Analog VoIP Gateways

TAU-36.IP

TAU-72.IP

User manual

Firmware version: 2.21.0

Firmware version: 2.21.0
Linux version: 312
Media processor version: v10_23_03_15
BPU version: v20210602

Factory default IP address 192.168.1.2
Username: admin
Password: rootpasswd

Firmware version	Issue data	Revisions
Version 2.21.0	18.05.2022	Added: – Configuring accounts for authorisation via RADIUS; – Uploading of certificates; – Display name configuration for SIP in CLI. Fixed: – Excluded flexible RADIUS authorisation mode; – Added changes to eliminate some vulnerabilities of device's subsystems (web, SSH); – SSH updated to the latest version; – Fixed CLIR operation.
Version 2.20.9	12.04.2022	Added: – Protection for SSH and Telnet against password cracking by iteration; – Logging of SSH and Telnet access attemts.
Version 2.20.7	30.09.2021	Added: – Diversion header in 302 response in accordance with RFC 5806;
Version 2.20.5	16.07.2021	Added: – Extending the range of values for the cadence of the acoustic signals "Busy" and "Disconnect" in the manual setting mode;
Version 2.20.4	07.06.2021	Added: – Rev. D support; – SNMP: Entity MIB support in accordance with RFC 6933;
Version 2.20.2	11.09.2020	Added: – "Call transfer" support by "Blind transfer";
Version 2.20.1	31.01.2020	Added: – Submenu "Passwords";
Version 2.20.0	11.11.2019	Added: – Default gateway selection for PPP connections;
Version 2.18.1	15.03.2019	Added: – Configuration of dialing pause (symbol 'w') in dialing plan
Version 2.18.0	03.09.2018	Added: – Call log view via web; – Call log upload via web and CLI; – Connected phone indication in port testing results; – AGC settings in subscriber profiles.
Version 2.17.2	02.07.2018	Added: – Digest authentication when authentication via web; – Network mask in firewall rules; – Password hiding in the configuration and web interface; – MTU, MRU, LCP echo failure, LCP echo interval, service name settings for PPP; – Increasing of CLAMPMSS value for PPP; – CLI - enhanced command list for PPPoE configuration; – CLI - enhanced passwd command syntax; – WEB and CLI passwords are synchronized; – Ability to use WAN interface without IP address; – Only caller name is available in CallerID. Fixed: – Scopes of MTU settings for PPP and VLAN interfaces; – Proper termination of PPP session with the device software restart.
Version 2.17.0	02.02.2018	Added: – Flexible authentication mode on RADIUS server; – Change operation of functional 'F' button;

		– The 'Modem' setting and service for subscriber port; – Reserve DNS configuration in CLI; – Ability to update firmware via FTP; – Simultaneous processing of 43, 66 and 67 DHCP protocol options; – Enhanced supported TR-069 parameters value.
Version 2.16.0	22.12.2017	Added: – Output 'overload busy' tone when 500, 502, 503 and 504 SIP response are received; – Enhanced CLI interface supported functional.
Version 2.15.0	31.07.2017	Added: – Diffserv parameter is replaced by DSCP; – Current SIP proxy server control via OPTIONS requests support; – Enhanced CLI interface supported functional; – iftable SNMP MIB2 support.
Version 2.14.0	11.02.2017	Added: – PPTP tunnel support; – IPSec tunnel support; – Firmware update art certain time (timed); – Configuration update at certain time; – Filtrations on MAC addresses; – Acoustic signal parameters configuration; – Dial plan profiles; – Call forward to a local subscriber is fixed; – Echo delay time configuration; – T2 timer configuration; – Individual Diffserv for RTP per port; – Diffserv for RTP for subscriber profile; – Rx AGC; – Tx AGC; – DNS failure is fixed.
Version 2.13.1	15.07.2015	Added: – Ability to configure MTU; – Ability to configure ports to get access via Telnet, SSH, HTTPS; – Ability to switch to redundant proxy only by INVITE request type.
Version 2.13	28.01.2015	Added: – Incorrect RTP/SAVP processing is fixed; – Call decline by 500 SIP INFO request reply receiving is fixed; – Misuse of accept header in SIP replies is fixed; – SIP headers display via web interface issues are fixed; – Automatic username and password fields in web interface filling is fixed; – Russified web interface; – Symbol '%' inputting in username, hot number, alt number, cf_no_answer, cf_busy, cf_unconditional, cf_out_of_service restriction; – Response for transition to a redundant proxy is changed from 408 to 505; – Expanding of Username and Password fields to 50 characters in SIP profile; – MWI service for SIP; – Ability to change the way of static/dynamic address obtaining in factory default configuration; – Ability to change factory default MAC address; – Updated files of time zones for NTP; – Prior channel through-connecting when calling to a call group; – Maximum amount of simultaneous web interface users is increased to four; – SIP domain transmission to request URI; – Application of Wait answer timeout for incoming calls; – Creation of DHCP option 82.
Version 2.12	18.09.2014	Added: – alert-info header processing; – Multihoming mode support; – Work behind NAT (STUN, PublicIP) support;

		– CgPN/CdPN modification support with incoming calls; – Optional depth of RURI check with incoming calls; – Configuration and firmware update via FTP/HTTP/HTTPS support; – Local log; – Configurable daylight saving time support; – Configuring the Speed/Duplex modes of switch ports.
Version 2.11	20.06.2014	Added: – SNMP. New blocking cause support (Receiver offhook); – WEB. Regexp dialplan modofocation: – Processing of the ABCD symbols in regexp routing plan; – Ability to replace S-timer by L-timer for variable symbol amount rules in regexp routing plan; – SNMP, WEB Increasing of the Call group amount up to 32; – H323 processing of the status enquiry message.
Version 2.10	12.05.2014	Added: – SIP. SIP-T support; – SIP. Port unregistration after restart; – SIP. Call waiting service support by Huawei algorithm; – SNMP. Hardware version reading via SNMP; – SNMP. Configuration of common system parameters; – SNMP. Configuration of TCP/UDP port ranges; – SNMP. Configuration of call limits; – SNMP. Distinctive ringing service configuration – Adding the 'stop dial by #' option in subscriber profile; – 'Call transfer' service control using IMS; – Monitoring of 'Call transfer' service setted using IMS; – Call transmission using 'Flash+4' combination; – 'Port registration delay' parameter value range is changed (ms); – WEB. The buttons for statistics, blocking and line testing data reset are added; – DHCP release message transmission when the device is resetting; – DHCP option 43 support; – DHCP option 121 support; – DHCP option 60 issued format control.
Version 2.9	11.02.2014	Added: – Redundant DNS configuration; – Access via web enable/disable; – Configuration of the TCP port for access via web by HTTP; – TR-069 protocol is realized; – Configuration of the failure events transmission to the syslog server; – Firewall configuration via web; – Configuration of the active session support mode for operations through NAT (SIP); – 3-way-conference startup mode on conference server (SIP) is realized; – Service (simulation service) management using IMS (3GPP TS 24.623) (SIP); – RFC2833 alignment with RFC3264 recomendation (SIP); – cpc-rus subscriber category transmission (SIP); – Call transmission within gateway without REFER query (SIP); – Music on hold support on G.723.1 G.729 G.726-32 codecs; – RADIUS server usage for authentication of users administering the device via web, telnet, SSH; – Serial groups registration state monitoring (web, SNMP); – IMS supply services status monitoring.
Version 2.6	28.08.2013	Added: – Configuration of time interval between port registration; – STP support; – LLDP support; – Fan control options enhancement; – Additional parameters output in the system info section; – SYSLOG parameters configuration via SNMP; – Factory settings monitoring via SNMP; – Line length recalculation in Appendix F.

Version 2.4	1.03.2013	Added: – Call reply answer timeout. – Routing plan regular expressions correctness review; – Distinctive ring service configuration; – RTCO-XR is realized; – Unified configuration file for all settings.

Version 2.3	19.11.2012	Added:
		– SIP profiles configuration;
		– List of the subscriber sets supply modes;
		– Subscriber profiles settings configuration via SNMP:
		  – Configuration of common SIP parameters.
		  – Specific SIP parameters' configuration.
		  – Codecs configuration.
		– Firmware update via SNMP;
		– Registration status monitoring on SIP server;
		– Port blocking status monitoring;
		– The 'Firewall configuration' appendix.
		Removed:
		– SIP-T processing configuration.

Version 2.2	02.07.2012	Added: – Information on the current supplementary services status; – PPPoE configuration; – CPC configuration; – P-RTP -stat configuration; – Inactive media streams removing during SDP session modification. Removed: – SIP-T point-point processing configuration;
Version 2.1	09.02.2012	Added: – Switch port status monitoring; – Reserve codec/protocol usage when fax is transmitting; – Echo cancelling with disabled non-linear NLP processor; – Encryption key setting.
Version 2.0	02.02.2012	Added: – Supply services configuration; – Autoconfiguration. Removed: – RADIUS configuration.
Version 1.11	9.09.2011	Added: – SIPconnected, H323connected parameters for SNMP monitoring; – Testing on long lines (ARM); – Simultaneous connections amount limit - Call limits. Removed: – Alert info support.
Version 1.10	26.08.2011	Added: – Home SIP server control with REGISTER messages; – RTCP configuration; – The 'Music on hold' service; – Switching to modem with session attributes point via rfc3108; – Registration retry interval configuration; – Default gateway and CoS configuration for VLAN; – Inbound configuration; – Ringback raising to a voice channel; – Parameters configuration via SNMP; – Symbol # transmission to a SIP URI as #
Version 1.9	11.04.2011	Added: – The '3-way-conference' service; – Connection establishment algorithms for '3-way-conference' service description; – Payphone mode configuration; – QoS & Bandwidth control - Quality of Service function and Bandwidth restriction configuration;
Version 1.8	09.12.2010	Added: – Safety measures instructions; – General switch operation guidelines;

		– Configuration of internal switching for SIP-proxy connection loss; – Pickup groups configuration. – Configuration of pickup codes; – Configuration of prefix with varying number count; – Web configurator access via HTTPS; – Tracing disabling, network traffic mirroring; – Connection establishment algorithms description; – Example of switch configuration using VLAN; – Example of IPBX configuration on TAU-72.IP/TAU-36.IP; – Phone line length calculation.
Version 1.7	22.09.2010	**Factory default IP address is changed to 192.168.1.2** Added: – Simultaneous channel amount interrelation with codec type table – RADIUS messages description; – First digit input waiting timer; – SIP settings: SIP MTU, short mode, 100rel; – Receiving media traffic control function; – Codec packetization configuration; – Min FLASH impulse detection limit configuration and FLASH detecting restriction; – SWITCH modes description; – Monitoring of SFP parameters, supporting DDM; – Configuration recording/reading to/from FTP, TFTP server; – Added the Logout button; – Call statistics; – CT service function enhancement.
Version 1.6	12.07.2010	– Table added - simultaneous channel amount. – Enable/disable telnet/ssh is added.
Version 1.5	09.04.2010	Web interface is fully updated. – Syslog is added. – Firmware update via web interface is added. – Failure description, output via SNMP is added.
Version 1.4	19.02.2010	– Local DNS, prefix priority description are added.
Version 1.3	14.01.2010	– 'General device configuration sequence' appendix is added.
Version 1.2	23.12.2009	– Subscriber port testing description is added.
Version 1.0	27.05.2009	First issue.

CONTENTS

TAU-36.IP/TAU-72.IP FIRMWARE UPDATE

The principle of firmware update and firmware files format has been changed in the latest versions. Strictly follow the instruction when updating.

Make sure that the name of the firmware version 2.21.X is tau72-2.21.X.

If the current gateway firmware version is less than 1.9.0 (including old versions, that have 4-digit version name) you should:

1. Have an access to a COM port, reserve firmware and configuration (if some update problem will happen).
2. Download firmware file **v.1.11.4:**
   https://eltex-co.com/catalog/tau-36-ip-en.php
3. Download firmware file **v.2.21.X:**
4. Reboot the gateway to clear RAM before updating.
5. Enter the web interface of the device. Go to *Service* → *Firmware upgrade* submenu. Click the *'Browse'* button in *'Universal firmware upgrade'* section, find and select firmware file **v.1.11.4**, then click *'Upgrade firmware'* button. Firmware file should be named as **firmware.tar.gz**.
6. The device will reboot at the end of the firmware update process.
7. After rebooting, enter to web interface and click the *'Save'* button in any configuration menu section, e.g. *'Network'* tab.
8. When the configuration is saved, update the firmware with previous steps using firmware file **v.2.21.X.** Make sure that the name of the firmware version 2.21.X file is **tau72-2.21.X.**

If it is impossible to update the firmware via the web interface, you should use alternative firmware update method described in APPENDIX B. ALTERNATIVE FIRMWARE UPDATE METHOD.

If the current gateway firmware version is in the range of 2.1.0 to 2.1.4 you should:

1. Download firmware file **v.2.1.4:**
   https://eltex-co.com/catalog/tau-36-ip-en.php
2. Download firmware file **v.2.21.X:**
3. Enter the web-interface of the device. Go to *Service* → *Firmware upgrade* submenu. Click the *'Browse'* button in *'Universal firmware upgrade'* section, find and select firmware file **v.2.1.4** then click *'Upgrade firmware'* button. Firmware file should be named as **tau72-2.1.4.**
4. After rebooting, update the firmware with previous steps using firmware file **v.2.21.X**. Make sure that the name of the firmware version 2.21.X file is **tau72-2.21.X.**

If the current gateway firmware version is in the range of 2.2.0 to 2.5.0 you should:

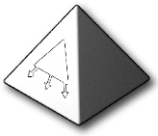
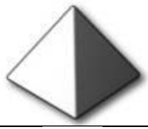
1. Download firmware file **v.2.5.0:** https://eltex-co.com/catalog/tau-36-ip-en.php
2. Download firmware file **v.2.21.X:**
3. Enter the web-interface of the device. Go to *Service → Firmware upgrade* submenu. Click the *'Browse'* button in *'Universal firmware upgrade'* section, find and select firmware file **v.2.5.0** then click *'Upgrade firmware'* button. Firmware file should be named as **tau72-2.5.0.**
4. After rebooting, update the firmware with previous steps using firmware file **v.2.21.X.** Make sure that the name of the firmware version 2.21.X file is **tau72-2.21.X.**

If the current firmware version is 2.5.0 and newer you should:

1. Download firmware file **v.2.21.X:**
2. Reboot the gateway to clear RAM before updating.
3. Enter the web-interface of the device. Go to *Service → Firmware upgrade* submenu. Click the *'Browse'* button in *'Universal firmware upgrade'* section, find and select firmware file **v.2.21.X**, then click *'Upgrade firmware'* button. Firmware file should be named as **tau72-2.21.X.**

If it is not possible to update the firmware via the web interface or other ways, you should use alternative firmware update method described in APPENDIX B. ALTERNATIVE FIRMWARE UPDATE METHOD. All the required files you can find in reserve_soft.zip archive.

DOCUMENT CONVENTIONS

Typographic element	Meaning
Bold font face	Notes, warnings, section headings, titles and table titles are written in bold.
Calibri Italic	Important information is written in Calibri Italic.
Courier New	Command entry examples, command execution results and program output are written in Courier New semibold.
<KEY>	Keyboard keys are written in upper-case and enclosed in angle brackets.
	Analogue phone unit icon
	TAU Analog VoIP Gateway icon
	Ethernet switch icon
	Softswitch ECSS-10 hardware-software switch icon
	Digital subscriber PBX icon
	Network connection icon
	Optical transmission medium

NOTES AND WARNINGS

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

Warnings inform users about hazardous conditions which may cause injuries or device damage and may lead to the device malfunctioning or data loss.

AUDIENCE

This user manual is intended for technical personnel that performs switch installation, configuration, monitoring, and maintenance using web configurator. Qualified technical personnel should be familiar with the operation basics of TCP/IP & UDP/IP protocol stacks and Ethernet networks design concepts.

Before working with the equipment it is strongly recommended to study the following manual.

1 INTRODUCTION

TAU-36.IP/TAU-72.IP Analog VoIP Gateways allow connecting analogue phone units to packed-based data networks accessible through copper-wire or optical Ethernet interfaces.

TAU-36.IP/TAU-72.IP could be used as a subscriber access point using SIP/SIP-T and H.323 protocols. Also provides an optimum telephone communication solution for underpopulated areas, offices, dwellings and remote facilities.

This operation manual describes intended use, key specifications, configuration, and firmware update methods for TAU-36.IP/TAU-72.IP VoIP gateways (hereinafter the 'device').

2 PRODUCT DESCRIPTION

2.1 Purpose

TAU-36.IP/TAU-72.IP is a subscriber VoIP gateway with integrated Layer 2 Ethernet switch that uses copper-wire and optical Gigabit Ethernet interfaces to establish connection to provider's IP network. In order to transfer data via IP networks, device converts analogue voice signals to digital data packets. Used for VoIP organization in dwellings and offices.

When utilized at the stage of transition from TDM to NGN networks, the terminal allows you to keep the existing network infrastructure and analogue subscribers to access IP networks.

Interfaces:

– 36 analogue FXS lines for TAU-36.IP and 72 analogue FXS lines for TAU-72.IP;
– 3 Ethernet 10/100/1000BASE-T electrical interfaces;
– 1 Mini-Gbic (SFP) Ethernet 1000BASE-X optical interfaces.

Device features:

– Integrated Layer 2 Ethernet switch;
– VoIP protocols: H.323, SIP/SIP-T1;
– Static address and DHCP support;
– DHCP options 1, 3, 6, 12, 15, 28, 33, 42, 43, 53, 54, 55, 60, 66, 67, 82, 120, 121;
– Echo cancellation (G.168 recommendation);
– Packet loss concealment (PLC);
– Voice activity detector (VAD);
– Silence suppression;
– DTMF tone detection and generation;
– DTMF transmission (INBAND, rfc2833, SIP/H.232 methods)
– Fax transmission:
  - T.30;
  - T.38 UDP Real-Time Fax;
  - upspeed/pass-through.
– Modem support:
  - Cisco NSE;
  - V.152 (G.711a/u VBD).
– Flexible numbering plan;
– Operation with and without external gatekeeper (H.323/RAS);
– IE, Firefox, Opera, Google Chrome browsers compatibility;
– BroadWorks platform compatibility;
– Support up to 8 SIP profiles;

[1] SIP-T only supports basic call establishment, additional types of service are not implemented

- Ability to operate without SIP proxy;
- Operation with multiple SIP proxy servers in various SIP profiles;
- Support for VoIP operation in the switch in case of SIP proxy server connection loss;
- Active session support for SIP protocol operations through NAT;
- Transmission of cpc-rus subscriber category via SIP protocol;
- Multi-user mode for access via Web interface - support of four userswith different access levels;
- Configuration file download/upload: via FTP/FTPS, TFTP, HTTP/HTTPS;
- Firmware update: via TFTP, HTTP/HTTPS;
- Automatic configuration and firmware update via FTP, TFTP, HTTP/HTTPS;
- Line parameter measurement;
- Extraneous voltage in the wires determination;
- Ability to use TCPdump utility application directly on the device;
- STP support;
- LLDP support;
- iptables network-level firewaall
- STUN support
- Numbering plan with capacity up to 1000 characters;
- Service (simulation service) management using IMS (3GPP TS 24.623);
- Remote monitoring, configuration and setup:
  - Web interface;
  - SSH;
  - Telnet;
  - SNMP v2, v3;
  - TR-069;
  - User authentication with RADIUS server.
- Embedded firewall with the ability of security rules flexible configuration;
- Adjustable access ports with the ability to block access for:
  - WEB (HTTP);
  - Telnet;
  - SSH.
- Supported suplementary services (Value Added services):
  - Call Hold/Retrieve;
  - Call Transfer;
  - Call Waiting;
  - Call Forward Busy;
  - Call Forward No Answer;
  - Call Forward Unconditional;
  - Call Forward Out Of Service;
  - Caller ID with ETSI FSK type 1, type 2;
  - Caller ID in DTMF format;
  - 'Russian Caller ID';

- Calling without Caller ID broadcasting;
- Hotline/warmline;
- Call Hunt;
- Call PickUp;
- 3-way conference (local or using conference server);
- Voice message waiting indicator – MWI;
- Do Not Disturb.

– Selection of power supply configuration: by DC or AC (for v4.0 and rev.B/rev.D);
– Ability of monitoring via Web interface:

- Subscriber lines status;
- Services status;
- Hardware platform;
- Switch network ports status.

– Logging;
– Maintenance of statistics on FXS port operation (port status, number of calls, last number dialed, number of packets transmitted/received/lost).

SIP, supported recomendations:

– RFC 3261 SIP 2.0;
– RFC 3262 SIP PRACK;
– RFC 4566 Session Description Protocol (SDP);
– RFC 3263 Locating SIP servers for DNS lookup SRV and A records;
– RFC 3264 SDP Offer/Answer Model;
– RFC 3265 SIP Notify;
– RFC 3311 SIP Update;
– RFC 3515 SIP REFER;
– RFC 3891 SIP Replaces Header;
– RFC 3892 SIP Referred-By Mechanism;
– RFC 5806 Diversion Indication in SIP;
– RFC 4028 SIP Session Timer;
– RFC 2976 SIP INFO Method;
– RFC 2833 RTP Payload for DTMF Digits, Flash event;
– RFC 3108 Attributes ecan and silenceSupp in SDP;
– RFC 4579 SIP. Call Control - Conferencing for User Agents;
– RFC 3372 SIP for Telephones (SIP-T);
– RFC 3398 ISUP/SIP Mapping;
– RFC 3204 MIME Media Types for ISUP and QSIG (ISUP support);
– RFC 3361 DHCP Option 120;
– RFC 3966 The tel URI for Telephone Numbers;
– SIP OPTIONS Keep-Alive (SIP Busy Out);
– NAT support.

2.2 Use cases

This manual covers the following TAU-36.IP/TAU-72.IP connection methods:

1. Subscriber access point. In this case the device acts as a gateway between analogue phone units and remote PBX, see the figure below. Gateway's subscriber ports are registered at the software switch — Softswitch. Supplementary services (value added services (VAS)) in this method are provided by the software switch.

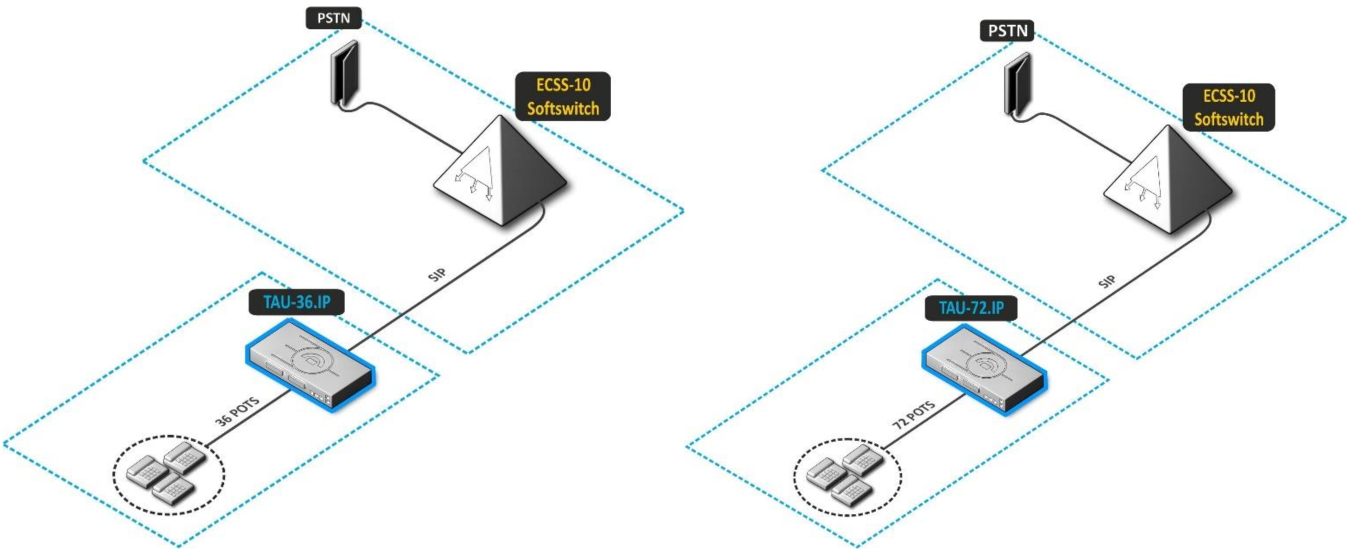


Fig. 1 — TAU-36.IP/TAU-72.IP subscriber access point

2. Distributed mini-PBX mode. In this case, the device acts as a mini-PBX that is able to access other gateways (TAU-32M.IP, TAU-72.IP, etc.) and Softswitch using SIP/H.323 protocols. The device processes supplementary services (VAS), call routing, see the figure below.

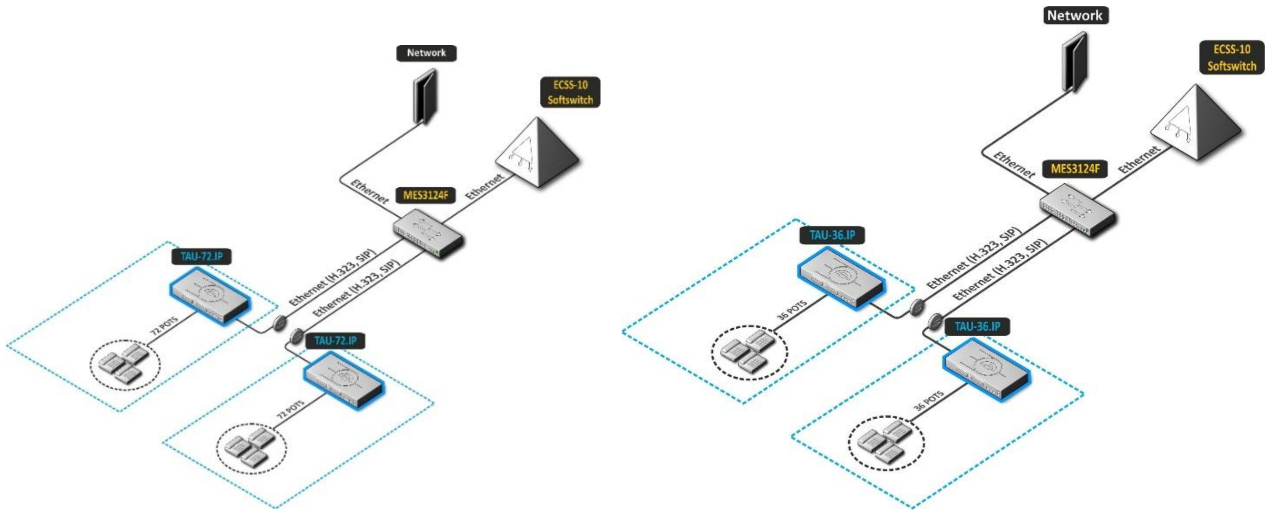


Fig 2 — TAU-36.IP/TAU-72.IP distributed mini-PBX

2.3 Design and operating principle

Subscriber voice signals are served to audio codecs of subscriber units, where they are encoded using one of the selected standards, and then sent as digital packets to the controller via internal backbone. In addition to voice signals, digital packets contain control and interaction signals.

Controller supports H.323 and SIP protocols and exchanging data between audio codecs and IP network via MII interface and Ethernet switch.

Figure 3a shows TAU-72.IP functional diagram.

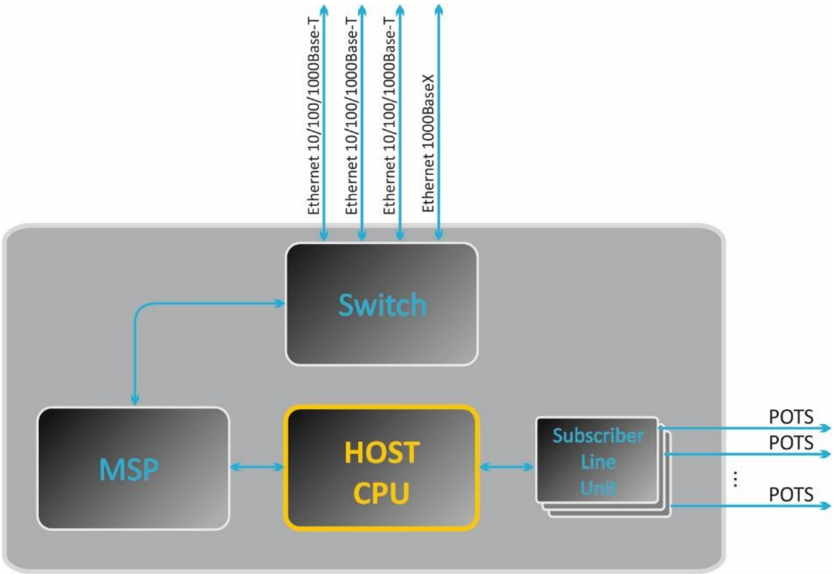


Figure 3a — TAU-72.IP functional diagram

Figure 3b shows TAU-36.IP functional diagram.

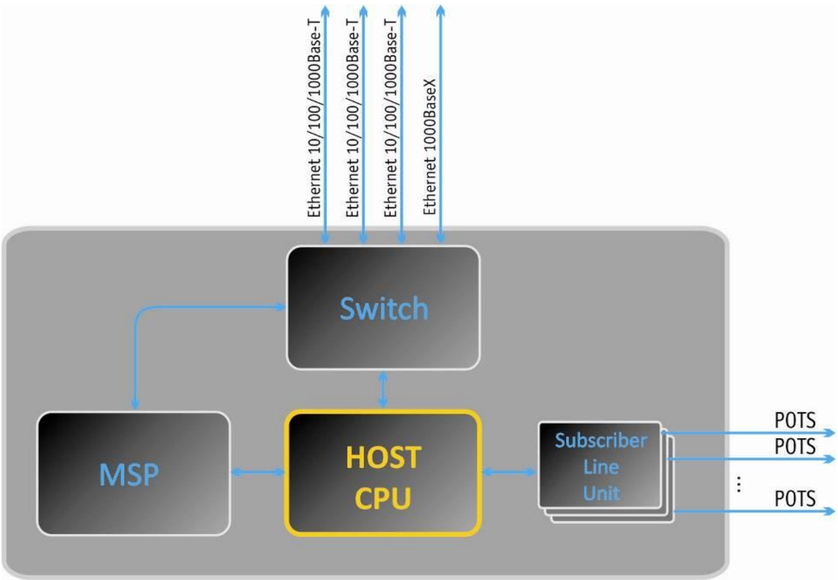


Figure 3b — TAU-36.IP functional diagram

2.4 Main specifications

Main specifications of the gateway are listed in following tables:

Table 1 — Main specifications of the gateway

Protocols and Standarts

Protocol stack	H.323 v3/v4/v5
Communication protocol for session initiation, monitoring and cancellation	SIP, SIP-T
Fax support	T.38 UDP Real-Time Fax pass- through (G.711A/U)
Modem support	V.152 CISCO NSE
Voice standards	VAD (voice activity detector) AEC (echo cancellation, G.168 recommendation) CNG (comfort noise generator) AGC (automatic gain control) PLC (packet loss concealment)

Voice codecs

Codecs	G.729, annex A, annex B G.711(PCMA, PCMU) G.723.1 (6.3 Kbps, 5.3 Kbps, Annex A) G.726-32 (for SIP only)

Number of simultaneous channels, supported by device depending on codec type

Codec	Number of channels	
	TAU-36.IP	TAU-72.IP
G.711 (A/U)	36	72
G.729 / 20-80	36	72
G.729 A / 10	36	62
G.723.1	36	58
G.726	36	72
T.38	36	54

Parameters of electrical Ethernet interface

Number of ports	3
Electrical connector	RJ-45
Data rate	Autonegotiation, 10/100/1000 Mbps duplex
Standards support	10/100/1000BASE-T

Parameters of optical Ethernet interface

Number of ports	V1.0, V2.0	V3.0, V4.0, rev.B/rev.D
	1	2
Optical connector	Mini-Gbic (SFP): 1) full-duplex, two-fiber with 1310 nm (Single-Mode), 1000BASE-X (LC connector), the supply voltage — 3.3V 2) duplex, single fiber with wavelengths in the transmission/reception 1310/1550 nm, 1000BASE-X (SC connector), the supply voltage — 3.3V	
Transfer rate, Mbps	1000 Mbps duplex	
Standards support	1000BASE-X	

Analogue user port specifications

Number of lines	TAU-36.IP	36
	TAU-72.IP	72
Loop resistance	Up to 3.4 kΩ	

Dialling reception	Pulse/DTMF
Caller ID	FSK (ITU-T V.23, Bell 202), DTMF, 'Russian Caller ID'
Comprehensive protective circuit	Comprehensive protective circuit (current and voltage). **To protect subscriber line curcuit from overload, cross must be equipped with cross protection modules. Recommended protection module is 'MK3 3-K' with cut-off voltage of 400 V.**
Remote measurement of parameters of the subscriber line	Yes
Parameters set	Programmable

Console parameters

RS-232 serial port	
Data rate, bps	115200
Electrical parameters of signals	According to ITU-T Recommendation V.28

Network and Configuration

Connection types	Static IP, DHCP client
Management	Web, RS-232 console, Telnet, SSH
Security	User name and password verification, HTTPS, FTPS

Physical specifications and ambient conditions

<table>
<tr><td rowspan="3">Power voltage</td><td>V1.0, V2.0, V3.0</td><td>V4.0</td><td>rev.B/rev.D</td></tr>
<tr><td rowspan="2">DC: -36..- 60 V</td><td>DC: -36..- 60 V</td><td>DC: -36..-72 V</td></tr>
<tr><td colspan="2">AC: ~100-240 V 50 Hz

When the device is installed in a small non ventilated closet, acceptable load capacity is up to 0.4 Erl per subscriber unit for AC powered devices, and 0.8 Erl — for DC powered. If forced air supply is used, it is possible for the device to operate under heavier load.</td></tr>
<tr><td>Power consumption without active subscribers</td><td colspan="3">30 W</td></tr>
<tr><td>Current consumption of active subscriber set</td><td colspan="3">30 mA</td></tr>
<tr><td>Operating temperature range</td><td colspan="3">From 0 to 40 °C</td></tr>
<tr><td>Relative humidity</td><td colspan="3">Up to 80 %</td></tr>
<tr><td rowspan="2">Ambient noise</td><td colspan="3">Launch and operational mode: 0 dB</td></tr>
<tr><td colspan="3">After processor heating: 50 dB</td></tr>
<tr><td>Dimensions (W × H × D)</td><td colspan="3">420 × 45 × 240 mm, 19' form-factor, 1U size</td></tr>
<tr><td>Weight</td><td colspan="3">3.2 kg</td></tr>
</table>

2.5 Design

TAU-36.IP/TAU-72.IP VoIP gateway has a metal 420 × 45 × 240 case.

TAU-36.IP front panel appearance is shown on Fig. 4a, 4b.

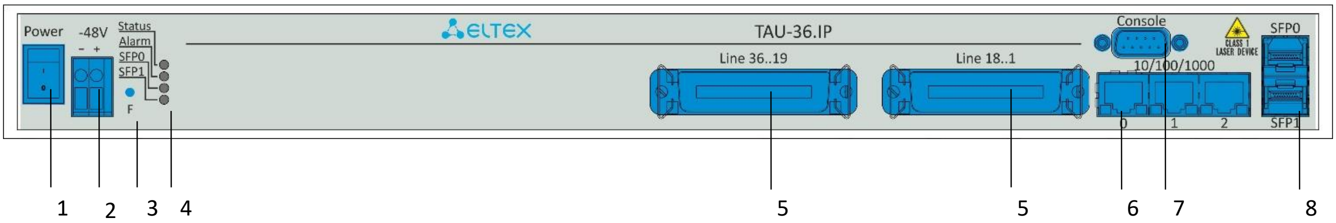


Fig. 4a — TAU-36.IP DC front panel appearance

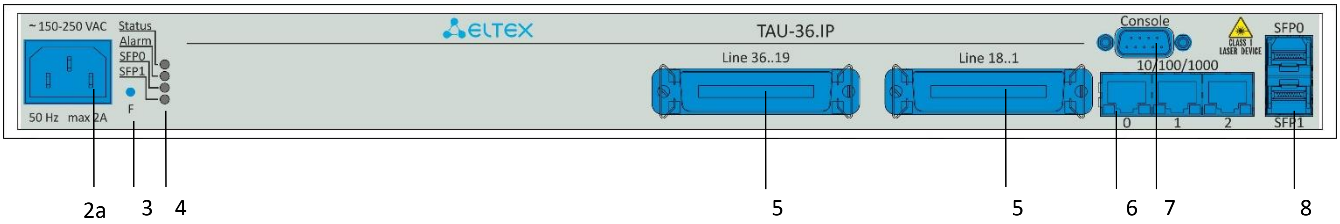


Fig. 4b — TAU-36.IP AC front panel appearance

Front panel appearance is shown on 4c-f.

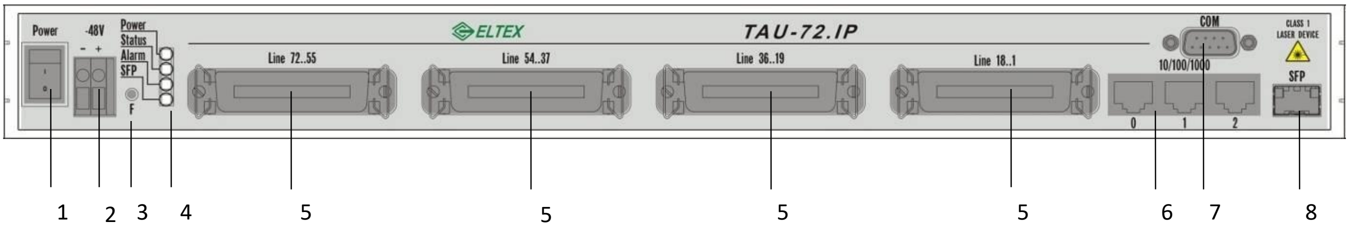


Fig. 4c — TAU-72.IP v2.0 front panel appearance

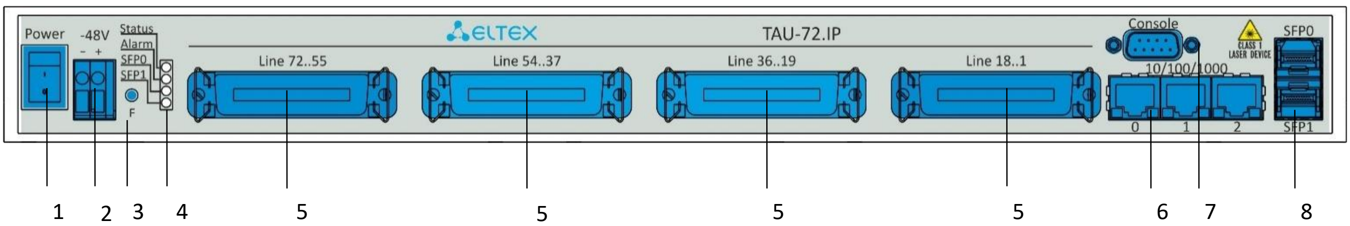


Fig. 4d — TAU-72.IP v3.0 front panel appearance

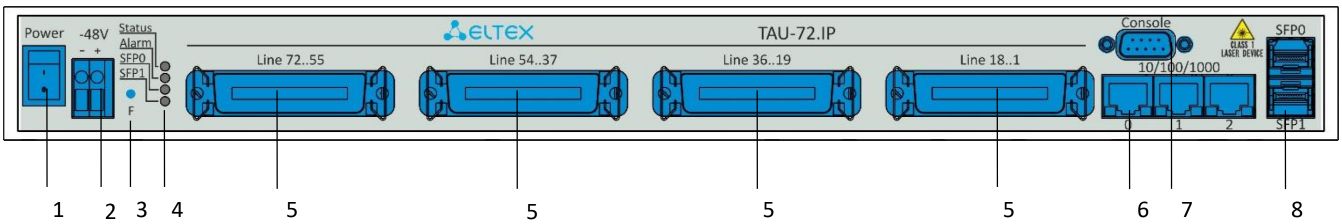


Fig. 4e — TAU-72.IP v4.0 and rev.B/rev.D DC front panel appearance

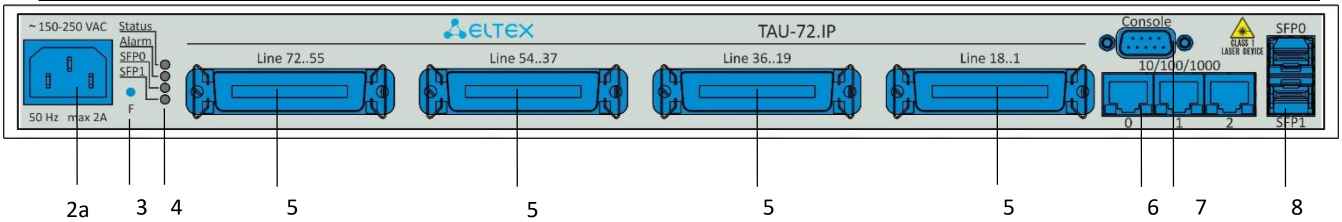


Fig. 4f — TAU-72.IP v4.0 and rev.B/rev.D AC front panel appearance

Connectors, LEDs and controls located on the front panel of the device are listed below.

Table 2 – Description of connectors, LEDs, and controls located on the front panel

№	Front panel elements	Description
1	***Power***	Power toggle
2	***-48V***	Connector for DC power supply with rated voltage 48 V DC
2a	***~100 – 240 VAC, 50 Hz max 2A***	Connector for AC power supply with voltage 100–240 V AC, 50 Hz
3	***F***	Function button
4	***Power***	Power supply indicator
	Status	Device operation indicator
	Alarm	Alarm indicator
	SFP (SFP0, SFP1)	Optical interface SFP processing indicator. Lights green when optic link is present
5	***Line 1...18, 19...36, 37...54, 55...72***	4 CENC-36M connectors for analogue phones connection (pin designation is listed in APPENDIX A. TAU-72.IP/TAU-36.IP VoIP GATEWAYS CONTACT PIN ASSIGNMENT)
6	***10/100/1000***	3 x RJ-45 ports of Ethernet 10/100/1000BASE-T interfaces
7	***COM***	RS-232 console port for local control of the device
8	***SFP (SFP0, SFP1)***	Chassis for optical SFP modules of 1000BASE-X Gigabit uplink interface used for IP network connection

The layout of the device rear panel is shown on figure 5.

Fig. 5 — TAU-36.IP/TAU-72.IP rear panel appearance

Earth bonding point is located on the rear panel of the device.

Pin assignment is listed in APPENDIX A. TAU-72.IP/TAU-36.IP VoIP GATEWAYS CONTACT PIN ASSIGNMENT.

2.6 Device ventilation

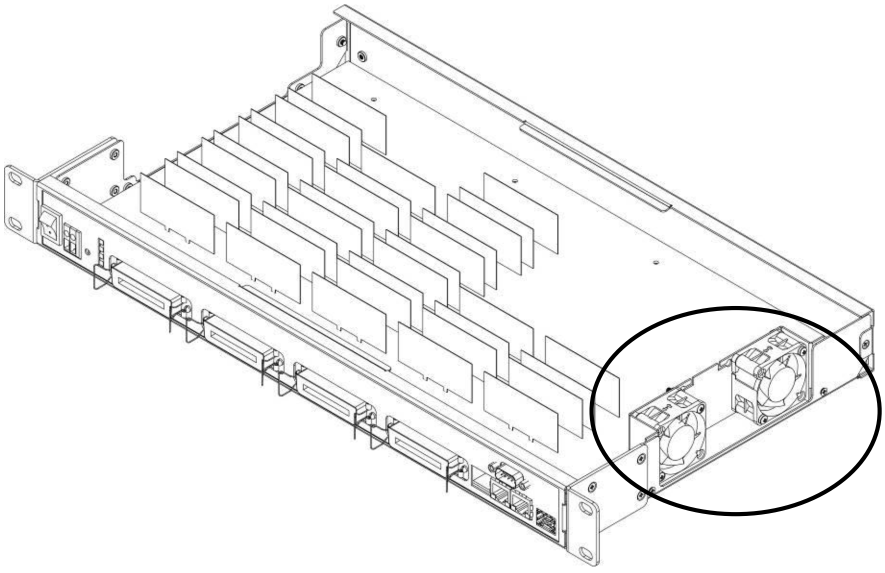


Fig. 6 — Fan location

There are ventilation openings on the device side panels that serve to remove heat. There are two fans installed in the side panel.

The air flow enters through the perforated right side panel of the device, passes through the entire range of internal components, cooling each of them, and is brought out with left perforated panel fans. The other panels of the device do not contain ventilation holes, which allows to maintain the necessary internal pressure of air flow.

Do not block any ventilation openings. This may cause overheating of the components, which may result in device malfunction.

If the device is being installed into a closed non-ventilated cabinet with volume less than 180l per device supplied by the DC, device performance will not exceed 0.8 Erlang per subscriber unit.

If the device is being installed into a closed non-ventilated cabinet with volume less than 180l per device supplied by the AC, device performance will not exceed 0.4 Erlang per subscriber unit.

2.7 Light indication

Power, [1]***Alarm, Status, SFP LEDs*** located on the front panel indicate the current state of the device. Table 3 lists possible states of the LEDs.

Table 3 - Device status LED indication

Indicator	Indicator State	Device state
Power1	solid green	Device power supply is on
	off	Device power supply is off
Status	solid red	Operating system is not loaded (together with LED ***Alarm***)
		Main application is not running (together with LED ***Alarm***, flashing in *Fatal* mode)
	solid yellow	Device initialization in progress, subscriber ports are not initialized yet
		Address is not obtained through DHCP (if dynamic address obtaining method is enabled)
	solid green	Subscriber ports are initialized, device is in operation
	off	Operating system has been loaded, board type identified
	flashes red, yellow, and green	**Factory Safemode** (together with LED ***Alarm***, flashing in *Fatal* mode), or **factory reset** (together with constantly solid ***Alarm*** LED)
Alarm	solid red	Alarm – port blocking, the output value of the parameter sensor platform within range
	solid on	*Warning* – port blocking, operating system loading
	flashes slowly (once per second)	*Error (failure)* – module sensor failure (SFP module installed, but there is no link)
	flashes rapidly (once per 200 ms)	*Fatal* (*critical failure*) – connection of the main application to subscriber ports is lost
	off	Normal state
SFP (SFP0, SFP1)	solid green	Optical link is present
	off	No optical link

Ethernet interface state is shown by 1000/100 socket built-in LED indicators.

Table 4 - Light indication of Ethernet 10/100/1000 interfaces

Yellow LED 10/100/1000	Green LED 10/100/1000	LED/Status
solid on	solid on	Port operates in 1000BASE-T mode, data transfer is inactive
solid on	flashes	Port operates in 1000BASE-T mode, data transfer is active
off	solid on	Port operates in 10/100BASE-TX, data transfer is inactive
off	flashes	Port operates in 10/100BASE-TX, data transfer is active

[1] For TAU-36.IP/TAU-72.IP v1.0, v 2.0 only

2.8 'F' Function Button Operation

To reboot the operating device, press and hold 'F' button located on the front panel of the device for 1–9 seconds. After releasing the button, the ***Alarm*** LED will become solid red and the device will reboot.

Also, this button allows you to reset the device to factory settings to get access to the device when the IP address or the password is forgotten or unknown. To do this, press and hold the 'F' button for 10-14 seconds until the ***Status*** LED begins to flash yellow, green and red alternatively. When the ***Alarm*** LED becomes solid red the button should be released. The configuration will be reset to factory settings and the device will be rebooted. After that, you can access the device by IP address ***192.168.1.2.*** When connecting to the web interface, the default password for ***admin*** username is ***rootpasswd.*** Further, you can view/change IP address and set a new password. If the button is not released during the period between 10 and 14 seconds, after a while all LEDs will go out (the device will start rebooting). Soon after the ***Status*** LED will begin to flash yellow, green and red alternatively, and the ***Alarm*** LED will begin to flash red. When releasing the 'F' button at this moment, the configuration will not be reset to factory settings and will switch to the ***Safemode***. This mode allows changing the factory configuration, in other words, selecting a method of network settings obtaining - statically or dynamically. If you continue to hold the ‘F’ button in the ***Safemode***, the cycle of the button operation will be repeated, that is, the restart will occur again if the button is held for 1–9 seconds, the reset to the factory settings if the button is held for 10–14 seconds.

For detailed description of the factory reset procedure, see Section 6.5 Reset the device to the factory settings.

2.9 Delivery package

2.9.1 TAU-36.IP delivery package

TAU-36.IP standard delivery package includes:
- VoIP Gateway TAU-36.IP;
- CENC-36M connector — 2 pcs (if there is no UTP CAT5E 18 cable in the order);
- CENC-36M connector’s locks — 4 pcs;
- Console cable;
- A mounting set for 19” rack;
- Technical passport.

For **DC** power supply devices:
- PVC 2 × 1.5 power cord — 2 m.

For **AC** power supply devices:
- Power supply cord europlug C13 1.8 m;

If ordered, delivery package may also include:
- 1000BASE-T/Mini-Gbic (SFP) optical interface — 1/2 pcs.
- UTP CAT5E 18 cable with CENC-36M connectors — 1 pcs.

2.9.2 TAU-72.IP delivery package

TAU-72.IP standard delivery package includes:
- Analog VoIP Gateway TAU-72.IP;
- CENC-36M connector — 4 pcs. (if there is no UTP CAT5E 18 cable in the order);
- CENC-36M connector’s locks — 4 pcs;
- Console cable;
- A mounting set for 19” rack;

– Technical passport.

For **DC** power supply devices:
– PVC 2 × 1.5 power cord — 2 m.

For **AC** power supply devices:
– Power supply cord europlug C13 1.8 m;

If ordered, delivery package may also include:
– 1000BASE-T/Mini-Gbic (SFP) optical interface — 1/2 pcs.
– UTP CAT5E 18 cable with CENC-36M connectors — 2 pcs.

3 INSTALLATION AND SAFETY MEASURES

This section describes safety measures and installation of the equipment into a rack and connection to a power supply.

Check the device for visible mechanical damage before installing and turning it on. In case of any damage, stop the installation, fill in a corresponding document and contact your supplier.

3.1 Safety instruction

3.1.1 General requirements

Any operations with the equipment should comply with the safety regulations for operation with electrical installations.

Operations with the equipment should be carried out only by personnel authorised in accordance with the safety requirements.

1. Before operating the device, all engineers should undergo special training.

2. The device should be connected only to properly operating supplementary equipment.

3. TAU-72.IP/TAU-36.IP gateway could be permanently used provided the following requirements are met:

   – Ambient temperature from 0 to +40 °C.
   – Relative humidity up to 80 % at +25 °C.
   – Atmosphere pressure from 6.0×10^4 to 10.7×10^4 Pa (from 450 to 800 mm Hg).

4. Do not expose the device to mechanical shock, vibration, smoke, dust, water, and chemicals.

5. Do not block air vents or place objects on the equipment to avoid overheating which may result in device malfunction.

6. To avoid failures caused by electrostatic discharge, we strongly recommend you to put on ESD belt, shoes or wrist strap to prevent electrostatic charge accumulation (for the wrist strap, ensure that it fits snugly to the skin) and to ground the device before operation starts.

3.1.2 Electrical Safety Requirements

1. Prior to connecting the device to a power source, ensure that the equipment case is grounded with an earth bonding point. The ground wire should be securely connected to the earth bonding point. The resistance between the earth bonding point and ground bus should be less than 0.1 Ω.

2. PC and measurement instruments should be grounded prior to connection to the device. The potential difference between the equipment case and the cases of the instruments should be less than 1 V.

3. Prior to turning the device on, ensure that all cables are undamaged and securely connected.

4. Make sure the device is off, when installing or removing the case.

3.1.3 Electrostatic Discharge Safety Measures

To avoid failures caused by electrostatic discharge, we strongly recommend you to:

1. Put on ESD belt, shoes or wrist strap to prevent electrostatic charge accumulation (for the wrist strap, ensure that it fits snugly to the skin) and to ground the the device before operation starts.

3.2 Installation procedure

1. Check the device for visible mechanical damage before installing and turning it on. In case of any damage, stop the installation, fill in a corresponding document and contact your supplier.

2. If the device was exposed to low temperatures for a long time before installation, leave it for 2 hours at ambient operating temperature prior to operation. If the device was exposed to high humidity for a long time, leave it for at least 12 hours in normal conditions prior to turning it on.

3. Mount the device. The device is intended to be installed into 19' rack using the mounting set or mounted on the horizontally oriented perforated shelf.

When the device is installed in a small non ventilated closet (less than 180 L per device), acceptable load capacity is up to 0.4 Erl per subscriber unit.

4. Ground the case of the device after installation. This should be done prior to connecting the device to the power supply. An insulated multiconductor wire should be used for earthing. The device grounding and the earthing wire section should comply with Electric Installation Code. The earth bonding point is located at the right bottom corner of the rear panel, see 5.

3.2.1 Opening the case

First power the device off, disconnect all the cables.

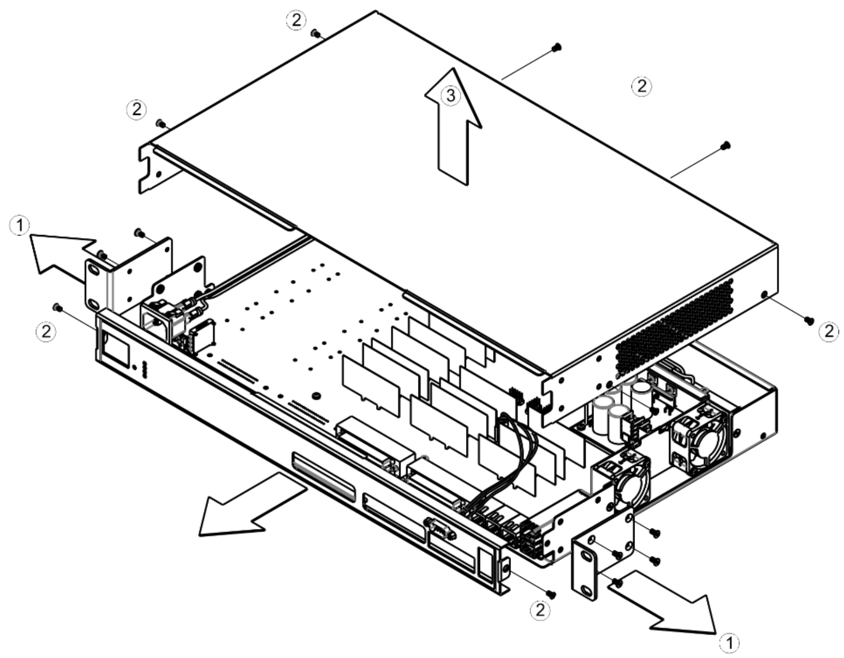


Fig. 7 — TAU-36.IP/TAU-72.IP case opening order

1. Detach brackets from device case using screwdriver.
2. Detach device front and top panel fixation screws, using screwdriver, as shown on 7.
3. Remove device top panel by pulling it up.

Execute actions that listed above in reverse order to assemble the device into case.

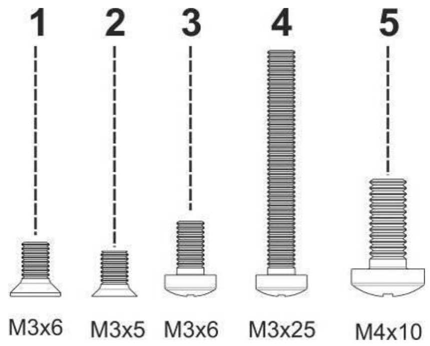


Fig. 8 —TAU-36.IP/ TAU-72.IP assembling screw types

The figure above shows screw types, used for assembling the device into case:

1. Rack brackets mounting.
2. Case parts mounting.
3. Board, ventilation unit, plug, rail mountings.
4. Fan mounting screw.
5. Earthing screw.

Don't use inappropriate screw type when assembling the device. Screw type changing may cause device failure.

3.3 Connecting the device

Connect subscriber lines, optical and electrical Ethernet cables to corresponding connectors.

To protect subscriber line curcuit from overload, cross must be equipped with cross protection modules. Recommended protection module is 'MK3 3-K' with cut-off voltage of 400 V.

The protection modules (MK3) are designed to protect the FXS and FXO sets of TAU-72M.IP and TAU-36M.IP gateways from dangerous surge voltages and currents in air cable strands caused by lightning discharge, high-voltage electric transmission lines, overhead wirings of electric railway and various industrial sources of impulse interferences as well as from contact with low voltage power lines.

The protection modules contain two voltage protection cascades (the first one is on the aerial fuse, the second one is on the semiconductor switches) and current protection (on the polymer posistors).

The installation of MK3 protection modules requires the grounding bar mounted on the linear side. The arrester is installed in normally closed connecting strip (Krone, Intercross or their compatibles) according to the marking on the device body. The connection diagram is shown in the figure below.

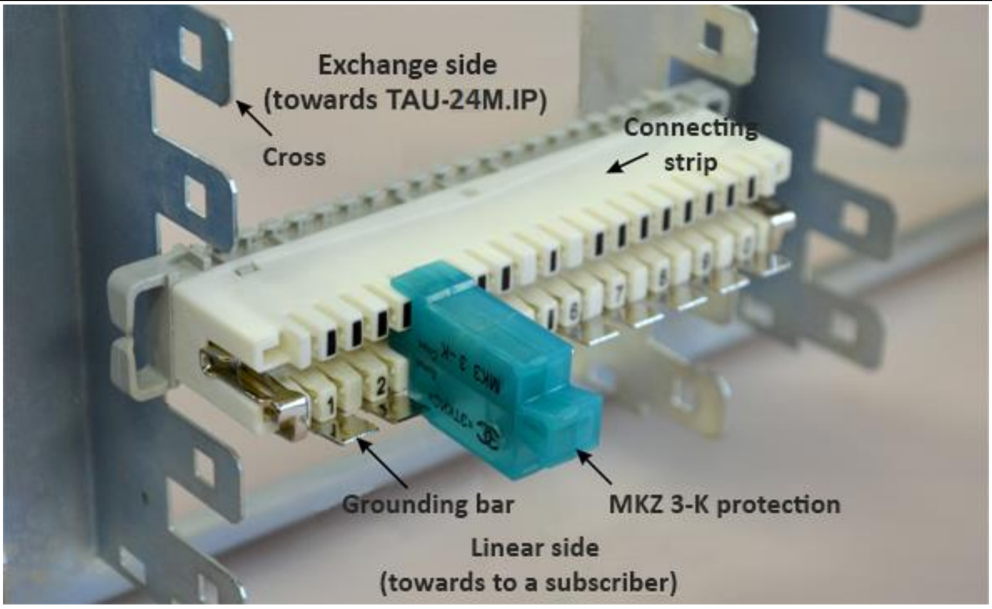


Fig. 9 - Connection diagram

Connect the power supply cable to the device. Depending on the provided sources, the device could be powered from grounded power outlet 220/110 V AC, 50/60 Hz, or from -48...-60 V DC power supply. To connect the device to 220 V AC electrical network, use the cable provided with the delivery package. To connect the device to DC power supply, use the cable with cross-section not less than 1mm^2.

When connecting to the 220 V AC power supply, it is necessary to install protection against electrical overstress (EOS).

Ensure that all cables are undamaged and securely connected.

Turn the device on and check the front panel LEDs to make sure the gateway is in normal operating conditions (Section 2.7 Light indication).

4 GENERAL OPERATION GUIDELINES

The easiest way to configure and monitor the device is to use the web interface, so we recommend you to use it for these purposes.

In order to prevent an unauthorized access to the device, we recommend you to change passwords for administrator, operator and non-privileged users. For setting password for web interface access, see Section 5.1.6.6 The 'Passwords' submenu. We recommend you to write down and store defined passwords in a safe place, inaccessible for intruders.

Device management from public networks must be forbidden. To allow management from the allocated VLAN, see section 5.1.1.3 The 'VLAN conf' submenu. Virtual Local Area Network. To disable unused protocols for management and change ports set by default, see section 5.1.1.1 The ‘Network’ submenu.

In order to prevent device configuration loss, e.g. after reset to factory settings, we recommend you to backup configuration each time significant changes are made and store backup files on a PC.

5 DEVICE CONFIGURATION

You can connect to the device using four methods: via web interface, via Telnet/SSH2 protocols, or via serial port (console parameters: 115200, 8, n, 1, n).

The device runs on Linux, settings are stored as text files in a directory ***/etc ~/config*** (in normal mode ***/etc ~*** is a link to the directory ***/etc***, when booting from pressing 'F' in directory ***/etc ~*** configured by the user, and in the ***/etc*** directory factory configuration of the device).

Configuration files can be edited by connecting the device via the RS-232 or Telnet using built-in text editor *joe*.

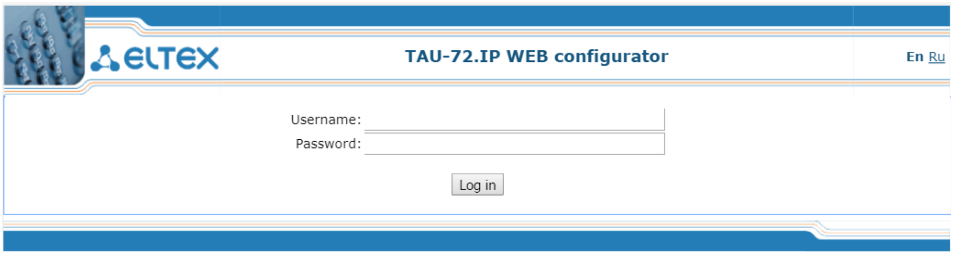
To save the contents of the directory ***/ etc ~*** non-volatile memory device, use the *save* command. The changes take effect after rebooting the device.

5.1 Configuration via WEB Interface. Administrator Access[1]

To configure the device, establish connection in the web browser, e.g. Firefox, Internet Explorer.

TAU-36.IP/TAU-72.IP factory default IP address — 192.168.1.2, network mask — 255.255.255.0

After entering IP address the device will request username and password.



Initial startup username: *admin*, password: *rootpasswd*.

For security reasons, duration of authorized access session is limited for 20 minutes, i.e. if you are inactive after establishing connection to the device interface for the stated amount of time, the session will be over. This restriction is not valid for '*Monitoring*' or '*System info*' pages, as these pages perform periodic polling of the device data.

Up to 4 users may connect to the device web interface simultaneously.

The following menu will appear on the administrator's terminal: to prevent unauthorized access to device in the future, it is recommended to change password (see Section 5.1.6.6).

In all tabs, the *Save* button stores configuration into the non-volatile (flash) memory of the device.

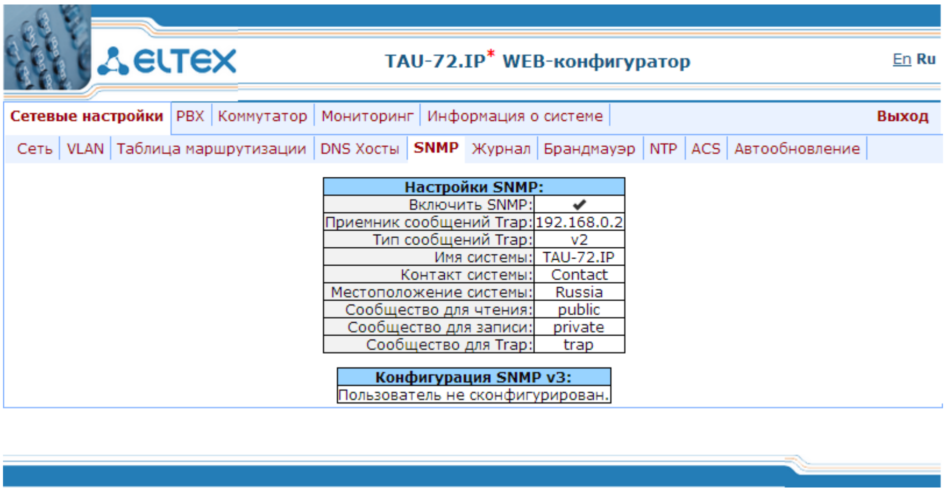
[1] The description is an example of the configurator for TAU-72.IP. For TAU-36.IP device settings are the same, the number of configurable ports — 36.

Web configurator language

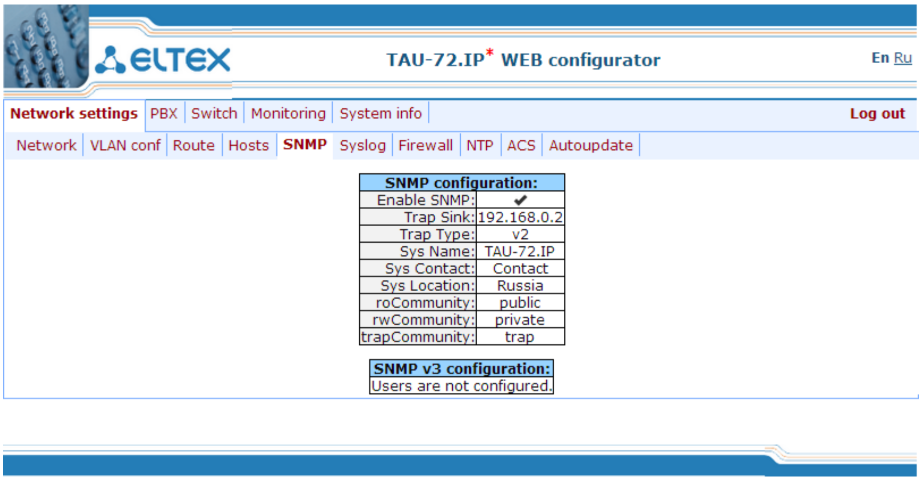
Web configurator allows you to select from two interface languages: *'Russian (Ru)'* or *'English (En)'*.

Firmware version default language is English. To change the interface language, select the respective link in the web configurator header bar (on the right side).

Example of web configurator menu in Russian:



Example of web configurator menu in English:



Indication of Changes in Web Configurator

Web configurator supports indication of configuration changes that is shown in the header bar of configuration interface (TAU-36.IP/TAU-72.IP web configurator). Table 5 lists indicator states ('*' character in the header bar of configuration interface).

Table 5 — Indicator state *

Indicator State	Description
* character is red	Changes has been made to the configuration, but it has not been saved to flash memory yet.
* character is not shown	No changes has been made to the configuration or changes has been successfully saved to flash memory;

When network settings are changed, web service on the device restarts, and when the connection is established using new address, '*' character will not be shown, but the configuration will still contain changes that are not saved to the flash memory.

lists description of configuration menu windows.

Table 6 — Description of configuration menu, administrator access

Menu (en)	Menu (ru)	Description
Network settings	***Сетевые настройки***	**Adjustment of the device network settings**
Network	*Сеть*	Configuration of network settings
IPSec	*IPSec*	Configuration of IPSec settings
VLAN conf	*VLAN*	VLAN configuration
Route	*Таблица маршрутизации*	Static route configuration for WAN and VLAN interfaces
Hosts	*DNS хосты*	Local DNS server configuration
SNMP	*SNMP*	SNMP agent configuration
Syslog	*Журнал*	Syslog server configuration
MAC filter	*Фильтр MAC*	Configuration of filtration by MAC addresses
Firewall	*Брандмауэр*	Configuration of denied/allowed IP server addresses
NTP	*NTP*	NTP configuration
ACS	*ACS*	TR-069 monitoring and management protocol settings
Autoupdate	*Автообновление*	Automatic update configuration
PBX	***PBX***	**VoIP (Voice over IP) configuration**
Main	*Основные функции*	Device basic settings
SIP/H323 Profiles	*Профили SIP/H323*	Configuration of SIP/H323 profiles
SIP Common	*SIP Общие*	SIP common settings
H323	*H323*	H323 protocol settings (works in profile 1 only)
Profile 1..8	*Профиль 1..8*	Configuration of profiles
SIP Custom	*SIP настройки профиля*	SIP custom settings for a profile
Codecs	*Кодеки*	Codec settings for a profile
Dialplan	*План набора*	Routing settings for a profile
Alert info	*Alert info*	Configuration of a distinctive ring, formed by Alert Info value
TCP/IP	*TCP/IP*	Configuration of network port range for various protocols
Ports	*Абонентские порты*	Configuration of device subscriber ports and subscriber profiles
Call limits	*Ограничение вызовов*	Configuration of simultaneous call limits
Suppl. Service Codes	*Услуги ДВО*	Configuration of supplementary service codes
Serial groups	*Группы вызова*	Configuration of serial groups
PickUp groups	*Группы перехвата*	Configuration of pickup groups
Distinctive ring	*Звонок особого типа*	'Distinctive ring' service administration
Modifiers	*Модификаторы*	Configuration of number modifiers
Acoustic signals	*Акустические сигналы*	Configuration of acoustic signals parameters
Dialplan profiles	*Профили плана нумерации*	Configuration of profiles for routing
Profile 1..4	*Профиль 1..4*	Configuration of profiles
Switch	***Коммутатор***	**Configuration of switch settings**
Switch ports settings	*Настройки портов коммутатора*	Configuration of integrated Ethernet switch ports
802.1q	*802.1q*	Configuration of packet routing rules for switch operation in 802.1q mode

QoS & Bandwidth control	*QoS и управление полосой пропускания*	Quality of service functions and bandwidth limits configuration
Monitoring	***Мониторинг***	**Device monitoring**
Port	*Порт*	Device subscriber ports status information
Status	*Статус*	Gateway hardware platform status information– voltages, temperature sensors, fans, SFP data
Switch	*Коммутатор*	Switch port status monitoring
Suppl. Service	*ДВО*	Information on the current status of supplementary services on subscriber port
IMS SS status	*Статус услуг IMS*	Monitoring of services, software controlled switch with support for IMS
Serial groups	*Группы вызова*	Monitoring of registration serial groups
IMS SS status	*Статус услуг IMS*	Information about current IMS services status
Serial groups	*Группы вызова*	Information about current serial groups status
System info	***Информация о системе***	**System info**
Device info	*Информация об устройстве*	View the device and network settings information
Route	*Таблица маршрутизации*	View the Routing table
ARP	*ARP*	View the ARP table
Service	***Сервисные функции***	**Firmware update, configuration file operations, rebooting device, setting/changing passwords**
Firmware upgrade	*Обновление ПО*	Subscriber units firmware update
Backup/Restore	*Управление конфигурацией*	Download/upload configuration files to/from PC
Reboot	*Перезагрузка*	Rebooting device
Security	*Безопасность*	Encryption feature
MOH	*Музыка*	Download/upload audio file for call hold service
Password	*Пароли*	Management of passwords used to access the device via Web interface
Call history	*Журнал вызовов*	View and upload of call log
Logout	***Выход***	**Finish the device administration session for the current user**

5.1.1 The 'Network settings' menu

In the *Network settings* menu, you can define network settings of the device.

5.1.1.1 The 'Network' submenu

In the *'Network'* submenu, you may specify the device name, IP address, subnet mask, network broadcast address*,* DNS server address, device access rules, etc.

DHCP is a protocol that allows to automatically obtain IP address and other settings required for operation in TCP/IP network. It allows the gateway to obtain all necessary network settings from DHCP server.

SNMP is a simple network management protocol. It allows the gateway to send real-time messages on occurred failures to controlling SNMP manager. Also allows the gateway to send real-time messages on occurred failures to controlling SNMP manager. Also, gateway SNMP agent supports monitoring of gateway sensors' status on request from SNMP manager.

DNS is a protocol that allows to obtain domain information. It allows the gateway to obtain IP address of the communicating device by its network name (hostname). It may be necessary, e.g. when specifying hosts in the routing plan or using network name of the SIP server as its address.

Telnet is a protocol that allows to establish mechanisms of control over the network. It allows you to remotely connect to the gateway from a computer for configuration and management purposes. For Telnet protocol operation, the data transfer process is not encrypted.

SSH is a protocol that allows to establish remote control over the network. Serves the similar purpose as Telnet protocol, but unlike the latter provides encryption of the transferred data.

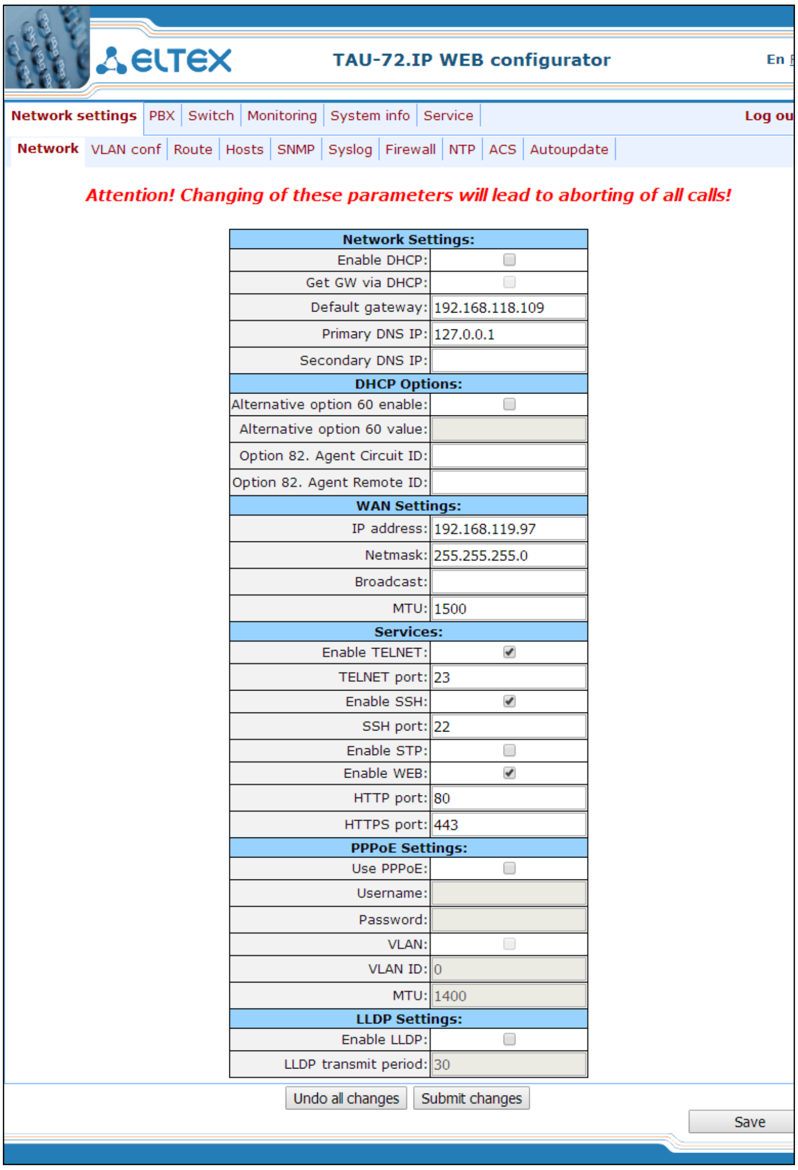
LLDP (Link Layer Discovery Protocol) is a data-link level protocol that allows network equipment to notify the neighbouring devices located in a local network on their capabilities and gather such notifications from the neighbouring devices.

STP (Spanning Tree Protocol) is a network protocol that allows to eliminate loops in the arbitrary Ethernet network topology, containing one or multiple network bridges connected with redundant links.

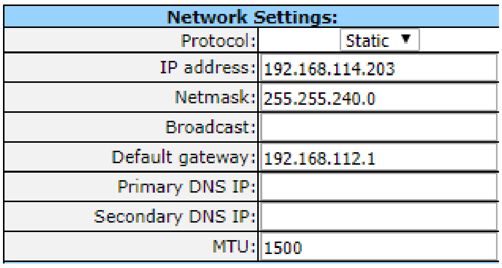
TR-069 is a technical specification that defines the Internet protocol for management of network equipment – CWMP (CPE WAN Management Protocol). The protocol allows for comprehensive device configuration, software updates, reading device information (software version, model, serial number, etc.), complete configuration file downloading/uploading, remote device restart (TR-069, TR-098, TR-104 specifications are supported).

STUN — network protocol that allows subscriber behind the NAT to define external IP-address.

You do not have to reboot the gateway in order to apply network settings. When applying settings, all current calls will be terminated.



When selecting 'Static' option in the 'Protocol' field, the following parameters are available:



<u>*Network settings:*</u>

– *Protocol* – selection of static or dynamic (DHCP) protocol to assign network settings.

<u>*Dynamic assignment of network settings:*</u>

To obtain network settings use DHCP.

Supported options:

1 – network mask;
3 – default network gateway address;
56 – DNS server address;
12 – device network name;
15–domain name;
28 – network broadcast address;
42 – NTP server address;
43 – specific vendor information (for option usage, see subsection *'TR-069 Monitoring and Management Protocol Settings'* below);
60 – specific vendor information (for option usage, see subsection *'DHCP Options'* below);
66 – TFTP server address (for option usage, see subsection *'Autoupdate Settings'* below);
67 – name of the file with firmware versions and configurations (for option usage, see subsection *'Autoupdate Settings'* below);
82 – agent informational parameter (Agent Circuit ID and Agent Remote ID suboptions);
120 – outbound SIP servers (for option usage, see Section 5.1.2.2.3SIP Custom Parameters (Profile n/SIP Custom));
121 – classless static routes (for option usage, see Section 5.1.1.4The 'Route' submenu).

- *Get GW via DHCP* – when checked, use default gateway obtained via DHCP;
- *Default gateway* – default address of a network gateway. I.e. the address of a gateway that receives all the traffic falling outside the scope of every static routing rule;
- *Primary DNS IP* – primary DNS server address. To use a local DNS, enter IP address 127.0.0.1 into the field;
- *Secondary DNS IP* – secondary DNS server address;
- *MTU* – maximum size of the packet that can be transmitted via WAN interface without fragmentation.

Static assignment of network settings:

- *IP address* – the device IP address;
- *Netmask* – the device network mask;
- *Broadcast* – the device subnet broadcast address;
- *Default gateway* – default address of a network gateway, i.e. the address of a gateway that receives all the traffic falling outside the scope of every static routing rule;
- *Primary DNS IP* – primary DNS server address. To use a local DNS, enter IP address 127.0.0.1 into the field;
- *Secondary DNS IP* – secondary DNS server address;
- *MTU* – maximum size of the packet that can be transmitted via WAN interface without fragmentation.

DHCP Options:

- *Alternative option 60 enable* – when checked, use alternative Option 60 value, specified by user. Otherwise, in Option 60 DHCP request the device will send specific vendor information in the following format:

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

where:

- Vendor – **Eltex**;
- Device type – depends on factory settings;
- Serial number – depends on factory settings;
- MAC address – depends on factory settings.

You may check factory settings and firmware version in 'System info' tab (Section 5.3.2 The 'System info' menu) of the web interface.

Example:

```
[VENDOR:Eltex][DEVICE:TAU72][HW:0x21][SN:MS5370043][WAN:00:01:09:44:33:22][VERSION:2.10.0]
```

- *Alternative option 60 value* – alternative Option 60 value (format: string), specified by user;

- *Option 82. Agent circuit identifier (Option 82. Agent Circuit ID* – allows to add Option 82, Suboption 1 – Agent Circuit ID, into DHCP request;

- *Option 82. Remote agent identifier (Option 82. Agent Remote ID* – allows to add Option 82, Suboption 2 – Agent Remote ID, into DHCP request.

<u>*Services:*</u>

- *Enable TELNET* – when checked, enable device access via Telnet protocol, otherwise it is disabled;

- *TELNET port* – TCP port (23 by default) for Telnet protocol operation;

- *Enable SSH* – when checked, enable device access via SSH protocol, otherwise it is disabled;

- *SSH port* – TCP port (22 by default) for SSH protocol operation;

To avoid unathorised access to the device by password iteration, IP address is blocked for 5 minutes in case of 3 times entering of invalid athorisation data. This feature is implemented for Telnet and SSH. Notification on the intrusion attempts is transferred to technical specialists via SYSLOG and/or SNMP.

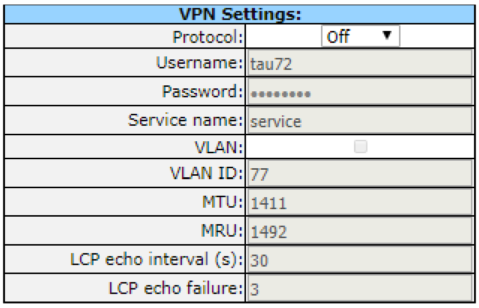
- *Enable STP* – when checked, STP is enabled;

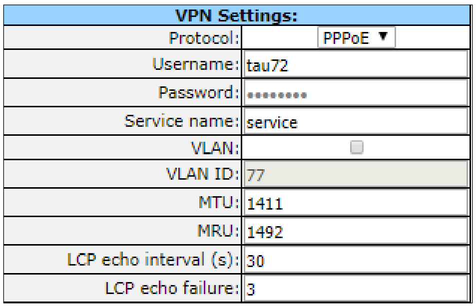
- *Enable WEB* – when checked, enable device access via web interface, otherwise it is disabled;

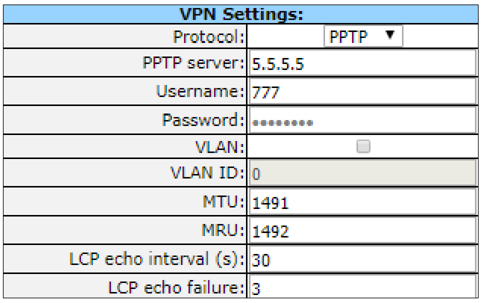
- *HTTP port* – web server port (80 by default) for HTTP protocol operation;

- *HTTPS port* – web server port (443 by default) for HTTPS protocol operation.

VPN Settings:







– *Protocol* – selection of protocol to create a VPN.

- *Off* – don't use VPN;
- *PPPoE* – use PPPoE for a tunnel creation;
- *PPTP* – use PPTP for a tunnel.

PPPoE Settings:

– *Username* – username for PPP server authentication;

– *Password* – password for PPP server authentication;

– *Service name* – service name requested when PPP connection establishing. Query must be replyed only by PPPoE server, that supports this service;

– *VLAN* – when checked, use separate VLAN for PPPoE access;

– *VLAN ID* – VLAN identifier*;*

– *MTU* – maximum packet size that could be transferred through PPP interface without fragmentation;

– *MRU* – maximum packet size that could be received through PPP interface without fragmentation;

– *LCP echo interval (s)* – period of request transmission for LCP echo PPP connection control;

– *LCP echo failure count* – permissible amount of errors connected with LCP echo requests transmission. In case this amount of LCP echo queries wasn't answered, PPP connection will be terminated.

If the network is managed through PPPoE, do not click the *Submit Changes* button after you finish PPPoE connection configuration as it may lead to connection loss. Go to *'VLAN conf'* tab first, set the setting for 'RTP/signalling/control traffic transmission via PPPoE', and then apply configuration changes using the *Submit Changes* button.

<u>*PPTP Settings:*</u>

- *PPTP server* – PPPT server IP address;
- *Username* – username for PPP server authentication;
- *Password* – password for PPP server authentication;
- *VLAN* – when checked, use separate VLAN for PPTP access;
- *VLAN ID* – VLAN identifier; *MTU* – maximum packet size that could be transferred through PPP interface without fragmentation;
- *MRU* – maximum packet size that could be received through PPP interface without fragmentation;
- *LCP echo interval (s)* – period of request transmission for LCP echo PPP connection control;
- *LCP echo failure count* – permissible number of errors connected with LCP echo requests transmission. In case this amount of LCP echo queries wasn't answered, PPP connection will be terminated.

If the network is managed through PPTP, do not click the *Submit Changes* button after you finish PPTP connection configuration as it may lead to connection loss. Go to *'VLAN conf'* tab first, set the setting for 'signalling/control traffic transmission via PPTP', and then apply configuration changes using the *Submit Changes* button.

<u>*LLDP Settings:*</u>

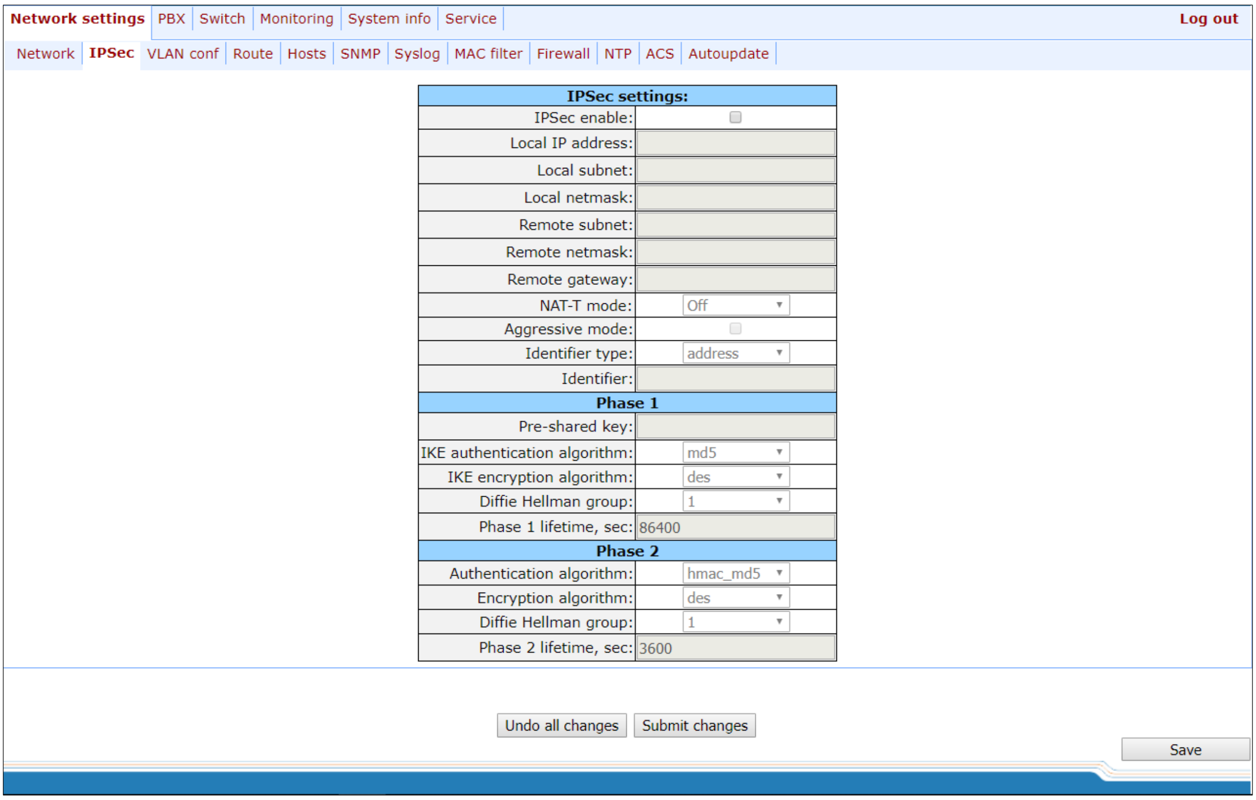
- *Enable LLDP* – when checked, enable LLDP protocol;
- *LLDP transmit period* – LLDP message transmission period. Default value: 30 seconds.

To apply changes, click the *Submit Changes* button. To discard all changes made to configuration, click the *Undo All Changes* button.

To store changes to non-volatile memory of the device, click the *Save* button.

5.1.1.2 The 'IPSec settings' submenu

In this submenu, you may configure IPSec encryption (IP Security). IPSec is a set of protocols to provide data protection (data is transmitted via IP). IPSec allows you to provide authentication, integrity check and/or IP-packets encryption. IPSec includes protocols for tamper-free key exchange in Internet.



<u>IPSec settings:</u>

- *IPSec enable* – when selected, permit to use IPSec protocol for data encryption;
- *Local IP address* – the device address for operation via IPSec protocol;
- *Local subnet* – local subnet address;
- *Local netmask* – local subnet mask;
- *Local subnet* in cooperation with *Local netmask* determine local subnet for creation of network-to-network or network-to-point topologies;
- *Remote subnet* – remote subnet address;
- *Remote netmask* – remote subnet mask;

  Remote subnet in cooperation with *Remote netmask* determine address of remote subnet for connection with using encryption via IPSec protocol. If mask has value 255.255.255.255 then connection is established with a single host. Mask that differs from 255.255.255.255 allows defining a whole subnet. Thus, functionality of the device allows you to organize the following 4 network topologies with using encryption traffic via IPSec protocol: point-to-point, network-to-point, point-to-network, network-to-network;

- *Remote gateway* – gateway used for remote network access.

- *NAT-T mode* – 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. You can choose one of the three 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-T settings become available when choosing NAT-T On/Force mode:

- *NAT-T UDP port* – UDP port for packets used for IPSec message encapsulation. Default value is 4500;
- *NAT-T keepalive packet transmission interval*, sec – periodic message transmission interval for UDP connection keepalive on the device performing NAT functions.

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

In ***Phase 1*** and ***Phase 2*** sections parameters and algorithms used in the first and the second steps of IPSec connection are configured.

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*;
- *Authentication algorithm* – select an authentication algorithm from the list: MD5, SHA1, SHA256, SHA384, SHA512;
- *Encryption algorithm* – select an encryption algorithm from the list: DES, 3DES, Blowfish, Cast128, AES;
- *Diffie Hellman group* – select Diffie-Hellman group;
- *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.

- *Authentication algorithm* – select an authentication algorithm from the list: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512;
- *Encryption algorithm* – select an encryption algorithm from the list: DES, 3DES, Blowfish, Twofish, Cast128, AES;
- *Diffie Hellman group* – select Diffie-Hellman group;

- *Phase 2 lifetime, sec* – time that should pass for data encryption key changeover (other name IPSec SA lifetime). Default value is 60 minutes (3600 seconds).

To apply changes, click the *Submit Changes* button. To discard all changes made to configuration, click the *Undo All Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

Settings for 'signalling/control traffic via IPSec' transmission are performed on the *'VLAN conf'* tab.

5.1.1.3 The 'VLAN conf' submenu. Virtual Local Area Network

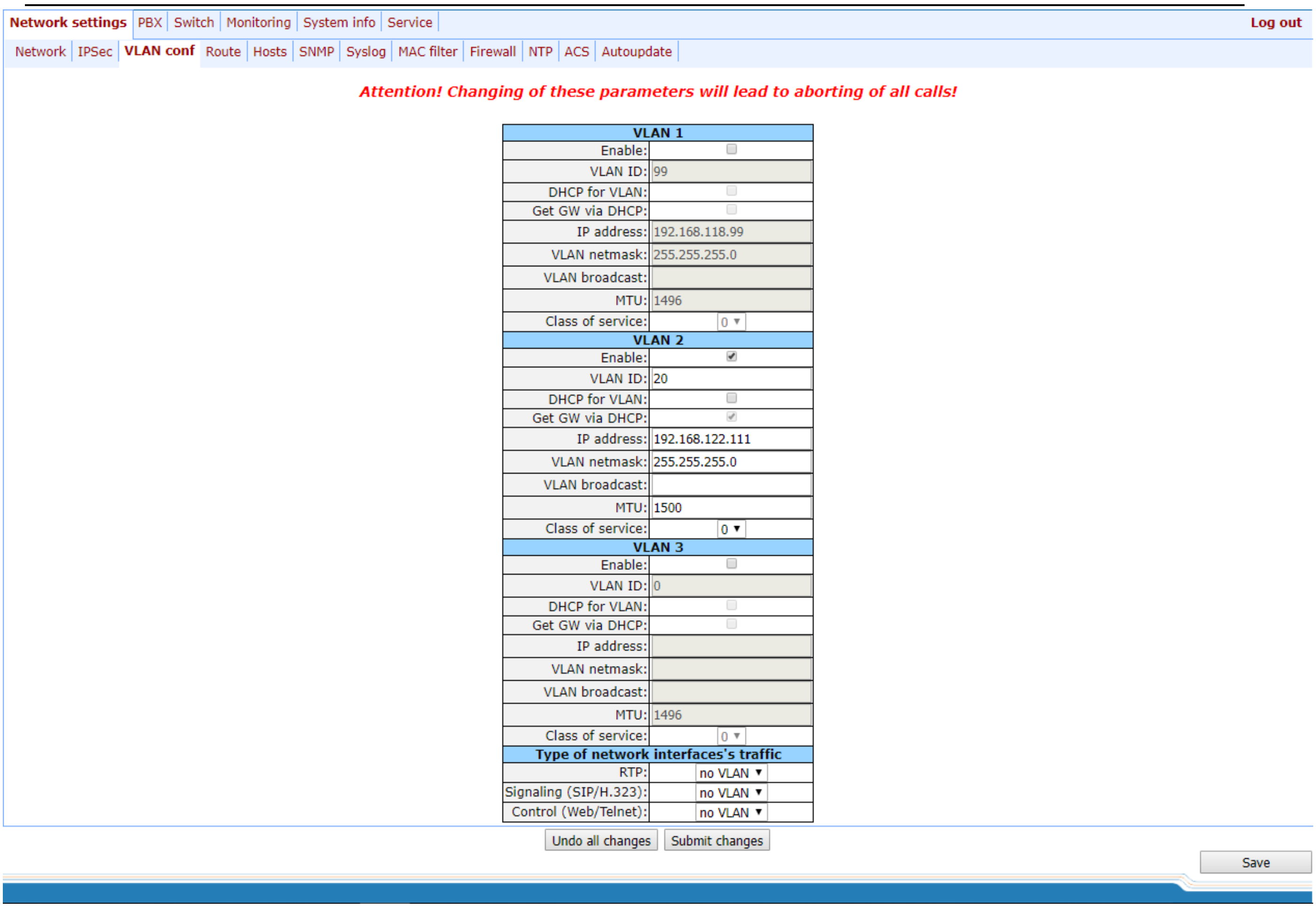
In *'VLAN conf'* submenu, you will be able to configure VLAN network settings and transmission of signals and voice traffic, and also set up device management through various VLAN networks.

You don't have to reboot the gateway in order to apply VLAN settings. When applying settings, all current calls will be terminated.

VLAN is a virtual local area network. VLAN consists 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.

Gateway software allows to set up device management (via web interface, TELNET, or SSH), transmission of signals (SIP, H.323/RAS protocol data) and voice traffic (RTP) through a single or multiple virtual local area networks. This feature may become useful, when a separate network is used for device management in organization.

IP addresses assigned to WAN interface as well as VLAN interfaces should belong to different subnets. For example, if you use a mask 255.255.240.0, IP addresses 192.168.1.6 and 192.168.2.199 will belong to a single network, and if you use a mask 255.255.255.0, they will belong to different networks.



In sections *VLAN1, VLAN2, VLAN3*, you may configure from one to three VLAN networks:

- *Enable* – when checked, enable VLAN;
- *VLAN ID* – VLAN identifier (1-4095);
- *DHCP for VLAN* – when checked, VLAN network settings will be obtained via DHCP;
- *Get GW via DHCP* – when checked, use default gateway obtained via DHCP;
- *IP address* – VLAN interface IP address;
- *VLAN netmask* – network mask used for VLAN interface;
- *VLAN broadcast* – subnet broadcast address of VLAN interface;
- *MTU* – maximum packet size that could be transferred through PPP interface without fragmentation (86-1500);
- *Class of service (802.1p)* – 802.1p priority for the current VLAN.

Traffic Type – VLAN Number

In section ***'Traffic Type – VLAN Number'***, you can assign one of three configured *VLANs* ***(VLAN1, VLAN2, VLAN3)*** or PPPoE interface to the specific traffic type:

– *RTP* – VLAN, PPPoE assignment for voice traffic;

– *Signaling (SIP/H.323)* – VLAN, PPPoE, PPTP, IPSec assignment for SIP/H323 signal traffic;

– *Control (WEB/Telnet)* – VLAN, PPPoE, PPTP, IPSec assignment for gateway management via web interface, telnet, and SSH.

Voice traffic will be transmitted via PPPoE only after the device is restarted.

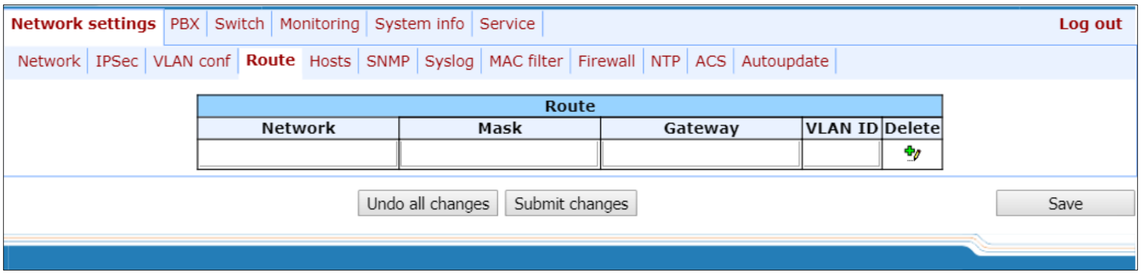
When selecting for all types: RTP, signalling and controlling PPPoE value won't have any IP address, even if IP address for WAN will be setted up in configuration.

To apply changes, click the *Submit Changes* button. To discard all changes made to configuration, click the *Undo All Changes* button.

5.1.1.4 The 'Route' submenu

In the *'Route' submenu'* you can configure static routes for WAN and VLAN interfaces.

Static routing allows you to route packets to defined IP networks or IP addresses through the specified gateways. Packets sent to IP addresses not belonging to the gateway IP network and falling outside the scope of static routing rules will be sent to the default gateway.



– *Network* – destination IP network or address;

– *Mask* – network mask. If IP address is specified in the 'Network' field, use the following mask: 255.255.255.255;

– *Gateway* – address of a network gateway that will be used for packet routing to the defined network (or IP address);

– *VLAN* – virtual local area network identifier (VLAN ID). Use it when destination IP network or IP address belong to virtual local area network, otherwise leave this field blank.

To add/apply a new route, enter the data in the field with icon, and click the *Submit Changes* button. To remove the route, select *'Delete'* checkbox and click the *Submit Changes* button.

To discard all changes made to configuration, click the *Undo All Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

Apart from configuration performed via web configurator, the gateway is able to receive static route settings via Option 121 of DHCP protocol. Routes in this option are sent as a list of 'destination description/gateway' pairs, the format is described in RFC 3442.

5.1.1.5 The 'Hosts' submenu

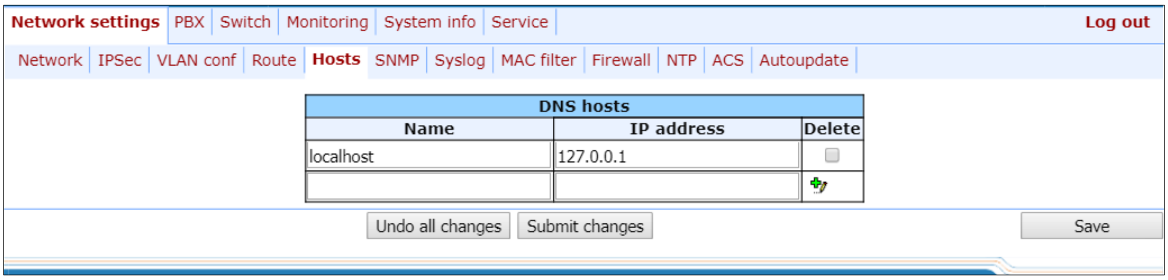
In the *'Hosts'* submenu, you can configure settings required for local DNS operation.

To enable local DNS, enter 127.0.0.1 into *'DNS'* field in the *'Network'* tab.

Local DNS — allows the gateway to obtain IP address of the communicating device by its domain name. 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 host names (domains) and their IP addresses. Also, local DNS allows you to configure SIP domain on a gateway (see Section 5.1.2.2.3 SIP Custom Parameters (Profile n/SIP Custom)).

Local DNS configuration involves definition of matches between hostnames and their respective IP addresses.

To enable local DNS, enter 127.0.0.1 into *'Primary DNS IP'* field in the *'Network'* tab. Also, local DNS will be used when configured DNS servers are not available.



<u>*Table of domain names (DNS hosts):*</u>

- *Name* – name of a host;
- *IP-address* – IP address of a host.

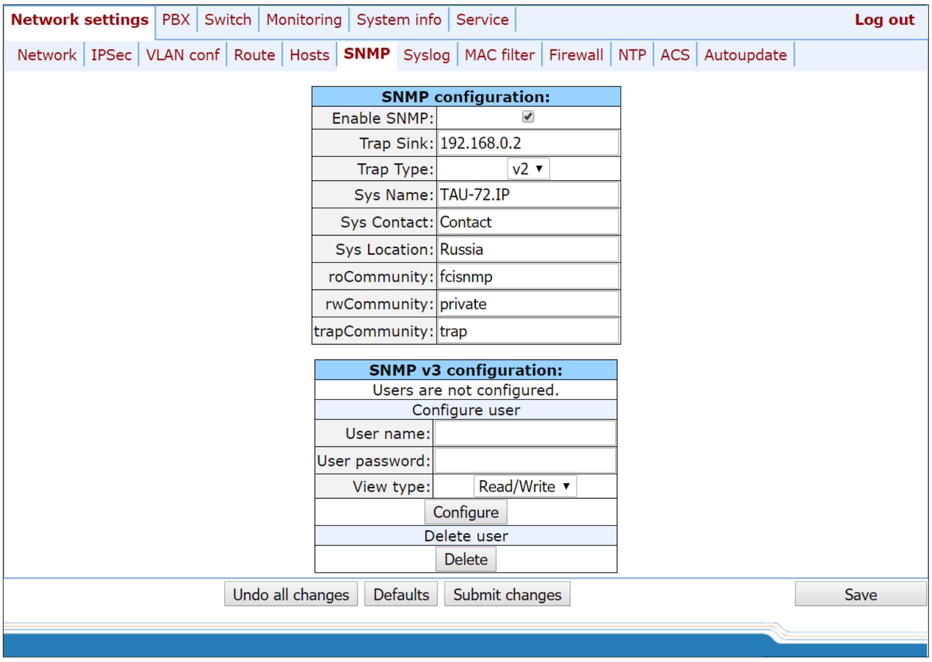
To add/apply a new route, enter the data in the field with icon, and click the *Submit Changes* button. To remove the route, select *'Delete'* checkbox and click the *Submit Changes* button.

After implementation of changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

5.1.1.6 The 'SNMP' submenu

TAU-72.IP/TAU-36.IP software allows to monitor status of the device and its sensors and also configuring certain parameters of the device via SNMP protocol. In *'SNMP'* submenu, you can configure settings of SNMP agent. Device supports SNMPv1, SNMPv2c, SNMPv3 protocol versions.

For detailed monitoring parameters and Traps description, see MIBs on disk shipped with the gateway.



After implementation of changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

<u>*SNMP configuration:*</u>

– *Trap Sink* – IP address of a trap recipient (manager server or proxy agent server);
– *Trap Type* – SNMP trap type (SNMP-trap or SNMPv2-trap);
– *SysName* – device system name;
– *SysContact* – device vendor contact information;
– *SysLocation* – device location;
– *roCommunity* – password for parameter reading (common: *public*);
– *rwCommunity* – password for parameter writing (common: *private*);
– *trapCommunity* – password located in traps.

<u>*SNMP v3 configuration:*</u>

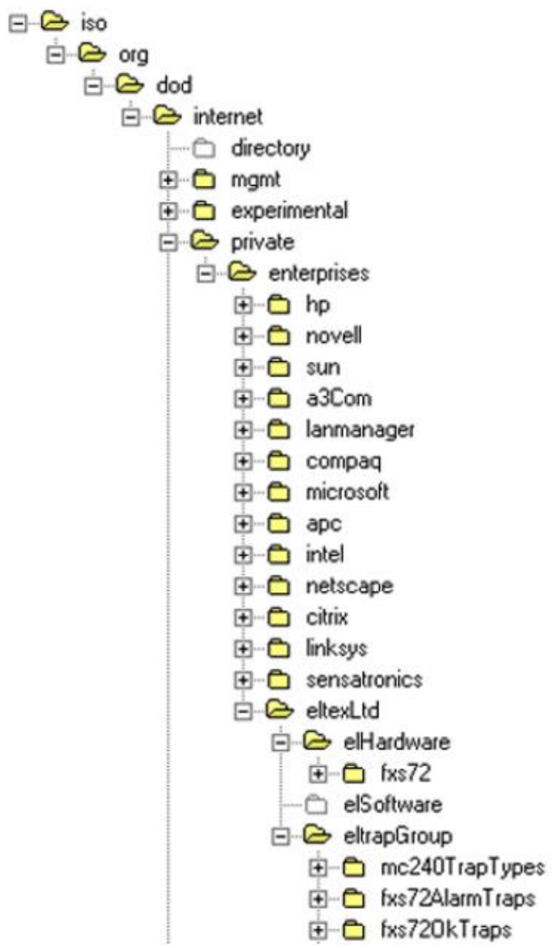
The system employs a single SNMPv3 user that executes SORM commands. SORM feature implementation is based on rfc3924 recommendation–Cisco Architecture for Lawful Intercept in IP Networks. To perform the pickup, the following MIBs are used: CISCO-IP-TAP-MIB.my and CISCO-TAP2-MIB.my.

– *User name* – account username;
– *User password* – access password. The password should contain 8 characters or more;
– *View type* – account access mode selection:
  - *Read/Write* – read/write mode;
  - *Read only* – read-only mode;
– *Delete* – click this button to delete all accounts for access via SNMP v3.

Click the *Configure* button to apply SNMPv3 user configuration. Settings will be applied immediately. Click the *Delete* button to delete the record.

To discard all changes made to configuration, click the *Undo All Changes* button. To set the default parameters, click the *Defaults* button. To apply changes, click the *Submit Changes* button.

<u>MIB Tree</u>



SNMP TRAP

SNMP agent sends a message (SNMP-trap or SNMPv2-trap), when the following events occur:

- Port is blocked;
- Port is unblocked;
- Unit power supply voltage is changed;
- Fans turned on/off;
- Fans malfunction;
- SFP module is installed, but there is no optical link;
- BPU connection lost/resumed;
- One of the following parameters falls outside of allowable limits:

  - For TAU-36.IP/TAU-72.IP rev.1.0-4.0:

    - Primary supply voltage should fall within the limits: 38V<Vbat<72V;
    - Ringer supply voltage should fall within the limits: 100V<Vring1<120V and 100V<Vring2<120V;
    - Temperature on a sensor should not exceed 90°c.

  - For TAU-36.IP/TAU-72.IP rev.B/rev.D:

    - Board supply voltage should fall within the limits: 8V<Vbat<16V;
    - temperature on a sensor should not exceed 90°c.

- Successful/unsuccessful firmware update;
- Successful/unsuccessful configuration download/upload.

5.1.1.6.1 The 'SNMP' submenu

The gateway supports monitoring of the following parameters via SNMP:

- ***Standardized Parameters***

Object identifier *mgmt.1.*

system	Table with network parameters, according to RFC 1213 (MIB-II)
interfaces	Table with network interfaces parameters, according to RFC 1213 (MIB-II)

Object identifier *mib-2.47.1.*

entityPhysical	Table with description of the physical nature of the device, according to RFC 6933 (Entity MIB)
entityMapping	Table with network interfaces correspondence, according to RFC 6933 (Entity MIB)

- ***General Gateway Data***

Object identifier *enterprises.35265.1.9.*

1	fxsDevName	Gateway name
2	fxsDevType	Gateway type

3	fxsDevCfgBuild	Firmware version
4	fxsFreeSpace	Free disk space
5	fxsFreeSpace	Free RAM
8	fxsCpuUsage	CPU utilization (%)

Object identifier *enterprises.35265.4.*

2	omsProductClass	Hardware platform version
3	omsSerialNumber	Device serial number (factory setting)
11	omsLinuxVersion	Linux version
12	omsFirmwareVersion	Media processor version
13	omsBPUVersion	Subscriber unit firmware version
14	omsFactoryType	Device type (factory setting)
15	omsFactoryMAC	Factory default MAC address

– ***Platform Sensor Parameters***

Object identifier *enterprises.35265.1.9.10*.

5	fxsMonitoringTemp1	Temperature measured by submodule 1 sensor
6	fxsMonitoringTemp2	Temperature measured by submodule 2 sensor
7	fxsMonitoringTemp3	Temperature measured by submodule 3 sensor
8	fxsMonitoringTemp4	Temperature measured by submodule 4 sensor
9	fxsMonitoringFanState	Fan status (on or off)
10	fxsMonitoringFan1Rotate	Fan health 1, if it's on
11	fxsMonitoringFan2Rotate	Fan health 2, if it's on
13	fxsMonitoringVinput	Board supply voltage,V
14	fxsMonitoringDevicePower	Type of power supply installed
15	fxsMonitoringPowerUnitTermo	Temperature measured by PS sensor[1]
16	fxsMonitoringFanRpm1	Fan 1 rotating speed[1]
17	fxsMonitoringFanRpm2	Fan 2 rotating speed1

List of the possible modes of supply of subscriber sets:

– *high* – 60 V;
– *normal* – 48 V;
– *low* – voltage less than 48 V.

[1] Used with TAU-36/72.IP rev.B/rev.D only.

– ***Call Monitoring***

Object identifier *enterprises.35265.1.9.12.1.1.*

2	fxsPortPhoneNumber	Subscriber number
3	fxsPortState	Port status
4	fxsPortUserName	Subscriber name
5	fxsPortTalkingNum	Number(s) of the remote subscriber or two subscribers in conference mode
6	fxsPortTalkingStartTime	Call start time
7	fxsPortSipConnected	Last known successful registration on SIP server
8	fxsPortH323Connected	Gatekeeper registration time
9	fxsPortSipConnecteNext	Amount of time until next SIP server registration
10	fxsPortSipConnecteState	SIP server registration status
11	fxsPortSipConnectHost	Registration SIP server address

List of possible port states:

– *hangdown* – phone is offhook;
– *hangup* – phone is onhook;
– *dial* – dialling number;
– *ringback* – send 'ringback' tone;
– *ringing* – send 'ringing' tone;
– *talking* – call in progress;
– *conference* – 3-way conference;
– *busy* – sending 'busy' tone;
– *hold* – port is on hold;
– *testing* – port is in testing mode.

List of possible registration states:

– *off* – registration disabled;
– *ok* – successful registration;
– *failed* – registration failed;

– ***Call group monitoring***

Object identifier *enterprises.35265.1.9.41.1.*

2	serialGroupPhone	Group sequential number
3	serialGroupRegistrationState	SIP server registration status
4	serialGroupRegistrationHost	Registration SIP server address
5	serialGroupLastRegistrationAt	Last known successful registration on SIP server
6	serialGroupNextRegistrationAfter	Remaining time for SIP server registration renewal
7	serialGroupH323GK	H.323 gatekeeper registration time

5.1.1.6.2 Device Configuration via SNMP

The gateway supports data readout and configuration via SNMP for the following settings:

– ***Custom Port Settings***

Object identifier *enterprises.35265.1.9.12.2.1.*

34	fxsPortConfigRowStatus	Row status (required in SNMP SET). Value for storing data in a file: 1
From the 'Custom' tab		
1	fxsPortConfigPhone	Phone (up to 20 characters)
2	fxsPortConfigUserName	User Name (up to 20 characters)
30	fxsPortConfigUseAltNumber	Use Alt. Number
29	fxsPortConfigAltNumber	Alt. Number (up to 20 characters)
83	fxsPortConfigUseAltNumberAsContact	Use alternative number as contact (only for serial groups members)
3	fxsPortConfigAuthName	Authentication name (up to 20 characters)
4	fxsPortConfigAuthPass	Authentication password (up to 20 characters)
5	fxsPortConfigCustom	Customizing
66	fxsPortConfigPortProfileID	Subscriber profile
67	fxsPortConfigSipProfileID	SIP/H.323 profile
18	fxsPortConfigHotLine	Hot Line
20	fxsPortConfigHotTimeout	Hot Timeout (0 to 300)
19	fxsPortConfigHotNumber	Hot Number (up to 20 characters)
27	fxsPortConfigClir	CLIR
48	fxsPortConfigDnd	Do Not Disturb (DND)
21	fxsPortConfigDisabled	Disabled
32	fxsPortConfigSipPort	SIP port (0 to 65535)
16	fxsPortConfigCallTransfer	Process flash
17	fxsPortConfigCallWaiting	Call Waiting
85	fxsPortConfigMwiDialtone	MWI
87	fxsPortConfigDscpForRtp	DSCP for RTP packets
From the 'Common' tab		
7	fxsPortConfigAON	CallerID
8	fxsPortConfigAONHideDate	Hide Date
9	fxsPortConfigAONHideName	Hide Name
11	fxsPortConfigMinFlashtime	Min Flashtime (ms) (70 to 1000)
12	fxsPortConfigMaxFlashtime	Max Flashtime (ms) (minflashtime to 1000)
13	fxsPortConfigGainr	Gain receive (-230 to 20)
14	fxsPortConfigGaint	Gain transmit (-170 to 60)
15	fxsPortConfigCategory	SS7 category (SIP-T)

76	fxsPortConfigCpcRus	Category
84	fxsPortConfigModifier	Modifier
33	fxsPortConfigCfgPriOverCw	Call Forward on Busy (CFB) has priority over Call Waiting (CW)
6	fxsPortConfigPlaymoh	Play music on hold
28	fxsPortConfigStopDial	Stop dial at #
10	fxsPortConfigTaxophone	Taxophone – operation in payphone mode
58	fxsPortConfigEnableCpc	CPC
59	fxsPortConfigCpcTime	CPC time (ms)
From the 'Call forward' tab		
22	fxsPortConfigCtBusy	Call Forward on Busy (CF Busy)
45	fxsPortConfigCfbNumber	CF Busy Number (up to 20 characters)
24	fxsPortConfigCtNoanswer	Call Forward on No reply (CF No reply)
46	fxsPortConfigCfnrNumber	CF No reply Number (up to 20 characters)
23	fxsPortConfigCtUnconditional	Unconditional Call Froward (CF Unconditional)
44	fxsPortConfigCfuNumber	CF Unconditional Number (up to 20 characters)
43	fxsPortConfigCtOutofservice	Call Forward on Out Of Service (CF Out Of Service)
47	fxsPortConfigCfoosNumber	CF Out Of Service Number (up to 20 characters)
25	fxsPortConfigCtNumber	Call Forward Number (CF Number)
26	fxsPortConfigCtTimeout	CF No reply (CFNR) Timeout (0 to 300)
From the 'Suppl. Service' tab		
36	fxsPortConfigDvoCtAttendedEn	Call answer attended enable
37	fxsPortConfigDvoCtUnattendedEn	Call answer unattended enable
38	fxsPortConfigDvoUnconditionalEn	Call forward unconditional enable
39	fxsPortConfigDvoCfBusyEn	Call forward on busy enable
40	fxsPortConfigDvoCfAnswerEn	Call forward on no reply enable
41	fxsPortConfigDvoCfServiceEn	Call forward on out of service enable
35	fxsPortConfigDvoCwEn	Call waiting enable
42	fxsPortConfigDvoDoDisturbEn	Do not disturb enable
From the 'Pick up groups' tab		
31	fxsPortConfigPickUp	Membership in PickUp groups (up to 86 characters)

These settings match ones described in Section 5.1.2.4.

– ***Subscriber profiles settings***

Object identifier *enterprises.35265.1.9.30.3.1.1.*

2	profilePortsAON	CallerID
3	profilePortsAONHideDate	Hide Date
4	profilePortsAONHideName	Hide Name

6	profilePortsMinFlashtime	Min Flashtime (ms) (70 to 1000)
7	profilePortsMaxFlashtime	Max Flashtime (ms) (minflashtime to 1000)
8	profilePortsGainr	Gain receive (0.1 dB)
9	profilePortsGaint	Gain transmit (0.1 dB)
10	profilePortsCategory	SS7 category (SIP-T)
35	profilePortsCpcRus	Category
43	profilePortsModifier	Modifier
13	profilePortsCfgPriOverCw	Call Forward on Busy (CFB) has priority over Call Waiting (CW)
1	profilePortsPlaymoh	Play music on hold
41	profilePortsStopDial	Stop dial at #
5	profilePortsTaxophone	Taxophone – operation in payphone mode
20	profilePortsEnableCpc	CPC
21	profilePortsCpcTime	CPC time (ms)
45	profilePortsDscpForRtp	DSCP for RTP packets
27	profilePortsRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, set '1' as value.

These settings match ones described in Section 5.1.2.4.

– ***Configuration of common SIP parameters***

Object identifier *enterprises.35265.1.9.30.1.1.*

1	sipCommonEnablesip	Enable SIP
6	sipCommonInviteInitT	Invite initial timeout (ms) (100 too 1000)
5	sipCommonInviteTotalT	Invite total timeout (ms) (1000 too 39000)
2	sipCommonShortmode	Short mode
3	sipCommonTransport	Transport
4	sipCommonSipMtu	SIP UDP MTU
7	sipCommonPortRegistrationDelay	Port registration delay (ms)
8	STUNEnable	Use STUN
9	stunServer	STUN server
10	stunInterval	STUN interval
11	sipPublicIp	PublicIP (address behind NAT)

These settings match ones described in Section 5.1.2.2.1.

– ***Common parameters configuration***

Object identifier *enterprises.35265.1.9.37.*

3	deviceName	Device name
8	siptUsePrefix	Use prefix (SIP-T)
9	siptPrefix	Prefix (SIP-T)
4	startTimer	Start timer
5	durationTimer	Duration timer
6	waitAnswerTimer	Wait answer timer
2	fansThresholdTemperature	Fans threshold temperature
1	fansForceEnable	Fans force enable

– ***Configuration of TCP/UDP port parameters***

Object identifier *enterprises.35265.1.9.45.*

1	rtpSipMin	Minimal UDP port (when operating via SIP)
2	rtpSipMax	Maximum UDP port (when operating via SIP)
3	interceptPortMin	COPM intercept UDP port min
4	interceptPortMax	COPM intercept UDP port max
8	dscpForSip	DSCP for SIP packets
7	verifyRemoteMediaAddress	Remote media address verification

– ***Call limits configuration***

Object identifier *enterprises.35265.1.9.46.1.*

2	clType	Type of interaction gateway
3	clHostOfNeighbourGateway	Host of neighbour gateway area
4	clSimultaneousCallsCount	Simultaneous calls count
5	clRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, its value should be as follows: to change the limit record, set value 1, to add a record–value 4, to remove a record–value 2.

– ***'Distinctive ring' service configuration***

Object identifier *enterprises.35265.1.9.47.1.*

2	drRule	Rule name
3	drRing	Ring, ms
4	drPause	Pause, ms
5	drSubscriberProfiles	Subscriber profiles
6	drRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, its value should be as follows: to change the limit record, set value 1, to add a record–value 4, to remove a record–value 2.

– ***Autoupdate configuration***

Object identifier *enterprises.35265.1.9.35.1*

1	fxsEnableAutoupdate	Enable autoupdate
2	fxsSource	Source
8	autoupdateProtocol	Autoupdate protocol
9	autoupdateAuth	Autoupdate authentication
10	autoupdateUser	Username
11	autoupdatePassword	Password
3	fxsTFTPServer	Autoupdate server
4	fxsConfigurationFile	Configuration file
5	fxsFirmwareVersion	Firmware versions file
6	fxsConfigurationUpdateInterval	Configuration update interval

– ***System log configuration***

Object identifier *enterprises.35265.1.9.38.*

1	runSyslog	Run syslog on startup
14	syslogToFile	Save log to file
2	syslogAddr	Syslog server address
3	syslogPort	Syslog server port
4	appErr	Errors
5	appWarn	Warnings
6	appInfo	Info
7	appDbg	Debug
13	appAlarm	Alarms
8	sipLevel	SIP debug level
9	h323Level	H.323 debug level
10	vapiEnabled	VAPI log enable
11	vapiLibLevel	Library debug level
12	vapiAppLevel	Application debug level
15	syslogStatus	Syslog status (on/off)

These settings match ones described in Section 5.1.1.7

– ***Specific SIP parameters' configuration***

Object identifier *enterprises.35265.1.9.30.1.3.1.*

3	sipProfileMode	Proxy mode
15	sipProfileProxy0	Proxy 1 address (up to 40 characters)
16	sipProfileRegrar0	Registrator 1 address (up to 40 characters)
17	sipProfileRegistration0	Use registration 1
18	sipProfileProxy1	Proxy 2 address (up to 40 characters
19	sipProfileRegrar1	Registrator 2 address (up to 40 characters)
40	sipProfileRegistration1	Use registration 2
20	sipProfileProxy2	Proxy 3 address (up to 40 characters
21	sipProfileRegrar2	Registrator 3 address (up to 40 characters)
41	sipProfileRegistration2	Use registration 3
22	sipProfileProxy3	Proxy 4 address (up to 40 characters
23	sipProfileRegrar3	Registrator 4 address (up to 40 characters)
42	sipProfileRegistration3	Use registration 4
24	sipProfileProxy4	Proxy 5 address (up to 40 characters
25	sipProfileRegrar4	Registrator 5 address (up to 40 characters)
43	sipProfileRegistration4	Use registration 5
4	sipProfileOptions	Main proxy control mode
62	sipProfileChangeover	Redundancy switching mode
63	sipProfileChangeoverBy408	Switching by timeout
5	sipProfileKeepalivet	Keepalive time (s)
61	sipProfileFullRuriCompliance	Full RURI analyse
7	sipProfileDomain	SIP domain (up to 20 characters)
6	sipProfileDomainToReg	Use SIP domain when registrating
8	sipProfileRegisterRetryInterval	Registration Retry Interval (s) (10 to 3600)
10	sipProfileInboundProxy	Inbound
9	sipProfileOutbound	Outbound
2	sipProfileObtimeout	Dial timeout (0 to 300)
11	sipProfileExpires	Expires (10 to 345600)
12	sipProfileAuthentication	Authentication and authorisation mode
13	sipProfileUsername	Username (up to 20 characters)
14	sipProfilePassword	Password (up to 20 characters)
60	sipProfileUseAlertInfo	Alert info
39	sipProfileRingback	Ringback when receiving 183 response
37	sipProfileCwRingback	Response type with CallWaiting
38	sipProfileRingbackSdp	Ringback raising to a caller

26	sipProfileDtmfmime	DTMF MIME Type
27	sipProfileHfmime	DTMF MIME Type
34	sipProfileUriEscapeHash	Forward '#' as '%23'
33	sipProfileUserPhone	Use tag User=Phone
49	sipProfileRemoveInactiveMedia	Remove inactive media
44	sipProfilePRTPstat	P-RTP-Stat
28	sipProfileCtWithReplaces	Use replaces
32	sipProfile100Rel	Reliable preliminary 100rel response delivery
46	sipProfileEnableTimer	Use RFC4028 timer
47	sipProfileMinSE	Min SE
48	sipProfileSessionExpires	Session expires
	NAT settings	
51	sipProfileKeepAliveMode	NAT Keep Alive Msg
50	sipProfileKeepAliveInterval	NAT Keep Alive Interval (s)
	Conference settings	
52	sipProfileConferenceMode	Conference mode
53	sipProfileConferenceServer	Conference server
	IMS settings	
54	sipProfileEnableIMS	Enable IMS
55	sipProfileXCAPNameForThreePartyConference	XCAP name for '3-way conference'
56	sipProfileXCAPNameForHotline	XCAP name for 'Hotline'
57	sipProfileXCAPNameForCallWaiting	XCAP name for 'Call waiting'

These settings match ones described in Section 5.1.2.2.3.

– ***Configuration of the distinctive type ring with alert info header***

Object identifier *enterprises.35265.1.9.30.1.5.1.*

1	cadenceNumber	Rule number
2	cadenceName	Alert Info string
3	cadenceRingRule	Expressions
4	cadenceRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, its value should be as follows: to change the limit record, set value 1, to add a record–value 4, to remove a record–value 2.

– ***Codecs configuration***

Object identifier *enterprises.35265.1.9.30.7.1.1.*

1	useG711A	Use G.711A
2	useG711U	Use G.711U
3	useG726to32	Use G.726-32
4	useG723	Use G.723
6	useG729B	Use G.729B
7	useG729A	Use G.729B
	Packetization time	
8	g711Ptime	G.711 Ptime
9	g729Ptime	G.729 Ptime
10	g723Ptime	G.723 Ptime
11	g726to32Ptime	G.726-32 Ptime
	Other settings	
12	g726to32PT	payload type for G.726-32 codec
13	dtmfTransfer	DTMF Transfer Type
14	flashTransfer	Flash Transfer Type
15	faxDetectDirection	Fax Detection
16	faxTransferCodec	Master Fax Transfer Codec
17	slaveFaxTransferCodec	Slave Fax Transfer Codec
18	modemTransfer	Modem Transfer
19	rfc2833PT	RFC2833 Payload Time
20	silenceSuppression	Silence suppression
21	echoCanceller	Echo canceller
22	nlpDisable	NLP disable
23	comfortNoise	Comfort noise
	RTCP configuration	
24	rtcpTimer	RTCP rimer
25	rtcpControlPeriod	RTCP activity control period
36	rtcpXR	RTCP-XR
	Fax/Modem configuration	
26	ciscoNsePT	NSE Payload Type
27	t38MaxDatagramSize	Max Datagram Size
28	t38Bitrate	Bitrate
	Jitter buffer configuration	
29	modemFaxDelay	Delay (modem/fax)
30	voiceMode	Mode

31	voiceDelayMin	Delay min
32	voiceDelayMax	Delay max
33	voiceDeletionThreshold	Deletion Threshold
34	voiceDeletionMode	Deletion mode
35	profilesCodecsRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, set '1' as value.
37	rfc3264PtCommon	Decoding rfc2833 with PT from answer SDP

These settings match ones described in Section 5.1.2.2.5.

– ***Configuration of a routing plan based on regular expressions***

Object identifier *enterprises.35265.1.9.30.5.3.1.*

1	profileRegExpDialOn	Regular expression dialplan
2	profileRegExpDialProtocol	Protocol
3	profileRegExpDialText	Expressions
4	profileRegExpDialRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, set '1' as value.

These settings match ones described in Section 5.1.2.2.5.4.

– ***Call group configuration***

Object identifier enterprises.35265.1.9.18.1.1.

Data readout performed for *enterprises.35265.1.9.18.fxsSerialGroupsNext* identifier allows you to get the number of the next free group. You can configure up to 8 groups in total.

1	fxsSerialGroupsPhone	Phone (up to 20 characters)
2	fxsSerialGroupsEnabled	Enabled
3	fxsSerialGroupsSerialType	Type
4	fxsSerialGroupsBusyType	Busy mode
5	fxsSerialGroupsTimeout	Timeout (o to 99)
6	fxsSerialGroupsSipPort	SIP port (0 to 65535)
7	fxsSerialGroupsAuthName	Group name (up to 20 characters)
8	fxsSerialGroupsAuthPass	Password (up to 20 characters)
9	fxsSerialGroupsPorts	Ports (up to 48 characters)
10	fxsSerialGroupsSipProfile	SIP/H.323 profile
11	fxsSerialGroupsRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, its value should be as follows: to change the serial group record, set value 1, to add a record–value 4, to remove a record–value 2.

These settings match ones described in Section 5.1.2.7.

– ***SNMP parameters configuration***

Object identifier *enterprises.35265.1.9.31.*

1	tauTrapSink	Trap Sink
2	tauTrapType	Trap Type
3	tauSysName	System Name
4	tauSysContact	System Contact
5	tauSysLocation	System Location
6	tauRoCommunity	roCommunity
7	tauRwCommunity	rwCommunity
8	tauTrapCommunity	trapCommunity
9	tauUserV3Name	Username
10	tauUserV3Password	User password
11	tauViewV3Type	View type
12	tauRestartSnmp	Allows to restart SNMP client

These settings match ones described in Section 5.1.1.6.

– ***Configuration of supplementary service codes***

Object identifier *enterprises.35265.1.9.20.*

2	tauVoipDvoCtAttended	Call transfer attended
3	tauVoipDvoCtUnattended	Call forward unattended
4	tauVoipDvoCfUnconditional	Unconditional Call Froward (CF Unconditional)
5	tauVoipDvoCfBusy	Call Forward on Busy (CF Busy)
6	tauVoipDvoCfNoanswer	Call Forward on No reply (CF No reply)
7	tauVoipDvoCfService	Call Forward on Out Of Service (CF Out Of Service)
1	tauVoipDvoCallwaiting	Call Waiting
8	tauVoipDvoDoDisturb	Do Not Disturb (DND)

These settings match ones described in Section 5.1.2.6

– ***Firewall settings configuration***

Object identifier *enterprises.35265.1.9.44.1.1*

2	startingSourceIpAddress	Starting source IP address
16	SourceMask	Network Mask
4	allSourceIpAddresses	All source IP addresses
5	ruleprotocol	Protocol
6	typeOfMessageICMP	Type of message (ICMP)
7	startingSourcePort	Starting source port
8	numberOfSourcePorts	Number of source ports
9	allSourcePorts	All source ports
10	startingDestinationPort	Starting destination port
11	numberOfDestinationPorts	Number of destination ports
12	allDestinationPorts	All destination ports
13	ruleTarget	Target
14	ruleMoveTo	Moves the rule in the table; specify a row to move the rule into (1 to 30).
15	ruleRowStatus	Row status. This parameter is mandatory for SNMP SET. To store data in a file, its value should be as follows: to change the rule, set value 1, to add a rule–value 4, to remove a rule–value 2.

Object identifier enterprises.35265.1.9.44.

2	firewallApply	Apply rules
3	firewallConfirm	Confirm applied rules

These settings match ones described in Section 5.1.2.6.

– ***Sevice functions***

Object identifier *enterprises.35265.1.9.*

15	fxsConfigSave	Save configuration into non-volatile memory
19	fxsReboot	Reboot gateway

5.1.1.6.3 Device Firmware Update

To do this, send 'set' request to OID 1.3.6.1.4.1.35265.1.9.25.0

Parameter type: s - string

Parameter format: ‘ <Firmware file name> <TFTP server IP address>’

Example: snmpset –v 2c –c private 192.168.16.70 .1.3.6.1.4.1.35265.1.9.25.0 s 'firmware.img72 192.168.16.44'

SNMP trap message will be sent to notify you on success or failure of firmware update operation.

5.1.1.6.4 Device configuration download/upload

Device configuration upload

To do this, send 'set' request to OID .1.3.6.1.4.1.35265.4.10.2.0

Parameter type: s - string

Parameter format: ‘<TFTP server IP address> <Configuration file name> upload’

or: ‘<HTTP server IP address> <Configuration file name> httpupload’

Example: snmpset –v 2c –c private 192.168.16.70 .1.3.6.1.4.1.35265.4.10.2.0 s ‘192.168.16.44 cfgTau72.crypt upload’

Device configuration download

To do this, send 'set' request to OID .1.3.6.1.4.1.35265.4.10.2.0

Parameter type: s - string

Parameter format: ‘<TFTP server IP address> <Configuration file name> download’

or: ‘<HTTP server IP address> <Configuration file name> httpdownload’

Example: snmpset –v 2c –c private 192.168.16.70 .1.3.6.1.4.1.35265.4.10.2.0 s ‘192.168.16.44 cfgTau72.crypt download’

Apply loaded changes

To do this, send 'set' request to OID .1.3.6.1.4.1.35265.4.10.2.0

Parameter type: s - string

Parameter format: '<TFTP server IP address> <Configuration file name> apply'

Example: snmpset –v 2c –c private 192.168.16.70 .1.3.6.1.4.1.35265.4.10.2.0 s ‘192.168.16.44 cfgTau72.crypt apply’

5.1.1.6.1 Events description sent in the TRAP, TRAP V2, INFORM messages

Table 7 — Description of events transmitted in Trap, Trap2, Inform messages

Event	Importance	Description	OID	Note
fxs72VbatAlarmTrap	MAJOR	The voltage Vbat =%1$d in beyond the permissible limits (38-72V)	1.3.6.1.4.1.35265.3.6.1	Parameter 1: voltage
fxs72VringAlarmTrap	MAJOR	The voltage Vring %2$d=%1$d beyond the permissible limits (100-120V)	1.3.6.1.4.1.35265.3.6.2	Parameter 1: voltage Parameter 2: the number of the inductor (1 or 2)
fxs72VInputAlarmTrap	MAJOR	Input voltage exceeds acceptable values (8-16 V)	1.3.6.1.4.1.35265.3.6.7	Parameter 1: input voltage value
fxs72TemperatureAlarmTrap	MAJOR	The temperature of sensor %2$d=%1$d	1.3.6.1.4.1.35265.3.6.3	Parameter 1: The temperature

		greater than the maximum value (90°C)		Parameter 2: The number of the temperature sensor (1-4)
fxs72TempmeasurementAlarmTrap	MAJOR	Temperature sensor's measurements are invalid	1.3.6.1.4.1.35265.3.6.13	
fxs72PowerUnitTermAlarm[1]	MAJOR	Temperature of power supply exceeds acceptable value (95 °C)	1.3.6.1.4.1.35265.3.6.21	
fxs72FanAlarmTrap	MAJOR	Fan %1$d is on, but does not rotate	1.3.6.1.4.1.35265.3.6.4	Parameter 1: The number of fan
fxs72FanLowSpeedAlarmTrap[1]	MAJOR	Rotation speed is less than 1000 cycles per minute	1.3.6.1.4.1.35265.3.6.22	
fxs72SSwAlarmTrap	MAJOR	No registration on MGC/SSW	1.3.6.1.4.1.35265.3.6.5	It is used for software version - Megaco
fxs72PortAlarmTrap	MINOR	Port %1$d is locked	1.3.6.1.4.1.35265.3.6.6	Parameter 1: The port number
fxs72VbatOkTrap	CLEAR	The voltage Vbat is OK	1.3.6.1.4.1.35265.3.7.1	
fxs72VringOkTrap	CLEAR	The voltage Vring %2$d is OK	1.3.6.1.4.1.35265.3.7.2	Parameter 2: the number of the inductor (1 or 2)
fxs72VInputOkTrap	CLEAR	Input voltage is OK	1.3.6.1.4.1.35265.3.7.7	
fxs72TemperatureOkTrap	CLEAR	The temperature of sensor %2$d is OK	1.3.6.1.4.1.35265.3.7.3	Parameter 2: The number of the temperature sensor (1-4)
fxs72TempmeasurementOkTrap	CLEAR	The problem with temperature measurements has been solved	1.3.6.1.4.1.35265.3.7.13	
fxs72PowerUnitTermOk[1]	CLEAR	Temperature of power supply is OK	1.3.6.1.4.1.35265.3.7.21	
fxs72FanLowSpeedOkTrap[1]	CLEAR	Fan rotation speed is OK	1.3.6.1.4.1.35265.3.7.22	
fxs72FanOkTrap	CLEAR	Fan %1$d is operating normally	1.3.6.1.4.1.35265.3.7.4	Parameter 1: The number of fan
fxs72SSwOkTrap	CLEAR	There is a registration on MGC/SSW	1.3.6.1.4.1.35265.3.7.5	It is used for software version - Megaco
fxs72PortOkTrap	CLEAR	Port %1$d is unlocked	1.3.6.1.4.1.35265.3.7.6	Parameter 1: The port number
fxs72VmodeSwitchTrap	INFO	Power supply is changed -%1$D V	1.3.6.1.4.1.35265.3.7.10	Parameter 1: new mode: 1 – 60V, 2 – 48V
fxs72FansSwitchTrap	INFO	Fan status changed	1.3.6.1.4.1.35265.3.7.11	Parameter 1: --disabled, 1-enabled
fxs72updateFwFail	MINOR	Error while updating firmware	1.3.6.1.4.1.35265.3.6.20	Parameter 1: The type of the error
fxs72updateFwOk	INFO	Firmware is updated	1.3.6.1.4.1.35265.3.7.20	
fxs72AuthFailedAlarmTrap	INFO	Attempt of password cracking by iteration has been detected (IP address from which access attempt has been made is specified)	1.3.6.1.4.1.35265.3.6.23	Parameter 1: 1 – telnet, 2 – ssh
fxs72BpuAlarmTrap	CRITICAL	No connection with BPU	1.3.6.1.4.1.35265.3.6.12	
fxs72BpuOkTrap	CLEAR	BPU connection restored	1.3.6.1.4.1.35265.3.7.12	

[1] Sent only by TAU-36/72.IP rev.B/rev.D.

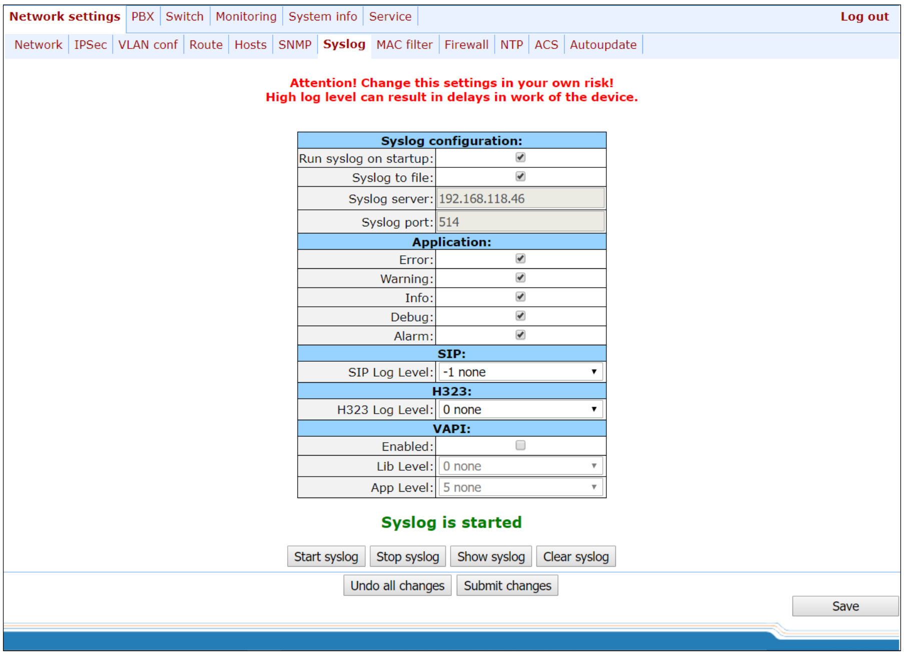
5.1.1.7 The 'Syslog' submenu. Syslog Protocol Configuration

In the *'Syslog'* menu, you may configure system log settings.

SYSLOG is a protocol, designed for transmission of messages on current system events. Gateway software generates system data logs on operation of system applications and signalling protocols, as well as occurred failures and sends them to SYSLOG server.

High debug levels may cause delays in operation of the device. IT IS NOT RECOMMENDED to use system log unless necessary.

System log should be used only when problems in gateway operation occur, and you have to identify the reason. To define the necessary debug levels, consult ELTEX Service Centre Specialist.



<u>*Syslog configuration:*</u>

– *Run syslog on startup* – when checked, run syslog on device startup;

– *Syslog to file* – when checked, save syslog into file to view it later via web interface;

– *Syslog server* – syslog *server* IP address;

– *Syslog Port* – port for *syslog* server incoming messages (514 by default);

<u>*Record type (APPLICATION):*</u>

– *Error* – send application failure messages to syslog server;

– *Warning* – send application warning messages to syslog server;

– *Info* – send application Info messages to syslog server;

– *Debug* – send application debug messages to syslog server;

– *Alarm* – send alarm event messages and information on unathorised access attempts to syslog server.

SIP:

– *SIP Log Level* – SIP protocol log level;

H.323:

– *H.323 Log Level* – H.323 protocol log level;

VAPI:

– *Enabled* – when checked, VAPI library logging is enabled, otherwise it is disabled;
– *Lib Level* – VAPI library log level;
– *App Level* – VAPI log level from the application side.

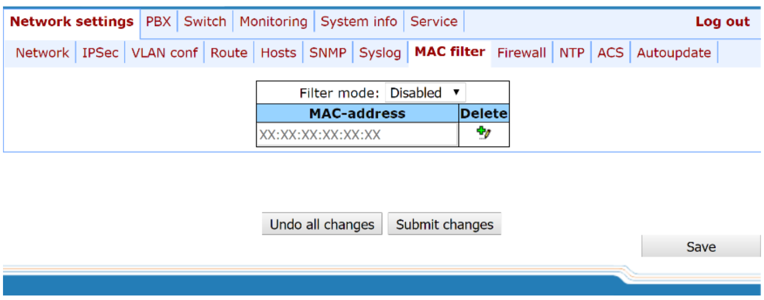
Use *Start and Stop* buttons to start and stop the output of logging information to the system log.

Use *Show* and *Clear* buttons available in syslog file saving mode to view the log via web interface and clear the log on the device.

To discard all changes made to configuration, click the *Undo All Changes* button. To apply changes, click the *Submit Changes* button.

5.1.1.8 The 'MAC filter' submenu

In the 'MAC filter' submenu, you may configure lists of permitted and denied MAC addresses from which the device is available.



– *Filter mode* – three operation modes are available: disabled, 'black list' or 'white list'.

To add MAC address to the table, enter the required address in the *'MAC address'* column in *AA:BB:CC:DD:EE:FF* format. To apply changes, click the *Submit Changes* button.

The maximum number of MAC addresses in the table is 30.

Adding addresses to the 'White list' requires at least one MAC address in the table, otherwise the 'Submit changes' button will be unavailable.

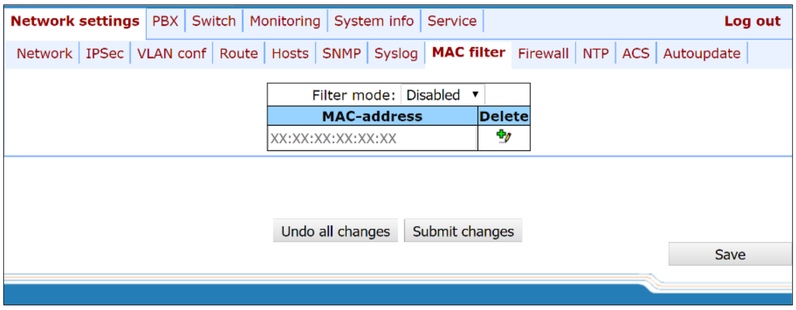
When using the 'White list', the 'Local DNS' functionality will not be available.

To delete a MAC address, select a flag opposite the required address and click in the *'Delete'* column.

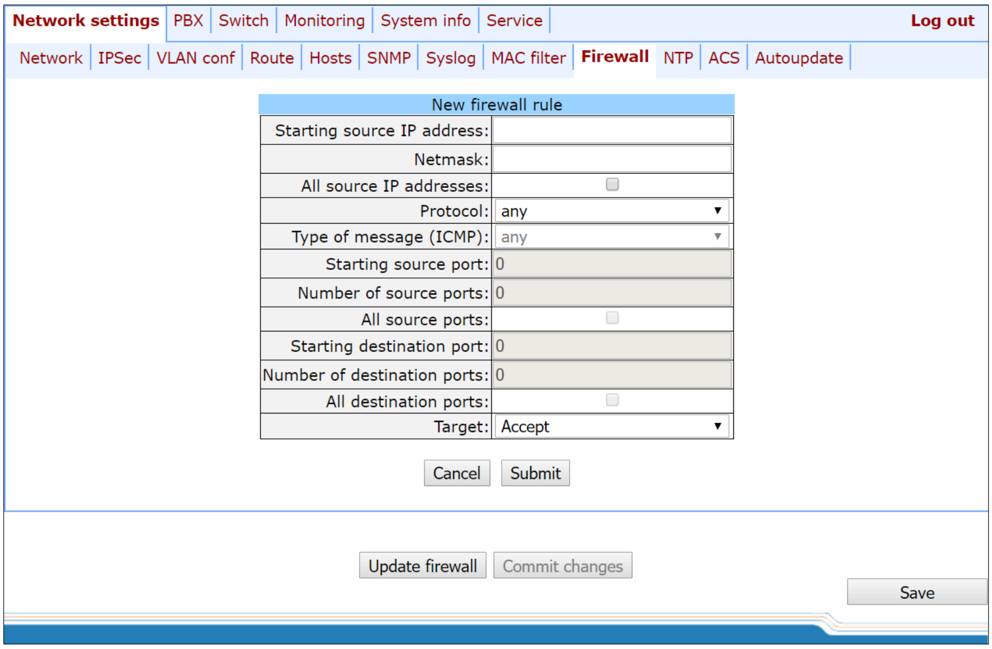
To discard all changes made to configuration, click the *Undo All Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

5.1.1.9 The 'Firewall' submenu

In the *'Firewall'* submenu, you may configure black and white lists of IP addresses to allow or deny them access to the device.



To add a new rule, click the *'New rule'* button.



<u>*New firewall rule:*</u>

– *Starting source IP address* – IP address or network address;

– *Mask* – network mask;

– *All source IP addresses* – when checked, the rule applies to all packet source IP addresses;

– *Protocol* – type of incoming packets' protocol that the rule to be applied to:

- *Any* – for UDP and TCP;

- *UDP* – for UDP;
- *TCP* – for TCP;
- *ICMP* – for ICMP.

– *Type of message (ICMP)* – type of ICMP message that the rule is created for;

– *Starting source port* – starting TCP/UDP port of the source port range;

– Number of source ports – *number of ports in the source port range;*

– *All source ports* – when checked, the rule applies to packets with any source port value;

– *Starting destination port* – starting TCP/UDP port (on the device) of the packet destination port range;

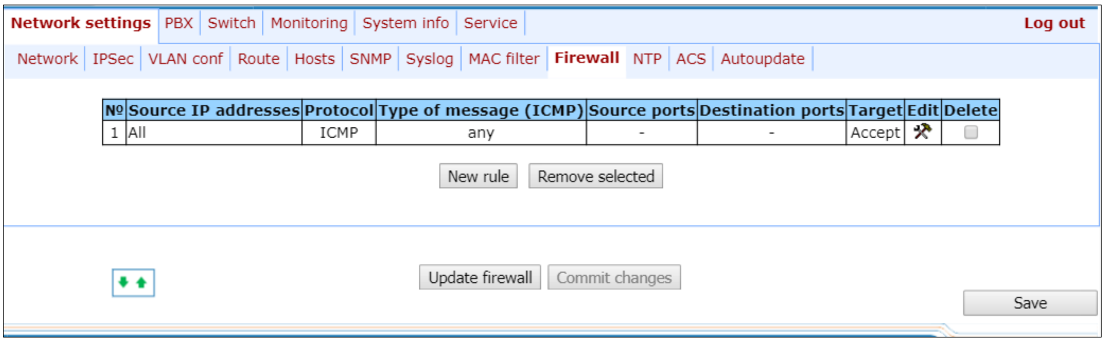
– *Number of destination ports* – number of ports in the packet destination port range;

– *All destination ports* – when checked, the rule applies to packets with any destination port value;

– *Target* – action to be performed on packets falling under this rule:

- *Accept;*
- *DROP*;
- *REJECT.*

To apply a new rule, click the *Submit* button.



To edit the rule, click icon in *'Edit'* column for the respective rule.

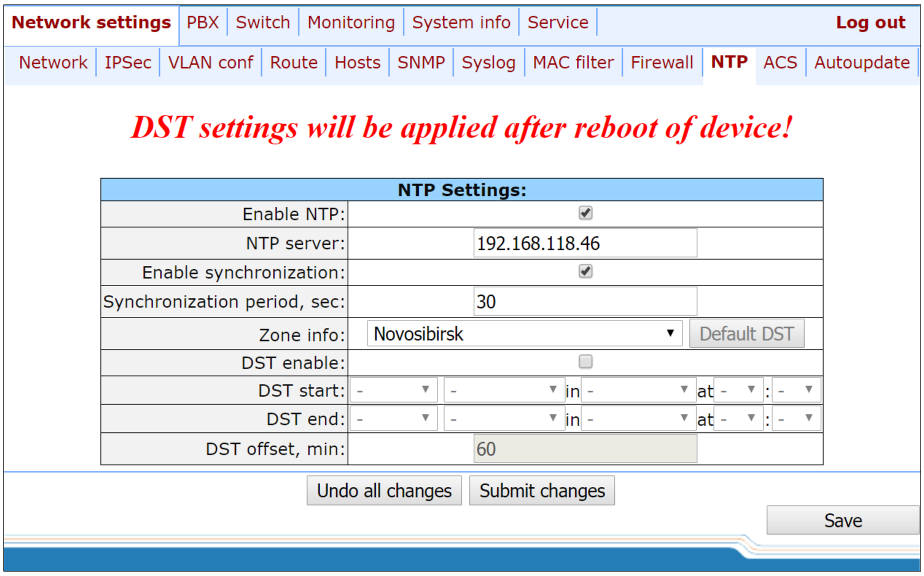
To change the rule sequence, select the necessary rule and move it to the desired position with buttons.

After all necessary rules has been added, click the *'Update firewall'* button to apply the rules. Next, you should click the *'Commit changes'* button in two minutes' interval after approving new rules, otherwise previous settings will be restored.

To discard all changes made to configuration, click the *Undo All Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

5.1.1.10 The 'NTP' submenu

NTP is a protocol designed for synchronization of real-time clock of the device. Allows to synchronize date and time used by the gateway against their reference values.



<u>*NTP Settings:*</u>

– *Enable NTP* – when checked, enable the synchronization of the device time with an external server via NTP protocol. Given that TAU is not equipped with real-time clock, in order to use the real time in monitoring and statistics tasks you should enable time synchronization with an external server;

– *NTP server* – NTP server address;

– *Enable synchronization* – when checked, perform periodic synchronization of the device with NTP server;

– *Synchronization period* – period of synchronization with NTP server (permissible value: 30 to 100000s);

– *Zone info* – timezone. Given that NTP server sends the time in a zero timezone, this setting allows to set local time on the device. If you need help on timezones, see APPENDIX L. HELP ON TIMEZONES;

Exclamation mark means that DST settings are not used for this timezone.

DST settings will be applied only after device restart.

– *DST enable* – when checked, device will perform daylight saving change and the set back process;

– *Default DST* button – allows to set standard DST periods for the current timezone by pressing the *Default DST* button;

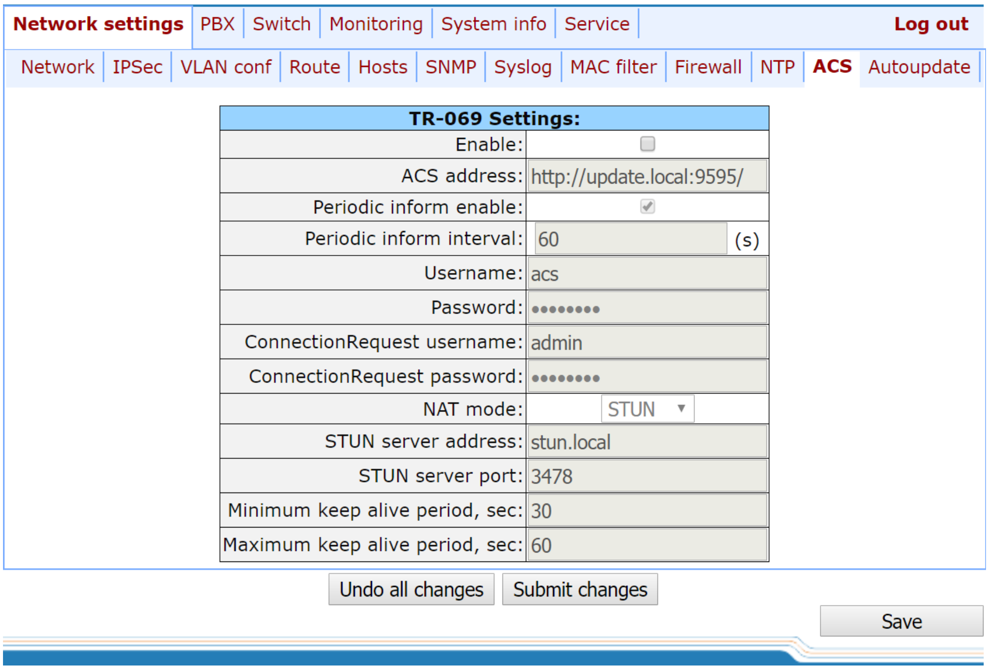
– *DST start* – defines the moment of daylight saving change;

– *DST end* – defines the moment of set back process;

– *DST offset, min* – time adjustment amount used in transition.

To discard all changes made to configuration, click the *Undo All Changes* button. To apply changes, click the *Submit Changes* button.

5.1.1.11 The 'ACS' submenu. TR-069 Monitoring and Management Protocol Configuration



<u>*TR-069 settings:*</u>

– *Enable* – when checked, enable device management via TR-069 protocol;

– *ACS address* – ACS server address. Enter address in the following format: ***http://<address>:<port>***, where:

  <address> – ACS server IP address or domain name;

  <port> – ACS server port, 10301 by default.

– *Periodic inform enable* – when checked, integrated TR-069 client will periodically poll ACS server at intervals equal to *'Periodic inform interval'* value in seconds. Goal of the polling is to identify possible changes in the device configuration;

– *Periodic inform interval* – ACS server polling interval;

– *Username* – username used by client to access the ACS server;

– *Password* – password used by client to access the ACS server;

– *ConnectionRequest username* – username used by ACS server to access the TR-069 client. Server sends ConnectionRequest notifications;

– *ConnectionRequest username* – password used by ACS server to access the TR-069 client. Server sends ConnectionRequest notifications.

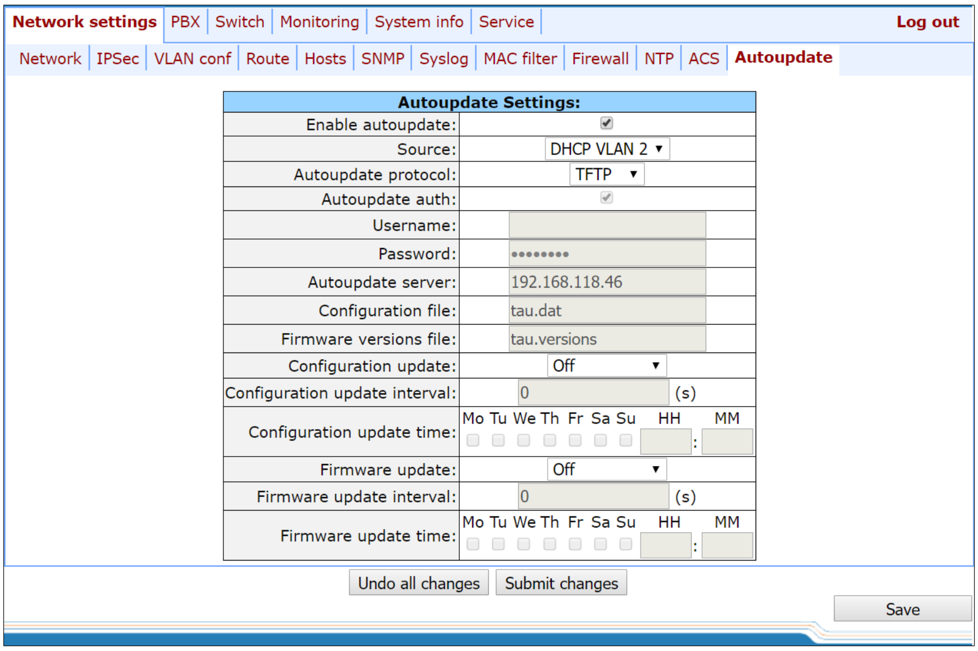
If there is a NAT (network address translation) between the client and ACS server, ACS server may not be able to establish the connection to client without specific technologies intended to prevent such situations. These technologies allow the client to identify its so called public address (NAT address 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* – TR-069 client operation mode in the presence of NAT; identifies the method, that will be used by client for obtaining its public address information. Available modes:

- *STUN* – use STUN protocol for public address identification. When choosing STUN client operation mode, you should define the following settings:
  - *STUN server address* – STUN server IP address or domain name;
  - *STUN server port* – STUN server UDP port (3478 by default);
  - *Minimum keep alive period, seconds and Maximum keep alive period, seconds* – define the time interval in seconds for periodic transmission of messages to STUN server for public address discovery and modification;
- *Public address (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. When the manual mode client ('Manual') is selected, the public client address should be specified manually:
  - *NAT address* – IP address of a public NAT.
- *Off* – NAT will no 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.

To discard all changes made to configuration, click the *Undo All Changes* button. To apply changes, click the *Submit Changes* button.

5.1.1.12 The 'Autoupdate' submenu Automatic update configuration



Autoupdate Settings:

- *Enable autoupdate* – when checked, device configuration and firmware will be updated automatically;
- *Source* – parameter obtaining method for autoupdate procedure:
  - *DHCP (VLAN 1, VLAN 2, VLAN 3)* – receive autoupdate parameters via DHCP Options 66 and 67;
  - *Static* – use autoupdate parameters specified in TAU-72.IP/TAU-36.IP configuration.
- *Autoupdate protocol* – a protocol, which will be used for autoupdate (TFTP/FTP/HTTP/HTTPS);
- *Autoupdate auth* – when checked, authentication settings will be used during autoupdate procedure;
- *Username* – login to access the autoupdate server;
- *Password* – password to access the autoupdate server;
- *Autoupdate server* – autoupdate server IP address or network name;
- *Configuration file* – name of the configuration file located on autoupdate server and its path;
- *Firmware versions file* – name of the firmware versions file located on autoupdate server and its path;
- *Configuration autoupdate* – select autoupdate mode: off, after interval or at the certain time update;
- *Configuration update interval* – automatically update configuration with the specified period in seconds;
- *Configuration update time* – selection of certain days and time when the update will be carried out;
- *Firmware autoupdate* – select autoupdate mode: off, after interval or at the certain time update;
- *Firmware update interval* – automatically update firmware with the specified period in seconds;
- *Firmware update time* – selection of certain days and time when the update will be carried out.

For autoupdate system operating procedure, see APPENDIX G. AUTOMATIC CONFIGURATION PROCEDURE AND GATEWEY FIRMWARE VERSION CHECK. To discard all changes made to configuration, click the *Undo All Changes* button. To apply changes, click the *Submit Changes* button.

In addition to static configuration of TR-069 client, the device supports DHCP Option 43 processing in the following format:

<suboption number><suboption length><suboption value>,

where:
- suboption number and length are passed in a numeric (Hex) format;
- suboption value is passed as ASCII code.

Gateway recognizes the following suboptions:

- 1 – *ACS URL* – ACS server URL.

Address should be received in the following format: **http://<address>:<port>**,

where:
<address> – ACS server IP address or domain name,
<port> – ACS server port number, 10301 by default (optional parameter);
- 2 – Provisioning code – identifier that allows ACS server to identify specific configuration parameters;
- 3 – *Login* – username used by client to access the ACS server;
- 4 – *Password* – password used by client to access the ACS server;
- 5 – autoupdate server address;

Address should be received in the following format: **<proto>://<address>[:<port>]**,

where:
<proto> – protocol (FTP, TFTP, HTTP, HTTPS),
<address> – autoupdate server IP address or domain name,
<port> – autoupdate server port (optional parameter);

- 6 – autoupdate configuration file name;

- 7 – autoupdate firmware file name.

Upon receiving Option 43, suboption 1, device launches management via TR-069 protocol.

Example of the option record:

```
01:10:68:74:74:70:3A:2F:2F:61:63:73:2E:72:75:3A:38:30:02:02:31:39:03:03:61:63:73:04:06:61:63
:73:61:63:73
```

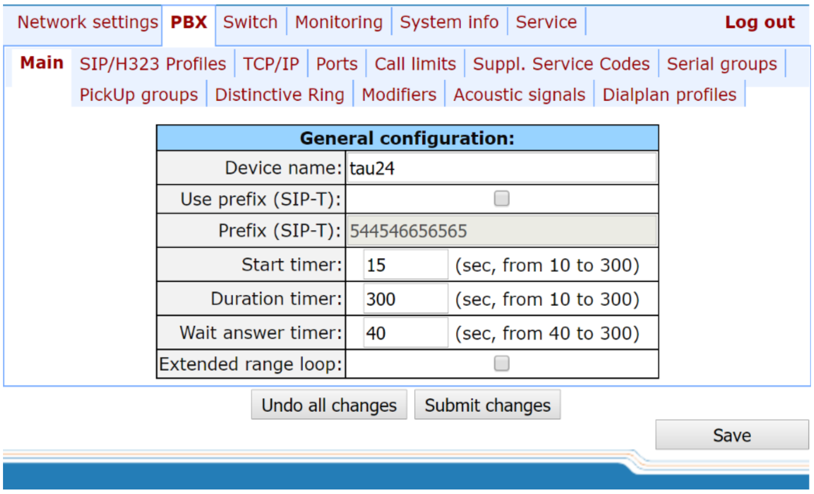
where:
01 – *ACS URL* suboption number;
10 – length, 16bytes (0x10 = 16 dec);
68:74:74:70:3A:2F:2F:61:63:73:2E:72:75:3A:38:30 – suboption value (http://acs.ru:80);
02 – Provisioning code suboption number;
02 – length, 2bytes;
31:39 – suboption value (19);
03 – Login suboption value;
03 – length, 3bytes;
61:63:73 – suboption value (acs);
04 – password suboption value;
06 – length, 6bytes;
61:63:73:61:63:73 – suboption value (acsacs).

5.1.2 The 'PBX' menu. VoIP Configuration

In the *'PBX'* menu, you can configure VoIP (Voice over IP): SIP/H.323 protocol configuration, Quality of Service configuration, FXS interface configuration, installation of codecs, numbering schedule, etc.

5.1.2.1 The 'Main' submenu.

In the*('Main')* submenu, you can configure basic device settings: set the device name, device prefix, and global timers.



<u>*General configuration:*</u>

– *Device name* – name of the device. Used for sending messages to SYSLOG server, enables device identification;

– *Use prefix (SIP-T)* – when checked, *Prefix (SIP-T)* parameter value will be used as a PBX prefix. This prefix will be added before the subscriber's number and will affect the number type: if the prefix is present, subscriber's number will be 'national'; if it is absent, then the number will be 'subscriber' (passed in CgPN parameter);

– *Prefix (SIP-T)* – PBX prefix (numeric string);

***Use prefix (SIP-T)* and *Prefix (SIP-T)* parameters are used only in gateway operation via SIP-T protocol. SIP-T protocol operation mode is defined by: in incoming communications–the presence of ISUP attachment in initializing SIP INVITE request, in outgoing communications–SIP-T protocol configuration in routing prefix (see Section 5.1.2.2.5.1 Routing rules configuration).**

– *Start timer* – dialling timeout for the first digit of a number; when there is no dialling during the specified time, 'busy' tone will be sent to the subscriber, and the dialling will end. It is used for table dial plan (see Section 5.1.2.2.5);

– *Duration timer* – complete number dialling timeout. Takes effect after the first digit of a number has been dialed*,* and specifies the time for dialling the full number;

– *Wait answer timer* – subscriber's response timeout for incoming and outgoing calls. If the subscriber fails to answer in the specified time, the call will be cleared back;

– *Fans threshold temperature* – device heating threshold temperature, when fans will be enabled for cooling. Parameter value is from 35 to 55 °C;

– *Fans force enable* – whren checked device heating threshold temperature identification function will be disabled and fans will work constantly.

To apply changes, click the *Submit Changes button.* To discard all changes made to configuration, click the *Undo All Changes* button*.* To store changes to non-volatile memory of the device, click the *Save* button.

5.1.2.2 The 'SIP/H323 Profiles' submenu

In the *'SIP/H323 Profiles'* submenu, you may configure SIP profiles and H.323 protocol. You may organize gateway operation with multiple carriers by configuring various SIP profiles on subscriber ports.

5.1.2.2.1 The SIP Common Parameters submenu (SIP Common)

In *'SIP Common'* tab, you may configure common SIP protocol parameters applied to all profiles.

SIP (Session Initiation Protocol) is a signalling protocol, used in IP telephony. It performs basic call management tasks such as starting and finishing session.

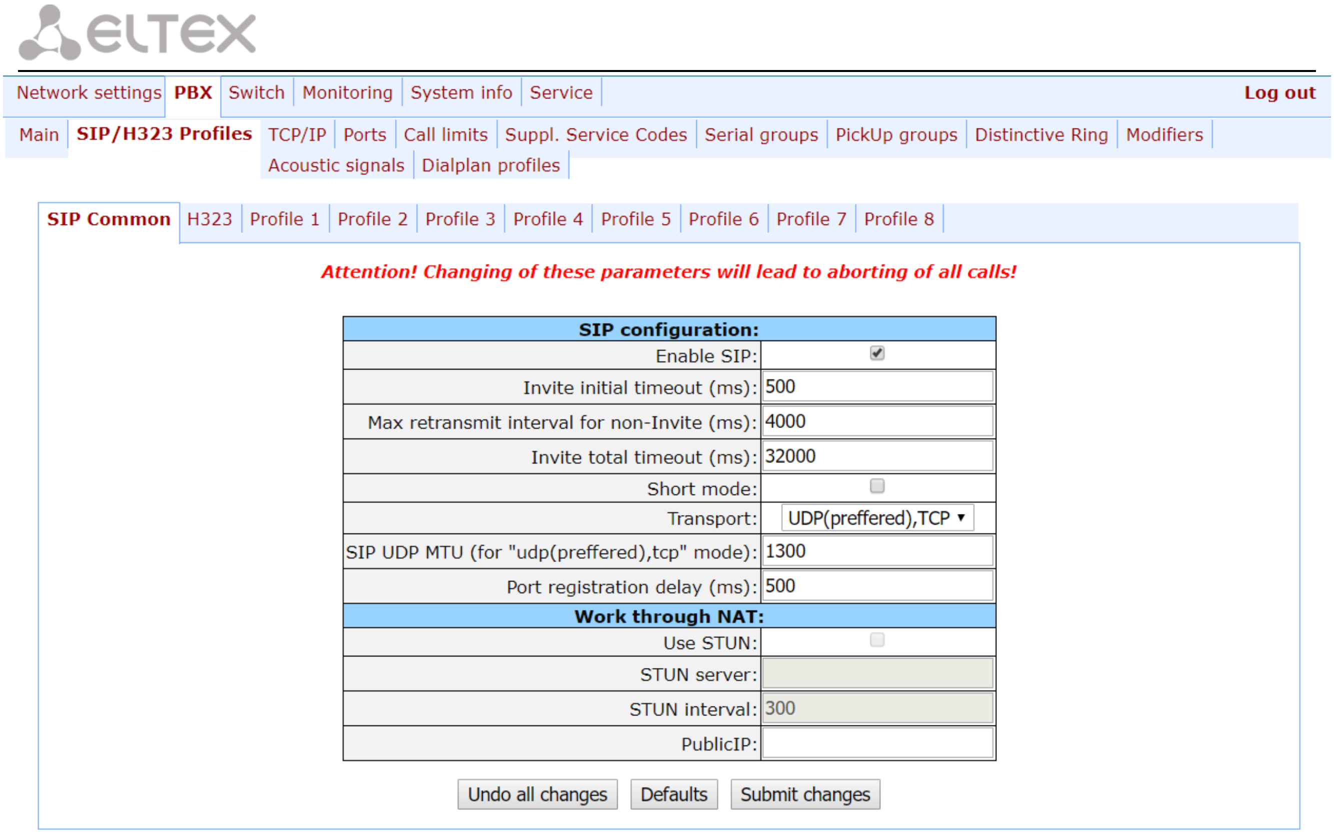
Addressing in SIP network based on SIP URI scheme:

sip:user@host:port;uri-parameters

where:

user – number of a SIP subscribe;
@ – separator located between the number and domain of a SIP subscriber;
host – domain or IP address of a SIP subscriber;
port – UDP port used for subscriber's SIP service operation;
uri-parameters – additional parameters.

One of the additional SIP URI parameters: user=phone. When this parameter is used, SIP subscriber number syntax should match TEL URI syntax described in RFC 3966. In this case, TAU-72.IP/TAU-36.IP will not clear-back calls, if SIP subscriber's number contains the following characters: '+', ';', '=', '?'.



You don't have to reboot the gateway in order to apply SIP settings. When applying settings, all current calls will be terminated.

<u>*SIP configuration:*</u>

– *Enable SIP* – when checked, SIP is enabled;

– *Invite initial timeout (ms)* – time interval between first and second INVITEs, when there is no response to the first one, in ms; the interval will be doubled for subsequent INVITEs (third, fourth, etc.) (e.g. for 300ms, the second INVITE will be sent in 300ms, the third is in 600ms, the fourth is in 1200ms, etc);

– *Max retransmit interval for non-Invite (ms)* – maximum time interval for retransmission of non-INVITE requests and replies to INVITE requests;

– *Invite total timeout (ms)* – total timeout for INVITE message transmission, in milliseconds. When this timeout expires, the direction is deemed to be unavailable. Allows to limit INVITE message retransmission, including messages used for SIP proxy availability identification;

Invite total timeout parameter is calculated depending on the required number of INVITE message retransmissions and the time interval between first and second INVITEs–*Invite initial timeout*–using the following equation:

Invite total timeout = 100+N

Where N is a number of INVITE message retransmissions. For example, in order to switch to redundant SIP-proxy, when there is no response to three INVITE messages and *Invite initial timeout* parameter value equals to 300ms, Invite total timeout should be:
100+300*1+300*2+300*4=2200ms.

– *Short mode* – when checked, use shortened field names in SIP protocol header, otherwise use complete names. Also, spaces will be removed from parameter strings in this mode;

– *Transport* – select transport layer protocol, used for SIP message transmission:

- *udp(preferred), tcp* – use both UDP and TCP protocols, but UDP priority will be higher;
- *tcp(preferred), udp* – use both UDP and TCP protocols, but TCP priority will be higher;
- *udp only* – use UDP protocol only;
- *Tcp only* – use TCP protocol only.

– *SIP UDP MTU (for 'udp(preffered), tcp' mode)* – maximum SIP protocol data size in bytes, sent with UDP transport protocol (according to RFC3261, recommended value is 1300). If SIP protocol data size exceeds specified value (it is possible, e.g. when qop authentication is used), TCP will be used as a transport protocol. This example applies to *udp(preferred), tcp* mode only.

– *Port registration delay (ms)* – delay between successive registrations of neighbouring gateway ports. Default value is 500ms. Longer delay may be necessary when the gateway operates through SBC that can temporarily block the reception of messages from gateway IP address or blacklist the gateway in case of large numbers of REGISTER queries.

Work through NAT:

When TAU gateway is located behind a NAT, it is necessary to discover an external NAT IP address for voice and signal traffic delivery to the gateway.

If NAT is used for incoming calls to the gateway, NAT address may be specified in request URI. Therefore, in order to process calls, you should set *'Full RURI compliance'* option in SIP profile.

– *Use STUN* – use STUN protocol for public NAT address discovery;

This setting is available only if the gateway operates via SIP protocol with UDP transport, i.e. the value of *Transport* parameter should be *udp only*.

– *STUN server* – STUN server IP address;

– *STUN interval* – STUN server polling period;

– *Public IP* – this setting contains a public NAT address to be used in cases, when it cannot be obtained via STUN protocol. This setting cannot be used in cases, when NAT dynamically obtains its external IP address.

Use the *Defaults* button to set default parameters (the figure below shows default values).

To apply changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

5.1.2.2.1.1 SIP-T Protocol Configuration

Configure the following parameters to utilize SIP-T protocol:

1. If you need to define a 'national' value for subscriber number type, configure the following parameters: *Use prefix (SIP-T)* and *Prefix (SIP-T).* For description of parameters, see Section 5.1.2.1 The 'Main' submenu.;

2. To route outgoing calls via SIP-T protocol, you should configure prefixes with the corresponding protocol (Protocol & Target: SIP-T Direct IP) and the type of the number fetched by the prefix (Number type). For description of parameters, see Section 5.1.2.2.5.1 Routing rules configuration;

3. To assign Caller ID category to the subscriber, use SS7 category (SIP-T) parameter in subscriber port configuration or subscriber profile. For description of parameters, see Section 5.1.2.4 The 'Ports Configuration of Subscriber Ports' submenu (Ports);

4. To receive international calls with '+' symbol preceding the number, you should configure 'User=Phone' option, see Section 5.1.2.2.3SIP Custom Parameters (Profile n/SIP Custom).

5.1.2.2.2 The 'H.323 Protocol' submenu

In *'H.323'* submenu, you can configure H.323 protocol settings.

H.323 protocol operation is possible only when Profile 1 is used. Use *Profile 1* to configure codecs and routing when H.323 protocol is used.

H.323 standard states specifications for audio and video data transmission via data networks and includes standards for video and voice codecs, public domain applications, call and system management.

H.323 stack of TAU-36.IP/TAU-72.IP gateway supports the following protocols:

– *H.245* is used for codec matching and opening of voice connection when faststart procedure is not used;

– *Q.931/H.225* – allows to establish and control a connection;

– *RAS* – allows for gatekeeper interactions;

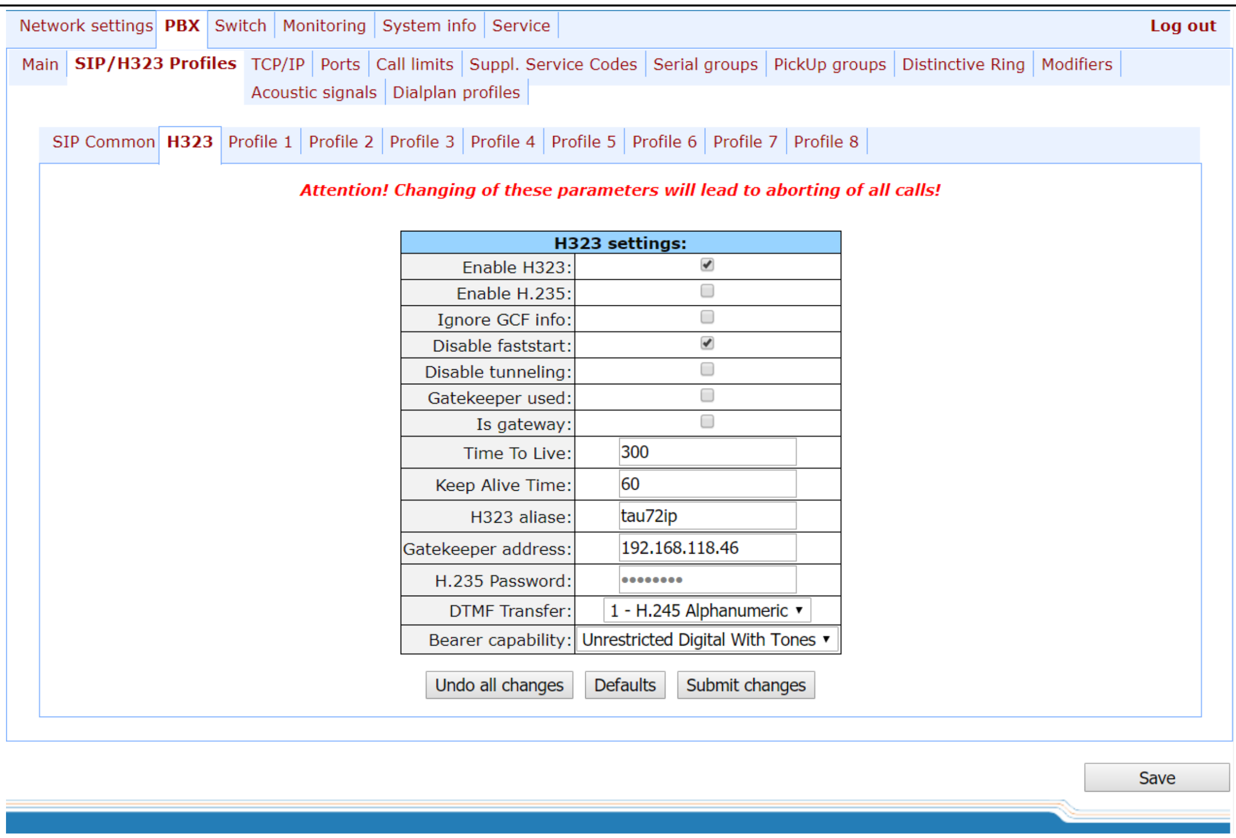
– *H.235* – authenticates calls during gatekeeper interactions;

– *H.450.1* – used during put on/remove from hold.

Gatekeeper allows for call processing inside its zone and interaction with other zones as well as call management. During gatekeeper operations, the gateway should register on the gatekeeper and perform authorization using login and password (H.235) depending on the local network policy. Only after successful registration gateway subscribers will be able to perform calls through the gatekeeper. Gateway registers on the gatekeeper for a limited amount of time–Time to live (TTL)–during which it should renew its registration. Keep alive timer is used for this purpose; upon expiration, the gateway sends a renewal request.

Faststart procedure enables 'fast' establishment of a voice connection. In this case, channel will be established before the start of capability coordination with H.245 protocol. *Tunnelling* procedure allows to transfer H.245 signalling via Q.931 signal channels. As a result, no additional TCP connection (or TCP port) is required for capability coordination.

You don't have to reboot the gateway in order to apply H.323 settings. When applying settings, all current calls will be terminated.



<u>*H323 settings:*</u>

– *Enable H323* – when checked, H.323 protocol is enabled;

– *Enable H.235* – when checked, use authentication on the gatekeeper with H.235 protocol;

– *Ignore GCF info* – when checked, output authentication data in RRQ message via H.235 protocol in any events, otherwise – only in case of reception of supported hash method in GCF message. This setting applies to operations with gatekeepers that do not send used hash method in a response to GRQ request. In this case, the gateway will transfer MD5-encrypted authentication data for all RRQs, even if supported hash method is not received from the gatekeeper;

– *Disable faststart – when checked,* faststart feature will be disabled;

– *Disable tunneling* – when checked, H.245 signal tunneling through Q.931 signal channels will be disabled;

– *Gatekeeper used* – when checked, use gatekeeper registration option;

– *Is gateway* – when checked, device registers on a gatekeeper as a gateway, otherwise–as a terminal device. When registered as a terminal device, the gateway registers all configured subscribers' numbers and a gateway name–H.323 alias–on a gatekeeper. When registered as a gateway, the gateway registers its name–H.323 alias–only. To simplify the gatekeeper configuration, we recommend using registration as a terminal device;

– *Time To Live* – time period in seconds, for which the device will keep its registration on a gatekeeper;

– *Keep Alive Time* – time period in seconds, after which the device will renew its registration on a gatekeeper;

– *H.323 alias* – name for registration on a gatekeeper;

- *Gatekeeper address* – IP address of a gatekeeper;
- *H.235 password* – password used for H.235 protocol authentication.
- *DTMF Transfer* – select transfer method for flash and DTMF tones via H.323 protocol (H.245 Alphanumeric, H.245 Signal, Q931 Keypad IE). Transfer of DTMF tones enables extension dialling feature;
  - *H.245 Alphanumeric* – basicstring compatibility is used for DTMF transmission, and *hookflash* compatibility for flash transmission (flash is transferred as '!' symbol);
  - *H.245 Signal* – dtmf compatibility is used for DTMF transmission, and *hookflash* compatibility for flash transmission (flash is transferred as '!' symbol);
  - *Q931 Keypad IE* – for DTMF and flash transmission (flash is transferred as '!' symbol), *Keypad* information element is used in INFORMATION Q931 message;
- *Bearer capability* – select information transfer service (*Speech, Unrestricted Digital, Restricted Digital, 3.1 kHz Audio, unrestricted Digitals with Tones*). We recommend using value '3.1 kHz Audio'. All other values used only for compatibility with communicating gateways.

'*DTMF Transfer*' item will be used only if there is an item *2–INFO–* is selected in *DTMF Transfer* item of the *Codecs conf*.

To ensure the successful renewal of device registration on gatekeeper, specify *Keep Alive Time* renewal period equal to *2/3* of *Time To Live* registration period. Moreover, for *Time To Live* parameter, we recommend specifying the same value as for the gatekeeper, so the registration renewal period–*Keep Alive Time*–of the gateway was less or equal to *Time To Live* value (transferred in responses). Otherwise, invalid configuration may lead to situations, where gatekeeper will void the gateway registration before the renewal, which in turn may lead to termination of all active connections, established through the gatekeeper.

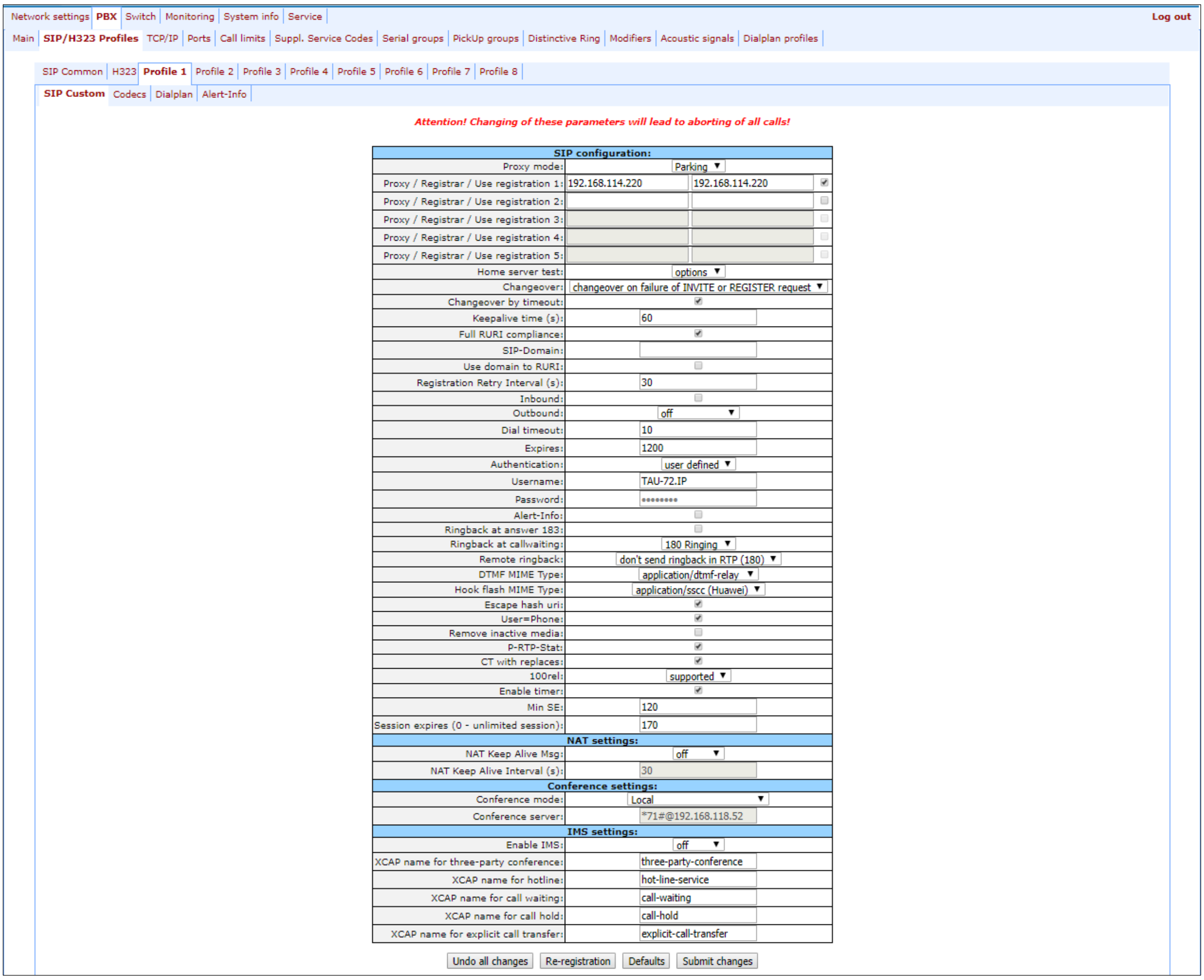
After implementation of changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

Use the *Defaults* button to set default parameters as shown in the figure above.

5.1.2.2.3 SIP Custom Parameters (Profile n/SIP Custom)

In *'Profile n/SIP Custom'* tab, you may configure SIP protocol parameters for each profile.

You don't have to reboot the gateway in order to apply SIP settings. When applying settings, all current calls will be terminated.



The 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 (when 'changeover by timeout' option is enabled), 503, or 505 is received, the gateway sends INVITE (or REGISTER) message to the first redundant SIP-proxy address, and 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 renew its registration and begin operation with the main SIP-proxy.

<u>*SIP configuration:*</u>

- *Proxy mode* – select SIP server (SIP-proxy) operation mode form the drop-down list:
  - *Off* – disabled;
  - *Parking* – SIP-proxy redundancy mode without main SIP-proxy management;
  - *Homing* – SIP-proxy redundancy mode with main SIP-proxy management.
- *Proxy/Registrar address 1..5* – SIP-proxy/registration server network address; you may define the port after the colon; if it is not specified, 5060 will be taken as the default port value;
- *Use registration 1..5* – when checked, register on server, otherwise registration server will not be used;
- *Home server test* – depending on the selected configuration, test the main *proxy* using OPTIONS, REGISTER, or INVITE messages in 'homing' redundancy mode;
- *Changeover* – this setting defines the request transmission error that will be used for redundant proxy changeover: INVITE and REGISTER, INVITE only, REGISTER or OPTIONS only;
- *Changeover by timeout* – when enabled, redundant proxy changeover will be performed when response 408 is received;
- *Keepalive time (s)* – period of time between OPTIONS or REGISTER management message transfers, in seconds;
- *Full RURI compliance* – when checked, all URI elements (u*ser, host and port*–subscriber number, IP address and UDP/TCP port) will be analyzed upon receiving an incoming call. If all URI elements match, the call will be assigned to the subscriber port. When unchecked, only subscriber number (user) will be analyzed, and if the number matches, the call will be assigned to the subscriber port;
- *SIP Domain* – SIP domain. Used when you need to pass *from* and *to* fields in the *'host'* parameter of SIP URI scheme;
- *Use domain to RURI* – use a domain in Request URI. In this case, domain will be sent in 'REGISTER', 'INVITE', 'SUBSCRIBE', 'NOTIFY', 'OPTIONS' Request URI. Does not apply in 'OPTIONS' requests, used for the main SIP server management (Home server test);
- *Registration Retry Interval (s)* – retry interval for SIP server registration attempts, when the previous attempt was unsuccessful (e.g., if response *'403 forbidden'* was received from the server);
- *Inbound* – when checked, receive all incoming calls from SIP-proxy, otherwise receive incoming calls from all hosts. When enabled, the routing to the proxy address will be created for all calls originated by addresses that differ from SIP-proxy (response *'305 Use proxy'* will be used with the address of the required server);
- *Outbound* – defines the mode for outgoing calls via SIP-proxy:
  - *off* – outgoing calls routed is performed according to the dialplan;
  - *On* – SIP-proxy will be used for outgoing calls in all cases;
  - *With busy tone* – SIP-proxy will be used for outgoing calls in all cases. If subscriber port is not registered for some reason, busy tone will be played on this port, when the phone is offhook.

In addition to static Outbound SIP server configuration, you may define dynamic configuration with DHCP Option 120. When this option is received, the gateway will use it in the first SIP profile (Profile 1) only; at that, *'Proxy/Registrar address'* settings will remain in effect and will still be used as SIP-proxy and registration server addresses. If you want to use addresses specified in Option 120 as SIP-proxy and registration server addresses, leave *'Proxy/Registrar address'* settings blank. As this option allows to send addresses of a multiple outbound SIP servers, *Proxy redundancy modes* described above will also work in this case.

– *Dial timeout (for Outbound)* – dialling timeout for the next digit (in 'Outbound' mode), in seconds. To dial without a timeout, you should use prefixes with the definite quantity of digits or use *'Stop dial at #'* setting separately for subscriber ports.

This setting is effective for 'Dialplan table' routing plan only.

– *Expires* – registration renewal time period;

– *Authentication* – defines device authentication mode:

- *Global* – enable SIP server authentication with common user name and password for all subscribers;
- *User defined* – enable SIP server authentication with different user names and passwords for each subscriber, user name and password for ports could be defined in 'PBX/Ports'.

– *Username* – username for *'global'* mode authentication;

– *Password* – password for *'global'* mode authentication (*'password'*, by default);

– *Alert Info* – process INVITE request 'Alert Info' header to send a non-standard ringing to the subscriber port. Cadence for a non-standard ringing may be configured in 'Alert Info' tab of the corresponding SIP profile;

– *Ringback at answer 183* – when checked, 'ringback' tone will be sent upon receiving '183 Progress' message. When this setting is used, the gateway will not generate a ringback tone to the local subscriber, if the voice frequency path is already forwarded at the time when the message 183 is received, or if message 183 contains SDP session description for the frequency path forwarding;

– *Ringback at callwaiting* – send *180* or *182* message, when the second call is received on the port with an active Call waiting service. Used to notify the caller (with a ringback tone of specific tonality) that their call is queued and waiting for response. Depending on the received message (180 Ringing or182 Queued), the caller gateway generates either a standard ringback (180 Ringing) or a non-standard one (182 Queued);

– *Remote ringback* – parameter defines, whether the gateway should send a ringback tone upon receiving an incoming call:

- *Don't send ringback in RTP (180)* – when an incoming call is received, the gateway will not generate a ringback tone and will return '180 ringing' response;
- *Don't send ringback in RTP (183)* – when an incoming call is received, the gateway will not generate a ringback tone and will return '183 progress' response;

- *Ringback with 180 ringing* – when an incoming call is received, the gateway will generate a ringback tone and send it to the communicating gateway in the voice frequency path. Voice frequency path forwarding will be performed along with '180 ringing' message transmission via SIP protocol;
- *Ringback with 183 progress* – when an incoming call is received, the gateway will generate a ringback tone and send it to the communicating gateway in the voice frequency path. Voice frequency path forwarding will be performed along with '183 ringing' message transmission via SIP protocol.

– *DTMF MIME Type* – MIME extension type used for DTMF transmission in SIP protocol INFO messages:

- *Application/dtmf* – DTMF is sent in application/dtmf extension ('*' and '#' are sent as digits 10 and 11);
- *Application/dtmf-relay* – DTMF is sent in application/dtmf-relay extension ('*' and '#' are sent as symbols '*' and '#');
- *Audio/telephone-event* – DTMF is sent in audio/telephone-event extension ('*' and '#' are sent as digits 10 and 11).

  DTMF transmission performed during the established session allows for extension dialling.

– *Hook Flash MIME Type* – MIME extension type used for Flash transmission in SIP protocol INFO messages:

- *As DTMF* – send in MIME extension configured in DTMF 'MIME Type' parameter. If *application/dtmf-relay* is used, then the flash will be sent as 'signal=hf'; if *application/dtmf* or *audio/telephone-event* is used, then the flash will be sent as the digit '16';
- *Application/Hook Flash* – flash is sent in Application/ Hook Flash extension (as 'signal=hf');
- *Application/Broadsoft* – flash is sent in Application/ Broadsoft extension (as 'event flashhook');
- *Application/sscc* – flash is sent in Application/ sscc extension (as event flashhook);
  Used when you have to send the flash impulse to the opposite device without update of session parameters;

For detailed information on operations with flash in application/broadsoft and application/sscc used for supplementary services, see APPENDIX J. PROCESSING OF INFO REQUESTS CONTAINING APPLICATION/BROADSOFT AND APPLICATION/SSCC AND USED FOR SUPPLEMENTARY SERVICES.

– *Escape hash uri* – when checked, send hash symbol (#) in SIP URI as escape sequence '%23', otherwise–as '#' symbol. When option user=phone is checked, hash symbol is always sent as '#' symbol regardless of *'Escape hash uri'*;

– *User=Phone* – when checked, use 'User=Phone' tag in SIP URI, otherwise it will not be used. Tag usage is described in the beginning of this section;

– *Remove inactive media* – when checked, remove inactive media streams during SDP session modification. Enables interaction with gateways that incorrectly handle rfc3264 recommendation (according to recommendation, the number of streams should not decrease during session modifications);

– *P-RTP-Stat* – use 'P-RTP-Stat' header in BYE request or in its reply to transfer RTP statistics;

- *CT with replaces* – when checked, use *'replaces'* tag while performing *'Call Transfer'* service, otherwise it will not be used. When the checkbox is selected, the gateway performing the service generates *'refer-to'* header, which–in addition to the address of a subscriber the call being transferred to–adds *'replaces'* tag that contains DIALOG ID (Call-ID, to-tag, from-tag) of a replaced call. It is recommended to use *'replaces'* tag in operations with SIP server, as this option mostly does not require the establishment of a new dialogue between SIP server and the subscriber that the call is being forwarded to;

- *100rel* – use reliable provisional responses (RFC3262):

  - *supported* – reliable provisional responses are supported;
  - *required* – reliable provisional responses are mandatory;
  - *off* – reliable provisional responses are disabled.

- *Enable timer* – when checked, enables support of SIP session timers (RFC 4028). During the voice session, UPDATE requests (if the opposite gateway supports them) or re-INVITE requests should be sent for connection management purposes;

- *Min SE* – minimal time interval for connection health checks (90 to 1800s, 120s by default);

- *Session expires* – 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).

<u>*NAT settings:*</u>

- *NAT Keep Alive Msg* – selection of an active session support mode for operations through NAT:

  - *Off* – disabled;
  - *options* – use OPTIONS request as an active session support message;
  - *notify* – use NOTIFY notification as an active session support message;
  - *CRLF* – use CRLF special request as an active session support message.

- *NAT Keep Alive Interval (s)* – active session support message transmission period. Permitted values–30 to 120 seconds.

<u>*Conference settings:*</u>

- *Conference mode*–conference assembly mode selection;

  - *Local* – conference assembly is performed locally at the gateway. Voice packets are mixed at the gateway;
  - *Remote (REFER to Focus)* – conference assembly is performed at the conference server. Voice packets are mixed at the server. In this mode, gateway sends to server the information on gateways which should be added to the conference. Next, conference server will add these gateways to the conference;
  - *Remote (REFER to User)* – conference assembly is performed at the conference server. Voice packets are mixed at the server. In this mode, gateway sends to subscribers the identifier of a conference, that they should connect to at the conference server. Next, gateways will add themselves to the conference;

For conference operation algorithms in various modes, see Section 7.3 3-way conference

– *Conference server* – conference server name in Remote mode operation;

<u>*IMS settings:*</u>

– *Enable IMS* – enable service (simulation service) management using IMS (3GPP TS 24.623);

Gateway supports:

- *Implicit subscription to IMS services* – in this subscription option, gateway will not send SUBSCRIBE requests after subscriber registration, and will only process NOTIFY requests received from IMS, which are used for service management:
- *Explicit subscription to IMS services* – in this subscription option, gateway will send SUBSCRIBE requests after subscriber registration, and upon successful subscription, will process NOTIFY requests received from IMS, which are used for service management.

When *'Enable IMS'* setting is enabled, *'Process flash'*, *'Call waiting'* and *'Hot line'* parameters will not be processed in subscriber port settings, as these services are managed by IMS server.

– *XCAP name for three-party conference* – a name sent in XCAP attachment for *'3-party conference' service management;*

– *XCAP name for hotline* – a name sent in XCAP attachment for *'Hotline' service management;*

– *XCAP name for call waiting* – a name sent in XCAP attachment for *'Call waiting' service management;*

– *XCAP name for call hold* – a name sent in XCAP attachment for *'Call hold' service management;*

– *XCAP name for explicit call transfer* – a name sent in XCAP attachment for 'Explicit call transfer' service management.

For forced registration renewal of subscriber ports with the current SIP profile, click the *Re-registration* button.

Use the *Defaults* button to set default parameters (the figure below shows default values).

To apply changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

5.1.2.2.3.1 Provisional response setting operation

SIP protocol defines two types of responses for connection initiating request (INVITE) – provisional and final. 2xx, 3xx, 4xx, 5xx and 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.

<u>*Setting operation for outgoing communications:*</u>

- *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.*

- *off* – 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.

<u>*Setting operation for incoming communications:*</u>

- *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;

- *off* – 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.

5.1.2.2.3.2 Configuration of Internal Switching for SIP-proxy Connection Loss

In order to perform intra-office calls when connection to SIP-proxy is lost, you should specify TAU-72.IP/TAU-36.IP gateway IP address as the last SIP-proxy. At that, 'Proxy mode' must be set to 'homing', otherwise, when the connection to the main SIP-proxy is restored, it will not be used afterwards.

5.1.2.2.3.3 SIP domain configuration via local DNS

In the current firmware version, it is possible to configure SIP domain using a local DNS. This option may become useful, for example, when you use redundant SIP-proxies in different domains.

<u>*SIP domain configuration order for 'n' profile:*</u>

1. To use a local DNS, leave DNS field in *'Network/Network settings'* tab blank or enter the value 127.0.0.1;

2. In *'Network/Hosts'* tab, enter the mapping of a host (SIP domain) to actual IP addresses of SIP proxy/SIP registrar;

3. *In* 'PBX/SIP-H323 Profiles/Profile n/SIP Custom' *tab,* specify domains for each pair of SIP proxy and SIP registrar;

4. Enable routing via SIP proxy by selecting *outbound* checkbox in ***'PBX/SIP-H323 Profiles/Profile n/SIP Custom'*** *tab,* or entering prefixes in 'PBX/SIP-H323 Profiles/Profile n/Dialplan (Dialplan table)' *tab.* If you configure prefixes, select SIP proxy protocol in *'Protocol&Target' field*.

5.1.2.2.4 Codecs Configuration (Profile n/Codecs)

In the *'Profile n/Codecs'* submenu, you may configure codecs used in the current profile.

TAU-72.IP/TAU-36.IP signal processor encodes analogue voice traffic and fax/modem data into digital signal and performs its reverse decoding. Gateway supports the following codecs: G.711A, G.711U, G.729, G723.1, G.726-32.

G.711 is 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 (Annex A).

G.723.1 codec is used together with 'Silence compression' setting. When the setting is enabled, Annex A support is enabled, otherwise it is disabled.

G.726-32 is a voice data compression codec that uses ADPCM compression algorithm at the rate of 32kbps.

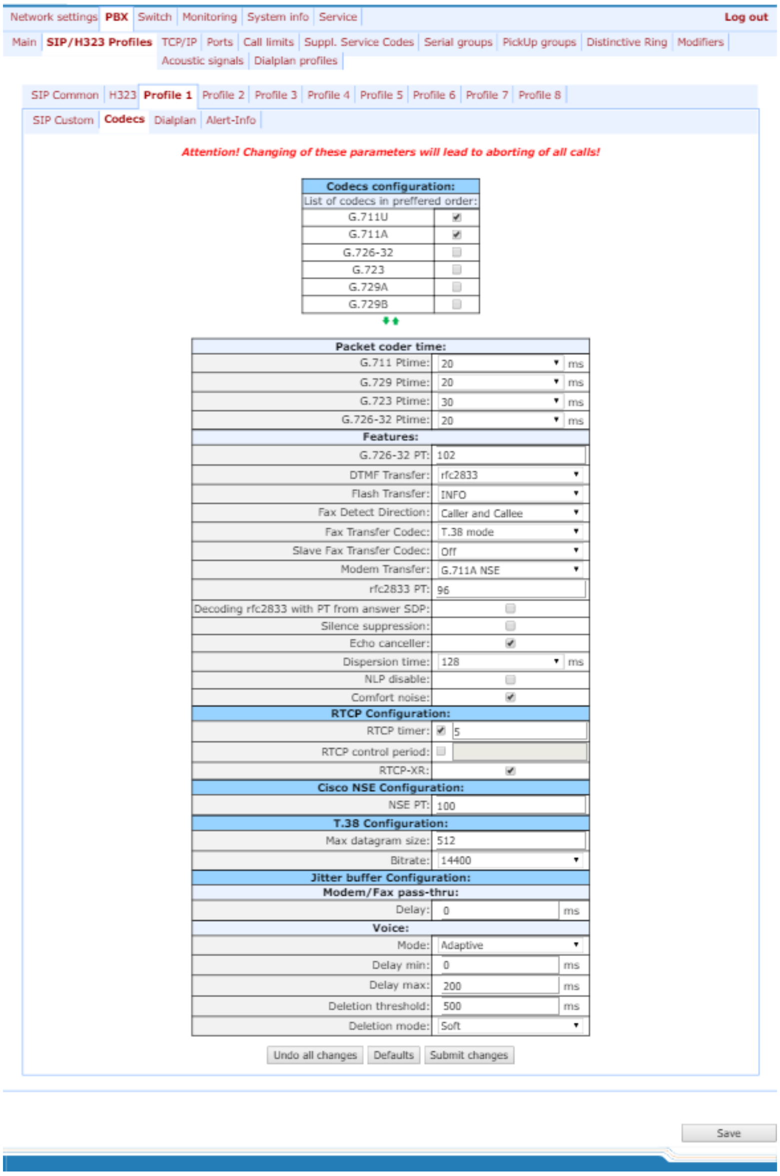
G.729 is also a voice data compression codec with the rate of 8kbps. As with G.723.1, G.729 codec supports voice activity detector and performs comfort noise generation (Annex B).

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 to perform reliable fax transmissions through unstable channels.

You don't have to reboot the gateway in order to apply codec settings. When applying settings, all current calls will be terminated!

In ***'Codecs configuration'*** section, you may select codecs and an order of their usage on connection establishment. Codec with the highest priority should be placed in top position.

Click the left mouse button to highlight the row with the selected codec. Use arrow buttons (up, down) to change the codec priority.



– *Use G.711A* – use G.711A codec;

– *Use G.711U* – use G.711U codec;

– *Use G.723* – use G.723.1 codec;

– *Use G.729A* – use G.729 annexA codec (when defining codec compatibility, non-standard codec description is sent via SIP: a=rtpmap:18 G729A/8000 a=fmtp:18 annexb=no);

– *Use G.729B* – use G.729 annexB codec;

– *Use G.726-32* – use G.726-32 codec.

G.726-32 codec used only in SIP protocol operations.

Packet coder time

In *'Packet coder time'* section, you should define packetization time, i.e. amount of voice data in milliseconds (ms), transmitted in a single RTP protocol voice packet:

- G711 Ptime – for G711 codec *(permitted values: 10, 20, 30, 40, 50, 60)*;
- G729 Ptime – for G729 codec *(permitted values: 10, 20, 30, 40, 50, 60, 70, 80)*;
- G723 Ptime – for G723 codec *(permitted values: 30, 60, 90)*;
- *G.726-32 –* for G.726-32 codec *(allowed values 10, 20, 30)*.

Features:

- *G.726-32 PT –* G.726-32 codec payload type (permitted values: 96 to 127).
- *DTMF Transfer –* DTMF tone transmission method. During established session, DTMF transmission is used for extension dialling;
  - *Inband* – inband, in RTP voice packets;
  - *RFC2833* – according to RFC2833 recommendation, as a dedicated payload in RTP voice packets;
  - *INFO* – outbound. For SIP protocol, INFO messages are used; the type of transmitted DTMF tones depends on MIME extension type (for detailed description, see Section 5.1.2.2.3). When H.323 protocol is used, DTMF transmission method depends on 'DTMF Transfer' parameter in H.323 tab (see Section 5.1.2.2.2).

In order to be able to use extension dialling during the call, make sure that the similar DTMF tone transmission method is configured on the opposite gateway.

- *Flash Transfer –* short clearback Flash transmission method. Flash transmission by the subscriber's port via IP network is possible only when Flash function operation mode 'Transmit flash' is configured on this port (see Section 5.1.2.4The ‘Ports Configuration of Subscriber Ports’ submenu (Ports)):
  - *Disabled* – Flash transmission is disabled;
  - *RFC2833* – Flash transmission is performed according to RFC2833 recommendation, as a dedicated payload in RTP voice packets;
  - *INFO* – Flash transmission is performed with SIP/H323 protocol methods. For SIP protocol, INFO messages are used; the type of transmitted Flash tone depends on MIME extension type (for detailed description, see Section 5.1.2.2.3). When H.323 protocol is used, flash transmission method depends on 'DTMF Transfer' parameter in H.323 tab (see Section 5.1.2.2.2)
- *Fax Detect Direction –* defines the call direction for fax tone detection and subsequent switching to fax codec:
  - *no detect fax* – disables fax tone detection, but will not affect fax transmission (switching to fax codec will not be initiated, but such operation still may be performed by the opposite gateway);
  - *Caller and Callee* – tones are detected during both fax transmission and receiving. During fax transmission, CNG FAX signal is detected from the subscriber's line. During fax receiving, V.21 signal is detected from the subscriber's line;

- *Caller* – tones are detected only during fax transmission. During fax transmission, CNG FAX signal is detected from the subscriber's line;
- *Callee* – tones are detected only during fax receiving. During fax receiving, V.21 signal is detected from the subscriber's line;

– *Fax Transfer Codec* – master protocol/codec used for fax transmissions:

- *fax transfer G.711A* – use G.711A codec for fax transmissions. Switching to G.711A codec will be performed when the corresponding tones are detected;
- *fax transfer G.711U* – use G.711U codec for fax transmissions. Switching to G.711U codec will be performed when the corresponding tones are detected;
- *T.38 mode* – use T.38 protocol for fax transmissions. Switching to T.38 will be performed when the corresponding tones are detected.

– *Slave Fax Transfer Codec* – slave protocol/codec used for fax transmissions. This codec is used when the opposite device does not support the priority:

- *fax transfer G.711A* – use G.711A codec for fax transmissions. Switching to G.711A codec will be performed when the corresponding tones are detected;
- *fax transfer G.711U* – use G.711U codec for fax transmissions. Switching to G.711U codec will be performed when the corresponding tones are detected;
- *T.38 mode* – use T.38 protocol for fax transmissions. Switching to T.38 will be performed when the corresponding tones are detected.
- *Off* – disable slave protocol/codec;

Master and slave protocols/codecs should differ from each other.

– *Modem Transfer* – defines switching into 'Voice band data' mode (according to V.152 recommendation). In VBD mode, the gateway disables the voice activity detector (VAD) and comfort noise generator (CNG), this is necessary for establishing a modem connection.

- *Off* – disable modem signal detection;
- *G.711A VBD* – use G.711A codec to transfer data via modem connection. Switching to G.711A codec in VBD mode will be performed when the CED tone is detected;
- *G.711U VBD* – use G.711U codec to transfer data via modem connection. Switching to G.711U codec in VBD mode will be performed when the CED tone is detected;
- *G.711A RFC3108* – use G.711A codec to transfer data via modem connection. When entering modem data transfer mode via SIP protocol, echo cancellation and VAD are disabled with attributes described in RFC3108 recommendation:
  - a=silenceSupp:off - - - -
  - a=ecan:fb off -;

- *G.711U RFC3108* – use G.711U codec to transfer data via modem connection. When entering modem data transfer mode via SIP protocol, echo cancellation and VAD are disabled with attributes described in RFC3108 recommendation:
  - a=silenceSupp:off - - - -
  - a=ecan:fb off -;
- *G.711A NSE* – CISCO NSE support, G.711A codec is used to transfer data via modem connection;
- *G.711U NSE* – CISCO NSE support, G.711U codec is used to transfer data via modem connection.

Cisco NSE support: when NSE 192 packet is received, gateway will switch to the selected codec and disable VAD; when NSE 193 packet is received, echo canceller will be disabled.

– *RFC2833 PT* – type of payload used to transfer packets via RFC2833. Permitted values: 96 to 127. RFC2833 recommendation describes the transmission of DTMF and Flash tones via RTP protocol. This parameter should conform to the similar parameter of a communicating gateway;

– *Decoding rfc2833 with PT from answer SDP* – when performing outgoing call, receive DTMF tones in rfc2833 format with payload type proposed by a communicating gateway. When unchecked, tones will be received with the payload type, configured on the gateway. Enables compatibility with gateways that incorrectly handle rfc3264 recommendation;

– *Silence suppression* – when checked, use voice activity detector (VAD) and silence suppression (SSup), otherwise they will not be used. Voice activity detector disables transmission of RTP packets during periods of silence, reducing loads in data networks;

– *Echo canceller* – when checked, use echo cancellation (tail length is up to 128ms);

– *Dispersion time* – echo signal, appearing with a delay of no more than the given value, will be jammed (up to 128 ms);

– *NLP disable* – when checked, use echo cancellation with disabled non-linear processor (NLP). When signal levels on transmission and reception significantly differ, useful signal may become suppressed by the NLP. Use this echo canceller operation mode to prevent the signal suppression;

– *Comfort noise* – when checked, use comfort noise generator. Used together with *'Silence compression (VAD)'* setting, as comfort noise packets are generated only upon voice pauses detection;

<u>*RTCP configuration*</u>

In *'RTCP configuration'* section, you may configure basic settings for device operation via RTCP protocol:

– *RTCP timer* – time period in seconds (5-65535), after which the device send control packets via RTCP protocol. When unchecked, RTCP will not be used;

– *RTCP control period* – control function of a voice frequency path status. Defines the period of time (RTCP timer), during which the opposite side will wait for RTCP protocol packets. When there are no packets in the specified period of time, established connection will be terminated due to loss of connection–cause 3 no route to destination. Control period value is calculated using the following equation: RTCP timer* RTCP control period, seconds. When unchecked, control feature will be disabled;

– *RTCP-XR* – when checked, generate 'RTCP Extended Reports' control packets according to RFC 3611.

Cisco NSE configuration

In *'Cisco NSE configuration'* section, you may configure codec payload type for modem transmission using CISCO NSE method:

- *NSE PT* – type of payload used to transfer packets via NSE. Permitted values: 96 to 127;

T38 configuration

In *'T38 configuration'* section, you may configure T.38 protocol parameters:

- *Max Datagram Size* – maximum datagram size. (Zero value means that T38MaxDatagram attribute will not be transferred via SIP, and the gateway will support the reception of datagrams up to 512bytes. Use zero value in interactions with gateways that do not support datagrams from 272bytes and higher). This parameter defines the maximum quantity of bytes that will be sent in T.38 protocol packet;

- *Bitrate* – maximum fax transfer rate (9600, 14400). This setting affects the ability of a gateway to work with high-speed fax units. If fax units support data transfer at 14400 baud, and the gateway is configured to 9600 baud, the maximum speed of connection between fax units and the gateway will be limited at 9600 baud. And vice versa, if fax units support data transfer at 9600 baud, and the gateway is configured to 14400 baud, this setting will not affect the interaction, maximum speed will be defined by the performance of fax units.

Jitter buffer configuration

In *'Jitter buffer configuration'* section, you may configure jitter buffer parameters.

Due to various factors, e.g. network overload, voice data packets may be served to the gateway at different speeds, and their arrival order may change. In order to compensate the jitter effect, the jitter buffer has been implemented. In jitter buffer, packets are saved as soon as they are received. Voice packets that came out of sequence (earlier or later) have their sequential number analyzed. After that, they are positioned into their respective places in a queue and sent further in the right order that allows to improve call quality for unstable communication channels.

Jitter buffer may be fixed or adaptive. The size of adaptive jitter buffer changes along with the average identified delay in voice packets' reception. When delay rises, the size of adaptive jitter buffer grows instantaneously, when delay lowers, buffer size shrinks in 10 seconds after the delay has been steadily reduced.

In ***'Modem/Fax pass-thru'*** section, you may configure the jitter buffer in fax/modem data transfer mode.

- *Delay* – the size of a fixed jitter buffer, used in fax or modem data transfer mode. Permitted value range is from 0 to 200ms.

'Voice' – jitter buffer voice connection settings.

- *Mode* – jitter buffer operation mode: fixed or adaptive;

- *Delay* – size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer. Permitted value range is from 0 to 200ms.

- *Delay max* – upper limit (maximum size) of adaptive jitter buffer, in milliseconds. Permitted value range is from 'Delay' to 200ms.

– *Deletion threshold* – threshold for immediate deletion of a packet, in milliseconds. When buffer size grows and packet delay exceeds this threshold, packets will be deleted immediately. Permitted value range is from 'Delay max' to 500ms;

– *Deletion mode* – buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit. In 'SOFT' mode, device uses intelligent selection pattern for deletion of packets that exceed the threshold. In 'HARD' mode, packets which delay exceeds the threshold will be deleted immediately.

To discard all changes made to configuration, click the *Undo All Changes button.* To discard all changes made to configuration, click the Undo All Changes button. To set default parameters, click the *Defaults* button (the figure below shows default values). To apply changes, click the *Submit Changes* button.

To store changes to non-volatile memory of the device, click the *Save* button.

5.1.2.2.5 The 'Routing and Pickup Code Configuration (Profile n/Dialplan)' submenu

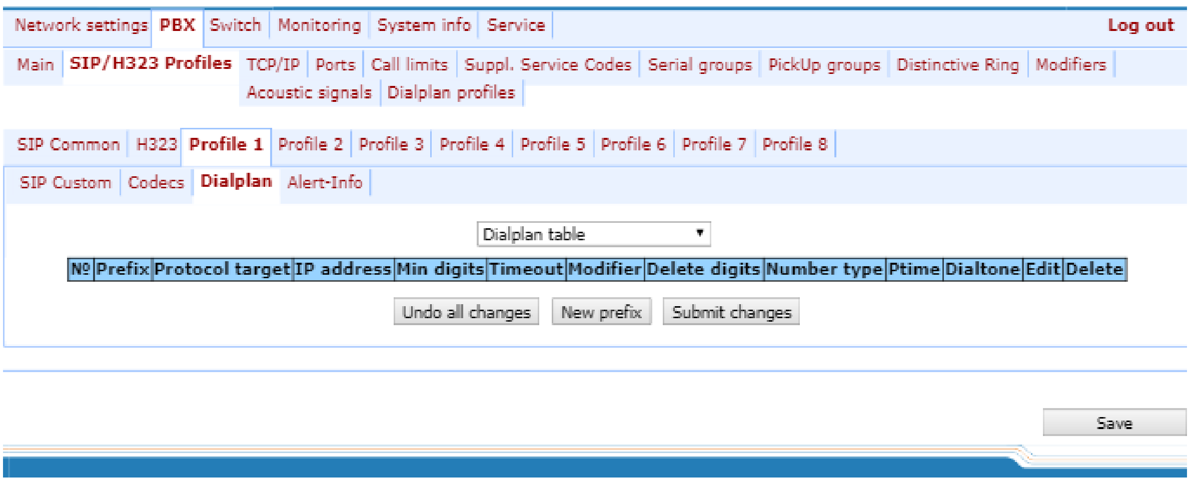
In the *'Profile n/Dialplan'* submenu, you may configure prefixes for routing and pickup groups for each profile.

TAU-72.IP/TAU-36.IP gateway **routing** is built on prefixes. Prefix is the first part of the callee number, and when it is combined with the quantity of digits of a dialed number and the dialling timeout, it comprises the routing rule. If a number dialed by the subscriber falls within the scope of a single rule, the call will be routed by this rule. If a dialed number falls within the scope of multiple rules, the call will be routed by the rule with the highest priority. When dialed number does not match any rules, busy tone will be played to the subscriber.

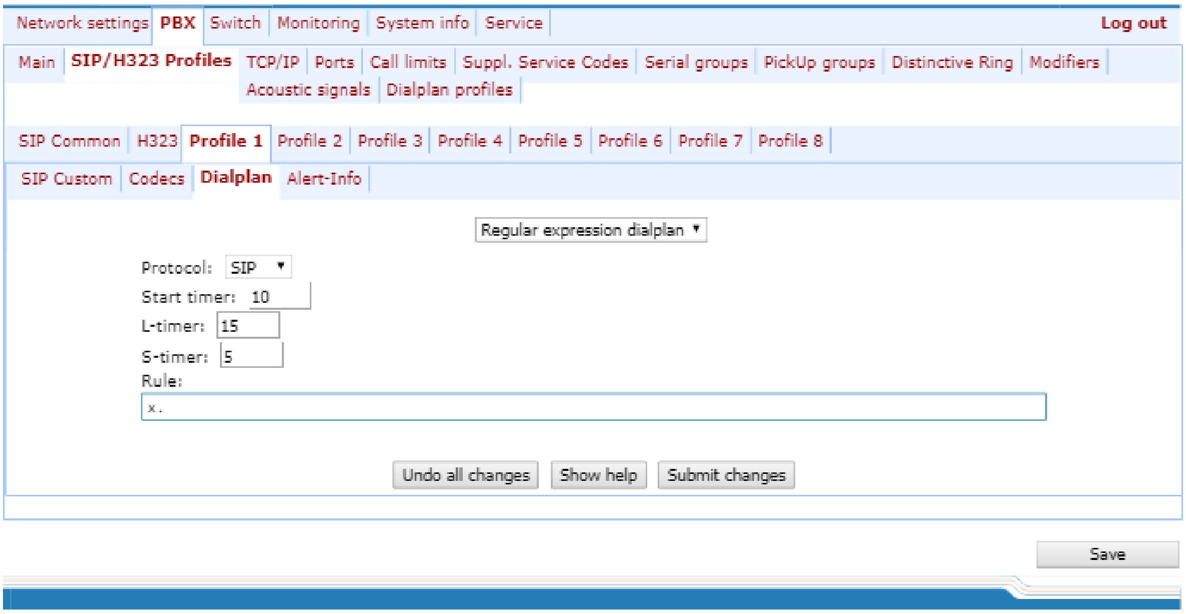
When SIP-proxy operates in outbound mode, all calls are routed via SIP-proxy; configuration of prefixes is optional in this case. In the absence of prefixes, the quantity of digits in the dialed number is not limited, and the end of dialling occurs on the expiration of 'outbound' timer, or on '#' button pressed (in case when Stop dial *at #* function is enabled on subscriber port). If you have to use outbound mode without the wait for the end of dialling on 'outbound' timer, you will have to configure prefixes.

Pickup group – subscriber group, authorized to receive (or intercept) any calls directed at another subscriber of the group.

Dialplan Table – table of routing prefixes' settings; for parameter description, see Section 5.1.2.2.5.1.



Regular Expression Dialplan–configuration of routing prefix through regular expressions, description of regular expressions format is given in Section 5.1.2.2.5.4.

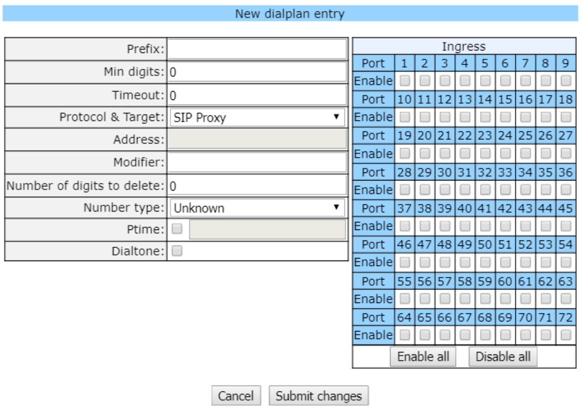


After implementation of changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

5.1.2.2.5.1 Routing rules configuration

Hover the mouse cursor over a row and left-click it to highlight with orange and make it active (available for moving). Use arrow buttons (up, down) to change the prefix sequence order. The higher the prefix row in configuration, the higher its priority.

To add a new prefix, click the *New prefix* button:



– *Prefix*;

– *Min digits* – minimum length of a number dialed by the prefix;

– *Timeout* – dialling timeout for the next digit of a number, in seconds. Begins operation, when the minimum length of a number dialed by the prefix is achieved. If the minimum length of a dialed number is already achieved, and no digits have been dialed during this timeout, the call is routed by the prefix. In order to route the call immediately on dialling the minimum length of a number, specify 0 as a dialling timeout for the next digit of a number;

– *Protocol&Target* – signalling protocol, used in prefix operations:

- *H.323 Gatekeeper* – H.323 protocol operation through the gatekeeper (possible for profile 1 only);
- *H.323 Direct IP* – H.323 point-to-point protocol operation (possible for profile 1 only);
- *SIP Proxy* – SIP protocol operation via SIP-proxy;
- *SIP Direct IP* – SIP point-to-point protocol operation;
- *SIP-T Direct IP* – SIP-T point-to-point protocol operation;
- PickUp Group – *pickup group;*

– *Address* – IP address of a communicating gateway in point-to-point operation mode (specified when H.323 Direct IP /SIP Direct IP is used);

– *Modifier* – dialling modifier, enables translation of a callee number. Modifier is added at the beginning of a dialed number.

– *Number of digits to delete* – dialling modifier, enables translation of a callee number. Defines the number of digits to be deleted from a dialed number for outgoing calls (the most significant digits of a number will be removed);

When outgoing call is performed using a prefix, the digit deletion modifier ('Number of digits to delete') is applied first to the dialed number, followed by the digit addition modifier ('Modifier').

– *Number type* – callee number type. Used only in SIP-T and H.323 protocol operations. Transferred in CdPN parameter;

– *Ptime* – when checked, defines the packetization time for the current direction, in seconds;

– *Dial tone* – send 'PBX response' tone when the first prefix digit is dialed. Usually, used with a prefix beginning with '8' to send the 'PBX response' tone for a long-distance direction. If there are multiple prefixes beginning with the same digit, but having different configurations of this setting, then a prefix with the highest priority will be responsible for determining whether the 'PBX response' tone will be sent or not;

To apply changes, click the *Submit Changes* button; to discard all changes, click *'Cancel'*.

To edit parameters of existing prefix, you may directly modify data in fields, of call the edit menu by clicking button in the respective row. To delete a prefix, click button.

To discard all changes made to configuration, click the *Undo All Changes* button. To apply changes, click the *Submit Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

5.1.2.2.5.2 Configuration of Prefix with Varying Number Count

Enables dialling by a single prefix with various quantity of digits using Dialplan Table. Prefix should be configured as follows:

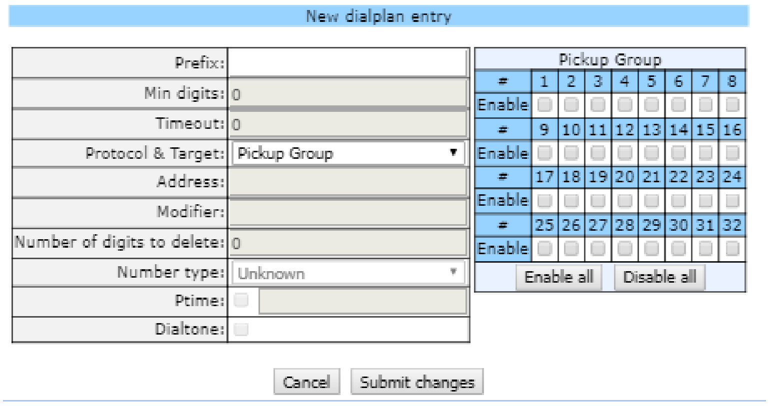
1. In *'Min digits'* field, enter a minimum quantity of digits for routing with this prefix;
2. In 'Timeout' field, dialling timeout for the next digit of a number should be greater than zero. In this case, when user dials the number with length that matches the minimum quantity of digits, gateway will wait for the next digit dialling during the specified timeout. If the digit is not dialed, prefix call will be performed with the minimum quantity of digits; if the digit is dialed, the timer will restart, and the gateway will wait again for the next digit dialling.

3. If dialling timeout for the next digit is zero, the call will be routed immediately when the length of a number equal to minimum quantity of digits is achieved.

4. *'Stop dial at #'* function allows to perform a call after the necessary quantity of digits are dialed without the wait for a timeout. It may be configured separately for each port in *'PBX/Ports/Edit/Custom'*. If this function is enabled for the port, user upon dialling a necessary number, the port may press # button on the phone unit (provided that the unit is configured for DTMF dialling mode), and after that the call will be routed immediately.

5.1.2.2.5.3 Configuration of pickup codes

Configuration of pickup groups affects the following settings:



– *Prefix* – pickup code. Sequence of digits (for example, *8) that, when dialed, allows any subscriber of the group to pickup the call received by another subscriber of the group;

– *Protocol&Target* – it's necessary to select a pickup group–PickUp;

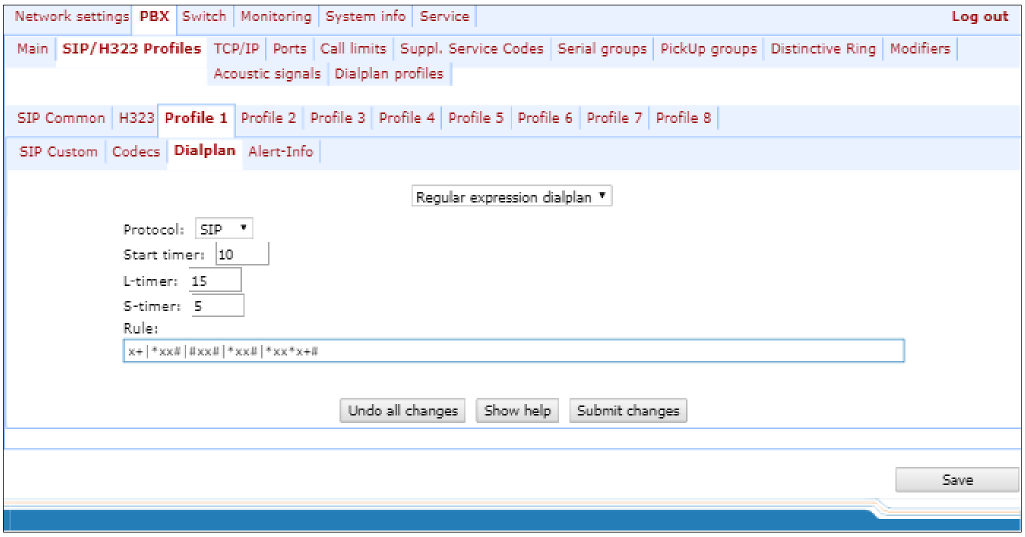
– *PickUp Group* – defines the list of groups, that will use this code for the call pickup. Thus, a single code may be used for call pickups in different groups.

To enable this pickup code for all groups, click the *Enable all* button. To disable this pickup code for all groups, click the *Disable all* button.

5.1.2.2.5.4 Configuration of Regular Expression Routing Rules

This section describes the configuration of regular expression routing rules.

To open the configuration page for regular expression routing rules, select *'Regular Expression Dialplan'* from the *'Dialplan'* drop-down list:



– *Protocol* – VoIP protocol name: H.323, SIP (H.323 may be used in profile 1 only);

– *L-timer* – activates, when the gateway detects the necessity of dialling of at least one more digit in order to achieve the compliance with any of the dialplan rules;

– *S-timer* – activates, when the dialling complies with one of the rules, but there is a possibility that further dialling will achieve compliance with another rule;

– *Rule* – field for routing rules written with regular expressions (up to 1000 characters). The structure and format of regular expressions that enable different dialling features are listed below.

Regular expression routing plan record rule ('Rule'):
Rule1| Rule2|..| RuleN
Rule= L{value} S{value} prefix@optional(parameters)

where:

L – L-timer (optional parameter),
S – S-timer(optional parameter).
Timers inside rules could be dropped; in this case, global timer values, defined before the parentheses, will be used.
Prefix–prefix part of the rule
@optional–optional part of the rule (may be skipped)
(parameters) – additional parameters (can be omitted)

Regular expressions' syntax

Prefix part of the rule

- **|** – logical **OR** – used to separate rules.
- **X** or **x** – any number from 0 to 9, equal to a range [0-9];
- **0** – **9** – numbers from 0 to 9;
- **'A', 'B', 'C', 'D'**–'A', 'B', 'C', 'D' characters;
- *****;
- **#**;
- **[ ]** – define ranges (with a hyphen), or enumeration (w/o spaces, commas, and other characters between the digits), e.g.

Range: **[1-5]** – 1,2,3,4, or 5;
Enumeration: **[138]** – 1,3, or 8;
Range and enumeration **[0-9*#]** – 0 to 9, and also * and #.

- **{min,max}** – define the repetition count for a character located outside the parentheses, a range or *# symbols.
  Min–minimum repetition count, *max*–maximum repetition count.

  {,max} – equal to {0,max};
  {min,} – equal to {min,inf}.

  Example:
  5{2,5} – '5' could be dialed up to 5 times.
  Equal to the following record: 55|555|5555|55555

- . – 'dot' special symbol means that a preceding digit, range, or '*', '#' characters may be repeated from one to infinity times. Equivalent to a record {0,}
  Example:
  5x.* – 'x' in this rule may be completely absent or may be present any number of times. Equivalent to a record 5*|5x*|5xx*|5xxx*|...

- **+** – digit, range, or '*', '#' characters preceding the '+' symbol may be repeated from one to infinity times. Equivalent to a record {1,}.

- **<:>** – modification of a number. Digits and '*', '#' characters preceding the colon will be replaced with those after the colon. Modification allows to remove **(<xx:>)**, add **(<:xx>)**, or replace **(<xx:xx>)** digits and symbols.

- **!** – dial block. Specified at the end of a rule and means that the dialling of numbers corresponding to the template will be blocked.

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

  8,**x**. – after dialling '8' subscriber will hear 'PBX response' tone.

- w – pause symbol for pulse dialing, equal to 0.5 seconds (supported on FXO ports). It is allowed to indicate up to 10 characters of a pause in a row, which is equivalent to a pause of 5 seconds, if one character is regarded as 0.5 seconds. Designed to interact with a gateway that has FXO ports and allows you to transfer the length of a pause for dialing to the opposite side. If the interacting party supports the processing of w symbols, then upon receipt of a request containing these symbols, it will withstand a pause (by the number of w symbols) in the FXO line when dialing by the pulse method.

- **'S', 'T'** – short (S) or long (T) timers are used in rules containing special repetition characters '{min,max}', '.', or '+' and are specified right after them. They define, which timer will work for the current rule when it is already possible to perform the the routing for the dialed number. If the timer is not specified, S-timer will be used by default. Allows to replace S-timer with L-timer in the current profile.

Optional part of the rule (may be skipped)

- **host:port** – routing to IP address. Usage of a port is effective for SIP protocol only. If @host:port is not specified, calls will be routed via SIP-proxy or H.323 gatekeeper.
  Example:
  1xxxx@192.168.16.13:5062–all five-digit dials, beginning with 1, will be routed to IP address 192.168.16.13 to port 5062

- **{pickup:x,xx}** – pickup group code dialling. You may specify multiple pickup groups using comma.
  Example:
  ***8@{pickup:1}** – '*8' code is used for the first pickup group

- **{local}** – routing inside the gateway to a local IP address. Must be used for internal routing, when the device receives its network settings dynamically (via DHCP protocol).

Additional parameters

Format: **(param1: value1, .., valueN; .. ;paramN: value1, .., valueN)**

- *param* – parameter name, several parameters are separated with a semicolon, all parameters are placed in common round brackets;
- *value* – parameter value, multiple values of one parameter are separated with a comma.

Valid parameters and their values

- *codecs parameter* – determines the list of codecs that will be used when making an outgoing call under the routing rule. It can take the following values: g711a, g711u, g723, g729x, g729b, g726_32.
  Example:
  (codecs: g711a, g711u).
  Note: in the given rule g729a codec is recorded as g729x;
- *profile parameter* – determines the 'routing profile' with the parameters of which the call will be made (see Section 5.1.2.12 The 'Dialplan profiles' submenu). It can take one of the following values: 1, 2, 3, 4. Example: (profile: 1).

Timers

- **S-timer** – activates, when the dialling complies with one of the rules, but it is possible that further dialling will achieve compliance with another rule;
- **L-timer** – activates, when the gateway detects the necessity of dialling of at least one more digit in order to achieve the compliance with any of the dialplan rules.

Timer values may be specified for a complete routing plan, as well as for the specific rule. Timer values may be specified for all templates in a routing plan; in this case values are listed before the opening parenthesis.

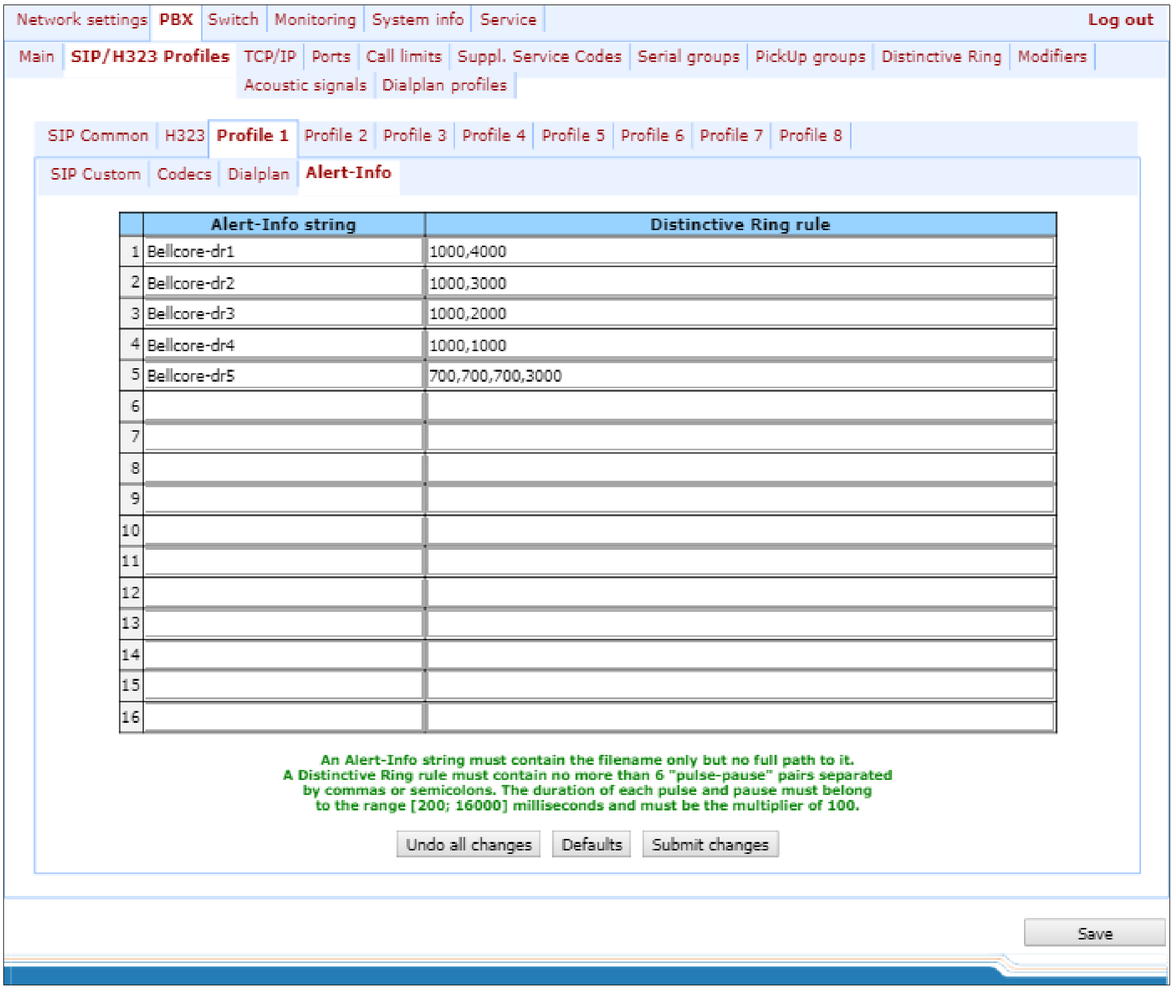
If these values are listed in one sequence only, they are effective only for this sequence.

Example of the dialplan record

```
L208,x.|520001@192.168.16.150:5061|52xxx[02-9]|1xxxx|<53:70>xxxx@192.168.16.13|
26x{,5}|*8@{pickup:1,6,32}|3[0-3]x+|34*{1,3}|35#x{0,}|36x.*|37[0-2]x+T
```

5.1.2.2.6 Alert-Info distinctive ring

In the *'Alert Info'* submenu, you may configure a distinctive ring, generated by the value from Alert Info header received in INVITE request. 16 various Alert Info values may be processed for each profile.



– *Alert-Info string* – signal name sent in Alert-Info header;

  Alert Info header appears as follows*: <http://ipaddr/signal>,*

  where:

  – *ipaddr* – IP address of a device, that the signal should be played from (not processed at TAU);

  – *signal* – signal name that should be used for generation of non-standard ringing.

– *Distinctive Ring rule* – non-standard ringing generation rule. Ringing tone is cyclic.

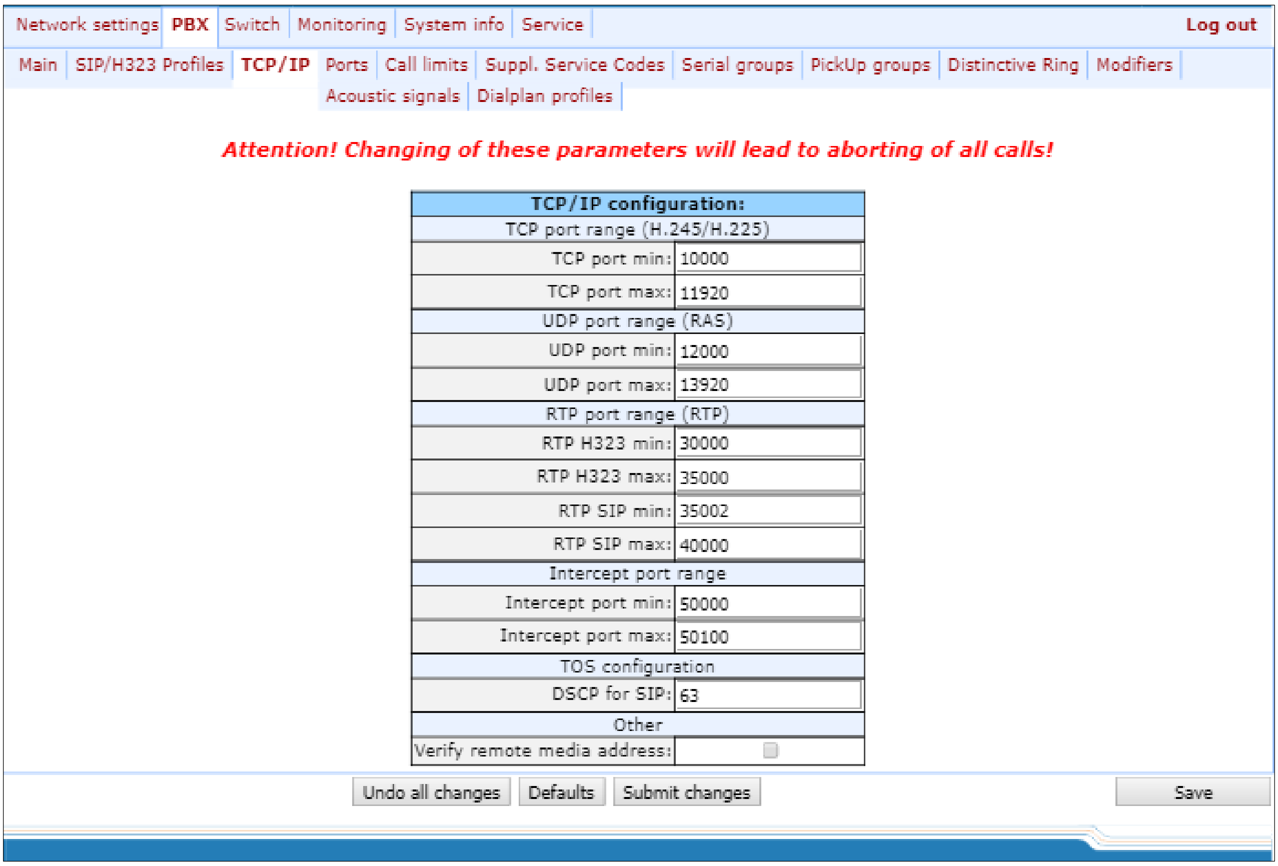
The rule includes up to 6 pairs of impulse/pause values; all values are comma-separated. Each value must be divisible by 100 and fall within the range from 200 to 16000ms.

For example, a record '700,700,700,3000' means that 700ms impulse will be sent first, followed by 700ms pause, then again 700ms impulse, 3s pause; after that, this sequence will be repeated.

5.1.2.3 The 'TCP/IP' submenu. Configuration of network ports

In *TCP/IP* submenu, you may configure network port range for various protocols.

You don't have to reboot the gateway in order to apply TCP/IP settings. When applying settings, all current calls will be terminated!



After implementation of changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

<u>*TCP/IP configuration:*</u>

– *TCP port range (H.245/H.225)* – range of network ports used for H.323 - H.245/H.225 stack protocols' operation:

- *TCP port min*–the lower limit of a TCP port range;
- *TCP port max*–the upper limit of a TCP port range.

– *UDP port range (RAS)*–range of network ports used for H.323 stack RAS protocol operation (RAS protocol is used during gatekeeper interactions):

- UDP port min–*the lower limit of a UDP port range.*
- UDP port max–*the upper limit of a UDP port range.*

– *RTP port range (RTP)*–range of network ports used for voice data protocol (RTP) operation:

- *RTP H323 min*–the lower limit of a range of RTP ports used for H.323 protocol operation;
- *RTP H323 max*–the upper limit of a range of RTP ports used for H.323 protocol operation;

- *RTP SIP min*–the lower limit of a range of RTP ports used for SIP protocol operation;
- *RTP SIP max*–the upper limit of a range of RTP ports used for SIP protocol operation.

– *Intercept port range*–range of network ports used for pickup traffic transmission (SORM):

- *Intercept port min*–the lower limit of a range of ports used for pickup traffic transmission (SORM feature);
- *Intercept port max*–the upper limit of a range of ports used for pickup traffic transmission (SORM feature).

SORM feature implementation is based on *rfc3924 recommendation–Cisco Architecture for Lawful Intercept in IP Networks.* To perform the pickup, the following MIBs are used: CISCO-IP-TAP-MIB.my and CISCO-TAP2-MIB.my.

– *Diffserv configuration;*

- *DSCP for SIP*–type of service for SIP packets. DSCP bits are the 6 high bits of the Diffserv field that is sent in IP protocol header; parameter value should be specified decimally. For utilized values, see Table below.

– *Other:*

- *Verify remote media address*–when checked, apply control to the media traffic received, otherwise it will not be controlled. This function controls the received media traffic (voice traffic, T38 fax) for established connection. If this traffic comes in from the host or port not specified in SIP/H.323 signalling exchange, it will be rejected.

To avoid the conflicts, ports used by H.225/H.245/RAS signalling and RTP should not overlap the ports used by SIP signalling (5060 by default, and also ports configured in 'ports' and 'serial groups' tabs.)

Table 8 – 'Type of service' (DSCP) field value:

DSCP parameter value	Description
0 (0x00)	Best effort – default value;
8 (0x08)	class 1;
10 (0x0A)	assured forwarding, low drop precedence (Class1, AF11);
12 (0x0C)	assured forwarding, low drop precedence (Class1, AF12);
14 (0x0E)	assured forwarding, low drop precedence (Class1, AF13);
16 (0x10)	class 2
18 (0x12)	assured forwarding, low drop precedence (Class2, AF21);
20 (0x14)	assured forwarding, low drop precedence (Class2, AF22);
22 (0x16)	assured forwarding, low drop precedence (Class2, AF23);
24 (0x18)	class 3
26 (0x1A)	assured forwarding, low drop precedence (Class3, AF31);
28 (0x1C)	assured forwarding, low drop precedence (Class3, AF32);
30 (0x1E)	assured forwarding, low drop precedence (Class3, AF33);
32 (0x20)	class 4
34 (0x22)	assured forwarding, low drop precedence (Class4, AF41);
36 (0x24)	assured forwarding, low drop precedence (Class4, AF42);
38 (0x26)	assured forwarding, low drop precedence (Class4, AF43);
40 (0x28)	class 5
46 (0x2E)	expedited forwarding, low drop precedence (Class5, Expedited Forwarding);
IP Precedence:	
0 (0x00)	IPP0 (Routine)
8 (0x08)	IPP1 (Priority)

16 (0x10)	IPP2 (Immediate)
24 (0x18)	IPP3 (Flash)
32 (0x20)	IPP4 (Flash Override)
40 (0x28)	IPP5 (Critical)
48 (0x30)	IPP6 (Internetwork Control)
56 (0x38)	IPP7 (Network Control)

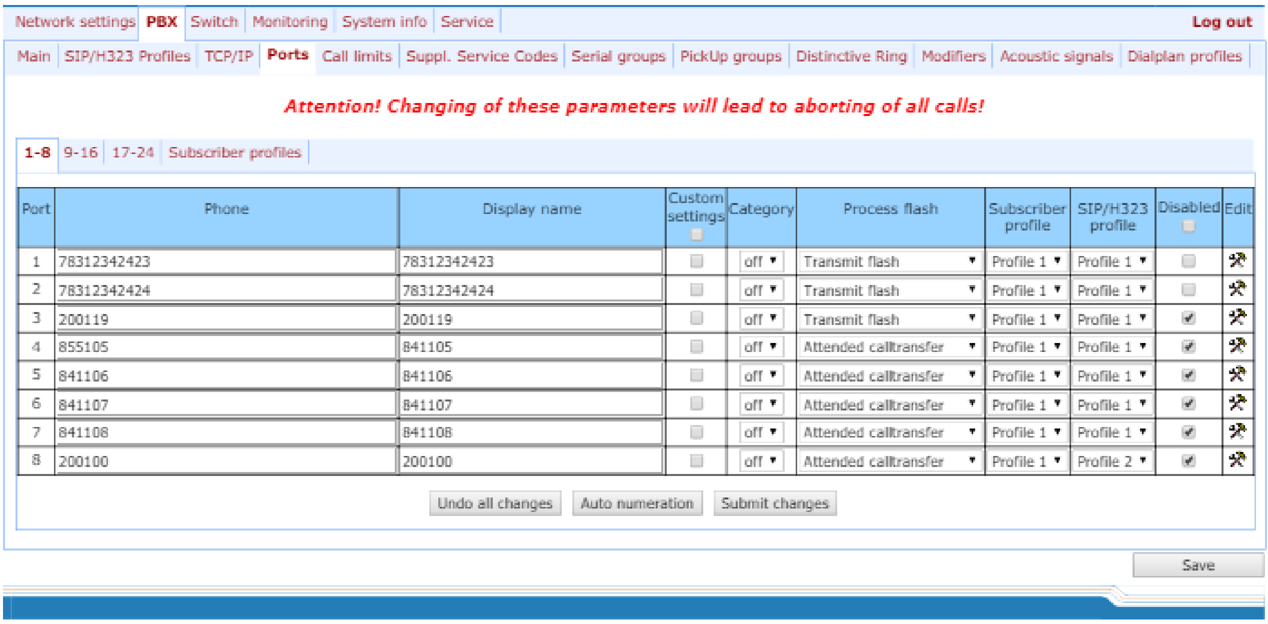
To discard all changes made to configuration, click the *Undo All Changes button.* To set default parameters, click the *Defaults* button (the figure below shows default values). To apply changes, click the *Submit Changes* button.

5.1.2.4 The 'Ports Configuration of Subscriber Ports' submenu (Ports)

In the *'Ports'* submenu, you may configure subscriber ports of the device.

You may use up to 8 subscriber profiles to configure the following port settings: *CallerID mode, Flash impulse duration, signal levels strengthening/weakening, priority between CFB and CW services, 'Music on hold' service, payphone mode.* In *'Subscriber profile'* item of the *'Custom' tab, you may assign one of the configured subscriber profiles to each port.* Profile 1 is assigned for all ports by default. To open the subscriber profile configuration window, click *'Subscriber profiles'* in *'PBX/Ports' tab.* If you have to configure a custom value for any of the parameters listed above, you have to configure it in *'PBX/Ports'* menu by clicking 'Edit /Common' button. To use custom settings, it is absolutely necessary to select 'Custom' checkbox (in *'PBX/Ports'* tab – 'Edit /Custom' or *'PBX/Ports'*) in the port configuration!

You don't have to reboot the gateway in order to apply port settings. Changing *'SIP port'* parameter will lead to termination of current calls. Changing other parameters will not disrupt any of the established connections!



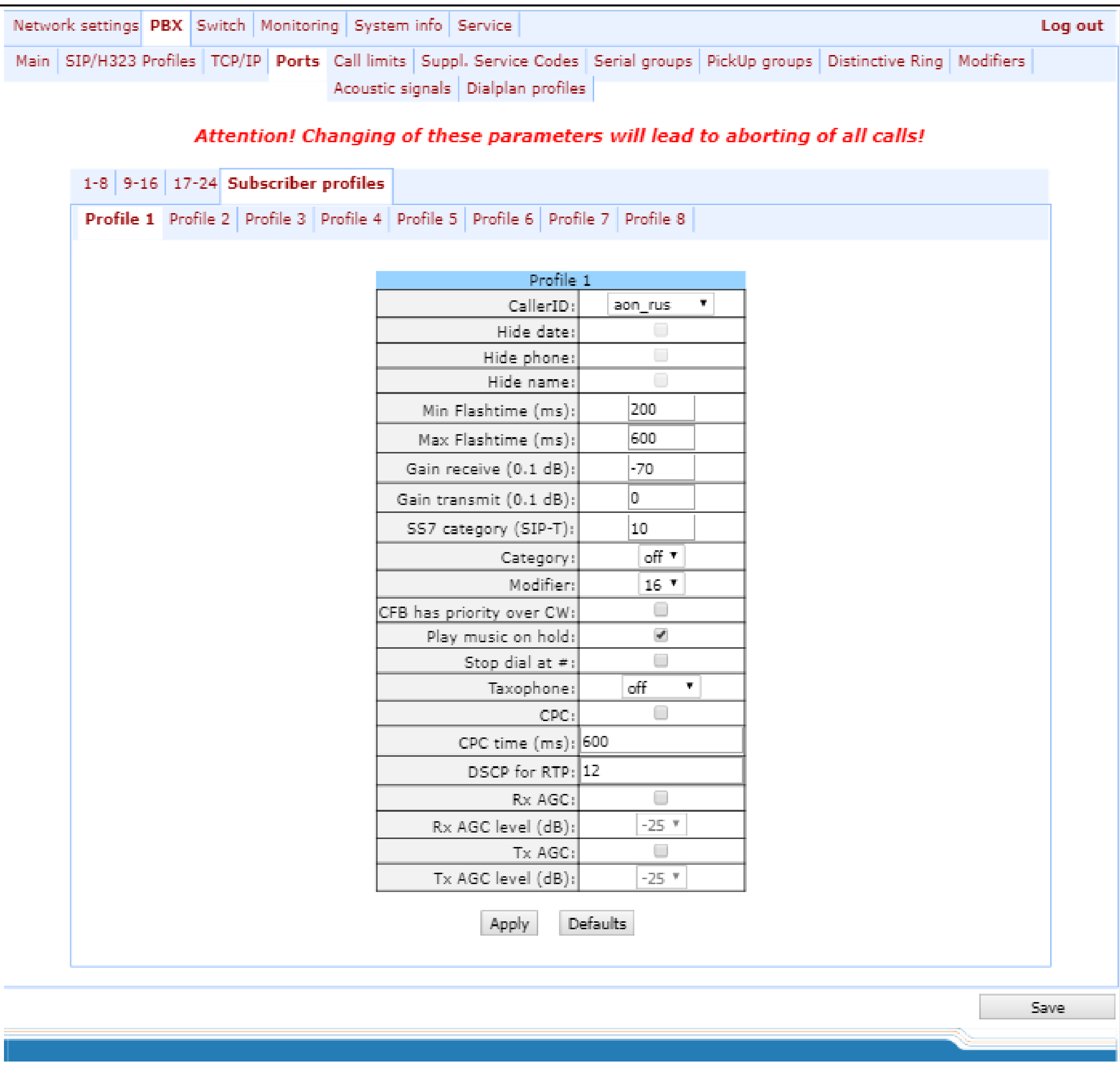
After implementation of changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

Configuration of ports

- *Port* – port number;
- *Phone* – subscriber's number;
- *Display name* – subscriber's name;
- *Custom* – when checked, use common settings for this port (configured by clicking the Edit button), otherwise use settings from the specified subscriber profile (configured in 'Subscriber profiles' tab);
- *Category* – select subscriber's category (cpc-rus), off–subscriber category will not be used. When this setting is enabled, the category will be sent in 'from' field, and 'tel uri' will be used instead of 'sip uri';
- *Process flash* – flash function operation mode (short clearback). For parameter description, see below;
- *Subscriber profiles* – number of the subscriber profile, which parameters will be used for the current port (use 'PBX/Ports/Subscriber profiles' tab to configure subscriber profile parameters);
- *SIP/H323 profile* – SIP/H323 profile number, that will be used for the current port;
- *Disabled* – when checked, the port is disabled, otherwise it will be enabled. To disable the service for ports, select checkboxes against the desired ports and click the Submit Changes button;
- *Edit*  – the button which allows you to enter the port settings editing mode;
- *Auto numeration* – automatic port enumeration.

Settings of subscriber profiles

You may configure subscriber profiles in *'Subscriber profiles'* tab:



Profile 1

– *CallerID* – select the Caller ID mode from the drop-down list. For Caller ID operation, subscriber's phone unit must support the selected method:

- *Off* – Caller ID is disabled;
- *Aon_rus* – 'Russian Caller ID' method. The number is served when subscriber's phone unit lifts the headset with its 500Hz frequency request;
- *Dtmf* – DTMF Caller ID method. The number is served between the first and second calls on the line by dual-frequency DTMF impulses;
- *Fsk_bell202, Fsk_v23*–FSK Caller ID method (using bell202 standard, or ITU-T V.23). The number is served between the first and second calls on the line by a stream of data with a frequency modulation;

To enable Caller ID information reception, connected phone unit should support the configured Caller ID method.

In Fsk_bell202, Fsk_v23 modes, Caller ID information is sent in MDMF format: time/date, subscriber's number and name.

– *Hide date* – when checked, in Fsk_bell202, Fsk_v23 modes, Caller ID information will be sent without time and date;

– *Hide phone* – when checked, in *Fsk_bell202, Fsk_v23* modes, Caller ID information will be sent without subscriber's number;

– *Hide name* – when checked, in Fsk_bell202, Fsk_v23 modes, Caller ID information will be sent without subscriber's name;

– *Min Flashtime(ms)* – the lower limit of Flash impulse duration (ms);

– *Max Flashtime(ms)* – the upper limit of Flash impulse duration (ms);

For correct operation of Flash button on the subscriber's phone unit, its configured duration of flash dialling should fall within the following range: (Min Flashtime – Max Flashtime). Please note, that small values (70-20ms) of the lower limit may lead to situations, when dialling of digits in pulse phone unit operation mode will be interpreted as flash dialling. When the upper limit value is less than flash dialling duration configured for the subscriber's phone unit, pressing flash button will cause the clearback.

If there is no effect (no 'PBX response' tone, indicating that the Hold service is performed) or the subscriber clearback occurs when you press the 'Flash' button, it means that configured 'Flash' settings for this port do not match the 'Flash' impulse generated by the phone unit, or 'Flash' is not processed by the gateway (Attendant CT, unattendant CT). If the *'Flash – Transmit flash'* impulse transmission mode has been configured, the absence of the effect may also mean that the opposite gateway is not processing 'Flash' received from the IP network.

– *Gain receive (0.1 dB)* – volume of voice reception (gain of the signal received from the communicating gateway and output to the speaker of the phone unit connected to TAU-72.IP/TAU-36.IP gateway);

– *Gain transmit (0.1 dB)* – volume of voice transmission (gain of the signal received from the microphone of the phone unit connected to TAU-72.IP/TAU-36.IP gateway and transmitted to the communicating gateway);

– *SS7 category (SIP-T)* – SS-7 category, sent in the SIP-T encapsulated message of SS-7 protocol. Corresponding Caller ID categories are listed in the table below.

Caller ID category	**SS-7 category**
1	10
2	225
3	228
4	11
5	226
6	15
7	227
8	12
9	229
10	224

– *Category* – select subscriber's category (cpc-rus), off–subscriber category will not be used. When this setting is enabled, the category will be sent in 'from' field, and 'tel uri' will be used instead of 'sip uri';

– *Modifier* – modifier table number, used for the current port;

- *CFB has priority over CW* – defines the priority between CFB (Forward on busy) and CW (Call wait) services. When checked, CFB service has a priority over CW, and vice versa;

- *Play music on hold* – use 'Play music on hold' service. When 'Hold' service is performed by this port, audio file stored in the gateway memory will be played to the opposite subscriber. When unchecked or the audio file is unavailable, 'hold' audio signal will be played to the opposite subscriber. To upload the audio file, use 'Service -> MOH' menu.

- *Stop dial at #* – when checked, use '#' button on the phone unit to end the dialling, otherwise '#' will be recognized as a DTMF symbol. When '#' is used to end the dialling, the call will be performed without the dialling timeout for the next digit;

- *Taxophone* – port operates in payphone mode:

  - *Off* – port operates in normal mode;
  - *Polarity* – payphone operation mode with polarity reversal. Perform line power polarity reversal on subscriber's response, and return it to original state on clearback;
  - *12kHz* – payphone mode without polarity reversal. Generates 12 kHz meter pulse;
  - *16kHz* – payphone mode without polarity reversal. Generates 16 kHz meter pulse.

- *CPC* – when checked, perform a short-time break of the subscriber loop on clearback from the opposite subscriber's side;

- *CPC time(ms)* – duration of a short-time break of the subscriber loop;

- *DSCP for RTP* – type of service for RTP packets. DSCP bits are the 6 high bits of the Diffserv field that is sent in IP protocol header; parameter value should be specified decimally. For utilized values, see Table .

- *Rx AGC* – when selected, a received signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise—the amplification will not be carried out;

- *Rx AGC Level* – determines the value of the level to which an analogue signal will be amplified when receiving (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB);

- *Tx AGC* – when selected, a transmitted signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise—the amplification will not be carried out;

- *Tx AGC Level* – determines the value of the level to which an analogue signal will be amplified when transmitting (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).

To apply settings, click the *Apply* button. To exit the submenu, click the *Cancel* button. To reset settings to default values, click the *Default* button.

Automatic enumeration

Click the *Auto numeration* button in *'Ports conf.'* window to show the following menu:

Auto numeration	
Prefix:	
First number:	
Postfix:	

Port 1	700000	Port 2	700001	Port 3	700002	Port 4	700003
Port 5	700004	Port 6	700005	Port 7	700006	Port 8	700007
Port 9	700008	Port 10	700009	Port 11	700010	Port 12	700011
Port 13	700012	Port 14	700013	Port 15	700014	Port 16	700015
Port 17	700016	Port 18	700017	Port 19	700018	Port 20	700019
Port 21	700020	Port 22	700021	Port 23	700022	Port 24	700023
Port 25	700024	Port 26	700025	Port 27	700026	Port 28	700027
Port 29	700028	Port 30	700029	Port 31	700030	Port 32	700031
Port 33	700032	Port 34	700033	Port 35	700034	Port 36	700035
Port 37	700036	Port 38	700037	Port 39	700038	Port 40	700039
Port 41	700040	Port 42	700041	Port 43	700042	Port 44	700043
Port 45	700044	Port 46	700045	Port 47	700046	Port 48	700047
Port 49	700048	Port 50	700049	Port 51	700050	Port 52	700051
Port 53	700052	Port 54	700053	Port 55	700054	Port 56	700055
Port 57	700056	Port 58	700057	Port 59	700058	Port 60	700059
Port 61	700060	Port 62	700061	Port 63	700062	Port 64	700063
Port 65	700064	Port 66	700065	Port 67	700066	Port 68	700067
Port 69	700068	Port 70	700069	Port 71	700070	Port 72	700071

In the opened window, you may perform enumeration using a mask. In the *'First number'* field, enter *XXXX* number for the first port. All other ports will be enumerated by the following rule:

XXXX + 1×N,

where:

N–port number,
Prefix and **postfix**–constant parts, added in the beginning and in the end of a number.

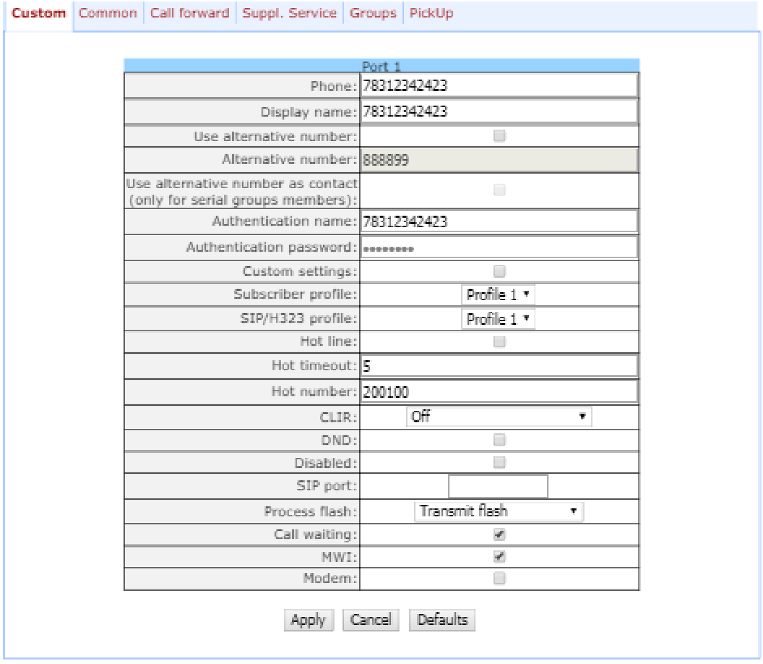
To start enumeration, click the *Start* button.

To return to *'Ports conf.'* menu, click the *Back* button.

Editing custom parameters of FXS type ports:

To edit parameters of a specific port, click button in the corresponding row.

'Custom' tab–FXS type port custom settings:



- *Phone* – subscriber's number;
- *User name* – subscriber's name;
- *Use alternative number* – when checked, use alternative number; otherwise it will not be used. May be used, when the gateway operates as a PABX, to assign a single subscriber's number to multiple phone lines;
- *Alternative number* – alternative subscriber's number. This number will be an alternative Caller ID of a subscriber and will be displayed on the subscriber's Caller ID display (transferred in the 'from' field URI in SIP protocol operations);
- *Use alternative number as contact (only for serial groups members)* – use an alternative number as a subscriber's contact (transferred in 'contact' header via SIP protocol). This setting is used only for ports located in the call group;
- *Authentication name* – username used for authentication. Used in SIP protocol operations, when in *'PBX/SIP-H323 Profiles/Profile n/SIP Custom'* menu the independent authentication mode is selected (Authentication – user defined);
- *Authentication password* – password used for authentication. Used in SIP protocol operations, when in *'PBX/SIP-H323 Profiles/Profile n/SIP Custom'* ***menu the independent authentication mode is selected*** *(Authentication – user defined);*
- *Custom* – when checked, use common settings for this port (configured by clicking the *Edit* button), otherwise use settings from the specified subscriber profile (configured in *'Subscriber profiles' tab).* When checked, selection of the subscriber profile will be unavailable for this port.
- *Subscriber profiles* – number of the subscriber profile, which parameters will be used for the current port (use *'PBX/Ports/Subscriber profiles'* tab to configure subscriber profile parameters);
- *SIP/H323 profile* – SIP/H323 profile number, that will be used for the current port;

– *Hotline/warmline* – when selected, Hotline/warmline service is enabled. This service allows to establish an outgoing connection automatically without dialling the number right after the lifting of a headset – 'hot line', or with a delay – 'warm line'. Direction of a service–from analogue phone line to VoIP;

This setting will not work, if 'IMS mode'–*'Enable IMS'* parameter in SIP profile settings–is enabled on the device.

– *Hot timeout* – delay timeout in seconds for the start of the automatic dialling when the 'warmline' service is enabled;

– *Hot number* – number that will receive the call when 'Hotline/warmline' is enabled;

– *CLIR* – calling line identification restriction service – when SIP:from value is set, subscriber's nimber will be hidden only in the 'from' field. When SIP:from and SIP:contact values are set, subscriber's number will be hidden both in the 'from' field and in the 'contact' field. When operating via H.323, the number will be hidden regardless of SIP values set: SIP:from, SIP:from or SIP:contact;

– *DND* – when checked, 'do not disturb' service (temporary restriction for incoming calls) is enabled;

– *Disabled* – when checked, the port is disabled;

– *SIP port* – local UDP port used for port operations via SIP protocol;

– *Process flash* – flash function operation mode (short clearback). When 'flash' button is pressed on the subscriber's phone unit – if the duration of dialling falls within the range (Min Flashtime – Max Flashtime)– there are several gateway behaviours:

- *Transmit flash* – transmit flash into the channel using method described in *'Flash Transfer'* item of the codec configuration (*Codecs conf.)* In this case, flash dialling will be processed by the communicating gateway;
- *Attended call transfer* — 'Call Transfer' service is enabled for the port with the wait for response of the subscriber, the call is being forwarded to. In this case, flash dialling will be processed locally by the gateway;
- *Unattended call transfer*— 'Call Transfer' service is enabled for the port without the wait for response of the subscriber, the call is being forwarded to. In this case, flash dialling will be processed locally by the gateway, and the call transfer will be performed when subscriber finished dialling a number;
- *No detect flash* — ignore (do not detect) short flash clearback, received from the subscriber;
- *Local CT* — transfer of the call to ports within the device is performed without REFER request transmission to the communicating gateway.
- *Blind attended transfer* – allow the usage of 'Call Transfer' service with both ways: with waiting for the subscriber to whom the call is transferred (same as 'Unattended calltransfer') and till his answer ('Blind transfer'). When 'Call Transfer' is performed, the gateway disconnects the called subscriber before answer, and sends to the subscriber on hold the address of the subscriber to whom the 'Call Transfer' should be performed. In this mode the flash message is handled locally by the gateway.

For *'Calltransfer'* service operation principles, see Section 7.1 The 'Call Transfer' service.

This setting will not work, if 'IMS mode'–*'Enable IMS'* parameter in SIP profile settings–is enabled on the device.

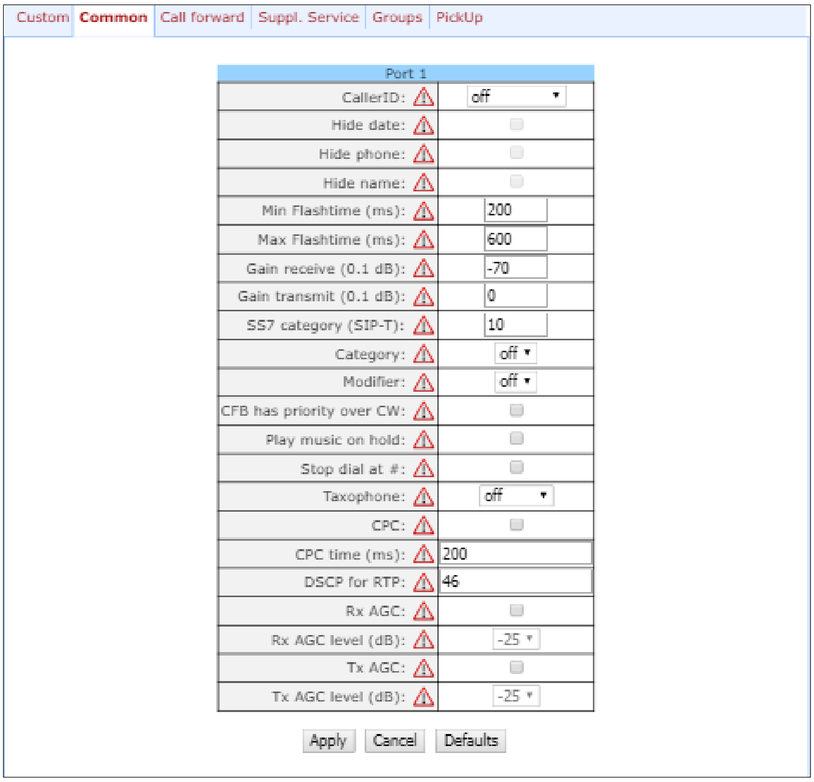
– *Call waiting* – when selected, Call waiting service will be enabled (this service is available in flash—call transfer function operation mode);

This setting will not work, if 'IMS mode'–*'Enable IMS'* parameter in SIP profile settings–is enabled on the device.

– *MWI* – when checked, 'Message waiting indicator' service will be enabled. When the service is enabled, if the user has unread voice messages, intermittent 'PBX response' tone will be played when the phone is offhook; after that, the tone will become continuous. Voice message box operation depends on the Softswitch resources, TAU only plays the notification.

– *Modem* – enables 'Modem' mode for a port. In this mode, all connections established by this port are performing with disabled echo canceller.

'Common' tab – FXS type port common settings:



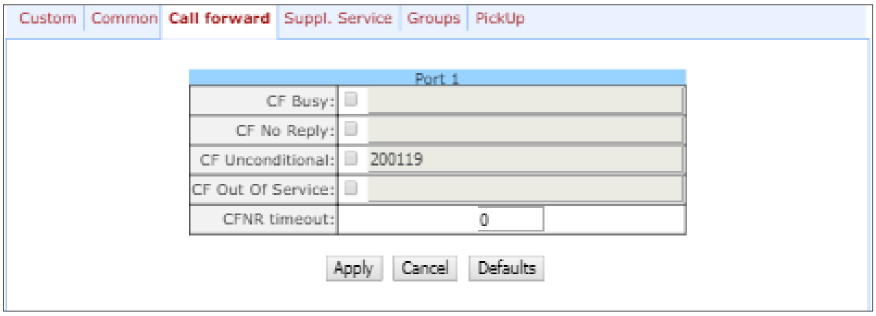
Description of fields is equivalent to *'PBX/Ports/Subscriber profiles'* tab fields shown above in Section 5.1.2.4 The 'Ports Configuration of Subscriber Ports' submenu (Ports).

Exclamation mark symbol means that the settings on this tab are taken from the subscriber profile.

With *'Defaults'* button, you may set the default values:
Min Flashtime – 200 ms;

Max Flashtime – 600 ms;
*Gain receive – -70 *0.1 dB;*
*Gain transmit – 0 *0.1 dB.*

'Call forward' tab—call forwarding service settings for FXS type port:



– *CF Busy* – when checked, CFB service is enabled—forward the call, when the subscriber is busy;

– *CF No reply* – when checked, CFNR service is enabled—forward the call, when there is no reply from the subscriber;

– *CF Unconditional* – when checked, CFU service is enabled—forward the call unconditionally;

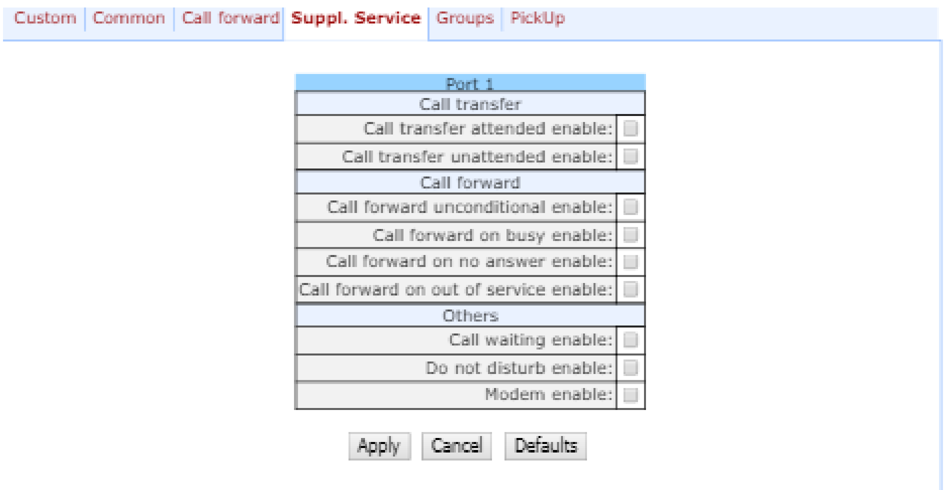
– *CF Out Of Service* – when checked, CFOOS service is enabled—forward the call, when the subscriber is out of service;

For each service, the number that the call is forwarded to, is shown in the rightmost field of the row.

– *CFNR timeout* – subscriber response timeout (in seconds) for 'Call forward on no reply' service.

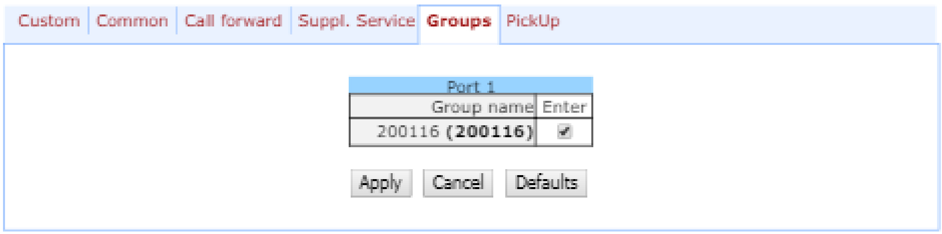
When performing any of the divert services, the SIP response message (302 Moved Temporarily) will include the 'Diversion' header with the reason parameter.

'Suppl. Service' tab allows you to enable/disable supplementary services. For detailed description of supplementary service operations, see Section 5.1.2.6 The 'Suppl. Service Codes' submenu.

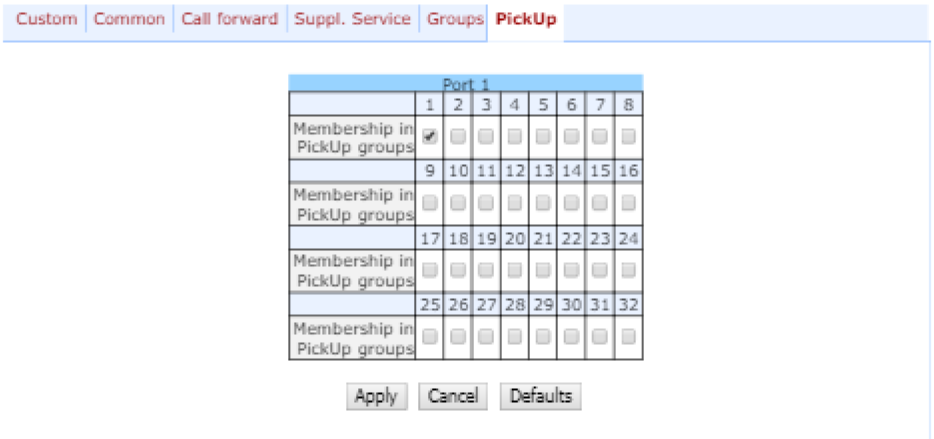


'Groups' tab allows you to add/remove ports to/from serial groups. For detailed description of serial discovery group operations, see Section 5.1.2.7 *The 'Serial groups' submenu*.

In *'Groups'* tab, you may see the list of configured serial groups. To add port to the group, you should select the checkbox against the respective group; to remove port, deselect the checkbox:



'PickUp' tab – add/remove ports to/from the pickup groups. For detailed description of pickup group operations, see Section 5.1.2.8The 'Pickup Group Configuration' submenu (Pickup Groups).

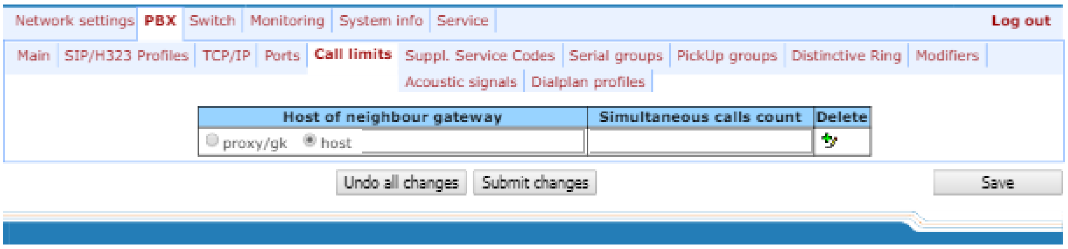


– *Membership in PickUp groups*–defines pickup groups that the port belongs to. Subscriber port that belongs to the group will be able to pickup the call received on any other port of this group.

To apply settings, click the *Apply* button. To reset settings to default values, click the *Default* button.

5.1.2.5 The 'Call Limits' submenu

In the *'Call limits'* submenu, you may configure simultaneous call limits for the communicating host.



– *Host of neighbour gateway*–hostname of a communicating gateway. To limit the calls via SIP-proxy or H323 Gatekeeper, select the ***'proxy/gk'*** checkbox (defines the total call limit through all proxies and from all profiles); to enter host address, select ***'host'***;

– *Simultaneous calls count*–maximum number of simultaneous (incoming and outgoing) calls.

To add/apply a new limit, enter the data in the field with icon, and click the *Submit Changes* button. To remove the limit, select *'Delete'* checkbox and *click the Submit* Changes button.

To discard all changes made to configuration, click the *Undo All Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

5.1.2.6 The 'Suppl. Service Codes' submenu

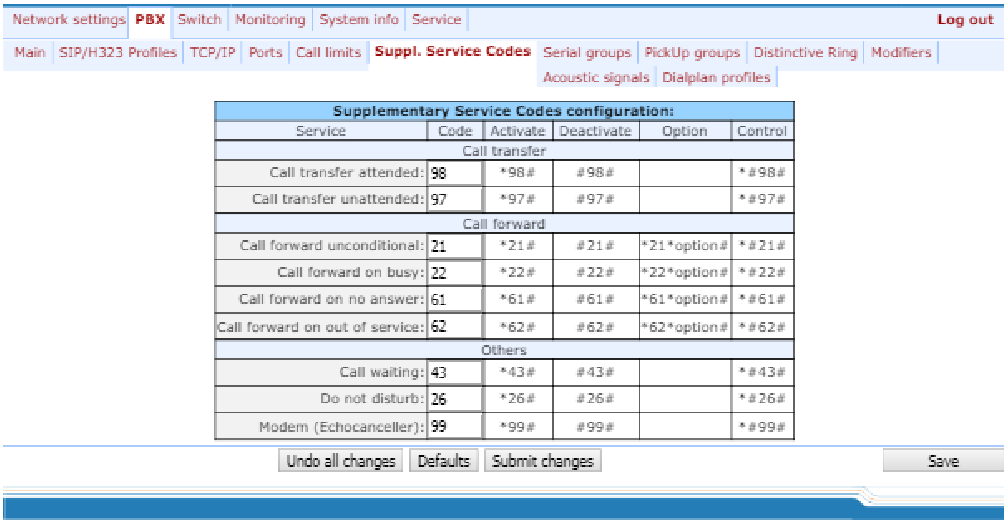
Configuration of Supplementary Service Codes Supplementary services are provided to each subscriber, but in order to use a specific service, the subscriber must enable it first at the service provider. Service providers may create their own service plans containing several supplementary services. To do this, in 5.1.2.4The 'Ports Configuration of Subscriber Ports' submenu (Ports) section, on ***Suppl. Service*** tab, select the checkboxes against the desired supplementary services.

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

- service activation–activation and additional data input;
- service verification;
- service cancellation–deactivation of a service.

When the activation code is entered or the service is cancelled, subscribers may hear either a *'confirmation'* tone (3 short tones), or a *'busy'* tone (intermittent tone with tone/pause duration–0.35/0.35s). *'Confirmation'* tone means that the service has been activated or cancelled successfully, *'busy'* tone–that this service is not enabled for this subscriber.

After service confirmation code entry, the subscriber may hear either *'PBX response'* tone (continuous) or a *'busy'* tone. *'PBX response'* tone means that the service has been enabled and activated for the subscriber, *'busy'* tone–that this service is not enabled for the subscriber.



Supplementary Service Codes configuration:					
Service	Code	Activate	Deactivate	Option	Control
Call transfer					
Call transfer attended:	98	*98#	#98#		*#98#
Call transfer unattended:	97	*97#	#97#		*#97#
Call forward					
Call forward unconditional:	21	*21#	#21#	*21*option#	*#21#
Call forward on busy:	22	*22#	#22#	*22*option#	*#22#
Call forward on no answer:	61	*61#	#61#	*61*option#	*#61#
Call forward on out of service:	62	*62#	#62#	*62*option#	*#62#
Others					
Call waiting:	43	*43#	#43#		*#43#
Do not disturb:	26	*26#	#26#		*#26#
Modem (Echocanceller):	99	*99#	#99#		*#99#

<u>*Supplementary Service Codes configuration:*</u>

- *Service*–type of supplementary service:
  - *Call transfer attended*–'Call transfer' service with the wait for response of the subscriber, the call is being forwarded to;
  - *Call transfer unattended*–'Call transfer' service without the wait for response of the subscriber, the call is being forwarded to;
  - *Call forward unconditional*–'Call forward unconditional' service;
  - *Call forward on busy*–'Forward on busy' service;

- *Call forward on no answer*–'Forward on no answer' service;
- *Call forward on out of service*–'Forward on out of service' service;
- *Call waiting – 'Call waiting' service;*
- *Do not disturb* – 'Do not disturb' service;
- *Modem (Echocanceller)* – 'Modem' service allows to disable echo canceller for subscriber port;

– *Code*–supplementary service code;

– *Activate*–service activation;

– *Deactivate*–service cancellation;

– *Option*–access code, used for service parameters' configuration and forwarding services–a number that the call will be forwarded to;

– *Control*–service verification.

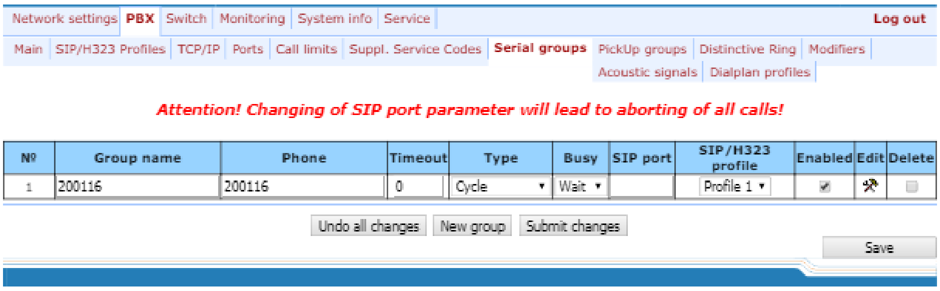
To discard all changes made to configuration, click the *Undo All Changes button.* To set the default values, click the *Defaults* button. To apply changes, click the *Submit Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

5.1.2.7 The 'Serial groups' submenu

In *'Serial groups'* submenu, you may administer the call groups. You may configure up to 32 call groups in total.

After implementation of changes, click the *Submit Changes* button; to discard all changes, click the *Undo All Changes* button; to save changes, click the *Save* button.

You don't have to reboot the gateway in order to apply call group settings. Changing SIP port parameter will lead to termination of current calls. Changing other parameters will disrupt the established connections for the current group only.



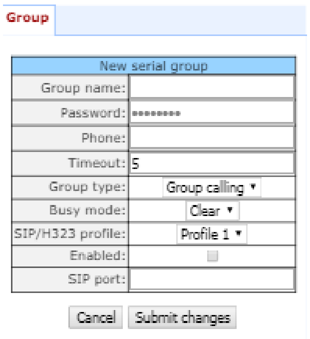
Call groups allow to perform call center features. Gateway supports 3 call group modes: group, delayed group and search.

In group mode, the call comes in to all free ports of the group simultaneously. When one of the group members answers, call transmission to other ports stops.

In the delayed group mode, the call comes in to the first free port in the group list, and then, after the specific timeout, the next free port in the list will be added to the main one, etc. When one of the group members answers, call transmission to other ports stops.

In the search mode, the gateway continuously searches for a free group member, and the call is transferred to their number.

To add a new group, click the *New group* button:



– *Group name*–name of the group (used for SIP server authentication);

– *Password*–password (used for SIP server authentication);

– *Phone*–call group phone number;

– *Timeout*–group member call timeout (used for group types 'serial calling' and 'cycle'), in seconds;

– *Group type*–call group type:

  - *Group calling*–call comes in to all group ports simultaneously;
  - *Serial calling*–call comes in to all ports in turns depending on the selected group member call timeout (when zero value is defined for call timeout, the call will be transferred to the next port, only if higher ports in a queue are busy);
  - *Cycle*–search begins from the first port in the call group.

– *Busy mode*–incoming call processing mode for situations when all group ports are busy (*clear*–call clearback, *wait*–call queueing);

– *SIP/H323 profile*–SIP/H323 profile number, that will be used for the current group;

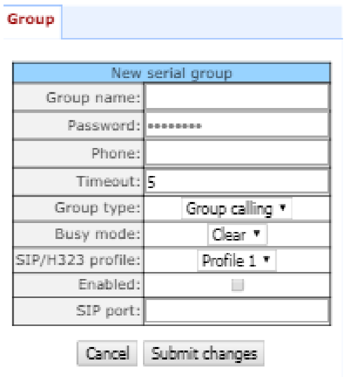
– *Enabled*–when checked, the call group is enabled;

If the call group does not contain any ports, the group will not be used even with *'Enabled'* flag checkbox selected.

– *SIP port*–local UDP port used for group operations via SIP protocol.

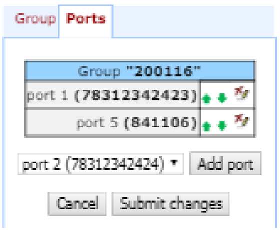
To edit parameters of an existing group, click button in the corresponding row.

'Group'–group settings:



For description of menu fields, see above.

'Ports' – group ports:



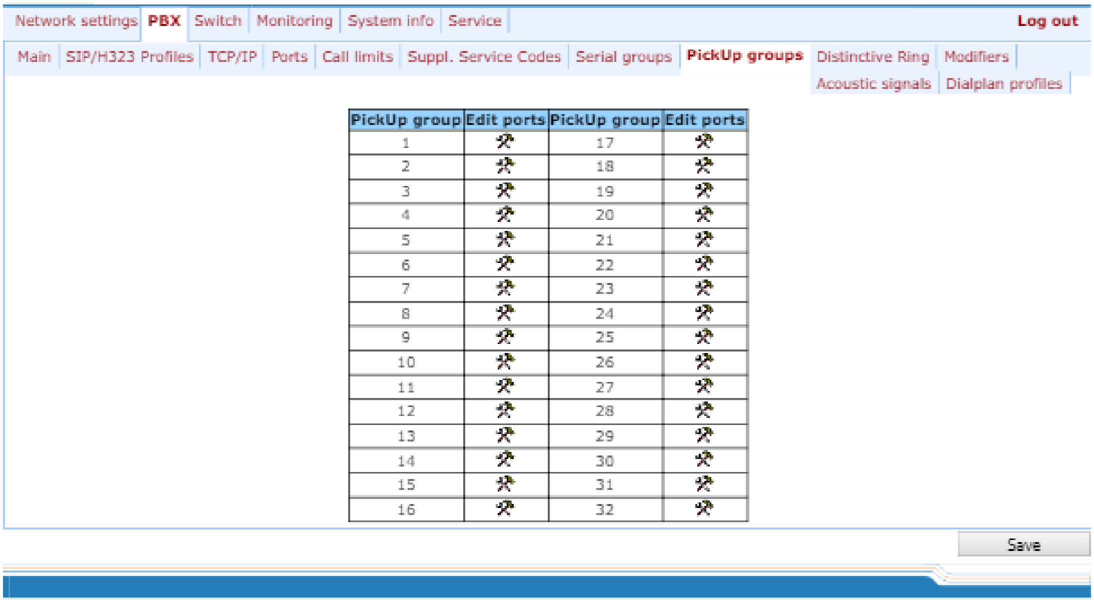
To add a port to a group, select the desired port from the drop-down list and click the *Add port* button.

To change the order of ports in a group, use arrow buttons (up, down); to delete a port from a group, click  button.

5.1.2.8 The 'Pickup Group Configuration' submenu (Pickup Groups)

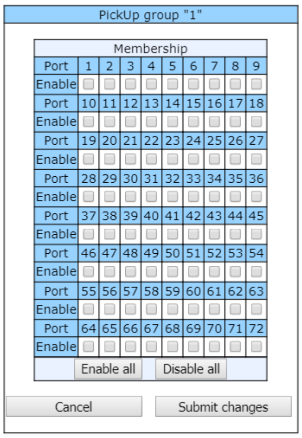
In *'PickUp groups'* submenu, you may configure pickup groups. You may configure up to 32 different pickup groups in total.

Pickup group–subscriber group, authorized to receive (or intercept) any calls directed at another subscriber of the group. I.e. each subscriber port that belongs to the group will be able to pickup the call received on any other port of this group by dialling a pickup code. To configure a pickup code, use *'PBX/SIP-H323 Profiles/Profile n/Dialplan'* tab; for description, see Section 5.1.2.2.5.3 Configuration of pickup codes.



– *PickUp group*–pickup group sequential number [1 .. 32];

– *Edit ports*–edit pickup group parameters. To edit pickup group parameters, click icon in the corresponding row:



Enable–when checked, the port belongs to the pickup group; otherwise, it does not belong to this group. To set permissions for all subscriber ports, click the *Enable all* button. To deselect checkboxes for all subscriber ports, click the *Disable all* button.

If you need to add a port into multiple groups at once, use 'PBX/Ports/ *Edit port* /PickUp' menu.

To quit the pickup group configuration dialog without saving, click the *Cancel button.* To save changes, click the *Submit Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

Service usage:

The call comes in to the phone unit of a subscriber that belongs to the pickup group. If the subscriber is unavailable or cannot answer the call for some reason, another subscriber that belongs to that group may answer the incoming call. To do this, they should pick up the phone and dial a pickup code, and the connection with the caller will be established after that.

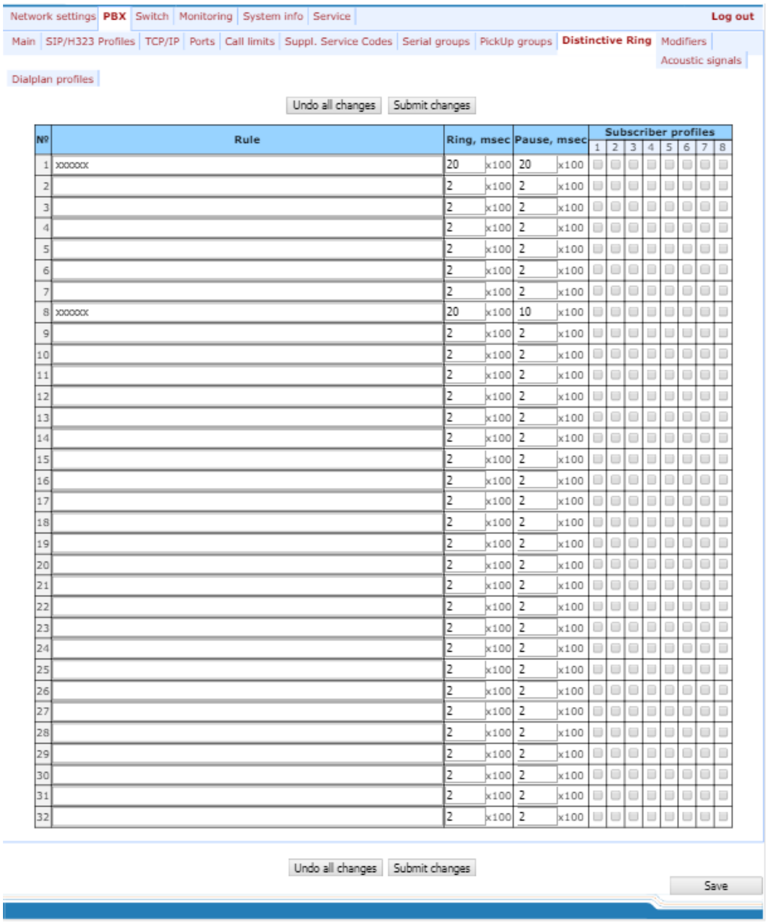
Pickup group may be used in combination with a call group; in this case, all ports that belong to a call group should belong to the pickup group as well. Thus, each port that belong to a call group will be able to pickup an incoming call to a group number.

When subscriber dials the pickup code when there are no incoming calls to a group number, they will hear 'busy' tone.

Pickup group operation will not be possible for calls coming in via SIP protocol with a ringback sent to the caller ('Remote ringback' setting) or via H.323 protocol (except for the calls that do not employ faststart and tunneling).

5.1.2.9 The 'Distinctive Ring' Service Configuration submenu

This setting allows for the non-standard ringing to the callee, which allows to identify the number/group of numbers that the call is originated from. In total, 32 variations of the 'distinctive ring' may be used.



№	Rule	Ring, msec		Pause, msec		Subscriber profiles 1	2	3	4	5	6	7	8
1	xxxxxx	20	x100	20	x100								
2		2	x100	2	x100								
3		2	x100	2	x100								
4		2	x100	2	x100								
5		2	x100	2	x100								
6		2	x100	2	x100								
7		2	x100	2	x100								
8	xxxxxx	20	x100	10	x100								
9		2	x100	2	x100								
10		2	x100	2	x100								
11		2	x100	2	x100								
12		2	x100	2	x100								
13		2	x100	2	x100								
14		2	x100	2	x100								
15		2	x100	2	x100								
16		2	x100	2	x100								
17		2	x100	2	x100								
18		2	x100	2	x100								
19		2	x100	2	x100								
20		2	x100	2	x100								
21		2	x100	2	x100								
22		2	x100	2	x100								
23		2	x100	2	x100								
24		2	x100	2	x100								
25		2	x100	2	x100								
26		2	x100	2	x100								
27		2	x100	2	x100								
28		2	x100	2	x100								
29		2	x100	2	x100								
30		2	x100	2	x100								
31		2	x100	2	x100								
32		2	x100	2	x100								

– *Rule*–mask of the number of the caller that will trigger the 'distinctive ring' with a call to the requested port;

– *Ring*–ringing duration;

– *Pause*–pause duration;

– *Subscriber profiles*–subscriber profiles which ports are affected by this rule.

Caller number mask record rule:

Rule1| Rule2|..| RuleN

Caller number mask syntax:

- **|**–logical **OR**–used to separate rules.
- **X** or **x**–any number from 0 to 9, equal to a range [0-9];
- **0** - **9**–numbers from 0 to 9;
- *****–* character;
- **#**–# character;
- **[ ]**–define ranges (with a hyphen), or enumeration (w/o spaces, commas, and other characters between the digits), e.g:

  Range: **[1-5]**–1,2,3,4, or 5;
  Enumeration: **[138]**–1,3, or 8;
  Range and enumeration **[0-9*#]**–0 to 9, and also * and #.

- **{min,max}**–define the repetition count for a character located outside the parentheses, a range or *# symbols.
  min–minimum repetition count, *max*–maximum repetition count.

  {,max}–equal to {0,max};
  {min,}–equal to {min,inf}.

  Example:
  5{2,5}–caller's number may be equal to 55, 555, 5555, or 55555

- **.** – 'dot' special symbol means that a preceding digit, range, or '*', '#' characters may be repeated from one to infinity times. Equivalent to a record {0,}

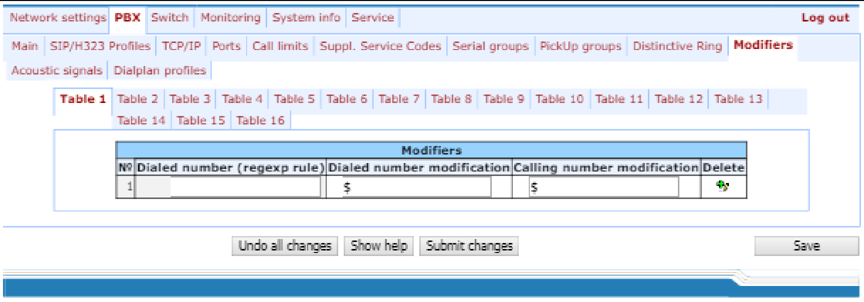
  Example:
  5x.* –'x' in this rule may be completely absent or may be present any number of times. Caller number may be equal to 5*, 5x*, 5xx*, 5xxx*, ...

- **+**–digit, range, or '*', '#' characters preceding the '+' symbol may be repeated from one to infinity times. Equivalent to a record {1,}.

5.1.2.10 The 'Modifiers' submenu

This setting allows for the modification of the associated and dialed numbers depending on the call direction. Modifiers are used in outgoing calls.

Modifiers work only when routing rules are used, described with regular expressions (Section 5.1.2.2.5.4); at that, in number modification routing rules, <:> characters should not be used.



The gateway allows you to configure 16 modifier groups, each group contains one or several modification rules:

– *Dialed number (regexp rule)*–dialed number mask;

– *Dialed number modification*–dialed number modification rule;

– *Calling number modification*–modification rule for TAU subscriber's number (caller's number).

Dialed number mask record rule:

Rule1| Rule2|..| RuleN

Caller number mask syntax:

- **|**– logical **OR**–used to separate rules.
- **X** or **x** – any number from 0 to 9, equal to a range [0-9];
- **0** – **9** – numbers from 0 to 9;
- *****;
- **#**;
- **[ ]** – define ranges (with a hyphen), or enumeration (w/o spaces, commas, and other characters between the digits), e.g:

  Range: **[1-5]**–1,2,3,4, or 5;
  Enumeration: **[138]**–1,3, or 8;
  Range and enumeration **[0-9*#]**–0 to 9, and also * and #.

- **{min,max}** – define the repetition count for a character located outside the parentheses, a range or *# symbols.
  min–minimum repetition count, *max*–maximum repetition count.

  {,max} – equal to {0,max};
  {min,} – equal to {min,inf}.

  Example:
  5{2,5} – dialed number may be equal to 55, 555, 5555, or 55555

- **.** – 'dot' special symbol means that a preceding digit, range, or '*', '#' characters may be repeated from one to infinity times. Equivalent to a record {0,}

  Example:
  5x.* –'x' in this rule may be completely absent or may be present any number of times. Dialed number may be equal to 5*, 5x*, 5xx*, 5xxx*, ...

- **+** – digit, range, or '*', '#' characters preceding the '+' symbol may be repeated from one to infinity times. Equivalent to a record {1,}.

Modification rule syntax:

- **–** or **.** – digit deletion;
- **X** or **x** – digit/symbol or character in this position remains unchanged;
- **?** –digit/symbol in this position remains unchanged;
- **+** – addition of the succeeding digits/symbols (0-9, *, #);
- **!** – breakdown finish, all other digits of a number are truncated;
- **$** – breakdown finish, all other digits of a number remain unchanged;
- **0-9**, **#** and ***** (without '+' sign) – substitution of a digit in this position.

Example:

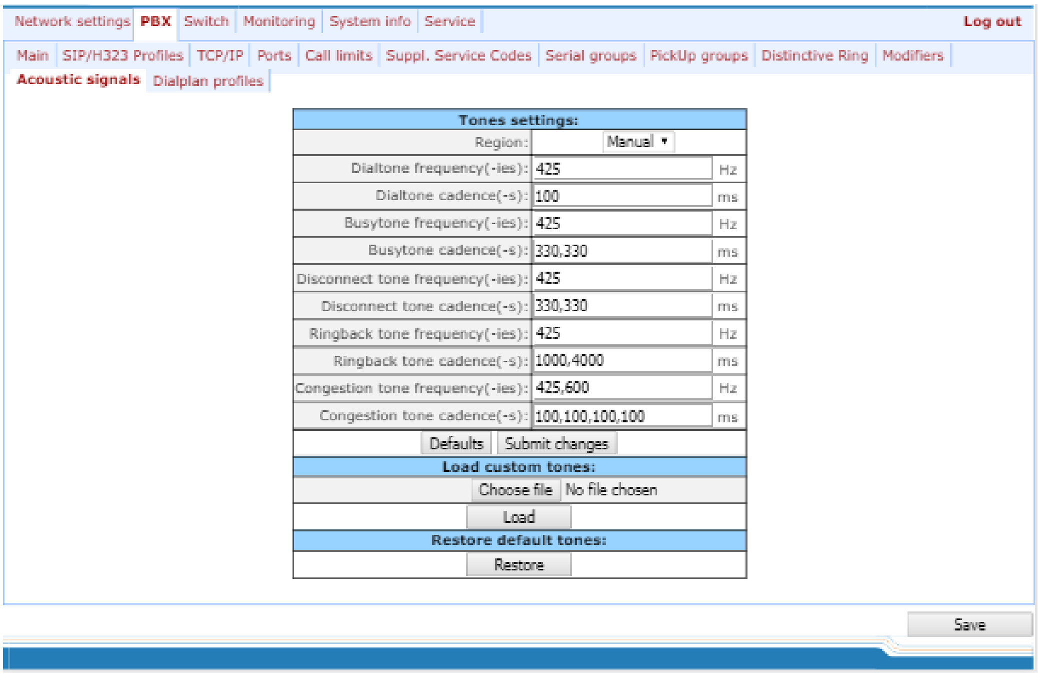
When calling to six-digit numbers, beginning with 5 and 6, you need to transform the subscriber number in such manner as to add 383 prefix into the beginning of the subscriber number, and replace the first digit of the dialled number to 7.

Dialed number: [5-6]xxxxx
Dialed number modification: 7xxxxx
Calling number modification: +383$

To discard all changes made to configuration, click the *Undo All Changes* button. To view the help of rules syntax, click the *Help* button. To apply changes, click the *Submit Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

5.1.2.11 The 'Acoustic signals' submenu

This setting allows for the modification of information acoustic signals parameters as well as for the upload of ready files with the tones settings.



– *Region* – determines the region for which acoustic signal parameters are set:

- Russia – sets the values of the acoustic signals parameters used in Russia;
- Iran – sets the values of the acoustic signals parameters used in Iran;
- Manual – sets the values of the acoustic signals parameters. In this case it is possible to set signal frequencies and cadences noted below.

– Dialtone frequency, Hz;

– Dialtone cadences, ms;

– Busytone frequency, Hz;

– Busytone cadences, ms. A value of 0 in the first position indicates that no 'Busy' signal will be generated and no 'Notification of Unathorized Handset/ROH' signal will be generated after 2 minutes if the handset is not available.

– Disconnect tone frequency, Hz;

– Disconnect tone cadences, ms. A value of 0 in the first position indicates that no 'Disconnect' signal will be generated and no 'Notification of Unathorized Handset/ROH' signal will be generated after 2 minutes if the handset is not available.

– Ringback tone frequency, Hz;

– Ringback tone cadences, ms;

– Congestion tone frequency, Hz;

– Congestion tone cadences, ms.

Clicking the *Defaults* button sets the standard tone values for Russia;

To apply changes, click the *Submit Changes* button. To store changes to non-volatile memory of the device, click the *Save* button.

To upload tones settings, click the *Select file* button and select a configuration file. Next click the *Load* button. The tones from an uploaded file will have priority over the tones configured in the 'Tones settings' section.

The requirements for the structure of tones configuration file are the following (the example contains standard frequency and time interval values):

```
dialtone_freq: 425
dialtone_time_rule: 1000
dialtone_time_rule: 425
busytone_time_rule: 330.330
ringbacktone_freq: 425
ringbacktone_time_rule: 1000, 4000
congestiontone_freq: 425
congestiontone_time_rule: 175.175
```

where:

dialtone_freq – 'Dial tone' frequencies, Hz (no more than 2 frequencies, the frequencies are separated with comma ',');

dialtone_time_rule – time intervals of duration and pause of a signal with given frequency, ms (for each frequency pause and signal length intervals are specified, time intervals are separated with comma ',').

Likewise, frequencies and time intervals are setting for other signals:

- *busytone* – 'busy' tone;
- *ringbacktone* – 'ringback' tone;
- *congestiontone* - 'overload busy' tone; issued when 500, 502, 503 and 504 SIP response are received.

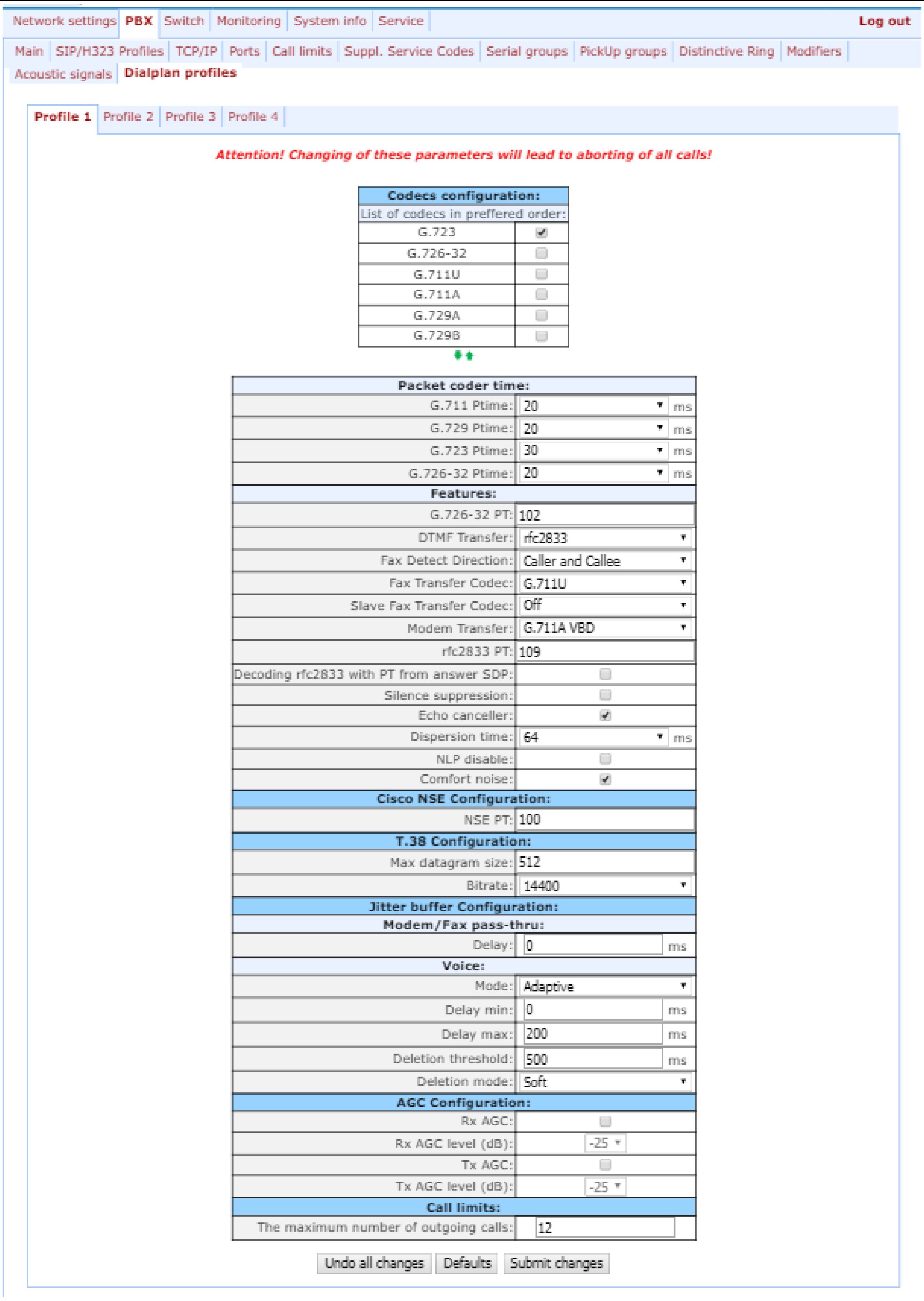
Value limits:

- the range for frequencies: 0 – 4000 Hz;
- the range for time intervals: 0 – 65535 ms.

To restore default settings, click the *Restore* button. With that, tones configured in the 'Tones settings' section start to be used.

5.1.2.12 The 'Dialplan profiles' submenu

In this section you may configure profiles of parameters used to certain directions, i.e. when making an outgoing call according to a certain routing rule, codecs will be used for this call and other attributes from this profile will be applied.



<u>*Codecs configuration*</u>

In Codecs configuration section you may select codecs and the order of their use while connection establishment. The highest priority codec must be set in the top position. When clicking left mouse button, a line with the selected codec is highlighted. To change codecs priority use arrows (up, down).

G.723.1 codec is used together with 'Silence compression' setting. When the setting is enabled, Annex A support is enabled, otherwise it is disabled.

– *G.711A* – use G.711A codec;

– *G.711U* – use G.711U codec;

– G.726-32 – use G.726-32 codec.

– *G.723* – use G.723.1 codec;

– *G.729A* – use G.729 annexA codec (when defining codec compatibility, non-standard codec description is sent via SIP: a=rtpmap:18 G729A/8000 a=fmtp:18 annexb=no);

– *G.729B* – use G.729 annexB codec.

G.726-32 codec used only in SIP protocol operations.

Packet coder time

In *Packet coder time* section you may see packetization time, i.e. amount of speech milliseconds (ms) transmitted in one RTP voice packet:

– *G711* – for G711 codec (permitted values: 10, 20, 30, 40, 50, 60);

– *G729* – for G729 codec (permitted values: 10, 20, 30, 40, 50, 60, 70, 80);

– *G723* – for G723 codec (permitted values: 30, 60, 90);

– *G.726-32* – for G.726-32 codec (allowed values 10, 20, 30).

Features:

– *G.726-32 PT* – G.726-32 codec payload type (permitted values: 96 to 127);

– *DTMF Transfer* – DTMF tone transmission method. During established session, DTMF transmission is used for extension dialling;

  - *Inband* – inband, in RTP voice packets;
  - *RFC2833* – according to RFC2833 recommendation, as a dedicated payload in RTP voice packets;
  - *INFO* – outbound. For SIP protocol, INFO messages are used; the type of transmitted DTMF tones depends on MIME extension type (for detailed description, see Section 5.1.2.2.3). When H.323 protocol is used, DTMF transmission method depends on 'DTMF Transfer' parameter in H.323 tab (see Section 5.1.2.2.2)

  In order to be able to use extension dialling during the call, make sure that the similar DTMF tone transmission method is configured on the opposite gateway.

– *Fax Detect Direction* – defines the call direction for fax tone detection and subsequent switching to fax codec:

  - *no detect fax* – disables fax tone detection, but will not affect fax transmission (switching to fax codec will not be initiated, but such operation still may be performed by the opposite gateway);
  - *Caller and Callee* – tones are detected during both fax transmission and receiving. During fax transmission, CNG FAX signal is detected from the subscriber's line. During fax receiving, V.21 signal is detected from the subscriber's line;
  - *Caller* – tones are detected only during fax transmission. During fax transmission, CNG FAX signal is detected from the subscriber's line;

   - *Callee* – tones are detected only during fax receiving. During fax receiving, V.21 signal is detected from the subscriber's line;

– *Fax Transfer Codec* – master protocol/codec used for fax transmissions:

   - *G.711A* – use G.711A codec for fax transmissions. Switching to G.711A codec will be performed when the corresponding tones are detected;
   - *G.711U* – use G.711U codec for fax transmissions. Switching to G.711U codec will be performed when the corresponding tones are detected;
   - *T.38 mode* – use T.38 protocol for fax transmissions. Switching to T.38 will be performed when the corresponding tones are detected.

– *Slave Fax Transfer Codec* – slave protocol/codec used for fax transmissions. This codec is used when the opposite device does not support the priority:

   - *G.711A* – use G.711A codec for fax transmissions. Switching to G.711A codec will be performed when the corresponding tones are detected;
   - *G.711U* – use G.711U codec for fax transmissions. Switching to G.711U codec will be performed when the corresponding tones are detected;
   - *T.38 mode* – use T.38 protocol for fax transmissions. Switching to T.38 will be performed when the corresponding tones are detected.
   - *Off* – disable slave protocol/codec;

The primary and redundant protocol/codec should differ from each other.

– *Modem Transfer* – defines switching into 'Voice band data' mode (according to V.152 recommendation). In VBD mode, the gateway disables the voice activity detector (VAD) and comfort noise generator (CNG), this is necessary for establishing a modem connection.

- *Off* – disable modem signal detection;
- *G.711A VBD* – use G.711A codec to transfer data via modem connection. Switching to G.711A codec in VBD mode will be performed when the CED tone is detected;
- *G.711U VBD* – use G.711U codec to transfer data via modem connection. Switching to G.711U codec in VBD mode will be performed when the CED tone is detected;
- *G.711A RFC3108* – use G.711A codec to transfer data via modem connection. When entering modem data transfer mode via SIP protocol, echo cancellation and VAD are disabled with attributes described in RFC3108 recommendation:

   - a=silenceSupp:off - - - -
   - a=ecan:fb off -;

- *G.711U RFC3108*–use G.711U codec to transfer data via modem connection. When entering modem data transfer mode via SIP protocol, echo cancellation and VAD are disabled with attributes described in RFC3108 recommendation:

   - a=silenceSupp:off - - - -
   - a=ecan:fb off -;

- *G.711A NSE* – CISCO NSE support, G.711A codec is used to transfer data via modem connection;
- *G.711U NSE* – CISCO NSE support, G.711U codec is used to transfer data via modem connection.

Cisco NSE support: when NSE 192 packet is received, gateway will switch to the selected codec and disable VAD; when NSE 193 packet is received, echo canceller will be disabled.

- *RFC2833 PT* – type of payload used to transfer packets via RFC2833. Permitted values: 96 to 127. RFC2833 recommendation describes the transmission of DTMF and Flash tones via RTP protocol. This parameter should conform to the similar parameter of a communicating gateway;

- *Decoding rfc2833 with PT from answer SDP* – when performing outgoing call, receive DTMF tones in rfc2833 format with payload type proposed by a communicating gateway. When unchecked, tones will be received with the payload type, configured on the gateway. Enables compatibility with gateways that incorrectly handle rfc3264 recommendation;

- *Silence suppression* – when checked, use voice activity detector (VAD) and silence suppression (SSup), otherwise they will not be used. Voice activity detector disables transmission of RTP packets during periods of silence, reducing loads in data networks;

- *Echo canceller* – when selected, echo cancellation is used;

- *Dispersion time* – echo signal, appearing with a delay of no more than the given value, will be jammed (up to 128 ms);

- *NLP disable* – when checked, use echo cancellation with disabled non-linear processor (NLP). When signal levels on transmission and reception significantly differ, useful signal may become suppressed by the NLP. Use this echo canceller operation mode to prevent the signal suppression;

- *Comfort noise* – when checked, use comfort noise generator. Used together with 'Silence compression (VAD)' setting, as comfort noise packets are generated only upon voice pauses detection;

*In **'Cisco NSE configuration'*** section, you may configure codec payload type for modem transmission using CISCO NSE method:

- *NSE PT* – type of payload used to transfer packets via NSE. Permitted values: 96 to 127.

In 'T38 configuration' section, you may configure T.38 protocol parameters:

- *Max Datagram Size* – maximum datagram size. (Zero value means that T38MaxDatagram attribute will not be transferred via SIP, and the gateway will support the reception of datagrams up to 512 bytes. Use zero value in interactions with gateways that do not support datagrams from 272 bytes and higher). This parameter defines the maximum quantity of bytes that will be sent in T.38 protocol packet;

- *Bitrate* – maximum fax transfer rate (9600, 14400). This setting affects the ability of a gateway to work with high-speed fax units. If fax units support data transfer at 14400 baud, and the gateway is configured to 9600 baud, the maximum speed of connection between fax units and the gateway will be limited at 9600 baud. And vice versa, if fax units support data transfer at 9600 baud, and the gateway is configured to 14400 baud, this setting will not affect the interaction, maximum speed will be defined by the performance of fax units.

*In **'Jitter buffer configuration'*** section, you may configure jitter buffer parameters.

Due to various factors, e.g. network overload, voice data packets may be served to the gateway at different speeds, and their arrival order may change. Such event is called 'jitter'.

In order to compensate the jitter effect, the jitter buffer has been implemented. In jitter buffer, packets are saved as soon as they are received. Voice packets that came out of sequence (earlier or later) have their sequential number analyzed. After that, they are positioned into their respective places in a queue and sent further in the right order that allows to improve call quality for unstable communication channels.

Jitter buffer may be fixed or adaptive. The size of adaptive jitter buffer changes along with the average identified delay in voice packets' reception. When delay rises, the size of adaptive jitter buffer grows instantaneously, when delay lowers, buffer size shrinks in 10 seconds after the delay has been steadily reduced.

*In **'Modem/Fax pass-thru'*** section, you may configure the jitter buffer in fax/modem data transfer mode:

– *Delay*–the size of a fixed jitter buffer, used in fax or modem data transfer mode. Permitted value range is from 0 to 200ms.

'Voice' – jitter buffer voice connection settings:

– *Mode* – jitter buffer operation mode: fixed or adaptive;

– *Delay* – size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer. Permitted value range is from 0 to 200ms.

– *Delay max* – upper limit (maximum size) of adaptive jitter buffer, in milliseconds. Permitted value range is from 'Delay' to 200ms.

– *Deletion threshold* – threshold for immediate deletion of a packet, in milliseconds. When buffer size grows and packet delay exceeds this threshold, packets will be deleted immediately. Permitted value range is from 'Delay max' to 500ms;

– *Deletion mode* – buffer adjustment mode. Defines the method of packet deletion during buffer adjustment to lower limit. In 'SOFT' mode, device uses intelligent selection pattern for deletion of packets that exceed the threshold. In 'HARD' mode, packets which delay exceeds the threshold will be deleted immediately.

The 'AGC configuration' section:

– *Rx AGC* – when selected, a received signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise — the amplification will not be carried out;

– *Rx AGC Level* – determines the value of the level to which an analogue signal will be amplified when receiving (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB);

– *Tx AGC* – when selected, a transmitted signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise — the amplification will not be carried out;

– *Tx AGC Level* – determines the value of the level to which an analogue signal will be amplified when transmitting (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).

The 'Call limit' section:

– *The maximum number of outgoing calls* - defines maximum amount of simultaneous outgoing calls, performing by this profile.

To discard all changes made to configuration, click the *Undo All Changes* button. To discard all changes made to configuration, click the *Undo All Changes* button. To set default parameters, click the *Defaults* button (the figure below shows default values). To apply changes, click the *Submit Changes* button.

5.1.3 The 'Switch' menu

In *'Switch'* menu, you may configure switch ports.

5.1.3.1 The 'Switch ports settings' submenu

In the *'Switch ports settings'* submenu, you may configure parameters of integrated Ethernet switch ports.

5.1.3.1.1 Configuration

The switch is able to work in four modes:

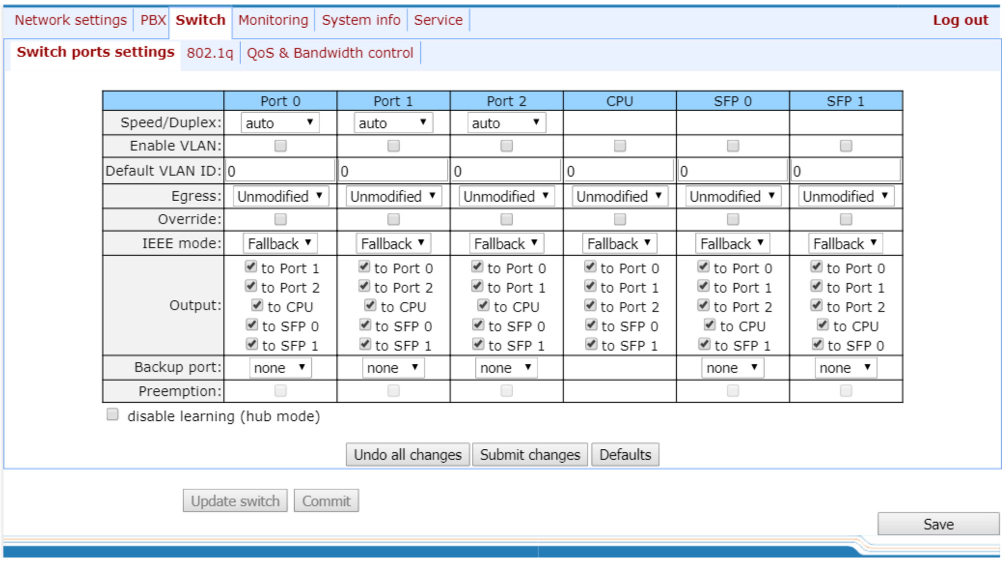
1. ***Without VLAN settings*** – to use this mode, *Enable VLAN* checkboxes should be deselected for all ports, *'IEEE Mode'* value should be set to *'Fallback'* for all ports, mutual availability of data ports should be set to *'Output'* with the respective checkboxes. *'802.1q'* routing table in *'802.1q'* tab should not contain any entries.

2. ***Port based VLAN*** – to use this mode, *'IEEE Mode'* value should be set to *'Fallback'* for all ports, mutual availability of data ports should be set to *'Output'* with the respective checkboxes. For VLAN operation, use *'Enable VLAN', 'Default VLAN ID', 'Egress'*, and *'Override'. '802.1q'* routing table in *'802.1q'* tab should not contain any entries.

3. ***802.1q*** – to use this mode, *'IEEE Mode'* value should be set to *'Check'* or *'Secure' for all ports.* For VLAN operation, use *'Enable VLAN', 'Default VLAN ID'*, and *'Override'.* Also, routing rules described in *'802.1q'* routing table in *'802.1q'* tab will apply.

4. ***802.1q + Port based VLAN.*** 802.1q mode may be used in combination with 'Port based VLAN'. In this case, *'IEEE Mode'* value should be set to *'Fallback'* for all ports, mutual availability of data ports should be set to *'Output'* with the respective checkboxes. For VLAN operation, use *'Enable VLAN', 'Default VLAN ID', 'Egress'*, and *'Override'*. Also, routing rules described in *'802.1q'* routing table in *'802.1q'* tab will apply.

For example, of switch configuration using VLAN, see Appendix D.



Gateway switch is equipped with 3 electrical Ethernet ports, 1/2 optic port and 1 port for CPU interactions:

– *Port0, port1, port2* – electrical Ethernet ports of the device*;*

– *CPU* – internal port linked to the device CPU;

– *SFP0, SFP1*[1] – optical (SFP) Ethernet ports of the device.

<u>*Switch settings:*</u>

– *Speed/Duplex* – speed and duplex settings of electrical Ethernet ports. Optical ports support only one mode: 1000 full duplex;

– *Enable VLAN* – when checked, enable *'Default VLAN ID', 'Override'* and *'Egress'* settings for this port, otherwise they will be disabled;

– *Default VLAN ID* – when an untagged packet is received at the port, this will be its VID; when a tagged packet is received at that port, its VID is considered to be specified in its VLAN tag;

– *Egress:*

- *unmodified* – packets will be sent by the port without any changes (i.e. as they came to another switch port);
- *untagged* – packets will always be sent without VLAN tag by this port;
- *tagged* – packets will always be sent with VLAN tag by this port;
- *double tag* – each packet will be sent with two VLAN tags–if received packet was tagged and came with one VLAN tag – if the received packet was untagged.

– *Override* – when checked, it is considered that any received packet has a VID, defined in *'default VLAN ID'.* True for both untagged and tagged packets.

– *IEEE mode:*

- *disabled* – for a packet received by this port, routing rules described in the *'output'* section of the table will be applied;
- *fallback*–if a packet with VLAN tag is received through this port, and there is a record in a '802.1q' routing table for this packet, then it falls within a scope of routing rules, specified in the record of this table; otherwise, routing rules specified in *'egress'* and *'output'* will be applied to it;
- *check*–if a packet with VID is received through the port, and there is a record in a '802.1q' routing table for this packet, then it falls within a scope of routing rules, specified in the current record of this table, even if this port does not belong to the group of this VID. Routing rules specified in *'egress'* and *'output'* will not apply to this port;
- *secure*–if a packet with VID is received through the port, and there is a record in a '802.1q' routing table for this packet, then it falls within a scope of routing rules, specified in the current record of this table; otherwise, it is <u>rejected.</u> Routing rules specified in *'egress'* and *'output'* will not apply to this port;

– *Output* – mutual availability of data ports. Defines privileges that allow packets received by this port to be transferred to flagged ports;

– *Backup port* – select a port from the list as a backup port. Used in direction reservation mode;

[1] For TAU-72.IP/TAU-36.IP v1, v2 appears status of one optic Ehernet port.

– *Preemption* – returns to master port on its availability. Used in direction reservation mode;

'*Backup port*' and '*Preemption*' are used for direction reservation. In this case, main and backup ports are connected to a single switch with Ethernet cables. Backup port should be connected only when switch settings has been applied and saved.

– *Hubmode*–Ethernet switch operation in hub mode. In hub mode, Ethernet switch will not learn MAC addresses of devices, that send packets, and all packets will be transferred to all switch ports. We recommend using this mode for network traffic mirroring from the switch ports to PC (tracing) only.

Update Switch and *Commit* buttons allow to retain access to the gateway when switch settings are applied. Click the *Commit* button in 30 seconds interval to confirm newly applied settings, or the previous settings will be restored.

– *Update Switch*–apply switch settings without restart;
– *Commit*–confirm applied settings.

Use the *Defaults* button to set default parameters (the figure below shows default values).

5.1.3.1.2 Tracing, Network Traffic Mirroring

To perform tracing, you should do the following:

1. *Configure hub mode*–in *'Switch'* tab, select *'Hubmode'* checkbox*,* then click *'Update Switch' and 'Commit'* buttons consequently.

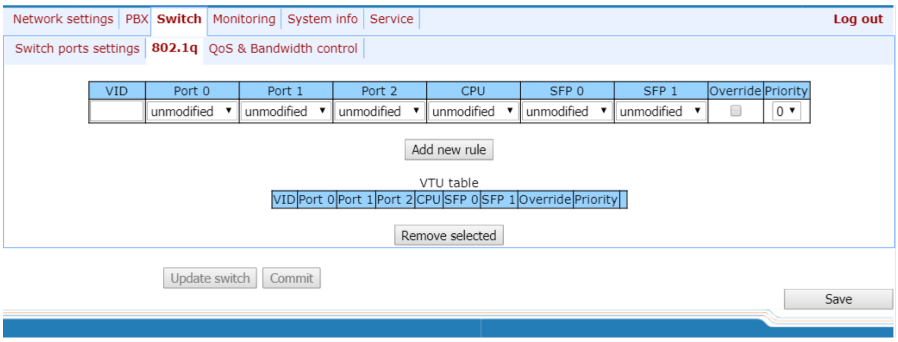
2. Connect a PC to perform the tracing directly to TAU Ethernet port.

3. Run the application on the PC that captures network traffic. In the application, select Ethernet interface connected to TAU-72.IP/TAU-36.IP as a traffic capture interface.

4. After tracing, save captured traffic into a file.

5.1.3.2 The '802.1q' submenu

In *'802.1q'* submenu, you may define the configuration of packet routing rules for switch operation in 802.1q mode.



Gateway switch is equipped with 2 electrical Ethernet ports, 1 optic port and 1 port for CPU interactions:

– *Port0, port1, port2*–electrical Ethernet ports of the device;

– *CPU*–internal port linked to the device CPU*;*

CPU	SFP 0	SFP 1	Override	Priority
unmodified	unmodified	unmodified	☐	0

– *SFP0, SFP1*–optical (SFP) Ethernet ports of TAU-72.IP/TAU-36.IP v1, v2 (v3, v4).

CPU	SFP	Override	Priority
unmodified	unmodified	☐	0

Adding records to the packet routing table (16 rules max.): in 'VID' field, enter an identifier of VLAN group, that the routing rule is created for, and assign actions for each port to be performed during transfer of packets with specified VID.

- *unmodified*–packets will be sent by the port without any changes (i.e. as they have been received);
- *untagged*–packets will always be sent without VLAN tag by this port;
- *tagged*–packets will always be sent with VLAN tag by this port;
- *not member*–packets with specified VID will not be sent by this port (i.e. the port is not the member of VLAN);

– *override*–when checked, override 802.1p priority for this VLAN; otherwise, leave the priority unchanged;

– *Priority*–802.1p priority assigned to packets by VLAN, if *'override'* checkbox is selected;

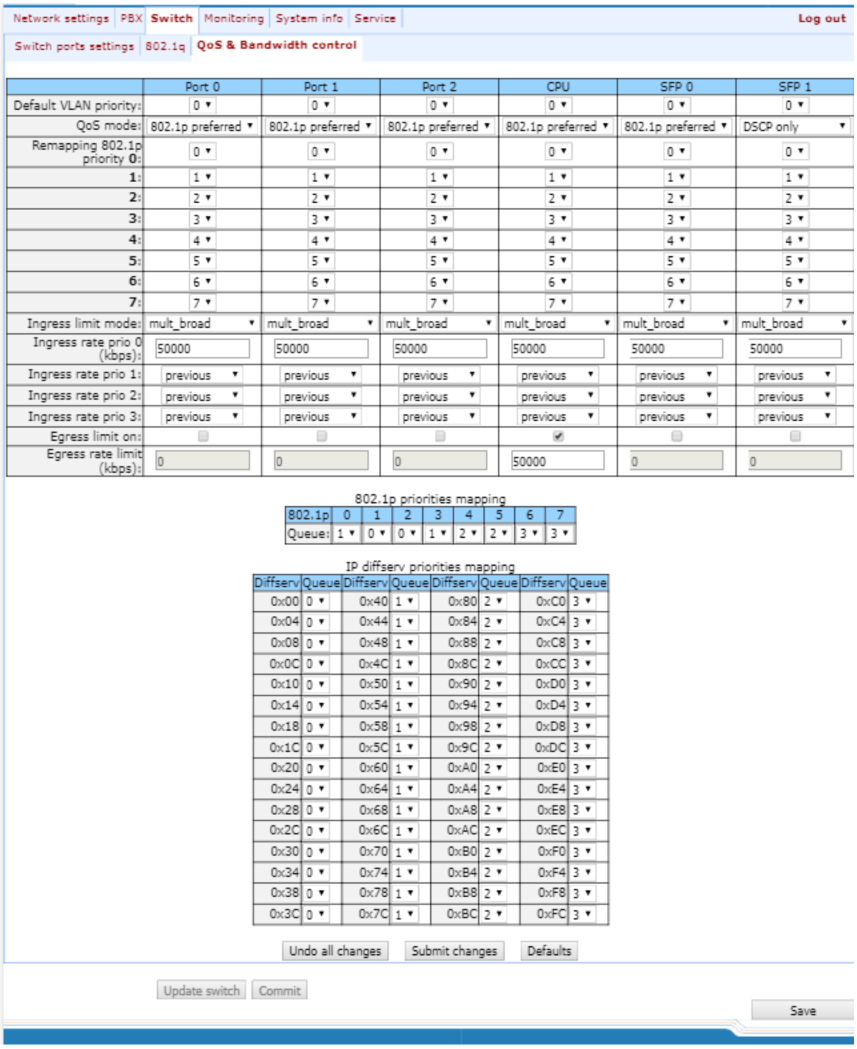
Then, click the *Add New Rule button.*

To remove records, select checkboxes for the rows to be removed and click the *Remove selected* button.

***Update Switch* and *Commit* buttons allow to retain access to the gateway when switch settings are applied. Click the *Commit* button in 30 seconds interval to confirm newly applied settings, or the previous settings will be restored.**

5.1.3.3 *The 'QoS & Bandwidth control' submenu*

In *'QoS & Bandwidth control'* submenu, you may configure Quality of Service functions and bandwidth restrictions.



– *Default vlan priority*–802.1p priority assigned to untagged packets, received by this port. If *802.1p* or *IP diffserv* priority is already assigned to the packet, this setting will not be used ('default vlan priority' will not be applied to packets containing IP header, when one of the QoS modes is in use: *DSCP only, DSCP preferred, 802.1p preferred*, and also to untagged packets;

– *QoS mode*–QoS operation mode:

- *DSCP only*–distribute packets into queues based on IP diffserv priority only;
- *802.1p only*–distribute packets into queues based on 802.1p priority only;
- *DSCP preferred*–distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, IP diffserv priority is used for queuing purposes;
- *802.1p preferred*–distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, 802.1p priority is used for queuing purposes;

– *Remapping 802.1p priority*–remap 802.1p priorities for untagged packets. Thus, a new value may be assigned for each priority received in VLAN packet;

– *ingress limit mode*–restriction mode for traffic coming to the port:

- *off*–no restriction;
- *all*–restrict all traffic;
- *mult_flood_broad*–multicast, broadcast, and flooded unicast traffic will be restricted;
- *mult_broad*–multicast and broadcast traffic will be restricted;
- *broad*–only broadcast traffic will be restricted.

This mode is not suitable for restriction of TCP/IP traffic coming to the port. It was designed to prevent the broadcast storm. If you try to restrict TCP/IP traffic using this mode, the result will not match the configured value.

– *ingress rate prio 0 (kbps)*–bandwidth restriction for incoming port traffic, priority 0. Permitted values–from 70 to 250000kbps;

– *ingress rate prio 1*–bandwidth restriction for incoming port traffic, priority 1. You can double the bandwidth (prev prio *2) of priority 0, or leave it unchanged (same as prev prio);

– *ingress rate prio 2*–bandwidth restriction for incoming port traffic, priority 2. You can double the bandwidth (prev prio *2) of priority 1, or leave it unchanged (same as prev prio);

– *ingress rate prio 3*–bandwidth restriction for incoming port traffic, priority 3. You can double the bandwidth (prev prio *2) of priority 2, or leave it unchanged (same as prev prio);

– *Egress limit on*–enable the bandwidth restriction for outgoing port traffic;

– *Egress rate limit*–bandwidth restriction for outgoing port traffic. Permitted values–from 70 to 250000kbps.

– *802.1p priorities mapping*–allows to distribute packets into queues depending on the 802.1p priority:

- *802.1p*–802.1p priority value;
- *Queue*–outgoing queue number.

– *IP diffserv priorities mapping*–allows to distribute packets into queues depending on the IP diffserv priority (for basic diffserv values, see Table 7):

- *diffserv*–IP diffserv priority value;
- *Queue*–outgoing queue number.

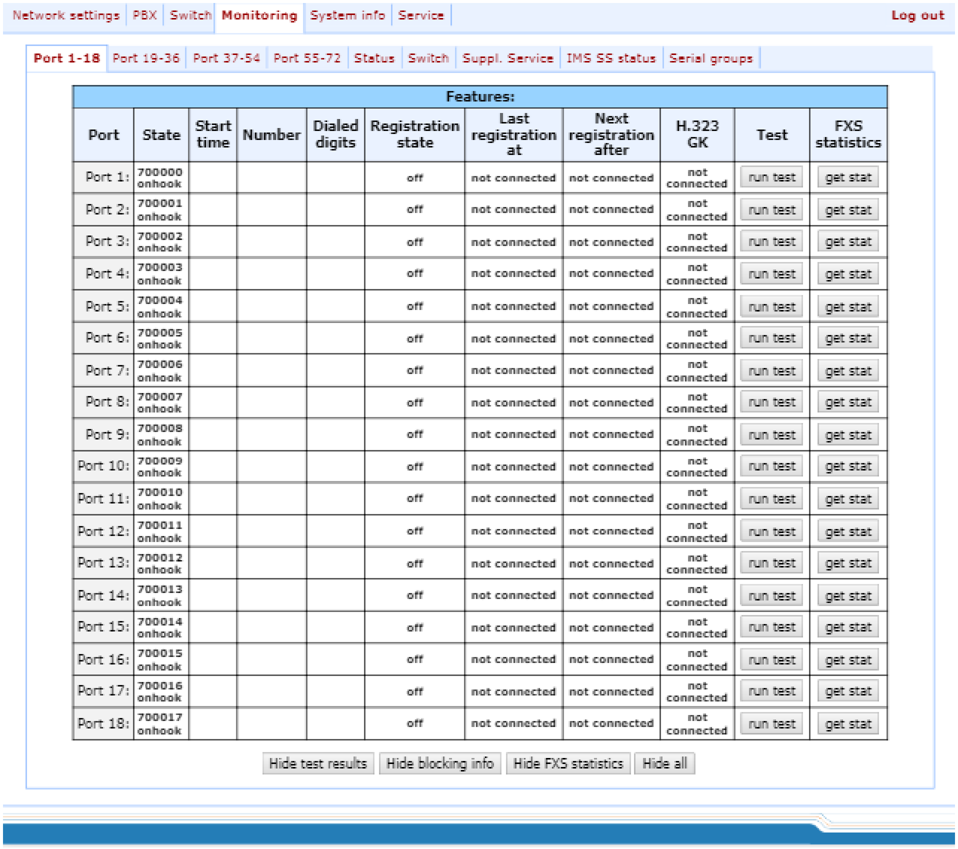
Queue 3 has the highest priority, queue 0–the lowest priority. Weighted packet distribution to outgoing queues 3/2/1/0 is as follows: 8/4/2/1.

5.1.4 The 'Monitoring' menu

In *'Monitoring'* menu, you may monitor the device status.

5.1.4.1 The 'Port' submenu Subscriber Port Monitoring

In *'Port'* submenu, you may view the information on device subscriber port status.



Features:

Port	State	Start time	Number	Dialed digits	Registration state	Last registration at	Next registration after	H.323 GK	Test	FXS statistics
Port 1:	700000 onhook				off	not connected	not connected	not connected	run test	get stat
Port 2:	700001 onhook				off	not connected	not connected	not connected	run test	get stat
Port 3:	700002 onhook				off	not connected	not connected	not connected	run test	get stat
Port 4:	700003 onhook				off	not connected	not connected	not connected	run test	get stat
Port 5:	700004 onhook				off	not connected	not connected	not connected	run test	get stat
Port 6:	700005 onhook				off	not connected	not connected	not connected	run test	get stat
Port 7:	700006 onhook				off	not connected	not connected	not connected	run test	get stat
Port 8:	700007 onhook				off	not connected	not connected	not connected	run test	get stat
Port 9:	700008 onhook				off	not connected	not connected	not connected	run test	get stat
Port 10:	700009 onhook				off	not connected	not connected	not connected	run test	get stat
Port 11:	700010 onhook				off	not connected	not connected	not connected	run test	get stat
Port 12:	700011 onhook				off	not connected	not connected	not connected	run test	get stat
Port 13:	700012 onhook				off	not connected	not connected	not connected	run test	get stat
Port 14:	700013 onhook				off	not connected	not connected	not connected	run test	get stat
Port 15:	700014 onhook				off	not connected	not connected	not connected	run test	get stat
Port 16:	700015 onhook				off	not connected	not connected	not connected	run test	get stat
Port 17:	700016 onhook				off	not connected	not connected	not connected	run test	get stat
Port 18:	700017 onhook				off	not connected	not connected	not connected	run test	get stat

Features:

– *Port*–subscriber port;

– *State*–number, configured on the port, port state, last known reason for port blocking:

- *offhook*–phone is offhook;
- *onhook*–phone is onhook;
- *dial*–dialling number;
- *ringback*–send 'ringback' tone;
- *ringing*–send 'ringing' tone;
- *talking*–call in progress;
- *conference*–3-way conference;
- *busy*–sending 'busy' tone;
- *hold*–port is on hold;
- *blocked*–port is blocked;
- *testing*–port is in testing mode.

– *Start time* – start a conversation;

– *Number* - Number(s) of the remote subscriber or two subscribers in conference mode;

– *Dialed digits*–digits dialled by the port before modification according to the routing plan;

– *Registration state*–SIP server registration status:

- *off*–registration disabled;
- *ok*–successful registration;

- *failed*–registration failed.

– *Last registration at*–last known successful registration on SIP server;

– *Next registration after*–remaining time for SIP server registration renewal;

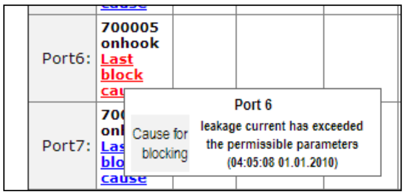
– *H.323 GK*–H.323 gatekeeper registration time;

– *Test*–testing parameters of a subscriber line corresponding to this port;

– *FXS statistic*–request statistics of voice traffic transmission for this port.

Information about the blocking

If port was in *'blocked'* state, then ***'Last block cause'*** link will be active (reason and time of the last known port blocking):



– *leakage current has exceeded the permissible parameters*–leakage current block;

– *temperature current has exceeded the permissible parameters*–temperature block;

– *power dissipation has exceeded the permissible parameters*–power dissipation block;

– *reinitialization by changing the input voltage*–port reinitialization due to input voltage fluctuations;

– *hardware reset*–hardware reset;

– *low Vbat level*–low input voltage level;

– *FXS port out of order*–port is out of order/faulty;

– *Receiver offhook*–offhook block. If the subscriber's phone is offhook, and the *'busy'* tone is played, after the expiry of two-minute interval the *'Receiver offhook'* tone will be played to the subscriber's phone, and the port will switch into the blocked state.

If the port is already in *'blocked'* state, and the ***'Last block cause'*** link is inactive, it means that the port was blocked when the phone is offhook. This blocking will be performed after the 'busy' tone is played to the subscriber's phone for two minutes. Upon the expiry of this time interval, a loud triple-tone will be played to the subscriber's phone notifying them that the phone is offhook.

To save the changes you must click the *Save* button.

When you click on the *Hide blocking* info button information on blocking will be removed.

When you click the *Hide all* button the results of tests of all types will be removed.

Port test

The ***Run test*** button, located against each port, allows to test the subscriber line associated with this port. When the button is pressed, the test will be executed (it may take up to one minute.) To see the results when the test finishes, hover the mouse cursor over the *'result'* link located against the respective port, or open the test results window by clicking the link:

Port 9 testing result	
testing result	external voltage failure
foreign DC voltage B (RING), V	0.00
foreign DC voltage A (TIP), V	0.00
line supply voltage, V	0.00
resist A (TIP) - B (RING), kOm	0.00
resist A (TIP) - GND, kOm	0.00
resist B (RING) - GND, kOm	0.00
capacity A (TIP) - B (RING), mkF	0.00
capacity A (TIP) - GND, mkF	0.00
capacity B (RING) - GND, mkF	0.00
Phone is connected	no

- *Common result*–test result status;
- *Foreign DC voltage B (RING), V*–foreign voltage in *B* wire *(RING), V;*
- *Foreign DC voltage A (TIP), V*–foreign voltage in *A* wire *(TIP), V;*
- *Line supply voltage, V*–line power supply voltage, V;
- *Ringing voltage, V*–call voltage, V;
- *Resist A (TIP)–B (RING), kOm*–resistance between *A (TIP)* and *B (RING)* wires, kΩ;
- *Resist A (TIP)-GND, kOm*–resistance between *A (TIP)* wire and ground *GND,* kΩ;
- *Resist B (RING)-GND, kOm*–resistance between *B (RING)* wire and ground *GND,* kΩ;
- *Capacity A (TIP)–B (RING), mkF*–capacity between *A (TIP)* and *B (RING)* wires, µF;
- *Capacity A (TIP)-GND, mkF*–capacity between *A (TIP)* wire and ground *GND,* µF;
- *Capacity B (RING)-GND, mkF*–capacity between *B (RING)* wire and ground *GND,* µF;
- *Phone is connected*-connected phone indication.

Do not launch the test for multiple ports simultaneously. Port test cannot be interrupted.

Test results description:

- *OK*–line test has been completed successfully;
- *TEST FAILURE*–invalid operand values were calculated during measurement. For example, division by zero has occurred. This error may appear in line resistance and capacity measurements upon the expiry of capacity measurement timeout;
- *STATE FAILURE*–occurs when the set detects leakage current, and during test, when the current line wire mismatches the required state;
- *RESISTANCE NOT MEASURED*–means that during the line resistance measurement one of the values was lower than the minimum allowed value (100Ω) As a rule, this error may be caused by a wire or ground short circuit;
- CAPACITANCE NOT MEASURED–means that during the line resistance measurement one of the values was lower than the minimum allowed value for line capacitance measurement (1800Ω). As a rule, this error may be caused by a phone offhook or a wire or ground short circuit;

– *EXTERNAL VOLTAGE FAILURE*–external voltage measured in line wires falls outside of allowable limits (-5V - +5V);

– TEST ERROR–test is interrupted by a processor command.

Click the H*ide test result* button to remove test result information.

When you click the *Hide all* button the results of tests of all types will be removed.

Performed Call Statistics

The ***Get stat*** button located against each port allows to get the statistics on performed calls for the specific port. Statistics form is formed by clicking on this button. To see the statistics, hover the mouse cursor over the *'results'* link located against the respective port, or open the test results window by clicking the link:

Port 9 FXS statistics	
State	onhook
Call count	0
Call phone	
Peak jitter	0
Lost packets	0
Transmitted packets	0
Transmitted octets	0
Received packets	0
Received octets	0

– *State*–current port status:

- *offhook*–phone is offhook;
- *onhook*–phone is onhook;
- *FXO offhook* – FXO port is busy;
- *FXO onhook* – FXO port is availiable;
- *dial*–dialling number;
- *ringback*–send 'ringback' tone;
- *ringing*–send 'ringing' tone;
- *talking*–call in progress;
- *conference*–3-way conference;
- *busy*–sending 'busy' tone;
- *hold*–port is on hold;
- *testing*–port is in testing mode.

– *Call count*–number of outgoing calls from the gateway startup;

– *Call phone*–last dialled number;

– *Peak jitter*–maximum jitter;

– *Lost packets*–quantity of lost packets;

– *Transmitted packets*–quantity of transferred voice packets;

– *Transmitted octets*–quantity of bytes in transferred voice packets;

– *Received packets*–quantity of received voice packets;

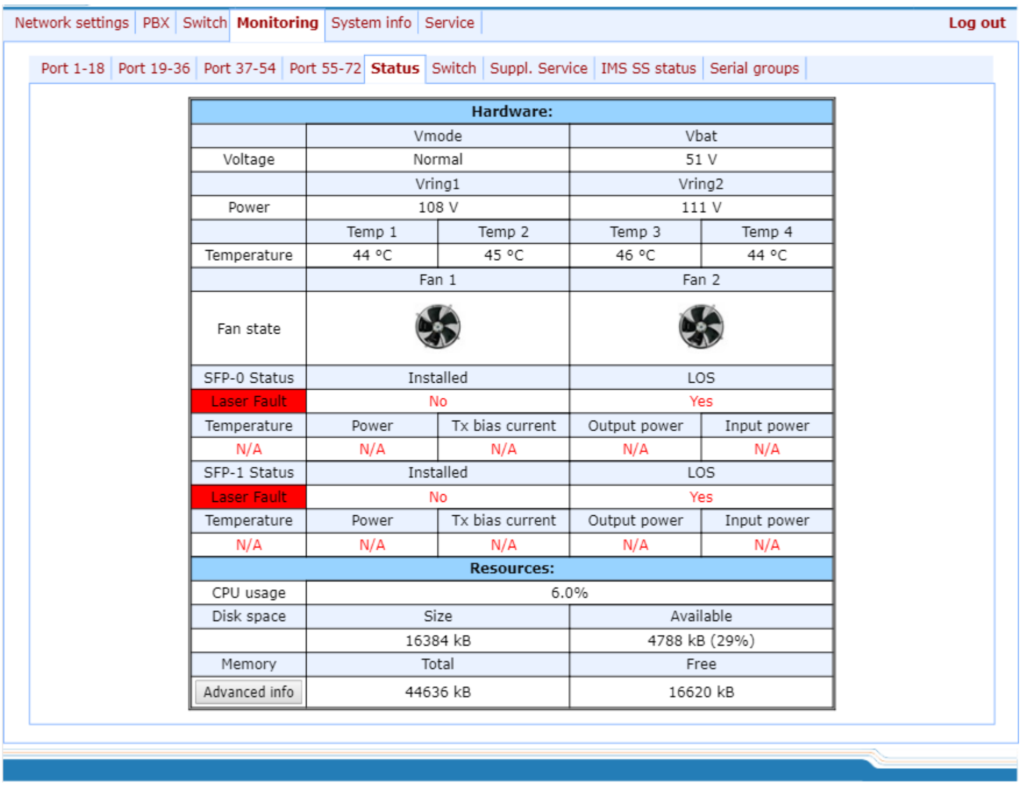
– *Received octets*–quantity of bytes in received voice packets;

When you click the *Hide FXS statistics* button, generated statistics on performed calls on this port will be deleted.

When you click the *Hide all* button the results of tests of all types will be removed.

5.1.4.2 The 'Status' submenu Board Parameter Status Monitoring

In the *'Status'* submenu, you can monitor physical parameters: of the board and SFP modules supporting DDM (digital diagnostics monitoring) function.



Hardware:				
	Vmode		Vbat	
Voltage	Normal		51 V	
	Vring1		Vring2	
Power	108 V		111 V	
	Temp 1	Temp 2	Temp 3	Temp 4
Temperature	44 °C	45 °C	46 °C	44 °C
	Fan 1		Fan 2	
Fan state				
SFP-0 Status	Installed		LOS	
Laser Fault	No		Yes	
Temperature	Power	Tx bias current	Output power	Input power
N/A	N/A	N/A	N/A	N/A
SFP-1 Status	Installed		LOS	
Laser Fault	No		Yes	
Temperature	Power	Tx bias current	Output power	Input power
N/A	N/A	N/A	N/A	N/A
Resources:				
CPU usage	6.0%			
Disk space	Size		Available	
	16384 kB		4788 kB (29%)	
Memory	Total		Free	
Advanced info	44636 kB		16620 kB	

<u>*Table 'Hardware'–platform sensor parameters:*</u>

– *'Parameter'*–controlled parameters;

– *'Value'*–controlled parameters' values:

– *Power, V* - device power supply parameters:

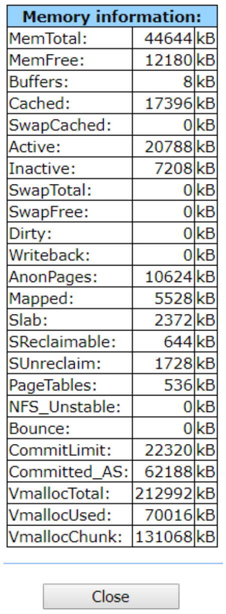
- *Vmode* - subscriber unit power supply mode, V;
- *Vbat* - secondary supply circuit voltage, V.
  Low - secondary supply circuit voltage is less than 44 V, units operating in low voltage mode.
  Normal - secondary supply circuit voltage is 44 V < Vbat < 55 V, units operating in normal voltage mode.
  Normal - secondary supply circuit voltage is more than 55 V, units operating in high voltage mode.

It is highly recommended not to use high voltage mode. It may cause subscriber unit overheat.

- *Power, V* - voltage generated by inductor, V. The device contains two magneto ringing sources: first is working with sets of 1-36, the second - with 37-72;
- *Temperature, °C*–temperature measured by sensors (each submodule has its own temperature sensor);
- *Fan state:*
  -  - fan enabled;
  -  - fan disabled;
  - Image  flashes periodically - fan failure.

Fans automatically enable when the temperature is more than 55°C and disable when the temperature is less than 45°C.

- *SFP-0 Status, SFP-1 Status*–status of SFP0 optical module:
  - *Installed*–indication of module installation ('Yes'–module is installed, 'No'–module is not installed);
  - *LOS*–indication of signal loss ('No'–no loss);
  - *Temperature, °C*–optical module temperature;
  - *Power, V*–optical module power supply voltage, V;
  - *Tx bias current, mA*–transmission bias current, mA;
  - *Output power, mW*–output power, mW;
  - *Input power, mW*–input power, mW.



Memory information:		
MemTotal:	44644	kB
MemFree:	12180	kB
Buffers:	8	kB
Cached:	17396	kB
SwapCached:	0	kB
Active:	20788	kB
Inactive:	7208	kB
SwapTotal:	0	kB
SwapFree:	0	kB
Dirty:	0	kB
Writeback:	0	kB
AnonPages:	10624	kB
Mapped:	5528	kB
Slab:	2372	kB
SReclaimable:	644	kB
SUnreclaim:	1728	kB
PageTables:	536	kB
NFS_Unstable:	0	kB
Bounce:	0	kB
CommitLimit:	22320	kB
Committed_AS:	62188	kB
VmallocTotal:	212992	kB
VmallocUsed:	70016	kB
VmallocChunk:	131068	kB

<u>*Resources–monitoring of system resources:*</u>

- *CPU usage* – percentage of CPU utilization;
- *Disk space* – information on disk space:
  - *Size* – disk space in kbytes;
  - *Available* – amount of free disk space in kbytes;
- *Memory* – amount of RAM:
  - *Total* – total amount of RAM in kbytes;
  - *Free* – free amount of RAM in kbytes.

Click the *Advanced info* button to open the window with advanced information on RAM utilization.

<u>*Permitted parameter values:*</u>

- Primary supply voltage should fall within the limits: *38 V < Vbat < 72 V;*
- Ringer supply voltage should fall within the limits: *100 V < Vring1 < 120 V* and *100 V < Vring2 < 120 V*;
- Temperature on a sensor should not exceed *90 °C*.

Fault indication:

– When the sensor malfunction occurs, the *'temperature detector failure'* value will blink red in its window.

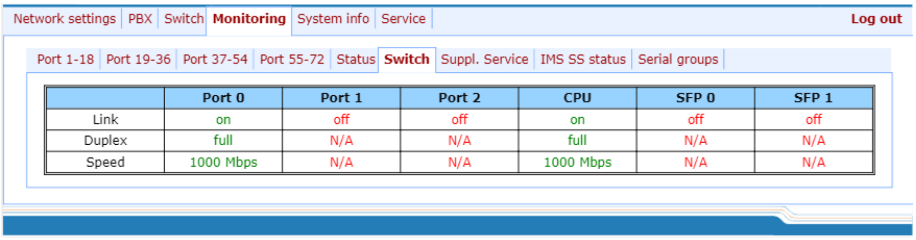
– Value falling outside of allowable limits will blink red.

– When the fan is out of order, a crossed out circle will blink.

5.1.4.3 The 'Switch' submenu. Switch port status monitoring

In *'Switch'* submenu, you may view status of integrated Ethernet switch ports.

The switch is equipped with 3 Gigabit Ethernet electrical ports (Port 0, Port 1, Port 2), 1/2[1] optical port (SFP 0, SFP 1), designed for connection to data networks and additional Ethernet devices, and 1 internal CPU port for connection to TAU HOST processor.



	Port 0	Port 1	Port 2	CPU	SFP 0	SFP 1
Link	on	off	off	on	off	off
Duplex	full	N/A	N/A	full	N/A	N/A
Speed	1000 Mbps	N/A	N/A	1000 Mbps	N/A	N/A

– *Link* – port state:

- *off* – port is inactive (no connection);
- *on* – port is active (connection established).

– *Duplex*–transceiver operation mode:

- *N/A* – value is not available, as the link is inactive;
- *Full* – full duplex;
- *half* – half-duplex.

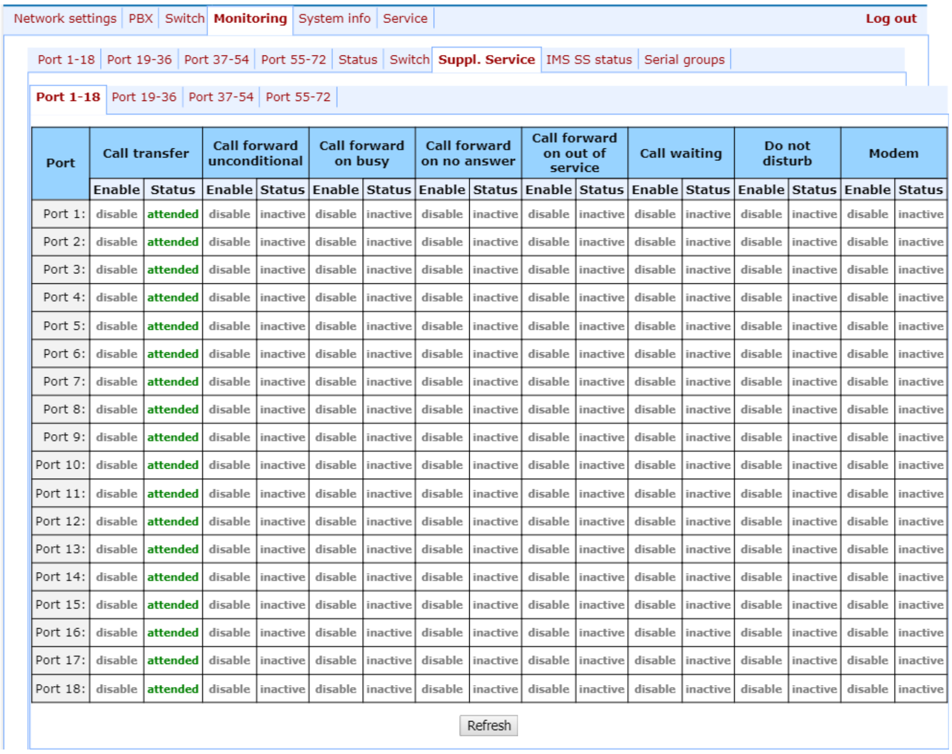
– *Speed* – data transfer rate for a port (*10 Mb, 100 Mb, 1000 Mb*):

- *N/A* – value is not available, as the link is inactive;
- *10 Mb, 100 Mb, 1000 Mb.*

[1] For TAU-36.IP/TAU-72.IP v1, v2 appears status of one optic Ehernet port.

5.1.4.4 The 'Suppl. Service' submenu. Supplementary Service Status Monitoring

In *Suppl. Service* submenu, you can view the current status of supplementary services for subscriber ports of the device.



Port	Call transfer		Call forward unconditional		Call forward on busy		Call forward on no answer		Call forward on out of service		Call waiting		Do not disturb		Modem	
	Enable	Status	Enable	Status	Enable	Status	Enable	Status	Enable	Status	Enable	Status	Enable	Status	Enable	Status
Port 1:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 2:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 3:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 4:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 5:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 6:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 7:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 8:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 9:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 10:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 11:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 12:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 13:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 14:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 15:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 16:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 17:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive
Port 18:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive

– *Enable* – service state (*'enable'*–enabled, *'disable'*–disabled);

– *Status* – service status:

There are three status types for *'Call transfer'* service:

- *Attended* —*'Call Transfer'* service is enabled for the port with the wait for response of the subscriber, the call is being forwarded to;
- *Unattended*—'Call Transfer' service is enabled for the port without the wait for response of the subscriber, the call is being forwarded to;
- *Off* – 'Call transfer' service is disabled.

For *'Call forward'* service, define the number configured for the call forwarding in the status field.

- *Call transfer* – 'Call transfer' service;
- *Call forward unconditional* – 'Call forward unconditional' service;
- *Call forward on busy* – 'Forward on busy' service;
- *Call forward on no answer* – 'Forward on no answer' service;
- *Call forward on out of service* – 'Forward on out of service' service;
- *Call waiting* – 'Call waiting' service;
- *Do not disturb* – 'Do not disturb' service;
- *Modem* – 'Modem' service.

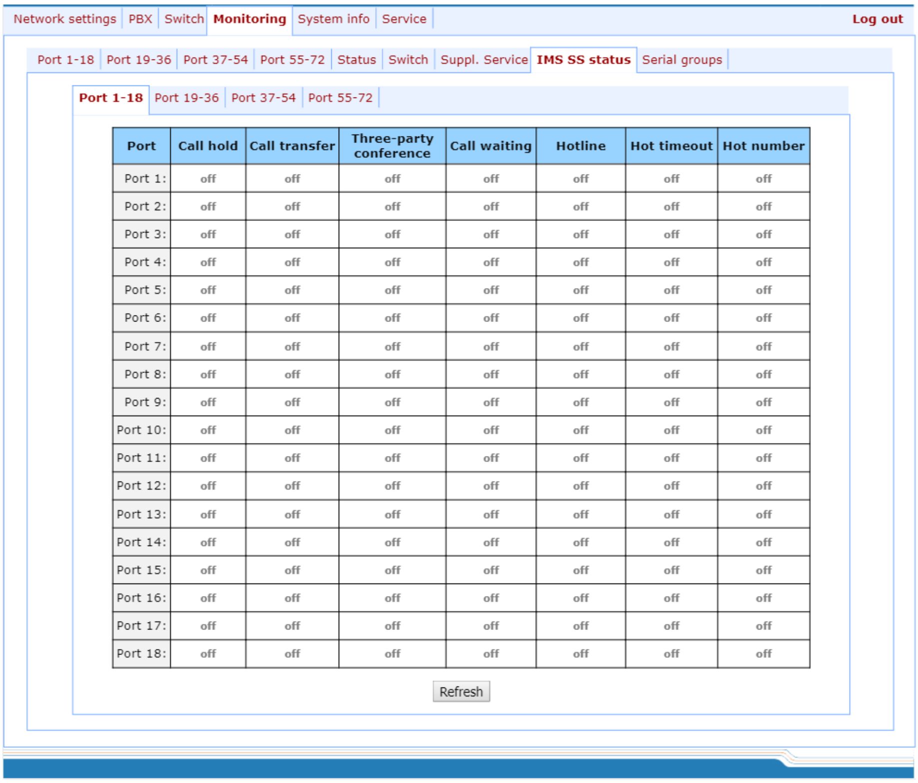
Status for other services:

- *Active* – enabled;
- *Inactive* – disabled.

Use the *Refresh* button to refresh table data.

5.1.4.5 The 'IMS service status' submenu. IMS SS status Monitoring

In *'IMS SS status'* menu, you may view the current state of services managed by the Softswitch with IMS support.



Port	Call hold	Call transfer	Three-party conference	Call waiting	Hotline	Hot timeout	Hot number
Port 1:	off	off	off	off	off	off	off
Port 2:	off	off	off	off	off	off	off
Port 3:	off	off	off	off	off	off	off
Port 4:	off	off	off	off	off	off	off
Port 5:	off	off	off	off	off	off	off
Port 6:	off	off	off	off	off	off	off
Port 7:	off	off	off	off	off	off	off
Port 8:	off	off	off	off	off	off	off
Port 9:	off	off	off	off	off	off	off
Port 10:	off	off	off	off	off	off	off
Port 11:	off	off	off	off	off	off	off
Port 12:	off	off	off	off	off	off	off
Port 13:	off	off	off	off	off	off	off
Port 14:	off	off	off	off	off	off	off
Port 15:	off	off	off	off	off	off	off
Port 16:	off	off	off	off	off	off	off
Port 17:	off	off	off	off	off	off	off
Port 18:	off	off	off	off	off	off	off

– *Port* – subscriber port number;

<u>*Services:*</u>

– *Call hold – 'Call hold'* service status;

– *Call transfer – 'Call transfer'* service status;

– *Three-party conference – '3-way Conference'* service status;

– *Call waiting – 'Call waiting'* service status;

– *Hotline – 'Hotline/warmline'* service status;

– *Hot timeout* – delay timeout in seconds for the start of the automatic dialling when the *'Hotline/warmline'* service is enabled;

– *Hot number* – number that will receive the call when 'Hotline/warmline' is enabled.

<u>*Service statuses:*</u>

– *Off* – IMS management is disabled;

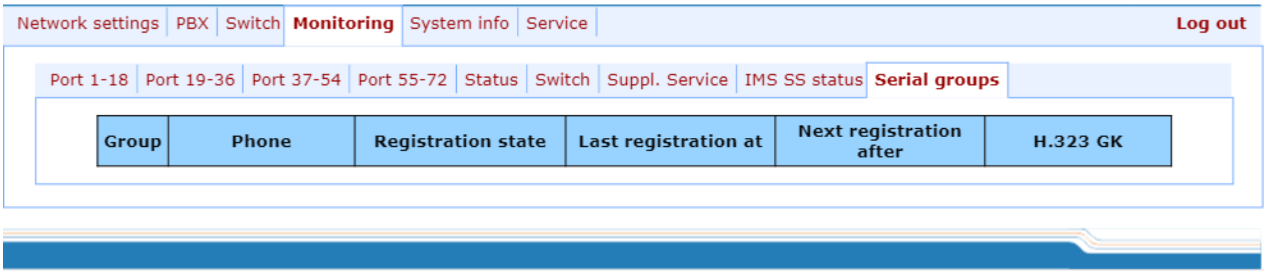
– *Disable* – service is disabled;

– *Enable* – service is enabled.

Use the *'Refresh'* button to refresh data.

5.1.4.6 The *'Serial groups'* submenu. *Serial Group Registration Status Monitoring*

In *'Serial groups'* menu, you may view the current state of serial group registration.



Description of informational window:

– *Group* – group sequential number;

– *Phone* – call group subscriber number;

– Registration state – *SIP server registration status:*

  - *Off* – registration disabled;
  - *Ok* – successful registration;
  - *Failed* – registration failed.

– *Last registration at* – last known successful registration on SIP server;

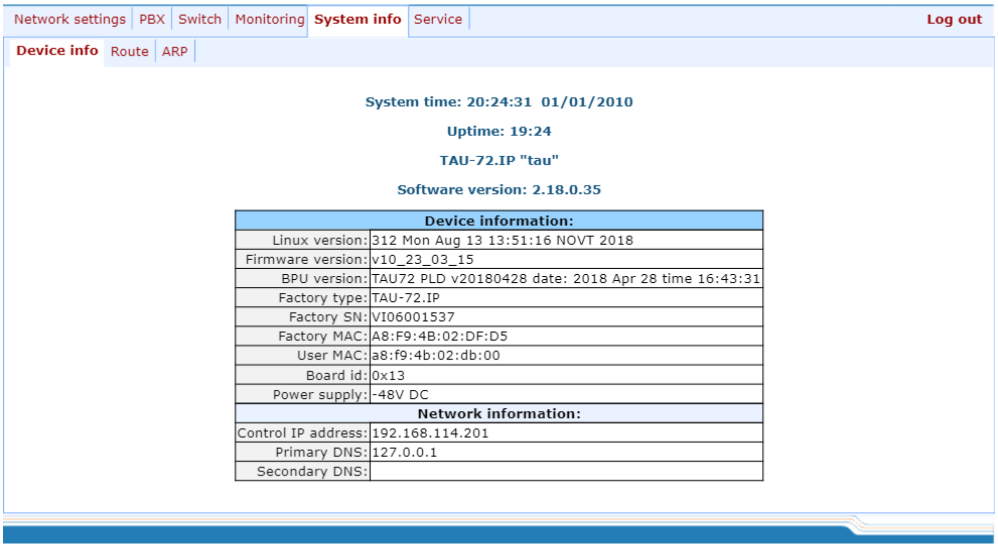
– *Next registration after* – remaining time for SIP server registration renewal;

– *H.323 GK* – H.323 gatekeeper registration time.

5.1.5 The 'System info' menu

5.1.5.1 The 'Device info' submenu

In *'System info'* menu, you can view the system information.



– *System time*–device system date and time in the following format: hours:minutes:seconds day/month/year;

– *Uptime*–time of the uninterrupted gateway operation;

– *TAU-72.IP/TAU-36.IP* – firmware version;

– *Software Version*–device firmware version.

<u>*Device information*</u>

– *Linux version*–Linux OS version;
– *Firmware version*–media processor firmware version;
– *BPU version*–hardware version;
– *Factory type, SN, MAC*–factory settings;
– *User MAC*–MAC address, defined by user. In this case, factory MAC address will be ignored. You can specify MAC address from the CLI console only;
– *Board id*–hardware platform version;
– *Power supply*–type of power supply installed (AC or DC).

<u>*Network information*</u>

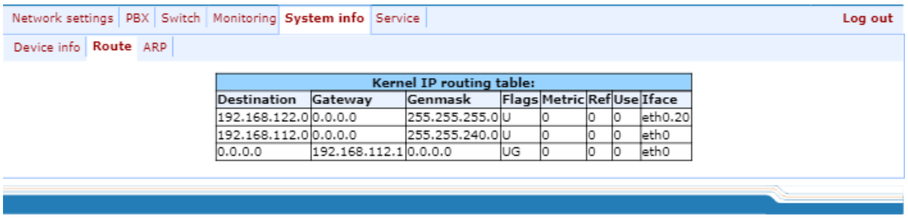
– *Control IP-address*–IP address of the device used for management purposes;

– *Primary DNS*–primary DNS server address;

– *Secondary DNS*–secondary DNS server address.

5.1.5.2 The 'Route' submenu

In the *'Route'* menu, you can view the current routing table.



Kernel IP routing table:

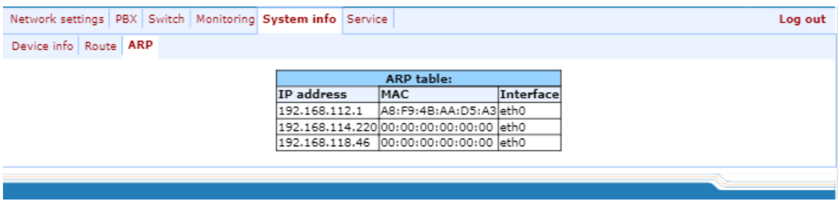
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.122.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0.20
192.168.112.0	0.0.0.0	255.255.240.0	U	0	0	0	eth0
0.0.0.0	192.168.112.1	0.0.0.0	UG	0	0	0	eth0

<u>*Kernel IP routing table:*</u>

- *Destination* – destination network of host address;
- *Gateway* – gateway representing a router network address that should receive the packet transferred to the defined destination address;
- *Genmask* – destination network mask;
- *Flags* – describes route properties. For the specific route, may be defined the following flags:
  - *U* – route is active;
  - *G* – route is directed to the gateway;
  - *H* – route is directed to the host, i.e. complete host address is defined as a destination. If this flag is missing, destination is a network address.
  - *D* – route was created by forwarding;
  - *M* – route was modified by forwarding.
- *Metric* – numeric index that defines the route preferability. The less the number, the higher the preferability of the route;
- *Ref* – number of references to the route for connection creation;
- *Use* – number of route discoveries performed by IP protocol;
- *Iface* – device network interface used for access through this route.

5.1.5.3 The 'ARP' submenu

In *'ARP'* menu, you can view the device ARP table.



ARP table:

IP address	MAC	Interface
192.168.112.1	A8:F9:4B:AA:D5:A3	eth0
192.168.114.220	00:00:00:00:00:00	eth0
192.168.118.46	00:00:00:00:00:00	eth0

ARP table

- *IP address*–IP address of destination host;
- *MAC*–MAC address of destination host;
- *Interface*–network interface, that the destination host is available through.

5.1.6 The 'Service' menu

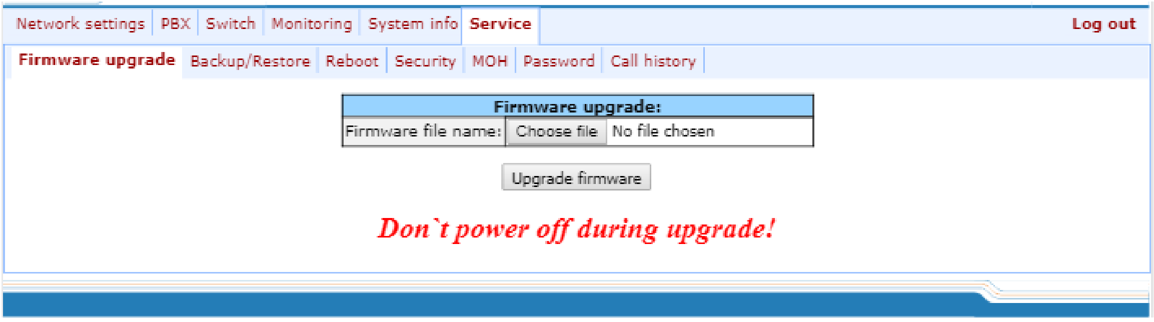
In *'Service'* menu, you may update the firmware, work with configuration files and other service features.

5.1.6.1 The 'Firmware upgrade' submenu

In the *'Firmware upgrade'* tab, you may update the firmware of the subscriber units.

For versions earlier than September, 2010 it is not permitted to update file system and Linux core simultaneously!

Updating from version, earlier 1.11.x should be processed according to the instruction, listed in the start of this manual.



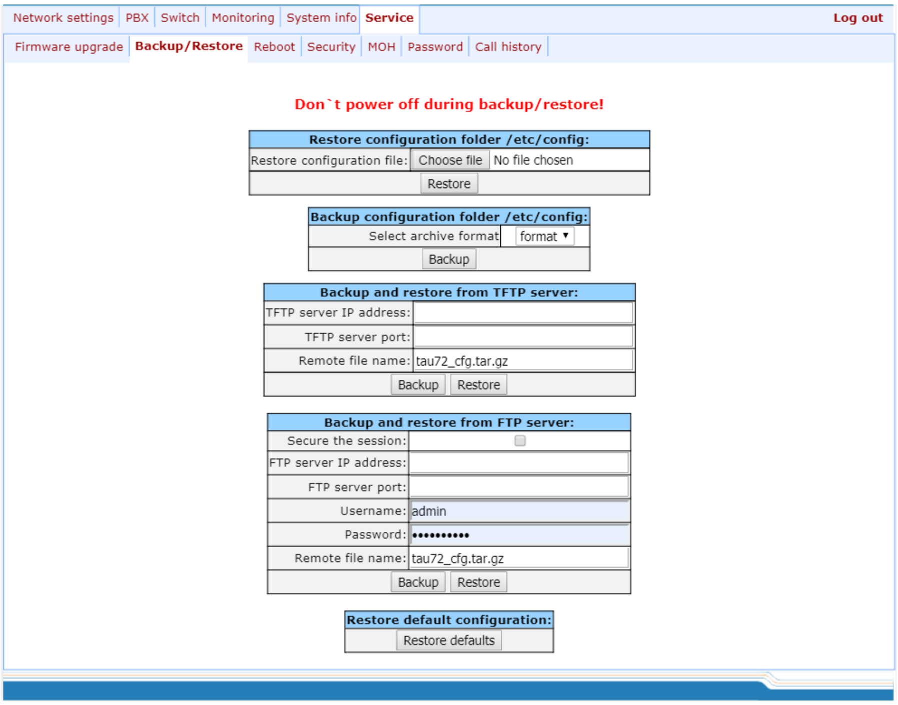
In *'Firmware upgrade'* section, you can update the TAU-72.IP/TAU-36.IP firmware (firmware file is an image named ***firmware.img***).

In the opened window, specify the path to the firmware file by clicking the *Select File* button and click the *Upgrade firmware* button.

5.1.6.2 The Download/Upload Configuration (Backup/Restore) submenu

In the *'Backup/Restore'* submenu, you may download/upload configuration files. We have implemented 3 ways to download/upload configuration files:

1. Using Web configurator;
2. Using TFTP server;
3. Using FTP server.



1. ***Download/upload configuration files using web configurator***

Restore configuration folder /etc/config section description:

– *Restore configuration file*–configuration file that should be uploaded to device from PC.

To upload the configuration file: select the configuration file in the *'Restore configuration file'* field using the *Select file* button (file name should be as follows: tau72_cfg, with tar, or tar.gz extension) and click *Restore.*

Backup configuration folder /etc/config section description:

– *Backup configuration folder /etc/config*–download configuration to PC (configuration files will be saved on a PC in archive tau72tar, or tau72_cfg.tar.gz depending on the selected format).

  To download configuration files or other folders to a PC, click the *Backup* button.

2. ***Download/upload files using TFTP server***

Backup/Restore from TFTP server:

– *TFTP Server IP Address*–TFTP server IP address;

– *TFTP Server Port*–TFTP server port number;

– *Remote File Name*–uploaded or downloaded file name.

Click the *Restore* button, to upload configuration files from TFTP server to device. Click the *Backup* button to download files from device to TFTP server.

3. Download/upload files using FTP server

Backup/Restore from FTP server:

- *Secure The Session*-when checked FTP server connection is secured using TLS (work by FTPS protocol), otherwise use unsecured connection (work by FTP protocol). To use FTPS protocol certificate should be generated in Service-Security menu;
- *FTP Server IP Address*–FTP server IP address;
- *FTP Server Port*–FTP server port number;
- *User Name* – username;
- *Password* – password;
- *Remote File Name*–uploaded or downloaded file name.

Click the *Restore* button, to upload configuration files to device. Click the *Backup* button to download files from device.

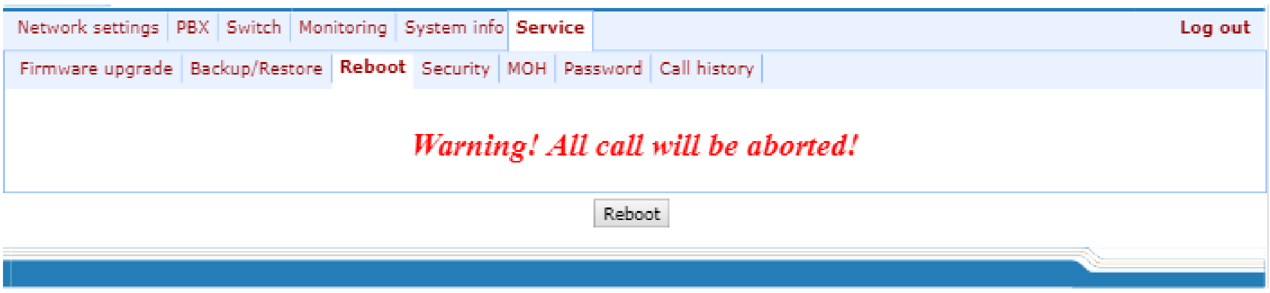
Click the *Restore default* button to reset the configuration to factory defaults.

When configuration resets to factory defaults, the device will be restarted automatically.

After you upload a new configuration using any of these methods, restart the device by clicking the *Reboot* button in the *'Reboot'* submenu.

5.1.6.3 The 'Reboot' submenu

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

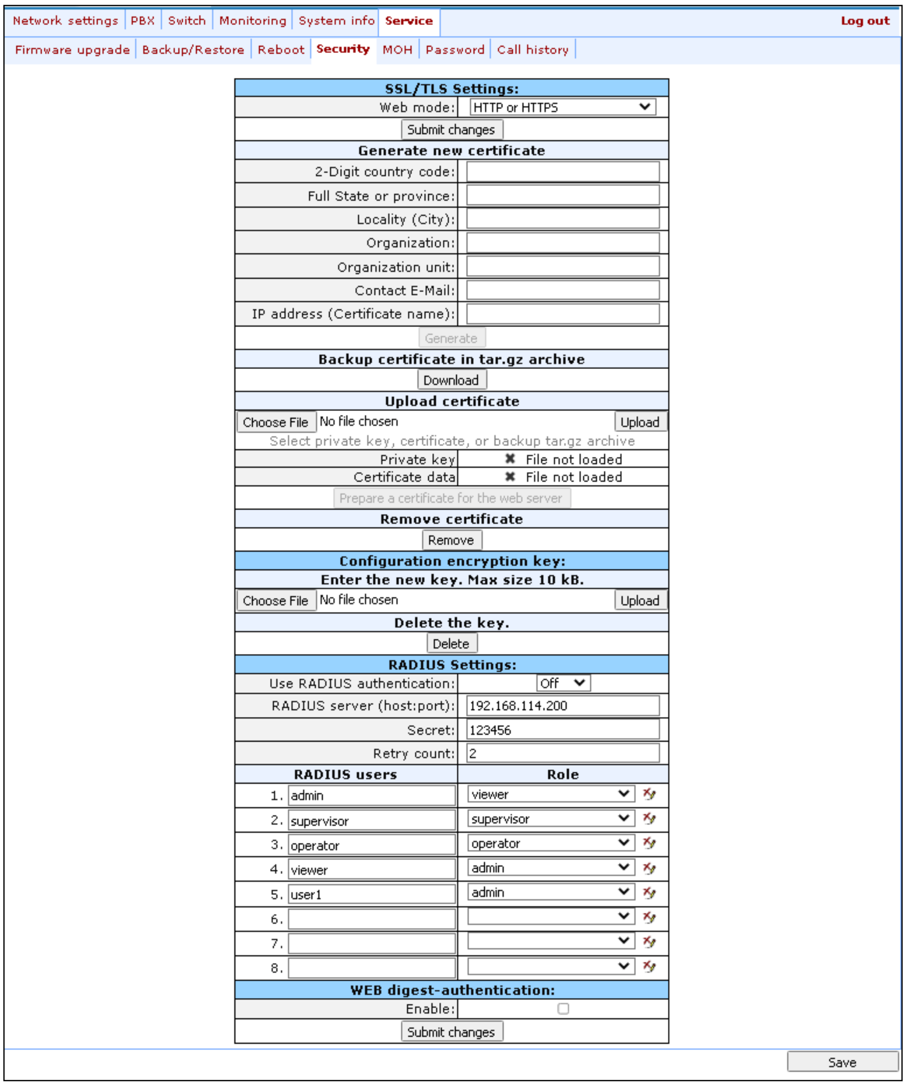


To reboot the device, click the *Reboot* button.

Before performing a reboot, make sure that all changes are saved, otherwise they will be lost.

5.1.6.4 The 'Security' submenu

In the *'Security'* submenu, you may obtain a self-signed certificate, which allows you to use an encrypted connection to the gateway via HTTP protocol and configuration file upload/download via FTPS protocol.



<u>*SSL/TLS settings:*</u>

– *WEB mode* – WEB configurator connection mode:

- *HTTP or HTTPS* – unencrypted connection–via HTTP–as well as encrypted connection–via HTTPS–is enabled. At that, connection via HTTPS is possible only when generated certificate is present;
- *HTTPS only* – only encrypted connection via HTTPS is enabled. Connection via HTTPS is possible only when generated certificate is present;

After making changes to the connection mode by the Web configurator, click the *Submit changes* button.

Generate new certificate:

- *2-Digit country code* – 2-digit code;
- *Full State or province* – location (region);
- *Locality (City)* – location (city);
- *Organization* – organization name;
- *Organization unit* – organization unit;
- *Contact E-Mail* – e-mail address;
- *IP address (Certificate name)* – gateway IP address.

When you enter all fields, click the *Generate* button to generate self-signed certificate.

Backup certificate in tar.gz archive:

To backup a certificate, click '*Download*'.

Upload certificate:

To upload a certificate and a private key to the device, select file with the certificate and the key by clicking '*Choose File*', then click '*Upload*'. The uploaded file will be displayed. Then click '*Prepare a certificate for the web server*'.

Remove certificate:

To remove certificate on the device, click '*Remove*'.

Configuration encryption key:

The key is used for configuration file encryption/decryption during its upload to/download from the device. When key is not defined, encryption will not work.

Encryption uses AES-256 algorithm.

For configuration file decryption on a PC, you may use *openssl* utility.
Usage: *openssl enc -aes-256-cbc -d -pass pass:'Password' -in 'encrypted file' -out 'decrypted file'*

To upload a new encryption key *'Enter the new key' max size 10 kB*, specify path to file to be uploaded to the device using the *Select file* button and click *'Upload'*.

To delete or change previously uploaded key, specify the path to the encryption key using the *'Browse'* button and then click *'Get access'*.

RADIUS Settings:

– *Use RADIUS authentication*–use RADIUS server for authentication of users administering the device via WEB, telnet, SSH. Parameter can take the following values:

  - *Disable*-disable;
  - *Strict*-authentication on RADIUS server. When out of service, no answer or denied server reply receiving local authorisation is disabled;
  - *Flexible*-authentication on RADIUS server. When out of service, no answer or denied server reply receiving local authorisation is enabled.

– *RADIUS server (host:port)*–RADIUS server IP address;

– *Password (Secret)*–password used by client to access the RADIUS server;

– *Retry count*–number of retries during the access to RADIUS server. If the server authorization has failed, you will be able to manage the device via the local COM port only.

On RADIUS server, you may configure passwords for any of the system users: admin, operator, supervisor, viewer. For detailed information on user privileges, see Section 5.1.6.6 The 'Passwords' submenu.

WEB digest-authentication configuration:

– *Enable*-enables WEB users digest-authentication.

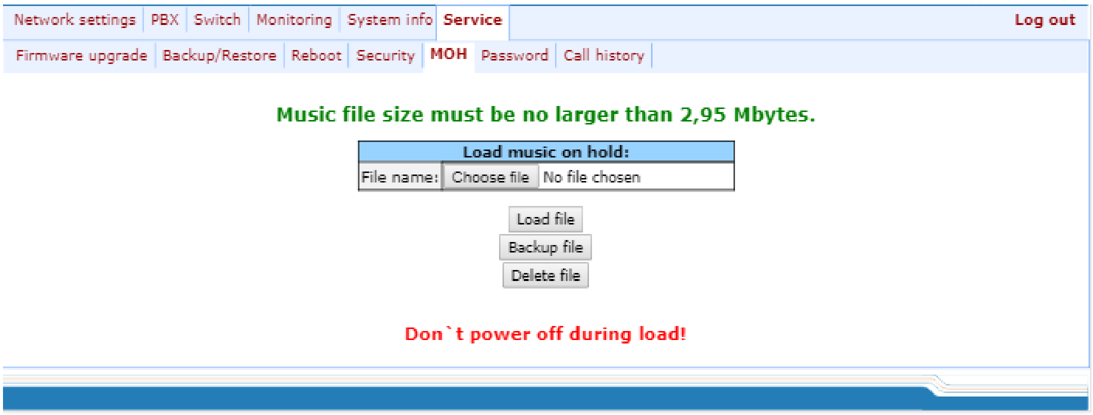
In this mode WEB authorisation through RADIUS will be unavailable

To save the changes click the *Save* button.

5.1.6.5 The 'MOH' submenu

In *'MOH'* submenu, you may upload/download audio file to/from the device in order to enable *'Music on Hold'* service. To activate *'Music on Hold'* service, select *'Play music on hold'* checkbox in subscriber port settings.

The service works correctly only when using G.711A and G.711U codecs.



– *Select file* – specify a file to upload to the device.

Audio file requirements:

Format: CCITT A-law
Attributes: 8000 kHz, 8 Bit, Mono
File extension: wav

To recode the file to the necessary format, you may use ffmpeg or any other conversion application.

Example use of ffmpeg:

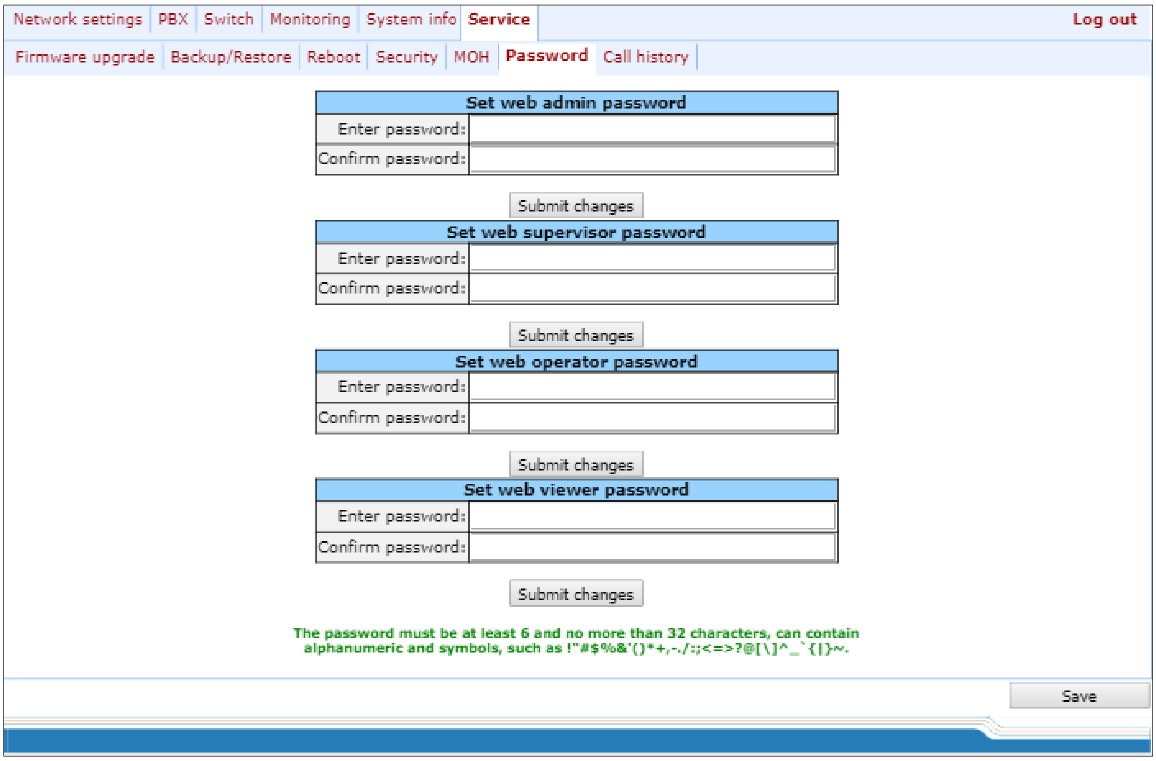
ffmpeg -fs <X>**M -i** <inputfilename> **-ar 8000 -acodec pcm_alaw -ac 1** <outputfilename>

where:
'X'–file size limit,
'inputfilename'–input file name,
'outputfilename'–output file name.

- *Load file* – button that allows you to upload the file to the device;
- *Backup file* – button that allows you to download the file to PC;
- *Delete file* – button that allows you to delete the file from the device.

5.1.6.6 The 'Passwords' submenu

In *'Passwords'* submenu, you may work with passwords for device access via Web interface.



<u>*Access passwords operations:*</u>

- *Set WEB admin password* – administrator password for device access via CLI or web interface (*admin* user);
- *Set supervisor password* – supervisor password for device access via CLI or web interface (*supervisor user*);
- *Set operator password* – operator password for device access via CLI or web interface (*operator* user);
- *Set viewer password* – viewer password for device access via CLI or web interface (*viewer* user).

CLI password become same with WEB password when updating firmware with versions 2.17 or lower to the higher versions.

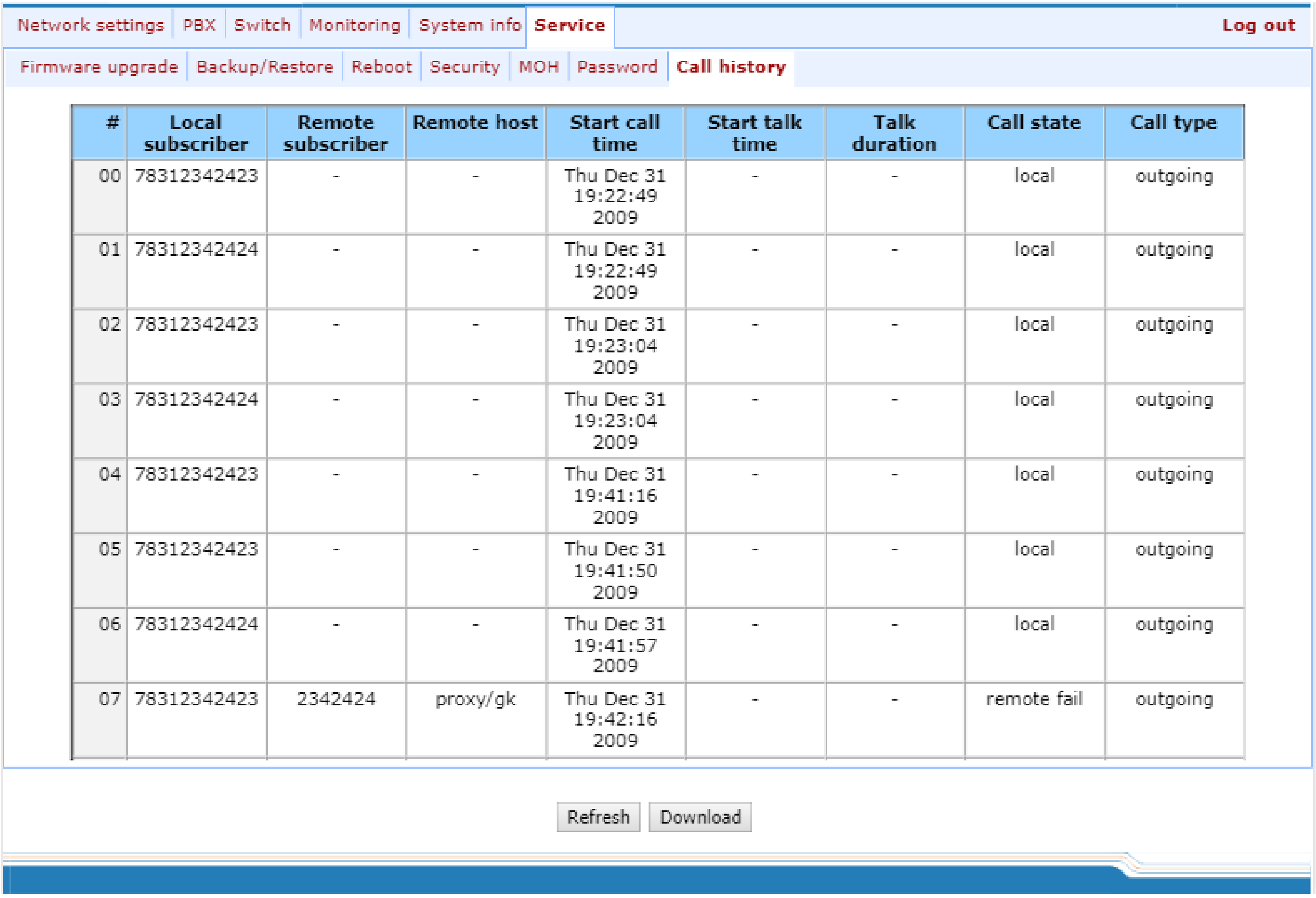
<u>*User rights:*</u>

- *admin* – has full access to the device;
- *supervisor* – will be able to access all device parameters in read-only mode;
- *operator* – will be able to access the device for monitoring, viewing the system information, and also for configuration of protocols, routing settings, subscriber ports and groups;
- *viewer* – will be able to access the device for monitoring and viewing the system information.

To change the password, enter a new password into *'Enter password'* field, and enter it again into 'Confirm password' field. To apply password, click the *Submit Changes* button. To save the changes click the *Save* button.

5.1.6.7 The 'Call history' submenu

In the *'Call history'* submenu, you may work with call log.



#	Local subscriber	Remote subscriber	Remote host	Start call time	Start talk time	Talk duration	Call state	Call type
00	78312342423	-	-	Thu Dec 31 19:22:49 2009	-	-	local	outgoing
01	78312342424	-	-	Thu Dec 31 19:22:49 2009	-	-	local	outgoing
02	78312342423	-	-	Thu Dec 31 19:23:04 2009	-	-	local	outgoing
03	78312342424	-	-	Thu Dec 31 19:23:04 2009	-	-	local	outgoing
04	78312342423	-	-	Thu Dec 31 19:41:16 2009	-	-	local	outgoing
05	78312342423	-	-	Thu Dec 31 19:41:50 2009	-	-	local	outgoing
06	78312342424	-	-	Thu Dec 31 19:41:57 2009	-	-	local	outgoing
07	78312342423	2342424	proxy/gk	Thu Dec 31 19:42:16 2009	-	-	remote fail	outgoing

Description of record fields:

– *#* - number of record;

– *Local subscriber*-gateway subscriber phone number;

– *Remote subscriber*-oncoming gateway subscriber phone number;

– *Remote host*-remote gateway network address;

– *Call start time*-incoming or outgoing call start time;

– *Conversation start time*-conversation start time after one subscriber's call reply;

– *Conversation duration*-time interval between subscriber's call reply and cal clearback;

– *Call status* - current call status (call, conversation, etc.);

– *Call direction*-incoming or outgoing call on gateway.

To update call list press *Update* button in log. To upload call list press *Upload* button.

5.1.6.8 User change

To change a user, click *'Log out'* link.

To change the access, enter the corresponding user name (admin, operator, viewer), password (passwords for various access levels are defined by 'admin' user in ***'Service/Password'*** tab) and click the *Log in* button.

5.2 Configuration via WEB Interface. Operator Access

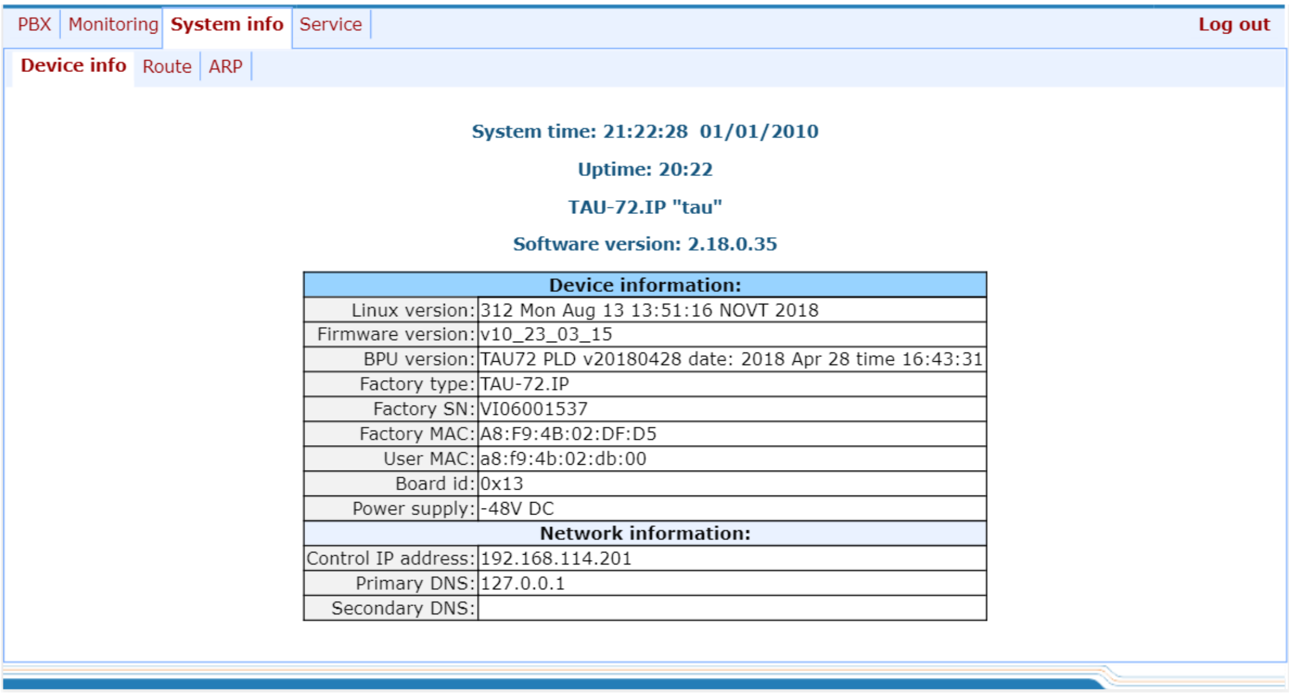
To configure the device, establish connection in the *web browser*, e.g. Firefox, Internet Explorer. Enter the device IP address into address bar of web browser.

TAU-36.IP/TAU-72.IP factory default IP address — 192.168.1.2, network mask — 255.255.255.0

After entering IP address the device will request username and password.

Username: ***operator***
Password: ***specified by admin.***

The following menu will appear on the operator's terminal:



Web configurator supports indication of configuration changes that is shown in the header bar of configuration interface (TAU-72.IP/TAU-36.IP WEB configurator). Table 5 lists indicator states ('*' character in the header bar of configuration interface).

In all tabs, the *Save* button stores configuration into the non-volatile (flash) memory of the device.

Operator will be able to view and edit routing and subscriber port configuration.

lists web configurator menu tabs available to the operator. For detailed web configurator description, see Section 5.1 of this document.

Table 9 - Description of configuration menu, operator access

Menu (en)	Menu (ru)	Description
PBX	***PBX***	**VoIP (Voice over IP) configuration**
Main	*Основные функции*	device basic settings
SIP/H323 Profiles	*Профили SIP/H323*	Configuration of SIP/H323 profiles
SIP Common	*SIP Общие*	SIP common settings

H323	*H323*	H323 protocol settings (works in profile 1 only)
Profile 1..8	*Профиль 1..8*	configuration of profiles
SIP Custom	*SIP настройки профиля*	SIP custom settings for a profile
Codecs	*Кодеки*	codec settings for a profile
Dialplan	*План набора*	routing settings for a profile
Alert info	*Alert info*	Configuration of a distinctive ring, formed by Alert Info value
TCP/IP	*TCP/IP*	configuration of network port range for various protocols
Ports	*Абонентские порты*	configuration of device subscriber ports and subscriber profiles
Call limits	*Ограничение вызовов*	configuration of simultaneous call limits
Suppl. Service Codes	*Услуги ДВО*	Configuration of supplementary service codes
Serial groups	*Группы вызова*	configuration of serial groups
PickUp groups	*Группы перехвата*	configuration of pickup groups
Distinctive ring	*Звонок особого типа*	'Distinctive ring' service administration
Modifiers	*Модификаторы*	configuration of number modifiers
Acoustic signals	*Акустические сигналы*	configuration of acoustic signals parameters
Dialplan profiles	*Профили плана нумерации*	configuration of profiles for routing
Profile 1..4	*Профиль 1..4*	configuration of profiles
Monitoring	***Мониторинг***	**device monitoring**
Port	*Порт*	device subscriber ports status information
Status	*Статус*	Gateway hardware platform status information–voltages, temperature sensors, fans, SFP data
Switch	*Коммутатор*	switch port status monitoring
Suppl. Service	*ДВО*	Information on the current status of supplementary services on subscriber port
IMS SS status	*Статус услуг IMS*	Monitoring of services, software controlled switch with support for IMS
Serial groups	*Группы вызова*	monitoring of registration serial groups
System info	***Информация о системе***	**system info**
Device info	*Информация об устройстве*	View the device and network settings information
Route	*Таблица маршрутизации*	Routing table configuration
ARP	*ARP*	ARP table configuration
Service	***Сервисные функции***	**firmware update, configuration file operations, rebooting device, setting/changing passwords**
Reboot	*Перезагрузка*	rebooting device
Call history	*Журнал вызовов*	view and upload of call log
Logout	***Выход***	**Finish the device administration session for the current user**

Before performing a reboot, make sure that all changes are saved, otherwise they will be lost.

5.3 Non-privileged user access for device monitoring

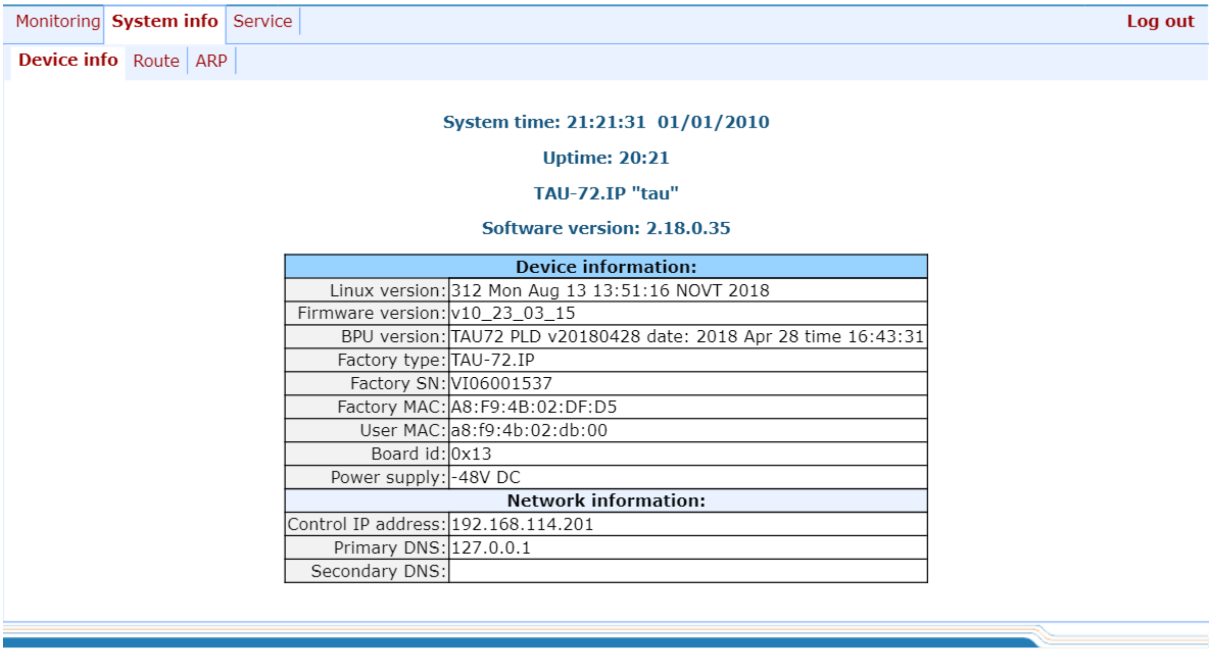
To monitor the device, establish connection in the web browser (hypertext document viewer), such as Firefox, Internet Explorer. Enter the device IP address into address bar of web browser.

TAU-72.IP/TAU-36.IP factory default IP address – 192.168.1.2, network mask–255.255.255.0

After entering IP address the device will request username and password.

Username*: viewer*
Password: *specified by admin*.

The following menu will appear on the operator's terminal:



Device information:	
Linux version:	312 Mon Aug 13 13:51:16 NOVT 2018
Firmware version:	v10_23_03_15
BPU version:	TAU72 PLD v20180428 date: 2018 Apr 28 time 16:43:31
Factory type:	TAU-72.IP
Factory SN:	VI06001537
Factory MAC:	A8:F9:4B:02:DF:D5
User MAC:	a8:f9:4b:02:db:00
Board id:	0x13
Power supply:	-48V DC
Network information:	
Control IP address:	192.168.114.201
Primary DNS:	127.0.0.1
Secondary DNS:	

Non-privileged users will only be able to view routing and subscriber port configuration.

5.3.1 The 'Monitoring' menu

For detailed tabs description, see Section 5.1.4 of this document.

5.3.2 The 'System info' menu

For detailed menu description, see Section 5.1.5 of this document.

5.3.3 The 'Service' menu

For detailed menu description, see Section 5.1.6 of this document.

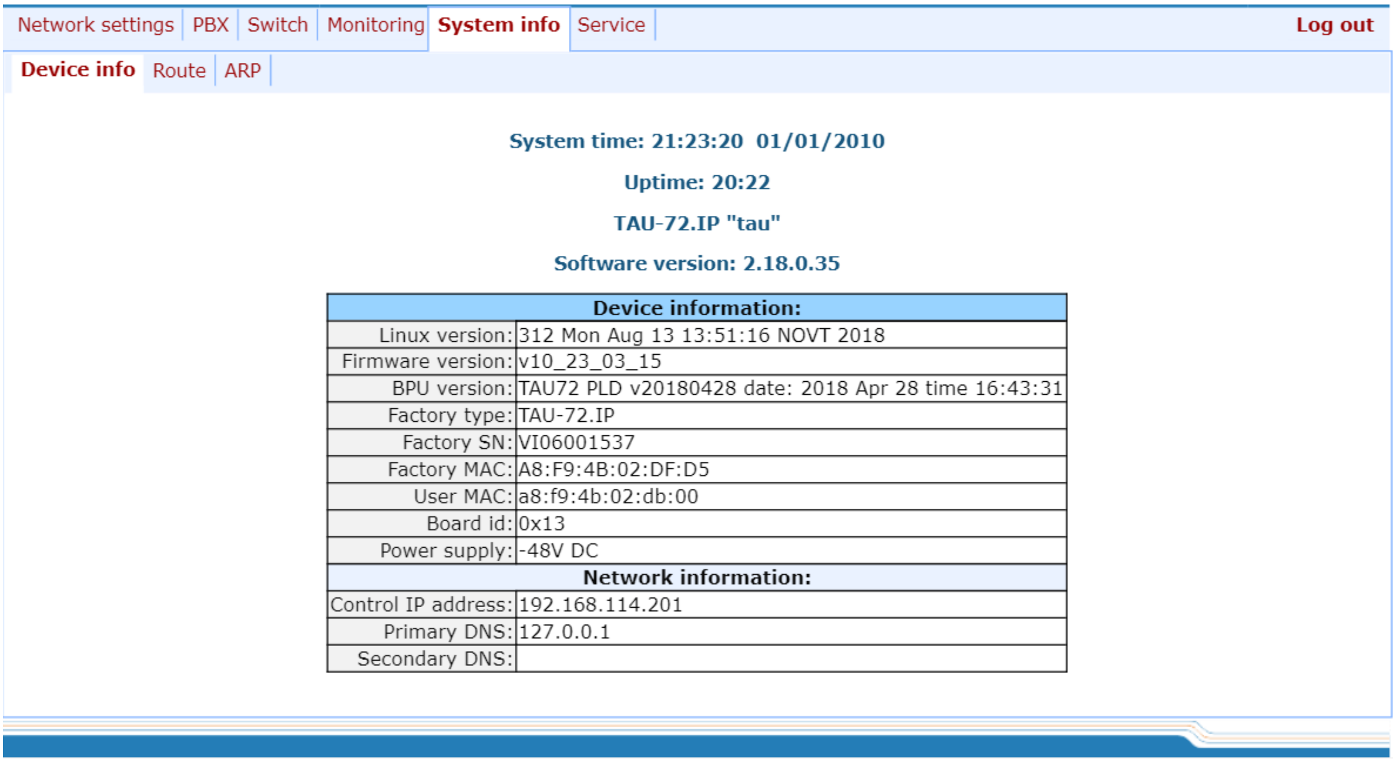
5.4 Supervisor Access

To login to the device, establish connection in the web browser (hypertext document viewer), such as Firefox, Internet Explorer. Enter the device IP address into address bar of web browser.

TAU-72.IP/TAU-36.IP factory default IP address – 192.168.1.2, network mask–255.255.255.0

After entering IP address the device will request username and password.

Username*: supervisor*
Password: *specified by admin*.



Supervisor will be able to access all parameters of the device in *read-only* mode.

6 COMMAND LINE MODE AND TERMINAL MODE OPERATION

6.1 Basic Commands

CLI is available when the connection to the device is established via RS-232 (connection parameters: 115200, 8, n, 1, n; username: *admin*, w/o password), or Telnet/SSH.

Command descriptions are listed in . Some of commands (marked as 'priv' in 'Privilege' column) executing only in privelege mode (available by enable command). Negotiation function executes opposite effect for command or sets default value for parameter.

Table 10 – List of available commands

Command						Parameter <value> value	Privilege	Description/Tip	Negotiation function 'no' command
exit						-	none	Stop CLI session	-
quit						-	none	Stop CLI session	-
help						-	none	CLI syntax tip	-
ping	<options>		<value>			IP address	none	Ping utility	-
	repeat	<value>				number:1-4294967295	none	Number of ping packets (default: 5)	-
	payload	<value>				number:0-65535	none	Ping packet payload size in bytes (default: 56)	-
	df-bit					-	none	Set 'don't fragment bit' (default: not setted)	-
	tos	<value>				number:0-255	none	Service type (default: 0)	-
	timeout	<value>				number:1-60	none	Reply waiting time, s (default: 2)	-
traceroute	<options>		<value>			IP address	none	TraceRoute utility	-
	df-bit					-	none	Set 'don't fragment bit' (default: not setted)	-
	repeat	<value>				number: 1-8	none	Retry amount in within one 'ttl' (defaut: 2)	-
	timeout	<value>				number:0-10	none	Reply waiting time, s (default: 2)	-
	ttl	<value>				number:1-255	none	Max time-to-live value (default: 255)	-
	tos	<value>				number:0-255	none	Service type (default: 0)	-
	icmp					-	none	Use ICMP ECHO instead of UDP datagramms (default: don't use)	-
	port	<value>				number:0-65535	none	UDP port used number (default: 33434)	
	size	<value>				number:40-32768	none	Packet size in bytes (default:100)	-
show	..					..	none	View command	-
	system					-	none	Show firmware version	-
	hwaddr					-	none	Show MAC address	-
	ipaddr					-	none	Show IP address	-
	netmask					-	none	Show network mask	-
	network					-	none	Show full network settings	-
	version					-	none	Show Configuration file version	-
	configuration					-	priv	Show full configuration	-
	voiceport	..				..	none	Voice ports information view	-

		statistic	<value>			number:1-36[1]	none	Show port statistic	-
		status	<value>			number:1-36[1]	none	Show port status	-
		configuration	<value>			number:1-36[1]	priv	Show port configuration	-
	voiceprofile	<value>				number:1-8	priv	Show voice profile configuration	-
	hw					-	none	Show hardware version	-
	switch					-	none	Show switch ports status	-
	call	..				..	none	Call information	-
		active					none	Show information about current calls during conversation	-
		history					none	Show call history	-
	proc					-	priv	Show current processes	-
	history					-	priv	Show previously entered commands in CLI history	-
enable						-	none	Switch to privilege mode	-
disable						-	priv	Get back to normal mode	-
passwd						-	priv	Set password for user	-
	admin	<value1> <value2>				1-old password 2-new password	priv	Set password for 'admin' user	-
	supervisor	<value1> <value2>				1-old password 2-new password	priv	Set password for 'supervisor' user	-
	operator	<value1> <value2>				1-old password 2-new password	priv	Set password for 'operator' user	-
	viewer	<value1> <value2>				1-old password 2-new password	priv	Set password for 'viewer' user	-
pbx	..					..	priv	PBX application management	-
	restart					-	priv	Command that allows to restart the main application	-
sip	..					..	priv	Sip application management	-
	reregistration	<value>				number:1-8	priv	Reregistrate ports for the chosen SIP profile	-
reset	<value>					dhcp|static	priv	Reset configuration - dhcp - network settings in reset configuration will be setted dynamically - dhcp - network settings in reset configuration will be static (IP address 192.168.1.2)	-
backup	<value1> <value2>					1-IP address 2-string:64 characters	priv	Create configuration backup	-
restore	<value1> <value2>					1-IP address 2-string:64 characters	priv	Restore the device configuration from backup	-
test	voiceport	<value>				number:1-36[1]	priv	Voice port testing (Phone connected to the line indication is present in test results)	-
reboot	<confirm>					yes/no	priv	Rebooting device	-
route	..					-	priv	Routing management	-
	add	<value1>	netmask <value2>	gateway <value3>		1-IP address 2-network mask address 3-IP address	priv	Add routing rule	-
	del	<value1>	netmask <value2>			1-IP address 2-network mask address	priv	Delete routing rule	-
	print					-	priv	Show routing table	-
save						-	priv	Save configuration into non-	-

[1] For TAU-36.IP. For TAU-72.IP parameter value: 1-72

								volatile memory	
shell						-	priv	Go into Linux console	-
unload	callhistory	<value1>	<value2>			1-IP address 2-string:64 characters	priv	Upload call log by TFTP protocol	-
upgrade	image	..				..	priv	Firmware update	-
		tftp	<value1> <value2>			1-IP address 2-string:64 characters	priv	Firmware update via TFTP protocol	
		ftp	<value1> <value2>			1-IP address 2-string:64 characters	priv	Firmware update via FTP protocol	
configure							priv	Enter the configuration mode	-
	do					-	priv	Execute top level command	-
	exit					-	priv	Exit the configuration mode	-
	no	<command>				-	priv	Cancel command	-
	network						priv	Enter the network settings configuration mode	-
		do				-	priv	Execute top level command	-
		no	<command>			-	priv	Cancel command	-
		exit				-	priv	Exit the network settings configuration mode	-
		mac	..			..	priv	MAC address management	-
			clear			-	priv	Delete user MAC address	-
			get			-	priv	Show user MAC address	-
			set	<value>		aa:bb:cc:dd:ee:ff	priv	Set user MAC address	-
		broadcast	<value>			IP address	priv	Set broadcast IP address	-
		control	<value>			n o	priv	Set traffic control interface	Set default interface (no_vlan) for traffic control
		rtp	<value>			n o	priv	Set RTP traffic interface	Set default interface (no_vlan) for RTP traffic
		siganlling	<value>			n o	priv	Set signal traffic interface	Set default interface (no_vlan) for signal traffic
		dhcp				-	priv	Set network configuration receiving via DHCP mode	Set static network setting configuration receiving mode
		dhcp_gateway				-	priv	Use default gateway, received via DHCP (default: don't use)	Use default gateway, setted in the device configuration
		dns	..			..	priv	DNS server management	-
			primary	<value>		IP address	priv	Set main DNS server IP address	-
			secondary	<value>		IP address	priv	Set redundant DNS server IP address	-
		dscp	..			..		DSCP tags management	-
			siganlling	<value>		number:0-63	priv	Set DSCP value for SIP packets (default: 26)	Set DSCP value for SIP packets to default
			media	..		..	priv	Configuration of DSCP for RTP/RTCP packets	-
				voicepo rt	<value1> <value2>	number:1-36[1] number:0-63	priv	Set DSCP value for RTP/RTCP packets for port (default: 46)	Set DSCP value for RTP/RTCP packets for port to default
				voicepr ofile	<value1> <value2>	number:1-8 number:0-63	priv	Set DSCP value for RTP/RTCP packets for voice profile (default: 46)	Set DSCP value for RTP/RTCP packets for voice profile to default
		gateway	<value>			IP address	priv	Set default gateway	-
		ipaddr	<value>			IP address	priv	Set IP address	-
		netmask	<value>			mask address	priv	Set network mask	-

[1]For TAU-36.IP. For TAU-72.IP parameter value: 1-72

		ntp	..			..	priv	NTP protocol settings	
			enable			-	priv	Enable NTP (default: disabled)	Disable NTP
			interval	<value>		number:30-100000	priv	Set time synchronization interval (default: disabled)	Disable periodic time synchronization
			ipaddr	<value>		IP address	priv	Set NTP server IP address	-
			timezone	<value>		-12..+12	priv	Set timezone (default: 0)	-
		snmp	..			..	priv	SNMP protocol configuration	-
			enable			-	priv	Enable SNMP (default: disabled)	Disable SNMP
			trapsink	<value>		IP address	priv	Set IP address for trap messages transmission	-
			traptype	<value>		v1|v2	priv	Set trap messages protocol version (default: v2)	Set trap messages protocol version to default
			rocomm	<value>		string:96 characters	priv	Set roCommunity value	-
			rwcomm	<value>		string:96 characters	priv	Set rwCommunity value	-
			trapcomm	<value>		string:96 characters	priv	Set trapCommunity value	-
		telnet				-	priv	Enable telnet (default: enabled)	Disable telnet
		ssh				-	priv	Enable SSHv2 (default: enabled)	Disable SSHv2
		web	..			..	priv	HTTP settings	-
			enable			-	priv	Enable HTTP (default: enabled)	Disable HTTP
			port			number:0-65535	priv	Set HTTP port value (default: 80)	Set HTTP port value to default
		autoupdate	..			..	priv	Autoupdate settings	-
			auth			-	priv	Allow authorization	-
			cfg	<value>		string	priv	Set configuration file name	-
			fw	<value>		string	priv	Set firmware file name	-
			interval_cfg	<value>		number	priv	Set configuration autoupdate interval	-
			interval_fw	<value>		number	priv	Set firmware autoupdate interval	-
			password	<value>		string	priv	Set password	-
			protocol	<value>		tftp ftp http https	priv	Set autoupdate protocol	-
			server-ip	<value>		IP address	priv	Set autoupdate server IP address	-
			src	<value>		d	priv	Set autoupdate interface	-
			enable			-	priv	Enable autoupdate	-
			username	<value>		string	priv	Set name	-
		pppoe	..			..	priv	Set PPPoE protocol configuration	-
			password	<value>		string	priv	Set password	-
			user	<value>		string	priv	Set user name	-
			enable			-	priv	Enable PPPoE	Disable PPPoE
			vid	<value>		number:1-4095	priv	Set VLAN network identifier for PPPoE/PPP traffic	-
			vlan			-	priv	Use VLAN for PPPoE/PPP traffic	Don't use VLAN for PPPoE/PPP traffic
			mtu			number:86-1492	priv	Set MTU for PPP traffic	-
			mru			number:86-1492	priv	Set MRU for PPP traffic	-
			lcpecho	..		..	priv	Set LCP protocol parameters	-
				failure	<value>	number:0-65535	priv	Set LCP packets receiving errors amount	Set default value (3) for LCP packets receiving errors amount
				interval	<value>	number:0-20	priv	Set LCP echo packets transmission interval, s	Set default (30 s) LCP echo packets transmission period

									value.
		vlan1	..			..	priv	VLAN1 interface configuration	-
			broadcast	<value>		IP address	priv	Set broadcast IP address	-
			cos	<value>		number:0-7	priv	Set 802.1p priority for VLAN network	Set default value (0) for 802.1p priority for VLAN network
			dhcp			-	priv	Set network configuration receiving via DHCP mode	Set static network setting configuration receiving mode
			dhcp_gateway			-	priv	Use default gateway, received via DHCP (default: don't use)	Use default gateway, setted in the device configuration
			vid	<value>		number:1-4095	priv	Set VLAN network identifier	-
			ipaddr	<value>		IP address	priv	Set IP address	-
			netmask	<value>		Mask address	priv	Set network mask	-
			enable			-	priv	Enable VLAN usage	Disable VLAN usage
		vlan2	..			..	priv	VLAN2 interface configuration	-
			broadcast	<value>		IP address	priv	Set broadcast IP address	-
			cos	<value>		number:0-7	priv	Set 802.1p priority for VLAN network	Set default value (0) for 802.1p priority for VLAN network
			dhcp			-	priv	Set network configuration receiving via DHCP mode	Set static network setting configuration receiving mode
			dhcp_gateway			-	priv	Use default gateway, received via DHCP (default: don't use)	Use default gateway, setted in the device configuration
			vid	<value>		number:1-4095	priv	Set VLAN network identifier	-
			ipaddr	<value>		IP address	priv	Set IP address	-
			netmask	<value>		Mask address	priv	Set network mask	-
			enable			-	priv	Enable VLAN usage	Disable VLAN usage
		vlan3	..			..	priv	VLAN3 interface configuration	-
			broadcast	<value>		IP address	priv	Set broadcast IP address	-
			cos	<value>		number:0-7	priv	Set 802.1p priority for VLAN network	Set default value (0) for 802.1p priority for VLAN network
			dhcp			-	priv	Set network configuration receiving via DHCP mode	Set static network setting configuration receiving mode
			dhcp_gateway			-	priv	Use default gateway, received via DHCP (default: don't use)	Use default gateway, setted in the device configuration
			vid	<value>		number:1-4095	priv	Set VLAN network identifier	-
			ipaddr	<value>		IP address	priv	Set IP address	-
			netmask	<value>		Mask address	priv	Set network mask	-
			enable			-	priv	Enable VLAN usage	Disable VLAN usage
	devname	<value>				string:96 characters	priv	Set device name	-
	timer	..				..	priv	Set timer values	-
		duration	<value>			number:10-300	priv	Restrict full number dial time, s (default: 300)	Set full number dial time to default
		waitanswer	<value>			number:40-300	priv	Set call reply wait timer value (default: 180)	Set call reply wait timer value to default
	sip	..				..	priv	SIP configuration	-
		profile 1..8					priv	Enter the SIP profile configuration mode	-
			do			-	priv	Execute top level command	-
			no	<command>		-	priv	Cancel command	-
			exit			-	priv	Exit the SIP profile configuration	-

								mode	
			proxy	..		..	priv	SIP proxy parameters configuration	-
				mode	<value>	none|park|home	priv	Set operations with SIP proxy server mode none - don't use proxy park - parking mode home - homing mode	-
				address	<value1> <value2>	1-number:1-5 2-IP address	priv	Set SIP proxy server IP address	-
			registrar	..		..	priv	SIP registrar parameters configuration	-
				address	<value1> <value2>	1-number:1-5 2-IP address	priv	Set SIP registrar IP address	-
				enable	<value>	number:1-5	priv	Enable registration on SIP registrar	Disable registration on SIP registrar
				interval	<value>	number:10-3600	priv	Set reregistration interval value (default: 30)	Set reregistration interval value to default
			domain	<value>			priv	Set SIP domain	Delete SIP domain
			expires	<value>			priv	Set expire period (default: 1800)	Set expire period to default
			auth	..		..	priv	Authorization parameters	-
				mode	<value>	user|global	priv	Set authorization mode (default: user) user-use voice ports settings global-use SIP section settings	Set default authorization mode
				name	<value>	string:96 characters	priv	Set authorization name	-
				passwo rd	<value>	string:96 characters	priv	Set authorization password	-
			codec	..		..	priv	Codec settings	-
				list	<value>	g a g b g a	priv	Configure authorized codecs list (Codecs should be listed in priority order from most to less priority) (default: g711a, g711u)	-
				ptime	<value1> <value2>	1 - g729|g711|g723|g726_32 2 - 10-80	priv	Set codec packetization time (default: g729 – 20 ms, g711 – 20 ms, g7231 – 30 ms, g726_32 – 20 ms)	Set codec packetization time to default
			dtmfmode	<value>		inband|rfc2833|info	priv	Set DTMF transmission mode (default: rfc2833) - inband - rfc2833 - info - by SIP INFO method	Set DTMF transmission mode to default
			fax	..		..	priv	Fax transmission parameters	-
				detect	<value>	none|caller|callee|both	priv	Setfax detection mode (default: both) - none - detection is disabled -caller| - detection on transmitting side - callee - detection on receiving side - both - detection on both side	-
				codec	<value>	g711a|g711u|t38	priv	Set fax codec (default: g711u)	-
			ecan	..		..	priv	Echo canceller parameters	-
				enable		-	priv	Enable echo canceller (default: enabled)	Disable echo canceller
				tail	<value>	8|16|24|32..128	priv	Set cancelling echo duration value, ms (default: 64)	-
			vad			-	priv	Enable VAD (default: disabled)	Disable VAD
			dialplan	..		..	priv	Dail plan parameters	-
				ltimer	<value>	number:1-30	priv	Set L-timer value (default: 15)	Set L-timer value to default

				stimer	<value>	number:1-10	priv	Set S-timer value (default: 8)	Set S-timer value to default
				start	<value>	number:10-300	priv	Set start timer value 300)	Set start timer value to default
				rule	<value>	string:1000 characters	priv	Set dialplan rule	-
	udp	..				..	priv	UDP transport parameters	-
		rtpport	sip	..		..	priv	UPD ports range for RTP packets transmission when operating by SIP protocol	-
				min	<value>	number:1024-65535	priv	Set min UDP port for RTP (default: 16384)	-
				max	<value>	number:1024-65535	priv	Set max UDP port for RTP (default: 32767)	-
	voice port 1..36[1]						priv	Enter the voice ports configuration mode	-
		do				-	priv	Execute top level command	-
		no	<command>			-	priv	Cancel command	-
		exit				-	priv	Exit the voice ports configuration mode	-
		username	<value>			string:96 characters	priv	Set phone number	-
		displayname	<value1> [value2] [value3]			1 – string:50 characters, 2 – string:50 characters (optional), 3 – string:50 characters (optional). All the parameters together should not exceed 50 characters.	priv	Set display name	-
		authname	<value>			string:96 characters	priv	Set authorization name	-
		password	<value>			string:96 characters	priv	Set authorization password	-
		profile	..			..	priv	Profile selection	-
			sip	<value>		number:1-8	priv	Set port SIP profile (default: 1)	-
			voice	<value>		number:1-8	priv	Set port voice profile (default: 1)	-
		disable				-	priv	Disable port (default: port enabled)	Enable port
		custom				-	priv	Disable voice profile settings usage (default: enabled)	Enable voice profile settings usage
		callerid	<value>			fsk|dtmf|rus	priv	Set CallerID type (default: CallerID disabled)	Disable CallerID
		flash	..			..	priv	Short clearback flash parameters	-
			min	<value>		number:70-2000	priv	Set min short clearback border (default: 200)	Set min short clearback border to default
			max	<value>		number:min-200	priv	Set max short clearback border (default: 600)	Set max short clearback border to default
		hybrid	..			..	priv	Difsystem parameters	-
			rx	<value>		number:-230-20	priv	Configure amplifying/attenuating of signal in receive circuit (default: -70)	Set amplifying/attenuating of signal in receive circuit to default
			tx	<value>		number:-170-60	priv	Configure amplifying/attenuating of signal in transmission circuit (default: 0)	Set amplifying/attenuating of signal in transmission circuit to default

[1] For TAU-36.IP. For TAU-72.IP command appears as: **voice port 1..72**

		stopdial				-	priv	Dial stop by '#' symbol usage (default: don't use)	Don't use dial stop by '#' symbol
	voice profile 1..8						priv	Enter the voice profile configuration mode	-
		do				-	priv	Execute top level command	-
		no	<command>			-	priv	Cancel command	-
		exit				-	priv	Exit the voice profile configuration mode	-
		callerid	<value>			fsk|dtmf|rus	priv	Set CallerID type (default: CallerID disabled)	Disable CallerID
		flash	..			..	priv	Short clearback flash parameters	-
			min	<value>		number:70-2000	priv	Set min short clearback border (default: 200)	Set min short clearback border to default
			max	<value>		number:min-200	priv	Set max short clearback border (default: 600)	Set max short clearback border to default
		hybrid	..			..	priv	Difsystem parameters	-
			rx	<value>		number:-230-20	priv	Configure amplifying/attenuating of signal in receive circuit (default: -70)	Set amplifying/attenuating of signal in receive circuit to default
			tx	<value>		number:-170-60	priv	Configure amplifying/attenuating of signal in transmission circuit (default: 0)	Set amplifying/attenuating of signal in transmission circuit to default
		stopdial				-	priv	Dial stop by '#' symbol usage (default: don't use)	Don't use dial stop by '#' symbol

6.1.1 Basic commands

do

Executing the top level command

Syntax

do <command>

Parameters

command – EXEC level command

Privilege

priv

Command mode

CONFIG, CONFIG-NETWORK, CONFIG-SIP, CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Example

```
tau-72(config)# do show ipaddr
IP address eth0: 192.168.118.119
```

exit

Command is designed to exit the configuration mode

Syntax

exit

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG, CONFIG-NETWORK, CONFIG-SIP, CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

no

Negotiation command.

Syntax

no <command>

Parameters

<command> - command Executes for command negotiation or default value setting

Privilege

priv

Command mode

CONFIG, CONFIG-NETWORK, CONFIG-SIP, CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Example

```
tau-72(config)# no timer duration
```

6.1.2 Top level commands (exec)

exit

CLI session exit command.

Syntax

exit

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

quit

CLI session exit command.

Syntax

quit

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

help

CLI syntax tip command.

Syntax

help

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

ping

Ping utility

Syntax

ping [repeat <value>] [payload <value>] [df-bit do|dont|want] [tos <value>] [timeout <value>] destination

Parameters

repeat-ping packets amount;

payload-ping packet payload size in bytes;

df-bit-set ‘don't fragment bit’;

tos-type of service;

timeout-reply witing time, s;

destination-destination host address.

< value > parameter value:

for repeat: 1-4294967295 (default is 5);

for payload: 0-65535 (default is 56);

for df-bit

do-set, prohibit fragmentation;

dont-don't set, allow fragmentation (default);

want-don't set locally for packets exceed MTU

for tos: 0-255 (default is 0);

for timeout: 1-60 (default is 2).

Privilege

none

Command mode

EXEC

Example

```
tau-72> ping 192.168.118.46
PING 192.168.118.46 (192.168.118.46) 56(84) bytes of data.
64 bytes from 192.168.118.46: icmp_seq=1 ttl=64 time=9.31 ms
64 bytes from 192.168.118.46: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 192.168.118.46: icmp_seq=3 ttl=64 time=1.29 ms
64 bytes from 192.168.118.46: icmp_seq=4 ttl=64 time=1.30 ms
64 bytes from 192.168.118.46: icmp_seq=5 ttl=64 time=1.34 ms
--- 192.168.118.46 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.019/2.854/9.311/3.230 ms
```

traceroute

TraceRoute utility

Syntax

traceroute [df-bit][repeat <value>][timeout <value>][ttl <value>][tos <value>][icmp] [port <value>][size <value>] destination

Parameters

df-bit-set ‘don't fragment bit’;

repeat-retries amount within one 'ttl';

timeout-reply witing time, s;

ttl-max time-to-live amount;

tos-type of service;

icmp-use ICMP ECHO instead of UDP datagrams;

port-number of used UDP-port;

size-packet size in bytes;

destination-destination host address.

< value > parameter value:

for repeat: 1-8 (default is 2);

for timeout: 0-10 (default is 2);

for ttl: 1-255 (default is 255);

for tos: 0-255 (default is 0);

for port: 1-65535 (default is 33434);

for size: 40-32768 (default is 100);

Privilege

none

Command mode

EXEC

Example

```
tau-72> traceroute 192.168.118.46
traceroute to 192.168.118.46 (192.168.118.46), 255 hops max, 100 byte packets
 1 192.168.118.46 (192.168.118.46) 1.510 ms 1.053 ms
```

show system

The command is intended for viewing firmware version.

Syntax

show system

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show system
TAU-72.IP
System version:   #2.17.2
Linux version:    #291 Thu Jul 20 15:46:00 NOVT 2017
Firmware version:  v10_23_03_15
BPU version:     TAU72 PLD v20170328 date: 2017 Mar 28 time 10:54:1
```

show hwaddr

The command is intended for viewing MAC address.

Syntax

show hwaddr

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show hwaddr
MAC address eth0: A8:F9:4B:0E:50:FE
```

show ipaddr

The command is intended for viewing IP address.

Syntax

show ipaddr

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show ipaddr
IP address eth0: 192.168.118.119
```

show netmask

The command is intended for viewing network mask.

Syntax

show netmask

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show netmask
Netmask eth0: 255.255.255.0
```

show network

The command is intended for viewing full network configuration.

Syntax

show network

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show network
================start dump config================
```

```
node: config.Network.network
        IPADDR: 192.168.118.119
        NETMASK: 255.255.255.0
        GATEWAY: 192.168.18.1
...
| Press any key to continue | Press 'q' to exit |
```

show version

The command is intended for viewing configuration file version.

Syntax

show version

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show version
Config version: 1.0
```

show configuration

The command is intended for viewing whole configuration.

Syntax

show configuration

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# show configuration
================start dump config================
node: config.Network.network
        IPADDR: 192.168.118.119
        NETMASK: 255.255.255.0
        GATEWAY: 192.168.18.1
...
| Press any key to continue | Press 'q' to exit |
```

show voiceport statistic

The command is intended for viewing port static.

Syntax

show voiceport statistic <value>

Parameters

< value > – parameter 1-36 [1] value.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show voiceport statistic 1

Statistic of pbx port 1:

       pbx call count     3
       pbx port state     onhook
       pbx last number    855102

       vapi statistic:

            send packet         453
            send octet          9060
            receive packet      451
            receive octet       9020
            packet lost         0
            peak jitter         1
```

show voiceport status

The command is intended for viewing port status.

Syntax

show voiceport status <value>

Parameters

< value > – parameter 1-36 [1] value.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show voiceport status 1
Status of pbx port 1: offhook
```

[1] For TAU-36.IP. For TAU-72.IP parameter value: 1-72.

show voiceport configuration

The command is intended for viewing port status.

Syntax

show voiceport configuration <value>

Parameters

< value > – parameter 1-36 [1] value.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# show voiceport configuration 1
================start dump config================
node: config.VOIP.ports.port_0
        phone: 855101
        user_name: 855101
        auth_name: 855101
        auth_pass: 855101
 ...
| Press any key to continue | Press 'q' to exit |
```

show voiceprofile

The command is intended for viewing voice profile configuration.

Syntax

show voiceprofile <value>

Parameters

< value > – parameter value: 1-8

Privilege

priv

Command mode

EXEC

Example

```
tau-72# show voiceprofile 1
================start dump config================
node: config.VOIP.ports.port_def_0
        aon: 4
        taxophone: 0
        min_flashtime: 200
        flashtime: 600
...
| Press any key to continue | Press 'q' to exit |
```

[1] For TAU-36.IP. For TAU-72.IP parameter value: 1-72.

show hw

The command is intended for viewing hardware status.

Syntax

show hw

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show hw
Vpower  11
Temp1 48, Temp2  45, Temp3  43, Temp4  43
SFP0: ST(0x7)- inserted 1, TxFault 1, LOS 1, TxDis 0
SFP0: Temp 65535, Power 65535, Cur 65535, ptx 65535, prx 65535
```

show switch

The command is intended for viewing switch ports status.

Syntax

show switch

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show switch
Port 0:
        Link: off
        Duplex: half
        Speed: 0Mbps
Port 1:
        Link: on
        Duplex: full
        Speed: 1000Mbps
SFP 0:
        Link: off
        Duplex: half
        Speed: 0Mbps
CPU:
        Link: on
        Duplex: full
        Speed: 1000Mbps
```

show call active

The command is intended for viewing current call information in a state of conversation.

Syntax

show call active

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show call active
PBX active calls:
|         855101|         855102|   192.168.16.8| Tue Jan  5 23:50:56 2010| Tue Jan  5 23:50:57 2010|                  33 sec |            talking|  outgoing|
|         855102|         855101|     voip.local| Tue Jan  5 23:50:56 2010| Tue Jan  5 23:50:57 2010|                  33 sec |            talking|  incoming|
```

show call history

The command is intended for viewing call history.

Syntax

show call history

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> show call history
PBX call history:
|No|          local|         remote|    remote host|          start call time|          start talk time|            talk duration|              state|      type|
|00|         855101|              -|              -| Sun Jan  3 23:02:00 2010|                        -|                        -|              local|  outgoing|
|01|         855101|              -|              -| Sun Jan  3 23:02:02 2010|                        -|                        -|              local|  outgoing|
|02|         855101|              -|              -| Sun Jan  3 23:02:20 2010|                        -|                        -|              local|  outgoing|
|03|         855102|              -|              -| Mon Jan  4 01:52:39 2010|                        -|                        -|              local|  outgoing|
|04|         855101|         855102|   192.168.16.8| Tue Jan  5 23:44:07 2010| Tue Jan  5 23:44:11 2010|                   2 sec |       remote clear|  outgoing|
|05|         855102|         855101|     voip.local| Tue Jan  5 23:44:07 2010| Tue Jan  5 23:44:11 2010|                   2 sec |        local clear|  incoming|
|06|         855101|         855102|   192.168.16.8| Tue Jan  5 23:44:49 2010| Tue Jan  5 23:44:51 2010|                   1 sec |       remote clear|  outgoing|
```

show proc

The command is intended for viewing current system processes.

Syntax

show proc

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# show proc
  PID USER       VSZ STAT COMMAND
    1 admin     1504 S    init [
    2 admin        0 SW<  [kthreadd]
    3 admin        0 SWN  [ksoftirqd/0]
    4 admin        0 SW<  [watchdog/0]
    5 admin        0 SW<  [events/0]
...
```

show history

The command is intended for viewing CLI commands history.

Syntax

show history

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# show history
    4  show voiceport statistic
    8  show voiceport statistic 1
    9  show voiceport status 1
   11  show voiceport configuration 1
   12  show voiceprofile 1
   13  show voiceprofile 1q
   16  disable
   17  show hw
   18  show switch
   25  show call active
   26  show call history
   27  enable
   28  show proc
   30  show history
```

enable

The command is intended for enter the privilege mode.

Syntax

enable

Parameters

Command contains no arguments.

Privilege

none

Command mode

EXEC

Example

```
tau-72> enable
tau-72#
```

disable

The command is intended for exit the privilege mode.

Syntax

disable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# disable
tau-72>
```

passwd admin

The command is intended for setting admin user password.

Syntax

passwd admin <value1><value2>

Parameters

value1 – previous password;

value2 – new password.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# passwd admin
Changing password for admin
New password:
Retype password:
```

passwd supervisor

The command is intended for setting supervisor user password.

Syntax

passwd supervisor <value1><value2>

Parameters

value1 – previous password;

value2 – new password.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# passwd supervisor
Changing password for supervisor
New password:
Retype password:
```

passwd operator

The command is intended for setting operator user password.

Syntax

passwd operator <value1><value2>

Parameters

value1 – previous password;

value2 – new password.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# passwd operator
Changing password for operator
New password:
Retype password:
```

passwd viewer

The command is intended for setting viewer user password.

Syntax

passwd viewer <value1><value2>

Parameters

value1 – previous password;

value2 – new password.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# passwd viewer
Changing password for viewer
New password:
Retype password:
```

pbx restart

The command is intended for restarting PBX application.

Syntax

pbx restart

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# pbx restart
Restart voip...
```

sip reregistration

The command is intended for reregistration the chosen SIP profile ports.

Syntax

sip reregistration <value>

Parameters

< value > parameter value: 1-8

Privilege

priv

Command mode

EXEC

Example

```
tau-72# sip registration 1
tau-72#
```

reset

The command is intended for resetting the configuration.

Syntax

reset <value>

Parameters

< value > – parameter value:

– dhcp — network settings in reset configuration will be setted dynamically

– static — network settings in reset configuration will be static (IP address 192.168.1.2)

Privilege

priv

Command mode

EXEC

Example

```
tau-72# reset static
Do you really want to reset configuration and restart device? (yes/no)
```

backup

The command is intended for configuration backup.

Syntax

backup <value1><value2>

Parameters

<value 1> – TFTP server IP address where configuration will be uploaded;

<value 2> – configuration file name (string: 64 characters)

Privilege

priv

Command mode

EXEC

Example

```
tau-72# backup 192.168.118.46 config.tar.gz
tau-72#
```

restore

The command is intended for restoring device configuration from backup.

Syntax

restore <value1><value2>

Parameters

<value 1> – TFTP server IP address where configuration will be downloaded from;

<value 2> – configuration file name (string: 64 characters)

Privilege

priv

Command mode

EXEC

Example

```
tau-72# restore 192.168.118.46 configtau.tar.gz
update_tftp_cfg.sh: set TFTP IP to 192.168.118.46
update_tftp_cfg.sh: CFG filename: configtau.tar.gz
tau-72#
```

test voiceport

The command is intended for testing the voiceport.

Syntax

test voiceport <value>

Parameters

<value> – number:1-36[1]

Privilege

priv

Command mode

EXEC

Example

```
tau-72# test voiceport 2
waiting result...
RING ext -0.37, V, TIP ext -0.37, V
Vbat. -31.45, V, Vring1.   nan, V, Vring2   nan, V
res T-R. 950.41, kOm; res T-G. 471.79, kOm; res R-G 670.24, kOm
cap T-R.  0.00, mkF; cap T-G.  0.00, mkF; cap R-G  0.00, mkF
end testing, result '0'
```

reboot

The command is intended for rebooting the device.

Syntax

reboot <confirm>

Parameters

< confirm > – yes/no

Privilege

priv

Command mode

EXEC

Example

```
tau-72# reboot
Do you really want to restart device? (yes/no)
```

[1] For TAU-36.IP. For TAU-72.IP parameter value: 1-72

route add

The command is intended for adding the route rule.

Syntax

route add <value1> netmask <value2> gateway <value3>

Parameters

<value1> – IP address;

<value2> – mask address;

<value3> – default gateway IP address.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# route add 192.168.1.0 netmask 255.255.255.0 gateway 192.168.118.77
tau-72#
```

route del

The command is intended for deleting route rule.

Syntax

route del <value1> netmask <value2>

Parameters

<value1> – IP address;

<value2> – mask address;

Privilege

priv

Command mode

EXEC

Example

```
tau-72# route del 192.168.1.0 netmask 255.255.255.0
tau-72#
```

route print

The command is intended for viewing route table.

Syntax

route print

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# route print
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.118.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.1.0     192.168.118.77  255.255.255.0   UG    0      0        0 eth0
192.168.16.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0.77
```

save

The command is intended for saving configuration to the volatile memory of the device.

Syntax

save

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# save
save config
Image 0: Flag 0, Image 1: Flag 1
tar: removing leading '/' from member names
compressed 126485 bytes to device 0
```

shell

The command is intended for enter the Linux console.

Syntax

shell

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# shell
BusyBox v1.15.3 (2017-09-05 14:59:00 +07) built-in shell (ash)
```

```
Enter 'help' for a list of built-in commands.
[admin@tau:/root]
```

unload callhistory

The command is intended for uploading call log via tftp protocol.

Syntax

Unload callhistory <value1> <value2>

Parameters

<value1> – TFTP server IP address where the call log will be uploaded;

<value2> – call log file name (string: 64 characters)

Privilege

priv

Command mode

EXEC

Example

```
tau-72# unload callhistory 192.168.118.46 callhistory.txt
tau-72#
```

upgrade image tftp

The command is intended for updating firmware via tftp protocol.

Syntax

upgrade image tftp <value1><value2>

Parameters

<value1> – TFTP server IP address where the firmware will be downloaded from;

<value2> – firmware file name (string: 64 characters)

Privilege

priv

Command mode

EXEC

Example

```
tau-72# upgrade image tftp 192.168.118.46 tau72.img
tau-72#
```

upgrade image tfp

The command is intended for updating firmware via tfp protocol.

Syntax

upgrade image tftp <value1><value2>

Parameters

<value1> – TFP server IP address where the firmware will be downloaded from;

<value2> – firmware file name (string: 64 characters)

Privilege

priv

Command mode

EXEC

Example

```
tau-72# upgrade image ftp 192.168.118.46 tau72.img
tau-72#
```

configure

The command is intended for enter the configuration mode.

Syntax

configure

Parameters

Command contains no arguments.

Privilege

priv

Command mode

EXEC

Example

```
tau-72# configure
tau-72(config)#
```

6.1.3 Configuration level commands

network

The command is intended for enter the network settings configuration.

Syntax

network

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG

Example

```
tau-72(config)# network
tau-72(config-net)#
```

devname

The command is intended for setting the device name.

Syntax

devname <value>

Parameters

<value> – string: 96 characters

Privilege

priv

Command mode

CONFIG

Example

```
tau-72(config)# devname tau72_hub
```

timer duration

The command is intended for restriction full number dial time, s.

Syntax

timer duration <value>

Parameters

<value> – number:10-300 (default: 300)

Privilege

priv

Command mode

CONFIG

Negotiation function 'no' command

Set full number dial time to default

Example

```
tau-72(config)# timer duration 44
```

timer waitanswer

The command is intended for setting reply waiting timer value.

Syntax

timer waitanswer <value>

Parameters

<value>.number: 40-300 (default: 180)

Privilege

priv

Command mode

CONFIG

Negotiation function 'no' command

Set call reply wait timer value to default

Example

```
tau-72(config)# timer waitanswer 170
```

sip profile 1..8

The command is intended for enter the SIP profiles configuration mode.

Syntax

sip profile 1..8

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG

Example

```
tau-72(config)# sip profile 1
tau-72(config-sip-profile)#
```

udp rtpport sip min

The command is intended for setting the minimal UDP port for RTP.

Syntax

udp rtpport sip min <value>

Parameters

<value> – number: 1024-65535 (default: 16384)

Privilege

priv

Command mode

CONFIG

Example

```
tau-72(config)# udp rtpport sip min 10000
```

udp rtpport sip max

The command is intended for setting the max UDP port for RTP.

Syntax

udp rtpport sip max <value>

Parameters

<value> – number: 1024-65535 (default: 32767)

Privilege

priv

Command mode

CONFIG

Example

```
tau-72(config)# udp rtpport sip max 12000
```

voice port 1..36[1]

The command is intended for enter the voiceports configuration mode.

Syntax

voice port 1..36

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG

Example

```
tau-36(config)# voice port 1
tau-36(config-voice-port)#
```

voice profile 1..8

The command is intended for enter the voice profiles configuration mode.

Syntax

voice profile 1..8

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG

Example

```
tau-72(config)# voice profile 2
```

[1] For TAU-36.IP. For TAU-72.IP command appears as: **voice port 1..72**

```
tau-72(config-voice-profile)#
```

6.1.4 Network settings level commands

mac clear

The command is intended for deleting user MAC address.

Syntax

mac clear

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# mac clear
```

mac get

The command is intended for viewing MAC address.

Syntax

mac get

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# mac get
```

mac set

The command is intended for setting user MAC address

Syntax

mac set <value>

Parameters

<value> – aa:bb:cc:dd:ee:ff

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# mac set a8:b8:78:56:4f:e3
ethaddr: set user MAC addr: a8:b8:78:56:4f:e3
ethaddr: to apply the changes you need to reboot system
```

broadcast

The command is intended for setting broadcast IP address.

Syntax

broadcast <value>

Parameters

<value>-IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# broadcast 192.168.118.254
```

control

The command is intended for setting the traffic control interface.

Syntax

control <value>

Parameters

<value> – no_vlan|vlan1|vlan2|vlan3|pppoe

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default interface (no_vlan) for traffic control

Example

```
tau-72(config-net)# control vlan1
```

rtp

The command is intended for setting the RTP traffic interface

Syntax

rtp <value>

Parameters

<value> – no_vlan|vlan1|vlan2|vlan3|pppoe

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default interface (no_vlan) for RTP traffic

Example

```
tau-72(config-net)# rtp vlan1
```

siganlling

The command is intended for setting the signal traffic interface

Syntax

signaling <value>

Parameters

<value> – no_vlan|vlan1|vlan2|vlan3|pppoe

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default interface (no_vlan) for signal traffic

Example

```
tau-72(config-net)# signaling vlan1
```

dhcp

The command is intended for setting the network settings receiving via DHCP mode

Syntax

dhcp

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set static network setting configuration receiving mode

Example

```
tau-72(config-net)# dhcp
```

dhcp_gateway

The command is intended for using default gateway received via DHCP (default: don't use).

Syntax

dhcp_gateway

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Use default gateway, setted in the device configuration

Example

```
tau-72(config-net)# dhcp_gateway
```

dns primary

The command is intended for setting main DNS server IP address.

Syntax

dns primary <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# dns primary 8.8.8.8
```

dns secondary

The command is intended for setting redundant DNS server IP address.

Syntax

dns secondary <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# dns secondary8.8.8.8
```

dscp signaling

The command is intended for setting DSCP value for SIP packets.

Syntax

dscp signaling <value>

Parameters

<value> – number:0-63 (default: 26)

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default DSCP value for SIP packets.

Example

```
tau-72(config-net)# dscp signaling 33
```

dscp media voiceport

The command is intended for setting DSCP value for RTP/RTCP packets for port.

Syntax

dscp media voiceport <value1><value2>

Parameters

<value1> – number: 1-36[1]

<value2> – number: 0-63 (default: 46)

[1] For TAU-36.IP. For TAU-72.IP parameter value: 1-72.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set DSCP value for RTP/RTCP packets for port to default.

Example

```
tau-72(config-net)# dscp media voiceport 3 63
```

dscp media voiceprofile

The command is intended for setting DSCP value for RTP/RTCP packets for voice profile.

Syntax

dscp media voiceprofile <value1><value2>

Parameters

<value1> – number: 1-8

<value2> – number: 0-63 (default: 46)

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set DSCP value for RTP/RTCP packets for voice profile to default

Example

```
tau-72(config-net)# dscp media voiceprofile 2 45
```

gateway

The command is intended for setting default gateway.

Syntax

gateway <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# gateway 192.168.118.99
```

ipaddr

The command is intended for setting IP address.

Syntax

ipaddr <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# ipaddr 192.168.118.9
```

netmask

The command is intended for setting network mask.

Syntax

netmask <value>

Parameters

<value> – mask address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# netmask 255.255.255.0
```

ntp enable

The command is intended for enabling NTP.

Syntax

ntp enable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable NTP.

Example

```
tau-72(config-net)# ntp enable
```

ntp interval

The command is intended for setting time synchronization interval.

Syntax

ntp interval <value>

Parameters

<value> – number: 30-100000 (default: periodic synchronization is disabled)

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable periodic time synchronization.

Example

```
tau-72(config-net)# ntp interval 60
```

ntp address

The command is intended for setting NTP server IP address.

Syntax

ntp address <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# ntp address 192.168.11.1
```

ntp timezone

The command is intended for setting the timezone.

Syntax

ntp timezone <value>

Parameters

<value>: -12..+12 (default: 0)

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# ntp timezone +1
```

snmp enable

The command is intended for enabling SNMP.

Syntax

snmp enable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable SNMP.

Example

```
tau-72(config-net)# snmp enable
```

snmp trapsink

The command is intended for setting trap messages transmission IP address.

Syntax

snmp trapsink <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# snmp trapsink 192.168.118.7
```

snmp traptype

The command is intended for setting trap messages protocol version.

Syntax

snmp traptype <value>

Parameters

<value> – v1|v2 (default: v2)

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default trap messages protocol version.

Example

```
tau-72(config-net)# snmp traptype v2
```

snmp rocomm

The command is intended for setting RO (read only) community value.

Syntax

snmp rocomm <value>

Parameters

<value> – string: 96 characters (public is default)

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# snmp rocomm test
```

snmp rwcomm

The command is intended for setting RO (write rights) community value.

Syntax

snmp rwcomm <value>

Parameters

<value> – string:96characters (private is default)

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# snmp rwcomm priv
```

snmp trapcomm

The command is intended for setting trap community value.

Syntax

snmp trapcomm <value>

Parameters

<value> – string:96 characters

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# snmp trapcomm testtrap
```

telnet

The command is intended for enabling telnet.

Syntax

telnet

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable telnet.

Example

```
tau-72(config-net)# telnet
```

ssh

The command is intended for enabling SSHv2.

Syntax

ssh

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable SSHv2.

Example

```
tau-72(config-net)# ssh
```

web enable

The command is intended for enabling HTTP.

Syntax

web enable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable HTTP.

Example

```
tau-72(config-net)# web enable
```

web port

The command is intended for setting HTTP port value.

Syntax

web port<value>

Parameters

<value> – number: 1-65535 (default: 80)

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default HTTP port value.

Example

```
tau-72(config-net)# web port 5000
```

autoupdate auth

The command is intended for authorization permission.

Syntax

autoupdate auth

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate cfg

The command is intended for setting configuration file name.

Syntax

autoupdate cfg <value>

Parameters

<value> – string

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate fw

The command is intended for setting firmware file name.

Syntax

autoupdate fw <value>

Parameters

<value> – string

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate interval_cfg

The command is intended for setting configuration autoupdate interval.

Syntax

autoupdate interval_cfg <value>

Parameters

<value> – number

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate interval fw

The command is intended for setting firmware update interval.

Syntax

autoupdate interval fw <value>

Parameters

<value> – number

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate password

The command is intended for setting the password.

Syntax

autoupdate password <value>

Parameters

<value> – string

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate protocol

The command is intended for setting autoupdate protocol.

Syntax

autoupdate protocol <value>

Parameters

<value> – tftp|ftp|http|https

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate server-ip

The command is intended for setting server IP address where autoupdate is being processed from.

Syntax

autoupdate server-ip <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate src

The command is intended for setting autoupdate interface.

Syntax

autoupdate src <value>

Parameters

<value> – dhcp|no_dhcp|vlan1_dhcp|vlan2_dhcp|vlan3_dhcp

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate enable

The command is intended for enabling the autoupdate.

Syntax

autoupdate enable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

autoupdate username

The command is intended for setting autoupdate username.

Syntax

autoupdate username<value>

Parameters

<value> – string

Privilege

priv

Command mode

CONFIG-NETWORK

pppoe password

The command is intended for setting the password for PPP channel authorization.

Syntax

pppoe password <value>

Parameters

<value> – string

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# pppoe password 66678rty7
```

pppoe user

The command is intended for setting username for PPP channel authorization.

Syntax

pppoe user <value>

Parameters

<value> – string

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# pppoe user admin
```

pppoe enable

The command is intended for enabling PPPoE protocol.

Syntax

pppoe enable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable PPPoE

Example

```
tau-72(config-net)# pppoe enable
```

pppoe vid

VLAN ID setting command for PPPoE/PPP traffic.

Syntax

pppoe vid <value>

Parameters

<value> – number: 1-4095

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# pppoe vid 453
```

pppoe vlan

The command allows to enable VLAN usage for PPPoE/PPP traffic.

Syntax

pppoe vlan

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Don't use VLAN for PPPoE/PPP traffic

Example

```
tau-72(config-net)# pppoe vlan
```

pppoe mtu

The command is setting MTU value for PPP traffic.

Syntax

mtu <value>

Parameters

<value> – number: 86-1492

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# pppoe mtu
```

pppoe mru

The command is setting MRU value for PPP traffic.

Syntax

mru <value>

Parameters

<value> – number: 86-1492

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# pppoe mru
```

pppoe lcpecho failure

The command is setting LCP echo packets errors receive amount.

Syntax

pppoe lcpecho failure <value>

Parameters

<value> – number: 0-65535

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default value (3) for LCP packets receiving errors amount

Example

```
tau-72(config-net)# pppoe lcpecho failure
```

pppoe lcpecho interval

The command is setting LCP echo packets transmission period, s.

Syntax

pppoe lcpecho interval <value>

Parameters

<value> – number: 0-20

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default (30 s) LCP echo packets transmission period value.

Example

```
tau-72(config-net)# pppoe lcpecho interval
```

vlan1/vlan2/vlan3 broadcast

The command is intended for setting broadcast IP address.

Syntax

vlan1/vlan2/vlan3 broadcast <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# vlan1 broadcast 192.168.17.254
```

vlan1/vlan2/vlan3 cos

The command is intended for setting 802.1p priority for VLAN network.

Syntax

vlan1/vlan2/vlan3 cos <value>

Parameters

<value> – number: 0-7

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set default (0) 802.1p priority for VLAN network.

Example

```
tau-72(config-net)# vlan1 cos 7
```

vlan1/vlan2/vlan3 dhcp

The command is intended for setting network settings receive via DHCP mode for VLAN network.

Syntax

vlan1/vlan2/vlan3 dhcp

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set static network settings operation mode

Example

```
tau-72(config-net)# vlan1 dhcp
```

vlan1/vlan2/vlan3 dhcp_gateway

The command is intended for using default gateway received via DHCP for VLAN network (default: don't use)

Syntax

vlan1/vlan2/vlan3 dhcp_gateway

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Use default gateway, setted in the device configuration

Example

```
tau-72(config-net)# vlan1 dhcp_gateway
```

vlan1/vlan2/vlan3 vid

The command is intended for setting VLAN ID.

Syntax

vlan1/vlan2/vlan3 vid <value>

Parameters

<value> – number: 0-4095

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# vlan1 vid 4022
```

vlan1/vlan2/vlan3 ipaddr

The command is intended for setting VLAN network IP address.

Syntax

vlan1/vlan2/vlan3 ipaddr <value>

Parameters

<value> – IP address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# vlan1 ipaddr 192.168.99.2
```

vlan1/vlan2/vlan3 netmask

The command is intended for setting VLAN network mask

Syntax

vlan1/vlan2/vlan3 netmask <value>

Parameters

<value> — mask address

Privilege

priv

Command mode

CONFIG-NETWORK

Example

```
tau-72(config-net)# vlan1 netmask 255.255.255.0
```

vlan1/vlan2/vlan3 enable

The command is intended for enabling VLAN usage.

Syntax

vlan1/vlan2/vlan3 enable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable VLAN usage

Example

```
tau-72(config-net)# vlan1 enable
```

6.1.5 SIP profiles configuration level commands

proxy mode

The command is intended for setting operations with SIP proxy server mode.

Syntax

proxy mode <value>

Parameters

<value> – none — don't use proxy;

– park — parking mode;

– home — homing mode.

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# proxy mode home
```

proxy address

The command is intended for setting SIP proxy server IP address (-main, 2-4 redundant).

Syntax

proxy address <value1><value2>

Parameters

<value1> – number: 1-5;

<value2> – IP address

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# proxy address 1 route.com:5063
```

registrar address

The command is intended for setting SIP registrar IP address (1-main, 2-4 redundant).

Syntax

registrar address <value1><value2>

Parameters

<value1> — number: 1-5;

<value2> — IP address

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# registrar address 1 route.com:5063
```

registrar enable

The command is intended for enabling registration on SIP registrar (1-main, 2-4 redundant).

Syntax

registrar enable <value>

Parameters

<value> – number: 1-5

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Enable registration on SIP registrar.

Example

```
tau-72(config-sip-profile)# registrar enable 1
```

registrar interval

The command is intended for setting reregistration interval value.

Syntax

registrar interval <value>

Parameters

<value> – number: 10-3600 (default: 30)

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set default reregistration interval value.

Example

```
tau-72(config-sip-profile)# registrar interval 400
```

domain

The command is intended for setting SIP domain.

Syntax

domain <value>

Parameters

<value> – 96 characters

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Delete SIP domain.

Example

```
tau-72(config-sip-profile)# domain voip.local
```

expires

The command is intended for setting registration expire period.

Syntax

expires <value>

Parameters

<value> – number: 0-2147483647 (default: 1800)

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set default registration expire period.

Example

```
tau-72(config-sip-profile)# expires 3600
```

auth mode

The command is intended for setting authorization mode.

Syntax

auth mode <value>

Parameters

<value> — use default voiceports settings;

global — use SIP section settings.

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set authorization mode.

Example

```
tau-72(config-sip-profile)# auth mode user
```

auth name

The command is intended for setting authorization name.

Syntax

auth name <value>

Parameters

<value> – string:96 characters

Privilege

priv

Command mode

CONFIG-SIP

auth password

The command is intended for setting authorization password.

Syntax

auth password <value>

Parameters

<value> – string:96 characters

Privilege

priv

Command mode

CONFIG-SIP

codec list

The command is intended for setting allowed codecs list.

Syntax

codec list <value> [value] [value] [value] [value]

Parameters

<value> – g729a|g729b|g711a|g711u|g723|g726_32

(Codecs should be listed in priority order from most to less priority: by default: g711a g711u)

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# codec list g711a g711u g723 g726_32 g729b
set_config(config.VOIP.profile.profile_0.codecs,g711a,1)
set_config(config.VOIP.profile.profile_0.codecs,g711u,2)
set_config(config.VOIP.profile.profile_0.codecs,g723,3)
set_config(config.VOIP.profile.profile_0.codecs,g726_32,4)
set_config(config.VOIP.profile.profile_0.codecs,g729b,5)
```

codec ptime

This command is intended for setting codec packetization time.

Syntax

codec ptime <value1><value2>

Parameters

<value1> – g729|g711|g723|g726_32;

<value2> – 10-80

(default: g729 – 20 ms, g711 – 20 ms, g7231 – 30 ms, g726_32 – 20 ms)

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set default packetization time.

Example

```
tau-72(config-sip-profile)# codec ptime g729 70
```

dtmfmode

The command is intended for setting DTMF transmission mode.

Syntax

dtmfmode <value>

Parameters

<value> — inband;

- rfc2833 (default);
- info-with SIP INFO method.

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set DTMF transmission mode to default.

Example

```
tau-72(config-sip-profile)# dtmfmode info
```

fax detect

The command is intended for setting fax detection mode.

Syntax

fax detect <value>

Parameters

<value> – none-detection disabled;

- caller - detection on transmitting side;
- callee - detection on receiving side;
- both-detection on both sides (default).

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# fax detect both
```

fax codec

The command is intended for setting fax codec.

Syntax

fax codec <value>

Parameters

<value> – g711a|g711u|t38 (by default: g711u)

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# fax codec t38
```

ecan enable

The command is intended for enabling echo canceller.

Syntax

ecan enable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# ecan enable
```

ecan tail

The command is intended for setting cancelling echo duration, ms.

Syntax

ecan tail <value>

Parameters

<value> – 8|16|24|32..128 (default: 64)

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# ecan tail 128
```

vad

The command is intended for enabling VAD.

Syntax

vad

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Disable VAD.

Example

```
tau-72(config-sip-profile)# vad
```

dialplan ltimer

The command is intended for setting L-timer value.

Syntax

dialplan ltimer <value>

Parameters

<value> – number: 1-30 (default: 15)

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set default L-timer value.

Example

```
tau-72(config-sip-profile)# dialplan ltimer 10
```

dialplan stimer

The command is intended for setting S-timer value.

Syntax

dialplan ltimer <value>

Parameters

<value> – number: 1-30 (default: 15)

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set default S-timer value.

Example

```
tau-72(config-sip-profile)# dialplan stimer 5
```

dialplan start

The command is intended for setting start timer value.

Syntax

dialplan start <value>

Parameters

<value> – number: 1-300 (default: 300)

Privilege

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set default start timer value.

Example

```
tau-72(config-sip-profile)# dialplan start 20
```

dialplan rule

The command is intended for setting dialplan rule.

Syntax

dialplan rule <value>

Parameters

<value> – string: 1000 characters

Privilege

priv

Command mode

CONFIG-SIP

Example

```
tau-72(config-sip-profile)# dialplan rule 'S5 L15 xxxxxx|xxxxxxx'
```

6.1.6 Port and port profiles settings level commands

username

The command is intended for setting phone number.

Syntax

username <value>

Parameters

<value> – string: 96 characters

Privilege

priv

Command mode

CONFIG-VOICEPORT

Example

```
tau-72(config-voice-port)# username 772001
```

displayname

The command is used to set display name.

Syntax

displayname <value1> [value2] [value3]

Parameters

<value1> – string: 50 characters

<value2> – string: 50 characters

<value3> – string: 50 characters

The sum of all the parameters (value1+value2+value3) should not exceed 50 characters.

Privilege

priv

Command mode

CONFIG-VOICEPORT

Example

```
tau-24(config-voice-port)# displayname Ivan Ivanov
```

authname

The command is intended for setting authorization name.

Syntax

authname <value>

Parameters

<value> – string: 96 characters

Privilege

priv

Command mode

CONFIG-VOICEPORT

Example

```
tau-72(config-voice-port)# authname 772001
```

password

The command is intended for setting authorization password.

Syntax

password <value>

Parameters

<value> – string: 96 characters

Privilege

priv

Command mode

CONFIG-VOICEPORT

Example

```
tau-72(config-voice-port)# password 7U7r2tt1u
```

profile sip

The command is intended for assigning SIP profile to port.

Syntax

profile sip <value>

Parameters

<value> – number:1-8 (default: 1)

Privilege

priv

Command mode

CONFIG-VOICEPORT

Example

```
tau-72(config-voice-port)# profile sip 1
```

profile voice

The command is intended for assigning voice profile to port.

Syntax

profile voice <value>

Parameters

<value> – number:1-8 (default: 1)

Privilege

priv

Command mode

CONFIG-VOICEPORT

Example

```
tau-72(config-voice-port)# profile voice 1
```

disable

The command is intended for disabling port.

Syntax

disable

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-VOICEPORT

Negotiation function 'no' command

Enable port.

Example

```
tau-72(config-voice-port)# disable
```

custom

The command is intended for disabling voice profile settings usage.

Syntax

custom

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-VOICEPORT

Negotiation function 'no' command

Enable voice profile settings usage.

Example

```
tau-72(config-voice-port)# custom
```

callerid

The command is intended for setting CallerID type.

Syntax

callerid<value>

Parameters

<value> – fsk|dtmf|rus (default: CallerID disabled)

Privilege

priv

Command mode

CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Negotiation function 'no' command

Disable CallerId.

Example

```
tau-72(config-voice-port)# callerid fsk
```

flash min

The command is intended for setting short clearback minimal border.

Syntax

flash min <value>

Parameters

<value> — number:70-2000 (default: 200)

Privilege

priv

Command mode

CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Negotiation function 'no' command

Set min short clearback border to default

Example

```
tau-72(config-voice-port)# flash min 70
```

flash max

The command is intended for setting short clearback max border.

Syntax

flash max <value>

Parameters

<value> – number: min-200 (default: 600)

Privilege

priv

Command mode

CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Negotiation function 'no' command

Set max short clearback border to default.

Example

```
tau-72(config-voice-port)# flash max 700
```

hybrid rx

The command is intended for setting signal amplifying/attenuating in receiving circuit.

Syntax

hybrid rx <value>

Parameters

<value> – number: -230..20 (default: -70)

Privilege

priv

Command mode

CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Negotiation function 'no' command

Set amplifying/attenuating of signal in receiving circuit to default.

Example

```
tau-72(config-voice-port)# hybrid rx -20
```

hybrid tx

The command is intended for setting signal amplifying/attenuating in transmission circuit.

Syntax

hybrid tx <value>

Parameters

<value> – number: -170..60 (default: 0)

Privilege

priv

Command mode

CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Negotiation function 'no' command

Set amplifying/attenuating of signal in transmission circuit to default.

Example

```
tau-72(config-voice-port)# hybrid tx 20
```

stopdial

The command is intended for enabling dial stop using # character.

Syntax

stopdial

Parameters

Command contains no arguments.

Privilege

priv

Command mode

CONFIG-VOICEPORT, CONFIG-VOICEPROFILE

Negotiation function 'no' command

Don't use dial stop by '#' symbol.

Example

```
tau-72(config-voice-profile)# stopdial
tau-72(config-voice-profile)#
```

6.2 Call statistic

6.2.1 Command line mode

CLI is available when the connection to the device is established via RS-232 (connection parameters: 115200, 8, n, 1, n; username: admin, w/o password), or Telnet/SSH.

To view the current call statistics, use `show call history` command.

Device RAM may store up to 2000 performed calls records. When the number of records exceeds 2000, the oldest records will be deleted, and the new ones will be added at the end of the file.

Table 11 — Call statistics record format

Record	Description
No	Sequence number of the record
Local	TAU-72.IP/TAU-36.IP subscriber number
Remote	Remote subscriber number
Remote host	Remote host IP address
Start call time	Call received/performed time
Start talk time	call start time
Duration	Duration of call (seconds)
State	Transient state, or reason for call clearing
Type	Call type (outgoing, incoming)

Table 12 — Transient states and reasons for call clearing output into statistics

Transient states	Description
seize	Incoming or outgoing occupation
talking	Subscriber in the call state
holding	TAU-72.IP/TAU-36.IP subscriber put a remote subscriber on hold
holded	TAU-72.IP/TAU-36.IP subscriber was put on hold by a remote subscriber
conference	Conference state, the subscriber is a 3-way conference initiator
Reasons for call clearing	**Description**
local	TAU-72.IP/TAU-36.IP subscriber put the phone offhook, didn't perform a call and put the phone back onhook
local busy	TAU-72.IP/TAU-36.IP subscriber is busy
remote busy	Remote subscriber is busy

invalid number	Invalid number is dialled
no answer	No response from subscriber
no local user	Incoming call to non-existent number
no remote user	Outgoing call to non-existent number
no route	Call to unavailable direction
local clear	TAU-72.IP/TAU-36.IP subscriber clearback
remote clear	Remote subscriber clearback
local fail	Local or remote failure that has occurred during the connection establishment. Possible error reasons: codec mismatch, problems during TCP connection establishment (when H.323 is used), overload, resource bottlenecks (bandwidth), etc.
remote fail	
remote redirection	Redirection (before—CFB, CFNR, or after the call—CT) performed by the remote subscriber
local redirection	Redirection (before—CFB, CFNR, or after the call—CT) performed by TAU-72.IP/TAU-36.IP subscriber
replaced	This call is replaced by another one while performing 'Call Transfer' service
pickuped	Call is picked up
pickuper succeed	'Call pickup' successfully performed by the subscriber
local limit	Call clearblack for the outgoing call concurrent connection limit
remote limit	Call clearblack for the incoming call concurrent connection limit

6.2.2 Statistic file operations

Call statistics file is located in /tmp folder on the device. To transfer the statistics file to a local PC, you should do the following:

1. Connect using RS-232 serial port (connection parameters: 115200, 8, n, 1, n; username: admin, w/o password). Go to Linux console by executing `enable`, and then `shell`. Call statistics file is located in 'tmp' folder.
2. To perform statistics file readout, run TFTP server on a PC, and specify a directory for the file transfer.
3. Go to 'tmp' folder using cd /tmp command and transfer statistics file to a local PC: tftp -pl voip_history <server ip address>

```
[root@fxs72 /root]$ cd /tmp
[root@fxs72 /root]$ tftp -pl voip_history <server IP address>
```

6.2.3 Port-specific Statistics

CLI is available when the connection to the device is established via RS-232 (connection parameters: 115200, 8, n, 1, n; username: admin, w/o password), or Telnet/SSH.

To view the port-specific statistics, use the following command: `show voiceport statistic <n>`, where <n>—port number.

Table 13 — Port statistics record format

Record	Description
Statistic of pbx port 1:	Port that statistics is gathered for
pbx call count	Number of calls performed by the port
pbx port state	Current port status
pbx last number	Last number dialled
vapi statistic:	Statistics for voice packets
send packet	Total amount of packets sent
send octet	Total amount of bytes sent
receive packet	Total amount of packets received

receive octet	Total amount of bytes received
packet lost	Total amount of packets lost
peak jitter	Peak jitter

6.3 Configuration writing/readout

To configuration readout from the device, connect using RS-232 serial port (connection parameters: 115200, 8, n, 1, n; username: admin, w/o password). Go to Linux console by executing `enable`, and then `shell`. Device configuration is located in 'etc' folder.

To perform the configuration readout, run TFTP server on a PC, and specify a directory for storing the configuration.

Configuration download commands:

```
[admin@fxs72 /admin]$cd /tmp
[admin@fxs72 /]$tar -cf conf.tar /etc/
[admin@fxs72 /]$tftp -pl conf.tar server ip-address
```

To upload the configuration, run TFTP server on a PC, and specify a directory with 'conf.tar' configuration file. The archive should contain 'etc' folder.

Configuration record commands:

```
[admin@fxs72 /admin]$cd /tmp
[admin@fxs72 /]$tftp -gl conf.tar server IP address
[admin@fxs72 /]$tar -xf conf.tar
```

Save settings using `'save'` command.

Restart the gateway using `'reboot -f'` command.

6.4 Setting password for 'admin' user

To set the password (factory settings: *rootpasswd*) connect to the gateway via COM port or telnet (factory settings address: 192.168.1.2, mask: 255.255.255.0) using terminal application, e.g. TERATERM.

Configuration procedure is as follows:

1. Connect the null modem cable to COM port of a PC and TAU module 'Console' port (if configuration is performed via COM port), or connect the computer to the module Ethernet port using Ethernet cable (if configuration is performed via Telnet/SSH).

2. Run the terminal application.

3. Configure COM port connection: data rate: 115200, data format: 8bit w/o parity, 1 stop bit, w/o flow control; or telnet connection: Factory default IP address: 192.168.1.2, port: 23.

4. Press <ENTER>. The following text will appear on screen:

```
**************************
*   TAU-72 FXS Gateway   *
**************************

fxs72 login:
```

5. Enter admin; for factory settings, the password is *rootpasswd*.

6. Enter the privilege mode:

```
enable
```

7. Enter 'passwd' command. The following text will appear on screen:

```
# passwd
Changing password for admin
New password:
```

8. Enter password, press <ENTER>, confirm password, press <ENTER>. The following text will appear on screen:

```
# passwd admin
Changing password for admin
New password:
Retype password:
Password for admin changed by admin
Oct 15 10:25:50 tmip auth.info passwd: Password for admin changed by admin
```

9. If the password is not applied (it may occur, if the device has a legacy firmware version installed with the legacy file system), check the contents of the 'passwd' file. To do this, go to Linux console by executing `enable` and then `shell` command, and edit the file using embedded editor *'joe'* (use arrow buttons to move the cursor; exit the editor without saving: <CTRL^C>, exit and save changes: <CTRL^(KX)>): joe /tmp/etc/passwd. Add 'x' character into admin user string.

File contents before the edit: admin::0:0: admin:/ admin:/bin/sh.

File contents after the edit: admin:x:0:0: admin:/ admin:/bin/sh.

10. Save settings using 'save' command.

11. Restart the gateway using 'reboot -f' command.

6.5 Reset the device to the factory settings

6.5.1 Reset the configuration to factory default

Press and hold the 'F' function button located on the front panel of the device from 10 to 14 seconds. Hold the button pressed until ***'Status'*** indicator flashes (flashed green and red rapidly) and ***'Alarm'*** indicator solid red, then release the button to avoid another reboot of the device. After releasing the button configuration will be reset and device will restart. After loading, the device will be accessible by IP address 192.168.1.2 via WEB interface (user—***admin***, password—***rootpasswd***), or Telnet/SSH (username—***admin***, password is not defined). Access via RS-232 console in this mode, just as for Telnet, will be unprotected (username—***admin***, password is not defined).

6.5.2 Reset the configuration to factory default using 'Safemode'

You can switch to 'Safemode' with two ways:

1. Turn the device off. Press and hold the 'F' function button located on the front panel of the device. While holding the button, turn the power on. Hold the button pressed until indicators will start flashing:

'Status' indicator will flash green and red rapidly, ***'Alarm'*** indicator will flash red, then release the button to avoid another reboot of the device.

2. Press and hold the 'F' function button located on the front panel of the device over than 15 seconds. First, device factory default reset indication will appear - ***'Status'*** indicator will flash green and red rapidly, ***'Alarm'*** indicator will be solid red. Don't release the button to avoid factory reset of the device. Then, all indicators will go outand device will start rebooting. Hold the button pressed until indicators will start flashing: ***'Status'*** indicator will flash green and red rapidly, ***'Alarm'*** indicator will flash red, then release the button to avoid another reboot of the device.

TAU-72.IP/TAU-36.IP will switch to 'safemode'. In this mode, the device will be accessible by IP address 192.168.1.2 via WEB interface (user—***admin***, password—***rootpasswd***), or Telnet (username—***admin***, password is not defined). Access via RS-232 console in this mode, just as for Telnet, will be unprotected (username—***admin***, password is not defined). Configuration won't be reset to factory default.

Reset the configuration to factory default:

1. Connect the null modem cable to COM port of a PC and TAU module 'Console' port (if configuration is performed via COM port), or connect the computer to the module Ethernet port using Ethernet cable (if configuration is performed via Telnet/SSH).
2. Run the terminal application.
3. Configure COM port connection: data rate: 115200, data format: 8bit w/o parity, 1 stop bit, w/o flow control; or telnet connection: 192.168.1.2, port 23.
4. Press <ENTER>. The following text will appear on screen:

```
*************************
*   TAU-72 FXS Gateway   *
*************************

fxs72 login:
```

Enter 'admin', password is not required.

5. To reset settings in the protected mode, execute the following commands:

   a. To reset settings in CLI mode and retain the console password, execute the following commands:

```
> enable
# reset static
```

   or if you need to set dynamic
   network parameters obtaining in factory default configuration (via DHCP):

```
> enable
# reset dhcp
```

   b. To reset settings in CLI mode and delete the console password, execute the following commands:

```
> enable
# shell
reset2defaults static
```

   or, if you have to define the dynamic obtaining of network settings in factory configuration (via DHCP protocol):

```
> enable
# shell
reset2defaults dhcp
```

7 SUPPLEMENTARY SERVICE USAGE

7.1 The 'Call Transfer' service

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—*'PBX -> Ports'*—by selecting *'Transmit Flash'* value in *'Flash transfer'* field, see Section 5.1.2.4. At that, you should specify the Flash impulse transfer method for utilized signalling protocol. 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—*'PBX -> Ports'*—by selecting *'Attended call transfer', 'Unattended call transfer', 'Local CT' or 'Blind attended transfer'* in *'Flash transfer'* field, see Section 5.1.2.4.

'Attended call transfer' 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 (a subscriber that performs the service).

'Attended call transfer' *service usage*:

While being in a call state with a Subscriber A, put him on hold with short clearback flash (R), wait for 'PBX response' tone and dial a 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;
- clearback — call transfer. Voice connection will be established between Subscribers A and C.

Figure 10 shows an algorithm of *'Attended call transfer'* service performed by Subscriber B via SIP protocol.

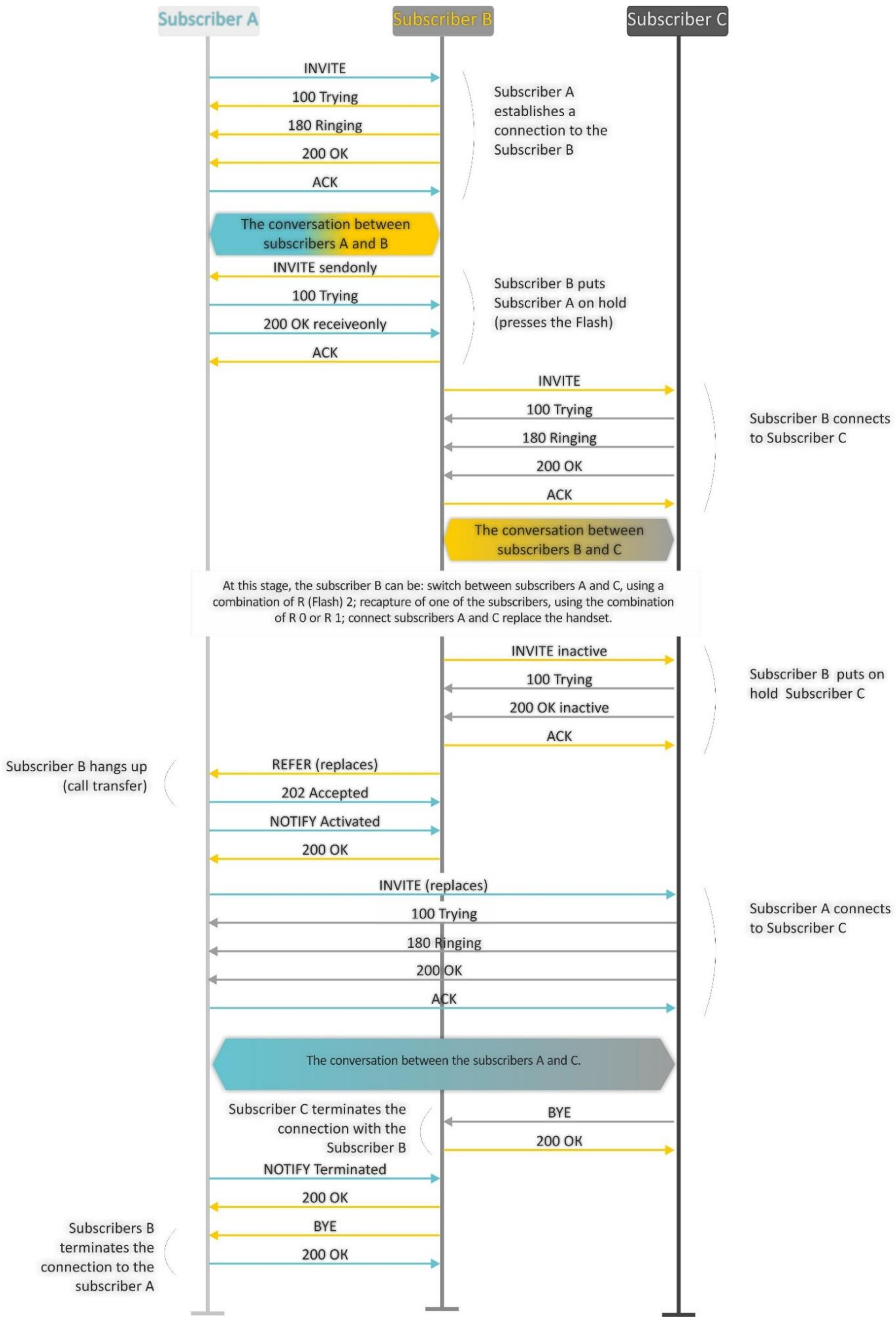


Fig. 10—Algorithm of *'Attended call transfer'* service performed by Subscriber B via SIP protocol

'Unattended call transfer' 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 A finishes dialling the number.

11 shows an algorithm of *'Unattended call transfer'* service performed by Subscriber B via SIP protocol.

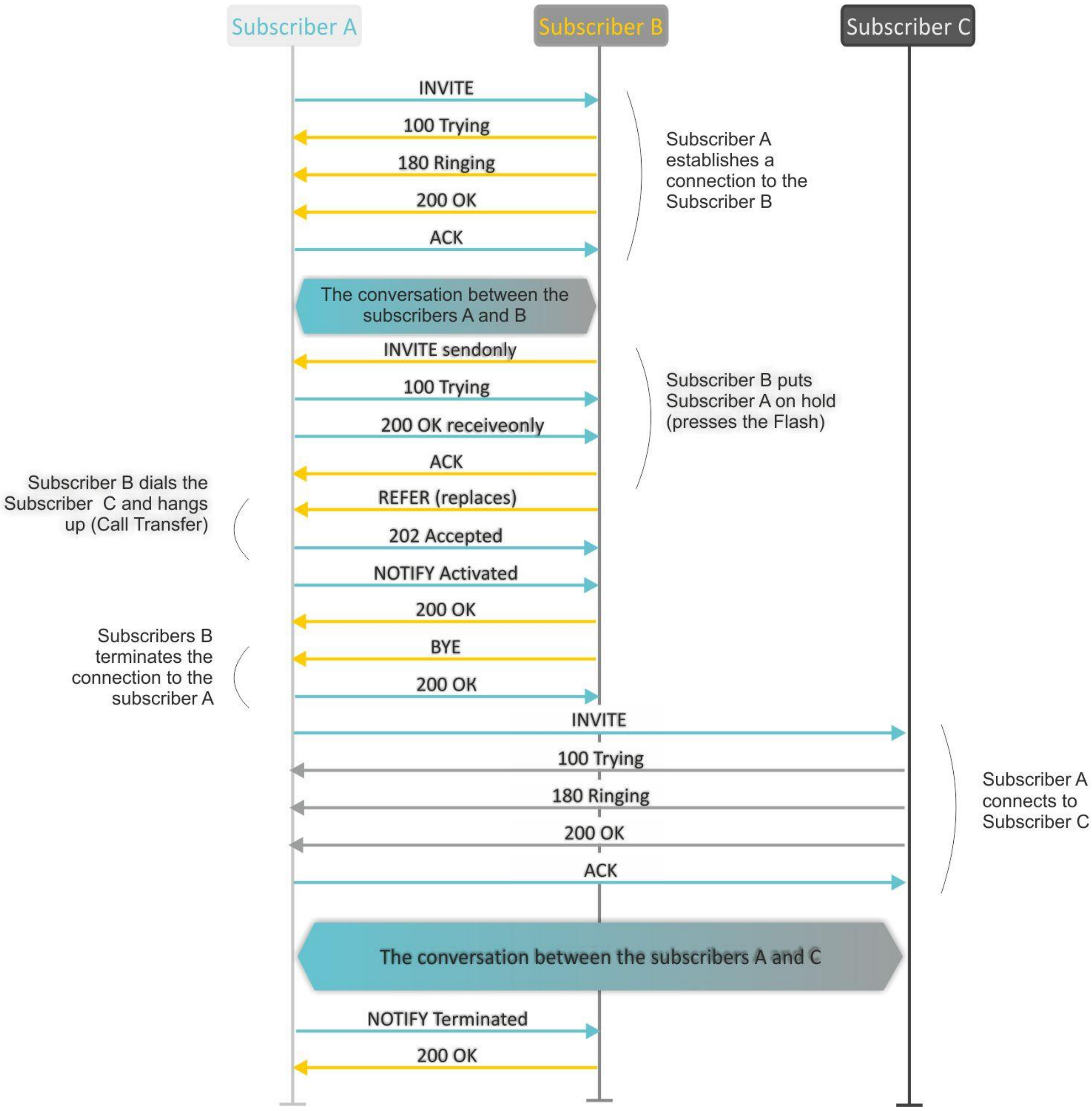


Fig. 11—Algorithm of *'Unattended call transfer'* service performed by Subscriber B via SIP protocol

The use of 'Blind attended transfer' service:

- Being in the conversation with subscriber "A", put him on hold with a short flash-break (R), wait for the signal *"Station answer"* and dial the number of subscriber "C".
- After subscriber "C" answers, use of the service is similar to the *"Attended calltransfer"* service described above;
- If you hang up the phone before subscriber "C" answers, *"Blind attended transfer"* will be performed. In this case the subscriber "B" (performing the service) recaptures the called subscriber "C", and sends to the subscriber "A" on hold the address of subscriber "C", to which the *"Call Transfer"* will be performed.

Figure 12 shows the algorithm of *"Blind attended transfer"* service by subscriber B via SIP protocol.

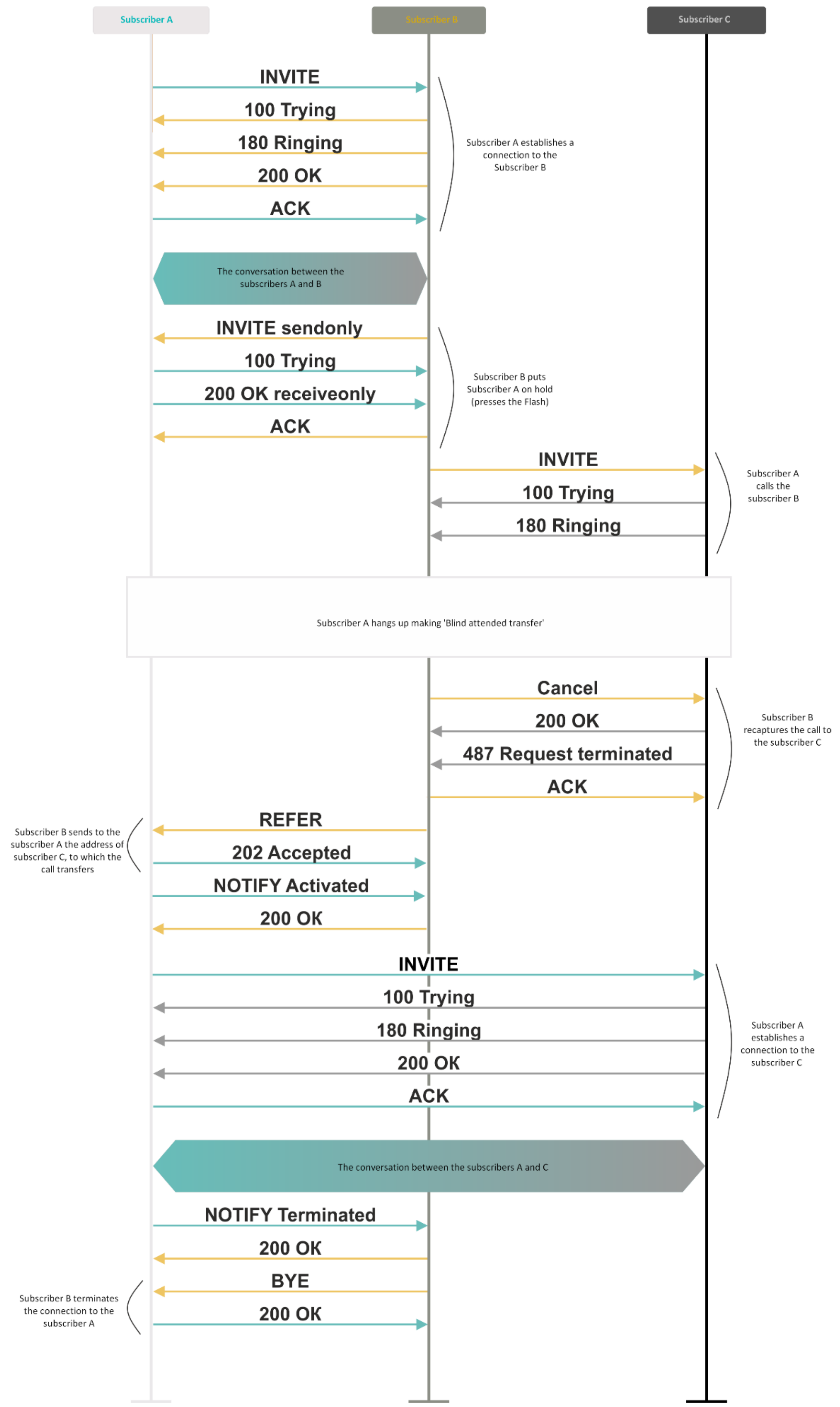


Fig. 12 — Algorithm of *"Blind attended transfer"* service by Subscriber B via SIP protocol

7.2 The Call Waiting service

This service allows to inform 'busy' users about new incoming calls with a special signal.

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

Access to this service is established via subscriber port settings menu—*'PBX -> Ports'*—by selecting *'Attended call transfer', 'Unattended call transfer',* or *'Local CT'* in *'Flash transfer'* 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:

- R 0 — reject a new call;
- R 1 — answer the waiting call and terminate the current call;
- R 2 — answer the waiting call and put the current call on hold; Further R 0/1/2/3/4 button actions are processed in accordance with the algorithm, described in Section 7.1 'Call Transfer' service;
- R – short clearback (flash).

7.3 3-way conference

Three-way conference is a service, that enables simultaneous phone communication for 3 subscribers. For entering conference mode, see Section 7.1 'Call Transfer'.

Subscriber that started the conference is deemed to be it's initiator, two other subscribers are the participants. 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 7.1 and 7.2.

13 shows an algorithm of *'3-way conference'* service performed locally on the device via SIP protocol.

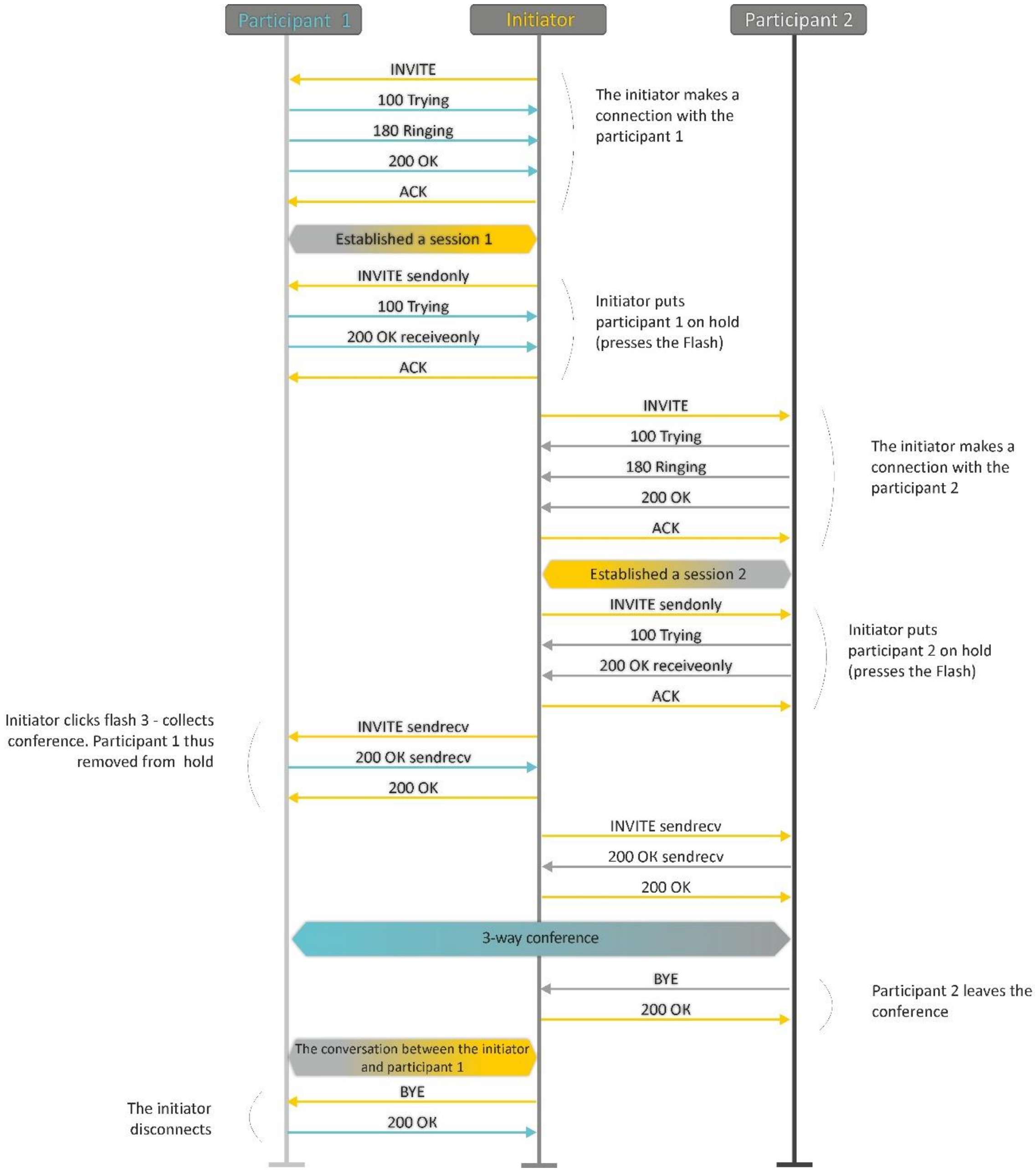


Fig. 13—Algorithm of *'3-way conference'* service performed locally on the device via SIP protocol

14 shows an algorithm of *'3-way conference'* service performed at the conference server via SIP protocol ('REFER to focus' option).

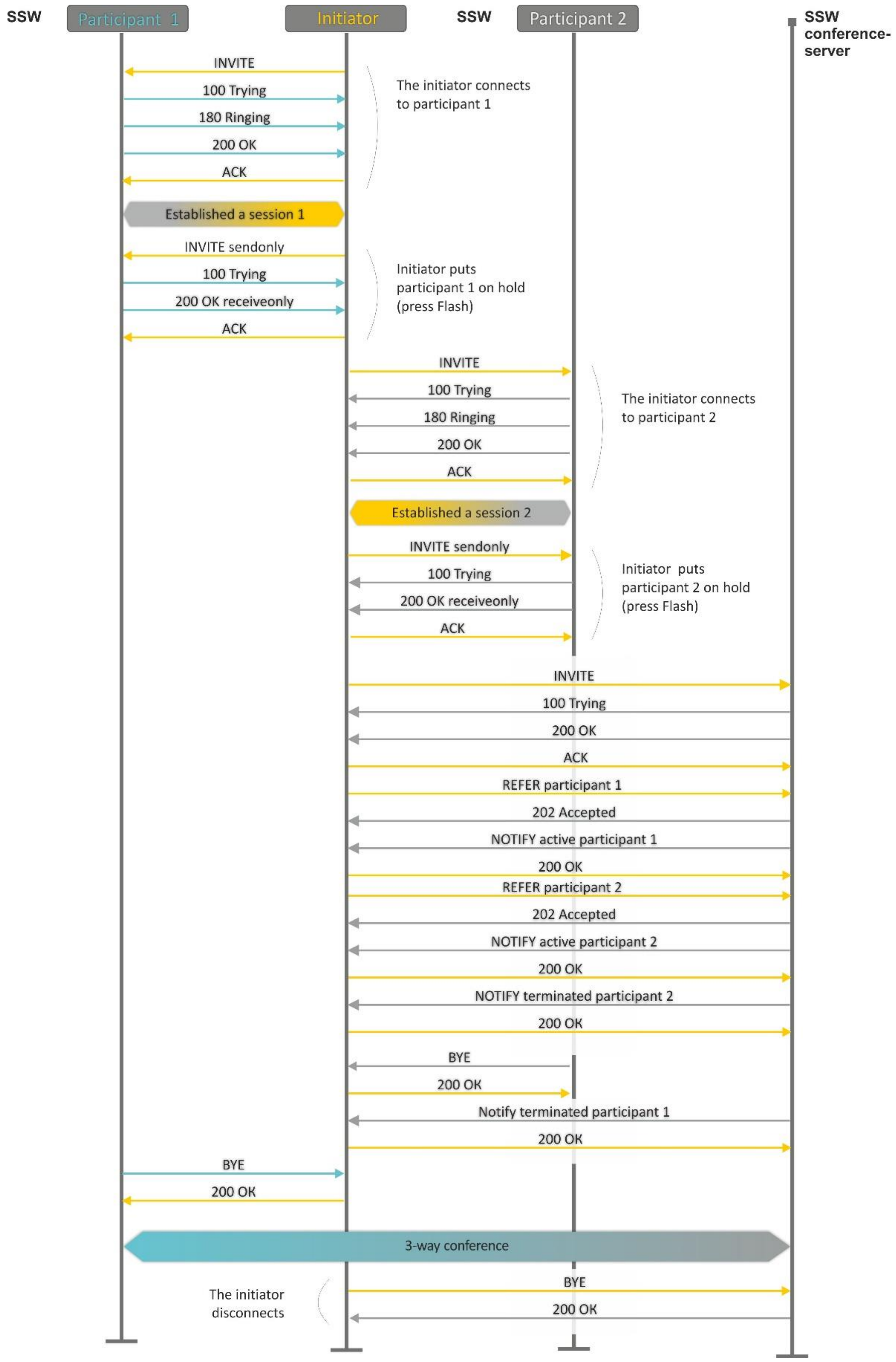


Fig. 14—Algorithm of *'3-way conference'* service performed at the conference server via SIP protocol (REFER to focus)

15 shows an algorithm of *'3-way conference'* service performed at the conference server via SIP protocol ('REFER to user' option).

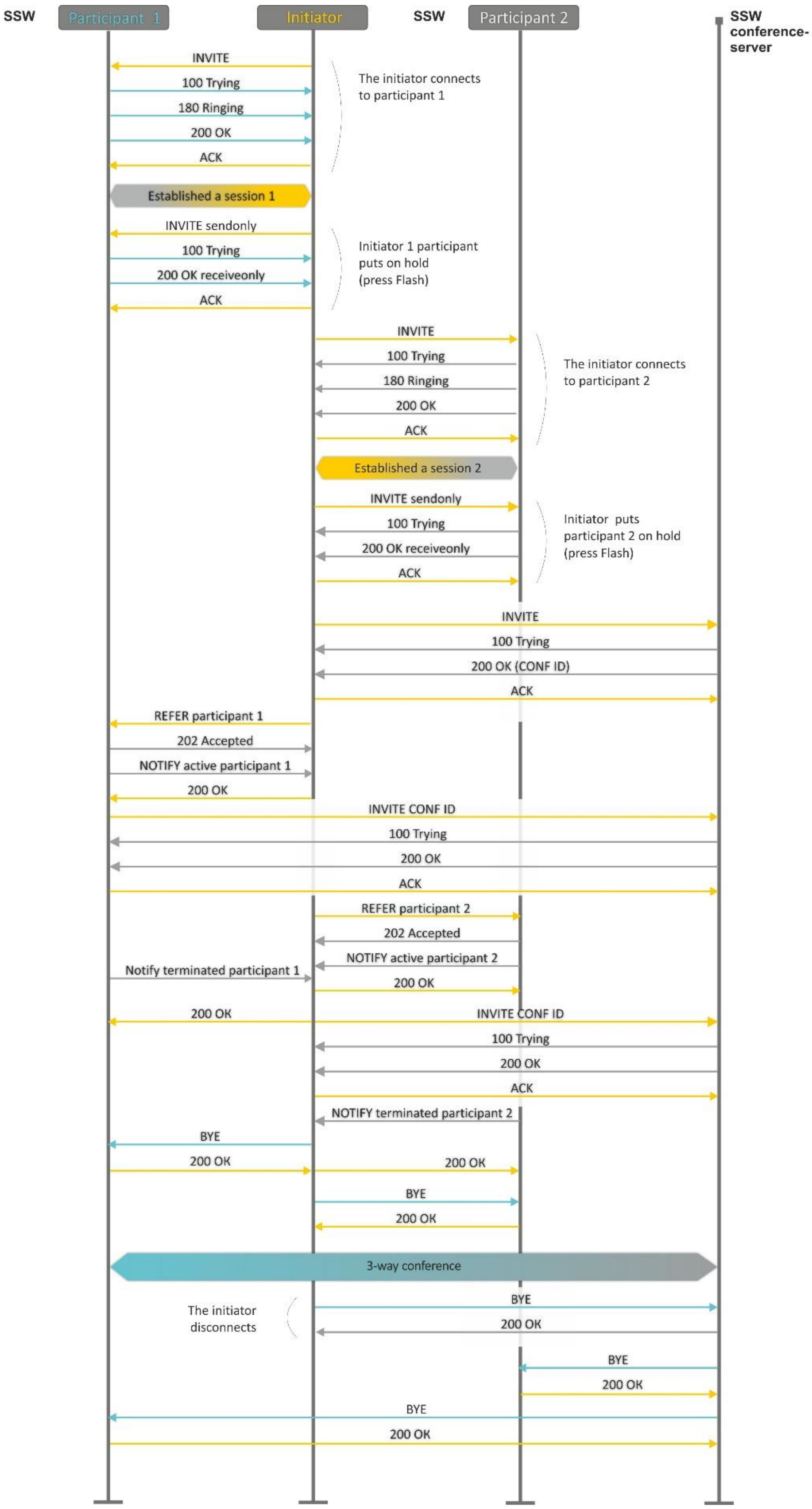


Fig. 15—Algorithm of *'3-way conference'* service performed at the conference server via SIP protocol (REFER to user)

8 CONNECTION ESTABLISHMENT ALGORITHMS

8.1 Algorithm of a Successful Call via SIP Protocol

SIP 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.

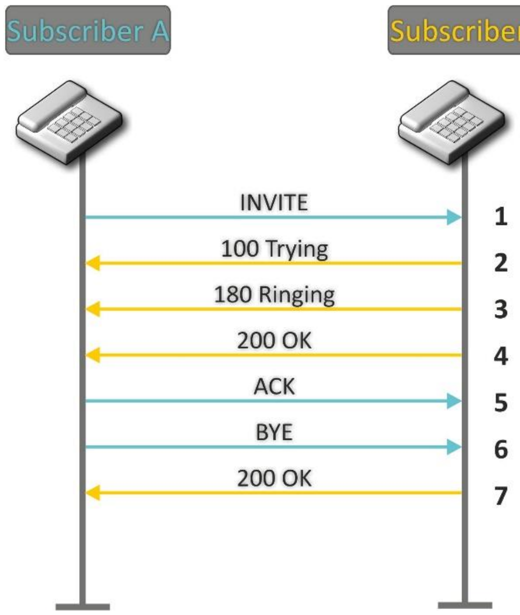


Fig. 16—SIP call algorithm

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.

8.2 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.

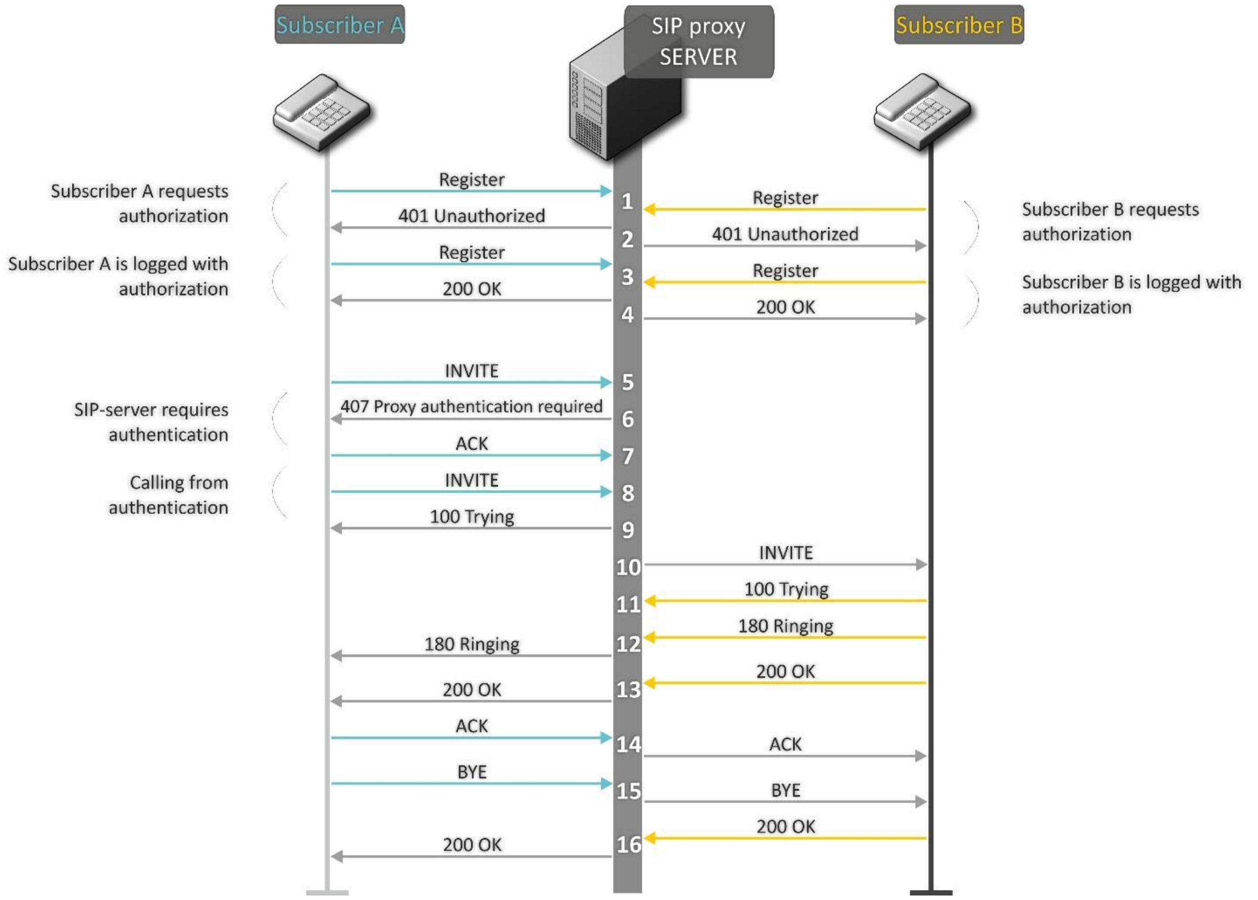


Fig. 17—Call algorithm involving SIP proxy server

Algorithm description:

Subscriber A and Subscriber B register at 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. 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.

8.3 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.

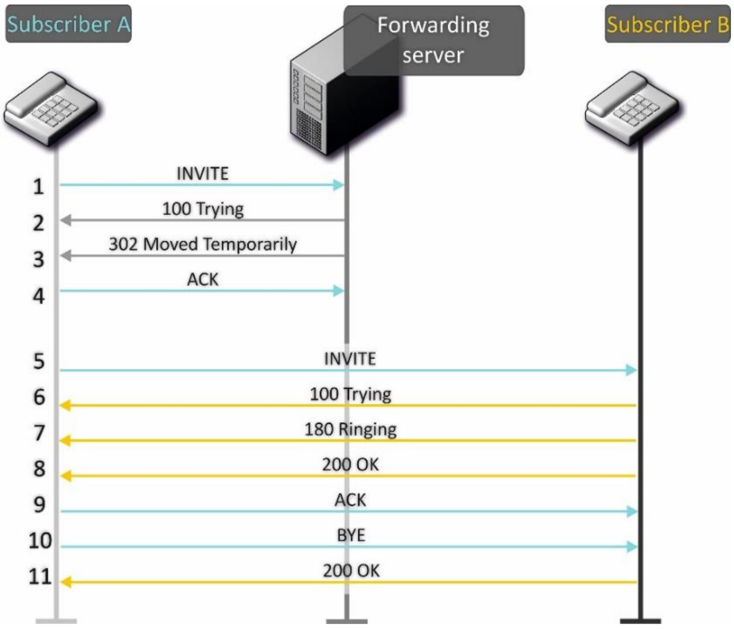


Fig. 18—Call algorithm involving forwarding server

Algorithm description:

1. Subscriber A rings up Subscriber B. Forwarding server receives the command for processing.

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. 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.

8.4 Algorithm of a Successful Call via H.323 Protocol

H.323 is ITU-T standard that describes specifications for audio and video data transmission via packet switching networks and includes standards for video and voice codecs, public domain applications, call and system management. H.323 protocol family includes three basic protocols: terminal equipment and zone controller interaction protocol—RAS, connection management protocol—H.225, and logic channel management protocol—H.245.

This section describes an example of a basic connection initiation scenario via H.323 protocol between two gateways without a gatekeeper.

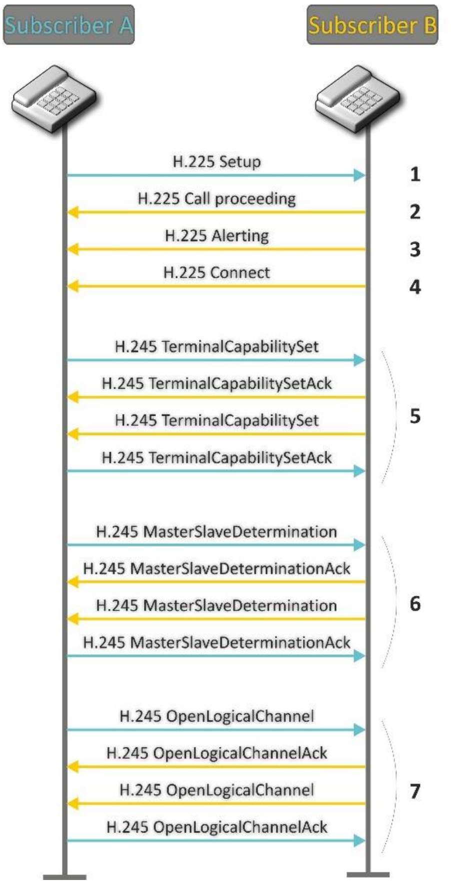


Fig. 19—H.323 call algorithm

Algorithm description:

Connection establishment (via ITU-Q.931/H.225 protocol):

1 Subscriber A gateway rings up Subscriber B (sends 'setup' message).
2 Subscriber B gateway sends a message, stating the possibility of process continuation.
3 Subscriber B gateway sends 'Alerting' notification message. 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 gateway answers the call.

Logic channel establishment (via H.245 protocol):

5 Subscriber A gateway informs Subscriber B gateway on its supported capabilities (TerminalCapabilitySet). Subscriber B gateway confirms the request (TerminalCapabilitySetAck). The same procedure is repeated in reverse direction from Subscriber B to Subscriber A.
6 Operation mode is defined—which gateway will be the 'master', and which will be the 'slave'.
7 Each gateway sends a message for a logic channel opening (OpenLogicalChannel). If gateways are ready to receive the data, they send confirmation messages on logic channel opening (OpenLogicalChannelAck). Call RTP sessions opens.

8.5 Algorithm of a Successful Call via H.323 Protocol with Gatekeeper

Gatekeeper performs address translation and manages H.323 terminals' access to network resources.

This section describes an example of a basic connection initiation scenario via H.323 protocol with a gatekeeper.

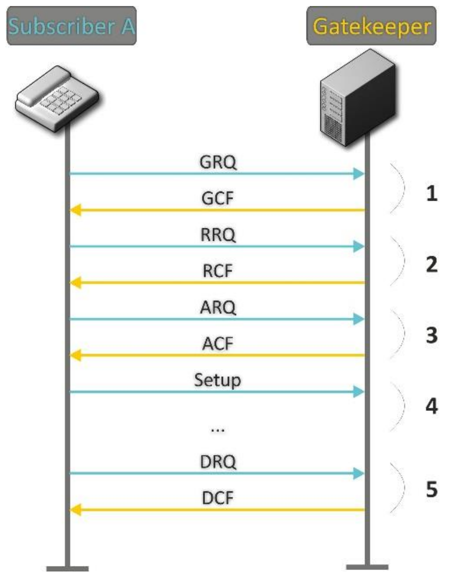


Fig. 20—Gatekeeper call algorithm

Call establishment algorithm for a subscriber and a gatekeeper:

1. Gatekeeper discovery:

   GRQ (gatekeeper request) — sending discovery request;
   GCF (gatekeeper confirm) — successful discovery.

2. Subscriber registration on a gatekeeper:

RRQ (registration request)—registration request;
RCF (registration confirm)—successful registration.

3. Request to access GK resources (when performing outgoing call):

   ARQ (admission request)—connection request;
   ACF (admission confirm)—successful response to request by the gatekeeper.

4. Call (similar to Paragraph 8.3).
5. GK call resources deallocation.

9 DESCRIPTION OF CONFIGURATION FILES

This section lists description of a configuration file, used by the device.

For *'cfg.yaml'* file description, see Tables 13 to 15.

To edit configuration files, you should:

1. Connect using RS-232 serial port (connection parameters: 115200, 8, n, 1, n; username: **admin**, w/o password). Go to Linux console by executing 'shell' command. Configuration file is located in 'etc/config' folder.
2. Edit the file using embedded editor *'joe'* (use arrow buttons to move the cursor; exit the editor without saving: `ctrl^c`, exit and save changes: `ctrl^(kx)): joe /etc/config/cfg.yaml;`
3. When you finish editing and exit the editor, save settings with `'save'` command.

9.1 Configuration file – CFG.YAML

Configuration file formation hierarchy:

```
#!version 1.0
Node1:
   Node2:
      Parameter1: Value1
      Parameter2: Value2
```

Configuration file version (#!version 1.0) is used for autoupdate.

When working with **CFG.YAML**, you should observe the following rules:

– Do not add/remove nodes;
– Do not use tab characters '/t';
Use spaces ' ' only;
– Add the same number a of spaces ' ' before each node with a specific nesting level.

9.1.1 VoIP configuration

Table 14—VoIP configuration

Field name	***Description***	***Values***
h323	**H.323 protocol configuration**	
enableh323	H.323 protocol	0-disable 1-enable
timetolive	Time period in seconds, for which the device will keep its registration on a gatekeeper	10-65535
keepalivetime	Time period in seconds, after which the device will renew its registration on a gatekeeper	10-65535
h235	Authentication on the gatekeeper with H.235 protocol	0-disable 1-enable

ignore_gcf	Output authentication data in RRQ message via H.235 protocol	0—only in case of reception of supported hash method in GCF message 1—in any events
disabletunneling	H.245 signal tunnelling through Q.931 signal channels	0—tunnelling enabled 1—tunnelling disabled
disablefaststart	faststart function	0—faststart enabled 0—faststart disabled
usegatekeeper	Registration on a gatekeeper	0-disable 1-enable
gatekeeperip	Gatekeeper IP address	A.B.C.D
h323aliase	Gateway identifier	String, 15 characters max.
isgateway	Method of device registration on gatekeeper	0 -registered as a terminal device registered as a gateway
dtmftransfer	Transfer method for flash and DTMF tones via H.323 protocol	1—H.245 Alphanumeric—basicstring compatibility is used for DTMF transmission, and hookflash compatibility for flash transmission (flash is transferred as '!' symbol). 2-H.245 Signal–dtmf compatibility is used for DTMF transmission, and hookflash compatibility for flash transmission (flash is transferred as '!' symbol); 3-Q931 Keypad IE – for DTMF and flash transmission (flash is transferred as '!' symbol), Keypad information element is used in INFORMATION Q931 message;
bearercapability	Select information transfer service (We recommend using value '3.1 kHz Audio'. All other values used only for compatibility with communicating gateways.)	0 – Speech 8 – Unrestricted Digita 9 – Restricted Digital 16 – 3.1 kHz Audio 17 – Unrestricted Digital With Tones
password	Password used for H.235 protocol authentication	String, 15 characters max.
range	**TCP/IP protocol settings**	
tcpportmin	The lower limit of a range of TCP ports used for H.323 - H.245/H.225 stack protocols' operation	1024-65535
tcpportmax	The upper limit of a range of TCP ports used for H.323 - H.245/H.225 stack protocols' operation	tcpportmin-65535
udpportmin	The lower limit of a range of UDP ports used for H.323 stack RAS protocol operation	1024-65535
udpportmax	The upper limit of a range of UDP ports used for H.323 stack RAS protocol operation	udpportmin-65535

rtph323min	The lower limit of a range of RTP ports used for H.323 protocol operation	1024-65535
rtph323max	The upper limit of a range of RTP ports used for H.323 protocol operation	rtph323min-65535
rtpsipmin	The lower limit of a range of RTP ports used for SIP protocol operation	1024-65535
rtpsipmax	The upper limit of a range of RTP ports used for SIP protocol operation	rtpsipmin-65535
intrcpmin	The lower limit of a range of ports used for pickup traffic transmission (SORM feature)	1024-65535
intrcpmax	The upper limit of a range of ports used for pickup traffic transmission (SORM feature)	Intrcpmin-65535
sip_dscp	Type of service for RTP packets (for utilized values, see Table)	0-255
verify_remote_media	Control of parameters of media traffic received	0–disable 1–enable
dvo	**Configuration of access codes for supplementary services**	
callwaiting	'Call waiting' service	00-99
ct_attended	'Call transfer' service with the wait for response of the subscriber, the call is being forwarded to	00-99
ct_unattended	'Call transfer' service without the wait for response of the subscriber, the call is being forwarded to	00-99
cf_unconditional	'Call forward unconditional' service (CFU)	00-99
cf_busy	'Forward on busy' service (CFB)	00-99
cf_noanswer	'Forward on no reply' service (CFNR)	00-99
cf_outofservice	'Forward on out of service' service (CFOOS)	00-99
dnd	Restrict all incoming calls, outgoing communication is possible	00-99
modem	Echo caneller disabling	00-99
sip	**SIP protocol configuration**	
enablesip	SIP protocol	0-disable 1-enable
invite_init_t	SIP timer—T1, ms	100-1000
invite_total_t	Total timeout for message transmission, ms	1000-39000
invite_init_max_t	SIP timer—T2, ms	1000 - 32000
transport	Transport layer protocol, used for SIP message transmission	0—Use both UDP and TCP protocols, UDP priority will be higher 1—Use both UDP and TCP protocols, TCP priority will be higher 2—Use UDP protocol only 3—Use TCP protocol only

sip_mtu	Maximum SIP protocol data size in bytes, sent with UDP transport protocol	1350-1450
shortmode	Use shortened field names in SIP protocol header	0-disable 1-enable
publicip	IP address of a public NAT	A.B.C.D
port_reg_delay_t	Timeout between successive registrations of neighbouring ports (ms)	500..5000
stun_enable	Use STUN server for public address discovery	0-disable 1-enable
stun_server	STUN server IP address	A.B.C.D
stun_interval	STUN server polling period	10-1800
general	**basic settings**	
device_name	device name	String, 15 characters max. or ''—parameter is not defined
start_timer	Dialling timeout for the first digit of a number; when there is no dialling during the specified time, 'busy' tone will be sent to the subscriber, and the dialling will end.	10-300
duration_timer	Complete number dialling timeout	10-300
wait_answer_timer	wait answer timer	40-300
use_uni	Use prefix in SIP-T protocol operations	0-disable 1-enable
unit_prefix	Prefix for SIP-T protocol operations	0–20 digits
fans_force_enable	continuous fan operation	0–disable (turn on at threshold) 1-enable
fans_threshold_temperature	Fans turn on threshold (˚C)	35..55
trace	**sip_level**	
sip_level	SIP protocol log level	-1..9
h323_level	H.323 protocol log level	0-6
vapi_level	VAPI library log level	AB, where: A=0..6 (Lib level) B=1..5 (APP level)
vapi_enabled	VAPI library logging	0-disable 1-enable
app_info	Send application info messages to Syslog server	0-disable 1-enable
app_warn	Send application warning messages to Syslog server	0-disable 1-enable
app_err	Send application failure messages to Syslog server	0-disable 1-enable
app_dbg	Send application debug messages to Syslog server	0-disable 1-enable
app_alarm	Send alarm event messages to Syslog server	0-disable 1-enable

trace_out	Direction of Syslog information output	off—do not store to syslog syslog_server—store to SYSLOG server stdout—store to STDOUT
syslog_addr	Syslog server IP address	A.B.C.D
syslog_port	Syslog server port for message reception	1-65535
run_syslog	Run Syslog on device startup	0-disable 1-enable
tones	**tone signal parameters configuration**	
country	preconfigurated settings for certain country selecting	Russia – tone signals used in Russia Iran – tone signals used in Iran Manual – manual tone signals configuration
dialtone_freq	'Station reply' tone frequency, Hz	200 - 3800
dialtone_cadence	'Station reply' tone cadences, ms	15 - 30000
busytone_freq	'Busy' tone frequency, Hz	200 - 3800
busytone_cadence	'Busy' tone cadences, ms,ms	two values divided by coma, without space between them 0 or 15 — 30000,15 — 30000 A value of 0 in the first position indicates that no 'Busy' signal will be generated and no 'Notification of Unathorized Handset/ROH' signal will be generated after 2 minutes if the handset is not available.
disconnect_freq	disconnect tone frequency, Hz	200 - 3800
disconnect_cadence	disconnect tone cadences, ms,ms	two values divided by coma, without space between them 0 or 15 — 30000,15 — 30000 A value of 0 in the first position indicates that no 'Disconnect' signal will be generated and no 'Notification of Unathorized Handset/ROH' signal will be generated after 2 minutes if the handset is not available.
ringbacktone_freq	'Ringback' tone frequency, Hz	200 - 3800
ringbacktone_cadence	'Ringback' tone cadences, ms,ms	two values divided by coma, without space between them 15 — 30000,15 — 30000
congestiontone_freq	'Congestion' tone frequency, Hz,Hz	two values divided by coma, without space between them 200 - 3800,200 - 3800
congestiontone_cadence	'Congestion' tone cadences, ms,ms,ms,ms	four values divided by coma, without space between them 15 — 30000,15 — 30000,15 — 30000,15 — 30000
limits	**call limits**	
limit_0 to 19	Call restriction	A.B.C.D or FQDN or [proxy] N

	Examples: limit_0: [proxy] 5 limit_1: 192.168.16.53 8	where: [proxy]—defines the restriction for calls through SIP-proxy or H.323 Gatekeeper N—number of simultaneous calls
groups	**call groups**	
group_0 to 31	call group configuration	
phone	Group number	String, 20 characters max. or ''—parameter is not defined
name	Group name used for authentication	String, 20 characters max. or ''—parameter is not defined
password	Authentication password	String, 20 characters max. or ''—parameter is not defined
ports	List of subscriber ports belonging to the group	String, 30 characters max., ports are comma-separated, or ''—parameter is not defined Enumeration of subscriber ports and pickup groups, used in a file, is less by 1 than enumeration, used in web interface and on the device housing!
type	Group type	0—group call 1—serial discovery group 2—cyclic group
timeout	Call timeout for a single group member	0-99
busy	Call queueing, when all group members are busy	0—group without a queue 1—group with a queue
enabled	Group usage	0-disable 1-enable
sip_port	Local UDP port used for port operations via SIP protocol	0-65535
profile_id	SIP profile number	0-7
cadences	**'Distinctive ring' service**	
cadence _0 .. 31	**you may use up to 32 'distinctive rings'**	
Enumeration of 'distinctive rings', used in a file, is less by 1 than enumeration, used in web interface! **'*cadence 0*' in a file corresponds to 'rule 1' in WEB interface.**		
rule	Mask of the number of the caller that will trigger the 'distinctive ring' with a call to the requested port	Syntax described in Section 5.1.2.9 The 'Distinctive Ring' Service Configuration submenu
ring	Ring duration	0-25500
pause	Pause duration	0-25500
mask	Subscriber profiles for ports using this rule	Profile numbers from 0 to 7, comma-separated
modifiers	**Modifier configuration**	
modifier_0 .. 15	**You can use up to 16 modifier groups**	
Enumeration of modifiers and their groups, used in a file, is less by 1 than enumeration, used in web interface! **Example: *'modifier_ 0'* in a file corresponds to 'modifier 1' in WEB interface**		

mod_rule_0..31	Rule for modification in a group, specify 3 parameters, space-delimited: number dialling rule, modification for a dialled number, modification for a calling number.	Syntax described in Section 5.1.2.10 The 'Modifiers' submenu
profile	**SIP profiles**	
- profile_0 .. 7	**SIP profile configuration**	
Enumeration of SIP profiles, used in a file, is less by 1 than enumeration, used in web interface! **Example: *'profile_0'* in a file corresponds to 'profile 1' in WEB interface.sip, codecs, regexprd, dialplan and sip_cadences parameters are configured separately for each profile.** ***Sip, codecs, regexprd, dialplan and sip_cadences* parameters are configured separately for each profile.**		
-- sip	**SIP protocol configuration**	
cw_ringback	Send 180 or 182 message, when the second call is received on the port with an active 'Call waiting' service	0—send 180 1—send 182
ringback	Parameter defines, whether the gateway should send a ringback tone upon receiving an incoming call	0-disable 1-enable
ringback_sdp	Transfer of 'ringback' tone upon receiving '183 Progress' message	0—when an incoming call is received, the gateway will not generate a ringback tone. 1—when an incoming call is received, the gateway will generate a ringback tone and send it to the communicating gateway in the voice frequency path. Voice frequency path forwarding will be performed along with '180 ringing' message transmission via SIP protocol; 1—when an incoming call is received, the gateway will generate a ringback tone and send it to the communicating gateway in the voice frequency path. Voice frequency path forwarding will be performed along with '183 ringing' message transmission via SIP protocol. 3-when an incoming call is received, the gateway will generate a ringback tone and will reply 183 progress.
100rel	Utilization of reliable provisional responses (RFC3262)	0—reliable provisional responses are supported 1—reliable provisional responses are mandatory 2—reliable provisional responses are disabled
no_replaces	Usage of 'replaces' tag during 'Call Transfer'	0–enable 1–disable
mode	SIP server operation mode (SIP-proxy)	0–disable 1—SIP-proxy redundancy mode without main SIP-proxy management 2—SIP-proxy redundancy mode with main SIP-proxy management
user_phone	Usage of 'User=Phone' tag in SIP URI	0-disable

		1-enable
uri_escape_hash	Transfer of hash symbol (#) in SIP URI	0—as '#' symbol 1—as escape sequence '%23'
dtmfmime	MIME extension type used for DTMF transmission in SIP protocol INFO messages	dtmf—DTMF is sent in application/dtmf extension ('*' and '#' are sent as digits 10 and 11) dtmfr—DTMF is sent in application/dtmf-relay extension ('*' and '#' are sent as symbols '*' and '#') audio–DTMF is sent in audio/telephone-event extension ('*' and '#' are sent as digits 10 and 11).
hfmime	MIME extension type used for Flash transmission in SIP protocol INFO messages	dtmf—flash is sent as 'signal=hf'; if application/dtmf is used, then the flash is sent as the digit '16' hookf—flash is sent in Application/ Hook Flash extension (as 'signal=hf') broadsoft—flash is sent in Application/ Broadsoft extension (as 'event flashhook') broadsoft—flash is sent in application/sscc extension (supports by huawei)
register_retry_interval	Retry interval for SIP server registration attempts, when the previous attempt was unsuccessful	10-3600
inbound_proxy	Rules for incoming calls	0—receive incoming calls from all hosts 1—receive incoming call from SIP-proxy only
domain	SIP domain	String, 20 characters max. or ''—parameter is not defined
domain_to_reg	Use domain for registration (REGISTER messages in request URI)	0-disable 1-enable
options	Test the main proxy using OPTIONS, REGISTER, or INVITE messages in 'homing' redundancy mode	0 – INVITE 1 – OPTIONS 2 – REGISTER
keepalivet	Period of time between OPTIONS or REGISTER management message transfers, ms	10000-3600000
outbound	Use SIP-proxy as an outbound proxy for outgoing calls	0-disable 1-enable 2—enable and play busy tone if port is not registered
obtimeout	Dialling timeout for directions not specified in configuration, when 'outbound proxy' and 'dialplan' routing rules are used, in seconds	0-300
expires	Registration renewal time period	10-345600

authentication	device authentication mode	1—enable SIP server authentication with common user name and password for all subscribers 2—enable SIP server authentication with different user names and passwords for each subscriber
registration	Usage of registration server Used value is a decimal number, calculated from the binary representation of a string of registrars being used. regrar: 4 3 2 1 0 I.e. usage of 3 and 4 registrars only will be equal to the following binary record: 11000, parameter value after conversion to a decimal system—24.	0-disable 1—use regrar_0 2—use regrar_1 4—use regrar_2 8—use regrar_3 16—use regrar_4 3—use regrar_0 and 1 7—use regrar_0, 1, 2 15—use regrar_0, 1, 2, 3 31—use all regrars
username	User name for 'global' mode authentication	String, 20 characters max. or ''—parameter is not defined
password	Password for 'global' mode authentication	String, 20 characters max. or ''—parameter is not defined
natsupport	Parameter is not used	
publicip	Parameter is not used	
stunserver	Parameter is not used	
reduce_sdp_ media_count	Remove inactive media streams during SDP session modification	0-disable 1-enable
p_rtp_stat	Use 'P-RTP-Stat' header in BYE request or in its reply to transfer RTP statistics	0-disable 1-enable
timer	SIP session timer support (RFC 4028)	0–disable 1–enable
min_se	Minimum time interval for connection health checks in seconds	90-1800
session_expires	Period of time in seconds that should pass before the forced session termination, if the session is not renewed in time	90-80000
proxy_0	SIP proxy server address (0—main, 1—first redundant, …)	String, 40 characters max. or ''—parameter is not defined
proxy_1		
proxy_2		
proxy_3		
proxy_4		
regrar _0	registration server address (0—main, 1—first redundant, …)	String, 40 characters max. or ''—parameter is not defined
regrar _1		
regrar _2		
regrar _3		
regrar _4		
keep_alive_mode	Active session support mode for operations through NAT	0—off—disabled

		1—options—use OPTIONS request as an active session support message 2—notify—use NOTIFY notification as an active session support message 3—CRLF—use CRLF special request as an active session support message
keep_alive_interval	Active session support message transmission period	30 - 120
conference_type	Conference assembly mode	0—Local—conference assembly is performed locally at the gateway Voice packets are mixed at the gateway. Voice packets are mixed at the gateway; 2 – Remote—conference assembly is performed at the conference server Voice packets are mixed at the server. Voice packets are mixed at the server. REFER to focus mode. 2 – Remote—conference assembly is performed at the conference server Voice packets are mixed at the server. Voice packets are mixed at the server. REFER to user mode.
Conference_serv_name	Conference server name in Remote mode operation	String, 50 characters max.
ims_notify_on	Service (simulation service) management using IMS (3GPP TS 24.623)	0-disable 1-implicit subscribe (without subscribe query transmission) 2-explicit subscribe (with subscribe query transmission)
xcap_conference_name	Name sent in XCAP attachment for '3-party conference' service management	String, 30 characters max.
xcap_hotline_name	Name sent in XCAP attachment for 'Hotline' service management	String, 30 characters max.
xcap_cw_name	Name sent in XCAP attachment for 'Call waiting' service management	String, 30 characters max.
xcap_callhold_name	Name sent in XCAP attachment for 'Call hold' service management	String, 30 characters max.
use_alert_info	'alert-info' header processing in INVITE request	0–disable 1–enable
changeover	Type of requests used for changeover to redundant proxy	0 – INVITE, REGISTER 1 – REGISTER 2 – INVITE 3 – OPTIONS
changeover_by_408	Redundant proxy changeover when response 408 is received	0—no changeover when response 408 received 1—perform changeover when response 408 received
ruri_full_compliance	RURI control for incoming call	0—partial control (user)

		1—full control (user, host, port)
-- codecs	**device codec settings**	
g711a	G.711A codec	0-disable 1, 2, 3, 4, 5—enable The value represents the codec utilization priority: 1—the highest, 5—the lowest. **Do not use two different g729 codecs simultaneously**
g711u	G.711U codec	
g726_32	G.726-32 codec	
g729a	G.729 annexA codec (when defining codec compatibility, codec description is sent via SIP specifying that annexB is not used: a=rtpmap:18 G729/8000 a=fmtp:18 annexb=no)	
g729b	G.729 annexB codec	
g723	G.723.1 codec	
g711pte	Amount of voice data in milliseconds (ms), transmitted in a single RTP protocol voice packet for G711 codec	10, 20, 30, 40, 50, 60
g729pte	Amount of voice data in milliseconds (ms), transmitted in a single RTP protocol voice packet for G729 codec	10, 20, 30, 40, 50, 60, 70, 80
g723pte	Amount of voice data in milliseconds (ms), transmitted in a single RTP protocol voice packet for G723.1 codec	30, 60, 90
g726_32_pte	Amount of voice data in milliseconds (ms), transmitted in a single RTP protocol voice packet for G726-32 codec	10, 20, 30
g726_32_pt	payload type for G.726-32 codec	96 – 127
faxdirection	Transmission direction for fax tone detection and subsequent switching to fax codec	0—tones are detected during both fax transmission and receiving. During fax transmission, CNG FAX signal is detected from the subscriber's line. During fax receiving, V.21 signal is detected from the subscriber's line (Caller and Callee); 1—tones are detected only during fax transmission. During fax transmission, CNG FAX signal is detected from the subscriber's line (Caller); 2—tones are detected only during fax receiving. During fax receiving, V.21 signal is detected from the subscriber's line (Callee); 3—disables fax tone detection, but will not affect fax transmission (off fax transfer)
dtmftransfer	DTMF tone transmission method	0—inband, in RTP voice packets; 1—according to RFC2833 recommendation, as a dedicated payload in RTP voice packets; 2—outband, with SIP/H323 protocol methods
flashtransfer	Short clearback Flash transmission method	0—Flash transmission disabled;

	(Flash transmission by the subscriber's port via IP network is possible only when 'Transmit flash' is configured on this port)	1—Flash transmission is performed according to RFC2833 recommendation, as a dedicated payload in RTP voice packets; 2—Flash transmission is performed with SIP/H323 protocol methods.
faxtransfer	Master protocol/codec used for fax transmissions	0—use G.711A codec for fax transmissions. 1—use G.711U codec for fax transmissions. 2—use T.38 protocol for fax transmissions.
slave_faxtransfer	Slave protocol/codec used for fax transmissions	0—use G.711A codec for fax transmissions. 1—use G.711U codec for fax transmissions. 2—use T.38 protocol for fax transmissions. 3—do not use slave protocol/codec for fax transmissions.
modemtransfer	Protocol used for data transfer (modem)	0—use G.711A codec in VBD (V.152) mode to transfer data via modem connection; 1—use G.711U codec in VBD (V.152) mode to transfer data via modem connection; 2—use G.711A codec to transfer data via modem connection. When entering modem data transfer mode via SIP protocol, echo cancellation and VAD are disabled with attributes described in RFC3108 recommendation: a=silenceSupp:off - - - - a=ecan:fb off -; 3—use G.711U codec to transfer data via modem connection. When entering modem data transfer mode via SIP protocol, echo cancellation and VAD are disabled with attributes described in RFC3108 recommendation: a=silenceSupp:off - - - - a=ecan:fb off -; 4—disable modem signal detection; 5—use G.711A codec in CISCO NSE mode to transfer data via modem connection; 6—use G.711U codec in CISCO NSE mode to transfer data via modem connection.
payload	Type of payload used to transfer RFC2833 packets	96-127
nse_payload	Type of payload used to transfer CISCO NSE packets	96-127

silencedetector	Voice activity detector (VAD) and silence suppression (SSup)	0-disable 1-enable
echocanceller	Echo cancellation	0-disable 1-enable
dispersion_time	Echo delay time, ms	8, 16, 24 - 128
ecan_nlp_disable	NLP disable	0—NLP enabled 1—NLP disabled
rtcp_period	The voice frequency path status control function. Defines the period of time, during which the opposite side will wait for RTCP protocol packets. When there is no packets in the specified period of time, established connection will be terminated. Control period value is calculated using the following equation: RTCP timer* RTCP control period seconds.	2-65535
rtcp_timer	Time period for control packet transfer via RTCP protocol, in seconds	5-65535
rtcp_xr	Send RTCP Extended Reports packets	0-disable 1-enable
rfc3264_pt_common	When performing outgoing call, receive DTMF tones in rfc2833 format with payload type proposed by a communicating gateway. When unchecked, tones will be received with the payload type, configured on the gateway. Enables compatibility with gateways that incorrectly handle rfc3264 recommendation.	0-disable 1-enable
comfortnoise	Comfort noise generator	0-disable 1-enable
jb_pt_delay	Size of a fixed jitter buffer, used in fax or modem data transfer mode (ms)	0-200
jb_vo_delay_min	Size of fixed jitter buffer or lower limit (minimum size) of adaptive jitter buffer (ms)	0-200
jb_vo_delay_max	Upper limit (maximum size) of adaptive jitter buffer (ms)	jb_vo_delay_min-200
jb_vo_adaptive	Use fixed or adaptive jitter buffer operation mode	0–fixed 1–adaptive
jb_vo_del_threshold	Threshold for immediate packet deletion (ms): - If call quality is more important than delays, we recommend to set the maximum value for this setting—500ms; - And vice versa, if delays have a priority over the quality, we recommend to set the minimum value for this setting;	jb_vo_delay_max-500

	- It is recommended, that 'Delay threshold' was greater than 'Delay max' for at least of 50ms.	
jb_vo_del_mode_soft	Setting defines the method of packet deletion during buffer adjustment to lower limit.	0—Hard mode 1—Soft mode
t38_bitrate	Maximum fax transfer rate	9600, 14400
t38_datagram	Maximum datagram size	272-512
regexprd	**configuration of gateway numbering schedule using regular expressions**	
regex_on	Configuration of a numbering scheme based on regular expressions	0—use dialplan, described in dialplan section 1—use numbering scheme based on regular expressions
proto	Signalling protocol	sip – SIP;h323 – H.323 (for profile_0 only).
regex	regular expression Example: regex: L15 S8 (5xxxx[x#*]@192.168.16.160:5062)	Syntax LX SY (Rule), where X—L-timer value, Y—S-timer value. For timer and Rule description, see Section 5.1.2.2.5.4 Configuration of Regular Expression Routing Rules **Enumeration of pickup groups, used in a file, is less by than enumeration, used in web interface!!!**
start_timer	start timer	10 - 300
dialplan	**configuration of prefixes for routing and pickup groups**	
dialplan_0 to 299	**Format:** d1 d2 d3 d4 d5 d6 d7 d8 d9 d10 d11 **Example:** 55 6 0 sip 192.168.16.92 '' 0 0 0 - 0 Where d1—prefix Value: String, 20 characters max; d2—minimum length of a number dialled by the prefix Value: 1-20; d3—dialling timeout for the next digit of a number, in seconds Value: 0-20; d4—signalling protocol, used in prefix operations: • h323—H.323 protocol operation (for *profile_0* only); • sip—SIP protocol operation; • sip-t—SIP-T protocol operation; • pickup—a pickup group; d5—address of a communicating gateway: • A.B.C.D or FQDN— in point-to-point operation mode; • 'gatekeeper'—when H.323 gatekeeper is used (for *profile_0* only); • 'proxy'—when SIP proxy is used. d6—dialling modifier, enables translation of a callee number. Modifier is added at the beginning of a dialled number. Value: string, up to 8 digits, in quotation marks; d7—dialling modifier, enables translation of a callee number. Defines the number of digits to be deleted from a dialled number for outgoing calls (the most significant digits of a number will be removed) Value: 0..20; d8—CdPN callee number type (for SIPT and H.323): • 0 – unknown; • 1 – subscriber; • 2 – national; • 3 – international;	

	d9—play 'PBX response' tone when the first prefix digit is dialled: • 0—do not play, • 1 – play; d10—enable routing with a prefix for subscriber ports. Defines the prefix availability for subscriber ports. Value: String, 100 characters max. *String formation rules:* –portN,..portM or +portN,..portM, where '–' means that access with a prefix is denied for ports, '–' - granted, portN,..portM—comma-separated list of ports. Example:+0,32—access is allowed for ports 1 and 33. **Enumeration of subscriber ports and pickup groups, used in a file, is less by 1 than enumeration, used in web interface and on the device housing!** d11—defines the preferred packetization time in SIP protocol operation. • 0-disable; • 10, 20, 30, 40, 50, 60, 70, 80, 90—packetization time.	
sip_cadences	**Non-standard ringing generated by 'alert-info' header processing**	
- sip_cadence_0 .. 15	**configuration of ringing generation rules**	
Enumeration of rules, used in a file, is less by 1 than enumeration, used in web interface!		
name	Signal received in alert-Info header	For description of these parameters, see Section 5.1.2.2.6 **Alert-Info distinctive ring**
ring_rule	Call transmitting formation rule	
ports	**configuration of device subscriber ports and subscriber profiles**	
port_def_0..7	settings of subscriber profiles	
Enumeration of subscriber profiles, used in a file, is less by 1 than enumeration, used in web interface! **Example: *'port_def_2'* in a file corresponds to 'profile 3' in WEB interface.**		
aon	Caller ID mode	0 - Caller ID is disabled; 1–'Russian Caller ID' method; 2 - DTMF Caller ID method; 3—FSK Caller ID method using bell202 standard; 4—FSK Caller ID method using ITU-T V.23 standard;
taxophone	Payphone mode	0—payphone mode is disabled 1—polarity reversal 2—16kHz meter pulse 3—12kHz meter pulse
category	SS category	0-255
min_flashtime	Lower limit of Flash impulse duration, ms	70-1000
flashtime	Upper limit of Flash impulse duration, ms	min_flashtime (no less than 200)-1000
gainr	Volume of voice reception, x0.1dB	-230-+20
gaint	Volume of voice transmission, x0.1dB	-170-+60
cfb_pri_over_cw	Priority between CFB (Forward on busy) and CW (Call wait) services	0—CW service has a priority over CFB

		1—CFB service has a priority over CW
aon_hide_name	Transmission of Caller ID information in Fsk_bell202, Fsk_v23 modes	0—information will be sent with a subscriber name 1—information will be sent without a subscriber name
aon_hide_date	Transmission of Caller ID information in Fsk_bell202, Fsk_v23 modes	0—Caller ID information will be sent with time and date 1—Caller ID information will be sent without time and date
playmoh	'Music on hold' service	0-disable 1-enable
enable_cpc	Use a short-time break of the subscriber loop on clearback from the opposite subscriber's side	0-disable 1-enable
cpc_time	Duration of a short-time break of the subscriber loop, ms	200-600
cpc_rus	Subscriber category;	0-disable 1-10—subscriber category
stop_dial	'#' button operation	0—recognize '#' as DTMF tone 1—use '#' to end the dialling
modifier	Modifier group used by this profile	0 - 15
dscp	Type of service for RTP packets (for utilized values, see Table)	0 - 255
agc_spk_enable	Rx AGC	0-disable 1-enable
agc_mic_enable	Tx AGC	0-disable 1-enable
agc_spk_level	Rx adjustment level, dB	-1,-4,-7,-10,-13,-16,-19,-22,-25
agc_mic_level	Tx adjustment level, dB	-1,-4,-7,-10,-13,-16,-19,-22,-25
port_0..71:	Individual ports 0...71 configuration	
Enumeration of subscriber ports, used in a file, is less by 1 than enumeration, used in web interface and on the device housing! Example, port_0 in file correspond to port 1 in WEB interface and device case.		
phone	Subscriber number	String, 50 characters max. or ''—parameter is not defined
user_name	subscriber name	String, 50 characters max. or ''—parameter is not defined
auth_name	User name used for authentication	String, 50 characters max. or ''—parameter is not defined
auth_pass	Authentication password	String, 50 characters max. or ''—parameter is not defined
hotnumber	number that will receive the call when 'Hotline/warmline' is enabled;	String, 20 characters max. or ''—parameter is not defined
custom	Individual port configuration usage	0-use general settings from main configuration for all ports 1-use individual port settings
aon	Caller ID mode	0 - Caller ID is disabled

		1–'Russian Caller ID' method 2 - DTMF Caller ID method 3—FSK Caller ID method using bell202 standard 4—FSK Caller ID method using ITU-T V.23 standard
taxophone	Payphone mode	0—payphone mode is disabled 1—polarity reversal 2—16kHz meter pulse 3—12kHz meter pulse
min_flashtime	Lower limit of Flash impulse duration, ms	70-1000
flashtime	Upper limit of Flash impulse duration, ms	min_flashtime (no less than 200)-1000
gainr	Volume of voice reception, x0.1dB	-230-+20
gaint	Volume of voice transmission, x0.1dB	-170-+60
category	SS category	0-255
calltransfer	'Call transfer' service	0-transmit flash to line using SIP INFO/H.245/Q.931 methods 1–Attended CT 2–Unattended CT 3-do not detect flash
callwaiting	'Call waiting' service	0-disable 1-enable
cfb_pri_over_cw	Priority between CFB (Forward on busy) and CW (Call wait) services	0—CW service has a priority over CFB 1—CFB service has a priority over CW
aon_hide_name	Transmission of Caller ID information in Fsk_bell202, Fsk_v23 modes	0—information will be sent with a subscriber name 1—information will be sent without a subscriber name
aon_hide_date	Transmission of Caller ID information in Fsk_bell202, Fsk_v23 modes	0—Caller ID information will be sent with time and date 1—Caller ID information will be sent without time and date
playmoh	'Music on hold' service	0-disable 1-enable
enable_cpc	Use a short-time break of the subscriber loop on clearback from the opposite subscriber's side	0-disable 1-enable
cpc_time	Duration of a short-time break of the subscriber loop, ms	200-600
port_profile_id	Subscriber profile number	0-7
profile_id	SIP profile number	0-7
hotline	'Hotline/warmline' service	0-disable 1-enable

hottimeout	Delay timeout in seconds for the start of the automatic dialling when the 'Warmline' service is enabled.	0-300
ct_busy	'Forward on busy' service (CFB)	0-disable 1-enable
ct_noanswer	'Forward on no reply' service (CFNR)	0-disable 1-enable
ct_timeout	Subscriber response timeout (for 'Call forward on no reply' service)	0-300
ct_unconditional	'Call forward unconditional' service (CFU)	0-disable 1-enable
ct_outofservice	'Forward on out of service' service (CFOOS)	0-disable 1-enable
cfnr_number	Number, that the call is forwarded to when there is no reply	String, 20 characters max. or ''—parameter is not defined
cfb_number	Number, that the call is forwarded to when the subscriber is busy	String, 20 characters max. or ''—parameter is not defined
cfu_number	Number for 'Call forward unconditional'	String, 20 characters max. or ''—parameter is not defined
cfoos_number	Number, that the call is forwarded to when the subscriber is out of service	String, 20 characters max. or ''—parameter is not defined
pickupgroup	Include/exclude port to/from the pickup group	String, 30 characters max., pickup groups that the port belongs to are comma-separated, or ''—parameter is not defined. **Enumeration of pickup groups, used in a file, is less by than enumeration, used in web interface! Example: 'value 0' in a file corresponds to 'group 1' in WEB interface.**
dvo_dnd_en	Permission to order supplementary services with the phone unit, DND service	0-disable 1-enable
dvo_cf_outofservice_en	Permission to order supplementary services with the phone unit, 'Forward on out of service' service (CFOOS)	0-disable 1-enable
dvo_cf_noanswer_en	Permission to order supplementary services with the phone unit, 'Forward on no reply' service (CFNR)	0-disable 1-enable
dvo_cf_busy_en	Permission to order supplementary services with the phone unit, 'Forward on busy' service (CFB)	0-disable 1-enable
dvo_cf_unconditional_en	Permission to order supplementary services with the phone unit, 'Call forward unconditional' service (CFU)	0-disable 1-enable
dvo_ct_unattended_en	Permission to order supplementary services with the phone unit, 'Call transfer' service without the wait for response of the subscriber, the call is being forwarded to	0-disable 1-enable

dvo_ct_attended_en	Permission to order supplementary services with the phone unit, 'Call transfer' service with the wait for response of the subscriber, the call is being forwarded to	0-disable 1-enable
dvo_callwaiting_en	Permission to order supplementary services with the phone unit, 'Call waiting' service	0-disable 1-enable
dvo_modem_en	Permission to order supplementary services with the phone unit, 'Modem' service	0-disable 1-enable
dnd	Restrict all incoming calls, outgoing communication is possible	0-disable 1-enable
usealtnumber	Alternative number	0-disable 1-enable
usealtnumber_as_private	Use an alternative number as a SIP contact	0-disable 1-enable
altnumber	Alternative subscriber number	String, 20 characters max. or ''—parameter is not defined
sip_port	Local UDP port used for port operations via SIP protocol	0-65535
stop_dial	'#' button operation	0—recognize '#' as DTMF tone 1—use '#' to end the dialling
clir	Service—calling line identification restriction service—CLIR	0-disable 1-enable
disabled	port status	0—port enabled 1—port disabled
cpc_rus	Subscriber category;	0-disable 1-10—subscriber category
modifier	Modifier group used by this profile	0-15
mwi_dialtone	'Message waiting indicator' service	0-disable 1-enable
agc_spk_enable	Rx AGC	0-disable 1-enable
agc_mic_enable	Tx AGC	0-disable 1-enable
agc_spk_level	Rx adjustment level, dB	-1,-4,-7,-10,-13,-16,-19,-22,-25
agc_mic_level	Tx adjustment level, dB	-1,-4,-7,-10,-13,-16,-19,-22,-25
dscp	Type of service for RTP packets (for utilized values, see Table 5.3)	0 - 255
modem	Modem mode	0-disabled (echo canceller usage is defined by SIP profile configuration) 1-enabled (echo canceller disabled)

9.1.2 Device network settings

Table 15—Device network settings (Network)

Field name	***Description***	***Values***
network	**device network settings**	
IPADDR	Device IP address in WAN network	A.B.C.D
NETMASK	Net mask for the device location	A.B.C.D
GATEWAY	Default network gateway address	A.B.C.D
BROADCAST	WAN network broadcasting address	A.B.C.D
MTU	Maximum transmission unit (WAN)	86-1500
AUTOUPDATE	Enable gateway software and configuration autoupdate	0-disable 1-enable
AUTOUPDATE_SRC	Autoupdate configuration source	no_dhcp dhcp dhcp_vlan1 dhcp_vlan2 dhcp_vlan3
AUTOUPDATE_TFTP	Autoupdate server address or domain name	String, 40 characters max.
AUTOUPDATE_CFG	Path to the configuration file	String, 40 characters max.
AUTOUPDATE_FW	Path to firmware versions file	String, 40 characters max.
AUTOUPDATE_PROTO	Autoupdate protocol	TFTP, FTP, HTTP, HTTPS
AUTOUPDATE_AUTH	Authentication on autoupdate server	0-disable 1-enable
AUTOUPDATE_USER	Authentication login	String, 20 characters max.
AUTOUPDATE_PASS	Authentication password	String, 20 characters max.
AUTOUPDATE_CFG_MODE	Configuration autoupdate	off-disable interval-with time intervals time-at certain times
AUTOUPDATE_FW_MODE	Firmware autoupdate	
CFG_TIME	Configuration autoupdate time	days (divided by coma) space time (00:00-23:59) 0-Sunday 1-Monday 2-Tuesday 3-Thursday 4-Friday 6-Saturday
FW_TIME	Firmware update time	
CFG_INTERVAL	Configuration update period, s	60 - 65535
FW_INTERVAL	Firmware update period, s	60 - 65535
PPPOE_ENABLE		0-disable 1-enable
PPPOE_ENABLE	username	String, 20 characters max.
PPPOE_PASSWORD	password	String, 20 characters max.
PPPOE_VLAN	Use separate VLAN for PPPoE access	0-disable 1-enable
PPPOE_VID	VLAN identifier, if there is a separate VLAN for PPPoE access	1-4095

PPPOE_MTU	Maximum transmission unit (PPP)	86-1400
PPPOE_MRU	Maximum receive unit (PPP)	86 - 1492
PPPOE_NAME	Service name	String, 20 characters max.
PPPOE_LCP_ECHO_INTERVAL	LCP ECHO packets transmission period	0-65535
PPPOE_LCP_ECHO_FAILURE	LCP ECHO packets transmission errors value	0-20
PPTP_ENABLE		0-disable 1-enable
PPTP_USER	username	String, 20 characters max.
PPTP_PASSWORD	password	String, 20 characters max.
PPTP_DNS	DNS server IP address	A.B.C.D
PPTP_SERVER	PPTP server IP address	A.B.C.D
PPTP_VLAN	Use VLAN	0-disable 1-enable
PPTP_VID	VLAN identifier	1-4095
PPTP_MTU	MTU	86 - 1400
PPTP_ACCESSTYPE	VLAN protocol	DHCP Static
PPTP_GW	default gateway	A.B.C.D
PPTP_IP	IP address	A.B.C.D
PPTP_NETMASK	netmask	A.B.C.D
PPTP_IF_MTU	Maximum transmission unit (PPP)	86 - 1492
PPTP_MRU	Maximum receive unit (PPP)	86 - 1492
PPTP_LCP_ECHO_INTERVAL	LCP ECHO packets transmission period	0-65535
PPTP_LCP_ECHO_FAILURE	LCP ECHO packets transmission errors value	0-20
DHCPD	DHCP usage in WAN network	0-disable 1-enable
DHCPD1, 2, 3	DHCP in VLAN1,2,3 networks	0-disable 1-enable
VLAN1, 2, 3	VLAN 1, 2, 3 usage	0-disable 1-enable
V1IPADDR V2IPADDR V3IPADDR	VLAN1,2,3 interface IP address	A.B.C.D
V1NETMASK V2NETMASK V3NETMASK	Net mask, used for VLAN1,2,3 interface	A.B.C.D
V1BROADCAST V2BROADCAST V3BROADCAST	VLAN destination for SIP/H323 signalling traffic	A.B.C.D
VID 1,2,3	VLAN 1, 2, 3 identifier	0-disable 1-enable
V1MTU V2MTU V3MTU	Maximum transmission unit VLAN 1, 2, 3	86-1496
COS 1,2,3	802.1p priority for VLAN 1, 2, 3	0-7
RTP_VLAN	RTP transfer interface	0-disable

		1 – VLAN1 2 – VLAN2 3 – VLAN3 4 – PPPoE
SIG_VLAN	Signalling transfer interface	0-disable 1 – VLAN1 2 – VLAN2 3 – VLAN3 4 – PPPoE
CTL_VLAN	Management interface	0-disable 1 – VLAN1 2 – VLAN2 3 – VLAN3 4 – PPPoE
DNSIP	Main DNS server IP address	A.B.C.D
RESERVED_DNSIP	Redundant DNS server IP address	A.B.C.D
NTPEN	NTP protocol	0-disable 1-enable
NTPIP	NTP server IP address	A.B.C.D
TELNET_PORT	TELNET port	1 - 65535
TELNET_EN	Device access via Telnet protocol	0-disable 1-enable
SSH_PORT	SSH port	1 - 65535
SSH_EN	Device access via SSH protocol	0-disable 1-enable
STP_EN	STP protocol	0-disable 1-enable
SNMP	SNMP protocol	0-disable 1-enable
DHCP_GW	Obtain default gateway network address in WAN network via DHCP	0-disable 1-enable
DHCP_GW1, 2, 3	Obtain default gateway network address in VLAN1,2,3 networks via DHCP	0-disable 1-enable
PPP_GW	Obtain the default network gateway address from the PPP server	0-disable 1-enable
NTP_INTERVAL	NTP server synchronization period	0-disable 30–100000—use with the defined period in seconds
ZONEINFO	Timezone	**for permitted values, see Appendix L**
DST_ENABLE	Daylight saving change	0-disable 1-enable
DST_START	Daylight saving change date and time	String, 50 characters max.
DST_END	Daylight saving change set back date and time	String, 50 characters max.
DST_OFFSET	DST offset, in minutes	0-720
WEB_PORT	WEB server port number for HTTPS protocol	1-65535; default is 80
HTTPS_PORT	WEB server port number for HTTPS protocol	1-65535; default is 443
WEB_EN	Device access via web interface	0-disable 1-enable

WEB_HTTPS_ONLY	Access to the web interface only via HTTPS	0 – disable 1 – enable
RADIUS_ENABLE	Use RADIUS server for authentication of users administering the device via WEB, telnet, SSH	0-disable 1-use strict 2-use flexible
RADIUS_SERVER	RADIUS server address	<address>–server IP address or domain name <port>-server port,
RADIUS_SECRET	Password to access the RADIUS server	String, 50 characters max.
RADIUS_RETRY	Number of retries during the access to RADIUS server If the server authorization has failed, you will be able to manage the device via the local COM port only.	0-10
USE_VENDOR_INFO	Use alternative value of DHCP Option 60	0-disable 1-enable
VENDOR_INFO	DHCP Option 60 alternative value	string, 255 characters max.
LANGUAGE	Web configurator language	en—English ru—Russian
opt82_cid	Agent circuit identifier	String, 255 characters max.
opt82_rid	Remote agent identifier	String, 255 characters max.
access	**Access configuration**	
admin_pass	Admin user password	String, 50 characters max.
supervisor_pass	supervisor user password	String, 50 characters max.
operator_pass	operator user password	String, 50 characters max.
viewer_pass	viewer user password	String, 50 characters max.
web_digest	digest web authentication	0-disable 1-enable
snmp	**SNMP protocol settings**	
agentproto	Transport protocol	udp
agentport	Transport port where agent is processing	0-65535
sys_object_id	Device OID	string, 40 characters max.
sys_name	Device system name	string, 20 characters max.
sys_location	Device location	string, 20 characters max.
sys_contact	Device manufacturer contact information	string, 20 characters max.
trap_sink	Trap receiver IP address	Proxy-agent or manager server in A.B.C.D format
trap_type	SNMP protocol version	v1 v2
trap_community	Password, contained in trap messages	String, 20 characters max.
rocommunity	password for parameter reading (common: public)	String, 20 characters max.
rwcommunity	password for parameter writing (common: private)	String, 20 characters max.
snmp_users	**SNMPv3 user configuration**	

user_0	SNMPv3 user	Login, password, access mode is written comma-separated in one string Access mode: - rw-read/write - ro-read
lldp	**LLDP protocol configuration**	
enable	LLDP protocol	0-disable 1-enable
tx_interval	LLDP message transmission period (s)	0..65535
tr069	**TR-069 Monitoring and Management Protocol Configuration**	
Enable	TR-069 device management process	0-disable 1-enable
URL	ACS server address	<address>—ACS server IP address or domain name, <port>—ACS server port, 10301 by default
Username	Username used by client to access the ACS server	String, 50 characters max.
Password	Password used by client to access the ACS server	String, 50 characters max.
PeriodicInformEnable	ACS server periodical polling performed by the integrated TR-069 client at intervals equal to 'Periodic inform interval' value, in seconds.	0-disable 1-enable
PeriodicInformInterval	ACS server polling interval, in seconds	0-65535
ConnectionRequestURL	Parameter is not used, value should be blank	
ConnectionRequestUsername	Username for ACS server access to TR-069 client. Server sends ConnectionRequest notifications	String, 50 characters max.
ConnectionRequestPassword	Password for ACS server access to TR-069 client. Server sends ConnectionRequest notifications	String, 50 characters max.
NATMode	TR-069 client operation mode in the presence of NAT	STUN/Manual/Off
NATAddress	IP address of a public NAT	String, 40 characters max.
STUNEnable	Use STUN protocol for public address identification	0-disable 1-enable
STUNServerAddress	STUN server IP address or domain name	String, 40 characters max.
STUNServerPort	STUN server UDP port	1-65535; default is 3478
STUNMinimumKeepAlivePeriod	The time interval in seconds for periodic transmission of messages to STUN server for public address discovery and modification, in seconds	0-100000
STUNMaximumKeepAlivePeriod	The time interval in seconds for periodic transmission of messages to STUN server for public address discovery and modification, in seconds	0-100000

9.1.3 Switch port settings

Table 16–Switch port settings (Switch)

Field name	***Description***	***Values***
vlan	**example of switch configuration using VLAN**	
hubmode	Ethernet switch operation in hub mode	0-disable 1-enable
Port mapping: 0—GE0 (GE2) 1—GE1 (GE1) 2—GE2 (GE0) 3—CPU port (CPU) 4—SFP0 port (SFP0) 5—SFP1 port (SFP1) In models of with one SFP port is used only SFP0		
portmask0..5	Mutual availability of data ports. Defines the port that will receive the data from this port.	A B C D E F, where A – port 0 B – port 1 C – port 2 D – port 3 E – port 4 F – port 5 A, B, C, D, E, and F may take the following values: 0—data transmission to port is disabled 1—data transmission to port is enabled
enable0..5	Use 'Default VLAN ID', 'Override' and 'Egress' settings on ports 0..5	0-disable 1-enable
vid0..5	Default VLAN ID	1-4095
im0..5	IEEE mode for ports 0-5	0 – fallback 1 – check 2 – secure
eg0..5	Packet transfer rules for ports 0..5	0—unmodified—packets will be sent by the port without any changes 1—untagged—packets will always be sent without VLAN tag by this port 2—tagged—packets will always be sent with VLAN tag by this port 3—double tag—each packet will be sent with two VLAN tags—if received packet was tagged and came with one VLAN tag—if the received packet was untagged
ov0..5	Override VLAN ID—when checked, it is considered that any received packet has a VID, defined in 'default VLAN ID' row	0-disable 1-enable

portmode0..5	Data transfer and port duplex mode. Ports 3..5 values should always be set to 'auto'	auto—automatic determination of speed and duplex 10f, 10h, 100f, 100h, 1000f—possible values for speed and duplex configuration
backup_port0..5	Slave port for operation in direction reservation mode	port0..5
preemption0..5	Return to the master port, if it is operational. Works in direction reservation mode	on—enable return to the master port off—stay on the slave port
vtu	**configuration of packet routing rules for switch operation in 802.1q mode (VTU Table)**	
vtu0 to vtu15	VTU rules	
vtu0.vid	VLAN identifier	1-4095
vtu0.port0	Port operation mode 0	0 – unmodified 1 – untagged 2 – tagged 3 – not member
vtu0.port1	Port operation mode 1	
vtu0.port2	Port operation mode 2	
vtu0.cpu	Port operation mode 3	
vtu0.sfp0	Port operation mode 4	
vtu0.sfp1	Port operation mode 5	
vtu0.override	VLAN priority override	0-disable 1-enable
vtu0.priority	VLAN priority	0-7
qos	**Quality of Service functions and bandwidth restrictions**	
ieee_pri	Distribution of packets into queues depending on the 802.1p priority Example: ieee_pri: 0xfa41 = 1111 1010 0100 0001. Packets with priorities 7 and 6 are placed into queue 3, with priorities 5 and 4—into queue 2, with priorities 1 and 2—into queue 0.	0xDCBA A-D—hex numbers; D—2 high bits—queue for priority: 7, low for priority: 6; C—2 high bits—queue for priority: 5, low for priority: 4; B—2 high bits—queue for priority: 3, low for priority: 2; A—2 high bits—queue for priority: 1, low for priority: 0; 00—queue 0 01—queue 1 10—queue 2 11—queue 3

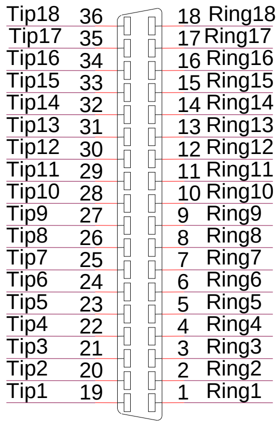
diffserv_remap - distribution of packets into queues depending on the IP diffserv priority	
diffserv_remap003C_mask	0xHGFEDCBA, where H—2 high bits—queue for priority: 0x3C, low for: 0x38; G—2 high bits—queue for priority: 0x34, low for: 0x30; F—2 high bits—queue for priority: 0x2C, low for: 0x28; E—2 high bits—queue for priority: 0x24, low for: 0x20; D—2 high bits—queue for priority: 0x1; C, low for: 0x18C—2 high bits—queue for priority: 0x14, low for: 0x10; B—2 high bits—queue for priority: 0x0C, low for: 0x08; A—2 high bits—queue for priority: 0x04, low for: 0x00; 00—queue 0, 01—queue 1, 10—queue 2, 11—queue 3
diffserv_remap407C_mask	0xHGFEDCBA, where H—2 high bits—queue for priority: 0x7C, low for: 0x78; G—2 high bits—queue for priority: 0x74, low for: 0x70; F—2 high bits—queue for priority: 0x6C, low for: 0x68; E—2 high bits—queue for priority: 0x64, low for: 0x60;

	D—2 high bits—queue for priority: 0x5C, low for: 0x58; C—2 high bits—queue for priority: 0x54, low for: 0x50; B—2 high bits—queue for priority: 0x4C, low for: 0x48; A—2 high bits—queue for priority: 0x44, low for: 0x40; 00—queue 0, 01—queue 1, 10—queue 2, 11—queue 3	
diffserv_remap80BC_mask	0xHGFEDCBA, where H—2 high bits—queue for priority: 0xBC, low for: 0xB8; G—2 high bits—queue for priority: 0xB4, low for: 0xB0; F—2 high bits—queue for priority: 0xAC, low for: 0xA8; E—2 high bits—queue for priority: 0xA4, low for: 0xA0; D—2 high bits—queue for priority: 0x9C, low for: 0x98; C—2 high bits—queue for priority: 0x94, low for: 0x90; B—2 high bits—queue for priority: 0x8C, low for: 0x88; A—2 high bits—queue for priority: 0x84, low for: 0x80; 00—queue 0, 01—queue 1, 10—queue 2, 11—queue 3	
diffserv_remapC0FC_mask	0xHGFEDCBA, where H—2 high bits—queue for priority: 0xFC, low for: 0xF8; G—2 high bits—queue for priority: 0xF4, low for: 0xF0; F—2 high bits—queue for priority: 0xEC, low for: 0xE8; E—2 high bits—queue for priority: 0xE4, low for: 0xE0; D—2 high bits—queue for priority: 0xDC, low for: 0xD8; C—2 high bits—queue for priority: 0xD4, low for: 0xD0; B—2 high bits—queue for priority: 0xCC, low for: 0xC8; A—2 high bits—queue for priority: 0xC4, low for: 0xC0; 00—queue 0, 01—queue 1, 10—queue 2, 11—queue 3	
tag_remap_mask0..5	Remap 802.1p priorities for untagged packets	0xHGFEDCBA, where H corresponds to packets with priority 7, A—with priority 0 A-H—assigned priority, permitted value range 0-7
prio0..5	802.1p priority assigned to untagged packets, received by this port and sent as tagged form the egress port	0-7
qos_mode0..5	QoS operation modes	0—distribute packets into queues based on IP diffserv priority only 1—distribute packets into queues based on 802.1p priority only 2—distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, IP diffserv priority is used for queuing purposes 3—distribute packets into queues based on IP diffserv and 802.1p priorities, if both priorities are present in the packet, 802.1p priority is used for queuing purposes
ingress_limit_mode0..5	Restriction mode for traffic coming to the port	0—no restriction 1-restrict all traffic

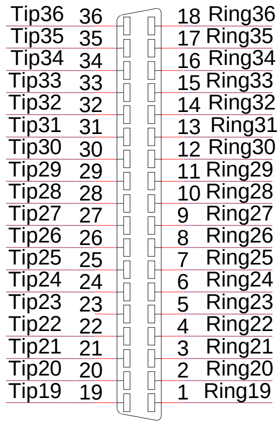
		2—multicast, broadcast, and flooded unicast traffic will be restricted 3—multicast and broadcast traffic will be restricted 4—only broadcast traffic will be restricted
ingress_rate0..5	Bandwidth restriction for traffic incoming to port 0-5 for queue 0, kbps	70-250000
ingress_mask0..5	Bandwidth restriction for traffic incoming to port 0-5 for queues 1-3, kbps rate0—band for queue 0 rate1—band for queue 1 rate2—band for queue 2 rate3—band for queue 3	0x0 – rate3= rate2= rate1= rate0 0x1 – rate3= rate2= rate1=2*rate0 0x2 – rate1= rate0, rate3= rate2=2*rate1 0x3 – rate1=2*rate0, rate3= rate2=2*rate1 0x4 – rate2= rate1=rate0, rate3=2*rate2 0x5 – rate2=rate1=2*rate0, rate3= =2*rate2 0x6 – rate1= rate0, rate2=2*rate1, rate3=2*rate2 0x7 – rate1=2*rate0, rate2=2*rate1, rate3=2*rate2
egress_rate0..5	Bandwidth restriction for traffic outgoing from the port, kbps	70-250000

APPENDIX A. TAU-72.IP/TAU-36.IP VoIP GATEWAYS CONTACT PIN ASSIGNMENT

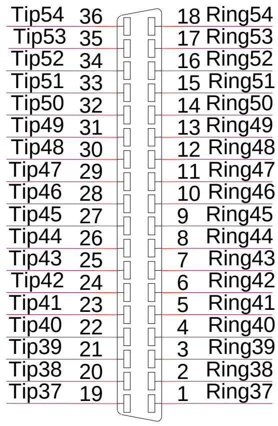
01...18



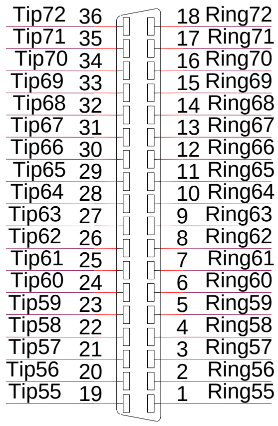
19...36



37...54



55...72



Ring[X] and Tip[X] contacts are designed for the phone unit connection.

Wire colour and terminal contact correspondence table (NENSHI NSPC-7019-18 cable)

Wire color	Connector contact	Wire color	Connector contact
White-blue	1	**Black-blue**	10
Blue	19	Blue	28
White-orange	2	**Black-orange**	11
Orange	20	Orange	29
White-green	3	**Black-green**	12
Green	21	Green	30
White-brown	4	**Black-brown**	13
Brown	22	Brown	31
Purple	5	**Yellow-blue**	14
Grey	23	Blue	32
Red-blue	6	**Yellow-orange**	15
Blue	24	Orange	33
Red-orange	7	**Yellow-green**	16
Orange	25	Green	34
Red-green	8	**Yellow-brown**	17
Green	26	Brown	35
Red-brown	9	**Yellow-grey**	18
Brown	27	Grey	36

Wire colour and terminal contact correspondence table (HANDIAN UTP 18PR cable)

Wire color	Connector contact	Wire color	Connector contact
White-blue	1	**Red-grey**	10
Blue	19	Grey	28
White-orange	2	**Black-blue**	11
Orange	20	Blue	29
White-green	3	**Black-orange**	12
Green	21	Orange	30
White-brown	4	**Black-green**	13
Brown	22	Green	31
Purple-grey	5	**Black-brown**	14
Grey	23	Brown	32
Red-blue	6	**Black-grey**	15
Blue	24	Grey	33
Red-orange	7	**Yellow-blue**	16
Orange	25	Blue	34
Red-green	8	**Yellow-orange**	17
Green	26	Orange	35
Red-brown	9	**Yellow-green**	18
Brown	27	Green	36

APPENDIX B. ALTERNATIVE FIRMWARE UPDATE METHOD

When you cannot update the firmware via web interface or CLI (telnet, RS-232), you may use an alternative firmware update method via console (RS-232).

To update the device firmware, you will need the following programs:

- Terminal program (for example: TERATERM);
- TFTP server program.

Firmware update procedure:

1 Connect to Ethernet port of the device;
2 Connect PC console port to the device console port using a crossed cable;
3 Run the terminal application;
4 Configure data rate: 115200, data format: 8bit w/o parity, 1 stop bit, w/o flow control;
5 Run TFTP server program and specify the path to 'chagall' folder. In this folder, create '300' subfolder, and place firmware.elf, initrd.300, zImage.300 in it (computer that runs TFTP server and the device should be located in a single network);
6 Turn the device on and stop the startup sequence by entering *stop* command in the terminal program window:

```
U-Boot 1.1.6 (Nov 13 2008 - 16:24:39) Mindspeed 0.06.2-candidate1

DRAM:  128 MB
Comcerto Flash Subsystem Initialization
found am29gl512 flash at B8000000
Flash: 64 MB
NAND:  64 MiB
In:    serial
Out:   serial
Err:   serial
Reserve MSP memory
Net:   comcerto_gemac0: config phy 0, speed 1000, duplex full
comcerto_gemac1: config phy 1, speed 1000, duplex full
comcerto_gemac0, comcerto_gemac1
Write 'stop' to stop autoboot (3 sec)..
FXS-72>>
```

7 Enter *set ipaddr* {device ip address} <ENTER>;
Example: set ipaddr 192.168.16.112
8 Enter *set netmask* {device network mask} <ENTER>;
Example: set netmask 255.255.255.0
9 Enter *set serverip* {IP address of a computer, that runs TFTP server} <ENTER>;
Example: set serverip 192.168.16.44
10 To activate the network interface, execute *mii i* <ENTER> command;
11 To update linux kernel, use *run updatecsp* command:

```
FXS-72>> run updatecsp
Using comcerto_gemac0 device
TFTP from server 192.168.16.44; our IP address is 192.168.16.112
Filename 'chagall/300/zImage.300'.
Load address: 0x1000000
Loading: #################################################################
         #################################################################
         #################################################################
         ##########################
done
```

```
Bytes transferred = 1130944 (1141c0 hex)
Erase Flash Sectors 11-23 in Bank # 2
Erasing 13 sectors... ......ok
Copy to Flash... ................ok
done
FXS-72>>
```

12 To update the media processor firmware, use *run updatemsp* command:

```
FXS-72>> run updatemsp
Using comcerto_gemac0 device
TFTP from server 192.168.16.44; our IP address is 192.168.16.112
Filename 'chagall/300/firmware.elf'.
Load address: 0x1000000
Loading: #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #############################
done
Bytes transferred = 1809497 (1b9c59 hex)
Erase Flash Sectors 24-55 in Bank # 2
Erasing 32 sectors... ................ok
Copy to Flash... ..........................ok
done
FXS-72>>
```

13 To update the file system, use *run updatefs* command:

```
FXS-72>> run updatefs
Using comcerto_gemac0 device
TFTP from server 192.168.16.44; our IP address is 192.168.16.112
Filename 'chagall/300/initrd.300'.
Load address: 0x1000000
Loading: #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         #################################################################
         ####################
done
Bytes transferred = 3759224 (395c78 hex)
Erase Flash Sectors 56-183 in Bank # 2
Erasing                            128                              sectors...
        ..................................................ok
Copy to Flash... .....................................................ok
done
FXS-72>>
```

14 Start up the device using *'run bootcmd'* command.

APPENDIX C. GENERAL DEVICE SETUP/CONFIGURATION PROCEDURE

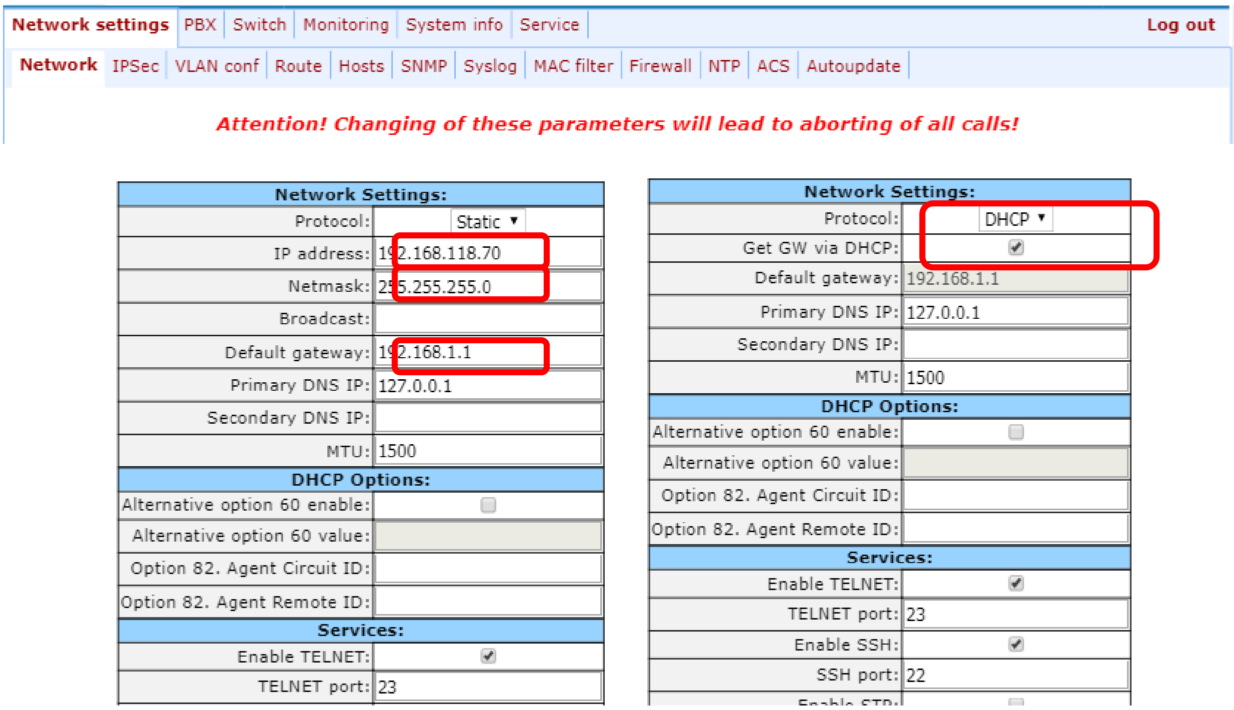
1. Using Ethernet cable, connect gateway Ethernet port to your local area network;

2. Device configuration is performed via WEB interface (see Paragraph 5.1 of this manual) using a web browser (e.g. Internet Explorer, Mozilla Firefox, Opera, Google Chrome). Initial connection to the gateway is performed by IP address, specified by the manufacturer (see documentation).

– In WEB configurator, specify the following settings in *'Network settings -> Network'* menu section:

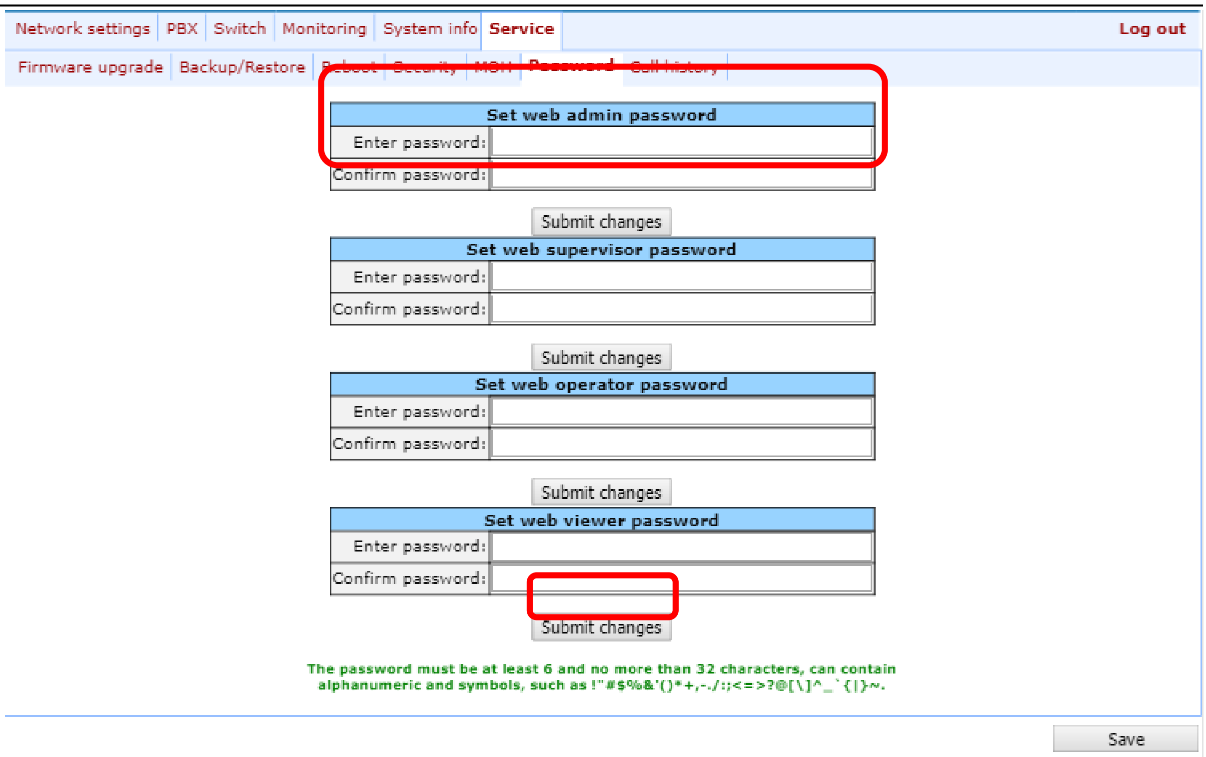
  - Device IP address corresponding to the established addressing in your network—*'IP address'* field;
  - Subnet mask—*'Netmask'* field;
  - Network gateway address—*'Default gateway'*.

– Or you can use TAU-36/72.IP as a DHCP server client in order to obtain IP address automatically: in *'Network settings -> Network'* menu section, select *'Use DHCP'* checkbox, and set the flag *'Get GW via DHCP'*.

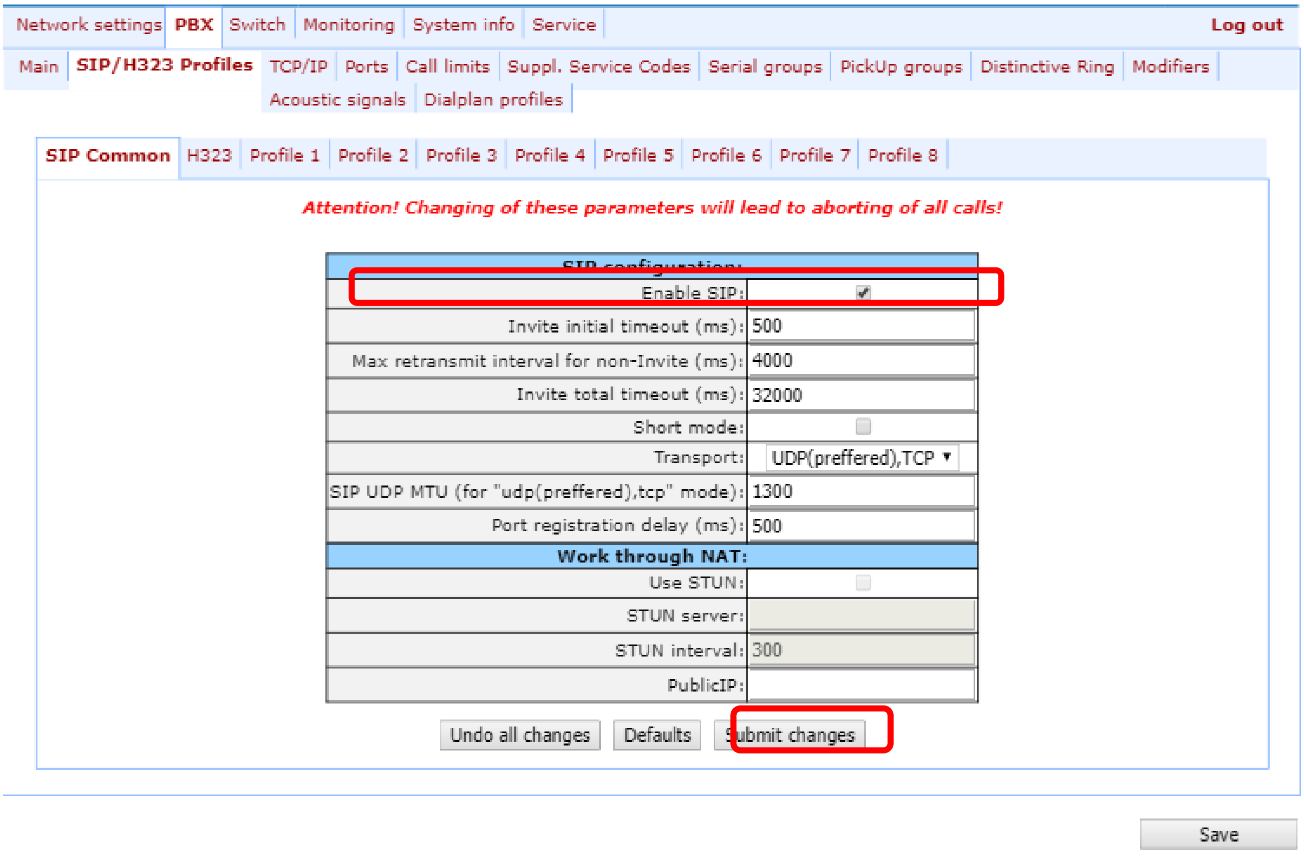


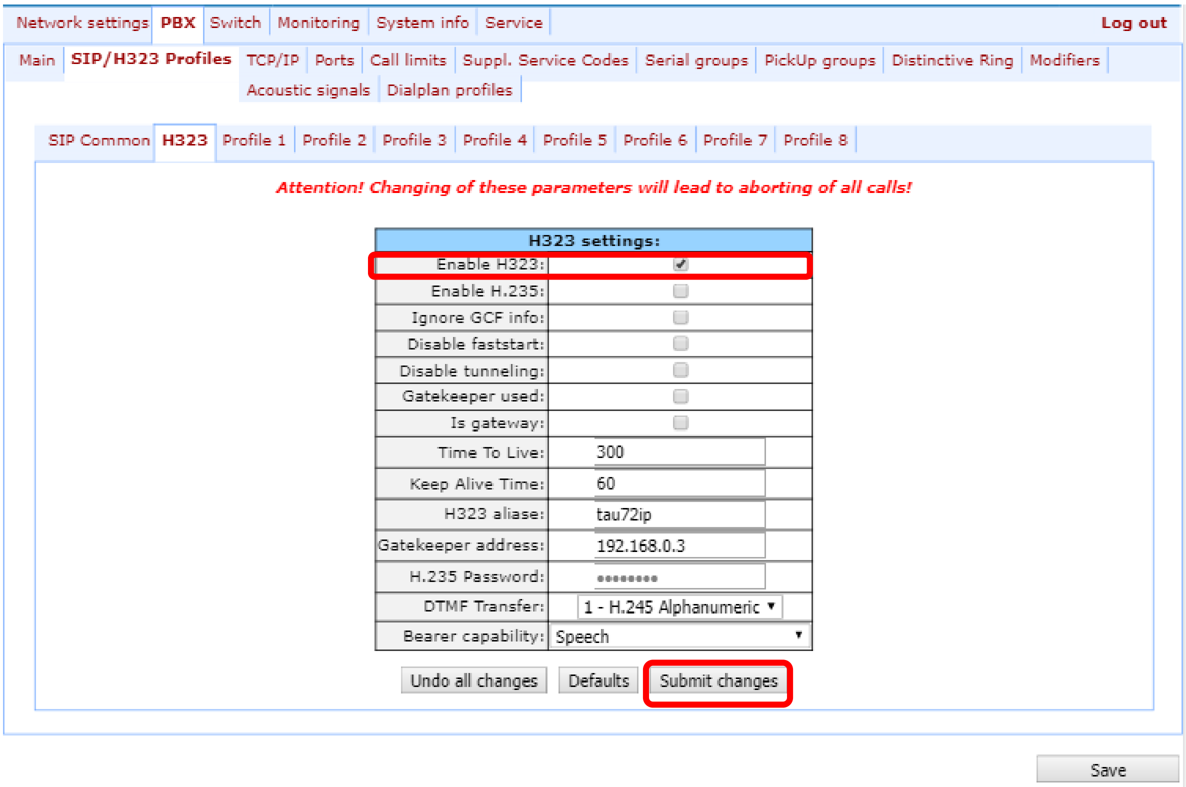
Make sure to apply changes with 'Submit Changes' button, located in the bottom of the page.

3. We highly recommend changing default password after device installation in *'Service ->Password'* menu section;

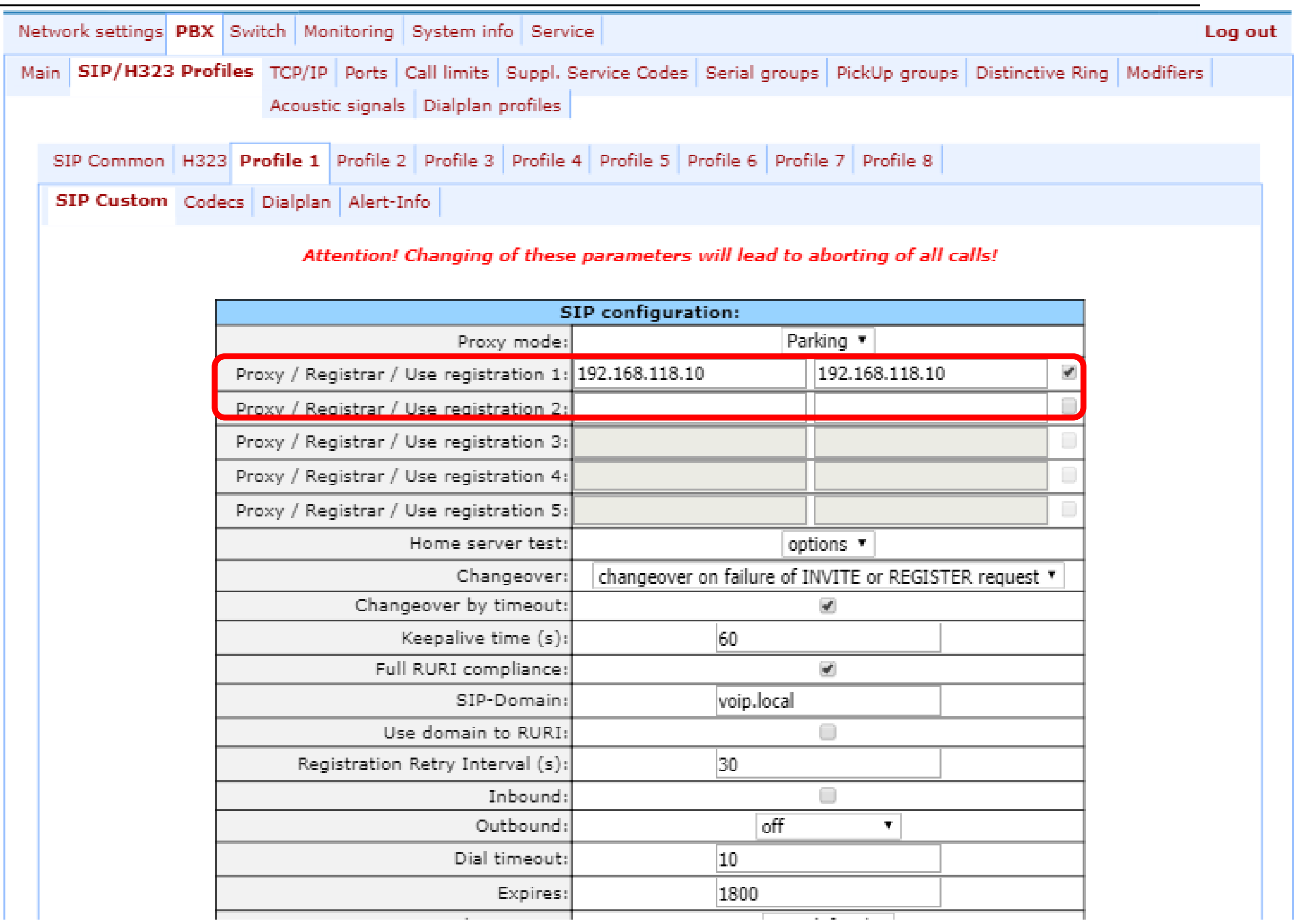


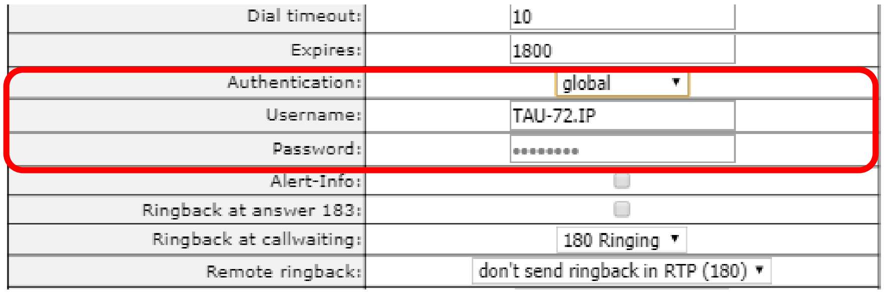
4. When the respective protocol *(SIP/H.323)* is used in *'PBX -> SIP/H323 Profiles -> SIP Common'* and *'PBX -> SIP/H323 Profiles -> H323'* menu sections, you should activate operation via these protocols by selecting *'Enable SIP', 'Enable H323'*;





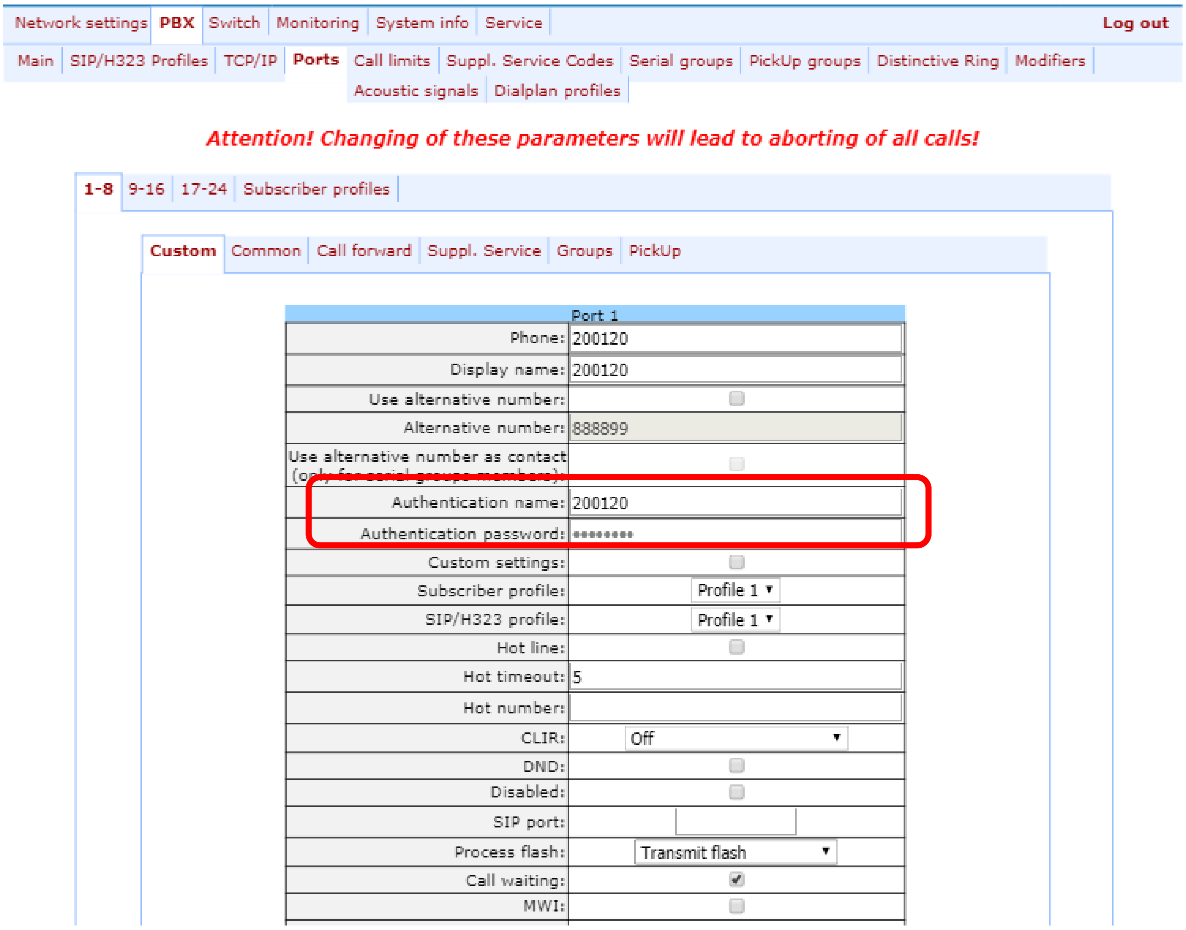
5. During SIP protocol operations (PBX -> SIP/H323 Profiles -> Profile ***n***), you have to configure SIP/H323 profile (by default, Profile 1 is defined for all subscriber ports). You may use up to 8 different profiles.



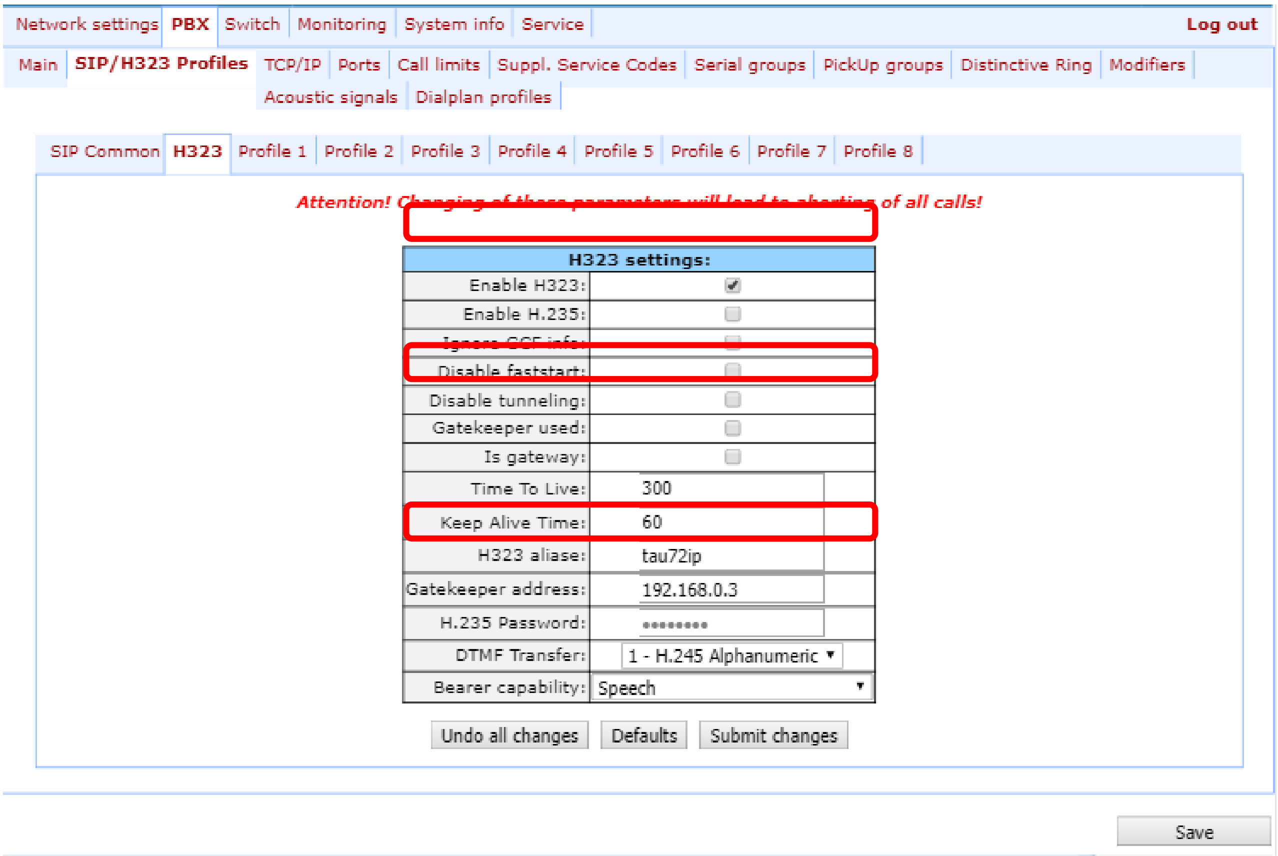


6. To be able to register device ports on the registration server, you should check *Use registrar* (in *'PBX/SIP-h232 profiles/Profile N/SIP profile settings*' menu) and define the SIP proxy server address in *'Proxy'* field, and registration server address in *'Registrar'* field. As a rule, a single device is used as a SIP proxy and registration server;

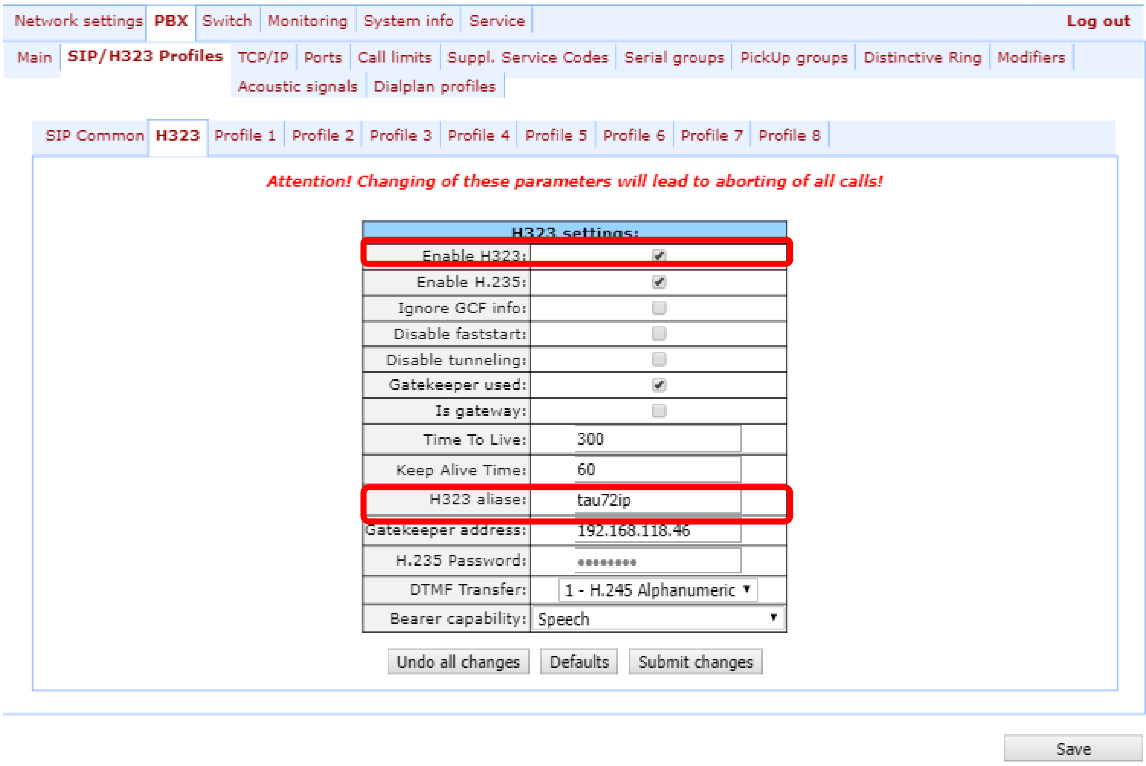
7. To enable port authorization, you should set the following value for *'Authentication'* parameter: *'global'* or *'user defined'* in 'PBX/SIP-h232 profiles/Profile ***N****/SIP profile settings'* menu. When *'global'* value is used, all ports will be authorized with the same name and password; in this case, authorization global name and password should be specified in *'Username'* and *'Password'* fields respectively in 'PBX/SIP-h232 profiles/Profile ***N****/SIP profile settings'* menu. When *'user defined'* value is used, each port will be authorized with its own name and password, in this case authorization name and password should be specified in *'PBX -> Ports -> Edit -> Custom'* section, *'Authentication name'* and 'Authentication password' fields respectively;



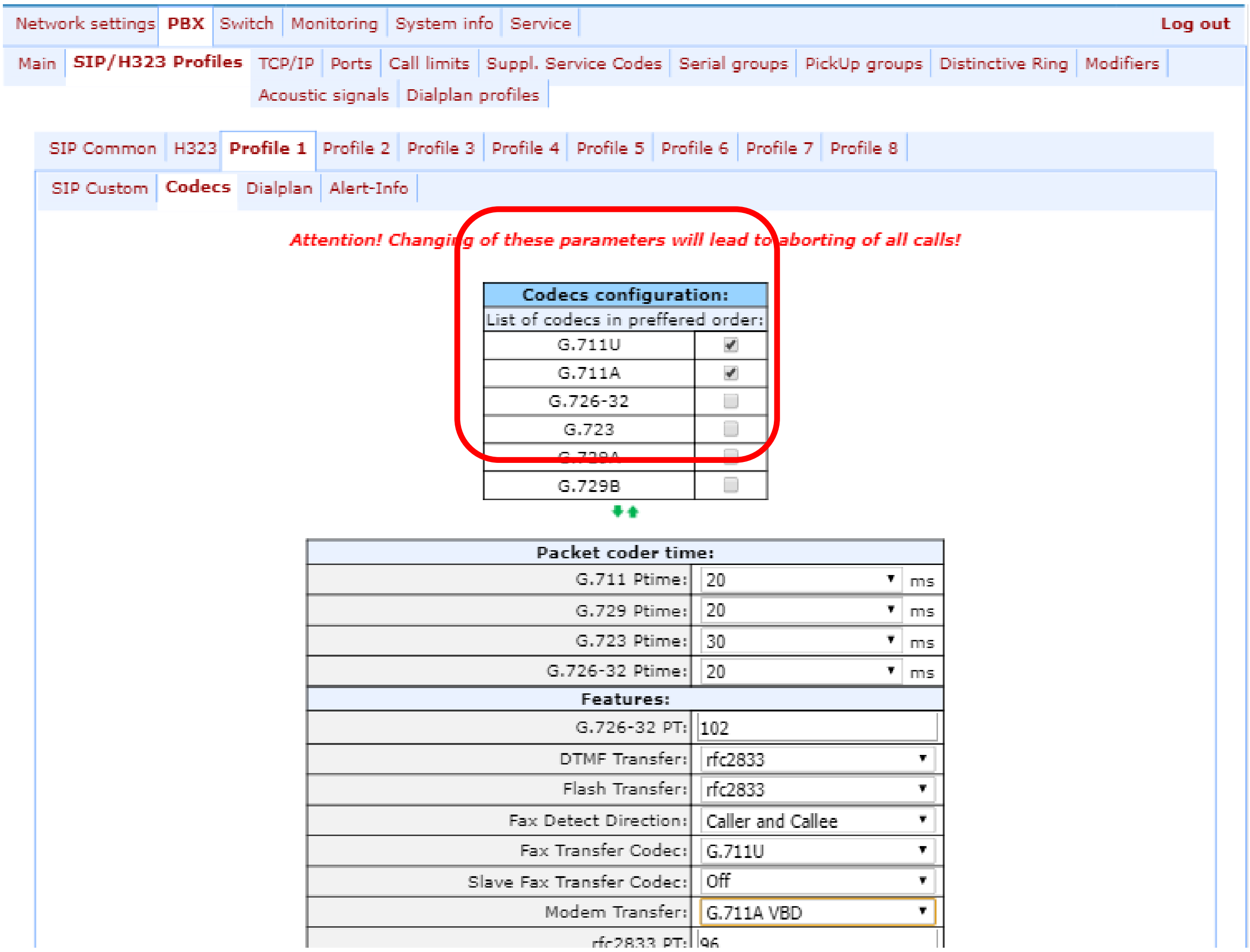
8. When gateway operates through the Gatekeeper via H.323 protocol, in *'PBX -> SIP/H323 Profiles -> H.323'* menu section, select the *'Gatekeeper used'* checkbox and define IP address in *'GateKeeper address' field.* H.323 protocol operation is possible only in Profile 1.



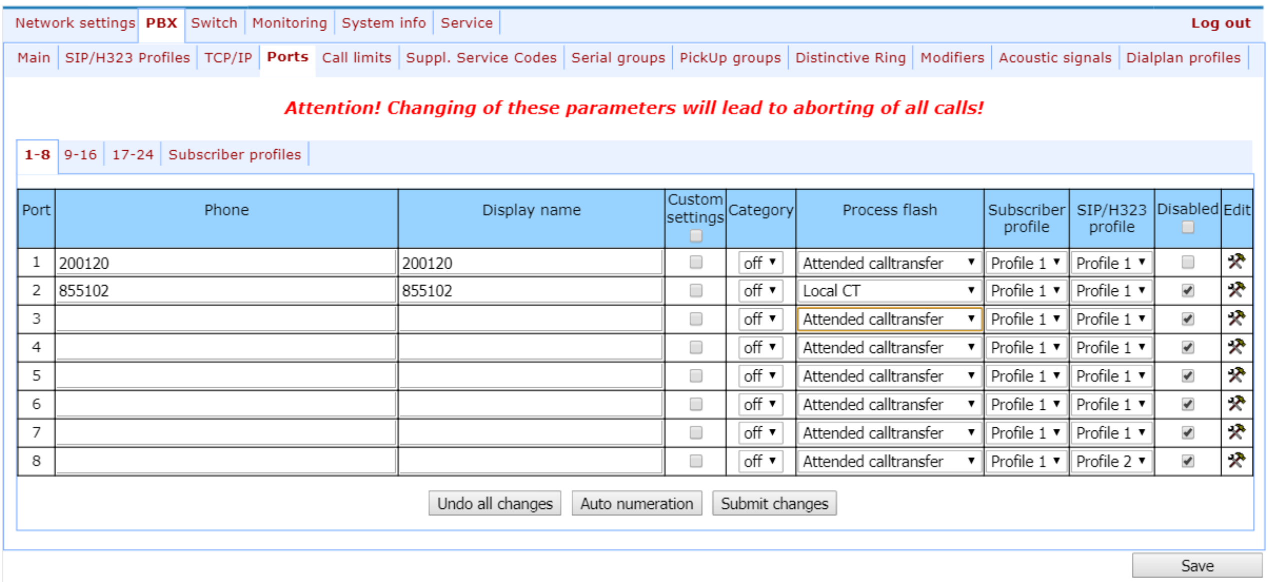
9. To enable device authorization on the Gatekeeper via H.235 protocol, in *'PBX -> SIP/H323 Profiles -> H.323'* menu section, select the *'Enable H.235'* checkbox and specify the name and password in *'H.323 aliase'* and *'H.235 Password'* fields respectively.



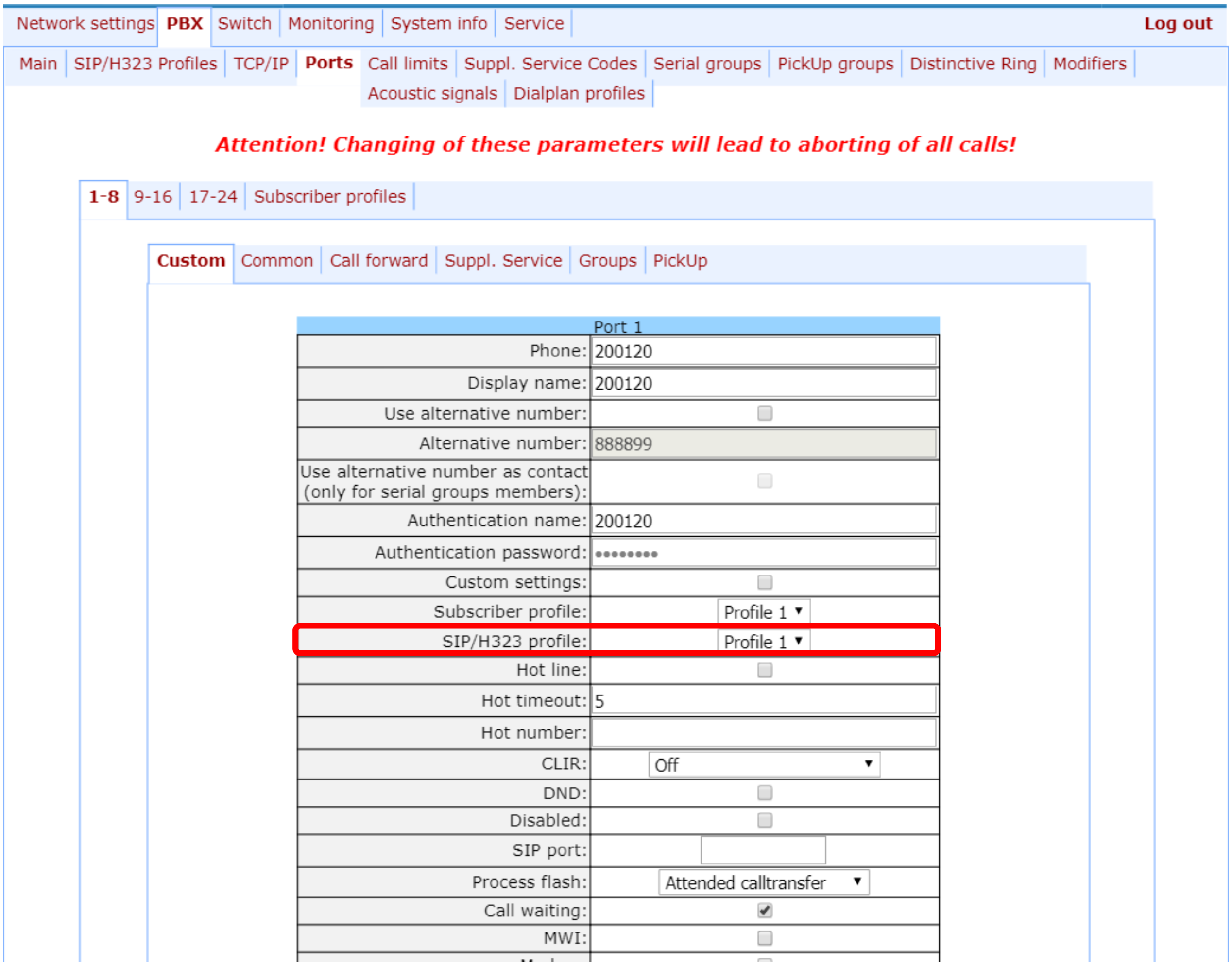
10. In *'PBX -> SIP/H323 Profiles -> Profile n -> Codecs'* section, select utilized codecs and define their selection priority. **During H.323 protocol operation, all settings should be configured in Profile 1;**



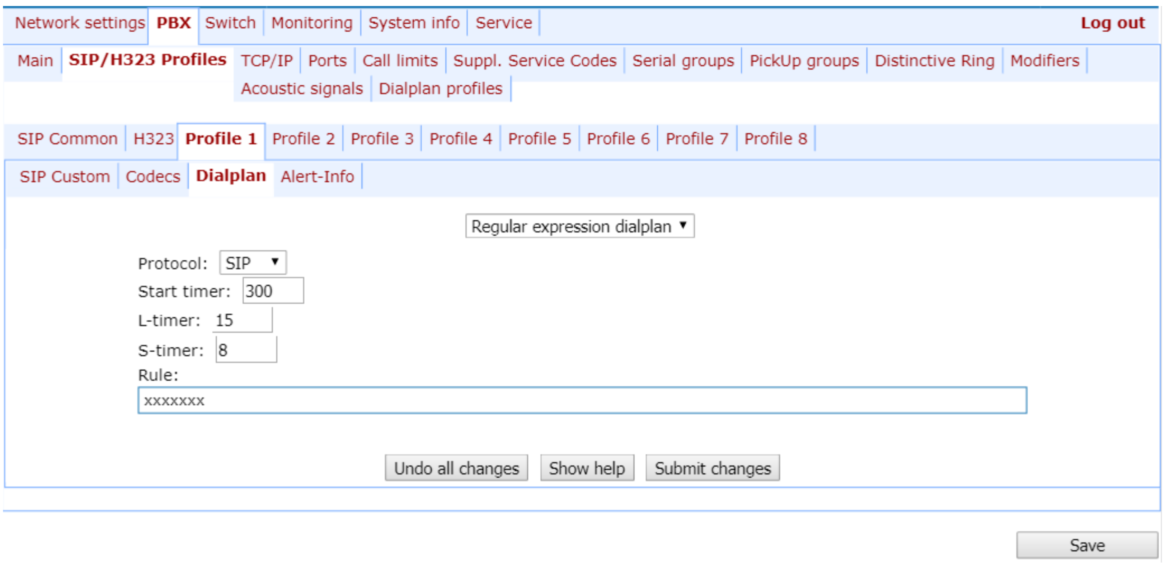
11. In *'PBX -> Ports'* section, assign phone numbers to device ports;



12. In subscriber port settings ('PBX -> Ports -> Edit -> Custom'), specify an active SIP profile number in *'SIP/H323 profile'* (by default, Profile 1 is defined for all subscriber ports);



13. Configure addressed dial peers (*'PBX -> SIP/H323 Profiles -> Profile n -> Dialplan'* menu section). During H.323 protocol operation, all settings should be configured in Profile 1;



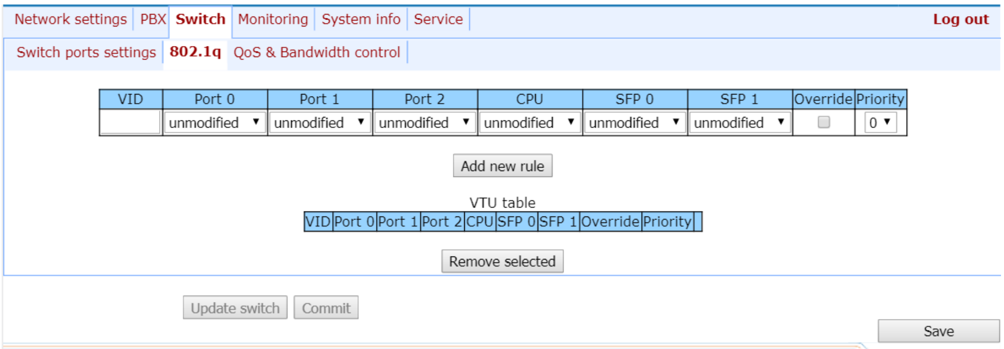
14. When basic parameters are configured, click *'Save'* button to save changes into the non-volatile memory of the device.

APPENDIX D. EXAMPLE OF SWITCH CONFIGURATION USING VLAN

Objective: Tagged traffic comes to the switch port 0 with the following tags: 101, 102 and 103. Packets with VLAN ID=101 should be sent untagged to the port 1, packets with VLAN ID=102 should be sent untagged to the port 2. VLAN 103 is proposed to be used for telephony and device management, i.e. packets with VLAN ID=103 should be sent untagged to the switch CPU port.

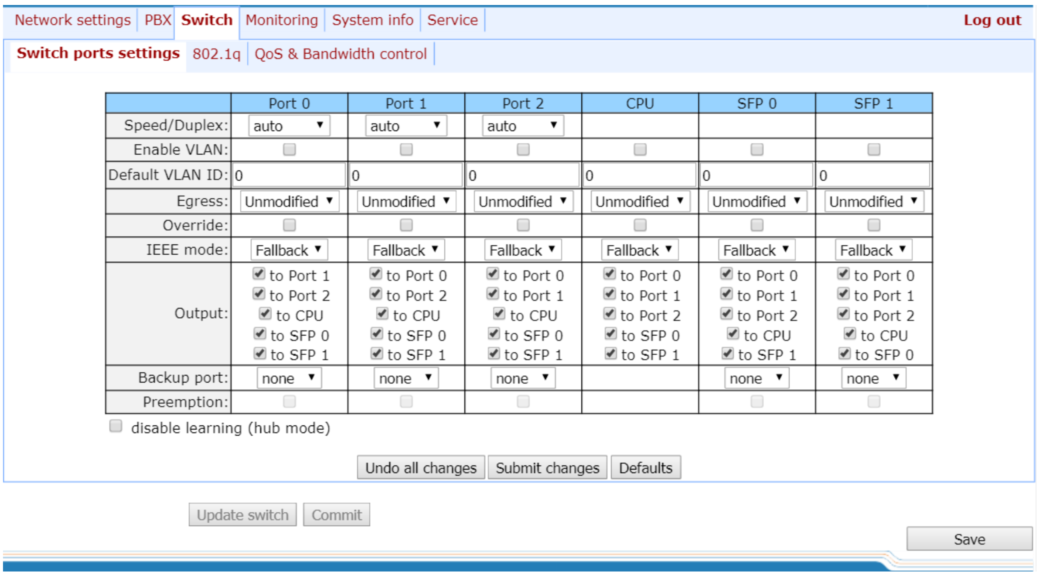
1. Using Ethernet cable, connect gateway Ethernet port to your local area network. Connect to the device using WEB configurator.

2. Define the packet routing rules—*'802.1q'*—in *'Switch -> 802.1q'* submenu.



- For VLAN 101, port 0 is tagged, port 1 is untagged, other ports are not members of this VLAN.
- For VLAN 102, port 0 is tagged, port 2 is untagged, other ports are not members of this VLAN.
- For VLAN 103, port 0 is tagged, CPU port is untagged, other ports are not members of this VLAN.

3. For switch ports, you should configure '802.1q' operation mode in 'Switch -> Switch ports settings' submenu, i.e. 'IEEE Mode = Secure'. For untagged traffic coming to ports 1, 2 and CPU to be transferred to port 0 tagged, you should configure the respective *'Default VLAN ID'* tags—101, 102 and 103—for ports 1, 2 and CPU. Also, select 'Enable VLAN' checkboxes for these ports, including port 0, that allow to use *'Default VLAN ID'* settings.



4. Click *'Update switch'* button to apply settings, connect to the device using 103 VLAN and confirm applied settings with *'Commit'* button.

5. After that, modified switch settings could be saved in the non-volatile memory with *'Save'* button.

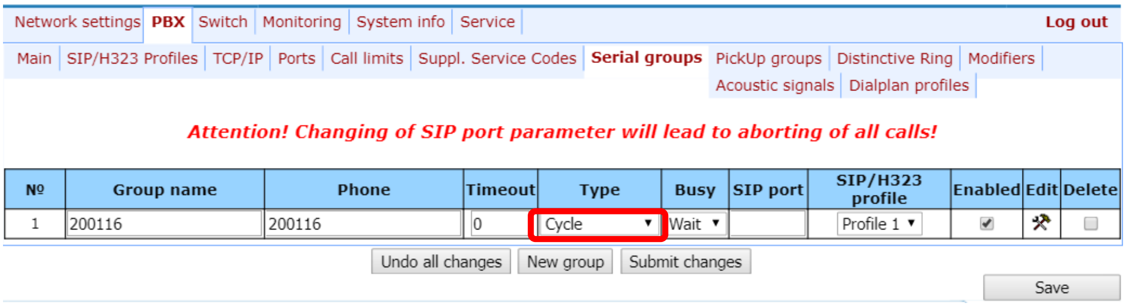
APPENDIX E. EXAMPLE OF PBX CONFIGURATION ON TAU-72.IP/TAU-36.IP

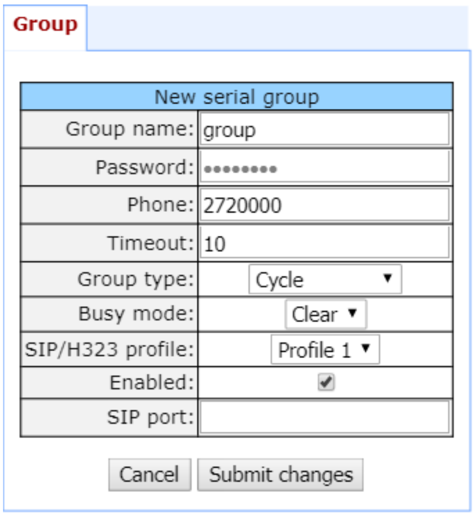
Objective: To build PBX for 4 subscriber numbers. A single number is allocated to PBX by a local exchange network—272xxxx. When a call comes to this number, it should be transferred to all four PABX subscriber ports in turns. Ringing time for each number is 10 seconds.

Solution:

1. Using Ethernet cable, connect gateway Ethernet port to your local area network. Connect to the device using WEB configurator.

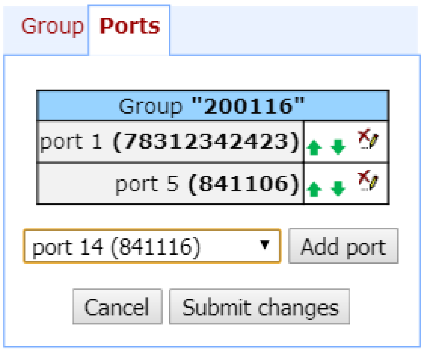
2. Usually, during the call group creation process at SIP server, only a single login/password is issued for multiple lines. At the gateway, you should create a cycle call group with 10 seconds timeout; to do this, click *'New group'* button in *'PBX -> Serial groups'* tab and fill in the required fields:



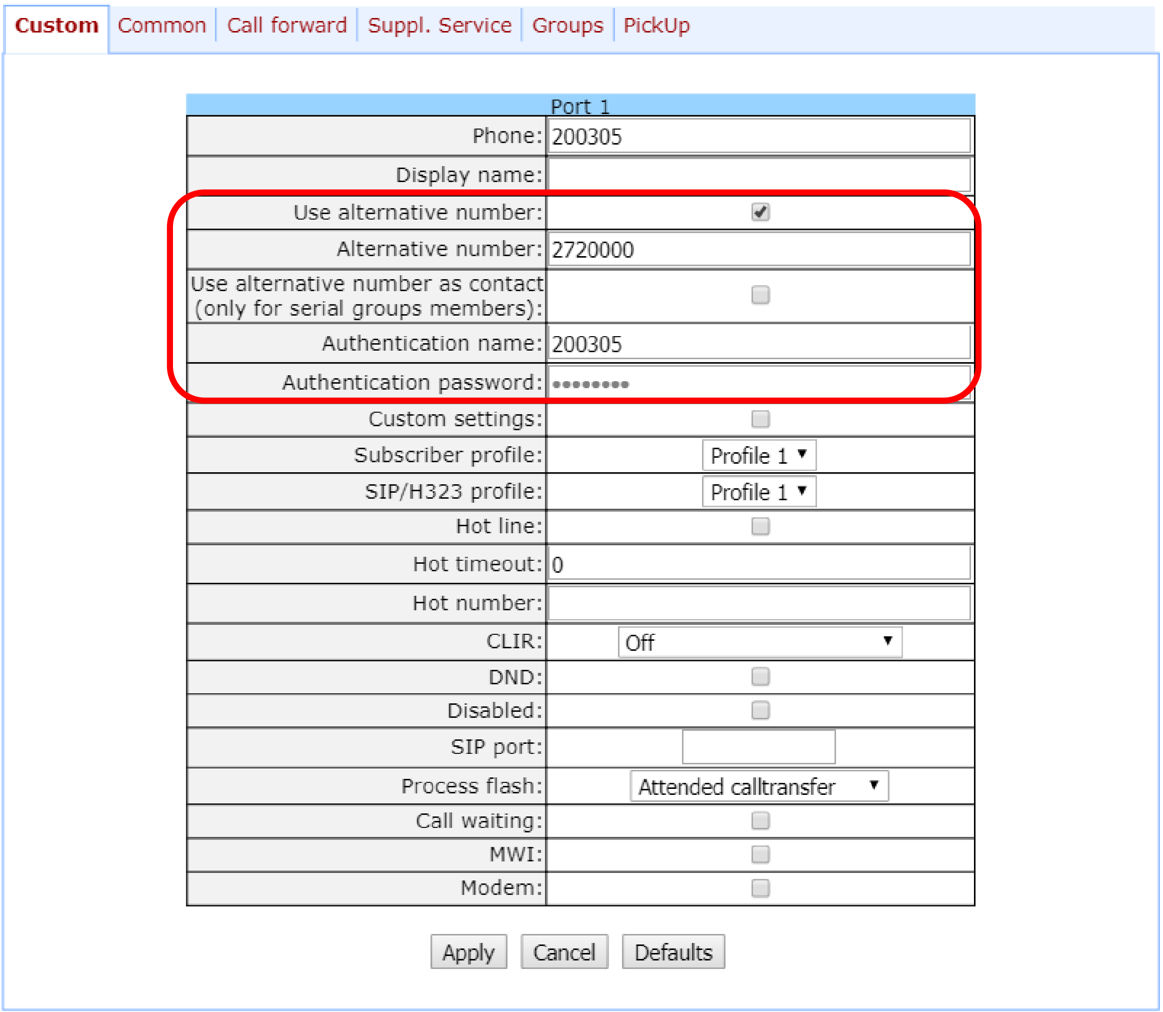


In group settings, specify login/password for registration on SIP server and assign the number allocated by a local exchange network (272xxxx) as a group number. Define SIP/H.323 profile for call group operation.

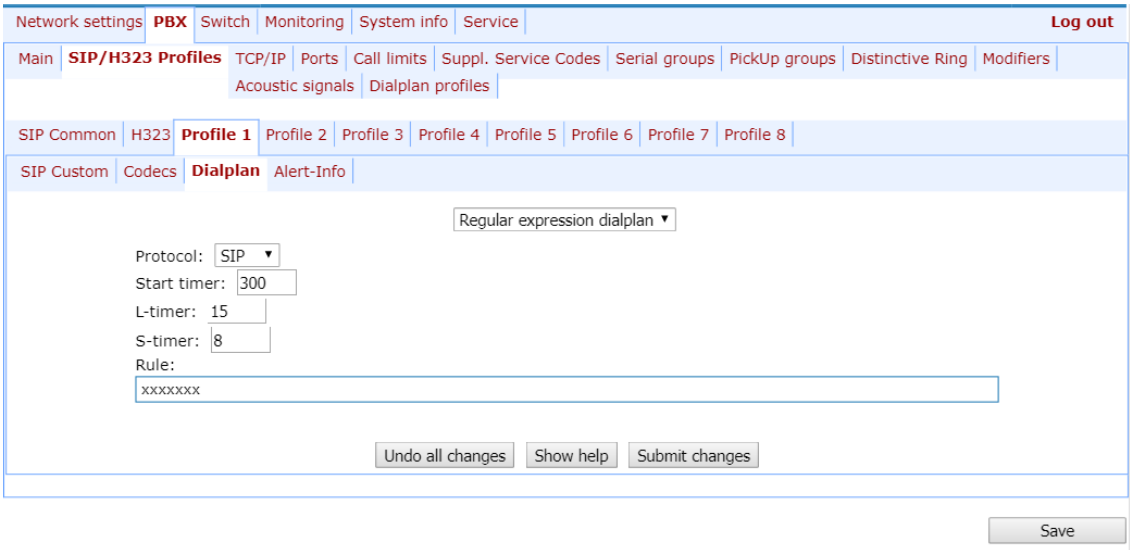
3. In group port settings ('*PBX -> Serial groups -> Edit*'), add ports into a call group (see Section 5.1.2.7 The '*Serial groups'* submenu).



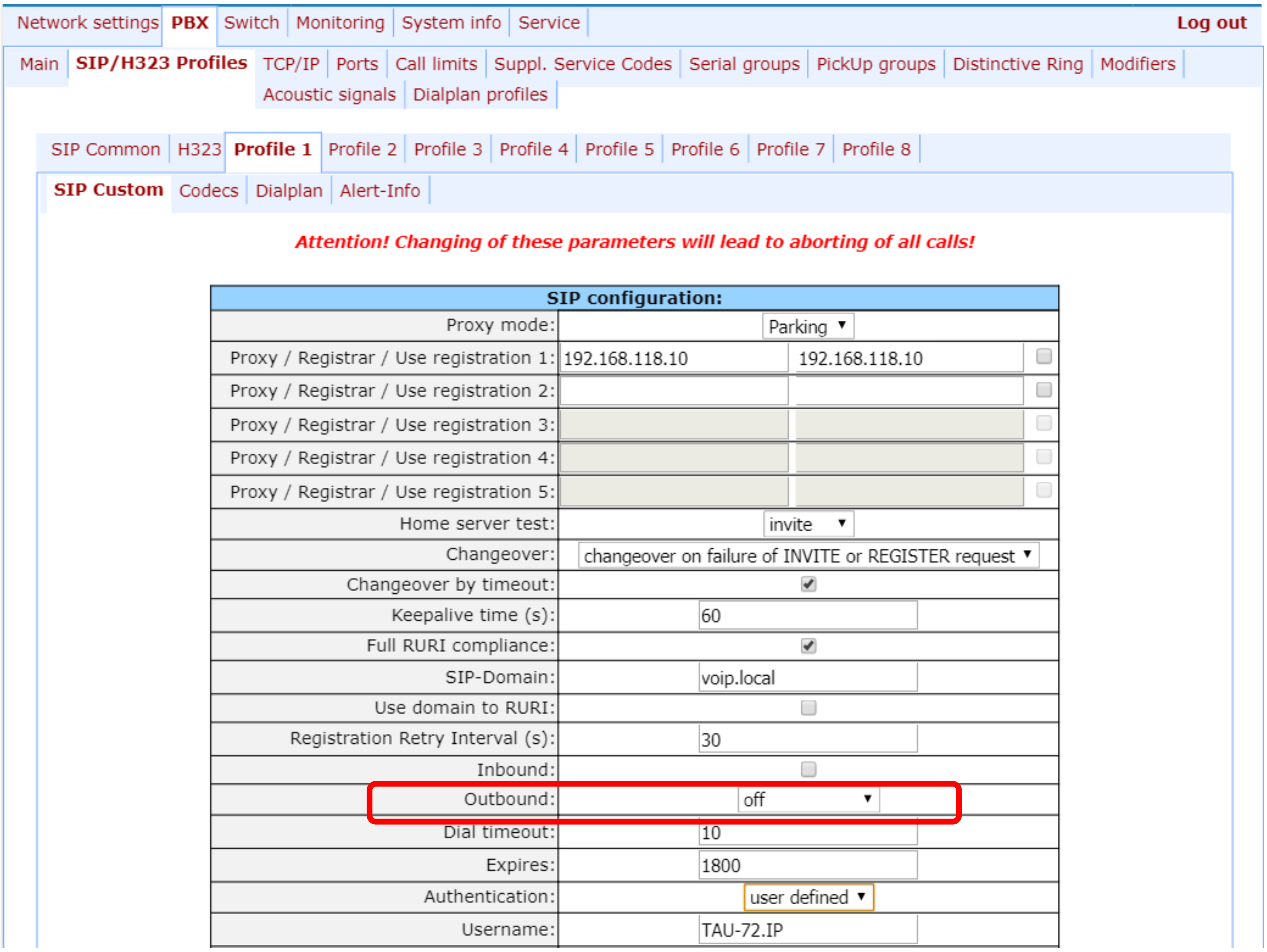
4. In subscriber port settings—'*PBX -> PORTS -> Edit -> Custom*' tab, define the internal subscriber dialplan. Given that during outgoing calls a number 272xxxx should be transferred as a Caller ID, you should configure an alternative Caller ID. Enumeration is defined by the '*Phone*' parameter in the port settings, and an alternative Caller ID is configured by selecting '*Use alt.number*' checkbox and specifying an external number in '*Alt.number*' field. Also, in port settings, define login/password for authentication on SIP server.



5. For outgoing calls routing, configure addressed dial peers in the respective SIP/H.323 profile (*'PBX -> SIP-H323 Profiles -> Profile n -> Dialplan'* menu section).



6. Or you may use the *outbound* mode (configured in *'PBX -> SIP/H323 Profiles -> Profile n -> SIP Custom'* section); in this case, all outgoing calls will be routed via SIP-proxy.



APPENDIX F. CALCULATION OF PHONE LINE LENGTH

Electrical resistance/cable type relationship for 1km of DC subscriber cable lines.

Cable grade for subscriber lines of local exchange network	Core diameter	Electrical resistance of 1km circuit, Ω, max.	Line length, km	
			Standard TA	TA RUS Rfull.max=2600Ω
TPP, TPPep, TPPZ, TPPepZ, TPPB,TPP epB, TPPZB, TPPBG, TPPepBG, TPPBbShp, TPPepBbShp, TPPZBbShp, TPPZepBbShp, TPPt	0.32	458.0	3.056	2.183
	0.40	296.0	4.729	3.378
	0.50	192.0	7.291	5.208
	0.64	116.0	12.068	8.621
	0.70	96.0	14.583	10.417
TPV, TPZBG	0.32	458.0	3.056	2.183
	0.40	296.0	4.729	3.378
	0.50	192.0	7.291	5.208
	0.64	116.0	12.068	8.621
	0.70	96.0	14.583	10.417
TG, TB, TBG, TK	0.40	296.0	4.729	3.378
	0.50	192.0	7.291	5.208
	0.64	116.0	12.068	8.621
	0.70	96.0	14.583	10.417
TStShp, TAShp	0.50	192.0	7.291	5.208
	0.70	96.0	14.583	10.417
TSV	0.40	296.0	4.729	3.378
	0.50	192.0	7.291	5.208
KSPZP	0.64	116.0	12.068	8.621
KSPP, KSPZP, KSPPB, KSPZPB, KSPPt, KSPZPt, KSPZPK	0.90	56.8	24.647	17.606

Phone line length calculation for different types of cable[1]:

1. Cable resistance at 20°C:

$$R_{Cab} = L_{Cab} \cdot R_{Sp20} (Ohm/km)$$

where:

R_{Sp20} [Ω/km] -specific DC cable resistance at 20°C (table value).

Cable length:

$$L_{Cab} = \frac{R_{Cab}}{R_{Sp20}} (km)$$

2. Loop length is twice:

$$L_{Loop} = 2 \cdot L_{Cab}$$

3. Loop resistance at 20°C

[1] Values from http://izmer-ls.ru/shle.html

$$R_{Loop} = L_{Loop} \cdot R_{Sp20} = 2 \cdot L_{Cab} \cdot R_{Sp20}$$

Loop length is: $L_{Loop} = \dfrac{R_{Loop}}{R_{Sp20}} (km)$

4. In case of phone lines, loop resistance includes phone unit resistance: 600Ω
   Equipment manufactured by Eltex provides maximum loop resistance of 3400Ω.
   Subsequently, loop resistance excluding the phone unit equals to 2800Ω.
   Thus, maximum loop length is calculated by the equation

   $$L_{Loop} = \frac{2800}{R_{Sp20}} (km)$$

   Line length is calculated by the equation:

   $$L_{Line} = L_{Cab} = \frac{L_{Loop}}{2} = \frac{2800}{2 \cdot R_{Sp20}} = \frac{1400}{R_{Sp20}} (km)$$

5. If you have to consider the cable temperature, the cable line length will be calculated with an adjustment:

   $$L_{Line} = \frac{1400}{R_{Sp20} \cdot (1 - a(T - 20))} (km)$$

where:

a is a temperature factor (table value);
T-cable temperature.

APPENDIX G. AUTOMATIC CONFIGURATION PROCEDURE AND GATEWEY FIRMWARE VERSION CHECK

1. Configuration parameters usage

'Enable autoupdate' is an option that allows to use automatic software and configuration updates, and perform their version checks in the defined periods of time.

AU-72.IP/TAU-36.IP automatic configuration and configuration file version check operation algorithm.

For each TAU-72.IP/TAU-36.IP, a reference configuration file is created; The archive contains cfg.yaml file, which can be edited. In /etc/config/cfg.yaml configuration file, specify its current version #ConfigFileVersion=YYYYMMDDHHMM:

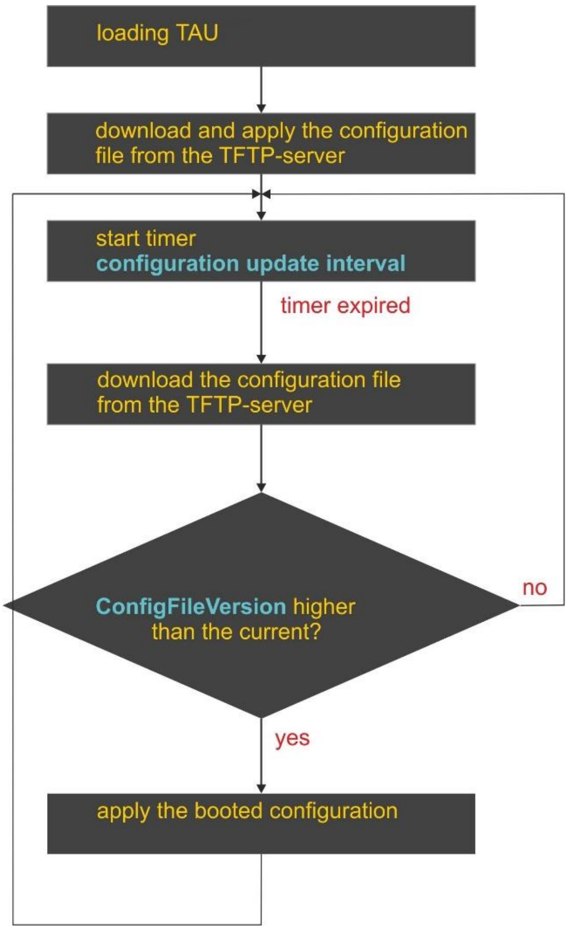
After configuration, you need to upnload the archive, not the cfg.yaml file.

```
#!version 1.0
#tau-72 YAML config file
#Tree hierarchy:
#node1:
#       node2:
#               param1: value1
#               param2: value2
#NOTE: use spaces ' ' instead of tab '/t'
#NOTE: Don't del/add nodes
#NOTE: Use ':' after param names
#Remember, that quantity of spaces must be multiply to 8

#ConfigFileVersion=201302010905

Network:
        network:
                HOSTNAME: tau72
```

During TAU-72.IP/TAU-36.IP startup, the gateway checks for the configuration file at the specified path on FTP/TFTP/HTTP/HTTPS server (and signs in to server, if necessary). If the configuration file is present, TAU will download it, store it in its file system and apply it as a current configuration file. Upon the expiry of *'Configuration update interval'* timeout or when *'Configuration update time'* is coming, the gateway will re-download the configuration file from the server and compare versions of the current and downloaded configuration files (ConfigFileVersion). If the downloaded file version is higher that the current one, TAU-72.IP/TAU-36.IP saves and applies a new configuration; otherwise, the current configuration remains active.

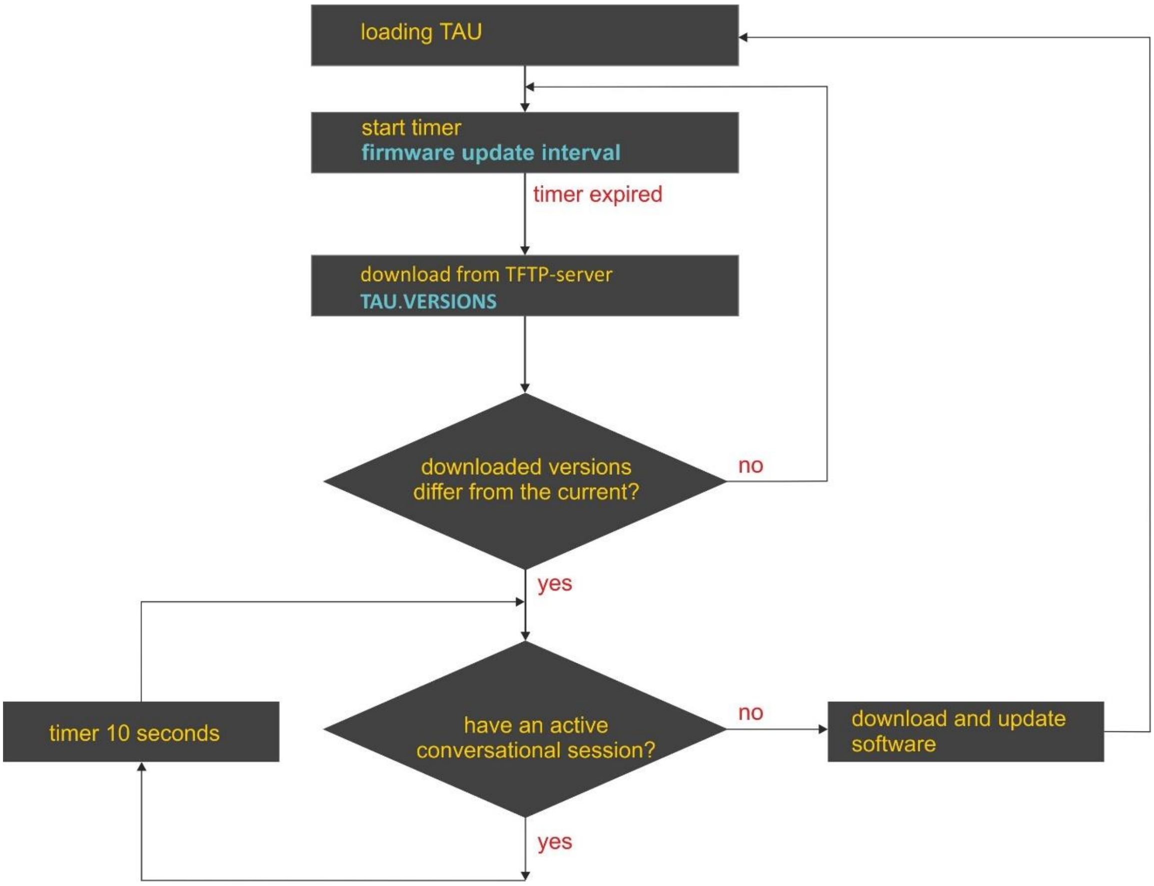
When the operator wants to modify the gateway configuration, he should upload the modified configuration file with increased 'ConfigFileVersion' value to the server, and the configuration will be updated automatically upon the expiry of *'Configuration update interval'* timeout or when *'Configuration update time'* is coming. After restart, TAU-72.IP/TAU-36.IP will download configuration file from the server; this measure will protect the gateway from improper configuration. If you experience problems after configuring the gateway via Web configurator, restart the device to download the reference configuration.

Flow chart


loading TAU
download and apply the configuration file from the TFTP-server
start timer
configuration update interval
timer expired
download the configuration file from the TFTP-server
ConfigFileVersion higher than the current?
no
yes
apply the booted configuration

2. Autoupdate and firmware version check operation algorithm

During TAU-72.IP/TAU-36.IP startup, and upon the expiry of *'Firmware update interval'* timeout or when *'Firmware update time'* is coming, the gateway checks for the version description file (tau.versions) at the specified path on TFTP server. If the configuration file is present, TAU-72.IP/TAU-36.IP will download it. This file contains information on versions of firmware files located at TFTP server as well as their paths and names. If versions of firmware located on server differ from the current ones (used by the gateway), the gateway checks for active call sessions. If there are no active call sessions, TAU-72.IP/TAU-36.IP will download firmware files with versions defined in tau.versions file. When download finishes, the gateway firmware will be updated; otherwise, 10 seconds timeout will be activated. When this timeout expires, the gateway checks again for active call sessions.



3. Automatic configuration and firmware version check: parameter obtaining methods

Method 1: Using DHCP Option 43 or Options 66 and 67 when DHCP is enabled in network settings or for one of VLANs.

Gateway default settings as follow:

Update mode	via **TFTP**
TFTP server	**update.local**
Path to file with firmware and configuration versions	**tau.versions**
Path to the configuration file	***tau72_<MAC>.dat***

tau72_<MAC>.dat-configuration file name. When such name is received, gateway substitutes ***<MAC>*** with its own MAC address.
Example: Transferred name of a configuration file is tau72_<MAC>.dat. When this name is received, the gateway generates availability request for tau72_ A8F94B887D27.dat file on TFTP server.

Configuration file is downloaded to PC via WEB interface in tau72_cfg.tar.gz format; to use it in autoconfiguration procedure, rename it to tau72_<MAC>.dat.

To edit the file on a PC, unarchive the file, modify its data and create a new archive in the same format taking into account the path to file /etc/config; next, rename it to tau72_<MAC>.dat.

If autoupdate server requires authorization, configure the following parameters: Autoupdate auth, Username, Password.

If the gateway receives Options 43, 66, and 67 from DHCP server simultaneously, Option 43 will have a priority in usage. Factory settings for automatic download of firmware and configuration files listed above will not work in this case.

Description of syntax for Option 43, 66, 67 and firmware and configuration version file: tau.versions

Option 43 syntax:

<suboption number><suboption length><suboption value>,

where:

- suboption number and length are passed in a numeric (Hex) format;
- suboption value is passed as ASCII code.

Suboptions necessary for autoupdate procedure:

- 5–autoupdate server address;
  Address should be received in the following format: **<proto>://<address>[:<port>]**,
  where
  <proto>–protocol (ftp, tftp, http, https),
  <address>–autoupdate server IP address or domain name,
  <port>–autoupdate server port (optional parameter);
- 6–autoupdate configuration file name;
- 7—autoupdate firmware file name;

Example of the option record:

```
05:11:68:74:74:70:3A:2F:2F:61:75:74:6F:2E:72:75:3A:38:30:06:09:61:75:74:6F:2E:63:6F:6E:66:07
:08:61:75:74:6F:2E:76:65:72
```

where:

05—autoupdate server address suboption number;
11—length, 17bytes (0x11 = 17 dec);
68:74:74:70:3A:2F:2F:61:75:74:6F:2E:72:75:3A:38:30—suboption value (http://auto.ru:80);
06—configuration file name suboption number;
09—length, 9bytes;
61:75:74:6F:2E:63:6F:6E:66—suboption value (auto.conf);
07—software file name suboption number;
08—length, 8bytes;
`61:75:74:6F:2E:6B:6D:67`—suboption value (auto.ver).

Option 66 syntax: TFTP server **FQDN** or **IP address**

DHCP server configuration examples:

```
Option tftp-server-name 'update.local'
Option tftp-server-name '192.168.1.3'
```

Option 67 syntax: ***'tau.versions file name and path; Configuration file name and path'***

Syntax **tau.versions file path:** ***conf-path/tau.versions***

Syntax **Configuration file path and name:** ***conf-path/tau72_<MAC>.dat***

Where ***conf-path***—configuration file path;

Example of Option 66 and 67 syntax, software file path and name, and gateway configuration for MAC address A8F94B887D27

Transferred parameters:

```
Option tftp-server-name 'update.local';
Option bootfile-name '/tau72ip/firmware/tau.versions;/tau72ip/conf/tau72_<MAC>.dat'
```

Method 2: Using autoupdate parameter configuration, specified in 'Autoupdate Settings' section, when the static address is assigned in network settings, or when PPPoE is selected.

In this case, 'Autoupdate protocol', 'Autoupdate server', 'Configuration file' and 'Firmware versions file' parameters are used, defined in 'Autoupdate Settings' section. If autoupdate server requires authorization, configure the following parameters: Autoupdate auth, Username, Password.

3.1. **tau.versions** file format and syntax

Format and syntax

FS={FSversion} firmware-pathFS/filenameFS
CSP={CSPversion} firmware-pathCSP/filenameCSP
MSP={MSPversion} firmware-pathMSP/filenameMSP
IMG={IMGversion} firmware-pathIMG/filenameIMG
ARM={ARMversion} firmware-pathARM/filenameARM

Where ***FSversion/CSPversion/MSPversion/ARMversion***—respective software version number;
firmware-pathFS,CSP,MSP,ARM—path to the respective software file;
filenameFS,CSP,MSP,ARM—name of the respective software file.

Software file types[1]*:*

- *FS*—file system with working application;
- *CSP*—gateway operating system;
- *MSP*—media processor software;
- *IMG*—complete software image, includes FS, CSP, MSP, and ARM;
- *ARM*—platform software.

Software file name format:

filenameFS – tau72.fs.{software version number}
filenameCSP – tau72.csp.{software version number}
filenameMSP – tau72.msp.{software version number}
filenameIMG – tau72.img.{software version number}
filenameARM – tau72.arm.{software version number}

tau.versions *file contents example:*

```
FS=1.8.0 fs/tau72.fs.1.8.0
CSP=209 csp/tau72.csp.209
MSP=GA_10_23_02_03 msp/tau72.msp. GA_10_23_02_03
IMG=2.1.0 tau72ip/firmware/img/tau72.img.2.1.0
ARM=20111117 arm/tau72.arm.20111117
```

[1] In current firmware version only IMG file type is supporting.

APPENDIX H. DEVICE FIREWALL CONFIGURATION-IPTABLES

Command	Description
`iptables`	Configuration of firewall rules
`iptables-save`	Save created firewall rules
`iptables-restore`	Restore initial firewall rules, if the current rules are not saved

To configure the firewall, connect to the gateway via COM port, SSH or Telnet (factory settings address: **192.168.1.2**, network mask: **255.255.255.0**) using terminal application, e.g. TERATERM, Putty, SecureCRT.

Firewall configuration procedure as follows:

1. *Configuration via COM port:*
   Connect the null modem cable to COM port of the PC and *'Console'* port of the device.
   Configuration via SSH, Telnet:
   Connect the computer to the Ethernet port of the device using Ethernet cable.

2. Run the terminal application;

3. Configure COM port connection: data rate: 115200, data format: 8bit w/o parity, 1 stop bit, w/o flow control; or telnet, ssh connection: Factory default IP address: 192.168.1.2, port: 23 (telnet), port 22 (ssh);

4. Enter `'admin'` as a login. Go to Linux shell by executing `'shell'` command.

5. Create necessary tables according to `iptables` utility manual, use `'iptables –h'` command to view the manual;

   `iptables` utility usage examples:

   a) accept TCP packets via port 25 from the host 212.164.54.162:

   ```
   iptables -A INPUT -s 212.164.54.162 -p tcp -m tcp --dport 25 -j ACCEPT
   ```

   b) reject all packets from the host 216.223.9.208:

   ```
   iptables -A INPUT -s 216.223.9.208 -j DROP
   ```

   c) reject all packets from the network 216.223.0.0/255.255.0.0:

   ```
   iptables -A INPUT -s 216.223.0.0/255.255.0.0 -j DROP
   ```

   d) view all tables:

   ```
   iptables -L
   ```

6. Save created rules with `'iptables-save'`.

To restore previous rules, if changes have not been saved yet, use 'Iptables-restore' command.

7. Enter `'save'` command to store the configuration into the non-volatile (flash) memory of the device.

APPENDIX J. PROCESSING OF INFO REQUESTS CONTAINING APPLICATION/BROADSOFT AND APPLICATION/SSCC AND USED FOR SUPPLEMENTARY SERVICES

1. Supplementary services, performed using BROADSOFT algorithm

Device supports 'Call waiting' service that uses algorithm performed by BROADSOFT softswitch. To perform the service, you should configure flash event transfer to application/broadsoft.

When the second call is received be the gateway, INFO request is received with contents:
'play tone CallWaitingToneN', where N may have a value from 1 to 4. Having received this request, the gateway will play 'notification' tone to the subscriber.

To release a notification tone, INFO request is received from the softswitch with contents: **'stop CallWaitingTone'.**

To put the first call on hold and respond to the second call, the subscriber should press <flash> button, gateway transfers INFO request with contents: **'event flashhook'.**

2. Supplementary services, performed using HUAWEI algorithm

Device supports 'Call waiting', 'Call transfer', and '3-way conference' services that use algorithm performed by HUAWEI softswitch. To perform these services, you should configure flash event transfer to application/sscc.

When the second call is received be the gateway, INFO request is received with contents:
tone-type=beep; beep-duration=X; beep-gap=Y; beep-times=Z. Having received this request, the gateway will play 'notification' tone to the subscriber with parameters: X—ring duration, Y—pause duration, Z—number of rings.

Other tones processed by the gateway are:

- **tone-type=busy** – 'busy' tone playback
- **tone-type=ringback** - 'ringback' tone playback
- **tone-type=specialdial** – 'PBX response' tone playback. Along with this tone, the softswitch sends 'dial-timer=N' parameter, that defines the dialling timeout from the gateway side. If N=0, the dialling timeout is unlimited. Used in order to dial the second subscriber number or code for the respective action execution (for example, 2—switch between subscribers, 3—conference.) If timeout is non-zero, when it passes, the gateway will transfer an additional INFO request containing all dialled digits during this timeout.

To put the first call on hold (to perform the second call or respond to the second call), the subscriber should press <FLASH> button, gateway transfers INFO request with contents: **'event flashhook'.**

APPENDIX L. HELP ON TIMEZONES

Date line (UTC-12) Baker Island,Howland Island PST12 USA/Minor Outlying Islands

USA Canada (UTC-10) Hawaii Time HST10 Pacific/Honolulu
USA Canada (UTC-9) Alaska Time AKST9AKDT,M3.2.0,M11.1.0 America/Anchorage
USA Canada (UTC-8) Pacific Time PST8PDT,M3.2.0,M11.1.0 America/Los_Angeles
USA Canada (UTC-7) Mountain Time MST7MDT,M3.2.0,M11.1.0 America/Denver
USA Canada (UTC-7) Mountain Time (Arizona, no DST) MST7 America/Phoenix
USA Canada (UTC-6) Central Time CST6CDT,M3.2.0,M11.1.0 America/Chicago
USA Canada (UTC-5) Eastern Time EST5EDT,M3.2.0,M11.1.0 America/New_York

Atlantic (UTC-4) Bermuda AST4ADT,M3.2.0,M11.1.0 Atlantic/Bermuda

Central and South America (UTC-3) Argentina ART3 America/Argentina/Buenos_Aires
Central and South America (UTC-3) Sao Paulo,Brazil BRT3BRST,M11.1.0/0,M2.5.0/0 America/Sao_Paulo

Europe (UTC+0) GMT0 GMT0 GMT0
Europe (UTC+0) Dublin,Ireland GMT0IST,M3.5.0/1,M10.5.0 Europe/Dublin
Europe (UTC+0) Lisbon,Portugal WET0WEST,M3.5.0/1,M10.5.0 Europe/Lisbon
Europe (UTC+0) London,GreatBritain GMT0BST,M3.5.0/1,M10.5.0 Europe/London

Europe (UTC+1) Amsterdam,Netherlands CET-1CEST,M3.5.0,M10.5.0/3 Europe/Amsterdam
Europe (UTC+1) Berlin,Germany CET-1CEST,M3.5.0,M10.5.0/3 Europe/Berlin
Europe (UTC+1) Brussels,Belgium CET-1CEST,M3.5.0,M10.5.0/3 Europe/Brussels
Europe (UTC+1) Bratislava,Slovakia CET-1CEST,M3.5.0,M10.5.0/3 Europe/Bratislava
Europe (UTC+1) Budapest,Hungary CET-1CEST,M3.5.0,M10.5.0/3 Europe/Budapest
Europe (UTC+1) Copenhagen,Denmark CET-1CEST,M3.5.0,M10.5.0/3 Europe/Copenhagen
Europe (UTC+1) Madrid,Spain CET-1CEST,M3.5.0,M10.5.0/3 Europe/Madrid
Europe (UTC+1) Oslo,Norway CET-1CEST,M3.5.0,M10.5.0/3 Europe/Oslo
Europe (UTC+1) Paris,France CET-1CEST,M3.5.0,M10.5.0/3 Europe/Paris
Europe (UTC+1) Prague,CzechRepublic CET-1CEST,M3.5.0,M10.5.0/3 Europe/Prague
Europe (UTC+1) Roma,Italy CET-1CEST,M3.5.0,M10.5.0/3 Europe/Rome
Europe (UTC+1) Zurich,Switzerland CET-1CEST,M3.5.0,M10.5.0/3 Europe/Zurich
Europe (UTC+1) Stockholm,Sweden CET-1CEST,M3.5.0,M10.5.0/3 Europe/Stockholm

Europe (UTC+2) Helsinki,Finland EET-2EEST,M3.5.0/3,M10.5.0/4 Europe/Helsinki
Europe (UTC+2) Kyiv,Ukraine EET-2EEST,M3.5.0/3,M10.5.0/4 Europe/Kiev
Europe (UTC+2) Athens,Greece EET-2EEST,M3.5.0/3,M10.5.0/4 Europe/Athens

Asia (UTC+2) Amman EET-2EEST,M3.5.4/0,M10.5.5/1 Asia/Amman
Asia (UTC+2) Beirut EET-2EEST,M3.5.0/0,M10.5.0/0 Asia/Beirut
Asia (UTC+2) Damascus EET-2EEST,J91/0,J274/0 Asia/Damascus
Asia (UTC+2) Gaza EET-2EEST,J91/0,M10.3.5/0 Asia/Gaza
Asia (UTC+2) Jerusalem GMT-2 Asia/Jerusalem
Asia (UTC+2) Nicosia EET-2EEST,M3.5.0/3,M10.5.0/4 Asia/Nicosia

Asia (UTC+3) Aden AST-3 Asia/Aden
Asia (UTC+3) Baghdad AST-3ADT,J91/3,J274/4 Asia/Baghdad
Asia (UTC+3) Bahrain AST-3 Asia/Bahrain
Asia (UTC+3) Kuwait AST-3 Asia/Kuwait
Asia (UTC+3) Qatar AST-3 Asia/Qatar
Asia (UTC+3) Riyadh AST-3 Asia/Riyadh
Europe (UTC+3) Moscow, Russia MSK-3 Europe/Moscow

Asia (UTC+3:30) Tehran IRST-3:30 Asia/Tehran

Asia (UTC+4) Baku AZT-4AZST,M3.5.0/4,M10.5.0/5 Asia/Baku
Asia (UTC+4) Dubai GST-4 Asia/Dubai
Asia (UTC+4) Muscat GST-4 Asia/Muscat
Asia (UTC+4) Tbilisi GET-4 Asia/Tbilisi
Asia (UTC+4) Yerevan AMT-4AMST,M3.5.0,M10.5.0/3 Asia/Yerevan

Asia (UTC+4:30) Kabul AFT-4:30 Asia/Kabul

Asia (UTC+5) Aqtobe AQTT-5 Asia/Aqtobe
Asia (UTC+5) Ashgabat TMT-5 Asia/Ashgabat
Asia (UTC+5) Dushanbe TJT-5 Asia/Dushanbe
Asia (UTC+5) Karachi PKT-5 Asia/Karachi
Asia (UTC+5) Oral ORAT-5 Asia/Oral
Asia (UTC+5) Samarkand UZT-5 Asia/Samarkand
Asia (UTC+5) Tashkent UZT-5 Asia/Tashkent
Asia (UTC+5) Yekaterinburg YEKT-5 Asia/Yekaterinburg

Asia (UTC+5:30) Calcutta IST-5:30 Asia/Calcutta
Asia (UTC+5:30) Colombo IST-5:30 Asia/Colombo

Asia (UTC+6) Almaty ALMT-6 Asia/Almaty
Asia (UTC+6) Bishkek KGT-6 Asia/Bishkek
Asia (UTC+6) Dhaka BDT-6 Asia/Dhaka
Asia (UTC+6) Qyzylorda QYZT-6 Asia/Qyzylorda
Asia (UTC+6) Thimphu BTT-6 Asia/Thimphu
Asia (UTC+6) Omsk OMST-6 Asia/Omsk

Asia (UTC+7) Jakarta WIT-7 Asia/Jakarta
Asia (UTC+7) Bangkok ICT-7 Asia/Bangkok
Asia (UTC+7) Vientiane ICT-7 Asia/Vientiane
Asia (UTC+7) Phnom Penh ICT-7 Asia/Phnom_Penh
Asia (UTC+7) Novosibirsk NOVT-7 Asia/Novosibirsk
Asia (UTC+7) Krasnoyarsk Asia/Krasnoyarsk

Asia (UTC+8) Chongqing CST-8 Asia/Chongqing
Asia (UTC+8) Hong Kong HKT-8 Asia/Hong_Kong
Asia (UTC+8) Shanghai CST-8 Asia/Shanghai

Asia (UTC+8) Singapore SGT-8 Asia/Singapore
Asia (UTC+8) Urumqi CST-8 Asia/Urumqi
Asia (UTC+8) Taiwan CST-8 Asia/Taipei
Asia (UTC+8) Ulaanbaatar ULAT-8 Asia/Ulaanbaatar
Asia (UTC+8) Irkutsk Asia/Irkutsk

Australia (UTC+8) Perth WST-8 Australia/Perth Perth

Asia (UTC+9) Dili TLT-9 Asia/Dili
Asia (UTC+9) Jayapura EIT-9 Asia/Jayapura
Asia (UTC+9) Pyongyang KST-9 Asia/Pyongyang
Asia (UTC+9) Seoul KST-9 Asia/Seoul
Asia (UTC+9) Yakutsk YAKT-9 Asia/Yakutsk
Asia (UTC+9) Tokyo JST-9 Asia/Tokyo

Australia (UTC+9:30) Adelaide CST-9:30CST,M10.5.0,M3.5.0/3 Australia/Adelaide
Australia (UTC+9:30) Darwin CST-9:30 Australia/Darwin

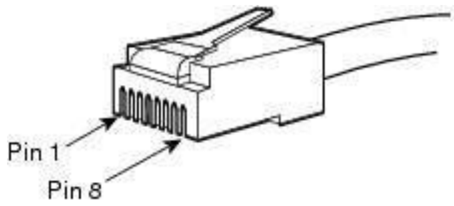
Australia (UTC+10) Brisbane EST-10 Australia/Brisbane
Australia (UTC+10) Melbourne,Canberra,Sydney EST-10EST,M10.5.0,M3.5.0/3 Australia/Melbourne
Australia (UTC+10) Hobart EST-10EST,M10.1.0,M3.5.0/3 Australia/Hobart

Asia (UTC+10) Vladivostok VLAST-10 Asia/Vladivostok
Asia (UTC+11) Magadan MAGT-11 Asia/Magadan
Asia (UTC+11) Srednekolymsk SRET-11 Asia/Srednekolymsk
Asia (UTC+11) Yuzhno-Sakhalinsk SAKT-11 Asia/Sakhalin
Australia (UTC+11) Tasmania AEDT-11 Australia/Tasmania
Asia (UTC+12) Anadyr ANAT-12 Asia/Anadyr
New Zeland (UTC+12) Auckland, Wellington NZST-12NZDT, M10.1.0, M3.3.0/3 Pacific/Auckland

APPENDIX M. CABLE CONNECTORS PIN DESIGNATION

Console port Console RJ-45 connector pin designations are listed in table above.

Table 17 – Console port Console RJ-45 connector pin designations

<table>
<tr><th>№ of pin</th><th>Purpose</th><th>Pin enumeration</th></tr>
<tr><td>1</td><td>Don't use</td><td rowspan="8">
</td></tr>
<tr><td>2</td><td>Don't use</td></tr>
<tr><td>3</td><td>TX</td></tr>
<tr><td>4</td><td>Don't use</td></tr>
<tr><td>5</td><td>GND</td></tr>
<tr><td>6</td><td>RX</td></tr>
<tr><td>7</td><td>Don't use</td></tr>
<tr><td>8</td><td>Don't use</td></tr>
</table>

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

https://eltex-co.com/support/

You are welcome to visit Eltex official website to get the relevant technical documentation and software:

Official website: **https://eltex-co.com/**
Download center: **https://eltex-co.com/support/downloads/**