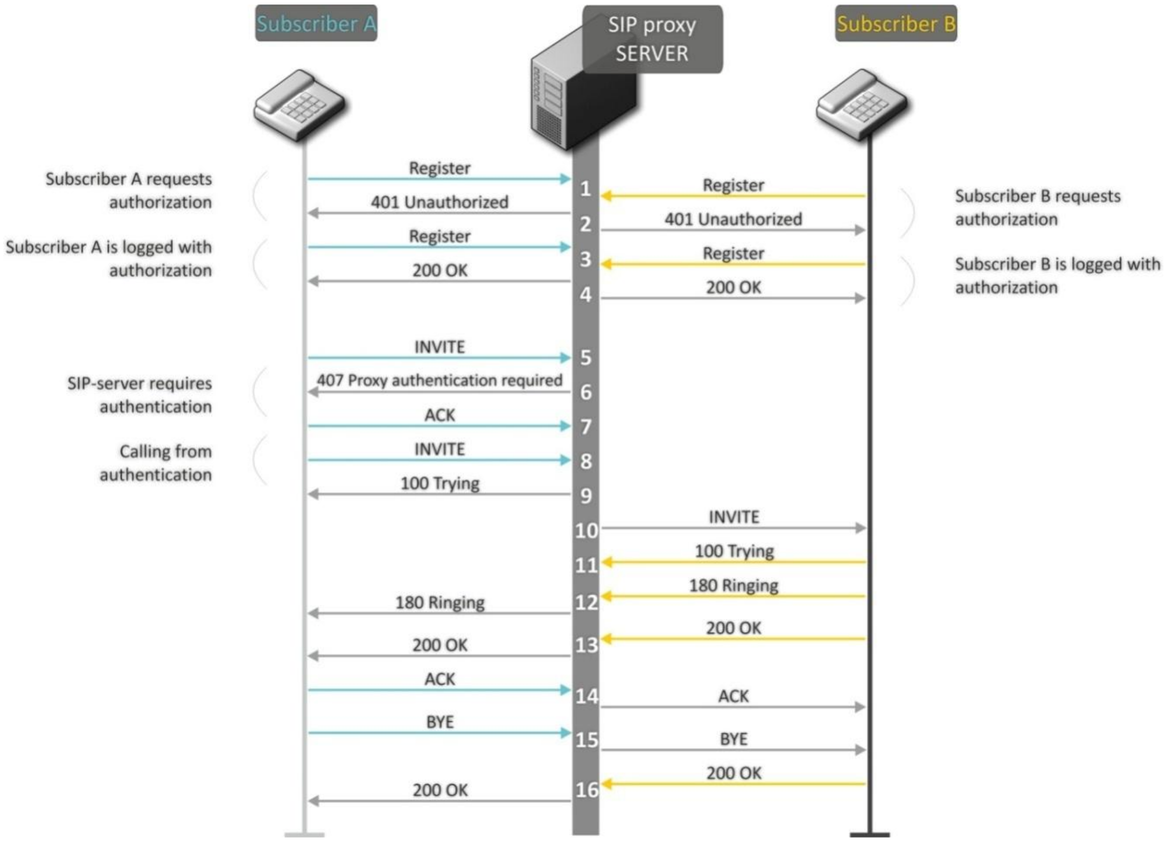


Algorithm description:

1. Subscriber A rings up Subscriber B.
2. Subscriber B gateway receives the command for processing.
3. Subscriber B is free. In this moment, 'ringing' tone is sent to the Subscriber B phone, and 'ringback' tone to Subscriber A phone.
4. Subscriber B answers the call.
5. Subscriber A gateway confirms session establishment.
6. Subscriber A clears back, 'busy' audio tone is sent to the Subscriber B.
7. Subscriber B gateway confirms received clearback command.

5.2 Call Algorithm Involving SIP Proxy Server

This section describes a connection initiation scenario between two gateways involving SIP proxy server. In this case, caller gateway (Subscriber A) should know subscriber's permanent address and proxy server IP address. SIP proxy server processes messages received from Subscriber A, discovers Subscriber B, prompts the communication session and performs router functions for two gateways.


Subscriber A
SIP proxy SERVER
Subscriber B
Subscriber A requests authorization
Subscriber A is logged with authorization
SIP-server requires authentication
Calling from authentication
Subscriber B requests authorization
Subscriber B is logged with authorization
Register
401 Unauthorized
Register
200 OK
INVITE
407 Proxy authentication required
ACK
INVITE
100 Trying
180 Ringing
200 OK
ACK
BYE
200 OK
Register
401 Unauthorized
Register
200 OK
INVITE
100 Trying
180 Ringing
200 OK
ACK
BYE
200 OK
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

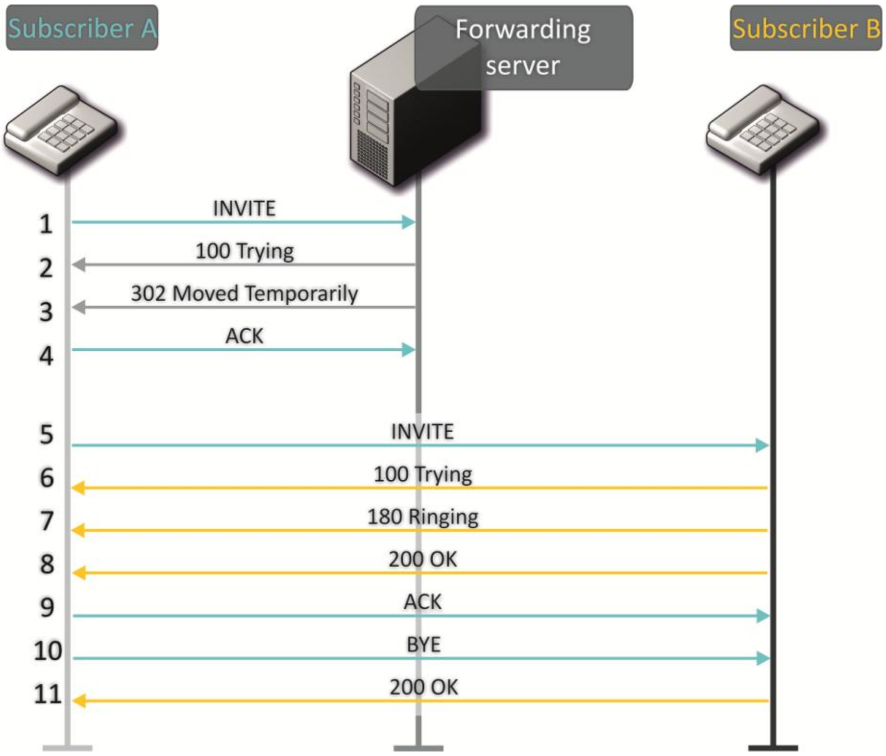
Algorithm description:

Registration at the SIP server.

1. Subscriber A and Subscriber B register at SIP server.
2. SIP server prompts for authorization.
3. Subscriber A and Subscriber B register at SIP server with authorization.
4. SIP server responses on successful registration.
5. Subscriber A rings up Subscriber B.
6. SIP server requests authentication.
7. Subscriber A gateway confirms received authorization request command.
8. Subscriber A rings up Subscriber B.
9. SIP server receives the command for processing.
10. SIP server translates Subscriber A call request directed at Subscriber B.
11. Subscriber B gateway receives the command for processing.
12. Subscriber B is free. In this moment, 'ringing' tone is sent to the Subscriber B phone, and 'ringback' tone to Subscriber A phone.
13. Subscriber B answers the call.
14. Subscriber A gateway confirms session establishment.
15. Subscriber A clears back, 'busy' audio tone is sent to the Subscriber B.
16. Subscriber B gateway confirms received clearback command.

5.3 Call Algorithm Involving Forwarding Server

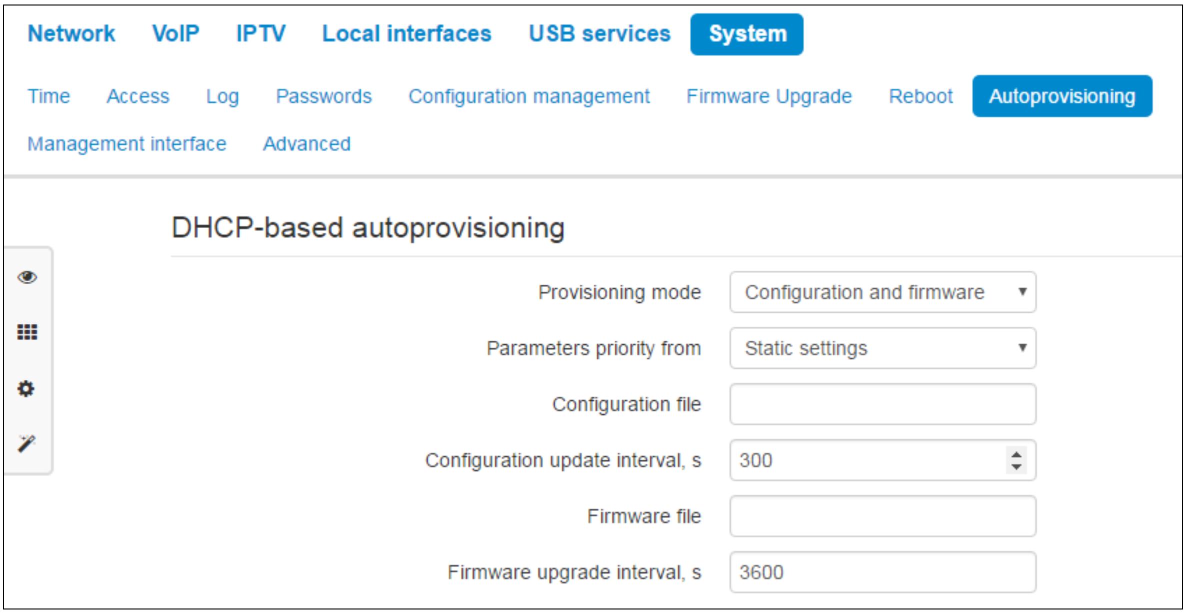
This section describes a connection initiation scenario between two gateways involving forwarding server. In this case, caller gateway (Subscriber A) establishes connection unassisted, and the forwarding server only translates callee permanent address into its current address. Subscriber obtains forwarding server address from the network administrator.



Algorithm description:

1. Subscriber A rings up Subscriber B. Call is sent to the forwarding server with the callee address information.
2. Forwarding server receives the command for processing.
3. Forwarding server requests the information on the Subscriber B current address from the location server. Received information (the callee current address and the list of callee registered addresses) is sent to Subscriber A in '302 moved temporarily' message.
4. Subscriber A gateway confirms the reception of reply from the forwarding server.
5. Subscriber A rings up Subscriber B directly.
6. Subscriber B gateway receives the command for processing.
7. Subscriber B is free. In this moment, 'ringing' tone is sent to the Subscriber B phone, and 'ringback' tone to Subscriber A phone.
8. Subscriber B answers the call.
9. Subscriber A gateway confirms session establishment.
10. Subscriber A clears back, 'busy' audio tone is sent to the Subscriber B.
11. Subscriber B gateway confirms received clearback command.

6 DEVICE AUTOMATIC UPDATE ALGORITHM BASED ON DHCP



DHCP-based autoprovisioning

Provisioning mode: Configuration and firmware

Parameters priority from: Static settings

Configuration file:

Configuration update interval, s: 300

Firmware file:

Firmware upgrade interval, s: 3600

Device automatic update algorithm is defined by the *'Parameter priority from'* value.

1. If the *'Static settings*' value is selected, then the full path (including access protocol and server address) to configuration file and firmware file will be defined by *'Configuration file'* and *'Firmware file'* parameters. Full path should be specified in URL format (HTTP and TFTP are supported):

<protocol>://<server address>/<path to file>, where

- <protocol> – protocol used for downloading corresponding files from the server (HTTP and TFTP are supported);
- <server address> – address of the server with a file to be downloaded (domain name or IPv4);
- <path to file> – path to file on the server.

You may use the following wildcards in URL (reserved words substituted with the specific values):

- *$MA* – MAC address – this wildcard in file URL is substituted by the native device MAC address;
- *$SN* – Serial number – this wildcard in file URL is substituted by the native device serial number;
- *$PN* – Product name – this wildcard in file URL is substituted by the model name (e.g. RG-5421G-Wac);
- *$SWVER* – Software version – this wildcard in file URL is substituted by the firmware version number;
- *$HWVER* – Hardware version - this wildcard in file URL is substituted by the device hardware version number.

For MAC address, serial number and model name, see 'Device' section on the monitoring page.

URL examples:

tftp://download.server.loc/firmware.file,
http://192.168.25.34/configs/RG-5400/my.cfg,
tftp://server.tftp/$PN/config/$SN.cfg,
http://server.http/$PN/firmware/$MA.frm и т.д.

At that, some URL parameters may be omitted. For example, configuration file may be specified in the following format:

http://192.168.18.6
or
config_rg24.cfg

If the system is unable to extract the necessary file downloading parameters (protocol, server address or path to file on server) from configuration file or firmware file URL, it will attempt to extract an unknown parameter from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), when address obtaining via DHCP is enabled for the Internet service (DHCP option format and analysis will be provided below). If the system is unable to extract missing parameter from DHCP options, default value will be used:

- Protocol: tftp;
- Server address: update.local;
- Configuration file name: rg24.cfg;
- Firmware file name: rg24.fw.

Thus, if you leave *'Configuration file'* and *'Firmware file'* fields empty, and Options 43 or 66, 67 with file locations are not obtained via DHCP, configuration file URL will be as follows:

tftp://update.local/rg24.cfg,

and the firmware file URL:

tftp://update.local/rg24.fw.

2. If 'DHCP options' value is selected, configuration file and firmware file URLs will be extracted from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), wherefore address obtaining via DHCP should be enabled for the Internet service (DHCP option format and analysis will be provided below). If DHCP options fail to provide some of the URL parameters, default parameter value will be used:

- Protocol: tftp;
- Server address: update.local;
- Configuration file name: rg24.cfg;
- Firmware file name: rg24.fw.

Option 43 format (Vendor specific info)

1|<acs_url>|2|<pcode>|3|<username>|4|<password>|5|<server_url>|6|<config.file>|7|<firmware.file>|8|<vlan_tag>

1 - TR-069 autoconfiguration server address code
2 - 'Provisioning code' parameter specification code;
3 - code of the username for TR-069 server authorization;
4 - code of the password for TR-069 server authorization;
5 - server address code; server address URL should be specified in the following format: tftp://address or http://address. The first version represents TFTP server address, the second version—HTTP server address;
6 - configuration file name code;
7 - firmware file name code;
8 - VLAN tag code for management.
"|" - mandatory separator used between codes and suboption values.

Algorithm of identification of configuration file and firmware file URL parameters from DHCP Options 43 and 66, 67.

1. DHCP exchange initialization

Device initializes DHCP exchange after the startup.

2. Option 43 analysis

When Option 43 is received, suboptions with codes 5, 6, and 7 are analyzed in order to identify the server address and the configuration and firmware file names.

3. Option 66 analysis

If Option 43 is not received from DHCP server or it is received but the system fails to extract the server address, Option 66 will be discovered. If the system fails to obtain the firmware file name, Option 67 will be discovered. They are used for TFTP server address and the firmware file path extraction respectively. Next, configuration and firmware files will be downloaded from Option 66 address via TFTP.

Special aspects of configuration updates.

Configuration file should be in**.tar.gz** format (this format is used when configuration is saved from the web interface in the 'System' - 'Configuration management' tab). Configuration downloaded from the server will be applied automatically and does not require device reboot.

Special aspects of firmware updates.

Firmware file should be in.tar.gz format. When the firmware file is loaded, the device unpacks it and checks its version (using 'version' file in tar.gz archive).

If the current firmware version matches the version of the file obtained via DHCP, firmware will not be updated. Update is performed only when firmware versions are mismatched. When the firmware image is written into the device flash memory, the Power indicator will flash green, orange and red in succession.

Do not power off or reboot the device, when the firmware image is written into the flash memory. These actions will interrupt the firmware update, that will lead to the device boot partition corruption. The device will become inoperable. To restore the device operation, use the instruction provided in Section 7.

7 SYSTEM RECOVERY AFTER FIRMWARE UPDATE FAILURE

If the failure occurred during the firmware update (via Web interface or DHCP-based automatic update)—for example, you have pressed power button by accident—and the device became inoperable (Power LED is solid red), use the following device recovery algorithm:

- Extract the contents of the firmware archive.
- Connect your PC to the device WAN port and specify the address for the network interface from 192.168.1.0/24 subnet.
- Launch TFTP client on the PC (for Windows, we recommend using Tftpd32), specify 192.168.1.6 as the remote host address and select linux.bin file from the extracted firmware archive.
- Run the command to send the file to the remote host (**Put** command). File transfer to *RG-5400* should start .
- If the file transfer process is started, wait until it finishes, after that *RG-5400* will write the firmware into the memory and launch the system automatically. Write time is approximately 5 minutes. When the device is successfully restored, the Power LED will be orange or green. Device will retain the configuration that was used before the failure. If the device is unreachable, reset the device to default settings.
- If the file transfer is not initiated, check the PC network settings for errors and try again. If you are unable to restore the device, send it to the service centre for repairs or connect it to the device via COM port using special adapter (if available).

APPENDIX A. CALCULATION OF PHONE LINE LENGTH

Table —Electrical resistance/cable type relationship for 1km of DC subscriber cable lines at 20°C ambient temperature.

Cable grade for subscriber lines of local exchange network	Core diameter, mm	Electrical resistance of 1km circuit, Ω, max.	Line length (other phone units), km	Line length ('Rus' phone units), km
TPP, TPPep, TPPZ, TPPepZ, TPPB,TPPepB, TPPZB, TPPBG, TPPepBG, TPPBbShp, TPPepBbShp, TPPZBbShp, TPPZepBbShp, TPPt	0,32	458,0	3,537	1,528
	0,40	296,0	5,473	2,365
	0,50	192,0	8,438	3,646
	0,64	116,0	13,966	6,034
	0,70	96,0	16,875	7,292
TPV, TPZBG	0,32	458,0	3,537	1,528
	0,40	296,0	5,473	2,365
	0,50	192,0	8,438	3,646
	0,64	116,0	13,966	6,034
	0,70	96,0	16,875	7,292
TG, TB, TBG, TK	0,40	296,0	5,473	2,365
	0,50	192,0	8,438	3,646
	0,64	116,0	13,966	6,034
	0,70	96,0	16,875	7,292
TStShp, TAShp	0,50	192,0	8,438	3,646
	0,70	96,0	16,875	7,292
TSV	0,40	296,0	5,473	2,365
	0,50	192,0	8,438	3,646
KSPZP	0,64	116,0	13,966	6,034
KSPP, KSPZP, KSPPB, KSPZPB, KSPPt, KSPZPt, KSPZPK	0,90	56,8	28,521	12,324

APPENDIX B. RUNNING USER-DEFINED SCRIPT UPON SYSTEM STARTUP

Sometimes, it is necessary to perform specific actions on the device startup, that may not be specified in the configuration file settings. For this purpose, *RG 5400* allows you to set the user-defined script in the configuration file. This script may feature any desired sequence of commands.

For user-defined script execution, use the following settings section in the configuration file:

```
UserScript:
  Enable: "0"
  URL: ""
```

'Enable' option allows (if the value is 1) or denies (if the value is 0) execution of the script which path is specified in the URL parameter.

Executed script may be located on the remote server or on the device itself. The script may be downloaded from the remote server via HTTP or TFTP. Consider configuration file examples for user-defined script execution from various sources.

1. Execution from HTTP server

   To execute the script from HTTP server, you should specify full path to file in HTTP-URL format within URL parameter:

   URL: “http://192.168.0.250/user-script/script.sh”

   After the device startup, script.sh file located in the 'user-script' folder at 192.168.0.250 will be downloaded automatically via HTTP from the server and executed afterwards.

2. Execution from TFTP server

   To execute the script from TFTP server, you should specify full path to file in TFTP-URL format within URL parameter:

   URL: “tftp://192.168.0.250/user-script/script.sh”

   After the device startup, script.sh file located in the 'user-script' folder at 192.168.0.250 will be downloaded automatically via TFTP from the server and executed afterwards.

3. Local script execution

   Due to file system specifics, local script should be located in the /etc/config folder only, as the contents of this folder are the only one that remain after the device reboot. Script in /etc/config folder may be created either with vi editor, or downloaded from the external TFTP server (using 'tftp –gluser.sh<TFTP-server address>' command). After creation of the script, you should set execution permissions with 'chmod 777 /etc/config/user.sh' command

   In the configuration file, local script execution URL should be as follows:

   URL: “File://etc/config/user.sh”

It is important to note, that the user script should begin with the '#!/bin/sh' directive.

TECHNICAL SUPPORT

For technical assistance in issues related to handling of ELTEXALATAU Ltd. equipment please address to Service Centre of the company:

Republic of Kazakhstan, 050032, Medeu district, microdistrict Alatau, 9 st. Ibragimova, 9
Phone:
+7(727) 220-76-10
+7(727) 220-76-07
E-mail: post@eltexalatau.kz

In official website of the ELTEXALATAU Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center in our technical forum:

http://www.eltexalatau.kz/en/